Real Numbers

Abstract

We began our rigorous development of number theory with **definitions** of $\mathbb{N}$ (the **natural numbers**), $\mathbb{Z}$ (the **integers**), and $\mathbb{Q}$ (the **rational numbers**). Our task now is to *complete* the rationals so that we can include $\sqrt{2}$, π, and other irrationals. There are at least three different ways to *construct* the **real numbers** $\mathbb{R}$, and these constructions are all *the same* in the sense of being *isomorphic*. In particular, they all satisfy the **axioms** of $\mathbb{R}$, which are basically the same as those for $\mathbb{Q}$, namely the **field axioms**, plus one more, the **least upper bound property**. As will be seen, this last axiom ensures that *all limits* of rational sequences are contained in $\mathbb{R}$, and in fact we can *construct* $\mathbb{R}$ in terms of sequences and their limits.

But there is another purpose to $\mathbb{R}$ besides 'including limits.' In fact, the way limits arise in the first place is through *approximation* of certain quantities, e.g. the length of the circumference of the circle approximated by inscribed polygons, or the diagonal of a square of side-length one approximated by rational multiples of the unit side-length. Real numbers are used in **measurement**, and for this reason MacLane's geometric construction, using Hilbert's update of Euclid's five postulates, is of utmost importance. It links the original Pythagorean theory of **magnitudes** to the modern set-theoretic formulation.

1 Axioms of the Real Numbers

The axioms of $\mathbb{R}$ break down into two types: **algebraic** and **analytic**. The algebraic axioms, **1**: 1-9 are the same as 4-13 of $\mathbb{Q}$, or any field whatsoever. We may also add **2**: 1-4 and **3**: 1-2 into the algebraic category. The only *analytic* axiom is **4**, the **least upper bound property**, is also called the **(order) completeness** of $\mathbb{R}$, and it is the axiom which makes limits, measurement, and calculus possible.

We simply *define* $\mathbb{R}$ to be a **structure**

$$(\mathbb{R}, \leq, -, ^{-1}, +, \cdot, 0, 1)$$

which is a *complete* and *totally ordered field*. Let us explain this: we define the real numbers $\mathbb{R}$ to be numbers (not yet characterized as a set, or anything in particular) having two unique elements, 0 and 1, and binary operations $+$ (**addition**) and $\cdot$ (**multiplication**), unary operations $-$ (**negation**) and $^{-1}$ (**multiplicative inversion**), as well as a **partial order** relation $\leq$, which all must satisfy the following axioms:

1. $(\mathbb{R}, -, ^{-1}, +, \cdot, 0, 1)$ is a **field**, that is for all real numbers $x,\ y,\ z$ we have

$$\left.\begin{array}{lll} 1. & x+(y+z)=(x+y)+z & (\textit{associativity of } +) \\ 2. & x+y=y+x & (\textit{commutativity of } +) \\ 3. & \exists 0\in\mathbb{R} \text{ such that } x+0=x & \\ 4. & \forall x\in\mathbb{R},\ \exists -x\in\mathbb{R} \text{ such that } x+(-x)=0 & \end{array}\right\} \begin{array}{l} (\mathbb{R},+) \textit{ is an} \\ \textit{abelian group} \end{array}$$

$$\left.\begin{array}{lll} 5. & x(yz)=(xy)z & (\textit{associativity of } \cdot) \\ 6. & xy=yx & (\textit{commutativity of } \cdot) \\ 7. & \exists 1\in\mathbb{R} \text{ such that } 1x=x \text{ and } 0\neq 1 & \\ 8. & \forall x\in\mathbb{R}\backslash\{0\},\ \exists x^{-1}\in\mathbb{R} \text{ such that } xx^{-1}=1 & \end{array}\right\} \begin{array}{l} (\mathbb{R}\backslash\{0\},\cdot) \textit{ is an} \\ \textit{abelian group} \end{array}$$

$$\begin{array}{lll} 9. & x(y+z)=xy+xz & (\textit{distributivity of } \cdot \textit{ over } +) \end{array}$$

2. $(\mathbb{R}, \leq)$ is a **totally ordered partially ordered set**, that is $\leq$ must satisfy, for all real numbers $x,\ y$ and z,

$$\begin{array}{lll} 1. & x\leq y \text{ or } y\leq x & (\textit{totality}) \\ 2. & x\leq x & (\textit{reflexivity}) \\ 3. & x\leq y \text{ and } y\leq x \implies x=y & (\textit{antisymmetry}) \\ 4. & x\leq y \text{ and } y\leq z \implies x\leq z & (\textit{transitivity}) \end{array}$$

3. The field operations $+$ and $\cdot$ are **compatible** with the partial order $\leq$ in the sense that for all $x, y, z \in \mathbb{R}$ we have

$$\begin{array}{lll} 1. & x\leq y \implies x+z\leq y+z & (\textit{preservation of order under addition}) \\ 2. & 0\leq x \text{ and } 0\leq y, \text{ then } 0\leq xy & (\textit{preservation of order under multiplication}) \end{array}$$

4. $\leq$ is a **complete** order relation, meaning it satisfies the **least upper bound property**: for any nonempty collection S of real numbers which is bounded above there exists a real number $\sup S$, the *least* or *smallest* upper bound. (The notation sup here stands for **supremum**, which is a Latinized form of 'least upper bound.')

Definition 1.1 *A collection S of real numbers is said to be* **bounded above** *by a real number M if every number x in the collection S satisfies*

$$x \leq M$$

Let us write

$$S^u \stackrel{\text{def}}{=} \{\text{all upper bounds of } S\}$$

and let us write

$$\sup S \stackrel{\text{def}}{=} \min S^u$$

which is the minimum, or smallest of the upper bounds. This number exists by fiat*, by Axiom 4.* ■

1.1 Motivation for the Least Upper Bound Axiom

Let us here consider the limitations of the rational numbers $\mathbb{Q}$ for conducting measurement.

Theorem 1.2 ($\mathbb{Q}$ is Densely Ordered) *Between any two distinct rational numbers p and q there exists a rational number r, and hence infinitely many rational numbers.*

Proof: If $p \neq q$ are rational numbers, then since $\mathbb{Q}$ is *totally* ordered have two cases

$$p < q \quad \text{and} \quad p > q$$

Case 1: $p < q$: In this case, the rational number $\frac{1}{2}(p+q) = \frac{1}{2}p + \frac{1}{2}q$ lies between p and q, as you can see directly:

$$\begin{aligned} p < q &\implies 2p < p + q < 2q \\ &\implies p < \frac{1}{2}(p+q) < q \end{aligned}$$

(*Note*: both implications seem to rely on Axiom **3** of $\mathbb{R}$ above, but looking at properties (10)-(11) of Theorem 3.12 in *Numbers*, and the subsequent constructions of $\mathbb{Z}$ and $\mathbb{Q}$, it would seem these are in fact derived from

Theorem 3.12 in the case of $\mathbb{Q}$: exercise!) Since this is true for each p and q, in particular it is true for p and $\frac{1}{2}(p+q)$, so that

$$p < \frac{1}{4}(p+q) = \frac{1}{2}\left(\frac{1}{2}(p+q)\right) < \frac{1}{2}(p+q) < q$$

Repeating this process for all $n \in \mathbb{N}$ we have a sequence of rational numbers $\left(\frac{1}{2^n}(p+q)\right)_{n\in\mathbb{N}}$ lying between p and q.

Case 2: $p > q$: reverse the roles of p and q in the proof of Case 1. ■

Theorem 1.3 (Archimedean Property of $\mathbb{Q}$) *For all $p, q \in \mathbb{Q}$ with $p > 0$, there exists a natural number $n \in \mathbb{N}$ such that $pn > q$.*

Remark 1.4 *If we imagine p and q as masses on a see-saw, or balance, then supposing p a smaller mass than q, e.g. Archimedes the man versus a mountain, $p < q$, then by multiplying the power of Archimedes n-fold times, e.g. by increasing the length of p's arm of the lever n-fold, the result is that Archimedes will lift the mountain. Our assumptions about $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ make this a* necessary *consequence.* ■

Proof: If $q \leq 0$, then $\exists 1 \in \mathbb{N}$ such that $1p = p > q$. Thus, assume that $q > 0$. Let $p = \frac{a}{b}$ and $q = \frac{c}{d}$, where $a, b, c, d \in \mathbb{N}$. Let us consider the options:

(1) $p = q$

(2) $p > q > 0$

(3) $0 < p < q$

The first two cases are included only out of logical pedantry. In the first case $\exists 2 \in \mathbb{N}$ such that $q = p < 2p$. In the second case, $p > q > 0$, and $\exists 1 \in \mathbb{N}$ such that $1p = p > q$.

We move on to the third and only interesting case, when $0 < p < q$. We need to find some $n \in \mathbb{N}$ such that $q < np$. I claim that

$$n = b(c+1)$$

will work if we take $p = \frac{a}{b}$ and $q = \frac{c}{d}$ as above. To see this, note first that $0 < p < q$ means $0 < \frac{a}{b} < \frac{c}{d}$, and therefore $0 < ad < bc$ (Theorem 3.12, *Numbers*). Since $0 < p < q$, all $a, b, c, d > 0$, and in particular this implies $a, b, c, d \geq 1$. In particular, $d \geq 1$ implies $dq \geq 1q \geq 1$, which we insert here:

$$c + 1 > c = d \cdot \frac{c}{d} = dq \geq q$$

citing again Theorem 3.12 in *Numbers* for the relevant maneouvers (that $c+1>c$ and $d\geq 1$ implying $dq\geq 1q\geq 1$). What do we gain from this? This:

$$q<c+1\leq a(c+1)=b(c+1)\frac{a}{b}=np$$

where $n=b(c+1)\in\mathbb{N}$. ■

Proposition 1.5 *The rationals* $\mathbb{Q}$ *do* **not** *satisfy the least upper bound property, meaning there does not always exist a least upper bound* $\sup S$ *in* $\mathbb{Q}$ *for arbitrary bounded subsets* $S\subseteq\mathbb{Q}$.

Proof: Though the rational numbers are densely ordered, they do not satisfy the least upper bound property. If we consider the subset

$$S=\{p\in\mathbb{Q}\,|\,p^2<2\}$$

then, first of all, S is nonempty because $1\in S$, and second of all S is bounded above by $2\in\mathbb{Q}$: all $p\in S$ satisfy $p<2$, for otherwise, if $p\geq 2$, we'll have $p^2\geq 4>2$. Thus, S^u, the set of upper bounds for S, is nonempty, because $2\in S^u$. Now comes the crux of the matter: though S^u is nonempty, it has no minimum, no $\sup S$, no least upper bound in $\mathbb{Q}$. For if you suppose to the contrary, that S has a least upper bound $\ell\in\mathbb{Q}$, then first of all $\ell^2\neq 2$ because $\ell=\sqrt{2}\notin\mathbb{Q}$, while both $\ell^2>2$ and $\ell^2<2$ lead to contradictions:

(1) Suppose $\ell^2<2$ (i.e. that $\ell\in S$). If $\ell=\sup S$ and $\ell^2<2$, then $\ell\in S$ and we conclude that $\ell=\max S$. This, however, cannot be: if we suppose $\ell=\max S$, then because $2-\ell^2>0$, the Archimedean property of $\mathbb{Q}$ says that $\exists n\in\mathbb{N}$ such that $n(2-\ell^2)>2\ell+1$. But then

$$n(2-\ell^2)>2\ell+1\geq 2\ell+\frac{1}{n}$$

or

$$2>\ell^2+2\frac{1}{n}\ell+\frac{1}{n^2}=\left(\ell+\frac{1}{n}\right)^2$$

whence $\ell+\frac{1}{n}\in S$ and $\ell+\frac{1}{n}>\ell$, so $\ell\neq\max S$, a contradiction. Consequently, if $\ell\in S$ then $\ell\neq\sup S$ because ℓ is not even an upper bound of S. This contradicts our assumption that $\ell=\sup S$.

(2) On the other hand, if we suppose that $\ell^2>2$, then ℓ is at least an upper bound of S, but we run into the problem that the set of upper bounds $S^u=\{r\in\mathbb{Q}\,|\,r>0,\ r^2>2\}$ of S has no minimum in $\mathbb{Q}$: since

$r > 0$ and $r^2 - 2 > 0$, the Archimedean property of $\mathbb{Q}$ guarantees that $\exists n, m \in \mathbb{N}$ such that $nr > 1$ and $m(r^2-2) > 2r$. Let $M = \max\{n, m\}$. Then $M \in \mathbb{N}$, and

$$Mr > 1 \quad \text{and} \quad M(r^2 - 2) > 2r \geq 2r - \frac{1}{M}$$

or

$$r > r - \frac{1}{M} > 0 \quad \text{and} \quad \left(r - \frac{1}{M}\right)^2 = r^2 - 2r\frac{1}{M} + \frac{1}{M^2} > 2$$

Thus, for all $\ell \in S^u$, there exists $r \in S^u$ with $\ell > r > 0$, so $\nexists \ell = \min S^u = \sup S$. ■

The least upper bound property is an abstraction used in the axiomatization of $\mathbb{R}$ considered separately from any concrete realization, whether using pure sets or some geometric model of the Euclidean plane (as in MacLane). Our first construction, via Dedekind cuts, uses it directly, but we'll come to see that this construction is isomorphic (i.e. essentially equivalent) to the one using limits, and also to MacLane's geometric 'number line' construction out of Hilbert's re-modeling of Eulidean geometry.

