

0.8 Polynomials

We now have fields: number systems in which we can add, subtract, multiply, and divide by anything nonzero. The next objects built on top of a field are polynomials. They will be everywhere in this book: as examples of vectors in Chapter 1, as the characteristic and minimal polynomials of a matrix later on, and as the reason some fields behave differently from others. This section says precisely what a polynomial is, introduces its degree, and explains why a polynomial is **not** the same thing as the function it defines.

0.8.1 What a polynomial is

At school, a polynomial is “an expression like $3x^2 - x + 2$ ”. That is a good picture, but it leaves one question open: what is x ? One tempting answer is that x is a number to be plugged in, so a polynomial is really a function. This answer breaks down as soon as we leave the familiar number systems.

Work over the field $\mathbb{F}_2 = \{0, 1\}$ of Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$), where $1 + 1 = 0$. The expressions $x^2 + x$ and 0 look different. But if we plug in the two elements of $\mathbb{F}_2$, we get $0^2 + 0 = 0$ and $1^2 + 1 = 1 + 1 = 0$. As functions on $\mathbb{F}_2$, the two are the same. If a polynomial *were* its function, then $x^2 + x$ would be the zero polynomial, and it would have no sensible degree. We want $x^2 + x$ to be a genuine polynomial of degree 2, so we must define polynomials by their coefficients alone.

A polynomial is its list of coefficients, and nothing else.

Definition 0.8.1. Polynomial

Let F be a field. A **polynomial over F** in the indeterminate x is a sequence $(a_0, a_1, a_2, \dots)$ of elements of F , indexed by $\mathbb{N}$, such that **only finitely many** a_k are nonzero. That is, there is some $N \in \mathbb{N}$ with $a_k = 0$ **for every** $k > N$.

The element a_k is the **coefficient of x^k** . We write the polynomial as

$$p = a_0 + a_1x + a_2x^2 + \cdots + a_Nx^N = \sum_{k=0}^N a_kx^k.$$

Two polynomials $p = \sum a_kx^k$ and $q = \sum b_kx^k$ are **equal** if and only if $a_k = b_k$ **for every** $k \in \mathbb{N}$.

In words: a polynomial is an infinite list of coefficients that is eventually all zero. The expression $\sum_{k=0}^N a_kx^k$ is only a way of displaying the list: x^k marks the position k , and we stop writing once the remaining coefficients are all zero. Two polynomials are equal exactly when they agree position by position. A sequence indexed by $\mathbb{N}$ is a function $\mathbb{N} \rightarrow F$, so this is just equality of functions in the sense of Definition 0.4.1.

There is one thing to check about the notation. The number N in the display is not unique: if $a_k = 0$ for every $k > N$, the same is true for every $k > N + 1$. Writing $\sum_{k=0}^N a_kx^k$ or $\sum_{k=0}^{N+1} a_kx^k$ only adds a term $0 \cdot x^{N+1}$, which we agree to drop. So the display names the same sequence whichever admissible N we use. We also drop terms with zero coefficient in the middle, write x for $1 \cdot x^1$, and write a_0 for a_0x^0 .

Example. Polynomials over various fields

Read off the coefficient sequence of each polynomial, and check it against [Definition 0.8.1](#).

$$\begin{aligned} 3x^2 - x + 2 &\in \mathbb{R}[x], & x^5 + \pi x^3 - \sqrt{2} &\in \mathbb{R}[x], \\ (1+i)x - i &\in \mathbb{C}[x], & x^2 + x &\in \mathbb{F}_2[x], \\ 7, & & 0. \end{aligned}$$

(The symbol $F[x]$ for the set of all polynomials over F is defined formally in [Definition 0.8.2](#) below.)

Solution. The first is the sequence $(2, -1, 3, 0, 0, \dots)$ of real numbers. It has finitely many nonzero terms, so it is a polynomial over $\mathbb{R}$.

The second is $(-\sqrt{2}, 0, 0, \pi, 0, 1, 0, \dots)$. Its coefficients are real but irrational; the definition only asks that they lie in the field.

The third is $(-i, 1+i, 0, \dots)$, a polynomial over $\mathbb{C}$.

The fourth is $(0, 1, 1, 0, \dots)$ with entries in $\mathbb{F}_2$. It is **not** the zero sequence, so it is not the zero polynomial, even though it vanishes at both points of $\mathbb{F}_2$.

The constant 7 is the sequence $(7, 0, 0, \dots)$. It is a polynomial over $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. Over $\mathbb{F}_2$ it would be $(1, 0, 0, \dots)$, because $7 = 1$ there.

The last, $0 = (0, 0, 0, \dots)$, is the **zero polynomial**. It is the degenerate case: every coefficient is zero, and the finiteness condition holds with $N = 0$. It matters because it is the one polynomial whose degree needs a special convention, as we will see.

Now the nonexample, by a minimal change. Take the polynomial $1 + x + x^2$, whose sequence is $(1, 1, 1, 0, 0, \dots)$, and change every later 0 to 1. The result $(1, 1, 1, 1, \dots)$, informally “ $1 + x + x^2 + x^3 + \dots$ ”, is still a sequence of elements of $\mathbb{R}$. What fails is the clause **only finitely many** coefficients are nonzero, so this is **not** a polynomial. (It is a *formal power series*, which we will not need.) Expressions such as $x^{-1} + 1$ and $\sqrt{x}$ are not polynomials either: they are not of the form $\sum a_k x^k$ with $k \in \mathbb{N}$ at all.

