

7 Factorization

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-10-20

Much like division, being able to express elements as a product of simpler elements distinguishes certain kinds of commutative rings.

7.0 Greatest Common Divisors

A greatest common divisor can be defined in any commutative ring.

7.0.1 Definition. Let a and b be nonzero elements in a commutative ring R . An element d in R is a *greatest common divisor* of a and b , denoted by $d := \gcd(a, b)$, if

(common divisor) the element d divides both a and b , and

(greatest) any element c in R , which divides both a and b , also divides d .

More pedantically, there exists elements p and q in R such that $a = dp$ and $b = dq$.

A greatest common divisor may not exist or may not be unique.

7.0.2 Example. We have $9 = (3)(3) = (2 + \sqrt{-5})(2 - \sqrt{-5})$ in the domain $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Both 3 and $2 + \sqrt{-5}$ divide 9, but neither divides the other. Thus, the elements 9 and $6 + 3\sqrt{-5}$ do not have a greatest common divisor in $\mathbb{Z}[\sqrt{-5}]$. $\diamond$

7.0.3 Example. In a field, any nonzero element is a unit and, thereby, divides any element. Ergo, for any pair of nonzero elements, any nonzero element is a greatest common divisor. $\diamond$

In a domain, we can understand all the greatest common divisors for a fixed pair of nonzero elements.

7.0.4 Lemma. Let d be a greatest common divisor for nonzero elements a and b in a domain R . An element e in R is also a greatest common divisor for a and b if and only if there exists a unit u in R such that $e = ud$.

When $R = \mathbb{Z}$, we typically impose uniqueness by requiring the greatest common divisor to be positive. When K is field and $R = K[x]$, we force uniqueness by requiring the greatest common divisor to be monic.

Proof. Suppose that e is a greatest common divisor for a and b . As e divides a and b , it follows that e divides d . Similarly, d divides a and b , so d divides e . Hence, there exists elements u and v in R such that $d = ue$ and $e = vd$. It follows that $d = ue = uvd$. Because R is a domain, we deduce that $1 = uv$.

Conversely, suppose there exists a unit u in R such that $e = ud$. Since d divides a , there exists x in R such that $a = xd = xu^{-1}e$, so e divides a . By symmetry, e also divides b . Assume that c divides a and b . Since d is a greatest common divisor for a and b , there exists w in R such that $d = wc$, so $e = uwc$. Thus, e is also a greatest common divisor for a and b . $\square$

Greatest common divisors exist in any principal ideal domain.

7.0.5 Theorem. For any nonzero elements a and b in a principal ideal domain R , there exists x and y in R such that $\gcd(a, b) = ax + by$. In particular, we have $\langle \gcd(a, b) \rangle = \langle a, b \rangle$.

The history of the equation $ax + by = \gcd(a, b)$ is more complicated and interesting than one might guess; see Granville (2024).

Proof. Consider the ideal $I := \langle a, b \rangle$. Since R is a principal ideal domain, there is a d in R such that $I = \langle d \rangle$, so $d = ax + by$ for some x and y in R . Both a and b are in I and I is generated by d , so d divides a and b . On the other hand, if an element c divides a and b , then c divides $ax + by = d$. We deduce that $d = \gcd(a, b)$.

Any generator for the ideal $\langle a, b \rangle$ is a greatest common divisor of a and b . Lemma 7.0.4 shows that, for any two greatest common divisors d and e , there exists a unit u in R such that $e = ud$ and $d = u^{-1}e$. Thus, we have $\langle e \rangle \subseteq \langle d \rangle$ and $\langle d \rangle \subseteq \langle e \rangle$, so $\langle d \rangle = \langle e \rangle$. $\square$

Greatest common divisors are computable in Euclidean domains.

