

5.4 Roots, Multiplicity, and the Formal Derivative

Over $\mathbb{Q}$, the polynomial $x^4 - 2x^3 + 2x - 1$ vanishes at 1 and at -1 , and nowhere else. Yet it has degree 4, and 1 behaves like three roots at once: $x^4 - 2x^3 + 2x - 1 = (x - 1)^3(x + 1)$. This section counts roots properly. It proves that a non-zero polynomial of degree n has at most n roots, that a polynomial over an infinite field is determined by its values, and what it means for a root to be repeated; then it shows how to see a repeated root without factoring, through the formal derivative of Section 4.5.

Here the integers have no twin. Section 5.3 followed *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.3 step by step, but an integer cannot be evaluated at a point. The main new tool is one fact from Section 5.1, the factor theorem (Theorem 5.1.3): c is a root of f if and only if $x - c \mid f$. Throughout, F is a field.

5.4.1 Counting roots

A root of f gives a factor of degree 1. Several distinct roots give several factors, and degrees add, so there cannot be too many of them.

Theorem 5.4.1. Counting Roots

Let F be a field, $f \in F[x]$, $k \geq 1$, and let $c_1, \dots, c_k \in F$ be **distinct** roots of f . Then

$$(x - c_1)(x - c_2) \cdots (x - c_k) \mid f.$$

If $f \neq 0$, then $k \leq \deg f$. In particular, a non-zero polynomial of degree n has at most n distinct roots in F .

Idea. Peel the roots off one at a time. If $f = (x - c_1) \cdots (x - c_{k-1})h$, then the next root c_k must be a root of h : at c_k the product of the factors $c_k - c_i$ is non-zero, because the roots are distinct and a field has no zero divisors. Then the factor theorem splits $x - c_k$ off h . Counting degrees at the end gives $k \leq \deg f$.

Proof. For $k \geq 1$ let $P_k := \prod_{i=1}^k (x - c_i)$, the product of a list in $F[x]$ (the recursion of Section 5.3, after Corollary 5.3.3). We prove “ $P_k \mid f$ for all distinct roots $c_1, \dots, c_k$ of f ” by Logic and Proof, Axiom 4.2.1 on $k \geq 1$ (on ω , Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Corollary 1.7.3 (b)).

For $k = 1$, $P_1 = x - c_1$, and $x - c_1 \mid f$ by Theorem 5.1.3 (b).

Suppose the claim holds for k , and let $c_1, \dots, c_{k+1}$ be distinct roots of f . By the claim for $c_1, \dots, c_k$, $f = P_k h$ for some $h \in F[x]$. Evaluating at c_{k+1} (Theorem 4.4.1, applied factor by factor along the recursion),

$$0 = f(c_{k+1}) = (c_{k+1} - c_1)(c_{k+1} - c_2) \cdots (c_{k+1} - c_k) h(c_{k+1}).$$

Each $c_{k+1} - c_i$ with $i \leq k$ is non-zero, since the roots are distinct, and a product of non-zero elements of a field is non-zero (Theorem 2.1.1 (g), by induction on the number of factors).

So $h(c_{k+1}) = 0$ by Theorem 2.1.1 (f). By Theorem 5.1.3 (b), $h = (x - c_{k+1})h_1$ for some $h_1 \in F[x]$, and by the recursion

$$f = P_k(x - c_{k+1})h_1 = P_{k+1}h_1.$$

So $P_{k+1} \mid f$.

Now let $f \neq 0$ and write $f = P_k h_1$. Then $h_1 \neq 0$, P_k is monic of degree k by (L1) of Section 5.3, and $\deg f = k + \deg h_1 \geq k$ by Theorem 4.3.2 (b). ■

Both hypotheses have a job: “distinct” in the factors $c_{k+1} - c_i \neq 0$, and “field” in the step “a product of non-zero elements is non-zero”.

🕒 **Second reading** · *Dropping a hypothesis*

Without “distinct”: 1, 1 is a list of two roots of $x - 1$, but $(x - 1)^2 \nmid x - 1$, by degrees (Proposition 5.1.1 (d)). Without “field”: over the ring $\mathbb{Z}/8\mathbb{Z}$, which has zero divisors, the polynomial $x^2 - 1$ of degree 2 has the four roots 1, 3, 5, 7, since $3^2 - 1 = 8$, $5^2 - 1 = 24$ and $7^2 - 1 = 48$ are multiples of 8; there $(3 - 1)(3 + 1) = 8 = 0$ with both factors non-zero.

Quick check. Can a polynomial over $\mathbb{Q}$ of degree 3 vanish at 1, 2, 3 and 4? Can a polynomial of degree at most 3?

Solution. Not one of degree 3: it is non-zero, so it has at most 3 distinct roots (Theorem 5.4.1). A polynomial of degree at most 3 can, but only the zero polynomial, whose degree is $-\infty \leq 3$.

5.4.2 Values determine the polynomial

Section 4.4 insisted that a polynomial is not a function: over $\mathbb{F}_2$, $x^2 + x$ and 0 have the same values (Example (Different Polynomials, Equal Functions)). Its warning promised that over a field such as $\mathbb{Q}$ the values do determine the polynomial. Counting roots pays that promise.

Theorem 5.4.2. Polynomials Determined by Values

Let F be a field and $f, g \in F[x]$.

- (a) Let $n \in \mathbb{N}$. If $\deg f \leq n$, $\deg g \leq n$, and $f(c_i) = g(c_i)$ for $n + 1$ distinct elements $c_0, \dots, c_n \in F$, then $f = g$.
- (b) If F is infinite and $f(c) = g(c)$ for **every** $c \in F$, then $f = g$.

Idea. Two polynomials that agree at a point differ by a polynomial with a root there. If they agree at more points than their degree allows, the difference has too many roots, so it is 0. An infinite field has as many points as we need.

