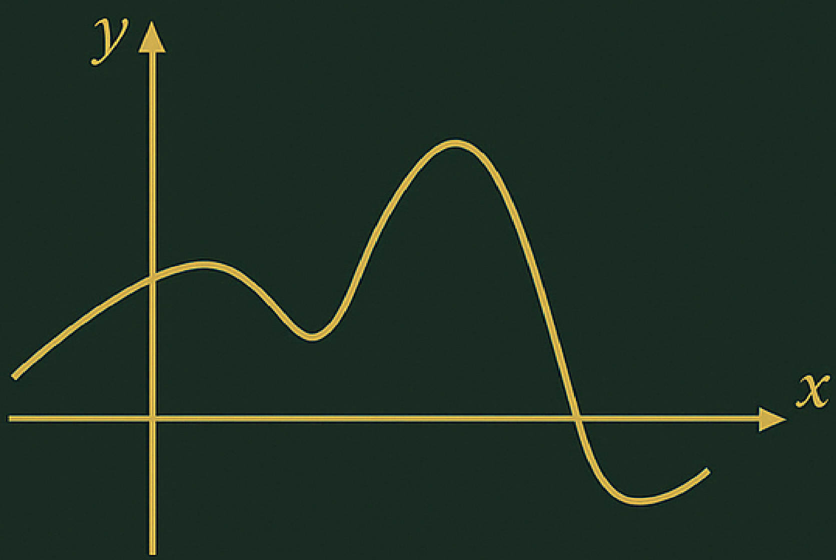
REAL ANALYSIS

A SELF-TAUGHT APPROACH



Luis Vasquez

REAL ANALYSIS

A Self-Taught Approach

Luis Vasquez

Contents

1 Introduction

1.1 Sources

The following notes are taken from the compilation of a few sources

- Zorich, V. A. (2004). Mathematical analysis I (R. Cooke, Trans.). Springer.
- MIT 18.100B Real Analysis, Spring 2025, available at the MIT OCW youtube channel

1.2 Purpose

This notes are taken in a way that is easy to understand math for myself (the author). No obscure proof or incomplete idea will be included, avoiding partial understanding of a certain topic. It also covers the need of having an easy-to-follow approach to *Real Analysis*, making it possible to read this through to revisit known topics without the need of rabbithole-ing at other sources. Since I will also be studying the course while taking this notes, the document as a whole will be written by hand without any AI slob nor blind copy/pasting, and since English is not my native language, typos may appear here and there.

*When I say **we**, it means you (the reader) and I. When I say **I/myself**, responsability only lies on me (the author).*

2 Base knowledge

2.1 What is a Field

"To verify that a set forms a field, we check that multiplication is well-defined. That is, independent of the choice of representative."

For example, for arbitrary rational numbers Q:

$$\frac{m_1}{n_1} \times \frac{p_1}{q_1}$$

And evaluate an equivalent expression with different representatives of the same numbers:

$$\frac{m_2}{n_2} \times \frac{p_2}{q_2}$$

Given that:

$$\frac{m_1}{n_1} = \frac{m_2}{n_2} \quad \text{and} \quad \frac{p_1}{q_1} = \frac{p_2}{q_2}$$

We wish to show that both products coincide. To review this, we start from the tautology (intuitive truth):

$$\frac{m_1}{n_1} = \frac{m_2}{n_2} \iff m_1 \times n_2 = m_2 \times n_1 \tag{A}$$

$$\frac{p_1}{q_1} = \frac{p_2}{q_2} \iff p_1 \times q_2 = p_2 \times q_1 \tag{B}$$

Then, operating the multiplication using both representatives:

$$\frac{m_1}{n_1} \times \frac{p_1}{q_1} = \frac{m_1 \cdot p_1}{n_1 \cdot q_1}$$
$$\frac{m_2}{n_2} \times \frac{p_2}{q_2} = \frac{m_2 \cdot p_2}{n_2 \cdot q_2}$$

Conveniently, we want to form $m_1 \times n_2$ to use the first ground truth:

$$\begin{aligned}
\frac{m_1}{n_1} \times \frac{p_1}{q_1} \times n_2 &= \frac{m_1 \cdot n_2 \cdot p_1}{n_1 \cdot q_1} \\
&= \frac{m_2 \cdot n_1 \cdot p_1}{n_1 \cdot q_1} \quad \text{(replacing using A)} \\
&= \frac{m_2 \cdot p_1}{q_1} \quad \text{(simplifying } n_1\text{)}
\end{aligned}$$

Applying the same logic for $p_1 \times q_2$ to use the second ground truth:

$$\begin{aligned}
\frac{m_1}{n_1} \times \frac{p_1}{q_1} \times n_2 \times q_2 &= \frac{m_2 \cdot p_1 \cdot q_2}{q_1} \\
&= \frac{m_2 \cdot p_2 \cdot q_1}{q_1} \quad \text{(replacing using B)} \\
&= m_2 \cdot p_2 \quad \text{(simplifying } q_1\text{)}
\end{aligned}$$

Finally, rearranging:

$$\begin{aligned}
\frac{m_1}{n_1} \times \frac{p_1}{q_1} \times n_2 \times q_2 = m_2 \cdot p_2 \\
\frac{m_1}{n_1} \times \frac{p_1}{q_1} = \frac{m_2 \cdot p_2}{n_2 \cdot q_2} \\
\frac{m_1}{n_1} \times \frac{p_1}{q_1} = \frac{m_2}{n_2} \times \frac{p_2}{q_2} \qquad \square
\end{aligned}$$

While not a rigorous proof, this gives us a first step to go from the intuition of a solution (particularly for $\mathbb{Q}$) to a more formal procedure based on the real definition of a field.

2.2 Formal definition

Definition
Field
2.1

A **field** $\mathbb{F}$ is a set with two operations: addition ($\oplus$) and multiplication ($\otimes$), with the following properties:

- $x, y \in \mathbb{F} \implies x \oplus y \in \mathbb{F}$
- $x, y \in \mathbb{F} \implies x \oplus y = y \oplus x$
- $x, y, z \in \mathbb{F} \implies (x \oplus y) \oplus z = x \oplus (y \oplus z)$
- $\exists\, 0 \in \mathbb{F}$ such that $\forall x \in \mathbb{F}, x \oplus 0 = x$
- $\forall x \in \mathbb{F}, \exists\, (-x) \in \mathbb{F}$ such that $x \oplus (-x) = 0$
- $x, y \in \mathbb{F} \implies x \otimes y \in \mathbb{F}$
- $x, y \in \mathbb{F} \implies x \otimes y = y \otimes x$
- $x, y, z \in \mathbb{F} \implies (x \otimes y) \otimes z = x \otimes (y \otimes z)$
- $\exists\, 1 \in \mathbb{F}$ such that $\forall x \in \mathbb{F}, x \otimes 1 = x$
- $\forall x \in \mathbb{F} \setminus \{0\}, \exists\, x^{-1} \in \mathbb{F}$ such that $x \otimes x^{-1} = 1$

The first five properties correspond to the addition operation, and the last five to the multiplication operation. In order to relate both sets of properties, the following axiom is stated:

Axiom
Distributive law
2.1

Let $x, y, z \in \mathbb{F}$. Then

$$x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z$$

Theorem
Zero uniqueness
2.1

For any field $\mathbb{F}$, there exists only one zero element.

Proof Assume 0_1 and 0_2 are zero elements in $\mathbb{F}$. Then

$$\forall x \in \mathbb{F}: \quad \begin{cases} 0_1 + x = x & \text{(A)} \\ 0_2 + x = x & \text{(B)} \end{cases}$$

Setting $x = 0_2$ in A, and be $x = 0_1$ in B:

$$x = 0_2 \implies \text{(A)}: \quad 0_1 + 0_2 = 0_2 \tag{C}$$
$$x = 0_1 \implies \text{(B)}: \quad 0_2 + 0_1 = 0_1 \tag{D}$$

From (C) and commutativity:

$$0_2 + 0_1 = 0_2$$

Comparing this result with (D):

$$\begin{aligned} 0_2 + 0_1 = 0_2 \quad \text{and} \quad 0_2 + 0_1 = 0_1 \\ \implies 0_1 = 0_2 \end{aligned}$$

□

2.3 Order

Definition Ordered sets 2.2

A set S is **ordered** when it has an ordering "$<$" such that for all $x, y \in S$, exactly one of the following properties holds:

1. $x = y$
2. $x < y$
3. $y < x$

Definition Ordered fields 2.3

A field $\mathbb{F}$ is **ordered** if it is also an ordered set. As a consequence, the following properties apply:

- $x, y \in \mathbb{F}, x < y \implies \forall z \in \mathbb{F}, x \oplus z < y \oplus z$
- $x, y \in \mathbb{F}, 0 < x, y \implies 0 < x \otimes y$

Theorem 2.2

Given $\mathbb{F}$ an ordered field. If $x < y$ and $0 < z$, then $x \otimes z < y \otimes z$.

Proof

We proceed by contradiction. Assume instead that:

$$x \otimes z \geq y \otimes z$$

Then adding $(-x \otimes z)$ on both sides, we maintain the ordering of the expression:

$$\begin{aligned} x \otimes z \oplus (-x \otimes z) &\geq y \otimes z \oplus (-x \otimes z) \\ 0 &\geq y \otimes z \oplus (-x \otimes z) \end{aligned}$$

Now, using Axiom 2.1, we get:

$$0 \geq z \otimes (y \oplus (-x))$$

From the initial conditions, $x < y$ implies $y \oplus (-x) > 0$. Since we also have $z > 0$, we would expect the product of these two to be > 0 by Definition 2.3 (second property). Hence:

$$0 \geq z \otimes (y \oplus (-x)) \quad \text{and} \quad 0 < z \otimes (y \oplus (-x))$$

This is a contradiction. $\square$

From this point forward, for better readability, $+$ and $\cdot$ (or $\times$) will be used instead of $\oplus$ and $\otimes$. They will still represent the abstraction of a field's addition and multiplication operations, without necessarily being the familiar operations we might expect them to be.

2.4 Completeness

Definition Bounds 2.4 — A set $X \subset \mathbb{F}$ ($\mathbb{F}$ ordered field) is said to be *bounded above* (or respectively, *bounded below*) if $\exists\ c \in \mathbb{F}$ such that $\forall a \in \mathbb{F}, a \leq x$ (or respectively, $x \leq a$). c is called upper (or respectively lower) bound of X.

