

6 Fractions and Division

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-10-03

Among the four basic arithmetic operations, division is uniquely and notably absent from the definition of a ring. As an explanation, the various ways of viewing fractions and division isolate different kinds of commutative rings.

6.0 Rings of Fractions

The procedure for constructing the rational numbers $\mathbb{Q}$ from the integers $\mathbb{Z}$ easily extends to any domain R . For any ordered pair (r, d) of elements in R where d is nonzero, the construction uses the relation: $(r, d) \equiv (r', d') \Leftrightarrow rd' - r'd = 0$. This works only when R is a domain, because this relation is transitive if and only if R has no zerodivisors. Nevertheless, it can be generalized as follows.

6.0.1 Definition. A subset D of a ring R is **multiplicative** if every finite product of elements in the set D belongs to D .

This is the same as saying that 1_R in D and the product of any pair of elements of D belongs to D .

6.0.2 Example. For any element f in R , the set of powers f^n , for all nonnegative integers n , is multiplicative. $\diamond$

6.0.3 Example. Let P be an ideal in a commutative ring R . For the complement $R \setminus P$ to be multiplicative, it is necessary and sufficient that P be prime ideal; see Proposition 5.3.8. $\diamond$

6.0.4 Example. The set of elements in a commutative ring R that are not zerodivisors is multiplicative. $\diamond$

6.0.5 Remark. The intersection of multiplicative subsets a ring is also multiplicative. The intersection of all multiplicative subsets containing a given set is the multiplicative set it generates.

The multiplicative set generated by a given subset consists of all the finite products of its elements.

6.0.6 Proposition. For any multiplicative subset D in a commutative ring R , there exists a commutative ring $R[D^{-1}]$ and a ring homomorphism $\eta: R \rightarrow R[D^{-1}]$ with the following properties:

(new units) The elements in the set $\eta(D)$ are units in $R[D^{-1}]$.

(universal) For any ring homomorphism $\psi: R \rightarrow S$ such that the elements in $\psi(D)$ are units in S , there exists a unique ring homomorphism $\hat{\psi}: R[D^{-1}] \rightarrow S$ such that $\psi = \hat{\psi} \circ \eta$.

We call $R[D^{-1}]$ the ring of fractions with demoninators in D .

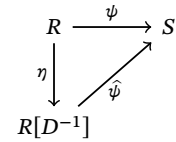


Figure 6.1: Commutative diagram arising from Proposition 6.0.6

Sketch of proof. Consider the set $R \times D$ with the relation:

$$(r, d) \equiv (s, e) \Leftrightarrow \text{there exists } c \text{ in } D \text{ such that } c(re - sd) = 0.$$

This relation is reflexive and symmetric. It is transitive because the equations $c(re - sd) = 0$ and $b(sf - te) = 0$ imply that

$$\begin{aligned} cbe(rf - td) &= bfcrc - cdbte + bfcsd - bfcsd \\ &= bf(c(re - sd)) + cd(b(sf - te)) = 0 \end{aligned}$$

and cbe is in D . Let $R[D^{-1}] := R \times D / \equiv$ be the quotient under this equivalence relation. For any ordered pair (r, d) , write r/d for the equivalent class containing the pair (r, d) in $R[D^{-1}]$.

Consider elements $f = r/d$ and $g = s/e$ in $R[D^{-1}]$. We claim that the equivalence classes $(re + sd)/de$ and $(rs)/(de)$ are independent of the chosen representatives for f and g . Given $f = r'/d'$, there exists c in D such that $c(rd' - r'd) = 0$ whence

$$\begin{aligned} c((re + sd)(d'e) - (r'e + sd')(de)) &= e^2(c(rd' - r'd)) = 0, \\ c((rs)(d'e) - (r's)(de)) &= es(c(rd' - r'd)) = 0. \end{aligned}$$

Thus, we have $(re + sd, de) \equiv (r'e + sd', d'e)$ and $(rs, de) \equiv (r's, d'e)$. Hence, the binary operations $(f, g) \mapsto f + g = (re + sd)/de$ and $(f, g) \mapsto fg = (rs)/(de)$ are well defined. One verifies that these two operations define a commutative ring structure on $R[D^{-1}]$: the additive identity is $0/1$ and the multiplicative identity is $1/1$. The map $\eta: R \rightarrow R[D^{-1}]$ defined, for any r in R , by $\eta(r) = r/1$ is a ring homomorphism, and the multiplicative inverse of $d/1$ is $1/d$.

