Math Journal

Isabelle Mills

September 14, 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 $f(A) = \mathbf{x}$, meaning f is surjective.

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:

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

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 $|A| = |B|$.

According to the hint, we set $A_1 = A$ and $A_n = f(A_{n-1})$ for all $n > 1$. Similarly, we set $B_1 = B$ and $B_n = f(B_{n-1})$ for all $n > 1$.

We can assume A_2 is a proper subset of B_1 because if $A_2 = B_1$, then we already have that f is a bijection. Also, as f is an injection, we know that $B_2 \subset A_2$. Thus by induction, we can conclude that:

$$A_1 \supset B_1 \supset A_2 \supset B_2 \supset A_3 \supset B_3 \supset \cdots$$

Now, the textbook recommends defining $h : A \longrightarrow B$ by:

$$h(x) = \begin{cases} f(x) & \text{if } x \in A_n - B_n \text{ for any } n \in \mathbb{Z}_+ \\ x & \text{otherwise} \end{cases}$$

I want to ask a professor about this definition because it urks me. My issue with this definition of h is that I feel like it should be possible for:

$$\bigcap_{n=1}^{\infty}(A_n \cap B_n) \neq \emptyset.$$

However, we wouldn't be able to know that some x is in that intersection and thus falls into case 2 until after an infinite number of steps.

On the other hand, $S_1 = \bigcup_{n=1}^{\infty}(A_n - B_n)$ is a valid definition for a set, as is $S_2 = A - S_1$. So the definition h is valid because it's saying that $h(x) = f(x)$ if $x \in S_1$ and $h(x) = x$ if $x \in S_2$.

Maybe my issue is just that I have trouble trusting the validity of a function definition if I can't actually evaluate that function myself. Although, there are lots of functions like that that I don't have any problem with. For example, given $g(x) = 0$ if x is rational and $g(x) = 1$ if x is irrational, what is $g(\pi^2)$?

Hopefully it is clear that h is in fact a valid function from A to B. Now firstly, we shall show that h is injective.

Let $x, y \in A$ such that $x \neq y$. If there are integers n and m such that $x \in A_n - B_n$ and $y \in A_m - B_m$, then $h(x) \neq h(y)$ because f is injective. Meanwhile, if no such n or m exists, then $h(x) \neq h(y)$ because $x \neq y$.

This leaves the case that there exists $n \in \mathbb{Z}_+$ such that $x \in A_n - B_n$ but for all $m \in \mathbb{Z}_+$, $y \notin A_m - B_m$. Then, note that $f(x) \in f(A_n - B_n)$. And since f is injective, we thus have that $f(x) \in f(A_n) - f(B_n) = A_{n+1} - B_{n+1}$. Therefore, as $y \notin A_{n+1} - B_{n+1}$, we know that $h(x) \neq y = h(y)$.

Next, we show h is surjective.

Let $y \in B$.

Suppose there exists $n \in \mathbb{Z}_+$ such that $y \in A_n - B_n$. We know that $n \neq 1$ since $y \in B$. Thus, there must exist $x \in A_{n-1}$ such that $y = f(x) \in f(A_{n-1}) = A_n$. Furthermore, this x can't be in B_{n-1} because otherwise y would be in B_n which we know isn't true. So, $x \in A_{n-1} - B_{n-1}$, meaning that $h(x) = f(x) = y$.

Meanwhile, if no such n exists, then we simply have that $h(y) = y$. Hence, $h(A) = B$.

Thus, we've shown that h is a bijection, meaning that $|A| = |B|$.

Exercise 7.7: Show that $|\{0,1\}^\omega| = |(\mathbb{Z}_+)^\omega|$.

Firstly, there's obviously a bijection exists between $\{0,1\}^\omega$ and $\{1,2\}^\omega$. Also, $\{1,2\}^\omega \subset (\mathbb{Z}_+)^\omega$. So, if we can construct an injective function from $(\mathbb{Z}_+)^\omega$ to $\{1,2\}^\omega$, then we can apply the result of exercise 7.6.a to prove this exercise's claim.

We shall create this injection using a diagonalization argument. Let $x \in (\mathbb{Z}_+)^\omega$. Then we define $f(x) = y \in \{1,2\}^\omega$ as follows:

$y(1) = 2$ if $x(1) = 1$. Otherwise $y(1) = 1$.

$y(2) = 2$ if $x(1) = 2$. Otherwise $y(2) = 1$.
$y(3) = 2$ if $x(2) = 1$. Otherwise $y(3) = 1$.

