Math Journal

Isabelle Mills

September 9, 2024

8/31/2024

My goal for today is to work through the appendix to chapter 1 in Baby Rudin. This appendix focuses on constructing the real numbers using Dedikind cuts.

We define a cut to be a set $\alpha \subset \mathbb{Q}$ such that:

1. $\alpha \neq \emptyset$
2. If $p \in \alpha$, $q \in \mathbb{Q}$, and $q < p$, then $q \in \alpha$.
3. If $p \in \alpha$, then $p < r$ for some $r \in \alpha$

Point 3 tells us that α doesn't have a max element. Also, point 2 directly implies the following facts:

a. If $p \in \alpha$, $q \in \mathbb{Q}$, and $q \notin \alpha$, then $q > p$.
b. If $r \notin \alpha$, $r, s \in \mathbb{Q}$, and $r < s$, then $s \notin \alpha$.

As a shorthand, I shall refer to the set of all cuts as R.

An example of a cut would be the set of rational numbers less than 2.

Firstly, we shall assign an ordering to R. Specifically, given any $\alpha, \beta \in R$, we say that $\alpha < \beta$ if $\alpha \subset \beta$ (a proper subset).

Here we prove that $<$ satisfies the definition of an ordering.

I. It's obvious from the definition of a proper subset that at most one of the following three things can be true: $\alpha < \beta$, $\alpha = \beta$, and $\beta < \alpha$.

   Now let's assume that $a \not< \beta$ and $\alpha \neq \beta$. Then $\exists p \in \alpha$ such that $p \notin \beta$. But then for any $q \in \beta$, we must have by fact b. above that $q < p$. Hence $q \in \alpha$, meaning that $\beta \subset \alpha$. This proves that at least one of the following has to be true: $\alpha < \beta$, $\alpha = \beta$, and $\beta < \alpha$.

II. If for $\alpha, \beta, \gamma \in R$ we have that $\alpha < \beta$ and $\beta < \gamma$, then clearly $\alpha < \gamma$ becuase $\alpha \subset \beta \subset \gamma$.

Now we claim that R equipped with $<$ has the least-upper-bound property.

Proof:
Let $A \subset R$ be nonempty and $\beta \in R$ be an upper bound of A. Then set $\gamma = \bigcup_{\alpha \in A} \alpha$. Firstly, we want to show that $\gamma \in R$

Since $A \neq \emptyset$, there exists $\alpha_0 \in A$. And as $\alpha_0 \neq \emptyset$ and $\alpha_0 \subseteq \gamma$ by definition, we know that $\gamma \neq \emptyset$. At the same time, we know that $\gamma \subset \beta$ since $\forall \alpha \in A$, $\alpha \subset \beta$. Hence, $\gamma \neq \mathbb{Q}$, meaning that γ satisfies property 1. of cuts.

Next, let $p \in \gamma$ and $q \in \mathbb{Q}$ such that $q < p$. We know that for some $\alpha_1 \in A$, we have that $p \in \alpha_1$. Hence by property 2. of cuts, we know that $q \in \alpha_1 \subset \gamma$, thus showing that γ satisfies property 2. of cuts.

Thirdly, by property 3. we can pick $r \in \alpha_1$ such that $p < r$ and $r \in \alpha_1 \subset \gamma$. So, γ satisfies property 3. of cuts.

With that, we've now shown that $\gamma \in R$. Clearly, γ is an upper bound of A since $\alpha \subset \gamma$ for all $\alpha \in A$. Meanwhile, consider any $\delta < \gamma$. Then $\exists s \in \gamma$ such that $s \notin \delta$. And since $s \in \gamma$, we know that $s \in \alpha$ for some $\alpha \in A$. Hence, $\delta < \alpha$, meaning that δ is not an upper bound of A. This shows that $\gamma = \sup A$.

Secondly, we want to assign $+$ and $\cdot$ operations to R so that R is an ordered field.

To start, given any $\alpha, \beta \in R$, we shall define $\alpha + \beta$ to be the set of all sums $r + s$ such that $r \in \alpha$ and $s \in \beta$.

