A Rigorous Introduction to the Reals

Gaurav Goel

gmgoel@gmail.com

gauravgoel@college.harvard.edu

August 5, 2019

Abstract

This paper follows the footsteps from the appendix of Chapter 1 from Rudin's Principles of Mathematical Analysis to construct real numbers from the rationals using Dedekind cuts, going significantly beyond the content in the text and filling all gaps in the proofs. It also covers the notion of completeness and non-denumerability of the reals, considering various equivalent descriptions, without the requirement of any knowledge of topology. The author hopes, that the paper will be used as an introduction to the reals that does not lose rigor, but is accessible to dedicated students with little knowledge of the topological principles, and that the knowledge that one gains from this paper can then be further strengthened and reinforced by a more complete, topological introduction to analysis. The choice of certain sources for certain proofs reflects what the author thought as the most illuminating proof that does not uses topology, and yet manages to capture the essence of the theorem being proven.

Contents

1 Introduction and Definitions

We, unlike Rudin [1], use the notation $\subseteq$ to denote "is a subset of", and reserve $\subset$ for proper subsets; but like him, assume that the reader has an understanding of the rationals, $\mathbb{Q}$.

Definition 1.1. Let S be a set. A (total) *order* on S is a relation $< \subseteq S \times S$ with the properties:
1. *Trichotomy.* If $x, y \in S$ then exactly one of $x < y$, $x = y$ and $y < x$ holds. If $y < x$ we write $x > y$.
2. *Transitivity.* For $x, y, z \in S$, $(x < y) \wedge (y < z) \implies x < z$.

An *ordered set* is a set S on which an order is defined. We take $\leq$ to mean "either $<$ or $=$", and define $\geq$ similarly.

Definition 1.2. Suppose S is an ordered set, and let $E \subseteq S$. If $\exists \beta \in S$ s.t. $\forall x \in E, x \leq \beta$ then we say that E is *bounded above*, and we call β an *upper bound* of E. Lower bounds are defined the same way with $\geq$ in place of $\leq$. An $E \subseteq S$ is said to be *bounded* if it is both bounded below and bounded above.

Definition 1.3. Suppose S is an ordered set, and that $E \subseteq S$ is bounded above. Suppose $\exists \alpha \in S$ with the following properties:
1. α is an upper bound of E.
2. If $\gamma < \alpha$ then γ is not an upper bound of E.

Then α is called the *least upper bound* or *supremum* of E and is written as $\alpha = \sup E$. That it is unique is obvious. The *greatest lower bound* or *infimum* is defined similarly, and is written as $\alpha = \inf E$. We note that E may or may not contain its supremum or infinum.

Definition 1.4. An ordered set S is said to possess the *least upper bound property* (shortened to LUBP) if the following is true: if $E \subseteq S, E \neq \emptyset$ and E is bounded above, then $\sup E$ exists in S.

Remark. $\mathbb{Q}$ does not possess the LUBP. Consider, for example, $E \subseteq \mathbb{Q}$ given by $E = \{p | p^2 < 2\}$.

Theorem 1. *Suppose S is an ordered set with the LUBP. Assume that $B \subseteq S, B \neq \emptyset$ and that B is bounded below. Then $\inf B$ exists in S.*

Proof. Let L be the set of all lower bounds of B. By definition, $L \subseteq S$. Since B is bounded below, $L \neq \emptyset$. Since $\forall x \in B, \forall y \in L, y \leq x$, hence L is bounded above and every $x \in B$ is an upper bound of L. Since S possesses the LUBP, $\sup L$ exists in S; call it α. We show that $\alpha = \inf B$.

We know that all members of B are upper bounds of L. If $\exists b \in B$ s.t. $b < \alpha = \sup L$, this contradicts the fact that α is the *least* upper bound. Hence, $\forall b \in B, \alpha \leq b$, implying that α is a lower bound of B.

Suppose $\exists \beta \in S, \beta > \alpha$ s.t. β is a lower bound of B. Then, by definition, $\beta \in L$. But α is an upper bound of L, implying $\beta \leq \alpha$, a contradiction. Hence, if $\beta \in S, \beta > \alpha$ then β is not a lower bound of B. Therefore, by definition, $\alpha = \inf B$. $\square$

2 Archimedean Property

In short, the Archimedean Property when possessed by an algebraic structure means that it does not contain any infinitely large or infinitesimally small elements. We see what algebraic structures here have this property. We begin first with the Well-Ordering Principle.

Well-Ordering Principle. For $S \subseteq \mathbb{N}_0 = \mathbb{N} \cup \{0\}$, $S \neq \emptyset \implies \exists a \in S$ s.t. $\forall b \in S, a \leq b$.

Corollary 1. *By appropriate translation, any non-empty susbet of integers that is bounded below has a least element.*

Theorem 2 (Archimedean Property for Natural Numbers)**.** $\forall a, b \in \mathbb{N}, \exists n \in \mathbb{N}$ *s.t.* $na > b$.

Proof. Assume to the contrary that $\forall n \in \mathbb{N}, na \leq b$. Then $S = \{b - na | n \in \mathbb{N}\} \subseteq \mathbb{N}_0$. By the Well-Ordering Principle, S has a least element, say $b - ma$. But because $b - (m+1)a \in S$ and $b - (m+1)a < b - ma$, we arrive at a contradiction to the minimality of $b - ma$. $\square$

Theorem 3 (Archimedean Property for Positive Rationals)**.** $\forall a, b \in \mathbb{Q}_{>0}, \exists n \in \mathbb{N}$ *s.t.* $na > b$.

Proof. Clearly, both this theorem and the previous one are equivalent to the following: $\forall b/a \in \mathbb{Q}_{>0}, \exists n \in \mathbb{N}$ s.t. $n > b/a$. $\square$

Corollary 3.1 (Archimedean Property for Rationals)**.** *If $a, b \in \mathbb{Q}$ and $a > 0$ then $\exists n \in \mathbb{N}$ s.t. $na > b$.*

It turns out that the real numbers also possess the Archimedean Property, as we shall demonstrate after we have a rigorous construction of the real numbers using Dedekind cuts.

3 Field Structure

Here, we discuss the definition of a field and its consequences.

Definition 3.1. A *field* is a set F with two operations $+, \cdot : F^2 \to F$, called *addition* and *multiplication* respectively, which satisfies the following field axioms:
 (A) *Axioms for addition*: $(F, +)$ forms an abelian group.
   (A0) *Closure.* $\forall x, y \in F, x + y \in F$.
   (A1) *Associativity.* $\forall x, y, z \in F, (x + y) + z = x + (y + z)$.
   (A2) *Existence of Identity.* $\exists 0 \in F$ s.t. $\forall x \in F, 0 + x = x$.
   (A3) *Existence of Inverse.* $\forall x \in F, \exists -x \in F$ s.t. $x + (-x) = 0$.
   (A4) *Commutativity.* $\forall x, y \in F, x + y = y + x$.
 (M) *Axioms for Multiplication*: $(F \setminus \{0\}, \cdot)$ forms an abelian group.
   (M0) *Closure.* $\forall x, y \in F, x \cdot y \in F$. $x \cdot y$ is also written as xy for brevity.
   (M1) *Associativity.* $\forall x, y, z \in F, (xy)z = x(yz)$.
   (M2) *Existence of Identity.* $\exists 1 \in F$ s.t. $1 = 0$ and $\forall x \in F, 1x = x$.
   (M3) *Existence of Inverse.* $\forall x \in F \setminus \{0\}, \exists 1/x \in F$ s.t. $x \cdot (1/x) = 1$.
   (M4) *Commutativity.* $\forall x, y \in F, xy = yx$.
 (D) *Distributivity.* $\forall x, y, z \in F, x(y + z) = xy + xz$.

Proposition 3.1 (Field Structure - Addition)**.** The axioms for addition imply the following. We omit the proofs and encourage the reader to try them.
   1. *Cancellation Law.* $x + y = x + z \implies y = z$.
   2. *Uniqueness of Identity.* $x + y = x \implies y = 0$.
   3. *Uniqueness of Inverse.* $x + y = 0 \implies y = -x$.
   4. *Pairing of Inverses.* $-(-x) = x$.

Proposition 3.2 (Field Structure - Multiplication)**.** Similarly, the axioms for multiplication imply the following.
   1. *Cancellation Law.* $x \neq 0 \land xy = xz \implies y = z$.
   2. *Uniqueness of Identity.* $x \neq 0 \land xy = x \implies y = 1$.
   3. *Uniqueness of Inverse.* $x \neq 0 \land xy = 1 \implies y = 1/x$.
   4. *Pairing of Inverses.* $1/(1/x) = x$.

Proposition 3.3 (Field Structure - Distributivity)**.** For any $x, y, z \in F$,
   1. $0x = 0$.
   2. *Null Factor Law.* $xy = 0 \implies x = 0 \lor y = 0$.
   3. $(-x)y = -(xy) = x(-y)$.
   4. $(-x)(-y) = xy$.

Definition 3.2. An *ordered field* is a field F which is also an ordered set, such that:
   1. $\forall x, y, z \in F, y < z \implies x + y < x + z$.
   2. $\forall x, y \in F, (x > 0) \land (y > 0) \implies xy > 0$.
If $x > 0$ we call x *positive*; if $x < 0$ we call it *negative*.

Proposition 3.4 (Ordered Field Structure)**.** Let F be an ordered field. For $x, y, z \in F$, the following hold. The proofs are omitted, but can be found in any standard text, e.g. Rudin.
   1. If $x > 0$ then $-x < 0$ and vice-versa.
   2. If $x > 0$ then $y < z \implies xy < xz$.
   3. If $x < 0$ then $y < z \implies xy > xz$.
   4. $x \neq 0 \implies x^2 > 0$. In particular, $1 > 0$.
   5. $0 < x < y \implies 0 < 1/y < 1/x$.

The set of rational numbers, $\mathbb{Q}$, follows the axioms of Definitions 3.1 and 3.2, as is readily checked. Hence, $\mathbb{Q}$ is an ordered field.

4 The Real Field - Dedekind Cuts

Theorem 4. *There exists an ordered field $\mathbb{R}$, with the LUBP. Moreover, it contains $\mathbb{Q}$ as a subfield.*

The second statement means that $\mathbb{Q} \subseteq \mathbb{R}$, the operations of addition and multiplication coincide with the usual ones on rationals, and that the positive rationals are the positive elements of $\mathbb{R}$. The members of $\mathbb{R}$ are called the *real numbers*.

Proof. We construct, stepwise, the field $\mathbb{R}$ from the rational numbers. We do so with the full gory details.

Step 1 The members of $\mathbb{R}$ will be certain subsets of $\mathbb{Q}$, called *cuts*. A *cut* is a set $\alpha \subseteq \mathbb{Q}$ with the following properties:

   (I) $\alpha \neq \emptyset$ and $\alpha \neq \mathbb{Q}$.

   (II) α is closed downward. If $p \in \alpha, q \in \mathbb{Q}$ and $q < p$ then $q \in \alpha$. This implies that: (a) $p \in \alpha \wedge q \notin \alpha \implies p < q$ and (b) $r \notin \alpha \wedge r < s \implies s \notin \alpha$.

   (III) α has no largest element. Formally, $p \in \alpha \implies \exists r \in \alpha$ s.t. $p < r$.

   The letters $p, q, r, \ldots$ are used to denote rationals and $\alpha, \beta, \gamma, \ldots$ are used to denote cuts.

Step 2 Define "$\alpha < \beta$" to mean $\alpha \subset \beta$. Let us check that this satisfies the requirements of Definition 1.1.

Trichotomy. It is clear at most one of the following hold: $\alpha < \beta, \alpha = \beta, \beta < \alpha$. To show that at least one holds, assume that the first two fail. Then $\alpha \not\subseteq \beta \implies \exists p \in \alpha$ s.t. $p \notin \beta$. Then $\forall q \in \beta, p \notin \beta \implies q < p$, hence $q \in \alpha$, by (II). Thus $\beta \subseteq \alpha$. Since $\beta \neq \alpha$, we conclude $\beta < \alpha$.

Transitivity. It is obvious that $(\alpha < \beta) \wedge (\beta < \gamma) \implies \alpha < \gamma$, since a proper subset of a proper subset is a proper subset.

Thus $\mathbb{R}$ is now an ordered set.

Step 3 The ordered set $\mathbb{R}$ has the LUBP.

To prove this, let $A \subseteq \mathbb{R}$ be nonempty and let $\beta \in \mathbb{R}$ be an upper bound of A. Define $\gamma = \bigcup\limits_{\alpha \in A} \alpha$. We show that $\gamma \in \mathbb{R}$ and that $\gamma = \sup A$.

We show that $\gamma \in \mathbb{R}$.

   (I) $A \neq \emptyset \implies \exists \alpha_0 \in A$. Since α_0 is cut, $\alpha_0 \neq \emptyset$ and $\alpha_0 \subseteq \gamma$ implies that $\gamma \neq \emptyset$. Next, $\forall \alpha \in A, \alpha \subseteq \beta \implies \gamma \subseteq \beta$ and hence $\gamma \neq \mathbb{Q}$.

