

2.3 Subfields

The fields met so far sit inside one another. $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, and each is a field with the sum and product of the next: $\mathbb{Q}$ inside $\mathbb{R}$ through the identification of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 5.4 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 5.4.1), and $\mathbb{R}$ inside $\mathbb{C}$ through Proposition 1.1.1. Between $\mathbb{Q}$ and $\mathbb{R}$ lies the set $\mathbb{Q}(\sqrt{2})$ of numbers $a + b\sqrt{2}$ with a, b rational. Sums and products of two such numbers are again of that form, but is $1/(1 + 2\sqrt{2})$? This section gives a short test that settles such questions once, and it finds, inside every field, a smallest field.

Throughout, $a - b := a + (-b)$ and $a/b := ab^{-1}$ for $b \neq 0$, as in Definition 2.1.1, and the rules of Theorem 2.1.1 are used freely, each cited by its letter.

2.3.1 Fields inside fields

A subset K of a field L inherits two operations, but only in a weak sense: $a + b$ and ab are defined for $a, b \in K$, as elements of L . For K to be a field with these operations, the sum and the product must land in K , and the elements that the axioms (F3), (F4), (F7) and (F8) ask for must be found in K . The natural guess is that nothing else needs checking.

A subfield is a subset that a field's own arithmetic never leaves.

Definition 2.3.1. Subfield

Let L be a field. A **subfield** of L is a subset $K \subseteq L$ such that

- $0 \in K$ and $1 \in K$;
- K is **closed under sums and products**: $a + b \in K$ and $ab \in K$ for all $a, b \in K$;
- K is **closed under negatives**: $-a \in K$ for every $a \in K$;
- K is **closed under inverses**: $a^{-1} \in K$ for every non-zero $a \in K$.

Here $0, 1, +, \cdot, -a$ and a^{-1} are those of L .

In words: the first clause asks for the two special elements of L ; the second says that the operations of L do not leave K ; the last two say that the negatives and inverses which L provides already lie in K .

Examples.

- L **itself** is a subfield of L . It is the largest one, and the degenerate case: every clause holds because $K = L$.
- $\mathbb{Q}$ **in** $\mathbb{R}$. Under the identification of a rational q with $\kappa(q) \in \mathbb{R}$, the embedding κ sends $0, 1$, sums, products, negatives and inverses of rationals to the same things in $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 5.4.1 (a), (c)). So all four clauses hold, and $\mathbb{Q}$ is a subfield of $\mathbb{R}$.
- $\mathbb{R}$ **in** $\mathbb{C}$. Chapter 1 checked the four clauses for the copy of $\mathbb{R}$ in $\mathbb{C}$. The zero $0 = (0, 0)$ and the one $1 = (1, 0)$ of $\mathbb{C}$ (Proposition 1.1.2 (d)) are the real numbers 0 and 1 under the identification $a = (a, 0)$ that follows Proposition 1.1.1, and Theorem 1.2.4 gives closure under sums, products, negatives and inverses. So $\mathbb{R}$ is a subfield of $\mathbb{C}$, and so is $\mathbb{Q}$, since a subfield of a subfield is a subfield: each clause of the inner one is a statement about the operations of the outer field.

Non-examples.

- $\{0\} \subseteq \mathbb{Q}$ is closed under sums, products, negatives and inverses (the last vacuously), and does not contain 1, since $1 \neq 0$ in a field.
- $\mathbb{N} \subseteq \mathbb{Q}$ contains 0 and 1 and is closed under sums and products, but not under negatives, since $-1 \notin \mathbb{N}$, nor under inverses, since $2^{-1} = 1/2 \notin \mathbb{N}$ (as for $\mathbb{Z}$ below).
- $\mathbb{Z} \subseteq \mathbb{Q}$ satisfies every clause except closure under inverses: $2^{-1} = 1/2 \notin \mathbb{Z}$, since $2x = 1$ has no solution $x \in \mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 3.1.3 (a)).

These are the non-examples (i)–(iii) of Example (Four Systems That Are Not Fields), now seen from inside $\mathbb{Q}$ (the fourth, $\mathbb{Z}/6\mathbb{Z}$, is not a subset of $\mathbb{Q}$): each fails as a subfield exactly where it failed as a field.

2.3.2 The subfield test

The guess above is right, and it comes with a converse and a shortcut. The converse says that a subset closed under the operations which happens to be a field cannot have its own zero or one: they must be those of L . The shortcut, part (c), reduces the four clauses to three checks.

Proposition 2.3.1. The Subfield Test

Let L be a field and $K \subseteq L$.

