[SQUEAKING]

[RUSTLING]

[CLICKING]

CASEY RODRIGUEZ: So here we are again. So I'm going to finish real quick proof of a theorem that I stated last time due to Cantor. So let me recall the setting.

So last time, we were finishing up what I had to say about cardinality, which remember, is a notion of size of sets. And at the end, for a given set A, then we defined the power set of A to be the set of all subsets of A.

And last time, for example, we did several of them or looked at a few different power sets. And simplest example is that the power set of the empty set is the set containing the empty set. In particular, the power has one more element than the empty set. The empty set has no elements. The power set of the empty set has one element, namely the empty set.

And we are looking at this to answer a question which I posed at the end of last class, namely, all the sets we saw from the integers to even numbers to rational numbers, which is on the assignment, all have the same cardinality as the natural numbers. And that's what we call the countably infinite.

And so a question would be, is there any set that is bigger in cardinality then the natural numbers? Is there any set that's uncountable? And so this theorem due to Cantor answers that and more.

And it says the following-- if A is any set, so if A is a set, then the cardinality of A is strictly smaller than the cardinality of the power set of A. And as a consequence is that the natural numbers have smaller size than the power set of the natural numbers, which has smaller size than the power set of the power set of the natural numbers, which is smaller in size than-- and so on. So there are an infinity of infinities. There is an infinity of infinite sizes.

So let's prove this theorem, and it's extremely clever and a bit mind boggling. So first, let me prove that A has cardinality less than or equal to the cardinality of the power set of A. So let A be a set.

First, we can show that the cardinality of A is less than or equal to the cardinality of the power set of A. So we need to find an injection, a one-to-one map from A into the power set of A. And the simplest one to choose is one that takes an element of A to the set containing just that element.

So define f from A into the power set of A by the function that takes x. And this should spit out a subset of A. So this will be the subset that consists solely of x.

And this is clearly one to one. I'll prove this right now. Then we need to prove that if f of x equals f of y, then x equals y, but this is clear from the definition.

Then if f of x equals f of y, this means the set containing x-- this is by the definition of how we've defined little f-- means that the set containing x is equal to the set containing y. But this means x equals y. They both contain one element.

Two sets are equal if and only if one side is an element of the other. That just means x equals y in the set. Thus, f is one to one, which since we found an injective map from A to the power set of A this means--

So now we want to show that they cannot have the same cardinality. We now show that A does not have the same cardinality as the power set of A. And these two statements are what is meant when we write down, recall the definition, of the cardinality of A or size of A being smaller than the cardinality of the power set of A.

So we're going to do this by a proof by contradiction. So that means we're going to assume that this does not hold and arrive at a false statement. So I assume that they do have the same cardinality.

So this is our initial assumption. We're going to derive a false statement from this assumption. And the only way to arrive at a false statement from a given assumption in a logically consistent fashion is that the original statement, namely this, is false. In other words, the thing we want to show is true.

So let's assume they have the same cardinality. What does that mean? Then there exists a bijective function g going from A to the power set of A.

Remember, a bijective function means that G is one to one and onto. One to one meaning different things of A gets mapped to different things of the power set. Onto means everything in the power set gets mapped onto from A.

So really, the fact that it's surjective is the only thing I'm going to use. And I'm going to define a weird set. And we're going to look at this set.

So define a set B. And this is a subset of A. B is a set of all x's in A such that x is not in f of x. This should be g.

So remember, g maps from A to the power set. So for any given x in A, g of x is a subset of A. So the condition to be in B is that this element x is not in the image of itself by G.

And B could be empty. There could be no x's in A that satisfy this. But it's just a subset of A, simply by definition. We're just looking at elements in A that satisfy a certain condition.

So since it's a subset of A, this means that it's a element of the power set of A. This is just how the power set is defined. Remember, it's all subsets of A

So B is an element of the power set of A. Therefore, something gets mapped to B under this map. So since g is surjective, there exists b in capital A such that g of little b equals capital B. So this just follows from the fact that g is a surjection, meaning everything in here must get mapped to by some element in A.

