3.2 Domains and Fields

What special kinds of commutative rings warrant recognition? We first name a distinguish collection of elements.

Definition 3.2.0. A ring element is a ***unit*** if it has a multiplicative inverse. The set of units in a ring R is denoted by $R^\times$.

The set $R^\times$ of units in any ring form a *group*: multiplication is an associated binary operation with an identity such each element has an inverse.

Example 3.2.1. We have $\mathbb{Z}^\times = \{1, -1\}$.

Example 3.2.2. For any positive integer n, the units in the ring $\mathrm{M}_{n,n}(R)$ of $(n \times n)$-matrix with entries in a commutative ring R are the invertible matrices; $\mathrm{GL}_n(R) = \mathrm{M}_{n,n}(R)^\times$

Remark 3.2.3. Lemma 2.2.2 and Definition 2.3.0 show that, for any positive integer ℓ, we have

$$(\mathbb{Z}/\langle \ell \rangle)^\times = \{[n]_\ell \mid n \in \mathbb{N}, 1 \leqslant n < \ell, \text{ and } \gcd(n, \ell) = 1\}$$

and $|(\mathbb{Z}/\langle \ell \rangle)^\times| = \phi(\ell)$. For instance, we have $(\mathbb{Z}/\langle 6 \rangle)^\times = \{1, 5\}$ and $(\mathbb{Z}/\langle 9 \rangle)^\times = \{1, 2, 4, 5, 7, 8\}$.

Problem 3.2.4. Verify that $(\mathbb{Z}[\mathrm{i}])^\times = \{1, -1, \mathrm{i}, -\mathrm{i}\}$.

Solution. Suppose that a Gaussian integer $a + b\,\mathrm{i}$ is a unit. There exists a Gaussian integer $c + d\,\mathrm{i}$ such that $(a + b\,\mathrm{i})(c + d\,\mathrm{i}) = 1$. It follows that $(a^2 + b^2)(c^2 + d^2) = |a + b\,\mathrm{i}|^2\,|c + d\,\mathrm{i}|^2 = 1$. Since the nonnegative integer $a^2 + b^2$ divides 1, we see that either $a^2 = 1$ and $b^2 = 0$, or $a^2 = 0$ and $b^2 = 1$. We deduce that ± 1 and $\pm\mathrm{i}$ are the only Gaussian units. □

Definition 3.2.5. A ***field*** is a nonzero commutative ring in which every nonzero ring element is a unit.

Richard Dedekind used the term "Zahlenkörper" (body of numbers) for we would call a division ring rather than a field as it does not require that multiplication be commutative. In 1893, Eliakim Moore was apparently the first person to use the English word "field" in its modern sense.

Example 3.2.6. Some of our favourite sets of numbers including $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields. However, the ring $\mathbb{Z}$ is not a field.

Any field can be used as the scalars for a vector space.

Definition 3.2.7. An element a in a ring R is *nilpotent* if there exists a positive integer k such that $a^k = 0$.

The term "nilpotent" was first used by Benjamin Peirce in 1870.

Lemma 3.2.8. *Let R be a commutative ring. For any nilpotent ring element a and any unit u in R, the difference $u - a$ is also a unit.*

Proof. Since there is a positive integer k such that $a^k = 0$ and a ring element v such that $uv = 1$, we have

$$\begin{aligned}(u - a)\big((u^{k-1} + u^{k-2}\,a + \cdots + u\,a^{k-2} + a^{k-1})\,v^k\big) &= (u^k - a^k)v^k \\ &= (u\,v)^k = 1\,.\end{aligned}$$ □

Proposition 3.2.9. *Let R be a commutative ring. The units in the polynomial ring $R[x]$ are the polynomials*

$$f = a_m\,x^m + a_{m-1}\,x^{m-1} + \cdots + a_1\,x + a_0$$

where m is a nonnegative integer, a_0 is a unit in R, and other coefficients $a_1, a_2, \ldots, a_m$ are nilpotent.

