

Fields

Linear algebra solves equations by adding, subtracting, multiplying, and dividing by numbers that are not zero, and by nothing else. A field is a number system in which exactly these moves work, under the usual rules. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* already defined fields and built three kinds of them: $\mathbb{Q}$, $\mathbb{R}$, and the integers modulo a prime p . Chapter 1 added $\mathbb{C}$. This chapter studies fields as a kind of object in their own right. It covers the rules every field obeys, the finite fields $\mathbb{F}_p$ and how to compute in them, fields inside fields, maps between fields that respect both operations, and one number, the **characteristic**, that says whether $1 + 1 + \cdots + 1$ can ever be 0. That number decides whether “ $2x = 0$, so $x = 0$ ” is a valid step, and the linear-algebra volumes ask about it again and again.

Two facts organize the chapter. A homomorphism of fields is forced to be injective, because a non-zero element has an inverse and its image must have one too. And every field contains exactly one smallest subfield, a copy of $\mathbb{Q}$ or of exactly one $\mathbb{F}_p$, onto which there is exactly one homomorphism. The chapter ends with the identity $(x + y)^p = x^p + y^p$, which holds in every field of characteristic p and fails for other exponents and in rings of composite characteristic. Fermat’s little theorem then takes a few lines: on $\mathbb{F}_p$ the map $x \mapsto x^p$ is a homomorphism of $\mathbb{F}_p$ to itself, and the only such map is the identity.

One definition, two books. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 2 defined “field” (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1), and the linear-algebra volumes cite the definition as Definition 2.1.1. Section 2.1 restates it under that name with the clauses (F1)–(F9) numbered as both books number them. A remark there proves that the two definitions describe the same objects; they differ only in where the condition $1 \neq 0$ is filed, inside (F7) here and as a clause of its own in *Number Systems*. Where *Number Systems* already proved a result, this chapter cites it. So Theorem 2.1.1 takes parts (a), (d) and (e) and the uniqueness of negatives from Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2, and the uniqueness of inverses, the absence of zero divisors and the inverse identities of part (g) from the paragraphs on units after Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.5.1, and proves cancellation and the fraction rules itself, and the proof of Theorem 2.2.2 is a citation of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.2.

What you need. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapters 2 and 3 above all; Chapter 1 of this volume, for examples; and smaller pieces of *Sets, Relations, and Cardinality* and *Logic and Proof*.

- From *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 2: commutative rings and fields 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), on nearly every page; the integers as a commutative ring (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.3.1), for the non-examples of Section 2.1; the copy of $\mathbb{N}$ in $\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.2.3), in Sections 2.1, 2.3 and 2.4 and for integer multiples in Section 2.5; the integers as an ordered ring (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.3.4), for negative multiples in Section 2.5; and the least element of a set of integers bounded below (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.6), which makes the characteristic well defined in Section 2.5; the multiples $n \cdot a$ of the “Multiples” paragraph of its Section 2.3, which Section 2.5 extends to negative n ; ordered fields and their rules (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5), and the order on $\mathbb{Q}$ from its positive elements (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.3), in a quick check of Section 2.1; the field $\mathbb{Q}$, built as classes of pairs (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$,

Definition 2.4.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.4.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.2.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.4.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.5.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.4.4), which Section 2.5 maps into every field of characteristic 0; the irrationality of $\sqrt{2}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1), used in Section 2.3; and the two-element ring that cannot be ordered (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (A field with two elements that cannot be ordered)), compared with in Section 2.2.

- From *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3: division with remainder, parity and the rules for divisibility (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.1.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 3.1.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1); the gcd, Bézout's theorem, Euclid's lemma and the test for primes (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.2.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.2.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 3.2.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.3.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 3.3.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 3.3.4); quotient rings and the rings $\mathbb{Z}/n\mathbb{Z}$, with the example $\mathbb{Z}/6\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, 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)); and units, their inverses modulo n , and the field $\mathbb{Z}/p\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.5.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.2). Section 2.2 gives these fields the name $\mathbb{F}_p$ that its Section 3.5 left to this chapter. Its move “least positive element, then divide” proves Proposition 2.5.2.
- From *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapters 4–6, for examples, comparisons and a few exercises only: $\mathbb{R}$ as a complete ordered field containing $\mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.2.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.3.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.6.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 5.4.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.4.1), from its Chapter 5; square roots in $\mathbb{R}$, the field $\mathbb{Q}(\sqrt{2})$ and its conjugation, and the theorem that $\mathbb{R}$ has no automorphism but the identity (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 6.4.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.4.5, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.4.6, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (Conjugation in $\mathbb{Q}(\sqrt{2})$), Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 6.1.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 6.3.4, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.1), from its Chapter 6; and the fraction rules and the embedding of $\mathbb{Q}$ into an ordered field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 4.1.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 4.2.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 4.2.2), from its Chapter 4, which remarks in Sections 2.1 and 2.5 compare with.
- From *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 1: the citing rule by which induction and recursion apply to $\mathbb{N}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 1.7.3), in Sections 2.4–2.6, and the axioms (Z5) and (Z6) (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Axiom 1.1.1) that make the set of subfields containing a given set a set, in Section 2.3.
- From Chapter 1 of this volume, for examples and review exercises only: $\mathbb{C}$ as a field containing $\mathbb{R}$ (Definition 1.1.1, Proposition 1.1.1, Proposition 1.1.2, Proposition 1.2.3, Theorem 1.2.4); conjugation and its rules (Definition 1.2.1, Theorem 1.2.2), the first automorphism of Section 2.4; complex square roots (Proposition 1.4.1), compared with in Section

