**Galois' Theory**
**Professor Dilip P. Patil**
**Department of Mathematics**
**Indian Institute of Science Bangalore**
**Lecture No 56**
**Embeddings**

(Refer Slide Time 00:26)

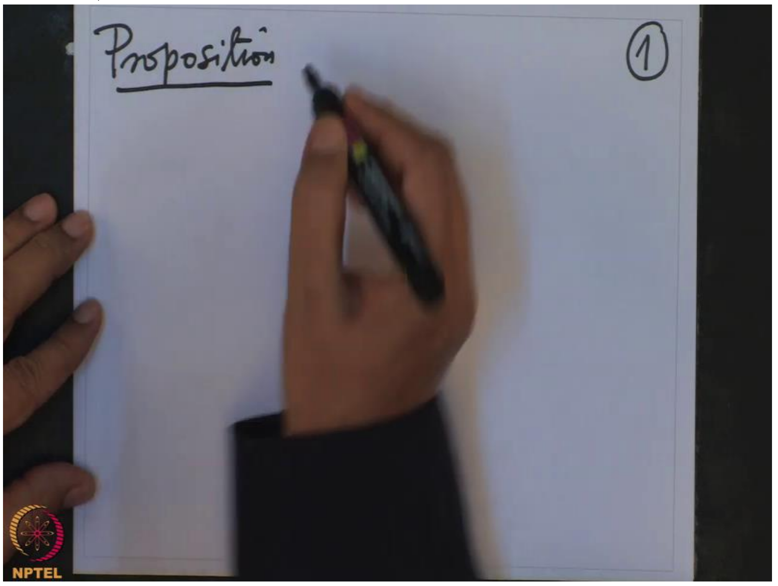

Ok now we prove the proposition which I have stated last time which characterizes

(Refer Slide Time 00:30)


perfect fields in terms of the irreducible polynomial is being separable. So let us recall what we are proving.

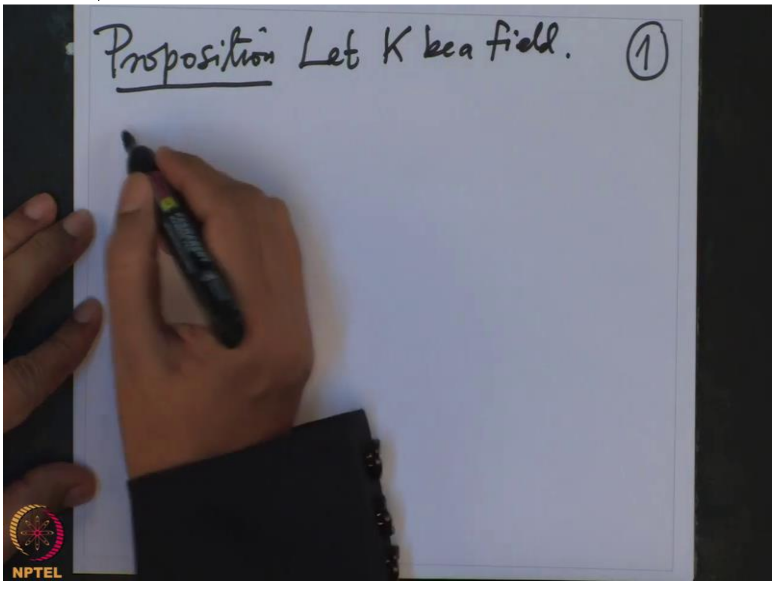
We are proving this proposition.

(Refer Slide Time 00:47)



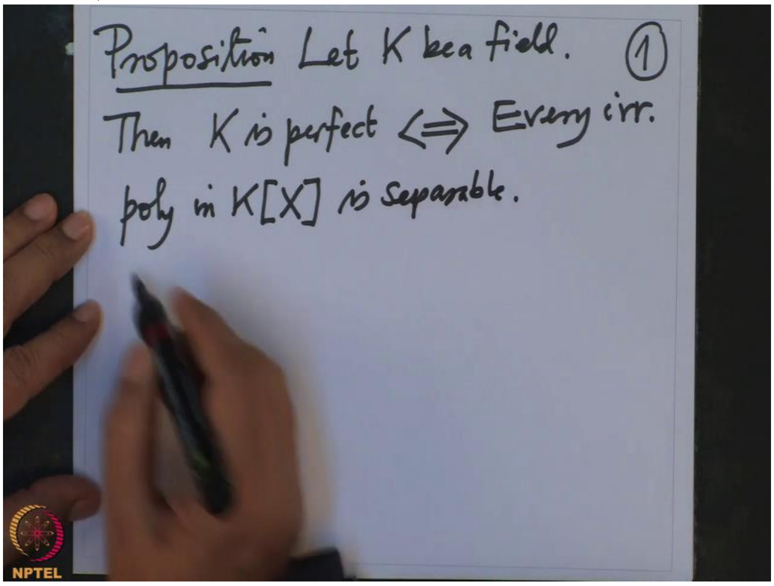

Let K be a field.

(Refer Slide Time 00:55)



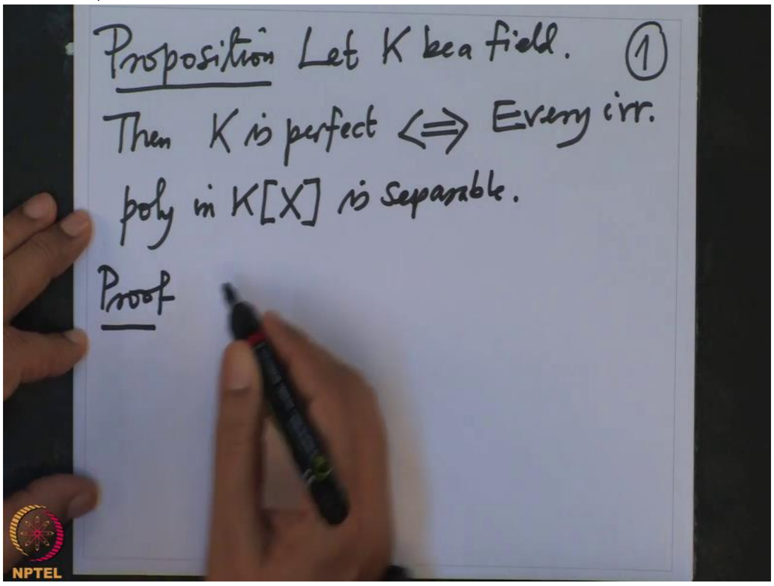

Then K is perfect if and only if every irreducible polynomial in K X is separable.

(Refer Slide Time 01:22)



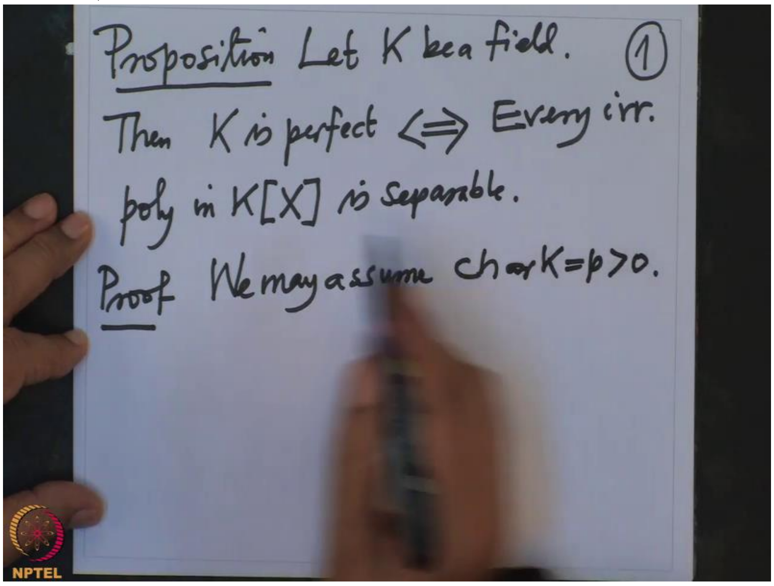

So proof

(Refer Slide Time 01:26)




We may assume characteristic of the field is p positive. Because if the

(Refer Slide Time 01:38)



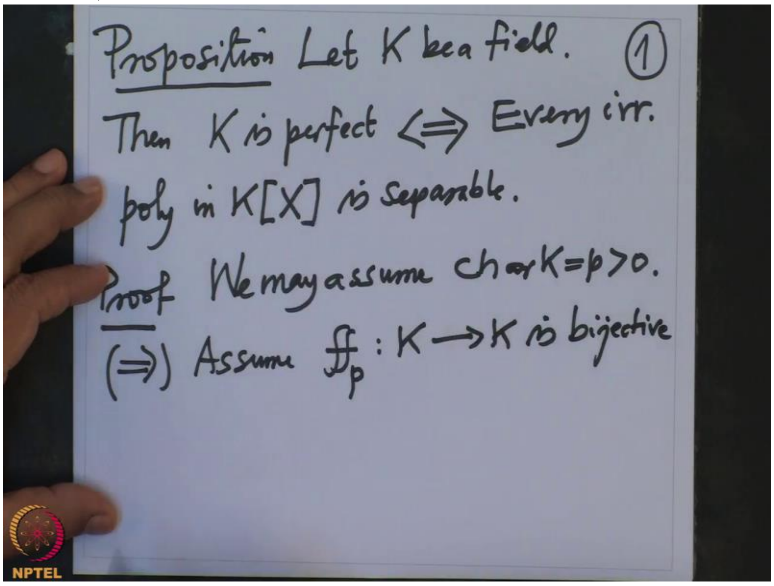

field is characteristic 0 then we know every polynomial, every irreducible polynomial is separable over characteristic 0 field because the derivative is non-zero and then the degree will be strictly smaller than f.

Therefore from there it is clear that irreducible polynomials are separable over characteristic 0 fields. Now therefore we assume characteristic p is positive. Now we will first prove this implication.

That we are assuming K is perfect and we want to show that every irreducible polynomial is separable. So we are assuming K perfect that means we are assuming, assume the Frobenius map which is from K to K is bijective.

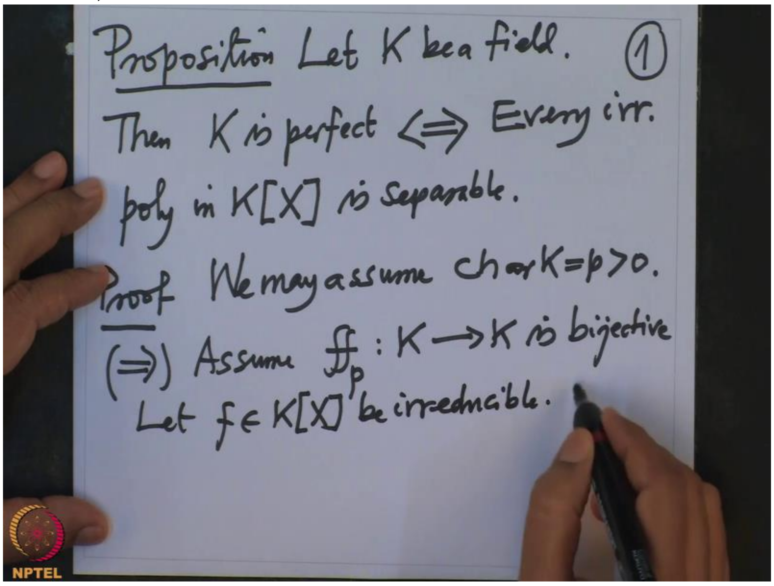
That is the definition we made, perfect definition.

(Refer Slide Time 02:38)



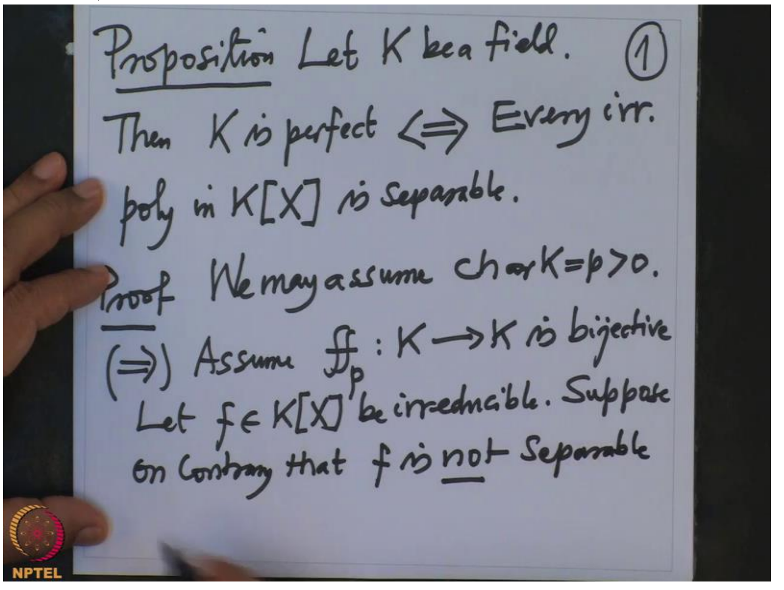

Field is perfect means this Frobenius map is bijective. Now suppose we want to prove what? Every irreducible polynomial is separable. So let f in K X be irreducible.

