

6.4 Two Non-Examples

The uniqueness theorem of Section 6.3 used three hypotheses in three different ways. The Archimedean property let rationals separate elements (Lemma 6.1.3). Completeness built the map as a supremum (Theorem 6.2.3), and it supplied square roots (Proposition 6.1.4). The order condition was either assumed of the map or, for complete fields, recovered from the square roots (Theorem 6.3.4). This section builds two ordered fields that are not $\mathbb{R}$, each missing something. The field $\mathbb{R}(x)$ of rational functions obeys every axiom of an ordered field and fails the Archimedean property; it has an order-preserving symmetry that moves x . The field $\mathbb{Q}(\sqrt{2})$ is Archimedean and not complete; it has a symmetry that does not preserve the order. A table at the end compares the four fields.

Throughout, $\mathbb{R}$ is the complete ordered field of Chapter 5 (Theorem 5.6.3), and we write q for $\iota_{\mathbb{R}}(q)$ when $q \in \mathbb{Q}$, as Section 5.4 did. Powers t^i of a real number t are those of Definition 4.2.1, and finite sums $\sum_{i=0}^d c_i$ of real numbers are defined by recursion, as in *Sets, Relations, and Cardinality*, Section 2.3 (Sets, Relations, and Cardinality, Definition 2.3.1), with $\mathbb{R}$ as the set of values; the empty sum is 0.

6.4.1 Polynomial functions

Chapter 4 met a field of quotients of polynomials, $\mathbb{Q}(t)$ (Example (A Non-Archimedean Ordered Field)), and stated without proof that it is an ordered field. Here proofs depend on such a field, so we build it from things we can check: functions on $\mathbb{R}$, compared at large arguments, with no algebra of formal polynomials.

For $d \in \mathbb{N}$ and a list $(a_0, a_1, \dots, a_d)$ of real numbers, the function

$$p: \mathbb{R} \rightarrow \mathbb{R}, \quad p(t) := \sum_{i=0}^d a_i t^i,$$

is the **polynomial function of the list**. A **polynomial function** is a function $\mathbb{R} \rightarrow \mathbb{R}$ that is the polynomial function of **at least one** list. When $a_d \neq 0$, the list has **top degree** d and **top coefficient** a_d .

The phrase “of at least one list” matters. Appending zeros to a list does not change its function: $(1, 2)$ and $(1, 2, 0)$ both give $t \mapsto 1 + 2t$. So degree and top coefficient belong to a list, not to a function, until we know more.

Examples. The **constant** $c \in \mathbb{R}$ is the polynomial function of the list (c) . The function $t \mapsto t$ is that of $(0, 1)$, and $t \mapsto t^2 - 100t$ is that of $(0, -100, 1)$, with top degree 2 and top coefficient 1. The list $(0, 0, 0)$ gives the zero function and has no top degree.

We compare such functions at large arguments. A statement $S(t)$ about real numbers t holds **for all large** t if there is $T \in \mathbb{R}$ such that $S(t)$ holds **for every** $t > T$. If $S_1(t)$ holds for $t > T_1$ and $S_2(t)$ for $t > T_2$, both hold for $t > \max\{T_1, T_2\}$; so finitely many statements that each hold for all large t hold together for all large t . The finiteness matters: infinitely many thresholds may have no maximum.

The basic fact is that far out, the top term wins.

Lemma 6.4.1. The Top Term Decides the Sign

Let $d \in \mathbb{N}$, let $a_0, \dots, a_d \in \mathbb{R}$ with $a_d \neq 0$, and let $p(t) = \sum_{i=0}^d a_i t^i$. Put

$$T := 1 + \sum_{i=0}^{d-1} \frac{|a_i|}{|a_d|}.$$

Then for every $t > T$, $p(t) \neq 0$, and $p(t)$ has the sign of a_d : $p(t) > 0$ if $a_d > 0$, and $p(t) < 0$ if $a_d < 0$.

Idea. Split off the top term: $p(t) = a_d t^d + R(t)$ with $R(t) = \sum_{i < d} a_i t^i$. For $t \geq 1$ every power t^i with $i < d$ is at most t^{d-1} , so $|R(t)|$ is at most $(\sum_{i < d} |a_i|) t^{d-1}$. That is smaller than $|a_d| t^d = |a_d| t \cdot t^{d-1}$ as soon as $|a_d| t > \sum_{i < d} |a_i|$, which is what $t > T$ guarantees. The $1 +$ in T makes $t \geq 1$.

Proof. Case $d = 0$. Then $p(t) = a_0$ for every t , with $a_0 \neq 0$, and the claim holds for every t (here $T = 1$, the sum being empty).

Case $d \geq 1$. Let $t > T$. Since $T \geq 1$, $t > 1 > 0$, so $t^i > 0$ and $1 \leq t^i \leq t^{d-1}$ for $0 \leq i \leq d-1$ (power laws in the ordered field $\mathbb{R}$, recorded in the ledger). Let $R(t) := \sum_{i=0}^{d-1} a_i t^i$ and $A := \sum_{i=0}^{d-1} |a_i| \geq 0$. By the triangle inequality Proposition 4.1.3 (e), applied term by term (induction on the number of terms), and $|a_i t^i| = |a_i| t^i$ (Proposition 4.1.3 (b)),

$$|R(t)| \leq \sum_{i=0}^{d-1} |a_i| t^i \leq A t^{d-1}.$$

From $t > T > A/|a_d|$ we get $|a_d| t > A$, and multiplying by $t^{d-1} > 0$ (Proposition 2.3.5 (c)),

$$A t^{d-1} < |a_d| t^d = |a_d t^d|.$$

So $|R(t)| < |a_d t^d|$. Now $p(t) = a_d t^d + R(t)$, where $t^d > 0$. If $a_d > 0$, then $a_d t^d > 0$ and $p(t) \geq a_d t^d - |R(t)| > 0$ (Proposition 4.1.3 (c)). If $a_d < 0$, then $a_d t^d < 0$ and $p(t) \leq a_d t^d + |R(t)| = -|a_d t^d| + |R(t)| < 0$. In both cases $p(t) \neq 0$ and has the sign of a_d . ■

So a polynomial function given by a list with a non-zero entry has, far out, a constant non-zero sign.

Quick check. For $p(t) = t^2 - 100t$, compute the threshold T of Lemma 6.4.1, and check the conclusion at $t = 102$. Is T the smallest threshold that works?

Solution. The list is $(0, -100, 1)$, so $T = 1 + (0 + 100)/1 = 101$. At $t = 102$, $p(102) = 102 \cdot 2 = 204 > 0$, the sign of the top coefficient 1. The threshold is not the smallest: $p(t) = t(t - 100) > 0$ already for every $t > 100$. The lemma promises a threshold, not the best one.

Three facts about these functions are all the algebra the field $\mathbb{R}(x)$ needs: sums and products

of polynomial functions are polynomial functions, the top coefficient of a product is the product of the top coefficients, and a list whose function vanishes far out is all zeros.

Lemma 6.4.2. Sums, Products and the Identity Principle

Let $p(t) = \sum_{i=0}^d a_i t^i$ and $r(t) = \sum_{j=0}^e b_j t^j$, for **arbitrary** lists $(a_0, \dots, a_d)$ and $(b_0, \dots, b_e)$ of real numbers (zero entries, and lists of zeros, are allowed).