Definition 2.5 — A set that is both bounded above and below, is called *bounded.*

Definition 2.6 — An element $a \in X$ is called the *largest* element of X if $\forall x \in X, x \leq a$. Respectively, $a \in X$ is called the *smallest* element of X if $\forall x \in X, a \leq x$. Simplifying the notation:

$$(a = maxX) := (a \in X \wedge \forall x \in X, x \leq a)$$
$$(a = minX) := (a \in X \wedge \forall x \in X, a \leq x)$$

These read as *maximal* and *minimal* of X. Now, given this definition, is important to notice that not every set, not even every bounded set, has a maximal or minimal element. For example:

$$X = \{x \in \mathbb{F} \mid 0 \leq x < 1\}$$

Only has a minimal element (0), but no maximal element, since $1 \notin X$

Definition Least Upper Bound 2.7 — The smallest $s \in X \subset \mathbb{F}$ that bounds X from above is called the *least upper bound* of X, and denoted $\sup X$ (read "the supremum of X")

$$(s = \sup X) := \forall x \in X((x \leq s) \wedge (\forall s' < s\ \exists x' \in X(s' < x'))$$

Let us unpack this definition:

- $\forall x \in X$: The following definition applies to every element in X.
- $(x \leq s)$: Given that s is an upper bound for X...
- $(\forall s' < s)\exists x' \in X(s' < x')$:
  - $(\forall s' < s)$: Considering any arbitrary s' smaller than our upper bound s
  - $\exists x' \in X$: There will be an element x' in X, so that...
  - $(s' < x')$: It is larger than the s', showing that s' is not an upper bound.

So in summary, s is $\sup X$ if and only if, s is an upper bound, and no smaller number s' is an upper bound of X, because we can find an x' that is not bounded by it.

Definition
Greatest Lower Bound
2.8

Similarly, the greatest $i \in X \subset \mathbb{F}$ that bounds X below is called the *greatest lower bound of* X, and denoted $\inf X$ (read "the infimum of X")

$$(i = \inf X) := \forall x \in X((i \leq x) \land (\forall i' < i \; \exists x' \in X(x' < i'))$$

Thus, we have now the following definitions:

$$\sup X := \min\{c \in \mathbb{F} | \forall x \in X(x \leq c)\}$$
$$\inf X := \max\{c \in \mathbb{F} | \forall x \in X(c \leq x)\}$$

It is important to note that the supremum and infimum of a set, as defined above, may not exist in an arbitrary ordered field $\mathbb{F}$. The definitions above specify what $\sup X$ and $\inf X$ mean *if they exist*, but they do not guarantee existence. We will address this issue shortly.

Theorem
Uniqueness of Supremum
2.3

Let $X \subset \mathbb{F}$ be a nonempty set in an ordered field $\mathbb{F}$. If X has a supremum, then this supremum is unique.

Proof

Suppose s_1 and s_2 are both suprema of X. We will show that $s_1 = s_2$.
Since $s_1 = \sup X$, we know that s_1 is an upper bound of X. Since $s_2 = \sup X$, we know that s_2 is the *least* upper bound of X. Therefore:

$$s_2 \leq s_1$$

By the same reasoning (swapping the roles of s_1 and s_2), since s_2 is an upper bound and s_1 is the least upper bound:

$$s_1 \leq s_2$$

By the antisymmetry property of order in $\mathbb{F}$, we have $s_1 \leq s_2$ and $s_2 \leq s_1$, which implies:

$$s_1 = s_2$$

Therefore, the supremum is unique. $\square$

The proof for the uniqueness of the infimum is analogous.

Example 2.1

Consider the ordered field $\mathbb{Q}$ of rational numbers, and let:

$$S = \{x \in \mathbb{Q} \mid x^2 < 2\}$$

The set S is nonempty (for instance, $1 \in S$) and bounded above (for instance, $2 \in \mathbb{F}$ is an upper bound). However, S has no supremum in $\mathbb{Q}$: if such a supremum existed, it would equal $\sqrt{2} \notin \mathbb{Q}$, so S has no least upper bound within the rational numbers. This shows that not every ordered field has the property that bounded sets possess suprema.

Definition Complete Ordered Field 2.9

An ordered field $\mathbb{F}$ is called *complete* if every nonempty subset of $\mathbb{F}$ that is bounded above has a supremum in $\mathbb{F}$.

Proposition 2.1

If $\mathbb{F}$ is a complete ordered field, then every nonempty subset of $\mathbb{F}$ that is bounded below has an infimum in $\mathbb{F}$.

Proof Let $X \subset \mathbb{F}$ be nonempty and bounded below. Define:

$$X' = \{-x \mid x \in X\}$$

1. X' is nonempty and bounded above
Since X is nonempty, $\exists x_0 \in X \Rightarrow -x_0 \in X'$ by definition of X'. Thus $X' \neq \emptyset$.
Now, X is bounded below by the proposition, so there exists $c \in \mathbb{F}$ such that:

$$\begin{aligned} &\forall x \in X, \quad c \leq x \\ &\forall x \in X, \quad -x \leq -c \end{aligned}$$

Since $-x \in X'$ and $-c \in \mathbb{F}$, we can be sure that X' is bounded above in $\mathbb{F}$.
Considering $\mathbb{F}$ is complete, and we proved X' is nonempty and bounded above, X' has a supremum in $\mathbb{F}$.

2. $-s$ is a lower bound for X.
Let $s = \sup X'$ and $x \in X$ be arbitrary. Then $-x \in X'$ by definition of X'. Since s is an upper bound for X':

$$\begin{aligned} \forall -x \in X', &\quad -x \leq s \\ \Rightarrow &\quad -s \leq x \end{aligned}$$

Showing that $-s$ is a lower bound for X.

3: $-s$ is the greatest lower bound for X.
Let $\ell \in \mathbb{F}$ be any lower bound for X.
Since ℓ is a lower bound for X:

$$\begin{aligned} \forall x \in X, &\quad \ell \leq x \\ \Rightarrow &\quad -x \leq -\ell \end{aligned}$$

Meaning that $-\ell$ is an upper bound for any $-x \in X'$. Since $s = \sup X'$, we have:

$$\begin{aligned} &s \leq -\ell \\ \Rightarrow\ &\ell \leq -s \end{aligned}$$

Showing that $-s$ is greater than or equal to every lower bound of X. Therefore, $-s = \inf X$. □

Theorem
Least Upper Bound Principle
2.4

Let $\mathbb{F}$ be a complete ordered field. Every nonempty subset of $\mathbb{F}$ that is bounded above has a unique least upper bound in $\mathbb{F}$.

Proof

Let $X \subset \mathbb{F}$ be nonempty and bounded above.
Existence: Since $\mathbb{F}$ is complete, by definition of completeness, X has a supremum in $\mathbb{F}$.
Uniqueness: By the Uniqueness of Supremum theorem, this supremum is unique.
Therefore, X has a unique least upper bound. $\square$

2.5 Archimedean property

Now that we achieved completeness on an ordered field, we can now extend the definitions and properties into a theorem/property that uses the result from the *Least Upper Bound principle* (Theorem 2.4).

Theorem
2.5

Let $\mathbb{F}$ be a complete ordered field, then

$$\forall x \in \mathbb{F}, \exists\ n \in \mathbb{N} \subset \mathbb{F} : n > x$$

Proof We first define the subset $\mathbb{N} \subset \mathbb{F}$ **inductively**, to work with a generalized version of the set of "natural numbers"

1. $1_{\mathbb{F}}$ is the multiplicative identity in $\mathbb{F}$
2. $n + 1_{\mathbb{F}} \in \mathbb{N}, \forall n \in \mathbb{N}$ defines the induction step over $\mathbb{N}$, using the addition operation from the field $\mathbb{F}$

We proceed by contradiction. Suppose $\exists x \in \mathbb{F}, \forall n \in \mathbb{N}$:

$$n \leq x$$

Meaning that $\mathbb{N}$ is bounded above. Now, since $\mathbb{N}$ is not empty, and is bounded by an element of the (complete ordered) field that contains it ($x \in \mathbb{F}$), then by *L.U.B. principle* (Theorem 2.4), $\mathbb{N}$ must have a supremum.

Let $s := \sup \mathbb{N} \in \mathbb{F}$ be that supremum of $\mathbb{N}$. Then, since s is the least upper bound, any element that is less than s will no longer be an upper bound for $\mathbb{N}$. Conveniently we take $s - 1_{\mathbb{F}}$:

$$\begin{aligned} \exists n_0 \in \mathbb{N} : & s - 1_{\mathbb{F}} < n_0 \\ & \Rightarrow s < n_0 + 1_{\mathbb{F}} \end{aligned}$$

But by our inductive definition of $\mathbb{N} : (n_0 + 1_{\mathbb{F}}) \in \mathbb{N}$. So we found out that s ($\sup \mathbb{N}$) fails to be an upper bound for an element in $\mathbb{N}$.

Therefore, our original assumption of x must be wrong. □

Now, is important to notice that $\mathbb{F}$ implies an archimedien field, but the opposite won't necessarily be true.

Example 2.2 Using an Archimedean field, that is not complete, let us take $\mathbb{F} = \mathbb{Q}$

$$x \in \mathbb{Q} \wedge n \in \mathbb{N} \subset \mathbb{Q}$$

It is true that, for any x there is a natural number n so that

$$n > x$$

But invoking the previous example (Example 2.1) we can take a subset of $\mathbb{Q}$ that is not bounded in $\mathbb{Q}$, failing to properly form a complete set.

Closing this chapter, let us emphazise the fact that the construction of $\mathbb{N} \subset \mathbb{F}$ by induction was crucial to generalize the property for any complete ordered field. Next we will explain why this wasn't necessary at all.

3 $\mathbb{R}$ as the complete ordered field

3.1 $\mathbb{F}$ is $\mathbb{R}$

Turns out there is a reason why it is called ***Real*** Analysis. So far we have worked over a generic *Complete Ordered Field* $\mathbb{F}$, that was also an *Archimedean* following the expected properties. We have finally reached the point were we can state that **any** set that manages to follow all these properties is actually identical to the set of real numbers $\mathbb{R}$. In fact, $\mathbb{R}$ is the only set that accomplishes this.

Most *Real Analysis* courses won't go into proving this, but as I already mentioned in the first chapter, I want to cover all doubts and missing point existent during a course like this.

We will go through the initial proofs needed to understand the main one. At the beginning its possible that some of them look unecessary or trivial, but I don't want to assume that much. Better to be safe than sorry.

3.1.1 Isomorphism

Our starting point will be defining what it means to have "equal fields".