Why insist on finitely many nonzero coefficients? Because we want to plug elements of the field into polynomials, which means forming the sum $\sum a_k c^k$, and in a field only finite sums make sense. Finiteness is also what gives every nonzero polynomial a highest power, its degree.

0.8.2 Adding and multiplying polynomials

The coefficient picture tells us how to add and multiply. Adding $3x^2 - x + 2$ and $x + 5$ at school means collecting like powers, so we add coefficients position by position. Multiplying means expanding every product $a_i x^i \cdot b_j x^j = a_i b_j x^{i+j}$ and collecting like powers, so the coefficient of x^k collects all pairs (i, j) with $i + j = k$.

Definition 0.8.2. The polynomial ring $F[x]$

Let F be a field. The set of **all** polynomials over F is denoted $F[x]$. For $p = \sum a_k x^k$ and

$q = \sum b_k x^k$ in $F[x]$, define the **sum** $p + q$ and the **product** pq by their coefficients:

$$p + q = \sum_k (a_k + b_k) x^k, \quad pq = \sum_k \left(\sum_{i=0}^k a_i b_{k-i} \right) x^k.$$

We must check that $p + q$ and pq are again polynomials, that is, that their coefficient sequences are eventually zero. Suppose $a_i = 0$ for every $i > m$ and $b_j = 0$ for every $j > n$. If $k > \max(m, n)$, then $a_k + b_k = 0 + 0 = 0$. If $k > m + n$, then in each product $a_i b_{k-i}$ either $i > m$ or $k - i > n$, because otherwise $k = i + (k - i) \leq m + n$. So every term is 0, and the coefficient of x^k in pq is 0. Hence both are polynomials, and addition and multiplication are well defined on $F[x]$.

With this multiplication, $x \cdot x$ has coefficient sequence $(0, 0, 1, 0, \dots)$, and by induction on k the k -th power of the polynomial x is the sequence with a 1 in position k and 0 elsewhere. So the notation x^k in [Definition 0.8.1](#) agrees with the actual power, and $\sum a_k x^k$ is an honest sum of products.

Example. A product, coefficient by coefficient

In $\mathbb{R}[x]$, compute $(3x^2 - x + 2)(x + 1)$ from the definition.

Solution. Here $(a_0, a_1, a_2) = (2, -1, 3)$ and $(b_0, b_1) = (1, 1)$, with all other coefficients 0. The coefficient of x^k in the product is $\sum_{i=0}^k a_i b_{k-i}$:

$$k = 0 : a_0 b_0 = 2,$$

$$k = 1 : a_0 b_1 + a_1 b_0 = 2 - 1 = 1,$$

$$k = 2 : a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 - 1 + 3 = 2,$$

$$k = 3 : a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 0 + 0 + 3 + 0 = 3,$$

and every coefficient with $k \geq 4$ is 0 by the argument above (here $m + n = 3$). Hence $(3x^2 - x + 2)(x + 1) = 3x^3 + 2x^2 + x + 2$, which is what expanding by hand gives.

The operations obey the rules we expect. We record them once, so that later sections can use them freely.

Theorem 0.8.1. Arithmetic in $F[x]$

Let F be a field and $p, q, r \in F[x]$. Then:

1. $p + q = q + p$ and $(p + q) + r = p + (q + r)$;
2. $p + 0 = p$, and $p + (-p) = 0$, where $-p = \sum (-a_k) x^k$;
3. $pq = qp$ and $(pq)r = p(qr)$;
4. $1 \cdot p = p$, where 1 is the constant polynomial $(1, 0, 0, \dots)$;
5. $p(q + r) = pq + pr$.

Idea. Two polynomials are equal when their coefficients agree, so each identity reduces to an identity between coefficients, which the field axioms supply. For products it helps to write the coefficient of x^k in pq symmetrically, as a sum over all pairs (i, j) of natural numbers with $i + j = k$.

Proof. Let $p = \sum a_k x^k$, $q = \sum b_k x^k$, and $r = \sum c_k x^k$. By Definition 0.8.1, it suffices to compare the coefficient of x^k on both sides, for each $k \in \mathbb{N}$.

Parts 1, 2, and 4 hold because in each position they are the corresponding field axioms of Definition 0.7.1: for example, the coefficient of x^k in $p + q$ is $a_k + b_k = b_k + a_k$, the coefficient in $q + p$. For 4, the coefficient of x^k in $1 \cdot p$ is $\sum_{i+j=k} e_i a_j$ with $e_0 = 1$ and $e_i = 0$ for $i \geq 1$, which equals a_k .

For 3, the coefficient of x^k in pq is $\sum_{i+j=k} a_i b_j$. Since multiplication in F is commutative, this equals $\sum_{i+j=k} b_j a_i$, the coefficient in qp . Next, the coefficient of x^k in $(pq)r$ is

$$\sum_{s+l=k} \left(\sum_{i+j=s} a_i b_j \right) c_l = \sum_{i+j+l=k} a_i b_j c_l,$$

where the equality uses distributivity and associativity in F . The same computation for $p(qr)$ gives $\sum_{i+s=k} a_i (\sum_{j+l=s} b_j c_l) = \sum_{i+j+l=k} a_i b_j c_l$. Therefore $(pq)r = p(qr)$.

