A Construction of the Real Numbers

Mu Alpha Theta

Aditya Pahuja

March 16, 2024

The most rigorous definition of $\mathbb{R}$ that the average high schooler receives is something to the effect of "the set of numbers formed by taking the integers and appending arbitrary sequences of digits after the decimal point" — symbolically, something like the set of all

$$\sum_{k \le n_0} \frac{a_k}{10^k}$$

where $a_{n_0}, a_{n_0-1}, \ldots$ are digits and n_0 is some integer (in other words, the decimal expansion is bounded on the left). While this is a mathematically sound definition of the real numbers, it doesn't give any insight into their structure.

Rather, the "morally correct" way of visualizing $\mathbb{R}$ is by understanding how it builds upon the structure of $\mathbb{Q}$; that is, by filling in "gaps" in $\mathbb{Q}$. For example, consider the sequence of rational numbers

$$a_n = \frac{\lfloor 10^n \sqrt{2} \rfloor}{10^n}$$

obtained by truncating $\sqrt{2}$ after n decimal places. The set $\{a_1, a_2, \ldots\}$ has no maximal element, but even more strongly, it does not have a smallest upper bound in $\mathbb{Q}$, even though it is bounded above (whereas if we had access to $\mathbb{R}$, we could say that it has a **least upper bound** of $\sqrt{2}$). In fact, all the properties that make $\mathbb{R}$ different from $\mathbb{Q}$ can be boiled down to the **least upper bound property**:

> Every subset $S \subset \mathbb{R}$ that is bounded above has a least upper bound; that is, there is a smallest b such that $b \ge s$ for all $s \in S$.

> **Exercise.** Convince yourself (not necessarily rigorously) that, if $\mathbb{R}$ contains $\mathbb{Q}$ and has the least upper bound property, then $\mathbb{R}$ does not have the "gaps" that riddle $\mathbb{Q}$, as well as the converse.

We will then define each element of $\mathbb{R}$ as follows:

> **Definition** (Dedekind's cuts) — A **cut** is defined as a nonempty proper subset $\alpha \subsetneq \mathbb{Q}$ with the following two properties:
>
> (i) If $p \in \alpha$, then every rational number smaller than p is also in α.
>
> (ii) If $p \in \alpha$, then $p < r$ for some $r \in \alpha$; in other words, α doesn't have a maximal element.

The idea is that each of these cuts should correspond directly to a real number, so we will simply take these sets as our elements of $\mathbb{R}$. Visually, they are "half of the number line":

It is a good idea to check that we have an inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$ given by the map $q \mapsto \{x < q : x \in \mathbb{Q}\}$ as you go along with the proof that $\mathbb{R}$ has the properties we want — in other words, check that the set $\overline{q} = \{x < q : x \in \mathbb{Q}\}$ behaves (in $\mathbb{R}$) the same way that q behaves (in $\mathbb{Q}$). This should also give you an even clearer picture of how exactly the cuts behave. Let's now make a wishlist of things that

$\mathbb{R}$ should satisfy; ideally, this list should contain the bare minimum information required to uniquely determine $\mathbb{R}$.

A. In order to have the least upper bound property, we need some notion of order.

B. We need the least upper bound property itself.

C. We should have a definition of adding two real numbers.

D. We should have a definition of multiplying two real numbers.

Property A.

Definition (Ordering of $\mathbb{R}$) — For $\alpha, \beta \in \mathbb{R}$, we say that $\alpha \le \beta$ if and only if $\alpha \subseteq \beta$, with the strict inequality $\alpha < \beta$ meaning $\alpha \subsetneq \beta$. As usual, we can also these as $\beta \ge \alpha$ and $\beta > \alpha$ respectively.

First, let's check that any two cuts are related by $\le$:

Theorem ($\mathbb{R}$ is linearly ordered)**.** For any α and β, either $\alpha \le \beta$ or $\beta \le \alpha$.

Proof. This should feel very obvious with our visualization of cuts. Indeed, if $\alpha \ne \beta$, then there exists a number in exactly one of the two cuts (WLOG $r \in \alpha$), which means r is greater than every element of β due to cut property (i) and thus $\beta \subseteq \alpha$. $\square$

This justifies us putting $\mathbb{R}$ on a line, since any sequence of real numbers can be ordered

$$\cdots \le \alpha_1 \le \alpha_2 \le \alpha_3 \le \alpha_4 \le \cdots .$$

We will later verify that this ordering is compatible with addition and multiplication in the way you would expect.