Proof. As f is a unit, there is a $g = b_n\,x^n + b_{n-1}\,x^{n-1} + \cdots + b_1\,x + b_0$ such that $f\,g = 1$. The definition of multiplication on $R[x]$ gives

$$\begin{aligned} a_m\,b_n &= 0 && \text{coefficients of } x^{m+n} \\ a_{m-1}\,b_n + a_m\,b_{n-1} &= 0 && \text{coefficients of } x^{m+n-1} \\ &\vdots \\ \sum_{j=0}^{k} a_{m-k+j}\,b_{n-j} &= 0 && \text{coefficients of } x^{m+n-k} \\ &\vdots \\ a_0\,b_1 + a_1\,b_0 &= 0 && \text{coefficients of } x^{1} \\ a_0\,b_0 &= 1 && \text{coefficients of } x^{0} \end{aligned}$$

The last equation shows that a_0 and b_0 are units in R.

When $m > 0$, we next prove, by strong induction on k, that $a_m^{k+1}\,b_{n-k} = 0$ for any $0 \leqslant k \leqslant n$. The equation $a_m\,b_n = 0$ is the base case. For all $0 \leqslant j < k$, assume that $a_m^{j+1}\,b_{n-j} = 0$. Multiplying the $(m+n-k)$-th equation by a_m^k, the induction hypothesis gives

$$0 = a_m^k\left(\sum_{j=0}^{k} a_{m-k+j}\,b_{n-j}\right) = \sum_{j=0}^{k} a_{m-k+j}\,a_m^{k-j-1}\,(a_m^{j+1}\,b_{n-j}) = a_m^{k+1}\,b_{n-k}\,.$$

Since $a_m^{n+1}\,b_0 = 0$ and b_0 is a unit, we deduce that a_m is nilpotent.

Lastly, we establish, by induction on m, that the ring elements $a_m, a_{m-1}, \ldots, a_1$ are all nilpotent. The assertion is vacuous when $m = 0$. Assume that $m > 0$. Since f is a unit and the previous paragraph proves that $a_m\,x^m$ is nilpotent, Lemma 3.2.8 shows that $f - a_m\,x^m$ is a unit. The induction hypothesis shows that $a_{m-1}, a_{m-2}, \ldots, a_1$ are nilpotent. □

Definition 3.2.10. A ring R is a ***domain*** if its nonzero and the product of two nonzero elements in R is nonzero.

A ring element a is a *zero divisor* if there exists a nonzero ring element b such that $a\,b = b\,a = 0$. Hence, a domain is a ring in which the only zero divisor is 0.

Proposition 3.2.11. *Every field is a domain.*

Proof. Let a and b be elements of a field. When $a\,b = 0$ and $b \neq 0$, we have $a = a\,1 = a\,(b\,b^{-1}) = (a\,b)\,b^{-1} = 0\,b^{-1} = 0$. □

Proposition 3.2.12. *Any finite domain is a field.*

Proof. Let R be a finite domain and consider a a nonzero ring element. The ring R being a domain implies that the map $x \mapsto ax$ is injective. The ring R being finite, it follows that this map is also surjective. Hence, there exists a ring element b in R such that $a\,b = 1$. Since a was arbitrary, the ring R is a field. □

Proposition 3.2.13. *Let ℓ be a nonnegative integer. The quotient ring $\mathbb{Z}/\langle\ell\rangle$ is a domain if and only if ℓ is a prime integer.*

Combining Proposition 3.2.12 and Proposition 3.2.13, we see that $\mathbb{Z}/\langle\ell\rangle$ is a field if and only if the generator ℓ is a positive prime integer. For a prime number p, the finite field $\mathbb{Z}/\langle p\rangle$ is frequently denoted by $\mathbb{F}_p$.

Proof.

⇐: Suppose that ℓ is prime. For any integers m and n such that $m\,n \equiv 0 \mod \ell$, it follows ℓ divides m or ℓ divides n, Thus, the quotient ring $\mathbb{Z}/\langle\ell\rangle$ is a domain.