But now, let's take a look at this B guy. There are two cases-- either b is in g of b or b is not in g of b. So b is in g of b.

If b is in g of b, remember this is equal to capital B, by definition. And to be in capital B means that x is not in g of x. So let me just write this again. This means b is in B, which means b is not in g of b. We started off with b and g of b, and ended with b is not in g of b. So we arrive at a false statement in this case.

Then there's one other case-- b is not in g of b. Then if b is not in g of b, this immediately implies, by the definition of little b, meaning g of b is in capital B. So let me write it this way. So if b is not in g of b, then from the definition of capital B, this implies that b is in capital B. That's just from the definition of capital B.

But now capital B is equal to g of little b, which is another contradiction. Because we started with this and ended with this. So what I've really proven is-- so let's ignore this contradiction mark here-- thus, we have shown that b in g of b implies b not in g of b. b not in g of b implies b is in g of b.

So we've proven the statement that b is in g of b if and only if b is not in g of b. And this is a very false statement-- cannot have some object being in the set if and only if it's not in the set. So we've arrived at a false statement. And therefore, our initial assumption which led us there, namely that the cardinality of the set A has the same cardinality as the power set of A, must have been false.

So it feels almost like you're being hoodwinked a little bit with this proof. But to give you some sort of cling or connection back to reality, what's underlying this argument or what's one way of understanding this argument is to think about-- so in some sense, what this argument does is make you talk about being in B while having to also reference B itself. And maybe this seems a bit wild because this is a math course, but you can do the statement just in the English language.

If I am to tell you that I am a liar, then if that statement is true, then what I just said, namely that I am a liar, is false, which means I'm not a liar. Therefore, "I am a liar" implies I'm not a liar. And vice versa-- if I say, "I am a liar," and that statement is false, meaning I'm not a liar, then that statement is true, which implies I am a liar.

So of course, I would not lie to you. I would just give you alternative facts. But that statement is kind of what's underlying this argument. So I'm going to put that there, true or false.

That's the connection to these two things, loosely, or at least the logic is contained in trying to verify this statement. So that's all I'm going to say about cardinality. We're going to move on to the real numbers now.

And so this is really, like I said in the previous lecture, our first real goal of the class is to describe R. namely, what exactly is the set of real numbers? What characterizes the set of real numbers?

And so let me state this as a theorem just completely ahead of time, so that it's there for us. And this is our goal, although we're not going to prove it. Our goal is just to understand what this theorem says.

So this is a complete description of what R is. There exists a unique ordered field containing Q with the least upper bound property, which we denote by R, instead of real numbers. So as you sit there and listen to this, you shouldn't have-- maybe you do, but you really shouldn't expect to have any idea about what this theorem says, what all these words mean.

So our goal for this lecture is to make sense of these words. So the rest you should understand. So our goal for this lecture is to make sense of these words, "ordered field," "least upper bound property." Because these are the two defining characteristics of R.

And I'm not going to prove this theorem. We're just going to take it as a given. We could prove this theorem but it takes quite a bit of time. And I'd rather start studying properties of R than building R. This is not so uncommon in math, that one is not especially interested in the proof of actually why certain things exist, but we are definitely interested in the properties of that thing once we know it exists.

So let's get started on making sense of what this theorem says. Let's start off with ordered stuff. This has ordered field, least upper bound property. Let's start off with what do I mean by order.

We've seen that just a little bit already when we talked about the natural numbers and this well-ordered property of the natural numbers. But I was just using words to label a certain property of the natural numbers. I didn't say they meant anything specifically. It was just a label for that. But when I say "order" now, this will definitely mean something.

So ordered sets and fields definition-- an ordered set is a set S with a relation, which we label with this less than symbol . And this relation satisfies two properties. One is you can always check whether two elements are bigger than each other or equal.