Proof. (a) By Theorem 4.3.1, $\deg(f - g) \leq \max(\deg f, \deg g) \leq n$ (the degree of $-g$ is that of g). By Theorem 4.4.1, $(f - g)(c_i) = f(c_i) - g(c_i) = 0$, so $c_0, \dots, c_n$ are $n + 1$ distinct roots of $f - g$. If $f - g \neq 0$, Theorem 5.4.1 gives $n + 1 \leq \deg(f - g) \leq n$, which is false. So $f - g = 0$.

(b) We first find enough distinct elements.

Claim. An infinite set S contains, for every $m \in \mathbb{N}$, a list of m distinct elements: an injective function $\{1, \dots, m\} \rightarrow S$.

Proof. By Logic and Proof, Axiom 4.2.1 on m . For $m = 0$ the empty function works. Suppose $s_1, \dots, s_m$ are distinct elements of S . The set $A := \{s_1, \dots, s_m\}$ has m elements, through the bijection $i \mapsto s_i$, so it is finite (Sets, Relations, and Cardinality, Definition 3.1.2). Since S is infinite (Sets, Relations, and Cardinality, Definition 3.1.3), $A \neq S$, and as $A \subseteq S$, **there is** $s \in S$ with $s \notin A$. Then $s_1, \dots, s_m, s$ are $m + 1$ distinct elements of S . ■

The claim is proved by induction on a statement of the form “there exists a list”, and each step takes one element from a non-empty set, once; no sequence of choices is made, so no axiom of choice is used. Now let $n := \max(\deg f, \deg g, 0) \in \mathbb{N}$. The claim with $S = F$ and $m = n + 1$ gives $n + 1$ distinct elements of F , at which f and g agree, and (a) gives $f = g$. ■

Over $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, which are infinite, equality of polynomials and equality of polynomial functions are therefore the same thing. Two polynomials with integer coefficients that agree at every integer are equal too: read them in $\mathbb{Q}[x]$, and apply (a) at $n + 1$ distinct integers. Part (a) says more, and it says it over every field: $n + 1$ values fix a polynomial of degree at most n . A line is fixed by two points, a parabola by three.

Warning. Over a finite field, (b) fails. For a prime p , every $c \in \mathbb{F}_p$ satisfies $c^p = c$ (Theorem 2.6.6 (a)), so the polynomial $x^p - x$, which is **not** 0 (its coefficient of x^p is 1), vanishes at every element of $\mathbb{F}_p$. For $p = 2$: $0^2 - 0 = 0$ and $1^2 - 1 = 0$, which is Example (Different Polynomials, Equal Functions). For $p = 3$: the values at 0, 1, 2 are 0, 0 and $8 - 2 = 6 = 0$. There is no conflict with (a): a polynomial of degree p needs $p + 1$ points, and $\mathbb{F}_p$ has only p .

Example. Polynomial Functions over a Finite Field

(a) Show that $x^3 + 2x$ and 0 have the same values on $\mathbb{F}_3$, and factor $x^3 + 2x$ in $\mathbb{F}_3[x]$.

(b) Let p be prime. Show that, in $\mathbb{F}_p[x]$,

$$x^p - x = \prod_{c=0}^{p-1} (x - c) = x(x-1)(x-2) \cdots (x-(p-1)).$$

Solution.

(a) In $\mathbb{F}_3$, $2 = -1$, so $x^3 + 2x = x^3 - x$. Its values at $0, 1, 2$ are $0, 1 - 1 = 0$ and $8 - 2 = 6 = 0$: the same as those of 0 , although $x^3 - x \neq 0$. So $0, 1, 2$ are three distinct roots, and by [Theorem 5.4.1](#), $x(x-1)(x-2) \mid x^3 - x$. Both are monic of degree 3, so the cofactor has degree 0 and, comparing leading coefficients, is 1:

$$x^3 + 2x = x(x-1)(x-2) \quad \text{in } \mathbb{F}_3[x].$$

Expanding confirms it: $x(x-1)(x-2) = x^3 - 3x^2 + 2x = x^3 + 2x$, since $3 = 0$.

(b) The elements $0, 1, \dots, p-1$ of $\mathbb{F}_p$ are distinct ([Definition 2.2.1](#)), and each is a root of $x^p - x$ by the warning. By [Theorem 5.4.1](#), the product P of the $x - c$ divides $x^p - x$; P is monic of degree p by (L1) of [Section 5.3](#), and so is $x^p - x$, because $p \geq 2 > 1$. As in (a), $x^p - x = P \cdot u$ with $\deg u = 0$, and comparing leading coefficients gives $u = 1$.

5.4.3 Re-centering at a point

To study a polynomial near a point c , it helps to write it in powers of $x - c$ instead of powers of x . For x^2 and $c = 1$: $x^2 = 1 + 2(x-1) + (x-1)^2$. Such an expansion always exists and is unique, and it is found by dividing by $x - c$ repeatedly.

Theorem 5.4.3. Expansion in Powers of $x - c$

Let F be a field, $f \in F[x]$ with $\deg f = n \geq 0$, and $c \in F$.

(a) There are **unique** $b_0, b_1, \dots, b_n \in F$ with

$$f = \sum_{j=0}^n b_j (x - c)^j.$$

(b) $b_0 = f(c)$, and b_n is the leading coefficient of f .

(c) For every $h \in F$, $f(c + h) = \sum_{j=0}^n b_j h^j$.

By [Theorem 4.3.2 \(b\)](#) and induction on j , each $(x - c)^j$ is monic of degree j ; so a sum $\sum_{j=0}^J d_j (x - c)^j$ with $d_J \neq 0$ has degree **exactly** J : the term $d_J (x - c)^J$ has degree J , every other non-zero term has smaller degree, and [Theorem 4.3.1](#) (with equality when the degrees differ, applied one term at a time) does the rest. The uniqueness half of (a) below uses this fact; part (b) uses its first clause, that $(x - c)^n$ is monic of degree n .

Idea. Divide f by $x - c$: the remainder is the constant $f(c)$, and the quotient has degree one less. Expand the quotient the same way, by induction, and multiply back by $x - c$. For uniqueness, compare degrees: a non-trivial combination of the powers $(x - c)^j$ has the degree of its highest term, so it is not 0.

