

Polynomials over a Field

Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Chapter 3 did arithmetic in $\mathbb{Z}$: divide with a remainder, take the least positive element of a set closed under combinations, and the greatest common divisor, Bézout's identity, Euclid's lemma and unique factorization follow. Chapter 4 built the ring $F[x]$ and its degree, but it did not divide one polynomial by another with a remainder. This chapter shows that over a field F the polynomials have the same arithmetic, with the degree in the part of the size and “monic” in the part of “positive”. It also proves what $\mathbb{Z}$ has no analogue for. A polynomial can be **evaluated**, so it has roots, and roots occupy the second half of the chapter. A root c is a factor $x - c$; a non-zero polynomial has no more distinct roots than its degree; a repeated root shows up in the formal derivative of Section 4.5; and values at enough points determine a polynomial, which is interpolation. Interpolation turns out to be the Chinese remainder theorem for the moduli $x - c$, and the ring $F[x]/\langle m \rangle$, built by *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3's quotient construction, is a field exactly when m is irreducible.

The chapter ends with the question that algebra courses usually leave to analysis: does every non-constant complex polynomial have a root? It does, and Section 5.6 proves it with no convergent sequences, no compactness, no continuity theorem and no polar form. The one analytic input is the supremum property of $\mathbb{R}$. It is used directly twice, to find a point where $|p|$ is smallest, and indirectly through the real square roots behind the modulus and behind the complex square roots. The factorization of real polynomials into linear factors and quadratics without real roots follows.

Two rings, one arithmetic. The first half of the chapter runs *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3 again, with these substitutions.

In $\mathbb{Z}$	In $F[x]$
the size of an integer	the degree
the units ± 1	the units, the non-zero constants
positive	monic
division with remainder	Theorem 5.1.2
Bézout's theorem, <i>Number Systems: From $\mathbb{N}$ to $\mathbb{R}$</i> , Theorem 3.2.1	Theorem 5.2.2
primes	monic irreducible polynomials
unique factorization, <i>Number Systems: From $\mathbb{N}$ to $\mathbb{R}$</i> , Theorem 3.3.5	Theorem 5.3.6
the ring $\mathbb{Z}/n\mathbb{Z}$	the ring $F[x]/\langle m \rangle$, Theorem 5.5.2
$\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime, <i>Number Systems: From $\mathbb{N}$ to $\mathbb{R}$</i> , Theorem 3.5.2	$F[x]/\langle m \rangle$ is a field iff m is irreducible, Theorem 5.5.3
the Chinese remainder theorem, <i>Number Systems: From $\mathbb{N}$ to $\mathbb{R}$</i> , Theorem 3.5.3	Theorem 5.5.5, for any number of moduli

Each polynomial proof is written out in full. The integer twins are compared with, never cited as a reason for a polynomial statement. The general facts about ideals, quotient rings and units are cited, not proved again. Integers enter only as integers: as coefficients, in the rational root test of Section 5.3 and the integer polynomials of Section 5.1, and as degrees and exponents.

What you need. Chapter 4 above all, and Chapter 2; Chapter 1 for Section 5.6 and a few

examples; *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3 for comparison and for the general theorems it proved once, and its $\mathbb{R}$ for Section 5.6; *Sets, Relations, and Cardinality*, Chapters 1–3; and induction from *Logic and Proof*, Chapter 4.