(Refer Slide Time 03:00)



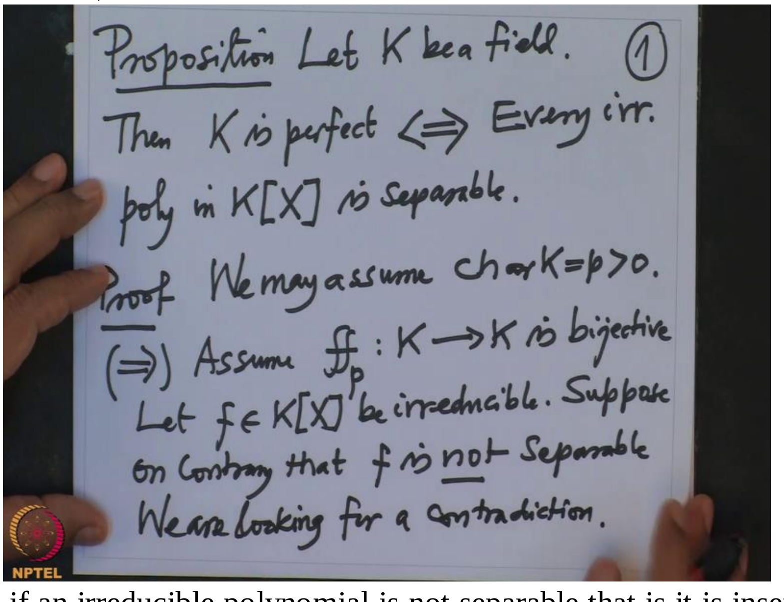

Suppose on the contrary we want to prove that, we want to prove that this f is separable. So suppose on the contrary that f is not separable, then we are looking for a contradiction.

(Refer Slide Time 03:20)



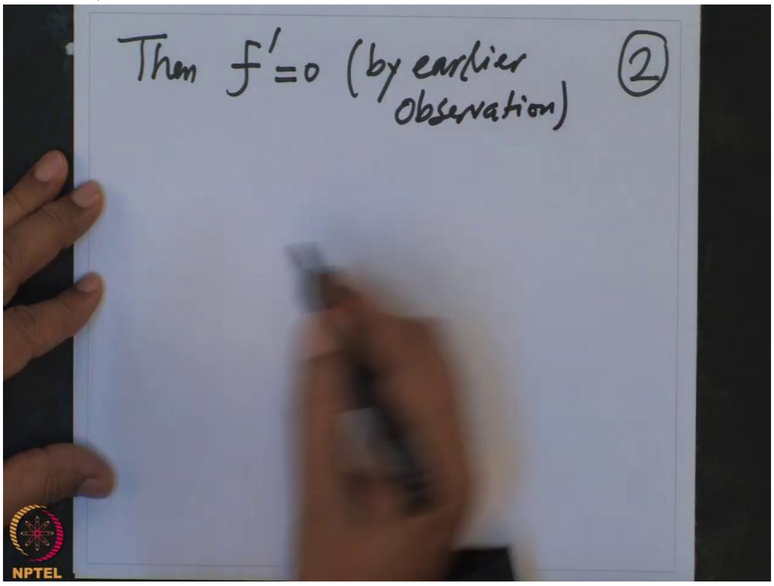

We are looking for, for a contradiction.

(Refer Slide Time 03:33)




So we have seen if an irreducible polynomial is not separable that is it is inseparable then we know f prime has to be 0. This is by earlier observation.

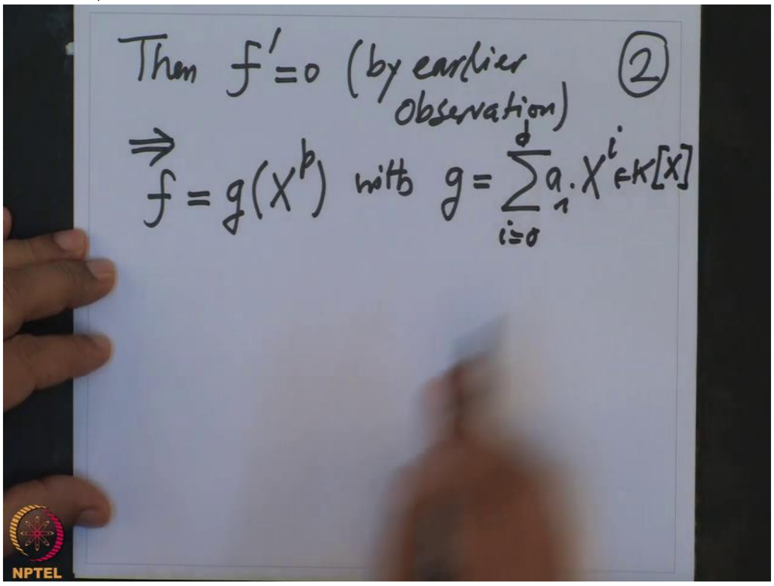
(Refer Slide Time 03:56)




The derivative is 0 and now we want to get a contradiction, contradiction to what we will get, contradiction to the fact that f is irreducible.

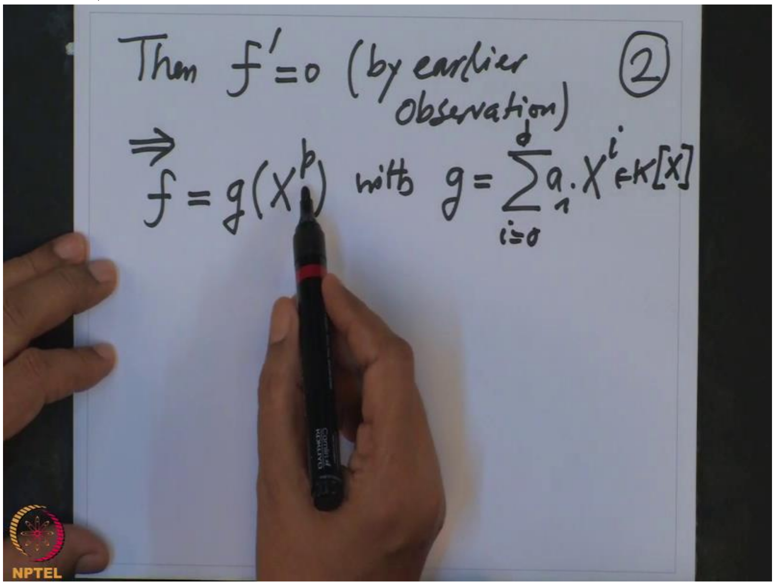
So f prime is 0 that will mean that f will be a polynomial so that will imply, f is a polynomial in X power p with g is a polynomial a i X power i, i from 0 to d. This is in K X.

(Refer Slide Time 04:32)



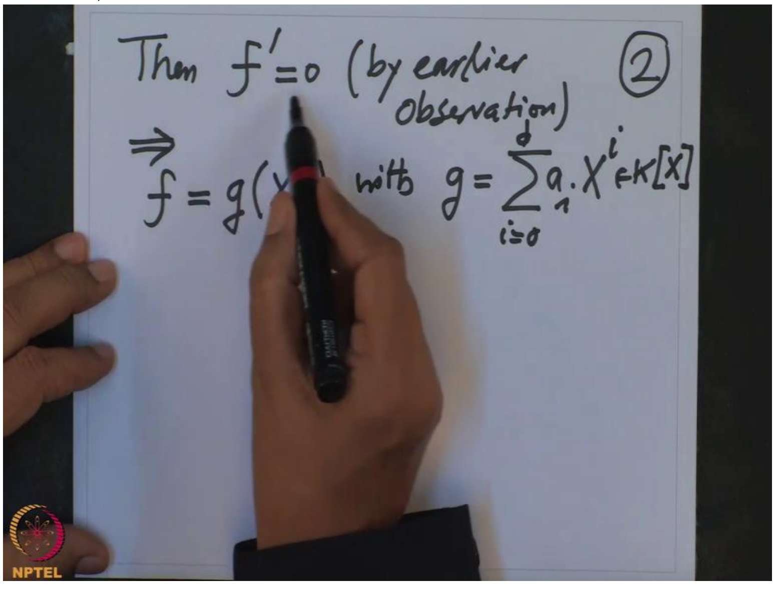

That means other

(Refer Slide Time 04:35)




powers which are the powers of X which are not in, not multiples of p;

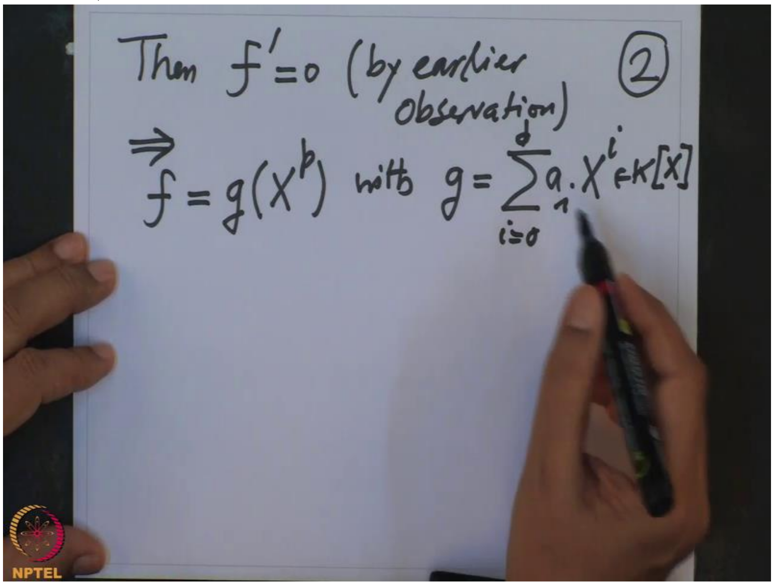
(Refer Slide Time 04:43)




they will be 0 because f prime is 0.

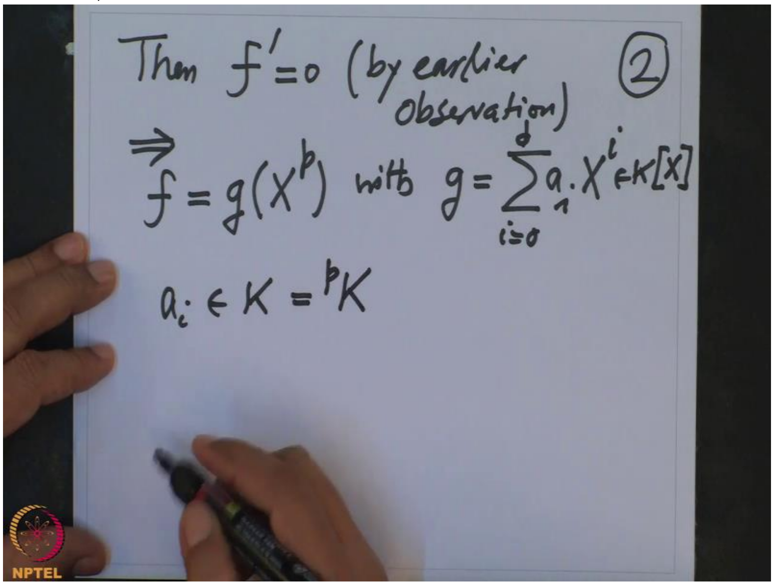
Now

(Refer Slide Time 04:48)




these a is are coefficients in a, so a is belong to K but K is the image of the Frobenius

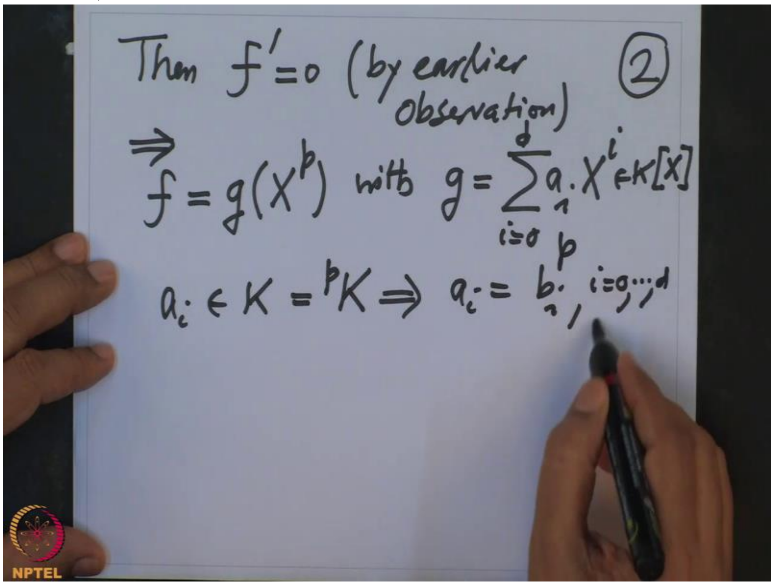
(Refer Slide Time 04:56)




because Frobenius is surjective. Therefore each a i, I will write it as some pth power of some element b i. So i is from 0 to d.