- (a) The function $p + r$ is the polynomial function of the list $(a_k + b_k)_k$, where the shorter list is first extended by zeros to the length of the longer.
- (b) The function $p \cdot r$ is the polynomial function of a list $(c_0, \dots, c_{d+e})$ whose last entry is $c_{d+e} = a_d b_e$. If moreover $a_d \neq 0$ and $b_e \neq 0$, then $a_d b_e \neq 0$: the product list has top degree $d + e$ and top coefficient $a_d b_e$.
- (c) (*Identity principle.*) If $p(t) = 0$ for all large t , then $a_i = 0$ for every i .

Part (b) gives no formula for the other entries c_k ; nothing below uses one. A consequence used in the next subsection: if each of two lists has a non-zero entry, the product of their functions is given by a list with a non-zero entry. Indeed, cut each list after its last non-zero entry (this drops only zero terms, so the function is unchanged); then (b) gives a list for the product whose last entry is a product of two non-zero reals, which is non-zero (Proposition 2.3.5 (f)).

Proof.

- (c) Suppose some $a_i \neq 0$. The indices $i \leq d$ with $a_i \neq 0$ form a non-empty set of integers bounded above by d , so it has a greatest element k (Proposition 2.3.6). Dropping the terms with $i > k$, which are 0, gives $p(t) = \sum_{i=0}^k a_i t^i$ with $a_k \neq 0$. By Lemma 6.4.1 there is T with $p(t) \neq 0$ for every $t > T$. If also $p(t) = 0$ for every $t > T'$, then $t := \max\{T, T'\} + 1$ gives $p(t) \neq 0$ and $p(t) = 0$, a contradiction. So every $a_i = 0$. ■

🕒 **Second reading** · *Proof of the sum and product rules*

Idea. Sums regroup term by term. For products, peel off the lowest coefficient of r : $r = b_0 + t \cdot r'$, where r' has a shorter list, and multiplying by t only shifts a list. Induction on the length of the list of r then keeps track of the last entry.

Proof.

- (a) Extending a list by zeros adds only terms $0 \cdot t^i = 0$, so it does not change the function. After extending, both lists have the same length $m+1$, and regrouping a finite sum term by term (commutativity and associativity of $+$, by induction on m) and distributivity give $\sum_{k=0}^m a_k t^k + \sum_{k=0}^m b_k t^k = \sum_{k=0}^m (a_k + b_k) t^k$.
- (b) Two special products come first. For $c \in \mathbb{R}$, $c \cdot p$ is the polynomial function of $(ca_0, \dots, ca_d)$, by distributivity over a finite sum (induction on the number of terms). And $t \cdot p(t) = \sum_{i=0}^d a_i t^{i+1}$, since $t \cdot t^i = t^{i+1}$ (Definition 4.2.1 (b) and commutativity);

re-indexing, $t \mapsto t \cdot p(t)$ is the polynomial function of the **shifted** list $(0, a_0, \dots, a_d)$, of length $d + 2$ with the same last entry a_d .

Now we prove (b) by induction on e (Logic and Proof, Axiom 4.2.1, base $P(0)$), for every list $(a_0, \dots, a_d)$ at once. For $e = 0$, $p \cdot r = b_0 \cdot p$, the function of $(b_0 a_0, \dots, b_0 a_d)$, of length $d + 1$ and last entry $a_d b_0$. For the step, let $e \geq 1$ and let r' be the function of $(b_1, \dots, b_e)$, a list with last index $e - 1$. Re-indexing as above, $r(t) = b_0 + t \cdot r'(t)$, so

$$p(t) r(t) = b_0 p(t) + t \cdot (p(t) r'(t)).$$

By the induction hypothesis, $p \cdot r'$ is the function of a list with last index $d + e - 1$ and last entry $a_d b_e$. Shifting gives a list for $t \mapsto t p(t) r'(t)$ with last index $d + e$ and last entry $a_d b_e$. The list of $b_0 \cdot p$ has last index $d \leq d + e - 1$, so in the sum (a) its extension has 0 in position $d + e$, and the last entry of the sum list is $a_d b_e + 0 = a_d b_e$. This is the claim for e .

Nothing here used a non-zero entry, so the statement holds for arbitrary lists. Only the last sentence of (b) uses that $\mathbb{R}$ has no zero divisors: $a_d \neq 0$ and $b_e \neq 0$ give $a_d b_e \neq 0$ (Proposition 2.3.5 (f)).

■

6.4.2 The field of rational functions

A rational function should be a quotient p/q of polynomial functions. As a function on $\mathbb{R}$ it is undefined where q vanishes, so we only ever look far out, where Lemma 6.4.1 keeps q away from 0, and we count two quotients as equal when they agree far out.

A rational function is a quotient of polynomial functions, seen only at large arguments.

Definition 6.4.1. The Ordered Field of Rational Functions

A **fraction** is a pair (p, q) of polynomial functions such that q is the polynomial function of a list with a **non-zero** entry. By Lemma 6.4.1, applied to that list cut after its last non-zero entry, there is $T_q \in \mathbb{R}$ with $q(t) \neq 0$ for every $t > T_q$; the **value** of the fraction at such t is the real number $p(t)/q(t)$.

- (a) Two fractions (p_1, q_1) and (p_2, q_2) are **equivalent** if $p_1(t)/q_1(t) = p_2(t)/q_2(t)$ **for all large t** . The set $\mathbb{R}(x)$ of **rational functions** is the set of equivalence classes (Sets, Relations, and Cardinality, Definition 2.5.4); the class of (p, q) is written $[p/q]$.

- (b) **Sum and product:**

$$\begin{aligned} [p_1/q_1] + [p_2/q_2] &:= [(p_1 q_2 + p_2 q_1)/(q_1 q_2)], \\ [p_1/q_1] \cdot [p_2/q_2] &:= [(p_1 p_2)/(q_1 q_2)]. \end{aligned}$$

- (c) **Positive set:** $P := \{[p/q] \in \mathbb{R}(x) : p(t)/q(t) > 0 \text{ for all large } t\}$, and $f < g$ means $g - f \in P$.

- (d) $x := [\text{id}_{\mathbb{R}}/1]$, where $\text{id}_{\mathbb{R}}: t \mapsto t$ is the polynomial function of $(0, 1)$ and 1 is the constant.

In words: (a) a rational function is known only through its values far out; (b) adds and multiplies by the school rules for fractions; (c) calls it positive if its values are eventually positive; (d) names

the simplest non-constant one.

Well-definedness. Every condition in the definition is a statement about values at all large t , and a value at a single t is computed in the field $\mathbb{R}$. In particular, sums and products are **pointwise at large t** : beyond the thresholds of the two denominators, the value of the sum fraction is the sum of the two values, and the value of the product fraction is their product (Lemma 4.1.1 (b) in $\mathbb{R}$). That is why equivalence of fractions is an equivalence relation, why the formulas give fractions, and why sum, product and P do not depend on the representatives; the fold checks each point.

🕒 **Second reading** · *The well-definedness checks*

- *Equivalence relation* (Sets, Relations, and Cardinality, Definition 2.5.1). Reflexive: take $T = T_q$. Symmetric: the definition is symmetric. Transitive: if the values of (p_1, q_1) , (p_2, q_2) agree for $t > T$ and those of (p_2, q_2) , (p_3, q_3) for $t > T'$, then those of the first and third agree for $t > \max\{T, T'\}$.
- *The formulas give fractions.* $p_1q_2 + p_2q_1$ and p_1p_2 are polynomial functions by Lemma 6.4.2 (a), (b), and q_1q_2 is given by a list with a non-zero entry, by the consequence stated after that lemma.
- *Values of a sum and a product.* For $t > \max\{T_{q_1}, T_{q_2}\}$, $q_1(t)q_2(t) \neq 0$, and by the fraction rules in $\mathbb{R}$ (Lemma 4.1.1 (b)) the value of the sum fraction is $p_1(t)/q_1(t) + p_2(t)/q_2(t)$, and that of the product fraction is the product of the values. Sums and products are **pointwise at large t** .
- *Independence of representatives.* If (p_1, q_1) is replaced by an equivalent fraction, its values change at no large t , so by the previous point the values of the sum and product fractions change at no large t : the new sum and product are equivalent to the old. The same holds for the second argument. By Theorem 2.2.1 (b), sum and product are well-defined functions $\mathbb{R}(x) \times \mathbb{R}(x) \rightarrow \mathbb{R}(x)$. In the same way, “positive for all large t ” does not depend on the representative, so P is well defined (Theorem 2.2.1 (c)).