- If K is a subfield of L , then K , with the restrictions of $+$ and $\cdot$ to $K \times K$, is a field (Definition 2.1.1). Its zero is 0_L , its one is 1_L , and the negative and the inverse of an element of K are those of L .
- Conversely, suppose that $a + b \in K$ and $ab \in K$ for all $a, b \in K$, and that K with the restricted operations is a field. Then K is a subfield of L : its zero 0_K is 0_L , its one 1_K is 1_L , and its negatives and inverses are those of L .
- K is a subfield of L **if and only if** $1 \in K$, $a - b \in K$ for all $a, b \in K$, and $ab^{-1} \in K$ for all $a, b \in K$ with $b \neq 0$.

Idea.

- The axioms (F1), (F2), (F5), (F6) and (F9) are identities that hold **for all** elements of L , so in particular for all elements of K ; nothing about K needs checking. The other axioms ask for elements, 0 , $-a$, 1 , a^{-1} , and the four clauses of Definition 2.3.1 put them in K . We call this move **test inside the big field**: the identities come free, and only closure and the special elements cost anything.
- runs the other way. An equation true in K is an equation in L , where cancellation and the uniqueness of negatives and inverses are available; so 0_K and 1_K are forced to be 0_L and 1_L .
- builds 0 , $-b$, b^{-1} , $a + b$ and ab out of 1 and the two operations “subtract” and “divide”.

Before reading on: in (b), where is it used that L is a field, and not just a commutative ring?

Proof.

- Since K is closed under sums and products, $+$ and $\cdot$ restrict to functions $K \times K \rightarrow K$. Axioms (F1), (F2), (F5), (F6) and (F9) hold for all elements of L , hence for all elements of K . (F3): $0 \in K$, and $a + 0 = a$ for $a \in K$. (F4): for $a \in K$, $-a \in K$ by closure

under negatives, and $a + (-a) = 0$. (F7): $1 \in K$, $a \cdot 1 = a$ for $a \in K$, and $1 \neq 0$ because this holds in L . (F8): for non-zero $a \in K$, $a^{-1} \in K$ by closure under inverses, and $aa^{-1} = 1$. So K is a field, and $0_L, 1_L, -a, a^{-1}$ witness its axioms; by the uniqueness of these elements in the field K (Theorem 2.1.1 (a), (c), applied in K), they are its zero, its one, its negatives and its inverses.

- (b) Write $0_K, 1_K$ for the zero and one of the field K . In K , $0_K + 0_K = 0_K$ by (F3); in L , $0_K + 0_L = 0_K$. So $0_K + 0_K = 0_K + 0_L$ in L , and additive cancellation in L (Theorem 2.1.1 (b)) gives $0_K = 0_L$. Next, $1_K \cdot 1_K = 1_K$ by (F7) in K , and $1_K \cdot 1_L = 1_K$ by (F7) in L . Since $1_K \neq 0_K = 0_L$, multiplicative cancellation in L (Theorem 2.1.1 (b)) gives $1_K = 1_L$. Now let $a \in K$, and let $x \in K$ be its negative in K : $a + x = 0_K = 0_L$, so $x = -a$ by the uniqueness of negatives in L (Theorem 2.1.1 (c)). Likewise, if $a \neq 0_K$, that is $a \neq 0_L$, its inverse $y \in K$ satisfies $ay = 1_K = 1_L$, so $y = a^{-1}$ by the uniqueness of inverses in L . Hence $0_L, 1_L \in K$, K is closed under the negatives and inverses of L , and with the hypothesis on sums and products, K is a subfield.
- (c) $(\Rightarrow)$ $1 \in K$ by definition. For $a, b \in K$, $-b \in K$, so $a - b = a + (-b) \in K$, by closure under negatives and sums. For $b \neq 0$, $b^{-1} \in K$, so $ab^{-1} \in K$, by closure under inverses and products.

$(\Leftarrow)$ First, $0 = 1 - 1 \in K$, since $1 + (-1) = 0$ by (F4). For $b \in K$, $-b = 0 + (-b) = 0 - b \in K$, by (F1) and (F3). For non-zero $b \in K$, $b^{-1} = 1 \cdot b^{-1} \in K$, by (F6) and (F7). For $a, b \in K$, $-b \in K$ and $-(-b) = b$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (a)), so $a + b = a - (-b) \in K$. For the product, let $a, b \in K$. If $b = 0$, then $ab = 0 \in K$ by Theorem 2.1.1 (d) and (F6). If $b \neq 0$, then $b^{-1} \in K$, and $b^{-1} \neq 0$, since $bb^{-1} = 1 \neq 0$ while $b \cdot 0 = 0$; so $a(b^{-1})^{-1} \in K$, and $(b^{-1})^{-1} = b$ (Theorem 2.1.1 (g)) gives $ab \in K$. So K contains 0 and 1 and is closed under sums, products, negatives and inverses: it is a subfield. ■

The answer to the prompt. Part (b) uses that L is a field in the step $1_K \cdot 1_K = 1_K \cdot 1_L \Rightarrow 1_K = 1_L$: canceling the factor 1_K means multiplying by its inverse in L , which exists because $1_K \neq 0$ and (F8) holds in L . The additive step uses only negatives, which every commutative ring has. The warning below shows the multiplicative step failing in a ring.