Proof. (a), *existence.* By Logic and Proof, Axiom 4.2.1 on n , for every f of degree n . If $n = 0$, f is a non-zero constant $b_0 = b_0(x - c)^0$. Let $\deg f = n + 1$. By Theorem 5.1.2 and Theorem 5.1.3 (a), $f = (x - c)q + f(c)$ with $q \in F[x]$. Since $\deg f \geq 1 > \deg f(c)$, Theorem 4.3.1 gives $\deg((x - c)q) = n + 1$, so $q \neq 0$ and $\deg q = n$ (Theorem 4.3.2 (b)). By the induction hypothesis, $q = \sum_{j=0}^n d_j(x - c)^j$. Then

$$f = f(c) + \sum_{j=0}^n d_j(x - c)^{j+1} = \sum_{j=0}^{n+1} b_j(x - c)^j,$$

with $b_0 := f(c)$ and $b_{j+1} := d_j$, by the distributive law for finite sums (Lemma 4.1.1 (b), ($\Sigma 2$)) and a shift of the summation index.

(a), *uniqueness.* If $\sum_{j=0}^n b_j(x - c)^j = \sum_{j=0}^n b'_j(x - c)^j$, then $\sum_{j=0}^n (b_j - b'_j)(x - c)^j = 0$ (Lemma 4.1.1 (b), ($\Sigma 1$), ($\Sigma 4$)). If some $b_j - b'_j$ were non-zero, the largest such j would be the degree of this sum, by the fact before the Idea; but the sum is 0. So $b_j = b'_j$ for every j .

(b) Evaluate at c (Theorem 4.4.1): $(c - c)^0 = 1$ and $(c - c)^j = 0$ for $j \geq 1$, so $f(c) = b_0$. The terms with $j < n$ have degree less than n , and $b_n(x - c)^n$ has coefficient b_n at x^n , since $(x - c)^n$ is monic of degree n ; so the coefficient of x^n in f , its leading coefficient, is b_n .

(c) Evaluate at $c + h$: $(x - c)$ takes the value h there, and Theorem 4.4.1 carries sums, products and powers through. ■

The coefficients b_j are computed by the existence proof: divide by $x - c$, keep the remainder as b_0 , divide the quotient by $x - c$, keep the remainder as b_1 , and so on until the quotient is a constant, which is b_n . The next example runs this.

Quick check. Expand x^3 in powers of $x - 1$ over $\mathbb{Q}$.

Solution. $x^3 = (x - 1)(x^2 + x + 1) + 1$, $x^2 + x + 1 = (x - 1)(x + 2) + 3$, $x + 2 = (x - 1) \cdot 1 + 3$. So $b_0 = 1$, $b_1 = 3$, $b_2 = 3$, $b_3 = 1$:

$$x^3 = 1 + 3(x - 1) + 3(x - 1)^2 + (x - 1)^3.$$

5.4.4 Multiplicity

The hook's polynomial $(x - 1)^3(x + 1)$ is divisible by $(x - 1)^3$ and not by $(x - 1)^4$. That exponent is what "three roots at once" means.

The multiplicity of a root counts how many factors $x - c$ can be split off.

Definition 5.4.1. Multiplicity of a Root

Let F be a field, $f \in F[x]$ **non-zero**, and $c \in F$. The **multiplicity** of c in f , written $\text{mult}_c(f)$, is the **largest** $m \in \mathbb{N}$ with $(x - c)^m \mid f$. The root c is **simple** if $\text{mult}_c(f) = 1$ and

multiple if $\text{mult}_c(f) \geq 2$.

In words: keep dividing f by $x - c$ while the division comes out exact; the number of exact divisions is the multiplicity.

Well defined. The set $M := \{m \in \mathbb{N} : (x - c)^m \mid f\}$ contains 0, since $(x - c)^0 = 1$ divides f . For $m \in M$, $m = \deg(x - c)^m \leq \deg f$ (Proposition 5.1.1 (d)), so M is bounded above, and it has a greatest element (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.6, with $\mathbb{N} \subseteq \mathbb{Z}$). By the factor theorem (Theorem 5.1.3 (b)), $1 \in M$ exactly when $f(c) = 0$, so

$$\text{mult}_c(f) = 0 \iff f(c) \neq 0.$$

For the direction from right to left: if $f(c) \neq 0$, no $m \geq 1$ lies in M either, since $(x - c)^m = (x - c)^{m-1}(x - c)$ (Lemma 4.1.1 (c)), so $(x - c)^m \mid f$ would give $x - c \mid f$ (Proposition 5.1.1 (b)), that is, $1 \in M$. Hence $M = \{0\}$. A multiplicity 0 means “not a root”. The zero polynomial is excluded because every power of $x - c$ divides it, and M would have no greatest element.

Examples. In $\mathbb{Q}[x]$, $\text{mult}_1((x - 1)^2) = 2$: $(x - 1)^2$ divides itself, and $(x - 1)^3$ does not, by degrees. $\text{mult}_0(x^2 + x) = 1$: the value at 0 is 0, and x^2 does not divide $x^2 + x$, since division with remainder gives $x^2 + x = x^2 \cdot 1 + x$ with remainder $x \neq 0$. And $\text{mult}_2(x^2 + x) = 0$, since the value at 2 is $6 \neq 0$.

The definition asks for a largest exponent, which is awkward to check directly. The next lemma replaces it by a single evaluation.

Lemma 5.4.4. Multiplicity through the Cofactor

Let F be a field, $f \in F[x]$ non-zero, $c \in F$ and $m \in \mathbb{N}$.

- (a) $\text{mult}_c(f) = m$ **if and only if** $f = (x - c)^m g$ for some $g \in F[x]$ with $g(c) \neq 0$.
- (b) Such a g is unique.
- (c) If $f = \sum_{j=0}^n b_j(x - c)^j$ is the expansion of Theorem 5.4.3, then $\text{mult}_c(f)$ is the **least** j with $b_j \neq 0$.

Idea. If the cofactor g vanished at c , one more factor $x - c$ would split off; if one more factor split off, cancellation would make g vanish at c . For (c), the expansion displays the cofactor directly.