Let $\psi: R \rightarrow S$ be a ring homomorphism such that the elements in $\psi(D)$ are units. Consider the map $\hat{\psi}: R[D^{-1}] \rightarrow S$ defined, for any r/d in $R[D^{-1}]$, by $\hat{\psi}(r/d) := \psi(r)(\psi(d))^{-1}$. When $r/d = r'/d'$, there is c in D such that $c(rd' - r'd) = 0$ so $\psi(c)(\psi(r)\psi(d') - \psi(r')\psi(d)) = 0$. Since the elements $\psi(c)$, $\psi(d)$, and $\psi(d')$ are units in S , it follows that $\psi(r)(\psi(d))^{-1} = \psi(r')(\psi(d'))^{-1}$, so the map $\hat{\psi}$ is well defined. One verifies that the map $\hat{\psi}$ is a ring homomorphism. By design, we have $\hat{\psi} \circ \eta = \psi$ and $\hat{\psi}$ is determined by this relation because

$$\begin{aligned} \hat{\psi}(r/d) &= \hat{\psi}((r/1)(1/d)) = \hat{\psi}(r/1)\hat{\psi}(1/d) = \psi(r)\hat{\psi}(1/d), \\ 1 &= \hat{\psi}(1/1) = \hat{\psi}(1/d)\hat{\psi}(d/1) = \hat{\psi}(1/d)\psi(d). \end{aligned}$$

□

6.0.7 Definition. When the multiplicative set D consists of all of the nonzerodivisors in the ring R , the commutative ring $R[D^{-1}]$ is the *total ring of fractions*. When R is a domain and $D = R \setminus \{0\}$, the ring $R[D^{-1}]$ is the *field of fractions* of R .

6.0.8 Example. Given an element f in R and $D := \{f^n \mid n \in \mathbb{N}\}$, we have $R_f := R[D^{-1}] \cong R[x]/\langle xf - 1 \rangle$. In particular, the Laurent polynomial ring $\mathbb{C}[x, x^{-1}]$ is the ring $\mathbb{C}[x]_x$. ◇

6.0.9 Definition. For any prime ideal P in commutative ring R , we write R_P for $R[(R \setminus P)^{-1}]$. The elements f/d with f in P and d not in P form an ideal P_P in R_P . Every element not in P_P is a unit in R_P . It follows that P_P is the unique maximal ideal in R_P . The process of passing from the ring R to the ring R_P is called *localization* at P .

6.0.10 Example. For the prime ideal $P = \langle 0 \rangle$ in $\mathbb{Z}$, we have $\mathbb{Z}_{(0)} = \mathbb{Q}$. The ring $\mathbb{C}(x) := \mathbb{C}[x]_{(0)}$ consists of all rational functions. ◇

Two elements in $R[D^{-1}]$ can always be written in the form f/d and g/d with f and g in R and d in D with the same denominator. For any f/d and g/e in $R[D^{-1}]$, we have $f/d = fe/de$ and $g/e = gd/de$.

The kernel of map $\eta: R \rightarrow R[D^{-1}]$ is the set f in R such that there exists c in D satisfying $cf = 0$. For the map η to be injective, it is necessary and sufficient that the set D contain no zerodivisor in R .

For the map η to be bijection, it is necessary and sufficient that every element d in D be a unit in R . The condition is necessary because $d/1$ is unit in $R[D^{-1}]$. It is sufficient because, for any d in D , the element d is unit in R and $f/d = fd^{-1}/1$ in $R[D^{-1}]$.

The map from the polynomial ring $R[x]$ to R_f is defined by $x \mapsto 1/f$.

For any field K , the field $K(x)$ of rational functions is $K[x]_{(0)}$. Every element in $K(x)$ can be written as f/g where f and g are polynomials in $K[x]$ and g is nonzero.

6.1 Univariate Polynomials

Unlike fractions, long division does not require a larger ring. As a prototype, we focus on the polynomial ring $R[x]$: a *polynomial* is a R -linear combination: $f := a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where $a_n, a_{n-1}, \dots, a_0$ are in the commutative ring R . In particular, the *monomials* x^j are independent over R , so $\sum_j a_j x^j = \sum_k b_k x^k$ if and only if $a_j = b_j$ for any nonnegative integer j .

