[SQUEAKING]

[RUSTLING]

[CLICKING]

CASEY RODRIGUEZ: OK, so let's finish the proof that we started at the end of the lecture last time. I usually don't end lectures in the middle of a proof. But since this lecture and the lecture before will come to you at the same time, I didn't feel so bad about it.

All right, so we were trying to prove this theorem that if there's a rational number so that it's equal to the supremum of the set, then x is bigger than or equal to 1 and its square gives me 2. And so far, what we've shown is that if I have an element, a rational number that is given by the supremum, then it's bigger than or equal to 1 and x squared has to be bigger than or equal to 2.

And so now, we would like to show that, in fact, x squared equals 2. Now, since x squared is bigger than or equal to 2, it's either equal to 2 or bigger than 2. And we want to show that the second possibility is not possible. So we're going to prove that the second possibility is not possible by contradiction. So let's assume that the thing that we say cannot happen does happen and we're going to derive a false statement.

So define h. This is going to be x squared minus 2 over 2x And so note a couple of things that since x squared is bigger than 2, this implies h is bigger than 0, which implies x minus h is less than x. So what is the contradiction going to be? It's going to be that this element x minus h is, in fact, an upper bound for the set E. And this will contradict the fact that x is the supremum. In other words, it's the least upper bound for the set E. There's no upper bound for E that can be less than x.

All right, so we now prove that x minus h is an upper bound for this set E. Now, let's take a look at x minus h squared. Then this is equal to x squared minus 2xh plus h squared.

Now, just given by if we just plug in what h is, this is equal to x squared minus x squared minus 2. So that's putting h in. And then the 2x here cancels with the 2x there. So I just get x squared minus 2 plus h squared, which equals 2 plus h squared. Now remember, h is a positive number. So 2 plus a positive number, this is bigger than 2. So x minus h squared is bigger than 2.

So now, I want to show-- I'm going to use this to show that x minus h is an upper bound for E So let q be in E. q squared is less than 2. Then I have q squared is less than 2, which is less than x minus h squared by what we just proved here. So let me write this out or just summarize that what we proved here was x minus h squared is bigger than 2.

So we have q squared is less than 2 is less than x minus h squared. So that means 0 is bigger than x minus h squared minus q squared. q squared is less than this so than if I just subtract it I get this inequality. So that implies that 0 is bigger than-- now, this is the difference of two squares. So I can write this as x minus h plus q minus q.

Now, if I just write out what x minus h is using the definition of h, this is equal to x squared plus 2 over 2x plus q over x minus h minus q. Now, the product of these two numbers is positive. This number is positive because q is positive. And so that means their sum is positive. So I have something positive times this. So I can divide by this positive thing and keep the inequality. So that implies that 0 is less than x minus h minus q, which implies that q is less than x minus h.

All right, so we started off with an element of E, an arbitrary element of E. And we proved that q is less than x minus h. Thus, for all q in E, q is less than x minus h, which implies that x minus h is an upper bound for E. So let me keep that board for now while I write the last sentence or so of this proof.

So we stated that x minus h is an upper bound for E, which implies since x is the supremum of E, it should be less than or equal to all upper bounds, which implies h is less than or equal to 0. But this is a direct contradiction to h being a positive number. So this is the false statement we ultimately prove.

But the idea is that if x squared is bigger than 2, you can find a lower bound-- I mean an upper bound, which is strictly smaller than x, which contradicts the fact that x is the greatest lower bound for E. But remember, what was our original assumption to begin with in this line of reasoning? That was that x squared is bigger than 2. And that concludes the proof.

All right, so this was a statement about just if I have some element that's a rational number and it's equal to the supremum, then it's square has to be 2. Now, I'm going to prove that basically no such element exists, and therefore that the rational numbers do not have the least upper bound property, which was the discussion above those two lines in that circle on that board up there.

So what's the theorem we're going to prove? The set E as before. So this is a rational number such that q is bigger than 0. q squared is less than 2. It is bounded above and has no supremum in Q. So I'm not just saying that-- so this set E sits inside my ordered set, which is my universe Q. I'm not saying that it doesn't have a supremum in E. I'm saying it doesn't have a supremum in the universe where it sits.