For 5, the coefficient of x^k in $p(q + r)$ is $\sum_{i+j=k} a_i (b_j + c_j) = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j$ by distributivity in F , which is the coefficient in $pq + pr$. This proves the theorem. ■

A set with an addition and a multiplication satisfying these rules is called a **commutative ring**; this is where the name “polynomial ring” comes from. We will not need the word again in this chapter. What matters is that we may now calculate with polynomials exactly as at school.

Quick check. Over $\mathbb{R}$, are $(x+1)^2$ and $x^2 + 2x + 1$ equal as polynomials? Over $\mathbb{F}_2$, are $(x+1)^2$ and $x^2 + 1$ equal as polynomials?

Solution. Both answers are yes, but for a reason that depends on the field. Expanding gives $(x+1)^2 = x^2 + 2x + 1$, with coefficient sequence $(1, 2, 1, 0, \dots)$. Over $\mathbb{R}$ this is exactly the sequence of $x^2 + 2x + 1$. Over $\mathbb{F}_2$ we have $2 = 1 + 1 = 0$, so the sequence is $(1, 0, 1, 0, \dots)$, which is the sequence of $x^2 + 1$.

0.8.3 Degree

The most useful single number attached to a polynomial is the highest power of x that actually occurs. Every nonzero polynomial has one: it has at least one nonzero coefficient and only finitely many, so there is a largest position holding a nonzero coefficient. The zero polynomial has no such position, and we must decide what to do with it.

Definition 0.8.3. Degree

Let $p = \sum a_k x^k \in F[x]$.

- If $p \neq 0$, the **degree** of p , written $\deg p$, is the **largest** $n \in \mathbb{N}$ with $a_n \neq 0$. The coefficient a_n is the **leading coefficient** of p , and p is **monic** if its leading coefficient is 1.

- The zero polynomial has degree $\deg 0 = -\infty$.

We use the conventions $-\infty < n$ and $-\infty + n = n + (-\infty) = -\infty$ for every $n \in \mathbb{N}$, and $-\infty + (-\infty) = -\infty$.

Examples, simplest first. A nonzero constant c has degree 0; its leading coefficient is c . The polynomial $x + 5 \in \mathbb{R}[x]$ is monic of degree 1. The polynomial $3x^3 + 2x^2 + x + 2$ from [Example \(A product, coefficient by coefficient\)](#) has degree 3 and leading coefficient 3. Over $\mathbb{F}_2$, $x^2 + x$ has degree 2, even though it vanishes at every point of $\mathbb{F}_2$.

Why $-\infty$, and not 0 or -1 ? Look at the formula we expect: the degree of a product is the sum of the degrees. With $\deg 0 = 0$ it fails at once, since $0 \cdot x = 0$ would give $0 = \deg 0 = \deg 0 + \deg x = 1$. With $\deg 0 = -1$ it fails too: $-1 = \deg(0 \cdot x) \neq \deg 0 + \deg x = 0$. The formula needs $\deg 0 + n = \deg 0$ for every n , and $-\infty$ is exactly the symbol with that property. The convention keeps a formula true, and that is its only job.

It turns out that the degree of a sum is controlled by the larger degree, and the degree of a product is the sum of the degrees:

Theorem 0.8.2. Degree of a sum

Let F be a field and $p, q \in F[x]$. Then

$$\deg(p + q) \leq \max(\deg p, \deg q),$$

with **equality** whenever $\deg p \neq \deg q$.

Proof. Let $p = \sum a_k x^k$, $q = \sum b_k x^k$, and $M = \max(\deg p, \deg q)$. If $M = -\infty$, then $p = q = 0$, so $p + q = 0$ and both sides are $-\infty$. Suppose $M \in \mathbb{N}$. For every $k > M$ we have $k > \deg p$ and $k > \deg q$, so $a_k = b_k = 0$ by [Definition 0.8.3](#). Hence the coefficient $a_k + b_k$ of x^k in $p + q$ is 0 for every $k > M$, and therefore $\deg(p + q) \leq M$.

Now suppose $\deg p \neq \deg q$; by symmetry we may assume $\deg p > \deg q$, so $M = \deg p \in \mathbb{N}$. Then $a_M \neq 0$ and $b_M = 0$, because $M > \deg q$. The coefficient of x^M in $p + q$ is $a_M + 0 = a_M \neq 0$, so $\deg(p + q) \geq M$. Together with the first part, $\deg(p + q) = M$. This proves the theorem. ■

The inequality can be strict: over any field, $\deg(x + (-x)) = \deg 0 = -\infty < 1$. The leading terms cancel. That is the only way the degree of a sum can drop.

Theorem 0.8.3. Degree of a product

Let F be a field and $p, q \in F[x]$. Then

$$\deg(pq) = \deg p + \deg q.$$

If p and q are nonzero, the leading coefficient of pq is the product of their leading coefficients.

Idea. Expanding $(a_mx^m + \text{lower terms})(b_nx^n + \text{lower terms})$, the only way to reach x^{m+n} is $a_mx^m \cdot b_nx^n$, and nothing reaches beyond. So the top coefficient is a_mb_n . The one real question is whether a_mb_n could be 0. In a field it cannot, and this is exactly where the field axioms enter.