More formally, an infinite sum with finitely many nonzero coefficients.

Ring homomorphisms on coefficient rings lift to the associated polynomial rings.

6.1.1 Proposition. *Let $\varphi: R \rightarrow S$ be a ring homomorphism. The map $\sum_j a_j x^j \mapsto \sum_j \varphi(a_j) x^j$ defines a ring homomorphism from $R[x]$ to $S[x]$. For any ring element b in S , there exists a unique ring homomorphism $\tilde{\varphi}: R[x] \rightarrow S$ that agrees with the map φ on constant polynomials*

Comment on the proof. The map $\tilde{\varphi}$ is a composition of the first ring homomorphism and the evaluation map $\text{ev}_b: S[x] \rightarrow S$ defined by $\text{ev}_b(f) := f(b)$. $\square$

Univariate polynomials come with an auxiliary function.

6.1.2 Definition. For any nonzero polynomial f in $R[x]$, the *degree* $\deg(f)$ is the largest integer k such that the coefficient a_k of the monomial x^k is nonzero. The nonzero element a_m in R satisfying $m = \deg(f)$ is the *leading coefficient* of the polynomial. A *monic* polynomial is one whose leading coefficient is 1_R .

6.1.3 Lemma. *Let f and g be two nonzero polynomials in $R[x]$.*

When $\deg(f) \neq \deg(g)$, the sum $f + g$ is nonzero and its degree is $\deg(f + g) = \max(\deg(f), \deg(g))$. Moreover, when $\deg(f) = \deg(g)$, the degree of the sum satisfies $\deg(f + g) \leq \deg(f)$.

We have $\deg(fg) \leq \deg(f) + \deg(g)$ and equality holds if the leading coefficient of f or g is a nonzerodivisor in R .

Proof. Let the leading coefficients of f and g be denoted by a_m and b_n respectively. Hence, the leading coefficient the sum $f + g$ is a_m when $m > n$ and b_n when $m < n$. When $m = n$, the coefficient of the monomial x^m in the sum $f + g$ is $a_m + b_n$ and the coefficients of all monomials of higher-degree are zero, so $\deg(f + g) \leq m$. The coefficient of the monomial x^{m+n} in the product fg is $a_m b_n$ and the coefficients of all monomials of higher-degree are zero, so $\deg(fg) \leq \deg(f) + \deg(g)$. $\square$

6.1.4 Proposition. *For any domain R , the polynomial ring $R[x]$ is also a domain and the units in $R[x]$ are the units in R .*

Proof. Suppose that f and g are nonzero polynomials in $R[x]$. Since $\deg(fg) = \deg(f) + \deg(g) \geq 0$, it follows that $fg \neq 0$. If $fg = 1$,

then we have $\deg(f) + \deg(g) = \deg(1) = 0$. Hence, f and g are both polynomials of degree 0 and, thereby, elements of R . $\square$

6.1.5 Theorem. *Let f and g be nonzero polynomials in $R[x]$ of degrees m and n respectively. Denote the leading coefficient of g by b_n and set $k := \max(m - n + 1, 0)$. There exist q and r in $R[x]$ such that*

$$b_n^k f = qg + r$$

where either $r = 0$ or $\deg(r) < n$. When b_n is a nonzerodivisor in R , the polynomials q and r are uniquely determined by these properties.

When b_n is a unit in R , one typically writes $f = q'g + r'$ where $q' := b_n^{-k}q$ and $r' := b_n^{-k}r$.

Proof. When $m < n$, it suffices to take $q = 0$ and $r = f$. When $m \geq n$, we proceed by induction on m . Write a_m for the leading coefficient of f and set $g := \sum_{j=0}^n b_j x^j$. Hence, we observe that $\deg(b_n^k f - b_n^{k-1} a_m x^{m-n} g) < m$. By the induction, there exists p and r in $R[x]$ such that $b_n^{k-1}(b_n f - a_m x^{m-n} g) = pg + r$ where $r = 0$ or $\deg(r) < n$. It follows that $b_n^k f = (b_n^{k-1} a_m x^{m-n} + p)g + r$ and $q := b_n^{k-1} a_m x^{m-n} + p$, proving existence.

