

2.1 The Field Axioms and the First Examples

Number Systems: From $\mathbb{N}$ to $\mathbb{R}$ defined fields (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 2.3.1) and built $\mathbb{Q}$, $\mathbb{R}$ and, for each prime p , the field $\mathbb{Z}/p\mathbb{Z}$. Chapter 1 added $\mathbb{C}$. This chapter looks at fields as a kind of object in their own right. Its first section restates the definition under the name that the linear-algebra volumes use, collects the rules that hold in every field, solves one and two linear equations in any field, and sorts the standard examples from the standard non-examples, naming in each case the clause that fails.

2.1.1 What solving equations needs

Here is a small system of equations, solved the way it is solved at school:

$$\begin{aligned} 2x + 3y &= 7, \\ x - y &= 1. \end{aligned}$$

Subtract twice the second equation from the first: $5y = 5$. Divide by 5: $y = 1$. Then $x = 1 + y = 2$. Check: $2 \cdot 2 + 3 \cdot 1 = 7$ and $2 - 1 = 1$.

List the moves. Equations were combined by sums and differences, one equation was scaled by a number, and one was divided by a number that is **not zero**. Silently, terms were also reordered, regrouped, and brackets were multiplied out. Elimination, the method the linear-algebra volumes run on systems of any size, uses these moves and nothing else.

Now stay inside $\mathbb{Z}$. The equation $2x = 1$ has integer coefficients and no integer solution: $2x$ is even and $1 = 2 \cdot 0 + 1$ is odd, and no integer is both (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Corollary 3.1.3 (a)). The move “divide by 2” leads out of $\mathbb{Z}$. So the dividing line between $\mathbb{Z}$ and $\mathbb{Q}$ is division, and division by every non-zero element is what the definition must ask for.

A field is a number system where you can add, subtract, multiply, and divide by anything non-zero, with the usual rules.

2.1.2 The definition

The definition lists the rules once, as clauses that can be checked and cited. The numbering is the one *Number Systems* used for commutative rings, and the one the linear-algebra volumes cite.

Definition 2.1.1. Field

A **field** is a set F together with two functions, **addition** $+: F \times F \rightarrow F$, $(a, b) \mapsto a + b$, and **multiplication** $\cdot: F \times F \rightarrow F$, $(a, b) \mapsto a \cdot b = ab$, satisfying the following clauses.

- (F1) $a + b = b + a$ **for all** $a, b \in F$.
- (F2) $(a + b) + c = a + (b + c)$ **for all** $a, b, c \in F$.
- (F3) **There is** an element $0 \in F$ such that $a + 0 = a$ **for every** $a \in F$.
- (F4) **For every** $a \in F$ there is an element $-a \in F$ such that $a + (-a) = 0$.
- (F5) $(ab)c = a(bc)$ **for all** $a, b, c \in F$.
- (F6) $ab = ba$ **for all** $a, b \in F$.

(F7) **There is** an element $1 \in F$ with $1 \neq 0$ such that $a \cdot 1 = a$ **for every** $a \in F$.

(F8) **For every non-zero** $a \in F$ there is an element $a^{-1} \in F$ such that $aa^{-1} = 1$.

(F9) $a(b + c) = ab + ac$ **for all** $a, b, c \in F$.

We write $a - b := a + (-b)$, and $a/b := ab^{-1}$ for $b \neq 0$.

Read the clauses in three groups.

- (F1)–(F4) speak only of addition. The order and the grouping of a sum do not matter, 0 changes nothing when added, and each element can be undone by its negative. Subtraction is built from these.
- (F5)–(F8) repeat those four statements for multiplication, with one change: an inverse is demanded only of a **non-zero** element. So division is defined only by non-zero elements, and no clause ever calls for division by 0. Clause (F7) also demands that the two neutral elements differ.
- (F9), the distributive law, is the single bridge between the two operations: it alone mentions both, and multiplying out brackets rests on it, with (F6) for a bracket on the left.

Mind the order of the quantifiers in (F3): there is **one** element 0 that works **for every** a . The weaker reading, “each a has its own z with $a + z = a$ ”, would let z change with a , and it is not what (F3) says. In (F4) the order is the other way round, as it has to be: the negative $-a$ depends on a .

Both operations are functions **into** F : a sum or product of two elements of F is again in F . For a candidate field cut out of a larger number system, that closure is where checking starts. We say “ F is a field” when the two operations are understood, and write $(F, +, \cdot)$ when they must be named.

Remark (The same definition in *Number Systems*). Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1 calls a set with two operations a **commutative ring** when (F1)–(F7) and (F9) hold, its (F7) asking only for an element 1 with $a \cdot 1 = a$; it calls a commutative ring a **field** when, in addition, $1 \neq 0$ and (F8) hold. Clause by clause, these are the conditions of Definition 2.1.1: the nine clauses are worded alike, and the only difference is where the condition $1 \neq 0$ is filed, inside (F7) here and as a separate clause there. So F is a field in the sense of Definition 2.1.1 **if and only if** it is a field in the sense of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1. Every result that *Number Systems* proves for fields, or for commutative rings, therefore applies to every field of this chapter, and conversely. The separate filing there has a purpose: it lets the one-element set $\{0\}$ count as a commutative ring (the zero ring) while keeping it out of the fields.