Proof. If $p = 0$ or $q = 0$, then $pq = 0$ by the definition of the product, so both sides equal $-\infty$ by the conventions in Definition 0.8.3. Suppose now $p = \sum a_kx^k$ and $q = \sum b_kx^k$ are nonzero, with $m = \deg p$ and $n = \deg q$. Then $a_m \neq 0$, $b_n \neq 0$, $a_i = 0$ for $i > m$, and $b_j = 0$ for $j > n$.

We showed after Definition 0.8.2 that the coefficient of x^k in pq is 0 for every $k > m + n$. For $k = m + n$, the coefficient is $\sum_{i+j=m+n} a_ib_j$. A term with $i > m$ has $a_i = 0$, and a term with $i < m$ has $j = m + n - i > n$, so $b_j = 0$. Hence only $i = m$, $j = n$ survives, and the coefficient is a_mb_n .

Since $a_m \neq 0$ and $b_n \neq 0$, Theorem 0.7.1 gives $a_mb_n \neq 0$, because a product of nonzero elements of a field is nonzero. Therefore $\deg(pq) = m + n$ and the leading coefficient of pq is a_mb_n , as claimed. ■

Warning. The field axioms are doing real work here. The same definitions make sense with coefficients in $\mathbb{Z}/6\mathbb{Z}$, which is **not** a field. There $(2x+1)(3x^2+x) = 6x^3 + 5x^2 + x = 5x^2 + x$, because $2 \cdot 3 = 6 = 0$. The factors have degrees 1 and 2, but the product has degree 2, not 3.

The first consequence is that polynomials over a field behave like integers: a product can only be zero if a factor is, and nonzero factors can be canceled.

Corollary 0.8.4. No zero divisors in $F[x]$

Let F be a field and $p, q, r \in F[x]$.

1. If $pq = 0$, then $p = 0$ or $q = 0$.
2. If $pq = pr$ and $p \neq 0$, then $q = r$.

Proof. For 1, we prove the contrapositive. Suppose $p \neq 0$ and $q \neq 0$. Then $\deg p, \deg q \in \mathbb{N}$, so by Theorem 0.8.3, $\deg(pq) = \deg p + \deg q \in \mathbb{N}$. In particular $\deg(pq) \neq -\infty$, so $pq \neq 0$.

For 2, suppose $pq = pr$ and $p \neq 0$. By Theorem 0.8.1, $p(q - r) = pq - pr = 0$. By part 1 and $p \neq 0$, we get $q - r = 0$, that is, $q = r$. This proves the corollary. ■

Quick check. Let $p, q \in \mathbb{R}[x]$ with $\deg p = 3$ and $\deg q = 2$. What are $\deg(pq)$, $\deg(p + q)$, and $\deg(p^2)$? Can you say what $\deg(p - x^3)$ is?

Solution. By Theorem 0.8.3, $\deg(pq) = 5$ and $\deg(p^2) = 6$. Since the degrees differ, Theorem 0.8.2 gives $\deg(p + q) = 3$. The degree of $p - x^3$ is not determined: if the leading coefficient of p is 1, the x^3 terms cancel and the degree is at most 2 (it could even be $-\infty$ if $p = x^3$); otherwise it is 3.

0.8.4 Polynomials of bounded degree

In linear algebra we constantly need “all polynomials up to a given size”. For instance, the quadratics $ax^2 + bx + c$ are described by three numbers, much like points of $\mathbb{R}^3$. So we give such collections names.

Definition 0.8.4. Polynomials of degree at most n

Let F be a field and $n \in \mathbb{N}$. The set of polynomials over F of degree **at most** n is

$$F[x]_{\leq n} = \{p \in F[x] : \deg p \leq n\} = \{a_0 + a_1x + \cdots + a_nx^n : a_0, \dots, a_n \in F\}.$$

The two descriptions agree: $\deg p \leq n$ says exactly that every coefficient beyond position n is zero, and the coefficients $a_0, \dots, a_n$ are then free, any of them allowed to be zero. In particular the zero polynomial lies in $F[x]_{\leq n}$, since $-\infty \leq n$.

Example. Inside $\mathbb{R}[x]_{\leq 2}$

Which of $3x^2 - 2x + 1$, $5x + 7$, -4 , 0 , and $x^3 - x^3 + x$ lie in $\mathbb{R}[x]_{\leq 2}$? Which lie in $\mathbb{R}[x]_{\leq 0}$?

Solution. All five lie in $\mathbb{R}[x]_{\leq 2}$. Their degrees are 2, 1, 0, $-\infty$, and 1 (the last is the polynomial x , since $x^3 - x^3 = 0$ as polynomials). Only -4 and 0 lie in $\mathbb{R}[x]_{\leq 0}$, which is the set of constant polynomials, 0 included.

Sometimes we need the degree to be exactly n , for instance when we speak of “a quadratic” and mean that the x^2 term is really there.

Definition 0.8.5. Polynomials of degree exactly n

Let F be a field and $n \in \mathbb{N}$. The set of polynomials over F of degree **exactly** n is

$$\begin{aligned} F[x]_{=n} &= \{p \in F[x] : \deg p = n\} \\ &= \{a_0 + a_1x + \cdots + a_nx^n : a_0, \dots, a_n \in F, a_n \neq 0\}. \end{aligned}$$

Example. Comparing the two notations

For each of $x^2 + 1$, $3x - 2$, and 0 , decide whether it lies in $\mathbb{R}[x]_{\leq 2}$ and whether it lies in $\mathbb{R}[x]_{=2}$.

