

2.6 The Gaps in the Rationals

The rationals now have everything Section 2.5 asked of them: they form an ordered field (Theorem 2.5.1), every rational lies below a natural number (Theorem 2.5.3), and no two rationals are neighbors, since their midpoint lies between them. Is anything missing? School geometry suggests an answer. The diagonal of a square with side 1 has a length whose square is 2, and no fraction seems to measure it. That picture is motivation only. This section proves the two facts behind it from the construction: no rational squares to 2, and the set of rationals whose square is below 2 has no least upper bound in $\mathbb{Q}$. We also build a sequence of rationals that closes in on the gap from above without ever landing in it. A later chapter of this volume fills the gap.

2.6.1 No rational squares to two

Throughout, $x^2 := x \cdot x$ and $2 := 1 + 1$, with $4 = 2 \cdot 2$ and so on; by the identifications of Sections 2.2 and 2.4 these are the natural numbers of the same names. Their sums and products may be computed in $\mathbb{N}$, since the maps ι and j preserve $+$ and $\cdot$ (Proposition 2.2.3, Proposition 2.4.4), and so may their comparisons (Theorem 2.3.4 (a), Theorem 2.5.1 (b)).

Logic and Proof, Chapter 2 proved that “ $\sqrt{2}$ is irrational” (Logic and Proof, Theorem 2.2.1), about the school rationals, by parity: an argument about even and odd integers. Parity is available here too, from Proposition 1.6.4 (d) for positive integers or from the integer part (Proposition 2.5.5; see Exercise R4). We prove the statement for the constructed $\mathbb{Q}$ by a different route, one that needs only the order and the least-element property of $\mathbb{Z}$, and that adapts to other non-squares (Exercise C2).

Theorem 2.6.1. No Rational Squares to Two

There is no $x \in \mathbb{Q}$ with $x^2 = 2$.

Idea. Work backwards from a supposed square root $x = p/q$. From $x^2 = 2$ we get $2 - x = x^2 - x = x(x - 1)$, so

$$x = \frac{2 - x}{x - 1} = \frac{2 - p/q}{p/q - 1} = \frac{2q - p}{p - q}.$$

Since $1 < x < 2$ (as $1^2 < 2 < 2^2$), the new denominator $p - q$ is positive and smaller than q . So no fraction for x can have a **least** positive denominator, while Proposition 2.3.6 says some fraction must. The written proof checks the descent with integers only: it never divides, and it verifies $(2q - p)^2 = 2(p - q)^2$ by expanding. *Before reading on: using only integers, why is the new denominator $q' := p - q$ positive, and why is $q' < q$?*

Proof. Suppose, for a contradiction, that $x \in \mathbb{Q}$ and $x^2 = 2$. Then $x \neq 0$, since $0^2 = 0$ (Proposition 2.3.2 (b)) and $2 > 0$. By (O1), $x > 0$ or $x < 0$; let $y := x$ in the first case and $y := -x$ in the second. Then $y > 0$ (Proposition 2.3.5 (a)) and $y^2 = x^2 = 2$, because $(-x)(-x) = xx$ (Proposition 2.3.2 (c)).

By Proposition 2.4.4 (b), $y = a/b$ with $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{>0}$, and $a > 0$ by Theorem 2.5.1 (a). By Definition 2.4.2, $y^2 = a^2/b^2$, and $2 = 2/1$, so $y^2 = 2$ says $a^2 \cdot 1 = 2b^2$ (Proposition 2.4.4 (b)). Hence the set

$$D := \{q \in \mathbb{Z}_{>0} : p^2 = 2q^2 \text{ for some } p \in \mathbb{Z}_{>0}\}$$

contains b , so it is non-empty, and 0 is a lower bound of it. By Proposition 2.3.6, D has a least element q . Choose $p \in \mathbb{Z}_{>0}$ with $p^2 = 2q^2$.

$q < p$. Suppose $p \leq q$. Since $p, q \geq 0$, Proposition 2.3.5 (g) gives $p^2 < q^2$ if $p < q$, and $p^2 = q^2$ if $p = q$; so $p^2 \leq q^2$, that is, $q^2 + q^2 \leq q^2$, and adding $-q^2$ (O3) gives $q^2 \leq 0$. But $q \neq 0$, so $q^2 > 0$ by Proposition 2.3.5 (e). This contradicts (O1), so $p \leq q$ fails, and $q < p$ by totality (Proposition 2.3.5 (i)).

$p < 2q$. Suppose $2q \leq p$. Since $2q, p \geq 0$, (g) (or equality, if $2q = p$) gives $(2q)^2 \leq p^2$, that is, $2q^2 + 2q^2 = 4q^2 \leq p^2$, so $2q^2 \leq 0$. But $2q^2 > 0$ by (O4). As before, $p < 2q$.

Descent. Let $p' := 2q - p$ and $q' := p - q$, integers. By Proposition 2.3.5 (a), $p < 2q$ gives $p' > 0$, and $q < p$ gives $q' > 0$; so $p', q' \in \mathbb{Z}_{>0}$ (Theorem 2.3.4 (b)). Adding $-q$ to $p < 2q$ (O3) gives $q' = p - q < q$. Expanding with Proposition 2.3.2 (c) and (d),

$$\begin{aligned} p'^2 - 2q'^2 &= (4q^2 - 4pq + p^2) - (2p^2 - 4pq + 2q^2) \\ &= 2q^2 - p^2 = 0. \end{aligned}$$

So $p'^2 = 2q'^2$ with $p' \in \mathbb{Z}_{>0}$, that is, $q' \in D$. But $q' < q$, and q is the least element of D . This contradiction shows that no $x \in \mathbb{Q}$ has $x^2 = 2$. ■

The answer to the prompt: $q' = p - q > 0$ because $q < p$, and $q' < q$ because $p < 2q$. These are the two inequalities “ $1 < x < 2$ ” of the Idea, written for integers. The hypothesis $p^2 = 2q^2$ is used in each of the three steps, and the minimality of q only once, in the final contradiction.