Quick check. Is $\mathbb{Q}_{>0}$, the set of positive rationals with the usual $+$ and $\cdot$ of $\mathbb{Q}$, a field?

Solution. No. Addition and multiplication do map $\mathbb{Q}_{>0} \times \mathbb{Q}_{>0}$ into $\mathbb{Q}_{>0}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.5.1, with (P1) of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.3). But (F3) fails. An element $z \in \mathbb{Q}_{>0}$ with $1 + z = 1$ would satisfy $z = 0 + z = ((-1) + 1) + z = (-1) + (1 + z) = (-1) + 1 = 0$ in the field $\mathbb{Q}$, by (F1), (F3), (F4) and (F2), and $0 \notin \mathbb{Q}_{>0}$. (Once (F3) fails, (F4) cannot even be stated.)

2.1.3 Rules that hold in every field

The definition's notation takes something for granted. The symbols 0 , $-a$ and a^{-1} are written as names of single elements, while (F3), (F4), (F7) and (F8) assert only that suitable elements **exist**. Were there two different zeros in some field, the symbols 0 , $a - b$ and a/b would be ambiguous. The next theorem removes the worry and collects the rules of school algebra that every field obeys. Most of it was proved in *Number Systems* for every commutative ring; we collect it under one name, citing the proofs there, and add the rules for fractions as part (g).

Theorem 2.1.1. Basic Properties of Fields

Let F be a field and let $a, b, c, d \in F$.

- (a) The element 0 in (F3) is unique, and the element 1 in (F7) is unique.
- (b) (Cancellation) If $a + b = a + c$, then $b = c$. If $ab = ac$ and $a \neq 0$, then $b = c$.
- (c) The negative $-a$ in (F4) is unique, and for $a \neq 0$ the inverse a^{-1} in (F8) is unique.
- (d) $0 \cdot a = 0$.
- (e) $(-1)a = -a$.
- (f) If $ab = 0$, then $a = 0$ or $b = 0$.
- (g) If $b \neq 0$ and $d \neq 0$, then $bd \neq 0$, $(bd)^{-1} = b^{-1}d^{-1}$, $(b^{-1})^{-1} = b$, and

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Idea. Work backwards from each goal to the clause that could produce it; each part then takes a few lines. For uniqueness, take two candidates and prove them equal. No clause says anything about $0 \cdot a$, so for (d) we manufacture a place where (F9) can act: $0 = 0 + 0$, distribute, cancel. In (f) the hypothesis $a \neq 0$ has exactly one use, which is to unlock (F8). The fraction rules in (g) come from one move: an element is identified by showing that it satisfies the defining equation of the element we want, and uniqueness finishes.

Proof. By the remark after Definition 2.1.1, F is a commutative ring in the sense of Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Definition 2.3.1, so Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Proposition 2.3.2 applies to it.

- (a) This is Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Proposition 2.3.2 (a).
- (b) Suppose $a + b = a + c$. Put $-a$ in front of each side and regroup with (F2): this gives $((-a) + a) + b = ((-a) + a) + c$. By (F1) and (F4), $(-a) + a = a + (-a) = 0$, so $0 + b = 0 + c$, and by (F1) and (F3) this says $b = c$.
Now suppose $ab = ac$ and $a \neq 0$. By (F8), a^{-1} exists. Using (F7), (F8), (F6) and (F5),

$$\begin{aligned} b &= b \cdot 1 = b(aa^{-1}) = (ba)a^{-1} = (ab)a^{-1} \\ &= (ac)a^{-1} = (ca)a^{-1} = c(aa^{-1}) = c \cdot 1 = c. \end{aligned}$$

- (c) The negative is unique by Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Proposition 2.3.2 (a). For $a \neq 0$, clause (F8) says that a is a unit of F in the sense of Number Systems: From $\backslash(\backslash n N \backslash)$ to $\backslash(\backslash n R \backslash)$, Definition 3.5.1, and the inverse of a unit is unique (the well-definedness paragraph after Number Systems: From $\backslash(\backslash n N \backslash)$ to

$\setminus(\setminus\mathbf{nR}\setminus)$, Definition 3.5.1).