To establish uniqueness, consider polynomials q, q', r , and r' in $R[x]$ such that $b_n^k f = qg + r = q'g + r'$ where $r = 0$ or $\deg(r) < m$ and $r' = 0$ or $\deg(r') < m$. It follows that $(q - q')g = (r' - r)$ where $r' - r = 0$ or $\deg(r' - r) < m$. As $m + \deg(q - q') = \deg(r' - r) < m$ is absurd, we conclude that $r = r'$ and $q = q'$. $\square$

6.1.6 Definition. A *root* of polynomial f in $R[x]$ is a ring element z in R such that $\text{ev}_z(f) = f(z) = 0$.

6.1.7 Corollary. *For any polynomial f in $R[x]$, there exists a polynomial q in $R[x]$ such that $f(x) = q(x)(x - z)$ if and only if we have $f(z) = 0$.*

Proof. Division implies that there exists polynomials q and r in $R[x]$ such that $f(x) = q(x)(x - z) + r(x)$ where $r = 0$ or $\deg(r) < 1$. In particular, the element r lies in the ring R . Evaluating at z yields $f(z) = q(z)(0) + r$, so we obtain $f(x) = q(x)(x - z) + f(z)$. $\square$

6.1.8 Proposition. *Let f be a polynomial in $R[x]$ and let z be an element in R . For any nonnegative integer m , the following are equivalent:*

- the polynomial f is divisible by $(x - z)^m$ but not by $(x - z)^{m+1}$;*
 - there exists g in $R[x]$ such that $f(x) = (x - z)^m g(x)$ and $g(z) \neq 0$.*
- Whenever $f \neq 0$, there exists a unique m satisfying these conditions.*

Proof.

$a \Rightarrow b$: Follows from Corollary 6.1.7.

$b \Rightarrow a$: If $f(x) = (x - z)^m g(x)$ where g does not have z as root, then f is divisible by $(x - z)^m$. Suppose that h in $R[x]$ exists satisfying $f(x) = (x - z)^{m+1} h(x)$. As $(x - z)^m$ is not a zerodivisor in $R[x]$, we would have $g(x) = (x - z)h(x)$ implying that $g(z) = 0$ which is contradiction. $\square$

6.2 Multiplicity of Roots

For the deepest insights, we need to count the roots of a polynomial correctly.

6.2.1 Definition. Let m be a nonnegative integer. For any f in $R[x]$, the element z in R is a root of **multiplicity** m if the polynomial f is divisible by $(x - z)^m$ but not $(x - z)^{m+1}$. A root of multiplicity 1 is a **simple** root and a root of multiplicity two is a **double** root.

6.2.2 Lemma. Let m and n be the multiplicities of the root z in R for the polynomials f and g in $R[x]$.

(sum) The sum $f + g$ has a root of multiplicity at least $\min(m, n)$ at z and is equal to $\min(m, n)$ whenever $m \neq n$.

(product) The product fg has a root of multiplicity at least $m + n$ at z and it is equal to $m + n$ whenever R is domain.

Sketch of proof. Set $f(x) = (x - z)^m p(x)$ and $g(x) = (x - z)^n q(x)$ where p and q in $R[x]$ satisfy $p(z) \neq 0 \neq q(z)$. When $m \leq n$, we have $f(x) + g(x) = (x - z)^m (p(x) + (x - z)^{n-m} q(x))$ and z is not a root of $p(x) + (x - z)^{n-m} q(x)$ when $m < n$. Similarly, we also have $f(x)g(x) = (x - z)^{m+n} p(x)q(x)$ and $p(z)q(z) \neq 0$ when R is a domain. $\square$

6.2.3 Proposition. Let R be a domain. For any nonzero f in $R[x]$ with distinct roots $z_1, z_2, \dots, z_\ell$ having multiplicities $m_1, m_2, \dots, m_\ell$, there is a polynomial g in $R[x]$ such that $z_1, z_2, \dots, z_\ell$ are not roots of g and

$$f(x) = (x - z_1)^{m_1} (x - z_2)^{m_2} \dots (x - z_\ell)^{m_\ell} g(x).$$

Proof. We proceed by induction on ℓ . The case $\ell = 1$ is covered by Proposition 6.1.8. Suppose that

$$f(x) = (x - z_1)^{m_1} (x - z_2)^{m_2} \dots (x - z_{\ell-1})^{m_{\ell-1}} h(x)$$

