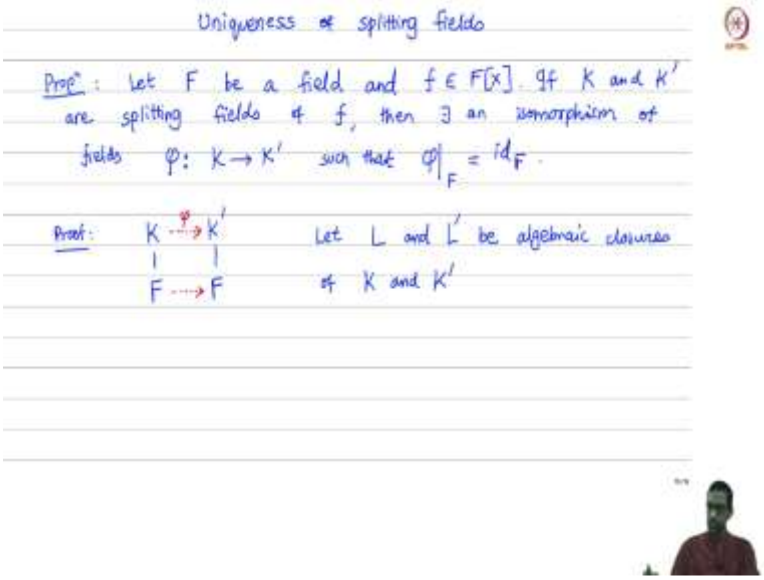
Algebra II
Professor – S. Viswanath
The Institute of Mathematical Sciences
Indian Institute of Technology, Madras
Uniqueness of Splitting Fields

(Refer Slide Time: 00:16)

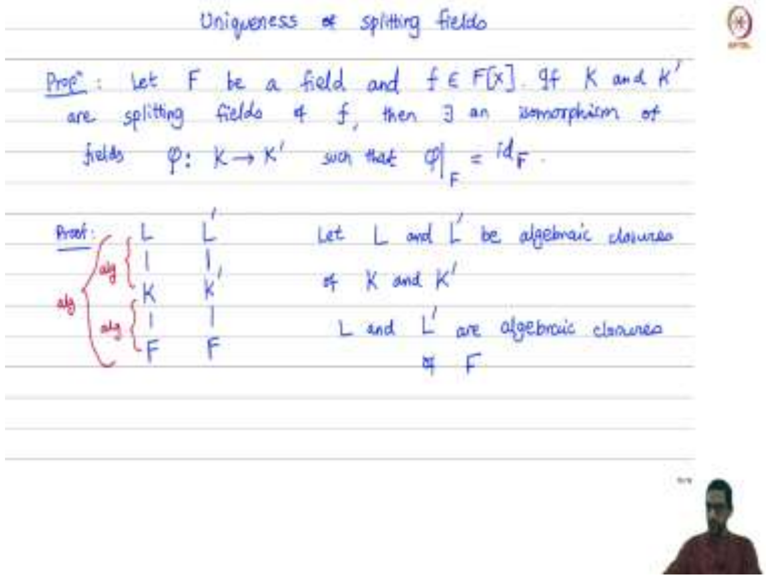


Let us talk about the Uniqueness of Splitting Fields. So, here is a formal statement proposition, let F be a field and small f denote a polynomial. If K and K dash are two splitting fields, are both splitting fields, are splitting fields of f, then they are isomorphic. In fact, more precisely there exists an isomorphism of fields, isomorphism of fields call it phi from K to K dash such that when you restrict that to F, it just gives you the identity map.

So, let us prove this. So, recall, it is good to draw the picture always. So, we have the following picture, the base field is F and I have two extensions K and K dash and they are both splitting fields of the same polynomial. And what we are claiming is that there exists a map, an isomorphism between these two fields, such that when you restrict that isomorphism to F, it just gives you the identity map.

So, that is what we need to show, and you may recall that, a similar thing has already been proved for the algebraic closure. So, let us just use the previous result that something analogous to this holds for algebraic closures. So, let me start by bringing the algebraic closures into the picture. So, let L and L dash be algebraic closures of K and K dash.