7.0.6 Lemma. *Let a and b be nonzero elements in an Euclidean domain R . For any q and r in R such that $a = qb + r$ with $r \neq 0$ and $\nu(r) < \nu(b)$, we have $\gcd(a, b) = \gcd(b, r)$.*

Proof. Let $d := \gcd(a, b)$. As d divides a and b , this ring element divides $a - qb = r$. Moreover, any element c , dividing b and r , also divides $a = bq + r$. It follows that c divides d . We deduce that d is a greatest common divisor of b and r . $\square$

7.0.7 Algorithm (Extended Euclidean Algorithm).

Input: Let a and b be elements in a Euclidean domain R .

Output: Elements x and y in R such that $ax + by = \gcd(a, b)$.

Set $(r', r, s', s, t', t) := (a, b, 1, 0, 0, 1)$;

While $r \neq 0$ do

Find elements q and r'' in R such that

$$r' = qr + r'' \text{ where } r'' = 0 \text{ or } \nu(r'') < \nu(r);$$

Set $(r', r, s', s, t', t) := (r, r' - qr, s, s' - qs, t, t' - qt)$;

Return (s', t') .

Outline of proof. The remainders r produce a decreasing sequence $\nu(r)$ of nonnegative integers, so eventually one of the remainders must be zero. Thus, the while-loop must terminate. Lemma 7.0.6 gives $\gcd(a, b) = \gcd(r', r)$, and one verifies that the equations $r = sa + tb$ and $r' = s'a + t'b$ hold throughout. $\square$

7.0.8 Example. When $R = \mathbb{F}_3[x]$, $f = x^3 + 2x^2 + 2$, and $g = x^2 + 2x + 1$, Algorithm 7.0.7 gives

r'	r	s'	s	t'	t	q
$x^3 + 2x^2 + 2$	$x^2 + 2x + 1$	1	0	0	1	x
$x^2 + 2x + 1$	$2x + 2$	0	1	1	$2x$	$2x + 2$
$2x + 2$	0	1	$x + 1$	$2x$	$2x^2 + 2x + 1$	

We have $(1)(x^3 + 2x^2 + 2) + (2x)(x^2 + 2x + 1) = 2x + 2 = \gcd(f, g)$. $\diamond$

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*.

Representing the local variables in the matrix $\begin{bmatrix} r' & s' & t' \\ r & s & t \end{bmatrix}$, the body of the loop performs two elementary row operations: adding $-q$ times the second row to the first row, and then swapping the two rows.

Table 7.1: Values of the local variables when using Algorithm 7.0.7 to compute $\gcd(x^3 + 2x^2 + 2, x^2 + 2x + 1)$

7.0.9 Example. When $a = 1254$, and $b = 1110$, Algorithm 7.0.7 gives

r'	r	s'	s	t'	t	q
1254	1110	1	0	0	1	1
1110	144	0	1	1	-1	7
144	102	1	-7	-1	8	1
102	42	-7	8	8	-9	2
42	18	8	-23	-9	26	2
18	6	-23	54	26	-61	3
6	0	54	-185	-61	209	

Table 7.2: Values of the local variables when using Algorithm 7.0.7 to compute $\gcd(1254, 1110)$

We deduce that $(54)(1254) + (-61)(1110) = 6 = \gcd(1254, 1110)$. $\diamond$

7.1 Unique Factorization

Commutative rings that enjoy some analogue of the fundamental theorem of arithmetic are particularly interesting.

7.1.1 Definition. A ring element a is *irreducible* if a is nonzero, a is not a unit, and the relation $a = bc$ implies that either b or c is a unit.

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

$$4 = (2)(2) = (2)(2)(2)(2) = (2)(2)(2)(2)(2)(2) = \dots \quad \diamond$$

By avoiding zerodivisors, being prime implies being irreducible.

7.1.3 Lemma. Let f be an element in a domain R . When the principal ideal $\langle f \rangle$ is prime, the element f is irreducible.