Definition
Field homomorphism 3.1

Let F, F' fields. A function $\phi : F \to F'$ is a homomorphism between F and F' iif. it preserves the defined operations in both fields:

$$\phi(x + y) = \phi(x) + \phi(y), \forall x, y \in F$$
$$\phi(x.y) = \phi(x).\phi(y), \forall x, y \in F$$

Definition
Field isomorphism 3.2

Let F, F' fields. A function $\phi : F \to F'$ is a isomorphism iif. it is a homomorphism and also a bijection

Lemma Injectivity by order preservation 3.1

Let F, F' fields, $\phi : F \to F'$. If ϕ preserves order from $\mathbb{F}$:

$$x < y \Rightarrow \phi(x) < \phi(y), x, y \in F$$

Then ϕ is injective.

Proof To establish injectivity, we must show that for any two identical images of the function ϕ, we get that their arguments were the same, guaranteeing the uniqueness of the image:
Let $x, y \in \mathbb{F}$ so that

$$\phi(x) = \phi(y)$$

By tricotomy of F:
Case 1: $x < y$:

$$\to \phi(x) < \phi(y)(\to\leftarrow)$$

Case 2: $y < x$:

$$\to \phi(y) < \phi(x)(\to\leftarrow)$$

$$\Rightarrow x = y$$

Then, ϕ is injective. □

Lemma Surjectivity by construction 3.2

Let F, F' fields, $\phi : F \to F'$. Define:

$$\mathrm{Im}_F := \{\phi(x), x \in F\}$$

Then, the bounded function $\phi' : F \to \mathrm{Im}_F$ is surjective

Proof To prove surjectivity, we need to show that every element in $y \in \text{Im}_F$ has an $x \in F$ such that $\phi'(x) = y$. Using the definition of our constructed set:

$$\begin{aligned} \forall y \in \text{Im}_F &\Leftrightarrow y \in \{\phi(x), x \in F\} \\ &\Rightarrow \exists x \in F / \forall y \in \text{Im}_F : y = \phi'(x) \end{aligned}$$

Finally proving that for any image of $\phi' \in \text{Im}_F$ we will have a preimage $x \in F$. Then ϕ' is surjective. □

On this first part, this surjectiveness by construction might be the bit that doesn't quite seem correct. Isn't it trivial to have surjectiveness if we grab the method ϕ and limit it to its image ϕ'?

The key here is that we first defined the set of images Im_F, and *then* proved the surjectiveness in it. The lemma confirms that the set we defined was *just right*. Not so big to leave some elements unreached, and not too small to make undefined preimages at some spots.

3.2 Sets construction

Now, to make it reasonable for a complete ordered field $\mathbb{F}$ to be isomorphic to our known $\mathbb{R}$, we need to start shaping it using the parts that make it up. Think of $\mathbb{R}$ as the joint set of irrational and rational numbers, which contain the other types of number as well.

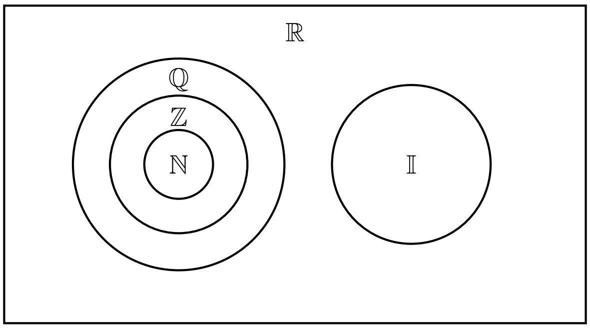


Figure 1: Hierarchy of number sets: Natural numbers ($\mathbb{N}$), Integers ($\mathbb{Z}$), Rationals ($\mathbb{Q}$), Irrationals ($\mathbb{I}$), and Real numbers ($\mathbb{R}$).

From this idea, we need to build $\mathbb{N}_\mathbb{F}$, $\mathbb{Z}_\mathbb{F}$, $\mathbb{Q}_\mathbb{F}$ and $\mathbb{I}_\mathbb{F}$ to finall get this $\mathbb{F}$ we want. This will all make sense in the last part of the process, and it is true that it will be a bit of a hussle to construct all of it (specially $\mathbb{I}_\mathbb{F}$ from $\mathbb{Q}_\mathbb{F}$), but we need to go step by step.

Definition
$\mathbb{N}_{\mathbb{F}}$ by induction
3.3

Let $\mathbb{F}$ be *the* complete ordered field. Using $1_{\mathbb{F}}$: multiplicative neutral of $\mathbb{F}$, we declare the following element contruction:

$$
\begin{aligned}
1_{\mathbb{F}} &:= 1_{\mathbb{F}} \\
2_{\mathbb{F}} &:= 1_{\mathbb{F}} + 1_{\mathbb{F}} \\
3_{\mathbb{F}} &:= 1_{\mathbb{F}} + 1_{\mathbb{F}} + 1_{\mathbb{F}} \\
&\vdots \\
n_{\mathbb{F}} &:= \sum_{1}^{n} 1_F
\end{aligned}
$$

Finally, we define the set:

$$\mathbb{N}_{\mathbb{F}} := \{1_{\mathbb{F}}, 2_{\mathbb{F}}, 3_{\mathbb{F}}, \dots\} = \{n_{\mathbb{F}} : n \in \mathbb{N}\}$$

Definition
$\mathbb{Z}_{\mathbb{F}}$ by extension
3.4

Within field $\mathbb{F}$, let the following:

1. $0_{\mathbb{F}}$: Additive identity
2. $-x$: Additive inverse

We define the set:

$$\mathbb{Z}_{\mathbb{F}} = \{0_{\mathbb{F}}\} \cup \mathbb{N}_{\mathbb{F}} \cup \{-x_{\mathbb{F}}, \forall n_{\mathbb{F}} \in N_{\mathbb{F}}\}$$

Definition
$\mathbb{Q}_\mathbb{F}$ by operation
3.5

Within field $\mathbb{F}$, let the following:

1. $a \in \mathbb{F}$
2. b^{-1} (multiplicative inverse of b) $\in \mathbb{F}$

we define the set:

$$\mathbb{Q}_\mathbb{F} := \{\frac{a}{b} : a \in \mathbb{Z}_\mathbb{F}, b \in \mathbb{N}_\mathbb{F}\}$$

Starting similarly to Theorem 2.5 (Archimedean property) we use the inductive approach to reach $\mathbb{N}_\mathbb{F}$. Fancy but not complicated at all. Later, we just extend integers in $\mathbb{F}$ to build by $\mathbb{Z}_\mathbb{F}$ to conclude defining $\mathbb{Q}_\mathbb{F}$ with the result of operating arbitrary elements $a, b \in \mathbb{F}$ as $a.b^{-1}$.

Notice how we only used existent elements from $\mathbb{F}$ computed using the field's operations and nothing else. Is important to mention that you as the reader don't know yet the usage of these new sets, although we could make a good guess.

Now comes the tricky part for us. One could think that the next steps involve 1. to prove that the irrational (in $\mathbb{F}$) is in fact buildable from $\mathbb{Q}_\mathbb{F}$, and 2. to prove that there is a isomorphism between this result and the $\mathbb{R}$ we know.

That won't be the case. If we would go down that path, we would just be creating an arbitrary function Φ that maps a generic $\mathbb{F}$ with $\mathbb{R}$ perfectly, losing all progress we made constructing these specific sets one by one (for a reason). The real strategy here is to first prove that Φ exists and *then* to try to extend this function to make it follow all expected properties in the irrationals. Buckle up.

3.3 Isomorphism in $\mathbb{Q}s$

Definition
ϕ function
3.6

Let $\phi : \mathbb{Q}_\mathbb{F} \to \mathbb{Q}$ defined as:

$$\phi(\frac{m}{n}) := \frac{m_\mathbb{F}}{n_\mathbb{F}}$$

Where:

- $m, n \in \mathbb{Q}$ $(m \in \mathbb{Z}, n \in \mathbb{Z}^+)$
- $m_\mathbb{F}, n_\mathbb{F} \in \mathbb{Q}_\mathbb{F}$

Lemma 3.3 $\phi : \mathbb{Q}_{\mathbb{F}} \to \mathbb{Q}$

$$\phi(\frac{m}{n}) := \frac{m_{\mathbb{F}}}{n_{\mathbb{F}}}$$

is an homomorphism

Proof For $m_1/n_1, m_2/n_2 \in \mathbb{Q}$

1. $\phi(x + y) = \phi(x) + \phi(y)$

$$\begin{aligned}\phi(m_1/n_1 + m_2/n_2) &= \phi(\frac{m_1.n_2 + m_2.n_1}{n_1.n_2}) \\ &= \frac{(m_1.n_2 + m_2.n_1)_{\mathbb{F}}}{(n_1.n_2)_{\mathbb{F}}} \\ &= \frac{(m_1.n_2)_{\mathbb{F}} + (m_2.n_1)_{\mathbb{F}}}{(n_1)_{\mathbb{F}}.(n_2)_{\mathbb{F}}} \\ &= \frac{(m_1)_{\mathbb{F}}.(n_2)_{\mathbb{F}} + (m_2)_{\mathbb{F}}.(n_1)_{\mathbb{F}}}{(n_1)_{\mathbb{F}}.(n_2)_{\mathbb{F}}} \\ &= \frac{(m_1)_{\mathbb{F}}}{(n_1)_{\mathbb{F}}} + \frac{(m_2)_{\mathbb{F}}}{(n_2)_{\mathbb{F}}}\end{aligned}$$

$$\phi(m_1/n_1 + m_2/n_2) = \phi(m_1/n_1) + \phi(m_2/n_2)$$

2. $\phi(x.y) = \phi(x).\phi(y)$

$$\begin{aligned}\phi(m_1/n_1.m_2/n_2) &= \phi(\frac{m_1.m_2}{n_1.n_2}) \\ &= \frac{(m_1.m_2)_{\mathbb{F}}}{(n_1.n_2)_{\mathbb{F}}} \\ &= \frac{(m_1)_{\mathbb{F}}.(m_2)_{\mathbb{F}}}{(n_1)_{\mathbb{F}}.(n_2)_{\mathbb{F}}} \\ &= \frac{(m_1)_{\mathbb{F}}}{(n_1)_{\mathbb{F}}}.\frac{(m_2)_{\mathbb{F}}}{(n_2)_{\mathbb{F}}}\end{aligned}$$

$$\phi(m_1/n_1.m_2/n_2) = \phi(m_1/n_1).\phi(m_2/n_2)$$

Finally, ϕ is an homomorphism. □

Now comes the monster. In order to get the isomorphism, we need to make sure ϕ preserves order to prove injectivity by Lemma 3.1, and this step alone takes several previous lemmas to cover it fully, and of course we will see them all. Just remember we are having fun.