So for all x, y in S, either x equals y, x is less than y, or that's just restating, y is less than x. And if x is less than y, and y is less than z, then x is less than z. So an ordered set is just a set with some relation which has two properties, namely that for any two elements in the set, I can compare the two. That's basically what this says. And I have this transitive property that if x is less than y, and y is less than z, then x is less than z.

And so as I said before, whenever you have some sort of mildly interesting definition, you should definitely try to come up with examples and non-examples. So what's the simplest example of an ordered set? Well, the natural numbers, which we discussed earlier, but also the integers, where I have to define what this relation means.

We say m is less than n, this m is less than n, if n minus m is a natural number. So this is how we define our order. So n is bigger than m if n minus m is a natural number.

And you can check that this is just the usual ordering on z. And that satisfies these two properties. The standard order on Q, namely that we'll say q is less than r if there exist natural numbers, m, n, such that r minus q equals m over n.

So these are just the usual orders of orderings on the integers and rational numbers that you're used to and that you know. I'm just writing out exactly how one would define this order. And you can check just using this definition of these orders that these orders satisfy 1 and 2.

Now, a simple non-example, which I guess you could call it a relation which satisfies 2 but not 1, is the following-- so let's take our set S to be-- and create the power set of the natural numbers. And we define a relation A less than B by A is less than B if A is a subset of B.

So I'm just defining a relation on the power set-- A less than B if A is a subset of B. And maybe I shouldn't even use less than, because this makes you think that it's automatically an order. So let's make it a script-looking less than.

This relation is not an order, though. I keep saying "order," so we usually refer to this relation as an order. So it's clear that it satisfies 2.

Why? Because A is a subset of B. B is a subset of C. Then A is a subset of C, i.e., A is less than C.

It just follows from the definition of what it means to be a subset of the other. If A is a subset of B, that means every element of A is an element of B. If B's an element of C, that means every element of B is an element of C. And therefore, every element of A is an element of C.

So this relation satisfies the second transitive property, but it doesn't satisfy the first. I cannot always measure if one thing is bigger than the other. Why is this?

For example, the set containing 0 does not equal the set containing 1. But neither of these things hold. So for something to be an order, or a set to be an ordered set, it has to have this property that I can always compare two elements of the set.

And for this relation, which seems like it could be an order-- it satisfies the second property-- it does not satisfy the first property because I cannot always compare two subsets of the natural numbers by saying one is a subset of the other. So we just saw that. We have two sets which are not equal, but one is not bigger than the other.

And so one more example, which again, I will leave for you to check that it does satisfy conditions 1 and 2 just based on how it's defined. For example, this is the dictionary ordering of Q Cartesian product Q. I think I wrote this down.

I mean, you should know what the Cartesian product is of two things. But let me just recall that I have two sets. The Cartesian product of A and B, this is the set of all ordered pairs of elements from those sets.

So the dictionary ordering of Q is what? So I need to define this relation which I claim is an order. So we'll say that a, b is less than q, r if one of two things happens. If either a is less than q or a equals q, and b is less than r-- so dictionary ordering or alphabetical ordering of Q.

You can just check and see which is smaller first. If they're both equal, then you check the next letter, and see which one's smaller there. So then this relation that I've defined here is in order on Q cross Q, making it an ordered set.

So this is what an ordered set is. We'll get to an ordered field in just a second. But now, let me define what I mean by this least upper bound property. And this is really what sets R apart from Q.

So we'll see in a minute that both R and Q are ordered fields, so that's not what separates R from Q, the rational numbers. But what does separate R from Q is the second property, the least upper bound property. So if I removed that property, and just said there exists a unique ordered field containing Q, that would just be Q. We don't need to add anything to it. But it's the second property, the least upper bound property, that really separates R from Q.

So to define this, I need to define what a least upper bound is. And this is all in the setting of an ordered set. Let S be an ordered set, and let E be a subset of S.

So I'm going to make a series of definitions here. First, if there exists an element of S-- so not necessarily the set I'm looking at, the subset I'm looking at-- such that for all x in E, x is less than or equal to b. So here, I have this order less than.