Proof. Suppose that $f = gh$ for some elements g and h in R . As the ideal $\langle f \rangle$ is prime, Proposition 5.3.8 shows that f divides either g or h . We may assume that f divides g , so there exists q in R such that $g = qf$. It follows that $f = gh = qfh$. Since R is a domain, we deduce that $1 = qh$, so h is a unit and f is irreducible. $\square$

7.1.4 Example. Consider the subring $\mathbb{C}[x^2, x^3] \subset \mathbb{C}[x]$. Comparing degrees, we see that 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 . $\diamond$

7.1.5 Example. We claim that the element 2 in $\mathbb{Z}[\sqrt{-3}]$ is irreducible but not prime. Suppose that $2 = (a + b\sqrt{-3})(c + d\sqrt{-3})$ for some integers a, b, c , and d . It follows that $2 = (a - b\sqrt{-3})(c - d\sqrt{-3})$ and $4 = (a^2 + 3b^2)(c^2 + 3d^2)$. As the equation $x^2 + 3y^2 = 2$ has no integral solutions, we see 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 element 2 is not

a unit. We deduce 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. $\diamond$

7.1.6 Proposition. *For any element f in a principal ideal domain R , the following are equivalent:*

- a. *the element f is irreducible,*
- b. *the ideal $\langle f \rangle$ is a nonzero maximal ideal,*
- c. *the ideal $\langle f \rangle$ is a nonzero prime ideal.*

Proof.

$a \Rightarrow b$: Suppose that $\langle f \rangle \subseteq \langle g \rangle$ for some g in R . Equivalently, there exists h in R such that $f = gh$. Since f is irreducible, either g or h is a unit, so $\langle f \rangle = \langle g \rangle$ or $\langle g \rangle = R$. Because every ideal is principal, we see that $\langle f \rangle$ is maximal.

$b \Rightarrow c$: Every nonzero maximal ideal is a nonzero prime ideal.

$c \Rightarrow a$: Follows from Lemma 7.1.3. $\square$

7.1.7 Definition. A domain R is a *unique factorization domain* if (factorization) every nonzero f in R can be written in the form

$f = u \prod_{j=1}^m g_j^{e_j}$ where u is a unit, each element g_j is irreducible, and each e_j is a positive integer;

(uniqueness) when $f = u \prod_{j=1}^m g_j^{e_j} = v \prod_{j=1}^n h_j^{e_j}$ are two such factorizations, we have $m = n$ and $g_j = c_j h_{\sigma(j)}$ for some units c_j in R and some permutation $\sigma \in \mathfrak{S}_m$.

7.1.8 Proposition. *Let R be a 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 ideal $\langle f \rangle$ is prime.*

Proof. Suppose that R is a unique factorization domain. Given g and h in R such that $gh \in \langle f \rangle$, there exists a q in R such that $gh = qf$. Factor g , h , and q into irreducibles. The uniqueness of factorization implies that the irreducible uf , for some unit u in R appears in the factorization of gh . This element is a factor of g or h , so $g \in \langle f \rangle$ or $h \in \langle f \rangle$. Proposition 5.3.8 shows the principal ideal $\langle f \rangle$ is prime.

Conversely, suppose that any 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 g_j and h_k are irreducible elements in R for all $1 \leq j \leq m$ and $1 \leq k \leq n$. We proceed, by induction on $\max\{m, n\} \geq 1$, to show that $m = n$ and $g_j = c_j h_{\sigma(j)}$ for some units c_j and $\sigma \in \mathfrak{S}_m$. The base step $\max\{m, n\} = 1$ has $g_1 = h_1$, so the claim is trivial. For the inductive step, the given equation shows that g_m divides $h_1 h_2 \cdots h_n$. As the ideal $\langle g_m \rangle$ is prime, there exists $1 \leq k \leq n$ such that 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 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 shows that $m-1 = n-1$ and $g_j = c_j h_{\sigma(j)}$ for some units c_j in R , for all $2 \leq j \leq m-1$, and some $\sigma \in \mathfrak{S}_{m-1}$. $\square$

7.2 Noetherian Rings

An exceptionally important class of rings is named in honour of Emmy Noether.

7.2.1 Definition. A commutative ring R is *noetherian* if any weakly ascending chain of ideals in R is eventually constant. Equivalently, for any sequence of nested ideals

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_{k-1} \subseteq I_k \subseteq I_{k+1} \subseteq \cdots,$$

there exists a nonnegative integer m such that $I_m = I_{m+1} = \cdots$.