Property B. This is actually very, very easy with the structure we've built up.

Theorem (Least upper bound property)**.** Let $S \subseteq \mathbb{R}$ be a set that is bounded above (i.e. there exists an Ω that is greater than every element of S) and let S' be the set of all upper bounds of S. Then, S' has a minimum, which is called the **supremum** of S and denoted $\sup(S)$.

Proof. Take the union U of all the elements of S. I claim that this is $\sup(S)$. Indeed, this is clearly a cut and an upper bound of S. Moreover, any upper bound U' of S has each element of S as a subset, so U' has the union of all the elements of S as a subset, i.e. $U \subset U'$, or equivalently $U \le U'$. $\square$

As an exercise, try to extract the symmetric **greatest lower bound property**:

Theorem (Greatest lower bound property)**.** Let $S \subseteq \mathbb{R}$ be a set that is bounded below and let S' be the set of all lower bounds of S. Then, S' has a maximum, which is called the **infimum** of S and denoted $\inf(S)$.

Property C.

Definition (Addition) — Given cuts α and β, their sum is defined as

$$\alpha + \beta = \{p + q : p \in \alpha,\ q \in \beta\}.$$

This definition is fairly straightforward: we get $\alpha + \beta$ by grabbing the sums of every pair of elements in α and β.

We want $\mathbb{R}$ to be an abelian group under addition, which means we want the following properties.

C1. Closure: The sum of cuts is actually a cut.

C2. Commutativity: For all α and β in $\mathbb{R}$, $\alpha + \beta = \beta + \alpha$.

C3. Associativity: For all $\alpha, \beta, \gamma \in \mathbb{R}$, $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

C4. Identity: There is a cut $\overline{0}$ such that for all $\alpha \in \mathbb{R}$, $\alpha + \overline{0} = \overline{0} + \alpha = \alpha$.

C5. Inverse: For each α, there is a cut $-\alpha$ such that $\alpha + (-\alpha) = \overline{0}$.

To verify closure, we need to check that the two cut properties hold.

(i) Suppose $p + q \in \alpha + \beta$ with $p \in \alpha$ and $q \in \beta$, and $r = q + p' < p + q$. Then, $p' < p$ means that $p' \in \alpha$, thus $p' + q \in \alpha + \beta$.

(ii) For any $p + q \in \alpha + \beta$, we can find a larger element in the cut by taking some $p' \in \alpha$ greater than p.

Commutativity and associativity are obvious because addition over $\mathbb{Q}$ has those properties (write it out yourself if you don't believe me).

The identity cut should correspond to 0, so we naturally have

$$\overline{0} = \{x < 0 : x \in \mathbb{Q}\}$$

(this of course agrees with the inclusion of $\mathbb{Q}$ in $\mathbb{R}$ detailed earlier). We then need to check that $\alpha + \overline{0} = \alpha$. Given some $p + x \in \alpha + \overline{0}$ where $p \in \alpha$ and $x \in \overline{0}$, we want $p + x$ to also be in α; this is obvious as $x < 0$ implies $p + x < p$. Conversely, if $p \in \alpha$, then there is a small positive ε such that $p + \varepsilon \in \alpha$, which means $-\varepsilon \in \overline{0}$ and so

$$(p + \varepsilon) + (-\varepsilon) = p \in \alpha + \overline{0}.$$

In other words, $\alpha \subseteq \alpha + \overline{0}$ and $\alpha + \overline{0} \subseteq \alpha$, which implies $\alpha = \alpha + \overline{0}$.

Finally, we need a reasonable definition of $-\alpha$. The idea here is to take a sort of "reverse cut" α^* that contains "almost all of" $\mathbb{Q}\backslash\alpha$, and then negate each element of this reverse cut to get the desired $-\alpha$. The nuance alluded to by "almost" is that we don't want this reverse cut to have a minimum, which would be the case if, for example, $\alpha = \overline{0}$ and we take

$$\alpha^* = \mathbb{Q}\backslash\overline{0} = \{x \geq 0 : x \in \mathbb{Q}\}.$$