   To prove (II) and (III), pick any $p \in \gamma$.

   (II) By definition of γ, $\exists \alpha_1 \in A$ s.t. $p \in \alpha_1$. For any $q \in \mathbb{Q}, q < p \implies q \in \alpha_1 \implies q \in \gamma$.

   (III) We know that $\exists r \in \alpha_1$ s.t. $r > p$. Then the same r lies in γ as well.

   Hence, $\gamma \in \mathbb{R}$. Now we show that $\gamma = \sup A$.

   It is clear that $\forall \alpha \in A, \alpha \leq \gamma$.

   Suppose $\delta < \gamma$. Then $\exists s \in \gamma$ s.t. $s \notin \delta$. Since $s \in \gamma, \exists \alpha \in A$ s.t. $s \in \alpha$. Hence, $\delta < \alpha$ and thus δ is not an upper bound of A. Hence, by definition, $\gamma = \sup A$.

Step 4 For $\alpha, \beta \in \mathbb{R}$, define $\alpha + \beta = \{r + s \mid r \in \alpha, s \in \beta\}$. We define $0^* = \{s \mid s \in \mathbb{Q}, s < 0\}$. Clearly, $0^* \in \mathbb{R}$. We verify that the axioms for addition from definition 3.1 hold, with 0^* being the identity for addition.

   (A0) We have to show that $\alpha + \beta \in \mathbb{R}$.

      (I) Clearly, $\emptyset \subset \alpha + \beta \subseteq \mathbb{Q}$. Let $r' \notin \alpha, s' \notin \beta$. Then $\forall r + s \in \alpha + \beta, r + s < r' + s' \implies r' + s' \notin \alpha + \beta$. Consequently, $\alpha + \beta \neq \mathbb{Q}$.

      For (II) and (III) pick any $p \in \alpha + \beta$. Then $\exists r \in \alpha, s \in \beta$ s.t. $p = r + s$.

      (II) If $q < p$, then $q - s < r$, so $q - s \in \alpha$, and $q = (q - s) + s \in \alpha + \beta$.

      (III) Choose $t \in \alpha$ s.t. $t > r$. Then $p < t + s$ and $t + s \in \alpha + \beta$.

      Hence, $\alpha + \beta$ satisfies the definition of a cut.

   (A1) Follows trivially from associativity in $\mathbb{Q}$.

   (A2) If $s \in 0^*$ and $r \in \alpha$, then $s + r < r$, hence $s + r \in \alpha$. Thus $0^* + \alpha \subseteq \alpha$. For the other side, pick $p \in \alpha$, and pick $r \in \alpha, r > p$. Then $p - r \in 0^*$ and $p = (p - r) + r \in 0^* + \alpha$, implying $\alpha \subseteq 0^* + \alpha$. Therefore, we conclude that $0^* + \alpha = \alpha$.

   (A3) Fix $\alpha \in \mathbb{R}$. Define $\beta = \{p \mid p \in \mathbb{Q} \wedge \exists t > 0 \text{ s.t. } -p - t \notin \alpha\}$. We show that $\beta \in \mathbb{R}$ and that $\alpha + \beta = 0^*$.

      (I) For some $s \notin \alpha$, let $p = -s - 1$. Then $-p - 1 \notin \alpha \implies p \in \beta$, hence $\beta \neq \emptyset$. If $q \in \alpha$ then $-q \notin \beta$, so $\beta \neq \mathbb{Q}$.

      For (II) and (III), choose $p \in \beta$, and choose $t > 0$ s.t. $-p - t \notin \alpha$.

      (II) $q < p \implies -q - t > -p - r$, hence $-q - t \notin \alpha$ so that $q \in \beta$.

      (III) Put $u = p + (t/2)$. Evidently, $u > p$ and $-u - (t/2) \notin \alpha$ so that $u \in \beta$.

      Hence, $\beta \in \mathbb{R}$.

      If $r \in \alpha$ and $s \in \beta$ then $-s \notin \alpha \implies r < -s \implies r + s < 0$ so that $\alpha + \beta \subseteq 0^*$. Now pick $v \in 0^*$ and let $w = -v/2$. Then $w > 0$. Now consider the set $E \subseteq \mathbb{Z}$ given by $E = \{m \mid mw \notin \alpha\}$. Pick $a \notin \alpha$. Since $w > 0$, by the Arhimedean property for rationals, $\exists n \in \mathbb{N}$ s.t. $nw > a \implies nw \notin \alpha \implies n \in E \implies E \neq \emptyset$. Now pick $b \in \alpha$. Again, $\exists l \in \mathbb{N}$ s.t. $lw > -b \implies b > (-l)w \implies -l \notin E$ and $l \notin E, k \leq l \implies k \notin E$ so that E is bounded below. Therefore, by Corollary 1, E has a minimal element; call it $n + 1$. Then $nw \in \alpha$ but $(n + 1)w \notin \alpha$. Put $p = -(n + 2)w$. Then $-p - w = (n + 1)w \notin \alpha \implies p \in \beta$, and $v = nw + p \in \alpha + \beta$ so that $0^* \subseteq \alpha + \beta$. Conseqeuntly, $\alpha + \beta = 0^*$. We denote such β, of course, by $-\alpha$.

   (A4) Again, this follows trivially from commutativity in $\mathbb{Q}$.

Step 5 Now that the addition defined in Step 4 satisfies the axioms for addition from Definition 3.1, Proposition 3.1 is valid in $\mathbb{R}$. Hence, we can prove the first of the requirements of Definition 3.2. We have to show that $\forall \alpha, \beta, \gamma \in \mathbb{R}, \beta < \gamma \implies \alpha + \beta < \alpha + \gamma$. Indeed, it is obvious from the definition of $+$ in $\mathbb{R}$ that $\alpha + \beta \subseteq \alpha + \gamma$. If we had $\alpha + \beta = \alpha + \gamma$, the cancellation law from Proposition 3.1 would imply $\beta = \gamma$,

contrary to the hypothesis.

It also follows that $\alpha > 0^* \iff -\alpha < 0^*$.

Step 6 Multiplication is a little more bothersome than addition in our context because products of negative rationals are positive. For this reason, we confine ourselves first to $\mathbb{R}_{>0} = \{\alpha \in \mathbb{R} | \alpha > 0^*\} \subset \mathbb{R}$.

For $\alpha, \beta \in \mathbb{R}_{>0}$, define $\alpha\beta = \{p | \exists r \in \alpha, s \in \beta, r > 0, s > 0 \text{ s.t. } p \leq rs\}$. Define $1^* = \{q | q \in \mathbb{Q}, q < 1\}$. Then we show that the axioms for multiplication and distributivity hold in $\mathbb{R}_{>0}$ with 1^* as the identity for multiplication.

Observe closely what $\alpha \in \mathbb{R}_{>0}$ means. $0^* \subset \alpha \implies \exists p \in \alpha \text{ s.t. } p \notin 0^*$, i.e. $p \geq 0$. By (III), $\exists r \in \alpha$ s.t. $r > p \geq 0$. If for $\alpha \in \mathbb{R}, \exists r \in \alpha \text{ s.t. } r > 0$ then $\forall q \in 0^*, q < r \implies 0^* \subseteq \alpha$. Since $r \notin 0^*, 0^* < \alpha$. Hence, $\alpha \in \mathbb{R}_{>0} \iff \alpha \in \mathbb{R} \land \exists r \in \alpha \text{ s.t. } r > 0$.

(M0) We have to show that $\alpha\beta \in \mathbb{R}_{>0}$.

   (I) Obviously $\alpha\beta \subseteq \mathbb{Q}$. Choose any $r \in \alpha, s \in \beta, r > 0, s > 0$. Then $p = rs \in \alpha\beta \implies \alpha\beta \neq \emptyset$. Now choose $r' \notin \alpha, s' \notin \beta$. Then necessarily $r' > 0$ and $s' > 0$. Consider $p' = r's'$. Since $\mathbb{Q}$ is an ordered field, using Proposition 3.4 and the fact that $\forall r \in \alpha, s \in \beta, r > 0, s > 0, r < r', s < s'$ we get that $rs < r's < r's' \implies p \notin \alpha\beta \implies \alpha\beta \neq \mathbb{Q}$.

   For parts (II) and (III), pick a $p \in \alpha\beta$ and choose r, s as specified such that $p \leq rs$.

   (II) Let $q < p$. Then the same choice of r, s shows that $q \in \alpha\beta$.

   (III) Choose $t \in \alpha$ s.t. $t > r$. Then $p \leq rs < ts$ and $ts \in \alpha\beta$.

   This shows that $\alpha\beta \in \mathbb{R}$. From (I), $\exists rs \in \alpha\beta$ s.t. $rs > 0$ so that $\alpha\beta \in \mathbb{R}_{>0}$.

(M1) It follows from associativity in $\mathbb{Q}$. Here's a sketch of why: we wish to show that $\forall \alpha, \beta, \gamma \in \mathbb{R}_{>0}, (\alpha\beta)\gamma = \alpha(\beta\gamma)$. Now $(\alpha\beta)\gamma = \{p | \exists r \in \alpha\beta, s \in \gamma, r > 0, s > 0 \text{ s.t. } p \leq rs\}$. But $r \in \alpha\beta \implies \exists q \in \alpha, t \in \beta, q > 0, t > 0 \text{ s.t. } r \leq qt$. Hence, $(\alpha\beta)\gamma = \{p | \exists q \in \alpha, t \in \beta, s \in \gamma, q, t, s > 0 \text{ s.t. } p \leq rs \leq qts\}$. Hence, defining $\alpha\beta\gamma$ as $\{p | \exists q \in \alpha, t \in \beta, s \in \gamma, q, t, s > 0 \text{ s.t. } p \leq qts\}$ is consistent with the previous definition (choose $r = qt$) and makes it obvious why multiplication is associative.

(M2) Clearly, $1^* \neq 0^*$. We have to show that $\forall \alpha \in \mathbb{R}_{>0}, 1^*\alpha = \alpha$.

   By definition, $1^*\alpha = \{p | \exists r \in 1^*, s \in \alpha, r > 0, s > 0 \text{ s.t. } p \leq rs\}$. Since $\forall r \in 1^*, r < 1$ and $s > 0$, $p \leq rs < s$. Hence, by (II) in α, $p \in \alpha$ so that $1^*\alpha \subseteq \alpha$.

   Now pick any $q \in \alpha$. We show that $q \in 1^*\alpha$, i.e. $\exists r \in 1^*, q' \in \alpha, r > 0, q' > 0 \text{ s.t. } q \leq rq'$. If $q \leq 0$, any choice works. If $q > 0$, then by (III) in $\alpha, \exists q' \in \alpha$ s.t. $q' > q > 0$. Let $r = q/q'$. Then $0 < r < 1 \implies r \in 1^*$ and $q = rq' \in 1^*\alpha$. Hence $\alpha \subseteq 1^*\alpha$. Combining, $1^*\alpha = \alpha$.

(M3) Pick $\alpha \in \mathbb{R}_{>0}$ and define $\beta = \{p | q \in \alpha \land q > 0 \implies \exists t > 0 \text{ s.t. } p < (1/q) - t\}$. We show that $\beta \in \mathbb{R}_{>0}$ and that $\alpha\beta = 1^*$.

   (I) Choose $t = 1/(2q)$ to see that $0 \in \beta$, so that $\beta \neq \emptyset$. Let $p \in \alpha, p > 0$. By (III) in α, choose $q \in \alpha$ s.t. $q > p > 0$. Then $1/p > 1/q > 0 \implies \nexists t > 0 \text{ s.t. } 1/p < (1/q) - t \implies 1/p \notin \beta$. Hence, $\beta \neq \mathbb{Q}$.

   For (II) and (III), pick $p \in \beta$.

   (II) Since $\forall q \in \alpha, q > 0 \exists t > 0 \text{ s.t. } p < (1/q) - t$, using the same t for any $p' < p$ shows that $p' \in \beta$.

   (III) Let $u = p + (t/2) > p$. Then $\forall q \in \alpha, q > 0 \exists (t/2) > 0 \text{ s.t. } u < (1/q) - (t/2) \implies u \in \beta$.

   Hence $\beta \in \mathbb{R}$. Since $0 \in \beta, \beta \in \mathbb{R}_{>0}$. Now we show that $\alpha\beta = 1^*$.

   Suppose $p \in \alpha\beta$. $p \leq 0 \implies p \in 1^*$. If $p > 0$, we know that $\exists r \in \alpha, s \in \beta, r > 0, s > 0 \text{ s.t. } p \leq rs$. Now $s \in \beta \implies \exists t > 0 \text{ s.t. } s < (1/r) - t$. Therefore, $p \leq rs < 1 - rt < 1 \implies p \in 1^*$. Consequently, $\alpha\beta \subseteq 1^*$.

