Constructing $\mathbb{R}$ from $\mathbb{Q}$

Tyler Jensen, Zikra Hashmi, Logan Barnhart

May 2022

1 Introduction

Theorem 1 (The existence of $\mathbb{R}$)**.** *There exists an ordered field in which every nonempty set that is bounded above has a least upper bound. In addition, this field contains $\mathbb{Q}$ as a subfield [1].*

What does the above theorem really say? Essentially, it says that $\mathbb{R}$ exists and behaves exactly how we think it does. The past year, we've been working with a number system whose existence we've assumed since day one, so our goal is to finally prove the above theorem and that all the work we've done in $\mathbb{R}$ has been valid! Do the countless (well, countable) sequences and series we proved converge even converge to existing values? Are we even allowed to say "Let epsilon greater than zero be fixed but arbitrary"?! Well, the answer is obviously yes, but lets make sure. For reference, we follow *Abbott* 8.6.

2 Dedekind Cuts

First, let's design some machinery to help us navigate the "real numbers." Dedekind cuts were created by German Mathematician, Richard Dedekind, whose proof will allow us to verify the existence of $\mathbb{R}$ with it's familiar properties. Its important to note that we only know about the existence of $\mathbb{Q}$. The concept we know as $\mathbb{R}$, is not defined currently.

Definition 1 (Dedekind Cut)**.** A subset A of $\mathbb{Q}$ is called a (Dedekind) *cut* if it possesses the following three properties:

(c1) $A \neq \emptyset$ and $A \neq \mathbb{Q}$.

(c2) If $r \in A$, then A also contains every rational $q < r$.

(c3) A does not have a maximum; that is, if $r \in A$, then there exists $s \in A$ with $r < s$ [1].

Exercise 1. (a) Fix $r \in \mathbb{Q}$. Show that the set $C_r = \{t \in \mathbb{Q} : t < r\}$ is a cut.

Which of the following subsets of $\mathbb{Q}$ are cuts?

(b) $S = \{t \in \mathbb{Q} : t \leq 2\}$

(c) $T = \{t \in \mathbb{Q} : t^2 < 2 \text{ or } t < 0\}$

(d) $U = \{t \in \mathbb{Q} : t^2 \leq 2 \text{ or } t < 0\}$

Proof.

(a) (c1) $C_r \neq \emptyset$ since $r - 1 \in C_r$. Also $C_r \neq \mathbb{Q}$ since $r \in \mathbb{Q}$ but $r \notin C_r$.

(c2) Fix an $s \in C_r$. So $s < r$ by definition. Given any rational, $p < s$, it follows that $p < r$, thus $p \in C_r$.

(c3) Proof by contradiction: Suppose that C_r has a maximum element, say M. Well, necessarily $M < r$ is true. But note that $M < \frac{M+r}{2} < r$ and $\frac{M+r}{2} \in \mathbb{Q}$, thus $\frac{M+r}{2} \in C_r$ with $M < \frac{M+r}{2}$ which is a contradiction. Thus C_r does not have a maximum element.

So C_r is a cut.

(b) Note that certainly, $2 \in S$. But also note that for any $p \in \mathbb{Q}$ with $p > 2$, $p \notin S$ so there is no element larger than 2 in S. This contradicts (c3), and therefore S is not a cut.

(c) The set T is a cut.

(c1) Certainly $T \neq \emptyset$ since $1^2 = 1 < 2$ means $1 \in T$. Also, $T \neq \mathbb{Q}$ since $2^2 = 4 > 2$, so $2 \notin T$.

(c2) Fix an element $s \in T$. If $s \leq 0$ then certainly for all rationals $p < s$, $p \in T$ by design. So what if $s > 0$? For an arbitrary rational $0 < p < s$, $p < s$ means $p^2 < s^2 < 2$, so certainly, $p \in T$. Since p was arbitrary, it's true for any rational $p < s$.

(c3) Proof by contradiction: Assume T has a maximum element, say M. Set $q = M - \frac{M^2-2}{M+2}$ Since $M^2 < 2$, it follows that $M^2 - 2 < 0$, so $q > M$. Also note that

$$\begin{aligned}
q^2 &= (M - \frac{M^2-2}{M+2})^2 \\
&= (\frac{2M+2}{M+2})^2 \\
&= \frac{4M^2+8M+4}{M^2+4M+4} \\
&= \frac{2M^2-4}{M^2+4M+4} + \frac{2M^2+8M+8}{M^2+4M+4} \\
&= \frac{2(M^2-2)}{M^2+4M+4} + 2 \\
&< 0 + 2 \\
q^2 &< 2.
\end{aligned}$$

as $M^2 - 2 < 0$. Thus, $q \in T$ while $q > M$ which is a contradiction, so T cannot have a maximum element.

(d) The set U is a cut since $U = T$:
Fix an element, $u \in U$. So $u^2 \leq 2$. But $u^2 \neq 2$, otherwise $u \notin \mathbb{Q}$ (We proved that $\sqrt{2} \notin \mathbb{Q}$ last semester, we don't even need to say that it's irrational since we don't know what those are yet, but we do know it is not in $\mathbb{Q}$). Then it must be true that $u^2 < 2$. Thus $u \in T$. Now fix an element $t \in T$. We know $t^2 < 2$, so certainly $t^2 \leq 2$, so $t \in U$. Since u and t were arbitrary, we know that $U \subseteq T$ and $T \subseteq U$, so $U = T$

□

Exercise 2. Let A be a cut. Show that if $r \in A$ and $s \notin A$, then $r < s$.