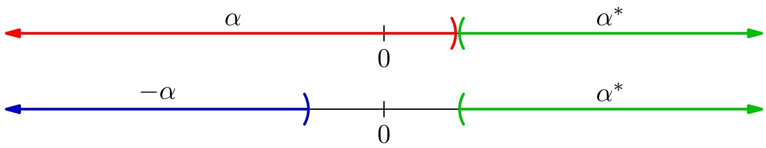
The natural workaround for this is to casework based on whether α has a supremum in $\mathbb{Q}$; in particular, set

$$\alpha^* = \begin{cases} \mathbb{Q}\backslash(\alpha \cup \{q\}) & \alpha = \overline{q} \text{ for some } q \in \mathbb{Q} \\ \mathbb{Q}\backslash\alpha & \text{otherwise} \end{cases}$$

so that we get

$$-\alpha = \{-x : x \in \alpha^*\}.$$

Some more pictures:



Now, we need to check that $\alpha+(-\alpha)$ is exactly the set of negative rational numbers. By construction, we can see $\alpha + (-\alpha)$ only contains negative rationals.

To prove that it contains all the negative rationals, observe that either $-\alpha \geq \overline{0}$ or $\alpha \geq \overline{0}$; suppose WLOG that the latter is true. Then, any negative rational r is contained in α.

Claim — There exists a rational d such that $r + d \in \alpha$ and $-d \in -\alpha$.

Proof. This is equivalent to saying $d + r \in \alpha$ and $d \in \alpha^*$, which, since $d + r < d$, is obvious. □

Picking such a d shows us that any $r < 0$ can be written as $(r + d) + (-d) \in \alpha + (-\alpha)$, which is what we wanted.

Property D. Multiplication can't be defined as directly as addition, since the product of two negative numbers is a positive number.

Definition (Multiplication) — For a positive real number α, define α' as $\alpha \backslash \overline{0}$. Then, if α and β are greater than $\overline{0}$, let $\alpha \cdot \beta$ be the smallest cut containing

$$\{pq : p \in \alpha',\ q \in \beta'\}.$$

We then extend this to negative numbers by

$$\alpha\beta = -(\alpha \cdot (-\beta)) = -((-\alpha) \cdot \beta) = (-\alpha) \cdot (-\beta)$$

The wishlist of properties is

D1. Closure: The product of two cuts is a cut.

D2. Commutativity: Multiplication of cuts is commutative.

D3. Associativity: Multiplication of cuts is associative.

D4. Identity: There exists a cut $\overline{1}$ such that $\alpha \cdot \overline{1} = \overline{1} \cdot \alpha = \alpha$.

D5. Inverse: For each α, there is a cut α^{-1} for which $\alpha \cdot \alpha^{-1} = \overline{1}$.

D6. Distributiveness: Multiplication distributes over addition, meaning for any cuts α, β, γ, we have
$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma.$$

Properties D1, D2, D3, and D6 are easy enough to check manually. D4 is also fairly simple, as we are porting the identity from $\mathbb{Q}$ again.

Multiplicative inverses are the same idea, too. We define them for positive α: take

$$(\alpha^{-1})' = \left\{ \frac{1}{p} : p \in \alpha^* \right\}$$

and extend to a cut α^{-1}. We can easily check that this is indeed the multiplicative inverse of α, and inverses of negative numbers follow.

Compatibility with order Finally, we need to check the following statements:

$$\alpha < \beta \implies \alpha + \gamma < \beta + \gamma$$
$$\alpha > \overline{0},\ \beta > \overline{0} \implies \alpha\beta > \overline{0}$$

The first one is fairly simple: since α is a subset of β, the set

$$\alpha + \gamma = \{p + q : p \in \alpha,\ q \in \beta\}$$

must be a subset of

$$\beta + \gamma = \{p + q : p \in \beta,\ q \in \gamma\}.$$

The second statement is obvious, since $\alpha\beta$ is forced to have some nonnegative elements if α and β have nonnegative elements.

Exercise. Strengthen the second inequality to

$$\alpha \geq \overline{0},\ \beta \geq \overline{0} \implies \alpha\beta \geq \overline{0}.$$

Exercise. Show that the two inequalities we proved are sufficient to give us the order structure that we expect in $\mathbb{R}$. Namely, prove the following statements:

(i) If $x > 0$, then $-x < 0$ (and vice versa).

(ii) If $x > 0$ and $y < z$, then $xy < xz$.

(iii) If $x < 0$ and $y < z$, then $xy > xz$.

(iv) For all x, $x^2 \geq 0$, with equality if and only if $x = 0$.

(v) If $0 < x < y$, then $0 < \frac{1}{y} < \frac{1}{x}$.