Solution. The polynomial $x^2 + 1$ has degree 2, so it lies in both. The polynomial $3x - 2$ has degree $1 \leq 2$, so it lies in $\mathbb{R}[x]_{\leq 2}$ but **not** in $\mathbb{R}[x]_{=2}$. The zero polynomial has degree $-\infty \leq 2$, so it lies in $\mathbb{R}[x]_{\leq 2}$, but $-\infty \neq 2$, so it is **not** in $\mathbb{R}[x]_{=2}$. In general $F[x]_{\leq n} = F[x]_{=n} \cup F[x]_{\leq n-1}$ for $n \geq 1$, and the union is disjoint.

The two sets differ in one small clause, $a_n \neq 0$, and that clause changes their behavior completely.

Warning. $F[x]_{\leq n}$ is closed under addition, but $F[x]_{=n}$ is **not**. For example $x^2 + x$ and $-x^2 + 1$ both lie in $\mathbb{R}[x]_{=2}$, but their sum $x + 1$ has degree 1. The leading terms cancel. Also $F[x]_{=n}$ does not contain 0. In Chapter 1 this is why $F[x]_{\leq n}$ is a subspace and $F[x]_{=n}$ is not.

The positive half is [Theorem 0.8.2](#) at work: if $\deg p \leq n$ and $\deg q \leq n$, then $\deg(p + q) \leq \max(\deg p, \deg q) \leq n$. Multiplying by a constant $c \in F$ also cannot raise the degree, by [Theorem 0.8.3](#).

0.8.5 Evaluation and roots

A polynomial is not a function, but every polynomial *defines* a function: plug an element of the field in for x .

Definition 0.8.6. Evaluation and roots

Let F be a field, $p = \sum_{k=0}^N a_k x^k \in F[x]$, and $c \in F$. The **value** of p at c is the element

$$p(c) = \sum_{k=0}^N a_k c^k = a_0 + a_1 c + \cdots + a_N c^N \in F,$$

where $c^0 = 1$. An element $c \in F$ is a **root** of p if $p(c) = 0$. The function $F \rightarrow F$, $c \mapsto p(c)$, is the **polynomial function** of p .

The value does not depend on the choice of N : enlarging N adds terms $0 \cdot c^k = 0$ (by Theorem 0.7.1), which do not change the sum. So $p(c)$ is well defined.

For example, $p = x^2 - 3x + 2 \in \mathbb{R}[x]$ has $p(0) = 2$ and $p(1) = 1 - 3 + 2 = 0$, so 1 is a root. Over $\mathbb{F}_3 = \{0, 1, 2\}$, the polynomial $x^3 + 2$ has $1^3 + 2 = 3 = 0$, so 1 is a root; the other two values are $0 + 2 = 2$ and $8 + 2 = 10 = 1$, so 1 is its only root in $\mathbb{F}_3$.

Evaluation turns the operations of $F[x]$ into the operations of F :

Theorem 0.8.5. Evaluation respects sums and products

Let F be a field, $p, q \in F[x]$, and $c \in F$. Then

$$(p + q)(c) = p(c) + q(c), \quad (pq)(c) = p(c)q(c),$$

and the constant polynomial a has value a at c .

Proof. Let $p = \sum_{i=0}^m a_i x^i$ and $q = \sum_{j=0}^n b_j x^j$, where we choose m and n large enough that all nonzero coefficients are included. The statement about constants is immediate from [Definition 0.8.6](#). For sums, taking $N = \max(m, n)$ and padding with zero coefficients, $(p + q)(c) = \sum_{k=0}^N (a_k + b_k) c^k = \sum_{k=0}^N a_k c^k + \sum_{k=0}^N b_k c^k$ by distributivity in F .

For products, all nonzero coefficients of pq occur at positions $k \leq m + n$, so

$$\begin{aligned} (pq)(c) &= \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) c^k \\ &= \sum_{i=0}^m \sum_{j=0}^n a_i b_j c^i c^j = \sum_{i=0}^m \sum_{j=0}^n (a_i c^i) (b_j c^j) \\ &= \left(\sum_{i=0}^m a_i c^i \right) \left(\sum_{j=0}^n b_j c^j \right), \end{aligned}$$

where the first equality is [Definition 0.8.2](#), the second uses distributivity and $c^{i+j} = c^i c^j$ and regroups the pairs (i, j) , the third uses **commutativity** of multiplication in F to move c^i past b_j , and the last is distributivity again. This shows $(pq)(c) = p(c)q(c)$. ■

Note which step used commutativity. In the next section we will plug a square matrix $\mathbf{A}$ into a polynomial. Products of matrices do not commute in general, but the proof only moves **scalars** past powers of $\mathbf{A}$, and multiplies powers of the same $\mathbf{A}$; both are still allowed for matrices, so the same identity will hold there.

As a first use, a root of a factor is a root of the product: if $q(c) = 0$, then $(pq)(c) = p(c) \cdot 0 = 0$. Conversely, if $(pq)(c) = 0$ then $p(c)q(c) = 0$, so $p(c) = 0$ or $q(c) = 0$ by Theorem 0.7.1. This is how one solves $x^2 - 3x + 2 = (x - 1)(x - 2) = 0$ at school.