   For the other direction, we first prove three preliminary lemmas.

   Lemma 4.1. For any $\alpha \in \mathbb{R}$, we have that $\forall \varepsilon \in \mathbb{Q}_{>0}, \exists p \in \alpha, q \notin \alpha \text{ s.t. } q - p < \varepsilon$.

   Proof. Pick any $p \in \alpha, q \notin \alpha$. If $q - p < \varepsilon$, we are done. Hence assume that $q - p \geq \varepsilon > 0$. Now, by the Archimedean property on positive rationals, we can pick an $N \in \mathbb{N}$ s.t. $N > (q - p)/\varepsilon$. Pick such an N and define $p_i = p + (q - p)/N$ for $i = 0, 1, \ldots, N$. We notice that $p_0 = p$ and $p_N = q$. Consider the set $S \subseteq \mathbb{N}_0 \cap [0, N]$ given by $S = \{n | p_n \notin \alpha\}$. Because $N \in S$, we see that S is a nonempty subset of nonnegative integers. Therefore, by the Well-Ordering Principle, it has a minimal element; call it r. Since $0 \notin S, r > 0$. Hence we find that $p_{r-1} \in \alpha, p_r \notin \alpha$ and $p_r - p_{r-1} = (q - p)/N < \varepsilon$ as needed. $\square$

   Lemma 4.2. For any $\alpha \in \mathbb{R}_{>0}$, we have that $\forall \varepsilon \in \mathbb{Q}_{>0}, \exists p \in \alpha, p > 0, q \notin \alpha \text{ s.t. } q - p < p\varepsilon$.

   Proof. Fix a $t \in \alpha$ s.t. $t > 0$. (We can do this because $\alpha \in \mathbb{R}_{>0}$). Now define $\varepsilon' = \frac{\varepsilon t}{2(1 + \varepsilon)}$, so that $0 < \varepsilon' < \frac{\varepsilon t}{1 + \varepsilon} < t$. Now by Lemma 4.1, pick $p \in \alpha, q \notin \alpha$ such that $0 < q - p < \varepsilon'$. Since $t \in \alpha$ but $q \notin \alpha$, we have $t < q$ so that we get $0 < t - \varepsilon' < q - \varepsilon' < p$ and hence $0 < \frac{1}{p} < \frac{1}{q - \varepsilon'} < \frac{1}{t - \varepsilon'}$. Then these p, q satisfy the condition because we get the chain of inequalities $0 < \frac{q-p}{p} < \frac{q-p}{t-\varepsilon'} < \frac{\varepsilon'}{t-\varepsilon'} < \varepsilon$. $\square$

   Lemma 4.3. If $\alpha \in \mathbb{R}_{>0}$ then $\forall v \in (0, 1), \gamma_v = v\alpha = \{vp | p \in \alpha\} \subset \alpha$.

   Proof. It is obvious that $\gamma_v \subseteq \alpha$, hence it suffices to demonstrate a $p \in \alpha \setminus \gamma$. Let $\varepsilon = 1 - v$ so that

5

$0 < \varepsilon < 1$. Using Lemma 4.2, pick a $p \in \alpha, p > 0, q \notin \alpha$ such that $q < p(1 + \varepsilon)$. Now $\forall p' \in \alpha, p' < q$ implying that $vp' = p'(1 - \varepsilon) < q(1 - \varepsilon) < p(1 - \varepsilon^2) < p$ so that $p \notin \gamma$. $\qquad \square$

Now pick $v \in 1^*$. If $v \le 0$ then picking any positive $r \in \alpha, s \in \beta$ shows that $v \in \alpha\beta$. Hence assume that $0 < v < 1$. Define $v' = (1 + v)/2$. Then $0 < v < v' < 1$. Now define $\gamma_{v'} = v'\alpha = \{v'p | p \in \alpha\}$. Using Lemma 4.3, choose a $r \in \alpha \setminus \gamma_{v'}$ and define $s = \frac{v}{r} > 0$. Then $\forall q \in \alpha, q > 0, r > v'q \iff s = \frac{v}{r} < \frac{v'}{r} < \frac{1}{q}$. Hence, we see that $\forall q \in \alpha, q > 0, \exists t = \frac{v'-v}{2r} > 0$ s.t. $s < (1/q) - t \implies s \in \beta$. Finally, $v = rs \in \alpha\beta$ so that $1^* \subseteq \alpha\beta$. This completes the proof that $\alpha\beta = 1^*$. Naturally, we denote such a β by $1/\alpha$.

- (M4) Follows trivially from commutativity in $\mathbb{Q}$.
- (D) To show that $\forall \alpha, \beta, \gamma \in \mathbb{R}_{>0}, \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

  Suppose that $p \in \alpha(\beta + \gamma)$. Then $\exists a \in \alpha, s \in \beta + \gamma, a > 0, s > 0$ s.t. $p \le as$. $s \in \beta + \gamma \implies \exists b \in \beta, c \in \gamma$ s.t. $s = b + c > 0$. We may WLOG assume that $b, c > 0$. To see why, first notice that atmost one of b, c is nonpositive. WLOG, if $b \le 0$, replacing it by a $b' \in \alpha$ s.t. $0 < b' < c$ (such a b' exists because $\alpha \in \mathbb{R}_{>0}$) and replacing c with $c - b'$ does not change the sum. Then we get that $p \le a(b + c) = ab + ac$. Since $ab \in \alpha\beta$ and $ac \in \alpha\gamma$, $ab + ac \in \alpha\beta + \alpha\gamma$ and thus $p \in \alpha\beta + \alpha\gamma$. Hence, we get that $\alpha(\beta + \gamma) \subseteq \alpha\beta + \alpha\gamma$.

  To proceed in the other direction, let $p \in \alpha\beta + \alpha\gamma$. Then $\exists t \in \alpha\beta, s \in \alpha\gamma$ s.t. $p = t + s$. Now $\exists a_1 \in \alpha, b \in \beta, a_1 > 0, b > 0$ s.t. $t \le a_1 b$ and $\exists a_2 \in \alpha, c \in \gamma, a_2 > 0, c > 0$ s.t. $s \le a_2 c$. Let $a = \max\{a_1, a_2\} \in \alpha$. Then $p \le a_1 b + a_2 c \le ab + ac = a(b + c)$ so that $p \in \alpha(\beta + \gamma)$. Hence, we get that $\alpha\beta + \alpha\gamma \subseteq \alpha(\beta + \gamma)$, finishing the proof.

Step 7 We can now prove the second of the requirements of Definition 3.2. We have to show that if $\alpha, \beta > 0^*$ then $\alpha\beta > 0^*$. But this is obvious because if we choose $r \in \alpha, s \in \beta, r > 0, s > 0$ then $rs > 0$ and $rs \in \alpha\beta$.

Step 8 We complete the definition of multiplication by setting $\alpha 0^* = 0^* \alpha = 0^*$ and by setting

$$\alpha\beta = \begin{cases} (-\alpha)(-\beta) & \alpha < 0^*, \beta < 0^* \\ -[(-\alpha)\beta] & \alpha < 0^*, \beta > 0^* \\ -[\alpha(-\beta)] & \alpha > 0^*, \beta < 0^*, \end{cases}$$

where the products on the right were defined in Step 6. Similarly, if $\alpha < 0^*$, we define $1/\alpha = -[1/(-\alpha)]$. To complete the definition of multiplication, all that remains to be shown is that the axioms (M) and (D) hold not just in $\mathbb{R}_{>0}$ but in $\mathbb{R}$. In this part the casework becomes tedious, but we highly encourage the reader to at least follow the working carefully, if not try to work through it themselves. To organize the cases below, whenever we have three variables (M1 and D), we let $C_N, N = 0, 1, \ldots, 7$ to denote the case where α, β, γ have signs according to the digits in the binary representation of N, with 0 indicating positive and 1 indicating negative. For instance, C_2 means $\alpha > 0^*, \beta < 0^*, \gamma > 0^*$ because $2_\chi = 010_2$.

We repeatedly use (a) the above definition of multiplication for negative reals, (b) properties from Step 6, and (c) the fact that $\forall \alpha \in \mathbb{R}, -(-\alpha) = \alpha$, which comes as a part of Proposition 3.1, which we have proven for the reals.

- (M0) It follows immediately from the definition that if $\alpha, \beta \in \mathbb{R}$ then $\alpha\beta \in \mathbb{R}$.
- (M1) We have to show that $\forall \alpha, \beta, \gamma \in \mathbb{R}, \alpha(\beta\gamma) = (\alpha\beta)\gamma$. If any of α, β, γ were to be 0^*, both sides would be 0^* and hence equal. Hence, we can assume $\alpha, \beta\gamma \ne 0^*$ split into $C_1, C_2, \ldots, C_7$.
  - (C_0) Follows from Step 6.
  - (C_1) $\alpha(\beta\gamma) = \alpha[-\beta(-\gamma)] = -[\alpha(\beta(-\gamma))] = -[(\alpha\beta)(-\gamma)] = (\alpha\beta)\gamma$.
  - (C_2) $\alpha(\beta\gamma) = \alpha[-(-\beta)\gamma] = -\alpha[(-\beta)\gamma] = -[\alpha(-\beta)]\gamma = [-\alpha(-\beta)]\gamma = (\alpha\beta)\gamma$.
  - (C_3) $\alpha(\beta\gamma) = \alpha[(-\beta)(-\gamma)] = [\alpha(-\beta)](-\gamma) = (-\alpha\beta)(-\gamma) = (\alpha\beta)\gamma$.
  - (C_4) $\alpha(\beta\gamma) = -[(-\alpha)(\beta\gamma)] = -[(-\alpha)\beta]\gamma = [-((-\alpha)\beta)]\gamma = (\alpha\beta)\gamma$.
  - (C_5) $\alpha(\beta\gamma) = (-\alpha)(-\beta\gamma) = (-\alpha)[\beta(-\gamma)] = [(-\alpha)\beta](-\gamma) = (-\alpha\beta)(-\gamma) = (\alpha\beta)\gamma$.
  - (C_6) $\alpha(\beta\gamma) = (-\alpha)(-\beta\gamma) = (-\alpha)[(-\beta)\gamma] = [(-\alpha)(-\beta)]\gamma = (\alpha\beta)\gamma$.
  - (C_7) $\alpha(\beta\gamma) = -[(-\alpha)(\beta\gamma)] = -[(-\alpha)((-\beta)(-\gamma))] = -[((-\alpha)(-\beta))(-\gamma)] = -[(\alpha\beta)(-\gamma)] = (\alpha\beta)\gamma$.

    Therefore, in all cases, we get associativity.
- (M2) If $\alpha > 0^*$ then by Step 6, $1^*\alpha = \alpha$.

  If $\alpha = 0^*$ then $1^*\alpha = 1^*0^* = 0^* = \alpha$.

  If $\alpha < 0^*$ then $1^*\alpha = -[1^*(-\alpha)] = -[(-\alpha)] = \alpha$.

  Therefore, in all cases, $1^*\alpha = \alpha$.
- (M3) If $\alpha > 0^*$ then by Step 6 we are done.

  If $\alpha = 0^*$ then we need not show an inverse, and indeed none exists in this definition.

  If $\alpha < 0^*$ then, by definition, $1/\alpha = -[1/(-\alpha)]$ so that $\alpha \cdot 1/\alpha = \alpha[-(1/(-\alpha))] = (-\alpha)[1/(-\alpha)] = 1$.

  Therefore, in all cases where $\alpha \ne 0^*$, we get an inverse.
- (M4) To show that $\forall \alpha, \beta \in \mathbb{R}, \alpha\beta = \beta\alpha$. If either of α, β were to be 0^*, both sides would be 0^* and hence equal. Hence, we can assume $\alpha, \beta \ne 0^*$ and split into the below cases.

6

If $\alpha > 0^*, \beta > 0^*$ then by Step 6 we are done.

If $\alpha > 0^*, \beta < 0^*$ then $\alpha\beta = -[\alpha(-\beta)] = -[(-\beta)\alpha] = \beta\alpha$.

If $\alpha < 0^*, \beta > 0^*$ then $\alpha\beta = -[(-\alpha)\beta] = -[\beta(-\alpha)] = \beta\alpha$.

If $\alpha < 0^8, \beta < 0^*$ then $\alpha, \beta = (-\alpha)(-\beta) = (-\beta)(-\alpha) = \beta\alpha$.

Therefore, in all cases, we get commutativity.

(D) To show that $\forall \alpha, \beta, \gamma \in \mathbb{R}, \alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma$. Again, if any of α, β, γ were to be 0^*, it is easy to verify that both sides would be equal. Hence, we can assume $\alpha, \beta, \gamma \neq 0^*$ and split into $C_1, C_2, \ldots, C_7$. To simplify our analysis, we can see that by commutativity of addition (which we have proven above holds for reals), $C_1 \iff C_2$ and $C_5 \iff C_6$ so that we only need to prove one of each pair. However, we need to break C_1 further as shown below.