Proof. Proof by contradiction: Suppose that $r \geq s$, $r \in A$, and $s \notin A$. But $s \leq r$ implies, by property (c2) of cuts, that $s \in A$. This is a contradiction, and thus $r < s$. □

Definition 2 ($\mathbb{R}$)**.** Define the *real numbers* $\mathbb{R}$ to be the set of all cuts in $\mathbb{Q}$ [1].

Now we have our hands on something that resembles a real number! As you could see in the first example, we have a cut that sets us up to conceive and begin to work with real numbers like $\sqrt{2}$. We want to verify that these real numbers act like the real numbers we are used to. That is, we need to prove that we can work with the real numbers like how we already "know" to work with them.

3 Field and Order Properties

$\mathbb{R}$ has some nice properties. One of those is that $\mathbb{R}$ is an ordered field. This section defines what an ordered field is.

Definition 3 (Operation)**.** Given a set F and two elements $x, y \in F$, an *operation* on F is a function that takes the ordered pair (x, y) to a third element $z \in F$ [1].

Definition 4 (Field)**.** A set F is a *field* if there exists two operations, addition $(x + y)$ and multiplication (xy), that satisfy the following list of conditions:

(f1) (commutativity) $x + y = y + x$ and $xy = yx$ for all $x, y \in F$.

(f2) (associativity) $(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$ for all $x, y, z \in F$.

(f3) (identity) There exist two special elements 0 and 1 with $0 \neq 1$ such that $x + 0 = x$, and $(x)(1) = x$ for all $x \in F$.

(f4) (inverse) Given $x \in F$, there exists an element $-x \in F$ such that $x + (-x) = 0$. If $x \neq 0$, there exists an element x^{-1} such that $(x)(x^{-1}) = 1$.

(f5) (distributive property) $x(y + z) = xy + yz$ for all $x, y, z \in F$ [1].

What field conditions do the sets we know have?

$\mathbb{N}$ has properties (f1), (f2), and (f5). It doesn't have (f3) because $0 \notin \mathbb{N}$ and it doesn't have (f4) because $n > 0$ $\forall n \in \mathbb{N}$.

$\mathbb{Z}$ has properties (f1), (f2), (f3), and (f5), but not (f4) because for $z \in \mathbb{Z}$, $\frac{1}{z} \notin \mathbb{Z}$ (except for $z = 1, -1$), so it doesn't have a multiplicative inverse.

$\mathbb{Q}$ has all 5 properties.

Definition 5 (Ordering)**.** An *ordering* on a set F is a relation, represented by $\leq$, with the following three properties:

(o1) For arbitrary $x, y \in F$, at least one of the statements $x \leq y$ or $y \leq x$ is true.

(o2) If $x \leq y$ and $y \leq x$, then $x = y$.

(o3) If $x \leq y$ and $y \leq z$, then $x \leq z$ [1].

Definition 6 (Ordered Field)**.** A field F is called an *ordered field* if F possesses an ordering $\leq$ that satisfies

(o4) If $y \leq z$, then $x + y \leq x + z$.

(o5) If $x \geq 0$ and $y \geq 0$, then $(x)(y) \geq 0$ [1].

Definition 7 (Ordering of $\mathbb{R}$)**.** Let A and B be two arbitrary elements of $\mathbb{R}$. Define $A \leq B$ to mean $A \subseteq B$ [1].

Exercise 3. Show that this defines an ordering on $\mathbb{R}$ by verifying properties (o1), (o2), and (o3).

Proof. Let A,B, and C be arbitrary elements of $\mathbb{R}$. That is, A, B and C are cuts. Now we verify properties (o1), (o2), and (o3).

(o1) Proof by contradiction: Assume that neither of $A \leq B$ or $B \leq A$ is true. This means that $A \nsubseteq B$ and $B \nsubseteq A$. Thus there is some $a_0 \in A$ such that $a_0 \notin B$ and there is some $b_0 \in B$ such that $b_0 \notin A$. However, as A and B are both cuts, exercise 2 applies. Thus, $a_0 \notin B$ implies that $a_0 > b$, where b is any element of B. Similarly, $b_0 \notin A$ implies that $b_0 > a$, where a is any element of A. As a_0 is an element of A, and b_0 is an element of B, this means that $a_0 > b_0$ and $b_0 > a_0$. This is a contradiction, and thus we have proved (o1).

(o2) If $A \leq B$ and $B \leq A$, this means that $A \subseteq B$ and $B \subseteq A$, which by the definition of set equality means that $A = B$.

(o3) If $A \leq B$ and $B \leq C$, then $A \subseteq B$, $B \subseteq C$, which means that $A \subseteq C$, that is $A \leq C$.

□

The above successfully proves that we have an ordering on $\mathbb{R}$, but it's not quite an ordered field yet. We first need to define some mathematical operations on $\mathbb{R}$.

4 Algebra in $\mathbb{R}$

We defined what an ordered field is, and showed that $\mathbb{R}$ has an ordering. But we need to define addition and multiplication in $\mathbb{R}$ and then show that these operations satisfy all the field and ordered field axioms, which will show that $\mathbb{R}$ is an ordered field.

Definition 8 (Addition in $\mathbb{R}$)**.** Given A and B in $\mathbb{R}$, define $A + B = \{a + b : a \in A \text{ and } b \in B\}$ [1].