Less than or equal to means just what it means in English, either x is less than b or x is equal to b, and the same thing with bigger than or equal to, and so on. But just keep in mind that this ordered set is a general ordered set. You could think of it as the dictionary ordering on Q cross Q.

So if there exists a b such that for all x in E, x is less than or equal to b, then we say that E is bounded above. And this element of b is an upper bound for E. So if I can find some element of my set bigger than everything in this set E, I say E's bounded above, and will be an upper bound.

I also have lower bounds. If there exists b in S such that for all x in E, b is smaller than or equal to everything in E, so b is less than or equal to x, then we say E is bounded below, and b is a lower bound for E. So b sits below everything in E.

Now, we call an element in S the least upper bound for E if it satisfies two conditions. One is, if there's a least upper bound, there should at least be an upper bound. b is an upper bound for E, and it should be, in some sense, the least of all upper bounds.

So if I take any other upper bound, b sub 0 should sit below that one. So an element is the least upper bound for a set E if it's an upper bound and it's the least among all other upper bounds. It sits below every other upper bound.

And in this case, we also say b0 is the supremum of E. And we write b0 equals sup E. Now, this was having to deal with upper bounds.

We can also deal with lower bounds or we also have a definition corresponding to lower bounds for what would be the greatest lower bound. So we call an element of S the greatest lower bound for E if two conditions hold, which is kind of similar to the conditions we had for at least upper bound. Except now for lower bounds, b0 is a lower bound for E, and it is the greatest of all lower bounds. If b is any lower bound for E, then b is less than or equal to b0.

And so there's some Latin name attached to least upper bound, so there's a Latin name attached to the greatest lower bound, which we call the infimum. We also call b0 the infimum of E. And we write b0 equals inf E.

So we have this mildly interesting and complex definition, which means we should look at some examples to get a feel for it. So let's look at some simple examples. So let's take our big ordered set to be Z. And let's take our set E to be minus 1, 0, and 2.

So what about this guy? What is the supremum? What is the infimum?

So really, if I'm going to prove or if I'm going to make a statement something is equal to the supremum or something is equal to the infimum, I should actually give a proof of that, meaning if I say something is an infimum or something is a supremum, then I need to prove that it satisfies these two conditions and these two conditions. But I'm just going over examples, so I will not give a full proof of that. This is just to get some intuition going.

So now, first off, what would be an upper bound for E? Well, 3, 4, 5-- 2 is an upper bound because 2 is bigger than or equal to everything in the set. So 2, 3, 4, 5-- these are all upper bounds for this set E.

But what is the supremum, meaning the least upper bound? That would be 2. If I take anything less than 2 that's not an upper bound because there's something in the set bigger than that. And if I take anything bigger than that, then this is going to be bigger than 2, but 2 is still an upper bound. So 2 is the least upper bound.

Now what about lower bounds? A lower bound would be minus 1, because minus 1 is less than or equal to everything in the set. But then so would be minus 2, minus 3, and so on. But the greatest lower bound would be minus 1.

Now let's do another example. Let's now look at S, the rational numbers, and let's take E to be a set of rational numbers such that 0 is bigger than or equal to-- Q is between 0 and 1 inclusive. So then what are some upper bounds?

Everything in E is less than or equal to 1. So 1 is also a perfectly good upper bound, 3/2, 5/4, 6/5, 7/6. Anything bigger than or equal to 1 is also an upper bound for this set. And the least upper bound would be 1.

So if I were to try to draw Q for this set-- let's not do that-- I usually draw this line is for the real number line, but let's imagine it's Q. So everything bigger than or equal to 1 sits above everything in E. So everything bigger than or equal to 1 is an upper bound, and the least upper bound is 1.

What are some lower bounds? Everything in the set E is bigger than or equal to 0. So 0 is a lower bound. So is minus 1/2, minus 1/3, minus 1/4, minus 1/5, and so on.