Remark. The proof assumes $x^2 = 2$, reaches a contradiction, and concludes $\neg(\exists x \in \mathbb{Q} x^2 = 2)$: its last step is $\neg I$ (Logic and Proof, Definition 2.2.1), not RAA (Logic and Proof, Definition 2.5.1), since what is refuted is the assumption and the conclusion is its negation. The steps “ $q < p$ ” and “ $p < 2q$ ” refute $p \leq q$ and $2q \leq p$ and then read the remaining case off trichotomy.

2.6.2 The set below the gap

Sets, Relations, and Cardinality, Section 2.6 stated, without proof, that the set of positive rationals with square below 2 has no least upper bound in $\mathbb{Q}$, and pointed out that the ambient set decides whether a supremum exists. We now prove it. By Proposition 2.3.5 (i) and Theorem 2.5.1, $\leq$ is a total order on $\mathbb{Q}$, so $(\mathbb{Q}, \leq)$ is a partially ordered set and the words of *Sets, Relations, and Cardinality*, Section 2.6 apply: upper bounds (Sets, Relations, and Cardinality, Definition 2.6.2) and a supremum, an upper bound s with (S1) $x \leq s$ for every x in the set and (S2) $s \leq u$ for every upper bound u (Sets, Relations, and Cardinality, Definition 2.6.5).

Theorem 2.6.2. A Bounded Set of Rationals with No Rational Supremum

Let

$$A := \{x \in \mathbb{Q} : x^2 < 2\}, \quad A^+ := \{x \in A : x > 0\} = \{x \in \mathbb{Q} : x > 0, x^2 < 2\}.$$

- (a) A is non-empty and bounded above in $(\mathbb{Q}, \leq)$, but A has no supremum in $\mathbb{Q}$.

- (b) A and A^+ have the same upper bounds in $\mathbb{Q}$. Hence A^+ is also non-empty and bounded above, and has no supremum in $\mathbb{Q}$.

Try it first (ten minutes): a rational $s > 0$ is offered as $\sup A$. Find a rational that proves the offer wrong, once in the case $s^2 < 2$ and once in the case $s^2 > 2$.

Idea. If $s^2 < 2$, we need an element of A above s . The obvious try is $s + h$ with $h > 0$ small, but $(s + h)^2 = s^2 + 2sh + h^2$ has an h^2 in it, and taming that needs a separate size estimate on h . If $s^2 > 2$, we need a smaller upper bound, and a guess $s - h$ runs into the same algebra.

A cleaner idea finds the new rational in one formula. If $s^2 > 2$, then $2/s < s$ and $(2/s)^2 = 4/s^2 < 2$: the gap lies between $2/s$ and s . Their average

$$t(s) := \frac{1}{2} \left(s + \frac{2}{s} \right) = \frac{s^2 + 2}{2s}$$

is smaller than s , and its square is still above 2; that is the smaller upper bound. If $s^2 < 2$, apply the same trick from the other side: $t(s)$ overshoots, so $u(s) := 2/t(s) = 4s/(s^2 + 2)$ undershoots, and it lands above s . Each claim is an identity in the field $\mathbb{Q}$, checked by clearing denominators. The proof uses [Theorem 2.6.1](#) exactly once, to rule out the third case $s^2 = 2$.

Proof.

- (a) *Non-empty:* $1^2 = 1 < 2$, so $1 \in A$. *Bounded above:* 2 is an upper bound. Indeed, let $x \in A$, and suppose $x > 2$. Then $0 \leq 2 < x$, so $4 = 2^2 < x^2$ by Proposition 2.3.5 (g), and $2 < 4$, so $2 < x^2$, against $x^2 < 2$ by (O1). So $x \leq 2$, by totality. *Two maps.* For $s \in \mathbb{Q}_{>0}$, we have $2s > 0$ by (O4), and $s^2 + 2 > 0$ by Proposition 2.3.5 (e) and (b); both are non-zero. Let

$$t(s) := \frac{s^2 + 2}{2s}, \quad u(s) := \frac{4s}{s^2 + 2}.$$

Both are rationals, and both are positive, by Proposition 2.5.2 (a) and (O4). They satisfy

$$\begin{aligned} t(s)^2 - 2 &= \frac{(s^2 - 2)^2}{4s^2}, & s - t(s) &= \frac{s^2 - 2}{2s}, \\ u(s) - s &= \frac{s(2 - s^2)}{s^2 + 2}, & 2 - u(s)^2 &= \frac{2(s^2 - 2)^2}{(s^2 + 2)^2}. \end{aligned} \tag{2.6.1}$$

Each identity is checked by multiplying both sides by its denominator, which is non-zero, so that the multiplication can be undone with the inverse. For the first, $2s \cdot t(s) = s^2 + 2$, so $4s^2(t(s)^2 - 2) = (s^2 + 2)^2 - 8s^2 = s^4 - 4s^2 + 4 = (s^2 - 2)^2$. For the second, $2s(s - t(s)) = 2s^2 - (s^2 + 2) = s^2 - 2$. For the third, $(s^2 + 2)(u(s) - s) = 4s - s^3 - 2s = s(2 - s^2)$. For the fourth, $(s^2 + 2)^2(2 - u(s)^2) = 2(s^2 + 2)^2 - 16s^2 = 2(s^2 - 2)^2$.

No supremum. Suppose, for a contradiction, that $s \in \mathbb{Q}$ is a supremum of A . By (S1) and $1 \in A$, $s \geq 1 > 0$, so $s \in \mathbb{Q}_{>0}$. By [Theorem 2.6.1](#), $s^2 \neq 2$, so by (O1), $s^2 < 2$ or $s^2 > 2$. In both cases $s^2 - 2 \neq 0$, so $(s^2 - 2)^2 > 0$ by Proposition 2.3.5 (e).

Case 1: $s^2 < 2$. Then $2 - s^2 > 0$, and the third identity of [Eq. 2.6.1](#) exhibits $u(s) - s$ as a product of positive elements (with Proposition 2.5.2 (a) for the reciprocal), so

$u(s) > s$. The fourth gives $2 - u(s)^2 > 0$, so $u(s)^2 < 2$ and $u(s) \in A$. So A has an element $u(s) > s$, and s is not an upper bound of A , against (S1).