2 Dedekind Cut Construction of $\mathbb{R}$

A **Dedekind cut** is a set A of the form $A = (-\infty, p) \subseteq \mathbb{Q}$, where $p \in \mathbb{Q}$, using interval notation. This is because $A \neq \varnothing$ by the Archimedean property of $\mathbb{Q}$, Theorem 1.3, since there always exists q such that $q < p$ because there always exists $-q \in \mathbb{Q}^+$ such that $-q > p$, and hence $\exists q = -(-q) \in \mathbb{Q}$ with $q < p$ whether p is positive or negative. Moreover, for any $x \in A = (-\infty, p)$ we have that $y \leq x \implies y \in A$, and since $p \notin A$ we have that $x < p \implies x \in A$, which by the order denseness of $\mathbb{Q}$, Theorem 1.2, means that all $y \in \mathbb{Q}$ with $x < y < p$ are in A, and there are infinitely many such y, so that $\nexists \max A$. Moreover, by the Archimedean property again, since $p \in \mathbb{Q}$, there exists $q \in \mathbb{Q}$ such that $p = 1p < q$, whence $\mathbb{Q} \backslash A \neq \varnothing$. Dedekind cuts allow us to define the real numbers as follows:

A **real number** A in this construction is a Dedekind cut, and $\mathbb{R}$ is the set of all Dedekind cuts of $\mathbb{Q}$. To make sure we give $\mathbb{R}$ the structure it needs, we must define a partial order $\leq$, the binary operations of addition $+$ and multiplication $\cdot$, and we must also give $\mathbb{R}$ the additive and multiplicative identities 0 and 1, and then show that these satisfy the usual properties. First, we define 0 and 1:

$$\begin{aligned} 0 &= \{p \in \mathbb{Q} \mid p < 0',\ 0' \in \mathbb{Q}\} \\ &= (-\infty, 0') \subseteq \mathbb{Q} \end{aligned}$$

$$\begin{aligned} 1 &= \{p \in \mathbb{Q} \mid p < 1',\ 1' \in \mathbb{Q}\} \\ &= (-\infty, 1') \subseteq \mathbb{Q} \end{aligned}$$

partial order Then, we define the **partial order** $\leq$ on the reals by requiring

$$A \leq B \iff A \subseteq B$$

with $A = B$ iff $A = B$ as sets. We define **addition** $+$ on $\mathbb{R}$ by letting

$$A + B = \{p + q \mid p \in A,\ q \in B\}$$

We define the **opposite** $-A$ of $A \in \mathbb{R}$ by

$$-A = \{p \in \mathbb{Q} \mid -p \notin A \text{ and } -p \neq \min \mathbb{Q} \backslash A\}$$

For example,

$$\begin{aligned} -5 &= \{p \in \mathbb{Q} \mid -p \notin 5 \text{ and } p \neq \min \mathbb{Q} \backslash 5\} \\ &= \{p \in \mathbb{Q} \mid -p > 5\} \\ &= \{p \in \mathbb{Q} \mid p < -5\} \end{aligned}$$

This definition is good because $\mathbb{Q}$ satisfies the Archimedean property by T 1.3, so (r, ∞) is nonempty. The opposite of a real number A, in turn, allows us to define the **absolute value** function $|\cdot| : \mathbb{R} \to \mathbb{R}_0^+$ by

$$|A| = \begin{cases} A, & \text{if } A \geq 0 \\ -A, & \text{if } A < 0 \end{cases}$$

A real number A is said to be **positive** if $A > 0$ and is said to be **negative** if $A < 0$. The **set of all positive real numbers** is denoted $\mathbb{R}^+$, the **set of all nonnegative numbers** is denoted $\mathbb{R}_0^-$ and equals $\mathbb{R}^- \cup \{0\}$, the **set of all negative real numbers** is denoted $\mathbb{R}^-$, and **set of all nonpositive numbers** is denoted $\mathbb{R}_0^-$ and equals $\mathbb{R}^- \cup \{0\}$.

the distance $d : \mathbb{R} \times \mathbb{R} \to \mathbb{R}_0^+$ between two real numbers A and B is given by

$$d(A, B) = |A - B|$$

Now we can define multiplication $\cdot$. We do this in two steps, first for $A, B > 0$, then for all $A, B \in \mathbb{R}$. If $A, B > 0$,

$$AB = \mathbb{Q}_0^- \cup \{qr \mid q \in A \cap \mathbb{Q}^+, r \in B \cap \mathbb{Q}^+\}$$

and in general, for all $A, B \in \mathbb{R}$ we say

$$AB = \begin{cases} 0, & \text{if } A = 0 \text{ or } B = 0 \\ |A||B|, & \text{if } A, B > 0 \text{ or } A, B < 0 \\ -|A||B|, & \text{if } A > 0 \;\&\; B < 0 \;\text{ or if }\; A < 0 \;\&\; B > 0 \end{cases}$$

For example

$$\begin{aligned} 5 \cdot 6 &= \mathbb{Q}_0^- \cup \{qr \mid q \in 5 \cap \mathbb{Q}^+, r \in 6 \cap \mathbb{Q}^+\} \\ &= (-\infty, 30) \subseteq \mathbb{Q} \end{aligned}$$

while

$$\begin{aligned} -5 \cdot 6 &= -|-5||6| \\ &= -(5 \cdot 6) \\ &= -(-\infty, 30) \subseteq \mathbb{Q} \\ &= (-\infty, -30) \subseteq \mathbb{Q} \end{aligned}$$

The **multiplicative inverse** of a *nonzero* real number A is defined by

$$A^{-1} = \left\{ p \in \mathbb{Q} \mid p \leq 0 \text{ or else } p > 0 \;\&\; \frac{1}{p} \notin A \;\&\; p \neq \min \mathbb{Q} \backslash A \right\}$$

For example,

$$\begin{aligned} 5^{-1} &= \left\{ p \in \mathbb{Q} \mid p \leq 0 \text{ or else } p > 0 \;\&\; \frac{1}{p} \notin 5 \;\&\; p \neq \min \mathbb{Q} \backslash A \right\} \\ &= \mathbb{Q}_0^- \cup \left\{ p \in \mathbb{Q} \mid \frac{1}{p} > 5 \right\} \\ &= \mathbb{Q}_0^- \cup \left\{ p \in \mathbb{Q} \mid p < \frac{1}{5} \right\} \\ &= (-\infty, 1/5) \end{aligned}$$

The multiplicative inverse of a negative real $A < 0$ is given by

$$A^- = -(|A|)^-$$

For example $-5^- = -(|-5|)^- = -(-\infty, 1/5) = (-\infty, -1/5)$. The multiplicative inverse is a good definition because, again, $\mathbb{Q}$ satisfies the Archimedean property, so $p > 0$ always exist such that $p < \frac{1}{q}$ for any $q > 0$.

The commutativity and associativity of addition and multiplication in $\mathbb{R}$, as well as distributivity of $\cdot$ over $+$, follow from the properties of $\mathbb{Q}$ and our definitions of $+$ and $\cdot$ in $\mathbb{R}$ above. In fact, all the points taken for axioms in the previous "construction" except the least upper bound follow from our definitions. We state this formally in the next theorem:

Theorem 2.1 *The set of real numbers* $\mathbb{R}$ *is a structure* $(\mathbb{R}, \leq, -, ^{-1}, +, \cdot, 0, 1)$ *which is a totally ordered field:*

1. $(\mathbb{R}, -, ^{-1}, +, \cdot, 0, 1)$ *is a field, that is for all* $x, y, z \in \mathbb{R}$ *we have*

1. $x + (y + z) = (x + y) + z$ (*associativity of* $+$)
2. $x + y = y + x$ (*commutativity of* $+$)
3. $\exists 0 \in \mathbb{R}$ *such that* $x + 0 = x$
4. $\forall x \in \mathbb{R},\ \exists! -x \in \mathbb{R}$ *such that* $x + (-x) = 0$

(items 1–4: $(\mathbb{R}, +)$ *is an abelian group*)

5. $x(yz) = (xy)z$ (*associativity of* $\cdot$)
6. $xy = yx$ (*commutativity of* $\cdot$)
7. $\exists 1 \in \mathbb{R}$ *such that* $1x = x$ *and* $0 \neq 1$
8. $\forall x \in \mathbb{R}\backslash\{0\},\ \exists x^{-1} \in \mathbb{R}$ *such that* $xx^{-1} = 1$

(items 5–8: $(\mathbb{R}\backslash\{0\}, \cdot)$ *is an abelian group*)

9. $x(y + z) = xy + xz$ (*distributivity of* $\cdot$ *over* $+$)

2. $(\mathbb{R}, \leq)$ *is a totally ordered set, that is for all* $x, y, z \in \mathbb{R}$ *we have*

1. $x \leq x$ (*reflexivity*)
2. $x \leq y$ *and* $y \leq x \implies x = y$ (*antisymmetry*)
3. $x \leq y$ *and* $y \leq z \implies x \leq z$ (*transitivity*)
4. $x \leq y$ *or* $y \leq x$ (*totalness*)

3. *The field operations* $+$ *and* $\cdot$ *are* **compatible** *with the partial order* $\leq$ *in the sense that for all* $x, y, z \in \mathbb{R}$ *we have*

1. $x \leq y \implies x + z \leq y + z$ (*preservation of order under addition*)
2. $0 \leq x$ *and* $0 \leq y$, *then* $0 \leq xy$ (*preservation of order under multiplication*)

Proof: These properties follow from those of $\mathbb{Q}$: **1.**1.

$$\begin{aligned} x + (y+z) &= x + \{b+c \mid b \in y,\ c \in z\} \\ &= \{a + (b+c) \mid a \in x,\ b \in y,\ c \in z\} \\ &= \{(a+b)+c \mid a \in x,\ b \in y,\ c \in z\} \\ &= \{a+b \mid a \in x,\ b \in y\} + z \\ &= (x+y)+z \end{aligned}$$

1.2. $x + y = \{a+b \mid a \in x,\ b \in y\} = \{b+a \mid a \in x,\ b \in y\} = y + x$.

1.3. We have already defined 0 and 1, so we only need check their defining properties. First, for any $x \in \mathbb{R}$ we have $x = (-\infty, r) \subseteq \mathbb{Q}$ for some $r \in \mathbb{Q}$, so we need to show

$$x+0 = \{a+b|a \in x,\ b \in 0\} = \{a+b|a \in (-\infty, r),\ b \in (-\infty, 0')\} = (-\infty, r) = x$$

which we do as follows: if $q \in x + 0$, then $q = a + b$ for some $a \in x$ and $b \in 0$, i.e. for some $a \in (-\infty, r)$ and $b \in (-\infty, 0')$. But clearly $a + b < a$, so $p = a + b \in x$, which shows that $x + 0 \subseteq x$. Conversely, if $a \in x$, then $\exists a' \in x$ and $b \in 0$ such that $a = a' + b \in x$ by the order denseness of $\mathbb{Q}$, since if $a \in x$ then $a < r$ and so $\exists a' \in x$ such that $a < a' < r$. Letting $b = -(a' - a) = a - a' \in 0$, we have that $a = a' + (a - a') = a' + b \in x + 0$. Thus $x \subseteq x + 0$, and therefore by the axiom of extensionality $x + 0 = x$.

1.4. If $x = (-\infty, r)$ is a real number, $r \in \mathbb{Q}$, then it's opposite $-x = (-infty, -r)$ is also its additive inverse or negative, which is shown as follows: first

$$x + (-x) = \{a+b \mid a \in x,\ b \in -x\} = \{a+b \mid a < r,\ b < -r\}$$

so if $r = 0$ then $x = 0$, so $-x = x = 0$ and by the previous point we have $x + (-x) = 0 + 0 = 0$. If $r > 0$ then $-r < 0$, so if $a < r$ and $b < -r$, then $a+b < r+(-r) = 0$, so $a+r \in 0$. If $r < 0$ then we apply the same reasoning to $r' = -r$. Thus for all $x \in \mathbb{R}$ we have that $\exists -x \in \mathbb{R}$ with $x + (-x)$. The uniqueness of $(-x)$ is shown as follows: if there were any other $y \in \mathbb{R}$ with $x + y = 0$, then

$$-x = -x + 0 = -x + (x+y) = (-x+x) + y = 0 + y = y$$

1.5. It suffices to prove the case $x, y, z > 0$, for the other cases follow from the first:

$$\begin{aligned}
x(yz) &= x \cdot \Big(\mathbb{Q}_0^- \cup \{bc \mid b \in y \cap \mathbb{Q}^+,\ c \in z \cap \mathbb{Q}^+\}\Big) \\
&= \mathbb{Q}_0^- \cup \{a(bc) \mid a \in x \cap \mathbb{Q}^+,\ b \in y \cap \mathbb{Q}^+,\ c \in z \cap \mathbb{Q}^+\} \\
&= \mathbb{Q}_0^- \cup \{(ab)c \mid a \in x \cap \mathbb{Q}^+,\ b \in y \cap \mathbb{Q}^+,\ c \in z \cap \mathbb{Q}^+\} \\
&= \Big(\mathbb{Q}_0^- \cup \{ab \mid a \in x \cap \mathbb{Q}^+,\ b \in y \cap \mathbb{Q}^+\}\Big) \cdot z \\
&= (xy)z
\end{aligned}$$

1.6. $xy = \{ab \mid a \in x,\ b \in y\} = \{ba \mid a \in x,\ b \in y\} = yx$.

1.7. It is enough to prove this for $x > 1$, for the other cases, $x < 0$ and $x = 0$ follow easily from the first. For any $x \in \mathbb{R}+$ we have $x = (-\infty, r) \subseteq \mathbb{Q}$ for some $r \in \mathbb{Q}^+$, so

$$x1 = \{ab \mid a \in x,\ b \in 1\}$$

We must show that $x1 = x$: first, if $p = ab \in x1$ for $a \in x$ and $b \in 1$, then since $b < 1'$ we have $p = ab < r$, so $p \in x$. Thus $x1 \subseteq x$. Conversely, if $p \in x$, then $\exists a = \frac{2pr}{p+r} \in x$ ($\frac{2pr}{p+r} < r$ since $2pr = pr + pr < pr + r^2$) and $\exists b = \frac{p+r}{2r} \in 1$ ($\frac{p+r}{2r} < 1'$ since $p + r < 2r$) such that

$$ab = \frac{2pr}{p+r} \cdot \frac{p+r}{2r} = p$$

Thus $x1 \supset x$, and by extensionality we have $x1 = x$.