And therefore, the rational numbers do not have the least upper bound property because this set is a set which is bounded above and has no supremum in q. So the first thing I want to show is that this set E is bounded above. Let q be in E. Then q squared is less than 2, which is less than 4. So this tells me 4 minus q squared is positive, which tells me 2 minus q times 2 plus q is positive.

Now, since 2 is positive and q is positive, 2 plus q is positive. So I can divide both sides of this inequality by this, 2 plus q, without changing the inequality, which implies-- I'm just going to flip this inequality. Thus, for all q in E, q is less than 2. So 2 is an upper bound for the set E.

OK, so that proves that the set E is bounded above. So now, I'm going to prove that no supremum mom exists by using the previous theorem, which says if I have a supremum, then its square must be 2. OK, so now, we show that the sup of E does not exist. And we do this by contradiction.

Now, I know it seems like a lot of the proofs we're doing are by contradiction. This should not give you the impression that all proofs should be done by contradiction. Many proofs that you will do in the homework can be done directly, meaning not by contradiction.

For example, this first little proof that E is bounded above, this is a direct proof, meaning I prove directly that it's bounded above. I do not assume that it's not bounded above and arrive at a contradiction. But proof by contradiction is very tempting because it at least gets you going somewhere. If you can assume not, then you get to a next step, which this assumption implies something else. And hopefully, you can keep going until you arrive at something false. But many theorems that you want to prove can be done directly.

All right, but not this one. Now, we show the supremum of the set does not exist. So by contradiction, so we will assume that such a supremum does exist. So suppose the supremum exists and call it x. All right, so x is the supremum arm of the set.

OK, so by the previous theorem, since x is an element of the rational numbers, whose square gives me-- which is the supremum of the set, then x is bigger than or equal to 1 and its square is 2. By the previous theorem, x is bigger than or equal to 1 and x squared equals 2. In fact, x has to be bigger than 1. It cannot equal 1 because the square would give me 1 not 2. All right, so I can make that statement that x is, in fact, bigger than 1, not just bigger than or equal to.

OK, so thus, since x is a rational, there exists m in natural numbers such that m is bigger than n and x is equal to m over n. So that just-- that's what it means for x to be a rational number and for it to be bigger than 1.

Thus, there exists an n such that n times x is a natural number. All right, just multiplying through by n, that means that n times x is equal to m, which is a natural number. So let S be the set of natural numbers so that when I multiply x by k I get a natural number. And so what we've shown, just based on our assumption, is that S is non-empty because n is in S

Now, this is a subset of natural numbers. So by the well-ordering property of N, this set S has a least element, which we'll call k0 in S. So what I'm going to show is that, in fact, this little guy k0 is not, in fact, the least element of this set S, which would contradict exactly how it's defined.

So define k1 to be k0 x minus k0. And note this is an integer. Why? Because k0 times x-- so k0 is in the set S, meaning k0 times x is a natural number. So it's an integer. k0 is a natural number. So the difference of two integers is, again, an integer. So k0 is a natural number. k0 times x is a natural number. So the difference of two natural numbers gives me an integer. But in fact, it's a natural number.

So it's a natural number. So let's go over here. So far, we have that k1 is a natural number. And I'm going to prove that k1 is actually less than k0. So since x squared equals 2-- I should say-- OK, so let's write it this way. Since x squared is equal to 2, this implies that 4 minus x squared is positive.

I mean, I just wrote down 2. 4 minus x squared is just 2. So this tells me, taking the difference, 2 minus x times 2 plus x is positive. 2 and x are positive. So I can divide this inequality through by this term and maintain the inequality, which implies 2 minus x is positive. And therefore, x is less than 2. So x is less than 2.

Then k1, which remember is k0 times x minus 1, is less than k0. So k0 is a natural number. It's positive. x minus 1 is bounded by 2 minus 1 equals k0. So what we've shown so far is that this number, k1, is a natural number. And it's less than k0. So I guess I don't have to write this positive part.

Now, let's remember what k0 was supposed to be. k0 is supposed to be the smallest element of this set S. It's the smallest natural number so that when I multiply it by x I get another natural number. And from this k0, I constructed a new natural number called k1, which is less than k0 and it's a natural number.

But here comes the fun part. If we compute what x times k1 is, this is, by definition, x times x times k0 minus k0. This is equal to x squared k0 minus x times k0, which equals 2 k0 minus x times k0 because x squared equals 2.

