Math Journal

Isabelle Mills

September 18, 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 $p \in \alpha, \quad q \in \mathbb{Q}$, 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 $p \in \alpha, \quad q \in \mathbb{Q}$, and $q \notin \alpha$, then $q > p$.
b. If $r \notin \alpha, \quad r, s \in \mathbb{Q}$, 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: $\alpha < \beta, \quad \alpha = \beta$, 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: $\alpha < \beta, \quad \alpha = \beta$, 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 $\gamma = \bigcup\limits_{\alpha \in A} \alpha$. 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 $\alpha \in R$, $\quad \alpha + 0^* = \alpha$.

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 $r \in \alpha, \quad s \in \beta, \quad r > 0$, 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:

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

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:

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

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:

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

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 $\forall A, B \in \mathcal{P}(\mathbb{Z}_+)$, $f(A) = f(B) \Longrightarrow A = B$. 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 $F = \bigcup\limits_{n=1}^{\infty} A_n$.

(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:

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

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.

Plus, some really commonly used theorems require the axiom of choice to prove them. For example, the union of countably many countable sets is countable. This makes it really easy to accidentally use the axiom of choice in a proof.

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 $S^{\mathsf{C}} \neq \emptyset$, 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 $\alpha \in S^{\mathsf{C}}$.

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 $a < b \Longleftrightarrow f(a) < f(b)$. 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.

Note: this theorem requires the axiom of choice to prove.

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

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

9/14/2024

Exercise 10.1: Show that every well-ordered set has the least-upper-bound property.

Let the set A with the order relation $<$ be well-ordered. Then consider any nonempty $B \subseteq A$ and suppose there exists $\alpha \in A$ such that $b < \alpha$ for all $b \in B$.

Let $U = \{a \in A \mid \forall b \in B,\ \ b \leq a\}$. Since $\alpha \in U$, we know that $U \neq \emptyset$. So, because A is well-ordered, we know that U has a least element β. This β is by definition the least upper bound of B. So $\sup B = \beta$.

Let X be a well-ordered set. Given $\alpha \in X$, let S_α denote the set $\{x \in X \mid x < \alpha\}$. We call S_α the section of X by α.

Lemma 10.2: There exists a well-ordered set A having a largest element Ω such that S_Ω is uncountable but every other section of A is countable.

Proof:
Starting off, let B be an uncountable well-ordered set. Then let C be the well-ordered set $\{1, 2\} \times B$ with the dictionary order. Clearly, given any $b \in B$, we have that $S_{(2,b)}$ is uncountable. So the set of $c \in C$ such that S_c is uncountable is not empty.

Let Ω be the least element of C such that S_Ω is uncountable. Then define $A = S_\Omega \cup \{\Omega\}$. This is called a minimal uncountable well-ordered set.

The reason we are considering $\{1, 2\} \times B$ instead of just B is that if we were just considering B, then we wouldn't be able to guarentee that there exists $b \in B$ such that S_b is uncountable.

User MJD on https://math.stackexchange.com wrote some good intuition for why this is.

While the set $\mathbb{Z}_+$ is countably infinite, all sections S_x of $\mathbb{Z}_+$ are finite. However, when considering $\{1,2\} \times \mathbb{Z}_+$ with the dictionary order, we have that $S_{(2,1)}$ is countably infinite. Furthermore, all sections of $S_{(2,1)}$ are finite. Thus, $S_{(2,1)}$ would be a minimal *countable* well-ordered set.

We call a set described by lemma 10.2 $\overline{S}_\Omega = S_\Omega \cup \{\Omega\}$.

Theorem 10.3: If A is a countable subset of S_Ω, then A has an upper bound in S_Ω.

Proof:
Let A be a countable subset of S_Ω. For all $a \in A$, we know that S_a is countable. Therefore, $B = \bigcup\limits_{a \in A} S_a$ is also countable, meaning that $S_\Omega - B \neq \emptyset$.

If we pick $x \in S_\Omega - B$, we must have that x is an upper bound to A because if $x < a$ for some $a \in A$, we would have that $x \in S_a \subseteq B$.

If you combine this with exercise 10.1, we know that A has a least upper bound.

Exercise 10.6: Let S_Ω be a minimal uncountable well-ordered set.

(a) Show that S_Ω has no largest element.