Exercise 4. (a) Show that (c1) and (c3) also hold for $A + B$. Conclude that $A + B$ is a cut ((c2) was proved by Abbott and we will include the proof below).

(b) Check that addition in $\mathbb{R}$ is commutative (f1) and associative (f2).

(c) Show that property (o4) holds.

(d) Show that the cut

$$O = \{p \in \mathbb{Q} : p < 0\}$$

successfully plays the role of the additive identity (f3). (Showing $A + O = A$ amounts to proving that these two sets are the same. The standard way to prove such a thing is to show two inclusions: $A + O \subseteq A$ and $A \subseteq A + O$.)

Proof. For the following problems, fix three real numbers (cuts), A, B, and C:

(a) (c1) Certainly $A + B \neq \emptyset$ since $A \neq \emptyset$ and $B \neq \emptyset$ there exists an $a_0 \in A$, $b_0 \in B$ so $a_0 + b_0 \in \mathbb{Q}$, thus $a_0 + b_0 \in A + B$. Also, $A + B \neq \mathbb{Q}$ as we know there exists $s, t \in \mathbb{Q}$ where $s \notin A$, so $a < s$ for all $a \in A$ and $t \notin B$, so $b < t$ for all $b \in B$. So for any $a \in A$, $b \in B$, $a + b < s + t$ which means $a + b \neq s + t$ for any a, b, and thus $s + t \notin A + B$, so $A + B \neq \mathbb{Q}$.

(c2) Let $a + b \in A + B$ be arbitrary and let $s \in \mathbb{Q}$ satisfy $s < a + b$. Then, $s - b < a$, which implies that $s - b \in A$. But then $s = (s - b) + b \in A + B$ (as $s - b \in A$ and $b \in B$).

(c3) Proof by contradiction: Assume $A + B$ has a maximum element, say $a_0 + b_0$ where $a_0 \in A$ and $b_0 \in B$. But A and B are cuts, so they do not have maximum elements. In other words, there exists an $a_1 \in A$ where $a_0 < a_1$ and there exists a $b_1 \in B$ where $b_0 < b_1$. So then it must be true that $a_0 + b_0 < a_1 + b_1$ and since $a_1 \in A$, and $b_1 \in B$, it's true that $a_1 + b_1 \in A + B$, which is a contradiction. So $A + B$ cannot have a maximum.
Thus, $A + B$ is a cut!

(b) (f1) Note that by definition, $A + B = \{a + b : a \in A \text{ and } b \in B\}$. Likewise, $B + A = \{b + a : b \in B \text{ and } a \in A\}$. Fix an arbitrary element of $A + B$, say c, so for some $a_0 \in A, b_0 \in B$, such that $c = a_0 + b_0$ by definition. But by the commutativity of rational numbers, $b_0 + a_0 = c$ as well, which means that $c \in B + A$. Now, fix an element of $B + A$, say d. Similar to before there exists $b_1 \in B, a_1 \in A$, where $d = b_1 + a_1$, and again by the commutativity of the rationals, $a_1 + b_1 = d$ meaning $d \in A + B$. Since c and d were arbitrary, we proved that $A + B \subseteq B + A$ and $B + A \subseteq A + B$, so $A + B = B + A$.

(f2) Note that $(A + B) + C = \{(a + b) + c : a + b \in A + B, c \in C\}$ (which means $a \in A, b \in B$ from cut addition) and $A + (B + C) = \{a + (b + c) : a \in A, b + c \in B + C\}$. Fix an element of $(A + B) + C$, say d. So for some $a_0 + b_0 \in A + B$ (Which then means $a_0 \in A, b_0 \in B$) and some $c_0 \in C$ it's true that $d = (a_0 + b_0) + c_0$. From the associativity of the rationals however, it's also true that $a_0 + (b_0 + c_0) = d$, but since $a_0 \in A$ and $b_0 + c_0 \in B + C$, then it must be true that $d \in A + (B + C)$, and since d was arbitrary, $(A + B) + C \subseteq A + (B + C)$. Next fix an element of $A + (B + C)$, call it e. We know that there is some $a_1 \in A$ and $b_1 + c_1 \in B + C$ (again, this means $b_1 \in B$ and $c_1 \in C$) where $e = a_1 + (b_1 + c_1)$. Once again, because of the associativity of rationals it's then true that $(a_1 + b_1) + c_1$. But $(a_1 + b_1) \in A + B$ and $c_1 \in C$, so it must be true that $e \in (A + B) + C$. Since e was arbitrary we now know that $A + (B + C) \subseteq (A + B) + C$. Thus $(A + B) + C = A + (B + C)$.

(c) (o4) Assume that $A \leq B$. So $A \subseteq B$. If $A = B$ then certainly $A + C \leq B + C$ because $A + C = B + C$, so let's say $A \subset B$. Then by definition there is a $b_0 \in B$ where $b_0 \notin A$, or from exercise 2, $a < b_0$ for all $a \in A$. So for any $c \in C$, $a + c < b_0 + c$, so it follows that $a + c \neq b_0 + c$ for any $a \in A$, which can only mean that $b_0 + c \notin A + C$, thus $A + C \subset B + C$. So, in either case $A + C \leq B + C$.