1.8. For any $x \in \mathbb{R}\backslash\{0\}$ we have $x = (-\infty, r) \subseteq \mathbb{Q}$ for some $r \in \mathbb{Q}\backslash\{0'\}$, and so $\frac{1}{r} = r^{-1} \in \mathbb{Q}\backslash\{0'\}$, whence $x^{-1} = (-\infty, r^{-1})$ is the multiplicative inverser of x, that is

$$xx^{-1} = \mathbb{Q}_0^- \cup \{ab \mid a \in x \cap \mathbb{Q}^+,\ b \in x^{-1} \cap \mathbb{Q}^+\} = 1 = (-\infty, 1') \subseteq \mathbb{Q}$$

which we can show as follows: we'll prove it for $x > 0$, since the case $x < 0$ follows from the first by considering $|x| = -x$: if $p = ab \in xx^{-1}$ for $0 < a < r$ and $0 < b < r^{-1}$, then $a < r$ and $b < r^{-1}$, so $p = ab < rr^{-1} = 1'$, whence $p \in 1$. This shows that

$$xx^{-1} = \mathbb{Q}_0^- \cup \{ab \mid a \in x \cap \mathbb{Q}^+, b \in x^{-1} \cap \mathbb{Q}^+\} \subseteq 1$$

To show the reverse inclusion, let $p \in 1$. If $p < 0$ then $p \in \mathbb{Q}_0^- \subseteq xx^{-1}$, so suppose $0 < p$, so that $0 < p < 1' \in \mathbb{Q}$. There are two cases, $x > 0$ and $x < 0$. We'll prove $x > 0$ since $x < 0$ follows from the $x > 0$ case by taking the absolute of x. Now, if $x > 0$, then $x = (-\infty, r)$ for some $r = \frac{h}{k} \in \mathbb{Q}^+$, where $h, k \in \mathbb{N}$. This produces three cases, $r < 1'$, $r = 1'$ and $r > 1'$. **a.** If $r = 1'$, then $x = 1$, so by 7 above we have that $x^2 = x1 = x = 1$, so $x = x^{-1}$, which exists because $x = 1$ exists. **b.** If $r > 1$, choose $p \in 1$, i.e. $p = \frac{m}{n} < 1'$ for some $m, n \in \mathbb{N}$, and let $a \in x \cap \mathbb{Q}^+$ be given by

$$a = 1 + \frac{N-1}{N}\left(\frac{h}{k} - 1\right) = \frac{(N-1)h + k}{Nk}$$

for some $N \in \mathbb{N}$ with $N > 1$, so that $1 < a < p$. Then, note that since $\frac{m}{n} < 1$ we have $1 - \frac{m}{n} > 0$, so by the Archimedean property of $\mathbb{Q}$ there exists an $N \in \mathbb{N}$ such that $1 < N\left(1 - \frac{m}{n}\right)$, or

$$1 - N\left(1 - \frac{m}{n}\right) < 0$$

Choose this N for our expression of a. We now need to find $b \in r^{-1}$, i.e. $b < \frac{k}{h}$, such that $ab = p$. Towards this end, note that by the above inequality and the fact that $0 < \frac{h}{k}$ iff $0 < \frac{k}{h}$ we have

$$\begin{aligned}
1 - N\left(1 - \frac{m}{n}\right) < 0 < \frac{k}{h} \quad &\iff \quad \frac{n - N(n-m)}{n} < \frac{k}{h} \\
&\iff \quad h\big(n - N(n-m)\big) < nk \\
&\iff \quad h\big(mN - n(N-1)\big) < nk \\
&\iff \quad mhN < nh(N-1) + nk \\
&\iff \quad \frac{mN}{nh(N-1) + nk} < \frac{1}{h} \\
&\iff \quad \frac{mNk}{nh(N-1) + nk} < \frac{k}{h} = r^{-1}
\end{aligned}$$

Thus, if we let

$$b = \frac{mNk}{nh(N-1) + nk} = \frac{mNk}{n(h(N-1) + k)}$$

we have that $b < r^{-1}$, so that $b \in x^{-1}$, and moreover,

$$ab = \frac{\cancel{(N-1)h + k}}{\cancel{Nk}} \cdot \frac{m\cancel{Nk}}{n\cancel{(h(N-1) + k)}} = \frac{m}{n} = p$$

Thus, if $r > 1$ we have that for all positive $p \in 1$, $\exists a \in x$ and $b \in x^{-1}$ such that $ab = p$, so $1 \subseteq xx^{-1}$. **c.** If $r < 1$, however, we may repeat the above procedure with $r' = r^{-1}$, that is by switching a and b, so $1 \subseteq xx^{-1}$ in this case too.

Hence by **a-c** we have that $1 \subseteq xx^{-1}$ in all cases where $0 < p < 1$, and since $1 \supset xx^{-1}$ by the previous arguments, we have by extensionality that $\forall x \in \mathbb{R}^+$, $\exists x^{-1}$ such that $xx^{-1} = 1$ whenever $0 < p < 1$. This is also true, trivially, when $p < 0$, as shown above, so it holds true for all $x > 0$. Finally, as promised, we show that the case $x < 0$ follows from that of $x > 0$: if $x < 0$, then $x^{-1} < 0$ also, and so $xx^{-1} = |x||x^{-1}|$, and the above procedure shows that $\exists x^{-1}$ making this true, namely $x^{-1} = (-\infty, r^{-1})$, which follows from the fact that we have $|x^{-1}| = |x|^{-1}$, so that $x^{-1} = -|x|^{-1}$.

1.9. Finally, distributivity follows from distributivity in $\mathbb{Q}$. It suffices to prove the case $x, y, z > 0$, for the other cases follow from the first by taking absolute values:

$$\begin{aligned} x(y+z) &= x \cdot \{b + c \mid b \in y,\ c \in z\} \\ &= \mathbb{Q}_0^- \cup \{a(b+c) \mid a \in x \cap \mathbb{Q}^+,\ b \in y \cap \mathbb{Q}^+,\ c \in z \cap \mathbb{Q}^+\} \\ &= \mathbb{Q}_0^- \cup \{ab + ac \mid a \in x \cap \mathbb{Q}^+,\ b \in y \cap \mathbb{Q}^+,\ c \in z \cap \mathbb{Q}^+\} \\ &= \Big(\mathbb{Q}_0^- \cup \{ab \mid a \in x \cap \mathbb{Q}^+,\ b \in y \cap \mathbb{Q}^+\}\Big) + \\ &\qquad \Big(\mathbb{Q}_0^- \cup \{ac \mid a \in x \cap \mathbb{Q}^+,\ c \in z \cap \mathbb{Q}^+\}\Big) \\ &= xy + xz \end{aligned}$$

2.1. Clearly, for all $x = (-\infty, r)$ we have $x = x$ as sets, so $x \leq x$ as well.

2.2. If $x = (-\infty, r)$ and $y = (-\infty, s)$ satisfy $x \leq y$ and $y \leq x$, then $(-\infty, r) \subseteq (-\infty, s)$ and $(-\infty, r) \supset (-\infty, s)$, so by extensionality $(-\infty, r) = (-\infty, s)$, whence $x = y$.

2.3. If $x = (-\infty, r)$, $y = (-\infty, s)$ and $z = (-\infty, t)$ satisfy $x \leq y$ and $y \leq z$, then $(-\infty, r) \subseteq (-\infty, s)$ and $(-\infty, s) \subseteq (-\infty, t)$, so by the definition of set inclusion we have

$$(-\infty, r) \subseteq (-\infty, s) \subseteq (-\infty, t) \implies (-\infty, r) \subseteq (-\infty, t)$$

or $x \leq z$.

2.4. For all $x = (-\infty, r), y = (-\infty, s) \in \mathbb{R}$ we have $r \leq s$ or $s \leq r$ by the totalness of $\mathbb{Q}$, whence $(-\infty, r) \subseteq (-\infty, s)$ or $(-\infty, r) \supset (-\infty, s)$, so that $x \leq y$ or $y \leq x$.

3.1. If $x = (-\infty, r)$ and $y = (-\infty, s)$ satisfy $x \leq y$, then for any $z = (-\infty, t)$ we have $x+z = \{a+b | a \in x,\ b \in z\}$ and $y+z = \{a+b | a \in y,\ b \in z\}$. But if $x \leq y$, then $x \subseteq y$, so if $a \in x$ then $a \in y$, whence if $a + b \in x + z$ then $a + b \in y + z$, so $x + z \subseteq y + z$ as sets, or $x + z \leq y + z$.

3.2. If $x = (-\infty, r)$ and $y = (-\infty, s)$ satisfy $0 \leq x$ and $0 \leq y$, then $r, s \geq 0$. If $r = s = 0$ then $x = y = 0$ and $xy = \mathbb{Q}_0^- = 0$. If $r, s > 0$ then $\exists a \in x \cap \mathbb{Q}^+$ and $b \in y \cap \mathbb{Q}^+$, so $ab > 0$ for such a and b, whence

$$xy = \mathbb{Q}_0^- \cup \{ab \mid a \in x \cap \mathbb{Q}^+,\ b \in y \cap \mathbb{Q}^+\}$$

so that

$$\mathbb{Q}_0^- \subsetneq \mathbb{Q}_0^- \cup \{ab \mid a \in x \cap \mathbb{Q}^+,\ b \in y \cap \mathbb{Q}^+\}$$

or $0 < xy$. Either way, then, $0 \leq xy$. ■

We may now state and prove the key property of $\mathbb{R}$:

Theorem 2.2 ($\mathbb{R}$ is Complete) *$\mathbb{R}$ as constructed above satisfies the least upper bound property: every nonempty subset S of $\mathbb{R}$ that is bounded above has a least upper bound, given by*

$$\sup S = \bigcup_{A \in S} A$$

Proof: If $S \subseteq \mathbb{R}$ and $\exists B \in \mathbb{R}$ such that $A \leq B$ for all $A \in S$, then we must check, first of all, that $\bigcup_{A \in S} A$ is a real number, that is a Dedekind cut. First, $\bigcup_{A \in S} A$ is nonempty because it consists of a union of nonempty sets, and also $\mathbb{Q} \backslash \left(\bigcup_{A \in S} A\right)$ is nonempty because, if $B \in \mathbb{R}$, then $\mathbb{Q} \backslash B$ is nonempty, so if $r \in \mathbb{Q} \backslash B$, then $r \neq A$ for all $A \in S$, because all $A \leq B$ means $A \subseteq B$. Moreover, $\bigcup_{A \in S} A$ has no greatest element, for if it did, say $m = \max \bigcup_{A \in S} A$, then $m \in A$ for some $A \in S$, so $m = \max A$, contradicting the fact that $\nexists \max A$. Finally, $\bigcup_{A \in S} A$ is a down-set of $\mathbb{Q}$, because if $x \in \bigcup_{A \in S} A$ and $y < x$, then, $x \in A$ for some $A \in S$, and A is a down-set, so $y \in A$, which means $y \in \bigcup_{A \in S} A$. Thus $\sup S = \bigcup_{A \in S} A$ is a real number. Finally, it is an upper bound of S, for clearly $A \subseteq \bigcup_{A \in S} A$ for all $A \in S$, and moreover it is the least upper bound, for clearly for all upper bounds B of S we have $\bigcup_{A \in S} A \subseteq B$ because all $A \in S$ satisfy $A \subseteq B$, whence $\sup S \leq B$ for all upper bounds B. ■

3 Cauchy Sequence Construction of $\mathbb{R}$

Another explicit construction of the reals arises from an attempt to fix a differnt problem with the rationals, that **not every sequence in $\mathbb{Q}$ converges *in* $\mathbb{Q}$**. For example the sequence $(1, 2, \frac{3}{2}, \frac{5}{4}, \frac{11}{8}, \frac{23}{16}, \dots)$ in $\mathbb{Q}$ converges to $\sqrt{2} \notin \mathbb{Q}$ (this sequence is constructed recursively using bisection method and calculus methods, namely the Intermediate Value Theorem– nevertheless, it is a sequence in $\mathbb{Q}$). We would like to make numbers out of all such *limits* of sequences in $\mathbb{Q}$. However, if we go about it directly we will run into several problems, the biggest of which is that we will make a set out of strange elements, elements which are constructed inside known sets, yet which do not belong to any known set. The 'limits' of some sequences in $\mathbb{Q}$ do not yet *exist* in any known set.

Another problem is that there may be *several* sequences with the same 'limit,' though eventually we want that limit to be a *single* number.

Our solution to the first problem is to make use only of **Cauchy sequences** in $\mathbb{Q}$, that is sequences which satisfy

$$\lim_{n,m \to \infty} |x_n - x_m| = 0$$

This makes no mention of limits, but it does allow us to introduce the limits later, once we embed $\mathbb{Q}$ in our new set $\mathbb{R}$. The way around the second problem is to do what we did in the definition of the integers and the rationals, to invent an *equivalence relation*, in this case an 'equivalence' between Cauchy sequences with the same 'limit,' that is with

$$(x_n)_{n\in\mathbb{N}} \text{ and } (y_n)_{n\in\mathbb{N}} \overset{\text{def}}{\iff} \lim_{n\to\infty} |x_n - y_n| = 0$$

for Cauchy sequences $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$. We have thus hit upon the following construction: we define the **real numbers** as equivalence classes of Cauchy sequences whose difference tends to zero (and are in this way 'equivalent'). Consider again the example of the sequence $(1, 2, \frac{3}{2}, \frac{5}{4}, \frac{11}{8}, \frac{23}{16}, \dots)$ in $\mathbb{Q}$. If we neglect to mention its 'limit' and speak only of the fact that it is a Cauchy sequence in $\mathbb{Q}$, then we can make an equivalence class $[(x_n)_{n\in\mathbb{N}}]$ out of the sequence and call this the square root of 2, that is $\sqrt{2} := [\mathbf{x}]$. More formally:

A **Cauchy sequence** in $\mathbb{Q}$ is a sequence $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}$ which satisfies

$$\forall \epsilon \in \mathbb{Q}^+,\ \exists N \in \mathbb{N} \text{ such that } m, n \geq N \implies |x_n - x_m| < \epsilon$$

that is

$$\lim_{n,m\to\infty} |x_n - x_m| = 0$$

The set C consisting of all Cauchy sequences in $\mathbb{Q}$ can be adorned with some algebraic structure: we define addition $+$, multiplication $\cdot$ and a **partial order** $\leq$ on C, as follows:

$$\begin{aligned}
&(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} := (x_n + y_n)_{n\in\mathbb{N}} \\
&(x_n)_{n\in\mathbb{N}} \cdot (y_n)_{n\in\mathbb{N}} := (x_n y_n)_{n\in\mathbb{N}} \\
&(x_n)_{n\in\mathbb{N}} \leq (y_n)_{n\in\mathbb{N}} \text{ iff } \forall\epsilon\in\mathbb{Q}^+,\ \exists N\in\mathbb{N} \text{ s.t. } n\geq N \implies x_n-\epsilon\leq y_n \\
&\qquad\qquad\qquad\qquad\text{or} \\
&\qquad\qquad\qquad (x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}
\end{aligned}$$

