

3.2 Domains and Fields

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

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

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

3.2.2 Remark. For all $n \in \mathbb{N}$, the units in the ring $\text{Mat}(n, R)$ are the invertible matrices; $\text{GL}(n, R) = (\text{Mat}(n, R))^\times$.

3.2.3 Remark. Lemma 2.1.2 and Definition 2.2.0 show that, for any positive $\ell \in \mathbb{N}$, we have

$(\mathbb{Z}/\langle \ell \rangle)^\times = \{[n]_\ell \mid n \in \mathbb{N}, 1 \leq n \leq \ell, \text{ and } \gcd(n, \ell) = 1\}$
and $|(\mathbb{Z}/\langle \ell \rangle)^\times| = \phi(\ell)$. For instance, we have $(\mathbb{Z}/\langle 6 \rangle)^\times = \{1, 5\}$ and $(\mathbb{Z}/\langle 9 \rangle)^\times = \{1, 2, 4, 5, 7, 8\}$.

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

Solution. Suppose that $a + bi \in \mathbb{Z}[i]$ is a unit. By definition, there exists $c + di \in \mathbb{Z}[i]$ such that $(a + bi)(c + di) = 1$. It follows that $(a^2 + b^2)(c^2 + d^2) = |a + bi|^2 |c + di|^2 = 1$. Since $a^2 + b^2$ is a positive integer dividing 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 $\pm i$ are the only units. $\square$

3.2.5 Definition. A *field* is a nonzero commutative ring such that every nonzero ring element is a unit.

3.2.6 Remark. Some of our favourite sets of numbers, including $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, are fields. The ring $\mathbb{Z}$ is not a field, because 2 is not a unit.

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

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

Proof. Since there exist $v \in R$ and a positive $k \in \mathbb{Z}$ such that $uv = 1$ and $a^k = 0$, we have

$$(u - a)((u^{k-1} + u^{k-2}a + \cdots + u a^{k-2} + a^{k-1})v^k) = (u^k - a^k)v^k = (uv)^k = 1. \quad \square$$

3.2.9 Proposition. For any commutative ring R , the units in the 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 each of other coefficients $a_1, a_2, \dots, a_m$ is 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 $fg = 1$. The definition of multiplication on $R[x]$ gives

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

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

In German and French, the terms "Körper" and "corps" often do not require commutativity. In 1893, Eliakim Moore was apparently first to use the English word "field" in its modern sense.

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

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

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

Suppose that $m > 0$. We next prove, by strong induction on k , that $a_m^{k+1} b_{n-k} = 0$ for any $0 \leq k \leq n$. The equation $a_m b_n = 0$ is the base case. For all $0 \leq j < k$, 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

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

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

Lastly, we prove, by induction on m , that $a_m, a_{m-1}, \dots, a_1$ are all nilpotent. The assertion is vacuous when $m = 0$, so the base case holds. Assume that $m > 0$. The previous paragraph shows that $a_m x^m$ is nilpotent. Since Lemma 3.2.8 proves that $f - a_m x^m$ is a unit, the induction hypothesis implies that each of the coefficients $a_{m-1}, a_{m-2}, \dots, a_1$ is nilpotent. $\square$

3.2.10 Definition. A ring R is a *domain* if it is not the zero ring and the product of nonzero elements in R is nonzero.

3.2.11 Proposition. 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 $a = a \cdot 1 = a(b b^{-1}) = (a b) b^{-1} = 0 b^{-1} = 0$. $\square$

3.2.12 Proposition. Any finite commutative domain is a field.

Proof. Let R be a finite domain. Let a be nonzero element in R . The ring R being a domain implies that the map $x \mapsto ax$ is injective; otherwise, there exists x and y in R such that $x \neq y$ and $ax = ay$ which would imply that $a(x - y) = 0$. The ring R being finite, it follows that this map is also surjective. Hence, there is an element b in R such that $ab = 1$. As a was arbitrary, the ring R is a field. $\square$

3.2.13 Proposition. Fix $\ell \in \mathbb{N}$. The quotient ring $\mathbb{Z}/\langle \ell \rangle$ is a domain if and only if ℓ is a prime integer.