(d) Let $a \in A$ be fixed but arbitrary. Since A is a cut, there exists an $a_0 \in A$ where $a < a_0$. So $a_0 = a + r$ where $r \in \mathbb{Q}, r > 0$. So $a_0 - r = a$. But $-r < 0$, so $-r \in O$. Thus $a_o + (-r) = a \in A + O$. So $A \subseteq A + O$. Now, let $o \in A + O$ be fixed but arbitrary. Using Definition 8, we can define $o = a + s$, where $a \in A$ and $s \in O$. Note that $s < 0$. So $o = a + s < a$. Since A is a cut, A contains every rational less than a, so $o \in A$. So $A + O \subseteq A$. Therefore, $A + O = A$.

□

Definition 9 (Additive Inverse)**.** Given $A \in R$, define $-A = \{r \in \mathbb{Q} : \text{ there exists } t \notin A \text{ with } t < -r\}$ [1].

Exercise 5. (a) Prove that $-A$ defines a cut.

(b) What goes wrong if we set $-A = \{r \in \mathbb{Q} : -r \notin A\}$?

(c) If $a \in A$ and $r \in -A$, show $a + r \in O$. This shows $A + (-A) \subseteq O$. Now, finish the proof of property (f4) for addition in Definition 4.

Proof. Fix an $A \in \mathbb{R}$

(a) (c1) A is a cut so we know that a $t \in \mathbb{Q}$ with $t > 0$ where $t \notin A$ exists. So $t < t+1$ which means that $-(t+1) \in -A$, so $-A \neq \emptyset$. To show that $-A \neq \mathbb{Q}$ we consider two cases.
Case 1) $A \geq O$ There exists a $q_0 \in \mathbb{Q}$ where $q_0 \notin A$ and $q_0 > 0$. Note that $-q_0 < 0$ so it's necessary that $-q_0 \in A$. But if $-q_0 \in A$, then $-q_0 < t$ for any $t \notin A$ since $t > a$ for every $a \in A$ which we proved in exercise 2. Since $-q < t$ for any $t \notin A$, $-q$ cannot be in $-A$.
Case 2) $A \leq O$. There exists an $a_0 \in A$. Note that $-(-a_0) = a_0$. Then $-(-a_0) < t$ for the same reason as above. Thus $-a_0 \notin -A$.

(c2) Given any $r \in -A$ we know that for some $t \in \mathbb{Q}, t < -r$. So, for any rational, $p < r$, we know that $-p > -r$ so it must be true for that same t that $t < -p$. Thus $p \in -A$. Since p was arbitrary, it's true that any rational less than r is in $-A$.

(c3) Proof by contradiction: Assume that $-A$ has a maximum, say r_0. So for some $t \in \mathbb{Q}, t \notin A$, it's true that $t < -r_0$. But also note that $t < \frac{t-r_0}{2} < -r_0$ so $-\frac{t-r_0}{2} \in -A$. But if $t < \frac{t-r_0}{2} < -r_0$, then $r_0 < -\frac{t-r_0}{2} < -t$ which is a contradiction. So $-A$ does not have a maximum element.

(b) Take the cut $A = \{r \in \mathbb{Q} : r < 2\}$. If we define $-A = \{r \in Q : -r \notin A\}$ then we would have $-2 \in -A$ along with every rational less than -2, but then $-A$ would have a maximum and fail to be a cut.

(c) Fix an $a_0 \in A$ and an $r_0 \in -A$. So for every $a \in A$, it's true that $a < -r_0$, including $a_0 < -r_0$. So it follows that $a_0 + r_0 < 0$ which means that $a_0 + r_0 \in O$. Since a_0 and r_0 were arbitrary, we can see that $A + (-A) \subseteq O$. To next prove that $O \subseteq A + (-A)$ we will first need a small piece of machinery.

Lemma 1 (The Archimedean property of $\mathbb{Q}$). *: For any $x, y \in \mathbb{Q}$ with $x > 0$, there is an $N \in \mathbb{N}$ such that $Nx > y$.*

Proof. if $y < 0$ then $N = 1$ works since $x > 0$. If $y > 0$ however, note that we can write $x = \frac{n}{m}$, and $y = \frac{u}{v}$ where $n, m, u, v \in \mathbb{N}$ since $x, y > 0$. So note that $y = \frac{u}{v} < u$ since $v \geq 1$. So if we let $N = \frac{m(v+1)}{n}$ then

$$\begin{aligned} Nx &= \frac{m(v+1)}{n} \cdot \frac{n}{m} \\ &= v + 1 \\ &> v \\ &\geq y \end{aligned}$$

So $Nx > y$ Since x and y were arbitrary, this is true for any $x, y \in \mathbb{Q}$ with $x > 0$. □

Back to the problem: fFix an $o \in O$. Let's set $q = \frac{|o|}{2}$, but since $o < 0$, $q = \frac{-o}{2}$. Note that there is an $N \in \mathbb{Z}$ where $Nq \in A$ while $(N+1)q \notin A$. If this were not true, then either A would be empty if $Nq \notin A$ or it would be the entire set of rational numbers if $(N+1)q \in A$ for all $N \in \mathbb{Z}$ both by the Archimedian property of $\mathbb{Q}$. So, if we let $r = -(N+2)q$ we can see that $r \in -A$ since $-r > (N+1)Q \notin A$. So,

$$\begin{aligned} Nq + r &= Nq + -(N+2)q \\ &= Nq - Nq - 2q \\ &= -2 \cdot \frac{-o}{2} \\ &= o \end{aligned}$$

So it must be true that $o \in A + (-A)$ since $Nq \in A$ and $-(N+2)q \in -A$. Since o is arbitrary, $O \subseteq A + (-A)$. Now we have proven that $A + (-A) \subseteq O$ and $O \subseteq A + (-A)$, thus $A + (-A) = O$.