Proof. (a) $(\Rightarrow)$ Let $m = \text{mult}_c(f)$, so $f = (x - c)^m g$ for some g . If $g(c) = 0$, then $g = (x - c)g_1$ (Theorem 5.1.3 (b)) and $(x - c)^{m+1} \mid f$, against the maximality of m . So $g(c) \neq 0$.

$(\Leftarrow)$ Let $f = (x - c)^m g$ with $g(c) \neq 0$; then $m \in M$. Suppose some $m' > m$ were in M . Then $(x - c)^{m+1}$ divides $(x - c)^{m'}$, hence f : say $f = (x - c)^{m+1} k = (x - c)^m ((x - c)k)$. Canceling $(x - c)^m \neq 0$ (Corollary 4.3.3 (b)) gives $g = (x - c)k$, so $g(c) = 0$, a contradiction. So m is the largest element of M .

(b) If $(x - c)^m g = (x - c)^m g'$, cancel $(x - c)^m \neq 0$.

(c) The coefficient b_n is the leading coefficient of f , so it is non-zero, and the set of j with $b_j \neq 0$ has a least element J (Sets, Relations, and Cardinality, Theorem 2.1.3). The terms

with $j < J$ vanish, so, taking the factor $(x - c)^J$ out of the remaining terms,

$$f = (x - c)^J g, \quad g := \sum_{i=0}^{n-J} b_{J+i}(x - c)^i.$$

Evaluating at c , as in [Theorem 5.4.3](#) (b), $g(c) = b_J \neq 0$. By (a), $\text{mult}_c(f) = J$. ■

The factor g is the **cofactor** of c in f . Multiplicities of a product add, because cofactors multiply.

Proposition 5.4.5. Multiplicity of a Product

Let F be a field, $f, g \in F[x]$ non-zero and $c \in F$. Then $\text{mult}_c(fg) = \text{mult}_c(f) + \text{mult}_c(g)$.

Proof. Let $m := \text{mult}_c(f)$ and $n := \text{mult}_c(g)$. By [Lemma 5.4.4](#) (a), $f = (x - c)^m u$ and $g = (x - c)^n v$ with $u(c) \neq 0$ and $v(c) \neq 0$. Then $fg = (x - c)^{m+n} uv$ ([Lemma 4.1.1](#) (c), commutativity of $F[x]$), $fg \neq 0$ ([Corollary 4.3.3](#) (a); a field is an integral domain), and $(uv)(c) = u(c)v(c) \neq 0$ ([Theorem 4.4.1](#), [Theorem 2.1.1](#) (f)). By [Lemma 5.4.4](#) (a) again, $\text{mult}_c(fg) = m + n$. ■

Quick check. Over $\mathbb{Q}$, find $\text{mult}_0(x^5 + x^3)$ and $\text{mult}_2(x^3 - 4x)$.

Solution. $x^5 + x^3 = x^3(x^2 + 1)$, and the cofactor $x^2 + 1$ has value $1 \neq 0$ at 0, so $\text{mult}_0 = 3$ by [Lemma 5.4.4](#) (a). $x^3 - 4x = (x - 2) \cdot x(x + 2)$, with cofactor value $2 \cdot 4 = 8 \neq 0$ at 2, so $\text{mult}_2 = 1$: a simple root.

All roots can now be split off at once. The roots of a non-zero f form a finite set: otherwise the claim in the proof of [Theorem 5.4.2](#) (b), applied to the set of roots, would give $\deg f + 1$ distinct roots, against [Theorem 5.4.1](#). So they can be listed without repetition.

Theorem 5.4.6. Splitting Off All Roots

Let F be a field and $f \in F[x]$ non-zero. Let $c_1, \dots, c_k \in F$, $k \in \mathbb{N}$, be the distinct roots of f in F (every root of f in F is one of them), and $m_i := \text{mult}_{c_i}(f)$. Then

$$f = (x - c_1)^{m_1} (x - c_2)^{m_2} \cdots (x - c_k)^{m_k} g$$

for some $g \in F[x]$ with **no** root in F , and $m_1 + m_2 + \cdots + m_k \leq \deg f$.

Idea. Split off the full power of one root with [Lemma 5.4.4](#). The cofactor keeps every other root, with the same multiplicity, because the power just removed does not vanish there; induction on the number of roots does the rest.

Proof. By Logic and Proof, Axiom 4.2.1 on k , we prove: for every non-zero f and every list $c_1, \dots, c_k$ of distinct elements of F whose entries are exactly the roots of f in F , the displayed factorization holds with g rootless. For $k = 0$, f has no root, and $g := f$ works with the empty product 1.

Assume the statement for k , and let the roots of f be exactly the distinct $c_1, \dots, c_{k+1}$. By Lemma 5.4.4 (a), $f = (x - c_{k+1})^{m_{k+1}} g_1$ with $g_1(c_{k+1}) \neq 0$; then $g_1 \neq 0$.

The roots of g_1 are exactly $c_1, \dots, c_k$. A root c of g_1 is a root of f (Theorem 4.4.1), and $c \neq c_{k+1}$, so $c = c_i$ with $i \leq k$. Conversely, for $i \leq k$, the polynomial $(x - c_{k+1})^{m_{k+1}}$ has the value $(c_i - c_{k+1})^{m_{k+1}} \neq 0$ at c_i (a power of a non-zero element of a field, Theorem 2.1.1 (g)), so its multiplicity at c_i is 0, and Proposition 5.4.5 gives

$$\text{mult}_{c_i}(g_1) = m_i - 0 = m_i \geq 1.$$

So c_i is a root of g_1 , with the same multiplicity as in f .

The statement for k , applied to g_1 and $c_1, \dots, c_k$, gives $g_1 = \prod_{i=1}^k (x - c_i)^{m_i} g$ with g rootless. Hence, by commutativity and associativity and the recursion of the product,

$$f = \left(\prod_{i=1}^k (x - c_i)^{m_i} \right) (x - c_{k+1})^{m_{k+1}} g = \left(\prod_{i=1}^{k+1} (x - c_i)^{m_i} \right) g.$$

For the degree, the product is monic of degree $\sum_i m_i$ by (L1) of Section 5.3, and $g \neq 0$, so $\deg f = \sum_i m_i + \deg g \geq \sum_i m_i$ (Theorem 4.3.2 (b)).