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

Suppose that ℓ is not prime. There are positive integers m and n such that $\ell = mn$, $1 < m < \ell$, and $1 < n < \ell$. Hence, we deduce that $m \not\equiv 0 \pmod{\ell}$ and $n \not\equiv 0 \pmod{\ell}$ but $mn \equiv 0 \pmod{\ell}$. Therefore, the quotient ring $\mathbb{Z}/\langle \ell \rangle$ is not a domain. $\square$

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

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 $\mathbb{F}_p$.

4 Polynomials

Copyright © 2026, Gregory G. Smith
Last Updated: 2026-10-08

Polynomials whose coefficients lie in a field form one of the most important examples of a commutative ring. Polynomial rings are ubiquitous in modern mathematics and indispensable in algebra.

Throughout the chapter, R denotes a commutative ring.

The hybrid word “polynomial” combines the Greek prefix *poly*, meaning ‘many,’ with the Latin suffix *nomen*, meaning ‘name’.

4.0 Polynomial Roots

What attributes distinguish polynomials? Univariate polynomials come with some terminology.

4.0.0 Definition. For any nonzero $f \in R[x]$, the *degree* $\deg(f)$ is the largest $k \in \mathbb{N}$ 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 has leading coefficient 1_R .

4.0.1 Remark. The polynomial $9x^3 - 3x^2 + 5x - 1$ 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 .

4.0.2 Lemma. Let f and g be nonzero polynomials in $R[x]$.

(add) When $\deg(f) \neq \deg(g)$, the sum $f + g$ is nonzero and

$$\deg(f + g) = \max(\deg(f), \deg(g)).$$

When $\deg(f) = \deg(g)$, we have $\deg(f + g) \leq \deg(f)$.

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

Proof. Let $a_m \in R$ be the leading coefficient of f and let $b_n \in R$ be the leading coefficient of g . Hence, the leading coefficient of the sum $f + g$ is a_m if $m > n$, and b_n if $m < n$. 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 $\deg(f + g) \leq m$. 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 $\deg(fg) \leq \deg(f) + \deg(g)$. $\square$

4.0.3 Proposition. For every domain R , the polynomial ring $R[x]$ is also a domain and the units in $R[x]$ are precisely the units in R ; $(R[x])^\times = R^\times$.

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

4.0.4 Theorem (Division with remainder). Let $f, g \in R[x]$ be nonzero polynomials such that $m := \deg(f)$ and $n := \deg(g)$. When b_n denote the leading coefficient of g and let $k := \max(m - n + 1, 0)$, there exists $q, r \in R[x]$ such that $b_n^k f = qg + r$ and $0 \leq \deg(r) < n$ or $r = 0$. When $b_n \in R$ is a nonzerodivisor, both q and r are uniquely determined.

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

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

Proof. We treat existence and uniqueness separately.

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

(uniqueness) Suppose that $q, p, r, s \in R[x]$ satisfy

$$b_n^k f = q g + r = p g + s, \quad \deg(r) < n, \quad \deg(s) < n.$$

It follows that $(q - p)g = (s - r)$ and $\deg(s - r) < n$. Since b_n is a nonzerodivisor, we deduce that $n + \deg(q - p) = \deg(s - r) < n$ and we conclude that $q = p$ and $r = s$. $\square$

Repackaging the induction leads to long division.

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

Solution. Long division gives

$$\begin{array}{r} 3x^2 - 6x - 1 \\ x^2 - 2x - 8 \overline{) 3x^4 - 12x^3 - 13x^2 + 59x + 1} \\ \underline{3x^4 - 6x^3 - 24x^2} \\ -6x^3 + 11x^2 + 59x \\ \underline{-6x^3 + 12x^2 + 48x} \\ -x^2 + 11x + 1 \\ \underline{-x^2 + 2x + 8} \\ 9x - 7 \end{array}$$

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

4.0.6 Definition. For all $b \in R$, the *evaluation map* $\text{ev}_b : R[x] \rightarrow R$ is defined, for all $a_0, a_1, \dots, a_m \in R$, by

$$\text{ev}_b(a_m x^m + a_{m-1} x^{m-1} + \dots + a_0) = a_m b^m + a_{m-1} b^{m-1} + \dots + a_0.$$

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

4.0.8 Corollary. For every nonzero polynomial $f \in R[x]$, the element $b \in R$ is a root of f if and only if $x - b$ is a divisor of f .