Examples. The constant $c \in \mathbb{R}$ gives the class $[c/1]$, with value c at every t . The class $x = [\text{id}_{\mathbb{R}}/1]$ has value t . The fraction whose numerator is $t \mapsto t$ and whose denominator is $t \mapsto t^2$ is equivalent to the fraction $(1, \text{id}_{\mathbb{R}})$: their values t/t^2 and $1/t$ agree for every $t > 0$. This is the usual cancellation, now a statement about values.

Proposition 6.4.3. Rational Functions Form an Ordered Field

- (a) $\mathbb{R}(x)$, with the sum, product and order of Definition 6.4.1, is an ordered field (Definition 2.3.2), with zero $[0/1]$, unit $[1/1]$, and positive elements exactly the elements of P .
- (b) The map $\mathbb{R} \rightarrow \mathbb{R}(x)$, $c \mapsto [c/1]$, is an order-preserving field map (Definition 6.1.1).

Idea. Every field identity holds at each large t , because it holds in $\mathbb{R}$ and the operations are pointwise there; so it holds in $\mathbb{R}(x)$. The two places where something more is needed are where an existence claim is made or a sign must be decided: the inverse of a non-zero class, and trichotomy. Both rest on Lemma 6.4.1: a fraction’s numerator, unless its list is all zeros, has an eventually constant sign.

◉ **Second reading** · *Proof that the rational functions form an ordered field*

Proof. Commutative ring. Each of (F1), (F2), (F5), (F6), (F9) of Definition 2.3.1 is an identity between classes built from given classes by sums and products. By the pointwise rule, its two sides have, at every large t , the values of the two sides of the same identity among real numbers, which holds in $\mathbb{R}$ (Theorem 5.2.3). So the two sides are equivalent fractions. For (F3), (F7) and (F4): $[0/1]$ and $[1/1]$ have values 0 and 1, so $f + [0/1] = f$ and $f \cdot [1/1] = f$; and $[(-p)/q]$, where $-p = (-1) \cdot p$ is a polynomial function by Lemma 6.4.2 (b), has value $-p(t)/q(t)$, so it is a negative of $[p/q]$. The table at the end of this proof writes out two of the identities.

$1 \neq 0$. If $[1/1] = [0/1]$, then $1 = 0$ at every $t > T$ for some T , and $t = T + 1$ gives $1 = 0$ in $\mathbb{R}$, which is false.

Inverses (F8). Let $f = [p/q] \neq [0/1]$. If every entry of a list of p were 0, then $p(t) = 0$ for all t , and f would have value 0 at all large t , so $f = [0/1]$. Hence p is the function of a list with a non-zero entry, (q, p) is a fraction, and for $t > \max\{T_p, T_q\}$ the value of $f \cdot [q/p]$ is $(p(t)/q(t))(q(t)/p(t)) = 1$. So $[q/p]$ is an inverse of f .

Positive set. We check (P1) and (P2) of Proposition 2.3.3. (P1): if $f, g \in P$, with values positive for $t > T$ and for $t > T'$ respectively, then for $t > \max\{T, T'\}$ the values of $f + g$ and fg are a sum and a product of two positive reals, hence positive by Proposition 2.3.5 (b) and (O4) in $\mathbb{R}$. (P2): let $f = [p/q]$. If a list of p is all zeros, then $f = [0/1]$, and neither f nor $-f$ is in P , since their values are 0 far out. Otherwise, cut the lists of p and q after their last non-zero entries; by Lemma 6.4.1, each of $p(t)$ and $q(t)$ has a constant non-zero sign for all large t , so $p(t)/q(t)$ has a constant non-zero sign for all large t (Proposition 2.5.2 (a) and Proposition 2.3.5 (c), (d)). If that sign is positive, $f \in P$; if negative, $-f \in P$. In this case $f \neq [0/1]$, since a value that is non-zero for all large t is not 0 for all large t . And $f \in P$, $-f \in P$ cannot both hold: at t beyond both thresholds the value would be positive and negative. So exactly one of $f \in P$, $f = 0$, $-f \in P$ holds.

By Proposition 2.3.3, $\mathbb{R}(x)$ with $f < g \Leftrightarrow g - f \in P$ is an ordered commutative ring whose positive elements are those of P . With (F8) and $1 \neq 0$, it is an ordered field. This proves (a).

- (b) The value of $[c/1]$ is c at every t . By the pointwise rule, $[(c + c')/1] = [c/1] + [c'/1]$ and $[cc'/1] = [c/1][c'/1]$, and $[1/1]$ is the unit. If $c < c'$, then $[c'/1] - [c/1] = [(c' - c)/1]$ has the positive value $c' - c$ at every t , so it lies in P , and $[c/1] < [c'/1]$.

■

Two field identities written out.

Identity	Value of the left side at large t	Value of the right side	Why equal in $\mathbb{R}$
(F9) $f(g + h) = fg + fh$	$u(t)(v(t) + w(t))$	$u(t)v(t) + u(t)w(t)$	(F9) in $\mathbb{R}$
(F2) $(f + g) + h = f + (g + h)$	$(u(t) + v(t)) + w(t)$	$u(t) + (v(t) + w(t))$	(F2) in $\mathbb{R}$

Here $u(t)$, $v(t)$, $w(t)$ are the values of chosen representatives of f , g , h , and “large” means beyond the maximum of the finitely many thresholds T_q involved. Each value column is computed with the pointwise rule for sums and products; the representatives produced by the formulas of Definition 6.4.1 (b) for the two sides are different fractions, but their values agree, and that is equivalence. Exercise B1 writes out one more identity, (F5), and the closure of P under sums.

From now on we write c for the class $[c/1]$ of a real number c , as (b) permits. Then for $q \in \mathbb{Q}$, $\iota_{\mathbb{R}(x)}(q) = q$: the composite $q \mapsto [\iota_{\mathbb{R}}(q)/1]$ is $\iota_{\mathbb{R}(x)}$ by Proposition 6.1.1, applied to the map of (b). Also, by induction on i , x^i is the class of $t \mapsto t^i$ (the product is pointwise), so the polynomial function $p(t) = \sum a_i t^i$ has class $\sum a_i x^i$, and $[p/q] = p(x)/q(x)$, a quotient in the field $\mathbb{R}(x)$. The notation for rational functions is now the familiar one.

Warning. The element x of $\mathbb{R}(x)$ is **not** a real number, and the order of $\mathbb{R}(x)$ is **not** “compare values at one t ”. At $t = 1$, the value of x is 1 and that of x^2 is also 1, yet $x < x^2$, since $t^2 - t > 0$ for every $t > 1$. A comparison made at one argument says nothing; a comparison made at all large arguments is the order.

The order is unusual in one way that matters for this chapter: x lies above every natural number.

Proposition 6.4.4. Rational Functions Are Not Archimedean

In $\mathbb{R}(x)$, $n \cdot 1 < x$ for every $n \in \mathbb{N}$. Hence $\mathbb{R}(x)$ is not Archimedean (Definition 4.2.2), and it is not complete (Definition 5.6.1).