Here we show that $\alpha + \beta \in R$.

1. Clearly, $\alpha + \beta \neq \emptyset$. Also, take $r' \notin \alpha$ and $s' \notin \beta$. Then $r' + s' > r + s$ for all $r \in \alpha$ and $s \in \beta$. Hence, $r' + s' \notin \alpha + \beta$, meaning that $\alpha + \beta \neq \mathbb{Q}$.

Now let $p \in \alpha + \beta$. Thus there exists $r \in \alpha$ and $s \in \beta$ such that $p = r + s$.

2. Suppose $q < p$. Then $q - s < r$, meaning that $q - s \in \alpha$. Hence, $q = (q - s) + s \in \alpha + \beta$.

3. Let $t \in \alpha$ so that $t > r$. Then $p = r + s < t + s$ and $t + s \in \alpha + \beta$.

Also, we shall define 0^* to be the set of all negative rational numbers. Clearly, 0^* is a cut. Furthermore, we claim that $+$ satisfies the addition requirements of a field with 0^* as its 0 element.

Commutativity and associativity of $+$ on R follows directly from the commutativity and associativity of addition on the rational numbers.

Also, for any $\alpha \in R$, $\alpha + 0^* = \alpha$.

If $r \in \alpha$ and $s \in 0^*$, then $r + s < r$. Hence $r + s \in \alpha$, meaning that $\alpha + 0^* \subseteq \alpha$. Meanwhile, if $p \in \alpha$, then we can pick $r \in \alpha$ such that $r > p$. Then, $p - r \in 0^*$ and $p = r + (p - r) \in \alpha + 0^*$. So, $\alpha \subseteq \alpha + 0^*$.

Finally, given any $\alpha \in R$, let $\beta = \{p \in \mathbb{Q} \mid \exists r \in \mathbb{Q}^+ \ s.t. \ -p - r \notin \alpha\}$.

To give some intuition on this definition, firstly we want to guarentee that for all $p \in \beta$, $-p$ is greater than all elements of α. Secondly, we add the $-r$ term to guarentee that β doesn't have a maximum element.

We claim that $\beta \in R$ and $\beta + \alpha = 0^*$. Hence, we can define $-\alpha = \beta$.

To start, we'll show that $\beta \in R$:

1. For $s \notin \alpha$ and $p = -s - 1$, we have that $-p - 1 \notin \alpha$. Hence, $p \in \beta$, meaning that $\beta \neq \emptyset$. Meanwhile, if $q \in \alpha$, then $-q \notin \beta$ because there does not exist $r > 0$ such that $-(-q) - r = q - r \notin \alpha$. So $\beta \neq \mathbb{Q}$.

Now let $p \in \beta$ and pick $r > 0$ such that $-p - r \notin \alpha$.

2. Suppose $q < p$. Then $-q - r > -p - r$, meaning that $-q - r \notin \alpha$. Hence, $q \in \beta$.

3. Let $t = p + \frac{r}{2}$. Then $t > p$ and $-t - \frac{r}{2} = -p - r \notin \alpha$, meaning $t \in \beta$.

Now that we've proved $\beta \in R$, we next prove that β is the additive inverse of α. To start, suppose $r \in \alpha$ and $s \in \beta$. Then $-s \notin \alpha$, meaning that $r < -s$. So $r + s < 0$, thus showing that $\alpha + \beta \subseteq 0^*$.

As for the other inclusion, pick any $v \in 0^*$ and set $w = -\frac{v}{2}$. Then because $w > 0$, we can use the archimedean property of $\mathbb{Q}$ to say that there exists $n \in \mathbb{Z}$ such that $nw \in \alpha$ but $(n+1)w \notin \alpha$. Put $p = -(n+2)w$. Then $p \in \beta$ because $-p - w = (n+1)w \notin \alpha$. And finally, $v = nw + p \in \alpha + \beta$. Thus, $0^* \subseteq \alpha + \beta$.

9/1/2024

Based on the definition of $+$, it's also hopefully clear that for any $\alpha, \beta, \gamma \in R$ such that $\alpha < \beta$, we have that $\alpha + \gamma < \beta + \gamma$.