And this last part, this is equal to k0 plus k0 minus x k0, which equals k1. Now, that's a natural number. That's a natural number. This natural number is bigger than this natural number. Therefore, their difference is, again, a natural number.

So this says that x times k1 is a natural number. Thus, k1 is in S and k1 is less than k0, which implies k0 is not the least element in S, which is a contradiction to the fact that it is the least element of S.

So what we've shown is assuming that this set E has a supremum in the rational numbers, then we arrive at a contradiction. So our original assumption must be false. Thus, sup E does not exist.

All right, so this proof is maybe a little different than-- if you've seen a proof of the fact that the square root of 2 is not a rational number, there's a different proof that maybe is a little bit simpler. But this one uses ordering instead to prove it, which I thought was pretty cool. And it's originally due to Dedekind.

OK, so we've discussed one aspect of the real numbers that was in that theorem that I stated earlier, which I'll restate in a minute, namely that it is a set that has the least upper bound property. So I stated that as a theorem. I'm not going to prove that theorem. We just want to understand exactly what sets the real numbers apart.

And one aspect of that-- there were two things. One is that it's an ordered field. And two is that it has the least upper bound property. So we've now discussed what the least upper bound property means. So we just need to fill in one other part about the real numbers, which is the fact that it's an ordered field.

And as I've said before, Q is also an ordered field. R is not special in that respect. But as the theorem stated at the middle of the last lecture, that R is, in fact, the unique ordered field with the least upper bound property. Remember, we've just proven that Q does not have the least upper bound property.

So in some sense, Q is missing stuff. It's missing stuff. It's missing square roots of 2, which is kind of an algebraic thing, namely I can't solve the equation x squared minus 2 equals 0 in the rational numbers. And the fact that it's missing, that you have this kind of algebraic defect manifests itself in this fact that Q is also missing things with respect to an order.

So Q, in short, this is me saying that has holes and R does not. I mean, that is probably the most basic statement one can make about R. And perhaps you heard in high school calculus and you're hearing repeated now, but in a nutshell, I mean, Q has holes and R does not. But this means something very specifically that R has the least upper bound property and Q does not.

All right, so let me talk about what ordered fields are. So first off, I need to define what a field is. So a set F is a field if it has two operations-- plus-- and I'm going to put a dot here in the middle-- times basically, such that you have a list of properties that hold with respect to these operations.

The first is with respect to-- so this is plus, this is times. This is addition, multiplication. So the first condition is that the set is closed with respect to taking sums. So if x y is in F, then x plus y is in F. This operation of additions should be commutative.

Commutativity, I hope that's how you spell it. This means that for all x y in F, x plus y equals y plus x. Associativity, so this is a condition that for all x, y, z in F, if I add x and y and then add , this is equal to adding x to the sum of y and z.

The fourth is that we have what's called an identity element, an additive identity element. There exists an element which I'll label 0 in the set F such that for all x in F, 0 plus x equals 0. And we also have additive inverses, namely for all x in F there exists an element which I call-- which I label minus x in F such that x plus minus x equals 0.

So these are the conditions on addition that should be satisfied for a field. So that's about addition. So the conditions for multiplication are similar. Namely, it needs to be closed with respect to multiplication. So if x y is in F, then x times y is in F.

Multiplication should also be commutative. So I'm just going to abbreviate that commutative as comm. For all x y in F, x times y equals y times x We also have associativity. Let's not shorten it by that. For all x, y, z in F, if I multiply x times y and then multiply it by z, it's the same as taking x and multiplying it by y times z.

The fourth property is the existence of multiplicative identity. There exists an element which I label as 1 in the set F such that for all x in F, 1 times x equals x. And then I also have multiplicative inverses for non-zero elements. For all x in F, take away 0-- so for everything in the field that's non-zero-- there exists an element which I call x to the minus 1 in F such that x times x to the minus 1 equals 1.

Now, these are statements about the two operations. There's one last assumption in the definition that connects the two. And that's the distributive law, namely that for all x, y, z in F, if I take x plus y times z, this is x times z plus y times z.

So all these conditions-- so a field is a set with two operations, plus and dot, meaning multiplication. And these two operations need to satisfy all of these conditions for my set to be called a field. So the clearest example is, of course, rational numbers with the usual plus and minus, I mean plus and multiplication defined as you learned as a child.