Proof. Let $n \in \mathbb{N}$. By Theorem 4.2.2, $n \cdot 1 = \iota_{\mathbb{R}(x)}(n)$, which is the class of the constant n . The difference $x - n$ has value $t - n$, positive for every $t > n$. So $x - n \in P$, that is, $n \cdot 1 < x$.

So the element x has no $n \in \mathbb{N}$ with $x < n \cdot 1$, which is the negation of the Archimedean property (Logic and Proof, Proposition 6.2.1). If $\mathbb{R}(x)$ were complete, it would be Archimedean by Theorem 6.1.2. So it is not complete. ■

The set $\{n \cdot 1 : n \in \mathbb{N}\}$ is non-empty and bounded above by x ; in fact it has no supremum, and Exercise C1 asks for a direct proof of that, with no appeal to Theorem 6.1.2.

Above every natural number sits x ; below every $1/n$ sits its reciprocal.

Example. An Element Smaller Than Every $1/n$

Show that $0 < 1/x < 1/n$ in $\mathbb{R}(x)$ for every $n \in \mathbb{Z}_{>0}$. Deduce that the sequence $(1/(n+1))_{n \in \mathbb{N}}$ does **not** converge to 0 in $\mathbb{R}(x)$ (Definition 4.3.2), and that “ $0 \leq a < 1/n$ for every $n \geq 1$ ” does not force $a = 0$.

Solution. The class $1/x = [1/\text{id}_{\mathbb{R}}]$ has value $1/t$, positive for $t > 0$; so $1/x > 0$. The class $1/n - 1/x$ has value $1/n - 1/t$, positive for every $t > n$ (Proposition 2.5.2 (b)); so $1/x < 1/n$.

Take $\varepsilon := 1/x \in \mathbb{R}(x)_{>0}$. For every $n \in \mathbb{N}$, $|1/(n+1) - 0| = 1/(n+1) > 1/x = \varepsilon$, so no N has $|1/(n+1) - 0| < \varepsilon$ for $n \geq N$; the sequence does not converge to 0. This is the sequence of Proposition 4.3.1, which is null exactly in Archimedean fields, and $\mathbb{R}(x)$ is not one. Finally, $a := 1/x$ satisfies $0 \leq a < 1/n$ for every $n \geq 1$, and $a \neq 0$.

A step about sequences in an ordered field that “obviously” holds is often the Archimedean property in disguise; $\mathbb{R}(x)$ is where to test it. It also shows why the rationals cannot separate elements without Archimedes (Lemma 6.1.3): the elements $1/x$ and $2/x$ are different, and the same rationals lie below each, namely the $q \leq 0$.

Example. A Positive Element That Is Not a Square

Show that $x > 0$ in $\mathbb{R}(x)$, but that there is no $f \in \mathbb{R}(x)$ with $f^2 = x$.

Solution. $x > 0$ because its value t is positive for $t > 0$.

Suppose $x = f^2$ with $f = [p/q]$. Comparing values, $t = p(t)^2/q(t)^2$ for all large t , so

$$h(t) := t \cdot q(t)^2 - p(t)^2 = 0 \quad \text{for all large } t.$$

By Lemma 6.4.2 (a), (b), h is the polynomial function of a list: q^2 and p^2 are products, $t \cdot q^2$ is a product with the function of $(0, 1)$, $-p^2$ is a product with the constant -1 , and h is a sum. We now find a non-zero entry of such a list, against the identity principle (c).

Cut the list of q after its last non-zero entry b_e (it has one, since (p, q) is a fraction). By (b), q^2 has a list with top degree $2e$ and top coefficient b_e^2 , and $t \cdot q^2$ has a list with top degree $2e + 1$ and top coefficient $b_e^2 \neq 0$.

If a list of p is all zeros, then $p^2 = 0$, so $t \cdot q(t)^2 = 0$ for all large t ; by (c), every entry of the list of $t \cdot q^2$ is 0, against $b_e^2 \neq 0$.

Otherwise, cut the list of p after its last non-zero entry a_d . By (b), p^2 has a list with top degree $2d$ and top coefficient a_d^2 , so $-p^2$ has one with top degree $2d$ and top coefficient $-a_d^2$. Now $2d \neq 2e + 1$: an integer is not both even and odd (Corollary 3.1.3 (a)). If $2e + 1 > 2d$, the sum list (a) for h has entry $b_e^2 + 0 \neq 0$ at index $2e + 1$; if $2d > 2e + 1$, it has entry $0 - a_d^2 \neq 0$ at index $2d$. Either way (c) is contradicted.

So x is not a square in $\mathbb{R}(x)$, while in $\mathbb{R}$ every positive element is one (Proposition 6.1.4).

Quick check. Is $-x$ a square in $\mathbb{R}(x)$? Is $x^2 - 2x + 1$? Answer each in one line, without the argument above.

Solution. $-x$ is not: $-x < 0$ because $x > 0$, and in any ordered field every square is ≥ 0 (Proposition 2.3.5 (e)). $x^2 - 2x + 1$ is: it equals $(x - 1)^2$ by Proposition 2.3.2 (d), since $\mathbb{R}(x)$ is a commutative ring. A sign test can only rule out negative elements; for the positive element x the example needed the top degrees.

6.4.3 The field $\mathbb{Q}(\sqrt{2})$

The second non-example sits inside $\mathbb{R}$. By Proposition 6.1.4 in the complete field $\mathbb{R}$, there is exactly one $r \geq 0$ in $\mathbb{R}$ with $r^2 = 2$; we write $\sqrt{2} := r$. (It is the element of Example (The Class of the Newton Sequence), by the uniqueness in Proposition 6.1.4.)

Definition 6.4.2. The Field Generated by the Square Root of Two

$$\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R},$$

with the sum, product and order of $\mathbb{R}$.

Proposition 6.4.5. An Archimedean Ordered Field Inside the Reals

- (a) (*Unique representation.*) If $a + b\sqrt{2} = a' + b'\sqrt{2}$ with $a, b, a', b' \in \mathbb{Q}$, then $a = a'$ and $b = b'$.
- (b) $\mathbb{Q}(\sqrt{2})$ is closed under sums, negatives and products, contains 0 and 1, and contains the inverse of each of its non-zero elements:

$$(a + b\sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}, \quad a^2 - 2b^2 \neq 0.$$

- (c) With the operations and order of $\mathbb{R}$, $\mathbb{Q}(\sqrt{2})$ is an Archimedean ordered field.

Idea. If two representations differed in the coefficient of $\sqrt{2}$, we could solve for $\sqrt{2}$ as a rational, which Theorem 2.6.1 forbids. Inverses come from the school trick of multiplying by $a - b\sqrt{2}$. The Archimedean property is inherited from $\mathbb{R}$, because $n \cdot 1$ is the same element in both fields.

Proof.

- (a) Suppose $b \neq b'$. Then $\sqrt{2} = (a - a')/(b' - b)$, a rational s . So $\iota_{\mathbb{R}}(s^2) = \iota_{\mathbb{R}}(s)^2 = 2 = \iota_{\mathbb{R}}(2)$, and $s^2 = 2$ since $\iota_{\mathbb{R}}$ is injective (Theorem 4.2.2), against Theorem 2.6.1. Hence $b = b'$, and then $a = a'$.