(C_0) Follows from Step 6.

(C_1) We break further. Recall that in this case $\alpha > 0^*, \beta > 0^*, \gamma < 0^*$.

    a. If $\beta + \gamma > 0^*$ then $\alpha(\beta + \gamma) - \alpha\gamma = \alpha(\beta + \gamma) + \alpha(-\gamma) = \alpha(\beta + \gamma - \gamma) = \alpha\beta$. Adding $\alpha\gamma$ to both sides we get the result.

    b. If $\beta + \gamma < 0^*$ then $-\alpha(\beta+\gamma)+\alpha\beta = \alpha[-(\beta+\gamma)]+\alpha\beta = \alpha[-\beta-\gamma]+\alpha\beta = \alpha[-\beta-\gamma+\beta] = \alpha(-\gamma) = -\alpha\gamma$. Adding $\alpha(\beta+\gamma) + \alpha\gamma$ to both sides we get the result.

This finishes C_1 and, by the equivalence, C_2.

(C_3) $-\alpha(\beta+\gamma) = \alpha[-(\beta+\gamma)] = \alpha[-\beta-\gamma] = \alpha[(-\beta)+(-\gamma)] = \alpha(-\beta)+\alpha(-\gamma) = -\alpha\beta - \alpha\gamma$. Adding $\alpha(\beta+\gamma)+\alpha\beta+\alpha\gamma$ to both sides we get the result.

(C_4) $\alpha(\beta+\gamma) = -[(-\alpha)(\beta+\gamma)] = -[(-\alpha)\beta + (-\alpha)\gamma] = -[(-\alpha)\beta] - [(-\alpha)\gamma] = \alpha\beta + \alpha\gamma$.

(C_5) $\alpha(\beta+\gamma) = -[(-\alpha)(\beta+\gamma)] = -[(-\alpha)\beta+(-\alpha)\gamma] = -[(-\alpha)\beta] - [(-\alpha)\gamma] = \alpha\beta + \alpha\gamma$. In the distributive step, we used C_1.

(C_7) $\alpha(\beta+\gamma)] = (-\alpha)[-(\beta+\gamma)] = (-\alpha)[-\beta-\gamma] = (-\alpha)[(-\beta)+(-\gamma)] = (-\alpha)(-\beta)+(-\alpha)(-\gamma) = \alpha\beta + \alpha\gamma$.

Therefore, in all cases, we get distributivity.

This completes the proof that $\mathbb{R}$ is an ordered field with the LUBP. Now it remains to be shown that $\mathbb{Q}$ is isomorphic to a subfield of $\mathbb{R}$.

Step 9 We associate with each $r \in \mathbb{Q}$ the set $r^* \subset \mathbb{Q}$ defined by $r^* = \{p | p < r\}$. It is clear that each r^* is a cut; that is $r^* \in \mathbb{R}$. Then these "rational cuts" satisfy the following properties:

(a) $r^* + s^* = (r+s)^*$

(b) $r^* s^* = (rs)^*$

(c) $r^* < s^* \iff r < s$.

Proof. We use the properties of $\mathbb{R}$ developed above, and prove the statements in a convenient order.

(c) If $r < s$ then $r \in s^* \setminus r^*$ so that $r^* < s^*$. If $r^* < s^*$ then $\exists p \in s^* \setminus r^*$. Hence $r \leq p < s$ so that $r < s$.

(a) Choose $p \in r^* + s^*$. Then $p = u + v$ where $u < r$, $v < s$. Hence $p < r + s$, which says that $p \in (r+s)^*$. Conversely, suppose that $p \in (r+s)^*$. Then $p < r + s$. Let $t = (r + s - p)/2$ and put $r' = r - t < r, s' = s - t < s$. Then $r' \in r^*, s' \in s^*$ and $p = r' + s' \in r^* + s^*$.

(b) If either of r or s is 0, then the conclusion is obvious since then both sides are 0^* (this follows from the first result of Proposition 3.3, which we know to hold for $\mathbb{R}$). Hence, assume that $r, s \neq 0$. First we show the result for $r, s > 0$.

By definition, $r^* s^* = \{p | \exists a \in r^*, b \in s^*, a > 0, b > 0 \text{ s.t. } p \leq ab\}$. Choose p in $r^* s^*$ and such a, b. Since $0 < a < r$ and $0 < b < s$, we have that $p \leq ab < rb < rs$ so that $p \in (rs)^*$. For the other direction, assume that $p \in (rs)^*$. Then $p < rs$. We have to show a, b such that $0 < a < r, 0 < b < s$ and $p \leq ab$. If $p \leq 0$, choosing $a = r/2, b = s/2$ suffices. Hence assume that $0 < p < \frac{p+rs}{2} < rs$. Then let $\varepsilon = \frac{1}{2} \min\{r, \frac{rs-p}{2s}\}$. Now because $r, s > 0$ and $rs - p > 0$, $\frac{rs-p}{2s} > 0$ so that $0 < \varepsilon < \min\{r, \frac{rs-p}{2s}\}$. This means that we can choose $a = r - \varepsilon$ and $b = \frac{p+rs}{2(r-\varepsilon)}$ since $0 < \varepsilon < r \implies 0 < r - \varepsilon < r$ and $\varepsilon < \frac{rs-p}{2s} \implies \frac{p+rs}{2(r-\varepsilon)} < s$.

We now show that $(-r)^* = -r^*$. Now $-r^* = \{p | \exists t > 0 \text{ s.t.} -p - t \notin r^*\}$ and $-p - t \notin r^* \iff -p - t \geq r \iff p + t \leq -r$. Hence, we see that such a t exists iff $p < -r$, that is iff $p \in (-r)^*$. The rest is just casework using (c).

If $r > 0, s < 0$ then $r^* > 0^*, s^* < 0^*$ so $r^* s^* = -[r^*(-s)^*] = -[(r(-s))^*] = -[(-rs)^*] = (rs)^*$.

If $r < 0, s > 0$ then $r^* < 0^*, s^* > 0^*$ so $r^* s^* = -[(-r)^* s^*] = -[((-r)s)^*] = -[(-rs)^*] = (rs)^*$.

If $r < 0, s < 0$ then $r^* < 0^*, s^* < 0^*$ so $r^* s^* = (-r^*)(-s^*) = (-r)^*(-s)^* = [(-r)(-s)]^* = (rs)^*$.

Therefore, in all cases, we get that $r^* s^* = (rs)^*$.

$\square$

This shows that the set of rational cuts $\mathbb{Q}^*$ is a subfield of $\mathbb{R}$ and that it is isomorphic to $\mathbb{Q}$. This isomorphism allows us to regard $\mathbb{Q}$ as a subfield of $\mathbb{R}$. It is, in fact, isomorphisms that allow us to embed $\mathbb{N} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Rudin then states, without proof, that any two ordered fields with the least upper bound property are isomoprhic; so that the first part of this theorem characterizes the real field completely. We, thus, finish the construction. $\square$

5   Is $\sqrt{2}$ real?

It is a standard proof in any mathematics textbook that $\sqrt{2}$ is irrational. Here, we use the above construction of the reals to show that there is indeed a real (in fact, two of them), whose square is 2.

Theorem 5. *There exists a positive real number whose square is* 2.

Proof. Let $\alpha \subseteq \mathbb{Q}$ be defined as $\alpha = \{p | p \le 0 \vee (p > 0 \wedge p^2 < 2)\}$. We show that $\alpha \in \mathbb{R}_{>0}$ and that $\alpha^2 = 2^*$.
  (I) $0 \in \alpha \implies \alpha \ne \emptyset$ and $2 \notin \alpha \implies \alpha \ne \mathbb{Q}$.
      For (II) and (III), pick a $p \in \alpha$.
 (II) If $p \le 0$ then $q < p \implies q \le 0 \implies q \in \alpha$. If $p > 0$ and $q \le 0$ then $q < p$ and $q \in \alpha$. If $0 < q < p$ then $0 < q^2 < p^2 < 2$ so that $q \in \alpha$.
(III) If $p < 0$ then $0 \in \alpha$ works. If $p \ge 0$ then define, as Rudin does, $q = \frac{2p+2}{p+2}$. Then it is an easy exercise to check that $p^2 < 2 \iff p < q \iff q^2 < 2$ so that $q \in \alpha$ is a greater element of α.
This means that $\alpha \in \mathbb{R}$. Since $0 \in \alpha, \alpha \in \mathbb{R}_{>0}$. Now, we show that $\alpha^2 = 2^*$.
Let $p \in \alpha^2$. Then $\exists a, b \in \alpha, a, b > 0$ s.t. $p \le ab$. Such a pair, by definition of α, must satisfy $a^2 < 2, b^2 < 2$, so that α. If $p \ge 2$ then $0 \le 2 < p \le ab \implies 0 < 4 \le p^2 \le a^2 b^2 < 4$, a contradiction. Therefore, $p < 2$ and $p \in 2^*$. This means that $\alpha^2 \subseteq 2^*$.
Now assume that $p \in 2^*$, i.e. $p < 2$. If $p \le 0$, choose any positive element t of $\alpha \in \mathbb{R}_{>0}$ so that $p \le 0 < t^2$ implying that $p \in \alpha^2$. Hence assume that $0 < p < 2$. Define $\varepsilon = \frac{1}{2} \min\{\frac{1}{10}, \frac{10(2-p)}{21p}\}$. Then $0 < \varepsilon < \min\{\frac{1}{10}, \frac{10(2-p)}{21p}\}$ so that $\varepsilon(2 + \varepsilon) < \varepsilon(2 + \frac{1}{10}) = \frac{21\varepsilon}{10} < \frac{2-p}{p}$. Multiplying both sides by $p > 0$, we get that $p\varepsilon(2+\varepsilon) < 2 - p \implies p(1+\varepsilon)^2 < 2$. Since $\alpha \in \mathbb{R}_{>0}$, by Lemma 4.2, we may choose $t \in \alpha, t > 0, s \notin \alpha$ such that $s - t < t\varepsilon$. For these s, t, we have that $p < \frac{2}{(1+\varepsilon)^2} \le \frac{s^2}{(1+e)^2} < t^2 < 2$. Hence we see that for this $t \in \alpha, t > 0$, we have $p \le t^2$ and hence $p \in \alpha^2$, implying that $2^* \subseteq \alpha^2$. This concludes the proof that $\alpha^2 = 2^*$. $\square$

6   Archimedean Property for Reals

As promised, we now follow give two proofs of the Archimedean Property for the real numbers, using the fact that it is an ordered field with the LUBP.

Theorem 6 (Archimedean Property for Reals)**.** *If $a, b \in \mathbb{R}$ and $a > 0$ then $\exists n \in \mathbb{N}$ s.t. $na > b$.*

Rudin mentions that "with very little extra effort", we may derive this from the construction we have developed above. This is the "very little extra effort" from the part of the author. To integrate the use of the symbols we developed above for the reals into the context we usually use them in, we now overload the usage of $<$ operator and use the same notation for the rational numbers as both numbers (when compared with each other) and for the rational cuts (when used with reals). In understanding the meaning from the context, one can develop an appreciation for the choice of symbols.

Proof 1. If $b \le 0$ then $0 \in a \setminus b$ so that $b < a$ and $n = 1$ works. Hence assume that $b > 0$. Now choose $q \notin b$, then $q > 0$. Since $a > 0$, $\exists t \in a, t > 0$. By the Archimedean Property on the Rationals, we may choose an $n \in \mathbb{N} \setminus \{1\}$ so that $(n-1)t > q$. Then $(n-1)t \in na \setminus b$ and so for this n, $na > b$. $\square$

The second proof is taken from Rudin, and with this proof he wishes to show how powerful the LUBP is.

Proof 2. Assume to the contrary that $\forall n \in \mathbb{N}, na \le b$. Then $\emptyset \subset S = \{na | n \in \mathbb{N}\} \subseteq \mathbb{R}$ is bounded above by b. Since $\mathbb{R}$ has the LUBP, $\alpha = \sup S$ exists in $\mathbb{R}$. Now $x > 0 \implies \alpha - x < \alpha$ so that $\alpha - x$ is not an upper bound of S. This means that $\exists m \in \mathbb{N}$ s.t. $\alpha - x < mx$. But then $\alpha < (m+1)x$, which is impossible since α is an upper bound of S. $\square$

It is interesting to observe how this proof is similar to that of the Archimedean Property for natural numbers. In both the cases, we assume the contrary and show a violation of the minimality of a bound.

7 Completeness of Reals

The rationals, despite being "dense" on the number line, are incomplete in the sense that there are still gaps in them (in fact, uncountably many of them). For example, it is possible for a continuous function on the rationals to change sign without hitting a zero (consider $p(x) = x^2 - 2$). The reals are, in this sense, complete, and form a continuum. This "completeness" has various equivalent formulations. We develop some of them as simple consequences of the LUBP.