So to show that a subset is a field, we rarely check nine axioms: we check (c), three closure statements, and (a) does the rest.

Warning. A subset of a ring can be a field with **another** one. In the ring $\mathbb{Z}/6\mathbb{Z}$, the subset $\{[0], [3]\}$ is closed under $+$ and $\cdot$: $[3] + [3] = [6] = [0]$ and $[3][3] = [9] = [3]$. With these operations it is a field with two elements, a copy of $\mathbb{F}_2$, but its one is $[3]$, not $[1]$. Part (b) has no counterpart here: $[3][3] = [3][1]$, and $[3]$ cannot be canceled, since $\mathbb{Z}/6\mathbb{Z}$ is not a field.

Likewise, a field structure with **other operations** does not make a subset a subfield: the set $\{0, 1\} \subseteq \mathbb{Q}$ with the tables of $\mathbb{F}_2$ is a field, but it is not a subfield of $\mathbb{Q}$, because the sum of $\mathbb{Q}$ gives $1 + 1 = 2 \notin \{0, 1\}$.

2.3.3 Square roots of two and of minus one

The question of the opening is now one application of the test. Recall that $\mathbb{R}$ is a complete ordered field (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Theorem 5.6.3), so by Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 6.1.4 there is exactly one $r \in \mathbb{R}$ with $r \geq 0$ and

$r^2 = 2$, and $\sqrt{2} := r$. The set $\mathbb{Q}(\sqrt{2})$ is that of Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Definition 6.4.2.

Example. The Field Generated by the Square Root of Two

Show that $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ is a field, namely a subfield of $\mathbb{R}$, and find the inverse of $1 + 2\sqrt{2}$.

Solution. We check the three conditions of Proposition 2.3.1 (c). All computations are in the field $\mathbb{R}$, with $(\sqrt{2})^2 = 2$, and they expand brackets by (F5), (F6), (F9) and Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Proposition 2.3.2 (c).

One. $1 = 1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Differences. For $a, b, c, d \in \mathbb{Q}$, $(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2}$, and $a - c, b - d \in \mathbb{Q}$.

Products, used below. $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$, again in $\mathbb{Q}(\sqrt{2})$.

Inverses. Let $y = c + d\sqrt{2} \neq 0$, with $c, d \in \mathbb{Q}$. First, the **conjugate** $c - d\sqrt{2}$ is not 0. If $d \neq 0$ and $c - d\sqrt{2} = 0$, then $\sqrt{2} = c/d \in \mathbb{Q}$, and $(c/d)^2 = 2$, against Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Theorem 2.6.1. If $d = 0$, then $c - d\sqrt{2} = c = y \neq 0$. Now

$$N := (c + d\sqrt{2})(c - d\sqrt{2}) = c^2 - 2d^2,$$

a rational number, and $N \neq 0$ by Theorem 2.1.1 (f) in $\mathbb{R}$, both factors being non-zero. Put $y' := c/N - (d/N)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Then $yy' = (c + d\sqrt{2})(c - d\sqrt{2})N^{-1} = NN^{-1} = 1$, so $y' = y^{-1}$ by the uniqueness of inverses (Theorem 2.1.1 (c)). Finally, for $x \in \mathbb{Q}(\sqrt{2})$, $xy^{-1} \in \mathbb{Q}(\sqrt{2})$ by the product formula.

By Proposition 2.3.1 (c), $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$, and by (a) it is a field.

The inverse of $1 + 2\sqrt{2}$. Here $c = 1$, $d = 2$ and $N = 1 - 8 = -7$, so

$$(1 + 2\sqrt{2})^{-1} = -\frac{1}{7} + \frac{2}{7}\sqrt{2} = \frac{-1 + 2\sqrt{2}}{7}.$$

Check: $(1 + 2\sqrt{2})(-1 + 2\sqrt{2}) = -1 + 2\sqrt{2} - 2\sqrt{2} + 8 = 7$.

The move “multiply by the conjugate” is the one that inverted complex numbers in Proposition 1.2.3. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 6.4, proved the same facts about $\mathbb{Q}(\sqrt{2})$ as part of an ordered field (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Proposition 6.4.5), and showed that it does not contain a square root of 3 (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Proposition 6.4.6).

Quick check. Is $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ a subfield of $\mathbb{R}$?