Now we can return to the question from the start of the section.

Example. Different polynomials, same function

Over $\mathbb{F}_2$, compare the polynomials $x^2 + x$ and 0, and the polynomials x^2 and x , both as polynomials and as functions $\mathbb{F}_2 \rightarrow \mathbb{F}_2$.

Solution. As polynomials, $x^2 + x$ has coefficient sequence $(0, 1, 1, 0, \dots)$ and 0 has $(0, 0, 0, \dots)$. They differ in position 1, so $x^2 + x \neq 0$ by [Definition 0.8.1](#). Its degree is 2.

As functions, $\mathbb{F}_2 = \{0, 1\}$ has two elements, and

$$0^2 + 0 = 0, \quad 1^2 + 1 = 1 + 1 = 0.$$

So the polynomial function of $x^2 + x$ is the zero function, the same as that of 0. Both elements of $\mathbb{F}_2$ are roots of a polynomial of degree 2 that is not the zero polynomial.

Similarly $x^2 \neq x$ as polynomials, but $0^2 = 0$ and $1^2 = 1$, so they define the same function. Indeed, by [Theorem 0.8.5](#), two polynomials define the same function exactly when their difference is a polynomial whose function is zero, and $x^2 - x = x^2 + x$ in $\mathbb{F}_2[x]$.

Warning. A polynomial is not a function. Two different polynomials can define the same polynomial function, as $x^2 + x$ and 0 do over $\mathbb{F}_2$. So “ $p(c) = 0$ for every $c \in F$ ” does **not** imply $p = 0$ in general, and we may never read off coefficients or a degree from the values alone. This happens over every finite field: if $F = \{c_1, \dots, c_q\}$, then $(x - c_1)(x - c_2) \cdots (x - c_q)$ has degree q by [Theorem 0.8.3](#), yet vanishes at every c_i by [Theorem 0.8.5](#). Over $\mathbb{F}_p$, [Exercise \(C2: A nonzero polynomial vanishing everywhere\)](#) below gives the shorter example $x^p - x$.

Over an infinite field such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, the problem disappears: a polynomial whose function is zero is the zero polynomial, so polynomials and polynomial functions can be identified. We prove this in Chapter 3 (in the section on applications of linear systems), once we can count roots. Until then, whenever we say two polynomials are equal we mean their coefficients agree.

0.8.6 Looking ahead

Two tools will be built on this section later.

Remark. Division with remainder. Over a field, if $f, g \in F[x]$ and $g \neq 0$, there are unique $q, r \in F[x]$ with $f = qg + r$ and $\deg r < \deg g$. This is long division of polynomials, and the convention $\deg 0 = -\infty$ makes “ $\deg r < \deg g$ ” cover the case $r = 0$. We state it here only for orientation; it is proved in Chapter 6 and is not used before then.

Remark. Polynomials in a matrix. In the next section, once matrices and their products are available, we substitute a square matrix $\mathbf{A}$ for x , replacing the constant term a_0 by $a_0\mathbf{I}$. This is how the characteristic and minimal polynomials of later chapters act on matrices.

0.8.7 Exercises

0.8.7.1 A. Check your understanding

Exercise. A1

- Define the degree of a polynomial over a field F , including the zero polynomial. State the formula for $\deg(pq)$.
- Is $1 + x + x^2 + x^3 + \cdots$, with every coefficient equal to 1, a polynomial over $\mathbb{R}$? Justify your answer.
- Determine whether the following statement is true: “for all $p, q \in F[x]$, $\deg(p + q) = \max(\deg p, \deg q)$.” Justify your answer.
- Determine whether the following statement is true: “if $p \in \mathbb{F}_2[x]$ and $p(c) = 0$ for every $c \in \mathbb{F}_2$, then $p = 0$.” Justify your answer.
- Explain why $F[x]_{=2}$ is **not** closed under addition, while $F[x]_{\leq 2}$ is.

Solution.

- For $p = \sum a_k x^k \neq 0$, $\deg p$ is the largest n with $a_n \neq 0$; and $\deg 0 = -\infty$. For all $p, q \in F[x]$, $\deg(pq) = \deg p + \deg q$ ([Theorem 0.8.3](#)).

- (b) No. Its coefficient sequence $(1, 1, 1, \dots)$ has infinitely many nonzero terms, so it fails the clause “only finitely many a_k are nonzero” of [Definition 0.8.1](#).
- (c) False. Take $p = x$ and $q = -x$. Then $p+q = 0$ has degree $-\infty$, while $\max(\deg p, \deg q) = 1$. Only the inequality $\leq$ holds in general ([Theorem 0.8.2](#)).
- (d) False. By [Example \(Different polynomials, same function\)](#), $p = x^2 + x$ satisfies $p(0) = p(1) = 0$, but $p \neq 0$.
- (e) The sum of x^2 and $-x^2 + 1$, both of degree exactly 2, is 1, of degree 0. For $F[x]_{\leq 2}$: if $\deg p \leq 2$ and $\deg q \leq 2$, then $\deg(p+q) \leq \max(\deg p, \deg q) \leq 2$ by [Theorem 0.8.2](#).