Proof. Let $g := x - b \in R[x]$. By division with remainder, there exist $q, r \in R[x]$ such that $f = qg + r$ and $\deg(r) < 1$ or $r = 0$. It follows that $r \in R$. Evaluating at b gives

$$\text{ev}_b(f) = \text{ev}_b(q) \text{ev}_b(g) + \text{ev}_b(r) = \text{ev}_b(q)(0) + r = r,$$

so we obtain $f = qg + \text{ev}_b(f)$. Thus, the remainder r equals 0 if and only if $\text{ev}_b(f) = 0$. $\square$

By design, the leading terms in the expression $b_n^k f - b_n^{k-1} a_m x^{m-n} g$ cancel.

Since g is monic, we do not need to multiply f by a power of the leading coefficient.

From the definition of addition and multiplication on $R[x]$, it follows that, for all $b \in R$ and all $f, g \in R[x]$, we have $\text{ev}_b(f + g) = \text{ev}_b(f) + \text{ev}_b(g)$, $\text{ev}_b(fg) = \text{ev}_b(f) \text{ev}_b(g)$, and $\text{ev}_b(1_{R[x]}) = 1_R$.

4.1 Multiplicity of a root

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

4.1.0 Proposition. *Let $b \in R$. For all $k \in \mathbb{N}$, a polynomial $f \in R[x]$ is divisible by $(x - b)^k$, but not by $(x - b)^{k+1}$, if and only if there exists $g \in R[x]$ such that $f = (x - b)^k g$ and $\text{ev}_b(g) = g(b) \neq 0$. When $f \neq 0$, there is a unique $k \in \mathbb{N}$ satisfying these conditions.*

Proof. Suppose that f is divisible by $(x - b)^k$ but not by $(x - b)^{k+1}$. Hence, there exists $g \in R[x]$ such that $f = (x - b)^k g$. If $\text{ev}_b(g) = 0$, then Corollary 4.0.8 would show that $g = (x - b)h$ for some $h \in R[x]$. However, this would establish that $f = (x - b)^{k+1}h$ contradicting our supposition. Thus, we deduce that $\text{ev}_b(g) \neq 0$.

Conversely, suppose that $f = (x - b)^k g$ and g does not have b as a root. By definition, f is divisible by $(x - b)^k$. Assume that there exists $h \in R[x]$ such that $f = (x - b)^{k+1}h$. Since $(x - b)^k$ is not a zerodivisor in $R[x]$, we would have $g = (x - b)h$ which implies that $\text{ev}_b(g) = g(b) = 0$, a contradiction. $\square$

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

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

4.1.2 Lemma. *Let j and k be the multiplicities of the root $b \in R$ for the polynomials f and g in $R[x]$ respectively.*

- (add) *The sum $f + g$ has a root b of multiplicity at least $\min(j, k)$, and the multiplicity is $\min(j, k)$ when $j \neq k$.*
- (multiply) *The product $f g$ has a root b of multiplicity at least $j + k$, and the multiplicity is $j + k$ when R is a domain.*

Proof. We may assume that $j \leq k$. There exist $p, q \in R[x]$ such that $f = (x - b)^j p$, $\text{ev}_b(p) \neq 0$, $g = (x - b)^k q$, and $\text{ev}_b(q) \neq 0$. It follows that

$$f + g = (x - b)^j (p + (x - b)^{k-j} q).$$

When $k - j > 0$, the element b is not a root of $p + (x - b)^{k-j} q$ because $\text{ev}_b(p) + (b - b)^{k-j} \text{ev}_b(q) = \text{ev}_b(p) \neq 0$. Similarly, it follows that $f g = (x - b)^{j+k} p q$ and $\text{ev}_b(p) \text{ev}_b(q) \neq 0$ when R is a domain. $\square$