Solution. No. It contains $2 = 2 + 0\sqrt{2}$, but not $2^{-1} = 1/2$. If $a + b\sqrt{2} = 1/2$ with $a, b \in \mathbb{Z}$ and $b \neq 0$, then $\sqrt{2} = (1/2 - a)/b$ would be rational, against Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to

$\backslash(\backslash\mathbb{N}\backslash)$, Theorem 2.6.1; and if $b = 0$, then $a = 1/2 \notin \mathbb{Z}$. So it is not closed under inverses. It satisfies the other three clauses, exactly as $\mathbb{Z} \subseteq \mathbb{Q}$ does.

The same test works inside $\mathbb{C}$, where $i^2 = -1$ plays the part of $(\sqrt{2})^2 = 2$, and $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ as above.

Example. Rational and Integer Complex Numbers

Let $\mathbb{Q}(i) := \{a + bi : a, b \in \mathbb{Q}\}$ and $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$, subsets of $\mathbb{C}$.

- (i) Show that $\mathbb{Q}(i)$ is a subfield of $\mathbb{C}$.
- (ii) Show that $\mathbb{Z}[i]$ contains 0 and 1 and is closed under differences and products, but is not a subfield of $\mathbb{C}$.
- (iii) Summarize the subfields of $\mathbb{C}$ met so far.

Solution. Real and imaginary parts are compared as in Definition 1.1.1: $a + bi = c + di$ with $a, b, c, d \in \mathbb{R}$ holds exactly when $a = c$ and $b = d$.

- (i) We use [Proposition 2.3.1 \(c\)](#). $1 = 1 + 0i \in \mathbb{Q}(i)$. Differences: $(a + bi) - (c + di) = (a - c) + (b - d)i$. Products: $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$, from $i^2 = -1$. Inverses: let $y = c + di \neq 0$ with $c, d \in \mathbb{Q}$; then $(c, d) \neq (0, 0)$. The rational number $M := c^2 + d^2$ is positive: $\mathbb{Q}$ is an ordered field (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Theorem 2.5.1), a non-zero square is positive (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.3.5 (e)) and $0^2 = 0 \cdot 0 = 0$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.3.2 (b)), so every square is non-negative, and a sum of a positive and a non-negative element is positive (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.3.5 (b)). So $M \neq 0$. Since $(c + di)(c - di) = c^2 + d^2 = M$, the element $y' := c/M - (d/M)i \in \mathbb{Q}(i)$ satisfies $yy' = MM^{-1} = 1$, so $y^{-1} = y' \in \mathbb{Q}(i)$ (Theorem 2.1.1 (c)), and then $xy^{-1} \in \mathbb{Q}(i)$ for $x \in \mathbb{Q}(i)$ by the product formula. So $\mathbb{Q}(i)$ is a subfield of $\mathbb{C}$.
- (ii) $0 = 0 + 0i$ and $1 = 1 + 0i$ lie in $\mathbb{Z}[i]$, and the difference and product formulas of (i), with integer a, b, c, d , give integer parts. But $2 \in \mathbb{Z}[i]$ has no inverse in $\mathbb{Z}[i]$. Suppose $u = a + bi \in \mathbb{Z}[i]$ had $2u = 1$. Then $u = 2^{-1} = 1/2$ in $\mathbb{C}$, by the uniqueness of inverses (Theorem 2.1.1 (c)) and because the inverse of 2 in $\mathbb{C}$ is the real number $1/2$ (Theorem 1.2.4), so $a + bi = 1/2 + 0i$, and comparing real parts gives $a = 1/2 \notin \mathbb{Z}$. So $\mathbb{Z}[i]$ is not closed under inverses.
- (iii) $\mathbb{Q}, \mathbb{Q}(i), \mathbb{R}$ and $\mathbb{C}$ are subfields of $\mathbb{C}$, and $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$, hence of $\mathbb{C}$:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R} \subseteq \mathbb{C}, \quad \mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{C}.$$

For $\mathbb{R}$ in $\mathbb{C}$ there is a second way to see it: by Proposition 1.1.1 the copy $\iota(\mathbb{R})$ of $\mathbb{R}$ in $\mathbb{C}$ is closed under $+$ and $\cdot$, since $\iota(a) + \iota(c) = \iota(a + c)$ and $\iota(a)\iota(c) = \iota(ac)$. It is a field with these operations. Every element of $\iota(\mathbb{R})$ is $\iota(a)$ for some $a \in \mathbb{R}$, so each identity among the axioms carries over from $\mathbb{R}$ through these two equations; for instance $\iota(a)(\iota(c) + \iota(e)) = \iota(a(c + e)) = \iota(ac + ae) = \iota(a)\iota(c) + \iota(a)\iota(e)$. In the same way $\iota(0)$, $\iota(-a)$, $\iota(1)$ and, for $a \neq 0$, $\iota(a^{-1})$ serve as the zero, the negatives, the one and the inverses; and $\iota(1) \neq \iota(0)$, and $\iota(a) \neq \iota(0)$ exactly when $a \neq 0$, because ι is injective. [Proposition 2.3.1 \(b\)](#) then says that it is a subfield, with the zero and one of $\mathbb{C}$.