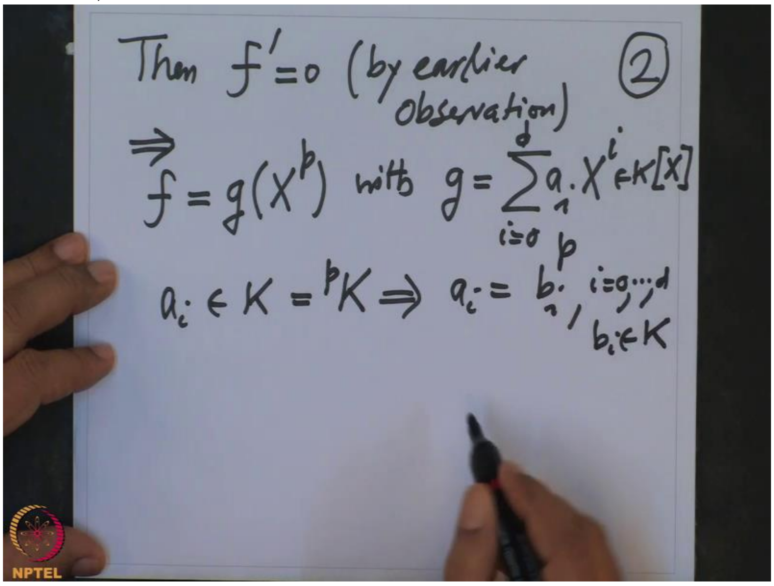
And

(Refer Slide Time 05:09)



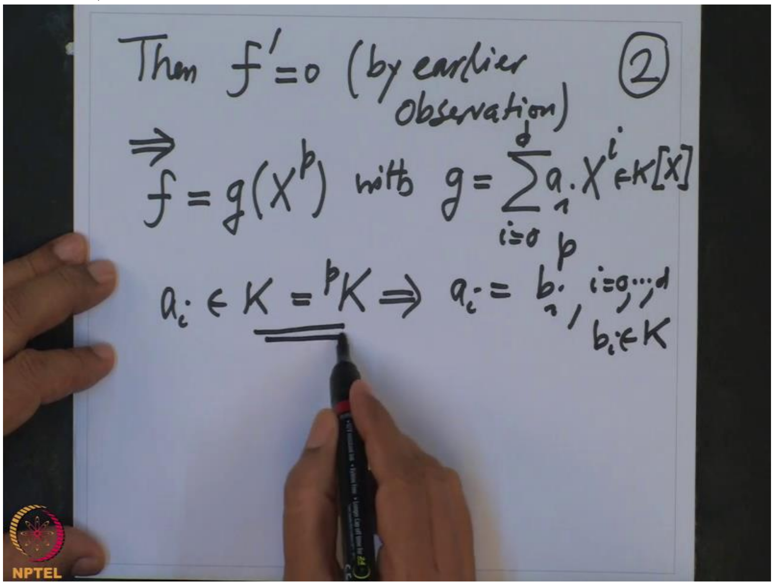

b is are element in K.

(Refer Slide Time 05:11)




So this is because the image is

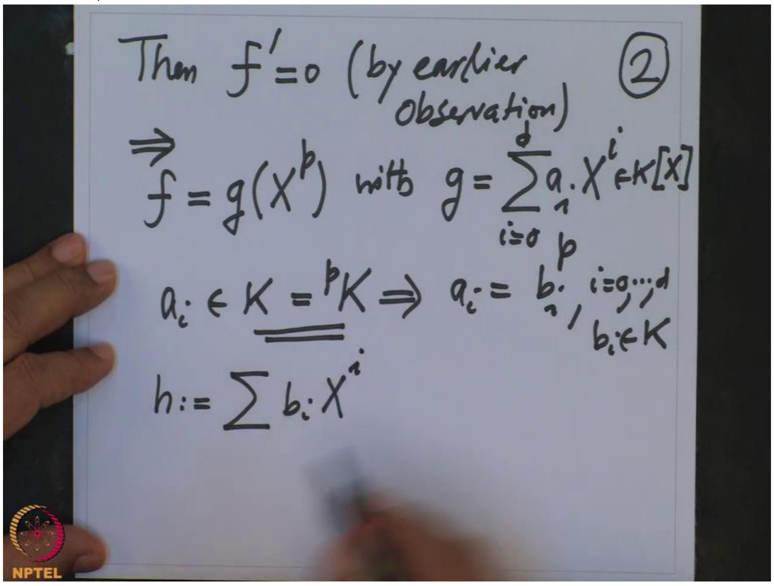
(Refer Slide Time 05:15)




everybody, so p is surjective therefore this, so therefore now look at these b is and look at the polynomial h I am defining.

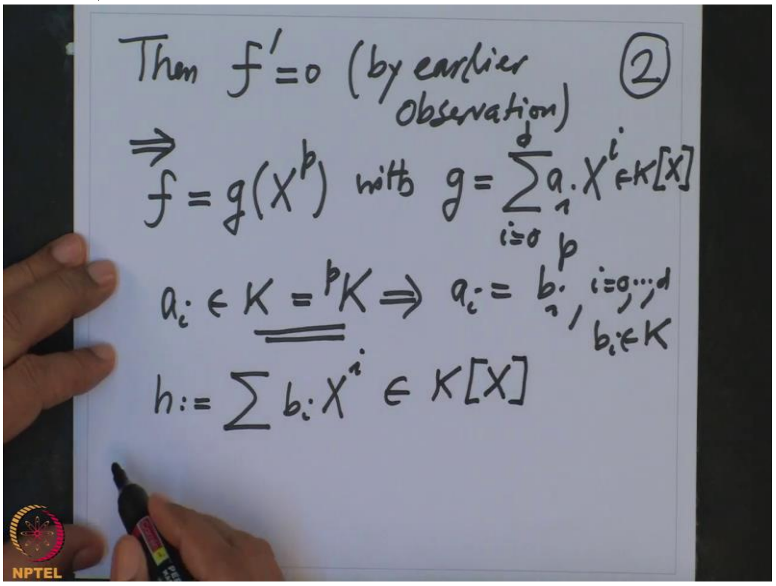
This is the polynomial b i X power i.

(Refer Slide Time 05:33)




Look at this polynomial. This is a polynomial in K X, Ok

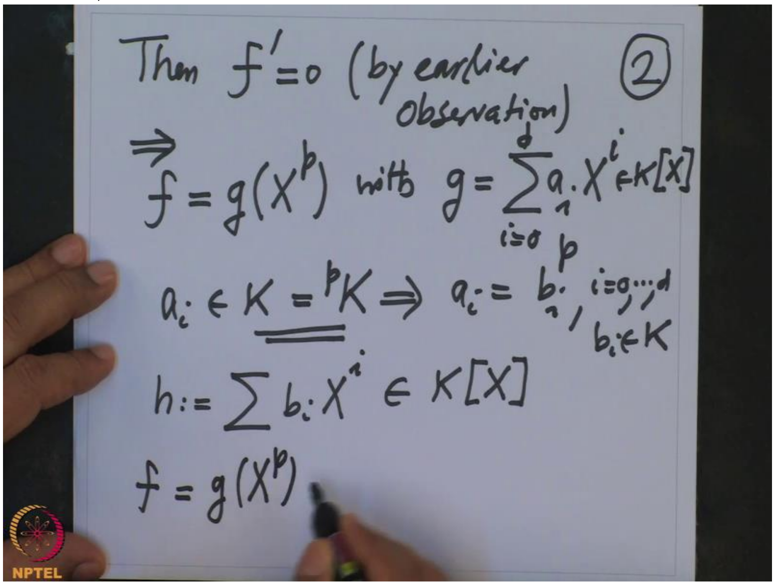
(Refer Slide Time 05:40)




and then what is f? Look at f. We want to get, we want to check that f is not irreducible now. That will be the contradiction.

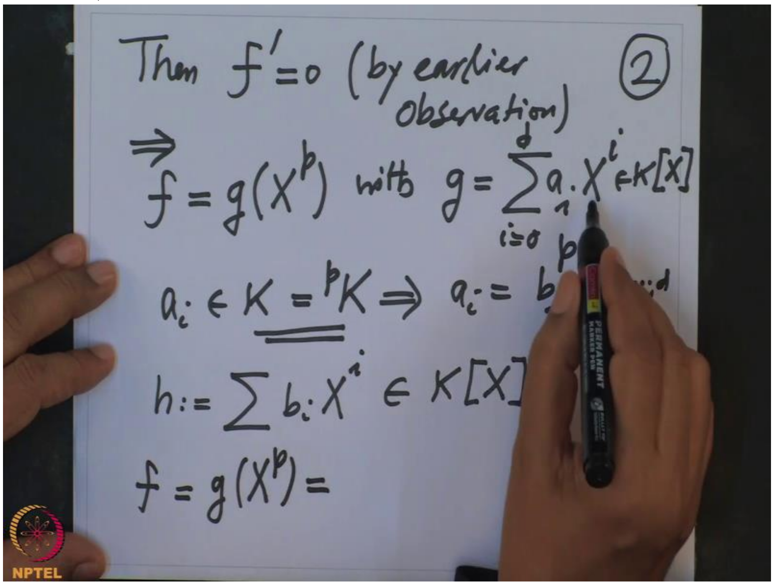
f equal to g of X power p,

(Refer Slide Time 05:53)




that means in g I should

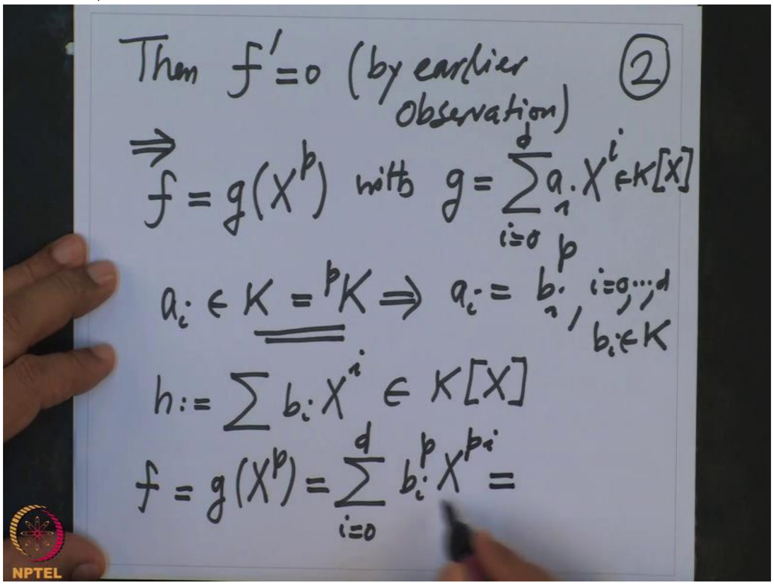
(Refer Slide Time 05:54)




put instead of X, X power p. So this is summation i equal to 0 to d and these a is are b i power, so this is b i power p and X i, X I will replace by X power p, so this is X p i.