(Refer Slide Time: 02:57)

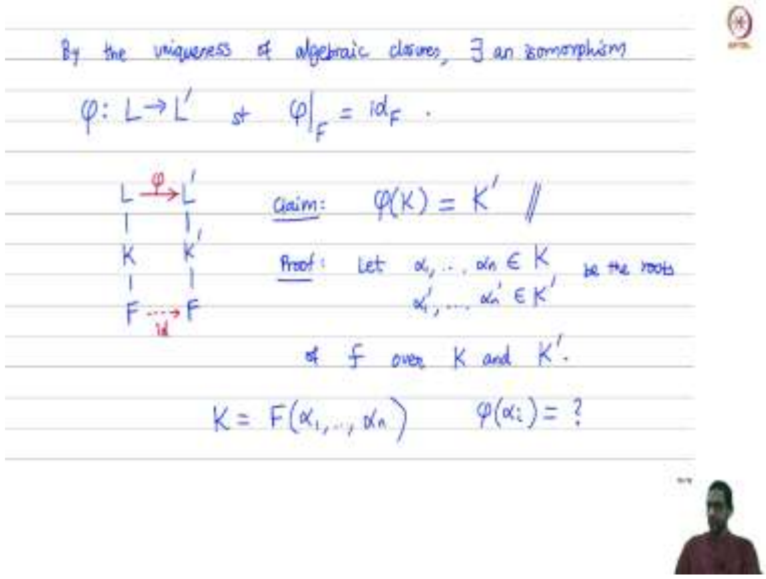


So, which means that my my picture in some sense is the following that narration to this tower of extensions I sort of put one more on top which is L and L dash. So, the additional property here is that L and L dash are algebraically closed. Now, observe that L and L dash are also algebraic closures of F. Why is that?

Because we call what is an algebraic closure, it is an algebraic extension of the base field which is also algebraically closed. So, now, in this case you know K or F is splitting field in particular it is algebraic, in fact, we have shown it is finite. So, this is an algebraic extension. I chose L to be an algebraic closure of K, which means L over K is an algebraic extension.

And we call the tower property of algebraic extensions, if we have, a sequence of algebraic extensions like this then the field on top is algebraic over the field on the bottom. So, this implies L is algebraic over F, an algebraic extension and of course, L is algebraically closed. So, that implies that L is an algebraic closure of the field F itself. So, this tells us that L and L dash are algebraic closures of the same field F.

(Refer Slide Time: 04:23)



And now, we use the uniqueness property by the uniqueness of algebraic closures, what we know is that there exists an isomorphism and isomorphism of fields phi from L to L dash, such that phi when restricted to the base field F is just the identity map on F. So, going back to the picture that we drew already, so this is really our field F, this is the tower here. And now we just go back and put the same thing here.

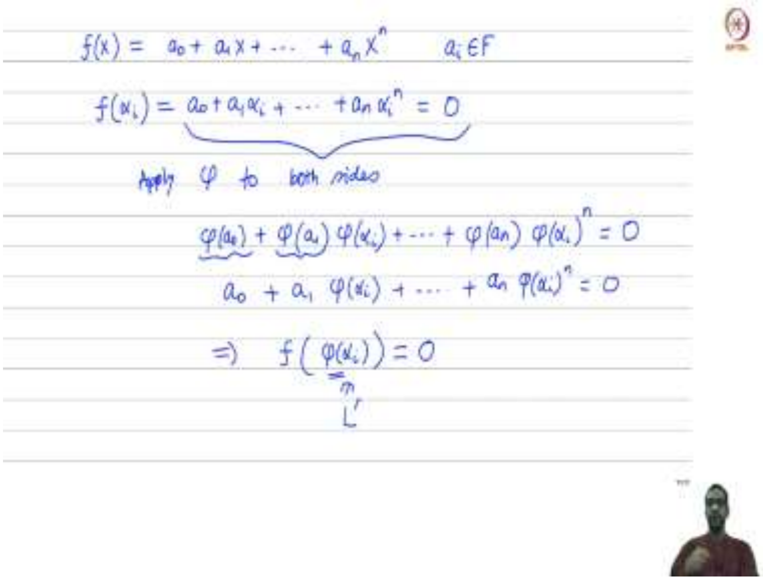
So, what we now know is the following that there is a now, there is now a map. Let us call it phi, such that when you restrict it to F, it gives you the identity. But of course, we wanted to prove the very same fact about K and K dash. And to do that, we simply claim that if you restrict phi to K, well, the image of phi of K is exactly the field K dash.