□

Definition 10 (Multiplication in $\mathbb{R}$)**.** Given $A \geq O$ and $B \geq O$ in $\mathbb{R}$, define the product [1]

$$AB = \{ab : a \in A, b \in B \text{ with } a, b \geq 0\} \cup \{q \in \mathbb{Q} : q < 0\}$$

Exercise 6. (a) Show that AB is a cut and that property (o5) holds.

(b) Propose a good candidate for the multiplicative identity (f3) on $\mathbb{R}$ and show that this works for all cuts $A \geq O$.

(c) Show the distributive property (f5) holds for non-negative cuts.

Proof.

(a) Let $A, B \in \mathbb{R}$, $A \geq O, B \geq O$ be arbitrary:

(c1) AB is non empty as AB contains -1 by definition, thus $AB \neq \emptyset$. A and B are non negative cuts thus there is a rational number $q \notin A$, $q \geq 0$ and a rational number $r \notin B$, $r \geq 0$. By exercise 2, we know that for every a in A, $a < q$. Likewise, for every b in B, $b < r$. Thus for any $t \in AB$, we consider two cases, $t < 0$, in which case $t < qr$ is clear. Or the case in which $t \geq 0$, then we can write $t = ab$ for any $a \in A, b \in B, a \geq 0, b \geq 0$. Thus $t = ab < qr$. So $t \neq qr$ for any $t \in AB$ which can only mean $qr \notin AB$. Thus $AB \neq \mathbb{Q}$.

(c2) Let $t \in AB$. Then let $r \in \mathbb{Q}$ satisfy $r < t$. There are two cases: $t < 0$ and $t \geq 0$. If $t < 0$, then $r \in AB$ as AB contains all negative rationals. If $t \geq 0$, we can write $t = ab$, where $a \in A, b \in B$ and $a \geq 0, b \geq 0$. As $r < ab$ this implies that $\frac{r}{b} < a$, which means that $\frac{r}{b} \in A$. Thus in the case that $r \geq 0$, $r = \frac{r}{b} \cdot b \in AB$, as r consists of an element in A, $\frac{r}{b}$, and an element in B, b. In the case that $r < 0$, then $r \in AB$ by definition.

(c3) Proof by contradiction: Assume AB has a maximum element, say M. As $M \in AB$, $M = a_0 b_0$, where $a_0 \in A$, $b_0 \in B$. Then as A and B are cuts there exists an $a_1 > a_0$ and a $b_1 > b_0$. Then $N = a_1 b_1 \in AB$, and $N > M$, which is a contradiction and thus AB has no maximum.

(b) We propose $I = \{r \in \mathbb{Q} : r < 1\}$. To show that $AI = I$, we need to show that $AI \subseteq A$ and $A \subseteq AI$. We begin by showing that $AI \subseteq A$. Fix a $t \in AI$. There are two cases, $t < 0$, and $t \geq 0$. We begin with $t < 0$. Then, as $A \geq 0$, $t \in A$. Now for $t \geq 0$, we can write $t = ai$, where $a \in A, i \in I, a \geq 0, i \geq 0$. We know that for any $i \in I$, $i < 1$, which implies $ai < a$, and thus $t = ai \in A$. Thus $AI \subseteq A$. Now for $A \subseteq AI$, fix an $a_0 \in A$. There are two cases $a_0 < 0$ or $a_0 \geq 0$. For $a_0 < 0$, $a_0 \in AI$ as AI contains all negative rationals. For $a_0 \geq 0$, there exists an $a_1 > a_0$ as A is a cut. Then $\frac{a_0}{a_1} < 1$, which means that $\frac{a_0}{a_1} \in I$. Thus $a_0 = a_1 \frac{a_0}{a_1} \in AI$.

(c) Let A, B, C be arbitrary real numbers. We begin by showing that $A(B+C) \subseteq AB + AC$. Remember, $A(B+C) = \{a(b+c) : a \in A, b+c \in B+C \text{ with } a, b+c \geq 0\} \cup \{q \in \mathbb{Q} : q < 0\}$ and $AB + AC = \{t + s : t \in AB, s \in AC\}$. Now fix a $d \in A(B+C)$. There are two cases, $d \geq 0$ or $d < 0$. We begin with $d \geq 0$. We can write $d = a_0(b_0 + c_0)$ where $a_0 \in A, b_0 + c_0 \in B + C$ and $a_0 \geq 0, b_0 + c_0 \geq 0$. Then we can write $d = a_0(b_0 + c_0) = a_0 b_0 + a_0 c_0$ by the distributive property of the rationals. Now there are two cases, $b_0 \geq 0, c_0 \geq 0$ or only one of b_0 and c_0 is greater than or equal to 0. We begin with $b_0 \geq 0, c_0 \geq 0$. Then, $a_0 b_0 \in AB$ and $a_0 c_0 \in AC$ (as all are positive) which implies that $d = a_0 c_0 + a_0 c_0 \in AB + BC$. Now for when only one of b_0 or c_0 is greater than or equal to zero. Without loss of generality assume $b_0 < 0$. Then $a_0 b_0 < 0$ and is thus in AB (as AB includes all negative rationals) and $a_0 c_0$ is in AC. Thus $d = a_0 b_0 + a_0 c_0 \in AB + AC$. Now we consider $d < 0$, then as $AB = \{ab : a \in A \text{ and } b \in B \text{ with } a, b \geq 0\} \cup \{q \in \mathbb{Q} : q < 0\}$ and as $AC = \{ac : a \in A \text{ and } c \in C \text{ with } a, c \geq 0\} \cup \{q \in \mathbb{Q} : q < 0\}$, $\frac{d}{2}$ is in both AB and AC as both AB and AC contain all negative rational numbers. Thus, $\frac{d}{2} + \frac{d}{2} = d \in AB + AC$.