- From Chapter 4: the ring $F[x]$ and its laws (Definition 4.1.1, Definition 4.2.1, Theorem 4.2.4, Lemma 4.1.1, Lemma 4.2.2); the degree and the leading coefficient, with the degree of a sum and of a product, the absence of zero divisors and the units (Definition 4.3.1, Theorem 4.3.1, Theorem 4.3.2, Example (Which Rings Are Integral Domains), Corollary 4.3.3, Proposition 4.3.4); evaluation, substitution and ring homomorphisms (Definition 4.4.1, Theorem 4.4.1, Theorem 4.4.2, Definition 4.4.2), with the polynomial over $\mathbb{F}_2$ that vanishes everywhere (Example (Different Polynomials, Equal Functions)); and, for Sections 5.4 and 5.5, the formal derivative and its rules (Definition 4.5.1, Theorem 4.5.1, Proposition 4.5.2).
- 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); the fields $\mathbb{F}_p$ (Definition 2.2.1); subfields (Definition 2.3.1, Proposition 2.3.1), for Section 5.2; the characteristic, integer multiples and Fermat's little theorem (Definition 2.5.1, Example (The characteristics of the standard fields), Lemma 2.5.1, Theorem 2.6.6), for Sections 5.4 and 5.5; and, in Section 5.6, the field $\mathbb{Q}(i)$ and complex conjugation (Example (Rational and Integer Complex Numbers), Example (Conjugation and Other Automorphisms)). Section 5.5 meets the four-element field of Exercise (C1: A Field with Four Elements) again, and Exercise R2 of Section 5.6 returns to Example (The Field Generated by the Square Root of Two).
- From Chapter 1, for Section 5.6 (and the difference of powers also for Exercises B2 and B3 of Section 5.1): the complex numbers as a field containing $\mathbb{R}$ (Definition 1.1.1, Theorem 1.2.4, Proposition 1.1.1); the conjugate and the modulus and their rules (Definition 1.2.1, Theorem 1.2.2, Proposition 1.2.1, Lemma 1.3.1); the triangle inequality and its variants (Theorem 1.3.2, Corollary 1.3.3); powers (Proposition 1.1.3, Lemma 1.1.4); complex square roots (Proposition 1.4.1); and conjugate roots (Proposition 1.6.4). Sections 5.2 and 5.5 use $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ in examples, and Exercise B3 of Section 5.5 compares $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ with $\mathbb{C}$. Chapter 1's polar form and k -th roots are not used, and Chapter 3 is not used.
- From *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3: ideals, quotient rings and units (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.4.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.5.1), cited for $F[x]$; the rules for divisibility, Euclid's lemma and fractions in lowest terms (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.3.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.3.6), for the rational root test; even and odd integers (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 3.1.3); the integer gcd and its Euclidean step (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.2.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 3.2.3), in two exercises; and the integer twins compared with in Sections 5.1–5.5: those in the table above and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.1.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.2.4, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Exercise (C2: Scaling the gcd), Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 3.3.4, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.1.
- From *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapters 1 and 2: $\mathbb{N} = \omega$, its order and well-ordering, and even and odd exponents (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 1.7.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 1.6.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 1.6.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 1.6.4); commutative rings and the rules of an ordered ring (Number

Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5); greatest elements of bounded sets of integers (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.6), for multiplicities; the irrationality of $\sqrt{2}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1), and the gap at $\sqrt{2}$ in $\mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.2), in Exercise C1 of Section 5.6; and maps on classes (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.2.1), for the Chinese remainder theorem.

- From *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapters 4–6, for Section 5.6: absolute values and powers in an ordered field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 4.1.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 4.2.1), from Chapter 4; $\mathbb{R}$ as a complete ordered field, its Archimedean property and the bound on powers of 2 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 5.6.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.6.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.4.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 5.6.1), with Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (Picking Representatives Is a Use of Choice) compared with, from Chapter 5; and non-negative square roots in $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4), from Chapter 6, which also supply $\sqrt{2}$ for examples in Sections 5.2–5.5.
- From *Sets, Relations, and Cardinality*: bijections (Sets, Relations, and Cardinality, Definition 1.4.5), from Chapter 1; the well-ordering of $\mathbb{N}$, the recursion theorem with its finite sums and products, equivalence classes and quotient sets, and suprema and infima (Sets, Relations, and Cardinality, Theorem 2.1.3, Sets, Relations, and Cardinality, Theorem 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.1, Sets, Relations, and Cardinality, Theorem 2.5.1, Sets, Relations, and Cardinality, Definition 2.5.4, Sets, Relations, and Cardinality, Definition 2.6.5), from Chapter 2; and finite and infinite sets (Sets, Relations, and Cardinality, Definition 3.1.2, Sets, Relations, and Cardinality, Definition 3.1.3, Sets, Relations, and Cardinality, Proposition 3.1.6, Sets, Relations, and Cardinality, Proposition 3.1.5), from Chapter 3, for Section 5.4 and Exercise C3 of Section 5.3.
- From *Logic and Proof*: induction and strong induction (Logic and Proof, Axiom 4.2.1, Logic and Proof, Theorem 4.2.2), 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.

Time. About 30 hours on the core track (all of A, one B and one C per section, the exit checks); about 45 hours for everything.

5.-1.1 Roadmap

- **Division with Remainder.** Divisibility over a field, associates and the one monic associate of a non-zero polynomial; division with remainder, with existence by an element of least degree and uniqueness by comparing degrees, and long division over $\mathbb{Q}$ and $\mathbb{F}_3$; and the remainder and factor theorems, which make a root c the same thing as a factor $x - c$.
- **Ideals, the Greatest Common Divisor, and the Euclidean Algorithm.** The ideal generated by finitely many polynomials; every ideal of $F[x]$ generated by exactly one monic polynomial; the gcd defined as the monic common divisor that every common divisor divides, with Bézout's theorem and coprimality; the Euclidean algorithm as a recursively defined sequence, with back-substitution; and division and the gcd unchanged when the field is enlarged.
- **Irreducible Polynomials and Unique Factorization.** Irreducibility over a field, decided by roots in degrees 2 and 3 and not beyond, as $x^4 + 4$ shows; Euclid's lemma and its consequences for irreducibles; an irreducible factor of least degree; unique factorization

into monic irreducibles, with uniqueness stated by a bijection of indices; the factorizations of $x^4 - 1$ over five fields; and the rational root test.