Case 2: $s^2 > 2$. The first identity gives $t(s)^2 - 2 > 0$, so $t(s)^2 > 2$. Then $t(s)$ is an upper bound of A : if some $x \in A$ had $x > t(s)$, then $0 < t(s) < x$ would give $2 < t(s)^2 < x^2$ by Proposition 2.3.5 (g), against $x^2 < 2$; so $x \leq t(s)$ for every $x \in A$. By (S2), $s \leq t(s)$. But the second identity, with $s^2 - 2 > 0$ and $2s > 0$, gives $s - t(s) > 0$, that is, $t(s) < s$. Then $t(s) < s \leq t(s)$, so $t(s) < t(s)$, against (O1).

Both cases are impossible, so A has no supremum in $\mathbb{Q}$.

- (b) Since $A^+ \subseteq A$, every upper bound of A is an upper bound of A^+ . Conversely, let u be an upper bound of A^+ . Since $1 > 0$ and $1^2 < 2$, $1 \in A^+$, so $u \geq 1 > 0$. Let $x \in A$. If $x > 0$, then $x \in A^+$ and $x \leq u$. Otherwise $x \leq 0 < u$ (Proposition 2.3.5 (i)). So u is an upper bound of A .

Conditions (S1) and (S2) for a set mention only the set of its upper bounds: (S1) says that s is one, and (S2) that it lies below all of them. So s is a supremum of A^+ if and only if it is a supremum of A , and by (a), A^+ has none. It is non-empty, since $1 \in A^+$, and bounded above, by 2.

■

The set A^+ is the set of *Sets, Relations, and Cardinality*, Section 2.6, so clause (b) is the statement left unproved there. The two descriptions differ only by the non-positive elements of A , which lie below every upper bound anyway.

Remark. Analysis on the Real Line, Chapter 1 proves the same conclusion for A^+ in $\mathbb{Q}$, as part of its motivation for the axioms of the real numbers, and then shows that A^+ does have a supremum in the real numbers. That is the sense of “gap”: a bounded set of rationals whose least upper bound, if it is anywhere, is not a rational.

Warning. “ A has no supremum in $\mathbb{Q}$, so A is unbounded” mixes up the two conditions a supremum needs. A is bounded above, by 2 for instance; what fails is (S2): among the rational upper bounds there is no least one, because every upper bound s is beaten by the smaller upper bound $t(s)$.

2.6.3 A rational sequence aimed at the gap

The map t does more than refute a candidate. Started at an upper bound, it produces a smaller one, and it can be applied again. Iterating it gives a sequence of rationals that approaches the gap from above.

Example. A Rational Sequence Aimed at the Gap

For $s \in \mathbb{Q}_{>0}$ let $t(s) := (s^2 + 2)/(2s)$. Define $x_0 := 2$ and $x_{n+1} := t(x_n)$ for $n \in \mathbb{N}$, and let $e_n := x_n^2 - 2$. Show that this defines a sequence with $x_n \in \mathbb{Q}_{>0}$ for every $n \in \mathbb{N}$, and that for every $n \in \mathbb{N}$:

- (i) $e_n > 0$, that is, $x_n^2 > 2$;

- (ii) $e_{n+1} = e_n^2/(4x_n^2) \leq e_n^2/8$;
 (iii) $x_n - x_{n+1} = e_n/(2x_n) > 0$, so $x_{n+1} < x_n$.

Compute $x_0, \dots, x_3$ and $e_0, \dots, e_3$.

Solution. The sequence. For $s \in \mathbb{Q}_{>0}$, $s^2 + 2 > 0$ and $2s > 0$, so $t(s) \in \mathbb{Q}_{>0}$ by (O4) and Proposition 2.5.2 (a): t maps $\mathbb{Q}_{>0}$ to $\mathbb{Q}_{>0}$. The recursion theorem (Sets, Relations, and Cardinality, Theorem 2.3.1, read on $\mathbb{N} = \omega$ as Theorem 1.5.1 by Corollary 1.7.3 (b)), with $X = \mathbb{Q}_{>0}$, starting value 2 and $g(n, s) := t(s)$, gives exactly one function $n \mapsto x_n$ from $\mathbb{N}$ to $\mathbb{Q}_{>0}$ with $x_0 = 2$ and $x_{n+1} = t(x_n)$. So every x_n is a positive rational, with no further argument.

Two identities. For $s \in \mathbb{Q}_{>0}$, $2s \cdot t(s) = s^2 + 2$. Hence $4s^2(t(s)^2 - 2) = (s^2 + 2)^2 - 8s^2 = (s^2 - 2)^2$ and $2s(s - t(s)) = 2s^2 - s^2 - 2 = s^2 - 2$. Multiplying by the inverses of $4s^2 \neq 0$ and $2s \neq 0$,

$$t(s)^2 - 2 = \frac{(s^2 - 2)^2}{4s^2}, \quad s - t(s) = \frac{s^2 - 2}{2s}. \quad (2.6.2)$$

(i). We use Logic and Proof, Axiom 4.2.1 (read on ω as Theorem 1.3.3 (b), by Corollary 1.7.3 (b)) for $P(n)$: $e_n > 0$. Base $P(0)$: $e_0 = 2^2 - 2 = 2 > 0$. Step: suppose $e_n > 0$. By Eq. 2.6.2 with $s = x_n$,

$$e_{n+1} = t(x_n)^2 - 2 = \frac{e_n^2}{4x_n^2}.$$

Here $e_n^2 > 0$ by Proposition 2.3.5 (e), since $e_n \neq 0$, and $1/(4x_n^2) > 0$ by Proposition 2.5.2 (a); so $e_{n+1} > 0$ by (O4). This proves (i) for every n .

(ii). The equation was just shown, for every n . By (i), $x_n^2 > 2$, so $4x_n^2 > 4 \cdot 2 = 8$ by Proposition 2.3.5 (c). From $0 < 8 < 4x_n^2$, Proposition 2.5.2 (b) gives $1/(4x_n^2) < 1/8$, and multiplying by $e_n^2 > 0$ (Proposition 2.3.5 (c)) gives $e_{n+1} < e_n^2/8$; in particular $e_{n+1} \leq e_n^2/8$.