Suppose $\alpha \in S_\Omega$ is the largest element of S_Ω. In that case, we'd have that $S_\alpha = S_\Omega - \{\alpha\}$. However, by theorem 10.3, we know that S_α is countable. This implies that $S_\Omega = S_\alpha \cup \{\alpha\}$ must also be countable, which is a contradiction.

(b) Show that for every $\alpha \in S_\Omega$, the subset $\{x \in S_\Omega \mid \alpha < x\}$ is uncountable.

Let $\alpha \in S_\Omega$. By the law of trichotomy, we know that:

$$S_\Omega = \{x \in S_\Omega \mid x < \alpha\} \cup \{\alpha\} \cup \{x \in S_\Omega \mid \alpha < x\}.$$

Now suppose $\{x \in S_\Omega \mid \alpha < x\}$ is countable. Then as both $\{x \in S_\Omega \mid x < \alpha\}$ and $\{\alpha\}$ are countable, we have a contradiction as the three's union must also be countable. But we know S_Ω isn't.

Some definitions I've been lacking:

1. Let A be a set and suppose x, y, z are any three different elements of A.

Simple [Default] Order Relation: $(<)$	Strict Partial Order Relation: $(\prec)$
Nonreflexivity: $x \not< x$ Transitivity: $x < y$ and $y < z \Rightarrow x < z$ Comparability: $x < y$ or $y < x$ is true	Nonreflexivity: $x \not\prec x$ Transitivity: $x \prec y$ and $y \prec z \Rightarrow x \prec z$

Basically, a partial order relation is allowed to not give an order for some pairings of elements. If someone just says a set is ordered, they mean the set is simply ordered.

2. Let A and B be sets ordered by $<_A$ and $<_B$ respectively. We say that A and B have the same order type if there exists an order-preserving bijection $f : A \longrightarrow B$, meaning that $\forall a_1, a_2 \in A, \;\; a_1 <_A a_2 \Longrightarrow f(a_1) <_B f(a_2)$.

   It is trivial to show that if f is an order-preserving bijection, then f^{-1} is also an order-preserving bijection.

3. If A is an ordered set and a and b are two different elements, then consider the set $S = \{x \in A \mid a < x < b\}$. If $S = \emptyset$ we say that b is the successor of a and a is the predecessor of b.

Exercise 10.2:

(a) Show that in a well-ordered set, every element except the largest (if one exists) has an immediate successor

Let A be a well-ordered set and let α be any element in A such that there exists $\beta \in A$ for which $\alpha < \beta$. Then consider the set $S = \{x \in A \mid \alpha < x < \beta\}$. If $S = \emptyset$, then we know α has β as its successor. Meanwhile, if $S \neq \emptyset$, then since A is well-ordered, we know that A has a least element γ. Thus, the set $\{x \in A \mid \alpha < x < \gamma\} = \emptyset$ and we know that γ is the successor of α.

(b) Find a set in which every element has an immediate successor that is not well-ordered.

Consider the set $\mathbb{Z}$ of all integers using the standard ordering. Then for any $n \in \mathbb{Z}$, we know that its successor is $n + 1$. At the same time though, the set of all negative integers has no least element. So $\mathbb{Z}$ is not well-ordered by $<$.

Exercise 10.6:

(c) Let X_0 be the subset of S_Ω consisting of all elements x such that x has no immediate predecessor. Show that X_0 is uncountable.

Suppose X_0 is bounded above by some $\alpha \in S_\Omega$. Thus, there is a predecessor $x \in S_\Omega$ for any y in the set $T = \{z \in S_\Omega \mid z > \alpha\}$.

Now define a function $f : \mathbb{Z}_+ \longrightarrow T$ such that $f(1) =$ the least element of T and $f(n) =$ the successor of $f(n-1)$ for all $n > 1$. We know this function is well-defined because S_Ω has no largest element according to exercise 10.6.a. So, all elements of S_Ω and thus T have a successor by exercises 10.2.a, meaning our formula for $f(n)$ is always defined no matter what $f(n-1)$ is. Hence, the principle of recursive definition guarentees a unique f exists.

Now it's easy to show that f is injective. For suppose that given some $x, n \in \mathbb{Z}_+$ we had that $f(x) = f(x+n)$. Then that would mean that:

$$f(x) < f(x+1) < \cdots < f(x+n-1) < f(x+n) = f(x)$$

Hence we have a contradiction as $f(x) < f(x)$.