7.1 Dedekind Completeness

An ordered field is said to be *Dedekind complete* if every Dedekind cut in that field is generated by a number of that field. The rationals are clearly not Dedekind complete, since the cut corresponding to $\sqrt{2}$ is not generated by a rational number. The reals are Dedekind complete, and that means that creating more Dedekind cuts will not give further structure.

Theorem 7 (Dedekind Completeness of the Reals). *Let $\alpha \subseteq \mathbb{R}$ be such that:*
  (I) $\alpha \neq \emptyset$ *and* $\alpha \neq \mathbb{R}$.
  (II) *If* $p \in \alpha, q \in \mathbb{R}$ *and* $q < p$ *then* $q \in \alpha$.
  (III) $p \in \alpha \implies \exists r \in \alpha$ *s.t.* $p < r$.
Then $\exists a \in \mathbb{R}$ *s.t.* $\alpha = \{x \in \mathbb{R} : x < a\}$.

Proof. This is a trivial consequence of the LUBP. (I) and (II) collectively imply that α is a nonempty subset of the reals that is bounded above (by any $b \notin \alpha$). Hence, $a = \sup \alpha$ exists in $\mathbb{R}$. Since a is an upper bound of α, we must have that $\alpha \subseteq \{x \in \mathbb{R} : x \leq a\}$. If $a \in \alpha$, by (III) we would obtain some $r \in \alpha$ s.t. $a < r$, a contradiction to a being an upper bound of α. This means that $\alpha \subseteq \{x \in \mathbb{R} : x < a\}$. We now show that $\{x \in \mathbb{R} : x < a\} \subseteq \alpha$. Pick any $q < a$ and let $0 < \varepsilon = a - q$. Since a is the *least* upper bound of α, exists $p \in \alpha \cap (a - \frac{\varepsilon}{2}, a)$, else $a - \frac{\varepsilon}{2}$ would be a smaller upper bound. Then for this p, $p \in \alpha$ and $q < p$ so that by (II) $q \in \alpha$, thus concluding the proof. □

7.2 Monotone Convergence Theorem

Definition 7.1. A *sequence* $\{a_n\}_{n \in \mathbb{N}}$ of reals is a mapping $a : \mathbb{N} \to \mathbb{R}$ that assigns to each natural number n a real number $a_n = a(n)$. A sequence $\{a_n\}$ is said to be *weakly increasing* if $\forall n \in \mathbb{N}, a_n \leq a_{n+1}$ and is said to be *weakly decreasing* if $\forall n \in \mathbb{N}, a_n \geq a_{n+1}$. We drop the term "weakly" when we drop the condition that equality be possible between successive terms in the above definition. A sequence is said to be *monotone* if it is either weakly increasing or weakly decreasing. . A sequence $\{a_n\}$ is said to be *bounded above* or *bounded below*, according to whether the set $\{a_n : n \in \mathbb{N}\}$ is (sometimes, the set of elements of the sequence is also denoted by $\{a_n\}$). A sequence $\{a_n\}$ is said to be *bounded* if the sequence $\{|a_n|\}$ is bounded above.

Definition 7.2. A sequence $\{a_n\}$ of reals is said to *converge* if $\exists L \in \mathbb{R}$ s.t. $\forall \varepsilon > 0 \, \exists N \in \mathbb{N}$ s.t. $n \geq N \implies |a_n - L| < \varepsilon$. We then call L the *limit* of $\{a_n\}$ and write $\lim_{n \to \infty} a_n = L$, sometimes also as $\lim_n a_n$ or simply $\lim a_n$.

Lemma 7.1. Every sequence $\{a_n\}$ with finite limit L is necessarily bounded.

Proof. Pick any $\varepsilon > 0$. By definition, $\exists N \in \mathbb{N}$ s.t. $\forall n \geq N, |a_n - L| < \varepsilon$. This means that, by the triangle inequality, $\forall n \geq N, |a_n| \leq |L| + |a_n - L| < |L| + \varepsilon$ so that $\max\{|a_1|, |a_2|, \ldots, |a_{N-1}|, |L| + \varepsilon\}$ is an upper bound of $\{|a_n| : n \in \mathbb{N}\}$. □

Lemma 7.2. Let set A s.t. $\emptyset \subset A \subset \mathbb{R}$ be bounded below. Define $-A = \{-x | x \in A\}$. Then $\sup(-A) = -\inf A$.

Proof. $\emptyset \subset A \subset \mathbb{R} \implies \emptyset \subset -A \subset \mathbb{R}$, and A is bounded below implies that $-A$ is bounded above, so that both sides are defined. Let $\alpha = \inf A$, then by definition, (a) $\forall x \in A, \alpha \leq x$ and (b) $\alpha < x \implies \exists y \in A$ s.t. $y \leq x$. Multiplying everything by -1, we get that (a)$\forall x \in A, -\alpha \geq -x$ and (b) $-\alpha > -x \implies \exists y \in A$ s.t. $-y \geq -x$, which is exactly the definition of $\sup(-A)$. □

Theorem 8 (Monotone Convergence Theorem). *If $\{a_n\}$ is a monotone sequnce of reals, then it has a finite limit iff it is bounded.*

Proof. For the sufficiency, assume first that the sequence $\{a_n\}$ is weakly increasing and bounded above. Then by the LUBP of the reals, $c = \sup_n \{a_n\}$ exists finitely. We show that $\lim_{n \to \infty} a_n = c$. By definition of supremum, $\forall \varepsilon > 0, \exists N \in \mathbb{N}$ s.t. $a_N > c - \varepsilon$, else $c - \varepsilon$ would be an upper bound of $\{a_n\}$, a contradiction. Since $\{a_n\}$ is weakly increasing and c an upper bound, we get that $0 \leq c - a_N < \varepsilon$ and that $\forall n \geq N, |c - a_n| \leq |c - a_N| < \varepsilon$. Therefore, by definition, $\lim_{n \to \infty} a_n = c$. Now if $\{a_n\}$ were to be weakly decreasing in stead, then the sequence $\{-a_n\}$ would be weakly increasing and bounded so that it would have a finite limit; call it $-c$. Then it is easy to see using Lemma 7.2 that $\lim_{n \to \infty} a_n = c$ here as well. Lemma 7.1 establishes the necessity. □

7.3   Bolzano-Weierstrass Theorem

The following is taken from Bartle and Sherbert[2].

Definition 7.3. Given a sequence $\{a_n\}$, consider an increasing sequence $\{n_k\}$ of positive integers. Then the sequence $\{a_{n_k}\}$ is called a *subsequence* of $\{a_n\}$. If it converges, its limit is called a *subsequential limit* of $\{a_n\}$.

Lemma 7.3. Every sequence $\{a_n\}$ of reals has a monotone subsequence.

Proof. We call the mth term a_m a "peak" if $\forall n \geq m, a_n \leq a_m$. Note that in a decreasing sequence, every term is a peak and in an increasing sequence, no term is a peak. We split into cases:

Case 1. $\{a_n\}$ has infinitely many peaks. Then we list the peaks by increasing subscripts $n_1 < n_2 < \cdots < n_k < \cdots$. Since each term is a peak, $a_{n_1} \geq a_{n_2} \geq \cdots \geq a_{n_k} \geq \cdots$ so that $\{a_{n_k}\}$ is a weakly decreasing subsequence.

Case 2. Suppose there are only finitely many (possibly zero) peaks. List them out by increasing subscripts: $a_{n_1}, a_{n_2}, \cdots, a_{n_r}$. Let $s_1 := m_r + 1$. Since a_{s_1} is not a peak, $\exists s_2 > s_1$ s.t. $a_{s_1} < a_{s_2}$. Since a_{s_2} is not a peak, $\exists s_3 > s_2$ s.t. $a_{s_2} < a_{s_3}$. Continuing this way, we get that the subsequence $\{a_{s_k}\}$ is increasing. $\square$

Theorem 9 (Bolzano-Weierstrass Theorem). *If $\{a_n\}$ is a bounded sequence of reals, then it has a convergent subsequence.*

Proof. By Lemma 7.3, $\{a_n\}$ has a monotone subsequence $\{a_{n_k}\}$. Since $\{a_n\}$ is bounded, $\{a_{n_k}\}$ must be bounded too. Then by the Monotone Convergence Theorem, $\{a_{n_k}\}$ is such a convergent subsequence. $\square$

7.4   Cauchy Completeness

This section is taken from Pugh[3].

Definition 7.4. A sequence $\{a_n\}$ is said to be a *Cauchy sequence* if $\forall \varepsilon > 0 \exists N \in \mathbb{N}$ s.t. $n, m \geq N \implies |a_n - a_m| < \varepsilon$.

Clearly, every convergent sequence of real numbers is a Cauchy sequence. To prove this, consider a convergent sequence $\{a_n\}$ with limit L. For given $\varepsilon > 0$, we may choose $N \in \mathbb{N}$ s.t. $n \geq N \implies |a_n - L| < \frac{\varepsilon}{2}$. This means that for $m, n \geq L$, by the triangle inequality, $|a_n - a_m| \leq |a_n - L| + |a_m - L| < \varepsilon$ as required. The converse of this statememnt is, along with the Archimedean property, equivalent to the other definitions of completeness. Here we only prove one direction of the equivalence.

Theorem 10. $\mathbb{R}$ *is* **complete** *with respect to Cauchy sequences. That is, every Cauchy sequence of reals is convergent.*

Proof. We first show that $\{a_n\}$ is bounded; indeed, the proof is similar to that of Lemma 7.1. Pick any $\varepsilon > 0$. By definition, $\exists N \in \mathbb{N}$ s.t. $\forall n \geq N, |a_n - a_N| < \varepsilon$. This means that, by the triangle inequality, $\forall n \geq N, |a_n| \leq |a_N| + |a_n - a_N| < |a_N| + \varepsilon$ so that $M = \max\{|a_1|, |a_2|, \ldots, |a_{N-1}|, |a_N| + \varepsilon\}$ is an upper bound of $\{|a_n| : n \in \mathbb{N}\}$. Now consider the set $S = \{x \in [-M, M] : \exists m \in \mathbb{N}, |\{n \in \mathbb{N} : a_n < x\}| = m\}$, that is the set of all $x \in [-M, M]$ such that $\exists$ infinitely many $n \in \mathbb{N}$ for which $a_n \geq x$. Clearly, $-M \in S$ and S is bounded above by M so that by the LUBP, $b = \sup S$ exists finitely in $[-M, M]$. We claim that $\lim a_n = b$.

Given $\varepsilon > 0$ we must show that $\exists N \in \mathbb{N}$ s.t. $n \geq N \implies |a_n - b| < \varepsilon$. Since the sequence $\{a_n\}$ is Cauchy, $\exists N_1 \in \mathbb{N}$ s.t. $m, n \geq N_1 \implies |a_m - a_n| < \frac{\varepsilon}{2}$. Since b is an upper bound of S, $b + \frac{\varepsilon}{2} \notin S$ meaning that there are only finitely many n s.t. $a_n \geq b + \frac{\varepsilon}{2}$ and thus $\exists N_2 \geq N_1$ s.t. $n \geq N_2 \implies a_n \leq b + \frac{\varepsilon}{2} \implies |a_n - b| \leq \frac{\varepsilon}{2}$. Since b is the supremum of S, the smaller number $b - \frac{\varepsilon}{2}$ cannot also be an upper bound meaning that $\exists x \in S$ s.t. $a_n \geq x > b - \frac{\varepsilon}{2}$ infinitely often. In particular, $\exists N \geq N_2$ s.t. $a_N > b - \frac{\varepsilon}{2}$. Since $N \geq N_2$ we have that $a_N \leq b + \frac{\varepsilon}{2}$ so that $a_N \in (b - \frac{\varepsilon}{2}, b + \frac{\varepsilon}{2}]$. Hence for $n \geq N$, we have that $|a_n - b| \leq |a_n - a_N| + |a_N - b| < \varepsilon$ as desired. $\square$

7.5   Cantor's Nested Intervals Theorem

Definition 7.5. We define *intervals* of reals as follows. For $a, b \in \mathbb{R}$ and $a < b$, define the *closed interval* $[a, b] = \{x | x \in \mathbb{R}, a \leq x \leq b\}$. Define the *open interval* $(a, b) = \{x | x \in \mathbb{R}, a < x < b\}$. We define *half-open* or *half-closed* interval $[a, b)$ and $(a, b]$ with the appropriate equality on one side only. We define the unbounded interval $[a, +\infty) = \{x | x \in \mathbb{R}, a \leq x\}$ and we define $(-\infty, a], (a, +\infty)$, and $(-\infty, a)$ analogously. We consider $[a, +\infty)$ and $(-\infty, a]$ to be closed, and $(a, +\infty)$ and $(-\infty, a)$ to be open. For $x \in \mathbb{R}$ and given a $\delta > 0$, we define the δ-neighborhood (shortened as δ-n.b.d.) of x as $N_\delta(x) = \{t : |t - x| < \delta\} = (x - \delta, x + \delta)$.