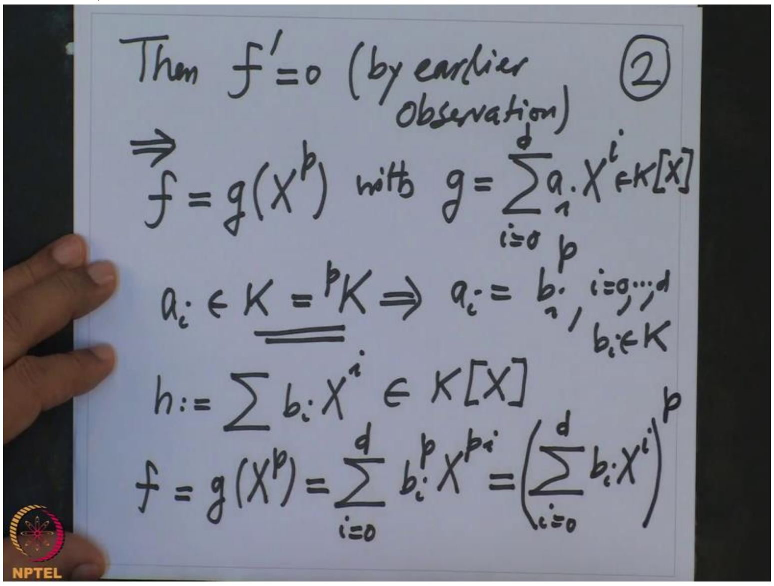
But now it is characteristic p, therefore

(Refer Slide Time 06:12)



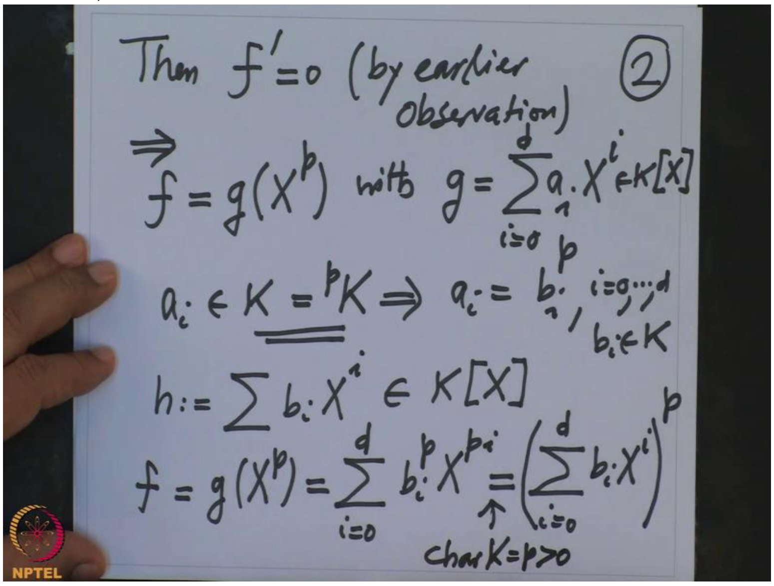

this sum is same thing as i equal to 0 to d, b i X power i and then I have taken that p out of the sum.

(Refer Slide Time 06:24)



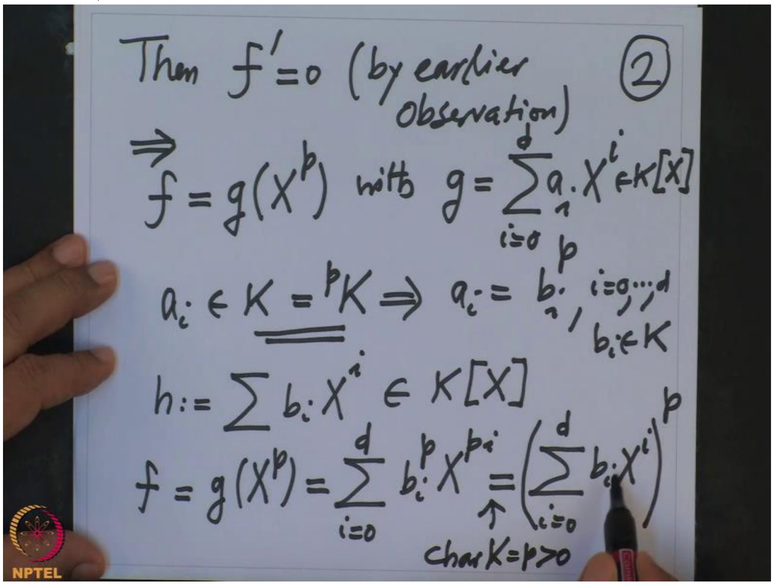

That is because p is a characteristic of the field. This equality follows from the fact that characteristic p is positive.

(Refer Slide Time 06:33)




This is when you expand by binomial, middle terms which are

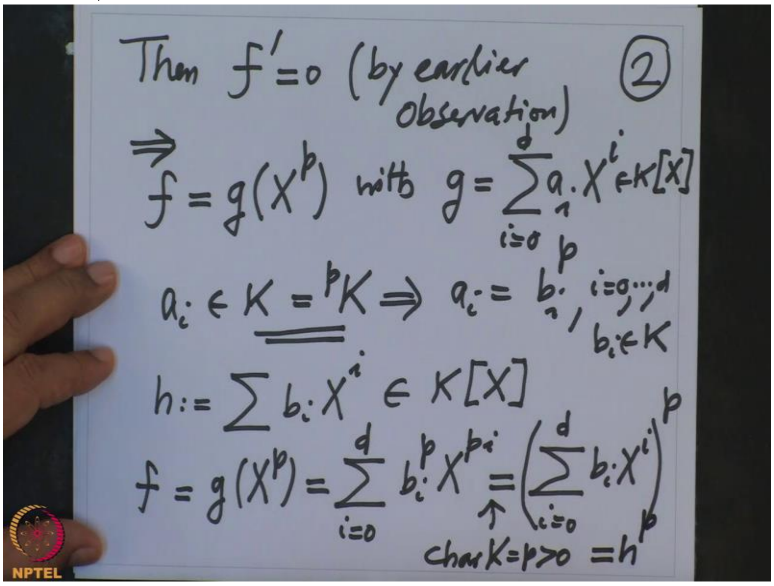
(Refer Slide Time 06:37)



binomial coefficients, middle binomial coefficients they are divisible by p therefore they are 0 in K. That is why, this equality.

But what is this? This is h power p.

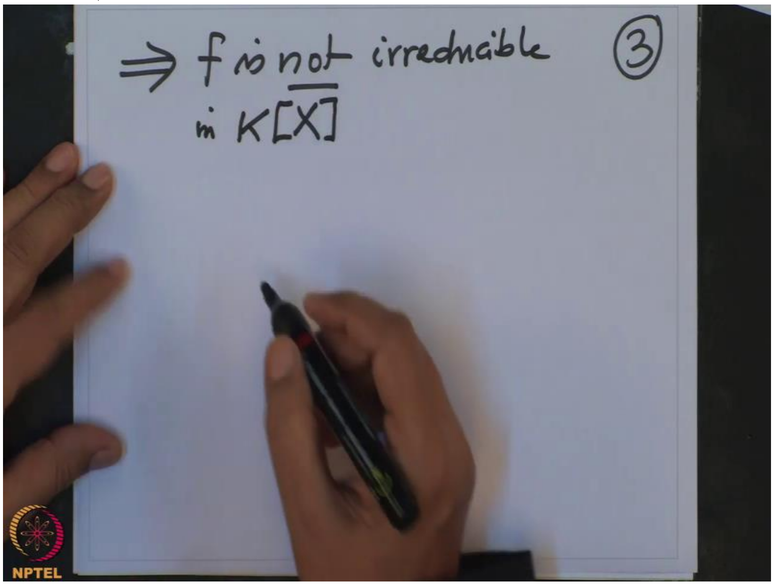
(Refer Slide Time 06:50)



This is precisely the definition of h. This is h power p which contradicts the irreducibility of f. p is at least 2.

So this f is not irreducible in K X. Therefore we, I have finished the

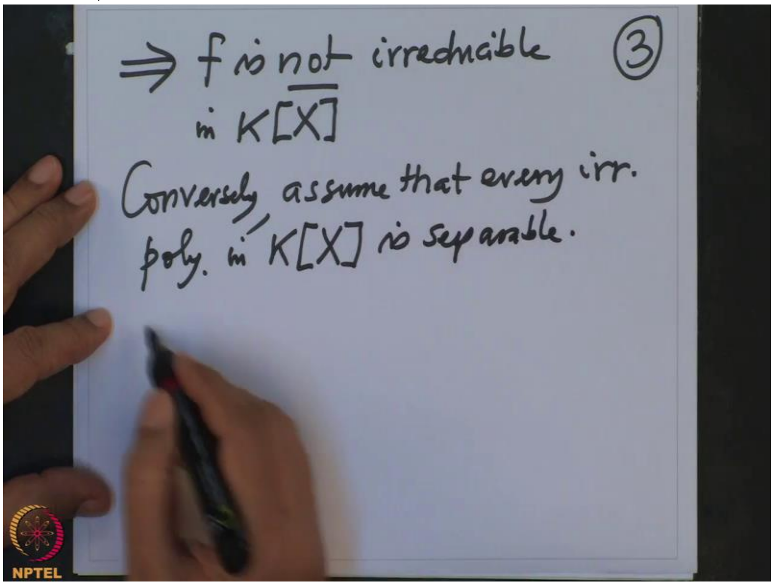
(Refer Slide Time 07:17)




proof of one implication. Conversely we need to prove that if f is; if every polynomial is irreducible then we want to prove that K is perfect.

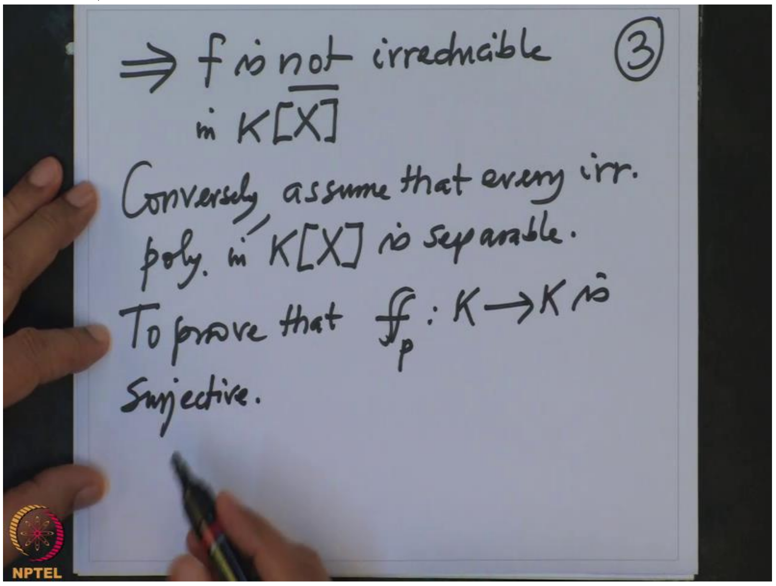
Conversely assume that every irreducible polynomial in K X is separable.

(Refer Slide Time 07:49)




And now to prove that f p Frobenius map is surjective. This is what we want to prove,

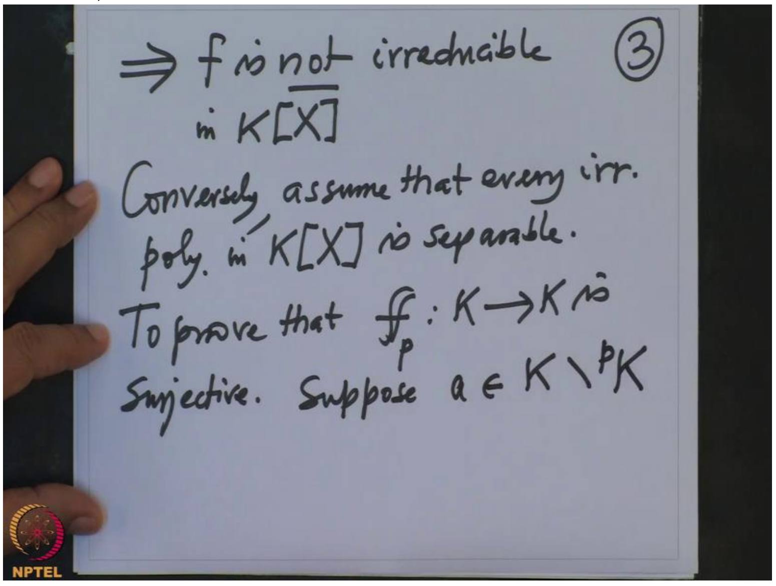
(Refer Slide Time 08:04)




alright.