Next, we show that f is surjective. Suppose the set $R = T - f(\mathbb{Z}_+) \neq \emptyset$. Then since S_Ω and hence T is well-ordered, we know that R has a least element β. But note that β has a predecessor γ which isn't in R. More specifically, since we know that the least element of T is in $f(\mathbb{Z}_+)$, we know that γ is at least the least of element of T. So $\gamma \in T$.

Thus we conclude that $\gamma \in T - (T - f(\mathbb{Z}_+)) = f(\mathbb{Z}_+)$, meaning there exists N such that $f(N) = \gamma$. But this means that $f(N+1) = \beta$, which contradicts that β is the least element of R.

With that, we've now shown that $f : \mathbb{Z}_+ \longrightarrow T$ is a bijection, meaning that T is countable. However, this contradicts exercise 10.6.b. which asserts that T is uncountable.

Therefore, we conclude that X_0 cannot be bounded above. And by theorem 10.3, that means that X_0 can't be a countable subset of S_Ω.

Exercise 10.4:

(a) Let $\mathbb{Z}_-$ be the set of negative integers in the usual order. Show that a simply ordered set A fails to be well-ordered if and only if it contains a subset having the same order type as $\mathbb{Z}_-$.

($\Longleftarrow$)
If for some $B \subseteq A$, we have that $f : \mathbb{Z}_- \longrightarrow B$ is an order preserving bijection, then we must have that B has no least element. Hence, not all subsets of A have a least element, meaning that A is not well-ordered.

($\Longrightarrow$)
If A is not well ordered, then we know there is a set $B \subseteq A$ with no least element. Now using the axiom of choice, choose any $\beta_1 \in B$. Then for all $n > 1$, choose $\beta_n \in B_{\beta_{n-1}}$. In other words, choose $\beta_n \in B$ such that $\beta_n < \beta_{n-1}$.

Finally, define $f : \mathbb{Z}_- \longrightarrow \{\beta_n \mid n \in \mathbb{Z}_+\}$ by the rule: $f(n) = \beta_{-n}$. This f is an order preserving bijection. Thus, the set $\{\beta_n \mid n \in \mathbb{Z}_+\} \subseteq A$ has the same order type as $\mathbb{Z}_-$.

(b) Show that if A is simply ordered and every countable subset of A is well-ordered, then A is well-ordered.

It's easy to show the contrapositive of this statement.

If A is not well-ordered, then by part a. we know there exists a set $B \subseteq A$ and a function $f : \mathbb{Z}_- \longrightarrow B$ that is an order-preserving bijection. Clearly, B has no least element. Also, the function $g(n) = f(-n)$ gives a bijection from $\mathbb{Z}_+$ to B, meaning that B is countable. Hence, we have shown that B is a countable subset of A that is not well-ordered.

Let J be a well-ordered set. A subset J_0 of J is said to be inductive if for every $\alpha \in J$, we have that $(S_\alpha \subseteq J_0) \implies \alpha \in J_0$.

Exercise 10.7: (The principle of transfinite induction) If J is a well-ordered set and J_0 is an inductive subset of J, then $J_0 = J$.

Proof:
Suppose $J_0 \neq J$. That would mean the set $J - J_0$ is nonempty. So let α be the least element of $J - J_0$. We know that S_α must be disjoint to $J - J_0$, meaning that $S_\alpha \in J_0$. But then by the inductiveness of J_0, we must have that $\alpha \in J_0$. This contradicts that α is the least element of $J - J_0$.

Exercise 10.10: (Theorem) Let J and C be well-ordered sets; assume that there is no surjective function mapping a section of J onto C. Then there exists a unique function $h : J \longrightarrow C$ satisfying for each $x \in J$ the equation:

$$(*) \qquad h(x) = \text{smallest element of } C - h(S_x).$$

Proof:

(a) If h and k map sections of J or all of J into C and satisfy $(*)$ for all x in their domains, then $h(x) = k(x)$ for all x in both domains.

Proof:
Suppose not. Let y be the smallest element of the domains of h and k for which $h(y) \neq k(y)$. Then note that $\forall z \in S_y$, we must have that $h(z) = k(z)$. Thus, we get a contradiction since:

$$h(y) = \text{smallest}(C - h(S_y)) = \text{smallest}(C - k(S_y)) = k(y).$$

(b) If there exists a function $h : S_\alpha \longrightarrow C$ satisfying $(*)$, then there exists a function $k : S_\alpha \cup \{\alpha\} \longrightarrow C$ satisfying $(*)$.