⇒: Suppose that ℓ is not prime. Hence, there exists positive integers m and n such that $\ell = m\,n$, $1 < m < \ell$, and $1 < n < \ell$. It follows that $m \equiv 0 \mod \ell$ and $n \equiv 0 \mod \ell$ but $m\,n \equiv 0 \mod \ell$. Therefore, the quotient ring $\mathbb{Z}/\langle\ell\rangle$ is not a domain. □

Exercises

Problem 3.2.14. In a commutative ring, demonstrate that the set of nilpotent elements forms a subring.

Problem 3.2.15. Establish that any subring of a domain is also a domain.

Problem 3.2.16. Let $\mathbb{F}_3 := \mathbb{Z}/\langle 3 \rangle$ be the field with 3 elements. Consider the commutative ring

$$\mathbb{F}_3[\mathrm{i}] := \{a + b\,\mathrm{i} \mid a, b \in \mathbb{F}_3 \text{ and } \mathrm{i}^2 \equiv -1 \equiv 2 \mod 3\}.$$

Verify that $\mathbb{F}_3[\mathrm{i}]$ is a field.

Problem 3.2.17. Let $\mathbb{F}_5 := \mathbb{Z}/\langle 5 \rangle$ be the field with 5 elements. Consider the commutative ring

$$\mathbb{F}_5[\mathrm{i}] := \{a + b\,\mathrm{i} \mid a, b \in \mathbb{F}_5 \text{ and } \mathrm{i}^2 \equiv -1 \equiv 4 \mod 5\}.$$

Confirm that $\mathbb{F}_5[\mathrm{i}]$ is not a domain.

Problem 3.2.18. Assume that the commutative ring R is a domain. Prove that R has characteristic 0 or has characteristic p where p is a positive prime number. When R has characteristic 0, show that it has a subring isomorphic to $\mathbb{Z}$. When R has characteristic p, show that it has a subring isomorphic to $\mathbb{Z}/\langle p \rangle$.

4 Polynomials

Last Updated: 9 February 2023

Together with the set of integers, polynomials whose coefficient lie in a field form the most important example of a commutative ring. Polynomial rings are ubiquitous in modern mathematics and indispensable in algebra and algebraic geometry.

The hybrid word "polynomial" combines the Greek prefix *poly*, meaning 'many' with the Latin suffix *nomen* meaning 'name'.

Throughout the chapter, R denotes a commutative ring.

4.0 Polynomial Roots

What attributes distinguish polynomials? Polynomials in a single indeterminate come with some terminology.

Definition 4.0.0. For any nonzero element f in the polynomial ring $R[x]$, the *degree*, denoted by $\deg(f)$, is the largest nonnegative integer k such that the coefficient a_k of the monomial x^k in f is nonzero. The nonzero element a_m in R satisfying $m = \deg(f)$ is the *leading coefficient*. A *monic* polynomial is one whose leading coefficient is 1_R.

Table 4.1: Low degree polynomials have distinctive names

Degree	Name
1	linear
2	quadratic
3	cubic
4	quartic
5	quintic
6	sextic
7	septic
8	octic

Example 4.0.1. The polynomial $9\,x^3 - 3\,x^2 + 5\,x - 1$ has degree 3 and leading coefficient 9, so it is not monic. The polynomial $x^{17} - 1$ is monic and has degree 17. A polynomial of degree 0 is a nonzero element in the coefficient ring R.

Lemma 4.0.2. *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 $\deg(f + g) = \max(\deg(f), \deg(g))$. When $\deg(f) = \deg(g)$, the degree of the sum satisfies $\deg(f + g) \leqslant \deg(f)$.*
- *We have $\deg(fg) \leqslant \deg(f) + \deg(g)$ and equality holds if the leading coefficient of f or g is not a zero divisor in R.*

Proof. Let a_m be the leading coefficient of f and let b_n be the leading coefficient of g. It follows that the leading coefficient the sum $f + g$ is a_m when $m > n$ and b_n with $m < n$. 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 we deduce that $\deg(f + g) \leqslant m$. 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 $\deg(fg) \leqslant \deg(f) + \deg(g)$. □

Proposition 4.0.3. *For any domain R, the polynomial ring $R[x]$ is also a domain and the units in $R[x]$ are the units in R.*

The only nilpotent element in a commutative domain is 0, so Proposition 3.2.9 proves this assertion when R is commutative.

