Constructing the Reals

Matthew Hanna

May 13, 2019

Theorem 1. *There exists an order field $\mathbb{R}$ that has the least upper bound property. Moreover, $\mathbb{Q} \subset \mathbb{R}$ in the sense that $\mathbb{R}$ contains $\mathbb{Q}$ as an ordered subfield.*

What the second statement means is that the operations that $\mathbb{Q}$ enjoys stay invariant when $\mathbb{Q}$ is extended to $\mathbb{R}$. For example, if $x, y \in \mathbb{Q}$ and $x + y \in \mathbb{Q}$. Since $\mathbb{Q} \subset \mathbb{R}$, we have $x, y \in \mathbb{R}$ and $x + y \in \mathbb{R}$ is exactly the same sum as defined in $\mathbb{Q}$.

Proof. We prove the existence of $\mathbb{R}$ by explicitly constructing it. We divide this construction into several steps.

Step 1: The members of $\mathbb{R}$ will be certain subsets of $\mathbb{Q}$ which we give the name *cuts*. A cut must satisfy the following definitions.

1. $\alpha \neq \mathbb{Q}$ and $\alpha \neq \emptyset$.

2. If $p \in \alpha$ and $q < p$, then $q \in \alpha$. This gives us a useful relation between α, some element guaranteed to be in α, and an arbitrary element of $\mathbb{Q}$. That is, if we know p and α are related by the inclusion relation and q and p are related by the order relation that $q < p$, then we know that q and α are related by the inclusion relation as well.

3. If $p \in \alpha$, then there exists some $r \in \mathbb{Q}$ such that $p < r$ and $r \in \alpha$. This says that α contains no maximal element, analogous to $A = \{p \in \mathbb{Q} \mid p^2 < 2\}$ as discussed earlier.

The letters $p, q, r \ldots$ denote the rational numbers where $\alpha, \beta, \gamma \ldots$ represent cuts.
Note that (3) says the cuts in have no maximal element. (2) carries with it the following two implications.
If $p \in \alpha$ and $q \notin \alpha$, then $p < q$.

If $r \notin \alpha$ and $r < s$, then $s \notin \alpha$.

Step 2: To show that $\mathbb{R}$ is an ordered set.
We define $\alpha < \beta$ to mean $\alpha \subset \beta$. Since whenever $\alpha \subset \beta$ and $\beta \subset \gamma$, we have $\alpha \subset \gamma$. Translated to our language of order relation, whenever $\alpha < \beta$ and $\beta < \gamma$, we have $\alpha < \gamma$. It is obvious that **at most one** of the following be true

$$\alpha < \beta \qquad \alpha = \beta \qquad \alpha > \beta$$

This is because if $\alpha \subset \beta$ then it is not the case that $\beta \subset \alpha$. If neither is the case, then we say that $\alpha = \beta$. To show that one must be necessarily true, assume that it is not the case $\alpha < \beta$ or $\alpha = \beta$. Then it is not the case that $\alpha \subset \beta$. This means that there is some $p \in \alpha$ for which $p \notin \beta$. This means by $p > b$ for any $b \in \beta$. This means $b \in \alpha$. Then, $\beta \subset \alpha$, which is $\beta < \alpha$. We have now established that $\mathbb{R}$ is an ordered set.

Step 3: To show that $\mathbb{R}$ has the least upper bound property.
To prove this, let A be a nonempty subset of $\mathbb{R}$ that is bounded above. What we mean is that there is some $\beta \in \mathbb{R}$ that contains every element of A. Now suppose that $\gamma = \bigcup\limits_{\alpha \in A} \alpha$. This means that $p \in \alpha$ if and only $p \in \gamma$. I claim that $\gamma = sup(A)$ and that $\gamma \in \mathbb{R}$.
Since A is non-empty, there must some $\alpha_1 \in A$. $\alpha_1 \neq \emptyset$ and since $\alpha_1 \subset \gamma$, $\gamma \neq \emptyset$. Since every $\alpha \in A$ satisfies the property that $\alpha \subset \beta$, since β is an upper bound. It follows that $\gamma \subset \beta$ since $\gamma = \bigcup\limits_{\alpha \in A} \alpha$. Since $\beta \neq \mathbb{Q}$, it follows that $\gamma \neq \mathbb{Q}$. Hence, γ satisfies condition (1) laid out in the beginning of this proof. Pick some $p \in \gamma$. Since, $\gamma = \bigcup\limits_{\alpha \in A} \alpha$, there must be some α_p such that $p \in \alpha_p$. Pick some $q \in \mathbb{Q}$ such that $q < p$. By condition 2, it follows that $q \in \alpha_p$. Since $\gamma = \bigcup\limits_{\alpha \in A} \alpha$, it must follow that $q \in \gamma$. Since q was chosen arbitrarily, it follows γ also satisfies condition 2. Now in the same α_p, pick some $r > p$, whose existence is guaranteed by condition 3. It follows that $r \in \gamma$. As p maybe chosen at random without changing this result, it follows that γ satisfies condition 3. Since γ satisfies all three conditions required to be an element of $\mathbb{R}$, we may state that $\gamma \in \mathbb{R}$.
It is obvious that $\alpha \leq \gamma$, this means that γ is an upper bound. Suppose $\delta < \gamma$, then there is some $s \in \gamma$ such that $s \notin \delta$. Since γ is precisely the union of all $\alpha \in A$, there is some α_s, which $s \in \alpha_s$ and since $s \notin \delta$, it is not the case that $s < \delta$ or $s = \delta$, we then apply the result from set 2, to obtain the

fact $\delta < s$. Hence, δ is not an upper bound. Since the only condition that forced δ to not be an upper bound was that $\delta < \gamma$, it follows that $\gamma = sup(A)$.