But anything less than or equal to 0 is a lower bound. Nothing bigger than 0 can be a lower bound because I can always find some-- so this is not a proof, but this is some explanation. Maybe I should have also said this for the upper bound statement, but anything bigger than 0 is not a lower bound.

Because what if I take some number, call it r, bigger than 0, and less than 1, then r cannot be a lower bound because I can find something in E less than r, namely r over 2. So therefore-- and we're going to do some proofs where we actually have to get our hands dirty and prove something is an infimum or the supremum. So you'll see how that works, but for now, let's just go off of intuition. The infimum of this set is 0.

Now, both of these examples so far have this property that both the sup and the inf belong to the set E that I'm looking at. But this is not necessarily always the case. So I could change this slightly so our universe, the ordered set we're looking in, is still Q, and the subset E is now, let's say, q is bigger than 0 and less than 1.

Then sup of E is still going to be 1, but this is not an element of this set E. It's of course an element of S, this universe we're in, but it's not an element of the set E. And likewise, the infimum is still 0, but it's not an element of E.

So there are situations where you have a set, a subset of an ordered set, which has an infimum and supremum which do not exist in this smaller set you're looking at. Whether or not the supremum or infimum may exist in the universe that you're looking at in the bigger set is an entirely different issue. In fact, that's the next issue we're going to talk about.

So let me just reiterate what we saw a minute ago. So we can be in some ordered set Z or Q, and the smaller set, which we're taking the inf or sup in, it could belong to the smaller set-- for example, in this case 1 and 0 were in the set E-- or not. There is this case where neither of them were in E.

And of course, if I put less than or equal to here, then I would had the inf in E and the sup not in E, and then vice versa. So inf's and sup's of these sets don't necessarily need to belong to that set you're looking at. But they at least existed in the big set Q.

Now, big, ordered sets-- so this ordered set that has this property that the inf and sup of bounded above and below sets exist in the bigger set always-- is what we call an ordered set with the least upper bound property. So the definition-- ordered set S has the least property if every subset of S which is non-empty and bounded above has a supremum in S. So a set has the least upper bound property if every non-empty bounded set has a supremum. And so we could come up with simple examples of sets that do have the least upper bound property.

For example, let's take S to be-- I mean, this is kind of the simplest one-- S with a single element, let's say 0. Here there's no order to put on it. Every element in here is equal to itself. And therefore, every non-empty subset of S is just the whole set, and the supremum would then be that one element. So this is kind of the silliest one you could do.

Let's say you could have two elements. And then if E is a subset of S, E is one of four guys. If E is a non-empty subset of S here, the order is 1, 0 is less than 1.

If E is equal to 0, then sup equals 0. If E is equal to 1, sup E equals 1. And if E is equal to 0, 1, this implies sup E equals 1. So this is in S, this is in S, this is in S. So every subset of S which is non-empty has a supremum in S. So these are not the most interesting examples of sets with this least upper bound property.

So for example, maybe a more interesting one would be if I take S to be, let's say, with the dots here, minus 3, minus 2, minus 1. So let me just write it this way-- minus 1, minus 2, minus 3, minus 4, and so on, with the usual ordering coming from the integers. So minus 2 is less than minus 1, minus 3 is less than minus 2, and so on.

I claim this that does have the least upper bound property. Why? Because if E is a subset of S, E non-empty.

In fact, both of these-- this was always bounded above because there's only two elements. And you can choose the biggest one, 1. Every subset of S is also bounded above by minus 1. So every subset of S is automatically bounded above.

So I just need to check that every non-empty set has a supremum in S. If E is a subset of S and is non-empty, then let me look at the set minus E. This is a label. This is not meant to mean anything always.

This is a label, which is the set of elements minus x. So I take all my elements in E, which is a subset of the negative integers. I take their minuses. This is now a subset of the natural numbers.

And since by the well-ordering property of the natural numbers, there exists an element in minus E such that it sits below everything in minus E for all x in E, which means that for all x in E, x is less than or equal to minus m. And I'll let you think about this just for a minute. But so m is in minus E, therefore minus m is in E.