These allow us to establish the equivalence relation on C that we want, namely that which 'equates' Cauchy sequences with the same limit (but without mentioning the limit):

$$(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}} \iff \lim_{n\to\infty}(x_n - y_n) = 0$$

To show that this defines an equivalence relation, let $\epsilon \in \mathbb{Q}^+$ be given. Then, because $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence, we have that $\exists N \in \mathbb{N}$ such that $n, m \geq N \implies |x_m - x_n| < \epsilon$, so

$$(x_n)_{n\in\mathbb{N}} \sim (x_n)_{n\in\mathbb{N}}$$

Next, suppose $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in C$ satisfy $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$, that is $\lim_{n\to\infty}(x_n - y_n) = 0$. Then clearly $\lim_{n\to\infty}(x_n - y_n) = \lim_{n\to\infty}(y_n - x_n) = 0$ because $|x_n - y_n| = |y_n - x_n|$ for all $n \in \mathbb{N}$, so

$$(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}} \implies (y_n)_{n\in\mathbb{N}} \sim (x_n)_{n\in\mathbb{N}}$$

Finally, if $(x_n)_{n\in\mathbb{N}} \sim (x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}} \sim (z_n)_{n\in\mathbb{N}}$, then $\forall\epsilon \in \mathbb{Q}^+$, $\exists N_1, N_2 \in \mathbb{N}$ such that $n \geq N_1 \implies |x_n - y_n| < \frac{\epsilon}{2}$ and $n \geq N_2 \implies |y_n - z_n| < \frac{\epsilon}{2}$, and as a result for all $n \geq N = \max\{N_1 |x_n - y_n|, N_2\} \implies$

$$|x_n - z_n| = |x_n - y_n + y_n - z_n| \leq |x_n - y_n| + |y_n - z_n| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

so $\lim_{n\to\infty}(x_n - z_n) = 0$ and $(x_n)_{n\in\mathbb{N}} \sim (z_n)_{n\in\mathbb{N}}$. This proves that

$$(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}} \text{ and } (y_n)_{n\in\mathbb{N}} \sim (z_n)_{n\in\mathbb{N}} \implies (x_n)_{n\in\mathbb{N}} \sim (z_n)_{n\in\mathbb{N}}$$

so $\sim$ is indeed an equivalence relation. The set of **real numbers** $\mathbb{R}$ is then defined as the quotient set on C by $\sim$, that is the set of all equivalence classes generated by $\sim$:

$$\mathbb{R} := C/\sim$$

We define addition $+$, multiplication $\cdot$ and a partial order $\leq$ on $\mathbb{R}$ as follows:

$$x + y = [(x_n)_{n\in\mathbb{N}}] + [(y_n)_{n\in\mathbb{N}}] := [(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}}] = [(x_n + y_n)_{n\in\mathbb{N}}]$$

$$xy = [(x_n)_{n\in\mathbb{N}}][(y_n)_{n\in\mathbb{N}}] := [(x_n)_{n\in\mathbb{N}}(y_n)_{n\in\mathbb{N}}] = [(x_n y_n)_{n\in\mathbb{N}}]$$

$$x \leq y \text{ or } [(x_n)_{n\in\mathbb{N}}] \leq [(y_n)_{n\in\mathbb{N}}] \iff \begin{array}{c} (x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}} \\ \text{or} \\ \exists N \in \mathbb{N} \text{ s.t. } n \geq N \implies x_n < y_n \end{array}$$

After we make sure (Lemma 3.2 below) that for all nonzero real numbers there exist Cauchy sequence consisting either entirely of positive rational numbers or entirely of negative rational numbers, we can define the **positive** and **negative real numbers**, as well as the **absolute value** of a real number, as follows:

A real number x is said to be **positive** if it has a representative Cauchy sequence $(x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^+$ consisting entirely of positive rational numbers. We denote this by $x > 0$ or $x \in \mathbb{R}^+$. The **set of all positive real numbers** is denoted $\mathbb{R}^+$. The **set of all nonnegative numbers** is denoted $\mathbb{R}_0^+$ and equals $\mathbb{R}^+ \cup \{0\}$. A real number x is said to be **negative** if it has a representative Cauchy sequence $(x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^+$ consisting entirely of negative rational numbers. We denote this by $x < 0$ or $x \in \mathbb{R}^-$. The **set of all negative real numbers** is denoted $\mathbb{R}^-$. The **set of all nonpositive numbers** is denoted $\mathbb{R}_0^-$ and equals $\mathbb{R}^- \cup \{0\}$. The**absolute value** function is the function $|\cdot| : \mathbb{R} \to \mathbb{R}_0^+$ is given by

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$

Lastly, the **distance** $d : \mathbb{R} \times \mathbb{R} \to \mathbb{R}_0^+$ between two real numbers x and y is given by

$$d(x, y) = |x - y|$$

We can also embed the rational numbers $\mathbb{Q}$ into $\mathbb{R}$ by considering the representative Cauchy sequences $(x, x, \dots)$ in $\mathbb{Q}$ for all $x \in \mathbb{Q}$. We define $f : \mathbb{Q} \hookrightarrow C/\sim$ by

$$f(x) = [(x, x, \dots)]$$

Clearly the field operations of $\mathbb{Q}$ are preserved by this function, by our definitions of $\leq$, $+$ and $\cdot$, so f is an order-isomorphism.

We now show formally that this construction of the reals yields a structure that is equivalent to the first two structures above:

Lemma 3.1 *The operations of addition $+$ and multiplication $\cdot$, as well as the relation of partial order $\leq$ on $\mathbb{R}$, are well defined. That is, if* $[(x_n)_{n\in\mathbb{N}}] = [(x'_n)_{n\in\mathbb{N}}]$ *and* $[(y_n)_{n\in\mathbb{N}}] = [(y'_n)_{n\in\mathbb{N}}]$, *then*

$$\begin{aligned}
&[(x_n)_{n\in\mathbb{N}}] + [(y_n)_{n\in\mathbb{N}}] = [(x'_n)_{n\in\mathbb{N}}] + [(y'_n)_{n\in\mathbb{N}}] \\
&[(x_n)_{n\in\mathbb{N}}][(y_n)_{n\in\mathbb{N}}] = [(x'_n)_{n\in\mathbb{N}}][(y'_n)_{n\in\mathbb{N}}] \\
&[(x_n)_{n\in\mathbb{N}}] \leq [(y_n)_{n\in\mathbb{N}}] \implies [(x'_n)_{n\in\mathbb{N}}] \leq [(y'_n)_{n\in\mathbb{N}}]
\end{aligned}$$

Proof: If $[(x_n)_{n\in\mathbb{N}}] = [(x'_n)_{n\in\mathbb{N}}]$ and $[(y_n)_{n\in\mathbb{N}}] = [(y'_n)_{n\in\mathbb{N}}]$, then $(x_n)_{n\in\mathbb{N}} \sim (x'_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}} \sim (y'_n)_{n\in\mathbb{N}}$, so that $\lim_{n\to\infty}(x_n - x'_n) = \lim_{n\to\infty}(y_n - y'_n) = 0$, that is,

$$\forall \epsilon \in \mathbb{Q}^+,\ \exists N \in \mathbb{N} \text{ such that } n \geq N \implies |x_n - x'_n| < \frac{\epsilon}{2} \text{ and } |y_n - y'_n| < \frac{\epsilon}{2}$$

whence

$$|(x_n+y+n)-(x'_n+y'_n)| = |(x_n-x'_n)+(y_n-y'_n)| \leq |(x_n-x'_n)|+|(y_n-y'_n)| < \frac{\epsilon}{2}+\frac{\epsilon}{2} = \epsilon$$

or $\lim_{n\to\infty}\big((x_n+y_n)-(x'_n+y'_n)\big) = \lim_{n\to\infty}\big((x_n-x'_n)+(y_n-y'_n)\big) = 0+0 = 0$. Consequently, $(x_n + y_n)_{n\in\mathbb{N}} \sim (x'_n + y'_n)_{n\in\mathbb{N}}$, whence

$$[(x_n)_{n\in\mathbb{N}}]+[(y_n)_{n\in\mathbb{N}}] := [(x_n+y_n)_{n\in\mathbb{N}}] = [(x'_n+y'_n)_{n\in\mathbb{N}}] =: [(x'_n)_{n\in\mathbb{N}}]+[(y'_n)_{n\in\mathbb{N}}]$$

Likewise, $\forall \epsilon \in \mathbb{Q}^+$, $\exists N \in \mathbb{N}$ such that given any $n \geq N$, if we define $M = \max\{1, |y_n|, |x'_n|\}$, we have

$$|x_n - x'_n| < \frac{\epsilon}{2M} \quad \text{and} \quad |x_n - x'_n| < \frac{\epsilon}{2M}$$

whence

$$\begin{aligned}
|x_n y_n - x'_n y'_n| &= |x_n y_n - x'_n y_n + x'_n y_n - x'_n y'_n| \\
&= |y_n(x_n - x'_n) + x'_n(y_n - y'_n)| \\
&\leq |y_n(x_n - x'_n)| + |x'_n(y_n - y'_n)| \\
&= |y_n||x_n - x'_n| + |x'_n||y_n - y'_n| \\
&\leq M|x_n - x'_n| + M|y_n - y'_n| \\
&< M\frac{\epsilon}{2M} + M\frac{\epsilon}{2M} \\
&= \epsilon
\end{aligned}$$

or $\lim_{n,m\to\infty}(x_n y_n - x'_n y'_n) = 0$, so that $(x_n y_n)_{n\in\mathbb{N}} \sim (x'_n y'_n)_{n\in\mathbb{N}}$, whence

$$[(x_n)_{n\in\mathbb{N}}][(y_n)_{n\in\mathbb{N}}] := [(x_n y_n)_{n\in\mathbb{N}}] = [(x'_n y'_n)_{n\in\mathbb{N}}] =: [(x'_n)_{n\in\mathbb{N}}][(y'_n)_{n\in\mathbb{N}}]$$

Finally, suppose $[(x_n)_{n\in\mathbb{N}}] \leq [(y_n)_{n\in\mathbb{N}}]$. If $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$, then we have by our assumptions $(x'_n)_{n\in\mathbb{N}} \sim (x_n)_{n\in\mathbb{N}}$ and $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}} \sim (y'_n)$, so by the transitivity of $\sim$ we have $(x'_n)_{n\in\mathbb{N}} \sim (y'_n)_{n\in\mathbb{N}}$, whence

$$[(x'_n)_{n\in\mathbb{N}}] \leq [(y'_n)_{n\in\mathbb{N}}]$$

If, on the other hand, $\exists N \in \mathbb{N}$ such that $n \geq N \implies x_n < y_n$, the we must have that $\exists N' \in \mathbb{N}$ such that $n \geq N' \implies x'_n < y'_n$, for otherwise, if for all $N' \in \mathbb{N}$ there are $n \geq N'$ for which $x'_n \geq y'_n$, then since since $(x_n)_{n\in\mathbb{N}} \sim (x'_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}} \sim (y'_n)_{n\in\mathbb{N}}$, we have for all $\epsilon \in \mathbb{Q}^+$ we have $|x_n - x'_n| < \epsilon$ and $|y_n - y'_n| < \epsilon$, so that $x_n > x'_n - \epsilon$ and $y_n < y'_n + \epsilon$, and hence

$$y_n \leq y'_n \leq x'_n \leq x_n$$

contradicting $x_n < y_n$ for all $n \geq N$. Thus in this case, too, we must have $[(x'_n)_{n\in\mathbb{N}}] \leq [(y'_n)_{n\in\mathbb{N}}]$. ■

Lemma 3.2 *Let* $0 \in \mathbb{R}$ *be given by* $[(0', 0', \cdots)]$*, the equivalence class represented by* $(0', 0', \dots)$ *in* $\mathbb{Q}$*. Then for all* $x \in \mathbb{R}\backslash\{0\}$ *there exists an* $\epsilon \in \mathbb{Q}^+$ *such that exactly one of the following holds for all representatives* $(x_n)_{n\in\mathbb{N}}$ *in* $\mathbb{Q}$ *of* x*:*

1. $x_n > \epsilon$ *for all but finitely many* $n \in \mathbb{N}$*.*
2. $x_n < -\epsilon$ *for all but finitely many* $n \in \mathbb{N}$*.*

In particular, for any $x \in \mathbb{R}\backslash\{0\}$ *we can obtain a new sequence* $(p_n)_{n\in\mathbb{N}}$ *from any representative sequence* $(x_n)_{n\in\mathbb{N}}$ *of* x *by discarding finitely many* *terms of* $(x_n)_{n\in\mathbb{N}}$*, with the property that either* $p_n > \epsilon$ *for all* $n \in \mathbb{N}$ *or else* $p_n < -\epsilon$ *for all* $n \in \mathbb{N}$*.*

Proof: Suppose not, that is suppose for all $\epsilon \in \mathbb{Q}^+$ there is a representative $(x_n)_{n\in\mathbb{N}}$ of $x \in \mathbb{R}\backslash\{0\}$ for which $x_n \leq \epsilon$ for infinitely many $n \in \mathbb{N}$ and such that $x_n \geq -\epsilon$ for infinitely many $n \in \mathbb{N}$. Then, in particular for $\frac{\epsilon}{2} \in \mathbb{Q}^+$ there is a representative $(x_n)_{n\in\mathbb{N}}$ of x such that $|x_n| \leq \frac{\epsilon}{2}$ for infinitely many terms. As a consequence, for any other representative $(y_n)_{n\in\mathbb{N}}$ of x, because $(y_n)_{n\in\mathbb{N}} \sim (x_n)_{n\in\mathbb{N}}$, we have that $\exists N \in \mathbb{N}$ such that $n \geq N \implies |y_n - x_n| < \frac{\epsilon}{2}$. Consequently,

$$|y_n| = |y_n - x_n + x_n| \leq |y_n - x_n| + |x_n| \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \tag{3.1}$$