- (b) Sums and negatives are clear. For products, with $(\sqrt{2})^2 = 2$,

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

$0 = 0 + 0\sqrt{2}$ and $1 = 1 + 0\sqrt{2}$. Let $a + b\sqrt{2} \neq 0$. If $b = 0$, then $a \neq 0$ and $a^2 - 2b^2 = a^2 \neq 0$. If $b \neq 0$ and $a^2 = 2b^2$, then $(a/b)^2 = 2$, against Theorem 2.6.1. So $a^2 - 2b^2 \neq 0$ in either case, and $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$ gives the displayed inverse, which lies in $\mathbb{Q}(\sqrt{2})$.

- (c) The field axioms (F1)–(F9) and the order axioms (O1)–(O4) are statements “for all elements”; they hold for all elements of $\mathbb{R}$ (Theorem 5.6.3), hence for all elements of the subset $\mathbb{Q}(\sqrt{2})$, which by (b) is closed under the operations and contains 0, 1, negatives and inverses. So $\mathbb{Q}(\sqrt{2})$ is an ordered field, with the same 1 and the same sums as $\mathbb{R}$; in particular $n \cdot 1$ is the same element in both. Let $y \in \mathbb{Q}(\sqrt{2})$. Since $\mathbb{R}$ is complete, it is Archimedean (Theorem 6.1.2), so $y < n \cdot 1$ for some $n \in \mathbb{N}$. This inequality holds in $\mathbb{Q}(\sqrt{2})$, whose order is that of $\mathbb{R}$. So $\mathbb{Q}(\sqrt{2})$ is Archimedean.



Being Archimedean is inherited by every ordered subfield of $\mathbb{R}$. Completeness is not.

Proposition 6.4.6. The Field Generated by the Square Root of Two Is Not Complete

The element 3 of $\mathbb{Q}(\sqrt{2})$ is positive and has no square root in $\mathbb{Q}(\sqrt{2})$. Hence $\mathbb{Q}(\sqrt{2})$ is not complete.

Idea. A square root $a + b\sqrt{2}$ of 3 would, by unique representation, have $2ab = 0$ and $a^2 + 2b^2 = 3$. So either $a^2 = 3$ or $(2b)^2 = 6$, with $a, 2b$ rational. Neither 3 nor 6 is a rational square, by the descent that showed 2 is not (Theorem 2.6.1). The descent there used $1 < y < 2$ for the would-be root y ; for 3 we use $1 < y < 2$ again, and for 6, $2 < y < 3$.

We isolate the descent as a claim; its proof is that of Theorem 2.6.1 with 2 replaced by n , and it sits in the fold.

Claim. Let $n, k \in \mathbb{N}$ with $k^2 < n < (k+1)^2$. Then no $y \in \mathbb{Q}$ has $y^2 = n$.

○ **Second reading** · *Proof of the claim: the descent*

Proof. Suppose $y \in \mathbb{Q}$ and $y^2 = n$. Then $y \neq 0$, since $n > k^2 \geq 0$. Replacing y by $-y$ if necessary, as in Theorem 2.6.1, we may take $y > 0$. By Proposition 2.4.4 (b), $y = a/b$ with $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{>0}$; then $a > 0$ by Theorem 2.5.1 (a), and $y^2 = n$ says $a^2 = nb^2$, as in Theorem 2.6.1. So the set

$$D := \{v \in \mathbb{Z}_{>0} : u^2 = nv^2 \text{ for some } u \in \mathbb{Z}_{>0}\}$$

contains b and is bounded below by 0. By Proposition 2.3.6 it has a least element v ; fix $u \in \mathbb{Z}_{>0}$ with $u^2 = nv^2$.

$kv < u$. Otherwise $0 \leq u \leq kv$, so $u^2 \leq k^2v^2$ (Proposition 2.3.5 (g), or equality), and $k^2v^2 < nv^2$ since $v^2 > 0$ (Proposition 2.3.5 (c), (e)). Then $u^2 < nv^2$, against $u^2 = nv^2$.

$u < (k+1)v$. Otherwise $0 \leq (k+1)v \leq u$, so $(k+1)^2v^2 \leq u^2 = nv^2 < (k+1)^2v^2$, a contradiction.

Descent. Put $v' := u - kv$ and $u' := nv - ku$. By the two inequalities, $0 < v' < v$. Multiplying $kv < u$ by $u > 0$ gives $v \cdot ku < u^2 = v \cdot nv$, so $ku < nv$ (if $ku \geq nv$, multiplying by $v > 0$ would give the reverse), and $u' > 0$. Expanding,

$$\begin{aligned} u'^2 - nv'^2 &= (n^2v^2 - 2nkuv + k^2u^2) - (nu^2 - 2nkuv + nk^2v^2) \\ &= (k^2 - n)(u^2 - nv^2) = 0. \end{aligned}$$

So $v' \in D$ and $v' < v$, against the choice of v . This proves the claim. ■

Proof. Since $1 < 3 < 4$ and $4 < 6 < 9$, the claim with $(n, k) = (3, 1)$ and $(6, 2)$ shows that neither 3 nor 6 is the square of a rational.

Now suppose $c = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, with $a, b \in \mathbb{Q}$, has $c^2 = 3$. By the product formula of Proposition 6.4.5 (b),

$$(a^2 + 2b^2) + 2ab\sqrt{2} = 3 + 0\sqrt{2},$$

so by unique representation, $2ab = 0$ and $a^2 + 2b^2 = 3$. Hence $a = 0$ or $b = 0$ (Proposition 2.3.5 (f), as $2 \neq 0$). If $b = 0$, then $a^2 = 3$; if $a = 0$, then $2b^2 = 3$, so $(2b)^2 = 6$. Both are excluded by the claim. So 3, which is positive, has no square root in $\mathbb{Q}(\sqrt{2})$.

If $\mathbb{Q}(\sqrt{2})$ were complete, Proposition 6.1.4 would give a square root of 3 in it. So $\mathbb{Q}(\sqrt{2})$ is not complete. ■

The proof found no explicit set without a supremum; it found a missing square root and let Proposition 6.1.4 supply the set. The set is easy to name: $\{y \in \mathbb{Q}(\sqrt{2}) : y \geq 0, y^2 < 3\}$ is non-empty and bounded above by 2, and in $\mathbb{R}$ its supremum is the square root $\sqrt{3}$ of 3 given by Proposition 6.1.4, which is not in $\mathbb{Q}(\sqrt{2})$.

○ **Second reading** · Why the supremum is the square root of three

The element $\sqrt{3}$ bounds the set above: $y \geq 0$ and $y^2 < 3 = (\sqrt{3})^2$ give $y < \sqrt{3}$ (Proposition 2.3.5 (g)). If $s < \sqrt{3}$, then, $\mathbb{R}$ being Archimedean (Theorem 6.1.2), Theorem 4.2.5 gives a rational q with $\max\{s, 0\} < q < \sqrt{3}$; then $q \geq 0$ and $q^2 < 3$, so q lies in the set and s is not an upper bound. Hence $\sqrt{3}$ is the least upper bound.

Quick check. Why does the descent claim not show that 4 is not a rational square? Which hypothesis fails?

Solution. There is no $k \in \mathbb{N}$ with $k^2 < 4 < (k+1)^2$: $k^2 < 4$ forces $k \leq 1$ (for $k \geq 2$, $k^2 \geq 4$), and then $(k+1)^2 \leq 4$. The descent needs the root $y = u/v$ to lie strictly between k and $k+1$, so that $0 < v' < v$; the natural choice $k = 2$ (for which $k^2 < n$ fails) gives $v' = u - 2v = 0$ when $y = 2$, and the descent stops. And indeed $4 = 2^2$.

The field $\mathbb{Q}(\sqrt{2})$ has a symmetry that the uniqueness theorem forbids in $\mathbb{R}$.