2.3.4 The smallest subfield

Subfields can be intersected, and that gives, for any set S of elements, a smallest field containing them.

Proposition 2.3.2. Intersections of Subfields

Let L be a field.

- (a) If $\mathcal{K}$ is a **non-empty** set of subfields of L , then $\bigcap \mathcal{K}$ is a subfield of L .
- (b) For every subset $S \subseteq L$ there is a **smallest** subfield of L containing S : a subfield K_S with $S \subseteq K_S$, contained in every subfield of L that contains S . It is $K_S = \bigcap \mathcal{K}_S$, where $\mathcal{K}_S$ is the set of subfields of L that contain S .

Proof.

- (a) The intersection $\bigcap \mathcal{K} = \{x \in L : x \in K \text{ for every } K \in \mathcal{K}\}$ is defined because $\mathcal{K}$ is a non-empty set of subsets of L (Sets, Relations, and Cardinality, Definition 1.2.4). We check Proposition 2.3.1 (c). Every $K \in \mathcal{K}$ contains 1, so $1 \in \bigcap \mathcal{K}$. If $a, b \in \bigcap \mathcal{K}$, then $a, b \in K$ for every $K \in \mathcal{K}$, so $a - b \in K$ for every $K \in \mathcal{K}$, by (c) applied to K ; hence $a - b \in \bigcap \mathcal{K}$. In the same way, $ab^{-1} \in \bigcap \mathcal{K}$ when $b \neq 0$.
- (b) $\mathcal{K}_S$ is a set, by Separation (Z6) from the power set of L , which exists by (Z5) (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Axiom 1.1.1). It is non-empty, since $L \in \mathcal{K}_S$. By (a), $K_S := \bigcap \mathcal{K}_S$ is a subfield of L . Every $K \in \mathcal{K}_S$ contains S , so $S \subseteq K_S$. And if K is a subfield containing S , then $K \in \mathcal{K}_S$, so $K_S \subseteq K$. Two smallest subfields containing S would each contain the other, so K_S is the only one. ■

The case $S = \emptyset$ asks for no element at all, and gives a subfield contained in every subfield. It has a name.

Definition 2.3.2. Prime Subfield

The **prime subfield** of a field L is the smallest subfield of L , that is, $K_\emptyset$ of Proposition 2.3.2 (b): the intersection of the set of **all** subfields of L .

In words: the prime subfield is what every subfield of L contains. Section 2.5 identifies it in every field, as a copy of $\mathbb{Q}$ or of exactly one $\mathbb{F}_p$. One case can be settled now: the prime subfield of $\mathbb{F}_p$ is $\mathbb{F}_p$ itself, because $\mathbb{F}_p$ has no other subfield. Indeed, let K be a subfield of $\mathbb{F}_p$. It contains 1 and is closed under $+$, so it contains every multiple $k \cdot 1$ with $k \in \mathbb{N}$, the multiples of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Section 2.3 (“Multiples”)*: $0 \cdot 1 = 0 \in K$, and if $k \cdot 1 \in K$, then $(k + 1) \cdot 1 = k \cdot 1 + 1 \in K$, so induction (Logic and Proof, Axiom 4.2.1) covers every k . In $\mathbb{Z}/p\mathbb{Z}$, $k \cdot [1] = [k]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (d)), and every element is $[k]$ for some $k \in \{0, \dots, p - 1\}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (b)). So $K = \mathbb{F}_p$.

The smallest subfield containing a given element is often easy to name. Exercise B2 shows that $\mathbb{Q}(\sqrt{2})$ is the smallest subfield of $\mathbb{R}$ containing $\sqrt{2}$; the reason to expect it is that a subfield containing $\sqrt{2}$ contains 1, hence every rational, and is closed under the sums and products that

build $a + b\sqrt{2}$.

2.3.5 Exercises

2.3.5.1 A. Check your understanding

Exercise. A1

These parts are about [Proposition 2.3.1](#) (b).

- Why must the one of a field $K \subseteq L$, closed under the operations of the field L , be 1_L ? Name the step of the proof.
- Run the proof of (b) on $K = \{[0], [3]\}$ inside the ring $\mathbb{Z}/6\mathbb{Z}$ (the warning). Which steps go through, and which step fails?
- In [Example \(The Field Generated by the Square Root of Two\)](#), is the commutativity (F6) of $\mathbb{Q}(\sqrt{2})$ checked, or inherited? From where?
- State the idea of the subfield test, parts (a) and (b), in two sentences.

Solution.