2.1 and used in Exercise R1 of Section 2.6; the power laws in a commutative ring (Proposition 1.1.3), compared with in Section 2.6; and the method by which $\mathbb{C}$ cannot be ordered (Proposition 1.4.3), reused in Exercise R3 of Section 2.6.

- From *Sets, Relations, and Cardinality*: functions, composition, bijections, inverse functions and images, and intersections of families of sets (Sets, Relations, and Cardinality, Definition 1.4.5, Sets, Relations, and Cardinality, Definition 1.4.2, Sets, Relations, and Cardinality, Theorem 1.4.4, Sets, Relations, and Cardinality, Definition 1.5.2, Sets, Relations, and Cardinality, Theorem 1.5.4, Sets, Relations, and Cardinality, Definition 1.6.1, Sets, Relations, and Cardinality, Definition 1.2.4), from its Chapter 1; primes, quotient sets, and the recursion theorem with its sums and powers, whose proofs Section 2.6 reuses in any commutative ring (Sets, Relations, and Cardinality, Definition 2.2.2, Sets, Relations, and Cardinality, Definition 2.5.4, Sets, Relations, and Cardinality, Theorem 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.1, Sets, Relations, and Cardinality, Definition 2.3.2, Sets, Relations, and Cardinality, Proposition 2.3.4), from its Chapter 2; finite and infinite sets and the pigeonhole principle (Sets, Relations, and Cardinality, Definition 3.1.2, Sets, Relations, and Cardinality, Proposition 3.1.6, Sets, Relations, and Cardinality, Example (Hilbert's Hotel), Sets, Relations, and Cardinality, Theorem 3.1.2, Sets, Relations, and Cardinality, Corollary 3.1.3, Sets, Relations, and Cardinality, Theorem 3.1.9), from its Chapter 3.
- From *Logic and Proof*: induction (Logic and Proof, Axiom 4.2.1), from its Section 4.2, and, for the five find-the-error exercises and the proof-ordering exercise of Section 2.3, the catalogue of moves that are not allowed (Logic and Proof, Example (What is not allowed)), from its Section 8.6.

No proof of a result rests on $\mathbb{R}$ or $\mathbb{C}$: they enter through examples, remarks and exercises. Nothing from linear algebra is used, and polynomials appear only as equations between elements, never as objects; Chapters 4 and 5 build them.

Time. About 25 hours on the core track (all of A, one B and one C per section, the exit checks); about 40 hours for everything.

2.-1.1 Roadmap

- **The Field Axioms and the First Examples.** What elimination needs, and the definition of a field with the clauses (F1)–(F9) and its agreement with the definition in *Number Systems*; the rules of every field, collected from the commutative-ring rules with the fraction rules added; the two square roots $\pm y$, with $\mathbb{Z}/8\mathbb{Z}$ as the ring where there are more; one linear equation and a system of two, solved in any field; $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ as fields; and $\mathbb{N}$, $\mathbb{Z}$, the zero ring and $\mathbb{Z}/6\mathbb{Z}$ as non-examples, each with the clause that fails.
- **Finite Fields from Modular Arithmetic.** The arithmetic of $\mathbb{Z}/n\mathbb{Z}$ recalled, with the tables of $\mathbb{F}_2$; Bézout's lemma in the form the linear-algebra volumes cite, and $\mathbb{Z}/n\mathbb{Z}$ as a field exactly for prime n ; the fields $\mathbb{F}_p$, with inverses found by trial and by the Euclidean algorithm and the elimination of Section 2.1 run over $\mathbb{F}_5$; why a non-zero class modulo a composite cannot always be divided by, and why $\mathbb{F}_p$ has no order; and, as an exercise, a field with four elements that is not $\mathbb{Z}/4\mathbb{Z}$.
- **Subfields.** Subfields, with examples and one-clause non-examples; the subfield test, which shows that a subfield is a field with the zero and one of the big field and reduces the check to 1, differences and quotients; $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ and $\mathbb{Q}(i) \subseteq \mathbb{C}$ as subfields, with $\mathbb{Z}[i]$ failing only at inverses; the warning that $\{[0], [3]\} \subseteq \mathbb{Z}/6\mathbb{Z}$ is a field with another one; and intersections of subfields, the smallest subfield containing a set, and the prime subfield, which for $\mathbb{F}_p$ is $\mathbb{F}_p$ itself.
- **Field Homomorphisms.** Homomorphisms, isomorphisms and automorphisms, and why