7.2.2 Example. Having only two ideals, any field is noetherian. $\diamond$

7.2.3 Example. The polynomial ring $\mathbb{Q}[x_0, x_1, x_2, \dots]$ with infinitely many variables is not noetherian because there exists an increasing sequence of distinct ideals $\langle x_0 \rangle \subset \langle x_0, x_1 \rangle \subset \langle x_0, x_1, x_2 \rangle \subset \cdots$. $\diamond$

7.2.4 Lemma. Let R be ring. For any ascending chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ of ideals in R , the union $I = \bigcup_{j=0}^{\infty} I_j$ is an ideal in R . Moreover, when I is finitely generated, there exists a nonnegative integer m such that $I = I_m$.

Proof. Let f and g be elements in the union I and let r be an element in R . There exists nonnegative integers i and j such that $f \in I_i$ and $g \in I_j$. We may assume $j \geq i$. As $I_i \subseteq I_j$, we deduce that $f \in I_j$. Since I_j is an ideal, it follows that $rf + g \in I_j \subseteq I$, so I is an ideal.

Suppose that $I = \langle f_1, f_2, \dots, f_n \rangle$ for some $f_1, f_2, \dots, f_n$ in R . For any index i satisfying $1 \leq i \leq n$, there is a nonnegative integer $\ell(i)$ such that $f_i \in I_{\ell(i)}$. Setting $m := \max\{\ell(1), \ell(2), \dots, \ell(n)\}$ gives $f_i \in I_m$ for all $1 \leq i \leq n$. We obtain $I = \langle f_1, f_2, \dots, f_n \rangle \subseteq I_m \subseteq I$, so $I = I_m$. $\square$

7.2.5 Theorem. A commutative ring R is noetherian if and only if every ideal in R is finitely generated.

Proof. Suppose that the ring R is noetherian. Let I be an ideal in R . If $I = \langle 0 \rangle$, then it is finitely generated. Otherwise, pick a nonzero element f_0 in I . If $I = \langle f_0 \rangle$, then I is finitely generated. Otherwise, pick an element f_1 in $I \setminus \langle f_0 \rangle$. If $I = \langle f_0, f_1 \rangle$ then I is again finitely generated. Otherwise, continue this process. Failing to produce a finite set of generators for I would give the strictly ascending chain $\langle f_0 \rangle \subset \langle f_0, f_1 \rangle \subset \langle f_0, f_1, f_2 \rangle \subset \cdots$, contradicting noetherianity.

Conversely, suppose that every ideal in R is finitely generated. Consider an ascending chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ of ideals in R and the union $I := \bigcup_{j=0}^{\infty} I_j$. Lemma 7.2.4 shows that I is ideal. Every ideal in R is finitely generated, so Lemma 7.2.4 also shows that there is a nonnegative integer m such that $I = I_m = I_{m+1} = \cdots$. $\square$

7.2.6 Corollary. Every principal ideal domain is noetherian. $\square$

The ascending chain condition was first studied by Emmy Noether (1921), but the nomenclature was introduced by Claude Chevalley (1943).

For any field K , the rings $\mathbb{Z}$, $K[x]$, and $K[[x]]$ are noetherian.

7.2.7 Proposition. *Every principal ideal domain is a unique factorization domain.*

Proof. Combining Proposition 7.1.6 and Proposition 7.1.8, it enough to prove that every nonzero nonunit in a principal ideal domain is a product of irreducibles. Suppose that R is principal ideal domain and the nonzero nonunit f in R is not a product of irreducibles. As f is not irreducible, it follows that $f = gh$ where neither g and h are units. Were both g and h a product of irreducibles, so would f be. Hence, at least one factor, say g , is not irreducible. We have $\langle f \rangle \subset \langle g \rangle$. Repeating this process, we produce an ascending chain of ideals that is not eventually constant. However, Corollary 7.2.6 shows that R is noetherian which is a contradiction. $\square$

7.2.8 Corollary (Fundamental theorem of arithmetic). *Any nonzero integer m can be written as $m = u p_1 p_2 \cdots p_\ell$ where $u = \pm 1$, each p_j is prime integer, and $\ell \geq 0$. This expression is unique except for the ordering of the primes.* $\square$

7.2.9 Hilbert Basis Theorem. *For any noetherian commutative ring R , the polynomial ring $R[x]$ is also noetherian.*

The initial version of this theorem was proved by David Hilbert (1890) in his seminal article on invariant theory.