Next, we shall define multiplication on R. Except, first we're going to limit ourselves to the set R^+ of all cuts greater than 0^*. So, given any $\alpha, \beta \in R^+$, we shall define $\alpha\beta$ to be the set of all $p \in \mathbb{Q}$ such that $p \leq rs$ where $r \in \alpha$, $s \in \beta$, $r > 0$, and $s > 0$.

Here we show that $\alpha\beta \in R^+$.

1. Clearly $\alpha\beta \neq \emptyset$. Also, take any $r' \notin \alpha$ and $s' \notin \beta$. Then $r's' > rs$ for all $r \in \alpha \cap \mathbb{Q}^+$ and $s \in \beta \cap \mathbb{Q}^+$ since all four rational numbers are positive. By extension, $r's'$ is greater than all the elements (both positive and negative) of $\alpha\beta$. So, $r's' \notin \alpha\beta$, meaning that $\alpha\beta \neq \mathbb{Q}$.

Now let $p \in \alpha\beta$. Based on our definition of $\alpha\beta$, we know that the conditions of a cut trivially hold for any negative p. So, we'll assume from now on that $p > 0$. (Also note that a positive choice of p must exist because both α and β by assumption have positive elements.)

Since $p \in \alpha\beta \cap \mathbb{Q}^+$, we know there exists $r \in \alpha$ and $s \in \beta$ such that $p = rs$ and $r, s > 0$.

2. Suppose $0 < q < p$ (the case where $q \leq 0$ is trivial). Then $\frac{q}{s} < r$, meaning that $\frac{q}{s} \in \alpha$. So, $q = \frac{q}{s} \cdot s \in \alpha\beta$.

3. Let $t \in \alpha$ so that $t > r$. Then $p = rs < ts$ and $ts \in \alpha\beta$.

Also, we shall define 1^* to be the set of all rational numbers less than 1. Clearly, 1^* is a cut. And we claim that $\cdot$ satisfies the multiplication requirements of a field with 1^* as its 1 element.

As before, commutativity and associativity of $\cdot$ on R^+ follows directly from commutativity and associativity of multiplication on the rational numbers.

Next, for any $\alpha \in R^+$, we have that $\alpha 1^* = \alpha$.

It's clear that for any rational number $r \leq 0$, we have that $r \in \alpha 1^*$ and $r \in \alpha$. So we can exclusively focus on positive rational numbers.

Now suppose $r \in \alpha \cap \mathbb{Q}^+$ and $s \in 1^*$. Then $rs < r$, meaning that $rs \in \alpha$. So $\alpha 1^* \subseteq \alpha$. Meanwhile, if $p \in \alpha \cap \mathbb{Q}^+$, then we can pick $r \in \alpha$ such that $r > p$. Then $\frac{p}{r} \in 1^*$ and $p = \frac{p}{r} \cdot r \in \alpha 1^*$. So, $\alpha \subseteq \alpha 1^*$.

Thirdly, given any $\alpha \in R^+$, define:

$$\beta = \{p \in \mathbb{Q} \mid p \leq 0\} \cup \{p \in \mathbb{Q}^+ \mid \exists r \in \mathbb{Q}^+ \; s.t. \; \tfrac{1}{q} - r \notin \alpha\}$$

Here we show that $\beta \in R^+$.

1. Clearly $\beta \neq \emptyset$. Also, if $q \in \alpha$, then $\frac{1}{q} \notin \beta$. Hence, $\beta \neq \mathbb{Q}$.

Now let $p \in \beta$ and pick $r > 0$ such that $\frac{1}{p} - r \notin \alpha$. Also, assume $p > 0$ because the proof is trivial if $p \leq 0$. (The fact that $p > 0$ in β exists is trivial to show.)

2. If $q \leq 0 < p$, then trivially $q \in \beta$. Meanwhile, if $0 < q < p$, then $\frac{1}{q} - r > \frac{1}{p} - r$, meaning that $\frac{1}{q} - r \notin \alpha$. Hence, $q \notin \beta$.