Since R is a domain and the root z_ℓ is distinct from $z_1, z_2, \dots, z_{\ell-1}$, it follows that z_ℓ is not a root of the polynomial

$$(x - z_1)^{m_1} (x - z_2)^{m_2} \dots (x - z_{\ell-1})^{m_{\ell-1}}.$$

The element z_ℓ is a root of multiplicity m_ℓ of the polynomial h and Proposition 6.1.8 yields $h(x) = (x - z_\ell)^{m_\ell} g(x)$ where $z_1, z_2, \dots, z_{\ell-1}$ are not roots of the polynomial g . $\square$

6.2.4 Corollary. Let R be a domain. For any nonzero f in $R[x]$ of degree m , the sum of multiplicities of all the roots of f is at most m . $\square$

To bound the number of roots via the degree, some hypothesis on the coefficient ring is necessary.

6.2.5 Example. Let n be a positive integer. Over the product ring $R = \prod_{j=0}^n \mathbb{Z}/\langle 2 \rangle$, all 2^{n+1} elements are roots of the polynomial $x^2 - x$ in $R[x]$, because addition and multiplication in coefficient ring R are defined pointwise and $x^2 - x = x(x - 1)$. $\diamond$

6.2.6 Corollary. *Let R be a domain. Consider nonzero polynomials f and g in $R[x]$. When there are distinct elements $z_0, z_1, \dots, z_m$ in R such that $f(z_i) = g(z_i)$ for all $0 \leq i \leq m$, we have $f = g$.*

Proof. The polynomial $h := f - g$ has degree at most m and has at least $m + 1$ roots, so $h = 0$. $\square$

6.2.7 Proposition. *Let $z_0, z_1, \dots, z_m$ be distinct elements in a field K . For any elements $b_0, b_1, \dots, b_m$ in K , there exists a unique polynomial f in $K[x]$ of degree at most m such that $f(z_j) = b_j$ for any $0 \leq j \leq m$.*

Proof. Uniqueness follows from Corollary 6.2.6. For each index j satisfying $0 \leq j \leq m$, consider the polynomial

$$g_j(x) := \prod_{k \neq j} \frac{(x - z_k)}{(z_j - z_k)}.$$

It follows that $\deg(g_j) = m$ and $g_j(z_k) = \delta_{j,k}$. Therefore, we may take $f(x) := \sum_{j=0}^m b_j g_j(x)$. $\square$

Although these polynomials are commonly named after [Joseph-Louis Lagrange \(1795\)](#), they were explicitly described in an earlier paper by [Edward Waring \(1779\)](#).

6.3 Euclidean Domains

Long division requires an appropriate auxiliary function.

6.3.1 Definition. A *Euclidean domain* is a domain R equipped with a function $\nu: R \setminus \{0\} \rightarrow \mathbb{N}$ such that, for any f in R and any g in $R \setminus \{0\}$, there exists elements q and r in R such that $f = qg + r$ and either $r = 0$ or $\nu(r) < \nu(g)$.

6.3.2 Example. The integers $\mathbb{Z}$ form a Euclidean domain where the function $\nu: \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ is defined, for any m in $\mathbb{Z}$, by $\nu(m) := |m|$. To see this, fix integers m and n . Consider all nonnegative integers of the form $m - jn$ where j is also an integer. Define r to be the smallest nonnegative integer of the form $m - jn$ and define q to be the integer j occurring in the expression $r = m - jn$. We conclude that $m = qn + r$ where either $r = 0$ or $r = |r| < |n|$. $\diamond$

6.3.3 Example. For any field K , the polynomial ring $K[x]$ forms a Euclidean domain where the function $\nu: K[x] \setminus \{0\} \rightarrow \mathbb{N}$ is defined, for any polynomial f in $K[x]$, by $\nu(f) := \deg(f)$. $\diamond$