Theorem 11 (Cantor's Nested Intervals Theorem). *Given a nested sequence of closed, bounded intervals of real numbers $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \cdots$, we must have that $\bigcap_{n=1}^{\infty} I_n \neq \emptyset$.*

Note that both the terms *closed* and *bounded* are very important, for we see that there are counterexamples whenever either term is missing: $\bigcap_{n=1}^{\infty} (0, \frac{1}{n}) = \emptyset$ and $\bigcap_{n=1}^{\infty} [n, +\infty) = \emptyset$.

Proof. Let the n$^{\text{th}}$ interval I_n be given by $I_n = [a_n, b_n]$ for some $a_n, b_n \in \mathbb{R}$. Note that this captures the fact that these are both *closed* and *bounded*. Consider the sequence $\{a_n\}$. Then this sequence is weakly increasing because of the nesting, and is also bounded by $\max\{|a_1|, |b_1|\}$. Therefore, by the Monotone Convergence Theorem, it has a finite limit which is its supremum; call it $c = \sup_n \{a_n\}$. We show that $c \in \bigcap_{n=1}^{\infty} I_n$. Pick any $n \in \mathbb{N}$. Because c is an upper bound of the sequence $\{a_n\}$, we must have $a_n \le c$. Now since by nesting b_n is also an upper bound of the sequence, c being the *least* upper bound means that $c \le b_n$. Combining, this means that $c \in [a_n, b_n]$. Since this is true for each n, we get that $c \in \bigcap_{n=1}^{\infty} [a_n, b_n]$. $\qquad\square$

A more leisurely and complete treatment can be found in Bartle and Sherbert[2].

7.6 Heine-Borel Theorem for $\mathbb{R}$

The Heine-Borel Theorem is one of the standard results in topology that a student learns early on. Here we state the general Heine-Borel theorem, but only prove a small special case of it that is a direct consequence of the completeness of the reals.

Theorem 12 (Heine-Borel Theorem). *For any $S \subseteq \mathbb{R}^n$, S is closed and bounded iff it is compact, i.e. every open cover of S has a finite subcover.*

Definition 7.6. A set $S \subseteq \mathbb{R}$ is called *compact* if every open cover of S has a finite subcover. This means that for an index set A such that if for $\alpha \in A$, U_α are open intervals and $S \subseteq \bigcup_{\alpha \in A} U_\alpha$, then $\exists$ finitely many $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$ s.t. $S \subseteq \bigcup_{k=1}^{n} U_{\alpha_k}$.

Theorem 13 (Special Case of Heine-Borel Theorem). *Any $[a, b] \subseteq \mathbb{R}$ must be compact.*

Note that any singleton set $\{a\}$ for $a \in \mathbb{R}$ must be compact, since only one open interval containing a suffices. Hence, we may assume that $a < b$.

Proof 1. Let A be an index set such that for each $\alpha \in A, U_\alpha$ is an open interval and $[a, b] \subseteq \bigcup_{\alpha \in A} U_\alpha$. Now for this open cover, consider the set $S = \{x \in [a, b] : [a, x]$ can be covered by finitely many $U_\alpha\}$. We show that $b \in S$. Now obviously $a \in S$ and b is an upper bound of S, so that $c = \sup S$ exists. Further $a \le c \le b \implies c \in [a, b]$. Now $\{U_\alpha\}_{\alpha \in A}$ covers $[a, b] \implies \exists \alpha_1 \in A$ s.t. $a \in U_{\alpha_1} = (p_1, q_1)$ for some p_1, q_1. Then $[a, a + \frac{q_1 - a}{2}] \subseteq U_{\alpha_1}$ can be covered by finitely many (just one) U_α and so $a + \frac{q_1 - a}{2} \in S$. Since c is an upper bound of S, $a < a + \frac{q_1 - a}{2} \le c \implies a < c$.
Again, since $\{U_\alpha\}$ covers $[a, b], \exists \alpha_2 \in A$ s.t. $c \in U_{\alpha_2} = (p_2, q_2)$ for some $p_2, q_2 \in \mathbb{R}$. Let $0 < \delta = \frac{1}{2} \min\{c - a, c - p_2, q_2 - c\}$ so that $N_\delta(c) \subseteq U_{\alpha_2}$. Since c is the supremum of S, $\exists t \in S \cap (c - \frac{\delta}{2}, c]$, else $c - \frac{\delta}{2}$ is a smaller upper bound. Then $[a, t]$ is compact $\implies \exists$ finitely many $\alpha_3, \alpha_4, \ldots, \alpha_n \in A$ s.t. $[a, t] \subseteq \bigcup_{k=3}^{n} U_{\alpha_k}$. Then $[a, c] \subseteq [a, t] \cup N_\delta(c) \subseteq \bigcup_{k=2}^{n} U_{\alpha_k}$ meaning that $c \in S$.
Now assume that $c < b$. Let $0 < \delta' = \frac{1}{2} \min\{\delta, b - c\}$ so that $N'_\delta(c) \subseteq U_{\alpha_2} \cap (a, b)$. This means that $[a, c + \frac{\delta'}{2}] \subseteq [a, c] \cup N_{\delta'}(c) \subseteq \bigcup_{k=2}^{n} U_{\alpha_k} \implies c + \frac{\delta'}{2} \in S$, a contradiction to c being an upper bound. $\qquad\square$

The following alternative proof, which beautifully uses the Nested Intervals Theorem, is taken from [4].

Proof 2. Assume that $[a, b]$ is non-compact. Then $\exists$ an open cover $\{U_\alpha\}$ of $[a, b]$ such that it has no finite subcover of $[a, b]$. Then, it cannot be covered by finitely many intervals from $\{U_\alpha\}$. Divide the interval $[a, b] = [a, \frac{1}{2}(a + b)] \cup [\frac{1}{2}(a + b), b]$. Not both of these can have a finite subcover of $\{U_\alpha\}$, else so does $[a, b]$. Pick one which does not have a finite subcover and call it $[a_1, b_1]$. Repeat this construction to get a nested sequence of closed, bounded intervals $[a, b] \supseteq [a_1, b_1] \supseteq [a_2, b_2] \supseteq \cdots$, none of which is compact. The width of these intervals $b_n - a_n = \frac{1}{2^n}(b - a)$ approaches 0. By Cantor's Nested Intervals Theorem, $\exists c \in \bigcap_{n=0}^{\infty} [a_n, b_n]$, where $[a_0, b_0] = [a, b]$. Since $\{U_\alpha\}$ covers $[a, b], \exists U_{\alpha_1} = (p, q) \in \{U_\alpha\}$ s.t. $c \in U_{\alpha_1}$. Then for $0 < \delta = \frac{1}{2} \min\{c - p, q - c\}$ we have that $N_\delta(c) \subseteq U_{\alpha_1}$. Now pick $n \in \mathbb{N}$ s.t. $n \ge \log_2 \frac{b - a}{\delta}$. This means that $0 < \frac{b - a}{\delta} \le 2^n \implies 0 < b_n - a_n \le \delta \implies [a_n, b_n] \subseteq N_{b_n - a_n}(c) \subseteq N_\delta(c) \subseteq U_{\alpha_1}$ meaning that $[a_n, b_n]$ has a finite subcover of $\{U_\alpha\}$, a contradiction. $\qquad\square$

7.7 Extreme and Intermediate Value Theorems

Definition 7.7. Given a function $f : \text{Dom}_f \subseteq \mathbb{R} \to \mathbb{R}$ and $S \subseteq \text{Dom}_f$, define the *image* of S under f as $f(S) = \{f(t) | t \in S\}$.

Definition 7.8. Given a function $f : \text{Dom}_f \subseteq \mathbb{R} \to \mathbb{R}$, we define the function to be *continuous* at $x \in \text{Dom}_f$ if $\forall \varepsilon > 0, \exists \delta > 0$ s.t. $f(N_\delta(x) \cap \text{Dom}_f) \subseteq N_\epsilon(f(x))$. We define a function f to be continuous on a set $C_f \subseteq \text{Dom}_f$ if f is continuous at all $x \in C_f$.

Theorem 14 (Boundedness Theorem)**.** *The set of values achieved by a continuous function on a closed interval forms a bounded subset of $\mathbb{R}$. Mathematically phrasing, given $a, b \in \mathbb{R}, a < b$ and a continuous function $f : [a, b] \to \mathbb{R}, \exists m, M \in \mathbb{R}$ s.t. $\forall x \in [a, b], m \leq f(x) \leq M$.*

The following is, in essence, from Pugh[3].

Main Proof 1. For $x \in [a, b]$, define $S = \{x \in [a, b] | \exists m, M \in \mathbb{R}, f([a, x]) \subseteq [m, M]\}$. We show that $b \in S$. Clearly, $a \in S$ and b is an upper bound of S. Since S is non-empty and bounded above, by the LUBP, $c = \sup S$ exists finitely and $a \leq c \leq b$. Now pick some $\varepsilon > 0$. By continuity of f at a, we have that $\exists \delta > 0$ s.t. $x \in [a, a + \delta) \implies f(x) \in (f(a) - \varepsilon, f(a) + \varepsilon)$. This means that $a + \frac{\delta}{2} \in S$. Since $c = \sup S$, we must have that $a + \frac{\delta}{2} \leq c$ implying that $a < c$.
This collectively means that $c \in (a, b]$, and hence f is continuous at c. Fix any $\varepsilon > 0$, and choose $\delta > 0$ s.t. $|x - c| < \delta \implies |f(x) - f(c)| < \varepsilon$. Now let $0 < \delta' = \min\{\delta, c - a\}$. Since c is the *least* upper bound of S, $\exists t \in S \cap (c - \frac{\delta'}{2}, c]$, else $c - \frac{\delta'}{2}$ would be a smaller upper bound. Then by definition of S, $\exists m, M \in \mathbb{R}$ s.t. $f([a, t]) \subseteq [m, M]$. This means that $f([a, c]) \subseteq f([a, t]) \cup f((c - \frac{\delta'}{2}, c]) \subseteq [m, M] \cup N_\varepsilon(f(c))$, which is bounded since it is a union of two bounded intervals. This proves that $c \in S$. Now if $c < b$, we could pick $0 < \delta'' = \frac{1}{2}\min\{\delta', b - c\}$ and then $f([a, c + \delta''])$ would still be a subset of $[m, M] \cup N_\varepsilon(f(c))$, meaning that $c + \delta'' \in S$, a contradiction to c being an upper bound of S. $\qquad\square$

The following alternative proof that uses the Bolzano-Weierstrass Theorem is from Bartle and Sherbet[2]. We first prove a preliminary lemma.

Lemma. If a convergent sequence $\{x_n\}$ is such that $\forall n \in \mathbb{N}, a \leq x_n \leq b$, then $a \leq \lim x_n \leq b$.

Proof. If that were not the case then either $x := \lim x_n < a$ or $x > b$. If $x < a$ then letting $0 < \varepsilon = \frac{1}{2}(a - x), \exists n \in \mathbb{N}$ s.t. $m \geq n \implies |x_m - x| < \varepsilon$, a contradiction since $N_\varepsilon(x) \cap [a, b] = \emptyset$. Similarly, if $x > b$ then we obtain a contradiction by letting $0 < \varepsilon = \frac{1}{2}(x - b)$. $\qquad\square$

Main Proof 2. Suppose that f is not bounded on $[a, b]$. Then $\forall n \in \mathbb{N}, \exists x_n \in [a, b]$ s.t. $|f(x_n)| > n$. Since $[a, b]$ is bounded, the sequence $X := \{x_n\}$ is bounded; hence, by the Bolzano-Weierstrass Theorem, there is a subsequence $X' = \{x_{n_r}\}$ of X that converges to a number x. By the preliminary lemma, we have that $x \in [a, b]$. This means that f is continuous at x. We claim that, by continuity, $\lim f(x_{n_r}) = f(x)$.
Pick $\varepsilon > 0$. Then by continuity of f at $x, \exists \delta > 0$ s.t. $\forall x' \in N_\delta(x) \cap [a, b] \neq \emptyset, |f(x) - f(x')| < \varepsilon$. Since $\lim x_{n_r} = x, \exists s \in \mathbb{N}$ s.t. $\forall r \geq s, |x_{n_r} - x| < \delta \implies |f(x_{n_r}) - f(x)| < \varepsilon$. This means that $\forall \varepsilon > 0, \exists s \in \mathbb{N}$ s.t. $\forall r \geq s, |f(x_{n_r}) - f(x)| < \varepsilon$, which is precisely what is meant by $\lim f(x_{n_r}) = f(x)$. Now since $x \in \text{Dom}_f$, $f(x)$ exists finitely. By Lemma 7.1, this means that the sequence $f(x_{n_r})$ is bounded, a contradiction to $|f(x_{n_r})| > n_r \geq r$. $\qquad\square$

To see that each of the hypotheses of the theorem statement is necessary, consider the following counterexamples whenever one is missing:
1. The domain must be bounded. For $f : [0, +\infty) \to \mathbb{R}$ given by $f(x) = x$, $f([0, +\infty))$ is not bounded.
2. The domain must be closed. For $f : (0, 1] \to \mathbb{R}$ given by $f(x) = 1/x$, $f((0, 1])$ is not bounded.
3. The function must be continuous. For $f : [0, 1] \to \mathbb{R}$ given by $f(x) = \begin{cases} 0 & x = 0, \\ 1/x & x \in (0, 1] \end{cases}$, $f([0, 1])$ is not bounded.