- (d) By Number Systems: From $\setminus(\setminus\mathbf{nN}\setminus)$ to $\setminus(\setminus\mathbf{nR}\setminus)$, Proposition 2.3.2 (b), $a \cdot 0 = 0$, and $0 \cdot a = a \cdot 0$ by (F6).
- (e) By Number Systems: From $\setminus(\setminus\mathbf{nN}\setminus)$ to $\setminus(\setminus\mathbf{nR}\setminus)$, Proposition 2.3.2 (c) with $a = 1$, $(-1)b = -(1 \cdot b)$ for every $b \in F$; and $1 \cdot b = b \cdot 1 = b$ by (F6) and (F7). Applied to $b = a$, this gives $(-1)a = -a$.
- (f) Suppose $ab = 0$. If $a = 0$ there is nothing to prove, so suppose $a \neq 0$. By (F8), a is a unit of F (Number Systems: From $\setminus(\setminus\mathbf{nN}\setminus)$ to $\setminus(\setminus\mathbf{nR}\setminus)$, Definition 3.5.1), and a unit is not a zero divisor (the paragraph after Number Systems: From $\setminus(\setminus\mathbf{nN}\setminus)$ to $\setminus(\setminus\mathbf{nR}\setminus)$, Definition 3.5.1): from $ab = 0$ it follows that $b = 0$. So $a = 0$ or $b = 0$.
- (g) Let $b \neq 0$ and $d \neq 0$. If $bd = 0$, then (f) would give $b = 0$ or $d = 0$; so $bd \neq 0$. By (F8), b and d are units of F . A product of units is a unit, with $(bd)^{-1} = b^{-1}d^{-1}$, and the inverse of a unit is a unit, with $(b^{-1})^{-1} = b$ (the closure paragraph after Number Systems: From $\setminus(\setminus\mathbf{nN}\setminus)$ to $\setminus(\setminus\mathbf{nR}\setminus)$, Definition 3.5.1). Here $b^{-1} \neq 0$, since $1 \neq 0$ by (F7) and so 0 is not a unit (the paragraph “Why this definition” after Number Systems: From $\setminus(\setminus\mathbf{nN}\setminus)$ to $\setminus(\setminus\mathbf{nR}\setminus)$, Definition 3.5.1); thus $(b^{-1})^{-1}$ is also the inverse that (F8) supplies, by (c).

For the sum, multiply out with (F9) and reorder with (F5) and (F6):

$$\begin{aligned}(ab^{-1} + cd^{-1})(bd) &= a(b^{-1}b)d + c(d^{-1}d)b \\ &= ad + cb = ad + bc,\end{aligned}$$

by (F8) and (F7) and then (F6). Multiplying both ends by $(bd)^{-1}$, and using $(bd)(bd)^{-1} = 1$ with (F5) and (F7) on the left, gives $ab^{-1} + cd^{-1} = (ad + bc)(bd)^{-1}$, which is the first displayed rule. For the product, (F5) and (F6) give $(ab^{-1})(cd^{-1}) = (ac)(b^{-1}d^{-1}) = (ac)(bd)^{-1}$, by the formula for $(bd)^{-1}$ just proved. This proves the theorem. ■

From now on we use $0 + a = a$ and $1 \cdot a = a$ silently; they follow from (F1), (F3), (F6) and (F7). The larger gain is that any school identity whose proof uses only (F1)–(F9) is true in every field: for instance $(a + b)^2 = a^2 + 2ab + b^2$, where $a^2 := aa$ and $2 := 1 + 1$ (Number Systems: From $\setminus(\setminus\mathbf{nN}\setminus)$ to $\setminus(\setminus\mathbf{nR}\setminus)$, Proposition 2.3.2 (d)), and $(-a)(-b) = ab$ (Number Systems: From $\setminus(\setminus\mathbf{nN}\setminus)$ to $\setminus(\setminus\mathbf{nR}\setminus)$, Proposition 2.3.2 (c)). Part (f) is the rule we will lean on most: a product of non-zero elements is non-zero.

Remark. Part (g), with the uniqueness of inverses in (c), is the content of Number Systems: From $\setminus(\setminus\mathbf{nN}\setminus)$ to $\setminus(\setminus\mathbf{nR}\setminus)$, Lemma 4.1.1 (a) and (b), which *Number Systems* proved for every field when it studied ordered fields. Part (f) and the inverse identities of (g) come from the paragraphs on units after Number Systems: From $\setminus(\setminus\mathbf{nN}\setminus)$ to $\setminus(\setminus\mathbf{nR}\setminus)$, Definition 3.5.1; the two fraction formulas are proved here rather than cited from Number Systems: From $\setminus(\setminus\mathbf{nN}\setminus)$ to $\setminus(\setminus\mathbf{nR}\setminus)$, Lemma 4.1.1, so that no theorem of this section rests on that chapter; only the examples $\mathbb{R}$ and $\mathbb{C}$ below lean on it.

Quick check. In a field, does $a^2 = 0$ imply $a = 0$?

Solution. Yes. $a^2 = aa = 0$, so by [Theorem 2.1.1](#) (f) with $b = a$, $a = 0$ or $a = 0$.

Warning. Cancellation needs its hypothesis. “If $ab = ac$, then $b = c$ ” is **false** without $a \neq 0$: in $\mathbb{Q}$, $0 \cdot 1 = 0 \cdot 2$, yet $1 \neq 2$. Every time a factor is canceled, say why it is not 0.

Part (f) has a consequence that school algebra uses all the time without naming it: an element has at most two square roots, and they are negatives of each other.

Corollary 2.1.2. Equal Squares

Let F be a field and $x, y \in F$. Then $x^2 = y^2$ if and only if $x = y$ or $x = -y$. In particular, $x^2 = 1$ if and only if $x = 1$ or $x = -1$.

Idea. Move everything to one side and factor: $x^2 - y^2 = (x - y)(x + y)$, the school identity, which holds in every field. A product is zero only when a factor is, by part (f), and the two factors give the two cases.

Proof. First, $(x - y)(x + y) = x^2 - y^2$. Indeed, by (F9) and (F6), $(x + (-y))(x + y) = xx + xy + (-y)x + (-y)y$, and Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (c) turns the last two terms into $-(yx)$ and $-(yy)$. Since $yx = xy$ by (F6), the terms xy and $-(xy)$ add to 0 by (F4), and what is left is $x^2 - y^2$.