Now, either we have for *all* $\varepsilon \in \mathbb{Q}^+$ that there are infinitely many y_n in $[-\varepsilon, \varepsilon]$ or else there exists some $\varepsilon_0 \in \mathbb{Q}^+$ such that $[-\varepsilon_0, \varepsilon_0]$ contains only finitely many y_n. The second case is impossible because of (3.1), so we proceed to the first case: let us denote by $(y_{n_k})_{k\in\mathbb{N}}$ the subsequence of the sequence lying in $[-\varepsilon, \varepsilon]$. Because $(y_n)_{n\in\mathbb{N}}$ is a Cauchy sequence, we have that $\exists N \in \mathbb{N}$ such that $m, n_k \geq N \implies$

$$|y_m| \leq |y_m - y_{n_k}| + |y_{n_k}| < 2\varepsilon$$

Since this is true for all $\varepsilon \in \mathbb{Q}^+$, we have that $\lim_{n\to\infty} y_n = 0$, so that $(y_n)_{n\in\mathbb{N}} \in [(0', 0', \dots)] = 0$, contrary to assumption. Thus, the assumption that for all $\epsilon \in \mathbb{Q}^+$ there is a representative $(x_n)_{n\in\mathbb{N}}$ of $x \in \mathbb{R}\backslash\{0\}$ for which $x_n \leq \epsilon$ for infinitely many $n \in \mathbb{N}$ must be wrong, and we must have only finitely many terms of the sequence $(x_n)_{n\in\mathbb{N}}$ lying in $(-\epsilon, \epsilon)$. Since $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence, infinitely many terms satisfy either $x_n > \epsilon$ or $x_n < -\epsilon$ for some $\epsilon \in \mathbb{Q}^+$. Discarding these terms gives us our desired strictly positive or strictly negative sequence $(p_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}$, as the case may be, that represents x. ■

Theorem 3.3 *The real numbers are a structure* $(\mathbb{R}, \leq, -, ^{-1}, +, \cdot, 0, 1)$ *which is a field:*

1. $(\mathbb{R}, -, ^{-1}, +, \cdot, 0, 1)$ *is a field, that is for all* $x, y, z \in \mathbb{R}$ *we have*

$$\left.\begin{array}{lll} 1. & x + (y + z) = (x + y) + z & (\text{associativity of } +) \\ 2. & x + y = y + x & (\text{commutativity of } +) \\ 3. & \exists 0 \in \mathbb{R} \text{ such that } x + 0 = x & \\ 4. & \forall x \in \mathbb{R},\ \exists! -x \in \mathbb{R} \text{ such that } x + (-x) = 0 & \end{array}\right\} (\mathbb{R}, +) \text{ is an abelian group}$$

$$\left.\begin{array}{lll} 5. & x(yz) = (xy)z & (\text{associativity of } \cdot) \\ 6. & xy = yx & (\text{commutativity of } \cdot) \\ 7. & \exists 1 \in \mathbb{R} \text{ such that } 1x = x \text{ and } 0 \neq 1 & \\ 8. & \forall x \in \mathbb{R}\backslash\{0\},\ \exists x^{-1} \in \mathbb{R} \text{ such that } xx^{-1} = 1 & \end{array}\right\} (\mathbb{R}\backslash\{0\}, \cdot) \text{ is an abelian group}$$

$$\begin{array}{lll} 9. & x(y + z) = xy + xz & (\text{distributivity of } \cdot \text{ over } +) \end{array}$$

2. $(\mathbb{R}, \leq)$ *is a totally ordered set, that is for all* $x, y, z \in \mathbb{R}$ *we have*

$$\begin{array}{lllll} 1. & x \leq x & & & (\textit{reflexivity}) \\ 2. & x \leq y \text{ and } y \leq x & \Longrightarrow & x = y & (\textit{antisymmetry}) \\ 3. & x \leq y \text{ and } y \leq z & \Longrightarrow & x \leq z & (\textit{transitivity}) \\ 4. & x \leq y \text{ or } y \leq x & & & (\textit{totalness}) \end{array}$$

3. *The field operations* $+$ *and* $\cdot$ *are* **compatible** *with the partial order* $\leq$ *in the sense that for all* $x, y, z \in \mathbb{R}$ *we have*

$$\begin{array}{lll} 1. & x \leq y \implies x + z \leq y + z & (\textit{preservation of order under addition}) \\ 2. & 0 \leq x \text{ and } 0 \leq y, \text{ then } 0 \leq xy & (\textit{preservation of order under multiplication}) \end{array}$$

Proof: **1**.1, 2, 5, 6, and 9 follow from the properties of $\mathbb{Q}$, the definition of Cauchy sequence, and the lemma, which guarantees the well-definedness of $+$, $\cdot$ and $\leq$. We'll demonstrate **1.**1., the others follow similarly: for

$x, y, z \in \mathbb{R}$, we have

$$\begin{aligned}
x + (y + z) &= [(x_n)_{n\in\mathbb{N}}] + [(y_n)_{n\in\mathbb{N}} + (z_n)_{n\in\mathbb{N}}] \\
&= [(x_n)_{n\in\mathbb{N}}] + [(x_n + y_n)_{n\in\mathbb{N}}] \\
&= [(x_n)_{n\in\mathbb{N}} + (x_n + y_n)_{n\in\mathbb{N}}] \\
&= \left[\left(x_n + (y_n + z_n)\right)_{n\in\mathbb{N}}\right] \\
&= \left[\left((x_n + y_n) + z_n\right)_{n\in\mathbb{N}}\right] \\
&= [(x_n + y_n)_{n\in\mathbb{N}} + (z_n)_{n\in\mathbb{N}}] \\
&= [(x_n + y_n)_{n\in\mathbb{N}}] + [(z_n)_{n\in\mathbb{N}}] \\
&= [(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}}] + [(z_n)_{n\in\mathbb{N}}] \\
&= (x + y) + z
\end{aligned}$$

1.3. We define $0 \in \mathbb{R}$ as the equivalence class of Cauchy sequences in $\mathbb{Q}$ converging to $0' \in \mathbb{Q}$, and represented by $\mathbf{0} = (0', 0', \dots)$ in $\mathbb{Q}$. This equivalence class satisfies $x + 0 = 0 + x = x$ for all $x = [(x_n)_{n\in\mathbb{N}}]$:

$$x + 0 = [(x_n)_{n\in\mathbb{N}}] + [\mathbf{0}] = [(x_n + 0')_{n\in\mathbb{N}}] = [(x_n)_{n\in\mathbb{N}}] = x$$

and likewise $0 + x = x$.

1.4. For each $x = [(x_n)_{n\in\mathbb{N}}] \in \mathbb{R}$ we define its additive inverse $-x$ to be $[(-x_n)_{n\in\mathbb{N}}]$, for then

$$x + (-x) = [(x_n)_{n\in\mathbb{N}}] + [(-x_n)_{n\in\mathbb{N}}] = [(x_n + (-x_n))_{n\in\mathbb{N}}] = [(0', 0', \dots)] = 0$$

Clearly $-x$ exists whenever x does, so each $x \in \mathbb{R}$ has an additive inverse.

1.7. We define $1 \in \mathbb{R}$ as the equivalence class of Cauchy sequences in $\mathbb{Q}$ converging to $1' \in \mathbb{Q}$, which is represented by $\mathbf{1} = (1', 1', \dots)$ in $\mathbb{Q}$. This equivalence class satisfies $x1 = 1x = x$ for all $x = [(x_n)_{n\in\mathbb{N}}]$:

$$x1 = [(x_n)_{n\in\mathbb{N}}] + [\mathbf{1}] = [(x_n 1')_{n\in\mathbb{N}}] = [(x_n)_{n\in\mathbb{N}}] = x$$

and likewise $1x = x$.

1.8. For each $x \in \mathbb{R}\backslash\{0\}$, let $(x_n)_{n\in\mathbb{N}}$ be one of the Cauchy sequences consisting entirely of nonzero rational numbers, guaranteed to exist by L 3.2. We define x's multiplicative inverse x^{-1} to be the equivalence class represented by this sequence

$$x^{-1} := \left[\left(\frac{1}{x_n}\right)_{n\in\mathbb{N}}\right]$$

This definition indeed gives x's inverse, for we have

$$xx^{-1} = [(x_n)_{n\in\mathbb{N}}]\left[\left(\frac{1}{x_n}\right)_{n\in\mathbb{N}}\right] = \left[(x_n)_{n\in\mathbb{N}}\left(\frac{1}{x_n}\right)_{n\in\mathbb{N}}\right] = \left[\left(x_n\frac{1}{x_n}\right)_{n\in\mathbb{N}}\right] = [(1', 1', \dots)] = 1$$

2.1. Clearly, for all $x \in \mathbb{R}$, because x is represented by a Cauchy sequence $(x_n)_{n\in\mathbb{N}}$, and because $(x_n)_{n\in\mathbb{N}} \sim (x_n)_{n\in\mathbb{N}}$, we have that $x \leq x$.

2.2. If $x \leq y$ and $y \leq x$, it is not possible that, for representatives $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ of x and y, respectively, $\exists N \in \mathbb{N}$ such that $n \geq N \implies x_n < y_n$ and $y_n < x_n$ simultaneously, so we must have $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$, in which case $x = [(x_n)_{n\in\mathbb{N}}] = [(y_n)_{n\in\mathbb{N}}] = y$.

2.3. Let $x \leq y$ and $y \leq z$, and let $(x_n)_{n\in\mathbb{N}}$, $(y_n)_{n\in\mathbb{N}}$ and $(z_n)_{n\in\mathbb{N}}$ be representatives of x, y and z, respectively. There are four cases: **1.** If $\exists N_1, N_2 \in \mathbb{N}$ such that $n \geq N_1 \implies x_n < y_n$ and $n \geq N_2 \implies y_n < z_n$, then $\exists N = \max\{N_1, N_2\}$ such that $n \geq N \implies x_n < y_n < z_n$, whence $x_n < z_n$ by the transitivity of $<$ in $\mathbb{Q}$, and therefore $x \leq z$. **2.** If, however, $\exists N \in \mathbb{N}$ such that $n \geq N \implies x_n < y_n$ and $(y_n)_{n\in\mathbb{N}} \sim (z_n)_{n\in\mathbb{N}}$, then $\forall \epsilon \in \mathbb{Q}^+$, $\exists N' \in \mathbb{N}$ such that $n \geq N' \implies |y_n - z_n| < \epsilon$, so that $y_n < z_n + \epsilon$, whence for $M = \max\{N, N'\}$ we have $n \geq M \implies x_n < y_n < z_n + \epsilon$. Since this is true for all $\epsilon \in \mathbb{Q}^+$, we have that $x_n < y_n \leq z_n$, so by transitivity we have that $\exists M = \max\{N, N'\} \in \mathbb{N}$ such that $n \geq N \implies x_n < z_n$. Thus, $x \leq z$ in this case too. **3.** Similarly, if $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$ and $\exists N \in \mathbb{N}$ such that $n \geq N \implies y_n < z_n$ so that $\forall \epsilon \in \mathbb{Q}^+$, $\exists N' \in \mathbb{N}$ such that $n \geq N' \implies |x_n - y_n| < \epsilon$, so that $x_n < y_n + \epsilon$. Consequently, for $M = \max\{N, N'\}$ we have $n \geq N \implies x_n < y_n + \epsilon < z_n + \epsilon$, whence $x_n < y_n + \epsilon \leq z_n$, so that $x_n < y_n$, and hence $x \leq z$ in this case too. **4.** Finally, if $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}} \sim (z_n)_{n\in\mathbb{N}}$, then by the transitivity of $\sim$ we have $(x_n)_{n\in\mathbb{N}} \sim (z_n)_{n\in\mathbb{N}}$, and so $x \leq z$. Thus in all cases we have $x \leq y$ and $y \leq z \implies x \leq z$.

2.4. Let $x, y \in \mathbb{R}$ be given. If $x = [(x_n)_{n\in\mathbb{N}}] = [(y_n)_{n\in\mathbb{N}}] = y$, then $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$, so $x \leq y$ (and $y \leq x$). If, on the other hand, $x \neq y$, then $(x_n)_{n\in\mathbb{N}} \not\sim (y_n)_{n\in\mathbb{N}}$, so there must exist an $\epsilon \in \mathbb{Q}^+$ such that $\forall N \in \mathbb{N}$ we have $n \geq N \implies |x_n - y_n| \geq \epsilon$. Consequently, there exists an $N \in \mathbb{N}$ such that for all $n \geq N$ we have $x_n < y_n$ or $y_n < x_n$ (we clearly cannot have both, for $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ are Cauchy sequences, and having $x_n < y_n$ and $y_m < x_m$ for arbitrarily large n and m would mean $\lim_{n\to\infty}(x_n - y_n) = 0$). If $x_n < y_n$, then $x < y$, while if $x_n > y_n$, then $x > y$.

3.1. If $x = [(x_n)_{n\in\mathbb{N}}] \leq [(y_n)_{n\in\mathbb{N}}] = y$, suppose $\exists N \in \mathbb{N}$ such that $n \geq N \implies x_n < y_n$. Then $x_n + z_n < y_n + z_n$ by the properties of $<$ in $\mathbb{Q}$, so $x + z \leq y + z$. If, on the other hand, $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$, then $x = [(x_n)_{n\in\mathbb{N}}] = [(y_n)_{n\in\mathbb{N}}] = y$, so clearly $x + z = y + z$, so in particular $x + z \leq y + z$.

3.2. Suppose $0 \leq x = [(x_n)_{n\in\mathbb{N}}]$ and $0 \leq y = [(y_n)_{n\in\mathbb{N}}]$. If $x = 0$ and $y = 0$, then clearly

$$xy = [(0', 0', \dots)][(0', 0', \dots)] = [(0'0', 0'0', \dots)] = [(0', 0', \dots)] = 0$$

If $x, y > 0$, then by L 3.2 there exist $\epsilon_1, \epsilon_2 \in \mathbb{Q}^+$ and representative Cauchy sequences $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$, respectively, such that $x_n, y_n > \epsilon = \min\{\epsilon_1, \epsilon_2\}$ for all $n \in \mathbb{N}$. Consequently, $x_n y_n > \epsilon$ for all $n \in \mathbb{N}$, whence $xy = [(x_n y_n)_{n\in\mathbb{N}}] > 0$. ■

Theorem 3.4 ($\mathbb{R}$ is Complete) *Every nonempty subset S of $\mathbb{R}$ that is bounded above has a least upper bound,* $\sup S = \min S^u$.