Proof:
Since there is no surjective function mapping a section of J onto C, we know that $C - h(S_\alpha) \neq \emptyset$. Hence, we can define $k(x) = h(x)$ for $x < \alpha$ and $k(\alpha) =$ smallest$(C - h(S_\alpha))$.

(c) If $K \subseteq J$ and for all $\alpha \in K$ there exists $h_\alpha : S_\alpha \longrightarrow C$ satisfying $(*)$, then there exists a function $k : \bigcup\limits_{\alpha \in K} S_\alpha \longrightarrow C$ satisfying $(*)$.

Proof:
Define $k = \bigcup\limits_{\alpha \in K} h_\alpha$.

We know k is a valid function definition because part (a) guarentees that for all $\alpha_1, \alpha_2 \in K$ greater than x, we have that $h_{\alpha_1}(x) = h_{\alpha_2}(x)$. Plus, given any $x \in \bigcup\limits_{\alpha \in K} S_\alpha$, we know that there is $\alpha \in K$ such that $\forall y \in S_x,\ \ k(y) = h_\alpha(y)$. This shows that k satisfies $(*)$ at any x due to the relevant h_α satisfying $(*)$.

(d) For all $\beta \in J$, there exists a function $h_\beta : S_\beta \longrightarrow C$ satisfying $(*)$.

Proof:
Let J_0 be the set of all $\beta \in J$ for which there exists a function $h_\beta : S_\beta \longrightarrow C$ satisfying $(*)$. Our goal is to show that J_0 is inductive. That way, we can conclude by transfinite induction (exercise 10.7) that $J_0 = J$.

Pick any $\beta \in J$ and suppose $S_\beta \in J_0$.

Case 1: β has an immediate predecessor α.

Then $S_\beta = S_\alpha \cup \{\alpha\}$. So, knowing that h_α satisfying $(*)$ exists, we can use part (b) to define h_β satisfying $(*)$.

Case 2: β has no immediate predecessor.

Then $S_\beta = \bigcup\limits_{\alpha \in S_\beta} S_\alpha$.

And since we assumed that there exists $h_\alpha : S_\alpha \longrightarrow C$ satisfying $(*)$ for all $\alpha \in S_\beta$, we thus know by part (c) that there exists a function from $\bigcup\limits_{\alpha \in S_\beta} S_\alpha = S_\beta$ to C satisfying $(*)$.

Thus in both cases, we have shown that $S_\beta \in J_0$ implies that $h_\beta : S_\beta \longrightarrow C$ satisfying $(*)$ exists. Or in other words, $S_\beta \in J_0 \Longrightarrow \beta \in J_0$.

(e) Finally, we now finish proving this theorem.

Case 1: J has a max element β.

Then since we know there exists $h_\beta : S_\beta \longrightarrow C$ satisfying $(*)$, we can apply part (b) to get a function h from $J = S_\beta \cup \{\beta\}$ to C satisfying $(*)$.

Case 2: J has no max element.

Then $J = \bigcup_{\beta \in J} S_\beta$.

And since there exists $h_\beta : S_\beta \longrightarrow C$ satisfying $(*)$ for all $\beta \in J$, we can thus apply part (c) to get a function h from $J = \bigcup_{\beta \in J} S_\beta$ to C satisfying $(*)$.

9/17/2024

Theorem (The Hausdorff maximum principle): Let A be a set and let $\prec$ be a strict partial order on A. Then there exists a maximal simply ordered subset B of A.

In other words, there exists a subset B of A such that B is simply ordered by $\prec$ and no subset of A that properly contains B is simply ordered by $\prec$.

Proof:
To start out, let J be a set well-ordered by $<$ such that the elements of A are indexed in a bijective fashion by the elements of J. In other words, $A = \{a_\alpha \in A \mid \alpha \in J\}$.

Assuming the well-ordering theorem, we know that J exists. Specifically let J refer to the same set as A but equip J with the well-ordering $<$ that we know exists instead of the partial ordering $\prec$ which we equipped A.

Now our goal is to construct a function $h : J \longrightarrow \{0, 1\}$ such that $h(\alpha) = 1$ if a_α is in our maximal simply ordered subset of A and $h(\alpha) = 0$ otherwise. To do this, we rely on the **general principle of recursive definition**.