Proof. Suppose that f and g are nonzero polynomials in $R[x]$. Since $\deg(f\,g) = \deg(f) + \deg(g) \geqslant 0$, it follows that $fg \neq 0$. When $f\,g = 1$, we have $\deg(f) + \deg(g) = \deg(1) = 0$. Hence, both f and g are polynomials of degree 0 and thereby elements of R. □

Theorem 4.0.4 (Division with remainder)**.** *Consider two nonzero elements f and g in the ring $R[x]$ having degrees m and n respectively. Let a_m be the leading coefficient of the polynomial f and set*

$$k := \max(n - m + 1, 0)\,.$$

There exists polynomials q and r in $R[x]$ such that $a_m^k\, g = q\, f + r$ and $0 \leqslant \deg(r) < m$ or $r = 0$. When a_m is a not a zero divisor in R, the polynomials q and r are uniquely determined by these properties.

Proof. We treat existence and uniqueness separately.

(existence) When $n < m$, simply take $q := 0$ and $r := a_m^k\, g$. When $n \geqslant m$, we proceed by induction on n. When $n = 0$, we have $m = 0$, $k = 1$, and $f = a_m$, so we may take $q := g$ and $r := 0$ for the base case. Assume $n > 0$ and let b_n denote the leading coefficient of g. It follows that $\deg(a_m^k\, g - a_m^{k-1}\, b_n\, x^{n-m} f) < n$. The induction hypothesis implies that, there exists p and r in the ring $R[x]$ such that $a_m^{k-1}(a_m\, g - b_n x^{n-m} f) = p\, f + r$ and $\deg(r) < m$ or $r = 0$, so $a_m^k\, g = (a_m^{k-1}\, b_n x^{n-m} + p) f + r$. Setting $q := a_m^{k-1}\, b_n x^{n-m} + p$ completes the induction step.

(uniqueness) Consider polynomials q, p, r, s in $R[x]$ such that $a_m^k\, g = q\, f + r = p\, f + s$, $\deg(r) < m$, and $\deg(s) < m$. It follows that $(q - p)\, f = (s - r)$ and $\deg(s - r) < m$. Since a_m is not a zero divisor, we have $m + \deg(q - p) = \deg(s - r) < m$ and we conclude that $q = p$ and $r = s$. □

Repackaging the induction leads to long division.

Problem 4.0.5. For the polynomials $g = 3\,x^4 - 12\,x^3 - 13\,x^2 + 59\,x + 1$ and $f = x^2 - 2\,x - 8$ in $\mathbb{Q}[x]$, find the quotient and remainder for division of g by f.

Solution. Long division gives

Since the leading coefficient of f is a unit in the coefficient ring, we do not need to multiply g by a power of it.

$$\begin{array}{r|l}
 & 3\,x^2 - 6\,x - 1 \\
\hline
x^2 - 2\,x - 8 & 3\,x^4 - 12\,x^3 - 13\,x^2 + 59\,x + 1 \\
 & \underline{3\,x^4 - 6\,x^3 - 24\,x^2} \\
 & \quad -6\,x^3 + 11\,x^2 + 59\,x \\
 & \quad \underline{-6\,x^3 + 12\,x^2 + 48\,x} \\
 & \quad\quad -x^2 + 11\,x + 1 \\
 & \quad\quad \underline{-x^2 + 2\,x + 8} \\
 & \quad\quad\quad 9\,x - 7
\end{array}$$

so $g \,//\, f = 3\,x^2 - 6\,x - 1$ and $g \,\%\, f = 9\,x - 7$. □

Problem 4.0.6. For the polynomials $g = x^5 - 9\,x^3 + 4\,x^2 + 2$ and $f = 6\,x^3 + 1$ in $\mathbb{Z}[x]$, find the quotient and remainder for division of g by f.