(iii). By Eq. 2.6.2 with $s = x_n$, $x_n - x_{n+1} = e_n/(2x_n)$, a product of the positive elements e_n and $1/(2x_n)$; so it is positive, and $x_{n+1} < x_n$ by Proposition 2.3.5 (a).

The first terms. By the definition of t ,

$$x_1 = \frac{4+2}{4} = \frac{3}{2}, \quad x_2 = \frac{9/4+2}{3} = \frac{17}{12}, \quad x_3 = \frac{289/144+2}{17/6} = \frac{577}{408}.$$

The errors are $e_0 = 2$, $e_1 = 9/4 - 2 = 1/4$, $e_2 = 289/144 - 2 = 1/144$ and $e_3 = 577^2/408^2 - 2 = 1/166464$, since $577^2 = 332929 = 2 \cdot 166464 + 1$ and $408^2 = 166464$. As a check on (ii): $e_1 = 2^2/(4 \cdot 4) = 1/4$, $e_2 = (1/16)/9 = 1/144$, and $e_3 = (1/144)^2/(4 \cdot 289/144) = 1/(144 \cdot 1156) = 1/166464$.

For orientation only (decimals are not part of this volume's toolkit), here are the terms in school decimals:

n	x_n	$e_n = x_n^2 - 2$	x_n , roughly
0	2	2	2
1	3/2	1/4	1.5
2	17/12	1/144	1.41667

n	x_n	$e_n = x_n^2 - 2$	x_n , roughly
3	577/408	1/166464	1.414216

The terms decrease, every one of them is an upper bound of A (a positive rational whose square exceeds 2, as in Case 2 of the proof above), and by (ii) the error is roughly squared at each step: after three steps, $e_3 = 1/166464$ is already below $1/100000$. The terms crowd together. Yet no rational L can be “the number they approach”, for if they approached L , their squares would approach L^2 , and the errors e_n force $L^2 = 2$, which [Theorem 2.6.1](#) forbids. This paragraph is a picture, not a proof: limits in $\mathbb{Q}$ have not been defined. A later chapter of this volume defines them, with $\varepsilon \in \mathbb{Q}_{>0}$, and proves that this sequence is Cauchy in $\mathbb{Q}$ yet has no limit in $\mathbb{Q}$, citing (i)–(iii) from this example.

Quick check. Is $3/2$ an upper bound of $A = \{x \in \mathbb{Q} : x^2 < 2\}$? Is $17/12$? Is $4/3$?

Solution. The first two are. Each is positive, and $(3/2)^2 = 9/4 > 2$ because $9 > 8$, while $(17/12)^2 = 289/144 > 2$ because $289 > 288$ (the comparison formula, [Theorem 2.5.1 \(a\)](#)). A positive rational b with $b^2 > 2$ bounds A : if $x \in A$ had $x > b$, then $x^2 > b^2 > 2$ by [Proposition 2.3.5 \(g\)](#), against $x^2 < 2$. (These are x_1 and x_2 of [Example \(A Rational Sequence Aimed at the Gap\)](#), and $17/12 = t(3/2)$ is the smaller upper bound that Case 2 of the proof of [Theorem 2.6.2](#) produces from $s = 3/2$.)

But $4/3$ is not, although it is positive: $(4/3)^2 = 16/9 < 2$ because $16 < 18$, so the hypothesis $b^2 > 2$ fails, and indeed $7/5 \in A$, as $(7/5)^2 = 49/25 < 2$ ($49 < 50$), while $7/5 > 4/3$ ($21 > 20$).

This chapter built two number systems by one method. From $\mathbb{N}$ to $\mathbb{Z}$: pairs (a, b) , identified when $a + d = b + c$, so that subtraction becomes possible. From $\mathbb{Z}$ to $\mathbb{Q}$: pairs (p, q) with $q > 0$, identified when $ps = rq$, so that division becomes possible. Each time an operation was defined on representatives and checked to be well defined ([Theorem 2.2.1](#)), and each axiom was reduced to the level below. The third step, from $\mathbb{Q}$ to the real numbers, takes the same route in a later chapter of this volume: the representatives are sequences of rationals like the one above, identified when their difference tends to 0, so that the gap found in this section, and every other gap of $\mathbb{Q}$, is filled.

2.6.4 Exercises

2.6.4.1 A. Check your understanding

Exercise. A1

These questions are about the proof of [Theorem 2.6.2](#).

- Where is [Theorem 2.6.1](#) used, and what would go wrong without it?
- Run the proof on $s = 3/2$ and on $s = 7/5$: which case applies, which rational does the proof produce, and why does it refute s ?
- Let F be an ordered field containing an element $r > 0$ with $r^2 = 2$, and let $A_F := \{x \in$

- $F : x^2 < 2\}$. Which step of the proof fails for A_F , and what happens to $t(r)$ and $u(r)$?
- (d) State the idea of the proof in two sentences.

Solution.

- (a) Once, right after a supposed supremum s is fixed: it excludes $s^2 = 2$, so that trichotomy leaves the two cases $s^2 < 2$ and $s^2 > 2$. Without it there is a third case, in which neither map helps: $(s^2 - 2)^2 = 0$, so the identities give $u(s) = s$ and $t(s) = s$.
- (b) For $s = 3/2$: $s^2 = 9/4 > 2$ (as $9 > 8$), so Case 2. The proof produces $t(3/2) = (9/4 + 2)/3 = 17/12$, an upper bound of A , since $(17/12)^2 = 289/144 > 2$; and $17/12 < 3/2$, since $17 \cdot 2 = 34 < 36 = 3 \cdot 12$. So $3/2$ is not the **least** upper bound. For $s = 7/5$: $s^2 = 49/25 < 2$ (as $49 < 50$), so Case 1. The proof produces

$$u(7/5) = \frac{28/5}{49/25 + 2} = \frac{28/5}{99/25} = \frac{140}{99},$$

which lies in A , since $140^2 = 19600 < 19602 = 2 \cdot 99^2$, and exceeds $7/5$, since $140 \cdot 5 = 700 > 693 = 7 \cdot 99$. So $7/5$ is not an upper bound.