Example. Conjugation in $\mathbb{Q}(\sqrt{2})$

Define $\sigma: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ by $\sigma(a + b\sqrt{2}) := a - b\sqrt{2}$ for $a, b \in \mathbb{Q}$. Show that σ is a bijection that respects sums and products and has $\sigma(1) = 1$, that it is not the identity, and that it is not order-preserving. Then find the line of the proof of Theorem 6.3.4 that fails for σ .

Solution. Well defined. By unique representation (Proposition 6.4.5 (a)), each element has exactly one pair (a, b) , so the formula defines a function.

Sums, products, 1. σ respects sums, since $(a - b\sqrt{2}) + (c - d\sqrt{2}) = (a + c) - (b + d)\sqrt{2}$. For products, by the product formula,

$$\sigma((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}).$$

And $\sigma(1) = \sigma(1 + 0\sqrt{2}) = 1$.

Bijjective. $\sigma(\sigma(a + b\sqrt{2})) = a + b\sqrt{2}$, so σ is its own two-sided inverse (Sets, Relations, and Cardinality, Theorem 1.5.4).

Not the identity, not order-preserving. $\sqrt{2} > 0$, since it is a non-zero element with $\sqrt{2} \geq 0$. But $\sigma(\sqrt{2}) = -\sqrt{2} < 0 = \sigma(0)$. So $\sigma(\sqrt{2}) \neq \sqrt{2}$, and $0 < \sqrt{2}$ while $\sigma(0) > \sigma(\sqrt{2})$.

The failing line. Step 1 of the proof of Theorem 6.3.4 begins: “there is $b \in F$ with $b \geq 0$ and $b^2 = a$ ”. For $a = \sqrt{2}$ there is no such b in $\mathbb{Q}(\sqrt{2})$. Indeed, if $c \in \mathbb{Q}(\sqrt{2})$ had $c^2 = \sqrt{2}$, then $\sigma(c)^2 = \sigma(c^2) = \sigma(\sqrt{2}) = -\sqrt{2} < 0$; but $\sigma(c)^2 \geq 0$, as every square in the ordered field $\mathbb{R}$ is (Proposition 2.3.5 (e)). So the step “ $\sigma(a) = \sigma(b)^2 > 0$ ” cannot start, and σ indeed sends the positive element $\sqrt{2}$ to a negative one. Step 2 works in any ordered field. Step 3 as written cites completeness of F , for the Archimedean property and for the target of Theorem 6.2.3, but its conclusion still holds in $\mathbb{Q}(\sqrt{2})$: if σ were order-preserving, then σ followed by the inclusion would be an order-preserving field map $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{R}$, hence the inclusion by the uniqueness clause of Theorem 6.2.3 (source $\mathbb{Q}(\sqrt{2})$, Archimedean by Proposition 6.4.5; target $\mathbb{R}$), and σ would be the identity. Only Step 1 genuinely fails.

Two maps into $\mathbb{R}$. Since $\mathbb{Q}(\sqrt{2})$ is Archimedean and $\mathbb{R}$ complete, Theorem 6.2.3 gives exactly one order-preserving field map $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{R}$; it is the inclusion. The composite of σ with the inclusion is a second map $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{R}$ that respects sums, products and 1. The uniqueness clause is not contradicted, because this second map is not order-preserving.

6.4.4 A symmetry that keeps the order

The conjugation of $\mathbb{Q}(\sqrt{2})$ escapes Theorem 6.3.4 by breaking the order. The field $\mathbb{R}(x)$ escapes Corollary 6.3.3 in the other way: it has a symmetry that keeps the order and still moves elements. The symmetry shifts the argument by 1.

Example. Shifting the Argument

For a polynomial function p , write p^+ for the function $t \mapsto p(t + 1)$. Show that $\sigma([p/q]) := [p^+/q^+]$ defines an order-preserving field automorphism σ of $\mathbb{R}(x)$ with $\sigma(x) = x + 1 \neq x$.

⌚ **Second reading** · *The checks for the shift*

Solution. (i) p^+ is a polynomial function. By induction on the length of a list of p (Logic and Proof, Axiom 4.2.1). A list of length 1 gives a constant p , and $p^+ = p$. For a list $(a_0, \dots, a_d)$ with $d \geq 1$, let p' be the function of $(a_1, \dots, a_d)$; re-indexing the sum, $p(t) = a_0 + t \cdot p'(t)$, so

$$p(t+1) = a_0 + (1+t) \cdot p'(t+1).$$

By the induction hypothesis p'^+ is a polynomial function, $t \mapsto 1+t$ is that of $(1,1)$, and Lemma 6.4.2 (b), (a) make the right side a polynomial function.

(ii) *Fractions go to fractions.* If (p, q) is a fraction, then $q(t) \neq 0$ for every $t > T_q$, so $q^+(t) \neq 0$ for every $t > T_q - 1$. If every entry of a list of q^+ were 0, then q^+ would vanish everywhere; so a list of q^+ has a non-zero entry, and (p^+, q^+) is a fraction. Its value at t is the value of (p, q) at $t+1$.

(iii) *Well defined, additive, multiplicative.* If (p_1, q_1) and (p_2, q_2) have equal values for every $t > T$, the shifted fractions have equal values for every $t > T-1$; so σ is well defined (Theorem 2.2.1 (a)). Since sums and products are pointwise at large t , and shifting the argument commutes with pointwise operations, $\sigma(f+g)$ and $\sigma(f) + \sigma(g)$ have the same values at all large t , and likewise for products. And $\sigma(1) = 1$, since a constant is unchanged by the shift.

(iv) *Order.* If $f \in P$, with positive values for $t > T$, then $\sigma(f)$ has positive values for $t > T-1$, so $\sigma(f) \in P$. For $f < g$, $\sigma(g) - \sigma(f) = \sigma(g-f) \in P$ (additivity gives $\sigma(-f) = -\sigma(f)$, as in Step 2 of the proof of Theorem 6.3.4), so $\sigma(f) < \sigma(g)$.

(v) *Bijective.* Shifting by -1 in the same way defines τ with $\tau(\sigma(f)) = f = \sigma(\tau(f))$: the values are shifted by 1 and back. By Sets, Relations, and Cardinality, Theorem 1.5.4, σ is bijective.

(vi) *It moves x .* $\sigma(x)$ has value $t+1$, which is the value of $x+1$; so $\sigma(x) = x+1$. And $x+1 \neq x$, since $1 \neq 0$.

Remark. So Corollary 6.3.3 needs its hypothesis. Its proof went through Theorem 6.2.3, whose uniqueness clause rests on Lemma 6.1.3, which needs the Archimedean property. In $\mathbb{R}(x)$ that lemma fails exactly here: every rational lies below x and below $x+1$, so x and $x+1$ have the same rationals below them, all of $\mathbb{Q}$, and nothing can tell them apart. An order-preserving map that fixes the rationals is free to send one to the other. No proof uses this example; only the table below cites it.

6.4.5 What each hypothesis buys

The table collects the four fields of this chapter. Each entry names where it is proved; no entry rests on an exercise.