Now, what's a non-example? The integers. So the integers come with plus and multiplication. However, it doesn't satisfy the existence of inverses, of multiplicative inverses in 5, but it does satisfy everything else. And typically, one would call z what's called a commutative ring, commutative because multiplication is also commutative.

But a ring in general does not necessarily have to satisfy multiplication. Being commutative, for example, the set of say 2 by 2 matrices form a ring. What's an example of another? What's another example of a field? Well, we have-- maybe I should have given this one first-- Z2, which is the simplest field there is. It's just the element of two-- it's just a set of two elements, 0 and 1, where I need to define what 1 plus 1 is, 1 plus 1 defined to be 0.

And 1 plus 1 is 0. And yeah, that's it. I mean, 0 times 0 would be 0. 0 times 1 would be 0. 0 plus 0 would be 0. And that gives you all of the rules you need to know to be able to define multiplication and addition on this set of these two elements.

This is a field because what is the inverse of 1? Well, it's just 1. And you can check that if I define addition by this rule along with the other rules that-- and along with-- that these defining plus and multiplication this way satisfies all the conditions of being a field.

A more non-trivial example would be, let's say, Z3. This is a set 0, 1, 2. Only now, the arithmetic-- so I didn't use such a fancy word here. But arithmetic is done mod 3 here. Here, it was mod 2, meaning if I want to add two elements, I add them, and then I take the remainder of that sum after dividing by 3.

So here, addition is defined mod 3. So if something is a multiple of 3, then I equate it to 0. So for example, 1 plus 2, which gives me 3, it's a multiple of 3. This is defined to be 0. 2 times 2, which equals 4, which equals 3 plus 1, multiples of 3 are 0. So that gives me 1.

In particular, this tells me that in this field, 2 times 2 equals 1. So the multiplicative inverse of 2 is given by itself, 2, all right? And a times b equals, let's say, d mod 3, all right? OK, so that's another example of a field. In fact, if you take mod p where p is a prime, you get another field. You get a finite field. So these are examples of what are called finite fields because exactly that-- they are fields and they have a finite number of elements.

Now, OK, based on just these assumptions that you assume your field to satisfy-- I mean, for it to be a field, you can prove all of the simple algebra statements that you've ever known simply from these axioms of fields. So for example, let me just give you the silliest example of a statement you can prove just using these elements-- I mean, these axioms.

You can prove the statement that for all x in F-- so F is a field here. So F throughout will be-- if x is a field, then for all x in F, 0 times x is 0. All we know about 0 is that, when you add it to x, you get x back. Actually, this should have been-- yeah, yeah, this is wrong. This should have been x.

Let me make sure there's no other errors. I don't think there are. That's another danger about not being able to lecture in person, is that errors on the board persist.

OK, so you can prove this blockbuster theorem just using these axioms. So let's do a quick proof of this. If x is in F, then 0 is equal to 0 times x plus the additive inverse of 0 times x because that's just the definition of the additive inverse. Every element has an additive inverse.

And now, 0 is equal to 0 plus 0 times x plus, again, the additive inverse of x. And now, I use the distributive law. This is 0 times x plus 0 times x plus the additive inverse of 0 times x. And that cancels with that. And I get 0 times x. So I started off with 0 and I arrived at it's equal to 0 times x, all right?

And you can prove other simple algebraic statements using these axioms as well. I think I'll put it in the assignment. And I'll just state you can also prove things like-- if I want to look at minus x, then this is equal to the additive inverse of 1 times x.

I mean, this is like-- it's not terribly interesting at the start. There are essentially some very deep theorems in algebra that you learn at another point in your life, but that won't be in this class. Actually, today is probably all we're going to talk about fields, which are algebraic things.

Algebraic things are, to me, nice because somehow you always deal with equality. So how hard could it be to prove two things are equal to each other? Yet, analysis deals a lot with inequality, which somehow is much more subtle. But that's just a little biased.

OK, so this is what a field is. A field is just, again, a set that has these two operations. What is an ordered field? So it's a field, first off, and which is also an ordered set-- but it can't just-- you can't have two different structures on your field and them not interact for that to be interesting-- so such that the algebraic structure and the order on the field are cohabitating nicely, meaning you have two conditions for all x, y, z in F.