Lemma Ordering in $\mathbb{N}_{\mathbb{F}}$ 3.4

For $n, k \in \mathbb{N}, n_{\mathbb{F}}, k_{\mathbb{F}} \in \mathbb{N}_{\mathbb{F}}$

1. If $n < k \to n_{\mathbb{F}} < k_{\mathbb{F}}$
2. If $n = k \to n_{\mathbb{F}} = k_{\mathbb{F}}$
3. If $n > k \to n_{\mathbb{F}} > k_{\mathbb{F}}$

Proof

1. $n = k \to n_{\mathbb{F}} = k_{\mathbb{F}}$

$$n_{\mathbb{F}} := \sum_{1}^{n} 1_F = \sum_{1}^{k} 1_F = n_{\mathbb{F}}$$

2. $n < k \to n_{\mathbb{F}} < k_{\mathbb{F}}$

$$n < k \Leftrightarrow \exists p \in \mathbb{N} : n + p = k$$

Now, $k_{\mathbb{F}}$ can be expressed as:

$$k_{\mathbb{F}} := \sum_{1}^{k} 1_F = \sum_{1}^{n} 1_F + \sum_{1}^{p} 1_F = n_{\mathbb{F}} + p_{\mathbb{F}}$$

Since $p > 1$, using order preservation in addition for fields (Definition 2.3) we have:

$$k_{\mathbb{F}} = n_{\mathbb{F}} + p_{\mathbb{F}} > n_{\mathbb{F}} + 0_{\mathbb{F}} > n_{\mathbb{F}}$$

3. $n > k \to n_{\mathbb{F}} > k_{\mathbb{F}}$

$$n > k \leftrightarrow k < n$$

From 2.

$$n_{\ltimes} > k_{\ltimes}$$

□

Lemma
Ordering in $\mathbb{Z}_\mathbb{F}$
3.5

For $n, k \in \mathbb{Z}, n_\mathbb{F}, k_\mathbb{F} \in \mathbb{Z}_\mathbb{F}$

1. If $n < k \to n_\mathbb{F} < k_\mathbb{F}$
2. If $n = k \to n_\mathbb{F} = k_\mathbb{F}$
3. If $n > k \to n_\mathbb{F} > k_\mathbb{F}$

Proof

1. $n = k \to n_\mathbb{F} = k_\mathbb{F}$
   (a) $n, k >= 0$: Same as the proof for $\mathbb{N}_\mathbb{F}$
   (b) $n, k < 0$:
   $$n = k \leftrightarrow -k = -n \to -k, -n \in \mathbb{N}$$
   We now proceed exactly as the proof for $\mathbb{N}_\mathbb{F}$
2. $n < k \to n_\mathbb{F} < k_\mathbb{F}$, similarly to $\mathbb{N}_\mathbb{F}$:
   $$n < k \Leftrightarrow \exists p \in \mathbb{N} : n + p = k$$
   (a) $n >= 0$: Since $n \in \mathbb{N} \to (n+p)_\mathbb{F} = n_\mathbb{F} + p_\mathbb{F}$
   (b) $n < 0$: Labeling $n = -t$ just to indicate it is negative by sign:
   $$\begin{aligned}&\to n = -t \leftrightarrow n_\mathbb{F} = -t_\mathbb{F} \wedge (-t) + p = k\\ &\to p = k + t\\ &\to p_\mathbb{F} = k_\mathbb{F} + t_\mathbb{F}\\ &\to p_\mathbb{F} = k_\mathbb{F} - n_\mathbb{F}\\ &\to n_\mathbb{F} + p_\mathbb{F} = k_\mathbb{F}\\ &\to n_\mathbb{F} + p_\mathbb{F} = k_\mathbb{F} = (n+p)_\mathbb{F}\end{aligned}$$
   Therefore, we prooved for any case of $n, k \in \mathbb{Z} : n < k \to n_\mathbb{F} < k_\mathbb{F}$
3. $n > k \to n_\mathbb{F} > k_\mathbb{F}$

   Labeling acrodingly: $n > k \leftrightarrow -n' > -k' \leftrightarrow n' < k' (n', k' \in \mathbb{N})$
   With this we just proceed as in 2

□

So far so "good". Now, before moving to $\mathbb{Q}$ we need an extra tool for operating multiplications in $\mathbb{Z}_\mathbb{F}$.

Lemma
Multiplication in $\mathbb{Z}_{\mathbb{F}}$
3.6

For any $n, k \in \mathbb{Z}$

$$(n.k)_{\mathbb{F}} = n_{\mathbb{F}}.k_{\mathbb{F}} \in \mathbb{F}$$

Proof

1. $n, k > 0$:

   We have:
   $$(n.k)_{\mathbb{F}} = \sum_{1}^{n.k} 1_{\mathbb{F}} = \sum_{1}^{n} \sum_{1}^{k} 1_{\mathbb{F}} = \sum_{1}^{n} k_{\mathbb{F}} = n_{\mathbb{F}}.k_{\mathbb{F}}$$
   Which is just adding the additive neutral $n.k$ times.

2. $n > 0, k < 0$:

   Writing k as $-m$ to denote negativeness, we have:
   $$(n.k)_{\mathbb{F}} = (n(-m))_{\mathbb{F}} = (-n.m)_{\mathbb{F}} = -(n.m)_{\mathbb{F}}$$
   From 1:
   $$(n.k)_{\mathbb{F}} = -n_{\mathbb{F}}.m_{\mathbb{F}} = n_{\mathbb{F}}. - m_{\mathbb{F}} = n_{\mathbb{F}}.k_{\mathbb{F}}$$

□

Lemma
Ordering in $\mathbb{Q}$
3.7

Let $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in \mathbb{Q}$

$$\frac{m_1}{n_1} < \frac{m_2}{n_2} \rightarrow (\frac{m_1}{n_1})_{\mathbb{F}} < (\frac{m_2}{n_2})_{\mathbb{F}}$$

Proof Arbitrary locking $n_1, n_2 \in \mathbb{N}$ without losing generalization, we have:

$$\frac{m_1}{n_1} < \frac{m_2}{n_2} \leftrightarrow m_1.n_2 < m_2.n_1$$

Maintaing the inequality direction Now, from Lemma 3.5:

$$m_1.n_2 < m_2.n_1 \leftrightarrow (m_1.n_2)_{\mathbb{F}} < (m_2.n_1)_{\mathbb{F}}$$

Next, from Lemma 3.6:

$$(m_1.n_2)_{\mathbb{F}} < (m_2.n_1)_{\mathbb{F}} \leftrightarrow (m_1)_{\mathbb{F}}.(n_2)_{\mathbb{F}} < (m_2)_{\mathbb{F}}.(n_1)_{\mathbb{F}}$$

Now, since we fixed $n1, n2 \in \mathbb{N}$, we can use $(n1.n2)_{\mathbb{F}}$ to divide the expression:

$$(m_1)_{\mathbb{F}}.(n_2)_{\mathbb{F}} < (m_2)_{\mathbb{F}}.(n_1)_{\mathbb{F}} \leftrightarrow \frac{(m_1)_{\mathbb{F}}.(n_2)_{\mathbb{F}}}{(n_1.n_2)_{\mathbb{F}}}.\frac{(m_2)_{\mathbb{F}}.(n_1)_{\mathbb{F}}}{(n_1.n_2)_{\mathbb{F}}}$$

Next, we just distribute and simplify:

$$\frac{(m_1)_{\mathbb{F}}.(n_2)_{\mathbb{F}}}{(n_1.n_2)_{\mathbb{F}}}.\frac{(m_2)_{\mathbb{F}}.(n_1)_{\mathbb{F}}}{(n_1.n_2)_{\mathbb{F}}} \leftrightarrow \frac{(m_1)_{\mathbb{F}}}{(n_1)_{\mathbb{F}}}.\frac{(m_2)_{\mathbb{F}}}{(n_1)_{\mathbb{F}}}$$

Finally, we have:

$$\frac{m_1}{n_1} < \frac{m_2}{n_2} \leftrightarrow \frac{(m_1)_{\mathbb{F}}}{(n_1)_{\mathbb{F}}}.\frac{(m_2)_{\mathbb{F}}}{(n_1)_{\mathbb{F}}}$$

$$\frac{m_1}{n_1} < \frac{m_2}{n_2} \leftrightarrow (\frac{m_1}{n_1})_{\mathbb{F}} < (\frac{m_2}{n_2})_{\mathbb{F}}$$

□

Now if we recall, we did all of this as a previous step for proving the injectivity of ϕ. We can make it happen now.

Lemma 3.8 $\phi : \mathbb{Q}_{\mathbb{F}} \to \mathbb{Q}$

$$\phi(\frac{m}{n}) := \frac{m_{\mathbb{F}}}{n_{\mathbb{F}}}$$

is injective

Proof Let $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in \mathbb{Q}$, such that:

$$\frac{m_1}{n_1} < \frac{m_2}{n_2}$$

By Lemma 3.7, we have:

$$\frac{m_1}{n_1} < \frac{m_2}{n_2} \to (\frac{m_1}{n_1})_{\mathbb{F}} < (\frac{m_2}{n_2})_{\mathbb{F}}$$

By definition of ϕ, we can replace:

$$\frac{m_1}{n_1} < \frac{m_2}{n_2} \to \frac{(m_1)_{\mathbb{F}}}{(n_1)_{\mathbb{F}}} < \frac{(m_2)_{\mathbb{F}}}{(n_2)_{\mathbb{F}}}$$

$$\frac{m_1}{n_1} < \frac{m_2}{n_2} \to \phi(\frac{m_1}{n_1}) < \phi(\frac{m_1}{n_1})$$

$$\Rightarrow \phi : \mathbb{Q} \to \mathbb{Q}_{\mathbb{F}} \text{ preserves order.}$$

Finally, from Lemma 3.1 (Injectivity by order preservation) we assert:

$$\Rightarrow \phi : \mathbb{Q} \to \mathbb{Q}_{\mathbb{F}} \text{ is injective.}$$

□

Lemma 3.9 $\phi : \mathbb{Q}_{\mathbb{F}} \to \mathbb{Q}$

$$\phi(\frac{m}{n}) := \frac{m_{\mathbb{F}}}{n_{\mathbb{F}}}$$

is surjective

Proof By set construction (Lemma 3.2) we defined $\phi : \mathbb{Q}_{\mathbb{F}} \to \mathbb{Q}$, meaning that:

$$\mathbb{Q} = Im(\mathbb{Q}_{\mathbb{F}})$$

Then

$$\phi \text{ is surjective.}$$

□

This completes the construction.