$y(4) = 2$ if $x(1) = 3$. Otherwise $y(4) = 1$.
$y(5) = 2$ if $x(2) = 2$. Otherwise $y(5) = 1$.
$y(6) = 2$ if $x(3) = 1$. Otherwise $y(6) = 1$.

$y(7) = 2$ if $x(1) = 4$. Otherwise $y(7) = 1$.

$\vdots$

Clearly f is an injection since $f(x_1) = f(x_2)$ implies that x_1 and x_2 have the same integers at all indices.

Exercise 7.6.b: (Schroeder-Bernstein theorem) If there are injections $f : A \longrightarrow C$ and $g : C \longrightarrow A$, then A and C have the same cardinality.

I did my work on paper and now it's late and I don't want to write more tonight.

9/11/2024

Since today's my day off, I'm gonna work through Munkres' textbook *Topology* some more.

Theorem 8.4 (Principle of recursive definition): Let A be a set and let a_0 be an element of A. Suppose ρ is a function assigning an element of A to each function f mapping a nonempty section of the positive integers onto A. Then there exists a unique function $h : \mathbb{Z}_+ \longrightarrow A$ such that:

$$(*) \qquad \begin{aligned} h(1) &= a_0 \\ h(i) &= \rho(h|_{\{1,\ldots,i-1\}}) \quad \text{for } i > 1. \end{aligned}$$

Proof outline:

Part 1: Given any $n \in \mathbb{Z}_+$, there exists a function $f : \{1, \ldots, n\} \longrightarrow A$ that satisfies $(*)$.

This is obvious from induction.

Part 2: Suppose that $f : \{1, \ldots, n\} \longrightarrow A$ and $g : \{1, \ldots, m\} \longrightarrow A$ both satisfy $(*)$ for all i in their respective domains. Then $f(i) = g(i)$ for all i in both domains.

Proof:
Suppose not. Let i be the smallest integer for which $f(i) \neq g(i)$.

We know $i \neq 1$ because $f(1) = a_0 = g(1)$. But then note that $f|_{\{1,\ldots,i-1\}} = g|_{\{1,\ldots,i-1\}}$. Hence:

$$f(i) = \rho(f|_{\{1,\ldots,i-1\}}) = \rho(g|_{\{1,\ldots,i-1\}}) = g(i).$$

This contradicts that i is the smallest integer for which $f(i) \neq g(i)$.

Part 3: Let $f_n : \{1, \ldots, n\} \longrightarrow A$ be the unique function satisfying $(*)$ (uniqueness was proven in part 2). Then we define:

$$h = \bigcup_{i=1}^{\infty} f_n$$

Because of part 2, we can fairly easily show that for each $i \in \mathbb{Z}_+$, there is exactly one element in h with i as it's first coordinate. Hence, the set h defines a functions from $\mathbb{Z}_+$ to A.

Also, hopefully it's clear that h satisfies $(*)$.

Axiom of choice: Given a collection $\mathcal{A}$ of disjoint nonempty sets, there exists a set C consisting of exactly one element from each element of $\mathcal{A}$.

A few notes:

1. If we restrict $\mathcal{A}$ to being a finite collection, then there is nothing controversial about this axiom. It only becomes controversial when $\mathcal{A}$ is allowed to be infinite.
2. There are multiple instances in baby Rudin where we made an infinite number of arbitrary choices. Looking at a lot of those proofs closer, I think many of them could avoid using the axiom of choice by specifying that we had to pick rational numbers in a set. However, being able to pick elements without worrying about a preexisting choice function is way easier.

   My take away from this is that not only does it make proofs cleaner to not worry about using constructed choice functions, but it's also perfectly acceptable now-a-days to use this axiom.

Lemma 9.2: (Existence of a choice function) Given a collection $\mathcal{B}$ of nonempty sets (not necessarily disjoint), there exists a function

$$c : \mathcal{B} \longrightarrow \bigcup_{B \in \mathcal{B}} B$$

such that $c(B)$ is an element of B for each $B \in \mathcal{B}$.

Proof:
Given any set $B \in \mathcal{B}$, we define $B' = \{(B, b) \mid b \in B\}$. Because $B \neq \emptyset$, we know that $B' \neq \emptyset$ as well. Furthermore, given $B_1, B_2 \in \mathcal{B}$ if $B_1 \neq B_2$, then we have that the first element of all the pairs in B_1' are different from that of B_2'. So B_1' and B_2' are disjoint.