■

So the multiplicities add up to at most $\deg f$: counted with multiplicity, a non-zero polynomial of degree n still has at most n roots. The case where nothing is left over has a name.

Definition 5.4.2. Splitting over a Field

Let F be a field and $f \in F[x]$ non-zero of degree n . The polynomial f **splits over** F if

$$f = a(x - a_1)(x - a_2) \cdots (x - a_n)$$

for some $a, a_1, \dots, a_n \in F$, repetitions among the a_i allowed. For $n = 0$ this says that $f = a$ is a non-zero constant.

If f splits, the multiplicities of its roots add up to **exactly** n : the rootless factor g of Theorem 5.4.6 is then a constant.

○ **Second reading** · Why nothing is left over

In the factorization of Theorem 5.4.6, suppose the rootless g had degree at least 1; it would have a monic irreducible factor q (Lemma 5.3.5), say $g = qh$. Since $g \mid f$, also $q \mid f$ (Proposition 5.1.1 (b)). As $f \neq 0$, $a \neq 0$, and q divides $a^{-1}f = (x - a_1)(x - a_2) \cdots (x - a_n)$ (Proposition 5.1.1 (c)). By Corollary 5.3.3 (c), $n \geq 1$ and $q \mid x - a_i$ for some i . Each $x - a_i$ is monic and, having degree 1, irreducible (Section 5.3), so Corollary 5.3.3 (d) gives $q = x - a_i$. Then $g(a_i) = q(a_i)h(a_i) = 0$ (Theorem 4.4.1), against g rootless. Hence g is a constant, non-zero as $f \neq 0$, and $\deg f = \sum_i m_i$

(Theorem 4.3.2 (b)).

For example, $x^2 - 2$ does not split over $\mathbb{Q}$: a splitting $a(x - a_1)(x - a_2)$ would make a_1 a rational root, and $a_1^2 = 2$ is impossible (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1). Over $\mathbb{R}$ it splits, as $(x - s)(x + s)$ with s the non-negative square root of 2 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4).

Example. Multiplicities by Repeated Division

Find the roots of $f := x^4 - 2x^3 + 2x - 1 \in \mathbb{Q}[x]$ with their multiplicities, and expand f in powers of $x - 1$.

Solution. The value at 1 is $1 - 2 + 2 - 1 = 0$, so divide by $x - 1$, and keep dividing while the remainder is 0:

$$\begin{aligned} x^4 - 2x^3 + 2x - 1 &= (x - 1)(x^3 - x^2 - x + 1) + 0, \\ x^3 - x^2 - x + 1 &= (x - 1)(x^2 - 1) + 0, \\ x^2 - 1 &= (x - 1)(x + 1) + 0, \\ x + 1 &= (x - 1) \cdot 1 + 2. \end{aligned}$$

So $f = (x - 1)^3(x + 1)$, and the cofactor $x + 1$ has the value $2 \neq 0$ at 1: $\text{mult}_1(f) = 3$ by Lemma 5.4.4 (a). At -1 , the cofactor of $x + 1$ is $(x - 1)^3$, with value $(-2)^3 = -8 \neq 0$, so $\text{mult}_{-1}(f) = 1$. There are no other roots: $f(c) = (c - 1)^3(c + 1) = 0$ forces $c = 1$ or $c = -1$ (Theorem 2.1.1 (f)). The multiplicities add up to $4 = \deg f$, and f splits over $\mathbb{Q}$, with $a = 1$ and $(a_1, a_2, a_3, a_4) = (1, 1, 1, -1)$.

The remainders 0, 0, 0, 2 and the last quotient 1 are the coefficients $b_0, \dots, b_4$ of Theorem 5.4.3 at $c = 1$, by its existence proof:

$$f = 2(x - 1)^3 + (x - 1)^4,$$

and the least j with $b_j \neq 0$ is 3, the multiplicity, as Lemma 5.4.4 (c) says. Expanding $(x - 1)^3((x - 1) + 2)$ confirms the expansion.

5.4.5 Repeated roots and the derivative

Finding multiplicities by division needs the root first. The formal derivative detects repeated roots, and repeated factors, without knowing them. Section 4.5 defined it with no limits: for $f = \sum_k f_k x^k$,

$$f' := \sum_{k \geq 1} (k \cdot f_k) x^{k-1}$$

(Definition 4.5.1), where $k \cdot f_k$ is the k -th multiple and $k \cdot 1$ may be 0 in F . It obeys the rules of calculus (Theorem 4.5.1): it is additive with $(af)' = af'$ for a constant a ; the product rule $(fg)' = f'g + fg'$ holds; and $(g^m)' = (m \cdot 1)g^{m-1}g'$, in particular $((x - c)^m)' = (m \cdot 1)(x - c)^{m-1}$ for $m \geq 1$. In characteristic 0, $f' = 0$ only for constant f , and $\deg f' = \deg f - 1$ when $\deg f \geq 1$ (Proposition 4.5.2 (a)); in characteristic p a non-constant polynomial can have derivative 0: over $\mathbb{F}_2$, $(x^2)' = (2 \cdot 1)x = 0$.

At a double root the graph of a real polynomial touches the axis, with slope 0. The formal

version of that picture needs no graph and no slope.

Theorem 5.4.7. Repeated Roots and the Derivative

Let F be a field, $f \in F[x]$ non-zero and $c \in F$.

- (a) c is a multiple root of f **if and only if** $f(c) = 0$ and $f'(c) = 0$.
- (b) If $\text{mult}_c(f) = m \geq 1$ and $m \cdot 1 \neq 0$ in F , then $f' \neq 0$ and $\text{mult}_c(f') = m - 1$.

Idea. Write $f = (x - c)^m g$ with $g(c) \neq 0$ and differentiate by the product rule. Both terms contain $(x - c)^{m-1}$, so $f' = (x - c)^{m-1} B$ with a bracket B whose value at c is $(m \cdot 1)g(c)$. Everything follows from looking at m and at that value.