Lemma 3.10 $\phi : \mathbb{Q}_{\mathbb{F}} \to \mathbb{Q}$

$$\phi(\frac{m}{n}) := \frac{m_{\mathbb{F}}}{n_{\mathbb{F}}}$$

is an isomorphism

Proof

1. By Lemma 3.3, ϕ is an homomorphism.
2. By Lemma 3.8 and Lemma 3.9, ϕ is bijective

Then, by Definition 3.2

$$\Rightarrow \phi \text{ is an isomorphism.}$$

$\square$

Securing this is a big step, and recalling our strategy we now need to use this isomorphism ϕ in $\mathbb{Q}_{\mathbb{F}} \to \mathbb{Q}$, and somehow transform it into a Φ that extends this to the whole $\mathbb{F} \to \mathbb{R}$.

Although this has being a long ride, personally I don't think this was a complex construction, or a hard-to-follow implementation of ϕ. Everything just landed in place.

The tricky part begins when we introduce Φ and try to understand what it really is. Still, I wouldn't include anything that I wouldn't find clear or satisfactory from a student's perspective (keep in mind I'm also learning while writing). If something feels confusing or lacks intuition, I prefer to leave it out entirely and try again.

3.4 Isomorphism in $\mathbb{R}$

We have successfully constructed an isomorphism $\phi : \mathbb{Q}_{\mathbb{F}} \to \mathbb{Q}$ that preserves all the important conditions (order, addition and multiplication), but our main goal is to extend this to all $\mathbb{R}$, starting from all $\mathbb{F}$.

So we expect a:

$$\Phi : \mathbb{F} \to \mathbb{R}$$

Such that:

1. Matches the former ϕ for all $\mathbb{Q}_{\mathbb{F}}$ into $\mathbb{Q}$
2. Remains an isomorphism
3. Preserves the field's struture (order, addition and multiplication)

The intuiton to create Φ was actually mentioned previously, on Example 2.1. We talked about how a subset S of an ordered field $\mathbb{Q}$ was bounded above by $\sqrt{2}$. The example talks more about how this S won't have a supremum, but the key idea we will be using is how this particular S was **bounded** by an irrational like $\sqrt{2}$. This is the relationship we need to apply to link irrational and rational numbers: **the first one bounds the second one**

With this idea, we can intuit that any **real number is actually defined by the numbers below it**. Take $\sqrt{2}$ for example:

1. $\sqrt{2}$ is greater than all the rationals q where $q < \sqrt{2}$: 1, 1.4, 1.41, 1.414, ...
2. $\sqrt{2}$ is less than all the rationals q where $q > \sqrt{2}$: 2, 1.5, 1.42, 1.4145, ...

The fact is that $\sqrt{2}$ is the only number placed in the boundary between these to sequences.

Formally:

$$\sqrt{2} := \sup\{q \in \mathbb{Q} : q < \sqrt{2}\}$$

Relating an irrational number, with all the rationals below it.

Definition
Φ function
3.7

For any $\alpha \in \mathbb{R}$, define $\Phi : \mathbb{R} \to \mathbb{F}$ as

$$\Phi(\alpha) := \sup\{\phi(q) : q \in \mathbb{Q}, q < \alpha\}$$

This new function Φ using the former isomorphism ϕ defined in $\mathbb{Q}$ does the exact same thing that $\sqrt{2}$ did in our example: bounds $\mathbb{Q}$. Since our main focus is to somehow extend the properties of the original ϕ, let us take the time to emphazise why this new Φ is not just an arbitrary function.

Lemma
3.11

For $r \in \mathbb{Q}$

$$\Phi(r) = \phi(r)$$

Proof

First, let us check the definition:

$$\Phi(\alpha) := \sup\{\phi(q) : q \in \mathbb{Q}, q < \alpha\}$$

If α happens to be a rational number r, it means that the supremum of all the rational values before this particular r are limited by $\phi(r)$, and this is the *Least Upper Bound* of the set.

1. $\phi(r)$ bounds $\{\phi(q) : q \in \mathbb{Q}, q < r\}$

   Knowing that ϕ preserves order:

   $$\begin{aligned} \forall q, q < r &\leftrightarrow \phi(q) < \phi(r) \\ &\leftrightarrow \phi(q) \leq \phi(r) \end{aligned}$$

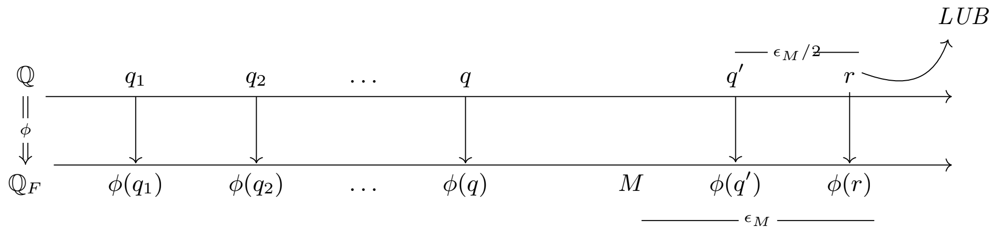
   $\Rightarrow \phi(r)$ bounds the set.

$\square$

Proof

2. $\phi(r)$ is the L.U.B. of $\{\phi(q) : q \in \mathbb{Q}, q < r\}$

let us visualize the approach



Assume M is an arbitrary upper bound, trying to make $\phi(r)$ not the $L.U.B.$

$$\rightarrow M < \phi(r) \rightarrow \phi(r) - M > 0$$

Let us denote ϵ_M as the distance between this assumed M and $\phi(r)$.

Now, let us not forget that by density in $\mathbb{Q}$ we are able to locate an arbitrary rational number between two other arbitrary rationals, or even better for our use case: we can position an arbitrary rational q' as close as we want to any other arbitrary rational.

Developing that idea:

$$\forall\ r \in \mathbb{Q}, \exists\ q' \in \mathbb{Q} : q' - \epsilon \leq r, \epsilon \in \mathbb{Q}$$

Now, $M \in \mathbb{Q}_{\mathbb{F}}$, but the density propery we are using for q' is in $\mathbb{Q}$. Luckily, we already proved that ϕ is ordered:

$$\forall\ r \in \mathbb{Q}, \exists\ q' \in \mathbb{Q}/\forall \epsilon > 0 : q' - \epsilon \leq r$$
$$\rightarrow \phi(q') - \phi(\epsilon) \leq \phi(r)$$

Now that we are entirely in $\mathbb{Q}_{\mathbb{F}}$ we will conveniently take this distance $\phi(\epsilon)$ as $\epsilon_M/2$, just to note that this will be smaller than the distance between M and r. No matter how close we assume M is to $\phi(r)$, by density in $\mathbb{Q}$ we can make sure that we can take half that distance (or a quarter, or a tenth, doesn't matter) to locate another image closer to $\phi(r)$.

$$\rightarrow M < \phi(q') < \phi(r) \rightarrow M \neq \text{ Upper bound}$$

$$\Rightarrow \Phi(r) := \sup\{\phi(q) : q \in \mathbb{Q}, q < r\} = \phi(r),\ \forall r \in \mathbb{Q}$$

□

Taking the time to proof this mapping for rationals wasn't a waste of time after all, since it confirms that our intuition about the definition of Φ isn't arbitrary, but respects the structure we already built.

3.4.1 Completeness of Φ

So far, our definition for Φ:

$$\Phi(\alpha) := \sup\{\phi(q) : q \in \mathbb{Q}, q < \alpha\}$$

Uses an internal set $S(\alpha) = \{\phi(q) : q \in \mathbb{Q}, q < \alpha\}$ that we can use to simplify our readability a bit:

$$\Phi(\alpha) := \sup(S(\alpha))$$

Now, to make Φ to make sense we need to make sure that S makes sense, and if we want to obtain the supremum of a poorly-define set, the whole definition crumbles.

Next, we will review how $S(\alpha)$ is well defined to avoid any issues further down.

Lemma 3.12 Set S:

$$\Phi(\alpha) := \sup\{S(\alpha)\} = \sup\{\phi(q) : q \in \mathbb{Q}, q < \alpha\}$$

is well defined in $\mathbb{R}$

Proof To proof this, what matters the most is that S is well-defined in $\mathbb{F}$. That automatically guarantees that Φ makes sense in $\mathbb{R}$.

1. $S(\alpha)$ is not empty:

   Using Theorem 2.5 (Archimedean theorem):

$$\begin{aligned}&\forall \alpha \in \mathbb{Q}, \exists\ n \in \mathbb{N} : n > \alpha\\&\rightarrow n > |\alpha|\\&\rightarrow -n < \alpha, -n \in \mathbb{Q}\end{aligned}$$

   Identifying $q = -n$ in S, we have a rational that is bounded by α, meaning that $\phi(-n) \in S(\alpha)$

2. $S(\alpha)$ is bounded above:

   Again, using Theorem 2.5:

$$\forall \alpha \in \mathbb{Q}, \exists\ n \in \mathbb{N} : n > \alpha$$

   Then, for any rational $q < \alpha$

$$\begin{aligned}&n > \alpha > q\\&\rightarrow q < n\\&\rightarrow \phi(q) < \phi(n) = n_{\mathbb{F}}\end{aligned}$$

   So $n_{\mathbb{F}}$ is an upper bound of S, for any $q < \alpha$

$\rightarrow S(\alpha)$ is well-defined in $\mathbb{F}$

$\rightarrow \Phi(\alpha) := \sup\{S(\alpha)\}$ is well-defined in $\mathbb{R}$ □

Now, while studying this a question came to me: if we already know that $\phi : \mathbb{Q} \rightarrow \mathbb{Q}_{\mathbb{F}}$ exists, why do we need to prove $S(\alpha)$ is non-empty? Can't we just pick any rational and map it?

The issue is that the set $S(\alpha)$ is not just any images of rationals, it's specifically: $S(\alpha) = \{\phi(q) : q \in \mathbb{Q} \text{ AND } q < \alpha\}$. The constraint $q < \alpha$ obligues us to prove that *there exists at least one rational q with $q < \alpha$*.