Solution. Since $\deg(g) - \deg(f) + 1 = 3$, we divide $6^3\, g$ by f. Long

division gives

$$\begin{array}{r|l} & 36\,x^2+0\,x-324 \\ \hline 6\,x^3+1 & 216\,x^5+0\,x^4-1944\,x^3+864\,x^2+0\,x+432 \\ & \underline{216\,x^5+0\,x^4\quad\;+0\,x^3\;+36\,x^2\qquad\qquad\quad} \\ & -1944\,x^3+838\,x^2+0\,x+432 \\ & \underline{-1944\,x^3\quad+0\,x^2+0\,x-324} \\ & 838\,x^2+0\,x+756 \end{array}$$

so $(6^3\,g) /\!/ f = 36\,x^2 - 324$ and $(6^3\,g) \,\%\, f = 838\,x^2 + 756$. □

Definition 4.0.7. For any ring element $b \in R$, the *evaluation map* $\mathrm{ev}_b \colon R[x] \to R$ is defined by

$$\mathrm{ev}_b(a_m\,x^m + a_{m-1}\,x^{m-1} + \cdots + a_0) = a_m\,b^m + a_{m-1}\,b^{m-1} + \cdots + b_0\,.$$

From the definiton of addition and multiplication on $R[x]$, it follows that, for any ring element $b \in R$ and any polynomials f and g in $R[x]$, we have $\mathrm{ev}_b(f+g) = \mathrm{ev}_b(f) + \mathrm{ev}_b(g)$, $\mathrm{ev}_b(f\,g) = \mathrm{ev}_b(f)\,\mathrm{ev}_b(g)$, and $\mathrm{ev}_b(1_{R[x]}) = 1_R$.

Definition 4.0.8. A *root* of polynomial f in the ring $R[x]$ is a ring element b in R such that $\mathrm{ev}_b(f) = f(b) = 0$.

Corollary 4.0.9. *For any polynomial g in the ring $R[x]$, the ring element b in R is a root of g if and only if $x - b$ is a divisor of g.*

Proof. Set $f := x - b$. Division with remainder implies that there exists polynomials q and r in the ring $R[x]$ such that $g = q\,f + r$ and $\deg(r) < 1$ or $r = 0$. It follows that $r \in R$. Evaluating at b yields $\mathrm{ev}_b(g) = \mathrm{ev}_b(q)\,\mathrm{ev}_b(f) + \mathrm{ev}_b(r) = \mathrm{ev}_b(q)\,(0) + r = r$, so we obtain $g = q\,f + \mathrm{ev}_b(g)$. Thus, the remainder r equals 0 if and only if $\mathrm{ev}_b(g) = 0$. □

Exercises

Problem 4.0.10. Let m and n be two positive integers such that m divides n. Verify that the polynomial $x^m - 1$ divides $x^n - 1$.

Problem 4.0.11. Let $R := \mathbb{Z}\big/\langle 6\rangle$. For the polynomials

$$g = x^5 + 3\,x^3 + 5\,x^2 + 2\,x + 1 \qquad \text{and} \qquad f = 2\,x^2 + 4\,x + 1$$

in $R[x]$, find a quotient and remainder for division of g by f.

Problem 4.0.12. Let K be a field. Consider two polynomials f and g in the ring $K[x]$ such that $\deg(g) > 0$. Confirm that there exist unique polynomials $h_0, h_1, \ldots, h_d$ in the ring $K[x]$ such that

$$f = h_0 + h_1\,g + h_2\,g^2 + h_3\,g^3 + \cdots + h_d\,g^d$$

and $\deg(h_j) < \deg(g)$ for all $1 \leqslant j \leqslant d$.

4.1 Multiplicity of a root

What does it mean to have a multiple root? To obtain the deepest insights, we need count the roots of a polynomial correctly.

Proposition 4.1.0. *Let f be a polynomial in $R[x]$ and let b be a ring element in the coefficient ring R. For any nonnegative integer k, the following are equivalent.*
(a) *The polynomial f is divisible by $(x-b)^k$ but not by $(x-a)^{k+1}$.*
(b) *There is a polynomial g in the ring $R[x]$ such that $f = (x-b)^k\, g$ and $\operatorname{ev}_b(g) = g(b) \neq 0$.*
Moreover, when $f \neq 0$, there exists a unique nonnegative integer k satisfying these conditions.