- In L , $1_K \cdot 1_K = 1_K = 1_K \cdot 1_L$, and $1_K \neq 0_K = 0_L$; multiplicative cancellation in L (Theorem 2.1.1 (b)) removes the factor 1_K and gives $1_K = 1_L$.
- The zero step goes through: $[0]$ is the zero of both, and $[0] + [0] = [0] + [0]$ cancels in any commutative ring. The negative step also goes through ($[3] + [3] = [0]$, so $-[3] = [3]$ in both). The one step fails: $[3][3] = [3] = [3][1]$, but $[3]$ has no inverse in $\mathbb{Z}/6\mathbb{Z}$ ($[3][x] \in \{[0], [3]\}$ for every x), so it cannot be canceled, and indeed $[3] \neq [1]$. The inverse step then has nothing to say.
- Inherited. (F6) holds for all elements of $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.2.3), hence for all elements of the subset $\mathbb{Q}(\sqrt{2})$; [Proposition 2.3.1](#) (a) records this. The solution of the example checks only the three conditions of (c).
- The identities among the field axioms hold for all elements of the big field, hence for the elements of any subset, so only closure and the special elements $0, 1, -a, a^{-1}$ need checking. Conversely, the zero and one of a field sitting inside L with L 's operations are forced, by cancellation in L , to be those of L .

2.3.5.2 B. Practice

Exercise. B1: Putting a proof in order

Here are the lines of the proof of [Proposition 2.3.1](#) (c) ($\Leftarrow$), shuffled, together with two lines that do not belong. Put the correct lines in an admissible order, say which other orders are admissible, and say what is wrong with each of the other two lines.

- Assume $1 \in K$, $a - b \in K$ for all $a, b \in K$, and $ab^{-1} \in K$ for all $a, b \in K$ with $b \neq 0$.
- $0 = 1 - 1 \in K$.
- For $b \in K$, $-b = 0 - b \in K$.
- For non-zero $b \in K$, $b^{-1} = 1 \cdot b^{-1} \in K$.
- For $a, b \in K$, $a + b = a - (-b) \in K$.

(vi) For $a, b \in K$: if $b \neq 0$, then $b^{-1} \in K$ and $b^{-1} \neq 0$ (as $bb^{-1} = 1 \neq 0 = b \cdot 0$), so $ab = a(b^{-1})^{-1} \in K$; if $b = 0$, $ab = 0 \in K$.

(vii) So K is a subfield of L .

The two extra lines: “(ii’) $0 \in K$, since $0 = bb^{-1}$ for any $b \in K$ ”, and “(vi’) $ab \in K$, because K is closed under multiplication”.

Solution. An admissible order is (i), (ii), (iii), (iv), (v), (vi), (vii). The constraints are what each line uses: (i) comes first and (vii) last; (ii) comes before (iii), which uses $0 \in K$, and before (vi), whose case $b = 0$ uses $0 \in K$; (iii) comes before (v), which uses $-b \in K$; (iv) comes before (vi), which uses $b^{-1} \in K$ (line (vi) itself checks $b^{-1} \neq 0$ before applying (i) to it). Any order respecting these is admissible; for instance (i), (ii), (iv), (iii), (vi), (v), (vii).

(ii’) is false: $bb^{-1} = 1$, not 0, and b^{-1} exists only for $b \neq 0$.

(vi’) is circular: closure under products is part of what the proof must establish, so the line cites the goal. This is entry (N9) of Logic and Proof, Example (What is not allowed).

Exercise. B2

Show that $\mathbb{Q}(\sqrt{2})$ is the smallest subfield of $\mathbb{R}$ containing $\sqrt{2}$, in the sense of [Proposition 2.3.2](#) (b).

Solution. Let K be a subfield of $\mathbb{R}$ with $\sqrt{2} \in K$. Since $1 \in K$ and K is closed under $+$, $n \cdot 1 \in K$ for every $n \in \mathbb{N}$, by induction (Logic and Proof, Axiom 4.2.1) as for $\mathbb{F}_p$ above; and in $\mathbb{R}$, $n \cdot 1 = n$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash$ to $\backslash(\backslash\mathbb{R}\backslash$), Theorem 5.4.1 (d), under the identification). Then $-n \in K$ by closure under negatives, so every integer lies in K (every integer is n or $-n$ with $n \in \mathbb{N}$, Number Systems: From $\backslash(\backslash\mathbb{N}\backslash$ to $\backslash(\backslash\mathbb{R}\backslash$), Proposition 2.2.3 (c)). For $m \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$, $n \neq 0$, so $m/n = mn^{-1} \in K$ by closure under inverses and products; and every rational is of this form (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash$ to $\backslash(\backslash\mathbb{R}\backslash$), Proposition 2.4.4 (b)). So $\mathbb{Q} \subseteq K$, and then $a + b\sqrt{2} \in K$ for all $a, b \in \mathbb{Q}$, by closure under sums and products. Hence $\mathbb{Q}(\sqrt{2}) \subseteq K$.