Proof: Let u be an upper bound of S, that is $x \leq u$ for all $x \in S$. If u is not rational, i.e. if u is not the image of a rational number under the embedding $f : \mathbb{Q} \to \mathbb{R}$ considered above, then we may choose another, larger u which *is*. So assume that u is a rational upper bound of S. Since S is nonempty, let $s \in S$ and let L be a rational number satisfying $L < s$. Then, define two rational sequences $(l_n)_{n\in\mathbb{N}}$ and $(u_n)_{n\in\mathbb{N}}$ as follows: $l_1 = L$, $u_1 = u$, and $m_n = (l_n + u_n)/2$ for all $n \in \mathbb{N}$. If $m_n \in S^u$, then let $u_{n+1} = m_n$ and $l_{n+1} = l_n$, while if $m \notin S^u$, then let $u_{n+1} = u_n$ and $l_{n+1} = m_n$. By induction, $u_n \in S^u$ and $l_n \notin S^u$ for all $n \in \mathbb{N}$. Considering the unique rationals $u'_n = f^{-1}(u_n)$, where f is our embedding, we have that $u = [(u'_n)_{n\in\mathbb{N}}]$ is the least upper bound of S, because clearly $s \leq u$ for all $s \in S$, and moreover $\lim_{n\to\infty}(l_n - u_n) = 0$, so $u = [(l'_u)_{n\in\mathbb{N}}]$ as well, where $l'_n = f^{-1}(l_n)$, so that if $b < u$, then $b_n < l_n$ for all $n \geq N$ for some $N \in \mathbb{N}$, whence b is not an upper bound. ■

4 Equivalence of All Constructions of $\mathbb{R}$

Having made the effort to abstract the properties of the integers, the rationals and the real numbers, we are now in a position to reap their fruits: we can show that all constructions of $\mathbb{R}$ are isomorphic, that is are in a one-to-one correspondence which preserves their algebraic properties (addition and multiplication and their associated properties), their order properties, and their least upper bound properties. That is if $\mathbb{R}$ and $\mathbb{R}'$ are two constructions, then for all $a, b \in \mathbb{R}$ and $a', b' \in \mathbb{R}'$ with $a \leftrightarrow a'$ and $b \leftrightarrow b'$ we have $a + b \leftrightarrow a' + b'$, $ab \leftrightarrow a'b'$ and $a \leq b \iff a' \leq' b'$, while for all $S \subseteq \mathbb{R}$ and $S' \subseteq \mathbb{R}'$ with $S \leftrightarrow S'$ we have $\sup S \leftrightarrow \sup S'$. Formally,

Theorem 4.1 *Every complete totally ordered field is both isomorphic and order-isomorphic to* $\mathbb{R}$*, so in this sense all constructions of* $\mathbb{R}$ *are equivalent.*

Proof: In what follows, suppose $\mathbb{R}$ is any construction of the reals satisfying the axioms given in Construction 1 of above, and let $(F, \leq', -', {}^{-1'}, +', \cdot', 1', 0')$ be any other construction of $\mathbb{R}$, by which we here mean any complete totally ordered field, so that F is an ordered field that satisfies the least upper bound property. By basic properties of rings, we know there a monomorphism (injective ring homomorphism) $f : \mathbb{Q} \hookrightarrow F$ which is also an order-embedding. We can extend this function to an embedding of $\mathbb{R}$ into F as follows: for each $r \in \mathbb{R}$ let

$$D_r = \{q \in \mathbb{Q} \mid q < r\}$$

be the associated Dedekind cut. Since D_r is nonempty and bounded above in $\mathbb{Q}$, we have that $f(D_r)$ is nonempty and bounded above in F, so applying the assumed least upper bound property of F we define the function $g : \mathbb{R} \to F$ by

$$g(r) = \sup f(D_r)$$

Then g is also a monomorphism and order-embedding, since if $r, s \in \mathbb{R}$, then

$$\begin{aligned}
&g(r+s) = \sup f(D_{r+s}) = \sup f(D_r) +' \sup f(D_s) = g(r) +' g(s) \\
&g(rs) = \sup f(D_{rs}) = \sup f(D_r) \cdot \sup f(D_s) = g(r)g(s) \\
&r \leq s \quad \Longrightarrow \quad g(r) = \sup f(D_r) \leq \sup f(D_s) = g(s) \\
&g(r) = g(s) \quad \Longrightarrow \quad r = s
\end{aligned}$$

and clearly g is an extension of f. We'll prove the second equation, since the other three follow similarly: if

$$x \leq' \sup f(D_{rs})$$

then $x \leq' a$ for any $a \in f(D_{rs})^u$, so in particular $x \leq' bc$ for all $b \in f(D_r)^u$, $c \in f(D_s)^u$, whence

$$x \leq' \sup f(D_r) \cdot' \sup f(D_s)$$

Conversely if

$$x \leq' \sup f(D_r) \cdot' \sup f(D_s)$$

then $x \leq' bc$ for all $b \in f(D_r)^u$, $c \in f(D_s)^u$. Now, for any

$$a \in f(D_{rs})^u \backslash \{\sup f(D_{rs})\}$$

there exist such b and c that also satisfy $bc \leq a$, as follows: if

$$a \in f(D_{rs})^u \backslash \{\sup f(D_{rs})\}$$

then $\sup f(D_{rs}) <' a$, so by the order denseness of $\mathbb{Q}$ we can always find a $p \in \mathbb{Q}$ such that

$$\sup f(D_{rs}) <' b = f(p) <' a$$

and then we can pick c to be

$$c = \frac{\sup f(D_{rs}) + a}{2b}$$

Then we have $\sup f(D_{rs}) <' bc <' a$. Because we can always find such b and c we must have

$$x \leq' \sup f(D_{rs})$$

We have just shown that $g(\mathbb{R}) \subseteq F$ and $\mathbb{R} \cong g(\mathbb{R})$. If we can show that $g(\mathbb{R}) \supset F$, we will have proved that g is surjective, and therefore bijective, and so an isomorphism (both a ring isomorphism and an order-isomorphism), and we will have thereby finished the proof. Towards this end, note first that F also satisfies the Archimedean property, which follows via T **??** from the fact that $\mathbb{R}$ is order-embedded into F and $\mathbb{R}$ satisfies the Archimedean property. Consequently, for any $k \in F$ there exists an $n \in \mathbb{N}$, and so a $g(n) \in F$, such that $-g(n) < k < g(n)$. Let

$$D_k = \{r \in \mathbb{R} \mid g(r) < k\}$$

and note that because $g(\mathbb{R}) \cong \mathbb{R}$ we have that we have that D_k and $g(D_k)$ are both nonempty and bounded above, so that $\exists \sup D_k \in \mathbb{R}$, whence $\exists g(\sup D_k) \in F$, and also $\exists \sup g(D_k) \in F$, and since $g(\mathbb{R}) \subseteq F$ we have that

$$\sup g(D_k) \leq g(\sup D_k) \tag{4.1}$$

by the least upper bound property of F. We claim that

$$\sup g(D_k) = g(\sup D_k) \tag{4.2}$$

Suppose not, that is suppose $\sup g(D_k) < g(\sup D_k)$. Then, by the Archimedean property of F, there is some $n \in \mathbb{N}$ such that

$$0 = g(\sup D_k) - g(\sup D_k) < g(n)^{-1} < g(\sup D_k) - \sup g(D_k) \tag{4.3}$$

This implies that

$$\sup g(D_k) < g(\sup D_k) - g(n)^{-1} < g(\sup D_k) \tag{4.4}$$

But then by (4.1), the second inequality in (4.4), and the definition of $g(\sup D_k)$ and $\sup g(D_k)$, the first of which implies that $g^{-1}(g(\sup D_k) - g(n)^{-1}) = \sup D_k - n \in D_k$, we have

$$g(\sup D_k) - g(n)^{-1} < \sup g(D_k)$$

which by the first inequality of (4.4) implies the contradiction

$$\sup g(D_k) < \sup g(D_k)$$

Hence we must have $\sup g(D_k) = g(\sup D_k)$, and so $g(k) \in g(\mathbb{R})$, whence

$$g(\mathbb{R}) \supset F$$

and consequently $g(\mathbb{R}) = F$. ■

5 Further Properties of $\mathbb{R}$

5.1 Exponentiation

If $a \in \mathbb{R}_0^+$ and $n \in \mathbb{N}$, then we define the nth power of a as

$$a^n := \overbrace{a \cdot a \cdots a}^{n \text{ times}}$$

This defines a real number, as we show in Theorem 5.5 below. We define a^0 as

$$a^0 = 1$$

for *all* $a \in \mathbb{R}$ (including 0), and we define a^{-n} for $a \in \mathbb{R}^+$ as

$$a^{-n} := \frac{1}{a^n} = \frac{1}{\underbrace{a \cdot a \cdots a}_{n \text{ times}}}$$

The number $\pm n \in \mathbb{Z}$ in the above three cases is called the **integer exponent** of a. Before we can define **nth roots**, however, we first need to show that they are real numbers! Theorem 5.8 below guarantees this fact, and this fact guarantees that the expression

$$a^{1/n}$$

also denoted $\sqrt[n]{a}$, is well defined and represents a unique real number. The notation $\sqrt[n]{a}$ is in keeping with that of the square root of a, which is denoted both as $\sqrt{a}$ and as $a^{1/2}$. Recall that one of the shortcomings of the rational numbers was that they did not contain the number $\sqrt{2}$. Theorem 5.8, therefore, remedies this problem, and ensures not only that $\sqrt{2}$, but $2^{1/n}$ for all $n \in \mathbb{N}$, is a real number. This holds not only for 2, of course, but for all $a \in \mathbb{R}_0^+$.

The expression $a^{-1/n}$ is defined in the same manner as above,

$$a^{-1/n} := \frac{1}{a^{1/n}}$$

and is also well defined by Theorem 5.5. Finally, since $a^{1/n}$ is a (nonnegative) real number, we can define the **fractional exponent** $a^{m/n}$ for $m/n \in \mathbb{Q}$, which we do as follows:

$$a^{m/n} := (a^m)^{1/n}$$

We will show below that, since $a^{m/n} \in \mathbb{R}$ for all $m/n \in \mathbb{Q}$, we also have that $a^b \in \mathbb{R}$ for all $b \in \mathbb{R}$. Thus, expressions like $\pi^{e\sqrt{2}}$ are well defined real numbers. This will require considerable machinery to develop, in particular a proper definition of the exponential and logarithmic functions e^x and $\ln x$. Then we will define a^b by $a^b := e^{b \ln a}$, so that for example $\pi^{e\sqrt{2}} = e^{e\sqrt{2}\ln \pi}$.

5.2 Basic Arithmetic and Order Properties of $\mathbb{R}$

Lemma 5.1 *The numbers* 0 *and* 1 *in* $\mathbb{R}$ *are unique.*

Proof: We know there is at least one 0 in $\mathbb{R}$, by Axiom **1**.3, and it satisfies $x + 0 = x$ for all $x \in \mathbb{R}$. Let us suppose there were a second zero, $0' \in \mathbb{R}$, satisfying $x + 0' = x$ for all $x \in \mathbb{R}$. Then, letting $0'$ play the role of x we have

$$0' = 0 + 0'$$

while letting 0 play the role of x gives

$$0 + 0' = 0$$

Therefore, $0' = 0 + 0' = 0$. This shows that there is no second zero, for it would be equal to the first.

Similarly, we know there is at least one 1 in $\mathbb{R}$, by Axiom **1**.7, and it is characterized by $1x = x$ for all $x \in \mathbb{R}$. If we suppose there were another $1'$ with this property, then by letting each of 1 and $1'$ play the role of x we have

$$1 = 11' = 1' \qquad \blacksquare$$

Lemma 5.2 (Cancellation Law) *For any* $x, y, z \in \mathbb{R}$ *we have*

$$x + z = y + z \implies x = y$$

and

$$x + z \leq y + z \implies x \leq y$$

Similarly, for $z \neq 0$,

$$xz = yz \implies x = y$$

Proof: Suppose first $x+z=y+z$. Then, using Axioms **1**.1, 3, and 4,

$$\begin{aligned} x &= x+0 \\ &= x+(z+(-z)) \\ &= (x+z)+(-z) \\ &= (y+z)+(-z) \\ &= y+(z+(-z)) \\ &= y+0 \\ &= y \end{aligned}$$

Suppose next that $x+z \leq y+z$, and use Axioms **1**.1, 3, 4 and **3**.1:

$$\begin{aligned} x &= x+0 \\ &= x+(z+(-z)) \\ &= (x+z)+(-z) \\ &\leq (y+z)+(-z) \\ &= y+(z+(-z)) \\ &= y+0 \\ &= y \end{aligned}$$

Finally, suppose $xz=yz$ and $z \neq 0$. Then, using Axioms **1**.6-8,

$$x = 1x = x1 = x(zz^{-1}) = (xz)z^{-1} = (yz)z^{-1} = y(zz^{-1}) = y1 = 1y = y \quad \blacksquare$$

Lemma 5.3 *Axiom* ***1**.9 has a right version,*

$$(x+y)z = xz+yz$$

Proof: Using Axioms **1**.6, 9 we have

$$(x+y)z = z(x+y) = zx+zy = xz+yz \quad \blacksquare$$

Lemma 5.4 $0x=0$ *and* $(-1)x=-x$ *for all* $x \in \mathbb{R}$.

Proof: First, observe that by Axioms **1**.3, 7 and the previous Lemma,

$$x+0 = x = 1x = (1+0)x = 1x+0x = x+0x$$

which by the Cancellation Law means $0=0x$. Using this result, Axioms **1**.3, 7 and the previous Lemma, we get

$$(-1)x+x = (-1)x+1x = ((-1)+1)x = 0x = 0 = (-x)+x$$

which by the Cancellation Law means $(-1)x=-x$. $\blacksquare$

Theorem 5.5 (Arithmetic Properties of $\mathbb{R}$) *For all $x, y, z, w \in \mathbb{R}$, the following hold:*

1. $-(-x) = x$
2. $x(-y) = -(xy) = (-x)y$
3. $(-1)x = -x$
4. $xy = x \implies y = 1$ *if* $x \neq 0$
5. $\frac{x}{x} = 1$ *if* $x \neq 0$
6. $\frac{x}{1} = x$
7. $xy \in \mathbb{R}\backslash\{0\}$ *if* $x, y \in \mathbb{R}\backslash\{0\}$
8. $\frac{1}{x} \cdot \frac{1}{y} = \frac{1}{xy}$ *if* $x, y \in \mathbb{R}\backslash\{0\}$
9. $\frac{z}{x} \cdot \frac{w}{y} = \frac{zw}{xy}$ *if* $x, y \in \mathbb{R}\backslash\{0\}$
10. $\frac{x}{y} + \frac{z}{w} = \frac{xw + yz}{yw}$ *if* $y, w \in \mathbb{R}\backslash\{0\}$
11. $x \neq 0 \implies \frac{1}{x} \neq 0$
12. $\frac{1}{\frac{x}{y}} = \frac{y}{x}$ *if* $x, y \in \mathbb{R}\backslash\{0\}$
13. $\frac{x/y}{z/w} = \frac{xw}{yz}$ *if* $x, y, z \in \mathbb{R}\backslash\{0\}$
14. $\frac{zx}{y} = z\frac{x}{y}$ *if* $y \in \mathbb{R}\backslash\{0\}$
15. $\frac{-x}{y} = \frac{x}{-y} = -\big(\frac{x}{y}\big)$ *if* $y \in \mathbb{R}\backslash\{0\}$

Proof: (1) Every x possesses a negative, $-x$, by Axiom **1**.4, and it satisfies

$$x + (-x) = 0$$

What is the negative of $-x$? Let us use the Cancellation Law:

$$x + (-x) = 0 = -(-x) + (-x) \quad \implies \quad x = -(-x)$$

(2) $x(-y) + xy = x((-1)y) + xy = (x(-1))y + xy = ((-1)x)y + xy = (-x)y + xy = ((-x) + x)y = 0y = 0 = -(xy) + xy$, so the Cancellation Law implies $x(-y) = -(xy)$ Similarly with $(-x)y = -(xy)$.