Proof.
(a)$\Rightarrow$(b): Follows from Corollary 4.0.9.
(b)$\Rightarrow$(a): Suppose that $f = (x-b)^k\, g$ and g does not have b as root. We see that f is divisible by $(x-b)^k$. Assume that there exists a polynomial h in the ring $R[x]$ such that $f = (x-b)^{k+1}\, h$. Since $(x-b)^k$ is not a zero divisor in $R[x]$, we would have $g = (x-b)\, h$ which implies that $\operatorname{ev}_b(g) = g(b) = 0$ which is contradiction. □

Definition 4.1.1. For any polynomial f in the ring $R[x]$ and any nonnegative integer k, the element b in the coefficient ring R is a root of *multiplicity* k if f is divisible by $(x-b)^k$ but not $(x-b)^{k+1}$. A root of multiplicity 1 is a *simple* root and a root of multiplicity 2 is a *double* root.

Any ring element b in R that is not a root is a root of multiplicity 0.

Lemma 4.1.2. *Let j and k be the multiplicities of the root b in R for the polynomials f and g in the ring $R[x]$ respectively.*
- *The sum $f+g$ has a root of multiplicity at least $\min(j,k)$ at b and is equal to $\min(j,k)$ when $j \neq k$.*
- *The product $f\,g$ has a root of multiplicity at least $j+k$ and it is equal to $j+k$ when R is domain.*

Proof. We may assume that $j \leqslant k$. There are polynomials p and q in $R[x]$ such that $f = (x-b)^j\, p$, $\operatorname{ev}_b(p) \neq 0$, $g = (x-b)^k\, q$, and $\operatorname{ev}_b(q) \neq 0$. It follows that $f + g = (x-b)^j\,(p + (x-b)^{k-j}\, q)$. When $k - j > 0$, the ring element b is not a root of $p + (x-b)^{k-j}\, q$ because $\operatorname{ev}_b(p) + (b-b)^{k-1}\, \operatorname{ev}_b(q) = \operatorname{ev}_b(p) \neq 0$. Similarly, we have $f\,g = (x-b)^{j+k}\, p\, q$ and $\operatorname{ev}_b(p)\, \operatorname{ev}_b(q) \neq 0$ when R is a domain. □

Proposition 4.1.3. *Let R be a domain. Given a nonzero polynomial f in the ring $R[x]$ with distinct roots $b_1, b_2, \ldots, b_\ell$ having multiplicities $k_1, k_2, \ldots, k_\ell$, there exists a polynomial g in $R[x]$ such that $b_1, b_2, \ldots, b_\ell$ are not roots of g and $f = (x-b_1)^{k_1}\,(x-b_2)^{k_2} \cdots (x-b_\ell)^{k_\ell}\, g$.*

Proof. We proceed by induction on ℓ. The base case $\ell = 1$ is covered by Proposition 4.1.0. Suppose that

$$f = (x-b_1)^{k_1}\,(x-b_2)^{k_2} \cdots (x-b_{\ell-1})^{k_{\ell-1}}\, h\,.$$

Since R is a domain and the root b_ℓ is distinct from $b_1, b_2, \dots, b_{\ell-1}$, it follows that b_ℓ is not a root of the polynomial

$$(x - b_1)^{k_1} (x - b_2)^{k_2} \cdots (x - b_{\ell-1})^{k_{\ell-1}}.$$

The element b_ℓ is a root of multiplicity k_ℓ of the polynomial h and Proposition 4.1.0 implies that $h = (x - b_\ell)^{k_\ell} g$ where $b_1, b_2, \dots, b_\ell$ are not roots of g. □

Corollary 4.1.4. *Let R be a domain. Given nonzero polynomial f in the ring $R[x]$ of degree m, the sum of multiplicities of all the roots of f is at most m.* □

Some hypothesis on the coefficient ring is necessary.