So suppose it is not surjective. So suppose, then we should get a contradiction, suppose so the image of the Frobenius is K p. So suppose I have an element a in K which is not in the image of Frobenius.

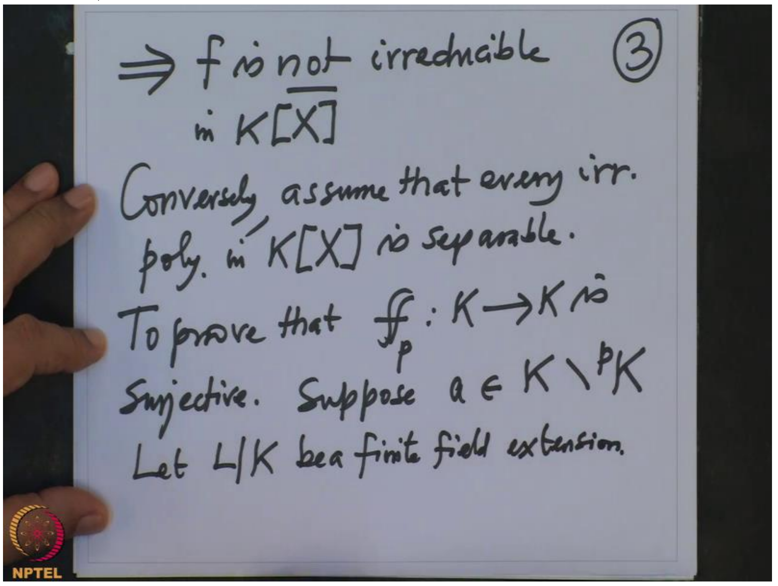
(Refer Slide Time 08:24)




Then I am looking for a contradiction.

So, now we have an element in the field which is not the pth power. So I look at the polynomial, I enlarge the field. So let L over K be finite field extension

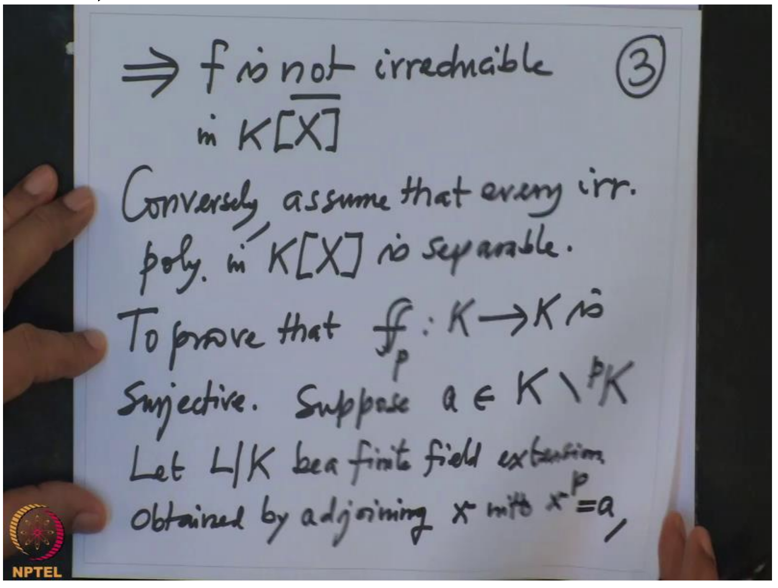
(Refer Slide Time 08:53)




which is obtained by adjoining pth root of a

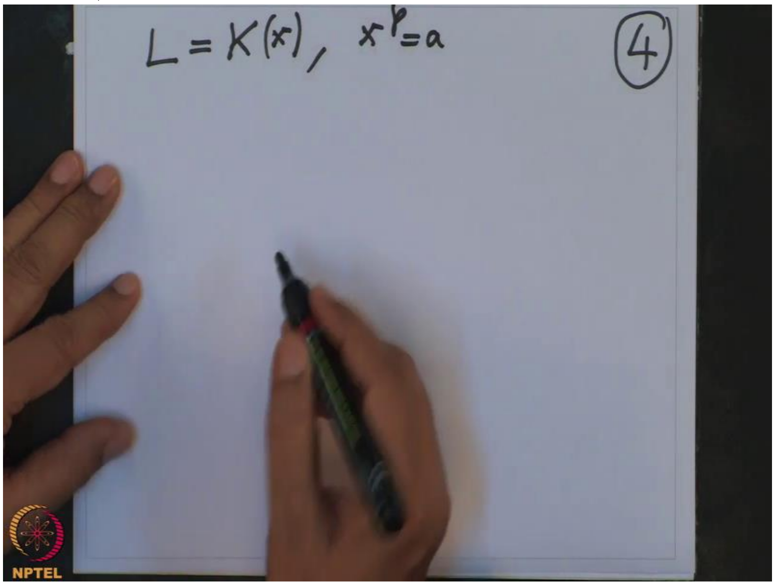
So adjoining x, x power p equal to L. So that is,

(Refer Slide Time 09:16)



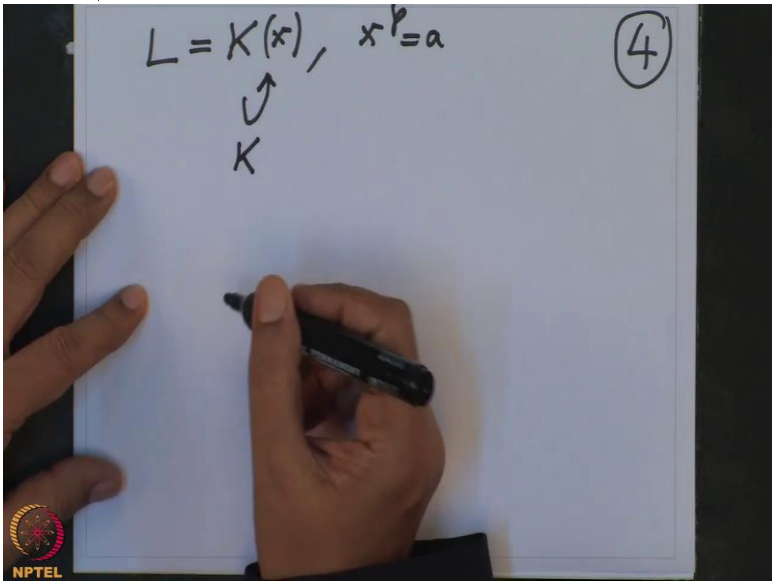

what I am saying is, look at the field extension L. L is the simple extension generated over K by x and x power p equal to a.

(Refer Slide Time 09:31)




So this is a field extension and this,

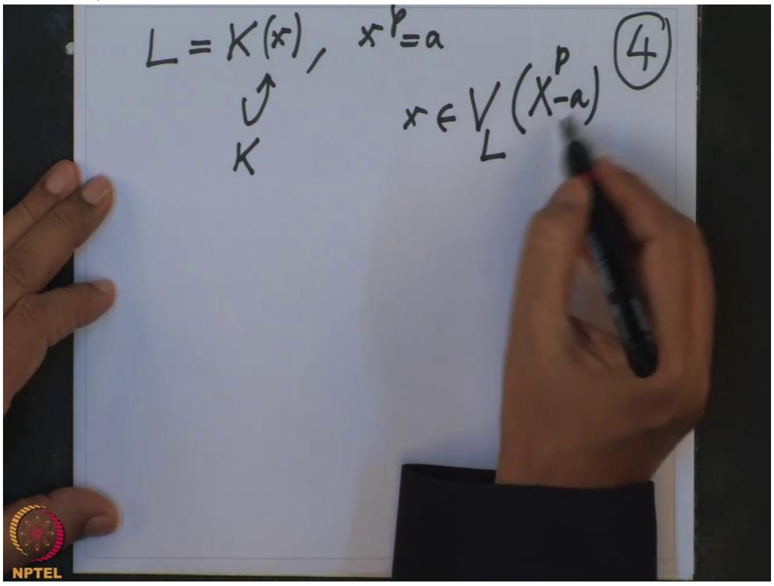
(Refer Slide Time 09:35)




this is the finite field extension.

So what is irreducible, so x belongs to the 0 set of the polynomial X power p minus a. It is one 0

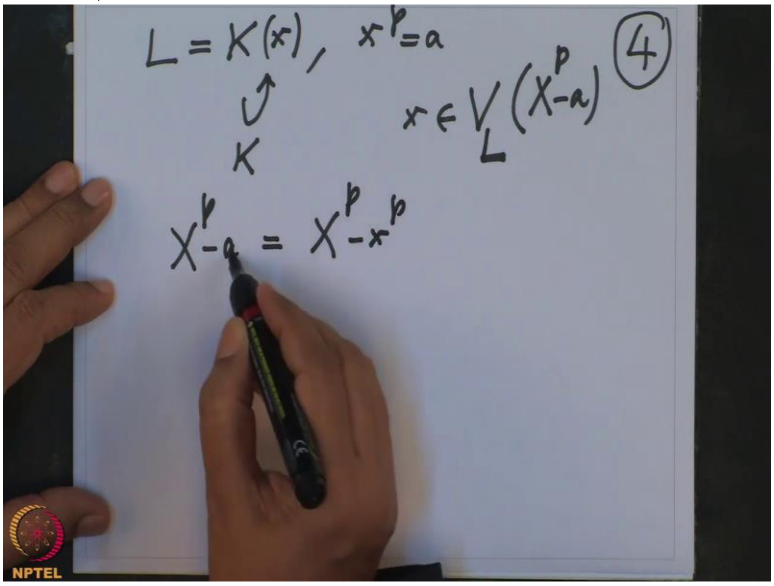
(Refer Slide Time 09:52)




of the polynomial. This is in L that is x.

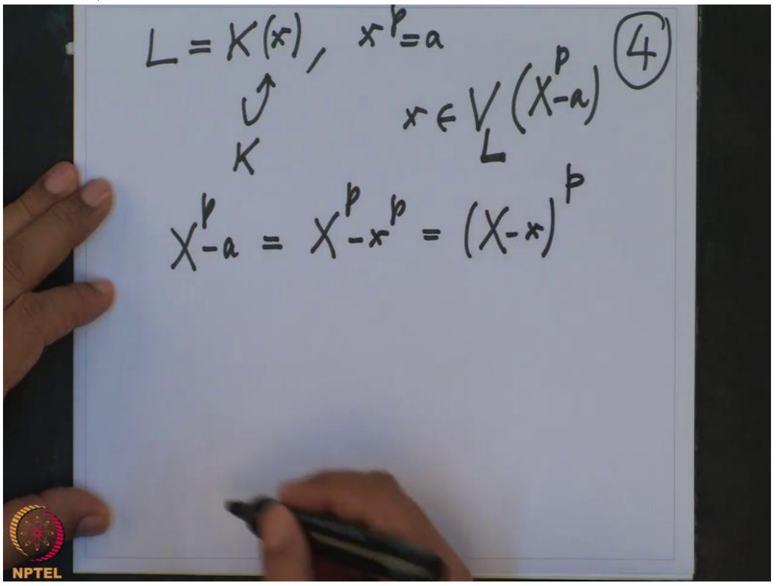
So look at the polynomial, this polynomial you want to study X power p minus a. This polynomial, when I write like this, X power p minus small x power p,

(Refer Slide Time 10:12)



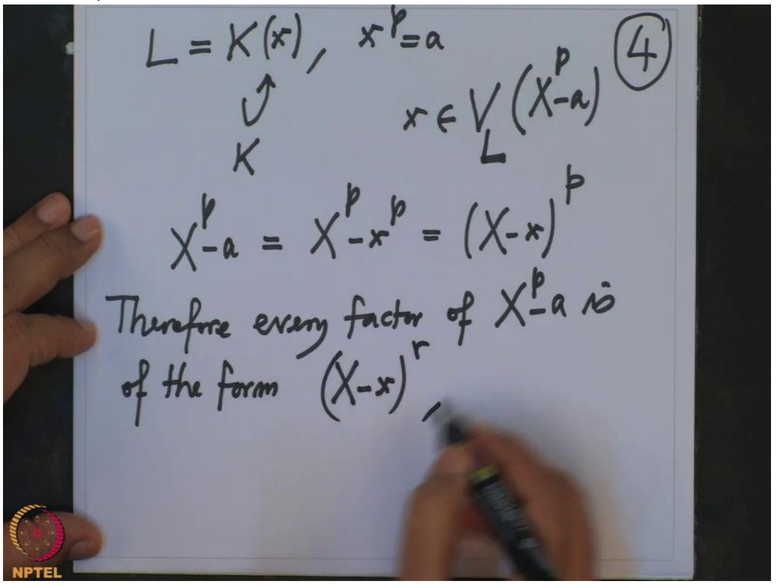

I will just a equal to x power p, this is X minus x power p.

