

Formal Polynomials

At school a polynomial is “an expression in x ”, and x is a number not yet chosen. Over the field $\mathbb{F}_2$ of Chapter 2 this picture breaks at once: $x^2 + x$ takes the value 0 at both elements, so as a function it is the zero function, yet we want it to have degree 2. This chapter therefore decides that a polynomial **is** its list of coefficients, a sequence with only finitely many non-zero entries, and that x is the name of a position, never a number. From that one decision it builds the polynomial ring $R[x]$ over any commutative ring R of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 2, and proves its laws with one device, **check on monomials, extend by additivity**, so that no double sum is ever reordered. It then attaches the degree and the leading coefficient, recovers “plugging in” as a ring homomorphism, and defines the derivative by its coefficients, with no limit in sight.

Which school rules survive depends on R , and the chapter keeps count. Over $\mathbb{Z}/6\mathbb{Z}$ the degree of a product can drop, because $[2][3] = [0]$. Over $\mathbb{Z}/4\mathbb{Z}$ the polynomial $1 + [2]x$ is its own inverse. Over every finite ring with $1 \neq 0$ some non-zero polynomial vanishes at every element, so a polynomial is not its function. Over $\mathbb{F}_p$ the derivative of x^p is 0. Each result says what it needs from R : nothing at all, no zero divisors, a unit leading coefficient, finiteness with $1 \neq 0$, or, for the derivative, the characteristic of a field. The chapter ends where Chapter 5 begins, with $R = F$ a field and division with remainder still to come.

One construction, many rings. The linear-algebra companion defines polynomials over a field F , and its later chapters cite this chapter’s results with F a field. Every such statement is the case $R = F$ of the statement proved here for a commutative ring, since a field is a commutative ring. Where a result really needs more than a commutative ring, the hypothesis is named at the point of use: no zero divisors (Theorem 4.3.2 (b), Corollary 4.3.3, Proposition 4.3.4), a unit leading coefficient (Theorem 4.3.2 (b)), R finite with $1 \neq 0$ (Proposition 4.4.4 (d)), or the characteristic of a field (Proposition 4.5.2).

What you need. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapters 2 and 3 above all, with index arithmetic in $\mathbb{N}$ from its Chapter 1; Chapter 2 of this volume; *Sets, Relations, and Cardinality*, Chapters 1 and 3 and Section 2.3 (and Section 2.5 for R3); and induction from *Logic and Proof*, Chapter 4.

- From *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 2: commutative rings, with $1 = 0$ allowed, and their algebra (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2); the multiples $n \cdot a$ of the “Multiples” paragraph of its Section 2.3; $\mathbb{Z}$ as an ordered commutative ring with a greatest element in every non-empty set bounded above (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.3.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.3.4, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.6); the field $\mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.4.3); and the copies $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.2.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.4.4). From its Chapter 1, the laws and the order of $\mathbb{N} = \omega$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 1.7.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 1.5.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 1.6.1).
- From *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3: division with remainder and the rules for divisibility (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.1.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1); ideals and quotient rings (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.4.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1); the rings $\mathbb{Z}/n\mathbb{Z}$ and the example $\mathbb{Z}/6\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$).

to $\mathbb{N}$, Definition 3.4.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (Multiplication modulo six and modulo five); units, the field $\mathbb{Z}/p\mathbb{Z}$ and the Chinese remainder map (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.5.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.3). Section 4.3 also pays a debt to its Chapter 4: the polynomial algebra that the field $\mathbb{Q}(t)$ of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (A Non-Archimedean Ordered Field) took on school credit.

- From Chapter 2: fields and the rule that a product of non-zero elements is non-zero (Definition 2.1.1, Theorem 2.1.1); $\mathbb{F}_p$ and the tables of $\mathbb{F}_2$ (Definition 2.2.1, Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$)); finite sums and integer multiples in a commutative ring (Lemma 2.6.1, Lemma 2.5.1); the characteristic, 0 or a prime (Definition 2.5.1, Theorem 2.5.3); and, for Section 4.4's Exercise C4, Fermat's little theorem (Theorem 2.6.6).
- From *Sets, Relations, and Cardinality*: functions and their equality, products and bijections (Sets, Relations, and Cardinality, Definition 1.4.1, Sets, Relations, and Cardinality, Proposition 1.4.1, Sets, Relations, and Cardinality, Definition 1.3.2, Sets, Relations, and Cardinality, Definition 1.4.5), from Chapter 1; the recursion theorem, with its sums, products and powers used as patterns (Sets, Relations, and Cardinality, Theorem 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.2), from Section 2.3; finite sets (Sets, Relations, and Cardinality, Definition 3.1.2, Sets, Relations, and Cardinality, Proposition 3.1.6), from Chapter 3.
- From *Logic and Proof*: induction (Logic and Proof, Axiom 4.2.1), from Section 4.2, and, for the two find-the-error exercises, the catalogue of moves that are not allowed (Logic and Proof, Example (What is not allowed)), from Section 8.6.