> **Theorem: (General principle of recursive definition):**
> Let J be a well-ordered set and C be any set. Given a function $\rho : \mathcal{F} \longrightarrow C$ where $\mathcal{F}$ is the set of all functions mapping sections of J into C, we have that there exists a unique functon $h : J \longrightarrow C$ satisfying that $h(\alpha) = \rho(h|_{S_\alpha})$ for all $\alpha \in J$.
>
> The proof for this is supplementary exercise 1. of this chapter. But I'm not going to do it because it's mostly identical to exercise 10.10.

Given any $\alpha \in J$ and $f : S_\alpha \longrightarrow \{0, 1\}$, define $\rho(\alpha) = 1$ if $a_\alpha \in A$ is comparable to all $a_\beta \in A$ such that $\beta \in f^{-1}(1)$ (the preimage of 1).

Note that a_α is comparable to a_β if either $a_\alpha \prec a_\beta$ or $a_\beta \prec a_\alpha$.

Then by the general principle of recursive definition, we know a unique function $h : J \longrightarrow \{0, 1\}$ exists such that for all $\alpha \in J$, we have that $h(\alpha) = 1$ only when a_α is comparable to all $a_\beta \in A$ such that $\beta \in S_\alpha$ and $h(\beta) = 1$.

Let $B = \{a_\alpha \in A \mid \alpha \in J \text{ and } h(\alpha) = 1\}$. Then given any $a_\alpha, a_\beta \in B$ such that $\alpha < \beta$, we know that either $a_\alpha \prec a_\beta$ or $a_\beta \prec a_\alpha$. Hence, B is simply ordered by $\prec$. At the same time, if $a_\gamma \notin B$, then we know $h(\gamma) = 0$, meaning there exists $a_\alpha \in B$ such that $\alpha < \gamma$ and a_γ is not comparable to a_α. This shows that any set properly containing B is not simply ordered by $\prec$.

Note that the maximal simply ordered subset B is not unique. In fact, choosing a different well-ordering of J is likely to give a completely different maximal simply ordered subset.

Let A be a set and let $\prec$ be a strict partial order on A. If B is a subset of A, we say an upper bound on B is an element c of A such that for every $b \in B$, either $b = c$ or $b \prec c$. A maximal element of A is an element m of A such that for no element a of A does the relation $m \prec a$ hold.

Zorn's Lemma: Let A be a set that is strictly partially ordered. If every simply ordered subset of A has an upper bound in A, then A has a maximal element.

Proof:
By the Hausdorff maximum principle, there exists a maximal simply ordered subset B of A. Let c be an element of A that is an upperbound to B. We claim that c is a maximal element of A. For suppose there exists $d \in A$ such that $c \prec d$. Then by the transitivity of $\prec$, we know that $b \preceq c \prec d \Longrightarrow b \prec d$ for all $b \in B$. Hence, $B \cup \{d\}$ is simply ordered by $\prec$. But this contradicts that B is a maximal simply ordered subset of A.

Exercise 11.1: If a and b are real numbers, define $a \prec b$ if $b - a$ is positive and rational.

- It's easy to show that $\prec$ is a strict partial order. After all, for all $a \in \mathbb{R}$, we have that $a - a$ is not positive. Also, if $a \prec b$ and $b \prec c$, then we know that $b - a = p$ and $c - b = q$ where $p, q \in \mathbb{Q}_+$. But then $c - a = c - b + b - a = p + q \in \mathbb{Q}_+$. So $a \prec c$.

- Clearly, given any $x \in \mathbb{R}$, the maximal simply ordered set containing x is the set $\{x + p \mid p \in \mathbb{Q}\}$.

Tangent: I never got around to writing this down last quarter. So here's a proof that assuming the axiom of choice, non-Lebesgue measurable sets exist.

Let $\mathcal{B}$ be the collection of sets of the form $S_x = [0,1] \cap \{x + p \mid p \in \mathbb{Q}\}$ where x is any real number. Obviously, all the sets in $\mathcal{B}$ are nonempty. We also claim that all the sets in $\mathcal{B}$ are disjoint. For suppose $S_x, S_y \in \mathcal{B}$ and $S_x \cap S_y \neq \emptyset$. Then fix $c \in S_x \cap S_y$ and consider any $a \in S_x$ and $b \in S_y$.