Proof. Let J be an ideal in $R[x]$. We claim that J is finitely generated. For all nonnegative integers n , let I_n be the set of all leading coefficients of polynomials of degree n in J . From the definition of addition and multiplication in $R[x]$, we see that I_n is an ideal in R . Observe that $I_n \subseteq I_{n+1}$ because the membership $f = ax^n + \cdots \in I_n$ implies $xf = ax^{n+1} + \cdots \in I_{n+1}$. As R is noetherian, there exists a nonnegative integer m such that $I_m = I_{m+1} = \cdots$ and, for all $0 \leq i \leq m$, each $I_i = \langle a_{i,1}, a_{i,2}, \dots, a_{i,k_i} \rangle$ for some positive integer k_i and some elements $a_{i,1}, a_{i,2}, \dots, a_{i,k_i}$ in R . Choose elements $f_{i,j} \in J$ such that the leading coefficient of $f_{i,j}$ is $a_{i,j}$ for all $0 \leq i \leq m$ and $1 \leq j \leq k_i$. We claim that J is generated these polynomials.

Suppose there is a polynomial g in J of minimal degree n such that $g \notin J' := \langle f_{i,j} \mid 0 \leq i \leq m \text{ and } 1 \leq j \leq k_i \rangle$. Set $\ell := \min(m, n)$. The definition of the ideal I_ℓ implies that the leading coefficient of g has the form $r_1 a_{\ell,1} + r_2 a_{\ell,2} + \cdots + r_{k_\ell} a_{\ell,k_\ell}$ for some $r_1, r_2, \dots, r_{k_\ell}$ in R . It follows that $h := g - x^{n-\ell}(r_1 f_{\ell,1} + r_2 f_{\ell,2} + \cdots + r_{k_\ell} f_{\ell,k_\ell})$ has degree less than n . Our choice of g guarantees that $h \in J'$. However, this implies that $g = h + x^{n-\ell}(r_1 f_{\ell,1} + r_2 f_{\ell,2} + \cdots + r_{k_\ell} f_{\ell,k_\ell})$ belongs to J' , which contradicts our supposition. $\square$

7.2.10 Corollary. *For any nonnegative integer n and any noetherian ring R , the polynomial ring $R[x_1, x_2, \dots, x_n]$ is also noetherian.* $\square$

7.3 Factoring polynomials

We showcase the basic features of polynomial factorization.

7.3.1 Definition. Let R be a unique factorization domain and let

$$f := a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \in R[x].$$

The **content** of f is defined to be $\text{cont}(f) := \gcd(a_m, a_{m-1}, \dots, a_0)$. The polynomial f is **primitive** if $\text{cont}(f) = 1$.

To define the content, we need to know that greatest common divisors exist. The greatest common divisor, if it exists, is unique only up to multiplication by a unit. Hence, the content really is an equivalence class.

7.3.2 Gauss Lemma. Let R be a unique factorization domain. For any polynomials f and g in $R[x]$, we have $\text{cont}(fg) = \text{cont}(f) \text{cont}(g)$. In particular, if f and g are primitive, then the product fg also is.