Proof. Let $m := \text{mult}_c(f)$. If $m = 0$, then $f(c) \neq 0$, so both sides of (a) are false, and (b) does not apply. Let $m \geq 1$, and write $f = (x - c)^m g$ with $g(c) \neq 0$ (Lemma 5.4.4 (a)). By Theorem 4.5.1,

$$\begin{aligned} f' &= (m \cdot 1)(x - c)^{m-1}g + (x - c)^m g' \\ &= (x - c)^{m-1} B, \quad B := (m \cdot 1)g + (x - c)g'. \end{aligned}$$

At c , $B(c) = (m \cdot 1)g(c)$ (Theorem 4.4.1).

(a) Here $f(c) = 0$. If $m \geq 2$, then $m - 1 \geq 1$ and $f'(c) = 0^{m-1}B(c) = 0$. If $m = 1$, then $f' = B$ and $f'(c) = (1 \cdot 1)g(c) = g(c) \neq 0$. So $f'(c) = 0$ exactly when $m \geq 2$, that is, when c is a multiple root.

(b) If $m \cdot 1 \neq 0$, then $B(c) = (m \cdot 1)g(c) \neq 0$ by Theorem 2.1.1 (f). So $B \neq 0$, hence $f' \neq 0$ (Corollary 4.3.3), and Lemma 5.4.4 (a) applied to $f' = (x - c)^{m-1}B$ gives $\text{mult}_c(f') = m - 1$. ■

The hypothesis $m \cdot 1 \neq 0$ in (b) is needed. Over $\mathbb{F}_3$, $f = x^3$ has $\text{mult}_0(f) = 3$, but $f' = (3 \cdot 1)x^2 = 0$, whose multiplicity is not even defined. Part (a) holds over every field.

Remark. **The polynomial $x^p - x$ has only simple roots.** Over $\mathbb{F}_p$, $(x^p - x)' = (p \cdot 1)x^{p-1} - 1$ by Theorem 4.5.1, and this is -1 , since $p \cdot 1 = 0$ in $\mathbb{F}_p$ (Example (The characteristics of the standard fields): $\text{char } \mathbb{F}_p = p$). The derivative -1 vanishes nowhere, so by (a) no root of $x^p - x$ is multiple. By Example (Polynomial Functions over a Finite Field) (b), every $c \in \mathbb{F}_p$ is a root, and each is simple: $x^p - x$ is the product of the p distinct factors $x - c$. This is the fact that Section 4.5's warning set aside.

The same computation, with an irreducible factor in place of $x - c$, detects repeated factors through a gcd, which the Euclidean algorithm of Section 5.2 computes without factoring anything.

Corollary 5.4.8. Repeated Factors and the Greatest Common Divisor

Let F be a field and $f \in F[x]$ with $\deg f \geq 1$.

- (a) If $p \in F[x]$ is irreducible and $p^2 \mid f$, then $p \mid \gcd(f, f')$. So if $\gcd(f, f') = 1$, no irreducible divides f twice, and f has no multiple root in F .
- (b) If F has characteristic 0 (Definition 2.5.1) and $\gcd(f, f') \neq 1$, then $p^2 \mid f$ for some irreducible p .

Idea. For (a), differentiate p^2g : every term keeps a factor p . For (b), take an irreducible p dividing both f and f' . If p divided f only once, $f = pg$, then p would divide $f' - pg' = p'g$, and hence p' , which in characteristic 0 is non-zero of smaller degree.

Proof. (a) Write $f = p^2g$. By Theorem 4.5.1,

$$f' = (2 \cdot 1)pp'g + p^2g' = p((2 \cdot 1)p'g + pg'),$$

so p divides both f and f' , and hence divides $\gcd(f, f')$ (Theorem 5.2.2 (b); $f \neq 0$). If $\gcd(f, f') = 1$, this would give $p \mid 1$, impossible since $\deg p \geq 1$ (Proposition 5.1.1 (d)). A multiple root c would give $(x - c)^2 \mid f$ with $x - c$ irreducible.

(b) Let $d := \gcd(f, f')$. It is monic ($f \neq 0$) and $d \neq 1$, so $\deg d \geq 1$, and d has a monic irreducible divisor p (Lemma 5.3.5). Then $p \mid f$ and $p \mid f'$ (Proposition 5.1.1 (b)). As for multiplicities, the set of $m \in \mathbb{N}$ with $p^m \mid f$ contains 0 and 1 and is bounded by $\deg f$ ($m \leq m \deg p = \deg p^m$); let $m \geq 1$ be its greatest element and write $f = p^m g$. Then $p \nmid g$, since otherwise $p^{m+1} \mid f$.

Suppose $m = 1$. Then $f' = p'g + pg'$, and p divides f' and pg' , so $p \mid f' - pg' = p'g$ (Proposition 5.1.1 (c)). By Corollary 5.3.3 (b), $p \mid p'$ or $p \mid g$, and $p \nmid g$. But F has characteristic 0 and $\deg p \geq 1$, so $p' \neq 0$ and $\deg p' = \deg p - 1 < \deg p$ (Proposition 4.5.2 (a)); then $p \nmid p'$ by Proposition 5.1.1 (d). This contradiction shows $m \geq 2$, and $p^2 \mid f$. ■

Characteristic 0 is used once, at $\deg p' = \deg p - 1$. Over $\mathbb{Q}$, a polynomial f therefore has a repeated irreducible factor exactly when $\gcd(f, f') \neq 1$, and that question is answered by the Euclidean algorithm (Theorem 5.2.5) with no factoring at all.

Quick check. Is 1 a multiple root of $x^3 - 3x + 2 \in \mathbb{Q}[x]$?

Solution. Yes. $f(1) = 1 - 3 + 2 = 0$, $f' = 3x^2 - 3$ and $f'(1) = 0$, so Theorem 5.4.7 (a) applies. Indeed $x^3 - 3x + 2 = (x - 1)^2(x + 2)$.