If x is less than y, then x plus z is less than y plus z. And one other condition-- x is positive. Or if x is bigger than 0 and y is bigger than 0, then x times y is bigger than 0. And I just use that terminology anyways right now. But for an ordered field F, if an element is bigger than 0, then we call it positive. Or if it's bigger than or equal to 0, we say x is positive and respectively non-negative.

So non-negative if x is bigger than or equal to 0, positive x is bigger than 0, and then likewise with negative and non-positive. And so the most basic example, again, is Q. Q is an ordered field with the usual order and with the usual algebraic structure on Q.

What is not an example is either one of the two fields I wrote down just a minute ago. So a non-example is this field here, 0, 1. So if I put an order on this, either 0 is less than 1 or 1 is less than 0. So remember, order does not have to necessarily correspond to the fact that 0 you connect to 0 in the integers and that 1 you connect to 1 in the integers. I mean, these are just two elements of a set. And an order would be saying either that element is less than that element or that element is less than that element. So let's consider either cases and suppose we have that order on this set and show that it does not turn this set into an ordered field.

So then either 0 is less than 1 or 1 is less than 0. So let's do the first case, 0 is less than 1. If 0 is less than 1, then what happens if I add 1 to each side? So 1 plus 0 would give me 1. 1 plus one would be 0. And therefore, it is not so less than 1 plus 1. So it does not satisfy the first property.

So if I have an order on Z2, two possibilities-- either 0 is less than 1 or 1 is less than 0. If 0 is less than 1, then, by the definition of addition on this set, if I add 1 to 0, I get 1. If I add 1 to 1, I get 0. And therefore, if I were to add 1 to both sides, I would not get a true inequality because I'm assuming 0 is less than 1. So this condition, number 1, does not hold for this order. And neither does it hold for choosing 1 is less than 0.

By the same logic, then 1-- so 1 plus 1 is not less than-- so this set is not-- this field cannot be turned into an ordered field. And essentially, the same thing that I've done here shows that you cannot have any finite ordered field.

So in general, there are no finite ordered fields. Now, just like we proved the blockbuster statement that 0 times anything in the field equals 0, we can also prove all of the manipulations of inequalities that you use without fear simply from, again, these axioms about an ordered field being a field and also satisfying these two inequalities-- I mean, these two conditions here for it to be an ordered field.

So for example, if F is an ordered field, then if x is an element of f and x is positive, this implies its additive inverse is negative and vice versa. If x is less than 0, then minus x is positive. So I know it's tempting to think, well yeah, just multiply this inequality by minus 1 to get this inequality. But remember, this is really a statement about the additive inverse of x.

So the proof is not hard. If x is positive, then-- well, I could write it this way. I can write it as 0 is less than x. Then by property number 1, I can add anything to both sides and get the same inequality-- and preserve the inequality. Therefore, minus x plus 0 is less than the additive inverse of x plus x.

Now, by the fact that 0 is the additive identity, a4, the left side, is going to be minus x. And by the definition of the additive inverse of x, The right-hand side is going to be 0. And that's it. So what's going in here is this is by a4 and a5. And this previous statement is by 1 in this definition before. And I'm not going to prove this statement as well. It's the essentially the same proof. I add minus x to both sides, which I can do by 1. And then I use a4 and a5 to conclude that x is-- that minus x is positive.

Let me just say See Proposition 1.1.8 in textbook for the other-- let's say for the other proofs of standard inequality manipulations.

So Q is an ordered field. And as I stated before about R, R will also-- R is also an ordered field. But it has a least upper bound property. So maybe you are asking yourself, how about some sort of greatest lower bound property? The least upper bound property is about sups.

Can we make a similar property about infs? Are there sets that have the least upper bound property that don't have, say, a greatest lower bound property, meaning does there exist something has the greatest lower bound property if every non-empty set which is bounded below has an infimum? That's kind of what I'm referring to, even though I haven't written it down.

OK, what is that leading up to? In the setting of ordered fields, there really is no difference between a least upper bound property and a greatest lower bound property. If I have an ordered field which satisfies the least upper bound property, then it also satisfies a greatest lower bound property, which I'll state as a theorem, and then we'll prove.