($\Rightarrow$) If $x^2 = y^2$, then $x^2 - y^2 = y^2 + (-y^2) = 0$ by (F4), so $(x - y)(x + y) = 0$. By [Theorem 2.1.1](#) (f), $x - y = 0$ or $x + y = 0$. In the first case, adding y to both sides gives $x = y$, by (F2), (F1), (F4) and (F3). In the second, y satisfies the defining equation of $-x$, so $y = -x$ by [Theorem 2.1.1](#) (c), and then $x = -(-x) = -y$ by Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (a).

($\Leftarrow$) If $x = y$, there is nothing to prove. If $x = -y$, then $x^2 = (-y)(-y) = yy = y^2$ by Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (c).

For the last sentence take $y = 1$, with $1^2 = 1$ by (F7). ■

Remark. The two square roots y and $-y$ can coincide even when $y \neq 0$: in the field with two elements of the next section, $1 + 1 = 0$, so $-1 = 1$. And the corollary needs (f), so it can fail in a commutative ring with zero divisors. In $\mathbb{Z}/8\mathbb{Z}$ we have $[3]^2 = [9] = [1]$, yet $[3] \neq [1]$ and $[3] \neq [-1] = [7]$, since 8 divides neither $3 - 1 = 2$ nor $3 - 7 = -4$. For $\mathbb{C}$, Chapter 1 proved the same fact directly from real and imaginary parts (Proposition 1.4.1 (b)); the corollary gives it in every field at once.

2.1.4 Solving linear equations in a field

The opening slogan promised that a field is where elimination works. Here is that promise kept for one equation in one unknown and for two equations in two unknowns.

Proposition 2.1.3. Linear Equations in a Field

Let F be a field and let $a, b, c, d, e, f \in F$.

- (a) If $a \neq 0$, the equation $ax = b$ has **exactly one** solution $x \in F$, namely $x = a^{-1}b$.
- (b) If $ad - bc \neq 0$, the system

$$\begin{aligned} ax + by &= e, \\ cx + dy &= f \end{aligned}$$

has **exactly one** solution $(x, y) \in F \times F$, namely

$$x = \frac{ed - bf}{ad - bc}, \quad y = \frac{af - ce}{ad - bc}.$$

Idea. Uniqueness and existence are separate jobs. For uniqueness, assume a solution and run the school elimination on it: one combination of the two equations kills y , another kills x , and each leaves an equation of the form (a). For existence, substitute the candidate and multiply out. The quantity $ad - bc$ is exactly the coefficient elimination produces, and the hypothesis lets us divide by it.

Proof.

- (a) By (F5), (F8) and (F7), $a(a^{-1}b) = (aa^{-1})b = 1 \cdot b = b$, so $x = a^{-1}b$ is a solution. If $ax = b$ and $ax' = b$, then $ax = ax'$ with $a \neq 0$, so $x = x'$ by cancellation ([Theorem 2.1.1 \(b\)](#)).
- (b) Write $D := ad - bc$, so $D \neq 0$.

Uniqueness. Let (x, y) be a solution. Multiply the first equation by d , the second by b , and subtract. Multiplying out with (F9), reordering with (F5) and (F6), and using Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (c) for the signs,

$$\begin{aligned} d(ax + by) - b(cx + dy) &= (ad)x + (bd)y - (bc)x - (bd)y \\ &= (ad - bc)x = Dx, \end{aligned}$$

while the right-hand sides give $de - bf = ed - bf$. So $Dx = ed - bf$. In the same way, $a(cx + dy) - c(ax + by) = (ad - bc)y = Dy$ and the right-hand sides give $af - ce$, so $Dy = af - ce$. By (a), applied twice with the non-zero coefficient D , $x = D^{-1}(ed - bf)$ and $y = D^{-1}(af - ce)$. These are the displayed values, since $D^{-1}u = uD^{-1} = u/D$ by (F6).

Existence. Put $x_0 := (ed - bf)D^{-1}$ and $y_0 := (af - ce)D^{-1}$. By (F5), (F6) and (F9), multiplying out and reordering with (F5) and (F6), and using Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$

to $\setminus(\setminus\mathbb{N}\setminus)$, Proposition 2.3.2 (c) for the signs,

$$\begin{aligned} ax_0 + by_0 &= (a(ed - bf) + b(af - ce))D^{-1} \\ &= (ade - abf + abf - bce)D^{-1} \\ &= e(ad - bc)D^{-1} = eDD^{-1} = e, \end{aligned}$$

by (F8) and (F7) at the end. Likewise

$$\begin{aligned} cx_0 + dy_0 &= (c(ed - bf) + d(af - ce))D^{-1} \\ &= (cde - bcf + adf - cde)D^{-1} \\ &= f(ad - bc)D^{-1} = f. \end{aligned}$$

So (x_0, y_0) is a solution, and by uniqueness it is the only one. ■

Both hypotheses have a job. Over $\mathbb{Z}$, part (a) fails: $2 \neq 0$, and $2x = 1$ has no integer solution, because the inverse 2^{-1} of (F8) is missing. And if $ad - bc = 0$, part (b) fails in every field: the system $x + y = 1$, $x + y = 0$ has no solution, since it would give $1 = 0$, while $x + y = 0$, $2x + 2y = 0$ has the solutions $(t, -t)$ for every $t \in F$, at least two of them ($t = 0$ and $t = 1$). The linear-algebra volumes treat n equations in n unknowns by the same elimination.