Problem 4.1.5. Over the ring $R = \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$, verify that all four elements are roots of the polynomial $x^2 - x$ in $R[x]$.

Solution. Since operation on R are defined entrywise, we have

$$\begin{aligned}
\big((0,0)\big)^2 - (0,0) &= (0,0) - (0,0) = (0,0), \\
\big((1,0)\big)^2 - (1,0) &= (1,0) - (1,0) = (0,0), \\
\big((0,1)\big)^2 - (0,1) &= (0,1) - (0,1) = (0,0), \\
\big((1,1)\big)^2 - (1,1) &= (1,1) - (1,1) = (0,0).
\end{aligned}$$

□

Table 4.2: Sums in $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$

+	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

Table 4.3: Products in $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$

×	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(1,0)	(0,0)	(1,0)	(0,0)	(1,0)
(0,1)	(0,0)	(0,0)	(0,1)	(0,1)
(1,1)	(0,0)	(1,0)	(0,1)	(1,1)

Our analysis of roots also shows that two polynomials that agree when evaluated at a sufficiently large, but finite, number of ring elements in a domain must be equal.

Corollary 4.1.6. *Let R be a domain and let m be a positive integer. Consider two nonzero polynomials f and g in the ring $R[x]$ of degree at most m. If there are $m + 1$ distinct elements $b_0, b_1, \dots, b_m$ in the coefficient ring R such that $\operatorname{ev}_{b_j}(f) = f(b_j) = g(b_j) = \operatorname{ev}_{b_j}(g)$ for all $0 \leqslant j \leqslant m$, then we have $f = g$.*

Proof. The polynomial $h := f - g$ has degree at most m and has at least $m + 1$ distinct roots. Corollary 4.1.4 implies that $h = 0$. □

Proposition 4.1.7 (Lagrange Interpolation)**.** *Let K be a field and let $b_0, b_1, \dots, b_m$ be $m + 1$ distinct elements of K. For any elements $c_0, c_1, \dots, c_m$ in K, there exists a unique polynomial f in the ring $K[x]$ of degree at most m such that $\operatorname{ev}_{b_j}(f) = f(b_j) = c_j$ for all $0 \leqslant j \leqslant m$.*

Proof. Uniqueness follows from Corollary 4.1.6. For all $0 \leqslant j \leqslant m$, consider the polynomial

$$g_j := \prod_{k \neq j} \frac{(x - b_k)}{(b_j - b_k)} \in K[x].$$

It follows that $\deg(g_j) = m$ and $\operatorname{ev}_{b_k}(g_j) = g_j(b_k) = \delta_{j,k}$. Thus, we may take $f := \sum_{j=0}^{m} c_j g_j$. □

The *Kronecker delta* is defined by

$$\delta_{j,k} := \begin{cases} 1 & \text{if } j = k, \\ 0 & \text{if } j \neq k. \end{cases}$$

In other words, $\delta_{j,k}$ is the (j,k)-entry in the identity matrix $\mathbf{I}$.

Exercises

Problem 4.1.8. Let R be a commutative ring. The *derivative operator* $D\colon R[x] \to R[x]$ is defined, for any polynomial

$$f = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \,,$$

by

$$D(f) = (m\, a_m) x^{m-1} + \big((m-1)\, a_{m-1}\big) x^{m-2} + \cdots + a_1 \,.$$

(i) Prove that the operator D is an R-linear map: for any two ring elements r and s in the coefficient ring R and any two polynomials f and g in the ring $R[x]$, we have

$$D(r\, f + s\, g) = r\, D(f) + s\, D(g) \,.$$

(ii) Prove that the operator D satisfies the product rule: for any two polynomials f and g in the ring $R[x]$, we have

$$D(f\, g) = D(f)\, g + f\, D(g) \,.$$

(iii) Let f be a polynomial in $R[x]$ and let b be an element in R. Prove that b is a root of f having multiplicity k with $k \geqslant 1$ if and only if b is a root of the derivative $D(f)$ having multiplicity k.