Now we prove two of very important theorems in the analysis of continuous functions. But first, we prove a lemma.

Lemma 7.4. If A, B are nonempty bounded subsets of $\mathbb{R}$ then
(i) $A \subseteq B \implies \sup A \leq \sup B$,
(ii) $\sup A, \sup B \leq \sup(A \cup B) \leq \max\{\sup A, \sup B\}$.

Proof. For (i), note that $A \subseteq B$ means that every upper bound of B is an upper bound of A. In particular, $\sup B$ is an upper bound of A so that $\sup A \leq \sup B$. The first part of (ii) is true because $A, B \subseteq A \cup B$. For the second part, assume that $x \in A \cup B$. Then $x \in A$ or $x \in B$. In either case, $x \leq \max\{\sup A, \sup B\}$ so that $\max\{\sup A, \sup B\}$ is an upper bound of $A \cup B$. This means that $\sup(A \cup B) \leq \max\{\sup A, \sup B\}$. $\qquad\square$

Now we proceed to the main theorems, again essentially following Pugh[3].

Theorem 15 (Extreme Value Theorem). *A continuous function on a closed domain takes its absolute minimum and maximum values. That is, given a continuous function $f : [a,b] \to \mathbb{R}, \exists x_m, x_M \in [a,b]$ s.t. $\forall x \in [a,b], f(x_m) \leq f(x) \leq f(x_M)$.*

Proof. The theorem is trivially true if $a = b$. Hence assume that $a < b$. We first show that $\exists x_M \in [a,b]$ s.t. $\forall x \in [a,b], f(x) \leq f(x_M)$. Let $M = \sup f([a,b])$, which exists by Theorem 14. If $f(a) = M$ we have found $x_M = a$. Hence consider the case where $f(a) < M$. Consider the set $S = \{x \in [a,b] : \sup f([a,x]) < M\}$. Since $a \in S \implies S \neq \emptyset$, and S is bounded above by b, we have that $c = \sup S$ exists and $a \leq c \leq b$ and so (a) f is continuous at c and (b) $f(c) \leq M$.

By continuity at a, for $0 < \varepsilon = \frac{1}{2}(M - f(a)), \exists \delta \in (0, \frac{b-a}{2}]$ s.t. $x \in [a, a+\delta) \implies f(x) \in (f(a) - \varepsilon, f(a) + \varepsilon)$. This means that $\sup f([a, a + \frac{\delta}{2}]) \leq M - \varepsilon < M$ so that $a + \frac{\delta}{2} \in S$ and $a < a + \frac{\delta}{2} \leq c \implies a < c$. Now since $[a,c] \subseteq [a,b]$, by Lemma 7.4, $\sup f([a,c]) \leq M$ and so we split into cases:

Case 1 If $\sup f([a,c]) < M$ then $c \in S$ and so $f(c) < M$. By continuity, for $0 < \varepsilon = \frac{1}{2}(M - f(c)), \exists \delta \in (0, \frac{c-a}{2}]$ s.t. $|x - c| < \delta \implies |f(x) - f(c)| < \varepsilon \implies f(x) < M - \varepsilon$. This means that $\sup(N_\delta(c)) \leq M - \varepsilon < M$. Now since $c = \sup S, \exists t \in S \cap (c - \delta, c]$. For this t, $\sup f([a,t]) < M \implies \sup f([a,t]) \leq M - \frac{M - \sup f([a,t])}{2} < M$. Now since $[a, c + \frac{\delta}{2}] \subseteq [a,t] \cup N_\delta(c)$, $f([a, c + \frac{\delta}{2}]) \subseteq f([a,t]) \cup f(N_\delta(c))$ so that by Lemma 7.4, $\sup f([a, c + \frac{\delta}{2}]) \leq \max\{\sup f([a,t]), \sup f(N_\delta(c))\} < M \implies c + \frac{\delta}{2} \in S$, a contradiction to c being an upper bound. Therefore, this case is not possible.

Case 2 If $\sup f([a,c]) = M$, $c \in S$. Now we proceed to use proof by contradiction to show that $f(c) = M$. If it were the case that $f(c) < M$ then by continuity for $0 < \varepsilon = \frac{1}{2}(M - f(c)), \exists \delta \in (0, \frac{c-a}{2}]$ s.t. $|x - c| < \delta \implies |f(x) - f(c)| < \varepsilon$. This means that $\sup f(N_\delta(c)) \leq M - \varepsilon < M$. Again, since $c = \sup S, \exists t \in S \cap (c - \delta, c]$. For this t, $f([a,t]) < M \implies \sup f([a,t]) \leq M - \frac{M - \sup f([a,t])}{2} < M$. Now $[a,c] \subseteq [a,t] \cup N_\delta(c)$ so that $M = \sup f([a,c]) \leq \max\{\sup f([a,t]), \sup f(N_\delta(c))\} < M$, a contradiction. This shows that $f(c) = M$ and hence we find that $x_M = c$ works.

To show the existence of $x_m \in [a,b]$ s.t. $\forall x \in [a,b], f(x_m) \leq f(x)$, we could use an argument similar to the one above by using $\inf f([a,x])$ in place of $\sup f([a,x])$ and slight modifications (and the reader is encouraged to fill in the details). However, we proceed indirectly. Consider the reflection of f in the x-axis; that is, consider the function $(-f) : [a,b] \to \mathbb{R}$ given by $(-f)(x) = -f(x)$. Now, it is obvious from the definition of continuity that the continuity of f implies the continuity of $(-f)$. This means that we may apply the first part of the proof to obtain $x_m \in [a,b]$ s.t. $\forall x \in [a,b], (-f)(x) \leq (-f)(x_m) \implies -f(x) \leq -f(x_m)$. This means that for this $x_m \in [a,b]$, we have $\forall x \in [a,b], f(x_m) \leq f(x)$, which is what we wanted to prove. $\square$

Theorem 16 (Intermediate Value Theorem). *For some $a,b \in \mathbb{R}, a < b$, consider an interval $[a,b] \subset \mathbb{R}$ and a continuous function $f : [a,b] \to \mathbb{R}$. Then we have that $\forall \gamma \in [\min\{f(a), f(b)\}, \max\{f(a), f(b)\}], \exists c \in [a,b]$ s.t. $f(c) = \gamma$.*

Proof. If $f(a) = f(b)$ then γ can take only one value, and $c = a$ or $c = b$ works. Hence, assume that $f(a) \neq f(b)$. First assume that $f(a) < f(b)$. If $\gamma = f(a)$ or $\gamma = f(b)$ we are done, since we can choose $c = a$ or $c = b$ respectively. Hence, assume that $\gamma \in (f(a), f(b))$. Now consider the set $S = \{x \in [a,b] : \sup f([a,x]) \leq \gamma\}$. Since $a \in S \implies S \neq \emptyset$ and S is bounded above by b, we have that $c = \sup S$ exists and $c \in [a,b]$. By continuity at a, for $0 < \varepsilon = \gamma - f(a), \exists \delta \in (0, \frac{b-a}{2}]$ s.t. $x \in [a, a+\delta) \implies f(x) \in (f(a) - \varepsilon, f(a) + \varepsilon) \implies f(x) < \gamma$. This means that $\sup f([a, a + \frac{\delta}{2}]) \leq \gamma$ so that $a + \frac{\delta}{2} \in S$ and $a < a + \frac{\delta}{2} \leq c \implies a < c$. We show that $f(c) = \gamma$ by showing that neither $f(c) < \gamma$ nor $f(c) > \gamma$ is possible.

If $f(c) < \gamma$, then by continuity of f at c, for $0 < \varepsilon = \gamma - f(c), \exists \delta \in (0, \frac{c-a}{2}]$ s.t. $x \in N_\delta(c) \implies f(x) \in N_\varepsilon f(c) \implies f(x) < \gamma$. This means that $\sup f(N_\delta(c)) \leq \gamma$. Since $c = \sup S, \exists t \in S \cap (c - \delta, c]$. For this t, $\sup f([a,t]) \leq \gamma$. Since $f([a, c + \frac{\delta}{2}]) \subseteq f([a,t]) \cup f(N_\delta(c))$ so that by Lemma 7.4, $\sup f([a, c + \frac{\delta}{2}]) \leq \max\{\sup f([a,t]), \sup f(N_\delta(c))\} \leq \gamma \implies c + \frac{\delta}{2}$, a contradiction to c being an upper bound.

If $f(c) > \gamma$, then by continuity of f at c, for $0 < \varepsilon = f(c) - \gamma, \exists \delta \in (0, \frac{c-a}{2}]$ s.t. $x \in N_\delta(c) \implies f(x) \in N_\varepsilon(f(c)) \implies \gamma = f(c) - \varepsilon < f(x)$. Since $c = \sup S, \exists t \in S \cap (c - \delta, c]$. For this t, $\sup f([a,t]) \leq \gamma$, a contradiction to $\gamma < f(t)$ as required.

Now if $f(a) > f(b)$ we can again assume that $\gamma \neq f(a)$ and $\gamma \neq f(b)$ so that $\gamma \in (f(b), f(a))$. Here we could again use an argument similar to the one above by using $\inf f([a,x])$ in place of $\sup f([a,x])$ and slight modifications (and, again, the reader is encouraged to fill in the details). However, here again, we proceed indirectly.[1] Consider again the reflection of f in the x-axis; that is, consider the function $(-f) : [a,b] \to \mathbb{R}$ given by $(-f)(x) = -f(x)$. Now, it is obvious, as before, that $(-f)$ is continuous. Now $f(a) > f(b) \implies (-f)(a) < (-f)(b)$ so that we may apply the first part of the proof to obtain that $\forall -\gamma \in ((-f)(a), (-f)(b)), \exists c \in [a,b]$ s.t. $(-f)(c) = -\gamma$. This is the same as saying that $\forall \gamma \in (f(b), f(a)), \exists c \in [a,b]$ s.t. $f(c) = \gamma$, *quod erat demonstrandum*. $\square$

---

[1]The author believes that this approach is cleverer than merely restating the above part of the proof with the infimum.

8 Non-denumerability of the Continuum

We have shown that there are gaps in the rational numbers, but the reals are complete. Just how much of the real number line do the rationals cover? The answer comes in two parts. The first is that the rationals are closely knit with the reals, that they are *dense* on the reals, meaning that every open interval of the reals contains at least one rational, and hence infinitely many of them. This also means that any real number can be approximated by a rational to any desired degree of accuracy. This part has been taken from Rudin[1].

Definition 8.1. A set $S \subseteq \mathbb{R}$ is said to be *dense* on $\mathbb{R}$ if $\forall a, b \in \mathbb{R}, a < b$, we have that $S \cap (a, b) \neq \emptyset$.

Theorem 17. *If $S \subseteq \mathbb{R}$ is dense on $\mathbb{R}$ then every open interval $\emptyset \subset (a, b) \subset \mathbb{R}$ contains infinitely many members of S.*

Proof. Suppose that some interval $\emptyset \subset (a, b) \subset \mathbb{R}$ has only finitely many members of S, and let these be denoted by $s_1, s_2, \ldots, s_n$ for some $n \in \mathbb{N}$ (note that $n \geq 1$ by our hypothesis that S is dense). Then each of the terms $s_1 - a, s_2 - a, \ldots, s_n - a$ is positive. Let $0 < \delta = \frac{1}{2} \min\{s_1 - a, s_2 - a, \ldots, s_n - a\}$. Then $(a, a + \delta) \cap S = \emptyset$, a contradiction to our hypothesis that S is dense. $\square$

Theorem 18. $\mathbb{Q}$ *is dense on* $\mathbb{R}$.

Proof. Consider any open interval $\emptyset \subset (a, b) \subset \mathbb{R}$. Since $a < b$, we have $b - a > 0$ so that by the Archimedean property of the reals (Theorem 6), $\exists n \in \mathbb{N}$ s.t. $n(b-a) > 1$. Since $1 > 0$, by applying Theoerm 6 again, we obtain $m_1, m_2 \in \mathbb{N}$ s.t. $m_1 \cdot 1 > na$ and $m_2 \cdot 1 > -na$ and hence $-m_2 < na < m_1$. Consider $E = \{m | na < m\} \subseteq \mathbb{Z}$. Since $m_1 \in E, E \neq \emptyset$ and since $-m_2 \notin E$ and $l \notin E, k \leq E \implies k \notin E$, E is bounded below. Therefore, by Corollary 1, E has a minimal element; call it m. Then $-m_2 < m \leq m_1$ and $m - 1 \leq na < m$. Combining, $na < m \leq 1 + na < nb$ and since $n > 0$, we have $a < \frac{m}{n} < b$ so that $\frac{m}{n} \in \mathbb{Q} \cap (a, b)$. $\square$

This theorem also immediately implies that the set of irrationals, $\mathbb{R} \setminus \mathbb{Q}$ is dense on $\mathbb{R}$.