2.1.5 Examples

Three fields are already at hand. Each was proved a field in the sense of Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Definition 2.3.1, and the remark after Definition 2.1.1 translates.

Example. The Fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

Explain why $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, with their usual addition and multiplication, are fields.

Solution. For $\mathbb{Q}$, built as classes of pairs of integers, Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Theorem 2.4.3 proves that it is a field in the sense of Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Definition 2.3.1. For $\mathbb{R}$, built as classes of Cauchy sequences of rationals, Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Theorem 5.2.3 does the same; there $1 \neq 0$ is part of the field clause. For $\mathbb{C} := \mathbb{R} \times \mathbb{R}$, Theorem 1.2.4 proves it, resting on the arithmetic laws Proposition 1.1.2 and the inverse Proposition 1.2.3. In each case the remark after Definition 2.1.1 turns “field in the sense of *Number Systems*” into “field in the sense of Definition 2.1.1”, with the same zero, one, negatives and inverses.

These three are infinite: each contains an injective image of the infinite set $\mathbb{N}$ (Sets, Relations, and Cardinality, Example (Hilbert’s Hotel)), through Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Proposition 2.2.3 (a), Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Proposition 2.4.4, Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Theorem 5.4.1 (b) and Proposition 1.1.1. A finite set has only finite subsets (Sets, Relations, and Cardinality, Proposition 3.1.6). The next section produces finite fields, and Section 2.3 produces fields strictly between $\mathbb{Q}$ and $\mathbb{R}$.

Changing an operation on a familiar set can give a new field; deciding means checking every clause.

Example. A New Multiplication on $\mathbb{Q}$

Show that $\mathbb{Q}$, with the usual addition and the new multiplication $a \odot b := -(ab)$, is a field, and find its one.

Solution. Addition is that of $\mathbb{Q}$, so (F1)–(F4) hold with the usual 0 and negatives. The new product is a function $\mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$. Each identity below is computed in the field $\mathbb{Q}$ (Example (The Fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$)), the signs by Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.3.2 (a) and (c). For all $a, b, c \in \mathbb{Q}$:

- (F5): $(a \odot b) \odot c = -((-ab)c) = abc = -(a(-bc)) = a \odot (b \odot c)$.
- (F6): $-(ab) = -(ba)$.
- (F9): $a \odot (b + c) = -(ab + ac) = -(ab) + (-ac) = a \odot b + a \odot c$, since $-(u + v) = (-1)(u + v) = -u + (-v)$ by Theorem 2.1.1 (e).
- (F7): the one is -1 , since $a \odot (-1) = -(a(-1)) = -(-a) = a$, and $-1 \neq 0$ (otherwise $1 = -(-1) = -0 = 0$, where $-0 = 0$ by Theorem 2.1.1 (c), since $0 + 0 = 0$).
- (F8): a non-zero a has the inverse a^{-1} , the usual one, since $a \odot a^{-1} = -(aa^{-1}) = -1$, the one of this field.

The one of a field need not be the number 1.

2.1.6 Non-examples

Each system below falls short of the slogan somewhere. For each, find the precise clause that breaks; a vague “it is not like $\mathbb{Q}$ ” teaches nothing.

Example. Four Systems That Are Not Fields

For each of the following, with its usual operations, name the clauses of Definition 2.1.1 that fail, with a witness: (i) $\mathbb{N}$; (ii) $\mathbb{Z}$; (iii) the zero ring $\{0\}$, with $0 + 0 := 0$ and $0 \cdot 0 := 0$; (iv) $\mathbb{Z}/6\mathbb{Z}$.

Solution.

- (i) *Number Systems* checked the minimal change from $\mathbb{N}$ to $\mathbb{Z}$: $\mathbb{N}$ satisfies (F1)–(F3), (F5)–(F7) and (F9), and (F4) fails at $a = 1$, since $1 + x \neq 0$ for every $x \in \mathbb{N}$ (the non-example after Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Definition 2.3.1). The condition $1 \neq 0$ holds, since it holds in $\mathbb{Z}$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Theorem 2.3.1), and $\mathbb{N} \subseteq \mathbb{Z}$ with ι injective (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.2.3 (a)). Clause (F8) fails too, at $a = 2$: a natural number x with $2x = 1$ would be an integer with $2x = 1$ (ι preserves products, Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.2.3 (a)), and there is none (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Corollary 3.1.3 (a)).
- (ii) $\mathbb{Z}$ is a commutative ring with $1 \neq 0$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Theorem 2.3.1), so (F1)–(F7) and (F9) hold. Only (F8) fails, at $a = 2$, by the same parity argument.
- (iii) Every clause other than (F7) and (F8) is an equation between elements of $\{0\}$, and each such equation reads $0 = 0$; (F8) holds because there is no non-zero element to

invert. The only candidate for the element 1 of (F7) is 0, and (F7) demands $1 \neq 0$. So exactly the condition $1 \neq 0$ inside (F7) fails. This is the reason the condition is there: without it, a one-element “field” would make every statement of the form “a field has a non-zero element” false.