(Refer Slide Time 10:18)



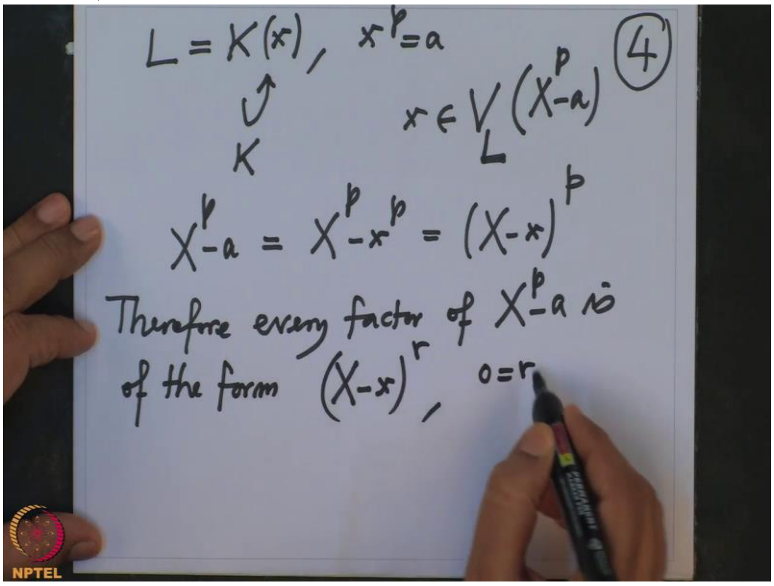

Therefore see, therefore what we know from this equation, every factor of X power p minus a is of the form X minus x power r

(Refer Slide Time 10:46)



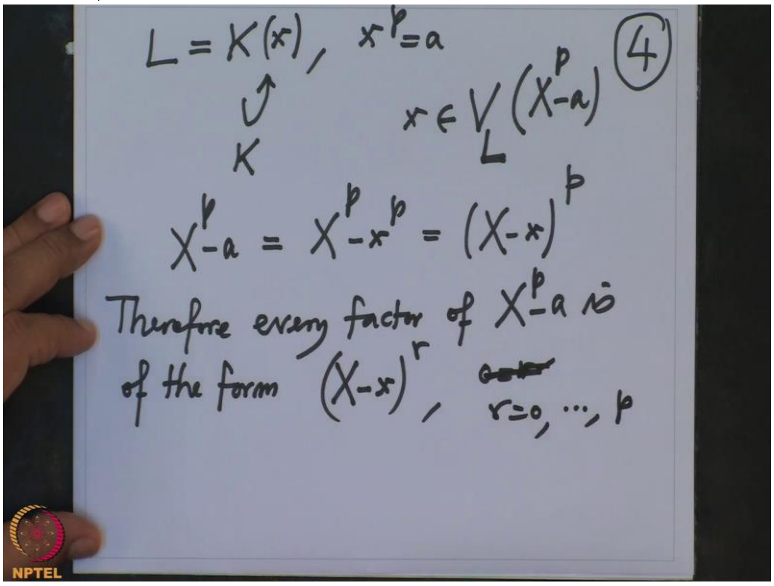

where r is from 0 to,

(Refer Slide Time 10:48)



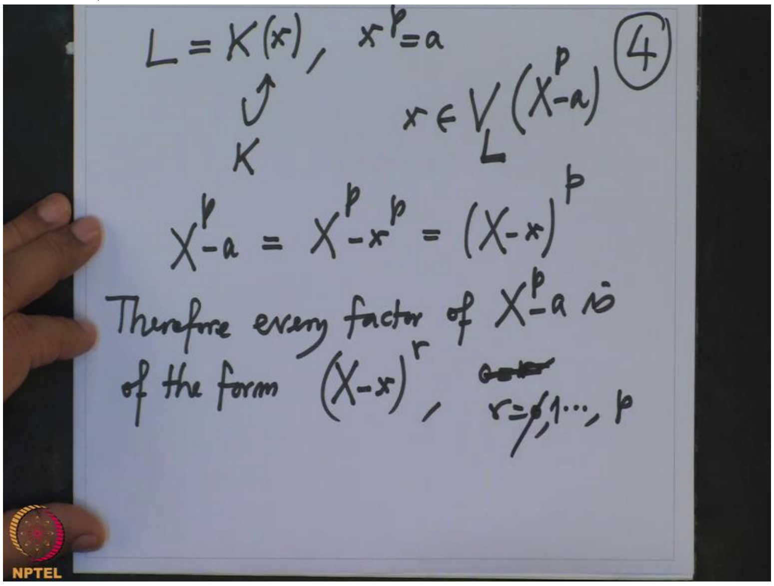

r is from 0 to p.

(Refer Slide Time 10:55)




Well, when r is equal to 0, this is just 1 which is a constant factor. So we are not interested in that. So this is

(Refer Slide Time 11:04)

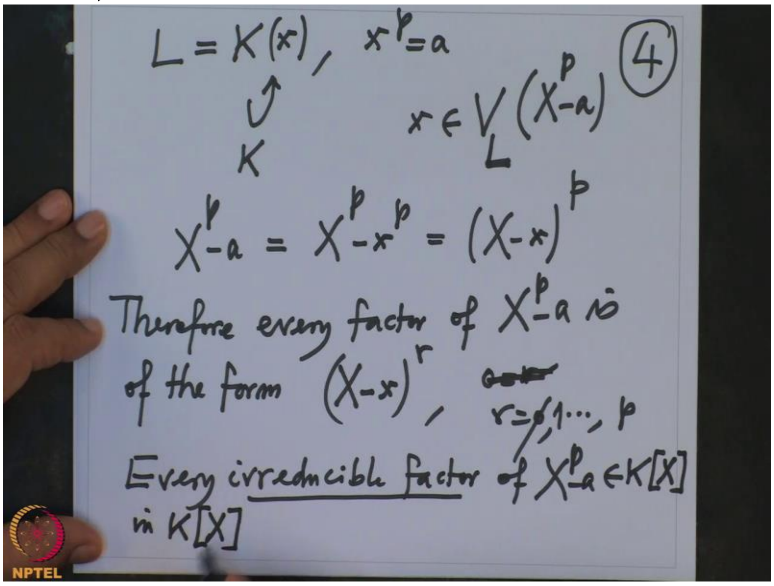



not interesting for us, so 1 to p.

And therefore what we know is every irreducible factor, every irreducible factor of this polynomial X power p minus a, this is a polynomial in K X

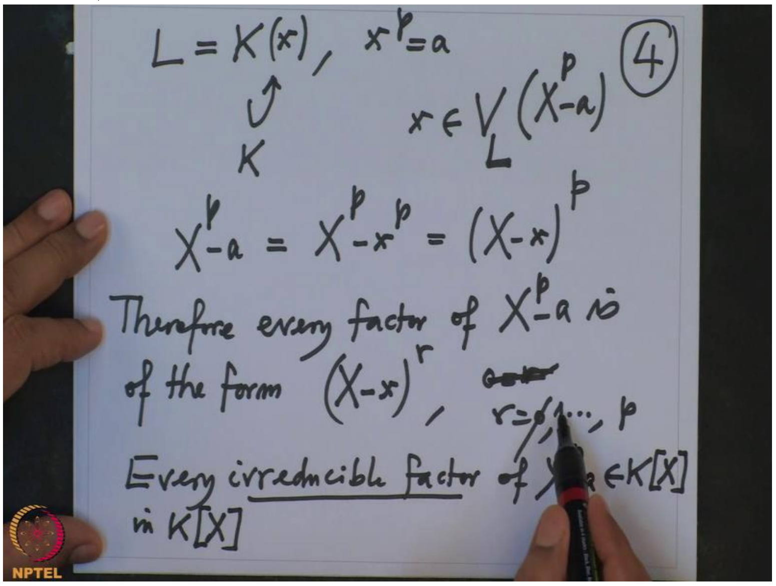
And I am considering irreducible factor also in K X.

(Refer Slide Time 11:34)



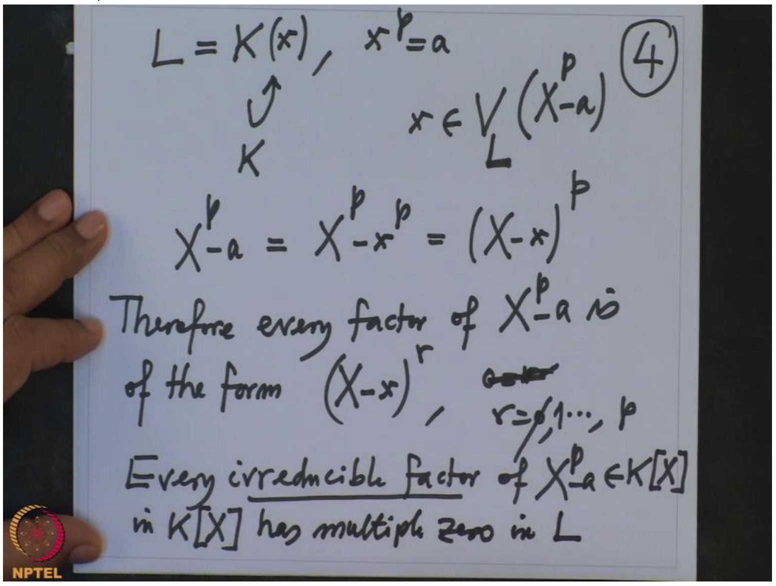

And it will be not

(Refer Slide Time 11:36)



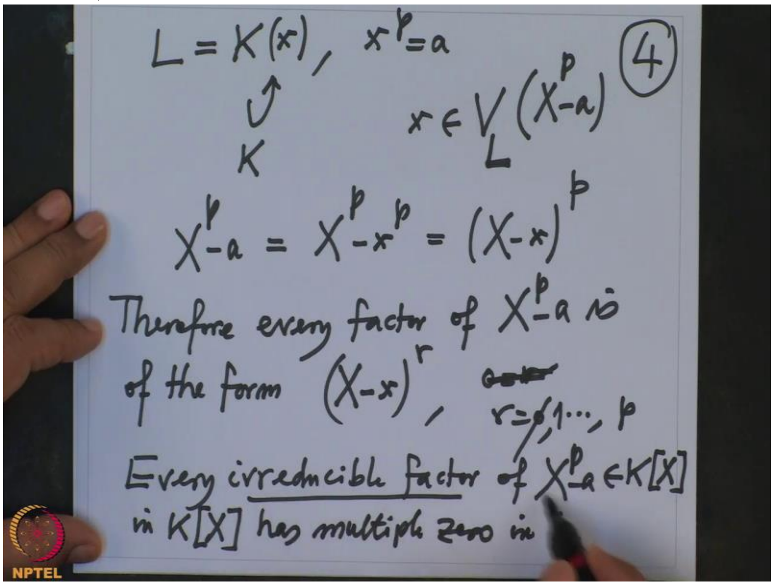

r equal to 1 so every irreducible factor has a multiple zero in L.