Now form the collection $\mathcal{C} = \{B' \mid B \in \mathcal{B}\}$. From before, we know that $\mathcal{C}$ is a collection of disjoint sets. So by the axiom of choice, there exists a set c consisting of exactly one element from each element of $\mathcal{C}$.

This set c is a subset of $\mathcal{B} \times \bigcup_{B \in \mathcal{B}} B$ which satisfies our definition of a choice function.

Hopefully it's obvious enough why c satisfies those properties.

A set A with an order relation $<$ is said to be well-ordered if every nonempty subset of A has a smallest element.

Tangent: inductiveness of $\mathbb{Z}_+$ is equivalent to the well-orderedness of $\mathbb{Z}_+$

This proof is taken from https://math.libretexts.org/ on their page for the well-ordering principle.

($\Longrightarrow$)
Suppose S is a nonempty subset of $\mathbb{Z}_+$ with no least element. Then let R be the set of lower bounds of S. Since 1 is the least element of $\mathbb{Z}_+$, we know that $1 \in R$.

Now given any $k \geq 1$, if $k \in R$, we know that $\{1, \ldots, k\}$ must be a subset of R. Also note that $R \cap S = \emptyset$ because if that wasn't true, we'd know that S has a least element. Therefore, $\{1, \ldots, k\} \cap S = \emptyset$. But then that shows that $k+1 \notin S$ since otherwise $k + 1$ would be the least element of S. Furthermore, since no element of $\{1, \ldots, k\}$ is in S, we automatically have that $k + 1 \in R$.

By induction, this means that $R = \mathbb{Z}_+$. Hence, we get a contradiction as S must be empty.

($\Longleftarrow$)
Let S be a subset of $\mathbb{Z}_+$ such that $1 \in S$ and $k \in S \Longrightarrow k+1 \in S$. Then suppose that $S \neq \mathbb{Z}_+$. In that case, we know that $S^C \neq \emptyset$, and since $\mathbb{Z}_+$ is well-ordered, we know there is a least element α of S^C.

Because $1 \in S$, we know that $\alpha \geq 2$. But then consider that $1 \leq \alpha - 1 < \alpha$. Therefore, $\alpha - 1 \in S$, thus implying that $\alpha \in S$. This contradicts that $\alpha \in S^C$.

From what I've heard, when defining the positive integers, one usally takes one of the two above properties as an axiom and then proves the other as a theorem. In Munkres' book, he starts with induction and proves well-orderedness.

Facts:

- If A with the order relation $<$ is well-ordered, then any subset of A is well-ordered as well with $<$ restricted to that subset.
- If A has the order relation $<_1$ and B has the order relation $<_2$ and both are well-ordered, then $A \times B$ is well-ordered with the dictionary order.
- Given any countable set A, we know there exists a bijection f from A to $\mathbb{Z}_+$. Hence, given $a, b \in A$, we can say that $a < b \iff f(a) < f(b)$. Then, A is well-ordered by $<$ with the least element of any subset S of A being the element $\alpha \in A$ such that $f(\alpha)$ is the least element in $f(S)$.
- If a set A is well-ordered, then we can make a choice function $c : \mathcal{P}(A) \longrightarrow A$ using that well-ordering.

  Specifically, given any $B \subseteq A$, assign $c(B) = \beta$ where β is the least element of B.

  This is why we can pick elements of $\mathbb{Q}$ without worrying about the axiom of choice.

An important theorem (which I will hopefully prove soon) is:

The Well Ordering Theorem: If A is a set, there exists an order relation on A that is well-ordering.

Exercise 10.5: Show that the well-ordering theorem implies the (infinite) axiom of choice.

Let $\mathcal{A}$ be a collection of disjoint sets. By the well-ordering theorem, we can pick an order relation on $\bigcup_{A \in \mathcal{A}} A$ that is well-ordering.

Note that the previous sentence is carefully worded to only make use of the finite axiom of choice. Specifically, the order relation we are picking is an element of some subset of $\bigcup_{A\in\mathcal{A}} A \times \bigcup_{A\in\mathcal{A}} A$.

If we had instead picked a well-ordering for each $A \in \mathcal{A}$, then that would require the axiom of choice as we would be making potentially infinitely many arbitrary choices of order relations.

Now let $C = \{a \in \bigcup_{A\in\mathcal{A}} A \mid \exists A \in \mathcal{A}\ s.t.\ a \in A \text{ and } \forall b \in A,\ \ a \leq b\}$.

Then C fulfils the properties of the set that the axiom of choice would guarentee exists.