We now show that $AB + AC \subseteq A(B+C)$. Now fix an $e \in AB + AC$. There are two cases, $e \geq 0$, or $e < 0$. We begin with $e \geq 0$. Then we can write $e = t + s$, where $t \in AB$ and $s \in AC$. Then either both of $t, s \geq 0$ or only one of t or s is greater than 0. In the case that both $t, s \geq 0$, by the definition of set multiplication, we can write $e = a_1 b_1 + a_1 c_1$, where $a_1 \in A, b_1 \in B, c_1 \in C$ with $a_1, b_1, c_1 \geq 0$. By the distributive property of the rationals, $e = a_1 b_1 + a_1 c_1 = a_1(b_1 + c_1)$. Thus $a_1 \in A$, and $b_1 + c_1 \in B + C$ (as $b_1 + c_1 \geq 0$), which implies that $e = a_1 b_1 + a_1 c_1 = a_1(b_1 + c_1) \in A(B+C)$. Next we consider the case that one of t or s is negative. Without loss of generality, assume that $s < 0$. Then, $t > 0$ (as if $t = 0$, e would be negative) implies that $t = a_2 b_2$ where $a_2 \in A, b_2 \in B, a_2 > 0, b_2 > 0$. This means that $e < a_2 b_2$, or we can write $e = a_2 b_2 + u$, where $u < 0$. We can then write $e = a_2(b_2 + \frac{u}{a_2})$, $\frac{u}{a_2} < 0$ and is thus in C, thus $a_2 \in A$, $b_2 + \frac{u}{a_2} \in B + C$ and thus $e = a_2(b_2 + \frac{u}{a_2}) \in A(B+C)$. In the case that $e < 0$, then $e \in A(B+C)$ as $A(B+C)$ contains all the negative rationals. Thus $A(B+C) = AB + AC$.

□

Definition 11 (Multiplicative Inverse)**.** For $A \in R, A \geq O$, we define [2]

$$A^{-1} = \{r \in \mathbb{Q} : 0 \ < r < t, \text{ for some } t \in \mathbb{Q} : \tfrac{1}{t} \notin A\} \cup O \cup \{0\}$$

Exercise 7. (a) Is this multiplicative inverse a cut?

(b) Does it work? That is, is $AA^{-1} = I$ where $I = \{t \in \mathbb{Q} : t < 1\}$?

Proof.

(a) (c1) Note that $-1 \in A^{-1}$, so the set is not empty. But also, $A^{-1} \neq \mathbb{Q}$ since we know $A \geq O$, if $A = O$ then it has no elements $a \geq 0$ so $A^{-1} = O$, and certainly $O \neq \mathbb{Q}$. So, let's assume $A > O$. Let's fix an $a_0 \in A, a_0 > 0$. If $\frac{1}{a_0} \in A^{-1}$ then for some $t \in \mathbb{Q}$ with $\frac{1}{t} \notin A$ it would be true that $\frac{1}{a_0} < t$. But that would also mean that $a_0 > \frac{1}{t}$, which would mean that $\frac{1}{t} \in A$ which cannot be true. So $\frac{1}{a_0} \notin A^{-1}$ and $A^{-1} \neq \mathbb{Q}$

(c2) Fix a $p \in A^{-1}$. Then let s satisfy $s < p$. If $p < 0$, then $s < 0$ and is in A^{-1} as $O \subseteq A^{-1}$. If $p \geq 0$, there are three cases $s < 0$, $s = 0$, and $s > 0$. If $s < 0$, then $s \in A^{-1}$ by the same argument as above. Ff $s = 0$, then $s \in A^{-1}$ by definition. If $s > 0$, we know that for $p > 0$, there exists a $t \in \mathbb{Q}$ such that $p < t$ and $\frac{1}{t} \notin A$. However, $0 < s < p < t$, and thus $s \in A^{-1}$.

(c3) Proof by contradiction: Suppose A^{-1} had a maximum element, say M. So for some $t \in \mathbb{Q}, \frac{1}{t} \notin A$, that $0 \leq M < t$. But then $M < \frac{M+t}{2} < t$ and $\frac{M+t}{2} \in \mathbb{Q}$, so $\frac{M+t}{2} \in A^{-1}$ which is a contradiction, so the set does not have a maximum element.

Thus, A^{-1} is a cut.

(b) Fix an arbitrary $A \in \mathbb{R}$. we want to show, is $AA^{-1} = I$.

(i) First, let's prove that $AA^{-1} \subseteq I$. Let's fix an $x \in AA^{-1}$. If $x \leq 0$, then certainly $x \in I$ since $x \leq 0 < 1$. If $x > 0$ then for some $a \in A, b \in A^{-1}, a, b > 0$ we can write $x = ab$. But for some $t \in \mathbb{Q}, \frac{1}{t} \notin A$, which means that $\frac{1}{t} > a$ from exercise 2, or $t < \frac{1}{a}$. But also, since $b \in A^{-1}$ so it must be true that $b < t$ So $x = ab < at < a \cdot \frac{1}{a} = 1$. So definitely $x < 1$ and $x \in I$. Since x was arbitrary, $AA^{-1} \subseteq I$.