Let F be an ordered field with the least upper bound property. Now, I'm going to prove that it has, if you like, a greatest lower bound property. Then if A is a subset of F, which is non-empty and bounded below, then inf A exists in F, meaning A has an infimum in the set F.

OK, so the proof of this is basically-- in some sense, we did something similar when we proved that one set given by all the minus 1, minus 2, minus 3 had the greatest upper bound property or the least upper bound property by taking its minus and then using, in a sense, the greatest lower bound property of the natural numbers, this well-ordering principle, to conclude that that set had the least upper bound property.

And that's what we're going to do here, is we're going to take a set which is bounded below, take its minus, if you like, which is now bounded above, take the sup of that set, which we can do, and show that that's the infimum of that set. So let me write over here. This should be not part of the proof, but some intuition.

And I'll draw it like F is a real number line, which it is because part of the statement about the real numbers is that it's the unique ordered field with the least upper bound property. But don't worry about that for now. Let's imagine we have a set A. And for now, I'll draw it like it's an interval, which is bounded below. So it stops after some point. And there's nothing there.

So it's bounded below, then if I look at minus A-- so here, I'm drawing 0. If I look at minus A, which is the set of elements-- the set of the additive inverses of A, I now have a set which is bounded above. So if this is a lower bound for A, then minus B will be an upper bound for minus A. And therefore, minus A has a least upper bound which, in this picture I'm drawing, looks like x.

And so then my goal is then to show that-- so here, let's go back to B. Here's A. And here's now minus x to show that minus x is an infinum of A. So that's the basic intuition on why this holds.

We're using the ordered field property to be able to take minuses. That's where the field property is coming in. And that minuses-- although we didn't prove this, it is one of those-- essentially, we did prove this, that if I have something positive and I multiply it through by minus 1 using this as well, then that reverses the inequality.

But again, these are short-- unless I'm telling you to prove a certain inequality, simple inequality statement like of this type, just freely use the inequality facts that you remember from high school. And just know that these persist for ordered fields with the least-- or ordered fields in general.

OK, so let's turn this intuition into a proof. Suppose A-- so I am not stating it here, but F is an ordered field with the least upper bound property. I'll go ahead and state it. F is an ordered field with the least upper bound property.

Let A be subset of F, A not equal to an empty set, A bounded below. Then that means there exists an element b in F such that b is less than or equal to a such that, for all a in capital A, b is less than or equal to a.

So I mean, the proof is essentially there and you just need to turn it into English because we're in Massachusetts. If you were in a different country, you'd turn into the language that's spoken there. You just need to turn it into written word. So there exists a lower bound for A.

Let me just note another set called minus-- which I'll label minus A. This is the set of all elements in F of the form minus the additive inverses of A, as a is in capital A. So it's the additive inverse of all elements in capital A. Then the fact that I have for all a in A b is less than or equal to a implies for all a in A, minus a is less than or equal to minus b because multiplying through by minus 1 flips the inequality.

That implies-- so minus b is bigger than or equal to every element of minus A So that implies b is an upper bound for the set minus A. So minus A is a non-empty subset of F, which is bounded above. Therefore, it has a supremum. Thus, there exists an x in F such that x equals sup of the set minus A.

And this is because we are assuming the least upper bound property, that every non-empty set which is bounded above has a supremum. I'm going to show this guy x is, in fact, the infimum of the set A, or minus x is the infimum of A.

So the fact that x is the supremum of minus A implies that for all a in capital A, minus a is less than or equal to x because x is supposed to be the least upper bound. So it's, in fact, an upper bound. So that means that for all a in A-- again, just flipping the inequalities-- minus x is less than or equal to A, which implies minus x is a lower bound for capital A.

We now have to show that minus x is the greatest lower bound of A. If I take any other lower bound of A, then minus x is bigger than or equal to that lower bound. Now show that if-- let's call it something else-- y is the lower bound for A, then y is less than or equal to minus x. And then that concludes the proof showing that minus x is, in fact, the infimum of A. And therefore, A has an infinum. We've actually identified what the infinum is. It's the sup of minus A.

OK, so let y be a lower bound for A. Then exactly how I showed for this single lower bound that I had for A, you can verify this again. Just go through the argument and replace b with y. Then minus y is an upper bound-- just look at the picture, replace b with y-- for minus A, which implies since x is the supremum of A-- so since x is the supremum of minus A, it's the least upper bound. So it has to be less than or equal to minus y.