Lemma Order-Preservation 3.13

For $\alpha, \beta \in \mathbb{R}$

$$\alpha < \beta \to \Phi(\alpha) < \Phi(\beta)$$

Proof let us start with two evaluations of set S:

- $S(\alpha) := \{\phi(q) : q \in \mathbb{Q}, q < \alpha\}$
- $S(\beta) := \{\phi(q) : q \in \mathbb{Q}, q < \beta\}$

If $\alpha < \beta$, then for any $\phi(q') \in S(\alpha)$:

$$\begin{aligned}\phi(q) \in S(\alpha) &\leftrightarrow \phi(q') \in \{\phi(q) : q \in \mathbb{Q}, q < \alpha\} \\ &\leftrightarrow \phi(q') \in \{\phi(q) : q \in \mathbb{Q}, q < \alpha < \beta\} \\ &\leftrightarrow \phi(q') \in \{\phi(q) : q \in \mathbb{Q}, q < \beta\} \\ &\leftrightarrow \phi(q') \in S(\beta)\end{aligned}$$

Then, going back to the statement:

$$\begin{aligned}\alpha < \beta &\Rightarrow S(\alpha) \subseteq S(\beta) \\ &\Rightarrow \sup(S(\alpha)) \leq \sup(S(\beta)) \\ &\Rightarrow \Phi(\alpha) \leq \Phi(\beta)\end{aligned}$$

Now, to prove that the images of α and β in Φ are strictly less than and not equal, we use the density of $\mathbb{Q}$ in $\mathbb{R}$ to locate arbitrary rationals r_α, r_β.

$$\begin{gathered}\forall \alpha, \beta \in \mathbb{R}, \exists\ r_\alpha, r_\beta \in \mathbb{Q} : \\ \alpha < \beta \to \alpha < r_\alpha < r_\beta < \beta\end{gathered}$$

Since $r_\beta < \beta \to \phi(r_\beta) \in S(\beta)$ by the definition of S. Now, knowing that for any element of $S(\beta)$ it will be less or equal to its supremum, we have:

$$\begin{aligned}\phi(r_\beta) &\leq \sup(S(\beta)) \\ \phi(r_\beta) &\leq \Phi(\beta)\end{aligned}$$

Now in the middle, by order preservation:

$$r_\alpha < r_\beta \leftrightarrow \phi(r_\alpha) < \phi(r_\beta)$$

And finally, since $\alpha < r_\alpha \to S(\alpha) \subseteq S(r_\alpha)$. Then:

$$\begin{aligned}&S(\alpha) \subseteq S(r_\alpha) \\ &\to \Phi(\alpha) \leq \Phi(r_\alpha) \\ &\to \Phi(\alpha) \leq \phi(r_\alpha) \text{ (Since } r_\alpha \in \mathbb{Q})\end{aligned}$$

Joining all results:

$$\begin{aligned}\Phi(\alpha) \leq \phi(r_\alpha) &< \phi(r_\beta) \leq \Phi(\beta) \\ &\Rightarrow \Phi(\alpha) < \Phi(\beta)\end{aligned}$$

Finally, $\alpha < \beta \Rightarrow \Phi(\alpha) < \Phi(\beta)$. □

Now comes the final sprint to proof that Φ maps $\mathbb{F}$ and $\mathbb{R}$ perfectly. Just as we did with ϕ, we need to prove isomorphism by proving bijection and homomorphism. From this last part, the only tricky step is for surjectiveness, since it uses a method that we haven't seeing before. We are almost there!

Lemma
Injectivity in Φ
3.14

Given $\Phi : \mathbb{R} \to \mathbb{F}$, for $\alpha, \beta \in \mathbb{R}$:

$$\alpha \neq \beta \to \Phi(\alpha) \neq \Phi(\beta)$$

Proof

From proven order preservation in Lemma 3.13, if $\alpha \neq \beta$

1. $\alpha < \beta \to \Phi(\alpha) < \Phi(\beta) \to \Phi(\alpha) \neq \Phi(\beta)$
2. $\alpha > \beta \to \Phi(\alpha) > \Phi(\beta) \to \Phi(\alpha) \neq \Phi(\beta)$

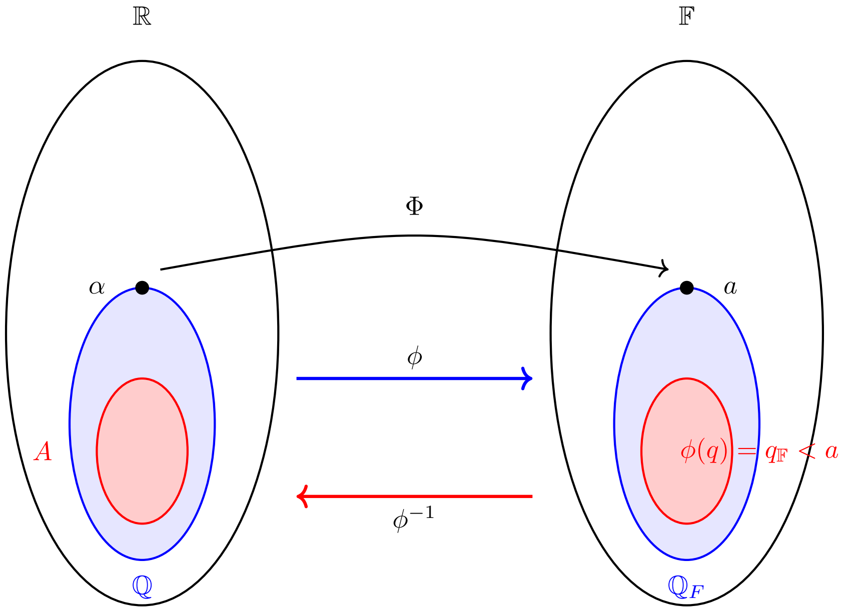
□

Lemma
Surjectivity in Φ
3.15

Given $\Phi : \mathbb{R} \to \mathbb{F}$:

$$\forall\ a \in \mathbb{F}, \exists\ \alpha \in \mathbb{R} : \Phi(\alpha) = a$$

Proof let us support the following ideas on the next diagram:



Picking an arbitrary $a \in \mathbb{F}$, we consider the set of rational elements of $\mathbb{F}$ that are strictly smaller than a:

$$\{q_{\mathbb{F}} \in \mathbb{Q}_{\mathbb{F}} : q_{\mathbb{F}} < a\}.$$

Now, since $\phi : \mathbb{Q} \to \mathbb{Q}_{\mathbb{F}}$ is an isomorphism (and hence injective), its inverse ϕ^{-1} exists. Applying ϕ^{-1} to the set above, we define

$$\begin{aligned} A &= \phi^{-1}(\{q_{\mathbb{F}} \in \mathbb{Q}_{\mathbb{F}} : q_{\mathbb{F}} < a\}) \\ &= \phi^{-1}(\{\phi(q) : q \in \mathbb{Q},\ \phi(q) < a\}) \\ &= \{q \in \mathbb{Q} : \phi(q) < a\}. \end{aligned}$$

Now let us consider $\alpha = \sup(A)$. We first show that α exists.

1. A is non-empty:

   Since $\mathbb{Q}_{\mathbb{F}}$ is dense in $\mathbb{F}$ and $a \in \mathbb{F}$, there exists $q_{\mathbb{F}} \in \mathbb{Q}_{\mathbb{F}}$ such that $q_{\mathbb{F}} < a$. By surjectivity of ϕ onto $\mathbb{Q}_{\mathbb{F}}$, there exists $q \in \mathbb{Q}$ with $\phi(q) = q_{\mathbb{F}}$. Hence $\phi(q) < a$ and therefore $q \in A$.

2. A is bounded above:

   Using the Archimedean property in $\mathbb{F}$, there exists $n_{\mathbb{F}} \in \mathbb{N}_{\mathbb{F}}$ such that $a < n_{\mathbb{F}}$. Since ϕ is order-preserving and maps $\mathbb{N}$ onto $\mathbb{N}_{\mathbb{F}}$, there exists $n \in \mathbb{N}$ with $\phi(n) = n_{\mathbb{F}}$.

   For every $q \in A$ we have $\phi(q) < a < n_{\mathbb{F}} = \phi(n)$, and by order preservation of ϕ this implies $q < n$. Hence n is an upper bound for A.

Therefore, $\alpha = \sup(A)$ exists. $\square$

Proof Now, what we want to achieve is that, given this arbitrary $a \in \mathbb{F}$, we reach a real number α such that $\Phi(\alpha) = a$. To do this, we show that the set A constructed above coincides with all rationals strictly smaller than its supremum.

Claim:

$$\{q \in \mathbb{Q} : q < \alpha\} = A.$$

- $\subseteq$:

  Let $q \in \mathbb{Q}$ with $q < \alpha$. Since $\alpha = \sup(A)$, q cannot be an upper bound for A. Hence there exists $q' \in A$ such that

  $$q < q' \leq \alpha.$$

  Since ϕ is order-preserving, we have

  $$\phi(q) < \phi(q').$$

  But $q' \in A$ implies $\phi(q') < a$, and therefore

  $$\phi(q) < a,$$

  which shows that $q \in A$.

- $\supseteq$:

  Let $q \in A$. By definition, $\phi(q) < a$. Since $\alpha = \sup(A)$, every element of A is smaller than or equal to α, and therefore

  $$q < \alpha.$$

  Thus $q \in \{q \in \mathbb{Q} : q < \alpha\}$.

Hence,

$$\{q \in \mathbb{Q} : q < \alpha\} = A.$$

So far we have shown that:

1. $\alpha = \sup(A)$ exists,
2. $A = \{q \in \mathbb{Q} : q < \alpha\}$.