And m less than or equal to minus x for all x in E implies that for all x in capital E is less than or equal to minus m. And therefore, I found an element actually in the set capital E that's bigger than or equal to everything in the set. You can convince yourself or write down a formal proof, if you like, that this implies that minus m is therefore the supremum.

And so using this trickery of going from one set that's bounded above to a different set, a subset of the natural numbers, you can also show, for example, Z has the least upper bound property, which I'm going to now shorten because those are a lot of things to write. LUBP, least upper bound property-- the integers also have this property.

But the integers are not all that interesting, again, because I cannot divide by an integer and stay in the set. For what we want to do, we want to be able to add, multiply, subtract, and divide. And we can't do that in the integers.

We can do that in the rational numbers. However, Q does not have this property. And we're going to prove this. So this is what we're going to prove in a couple of theorems here, but let me just put this out in front.

Q does not have the least upper bound property. And where does this come from? This comes from the simple fact which if you believe your-- I don't want to call it Greek mythology, but maybe it's Greek mythology strictly speaking-- that some young guy discovered that the square root of 2 is not a rational number and then he got thrown off a cliff.

That's who we have to thank for showing us that Q is not perfect, that it does have this algebraic property which I just referenced-- the fact that you can add, subtract, multiply, and divide and stay within the set. But it does not have square roots of prime numbers, but square root of 2 in it. And this then manifests itself in this least upper bound property by giving an example of a set which is bounded above which does not have a supremum in the set Q.

So basically, if E is the set of rational numbers-- I have not stated a theorem yet, but I'm just telling you what we're about to do-- if E is the subset of rational numbers where positive and q squared is less than 2, then sup E does not exist in the rational numbers. So therefore, we would have found a set which is bounded above which does not have a supremum in the rational numbers. And therefore, the rational numbers do not have the least upper bound property.

So this is what we're going to do. And I'll prove-- state a couple of theorems that spell all this out. So first, I'm going to prove a theorem about a what the supremum of such a set would have to satisfy. So if x is in Q-- this is a statement of a theorem-- if x is in Q, and if x equals the supremum of the set, then x is bigger than or equal to 1, and x squared equals 2.

So we're just saying-- don't try to take this as necessarily contradicting what I wrote there because that was not a statement of a theorem yet. I'm stating this theorem that if I have such a supremum in Q of the set, then it would have to square and give me 2. I'm not saying such an element exists. I'm just saying if there is any element of Q that is the supremum of this set, then it has to be bigger than or equal to 1, and it squares 2.

So let's give a proof of this. And because I don't want to keep writing the set again, so I'm going to use the notation that I used in the comments. Let E be the set that I'm interested in. So this should be-- and suppose we have an element of Q which is the supremum of E.

So first off, what would be one element of E? What's one rational number whose square is less than 2? 1. So since 1 is in E, square is less than 2, and x is the supremum of E, meaning it's an upper bound for E, it must be bigger than or equal to everything an E, in particular for 1. That implies x is bigger than or equal to 1. So that's the first part of the theorem I want to prove.

So now we're going to prove two inequalities to show that x squared is actually equal to 2. We're going to prove-- so this is a common trick in analysis, that if I have two things that I would like to show equal to each other, sometimes a way to show that is by showing one is less than or equal to that. And this is less than or equal to that.

So one side is less than or equal to the other side and vice versa, which immediately implies they must equal each other. So that's what we're going to do. And we're going to now prove that x squared is bigger than or equal to 2. We'll then prove that x squared is less than or equal to 2, and therefore, x squared equals 2.

So to do this, we'll do this by contradiction. So let's assume-- everything else we've done so far is still true, but now we want to prove this statement. So we're going to assume that this statement is false.

I assume that x squared is less than 2. So we'll define a certain rational number, h, which is a smaller of two rational numbers. It's going to be the smaller of 1/2 and 2 minus x squared over 2 over 2x plus 1. And let me just reiterate this is less than 1 because it's the smaller of 1/2 and this number.