So, if you prove this, then you are done, because then all you have to do is to restrict the map phi to K, and that restriction will will give you a map onto K dash. So, it will become a it will become a one to one on two map, it will become the isomorphism that we want. So, let us prove this fact. So, the first statement, well, we need to use something about K and K dash. Recall that they are the splitting fields of the polynomial F.

So, we know that F splits over K as well as over K dash. So, let us call the zeroes of F something. So, let alpha 1, alpha n belong to K and alpha 1 dash, alpha 2 dash, alpha n dash be elements of K dash, be the zeroes of F, be the roots of F, be the roots of the polynomial F in or over K and K dash. These are the roots over K and K dash.

Now, we also know because they are the splitting fields that K is generated by F and the roots, K dash similarly is generated by F and the roots. But let us ask. So, K, let us start with K, K we know is generated with, the subfield of K generated by F and the roots of the polynomial F are exactly, is exactly, is just the field K itself. Now, let us ask what can we say about the action of phi on the alpha is? The alpha is a generators. And to determine the the image of phi here, it is sort of enough to work out the image of the generators.

(Refer Slide Time: 07:44)



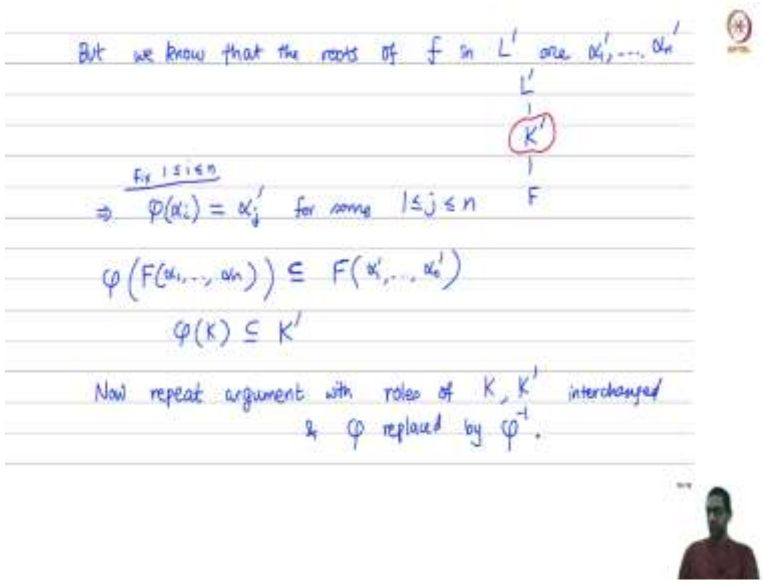
So, observe that what is alpha i alpha i the root of the polynomial F. So, if f of x is a polynomial a0 plus a1x plus bla bla bla, an x power n ai is our all coefficients from F, then what we know is that if you plug in any of the alpha i's, so if you plug in alpha i for x, then that gives me 0. So, in other words, plus x at an alpha i power n is 0. Now, we apply phi to both sides of this equation.

So, we will take this equation and apply phi to both sides. So, phi it will just change this to an equation in L dash rather than L. Now, what what do you get? Well, the left-hand side becomes phi of a naught plus five of a1 alpha i what I write that using the homomorphism property, like this, phi of an phi of alpha i the whole to the n is equal to phi of 0, which is 0 itself. I have used all the homomorphism properties of phi.

And now recall that phi was identity on F. So, phi of a naught is just a naught itself, plus this coefficient phi a1 does not change. It is it is a1 again phi alpha i, and so on. So, this is just going to be an phi alpha i to the n 0. And well, what does that mean?

It just says that the element phi alpha i is again a root of the polynomial F, except of course, phi alpha i in is in, you know, it is on the other side. It is an element of L dash rather than an element of L. But all we are saying is that if you apply you take a root of F in L, and you apply phi to it, what you get is a root of F in L dash.

(Refer Slide Time: 09:55)



Now, but we sort of know what the roots of F in L dash are, but we know that roots of F over the field L dash are exactly the alpha i dashes. Why is that? Well, you may say that well, those are actually the roots of the field F in in K dash rather than in L dash. K dash is a smaller field L dash is larger, but if you know the roots in a smaller field, so, if here are all the roots F splits completely over K dash.