- (c) The step “ $s^2 \neq 2$ ”: in F the candidate $s = r$ satisfies $r^2 = 2$, and it falls in neither case. Indeed r is the supremum of A_F in F : it is an upper bound (if $x > r > 0$, then $x^2 > 2$), and an upper bound $v < r$ would have $v > 0$ (as $1 \in A_F$) and $v^2 < 2$, and then $u(v) \in A_F$ with $u(v) > v$, as in Case 1. The maps fix r : $t(r) = (2 + 2)/(2r) = 2/r = r$, since $r \cdot r = 2$, and $u(r) = 4r/4 = r$.
- (d) Suppose a rational s were the supremum; since no rational squares to 2, either $s^2 < 2$ or $s^2 > 2$. The explicit rationals $u(s)$ and $t(s)$ then give, respectively, an element of the set above s or an upper bound below s , so s fails (S1) or (S2).

2.6.4.2 B. Practice

Exercise. B1: Put the proof in order

Here are lines of a proof of [Theorem 2.6.1](#), shuffled, together with two lines that do not belong. Write the lines of a correct proof in a correct order, and say what is wrong with each line you leave out.

- (i) Set $p' := 2q - p$ and $q' := p - q$; both are positive integers, by the two inequalities between p and q .
- (ii) Write $x = a/b$ with $a, b \in \mathbb{Z}_{>0}$; then $a^2 = 2b^2$.
- (iii) Since $p^2 = 2q^2$, we have $p < q$.
- (iv) Since $q' = p - q < q$, this contradicts the choice of q ; so no rational squares to 2.
- (v) Suppose $x \in \mathbb{Q}$ has $x^2 = 2$; replacing x by $-x$ if necessary, take $x > 0$.
- (vi) $p < 2q$, since $p \geq 2q$ would give $p^2 \geq 4q^2 > 2q^2$.
- (vii) Choose such an x with the least positive value.
- (viii) Among all pairs (p, q) of positive integers with $p^2 = 2q^2$, choose one with q least (Proposition 2.3.6; b is such a q).
- (ix) Expanding, $p'^2 - 2q'^2 = 2q^2 - p^2 = 0$, so $p'^2 = 2q'^2$.
- (x) $q < p$, since $p \leq q$ would give $2q^2 = p^2 \leq q^2$, that is, $q^2 \leq 0$.

Solution. An admissible order is

$$(v), (ii), (viii), (x), (vi), (i), (ix), (iv).$$

Lines (x) and (vi) may be exchanged, since neither uses the other. Otherwise the order is forced by what each line uses: (ii) needs the $x > 0$ of (v); (viii) needs the pair (a, b) of (ii), which makes the set of such q non-empty; (x) and (vi) are about the pair fixed in (viii), and if they came before it, the pair might change afterwards; (i) needs both inequalities; (ix) needs the definitions in (i); and (iv) needs $q' \in \mathbb{Z}_{>0}$ with $p'^2 = 2q'^2$, from (i) and (ix), and $q' < q$, which comes from (vi).

Line (vii) is legal but does no work. There is only one positive rational x with $x^2 = 2$: if $0 < x < y$ had $x^2 = y^2 = 2$, then Proposition 2.3.5 (g) would give $2 = x^2 < y^2 = 2$, against (O1). So “the least” just picks out the x of (v) and gives nothing new. The descent does not produce a smaller x : it keeps the number and shrinks its denominator, $p'/q' = p/q$, so choosing x least never leads to a contradiction. What must be least is the denominator q , as in (viii).

Line (iii) fails. Its conclusion is false: from $p^2 = 2q^2$ and $q > 0$ we get $p^2 > q^2$, hence $q < p$ by Proposition 2.3.5 (g), the opposite of (iii). It also clashes with (x).

Exercise. B2

Let $A := \{x \in \mathbb{Q} : x^2 < 2\}$ and $A^+ := \{x \in \mathbb{Q} : x > 0, x^2 < 2\}$. Without looking back, prove that A and A^+ have the same upper bounds in $\mathbb{Q}$, and deduce from Theorem 2.6.2 (a) that A^+ has no supremum in $\mathbb{Q}$.

Solution. ($\subseteq$) for upper bounds: if u bounds A , it bounds the subset $A^+ \subseteq A$. Conversely, let u bound A^+ . Since $1 > 0$ and $1^2 = 1 < 2$, $1 \in A^+$, so $1 \leq u$ and $u > 0$. Let $x \in A$. If $x > 0$, then $x \in A^+$, so $x \leq u$. If $x \leq 0$, then $x \leq 0 < u$. So u bounds A .

Now suppose s were a supremum of A^+ . Then s is an upper bound of A^+ , hence of A (S1), and $s \leq u$ for every upper bound u of A^+ , which are exactly the upper bounds of A (S2). So s would be a supremum of A , which Theorem 2.6.2 (a) excludes. Hence A^+ has no supremum in $\mathbb{Q}$.

Exercise. B3

Compute x_4 of Example (A Rational Sequence Aimed at the Gap), as a fraction of integers, and $e_4 = x_4^2 - 2$. Check your value of e_4 against (ii) of the example. Hence x_4 is an upper bound of $\{x \in \mathbb{Q} : x^2 < 2\}$ below x_3 .

Solution. With $x_3 = 577/408$,

$$x_4 = t(x_3) = \frac{577^2 + 2 \cdot 408^2}{2 \cdot 577 \cdot 408} = \frac{332929 + 332928}{470832} = \frac{665857}{470832}.$$

Then $665857^2 = 443365544449$ and $470832^2 = 221682772224$, and $443365544449 - 2 \cdot$

221682772224 = 1, so

$$e_4 = \frac{1}{221682772224}.$$

By (ii), $e_4 = e_3^2/(4x_3^2) = 1/(166464 \cdot 4 \cdot 332929)$, and $4 \cdot 166464 \cdot 332929 = 221682772224$, which agrees. Since $x_4 > 0$ and $e_4 > 0$, x_4 bounds the set (the argument of the Quick check), and $x_4 < x_3$ by (iii).