(Refer Slide Time 11:54)



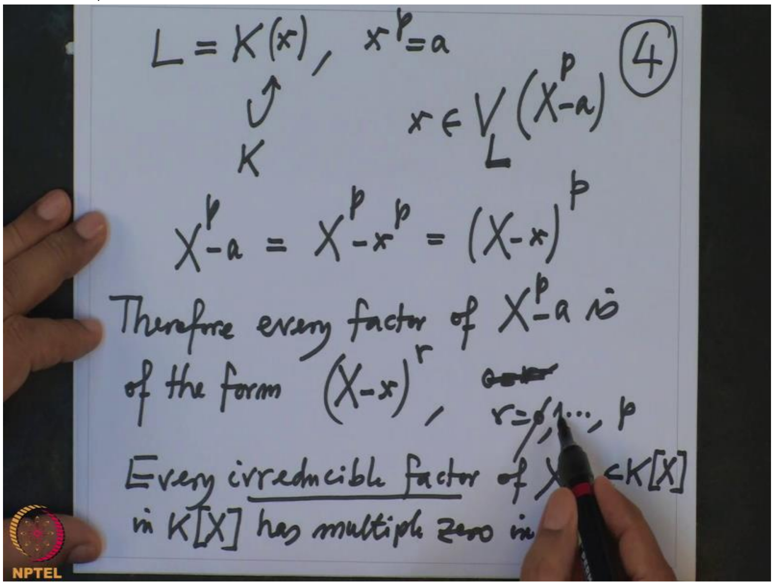

So the same X will be multiple zero because if you take irreducible factor of this polynomial,

(Refer Slide Time 12:01)



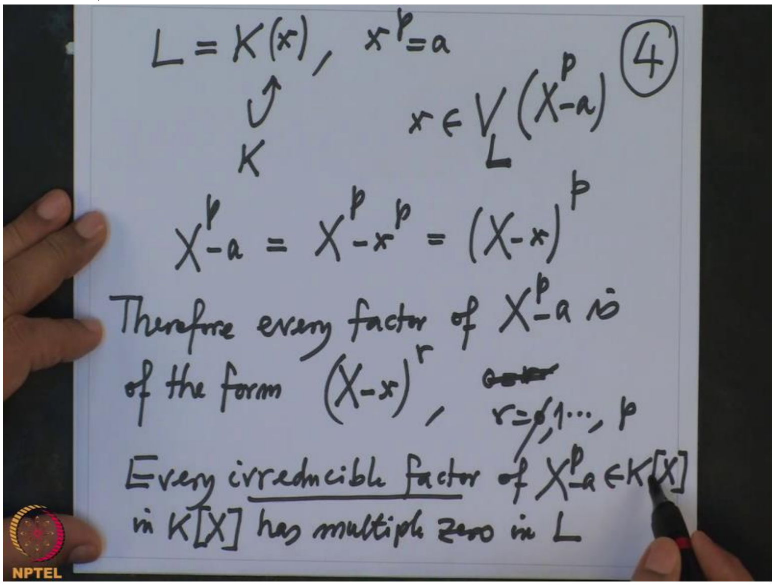

that, first of all

(Refer Slide Time 12:02)



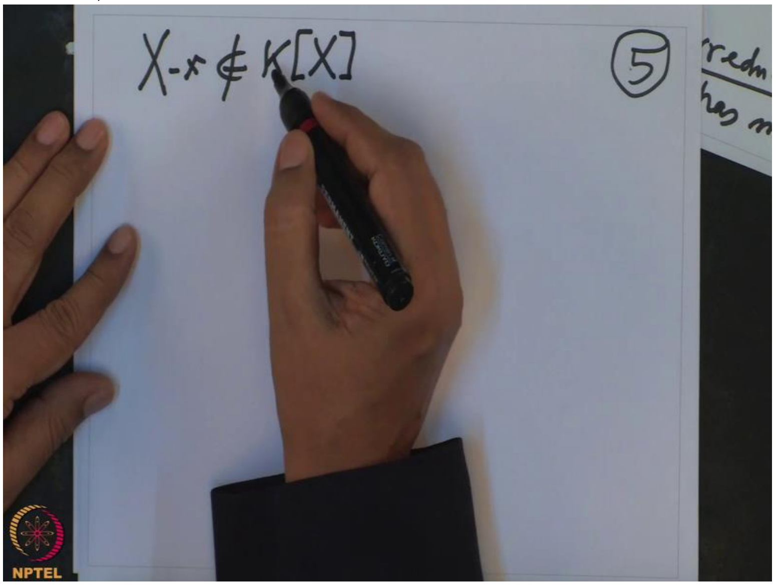

that is not X minus x because that X minus x is not a polynomial in K X.

(Refer Slide Time 12:10)




So since, since this polynomial X minus x, this is not in K X, so all irreducible factors in K X,

(Refer Slide Time 12:27)

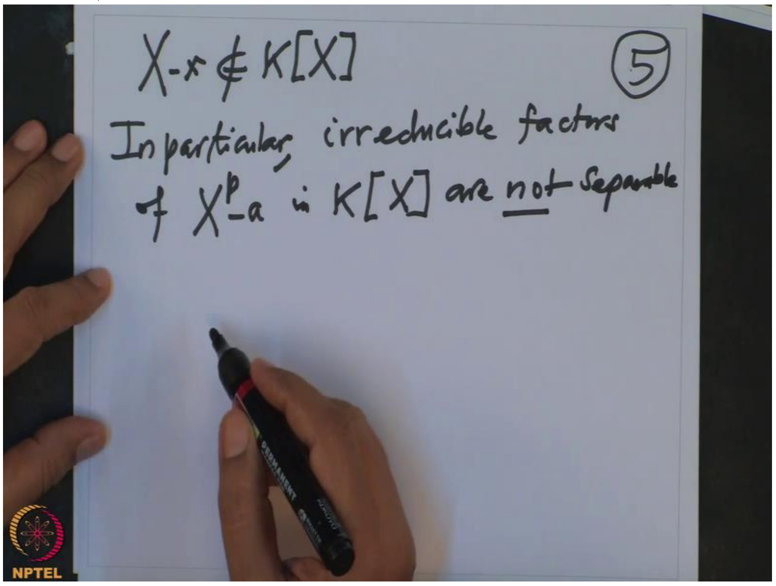



they will be higher powers of this. Therefore they have multiple zeroes.

So therefore they are not separable, so what we proved is in particular irreducible factors of X power p minus a in K X are not separable.

This is a contradiction

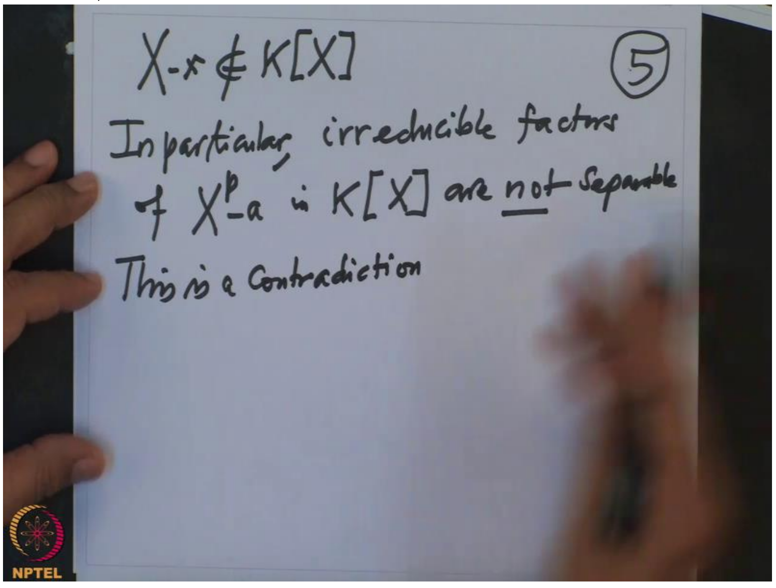
(Refer Slide Time 13:09)




to our assumption. We are assuming that every irreducible polynomial in K X are separable. But here we produce irreducible polynomials in K X which are not separable.

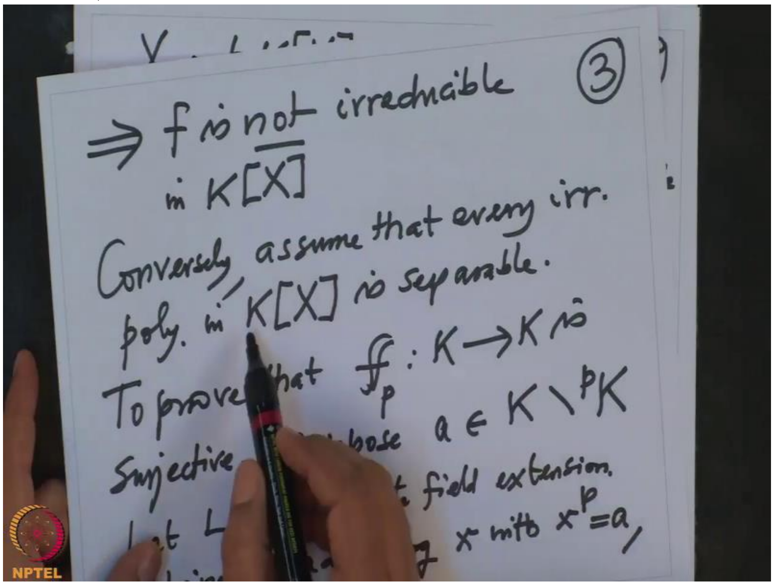
This is a contradiction,

(Refer Slide Time 13:29)



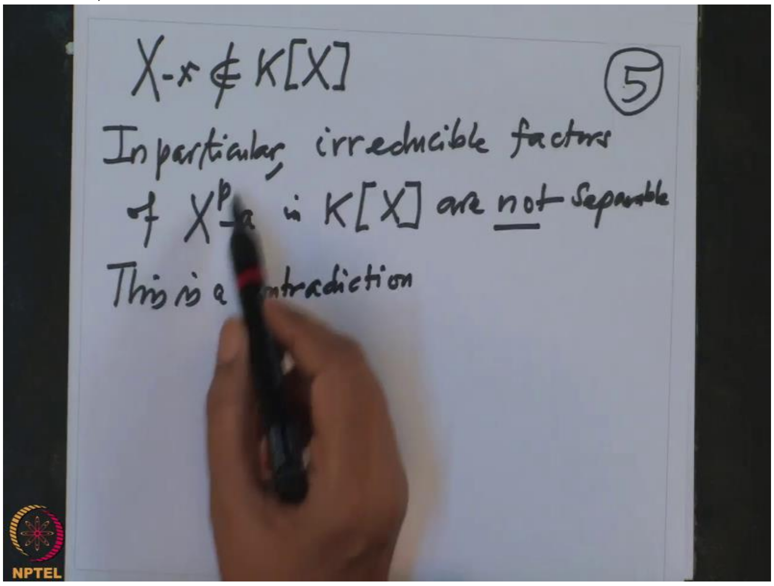

so remind you we are assuming that

(Refer Slide Time 13:33)




every irreducible polynomial in K X is separable but here we produce irreducible

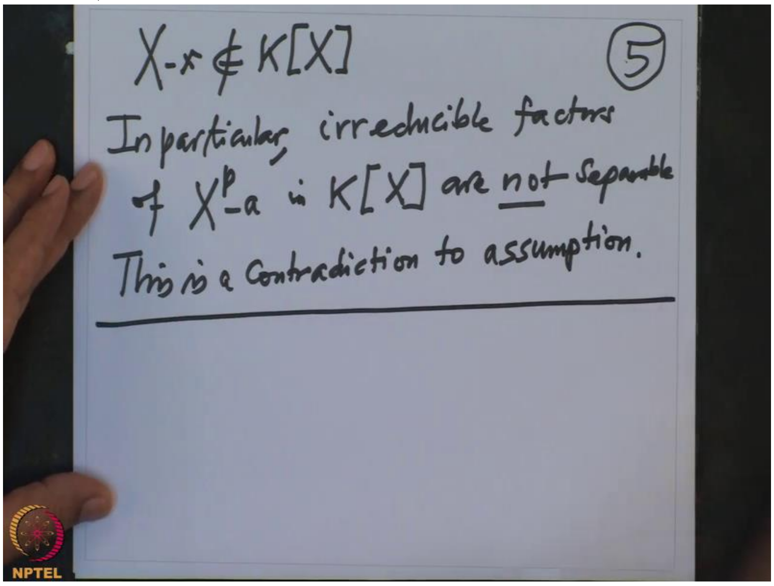
(Refer Slide Time 13:41)




polynomial which is a factor of this could be this itself.