- (iv) $\mathbb{Z}/6\mathbb{Z}$ is a commutative ring with $[1] \neq [0]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 3.4.3 (a), (c)), so (F1)–(F7) and (F9) hold. But $[2][3] = [6] = [0]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (Multiplication modulo six and modulo five)), while $[2] \neq [0]$ and $[3] \neq [0]$, since 6 divides neither 2 nor 3. If $[2]$ had an inverse u , then $[3] = (u[2])[3] = u([2][3]) = u[0] = [0]$, by (F7), (F8), (F6), (F5) and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b), which is false. So (F8) fails at $[2]$. Had $\mathbb{Z}/6\mathbb{Z}$ been a field, Theorem 2.1.1 (f) would have forbidden the product $[2][3] = [0]$ outright.

The first linear-algebra volume meets one more kind of non-example, the square matrices, where (F6) fails: two matrices can give different products in the two orders.

2.1.7 Why these axioms

Drop a clause and something we use breaks.

- **Without (F8)**, elimination halts at the first coefficient that cannot be inverted, as $2x = 1$ over $\mathbb{Z}$ showed.
- **Without (F6)**, numbers would not commute with each other. Linear algebra swaps scalars constantly (in the first linear-algebra volume, when a vector is multiplied by two numbers in turn), so commutativity is kept.
- **Without $1 \neq 0$** , the zero ring of Example (Four Systems That Are Not Fields) (iii) would count as a field.

The word “field” is a historical label; nothing in it is meant literally.

Warning. Order is not part of a field. Clauses (F1)–(F9) say nothing about $<$, so “squares are ≥ 0 ” has no meaning in a general field, and read in $\mathbb{C}$ it is false, since $i^2 = -1$ (Chapter 1). Likewise “ $1 + 1 \neq 0$ ” is not a clause, and it fails in the field with two elements of the next section. In a general field, never use an inequality.

2.1.8 Exercises

2.1.8.1 A. Check your understanding

Exercise. A1

- State the definition of a field.
- Which clauses of Definition 2.1.1 does each of $\mathbb{N}$, $\mathbb{Z}$ and the zero ring $\{0\}$ fail?
- True or false: in every field, $ab = ac$ implies $b = c$. Justify your answer.
- Which parts of Theorem 2.1.1 fail in the commutative ring $\mathbb{Z}/6\mathbb{Z}$? Give a witness for each.
- Use Proposition 2.1.3 to solve $3x + 2y = 1$, $x - y = 2$ in $\mathbb{Q}$.

Solution.

- (a) A field is a set F with two functions $+, \cdot: F \times F \rightarrow F$ satisfying (F1)–(F9) of [Definition 2.1.1](#), where (F7) includes $1 \neq 0$ and (F8) asks for inverses of non-zero elements only.
- (b) $\mathbb{N}$: (F4), at $a = 1$, and (F8), at $a = 2$. $\mathbb{Z}$: only (F8), at $a = 2$. $\{0\}$: only the condition $1 \neq 0$ in (F7). (See [Example \(Four Systems That Are Not Fields\)](#).)
- (c) False. With $a = 0$, $b = 1$, $c = 2$ in $\mathbb{Q}$: $0 \cdot 1 = 0 = 0 \cdot 2$, but $1 \neq 2$. Cancellation needs $a \neq 0$ ([Theorem 2.1.1](#) (b)).
- (d) Multiplicative cancellation in (b) fails: $[2][1] = [2]$ and $[2][4] = [8] = [2]$, but $[1] \neq [4]$, since 6 does not divide $4 - 1 = 3$. Part (f) fails: $[2][3] = [0]$ with $[2], [3] \neq [0]$. The first clause of (g) fails for the same pair: $[2] \neq [0]$, $[3] \neq [0]$, but $[2][3] = [0]$. The uniqueness of inverses in (c) is not violated, but for $[2]$ it says nothing, since $[2]$ has no inverse ([Example \(Four Systems That Are Not Fields\)](#) (iv)). Parts (a), (d) and (e) hold in every commutative ring (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (a)–(c), with (F6), (F7)), and so does additive cancellation, whose proof in (b) uses only (F1)–(F4).
- (e) Here $a = 3$, $b = 2$, $c = 1$, $d = -1$, $e = 1$, $f = 2$, and $ad - bc = -3 - 2 = -5 \neq 0$. So

$$x = \frac{1 \cdot (-1) - 2 \cdot 2}{-5} = \frac{-5}{-5} = 1, \quad y = \frac{3 \cdot 2 - 1 \cdot 1}{-5} = \frac{5}{-5} = -1.$$

Check: $3 \cdot 1 + 2 \cdot (-1) = 1$ and $1 - (-1) = 2$.

2.1.8.2 B. Practice

Exercise. B1

Let F be a field and $a, b, x \in F$. Prove:

- (a) $-(a - b) = b - a$;
- (b) if $a \neq 0$, then $-a \neq 0$ and $(-a)^{-1} = -(a^{-1})$;
- (c) $x^2 = x$ if and only if $x = 0$ or $x = 1$;
- (d) $x^2 + x = 0$ if and only if $x = 0$ or $x = -1$.