$\varphi(1) = 1$ is required; the theorem that a homomorphism keeps 0, negatives and inverses, is injective, and maps its domain onto a subfield isomorphic to it; conjugation of $\mathbb{C}$ and of $\mathbb{Q}(\sqrt{2})$ as automorphisms, and $\mathbb{R}$ with none but the identity; and the pairs $\mathbb{C} \rightarrow \mathbb{R}$, $\mathbb{F}_2 \rightarrow \mathbb{Q}$ and $\mathbb{Q} \rightarrow \mathbb{F}_p$ with no homomorphism at all.

- **Integer Multiples, the Characteristic, and the Prime Subfield.** Integer multiples $n \cdot a$ in a commutative ring, negative n included, with the proof for negative n in a second-reading fold; the characteristic, the theorem that $n \cdot 1 = 0$ exactly when $\text{char } F$ divides n (so 2 is invertible exactly when $\text{char } F \neq 2$), and the theorem that it is 0 or a prime; its invariance under subfields and homomorphisms, and the characteristics of the standard fields; the prime subfield as the image of the unique homomorphism from $\mathbb{Q}$ or $\mathbb{F}_p$, so that a homomorphism has no choice on it and $\mathbb{Q}$ and $\mathbb{F}_p$ have no automorphism but the identity; and finite fields, which have prime characteristic.
- **The Binomial Theorem, the Frobenius Map, and Fermat's Little Theorem.** Finite sums in a commutative ring; binomial coefficients by Pascal's rule, with no division, and the absorption identity; the binomial theorem in a commutative ring and the prime dividing the middle coefficients of row p ; the Frobenius map $x \mapsto x^p$, a homomorphism in characteristic p and an automorphism of a finite field; Fermat's little theorem, with powers and inverses computed in $\mathbb{F}_7$, $\mathbb{F}_{31}$ and $\mathbb{F}_{101}$; and review exercises on complex square roots (Chapter 1), square roots in $\mathbb{Q}(\sqrt{2})$, fields that cannot be ordered, and the homomorphisms $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{R}$.

2.-1.2 Named moves

- **Test inside the big field.** For a subset K of a field L , the identities (F1), (F2), (F5), (F6) and (F9) hold in K because they hold for all elements of L ; only closure and the elements 0, 1, $-a$ and a^{-1} need checking. It is named in the Idea of the subfield test (Proposition 2.3.1) in Section 2.3. Through that test it shows that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$ are fields and that an intersection of subfields is a subfield in Section 2.3, and that the image of a homomorphism is a subfield in Section 2.4. The warning of Section 2.3 marks its limit: inside a ring that is not a field, a subset can be a field whose one is not that of the ring, as $\{[0], [3]\} \subseteq \mathbb{Z}/6\mathbb{Z}$ is.
- **Push the equation through φ .** To find $\varphi(x)$, apply φ to an equation that x satisfies, such as $a + (-a) = 0$, $aa^{-1} = 1$, $i^2 = -1$ or $p \cdot 1 = 0$, and solve the resulting equation in the target field, where it often has only one solution. It is named in Section 2.4, after the proof of Proposition 2.4.1, whose parts (a) and (b) run it in full. Exercise B1 of Section 2.4 leaves its last step to you, and Exercise B2 there its last half. When the pushed equation has no solution in the target, it proves that no homomorphism exists (Example (Pairs of Fields with No Homomorphism)). Section 2.5 uses it for the uniqueness half of Theorem 2.5.5, and Exercise R4 of Section 2.6 to find the homomorphisms $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{R}$.
- **Count copies of 1.** A question about integers acting on a field becomes a question about the elements $n \cdot 1$: by Lemma 2.5.1, $n \cdot a = (n \cdot 1)a$, and $n \mapsto n \cdot 1$ respects sums and products. Then the move of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3, “take the least positive element, then divide by it”, turns “ $n \cdot 1 = 0$ ” into “ $\text{char } F$ divides n ” (Proposition 2.5.2). Section 2.5 names only the second step; the name “count copies of 1” is given here. Since a homomorphism sends $n \cdot 1$ to $n \cdot 1$, it has no choice on the prime subfield (Corollary 2.5.6). In Section 2.6 the same counting kills the middle terms of $(x + y)^p$, and that rigidity turns the Frobenius map of $\mathbb{F}_p$ into Fermat's little theorem.