Proof. Write $f = \text{cont}(f) f^\circ$ and $g = \text{cont}(g) g^\circ$ where f° and g° are primitive polynomials. Since $fg = \text{cont}(f) \text{cont}(g) f^\circ g^\circ$, it suffices to verify that $f^\circ g^\circ$ is primitive. Set $f^\circ = a_0 + a_1 x + \cdots + a_m x^m$ and $g^\circ = b_0 + b_1 x + \cdots + b_n x^n$ where $a_0, a_1, \dots, a_m$ and $b_0, b_1, \dots, b_n$ are in R . Suppose that the coefficients of $f^\circ g^\circ$ have a common divisor d which is not a unit. If p is a prime divisor of d , then p must divide all the coefficients of $f^\circ g^\circ$. As f° and g° are primitive, p does not divide all the coefficients of f° or g° . Let a_r be the first coefficient of f° not divisible by p and let b_s be the first coefficient of g° not divisible by p . Consider the coefficient of x^{r+s} in $f^\circ g^\circ$; it has the form

$$a_r b_s + (a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \cdots) + (a_{r-1} b_{s+1} + a_{r-2} b_{s+2} + \cdots).$$

By hypothesis p divides this sum. Moreover, all the terms in the first parenthesis are divisible by p (because p divides b_j for all $j < s$) and all terms in the second parenthesis are divisible by p (because p divides a_i for all $i < r$). It follows that p divides $a_r b_s$. As p is prime, p divides either a_r or b_s contrary to our choice of a_r and b_s . This contradiction shows that no prime divides all the coefficients of $f^\circ g^\circ$ and hence $f^\circ g^\circ$ is primitive. $\square$

Replacing the coefficient domain by its field of fractions does not alter irreducibility.

7.3.3 Lemma. Let R be a unique factorization domain and let K be its field of fractions.

For any nonzero polynomial f in $K[x]$, we have $f = c f^\circ$ where c in K and f° is a primitive polynomial in $R[x]$. This factorization is unique up to multiplication by a unit of R .

Let f be a polynomial in $R[x]$ having positive degree. If f is irreducible in $R[x]$, then f is irreducible in $K[x]$.

Proof. Given a common denominator d for the nonzero coefficients of f , we obtain $f = (1/d) \tilde{f}$ where $\tilde{f}$ in $R[x]$. Setting $c := \text{cont}(\tilde{f})/d$,

it follows that $f = c f^\circ$ where f° is primitive in $R[x]$. Suppose that $f = (a/b)g$ where a/b in K and g in $R[x]$ is primitive. It follows that $a d g = b \text{cont}(f) f^\circ$. Taking the content of both sides yields $u a d = b \text{cont}(f)$ for some unit u in R . We deduce that $u g = f^\circ$.

Since $\text{cont}(f)$ divides f , the polynomial f is primitive in $R[x]$. Suppose that f is reducible in $K[x]$. It follows that $f = g_1 g_2$ where g_j in $K[x]$ and $\deg(g_j) > 0$ for all $1 \leq j \leq 2$. The first part of this lemma implies $g_j = c_j h_j$ for some c_j in K and some primitive h_j in $R[x]$. Hence, $f = c_1 c_2 h_1 h_2$ and the product $h_1 h_2$ is primitive by Lemma 7.3.2. The first part of this lemma implies f and $h_1 h_2$ differ by multiplication by a unit of R , which contradicts the irreducibility of f in $R[x]$. $\square$

7.3.4 Theorem. *For any unique factorization domain R , the polynomial ring $R[x]$ is also a unique factorization domain.*

Proof. Let K be the field of fractions for R . Consider a nonzero f in $R[x]$. As $K[x]$ is a unique factorization domain, we can write $f = p_1 p_2 \cdots p_r$ where p_j in $K[x]$ is irreducible for all $1 \leq i \leq r$. Lemma 7.3.3 establishes that $p_j = c_j q_j$ for some c_j in K and some primitive q_j in $R[x]$. Hence, we see that $f = c q_1 q_2 \cdots q_r$ where $c = \prod_j c_j \in K$. Write $c = a/b$ for some a and b in R . Taking contents, Lemma 7.3.2 gives $\text{q cont}(b f) = \text{cont}(a q_1 q_2 \cdots q_r) = a$. Thus, we obtain $b \text{cont}(f) = a$ so b divides a and $\text{cont}(f) = c \in R$. Since each q_j is irreducible in $K[x]$, it is irreducible in $R[x]$. The ring R is a unique factorization domain, so we have $c = u d_1 d_2 \cdots d_s$ where each d_i is irreducible in R and u is a unit in R . It follows that $f = u d_1 d_2 \cdots d_s q_1 q_2 \cdots q_r$ is a factorization of f into a product of irreducible elements in $R[x]$.