6.3.4 Example. For any field K , the power series ring $K[[x]]$ is a Euclidean domain where the function $\nu: K[[x]] \setminus \{0\} \rightarrow \mathbb{N}$ is defined, for any f in $K[[x]]$, by $\nu(f) = \text{ord}(f)$ and

$$\text{ord}(f) := \min(k \mid a_k \neq 0 \text{ where } f = \sum_{k \geq 0} a_k x^k).$$

When $m = \text{ord}(f) < \text{ord}(g) = n$, we have $f = 0g + f$. Otherwise $m \geq n$, we have $f = x^m p$ and $g = x^n q$ where p and q in $K[[x]]$ are units, so $f = x^{m-n} p q^{-1} g + 0$. $\diamond$

6.3.5 Example. We claim that the ring $\mathbb{Z}[i]$ is a Euclidean domain where $\nu: \mathbb{Z}[i] \rightarrow \mathbb{N}$ is defined by $\nu(a + bi) := a^2 + b^2$.

Geometric Reasoning: The elements of $\mathbb{Z}[i]$ form a square lattice in $\mathbb{C}$. The ideal $\langle z \rangle$, all multiples of z , forms a similar lattice: if we write $z = re^{i\theta}$, then the lattice corresponding to $\langle z \rangle$ is obtained by rotating through the angle θ followed by stretching by the factor $r = |z|$. It is clear that for every w in $\mathbb{C}$, there is at least one point of the lattice corresponding to $\langle z \rangle$ whose square distance from w is at most $(1/2)|z|^2$. Let that point be qz and set $p := w - qz$. It follows that $|p|^2 \leq (1/2)|z|^2 < |z|^2$ as required. Since there may be more than one choice for qz , this division with remainder is not unique.

Algebraic Reasoning: Divide w in $\mathbb{C}$ by z : $w = cz$ where $c = x + yi$ in $\mathbb{C}$. Choose a nearest Gaussian integer: $x := a + x_0$, $y := b + y_0$ where a and b are integers and $-1/2 \leq x_0, y_0 < 1/2$. It follows that the product $(a + bi)z$ is the required point in $\langle z \rangle$ because we have $|x_0 + y_0 i|^2 < 1/2$ and $|w - (a + bi)z|^2 = |z(x_0 + y_0 i)|^2 < (1/2)|z|^2$. $\diamond$

6.3.6 Definition. A *principal ideal domain* is a domain in which every ideal is principal: generated by a single element.

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

Proof. Let I be an ideal in a Euclidean domain R . When $I = \langle 0 \rangle$, the ideal I is principal, so we may assume $I \neq \langle 0 \rangle$. By the well-ordering property of the integers, the set of all degrees of nonzero elements in I has a minimum, say n . Choose f in I with $\nu(f) = n$. As f in I , we have $\langle f \rangle \subseteq I$. For any g in I , there exists q and r in R such that $g = qf + r$ and either $r = 0$ or $\nu(r) < \nu(f)$. However, we have $r = g - qf \in I$ so our choice of f implies that $r = 0$. Therefore, we deduce that $g = qf$ and $I \subseteq \langle f \rangle$. $\square$

6.3.8 Example. We claim that the ideal $\langle 2, x \rangle$ in $\mathbb{Z}[x]$ is not principal. Suppose that $\langle f \rangle = \langle 2, x \rangle$ for some polynomial f in $\mathbb{Z}[x]$. It follows that $gf = 2$ for some g in $\mathbb{Z}[x]$. Since $\deg(g) + \deg(f) = \deg(2) = 0$, we deduce that f and g are integers. Hence, we have $f = \{\pm 1, \pm 2\}$. Since $\langle 2, x \rangle$ is a maximal ideal, the element f cannot be a unit, so $f = \pm 2$. However, we would also have $x \in \langle f \rangle$, so $x = 2h$ for some h in $\mathbb{Z}[x]$ which is absurd. $\diamond$

6.3.9 Example. We claim that the ideal $\langle 2, 1 - \sqrt{-3} \rangle$ in $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{C}$ is not principal. Suppose that $\langle a + b\sqrt{-3} \rangle = \langle 2, 1 - \sqrt{-3} \rangle$ for some integers a and b . It follows that $g(a + b\sqrt{-3}) = 2$ for some g in $\mathbb{Z}[\sqrt{-3}]$. Taking absolute values in $\mathbb{C}$ gives $|g| (a^2 + 3b^2) = 2$, so $a^2 + 3b^2 \in \{\pm 1, \pm 2\}$. Because a and b are integers, we must have $a = \pm 1$ and $b = 0$ which contradicts the fact that $\langle 2, 1 - \sqrt{-3} \rangle$ is a maximal ideal. $\diamond$