Next we will prove that $I \subseteq AA^{-1}$. So fix an element $i \in I$. We know that surely $i < 1$. If $i < 0$ then it is most definitely in AA^{-1}, so assume $0 \leq i < 1$, but if $i = 0$, since $0 \in A^{-1}$, fix an $a \in A$, and note that $0 \cdot a = 0 = i \in AA^{-1}$. So, assuming $0 < i < 1$, we know that there must be an $N \in \mathbb{N}$ where $i^N \in A$ but $i^{N-1} \notin A$ since if it were not true then either $A = \emptyset$ or $A = \mathbb{Q}$. Also, without loss of generality, assume $A \subseteq I \subseteq A^{-1}$ since we know some ordering must occur by the order properties of $\mathbb{R}$. So, we know that since $0 < i < 1$, it's true that $i^N < i < i^{N-1}$. Since $i^N \in A$, we know there exists a number between i^N and i which is also in A. Let's write this number as $i(i^{N-1} + \epsilon)$. For this number to be in A, we need $i(i^{N-1} + \epsilon) < b \leq 1$ since $A \subseteq I$. Solving for ϵ we find that $\epsilon < \frac{b - i^N}{i}$ which is a positive quantity since $b > i^n$ necessarily. Since $i < 1$, such an ϵ that satisfies the property would be $\epsilon = b - i^N$. Now that we have an epsilon, note that $i^{N-1} + \epsilon > i^{N-1}$, so $\frac{1}{i^{N-1}+\epsilon} < \frac{1}{i^{N-1}}$, and $\frac{1}{i^{N-1}+\epsilon} \in A^{-1}$. Similarly, We constructed ϵ so that specifically $i(i^{N-1} + \epsilon) \in A$. So, we can see that $i(i^{N-1} + \epsilon) \cdot \frac{1}{i^{N-1}+\epsilon} = i$ which must mean that $i \in AA^{-1}$. Thus $I \subseteq AA^{-1}$. and finally $AA^{-1} = I$.

□

So far we have only mentioned multiplication between non negative real numbers. What about the case for negative real numbers?

Definition 12. For any $A, B \in \mathbb{R}$, define [1] $AB = \begin{cases} \text{as given} & \text{if } A \geq O \text{ and } B \geq O \\ -[A(-B)] & \text{if } A \geq O \text{ and } B < O \\ -[(-A)B] & \text{if } A < 0 \text{ and } B \geq O \\ -(A)(-B) & \text{if } A < O \text{ and } B < O \end{cases}$

The proofs of these cases are largely uneventful and can be verified on one's own.

And with that we have proven that $\mathbb{R}$ is not only a field by showing it's commutative, associative, it has the 0 and 1 identity elements, along with inverse functions and the distributive property, but we have also shown it's an ordered field by proving all of the ordering axioms.

5 Least Upper Bounds

Definition 13 (Least Upper Bound)**.** A set $\alpha \subseteq \mathbb{R}$ is *bounded above* if there exists a $B \in \mathbb{R}$ such that $A \leq B$ for all $A \in \alpha$. The number B is called an *upper bound* for α. A real number $S \in \mathbb{R}$ is the *least upper bound* for a set $\alpha \subseteq \mathbb{R}$ if it meets the following two criteria:

(i) S is an upper bound for α

(ii) if B is any upper bound for α, then $S \leq B$ [1].

Exercise 8. Let $\alpha \subseteq \mathbb{R}$ be nonempty and bounded above, and let S be the *union* of all $A \in \alpha$.

(a) First, prove that $S \in \mathbb{R}$ by showing that it is a cut.

(b) Now, show that S is the least upper bound for α.

Proof.

(a) (c1) We know that $\alpha \neq \emptyset$, thus there is some $A \in \alpha$. Call this A, A'. As S is the union of all the $A \in \alpha$, S contains A' and thus $S \neq \emptyset$. We also know that α is bounded by above by some real number, say B. This means that for every $A \in \alpha$, $A \subseteq B$. Since B is a cut there is some rational number $q \notin B$ which implies that $q \notin A$ for every $A \in \alpha$. As S can only contain elements from $A \in \alpha$ and q is in not in any $A \in \alpha$, it follows that $q \notin S$. Thus $S \neq \mathbb{Q}$.

(c2) Fix an $r \in S$. Then this $r \in A'$ for some $A' \in \alpha$. As A' is a cut, every rational number less than r is in A'. And S contains every A, thus S contains every rational less than r.

(c3) Proof by contradiction: Assume that S has a maximum, say M. Then M is in some $A \in \alpha$. Call this A, A'. A' is a cut, thus there exists an $N \in A'$ such that $N > M$. As $N \in A'$, this means that $N \in S$. Thus there exists an $N \in S$, where $N > M$, implying that M is not a maximum. This is a contradiction and thus S cannot have a maximum.

(b) (i) As $S = \bigcup_{A \in \alpha} A$, every $A \in \alpha$ is a subset of S. Or, for every $A \in \alpha$, $A \leq S$. Thus S is an upper bound for α.