We know $c - x = p_1$, $a - x = p_2$, $c - y = q_1$, and $b - y = q_2$ where $p_1, p_2, q_1, q_2 \in \mathbb{Q}$. Thus, we have that $a - y = (a-x) + (x-c) + (c-y) = p_2 - p_1 + q_1 \in \mathbb{Q}$. Similarly, we have that $b - x = (b-y) + (y-c) + (c-x) = q_2 - q_1 + p_1 \in \mathbb{Q}$. This tells us that $a \in S_y$ and $b \in S_x$. And since this works for all $a \in S_x$ and $b \in S_y$, we thus must have that $S_x = S_y$.

Now using the axiom of choice, let V be a set containing one element from each set in $\mathcal{B}$.

To show that V is nonmeasurable, we'll reach a contradiction by supposing V is measurable. Let $q_1, q_2, \ldots$ be an enumeration of all the rational numbers in the set $[-1,1]$. Then having defined $V + q_n = \{v + q_n \mid v \in V\}$, consider the set: $\bigcup\limits_{n \in \mathbb{Z}_+} (V + q_n)$.

Obviously, since $V \subseteq [0,1]$, we know that $\bigcup\limits_{n \in \mathbb{Z}_+} (V + q_n) \subseteq [-1,2]$.

Also, consider any $x \in [0,1]$ and let v be the element of V which was chosen from the set $S_x \in \mathcal{B}$. Then $v - x = p$ where p is some rational number in $[-1,1]$. So, we also know that $[0,1] \subseteq \bigcup\limits_{n \in \mathbb{Z}_+} (V + q_n)$. This means that $1 \leq \mu(\bigcup\limits_{n \in \mathbb{Z}_+} (V + q_n)) \leq 3$.

But now note that for any $n, m \in \mathbb{Z}_+$, we have that $n \neq m \Longrightarrow V + q_n \cap V + q_m = \emptyset$. To prove this, assume $V + q_n \cap V + q_m \neq \emptyset$. Thus, there would exist $v, u \in V$ such that $v + q_n = u + q_m$. In turn, we'd have that $v - u = q_m - q_n \in \mathbb{Q}$, which means that $v \in S_u$. However, this contradicts that V has only one element of S_u.

Now since μ is countably additive, we have that $\mu(\bigcup\limits_{n \in \mathbb{Z}_+} (V + q_n)) = \sum\limits_{n=1}^{\infty} \mu(V + q_n)$.

Finally, note that $\mu(V) = \mu(V + q_n)$ for all n. Thus $\sum\limits_{n=1}^{\infty} \mu(V + q_n) = \sum\limits_{n=1}^{\infty} \mu(V)$ is either 0 or ∞.

But this contradicts our earlier finding that the measure was between 1 and 3. So, we conclude that $V \notin \mathfrak{M}(\mu)$. ■

Exercise 11.2:

(a) Let $\prec$ be a strict partial order on the set A. Define a (non-strict partial) relation $\preceq$ on A by letting $a \preceq b$ if either $a \prec b$ or $a = b$. Show that this relation has the following properties which are called the *partial order axioms*:

(i) $a \preceq a$ for all $a \in A$

This is true because $a = a$ for all $x \in A$.

(ii) $a \preceq b$ and $b \preceq a \Longrightarrow a = b$.

Given any $a, b \in A$ such that $a \preceq b$ and $b \preceq a$, if $a \neq b$, then we'd have that $a \prec b$ and $b \prec a$. This gives a contradiction since $a \prec b \prec a \Longrightarrow a \prec a$ which is not allowed.

(iii) $a \preceq b$ and $b \preceq c \Longrightarrow a \preceq c$

Proving this is a matter of considering six rather trivial cases.

(b) Let P be a relation on A satisfying the three axioms above. Define a relation S on A by letting $a\,S\,b$ if $a\,P\,b$ and $a \neq b$. Show that S is a strict partial order on A.

Obviously, $a \not{S}\, a$ for all $a \in A$ since $a = a$ for all $a \in A$. Meanwhile, suppose $a\,S\,b$ and $b\,S\,c$. Then we know that $a\,P\,b$ and $b\,P\,c$, meaning that $a\,P\,c$. So we just need to show that $a \neq c$ and then we will have proven that $a\,S\,c$.

Suppose $a = c$. Then we know that $c\,P\,a$ and $a\,P\,b$, meaning that $c\,P\,b$. But then since $b\,P\,c$, we know that $b = c$. This contradicts that $b\,S\,c$.