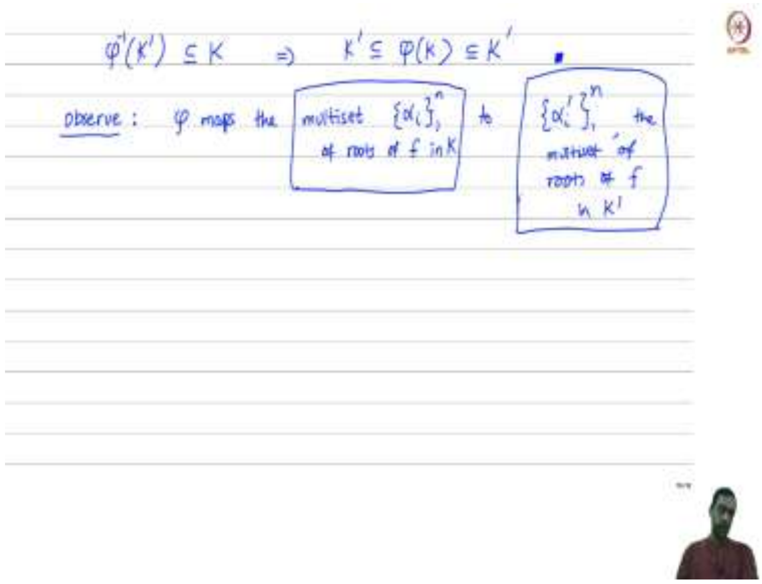
So, all n roots have been obtained, and they are elements of K dash, then when you view the same polynomial as a polynomial over a larger field, the roots continue to be the same. So, you cannot get any any additional roots when you go to a larger extension field because all n roots have already been realised inside K dash.

So, I am just repeating sort of things which you have seen before. But what this implies is the following, this means that when I apply phi on alpha i that is supposed to be one of the roots of F in L dash and therefore, it must be one of the alpha j dashes, for some j between 1 and n. And this is true for each i. So, for each i, so, this is for you fix an i from 1 to n, and you apply phi on the root alpha i, it must be one of the alpha j primes.

So, what this means is that if you if you think about the image of phi, which is what we are trying to compute, if you apply phi to K elements of K are just elements of the extension field F alpha 1, alpha 2, alpha n. Then this is just going to be well, it is going to be a subset if you wish of, so, when you apply phi to this, this is going to be a subset of F adjoined. So, what are the possible images of alpha 1, alpha 2, alpha n under phi, they are just some of the alpha j primes.

So, whatever it is you are going to get an answer which lies inside the subfield of L dash generated by F and alpha 1 dash, alpha 2 dash, alpha n dash. So, this is exactly the statement that phi of K is a subset of K dash, because the right-hand side is exactly K dash. But now, we just sort of repeat the argument with now, repeat the argument with the rolls of K and K dash sort of interchanged, repeat the argument with rolls of K, K dash interchanged. And phi, replaced by the inverse isomorphism.

(Refer Slide Time: 13:22)



So, you just switch the order of everything, just think of K dash to K maps, from K dash to K or maps, from L dash to L and so, and just repeat the same arguments, then what you conclude is that phi inverse now acting on K dash is a subset of K Now, what does this mean? Of course, this says that I can apply phi to both sides of this equation it says K prime is a subset of phi K.

Now, we have already shown the first part of the argument said that phi K was a subset of K prime and that is exactly what we wanted to prove. So, now we are done. So, what we are managed to show is by passing to the algebraic closure and constructing an isomorphism at the level of algebraic closures, that map restricts to an isomorphism between the two splitting fields. So, this proves the uniqueness of the the splitting fields.

And the little fact that came up in the proof is of course, useful observe that what we also showed is that this map between the splitting fields has the following property that phi maps the multiset of roots of F to, so, this is the multiset of roots in over K it maps those to the multiset of roots. So, this is the multiset of roots of F in K, this is mapped to alpha i dash. Which is what? It is just the the multi set of roots of F in K dash.

So, it maps roots, the set of roots or the multi set of roots to the multi set of roots. So that is something that is useful to keep in mind.