(ii) Proof by contradiction: Assume there is some upper bound for α that is smaller than S. Call this upper bound C. Since C is an upper bound of α it must be that $A \subseteq C$ for all $A \in \alpha$. If C is a smaller bound than S, then $C \leq S$ which is $C \subseteq S$, but particularly $C \subset S$. If $C \subset S$, then there is an element $s \in S$ where $s \notin C$. But by the construction of S, it is necessarily true that $s \in A'$ for some $A' \in \alpha$. If this were true then $A' \nsubseteq C$, which would mean C isn't an upper bound on α. Thus $C = S$ has to be the least upper bound on α.

□

We're so close! So far we have proven that $\mathbb{R}$ is an ordered field for which every nonempty set of real numbers that is bounded above has a least upper bound. We're so close! All we need to do is prove that $\mathbb{Q}$ is a subfield of $\mathbb{R}$ and thus inherits all the properties we love about the real numbers.

Exercise 9. Consider the collection of so-called "rational" cuts of the form

$$C_r = \{t \in \mathbb{Q} : t < r\}$$

where $r \in \mathbb{Q}$.

(a) Show that $C_r + C_s = C_{r+s}$ for all $r, s \in \mathbb{Q}$. Verify $C_r C_s = C_{rs}$ for the case when $r, s \geq 0$.

(b) Show that $C_r \leq C_s$ if and only if $r \leq s$ in $\mathbb{Q}$.

Proof.

(a) Fix an arbitrary element of $C_r + C_s$, and call it t. So by definition, $t = u + v$ where $u \in C_r$ and $v \in C_s$. So $t = u + v < r + s$ by definition of the two sets, so $t \in C_{r+s}$ and since t is arbitrary, that means that $C_r + C_s \subseteq C_{r+s}$. Now, lets fix an element in C_{r+s} and again call it t. By definition, we know that $t < r + s$. So that means that $r + s - t > 0$. To prove that C_{r+s} is a subset we need a good old fashioned ϵ, so set $\epsilon = r + s - t$.

First see that $r - \frac{\epsilon}{2} < r$ so it's an element of C_r. Similarly, $s - \frac{\epsilon}{2} < s$ which is then an element of C_s. But note that

$$\begin{aligned} r - \frac{\epsilon}{2} + s - \frac{\epsilon}{2} &= r - \frac{r+s-t}{2} + s - \frac{r+s-t}{2} \\ &= r + s - (r+s-t) \\ &= t \end{aligned}$$

So t can be written as $t = u + v$ where $u \in C_r$ and $v \in C_s$, which can only mean that $t \in C_r + C_s$. Again, since t was arbitrary, it means that $C_{r+s} \subseteq C_r + C_s$.

Thus $C_r + C_s = C_{r+s}$

We verify $C_r C_s = C_{rs}$. We first want to show that $C_r C_s \subseteq C_{rs}$. Fix an element $t \in C_r C_s$. If $t < 0$, then $t \in C_{rs}$ as $C_{rs} \geq 0$. If $t \geq 0$, we can write $t = uv$, $u \in Cr, v \in Cs, u, v \geq 0$. We know that $u < r$ and $v < s$ which implies that $uv < rs$ and thus $t = uv \in C_{rs}$. Thus $C_r C_s \subseteq C_{rs}$. Next we want to show that $C_{rs} \subseteq C_r C_s$. So, fix an element of C_{rs} and once again call it t. Similarly, if $t < 0$ it isn't very interesting, since it will be in $C_r C_s$ by how we defined our product. So, let $t > 0$. By definition $t < rs$. So $\frac{t}{r} < s$ is true which means $0 < s - \frac{t}{r}$, i.e. $s - \frac{t}{r}$ is a positive rational number, which means we can find a $p \in \mathbb{Q}$ where $0 < p < s - \frac{t}{r}$. But $0 < p < s - \frac{t}{r}$ means

$$\frac{t}{r} < s - p$$

or

$$t < r(s-p)$$

$$\frac{t}{s-p} < r$$

so

$$\frac{t}{s-p} \in C_r$$

And since $p > 0$ it must be true that $s - p < s$ or $s - p \in C_s$. But...

$$\frac{t}{s-p} \cdot (s-p) = t$$

There it is, t can be written as $t = uv$ where $u \in C_r$ and $v \in C_s$ which can only mean $t \in C_r C_s$. So, $C_{rs} \subseteq C_r C_s$.

Thus! $C_r C_s = C_{rs}$.

(b) ($\Rightarrow$) Assume $r \leq s \in \mathbb{Q}$

Let $t \in C_r$ be fixed but arbitrary. So $t < r \in \mathbb{Q}$. But $r \leq s$, so $t < s$. So t is in C_s. So $C_r \leq C_s$, using the notation defined in 7.

($\Leftarrow$) Assume $C_r \leq C_s$. This can be proven by splitting it into two separate cases:

Case 1: $C_r = C_s$

This is simple, since if the sets are equal, then the conditions for an element to be in the set must be the same, so $r = s$.

Case 2: $C_r \subset C_s$

Since this is a proper subset, there exists some element $u \in C_s$ such that $u \notin C_r$ This means that $u \geq r$. Since $u < s$ so it follows that $r < s$.

Combining both cases, $r \leq s$.

□

Thus we have proved theorem 1. That is, we constructed $\mathbb{R}$ from $\mathbb{Q}$ using Dedekind Cuts.

References

[1] Stephen Abbott. *Understanding Analysis*. Springer, 2016.

[2] *Construction R from Q*. URL: `%5Curl%7Bhttps://www.amherst.edu/media/view/182802/original/Contruction%2BR%2Bfrom%2BQ.pdf%7D`.