4.1.3 Proposition. *Let R be a domain. For every nonzero $f \in R[x]$ with distinct roots $b_1, b_2, \dots, b_e$ having multiplicities $k_1, k_2, \dots, k_e$, there exists $g \in R[x]$ such that $b_1, b_2, \dots, b_e$ are not roots of g and*

$$f = (x - b_1)^{k_1} (x - b_2)^{k_2} \dots (x - b_e)^{k_e} g.$$

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

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

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

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

The element b_e is a root of multiplicity k_e of the polynomial h and Proposition 4.1.0 implies that $h = (x - b_e)^{k_e} g$ where $b_1, b_2, \dots, b_e$ are not roots of g . $\square$

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

Some hypothesis on the coefficient ring is necessary.

4.1.5 Problem. 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

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

Our analysis of roots also establishes that any polynomials that agree when evaluated at a sufficiently large number of elements in a domain must be equal.

4.1.6 Corollary. *Let R be a domain, fix a positive $m \in \mathbb{N}$, and consider nonzero $f, g \in R[x]$ of degree at most m . When there exists distinct $b_0, b_1, \dots, b_m \in R$ such that $\text{ev}_{b_j}(f) = f(b_j) = g(b_j) = \text{ev}_{b_j}(g)$ for all $0 \leq j \leq m$, we have $f = g$.*

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

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

Proof. Uniqueness follows from Corollary 4.1.6. For all $0 \leq j \leq m$, 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 $\text{ev}_{b_k}(g_j) = g_j(b_k) = \delta_{j,k}$. Thus, we may take $f := \sum_{j=0}^m c_j g_j$. $\square$

4.1.8 Problem. Consider $f := x^5 - 9x^3 + 4x^2 + 2 \in \mathbb{Z}[x]$ and $g := 6x^3 + 1 \in \mathbb{Z}[x]$. Find the quotient and remainder for division of $6^3 f$ by g .

Solution. Long division gives

$$\begin{array}{r} 36x^2 + 0x - 324 \\ 6x^3 + 1 \overline{) 216x^5 + 0x^4 - 1944x^3 + 864x^2 + 0x + 432} \\ \underline{216x^5 + 0x^4 + 36x^2} \\ -1944x^3 + 828x^2 + 0x + 432 \\ \underline{-1944x^3 + 0x^2 + 0x - 324} \\ 828x^2 + 0x + 756 \end{array}$$

so $(6^3 g) // f = 36x^2 - 324$ and $(6^3 g) \% f = 828x^2 + 756$. $\square$

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)

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 I .

4.2 Exercises

4.2.1 Problem. Determine which of the following statements are true. If a statement is false, provide a counterexample and, if possible, salvage it by modifying the statement so that it becomes true.

- i. Every polynomial in $R[x]$ has only finitely many nonzero coefficients.
- ii. The quotient and remainder arising in division with remainder are always unique.
- iii. Dividing by a nonzero constant polynomial always produces zero as the remainder.
- iv. Every nonconstant polynomial over a field has a root in that field.
- v. If R is finite, then $R[x]$ is finite.
- vi. A polynomial of degree n has exactly n distinct roots.
- vii. If a polynomial has more roots than its degree, then it must be the zero polynomial.

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

4.2.3 Problem. Let $R := \mathbb{Z}/\langle 6 \rangle$. Consider $f := x^5 + 3x^3 + 5x^2 + 2x + 1 \in R[x]$ and $g := 2x^2 + 4x + 1 \in R[x]$. Find a quotient and remainder for division of $2^3 g$ by f .

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

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

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

4.2.5 Problem. Let R be a commutative ring. The *derivative operator* $D: R[x] \rightarrow R[x]$ is defined, for every $f := a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0 \in R[x]$, by

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

- i. Demonstrate that the operator D is an R -linear map: for all $r, s \in R$ and all $f, g \in R[x]$, we have $D(rf + sg) = rD(f) + sD(g)$.
- ii. Prove that D satisfies the product rule: for all $f, g \in R[x]$, we have $D(fg) = D(f)g + fD(g)$.
- 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 $k \geq 1$ if and only if b is a root of $D(f)$ having multiplicity k .