Combining these, we obtain

$$\sup(A) = \sup\{q \in \mathbb{Q} : q < \alpha\}.$$

By definition of Φ, we have

$$\begin{aligned}\Phi(\alpha) &= \sup\{\phi(q) : q \in \mathbb{Q},\ q < \alpha\} \\ &= \sup\{\phi(q) : q \in A\}.\end{aligned}$$

But by construction of A,

$$\{\phi(q) : q \in A\} = \{q_{\mathbb{F}} \in \mathbb{Q}_{\mathbb{F}} : q_{\mathbb{F}} < a\}.$$

Since $\mathbb{Q}_{\mathbb{F}}$ is dense in $\mathbb{F}$ and a is an upper bound for this set, it follows that

$$\sup\{q_{\mathbb{F}} \in \mathbb{Q}_{\mathbb{F}} : q_{\mathbb{F}} < a\} = a.$$

Therefore,

$$\Phi(\alpha) = a,$$

which proves that Φ is surjective. $\square$

Now that this is done, we can conclude that Φ is a bijection. Next we will just cover the requirements to proof homomorphism and finish the whole demonstration. But first, a handy property:

Lemma 3.16 Let sets X, Y, then:

$$\sup(X+Y) = \sup(X) + \sup(Y)$$

Proof As always, to prove that something is a supremum of a set, we need to prove both the bound is what we expect, and that it is in fact the *Least Upper Bound*

1. Bound:

   We have:

$$\begin{aligned} X+Y := \{x+y, x \in X, y \in Y\} \\ \to \forall x \in X, x \leq \sup(X) \\ \to \forall y \in Y, y \leq \sup(Y) \\ \to x+y \leq \sup(X) + \sup(Y) \\ \Rightarrow \sup(X) + \sup(Y) \text{ bounds } X+Y \end{aligned}$$

2. $\sup(X) + \sup(Y)$ is $L.U.B$

   Assume a new upper bound M so that $M < \sup(X) + \sup(Y)$. Then

$$\epsilon = (\sup X + \sup Y - M) > 0$$

   Now, since $x < \sup X$ and $y < \sup Y, \forall x \in X, y \in Y$ respectively, we can take any small amount $\epsilon/2$ that would satisfy:

$$\begin{aligned} x + \epsilon/2 > \sup X \to x > \sup X - \epsilon/2 \\ y + \epsilon/2 > \sup Y \to y > \sup Y - \epsilon/2 \end{aligned}$$

   Adding up:

$$x + y > \sup X + \sup Y - \epsilon = M$$

   The, we found an $x + y \in X + Y$ that is not bounded by M.
   $\Rightarrow M$ fails to bound $X + Y$
   $\Rightarrow \sup X + \sup Y$ is the $L.U.B$ of $X + Y$

$\square$

Lemma
Homomorphism in Φ
3.17

$\Phi : \mathbb{R} \to \mathbb{F}$ is an homomorphism

Proof As we already know, we need to prove preservation of addition and multiplication. Let $\alpha, \beta \in \mathbb{R}$

1. $\Phi(\alpha+\beta) = \Phi(\alpha) + \Phi(\beta)$

   Claim: Recalling the definition of $S(\alpha) := \{\phi(q), q \in \mathbb{Q}, q < \alpha\}$, we will proof $S(\alpha+\beta) = S(\alpha) + S(\beta)$

   i. $\subseteq$**:**

   Let $\phi(q) \in S(\alpha+\beta)$

   $$\rightarrow q < \alpha + \beta \text{ (by definition of S)} \rightarrow q - \alpha < \beta$$

   Next, by density in $\mathbb{Q}$, there must be an arbitrary q' such that:

   $$\rightarrow q - \alpha < q' < \beta$$

   $$\begin{aligned} &\rightarrow_1 q - \alpha < q' \leftrightarrow q - q' < \alpha \\ &\rightarrow_2 q' < \beta \end{aligned}$$

   $$\begin{aligned} &\rightarrow_1 q - q' \in S(\alpha) \\ &\rightarrow_2 q' \in S(\beta) \end{aligned}$$

   Finally, with some clever operations in ϕ using its property for preserving addition:

   $$\begin{aligned} \phi(q) = \phi(q - q' + q') = \phi(q - q') + \phi(q') \\ \Rightarrow \phi(q) \in S(\alpha) + S(\beta) \end{aligned}$$

   ii. $\supseteq$**:**

   Let $\phi(q_1) + \phi(q_2) \in S(\alpha) + S(\beta)$, where $q_1 < \alpha \wedge q_2 < \beta$

   $$\begin{aligned} \rightarrow q_1 + q_2 < \alpha + \beta \wedge q_1 + q_2 \in \mathbb{Q} \\ \rightarrow q_1 + q_2 \in S(\alpha) + S(\beta) \end{aligned}$$

   Concluding that $S(\alpha+\beta) = S(\alpha) + S(\beta)$. Applying supremum to both sides, we have:

   $$\sup(S(\alpha+\beta)) = \sup(S(\alpha) + S(\beta))$$

   And from Lemma 3.16:

   $$\begin{aligned} \sup(S(\alpha+\beta)) = \sup(S(\alpha)) + \sup(S(\beta)) \\ \Rightarrow \Phi(\alpha+\beta) = \Phi(\alpha) + \Phi(\beta) \end{aligned}$$

$\square$

Proof

2. $\Phi(\alpha \cdot \beta) = \Phi(\alpha) \cdot \Phi(\beta)$

i. $\Phi(\alpha)\Phi(\beta)$**: Upper Bound for** $S(\alpha\beta)$

let us take any $\phi(q) \in S(\alpha\beta)$ where $q < \alpha\beta$.

By density of $\mathbb{Q}$ in $\mathbb{R}$, we can write:

$$q = q_1 \cdot q_2$$

where $q_1, q_2 \in \mathbb{Q}$ with $q_1 < \alpha$ and $q_2 < \beta$.

Since $q_1 < \alpha$ and $q_1 \in \mathbb{Q}$:

$$\phi(q_1) \in S(\alpha)$$

Therefore:

$$\phi(q_1) \leq \sup S(\alpha) = \Phi(\alpha)$$

Similarly, since $q_2 < \beta$ and $q_2 \in \mathbb{Q}$:

$$\phi(q_2) \leq \Phi(\beta)$$

Since ϕ preserves multiplication on rationals:

$$\phi(q) = \phi(q_1 q_2) = \phi(q_1) \cdot \phi(q_2)$$

Since all values are positive, we can multiply the inequalities:

$$\phi(q) = \phi(q_1) \cdot \phi(q_2) \leq \Phi(\alpha) \cdot \Phi(\beta)$$

This holds for every element of $S(\alpha\beta)$.

$\Rightarrow \Phi(\alpha)\Phi(\beta)$ is an upper bound for $S(\alpha\beta)$

ii. $\Phi(\alpha)\Phi(\beta)$**: *L.U.B.* of** $S(\alpha\beta)$

We need to prove that for any $q \in S(\alpha.\beta)$, it will be bounded by $\Phi(\alpha) \cdot \Phi(\beta)$. This is equivalent to proof that there is an $\epsilon_{\mathbb{F}} > 0$, the smallest of them all, that makes $\phi(q) + \epsilon_{\mathbb{F}} > \Phi(\alpha) \cdot \Phi(\beta)$.

Let $q = q_1.q_2, q_1 < \alpha \wedge q_2 < \beta$. Next, we define a distance δ small enough that:

$$q_1 + \delta > \alpha \wedge q_2 + \delta > \beta$$

Knowing this, our δ must be a positive number in $\mathbb{Q}$. So let us define it as

$$\delta \in \mathbb{Q}, 0 < \delta < 1$$

We will revisit this definition of δ later. Next we operate:

$$\begin{aligned}\rightarrow \alpha < q_1 + \delta &\leftrightarrow \Phi(\alpha) < \Phi(q_1 + \delta)\\ &\leftrightarrow \Phi(\alpha) < \Phi(q_1 + \delta)\\ &\leftrightarrow \Phi(\alpha) < \phi(q_1 + \delta)\ (q_1 + \delta \in \mathbb{Q})\end{aligned}$$

Identically, we make the same operation for β and q_2

$$\begin{aligned}&\rightarrow \Phi(\alpha) < \phi(q_1 + \delta)\\ &\rightarrow \Phi(\beta) < \phi(q_2 + \delta)\end{aligned}$$

□

Proof Multiplying both inequalities we have:

$\Phi(\alpha) \cdot \Phi(\beta) < \phi(q_1 + \delta) \cdot \phi(q_2 + \delta)$
$\Phi(\alpha) \cdot \Phi(\beta) < \phi((q_1 + \delta) \cdot (q_2 + \delta))$ (ϕ: isomorphism allows multiplication distribution)
$\Phi(\alpha) \cdot \Phi(\beta) < \phi(q_1.q_2 + \delta(q_1 + q_2) + \delta^2)$
$\Phi(\alpha) \cdot \Phi(\beta) < \phi(q_1.q_2) + \phi(\delta(q_1 + q_2) + \delta^2)$

let us leave the inequality there to see more deeply what we want to achieve using δ.
The intuiton here is to find a value for δ that allows the inequality to hold, no matter what.
From the definition:

$$\delta < 1 \rightarrow \delta^2 < \delta$$

Also:

$$q_1 + q_2 < \alpha + \beta$$

Multiplying both:

$$\begin{aligned} \delta(q_1 + q_2) &< \delta(\alpha + \beta) \\ \delta(q_1 + q_2) + \delta^2 &< \delta(\alpha + \beta) + \delta \\ \delta(q_1 + q_2) + \delta^2 &< \delta(\alpha + \beta + 1) \end{aligned}$$

Now allow me to do a "cleanup". let us redefine δ (still between 0 and 1) as:

$$0 < \delta < min\{\frac{\epsilon}{\alpha + \beta + 1}, 1\}, \epsilon > 0 \in \mathbb{Q}$$

But why? Just to do a clean simplification and end up with an isolated $\epsilon \in \mathbb{Q}$, independent from anything else.
Going back to the inequality, we notice that the terms start to unfold:

$$\begin{aligned} &\Phi(\alpha) \cdot \Phi(\beta) < \phi(q_1.q_2) + \phi(\delta(q_1 + q_2) + \delta^2) \\ &\qquad \rightarrow < \phi(q) + \phi(\delta(q_1 + q_2) + \delta^2) < \phi(q) + \phi(\delta(\alpha + \beta + 1)) = \phi(q) + \phi(\epsilon) \\ &\rightarrow \Phi(\alpha) \cdot \Phi(\beta) < \phi(q) + \phi(\epsilon) \\ &\rightarrow \Phi(\alpha) \cdot \Phi(\beta) < \phi(q) + \epsilon_{\mathbb{F}} \end{aligned}$$

This means that, by choosing a correct δ dependent of α and β, we get an arbitrary positive distance (margin) ϵ, which shows that $\Phi(\alpha) \cdot \Phi(\beta)$ is *L.U.B.* of $\phi(q)$.

$$\Rightarrow \Phi(\alpha.\beta) = \sup\{\phi(q), q \in \mathbb{Q}, q < \alpha.\beta\} = \Phi(\alpha) \cdot \Phi(\beta)$$
$$\Rightarrow \Phi : \text{ Homomorphism}$$

$\square$

Finally, we reached Rome

Lemma
Isomorphism Φ
3.18

$\Phi : \mathbb{R} \to \mathbb{F}$ is an isomorphism

Proof

1. By Lemma 3.14 and Lemma 3.15, Φ is bijective.
2. By Lemma 3.17, Φ is an homomorphism

For any complete ordered field $\mathbb{R}$, there exists an isomorphism Φ such that:

$$\Phi : \mathbb{R} \to \mathbb{F}$$

□

Personally, this is the first time I have been this rigorous with a proof, covering as much detail as I felt necessary to reach the result. For me, the real reward was the joy of knowing I understood all the pieces needed to build the puzzle, and I hope you found it equally rewarding.