- **Roots, Multiplicity, and the Formal Derivative.** At most n roots for a non-zero polynomial of degree n ; a polynomial fixed by its values at $n + 1$ points, and over an infinite field by its function, but not over $\mathbb{F}_p$; the expansion in powers of $x - c$; multiplicity, splitting off all roots, and splitting over a field; and repeated roots and repeated factors detected by the formal derivative and by $\gcd(f, f')$.
- **Interpolation, Quotient Rings, and the Chinese Remainder Theorem.** Lagrange polynomials and the unique interpolating polynomial of degree at most n ; congruence modulo a polynomial and the ring $F[x]/\langle m \rangle$, named by the remainders and a field exactly when m is irreducible, with a field of four elements and a copy of $\mathbb{C}$; the Chinese remainder theorem for any number of pairwise coprime moduli; interpolation as its case of linear moduli; and values and derivatives prescribed at once.
- **The Fundamental Theorem of Algebra.** Why the field axioms cannot suffice; a growth bound and a Lipschitz bound in place of continuity; the minimum of $|p|$, found by nested squares and two uses of the supremum property; d'Alembert's lemma, with its direction found by square roots instead of polar form; the theorem and the splitting of complex polynomials; and real polynomials, whose irreducible factors are linear or quadratic without real root, so that one of odd degree has a real root. Review exercises return to Chapters 2 and 4 and to *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3.

5.-1.2 Named moves

- **Least degree, then divide.** In a set of polynomials closed under the right operations, take a non-zero element d of least degree and divide any element of the set by d ; the remainder lies in the set and has smaller degree, so it is 0. It is *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3's "least positive element, then divide", with degree in place of size. Named in Section 5.2, it proves there that every ideal of $F[x]$ has one monic generator (Theorem 5.2.1), and Bézout's theorem with it; its first, unnamed use is the existence half of division with remainder in Section 5.1. Exercise C1 of Section 5.2 asks for the whole proof, Exercise B2 of Section 5.3 leaves its last step to you, and Exercise C2 of Section 5.6 asks you to name it and carry it out.
- **Evaluate at a root.** In $f = qg + r$, evaluate at a root of g : the term qg vanishes, and the value of r is read off. Named in Section 5.1, it proves the remainder theorem and finds remainders without dividing (Example (Remainders without dividing), Exercise C2). In Section 5.5 it makes each Lagrange polynomial vanish at the other nodes, turns a congruence modulo $x - c$ into a value at c (Proposition 5.5.6), and reads a value and a derivative off a congruence modulo $(x - c)^2$ (Example (Values and derivatives at once)).
- **Compare degrees.** To show that two polynomials are equal, show that their difference has smaller degree than any non-zero polynomial of its kind can have: a non-zero multiple of g has degree at least $\deg g$, and a non-zero polynomial with $n + 1$ distinct roots has degree at least $n + 1$. Named in Section 5.1, it gives the uniqueness of the quotient and the remainder in Section 5.1, of the expansion in powers of $x - c$ in Section 5.4, of the representative of degree less than $\deg m$ in each class and of the solution of the Chinese remainder theorem in Section 5.5, and, with the root count, of the polynomial through given points in Sections 5.4 and 5.5.
- **Keep the quarter that keeps the infimum.** To find a point where a quantity bounded below attains its infimum, halve a square, keep the first quarter in a fixed order whose infimum is the same, and take the point common to all the squares, which completeness supplies. It is *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 5's bisection, now in the plane, and the fixed order makes each step a rule, so no choice is made. Named in Section 5.6, it

proves there that $|p|$ attains its minimum (Theorem 5.6.3); Exercise A1 there runs it for $x^2 + 1$, and Exercise C3 uses it to repair a flawed proof.

- **Multiply the Bézout identity**, reused from *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3. From $af + bg = 1$, multiply by h and read off what divides h . It proves Euclid's lemma for polynomials (Theorem 5.3.2) and the rule for coprime divisors (Proposition 5.3.4) in Section 5.3. In Section 5.5 two such identities multiplied together show that coprimality survives products (Lemma 5.5.4), the identity read modulo m gives inverses in $F[x]/\langle m \rangle$, and one identity per modulus builds the solution of the Chinese remainder theorem. That chapter's third move, computing on representatives, is not repeated: Section 5.5 cites its quotient-ring theorem.