Now, when you write a proof, as you'll see, it's going to be magic that somehow this h does something magical. That's not exactly how you come up with proofs. How it comes up is you take an inequality that you want to mess with, you fiddle around with it, and you see that if h is given by something, then it breaks the inequality or it satisfies the inequality, which whichever one you're trying to do.

So since x squared is less than 2, h is positive. It's the minimum of a 1/2 and this number. So if it's a 1/2, it's positive. If it's this one, then it's still positive.

And what I'm going to prove now is that x plus h is in E. Its square is less than 2. This will give us our contradiction, because x is supposed to be an upper bound for E, and therefore, x is supposed to be bigger than or equal to x plus h.

But this is x plus a positive number. x plus a positive number is bigger than x. So how do we do this?

We have to compute the square of this and show it's less than 2. And that's where our choice of h comes from. We compute that x plus h squared-- this is x squared plus 2xh plus h squared-- now this is less than x squared plus 2xh plus h.

Why? Because h times h is less than h since h is less than 1. So this is why we chose h to be less than 1, so that I can get rid of this square, and somehow just have a single h floating around, which I can then use to show x plus h is in E. So when I write the string of inequalities, this thing is supposed to be equal to the next thing. This is not saying x plus h squared is equal to what I'm about to write now.

So this is equal to x squared plus 2x plus 1 times h. Now, h is the minimum of these two numbers. So h is going to be smaller than or equal to this thing.

And so this is 2 minus x squared over 2. Write it this way, so I had what I had before. And then times 2 minus x squared over 2, 2x plus 1.

So now some magic is happening. This cancels with that. And I have 2 minus x squared over 2, which is less than 2 minus x squared, so less than x squared plus 2 minus x squared, because I took a 1/2 of it, equals 2.

So summarizing, we started off with x plus h squared, and we showed it was less than 2. And therefore, x plus h is in E. But if I have an element of E-- let's see where are we on space.

But I have an element of E which is bigger than x. So that implies that x is not equal to the supremum of the set. Remember by definition, something is the supremum if it's an upper bound for the set. Something's not an upper bound if you can find something in the set bigger than b0.

And this is also a good exercise to do when you come across a new definition, is to try and negate it to understand it a little bit better. So let me write here next to b is an upper bound for E-- let me write what this means, actually, here. Let me write this here.

b0 is not-- so what's the negation of being an upper bound-- so not an upper bound for E if there exists an x in E such that x is bigger than b0. So we have found an element-- so going back to our proof, we have found an element of our set E which is bigger than x, which means that x is not the supremum of E, which is a contradiction to our assumption.

These are assumptions for the theorem. So we're always assuming this. So this is a contradiction. Thus our assumption that x squared is bigger than or equal to 2-- I mean less than 2, which is different from our assumptions of the theorem, is false.

So now, we want to prove that x squared equals 2. So we now show x squared equals 2. Since x squared-- so this is not exactly the proof. Just I'm going to rewrite it a little differently so it's maybe clear that instead of showing also x squared is less than or equal to 2, which we know the less than cannot happen, let's just show that x squared cannot be bigger than 2.

Since x squared is bigger than or equal to 2, this means either x squared equals 2, which we want to show, or x squared is bigger than 2. So let's rule out this case. We now show that the case x squared bigger than 2 cannot hold.

So suppose otherwise. We're going to do this-- this is going to be a proof by contradiction, as well. I guess when I say x squared bigger than 2 cannot hold, I'm also saying x squared must be less than or equal to 2. But anyway, so let's show this cannot hold.

So we're going to do this by contradiction, as well. So we're trying to show this cannot hold. So let's assume that it does hold. So that's the negation of what we want to show, which is this statement, that x squared greater than 2 does not hold.

So assume x squared is bigger than 2. So what we're going to do is we're going to find an upper bound for the set E which is strictly smaller than x. And we have to do that next time because I think I'm about to run out of time. So I hate to stop the proof here, but we'll finish this in the next lecture.