3.5 Consequences of completeness

Being completely honest, Proving $\mathbb{R}$ uniquess drained me completely, so is fair to just check a few smaller extensions (consequence of this proof) to see how the visited properties are used in other, more specific lemmas. They also use cool last names to name them, so we can brag about knowing about the *Weierstrass-Cauchy-DiCaprio-Cumberbatch principle of boiling water in* $\mathbb{R}^6$, and a great excuse to give some color to the notes with some diagrams.

Definition
3.8

A function $f : \mathbb{N} \to X$ is a *sequence* of elements of X. So that:

$$f(n) := x_n, x_n \in X$$

Definition 3.9

Let $X_1, X_2, \ldots, X_n, \ldots$ be a sequence of sets. If $X_1 \supset X_2 \supset \ldots X_n \cdots \supset \ldots, \forall n \in \mathbb{N}$, we say the sequence is *nested*.

Lemma Cauchy-Cantor principle 3.19

Nested Interval Lemma: Let a sequence of closed intervals:

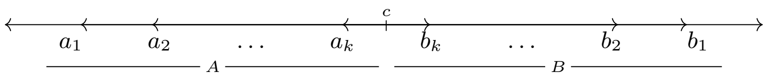
$$I_1 \supset I_2 \supset I_3 \supset \ldots I_n \supset$$

Then, there exists a point $c \in \mathbb{R}$ belonging to all the intervals in the sequence. Additionally, if for any $\epsilon > 0$, there exists an interval I_k such that $\|I_k\| < \epsilon$, then the element c is unique.

Proof Defining clearly $I_k = [a_k, b_k]$, as any arbitrary closed interval in the nested sequence. Then the sets:

$$A := \{a_k, k \in \mathbb{N}\}, B := \{b_k, k \in \mathbb{N}\}$$

Are formed using the left and right limits of the intervals mentioned.



Since A is a subset of $\mathbb{R}$, by density of $\mathbb{Q}$:

$$\exists c = \sup(A) \in \mathbb{R}, \forall a_k : a_k < c$$

Additionally (and supported by the diagram) all elements from B bound A:

$$\forall b_k \in B, \forall a_k inA : a_k < b_k$$

Now, $c = \sup(A)$ is the least upper bound, so any element from B must be greater than c.

$$\rightarrow a_k < c < b_k$$

Finally, take special care of how *for all* a_k, b_k we found that exists a real number c that satisfies this inequality, meaning that c belongs to any interval I_k in the nested sequence.
For the second part, condition says that for any distance $\epsilon > 0$, there is an interval I_k smaller in length than ϵ. Now, assuming there is $c1, c2 \in \mathbb{R}$, and for all a_k, b_k limits of the nested intervals:

$$\begin{aligned} a_k < c_1 < c_2 < b_k \\ \rightarrow -c_1 < -a_k \land c_2 < b_k \\ \rightarrow c_2 - c_1 < b_k - a_k \end{aligned}$$

Then, making $b_k = a_k + \epsilon$:

$$\rightarrow c_2 - c_1 < \epsilon, \forall \epsilon > 0$$

Then, the distance between c_1 and c_2 must be less than any positive number.

$$\begin{aligned} &\rightarrow c_2 - c_1 = 0 \\ &\Rightarrow c = c_2 = c_1 \text{ is unique.} \end{aligned}$$

□

A. Proof Techniques Toolkit

I wanted to take the time to review the proof techniques used per chapter. This appendix collects these with an example on each.

A.1 Archimedean Property

Definition: For any complete ordered field F, given any $x \in F$, there exists $n \in \mathbb{N}_F$ such that $n > x$.

Intuition: No matter how large a number you pick, you can always find a natural number bigger than it. This means the natural numbers are unbounded—they grow without limit.

Used to:

- Show sets are bounded (by finding an n that works as an upper bound)
- Show sets are non-empty (by finding a negative n that serves as a lower element)
- Construct rationals or integers around arbitrary real numbers

Example:

Problem: Let $S = \{1 - \frac{1}{n} : n \in \mathbb{N}\}$. Show that S is bounded above.

Solution: By the Archimedean property, for the number 2, there exists $n \in \mathbb{N}$ with $n > 2$. For any element $1 - \frac{1}{n} \in S$, we have

$$1 - \frac{1}{n} < 1 < 2 < n.$$

Hence 2 is an upper bound for S. □

A.2 Density of $\mathbb{Q}$ in $\mathbb{R}$

Definition: Between any two real numbers $\alpha < \beta$, there exists a rational number r such that $\alpha < r < \beta$.

Formally: $\forall \alpha, \beta \in \mathbb{R}$ with $\alpha < \beta$, $\exists r \in \mathbb{Q}$ such that $\alpha < r < \beta$.

Intuition: The rationals are "everywhere" in the reals—no matter how close two real numbers are, you can always squeeze a rational between them. This allows us to:

- Approximate irrational numbers by rational numbers
- Find elements "as close as we want" to a target value
- Bridge constructions between $\mathbb{Q}$ and $\mathbb{R}$

Example:

Problem: Show that between $\sqrt{2}$ and $\sqrt{3}$, there exists a rational number.

Solution: We have $\sqrt{2} \approx 1.414\ldots$ and $\sqrt{3} \approx 1.732\ldots$. Take $r = \frac{3}{2} = 1.5$. Since $1.414 < 1.5 < 1.732$, we have

$$\sqrt{2} < \frac{3}{2} < \sqrt{3},$$

and $\frac{3}{2} \in \mathbb{Q}$. □

A.3 Proof by Contradiction

Definition: To prove a statement P, assume $\neg P$ and derive a contradiction. Since assuming $\neg P$ leads to something impossible, P must be true.

Intuition: "If assuming the opposite leads to nonsense, then the original must be true." This technique is especially powerful when:

- Direct proof is difficult or unclear
- You want to prove something doesn't exist
- You want to prove a uniqueness property (by assuming two things exist and deriving a contradiction)

Example:

Problem: Prove that $\sqrt{2}$ is irrational.

Solution: Suppose $\sqrt{2} \in \mathbb{Q}$. Then $\sqrt{2} = \frac{p}{q}$ where $p, q \in \mathbb{Z}$, $q \neq 0$, and $\gcd(p, q) = 1$ (in lowest terms).

Squaring both sides: $2 = \frac{p^2}{q^2}$, so $p^2 = 2q^2$.

Thus p^2 is even, which implies p is even (if p were odd, p^2 would be odd). Write $p = 2k$ for some $k \in \mathbb{Z}$.

Then $(2k)^2 = 2q^2$, so $4k^2 = 2q^2$, hence $q^2 = 2k^2$.

Thus q^2 is even, so q is even.

But then both p and q are even, contradicting $\gcd(p, q) = 1$.

Therefore $\sqrt{2} \notin \mathbb{Q}$. $\square$

A.4 Mathematical Induction

Definition: To prove a statement $P(n)$ holds for all $n \in \mathbb{N}$:

1. *Base case:* Show $P(1)$ is true
2. *Inductive step:* Assume $P(k)$ is true (inductive hypothesis), then prove $P(k+1)$ is true

Intuition: Like dominoes—if the first one falls (base case) and each falling domino knocks over the next (inductive step), then all dominoes fall. We use induction for:

- Constructing $\mathbb{N}_F$ step-by-step
- Proving properties that hold "for all natural numbers"
- Building sequences or recursive structures

Example:

Problem: Prove that for all $n \in \mathbb{N}$, the sum $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

Solution:

Base case ($n = 1$): LHS $= 1$, RHS $= \frac{1(2)}{2} = 1$. ✓

Inductive step: Assume the formula holds for $n = k$, i.e.,

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

We must show it holds for $n = k + 1$:

$$\begin{aligned}
1 + 2 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\
&= (k+1)\left[\frac{k}{2} + 1\right] \\
&= (k+1) \cdot \frac{k+2}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

This is exactly the formula for $n = k + 1$. By induction, the formula holds for all $n \in \mathbb{N}$. □

A.5 Supremum Arguments

Definition: To prove $s = \sup(S)$, we must show:

1. s is an upper bound: $\forall x \in S$, $x \leq s$
2. s is the *least* upper bound: $\forall \varepsilon > 0$, $\exists x \in S$ such that $s - \varepsilon < x \leq s$

Equivalently for (2): For any $s' < s$, there exists $x \in S$ with $x > s'$ (so s' is not an upper bound).

Intuition: The supremum is the "ceiling" of a set—nothing in the set exceeds it, but you can get arbitrarily close to it from below. This technique is used constantly to:

- Define functions via suprema of rational approximations
- Show that bounds are tight (no smaller bound works)
- Bridge rational approximations to real limits

Example:

Problem: Let $S = \{1 - \frac{1}{n} : n \in \mathbb{N}\}$. Prove that $\sup(S) = 1$.

Solution:

1. *Upper bound:* For any $n \in \mathbb{N}$, we have $\frac{1}{n} > 0$, so $1 - \frac{1}{n} < 1$. Thus 1 is an upper bound for S.

2. *Least upper bound:* Let $\varepsilon > 0$. By the Archimedean property, there exists $N \in \mathbb{N}$ with $N > \frac{1}{\varepsilon}$, so $\frac{1}{N} < \varepsilon$. Then $1 - \frac{1}{N} \in S$ and

$$1 - \left(1 - \frac{1}{N}\right) = \frac{1}{N} < \varepsilon,$$

meaning $1 - \varepsilon < 1 - \frac{1}{N} \leq 1$.

So within any ε-neighborhood of 1, there exists an element of S. Thus 1 is the least upper bound. □

A.6 Trichotomy in Ordered Fields

Definition: In an ordered field F, for any $x, y \in F$, exactly one of the following holds:

1. $x = y$
2. $x < y$
3. $x > y$

Intuition: Any two elements are either equal or one is strictly larger—no other options exist. This fundamental property is used in:

- Proof by cases (exhaustively considering all three possibilities)
- Proving injectivity (if $f(x) = f(y)$, then x cannot be $<$ or $>$ than y)
- Establishing contradictions in order-preservation arguments

Example:

Problem: Prove that if $x^2 = y^2$ in an ordered field F, then $x = y$ or $x = -y$.

Solution: We have $x^2 - y^2 = 0$, so $(x - y)(x + y) = 0$.

In a field, a product equals zero if and only if at least one factor equals zero. Thus $x - y = 0$ or $x + y = 0$.

- If $x - y = 0$, then $x = y$.
- If $x + y = 0$, then $x = -y$.

By trichotomy, these are the only possibilities (we cannot have both $x - y \neq 0$ and $x + y \neq 0$ simultaneously if $x^2 = y^2$). $\square$