	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{R}(x)$	$\mathbb{R}$
Archimedean	yes: Theorem 2.5.3	yes: Proposition 6.4.5	no: Proposition 6.4.4	yes: Theorem 5.6.3, Theorem 6.1.2
complete	no: see below	no: Proposition 6.4.6	no: Proposition 6.4.4	yes: Theorem 5.6.3
every positive element a square	no: Theorem 2.6.1	no: Proposition 6.4.6	no: Example (A Positive Element That Is Not a Square)	yes: Proposition 6.1.4
only field automorphism the identity	yes: see below	no: Example (Conjugation in $\mathbb{Q}(\sqrt{2})$)	no: Example (Shifting the Argument)	yes: Theorem 6.3.4

Two entries need a line. $\mathbb{Q}$ is not complete: if it were, Proposition 6.1.4 would give a rational square root of 2, against Theorem 2.6.1. And a map $\sigma: \mathbb{Q} \rightarrow \mathbb{Q}$ that respects sums and products and fixes 1 is the identity, with no order hypothesis: by Proposition 6.1.1 with $F = L = \mathbb{Q}$, $\sigma = \sigma \circ \iota_{\mathbb{Q}} = \iota_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$, the last equality by the uniqueness clause of Theorem 4.2.2, since $\text{id}_{\mathbb{Q}}$ is such a map.

Read across, the table shows what the uniqueness theorem used. $\mathbb{Q}(\sqrt{2})$ has the Archimedean property and lacks square roots, and its symmetry breaks the order. $\mathbb{R}(x)$ lacks the Archimedean property, and its symmetry keeps the order. Of these three, only $\mathbb{R}$, which has both, has no symmetry at all. Read down, the column of $\mathbb{Q}$ shows that the last row does not characterize $\mathbb{R}$: a field can be rigid for a cheaper reason, having nothing besides rationals to move.

6.4.6 Exercises

6.4.6.1 A. Check your understanding

Exercise. A1

- Is $x^2 - 100x$ positive in $\mathbb{R}(x)$? Justify your answer.
- Here is an argument. “ $\mathbb{Q}(\sqrt{2})$ is Archimedean, so by Theorem 6.2.3 it has an order-preserving field map into the complete ordered field $\mathbb{R}$. Hence $\mathbb{Q}(\sqrt{2})$ is complete.” Is the conclusion true? Which step fails?
- Put $1/x$, $1/x^2$ and $1/10^6$ in increasing order in $\mathbb{R}(x)$.

Solution.

- Yes. Its value $t^2 - 100t = t(t - 100)$ is positive for every $t > 100$. (Or: the list $(0, -100, 1)$ has top coefficient $1 > 0$, and [Lemma 6.4.1](#) applies with $T = 101$.)
- The conclusion is false ([Proposition 6.4.6](#)). The illegal step is the last: completeness of the target says nothing about suprema in the source. A set $A \subseteq \mathbb{Q}(\sqrt{2})$ that is bounded above has a supremum in $\mathbb{R}$, but it may lie outside $\mathbb{Q}(\sqrt{2})$: for $A = \{y \in \mathbb{Q}(\sqrt{2}) : y \geq 0, y^2 < 3\}$ it is $\sqrt{3}$, which is not in $\mathbb{Q}(\sqrt{2})$ (the remark after [Proposition 6.4.6](#)).

(c) $0 < 1/x^2 < 1/x < 1/10^6$. The value of $1/x - 1/x^2$ is $(t-1)/t^2 > 0$ for $t > 1$, and that of $1/10^6 - 1/x$ is $1/10^6 - 1/t > 0$ for $t > 10^6$.

6.4.6.2 B. Practice

Exercise. B1

Prove that multiplication in $\mathbb{R}(x)$ is associative and that the positive set P is closed under sums. In each, choose representatives, name a threshold T beyond which every denominator involved is non-zero (and, for P , every value involved is positive), compute the values of both sides at $t > T$ with the pointwise rule, and say which fact about $\mathbb{R}$ makes them equal or positive.

Solution. Associativity. Let $f = [p_1/q_1]$, $g = [p_2/q_2]$, $h = [p_3/q_3]$, and $T := \max\{T_{q_1}, T_{q_2}, T_{q_3}\}$. For $t > T$, the denominators of all fractions involved are non-zero, and by the pointwise rule the value of $(fg)h$ is $(u(t)v(t))w(t)$ and that of $f(gh)$ is $u(t)(v(t)w(t))$, where u, v, w are the values of the three fractions. These are equal by (F5) in $\mathbb{R}$. So the two fractions produced by the formula have equal values for every $t > T$: they are equivalent, and $(fg)h = f(gh)$.

Closure of P under sums. Let $f, g \in P$: the value of f is positive for $t > T_1$ and that of g for $t > T_2$ (these thresholds may be taken $\geq T_{q_1}, T_{q_2}$). For $t > \max\{T_1, T_2\}$, the value of $f + g$ is $u(t) + v(t) > 0$ by (O3) in $\mathbb{R}$ (Proposition 2.3.5 (b)). So $f + g \in P$. The finiteness of the list of thresholds is what lets us take a maximum.

Exercise. B2

Show that no rational number squares to 5 or to 10. Then show that 5 has no square root in $\mathbb{Q}(\sqrt{2})$.

Solution. Since $2^2 = 4 < 5 < 9 = 3^2$ and $3^2 = 9 < 10 < 16 = 4^2$, the claim stated with Proposition 6.4.6, with $(n, k) = (5, 2)$ and $(10, 3)$, shows that neither is a rational square. (The descent there checks $u'^2 - nv'^2 = (k^2 - n)(u^2 - nv^2)$ for these values too; the identity holds for all n, k .)

Now let $c = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$ and $c^2 = 5$. By the product formula, $(a^2 + 2b^2) + 2ab\sqrt{2} = 5 + 0\sqrt{2}$, so by unique representation (Proposition 6.4.5 (a)), $2ab = 0$ and $a^2 + 2b^2 = 5$. If $b = 0$, then $a^2 = 5$; if $a = 0$, then $2b^2 = 5$, so $(2b)^2 = 10$. Both are excluded. Hence 5 has no square root in $\mathbb{Q}(\sqrt{2})$.

Exercise. B3

Show that $x^3 + 1$ is positive in $\mathbb{R}(x)$ but is not a square there.

Hint: the argument of Example (A Positive Element That Is Not a Square), with $t^3 + 1$ in place of t .

Solution. Positive. $t \mapsto t^3 + 1$ is the function of $(1, 0, 0, 1)$, with top coefficient $1 > 0$; by [Lemma 6.4.1](#) its value is positive for all large t .

Not a square. Suppose $x^3 + 1 = [p/q]^2$. Then $h(t) := (t^3 + 1)q(t)^2 - p(t)^2 = 0$ for all large t , and h is the function of a list by [Lemma 6.4.2](#) (a), (b). Cut q after its last non-zero entry b_e . By (b), $(t^3 + 1) \cdot q^2$ has a list with top degree $3 + 2e = 2e + 3$, odd, and top coefficient $1 \cdot b_e^2 \neq 0$. If a list of p is all zeros, then $(t^3 + 1)q(t)^2 = 0$ for all large t , and (c) contradicts $b_e^2 \neq 0$. Otherwise cut p after its last non-zero entry a_d ; then $-p^2$ has a list with top degree $2d$, even, and top coefficient $-a_d^2 \neq 0$. Since $2d \neq 2e + 3$ (Corollary 3.1.3 (a)), the sum list for h has the non-zero entry b_e^2 or $-a_d^2$ at index $\max\{2d, 2e + 3\}$, against [Lemma 6.4.2](#) (c). So $x^3 + 1$ is not a square.

6.4.6.3 C. Going deeper

Exercise. C1: Exit check: the supremum property fails in the rational functions

Show directly from Definition 5.6.1, without Theorem 6.1.2, that $\mathbb{R}(x)$ is not complete.

Solution. Let $A := \{n \cdot 1 : n \in \mathbb{N}\} \subseteq \mathbb{R}(x)$. It is non-empty ($0 \cdot 1 \in A$), and it is bounded above by x : the value of $x - n$ is $t - n > 0$ for $t > n$ ([Proposition 6.4.4](#)).