0.8.7.2 B. Practice

Exercise. B1: Sums, products, and degrees

- (a) In $\mathbb{R}[x]$, let $p = 2x^3 - x + 4$ and $q = -2x^3 + x^2 + 3$. Compute $p+q$ and pq , and give their degrees. Which inequality or formula from this section does each degree illustrate?
- (b) In $\mathbb{F}_3[x]$, compute $(x+2)(x^2+x+1)$. Hence find all roots in $\mathbb{F}_3$ of the product.

Solution.

- (a) Adding coefficients gives $p+q = x^2 - x + 7$, of degree 2. Here $\deg p = \deg q = 3$ and the x^3 terms cancel, so the inequality of [Theorem 0.8.2](#) is strict. Expanding,

$$pq = -4x^6 + 2x^5 + 2x^4 - 3x^3 + 4x^2 - 3x + 12,$$

of degree $6 = 3 + 3$, as [Theorem 0.8.3](#) predicts; its leading coefficient is $2 \cdot (-2) = -4$.

- (b) Expanding, $(x+2)(x^2+x+1) = x^3 + 3x^2 + 3x + 2$. In $\mathbb{F}_3$ we have $3 = 0$, so the product is $x^3 + 2$. By [Theorem 0.8.5](#) and [Theorem 0.7.1](#), c is a root of the product if and only if $c+2 = 0$ or $c^2 + c + 1 = 0$. The first gives $c = 1$. For the second, the values at 0, 1, 2 are 1, $3 = 0$, and $7 = 1$. Hence the only root in $\mathbb{F}_3$ is $c = 1$, which occurs in both factors.

Exercise. B2: Degree of a composition

For $p = \sum_{k=0}^m a_k x^k$ and q in $F[x]$, define the **composition** $p \circ q = \sum_{k=0}^m a_k q^k \in F[x]$, where $q^0 = 1$.

- (a) Prove that if p and q are nonconstant, then $\deg(p \circ q) = \deg p \cdot \deg q$.
- (b) Give an example showing the formula fails when q is constant.

Hint: first find $\deg(q^k)$.

Solution.

- (a) Let $m = \deg p \geq 1$ and $d = \deg q \geq 1$, so $a_m \neq 0$. By [Theorem 0.8.3](#) and induction on k ([Theorem 0.2.7](#)), $\deg(q^k) = kd$ for every $k \in \mathbb{N}$: the case $k = 0$ is $\deg 1 = 0$, and $\deg(q^{k+1}) = \deg(q^k) + \deg q = kd + d$. Hence, again by [Theorem 0.8.3](#), $\deg(a_m q^m) = 0 + md = md$, and for $k < m$, $\deg(a_k q^k) \leq kd < md$ (it is kd or $-\infty$). Let $s = \sum_{k=0}^{m-1} a_k q^k$. Applying [Theorem 0.8.2](#) $m-1$ times gives $\deg s \leq \max_{k < m} \deg(a_k q^k) < md$. Since

$\deg s \neq \deg(a_m q^m)$, the equality case of [Theorem 0.8.2](#) gives $\deg(p \circ q) = \deg(s + a_m q^m) = md$. This proves $\deg(p \circ q) = \deg p \cdot \deg q$.

- (b) Take $p = x - 1$ and $q = 1$. Then $p \circ q = 1 - 1 = 0$ has degree $-\infty$, while $\deg p \cdot \deg q = 1 \cdot 0 = 0$.

Exercise. B3: All small polynomials over $\mathbb{F}_2$

List all polynomials in $\mathbb{F}_2[x]_{\leq 2}$. For each, give its degree and its polynomial function (the values at 0 and 1). Hence determine which of them define the zero function, and explain why every function $\mathbb{F}_2 \rightarrow \mathbb{F}_2$ is the polynomial function of exactly two of them.

Solution. A polynomial $a_0 + a_1x + a_2x^2$ with $a_i \in \mathbb{F}_2$ has value a_0 at 0 and $a_0 + a_1 + a_2$ at 1. With $2^3 = 8$ choices of coefficients:

polynomial	degree	value at 0	value at 1
0	$-\infty$	0	0
1	0	1	1
x	1	0	1
$x + 1$	1	1	0
x^2	2	0	1
$x^2 + 1$	2	1	0
$x^2 + x$	2	0	0
$x^2 + x + 1$	2	1	1

The zero function requires $a_0 = 0$ and $a_0 + a_1 + a_2 = 0$, that is, $a_0 = 0$ and $a_1 = a_2$. Hence exactly 0 and $x^2 + x$ define the zero function.

A function $f: \mathbb{F}_2 \rightarrow \mathbb{F}_2$ is determined by the pair $(f(0), f(1))$. Given such a pair (u, v) , the polynomial $a_0 + a_1x + a_2x^2$ defines f exactly when $a_0 = u$ and $a_1 + a_2 = v - u$. The first fixes a_0 , and for each of the two choices of a_2 the second fixes $a_1 = v - u - a_2$. Therefore exactly two of the eight polynomials define f , and the table confirms this.

0.8.7.3 C. Going deeper

Exercise. C1: Roots of a quadratic

Let F be a field.

- Let $p = ax^2 + bx + c \in F[x]$ and $r \in F$ with $p(r) = 0$. Prove that $p = (x - r)(ax + (b + ar))$.
- Deduce that a nonzero polynomial in $F[x]_{\leq 2}$ has at most 2 roots in F .
- The same definitions make sense with coefficients in $\mathbb{Z}/8\mathbb{Z}$. Show that $x^2 - 1$ has four roots there, and name the step of (b) that breaks.