And flipping the inequality again on that means that y is less than or equal to minus x which is what we wanted to prove. Thus, the inf of A exists. And we've, in fact, showed that it's equal to the sup of minus A. So in an ordered field with the least upper bound property, not only does every set which is bounded above have a supremum, every set which is bounded below has an infimum.

So now, we move on and not talk about generalities, but we're just going to focus on R, the set of real numbers. And I'm just going to, again, state this theorem about the existence of R and its properties, so just to bring this all back to our goal of describing exactly what R is or what separates it from Q is that-- so there exists a unique ordered field with the least upper bound property containing Q. And this field we denote by R.

So Q does-- just to bring this back, so we started off in ancient times with the natural numbers. We moved to the integers so that we could take additive inverses, although they didn't call them that. And we wanted 0. And then we moved to the rational numbers because we didn't have ways to solve the equation 2x plus 1 equals 0.

And so we moved on from Q to R essentially because we can't solve the equation x squared minus 2 equals 0. And this inability to solve x squared minus 2 equals 0, although an algebraic fact, in fact means that Q is incomplete as an ordered set. It does not have this least upper bound property.

And what characterizes the real numbers is that it is an ordered field containing Q. And it's the unique one with the least upper bound property. This unique should be kind of in quotes because unique up to what's called isomorphism. Isomorphism is a fancy way of saying what you call apples I call manzanas, essentially.

OK, so this is what R is. It's the unique ordered field with the least upper bound property containing Q. So I'm not going to prove this theorem. The way you usually prove this theorem, you construct R either as what are called Dedekind cuts or as equivalence classes of Cauchy sequences. We'll talk about Cauchy sequences soon-ish.

But I'm more interested in proving properties about R, and then going on to functions on R, limits, which is what analysis is, is the study of limits, rather than get tied up in really non-analytic facts, algebraic facts trying to construct this R, the actual field. So we're just going to take this as a given. And now, we're going to go from here and start proving facts about real numbers.

Where Q failed, R succeeds. So the first fact is that there exists a unique element in R such that r is positive and r squared equals 2. So we saw before that if I replace this with Q, ta rational number, that's false. There does not exist a rational number whose square is 2. But in the real numbers, there does.

And right now, maybe you're tempted to just say, yeah, you set R equal to square root of 2. Well, what is square root of 2? I mean, how do you come up with that guy? So we have to come up with some element of R whose square is 2. Now, we basically did that a minute ago in the rational numbers. And kind of the same proof works here.

So let E be the set of all x's in R such that x is positive and x squared is less than 2. So earlier in the lecture and at the end of the last lecture, we had q here, right? Well, the same proof, basically And what we did earlier-- then E is bounded above by 2. So R, which I-- so sup E tilde exists in R.

So I have this set. It's bounded above by 2. I mean, we did the proof earlier. So by the least upper bound property of R, the supremum exists. Call this element little r.

Then the same proof-- I'm not going to do it again because we've already done it. And all you need to do is replace q's with r's-- shows r is bigger than or equal to 1. In fact, it's bigger than 1. And r squared equals 2. So there does exist an element of r which is positive and whose square is 2. Now, I will prove that it's unique.

So now, I want to prove that r is unique. That means if I take-- if there's some other element in capital R that satisfies these two inequalities, then it must be equal to my original r. So suppose r tilde is in R. r tilde is bigger than 0. And r tilde squared equals 2.

Then since their square is the same number, namely 2, 0 is equal to r tilde minus r squared, which equals r tilde plus r, r tilde minus r. Now, both r and r tilde are positive. So r plus r tilde is positive. In particular, it's non-zero. So since it's a field, I can therefore divide or multiply both sides by the additive inverse of this thing and arrive at 0 is equal to r tilde minus r or r equals r tilde. So there exist only one element in the real numbers which is positive and whose square is 2.

And I'll put it on the assignment, namely that-- so this shows what? Square root of 2 exists. But you can then show a cube root of 2 exists in R. And we'll not prove this. But you can show, in general, that if x is in R, then x to the 1 over n-- that should say x-- is positive for all natural numbers.

So where Q failed, R succeeds. And it's doing this-- or the fact that it does succeed is not coming from an algebraic property of R. It's coming from this property about its order. All right, we'll stop there.