Step 4: If α and β are both elements of $\mathbb{R}$, then we define $\alpha + \beta$ to be the set of all sums $a + b$ where $a \in \alpha$ and $b \in \beta$.
Define 0^* to be the set of all negative rational numbers. It is clear that 0^* satisfies the 3 conditions required to be a cut. Namely, $0^* \neq \emptyset$ since we know there is at least one element in 0^*. Also, we have that $0^* \neq \mathbb{Q}$ since we may find at least one rational (more specifically, any positive rational) which is not an element of $\mathbb{Q}$ Next, suppose $p \in 0^*$ and assume $q < p$. Then, we have the case that q is also a negative rational. Hence, condition 2 is satisfied. Now, pick $p \in 0^*$. Now, pick $r = \frac{p}{2}$. It is known that $r \in 0^*$ and that $r > p$. Hence, 0^* satisfies condition 3. And, with that, 0^* is a cut. We will now prove that the addition of elements of $\mathbb{R}$ defined above satisfies the conditions need to be considered addition.

1. First, we must show closure, which is: whenever $\alpha, \beta \in \mathbb{R}$, it follows that $\alpha + \beta \in \mathbb{R}$. In other words, we are required to that $\alpha + \beta$ is also a cut.

   (a) Since α and β are both non-empty, it follows that the set $\alpha + \beta$ is also non-empty. Pick $r, s \in \mathbb{Q}$ so that $r > a$ for any $a \in \alpha$ and $s > b$ for any $b \in \beta$. It follows that $r + s > a + b$ for any $a + b \in \alpha + \beta$. Hence, $\alpha + \beta$ is bounded above, therefore $\alpha + \beta \neq \mathbb{Q}$ Therefore $\alpha + \beta$ has property (1).

   (b) Pick $p \in \alpha + \beta$ Then, it follows, by definition, that $p = r + s$ for some $r \in \alpha$ and $s \in \beta$. Now pick $q < p$. Since $p - s = r$, we have $q - s < r$. Because α satisfies property (2), $q - s \in \alpha$. (And, by a similar argument, we have the result that $q - r \in \beta$.) Since $(q - s) \in \alpha$ and $s \in \beta$, it follows that $(q - s) + s \in \alpha + \beta$. Hence, $\alpha + \beta$ satisfies condition 2.

   (c) Consider some $p = r + s \in \alpha + \beta$ for some $r \in \alpha$ and $s \in \beta$. Since α and β each satisfy condition 3, it follows that there some $r' \in \alpha$ and some $s' \in \beta$ for which $r' > r$ and $s' > s$. Since $r' \in \alpha$ and $s' \in \beta$, it follows that $r' + s' \in \alpha + \beta$ and that $r' + s' > r + s$. Hence, $\alpha + \beta$ satisfies condition 3.

2. We now prove that this addition is commutative.
   Assume $\alpha + \beta$. Then, by definition, $\alpha + \beta = \{r + s \mid r \in \alpha, s \in \beta\}$ and we know that $\beta + \alpha = \{s + r \mid r \in \alpha, s \in \beta\}$ But since, $r, s \in \mathbb{Q}$,

we know that $r + s = s + r$. so $\alpha + \beta = \{s + r \mid r \in \alpha, s \in \beta\}$ Since $\alpha+\beta$ and $\beta+\alpha$ are the same set in set builder notation, we know that $\alpha + \beta = \beta + \alpha$, as was required.

3. We prove that this addition is associative.
   We pick $\alpha, \beta, \gamma \in \mathbb{R}$. Consider $(\alpha + \beta) + \gamma$ In the language of set theory, this is $(\alpha + \beta) + \gamma = \{(a + b) + c \mid a \in \alpha, b \in \beta, c \in \gamma\}$ Since $a, b, c \in \mathbb{Q}$, we have $(\alpha + \beta) + \gamma = \{a + (b + c) \mid a \in \alpha, b \in \beta, c \in \gamma\}$ since addition in $\mathbb{Q}$ is associative. Converting to the right hand side into the language of this proof, we have $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$. This is what we wanted to show.