2.6.4.3 C. Going deeper

Exercise. C1: Exit check: the gap at $\sqrt{2}$

Prove that no rational number squares to 2, and that the set $\{x \in \mathbb{Q} : x^2 < 2\}$ has no supremum in $\mathbb{Q}$.

Solution. No rational squares to 2. Suppose $x \in \mathbb{Q}$ with $x^2 = 2$. Then $x \neq 0$, and replacing x by $-x$ if needed ($(-x)^2 = x^2$), $x > 0$. Write $x = a/b$ with $a, b \in \mathbb{Z}_{>0}$ (Proposition 2.4.4 (b), Theorem 2.5.1 (a)); then $a^2 = 2b^2$. Among all $q \in \mathbb{Z}_{>0}$ for which some $p \in \mathbb{Z}_{>0}$ has $p^2 = 2q^2$, take the least (Proposition 2.3.6; the set contains b and is bounded below by 0), with its p . Then $q < p$ (else $p^2 \leq q^2$ by Proposition 2.3.5 (g), so $q^2 \leq 0$, against $q^2 > 0$) and $p < 2q$ (else $4q^2 \leq p^2 = 2q^2$, so $2q^2 \leq 0$). So $p' := 2q - p$ and $q' := p - q$ are positive integers with $q' < q$, and $p'^2 - 2q'^2 = 2q^2 - p^2 = 0$ by expanding. This contradicts the choice of q .

Bounded above. 2 bounds the set A : $x > 2$ would give $x^2 > 4 > 2$ (Proposition 2.3.5 (g)). And $1 \in A$.

No supremum. Suppose $s \in \mathbb{Q}$ is a supremum of A . As $1 \in A$, $s \geq 1 > 0$, and $s^2 \neq 2$ by the first part.

If $s^2 < 2$, let $u := 4s/(s^2 + 2) \in \mathbb{Q}_{>0}$. Clearing denominators, $u - s = s(2 - s^2)/(s^2 + 2) > 0$ and $2 - u^2 = 2(s^2 - 2)^2/(s^2 + 2)^2 > 0$. So $u \in A$ and $u > s$: s is not an upper bound.

If $s^2 > 2$, let $t := (s^2 + 2)/(2s) \in \mathbb{Q}_{>0}$. Clearing denominators, $t^2 - 2 = (s^2 - 2)^2/(4s^2) > 0$ and $s - t = (s^2 - 2)/(2s) > 0$. So $t^2 > 2$, and t bounds A (an $x \in A$ with $x > t > 0$ would have $x^2 > t^2 > 2$); and $t < s$. So s is not the least upper bound.

By trichotomy one of the two cases holds, and each contradicts the choice of s . So A has no supremum in $\mathbb{Q}$.

Marking scheme. (10 points) - 4: no rational squares to 2: sets up a least denominator, or any other correct route (1); proves the key inequalities $q < p < 2q$, or the parity step of another route (2); reaches the contradiction (1). - 1: shows that A is bounded above, with an explicit upper bound, and non-empty. - 2: the case $s^2 < 2$: an explicit element of A larger than s , with both properties verified. - 2: the case $s^2 > 2$: an explicit smaller rational, verified to be an upper bound of A . - 1: concludes by trichotomy, with $s^2 = 2$ excluded by the first part. Fatal errors (0 for the step): assuming that $\sqrt{2}$ exists (in $\mathbb{Q}$ or in a larger field) and comparing s with it; “ $s^2 < 2$, so $s + \varepsilon \in A$ for small ε ” with no ε exhibited and checked. A second route for the first part, by parity (every integer is $2m$ or $2m + 1$, with $m = \lfloor a/2 \rfloor$ from Proposition 2.5.5, and not both), earns the same 4 points: 1 for the least denominator, 2 for “ p even, then q even”, 1 for the contradiction.

Exercise. C2: Which integers have a rational square root?

For which $n \in \mathbb{Z}_{>0}$ does the set $A_n := \{x \in \mathbb{Q} : x^2 < n\}$ have a supremum in $\mathbb{Q}$? Prove your answer.

Solution (Hint 1). First find $k \in \mathbb{N}$ with $k^2 \leq n < (k+1)^2$, and treat $n = k^2$ on its own. For $k^2 < n$, adapt both proofs of this section: the descent, and then the two maps.

Solution (Hint 2). Let $T := \{m \in \mathbb{Z} : m \geq 0, n < m^2\}$. It contains $n+1$, it is bounded below by 0, and $0 \notin T$; so its least element is $k+1$ for some $k \in \mathbb{N}$. In the descent for $k^2 < n$, try $q' := p - kq$.

Solution. Answer: exactly when $n = k^2$ for some $k \in \mathbb{N}$, and then the supremum is k .

Finding k . Let $T := \{m \in \mathbb{Z} : m \geq 0, n < m^2\}$. Since $n+1 \geq 1$, $(n+1)^2 \geq n+1 > n$ (Proposition 2.3.5 (c)), so $n+1 \in T$; 0 is a lower bound of T ; and $0 \notin T$, as $0^2 = 0 < n$. By Proposition 2.3.6, T has a least element l . Since $0 \notin T$ and $l \geq 0$, we have $l > 0$, so $l \geq 1$ by discreteness (Theorem 2.3.4 (c)); then $l-1 \geq 0$ by (O3), so $k := l-1 \in \mathbb{N}$ by Theorem 2.3.4 (b). Then $n < (k+1)^2$, and $k \notin T$ with $k \geq 0$ gives $k^2 \leq n$. So either $n = k^2$ or $k^2 < n < (k+1)^2$.

Case $n = k^2$. Here $k \geq 1$, since $n \geq 1$. We show $k = \sup A_n$. (S1): if $x \in A_n$ had $x > k$, then $x > k \geq 0$ would give $x^2 > k^2 = n$ (Proposition 2.3.5 (g)), against $x^2 < n$; so $x \leq k$. (S2): let v be an upper bound of A_n , and suppose $v < k$. Let $w := v$ if $v \geq 0$ and $w := 0$ otherwise; then $v \leq w$ and $0 \leq w < k$. Let c be the midpoint of w and k (Section 2.5): $w < c < k$. Then $c > 0$ and $c^2 < k^2 = n$ by (g), so $c \in A_n$, and $c > w \geq v$, so v is not an upper bound. Hence $k \leq v$ for every upper bound v , and k is the supremum.