Solution.

- (a) By (F1) and (F2), $(a - b) + (b - a) = (a + (-a)) + (b + (-b)) = 0 + 0 = 0$, using (F4) and (F3). So $b - a$ satisfies the defining equation of $-(a - b)$, and $-(a - b) = b - a$ by the uniqueness of negatives ([Theorem 2.1.1](#) (c)).
- (b) If $-a = 0$, then $a = -(-a) = -0 = 0$, by Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (a) and $0 + 0 = 0$; so $-a \neq 0$. By Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (c) and (F8), $(-a)(-(a^{-1})) = aa^{-1} = 1$. So $-(a^{-1})$ satisfies the defining equation of $(-a)^{-1}$, and the two are equal by [Theorem 2.1.1](#) (c).
- (c) By (F7), (F9) and Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (c), $x(x - 1) = xx + x(-1) = x^2 - x$. So $x^2 = x$ if and only if $x(x - 1) = 0$, adding $-x$ or x to both sides. By [Theorem 2.1.1](#) (f), $x(x - 1) = 0$ gives $x = 0$ or $x - 1 = 0$, that is, $x = 1$. Conversely, $0^2 = 0$ by [Theorem 2.1.1](#) (d), and $1^2 = 1$ by (F7).

- (d) By (F7) and (F9), $x(x+1) = x^2 + x$. So $x^2 + x = 0$ means $x(x+1) = 0$, which by [Theorem 2.1.1](#) (f) gives $x = 0$ or $x+1 = 0$, and the latter means $x = -1$ by the uniqueness of negatives ([Theorem 2.1.1](#) (c)). Conversely, $0^2 + 0 = 0$ by [Theorem 2.1.1](#) (d) and (F3), and $(-1)^2 + (-1) = 1 + (-1) = 0$, since $(-1)(-1) = 1 \cdot 1 = 1$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (c).

Exercise. B2

Let F be a field and $a, b, c, d \in F$ with $b \neq 0$ and $d \neq 0$. Prove that $a/b = c/d$ if and only if $ad = bc$.

Solution. ($\Rightarrow$) Multiply both sides of $ab^{-1} = cd^{-1}$ by bd . Reordering with (F5) and (F6), and using (F8) and (F7), the left side becomes $a(b^{-1}b)d = ad$ and the right side $c(d^{-1}d)b = cb = bc$. So $ad = bc$.

($\Leftarrow$) By [Theorem 2.1.1](#) (g), $bd \neq 0$ and $(bd)^{-1} = b^{-1}d^{-1}$. Multiply both sides of $ad = bc$ by $b^{-1}d^{-1}$: reordering as before, the left side becomes $ab^{-1}(dd^{-1}) = ab^{-1}$ and the right side $(bb^{-1})cd^{-1} = cd^{-1}$. So $a/b = c/d$.

Exercise. B3: Which Are Fields?

Determine which of the following are fields. Justify your answer.

- (a) $\mathbb{Q}$, with the usual addition and the new multiplication $a \odot b := 2ab$.
- (b) $\mathbb{Q}$, with the usual addition and the new multiplication $a \odot b := ab + 1$.
- (c) The set $\{0, 1\} \subseteq \mathbb{Q}$, with the addition and multiplication of $\mathbb{Q}$.

Solution.

- (a) **A field.** Addition is that of $\mathbb{Q}$, so (F1)–(F4) hold with the usual 0 and negatives. The new product is a function $\mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$. For all $a, b, c \in \mathbb{Q}$: (F5) $(a \odot b) \odot c = 2(2ab)c = 4abc = 2a(2bc) = a \odot (b \odot c)$; (F6) $2ab = 2ba$; (F9) $a \odot (b + c) = 2a(b + c) = 2ab + 2ac = a \odot b + a \odot c$. For (F7) the one is $\frac{1}{2}$: $a \odot \frac{1}{2} = 2a \cdot \frac{1}{2} = a$, and $\frac{1}{2} \neq 0$. For (F8), a non-zero a has the inverse $\frac{1}{4a}$, since $a \odot \frac{1}{4a} = \frac{2a}{4a} = \frac{1}{2}$, the one of this field. Each identity is computed in the field $\mathbb{Q}$ ([Example \(The Fields \$\mathbb{Q}\$, \$\mathbb{R}\$ and \$\mathbb{C}\$ \)](#)). The one of a field need not be the number 1; Exercise B3 of Section 2.4 shows that this field is $\mathbb{Q}$ in disguise.
- (b) **Not a field:** (F9) fails. For all a, b, c , $a \odot (b + c) = ab + ac + 1$, while $a \odot b + a \odot c = ab + ac + 2$, and $1 \neq 2$. For instance $a = b = c = 0$ gives $1 \neq 2$.
- (c) **Not a field:** addition is not a function $\{0, 1\} \times \{0, 1\} \rightarrow \{0, 1\}$, since $1 + 1 = 2 \notin \{0, 1\}$. (The next section puts a different addition on a two-element set and obtains a field.)