3. Let $t = \frac{1}{\frac{1}{p} - \frac{r}{2}}$. Then since $\frac{1}{p} - r \notin \alpha$, we know that $\frac{1}{p} - \frac{r}{2} > 0$. Also since $\frac{1}{t} = \frac{1}{p} - \frac{r}{2} < \frac{1}{p}$, we have that $t > p$. But note that $\frac{1}{t} - \frac{r}{2} = \frac{1}{p} - r \notin \alpha$. Hence $t \notin \beta$.

We claim that $\beta\alpha = 1^*$. Hence, we can define $\frac{1}{\alpha} = \beta$.

To start, suppose $r \in \alpha \cap \mathbb{Q}^+$ and $s \in \beta \cap \mathbb{Q}^+$. Then $\frac{1}{s} \notin \alpha$, meaning that $r < \frac{1}{s}$. So $rs < 1$, thus showing that $\alpha\beta \subseteq 1^*$.

The other inclusion has a more complicated proof. Firstly, take any $v \in 1^* \cap \mathbb{Q}^+$ (the proof is trivial if $v \leq 0$). Then set $w = \frac{1}{v}$, meaning that $w > 1$. Now since $\alpha \in R^+$, we know there exists $n \in \mathbb{Z}$ such that $w^n \in \alpha$ but $w^{n+1} \notin \alpha$. Then as $w^{n+2} > w^{n+1}$, we know that $\frac{1}{w^{n+2}} \in \beta$. Hence, $v^2 = w^n \frac{1}{w^{n+2}} \in \alpha\beta$.

Now that we've shown that the square of every $v \in 1^* \cap \mathbb{Q}^+$ is also in $\alpha\beta$, we next show that there exists $z \in 1^* \cap \mathbb{Q}^+$ such that $z^2 > v$. Suppose $v = \frac{p}{q}$ where $p, q \in \mathbb{Z}^+$. Then set $z = \frac{p+q}{2q}$. Importantly, since $p < q$, we still have that $z \in 1^*$. But also note that:

$$z^2 - v = \tfrac{p^2+2pq+q^2}{4q^2} - \tfrac{4pq}{4q^2} = \tfrac{p^2-2pq+q^2}{4q^2} = \left(\tfrac{p-q}{2q}\right)^2 \geq 0$$

Thus as $v < z^2$ and $z^2 \in \alpha\beta$, we have that $v \in \alpha\beta$ as well. So $1^* \subseteq \alpha\beta$.

Finally, so long as $\alpha, \beta, \gamma \in R^+$, we have that $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ because the rational numbers satisfy the distributive property.

Notably, in proving that $\alpha\beta \in R^+$ before, we also guarenteed that for $\alpha, \beta > 0$, we have that $\alpha\beta > 0$.

9/7/2024

Now we still need to extend our definition of multiplication from R^+ to all of R. To do this, set $\alpha 0^* = 0^*\alpha = 0^*$ and define:

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

Having done that, reproving those properties of multiplication on all of R just becomes a matter of addressing many cases and using the identity that $(-(-\alpha)) = \alpha$.

Note that that identity can be proven just from the addition properties of a field.

Because I'm bored with this construction at this point, I'm going to skip reproving those properties.

So now that we've established that R is a field, all we have left to do is to show that all numbers $r, s \in \mathbb{Q}$ are represented by cuts $r^*, s^* \in R$ such that:

- $(r + s)^* = r^* + s^*$
- $(rs)^* = r^*s^*$
- $r < s \iff r^* < s^*$

Again, I'm super bored and demotivated at this point. So, I'm going to skip showing this.

With all that done, we've now shown that R satisfies all of the properties of real numbers. That concludes the proof of the existence theorem of the real numbers.

9/9/2024

Today I'm just looking at James Munkres' book *Topology*. Now while I'm done with the era of my life of taking exhaustive notes on a textbook, I still want to write down some interesting proofs. I also hope to do some exercises.

Theorem 7.8: Let A be a nonempty set. There is no injective map $f : \mathcal{P}(A) \longrightarrow A$ and there is no surjective map $g : A \longrightarrow \mathcal{P}(A)$.