Hint for (b): use (a) together with [Theorem 0.8.5](#).

Solution.

- (a) Since $p(r) = 0$, we have $ar^2 + br + c = 0$, so $c = -ar^2 - br$. Expanding with [Theorem 0.8.1](#),

$$\begin{aligned}(x - r)(ax + (b + ar)) &= ax^2 + (b + ar)x - arx - r(b + ar) \\ &= ax^2 + bx - (br + ar^2) = ax^2 + bx + c = p.\end{aligned}$$

- (b) Let $p \neq 0$ with $\deg p \leq 2$. *Case 1.* $\deg p = 0$. Then $p = c \neq 0$ is constant and $p(r) = c \neq 0$ for every r , so p has no roots. *Case 2.* $\deg p = 1$, say $p = bx + c$ with $b \neq 0$. Then $p(r) = 0$ if and only if $r = -b^{-1}c$, so p has exactly one root. *Case 3.* $\deg p = 2$, say $p = ax^2 + bx + c$ with $a \neq 0$. If p has no root we are done. Otherwise let r be a root. By (a), $p = (x - r)q$ with $q = ax + (b + ar)$, of degree 1 since $a \neq 0$. Let s be any root of p . By [Theorem 0.8.5](#), $0 = p(s) = (s - r)q(s)$, so $s = r$ or $q(s) = 0$ by Theorem 0.7.1. By Case 2, q has exactly one root. Hence every root of p is r or the root of q , and p has at most 2 roots. This proves the claim.
- (c) In $\mathbb{Z}/8\mathbb{Z}$, $1^2 = 1$, $3^2 = 9 = 1$, $5^2 = 25 = 1$, and $7^2 = 49 = 1$, so 1, 3, 5, 7 are four roots of $x^2 - 1$. The argument in (b) breaks at “ $(s - r)q(s) = 0$ implies $s - r = 0$ or $q(s) = 0$ ”: for $r = 1$, $s = 3$ we get $(3 - 1)(3 + 1) = 2 \cdot 4 = 0$ with both factors nonzero. That step needs the field property that a product of nonzero elements is nonzero.

Exercise. C2: A nonzero polynomial vanishing everywhere

Let p be a prime and $F = \mathbb{F}_p$.

- (a) Fix $a \in F \setminus \{0\}$. Prove that the map $F \setminus \{0\} \rightarrow F \setminus \{0\}$, $b \mapsto ab$, is a bijection.
- (b) Deduce that $a^{p-1} = 1$ for every $a \in F \setminus \{0\}$.
- (c) Hence show that the polynomial $x^p - x \in \mathbb{F}_p[x]$ is not the zero polynomial but that its polynomial function is the zero function.

Hint for (b): multiply together all the elements of $F \setminus \{0\}$ in two ways.

Solution.

- (a) The map lands in $F \setminus \{0\}$, since a product of nonzero elements of a field is nonzero (Theorem 0.7.1). It is injective: if $ab = ab'$, multiplying by a^{-1} gives $b = b'$. The set $F \setminus \{0\}$ is finite with $p - 1$ elements, so an injective map from it to itself is surjective by Theorem 0.4.9, hence bijective.
- (b) Let P be the product of all $p - 1$ elements of $F \setminus \{0\}$; it is nonzero by Theorem 0.7.1. Since $b \mapsto ab$ is a bijection by (a), the elements ab , as b runs over $F \setminus \{0\}$, are the same elements in a different order. Multiplication in F is commutative and associative, so the product does not depend on the order, and

$$P = \prod_{b \neq 0} (ab) = a^{p-1} \prod_{b \neq 0} b = a^{p-1} P.$$

Multiplying by P^{-1} gives $a^{p-1} = 1$.

- (c) The coefficient of x^p in $x^p - x$ is $1 \neq 0$, so the polynomial is nonzero, of degree p . For its function: $0^p - 0 = 0$, and for $a \neq 0$, (b) gives $a^p - a = a \cdot a^{p-1} - a = a - a = 0$.

Hence every element of $\mathbb{F}_p$ is a root, and the polynomial function of $x^p - x$ is the zero function. For $p = 2$ this is $x^2 - x = x^2 + x$, the polynomial of [Example \(Different polynomials, same function\)](#).

Exercise. C3: Which polynomials have inverses?

- (a) Let F be a field and $p, q \in F[x]$ with $pq = 1$. Prove that p and q are nonzero constants.
- (b) Show that (a) fails with coefficients in $\mathbb{Z}/4\mathbb{Z}$ by computing $(2x + 1)^2$ there.

Solution.

- (a) Since $pq = 1 \neq 0$, neither p nor q is the zero polynomial, so $\deg p, \deg q \in \mathbb{N}$. By [Theorem 0.8.3](#), $\deg p + \deg q = \deg 1 = 0$. Two natural numbers with sum 0 are both 0, so $\deg p = \deg q = 0$. Therefore p and q are nonzero constants.
- (b) In $\mathbb{Z}/4\mathbb{Z}$, $(2x + 1)^2 = 4x^2 + 4x + 1 = 1$, because $4 = 0$. So $2x + 1$ has degree 1 and is its own inverse. The proof of (a) breaks at [Theorem 0.8.3](#), which fails here because the leading coefficient $2 \cdot 2 = 4 = 0$.