Corollary 18.1. $\mathbb{R} \setminus \mathbb{Q}$ *is dense on* $\mathbb{R}$.

Proof. We know that $\sqrt{2} \notin \mathbb{Q}$. Consider any open interval $\emptyset \subset (a, b) \subset \mathbb{R}$. Now consider the modified interval $\left(\frac{a}{\sqrt{2}}, \frac{b}{\sqrt{2}}\right)$. Using the density of $\mathbb{Q}$ on $\mathbb{R}$, we may pick $r \in \mathbb{Q} \cap \left(\frac{a}{\sqrt{2}}, \frac{b}{\sqrt{2}}\right)$ such that $r \neq 0$, which is possible since $\mathbb{Q} \cap \left(\frac{a}{\sqrt{2}}, \frac{b}{\sqrt{2}}\right)$ has infinitely many elements. Then $\frac{a}{\sqrt{2}} < r < \frac{b}{\sqrt{2}}$ and $\sqrt{2} > 0$ implies that $a < r\sqrt{2} < b$. Since the rationals are closed under multiplication and $r \neq 0$, $r\sqrt{2} \notin \mathbb{Q}$ so that $r\sqrt{2} \in \left(\mathbb{R} \setminus \mathbb{Q}\right) \cap (a, b)$. $\square$

Corollary 18.2. *For any given $x \in \mathbb{R}$, $\forall \varepsilon > 0, \exists q \in \mathbb{Q}$ s.t. $|x - q| < \varepsilon$.*

Proof. By the theorem, $\exists q \in \mathbb{Q} \cap N_\varepsilon(x)$. $\square$

This discussion shows that there are infinitely many rationals and irrationals in any open interval on the reals. However, the second part of the answer, and the more truthful one, is that even though there are infinitely many of the rationals and infinitely many of the reals, the set of rationals is much, much smaller than the set of reals. We put this on more formal footing in the following discussion.

Definition 8.2. For sets A and B, we say that they are *equivalent*, written as $A \sim B$ if there exists a bijective function $f : A \to B$. For finite sets, this means that both the sets have the same cardinality, i.e. $|A| = |B|$. We then retain this as the definition of the statement $|A| = |B|$ even when A and B are not finite.

We denote the "cardinality" of the set of natural numbers by $|\mathbb{N}| = \aleph_0$. By this we mean that if for some set S, we write $|S| = \aleph_0$, what we mean is nothing more than $S \sim \mathbb{N}$. Similarly, we denote the "cardinality" of the continuum of real numbers by $|\mathbb{R}| = \mathfrak{c}$. We introduce some more terminology.

Definition 8.3. For $n \in \mathbb{N}$, let $I_n = \mathbb{N} \cap [1, n]$. For a set A, we say that A is:
(a) *finite* if $A = \emptyset$ or $\exists n \in \mathbb{N}$ s.t. $A \sim I_n$.
(b) *infinite* if it is not finite.
(c) *countable* or *denumerable* if $A \sim \mathbb{N}$.
(d) *uncountable* or *non-denumerable* if it is neither finite not countable. Then we write $\aleph_0 < |A|$.

We notice three obvious and easy to prove facts:

1. $\mathbb{N} \sim \mathbb{Z}$, since the function $f : \mathbb{N} \to \mathbb{Z}$ defined by the formula $f(n) = \begin{cases} \frac{n}{2} & n \text{ even,} \\ -\frac{n-1}{2} & n \text{ odd.} \end{cases}$ is a bijection, as can be easily verified.
2. Obviously, for every sequence $\{x_n\}$ of distinct reals we have that $\{x_n\} \sim \mathbb{N}$.
3. Given any $a, b \in \mathbb{R}, a < b$ we have that $|(a, b)| = \mathfrak{c}$. To see this, consider the function $f : (a, b) \to \mathbb{R}$ given by $f(x) = \tan\left(\frac{\pi}{b-a}\left(x - \frac{a+b}{2}\right)\right)$, which can again be easily verified to be a bijection.

Now we prove something that is definitely not very obvious, yet equally easy to prove.

Lemma. Every infinite subset of E of a countable set S is countable.

Proof. Let S be countable. Then $S \sim \mathbb{N} \sim \{x_n\}$ means that we can order the elements of S in a sequence $x_1, x_2, x_3, \ldots$. Consider the set of indices $A_1 = \{n | n \in \mathbb{N}, x_n \in E\}$. Since E is infinite, A is a nonempty subset of natural numbers, so by the Well-Ordering principle, it has a minimal element; call it n_1. Now define $A_2 = \{n | n \in \mathbb{N}, n > n_1, x_n \in E\}$. Since E is infinite, A_2 is nonempty and again and so has a minimal element n_2. We know that a finite set cannote exhaust an infinite set and so continuing this way we get an infinite sequence of elements $\{x_{n_k}\}$, each in E. Further because of the way we choose n_k, every element in E in the first $n_k \geq k$ elements of S is exhausted by $\{x_{n_l}\}_{l=1}^k$. As k gets arbitrarily large, we see that every element of S is captured in the sequence $\{x_{n_k}\}$ and so $E = \{x_{n_k}\} \sim \mathbb{N}$. $\square$

Theorem 19. $\mathbb{Q}$ *is countable. That is,* $|\mathbb{Q}| = \aleph_0$.

Proof. By the previous lemma, it suffices to show a bijective function from $\mathbb{Q}$ to an infinite subset of the natural numbers. Now clearly any $q \in \mathbb{Q}$ can be written uniquely as $q = s \cdot \frac{a}{b}$ where $a, b \in \mathbb{N}$ with $\gcd(a,b) = 1$ and $s \in \{-1, 0, 1\}$ (a, b are unique when $s \neq 0$). Then $f : \mathbb{Q} \to \{2^a 3^b 5^{s+1} : a, b \in \mathbb{N}, \gcd(a,b) = 1, s \in \{-1, 1\}\} \cup \{5\}$ defined by $f(s \cdot \frac{a}{b}) = \begin{cases} 2^a 3^b 5^{s+1}, & \text{when } s \neq 0, \\ 5, & \text{when } s = 0. \end{cases}$ is a bijection, from the well-known Unique Factorization Theorem on natural numbers. $\square$

If you find this unsettling, rest assured that you are not the only one. We now proceed to prove what we aimed to. The following argument, originally due to Cantor, has been taken from Dunham's The Calculus Gallery[5].

Theorem 20. *If $\{x_n\}$ is a sequence of distinct reals, then for any $a, b \in \mathbb{R}, a < b$ we have that $(a, b) \setminus \{x_n\} \neq \emptyset$.*

Proof. Consider the subset $A = \{n \in \mathbb{N} : x_n \in (a, b)\} \subseteq \mathbb{N}$. If $A = \emptyset$ or $A \sim I_1$ then the theorem is true since (a, b) has infinitely many elements, and a finite set cannot exhaust an infinite set. Hence, assume that A has at least two distinct elements. Then, by the Well-Ordering principle, A has a minimal element n_1 and $A \setminus \{n_1\}$ has a minimal element n_2. Let $a_1 = \min\{x_{n_1}, x_{n_2}\}$ and $b_1 = \max\{x_{n_1}, x_{n_2}\}$. Then by stipulation that $\{x_n\}$ is a sequence of distinct reals, $a < a_1 < b_1 < b$. Further, if $x_n \in (a_1, b_1)$ then $n > n_2 > n_1 \geq 1 \implies n \geq 3$; recognizing that at least two sequence terms are used up in identifying a_1 and b_1, so any term lying strictly between them has subscript at least 3.
Now consider the set $A_1 = \{n \in \mathbb{N} : x_n \in (a_1, b_1)\} \subseteq \mathbb{N}$. Again A_1 has at least two elements, and by repeating the above, we generate two numbers a_2, b_2 such that $a < a_1 < a_2 < b_2 < b_1 < b$ and $x_n \in (a_2, b_2) \implies n \geq 5$. We continue this process for $r \in \mathbb{N}$, setting $A_r = \{n \in \mathbb{N} : x_n \in (a_r, b_r)\} \subseteq \mathbb{N}$. If at any step, there was one or fewer sequence numbers in (a_r, b_r), we would be done. The only potential difficulty that could arise is if we get a pair of infinite sequences $\{a_r\}$ and $\{b_r\}$ such that $a < a_1 < a_2 < \cdots < a_r < \cdots < b_r < \cdots < b_2 < b_1 < b$ with there being at least two terms from $\{x_n\}$ in each (a_r, b_r), having the property that $x_n \in (a_r, b_r) \implies n \geq 2r + 1$. In that case, we get a nested sequence of closed, bounded intervals $[a_1, b_1] \supseteq [a_2, b_2] \supseteq [a_3, b_3] \supseteq \cdots \supseteq [a_r, b_r] \supseteq \cdots$, which by Cantor's Nested Intervals Theorem 11, must have a common point, say c. It is obvious that $c \in (a, b)$, because $c \in [a_1, b_1] \subset (a, b)$. We now show that $c \notin \{x_n\}$.
Suppose that $c \in \{x_n\}$; then $\exists N \in \mathbb{N}$ s.t. $c = x_N$. But since $c \in \bigcap_{n=1}^{\infty} [a_n, b_n]$, we must have that $c \in [a_{N+1}, b_{N+1}]$ meaning that $a_N < a_{N+1} \leq c \leq b_{N+1} < b_N \implies c = x_N \in (a_N, b_N)$. But because of the way the intervals are constructed, this would mean that $N \geq 2N + 1$, an absurdity. This means that $c \in (a, b) \setminus \{x_n\}$ as needed. $\square$

And from here, we get the result we were looking for.

Corollary 20.1. *The real numbers are non-denumerable. That is,* $\aleph_0 < \mathfrak{c}$.

Proof. Since for any $a, b \in \mathbb{R}, a < b$ we have that $\mathbb{R} \sim (a, b)$, it suffices to show that the set (a, b) is non-denumerable. Let $S \subseteq (a, b)$ be denumerable. Then its elements can be arranged in a sequence of the form $\{x_n\}$. By Theorem 20, such a sequence cannot exhaust (a, b) so that $(a, b) \setminus S \neq \emptyset$. This means that S must be a proper subset of (a, b). We have proven that any denumerable subset of (a, b) must be a proper subset; from this we get the result because if (a, b) was denumerable, it would be a proper subset of itself, a contradiction. $\square$

This shows that while both the sets $\mathbb{Q}$ and $\mathbb{R}$ are infinite, there is some meaning to the statement $|\mathbb{Q}| < |\mathbb{R}|$ in that $\mathbb{Q}$ is denumerable, but $\mathbb{R}$ is not; that there are vastly more reals than there are rationals. These concepts of analyzing how "big" or "small" a set is fall in the domain of *measure theory*. A way to measure how "big" a set $S \subseteq \mathbb{R}$ is by the Lebesgue measure μ, where for $a, b \in \mathbb{R}, a \leq b$, $\mu([a, b]) = \mu((a, b)) = b - a$, and the outer measure $\mu^*(S) = \inf\{\sum_{n=1}^{\infty} \mu(I_n) : \{I_n\}_{n \in \mathbb{N}} \text{ is an open cover of } S\}$. With some more details, it can be shown that the measure of any denumerable set is 0, and hence by Theorem 19, $\mu(\mathbb{Q}) = 0$. These details can be found in

any modern textbook on analysis. In particular, Rudin[1] has a lot to say on measure theory. The Lebesgue measure then allows us to construct a Lebesgue integral on the reals as a stronger tool to compute integrals than Riemann's construction.

Thus, while the rationals are *dense* on the set of reals, *almost all* real numbers are not rational. This finishes our answer to the question about how much of the real number line the rationals cover.

Since Newton's and Liebniz's conception of calculus, it took mathematicians centuries to put it on firm footing, and building a rigorous theory of the reals was an important part of it. An understanding of the reals is a key part of the repertoire of any modern-day analyst, and it also helps appreciate that mathematics works by putting things on a firm footing, and not just talking about vague concepts, nor relying on intuition.

References

[1] W. Rudin, *Principles of Mathematical Analysis*. Mc Graw Hill Education (India) Private Limited, third ed., 2015.

[2] R. G. Bartle and D. R. Sherbert, *Introduction to Real Analysis*. John Wiley & Sons, Inc., fourth ed., 2011.

[3] C. C. Pugh, *Real Mathematical Analysis*. Springer, 2017.

[4] "Completeness of the reals: a snyopsis." `http://www-math.ucdenver.edu/~wcherowi/courses/m3000/lecture12b.pdf`.

[5] W. Dunham, *The Calculus Gallery*. Princeton University Press, 2008.