It remains to check uniqueness. Suppose that we have a second factorization: $f = u' d'_1 d'_2 \cdots d'_t q'_1 q'_2 \cdots q'_k$ where each q'_j in $R[x]$ is primitive and d'_j in R is irreducible. Since this is also a factorization in $K[x]$ and the factorization there is unique, it follows that $r = k$ and $q'_j = q_j$ (up to units and reordering). If primitive polynomials differ by a unit in $K[x]$, then they also differ by a unit in $R[x]$. Lastly, we have $\text{cont}(f) = u' d'_1 d'_2 \cdots d'_t = u d_1 d_2 \cdots d_s$ so $s = t$ and $d'_j = d_j$ (up to units and reordering). $\square$

7.3.5 Example. The ring $\mathbb{Z}[x]$ is a unique factorization domain, but not a principal ideal domain. $\diamond$

7.3.6 Corollary. *For any nonnegative integer n and any unique factorization domain R , the polynomial ring $R[x_1, x_2, \dots, x_n]$ is also a unique factorization domain.*

Proof. We proceed by induction on n . When $n = 0$, the assertion is

trivial. Since Theorem 7.3.4 establishes the induction step, the claim follows. $\square$

7.4 Exercises

7.4.1 Problem. Euclid proves that there are infinitely many prime integers in the following way: if $p_1, p_2, \dots, p_k$ are prime numbers, then any prime factor of the integer $1 + p_1 p_2 \cdots p_k$ must be different from p_i for all $1 \leq i \leq k$.

- i. Adapt this argument to demonstrate that, for any field K , there are infinitely many monic irreducible polynomials in $K[x]$.
- ii. Explain why the argument fails for the formal power series ring $K[[x]]$ over a field K .
- iii. Adapt this argument to show that the set of prime integers of the form $4n - 1$ is infinite.

7.4.2 Problem. Let R be a principal ideal domain and let K be its field of fractions.

- i. Suppose $R = \mathbb{Z}$. Write $r = 7/24 \in \mathbb{Q}$ in the form $r = a/8 + b/3$.
- ii. Consider $g := pq$ in R where p and q are relatively prime. Prove that every fraction $f/g \in K$ can be written in the form

$$\frac{f}{g} = \frac{a}{q} + \frac{b}{p}$$

for some a and b in R .

- iii. Let $g := p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ in R be the factorization of the element g into irreducible elements $p_1, p_2, \dots, p_k$ such that the relation $p_i = u p_j$ for some unit u in R implies that $i = j$. Prove that every fraction $r = f/g \in K$ can be written in the form

$$r = \sum_{i=1}^k \frac{h_i}{p_i^{m_i}}$$

for some h_i in R for all $1 \leq i \leq k$.

7.4.3 Problem. 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.

7.4.4 Problem. 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 $N: \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{Z}$ defined, for any integers a and b , by $N(a + b\sqrt{-5}) = a^2 + 5b^2$ 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 $\mathbb{Z}[\sqrt{-5}]$.