(3) This was Lemma 5.4.

(4) This was Lemma 5.1.

(5) This is an Axiom, **1**.8, so I don't know what it's doing in a theorem.

(6) Follows from the fact that $1^{-1} = 1$ on account of $1 \cdot 1 = 1 = 1 \cdot 1^{-1}$ and the Cancellation Law, Lemma 5.2.

(7) If $xy = 0$, then either x or y must equal 0. Suppose $y \neq 0$, and observe that

$$x = 1x = x1 = x(yy^{-1}) = (xy)y^{-1} = 0y^{-1} = 0$$

Reversing the roles of x and y shows that if $x \neq 0$, the $y = 0$. It is of course possible that both x and y equal 0. All this shows that if $xy = 0$ then $x = 0$ or $y = 0$, which is the contrapositive of $x \neq 0$ and $y \neq 0$ implies $xy \neq 0$.

(8) This is the statement that $x^{-1}y^{-1} = (xy)^{-1}$. We already know that if $x, y \neq 0$, then $xy \neq 0$, so all of x, y, and xy have multiplicative inverses. Now observe that

$$(xy)(x^{-1}y^{-1}) = y(xx^{-1}) = yy^{-1} = 1 = (xy)(xy)^{-1}$$

so by the Cancellation Law we must have $x^{-1}y^{-1} = (xy)^{-1}$. I skipped a couple of commutations and associations in the above line, FYI.

(9) This is just the associative and commutative laws, Axioms **1**.5-6, plus (8) above:

$$\begin{aligned}\frac{z}{x} \cdot \frac{w}{y} = (zx^{-1})(wy^{-1}) = z(x^{-1}w)y^{-1} = z(wx^{-1})y^{-1} \\ = (zw)(x^{-1}y^{-1}) = zw(xy)^{-1} = \frac{zw}{xy}\end{aligned}$$

(10) We'll use Axioms **1**.5-9: since $y \neq 0$ and $w \neq 0$, $y^{-1} = \frac{1}{y}$ and $w^{-1} = \frac{1}{w}$ exist, so

$$\begin{aligned}\frac{x}{y} + \frac{z}{w} &= (xy^{-1}) + (zw^{-1}) \\ &= (xy^{-1})1 + (zw^{-1})1 \\ &= (xy^{-1})(ww^{-1}) + (zw^{-1})(yy^{-1}) \\ &= x(y^{-1}w)w^{-1} + z(w^{-1}y)y^{-1} \\ &= x(wy^{-1})w^{-1} + z(yw^{-1}y^{-1} \\ &= (xw)(y^{-1}w^{-1}) + (zy)(w^{-1}y^{-1}) \\ &= (xw)(y^{-1}w^{-1}) + (zy)(y^{-1}w^{-1}) \\ &= (xw + zy)(y^{-1}w^{-1}) \\ &= \frac{xw + yz}{yw}\end{aligned}$$

(11) If $x \neq 0$, then x^{-1} exists and $xx^{-1} = 1$. But $1 \neq 0$ by Axiom **1**.7, so by the proof of (8) above we must have $x^{-1} \neq 0$.

(12) This just says that $(xy^{-1})^{-1} = x^{-1}y$, which follows from the fact that $(y^{-1})^{-1} = y$ in the same way that $-(-y) = y$ (as in (1) above).

(13) Combining (9) and (12) above, we get

$$\frac{x/y}{z/w} = \frac{x}{y} \cdot \frac{w}{z} = \frac{xw}{yz}$$

(14) This is nothing but associativity and commutativity, Axioms **1**.5-6:

$$\frac{zx}{y} = (xz)y^{-1} = (zx)y^{-1} = z(xy^{-1}) = z\frac{x}{y}$$

(15) This is nothing but (2) applied to $-(xy^{-1})$. ■

Theorem 5.6 (Order Properties of $\mathbb{R}$) *For all $x, y, z, w \in \mathbb{R}$, the following hold:*

1. $x > y$ *and* $z > w \implies x + z > y + w$
2. $x, y > 0 \implies x + y > 0$ *and* $xy > 0$
3. $x > 0 \iff -x < 0$
4. $x > y \iff -x < -y$
5. $x > y$ *and* $z < 0 \implies xz < yz$
6. $x \neq 0 \implies x^2 > 0$
7. $-1 < 0 < 1$
8. $xy > 0 \iff$ *either* $x, y > 0$ *or* $x, y < 0$
9. $x > 0 \implies \frac{1}{x} > 0$
10. $x > y > 0 \implies \frac{1}{x} < \frac{1}{y}$
11. $x < y \implies x < \dfrac{x+y}{2} < y$

Proof: (1) Suppose $x > y$ and $z > w$. By Axiom **3**.1, we have $x + z > y + z$ and $y + z > y + w$. The transitivity of $>$ then shows that $x + z > y + w$.

(2) Let $x, y > 0$ and observe that Axioms **1**.3 and **3**.1 give $x + y > 0 + y = y$, so since $y > 0$ transitivity of $>$ ensures $x + y > 0$. Axiom **3**.1 also ensures $xy \geq 0$. To see that $xy > 0$ when $x, y > 0$, note that $xy = 0$ only if $x = 0$ or $y = 0$ (as in the proof of Theorem 5.5, (7)).

(3) Suppose $x > 0$ and use Axioms **1**.3 and **3**.1:

$$0 = x + (-x) > 0 + (-x) = -x$$

Conversely, if $0 > -x$, then adding x to both sides gives

$$x = x + 0 > x + (-x) = 0$$

(4) Suppose $x > y$ and add $-x$ to both sides and then $-y$ to both sides, making use of Axiom **3**.1:

$$x > y \iff 0 = x + (-x) > y + (-x)$$
$$\iff \begin{cases} -y = (-y) + 0 \\ \quad > (-y) + (y + (-x)) \\ \quad = ((-y) + y) + (-x) \\ \quad = 0 + (-x) \\ \quad = -x \end{cases}$$

(5) Let $x > y$ and $0 > z$. Then by (3) above we have $0 < (-z)$, and hence Axioms **1**.9, **3**.1-2 and (1)-(2) of Theorem 5.5 apply to give

$$x + (-y) > 0 \text{ and } (-z) > 0 \implies -(zx) + zy = (-z)(x + (-y)) > 0$$

which means, again by Axiom **3**.1, $zy > zx$, and thus by commutativity (Axiom **1**.6) $yz > xz$.

(6) Let $x \neq 0$ and consider x^2. If $x > 0$, then Axiom **3**.2 gives $x^2 > x \cdot 0 = 0$ (the last equality by Lemma 5.4), while if $x < 0$, then $-x > 0$ by (3) above. Now, observe that for any $x \in \mathbb{R}$ we have by associativity (Axiom **1**.5), Lemma 5.4 and Theorem 5.5

$$(-1)^2 x = (-1)((-1)x) = (-1)(-x) = -(-x) = x$$

so Lemma 5.1 applies to tell us that $(-1)^2 = 1$. We use this in combination with $-x > 0$ as follows:

$$x^2 = 1x^2 = (-1)^2 x^2 = ((-1)x)^2 = (-x)^2 > (-x)0 = 0$$

the last inequality following from Axiom **3**.2 and the last equality from Lemma 5.4.

(7) We know from Axiom **1**.7 that $0 \neq 1$, while from (6) above we have

$$1 = 1^2 > 0$$

and from (3) above we consequently have $0 > -1$.

(8) Suppose $xy > 0$. We know that $x, y \neq 0$, else $xy = 0$ (see proof of (7) in Theorem 5.5), hence $x > 0$ or $x < 0$ and similarly with y. Suppose first $x > 0$. If $y < 0$, then (5) above gives $xy < y \cdot 0 = 0$, which is in contradiction with our assumption, so we must have $y > 0$. Reversing the roles of x and y shows that if $y > 0$, then $x > 0$. If, on the other hand, $x < 0$, then $y < 0$, for otherwise, if $y > 0$, (5) above gives $xy < 0y = 0$, a contradiction. Similarly $y < 0$ implies $x < 0$.

(9) Let $x > 0$ and observe that by (7) above we have $x^{-1}x = 1 > 0$, so (8) applies to give $x^{-1} > 0$.

(10) Let $x > y > 0$. By transitivity of $>$ we have $x > 0$, and hence by (9) we conclude that $x^{-1}, y^{-1} > 0$, which means $0 < 1 = x^{-1}x < x^{-1}y$ and hence $0 < y^{-1} = y^{-1}1 < x^{-1}yy{-}1 = x^{-1}1 = x^{-1}$, using Axioms **1**.5, 7, 8.

(11) Suppose $x < y$ and consider $\frac{x+y}{2} = \frac{1}{2}(x+y) = x/2 + y/2$. Now, $0 < 1$ implies $1 = 1 + 0 < 1 + 1 = 2$, by Axiom **3**.1, so that by (8) and (10) above we get $0 < 1/2 < 2/2 = 1$. Multiplying through by x and using Axiom **3**.2 we conclude $x/2 < x1 = x$ if $x > 0$, and $x/2 > x$ if $x < 0$ by (5) above. If $x > 0$, then by transitivity $y > 0$ too, and we conclude that $y/2 < y$ as well, and $x < y$ implies $x/2 < y/2$. This means

$$\begin{aligned} x = 1x = \frac{2}{2}x = \frac{1}{2}(1+1)x = \frac{1}{2}(1x+1x) &= \frac{1}{2}(x+x) \\ &= \frac{x}{2} + \frac{x}{2} < \frac{x}{2} + \frac{y}{2} < \frac{y}{2} + \frac{y}{2} = y \end{aligned}$$

where the last equality follows from similar reasoning as the LHS for x. If $x < 0$, then $y < 0$, too, and we can apply the above argument to $0 < -x < -y$ and conclude that

$$-x < -\frac{x+y}{2} < -y$$

from which it follows (by (3) and (5)) that

$$x < \frac{x+y}{2} < y \qquad \blacksquare$$

Theorem 5.7 *For all $x, y, x_1, \ldots, x_n \in \mathbb{R}$ and all $n \in \mathbb{N}$ we have*

1. $|x+y| \leq |x| + |y|$ (*Triangle Inequality*)
2. $|x_1 + x_2 + \cdots + x_n| \leq |x_1| + |x_2| + \cdots + |x_n|$
3. $|xy| = |x||y|$

Proof: (1) This boils down to cases, which are four, $x, y > 0$, $x, y < 0$, $x > 0$ and $y < 0$, and $x < 0$ and $y > 0$. If $x, y > 0$, then this is just an identity

$$|x+y| = x + y = |x| + |y| \leq |x| + |y|$$

If $x, y < 0$, then

$$|x+y| = -(x+y) = (-x) + (-y) = |x| + |y| \leq |x| + |y|$$

If, on the other hand, say $x < 0$ and $y > 0$, then $x < x + y < y$, so

$$|x+y| < \max\{|x|, |y|\} < |x| + |y|$$

Similarly with $x > 0$ and $y < 0$.

(2) Follows inductively: We have $|x_1 + x_2| \leq |x_1| + |x_2|$ by (1) above, so suppose $|x_1 + x_2 + \cdots + x_n| \leq |x_1| + |x_2| + \cdots + |x_n|$ for some $n \geq 2$ and consider the $(n+1)$st case:

$$\begin{aligned} |(x_1 + x_2 + \cdots + x_n) + x_{n+1}| &\leq |x_1 + |x_2 + \cdots + x_n| + |x_{n+1}| \\ &\leq |x_1| + |x_2| + \cdots + |x_n| + |x_{n+1}| \end{aligned}$$

where the first inequality is by (1) and the second by our induction hypothesis.