Suppose $s \in \mathbb{R}(x)$ is a supremum of A . For every $n \in \mathbb{N}$, $n + 1 \in \mathbb{N}$, so $(n + 1) \cdot 1 \leq s$ by (S1), that is, $n \cdot 1 + 1 \leq s$ (Definition 4.2.1 (a)), and $n \cdot 1 \leq s - 1$. So $s - 1$ is an upper bound of A , and (S2) gives $s \leq s - 1$, that is, $1 \leq 0$, which is false in an ordered field (Proposition 2.3.5 (e)). So A has no supremum, and $\mathbb{R}(x)$ is not complete.

Marking scheme. (10 points) - 2: exhibits a non-empty set bounded above, with the bound verified (here x , by a threshold for the value of $x - n$, or by [Lemma 6.4.1](#)). - 3: supposes a supremum s , and uses (S1) on $(n + 1) \cdot 1$. - 3: plays leastness against $s - 1$: either shows that $s - 1$ is an upper bound, from $(n + 1) \cdot 1 \leq s \Rightarrow n \cdot 1 \leq s - 1$ for every n , or notes $s - 1 < s$ so that (S2) gives n with $n \cdot 1 > s - 1$. - 2: reaches the contradiction (with (S2), or with (S1) via $(n + 1) \cdot 1 > s$), concluding that no supremum exists. Fatal errors (0 for the step): proving only “not Archimedean” and stopping; treating x as a real number (for instance, “take $n > x$ ”).

Exercise. C2: A complete ordered field is uncountable

Let F be a complete ordered field. Write 3^n for the power $(3 \cdot 1_F)^n$ of Definition 4.2.1. For $s = (s_n)_{n \in \mathbb{N}} \in \{0, 1\}^{\mathbb{N}}$, let

$$S_k(s) := \sum_{n=0}^k \frac{2s_n}{3^{n+1}} \quad (k \in \mathbb{N}), \quad \Phi(s) := \sup_{k \in \mathbb{N}} S_k(s).$$

- (a) Show that $\Phi(s)$ exists.
- (b) Show that $\Phi: \{0, 1\}^{\mathbb{N}} \rightarrow F$ is injective.
- (c) Deduce that F is uncountable (Sets, Relations, and Cardinality, Theorem 3.4.1).

Solution (Hint 1). Think of ternary expansions that use only the digits 0 and 2. For (a), find a single upper bound for all $S_k(s)$ by comparing with $s_n = 1$ for every n .

Solution (Hint 2). For (b), let j be the least index where s and s' differ (it exists by least elements), with $s_j = 1$ and $s'_j = 0$, and put $c := S_{j-1}(s) = S_{j-1}(s')$ (with $c := 0$ if $j = 0$).

Solution. Tail bound. For $k \leq m$, by induction on m (Logic and Proof, Axiom 4.2.1), exactly as in Eq. 5.6.3 but in F :

$$0 \leq S_m(s) - S_k(s) \leq \frac{1}{3^{k+1}} - \frac{1}{3^{m+1}},$$

since passing from m to $m+1$ adds $2s_{m+1}/3^{m+2} \in [0, 2/3^{m+2}]$, and $-1/3^{m+1} + 2/3^{m+2} = -1/3^{m+2}$. In particular $S_k(s)$ is non-decreasing in k .

- (a) The set $\{S_k(s) : k \in \mathbb{N}\}$ is non-empty, and bounded above by 1: $S_k(s) \leq S_0(s) + 1/3 - 1/3^{k+1} \leq 2/3 + 1/3 = 1$ by the tail bound with $k = 0$. Since F is complete, $\Phi(s)$ exists.
- (b) Let $s \neq s'$. The set of indices where they differ is a non-empty subset of $\mathbb{N}$, so it has a least element j (Proposition 2.3.6); say $s_j = 1$ and $s'_j = 0$. Let $c := S_{j-1}(s) = S_{j-1}(s')$, the sums agreeing up to $j-1$ (with $c := 0$ if $j = 0$). Then $\Phi(s) \geq S_j(s) = c + 2/3^{j+1}$ by (S1). For $k \geq j$, the tail bound gives $S_k(s') \leq S_j(s') + 1/3^{j+1} = c + 1/3^{j+1}$; for $k < j$, $S_k(s') \leq S_j(s') = c$. So $c + 1/3^{j+1}$ is an upper bound of the $S_k(s')$, and $\Phi(s') \leq c + 1/3^{j+1}$ by (S2). Hence $\Phi(s) - \Phi(s') \geq 1/3^{j+1} > 0$, and $\Phi(s) \neq \Phi(s')$.
- (c) If F were countable, there would be an injection $g: F \rightarrow \mathbb{N}$ (Sets, Relations, and Cardinality, Theorem 3.2.2), and $g \circ \Phi$ would be an injection $\{0, 1\}^{\mathbb{N}} \rightarrow \mathbb{N}$ (Sets, Relations, and Cardinality, Theorem 1.4.4), making $\{0, 1\}^{\mathbb{N}}$ countable, against Sets, Relations, and Cardinality, Theorem 3.4.1.

Alternatively, by Corollary 6.3.2 there is a bijection $F \rightarrow \mathbb{R}$, and $\mathbb{R}$ is uncountable by Exercise (R3). The route above shows that uncountability follows from the supremum property directly, with no construction behind it.

Marking scheme. (10 points) - 2: (a), a common upper bound for the partial sums, and completeness invoked for the supremum. - 2: the tail bound, by induction, in F . - 4: (b), the first differing index j by least elements, the lower bound $c + 2/3^{j+1}$ for $\Phi(s)$ by (S1), and the upper bound $c + 1/3^{j+1}$ for $\Phi(s')$ by (S2). - 2: (c), the composite injection and the uncountability of $\{0, 1\}^{\mathbb{N}}$. The second route, by Corollary 6.3.2 and the uncountability of $\mathbb{R}$, also earns these 2 points; (a) and (b) are still marked as above. Fatal errors (0 for the step): treating $\Phi(s)$ as an infinite sum computed term by term; using decimal or ternary expansions of real numbers as known facts.

Exercise. C3: Increasing and bounded

Let F be a complete ordered field and $(a_n)_{n \in \mathbb{N}}$ a sequence in F with $a_n \leq a_{n+1}$ for every n , whose set of values is bounded above. Prove that $a_n \rightarrow s$ in F (Definition 4.3.2), where s is the supremum of the set of values. Here is the start of a proof. *Name the move, then complete it.*

“Let $s := \sup\{a_n : n \in \mathbb{N}\}$, which exists because the set is non-empty and bounded above and F is complete. Let $\varepsilon \in F_{>0}$”

Solution. The move is **construct a point as a supremum, and use its leastness through “ $s - \varepsilon$ is not an upper bound”**, which hands us a witness. It built square roots in Proposition 6.1.4; here it builds a limit.

Completion. Since $s - \varepsilon < s$ and s is the least upper bound, $s - \varepsilon$ is not an upper bound of the values, so $a_N > s - \varepsilon$ for some $N \in \mathbb{N}$. For $n \geq N$, $a_N \leq a_n$, by induction on $n - N$ from $a_m \leq a_{m+1}$; and $a_n \leq s$ by (S1). So

$$s - \varepsilon < a_N \leq a_n \leq s < s + \varepsilon,$$

that is, $|a_n - s| < \varepsilon$ for every $n \geq N$ (Proposition 4.1.3 (d)). Since ε was arbitrary, $a_n \rightarrow s$. Here N depends on ε .