Bibliography

- Arnold, Vladimir I. 1998. *On teaching mathematics*, Russian Math. Surveys 53, no. 1, 229–236.
- Cayley, Arthur. 1854. *On the theory of groups, as depending on the symbolic equation $\theta^n = 1$* , Phil. Mag. (4) 42, no. 7, 40–47.
- . 1893. *Note on the so-called quotient G/H in the theory of groups*, Amer. J. Math. 15, no. 4, 387–388.
- Cauchy, Augustin Louis. 1844. *Mémoire sur les arrangements que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre*, Exercices d'analyse et de physique mathématique 3, 151–252.
- Chevalley, Claude. 1943. *On the theory of local rings*, Ann. of Math. (2) 44, 690–708.
- Cox, David A. 2011. *Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first*, Amer. Math. Monthly 118, no. 1, 3–21.
- Dedekind, Richard. 1871. *Supplement X*, in *Vorlesungen über Zahlentheorie* by Peter Gustav Lejeune Dirichlet, Braunschweig: Vieweg.
- de Groot, Johannes. 1959. *Groups represented by homeomorphism groups*, Math. Ann. 138, 80–102.
- Dyck, Walther. 1882. *Gruppentheoretische Studien*, Math. Ann. 20, no. 1, 1–44.
- Eisenstein, Gotthold. 1850. *Über die Irreducibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, J. Reine Angew. Math. 39, 160–179.
- Frucht, Roberto. 1939. *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*, Compositio Math. 6, 239–250.
- Galois, Évariste. 1846. *Œuvres Mathématiques*, J. Math. Pures Appl. XI, 381–444.
- Granville, Andrew. 2024. *It is not "Bézout's identity"*. available at [arXiv:2406.15642](https://arxiv.org/abs/2406.15642) [math.HO].
- Hilbert, David. 1890. *Über die Theorie der algebraischen Formen*, Mathematische Annalen 36, 473–534.
- . 1897. *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung 4, no. I–XVIII, 175–546.
- Hodges, Wilfrid. 1979. *Krull implies Zorn*, J. London Math. Soc. (2) 19, no. 2, 285–287.
- Jordan, Camille. 1861. *Mémoire sur le nombre des valeurs des fonctions*, Journal de l'École polytechnique 22, 113–194.
- . 1870. *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris. 667 p.
- Klein, Felix. 1884. *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Teubner, Leipzig.
- Krull, Wolfgang. 1929. *Idealtheorie in Ringen ohne Endlichkeitsbedingung*, Math. Ann. 101, no. 1, 729–744.
- Lagrange, Joseph-Louis. 1771. *Suite des réflexions sur la résolution algébrique des équations. Section troisième. De la résolution des équations du cinquième degré & des degrés ultérieurs*, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin 5, no. 4, 138–254.
- . 1795. *Leçon Cinquième. Sur l'usage des courbes dans la solution des problèmes*, Leçons Élémentaires sur les Mathématiques. Republished in Serret, Joseph-Alfred, ed. (1877). *Oeuvres de Lagrange*. Vol. 7. Gauthier-Villars. pp. 271–287.
- Miller, George Abram. 1910. *On a method due to Galois*, The Quarterly Journal of Pure and Applied Mathematics 41, 382–384.
- Möbius, August F. 1832. *Über eine besondere Art von Umkehrung der Reihen*, J. Reine Angew. Math. 9, 105–123.
- Noether, Emmy. 1921. *Idealtheorie in Ringbereichen*, Math. Ann. 83, no. 1-2, 24–66.
- . 1927. *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Ann. 96, no. 1, 26–61.
- Novikov, Pëtr Sergeevich. 1955. *Ob algoritmičeskoj nerazrešimosti problemy toždestva slov v teorii grupp*, Izdat. Akad. Nauk SSSR, Moscow. Trudy Mat. Inst. Steklov. no. 44.

- Poonen, Bjorn. 2019. *Why all rings should have a 1*, Math. Mag. 92, no. 1, 58–62.
- Sabidussi, Gert. 1960. *Graphs with given infinite group*, Monatsh. Math. 64, 64–67.
- Schönemann, Theodor. 1846. *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, J. Reine Angew. Math. 32, 93–105.
- Smith, Henry J. S. 1861. *On systems of linear indeterminate equations and congruences*, Philos. Trans. Roy. Soc. . 151, 293–32.
- Sylow, Ludwig. 1872. *Théorèmes sur les groupes de substitutions*, Math. Ann. 5, no. 4, 584–594.
- Waring, Edward. 1779. *Problems concerning interpolations*, Philosophical Transactions of the Royal Society 69, 59–67.
- Wielandt, Helmut. 1959. *Ein Beweis für die Existenz der Sylowgruppen*, Arch. Math. 10, no. 1, 401–402.
- Zorn, Max. 1935. *A remark on method in transfinite algebra*, Bull. Amer. Math. Soc. 41, no. 10, 667–670.