Conversely, $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$ ([Example \(The Field Generated by the Square Root of Two\)](#)) containing $\sqrt{2} = 0 + 1\sqrt{2}$. So it is the smallest such subfield.

Exercise. B3

Inside $\mathbb{C}$ (with $\mathbb{R} \subseteq \mathbb{C}$), show that $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(i) = \mathbb{Q}$.

Solution. ($\supseteq$) A rational a is $a + 0\sqrt{2}$ and $a + 0i$.

($\subseteq$) Let $x = a + b\sqrt{2} = c + di$ with $a, b, c, d \in \mathbb{Q}$. The number $a + b\sqrt{2}$ is real, so its imaginary part is 0; the imaginary part of $c + di$ is d . Comparing parts (Definition 1.1.1), $d = 0$ and $a + b\sqrt{2} = c$. If $b \neq 0$, then $\sqrt{2} = (c - a)/b \in \mathbb{Q}$, against Number Systems: From $\backslash(\backslash\mathbb{N}\backslash$ to $\backslash(\backslash\mathbb{R}\backslash$), Theorem 2.6.1. So $b = 0$, and $x = a \in \mathbb{Q}$.

By [Proposition 2.3.2](#) (a), this also shows again that $\mathbb{Q}$ is a subfield of $\mathbb{C}$.

Exercise. B4

Let $\sqrt{3}$ be the non-negative real number with square 3 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4), and $\mathbb{Q}(\sqrt{3}) := \{a + b\sqrt{3} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$. Show that $\mathbb{Q}(\sqrt{3})$ is a subfield of $\mathbb{R}$, and that $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{3})$. Hence deduce that the union of two subfields need not be a subfield.

Hint: the claim stated with Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.4.6 says which integers are not squares of rationals.

Solution. The claim stated with Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.4.6 says: if $n, k \in \mathbb{N}$ and $k^2 < n < (k+1)^2$, no rational squares to n . We use it for $(n, k) = (3, 1)$ and $(6, 2)$, since $1 < 3 < 4$ and $4 < 6 < 9$.

$\mathbb{Q}(\sqrt{3})$ is a subfield. Exactly as in [Example \(The Field Generated by the Square Root of Two\)](#), with 3 in place of 2: the product is $(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}$; for $y = c + d\sqrt{3} \neq 0$, the conjugate $c - d\sqrt{3}$ is non-zero (if $d \neq 0$, it would make $\sqrt{3} = c/d$ rational, against the claim with $(3, 1)$), $N := c^2 - 3d^2 \neq 0$, and $y^{-1} = c/N - (d/N)\sqrt{3}$.

Not in $\mathbb{Q}(\sqrt{2})$. If $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2})$, then $\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2})$, a square root of 3 in $\mathbb{Q}(\sqrt{2})$, against Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.4.6.

Not in $\mathbb{Q}(\sqrt{3})$. If it were, then $\sqrt{2} = (\sqrt{2} + \sqrt{3}) - \sqrt{3} \in \mathbb{Q}(\sqrt{3})$, say $\sqrt{2} = a + b\sqrt{3}$ with $a, b \in \mathbb{Q}$. Squaring,

$$2 = (a^2 + 3b^2) + 2ab\sqrt{3}, \quad \text{that is,} \quad (a^2 + 3b^2 - 2) + 2ab\sqrt{3} = 0.$$

If $ab \neq 0$, then $\sqrt{3} = (2 - a^2 - 3b^2)/(2ab) \in \mathbb{Q}$, against the claim with $(3, 1)$. So $ab = 0$, and then $a^2 + 3b^2 = 2$. If $b = 0$, then $a^2 = 2$, against Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1. If $a = 0$, then $3b^2 = 2$, so $(3b)^2 = 6$, against the claim with $(6, 2)$.

The union. $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and $\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, but their sum is in neither. So $\mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{3})$ is not closed under sums, and is not a subfield of $\mathbb{R}$, although both pieces are.

2.3.5.3 C. Going deeper

Exercise. C1: A finite subset closed under the operations

Let L be a field and $K \subseteq L$ a **finite** subset with $1 \in K$, closed under $+$ and $\cdot$. Show that $0 \in K$, that K is closed under negatives and under inverses of non-zero elements, and hence that K is a subfield of L . Then show that the hypothesis “finite” cannot be dropped.

Solution (Hint 1). For $b \in K$, which maps $K \rightarrow K$ can you build from b and the two operations?

Solution (Hint 2). The maps $x \mapsto x + b$ and $x \mapsto bx$ go from K to K . Why are they injective, and what does finiteness then give?

Solution. A finite set has no injection onto a proper part. Let $f: K \rightarrow K$ be injective. If f were not surjective, its image $f(K)$ (Sets, Relations, and Cardinality, Definition 1.6.1) would be a proper subset of K , and f , with codomain $f(K)$, would be a bijection $K \rightarrow f(K)$, against Sets, Relations, and Cardinality, Theorem 3.1.9. So every injective map $K \rightarrow K$ is surjective.