Chapters 1 and 3 enter only through the review exercises of Section 4.5: the complex numbers and their conjugate in R2, groups and their homomorphisms in R1. The countability results of *Sets, Relations, and Cardinality*, Chapter 3, and its quotient sets (Sets, Relations, and Cardinality, Definition 2.5.4, Section 2.5) enter only through R3. Sections 4.1 and 4.4 also compare two results with Chapter 1 (Proposition 1.1.3, Lemma 1.1.4) without using them. Outside R2, no proof in the chapter uses $\mathbb{R}$ or $\mathbb{C}$.

Time. About 25 hours on the core track (all of A, one B and one C per section, the exit checks); about 35 hours for everything.

4.-1.1 Roadmap

- **Polynomials as Coefficient Sequences.** Why “an expression in x ” fails over $\mathbb{F}_2$; a polynomial over a commutative ring as a sequence $\mathbb{N} \rightarrow R$ with only finitely many non-zero entries, with monomials, $x = (0, 1, 0, \dots)$, equality by comparing coefficients, the display $\sum_k p_k x^k$ as notation only, the zero ring, and the non-example $(1, 1, 1, \dots)$; and a lemma collecting finite sums (which need only an addition), products of lists, powers and multiples, with the proofs of its new parts in a second-reading fold.
- **The Polynomial Ring.** The sum taken position by position and the product as a convolution, closed in $R[x]$ and computed over $\mathbb{Q}$, $\mathbb{F}_3$ and $\mathbb{Z}/6\mathbb{Z}$; every polynomial an honest sum of its monomials; multiplication by a monomial as a shift and a scaling; the lemma that two maps additive in each argument and equal on monomials are equal; and the theorem that $R[x]$ is a commutative ring containing R as its constants, with associativity proved on monomials instead of by reordering double sums.
- **Degree, Leading Coefficients, and Integral Domains.** Degree with $\deg 0 = -\infty$, the leading coefficient and monic polynomials; the degree of a sum; the degree of a product, whose top coefficient is $\text{lc}(p)\text{lc}(q)$ in every commutative ring, so that degrees add exactly

when that product is non-zero, as over a ring with no zero divisors or for a unit leading coefficient; integral domains, with $R[x]$ an integral domain exactly when R is; the units of $R[x]$ over an integral domain, and the non-constant unit $1 + [2]x$ over $\mathbb{Z}/4\mathbb{Z}$; and the sets $R[x]_{\leq n}$ and $R[x]_{=n}$.

- **Evaluation, Substitution, and Polynomial Functions.** The value $p(c)$, roots, and evaluation respecting sums and products; ring homomorphisms and two impostors; the substitution principle, that one ring homomorphism $R[x] \rightarrow S$ extends a given $\varphi: R \rightarrow S$ and sends x to a given s , and only one; changing coefficients along φ , with reduction modulo n and the exact condition for the degree to drop, and the composition $p \circ q$; and the ring R^R of functions, with polynomial composition matching composition of functions and, over every finite ring with $1 \neq 0$, a non-zero polynomial whose function is 0.
- **The Formal Derivative.** The derivative defined by $(f')_k = (k+1) \cdot f_{k+1}$, the role of the element $n \cdot 1$, and examples in five rings; the sum, product and power rules in every commutative ring, the product rule by checking on monomials; over a field, $f' = 0$ exactly for the constants in characteristic 0 and exactly for the polynomials in x^p in characteristic p ; and review exercises that return to groups (Chapter 3), complex conjugation (Chapter 1) and countability (*Sets, Relations, and Cardinality*, Chapter 3).

4.-1.2 Named moves

- **Compare coefficients.** Two polynomials are equal if and only if their coefficients agree in every position, so an identity in $R[x]$ is proved by computing the k -th coefficient of both sides for an arbitrary k . It is *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 2's "reduce to the level below", now with sequences. Named in Section 4.1, it proves the additive laws and both distributive laws of $R[x]$ in Section 4.2 and the linearity of the derivative in Section 4.5.
- **Check on monomials, extend by additivity.** Two maps of up to three polynomial arguments that are additive in each argument, and agree when every argument is a monomial, agree everywhere (Lemma 4.2.3). It proves commutativity and associativity of the product in Section 4.2, evaluation and substitution respecting products in Section 4.4, and the product rule in Section 4.5. Exercise B2 of Section 4.2 leaves its last step to you, and Exercise C2 of Section 4.4 its second half.
- **Look at the top coefficient.** The coefficient of $x^{\deg p + \deg q}$ in pq is $\text{lc}(p)\text{lc}(q)$, and nothing sits above it; every question about the degree of a product becomes the question whether that one element of R is 0. It proves the degree formula in Section 4.3 and, through it, the absence of zero divisors and the units of $R[x]$; in Section 4.4 it shows that the product of the factors $x - c$ over a finite ring is monic, and Exercise B1 there uses it for the degree of a composition.
- **A homomorphism out of $R[x]$ is fixed by the constants and x .** To show that two ring homomorphisms out of $R[x]$ agree, check that they agree on the constants and on x (Theorem 4.4.2 (b)). Named in Section 4.4, it proves there that composing polynomials matches composing their functions, and Exercise B3 of Section 4.4 uses it to invert the shift $p \mapsto p \circ (x + c)$.