6.3.10 Example. The rings

- $\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ where $\alpha := (1 + \sqrt{-19})/2$,
- $\mathbb{R}[x, y]/\langle x^2 + y^2 + 1 \rangle$,
- $\mathbb{Q}[x, y]/\langle y^2 - 2x^2 - 5 \rangle$,

are principal ideal domains but not Euclidean domains. For more details, see

- Jack C. Wilson, A principal ideal ring that is not a Euclidean ring, *Mathematics Magazine* 46 (1973) 34–38;
- Anthony J. Bevelacqua, A family of non-Euclidean PIDs, *American Mathematical Monthly* 123 (2016), no. 9, 936–939. $\diamond$

6.4 Exercises

6.4.1 Problem. Determine which of the following statements are true. If a statement is false, then provide a counterexample.

- i. The product of any two multiplicative sets is multiplicative.
- ii. Every domain is isomorphic to a subring of a field.
- iii. The ring $\mathbb{Q}[i] := \{a + bi \mid a, b \in \mathbb{Q}\}$ is isomorphic to the field of fractions for the ring $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$.
- iv. Any field K is a Euclidean domain when equipped with the function $\nu: K \setminus \{0\} \rightarrow \mathbb{N}$ defined, for any nonzero k in K , by $\nu(k) = 1$.

Can the false statements be salvaged in some way? In other words, can one find a closely related nontrivial true statement.

6.4.2 Problem. Consider two multiplicative subsets D and E in a commutative ring R satisfying $D \subseteq E$. Let $\varphi: R[D^{-1}] \rightarrow R[E^{-1}]$ be the ring homomorphism defined, for any fraction r/d in $R[D^{-1}]$, by $\varphi(r/d) = r/d$. Prove that the following statements are equivalent:

- a. The map φ is a ring isomorphism.
- b. For any e in E , the fraction $e/1$ is a unit in $R[D^{-1}]$.
- c. For any e in E , there exists an s in R such that $es \in D$.

6.4.3 Problem. For any field K , let $K((x))$ be ring of formal Laurent series with coefficients in K :

$$K((x)) := \left\{ \sum_{i=m}^{\infty} a_i x^i \mid a_i \in K, m \in \mathbb{Z} \right\}$$

where the ring operations are defined as in the ring of formal power series $K[[x]]$. Prove that the commutative ring $K((x))$ is isomorphic to the fields of fractions for the domain $K[[x]]$.

6.4.4 Problem. Let R be a commutative ring. Consider the *derivative operator* $D: R[x] \rightarrow R[x]$ defined, for any polynomial

$$f := a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

in $R[x]$, by

$$D(f) := (n a_n) x^{n-1} + ((n-1) a_{n-1}) x^{n-2} + \cdots + a_1.$$

- i. Prove that the operator D is an R -linear map: for any r and s in the coefficient ring R , and any f and g in the polynomial ring $R[x]$, we have $D(rf + sg) = rD(f) + sD(g)$.
- ii. Prove that the operator D satisfies the Leibniz product rule: for any f and g in the polynomial ring $R[x]$, we have

$$D(fg) = D(f)g + fD(g).$$

- iii. Let f be a polynomial in $R[x]$. Assume that z in R is root of f having multiplicity m with $m \geq 1$. Prove that z is also a root of the derivative $D(f)$ having multiplicity at least $m - 1$. Moreover, when the product $m 1_R$ is invertible in R , prove that z is a root of the derivative $D(f)$ having multiplicity $m - 1$.

6.4.5 Problem. Let $\omega := \frac{1}{2}(-1 + \sqrt{3}i)$ be one of the complex roots of the polynomial $x^2 + x + 1$ in $\mathbb{C}[x]$. Prove that the commutative domain $\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a Euclidean domain with the function $\nu: \mathbb{Z}[\omega] \rightarrow \mathbb{N}$ defined, for any $a + b\omega$ in $\mathbb{Z}[\omega]$, by $\nu(a + b\omega) = a^2 - ab + b^2$.

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.