5.4.6 Exercises

5.4.6.1 A. Check your understanding

Exercise. A1

- (a) Find mult_1 and mult_{-1} of $x^4 - 2x^3 + 2x - 1 \in \mathbb{Q}[x]$.
- (b) In $\mathbb{F}_3[x]$, let $f = x^3$. Is 0 a multiple root by the test of [Theorem 5.4.7](#) (a)? Does part (b) apply?
- (c) True or false: a polynomial over $\mathbb{Q}$ of degree at most 2 that vanishes at 1, 2, 3 is the zero polynomial.
- (d) True or false: a polynomial over $\mathbb{F}_2$ that vanishes at every element of $\mathbb{F}_2$ is the zero polynomial.

Solution.

- (a) 3 and 1 ([Example \(Multiplicities by Repeated Division\)](#)).
- (b) Yes: $f(0) = 0$ and $f' = (3 \cdot 1)x^2 = 0$, so $f'(0) = 0$, and 0 is a multiple root (its multiplicity is 3). Part (b) does not apply: $m = 3$ and $3 \cdot 1 = 0$ in $\mathbb{F}_3$; indeed $f' = 0$, and its multiplicity is not 2, it is not defined.
- (c) True: a non-zero polynomial of degree at most 2 has at most 2 distinct roots ([Theorem 5.4.1](#)), or [Theorem 5.4.2](#) (a) with $n = 2$ and $g = 0$.
- (d) False: $x^2 + x \neq 0$ vanishes at 0 and 1 ([Example \(Different Polynomials, Equal Functions\)](#)). Part (b) of [Theorem 5.4.2](#) needs an infinite field.

5.4.6.2 B. Practice

Exercise. B1: Put the proof in order

The following lines contain a proof of the divisibility part of [Theorem 5.4.1](#), shuffled, together with two lines that do not belong. Write the seven correct lines in an order that makes a proof, say which other orders are also admissible, and say why each of the other two lines fails.

- (i) We use induction on k ; for $k = 1$, $x - c_1 \mid f$ by the factor theorem.
- (ii) Assume the claim for every list of $k - 1$ distinct roots, and let $c_1, \dots, c_k$ be distinct roots of f .
- (iii) Write $f = (x - c_1) \cdots (x - c_{k-1}) h$.
- (iv) Evaluate at c_k : $0 = (c_k - c_1) \cdots (c_k - c_{k-1}) h(c_k)$.
- (v) Each $c_k - c_i$, $i < k$, is non-zero, since the roots are distinct.
- (v') Each $c_k - c_i$, $i < k$, is non-zero, since $c_k \neq 0$.
- (vi) A product of non-zero elements of a field is non-zero, so $h(c_k) = 0$.
- (vi') $h(c_k) = 0$, because $f(c_k) = 0$.
- (vii) By the factor theorem, $h = (x - c_k)h_1$, so $f = (x - c_1) \cdots (x - c_k) h_1$.

Solution. An admissible order is (i), (ii), (iii), (iv), (v), (vi), (vii):

We use induction on k ; for $k = 1$, $x - c_1 \mid f$ by the factor theorem. Assume the claim for every list of $k - 1$ distinct roots, and let $c_1, \dots, c_k$ be distinct roots of f . Write $f = (x - c_1) \cdots (x - c_{k-1})h$. Evaluate at c_k : $0 = (c_k - c_1) \cdots (c_k - c_{k-1})h(c_k)$. Each $c_k - c_i$, $i < k$, is non-zero, since the roots are distinct. A product of non-zero elements of a field is non-zero, so $h(c_k) = 0$. By the factor theorem, $h = (x - c_k)h_1$, so $f = (x - c_1) \cdots (x - c_k)h_1$.

Lines (i) and (ii) set up the induction and come first, in that order; (iii) uses the hypothesis of (ii). Line (v) uses only the distinctness from (ii), so it may come anywhere after (ii) and before (vi); in particular (iv) and (v) may be exchanged, and (v) may even precede (iii). Line (vi) needs both (iv) and (v), and (vii) needs (vi) and (iii). So the admissible orders are: (i), (ii), then (iii), (iv), (v) with (iv) after (iii) and (v) anywhere among them, then (vi), (vii).

The distractor (v') gives a wrong reason: $c_k = 0$ is allowed, and $c_k \neq 0$ says nothing about $c_k - c_i$. The distractor (vi') skips the cancellation: $f(c_k) = 0$ only says that the product in (iv) is 0, and passing to $h(c_k) = 0$ needs both (v) and the absence of zero divisors. Over a ring with zero divisors the step fails: over $\mathbb{Z}/8\mathbb{Z}$, $x^2 - 1 = (x - 1)(x + 1)$ has the root 3, yet neither factor vanishes at 3.

Exercise. B2: Expansions at a point

- (a) Expand $x^3 - 2x + 5 \in \mathbb{Q}[x]$ in powers of $x - 1$.
- (b) Find $\text{mult}_{-2}(x^3 - 3x + 2)$ from the first two coefficients of an expansion in powers of $x + 2$.

Solution.

- (a) Divide by $x - 1$ three times:

$$\begin{aligned} x^3 - 2x + 5 &= (x - 1)(x^2 + x - 1) + 4, \\ x^2 + x - 1 &= (x - 1)(x + 2) + 1, \\ x + 2 &= (x - 1) \cdot 1 + 3. \end{aligned}$$

By the existence proof of [Theorem 5.4.3](#), $x^3 - 2x + 5 = 4 + (x - 1) + 3(x - 1)^2 + (x - 1)^3$. Expanding the right side gives back $x^3 - 2x + 5$.

- (b) Here $c = -2$ and $x - c = x + 2$. First $x^3 - 3x + 2 = (x + 2)(x^2 - 2x + 1) + 0$, so $b_0 = 0$; then $x^2 - 2x + 1 = (x + 2)(x - 4) + 9$, so $b_1 = 9 \neq 0$. By [Lemma 5.4.4](#) (c), $\text{mult}_{-2} = 1$: -2 is a simple root.