(3) This again follows by cases. This is clearly true for $x, y > 0$ because each side is their positive product. For $x, y < 0$, we have

$$|xy| = xy = 1xy = (-1)^2 xy = ((-1)x)((-1)y) = (-x)(-y) = |x||y|$$

The first equality follows from Theorem 5.6, (8), and the fourth equality from commutativity and associativity, and the fifth from Lemma 5.4. For $x < 0$ and $y > 0$, we have $|x| = -x$ and $|y| = y$, so $xy < 0$ and

$$|xy| = -(xy) = (-x)y = |x||y|$$

by Theorem 5.5, (2) and Theorem 5.6, (5). Similarly with $x > 0$ and $y < 0$. ■

Theorem 5.8 (Existence-Uniqueness of the n-th Root) *For any $a \in \mathbb{R}^+$ and any $n \in \mathbb{N}$ there exists a unique n-th root, a real number $b > 0$ such that $b^n = a$.*

Proof: The proof is totally dependent on the least upper bound property of $\mathbb{R}$. Let $A = \{x \in \mathbb{R}^+ \mid x^n \leq a\}$. Then A is bounded above (by 1 if $a \leq 1$, and by a if $a \geq 1$), so that $b = \sup A$ exists. We suppose $b^n \neq a$ by way of supposing $b^n < a$ and $b^n > a$ in turn, and derive contradictions, to conclude that $b^n = a$. First, suppose $b^n < a$ and let $\epsilon = a - b^n$ and $h \in (0, 1]$ be given by $h = \frac{\epsilon}{(1+b)^n - b^n}$. Then by the binomial theorem,

$$\begin{aligned}
(b+h)^n &= b^n + nb^{n-1}h + \frac{n(n-1)}{2!}b^{n-2}h^2 + \cdots + nbh^{n-1} + h^n \\
&= b^n + h\left[nb^{n-1} + \frac{n(n-1)}{2!}b^{n-2}h + \cdots + nbh^{n-2} + h^{n-1}\right] \\
&\leq b^n + h\left[nb^{n-1} + \frac{n(n-1)}{2!}b^{n-2} + \cdots + nb + 1\right] + hb^n - hb^n \\
&= b^n + h\left[b^n + nb^{n-1} + \frac{n(n-1)}{2!}b^{n-2} + \cdots + nb + 1\right] - hb^n \\
&= b^n + h(b+1)^n - hb^n \\
&= b^n + h[(b+1)^n - b^n] \\
&= b^n + \frac{\epsilon}{(1+b)^n - b^n}[(b+1)^n - b^n] \\
&= b^n + \epsilon \\
&= a
\end{aligned}$$

But this shows that $\exists c = b + h > b$ such that $c^n \leq a$, which contradicts the assumption that $c \leq b$, b being an upper bound. Similarly, if we suppose $b^n > a$, let $\epsilon = b^n - a$, and $h \in (0,1]$ given by $h = \frac{\epsilon}{(1+b)^n - b^n}$. Then by the binomial theorem,

$$\begin{aligned}
(b-h)^n &= b^n - nb^{n-1}h + \frac{n(n-1)}{2!}b^{n-2}h^2 - \cdots + (-1)^{n-1}nbh^{n-1} + (-1)^n h^n \\
&= b^n - h\left[nb^{n-1} - \frac{n(n-1)}{2!}b^{n-2}h + \cdots + (-1)^{n-2}nbh^{n-2} + (-1)^{n-1}h^{n-1}\right] \\
&\geq b^n - h\left[nb^{n-1} + \frac{n(n-1)}{2!}b^{n-2}h + \cdots + nbh^{n-2} + h^{n-1}\right] \\
&\geq b^n - h\left[nb^{n-1} - \frac{n(n-1)}{2!}b^{n-2} + \cdots + nb + 1\right] + hb^n - hb^n \\
&= b^n - h\left[b^n + nb^{n-1} + \frac{n(n-1)}{2!}b^{n-2} + \cdots + nb + 1\right] + hb^n \\
&= b^n - h(b+1)^n + hb^n \\
&= b^n - h[(b+1)^n - b^n] \\
&= b^n - \frac{\epsilon}{(1+b)^n - b^n}[(b+1)^n - b^n] \\
&= b^n - \epsilon \\
&= a
\end{aligned}$$

But this shows that $\exists c = b - h < b$ such that $c^n \leq a$, which contradicts the assumption that b is the *least* upper bound for A – we have just found a smaller one, c. Consequently, the assumption that $b \neq a$ leads to contradictions, and we must therefore have $b = a$. ■

Theorem 5.9 (Exponent Laws in $\mathbb{R}$) *For all $a, b \in \mathbb{R}^+$ and $p, q \in \mathbb{Q}$ the following hold:*

1. $a^p a^q = a^{p+q}$
2. $(a^p)^q = a^{pq}$
3. $a^q b^q = (ab)^q$

If $p, q \in \mathbb{N}$, then the theorem holds for all *$a, b \in \mathbb{R}$.*

Proof: We prove this for $m, n \in \mathbb{Z}$ first, then for $1/m$ and $1/n$, and finally for $p, q \in \mathbb{R}$.

1. a. First we prove this for $m, n \in \mathbb{N}$ by induction on m. For a fixed $n \in \mathbb{N}$ and $a \in \mathbb{R}$, we have by definition that $a^n a^1 = a^n a = a^{n+1}$, so the case $m = 1$ is proved. Now suppose that $a^n a^m = a^{n+m}$, and note that $a^n a^{m+1} = a^n(a^m a^1) = (a^n a^m)a^1 = a^{m+n} a^1 = a^{m+n+1}$, so it holds for all $m \in \mathbb{N}$. For the case $m = 0$ note that $a^n a^0 = a^n 1 = a^n = a^{a+0}$. Finally, we extend this to $m \in \mathbb{Z}^-$ by noting that $a^{-n} = 1/a^n$ by definition for any $n \in \mathbb{N}$, so for any $n \in \mathbb{Z}$ and $-m \in \mathbb{Z}^-$ we have

$$a^n a^{-m} = a^n \frac{1}{a^m}$$

If $m = n$ then clearly they cancel and $a^n a^{-m} = 1 = a^0 = a^{n-n} = a^{n-m}$. If $m < n$, then

$$a^n a^{-m} = \frac{a^n}{a^m} = \frac{\overbrace{a \cdots a}^{m}\overbrace{a \cdots a}^{n-m}}{\underbrace{a \cdots a}_{m}} = a^{n-m}$$

and if $m > n$, then by the same argument we have $a^n a^{-m} = \frac{1}{a^{m-n}} = a^{-(m-n)} = a^{n-m}$.

b. For a fixed $n \in \mathbb{N}$ and $a \in \mathbb{R}$, we have $(a^n)^1 = a^n = a^{n \cdot 1}$, so the statement holds for $m = 1$. If we suppose it holds for $m \geq 1$, then $(a^n)^{m+1} = (a^n)^m(a^n) = a^{mn}a^n = a^{mn+n} = a^{n(m+1)}$, so it holds for all $m \in \mathbb{N}$. We can generalize this to $\mathbb{Z}$ using the same procedure as in 1 above.

c. For $a, b \in \mathbb{R}$ we have $a^1 b^1 = ab = (ab)^1$ by definition, so suppose the statement holds for some $m \geq 1$. Then $a^{m+1}b^{m+1} = a^m a b^m b = a^m b^m ab =$

$(ab)^m(ab) = (ab)^{m+1}$, so it holds for all $m \in \mathbb{N}$. We can generalize this to $\mathbb{Z}$ using the same procedure as in 1 above.

2. a. If $a \in \mathbb{R}^+$ and $m, n \in \mathbb{N}$, then let $x = a^{1/n}a^{1/m}$. By 1.a. and b. above we have

$$x^{mn} = (a^{1/m}a^{1/n})^n = (a^{1/m})^{mn}(a^{1/n})^{mn} = \big((a^{1/m})^m\big)^n\big((a^{1/n})^n\big)^m = a^n a^m = a^{n+m}$$

and therefore $x = (x^{mn})^{1/mn} = (a^{n+m})^{1/mn} = a^{(n+m)/mn} = a^{1/n+1/m}$, or

$$a^{1/n}a^{1/m} = a^{1/n+1/m}$$

b. If $a \in \mathbb{R}^+$ and $m, n \in \mathbb{N}$, then let $x = (a^{1/n})^{1/m}$. By 1.b. above we have $x^m = a^{1/m}$, and $x^{mn} = a$, so $x = a^{1/mn}$.

c. If $a, b \in \mathbb{R}^+$ and $m \in \mathbb{N}$, then let $x = a^{1/m}b^{1/m}$. Then by 1.a. above we have $x^m = (a^{1/m}b^{1/m})^m = (a^{1/m})^m(b^{1/m})^m = ab$, so $x = (ab)^{1/m}$.

Combining parts **1** and **2** gives the result for $p, q \in \mathbb{R}$. ■

Theorem 5.10 *If there is a real number $x \geq 0$ which satisfies $x < y$ for all $y > 0$, then $x = 0$.*

Proof: If $x > 0$, then $x < x$, which is impossible. ■

Theorem 5.11 (Archimedean Property of $\mathbb{R}$) *For all $x, y \in \mathbb{R}^+$ there is an $n \in \mathbb{N}$ such that $y < nx$.*

Proof: Suppose not, that is suppose for all $n \in \mathbb{N}$ we have $nx \leq y$. Then the subset

$$S = \{nx \mid x \in \mathbb{R}^+ \text{ and } nx \leq y \text{ for all } n \in \mathbb{N}\}$$

of $\mathbb{R}$ is bounded above by y. But then by the order-completeness of $\mathbb{R}$ the number $s = \sup S = \min S^u$ exists in $\mathbb{R}$ and satisfies $s \leq y$. Now, since $x > 0$, we have $-x < 0 = s - s$, or $s - x < s$, and $s - x \notin S^u$, i.e. there exists an $n \in \mathbb{N}$ such that $nx \in S$ and $nx > s - x$. But then $(n+1)x > s$, which means $s \neq \sup S$, a contradiction. ■

Theorem 5.12 (Every Open Interval Contains a Rational Point) *If $a < b$ for some $a, b \in \mathbb{R}$, then there is a $q \in \mathbb{Q}$ such that $a < q < b$.*

Proof: By the Archimedean property of $\mathbb{R}$ there exist numbers $m, n, p \in \mathbb{N}$ such that $n(b-a) > 1$, $m > na$ and $p > -na$. Combining these we get

$$-p < na < m \tag{5.1}$$

We can of course choose $-p$ and m to satisfy $-p = r - 1$ and $m = r$ for some $r \in \mathbb{Z}$, so that

$$r - 1 \leq na < r \tag{5.2}$$

Now, this gives $na \overset{(5.2)}{<} r \overset{(5.2)}{\leq} na + 1 < nb$, or $na < r < nb$, which gives

$$a < \frac{r}{n} < b$$

so let $q = r/n \in \mathbb{Q}$. ■

Corollary 5.13 (Every Open Interval Contains an Irrational Point) *If $a < b$ for some $a, b \in \mathbb{R}$, then there is an $r \in \mathbb{R}\backslash\mathbb{Q}$ such that $a < r < b$.*

Proof: The open interval $(a/\sqrt{2}, b/\sqrt{2})$ contains a rational point q, so

$$\frac{1}{\sqrt{2}}a < q < \frac{1}{\sqrt{2}}b$$

whence $a < q\sqrt{2} < b$, and $q\sqrt{2}$ is irrational. (We could also have proved this directly, as above.) ■

Theorem 5.14 *For every $x \in \mathbb{R}$ there is a unique $n \in \mathbb{Z}$ such that $x - 1 < n \leq x$, called the* **integer part of** *x and denoted $[x]$.*

Proof: By the Archimedean property of $\mathbb{R}$, for any $x \in \mathbb{R}$ we can find $M, N \in \mathbb{N}$ such that $M > x$ and $N > -x$, or

$$-N < x < M \tag{5.3}$$

Now, consider the subset $S = \{n \in \mathbb{N} \mid -N - 1 + n \leq x\}$ of $\mathbb{N}$. By (5.3) we know that $1 \in S$ but $M + N + 1 \notin S$, so S is a nonempty subset of $\mathbb{N}$. By the well-ordering property of $\mathbb{N}$ we know that $\mathbb{N}\backslash S$ has a smallest element $n + 1$. Thus, $n \in S$ but $n + 1 \notin S$, i.e.

$$-N - 1 + n \leq x \qquad\qquad -N + n > x$$

Subtracting 1 from both sides of the second inequality and combining the two we get

$$x - 1 < -N - 1 + n \leq x$$

Since $-N-1+n \in \mathbb{Z}$, we have established the existence part of the statement. As to uniqueness, supose there were two integers $p, q \in \mathbb{Z}$ satisfying $x - 1 < p, q \leq x$. Then, since $|p - q| \in \mathbb{Z}$ and $|p - q| < x - (x - 1) = 1$, we see that $p = q$. ■

Theorem 5.15 *For every real x number there is a sequence of rational numbers converging to x. This sequence* $(q_n)_{n\in\mathbb{N}}$ *in* $\mathbb{Q}$ *can always be given by* $q_n = \frac{[nx]}{n}$.

Proof: By the previous theorem, 5.14, we have for all $n \in \mathbb{N}$ that $nx - 1 < [nx] \leq nx$, so that dividing by n we arrive at

$$x - \frac{1}{n} < \frac{[nx]}{n} \leq x < x + \frac{1}{n}$$

from which we get $-\frac{1}{n} < \frac{[nx]}{n} - x < \frac{1}{n}$, or

$$\left| \frac{[nx]}{n} - x \right| < \frac{1}{n}$$

Letting $\epsilon = \frac{1}{n}$ we see that $\lim_{n\to\infty} \frac{[nx]}{n} = x$. ■

Theorem 5.16 *For every real x number there is a sequence of irrational numbers converging to x. This sequence* $(p_n)_{n\in\mathbb{N}}$ *in* $\mathbb{R}\backslash\mathbb{Q}$ *can always be given by* $q_n = \frac{[nx]+\sqrt{2}}{n}$.

Proof: As in the previous theorem we have

$$x - \frac{1}{n} < \frac{[nx]}{n} \leq x < x + \frac{1}{n}$$

from which we get $x - \frac{1}{n} - \frac{\sqrt{2}}{n} < x - \frac{1}{n} + \frac{\sqrt{2}}{n} < \frac{[nx]}{n} + \frac{\sqrt{2}}{n} \leq x < x + \frac{1}{n} + \frac{\sqrt{2}}{n}$, or

$$x - \frac{1 + \sqrt{2}}{n} < \frac{[nx] + \sqrt{2}}{n} < x + \frac{1 + \sqrt{2}}{n}$$

Subtracting x from all sides then gives $-\frac{1+\sqrt{2}}{n} < \frac{[nx]+\sqrt{2}}{n} - x < \frac{1+\sqrt{2}}{n}$, or

$$\left| \frac{[nx] + \sqrt{2}}{n} - x \right| < \frac{1 + \sqrt{2}}{n}$$

Letting $\epsilon = \frac{1+\sqrt{2}}{n}$ we see that $\lim_{n\to\infty} \frac{[nx]+\sqrt{2}}{n} = x$. Of course $\frac{[nx]+\sqrt{2}}{n}$ is irrational, because $\frac{[nx]}{n}$ is rational and $\sqrt{2}$ is irrational, so $\frac{\sqrt{2}}{n}$ is also irrational, and therefore $\frac{[nx]}{n} + \frac{\sqrt{2}}{n}$ is irrational, else the difference of two rational numbers,

$$\frac{[nx]}{n} + \frac{\sqrt{2}}{n} - \frac{[nx]}{n} = \frac{\sqrt{2}}{n}$$

would be rational. ■