4. If $r \in \alpha$ and $s \in 0^*$, then we know that $r + s < r$ since 0^* is the set of all negative rationals. Since we have proved closure under addition of cuts and by condition 2 of this proof, we know that $\alpha + 0^* \subseteq \alpha$. Now, pick $p \in \alpha$ and by condition 3, we know that we may pick some $p \in \alpha$ such that $r > p$. Therefore, $p - r \in 0^*$. Which yields the result that $p = r + (p - r) \in \alpha + 0^*$. Hence, $\alpha \subseteq \alpha + 0^*$. By the double inclusion argument, we have $\alpha = \alpha + 0^*$. Hence, we have shown the existence of an additive identity, namely 0^*.

5. Let $\alpha \in \mathbb{R}^+$ be a fixed cut. Now let β be the set of all $p \in \mathbb{Q}$ with the following property: *There exists a rational* $r > 0$ *such that* $-p-r \notin \alpha$. For example, let α be the cut associated with $\sqrt{2}$. Consider $p = -2$, it is very easy to see that there is some rational r, for example $r = 0.1$ such that $-(-2) - 0.01$ is not in the cut associated with $\sqrt{2}$.
   We must show that β *is a cut and that* $\alpha + \beta = 0^*$.
   Suppose $s \notin \alpha$ such an s is guaranteed to existed by the condition that $\alpha \neq \mathbb{Q}$. We intuitively think of this as $s > \alpha$. Now, consider $p = -s - 1$ and pick $r = 1$. It is easy to see that $-p - 1 \notin \alpha$ since $-p - 1 = -(-s - 1) - 1 = s + 1 - 1 = s$. Therefore $p \in \beta$. Since existence of s is guaranteed, this construction of p based on s is also guaranteed. Hence, β is not empty. If $q \in \alpha$, then, by the fact that $\mathbb{R}$ is ordered, we have $-q \notin \beta$. Hence, $\beta \neq \mathbb{Q}$. Thus, β satisfies condition 1.
   Now pick $p \in \beta$ and choose r accordingly so that $-p-r \notin \alpha$. If $q < p$, it easily follows that $-q - r > -p - r$. Therefore, $-q - r \notin \alpha$. Hence $q \in \beta$. Condition 2 is satisfied.
   Now, let $t = p + \frac{r}{2}$. It easily follows that $t > p$. Then $-t - \frac{r}{2} = -(p + \frac{r}{2}) - \frac{r}{2} = -p - r \notin \alpha$. Hence, $t \in \beta$. Condition 3 is satisfied and with that we have shown that β is a cut.

Let $r \in \alpha$ and $s \in \beta$. Then, $-s \notin \alpha$. Therefore, $r < -s$. Hence, $r + s < 0$. This shows that $r + s \subseteq 0^*$. To prove the reverse inclusion, pick $v \in 0^*$ and $w = -\frac{v}{2}$. Since, v is a negative rational, by definition, $w > 0$. There is some $n \in \mathbb{Z}$ for which $nw \in \alpha$ but $(n+1)w \notin \alpha$. It is easy quite easy to argue why. Pick $a_\epsilon \in \alpha$ so that $d(a_\epsilon, \alpha) < \epsilon$ for positive rational ϵ. We may then choose n to be the floor of $\frac{a_\epsilon}{w}$. and as $\epsilon \to 0$, it follows that n is the desire integer as above. Now, let $p = -(n+2)w$. Since $-p - w = (n+2)w - w = (n+1)w \notin \alpha$, $p \in \beta$. We also have the added bonus that:

$$p + nw \in \beta + \alpha$$

$$p + nw = -(n+2)w + nw$$
$$-(n+2)w + nw = (n+2)\frac{v}{2} - n\frac{v}{2}$$

.

$$p + nw = v \in \alpha + \beta$$

Hence, $0^* \subseteq \alpha + \beta$. We have shown that $\alpha + \beta = 0^*$.

Step 5: We have prove that the addition of cuts as defined earlier does satisfy the axioms for something to be considered addition in the traditional sense. We get the following truths about $\mathbb{R}$ for free.

1. If $\alpha + \beta = \alpha + \gamma$, then $\beta = \gamma$.
2. If $\alpha + \beta = \alpha$, then $\beta = 0^*$
3. If $\alpha + \beta = 0^*$, then $\beta = -\alpha$
4. $-(-\alpha) = \alpha$

All of which hold for any $\alpha, \beta, \gamma \in \mathbb{R}$. By the clever construction of $\mathbb{R}$, we may also prove other intuitive theorems which do not strictly follow from the axioms for addition. Consider $\beta, \gamma \in \mathbb{R}$ in which $\beta < \gamma$. By definition, this means that $\beta \subset \gamma$. And, by how addition is defined, it follows that $\alpha + \beta \subset \alpha + \gamma$. This implies that $\alpha + \beta < \alpha + \gamma$. Now consider $\alpha > 0^*$. By the result in step 4, we know there exists some $-\alpha \in \mathbb{R}$ in which $\alpha + -\alpha = 0$. Therefore, we have $\alpha + -\alpha > 0^* - \alpha$. We rewrite the LHS as 0^* and we may rewrite RHS as $-\alpha$ because we have established that 0^* is the additive identity for $\mathbb{R}$. So we have the result that $0^* > -\alpha$. □