Case $k^2 < n < (k+1)^2$. Then $n \geq 2$, since $n = 1 = 1^2$ is the other case; so $1 \in A_n$.

- (i) *No rational squares to n .* Suppose $x^2 = n$ with $x \in \mathbb{Q}$; as in Theorem 2.6.1, we may take $x > 0$, and then $p^2 = nq^2$ for some $p, q \in \mathbb{Z}_{>0}$, with q least among all such denominators (Proposition 2.3.6). Multiplying $k^2 < n < (k+1)^2$ by $q^2 > 0$ gives $(kq)^2 < p^2 < ((k+1)q)^2$, so $kq < p < (k+1)q$ by (g). Let

$$p' := nq - kp, \quad q' := p - kq.$$

Then $0 < q' < q$. For p' , expand:

$$q \cdot p' = nq^2 - kpq = p^2 - kpq = p(p - kq) > 0$$

by (O4); since $q > 0$, $p' \leq 0$ would give $qp' \leq 0$ (Proposition 2.3.5 (c)), so $p' > 0$. (The bounds alone do not give this: for $n = 5$, $k = 2$, $q = 10$, $p = 28$, we have $kq < p < (k+1)q$, but $nq - kp = -6$. It is $p^2 = nq^2$ that forces the sign.) Finally, expanding,

$$p'^2 - nq'^2 = (k^2 - n)(p^2 - nq^2) = 0,$$

so q' is a smaller admissible denominator, a contradiction.

- (ii) *No supremum.* The proof of Theorem 2.6.2 (a) goes through with n in place of 2, using (i) where it used Theorem 2.6.1. The set A_n contains 1 and is bounded above by n (if $x > n \geq 1$, then $x^2 > n^2 \geq n$). For $s \in \mathbb{Q}_{>0}$, let

$$t(s) := \frac{s^2 + n}{2s}, \quad u(s) := \frac{2ns}{s^2 + n}.$$

Clearing denominators as before,

$$\begin{aligned} t(s)^2 - n &= \frac{(s^2 - n)^2}{4s^2}, & s - t(s) &= \frac{s^2 - n}{2s}, \\ u(s) - s &= \frac{s(n - s^2)}{s^2 + n}, & n - u(s)^2 &= \frac{n(s^2 - n)^2}{(s^2 + n)^2}. \end{aligned}$$

A supremum s would satisfy $s \geq 1 > 0$ and $s^2 \neq n$ by (i). If $s^2 < n$, then $u(s) \in A_n$ and $u(s) > s$; if $s^2 > n$, then $t(s)$ is an upper bound of A_n with $t(s) < s$. Either way s is not the supremum.

So A_n has a supremum in $\mathbb{Q}$ exactly when n is the square of a natural number.

Marking scheme. (10 points) - 2: produces $k \in \mathbb{N}$ with $k^2 \leq n < (k+1)^2$, from a least element. - 2: the case $n = k^2$: checks (S1) and (S2) for k . - 3: the case $k^2 < n$: no rational squares to n , by a descent with a least denominator (or another correct route), including a proof that the new numerator is positive. - 2: the two maps (or any explicit rationals) and the two cases, as in the proof for 2. - 1: states the answer: exactly the squares of natural numbers. Fatal errors (0 for the step): using a square root of n , or the floor of one, as if it existed; deducing $nq - kp > 0$ from $kq < p < (k+1)q$ alone.

2.6.4.4 R. Review

Exercise. R1

Prove, by induction on m , that for all $m, n \in \mathbb{N}$: if $m + n = m$, then $n = 0$. Use only the equations of addition ($m+0 = m$, $m+(n+1) = (m+n)+1$, $0+n = n$, $(m+1)+n = (m+n)+1$) and the fact that $k+1 = l+1$ implies $k = l$. Do not use cancellation or any fact about the order: cancellation gives the claim in one line ($m+n = m+0$), and it is itself proved from the facts this exercise asks you to use.

Solution. We use Theorem 1.3.3 (b) (the form of Logic and Proof, Axiom 4.2.1 on $\omega = \mathbb{N}$, by Corollary 1.7.3 (b)) on m , for the property $P(m)$: “for every $n \in \mathbb{N}$, if $m+n = m$, then $n = 0$ ”. Keeping “for every n ” inside $P(m)$ lets the step use the hypothesis for the same n .

Base $P(0)$. Let $0+n = 0$. Since $0+n = n$ (Theorem 1.5.3 (a)), $n = 0$.

Step. Assume $P(m)$, and let $(m+1)+n = m+1$. By Theorem 1.5.3 (a), $(m+1)+n = (m+n)+1$, so $(m+n)+1 = m+1$. By Corollary 1.5.2, $m+n = m$. By $P(m)$, $n = 0$. This proves $P(m+1)$.

By induction, $P(m)$ holds for every $m \in \mathbb{N}$.

Cancellation (Proposition 1.6.3 (b)) and the order facts are deliberately not used: each gives

a one-line proof, and cancellation is itself proved by peeling off one successor at a time with Corollary 1.5.2, the move of the step above.

Exercise. R2

Show that the set $\mathbb{Q}$, as constructed in this chapter, is countable.

Solution. The tools are the results on countable sets of *Sets, Relations, and Cardinality*, Chapter 3, read on $\mathbb{N} = \omega$ through the dictionary of Section 1.7 (Corollary 1.7.3 and the table after it).

$\mathbb{Z}$ is countable. $\mathbb{N} \times \mathbb{N}$ is countable (Sets, Relations, and Cardinality, Theorem 3.2.6). The map $a \mapsto [a]$, from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$, is surjective, since every class is the class of each of its elements (Sets, Relations, and Cardinality, Definition 2.5.4). By Sets, Relations, and Cardinality, Proposition 3.2.4, $\mathbb{Z}$ is countable.

$\mathbb{Z} \times \mathbb{Z}_{>0}$ is countable. $\mathbb{Z}_{>0} \subseteq \mathbb{Z}$ is countable by Sets, Relations, and Cardinality, Proposition 3.2.3, and the product of two countable sets is countable (Sets, Relations, and Cardinality, Corollary 3.2.7 (a)).