Zero. Let $t: K \rightarrow K$, $t(x) := x + 1$, a map into K because K is closed under $+$ and $1 \in K$. It is injective: $x + 1 = x' + 1$ gives $1 + x = 1 + x'$ by (F1), so $x = x'$ by additive cancellation in L (Theorem 2.1.1 (b)). So it is surjective, and some $x \in K$ has $x + 1 = 1 = 0 + 1$, so $1 + x = 1 + 0$ by (F1); canceling, $x = 0$. So $0 \in K$.

Negatives. Let $b \in K$. The map $x \mapsto x + b$ is injective in the same way, hence surjective, and $0 \in K$ is a value: $x + b = 0$ for some $x \in K$. By the uniqueness of negatives in L , $x = -b$.

Inverses. Let $b \in K$, $b \neq 0$. The map $x \mapsto bx$ goes from K to K and is injective by multiplicative cancellation in L , which uses $b \neq 0$. So it is surjective, $bx = 1$ for some $x \in K$, and $x = b^{-1}$ by the uniqueness of inverses in L .

So K is a subfield. Note that $K \neq \emptyset$ need not be assumed: $1 \in K$.

Finiteness is needed. $\mathbb{N} \subseteq \mathbb{Q}$ contains 1 and is closed under $+$ and $\cdot$, and $-1 \notin \mathbb{N}$. The argument breaks at “injective, hence surjective”: $x \mapsto x + 1$ is injective on $\mathbb{N}$, and 0 is not a value.

Marking scheme. (10 points) - 2: a finiteness argument with its reason: an injective map from a finite set to itself is surjective (Sets, Relations, and Cardinality, Theorem 3.1.9, or a count), or pigeonhole on a sequence in K (Sets, Relations, and Cardinality, Theorem 3.1.2). - 2: $0 \in K$, from a translation map and cancellation, or from a repetition $m \cdot 1 = n \cdot 1$ with $m < n$ and cancellation in L , **before** 0 is used. - 2: negatives, from surjectivity of $x \mapsto x + b$ and uniqueness of negatives in L , or from a repetition $i \cdot b = j \cdot b$ with $i < j$, giving $-b = (j - i - 1) \cdot b$. - 2: inverses, with the cancellation by b justified by $b \neq 0$ (injectivity of $x \mapsto bx$, or $b^i = b^j$ with $i < j$ giving $b^{j-i} = 1$ and $b^{-1} = b^{j-i-1}$). - 2: a witness that finiteness is needed ($\mathbb{N} \subseteq \mathbb{Q}$, or $\mathbb{Z} \subseteq \mathbb{Q}$ for inverses). Fatal errors (0 for the step): using $0 \in K$ or $-b \in K$ to build the translation before proving it; “injective, hence surjective” (or pigeonhole) without finiteness.

Exercise. C2: Find the error

Here is an argument. Is its conclusion true? Does the argument prove it? If not, name the line that fails and why.

“ $\mathbb{Q}(\sqrt{2})$ is closed under inverses. (1) Let $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ be non-zero. (2) Then

$$(a + b\sqrt{2})^{-1} = \frac{1}{a} + \frac{1}{b\sqrt{2}} = \frac{1}{a} + \frac{1}{2b}\sqrt{2}.$$

(3) Both coefficients are rational, so the inverse lies in $\mathbb{Q}(\sqrt{2})$.”

Solution. The conclusion is **true** (Example (The Field Generated by the Square Root of Two)). The argument does not prove it.

Line (2) fails. Its first equality uses the general “fact” $1/(x+y) = 1/x + 1/y$, which is neither proved nor true; so the line cites nothing, entry (N9) of Logic and Proof, Example (What is not allowed). It also divides by a and by b , either of which may be 0 (for $\sqrt{2} = 0 + 1\sqrt{2}$, $a = 0$). The second equality, $1/(b\sqrt{2}) = (1/(2b))\sqrt{2}$, is correct for $b \neq 0$.

Counterexample to the step. $x = y = 1$ in $\mathbb{Q}$: $1/(1+1) = 1/2$, while $1/1 + 1/1 = 2$. In the case at hand, $a = b = 1$: the formula gives $1 + \frac{1}{2}\sqrt{2}$, and $(1 + \sqrt{2})(1 + \frac{1}{2}\sqrt{2}) = 2 + \frac{3}{2}\sqrt{2} \neq 1$; the true inverse is $-1 + \sqrt{2}$.

Repair. Multiply by the conjugate, as in Example (The Field Generated by the Square Root of Two): $(a + b\sqrt{2})^{-1} = (a - b\sqrt{2})/(a^2 - 2b^2)$.