In other words, the power set of a set has strictly greater cardinality.

Proof:
If such an injective f existed, then that would imply a surjective g exists. So, we just need to show that any function $g : A \longrightarrow \mathcal{P}(A)$ isn't surjective.

Let $g : A \longrightarrow \mathcal{P}(A)$ be any function and define $B = \{a \in A \mid a \in A - g(a)\}$. Clearly, $B \subseteq A$. However, B cannot be in the image of g. After all, suppose there exists $a_0 \in A$ such that $g(a_0) = B$. Then we get a contradiction because:

$$a_0 \in B \iff a_0 \in A - g(a_0) \iff a_0 \in A - B$$

Hence, $g(A) \neq \mathcal{P}(A)$ and we conclude that g can't be surjective. ■

Exercise 7.3: Let $X = \{0, 1\}$. Show there is a bijective correspondence between the set $\mathcal{P}(\mathbb{Z}_+)$ and the Cartesian product X^ω.

For any set $A \in \mathcal{P}(\mathbb{Z}_+)$, define $f(A)$ to be the ω-tuple $\mathbf{x}$ such that for all $i \in \mathbb{Z}^+$, $\mathbf{x}_i = 1$ if $i \in A$ and $\mathbf{x}_i = 0$ if $i \notin A$. Then clearly f is injective as $\forall A, B \in \mathcal{P}(\mathbb{Z}_+)$, $f(A) = f(B) \implies A = B$. Also, given any $\mathbf{x} \in X^\omega$, we know that the set $A = \{i \in \mathbb{Z}_+ \mid \mathbf{x}_i = 1\}$ satisfies that $f(A) = \mathbf{x}$.

Hence, f is a bijective function between $\mathcal{P}(\mathbb{Z}_+)$ and X^ω.

Note that this construction still works if $\mathbb{Z}_+$ is replaced with any countably infinite set.

Exercise 7.5: Determine whether the following sets are countable or not.

(f) The set F of all functions $f : \mathbb{Z}_+ \longrightarrow \{0, 1\}$ that are "eventually zero", meaning there is a positive integer N such that $f(n) = 0$ for all $n \geq N$.

F is countable. To see why, let:

$$A_n = \{f : \mathbb{Z}_+ \longrightarrow \{0, 1\}^\omega \mid \forall i \geq n, \;\; f(i) = 0\}$$

Thus each A_n is finite (with 2^n elements) and $F = \bigcup_{n=1}^{\infty} A_n$.

(g) The set G of all functions $f : \mathbb{Z}_+ \longrightarrow \mathbb{Z}_+$ that are eventually 1.

G is countable. To see why, let:

$$A_n = \{f : \mathbb{Z}_+ \longrightarrow \mathbb{Z}_+ \mid \forall i \geq n, \;\; f(i) = 1\}$$

Then each A_n has a bijective correspondence with $(\mathbb{Z}_+)^n$, meaning each A_n is countable, and $G = \bigcup_{n=1}^{\infty} A_n$.

The same argument applies to all functions $f : \mathbb{Z}_+ \longrightarrow \mathbb{Z}_+$ that are eventually any constant.

(h) The set H of all functions $f : \mathbb{Z}_+ \longrightarrow \mathbb{Z}_+$ that are eventually constant.

H is countable. To see why, let A_n be the set of all functions $f : \mathbb{Z}_+ \longrightarrow \mathbb{Z}_+$ that are eventually n. Because of part g of this exercise, we know that each A_n is countable. Also, $H = \bigcup_{n=1}^{\infty} A_n$.

(i) The set I of all two-element subsets of $\mathbb{Z}_+$

(j) The set J of all finite subsets of $\mathbb{Z}_+$.

Both I and J are countably infinite. We know this because we can define surjections from $(\mathbb{Z}_+)^2$ to I and $\bigcup_{n=1}^{\infty} (\mathbb{Z}_+)^n$ to J.

(Finite cartesian products of countable sets and unions of countably many countable sets are countable.)

Exercise 7.6.a: Show that if $B \subset A$ and there is an injection $f : A \longrightarrow B$, then $|A| = |B|$.