$\mathbb{Q}$ is countable. The map $(p, q) \mapsto [(p, q)]$, from $\mathbb{Z} \times \mathbb{Z}_{>0}$ to $\mathbb{Q}$, is surjective (Sets, Relations, and Cardinality, Definition 2.5.4), so $\mathbb{Q}$ is countable by Sets, Relations, and Cardinality, Proposition 3.2.4.

(Section 1.7 lets a review exercise cite Sets, Relations, and Cardinality, Theorem 3.2.6 and Sets, Relations, and Cardinality, Corollary 3.2.7 (a), which run on ω through Proposition 1.6.4.) The conclusion is Sets, Relations, and Cardinality, Theorem 3.2.8 for the constructed $\mathbb{Q}$; that theorem, about the school rationals, is not used.

Exercise. R3

Let $A := \{x \in \mathbb{Q} : x^2 < 2\}$ and $s \in \mathbb{Q}$. Write “ s is a supremum of A in $\mathbb{Q}$ ” in symbols, with bounded quantifiers. Then write its negation, moving $\neg$ inward as far as it goes and naming the law used at each step. The proof that A has no supremum in $\mathbb{Q}$ has two cases; which half of the negation does each case establish, and with which witness?

Solution. By Sets, Relations, and Cardinality, Definition 2.6.5, “ s is a supremum of A ” is the conjunction of (S1) and (S2):

$$(\forall x \in A \ x \leq s) \wedge \forall v \in \mathbb{Q} ((\forall x \in A \ x \leq v) \rightarrow s \leq v).$$

Its negation is, by Logic and Proof, Proposition 2.5.5 (d),

$$\neg(\forall x \in A \ x \leq s) \vee \neg\forall v \in \mathbb{Q} ((\forall x \in A \ x \leq v) \rightarrow s \leq v).$$

By Logic and Proof, Proposition 6.2.3 (a), the first disjunct becomes $\exists x \in A \neg(x \leq s)$, that is, $\exists x \in A \ s < x$ (totality of $\leq$, Proposition 2.3.5 (i)). By Logic and Proof, Proposition 6.2.3

(a) and then Logic and Proof, Proposition 6.2.2, the second becomes

$$\exists v \in \mathbb{Q} ((\forall x \in A \ x \leq v) \wedge \neg(s \leq v)),$$

that is, there is an upper bound v of A with $v < s$. In words: s fails to be the supremum when **some element of A lies above s** , or **some upper bound lies below s** .

In the proof of [Theorem 2.6.2](#), Case 1 ($s^2 < 2$) establishes the first disjunct, with witness $x = u(s) = 4s/(s^2 + 2)$. Case 2 ($s^2 > 2$) establishes the second, with witness $v = t(s) = (s^2 + 2)/(2s)$. (The proof itself needs no negation law: it derives a contradiction from (S1) in Case 1 and from (S2) in Case 2.)

Exercise. R4

Is there a rational number x with $x^3 = 2$, where $x^3 := x^2 \cdot x$? Prove your answer.

Solution. No. The tool is descent on the denominator, as in [Theorem 2.6.1](#), but run with parity, which Proposition 2.5.5 supplies.

Parity. For every $a \in \mathbb{Z}$ there is $m \in \mathbb{Z}$ with $a = 2m$ or $a = 2m + 1$, and not both forms occur. Indeed, let $m := \lfloor a/2 \rfloor$ (Proposition 2.5.5): $m \leq a/2 < m + 1$, so $2m \leq a < 2m + 2$ (Proposition 2.3.5 (c)). The integer $r := a - 2m$ has $0 \leq r < 2$; if $r > 0$, then $r \geq 1$, and if $r > 1$, then $r \geq 2$, by discreteness (Theorem 2.3.4 (c)); so $r = 0$ or $r = 1$. If $2m = 2m' + 1$, then $d := m - m'$ has $2d = 1$; but $d \leq 0$ gives $2d \leq 0$, and $d \geq 1$ gives $2d \geq 2$, and by discreteness one of these holds. Moreover an odd cube is odd:

$$(2m + 1)^3 = 2(4m^3 + 6m^2 + 3m) + 1.$$

Descent. Suppose $x \in \mathbb{Q}$ and $x^3 = 2$. Then $x > 0$: $x = 0$ gives $x^3 = 0$, and $x < 0$ gives $x^2 > 0$ and $x^3 = x^2 \cdot x < 0$ (Proposition 2.3.5 (e), (c)). So $x = p/q$ with $p, q \in \mathbb{Z}_{>0}$ and $p^3 = 2q^3$ (Proposition 2.4.4 (b), Definition 2.4.2). Take q least among such denominators (Proposition 2.3.6), with its p . Since $p^3 = 2q^3$ has the even form, p is not odd (its cube would be odd), so $p = 2m$ with $m \in \mathbb{Z}$, and $m > 0$ because $p > 0$ ($m \leq 0$ would give $2m \leq 0$). Then $2q^3 = 8m^3$, and canceling the non-zero factor 2 (Proposition 2.3.5 (f)), $q^3 = 2(2m^3)$. So q is not odd either: $q = 2l$ with $l \in \mathbb{Z}_{>0}$. Then $8m^3 = 2 \cdot 8l^3$, so $m^3 = 2l^3$, and $l < l + l = q$. So l is a smaller admissible denominator, with $m \in \mathbb{Z}_{>0}$: a contradiction.

Why the look-alike fails. The substitution $p' := 2q - p$, $q' := p - q$ of the square-root proof came from $x = (2 - x)/(x - 1)$, which used $x^2 = 2$. For cubes the same algebra fails: expanding,

$$(2q - p)^3 - 2(p - q)^3 = -3p^3 + 12p^2q - 18pq^2 + 10q^3,$$

which is not a constant multiple of $p^3 - 2q^3$ (it has a p^2q term), so this identity gives no way to derive $p'^3 = 2q'^3$ from $p^3 = 2q^3$, and the descent has no smaller pair to move to. Parity, by contrast, works for every power: “even cube, so even base” is the same argument for squares and cubes.