2.1.8.3 C. Going deeper

Exercise. C1: Exit check: rules from the axioms

Let F be a field and $a, b, x, y \in F$. Prove the following from (F1)–(F9), using of [Theorem 2.1.1](#)

only part (c) (uniqueness of negatives and inverses) and part (e) $((-1)a = -a)$, and citing no result of *Number Systems*.

- (a) $0 \cdot a = 0$.
- (b) If $ab = 0$, then $a = 0$ or $b = 0$.
- (c) $x^2 = y^2$ if and only if $x = y$ or $x = -y$.

Solution.

- (a) By (F3), $0 + 0 = 0$, so by (F9), $a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$. Add $-(a \cdot 0)$, which exists by (F4), to both sides. On the left this gives 0. On the right, by (F2), (F4) and (F3), $(a \cdot 0 + a \cdot 0) + (-(a \cdot 0)) = a \cdot 0 + (a \cdot 0 + (-(a \cdot 0))) = a \cdot 0 + 0 = a \cdot 0$. So $0 = a \cdot 0$, and $0 \cdot a = a \cdot 0 = 0$ by (F6).
- (b) Suppose $ab = 0$. If $a = 0$, we are done. Otherwise a^{-1} exists by (F8), and by (F7), (F8), (F5) and (F6),

$$b = b \cdot 1 = b(aa^{-1}) = (ba)a^{-1} = (ab)a^{-1} = 0 \cdot a^{-1} = 0,$$

the last step by (a).

- (c) *Two sign rules.* For $u, v \in F$, part (e), (F5) and (F6) give $(-u)v = ((-1)u)v = (-1)(uv) = -(uv)$. Hence $(-1)(-1) = -(1 \cdot (-1)) = -(-1) = 1$, where $1 \cdot (-1) = -1$ by (F6), (F7), and $-(-1) = 1$ by part (c), since $(-1) + 1 = 0$ by (F1), (F4). So $(-y)(-y) = ((-1)y)((-1)y) = ((-1)(-1))(yy) = yy$, by (F5) and (F6).

The factorization. By (F9), (F6) and the first sign rule,

$$\begin{aligned} (x + (-y))(x + y) &= xx + xy + (-y)x + (-y)y \\ &= xx + xy + (-(xy)) + (-(yy)), \end{aligned}$$

using $yx = xy$ by (F6). By (F2), (F4) and (F3) the middle terms cancel, so $(x - y)(x + y) = x^2 - y^2$.

($\Rightarrow$) If $x^2 = y^2$, then $x^2 - y^2 = 0$ by (F4), so $(x - y)(x + y) = 0$, and (b) gives $x - y = 0$ or $x + y = 0$. From $x - y = 0$, adding y and using (F2), (F1), (F4), (F3) gives $x = y$. From $x + y = 0$, x satisfies the defining equation of $-y$ (with (F1)), so $x = -y$ by part (c).

($\Leftarrow$) If $x = y$ there is nothing to prove; if $x = -y$, then $x^2 = (-y)(-y) = y^2$ by the sign rules.

Marking scheme. (10 points)

- 2: for (a), writes $0 = 0 + 0$ and multiplies out $a(0 + 0)$ by (F9).
- 2: cancels $a \cdot 0$ by adding its negative, naming (F2), (F4) and (F3).
- 1: obtains $0 \cdot a$ from $a \cdot 0$ by (F6).
- 2: for (b), treats the case $a = 0$ separately and spends $a \neq 0$ on (F8).
- 1: writes the chain $b = b \cdot 1 = \dots = 0$ with each clause named.
- 1: proves $(x - y)(x + y) = x^2 - y^2$, justifying the cancellation of xy against $-(yx)$, and concludes by (b).
- 1: proves the converse, deriving $(-y)(-y) = yy$ from part (e), (F5) and (F6).

Fatal errors (0 for the step): dividing by a without $a \neq 0$; “ $0 \cdot a = 0$ is obvious”; citing (b)

of the exercise inside the proof of (a). A proof of (c) that factors as $(x + y)(x - y)$ or that cites (b) as “no zero divisors” earns the same points.

Exercise. C2: Find the error

Here is a claim with a proof.

Claim. In a field F , if $x \in F$ and $x^2 = x$, then $x = 0$ or $x = 1$.

Proof. (1) Let $x^2 = x$. (2) Dividing both sides by x gives $x = 1$. (3) So $x = 0$ or $x = 1$.

Is the claim true? Does the proof prove it? If not, name the line that fails, the error, and give a counterexample to the step.

Solution. The **claim is true**: it is [Exercise \(B1\)](#) (c).

The **proof is wrong**, at line (2). Dividing by x means multiplying by x^{-1} , which (F8) supplies only when $x \neq 0$. No line provides $x \neq 0$, so the step cites an unavailable “fact”, cancellation of x without $x \neq 0$: entry (N9) of Logic and Proof, Example (What is not allowed). Line (3) is a correct weakening of (2) by $\forall I$; the proof fails only at (2).

A counterexample to the step: $x = 0$ satisfies $x^2 = x$, and “ $x = 1$ ” is false for it, in every field. The step’s conclusion fails, although the claim’s does not.

A repair: $x^2 = x$ gives $x(x - 1) = 0$, and [Theorem 2.1.1](#) (f) gives $x = 0$ or $x - 1 = 0$, which treats both cases at once.