Exercise. B3: Functions on a finite field

Let p be prime and $f, g \in \mathbb{F}_p[x]$. Prove that $f(c) = g(c)$ for every $c \in \mathbb{F}_p$ if and only if $x^p - x \mid f - g$. Then find a polynomial of degree less than 5 with the same values on $\mathbb{F}_5$ as $x^7 + x$.

Solution. ($\Leftarrow$) If $f - g = (x^p - x)h$, then for $c \in \mathbb{F}_p$, $f(c) - g(c) = (c^p - c)h(c) = 0$, since $c^p = c$ ([Theorem 2.6.6](#) (a)).

($\Rightarrow$) If f and g agree on $\mathbb{F}_p$, then $0, 1, \dots, p-1$ are p distinct roots of $f - g$, so $\prod_{c=0}^{p-1} (x - c) \mid f - g$ by [Theorem 5.4.1](#), and that product is $x^p - x$ ([Example \(Polynomial Functions over a Finite Field\)](#) (b)).

For $p = 5$: $x^7 = x^2 \cdot x^5$, and $x^7 - x^3 = x^2(x^5 - x)$, so $(x^7 + x) - (x^3 + x) = x^2(x^5 - x)$ is

a multiple of $x^5 - x$. By the first part, $x^3 + x$ has the same values as $x^7 + x$ on $\mathbb{F}_5$, and its degree is $3 < 5$.

5.4.6.3 C. Going deeper

Exercise. C1: The coefficients as derivatives

Let F be a field of characteristic 0, $f \in F[x]$ of degree $n \geq 0$, $c \in F$, and $f = \sum_{j=0}^n b_j(x-c)^j$ as in Theorem 5.4.3. Prove that

$$b_j = \frac{f^{(j)}(c)}{j! \cdot 1} \quad (0 \leq j \leq n),$$

where $f^{(j)}$ is the j -th formal derivative (Definition 4.5.1). Check the formula on the expansion of Exercise B2 (a) at $j = 2$.

Solution (Hint 1). Compute the j -th derivative of $(x-c)^i$ first.

Solution (Hint 2). By induction on j , $((x-c)^i)^{(j)} = ((i(i-1)\cdots(i-j+1)) \cdot 1)(x-c)^{i-j}$ for $j \leq i$, and 0 for $j > i$.

Solution. The derivatives of the powers. We prove the formula of Hint 2 by Logic and Proof, Axiom 4.2.1 on j , for all i . For $j = 0$ the coefficient is the empty product 1. Suppose it holds for j . If $j+1 \leq i$, then $i-j \geq 1$ and, by Theorem 4.5.1 (a) and (c),

$$((x-c)^i)^{(j+1)} = ((i \cdots (i-j+1)) \cdot 1)((i-j) \cdot 1)(x-c)^{i-j-1},$$

and $(u \cdot 1)(v \cdot 1) = (uv) \cdot 1$ (Lemma 2.5.1 (b)) gives the coefficient $(i \cdots (i-j)) \cdot 1$. If $j+1 = i+1$, the i -th derivative is the constant $(i! \cdot 1)$, whose derivative is 0; and the derivative of 0 is 0 for larger j .

The coefficients. Since the derivative is additive with $(af)' = af'$ for constants a (Theorem 4.5.1 (a)), so is the j -th derivative (induction on j), and

$$f^{(j)} = \sum_{i=j}^n b_i((i \cdots (i-j+1)) \cdot 1)(x-c)^{i-j}.$$

At $x = c$, every term with $i > j$ vanishes, and the term $i = j$ is $b_j(j! \cdot 1)$. So $f^{(j)}(c) = (j! \cdot 1)b_j$. In characteristic 0, $j! \cdot 1 \neq 0$ (Definition 2.5.1, as $j! \geq 1$), and dividing gives the formula.

Check. For $f = x^3 - 2x + 5$, $f'' = 6x$ and $f''(1) = 6$, so $b_2 = 6/2 = 3$, as in Exercise B2 (a).

Exercise. C2: Repeated factors through the gcd

- (a) Using only $\gcd(f, f')$, decide whether $f := x^4 - 2x^3 + 2x - 1 \in \mathbb{Q}[x]$ has a repeated irreducible factor.

- (b) Over $\mathbb{F}_2$, let $f := x^4 + 1$. Compute f' and $\gcd(f, f')$, and explain why part (b) of [Corollary 5.4.8](#) does not apply.

Solution.

- (a) $f' = 4x^3 - 6x^2 + 2$. The Euclidean algorithm (Theorem 5.2.5):

$$\begin{aligned} f &= \left(\frac{1}{4}x - \frac{1}{8}\right)f' - \frac{3}{4}(x^2 - 2x + 1), \\ f' &= \left(-\frac{3}{4}(x^2 - 2x + 1)\right)\left(-\frac{8}{3}(2x + 1)\right) + 0. \end{aligned}$$

The last non-zero remainder is $-\frac{3}{4}(x^2 - 2x + 1)$, so $\gcd(f, f') = x^2 - 2x + 1 \neq 1$. As $\mathbb{Q}$ has characteristic 0, [Corollary 5.4.8](#) (b) says that f has a repeated irreducible factor. (Indeed $f = (x - 1)^3(x + 1)$, [Example \(Multiplicities by Repeated Division\)](#).)

- (b) $f' = (4 \cdot 1)x^3 = 0$ in $\mathbb{F}_2$. Then $\langle f, 0 \rangle = \langle f \rangle$, whose monic generator is f itself, so $\gcd(f, f') = f = x^4 + 1 \neq 1$ (Theorem 5.2.2 (c)). Part (b) of the corollary assumes characteristic 0, and $\mathbb{F}_2$ has characteristic 2 (Definition 2.5.1: $1 \neq 0$, $2 \cdot 1 = 0$). Its proof uses that hypothesis at $\deg p' = \deg p - 1$, which fails in characteristic 2: $(x^2 + 1)' = 0$. Here the conclusion happens to hold anyway, since $x^4 + 1 = (x + 1)^4$ in $\mathbb{F}_2$, but it is not given by the corollary; the gcd f records only that $f' = 0$.