This is a contradiction to assumption. So this completes,

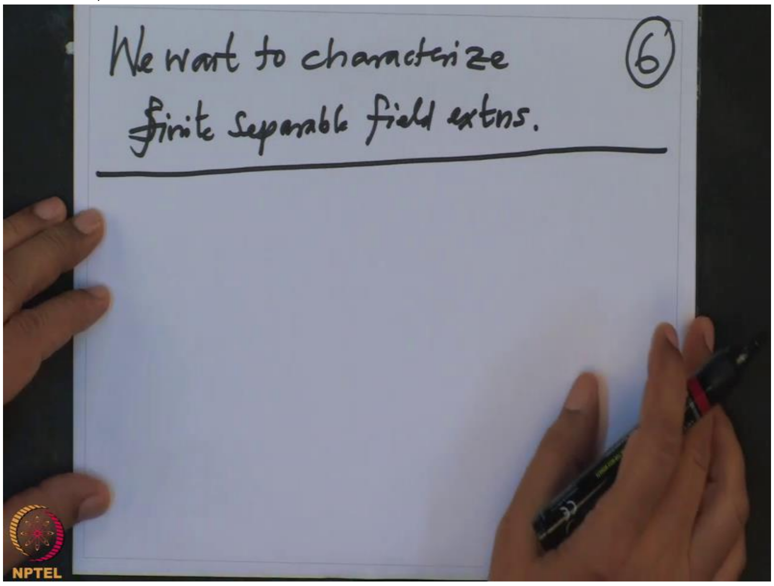
(Refer Slide Time 13:53)




this completes the characterization of perfect field. Now I want to characterize separable field extensions.

So next is we want to characterize finite separable field extensions. This is what we want to do.

(Refer Slide Time 14:36)

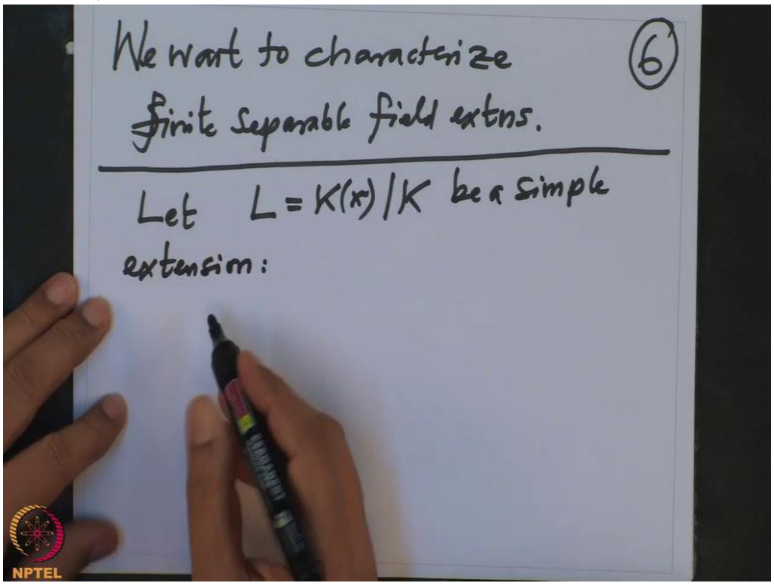



So recall that when we say finite field extension is called separable if every polynomial, every element is separable. That means minimal polynomials are separable polynomials. But this is too much checking.

So I want to find economical way to check that a given finite field extension is separable, possibly in terms of the degree of the field extensions. So this is what I want to do it. So first of all note that let us do checking for simple extension.

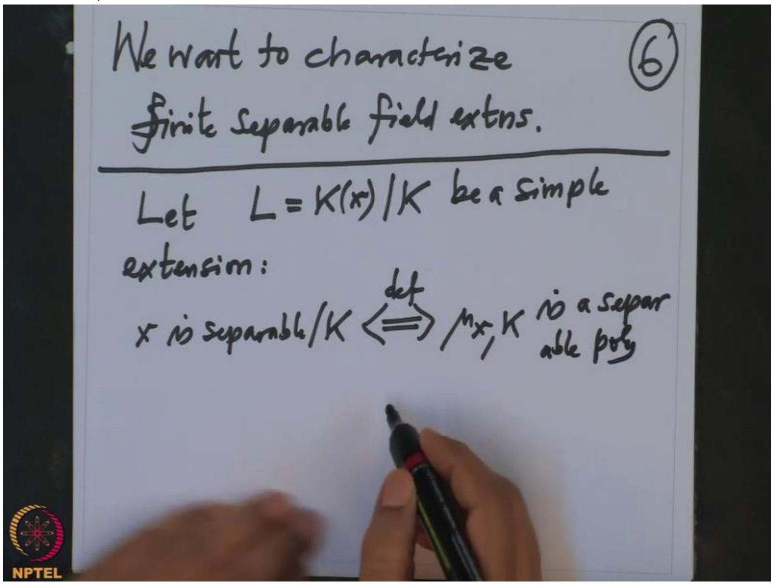
So let L equal to K x over K be a simple extension.

(Refer Slide Time 15:44)



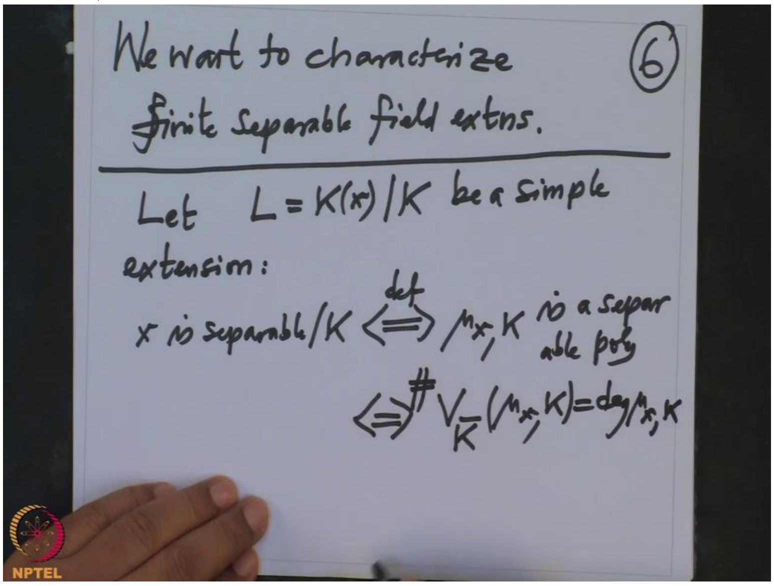

Then we want to, so x is separable over K, that is if and only if, this is a definition of separability of an element mu x over K is a separable polynomial.

(Refer Slide Time 16:10)



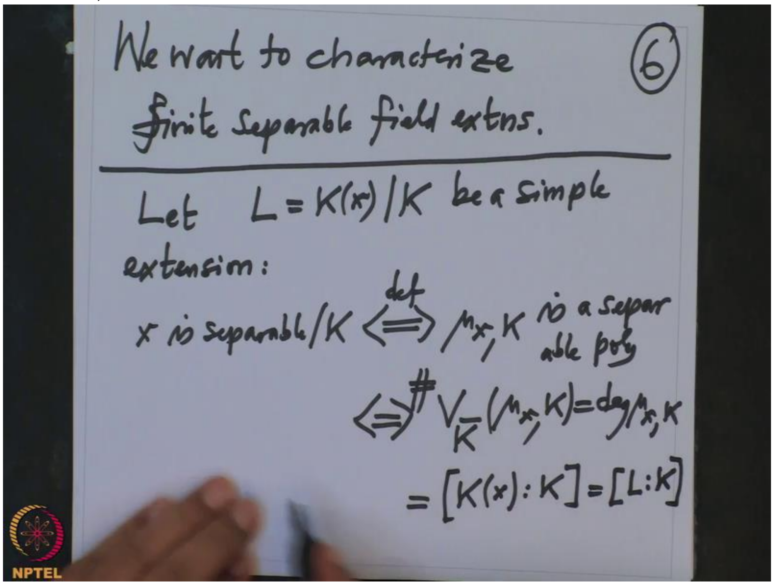

That is if and only if the 0 set of mu x in K bar, this cardinality equal to the degree of the mu x,

(Refer Slide Time 16:27)



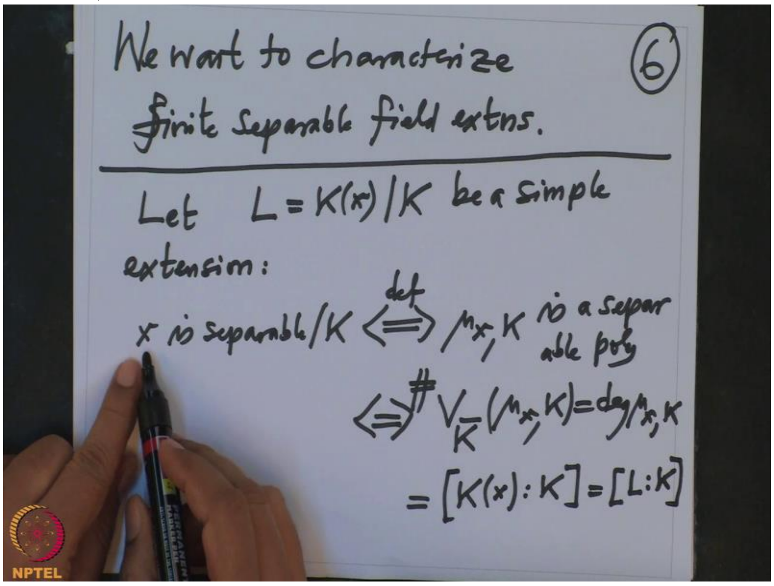

as many as zeroes. But this degree of mu x is equal to the degree of K x over K; that is L over K.

(Refer Slide Time 16:42)



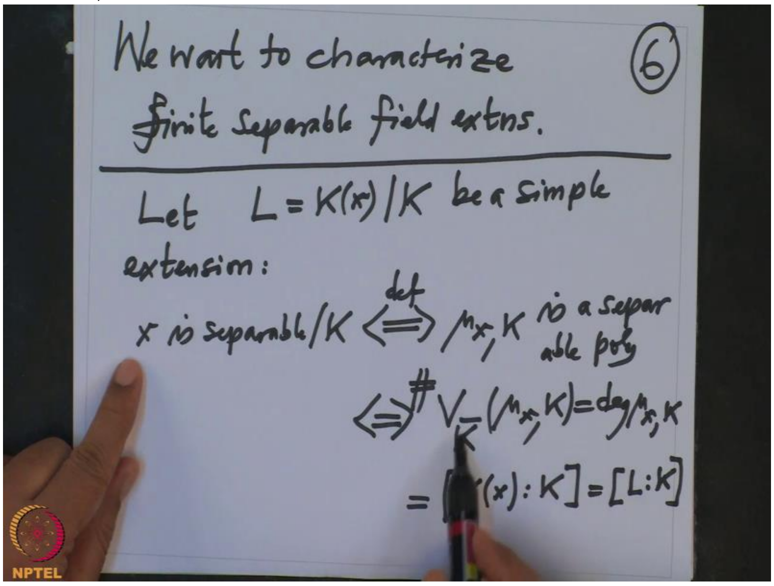

So an element, a generating

(Refer Slide Time 16:43)



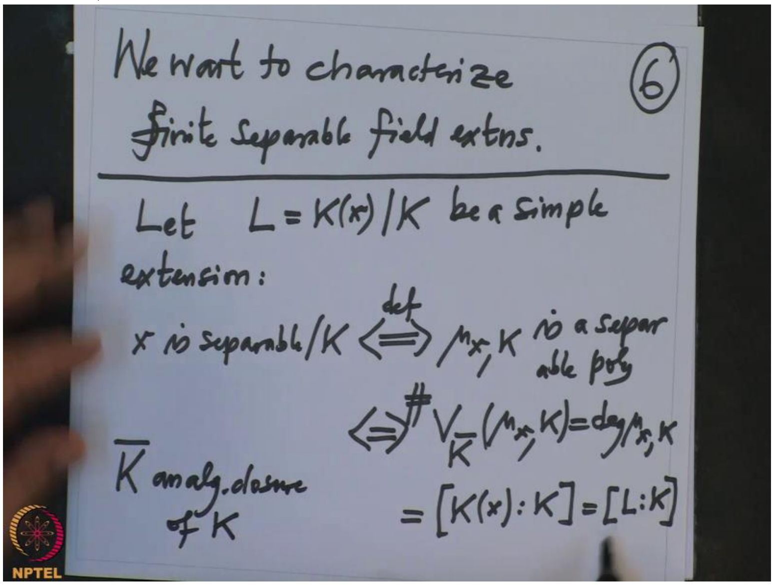

element is a separable over K that is, if and only if the degree of the field extension is exactly equal to the,

(Refer Slide Time 16:54)




the number of zeroes of the irreducible polynomial of x inside the algebraic closure of K. So here K bar is an algebraic closure of K. So this

(Refer Slide Time 17:12)



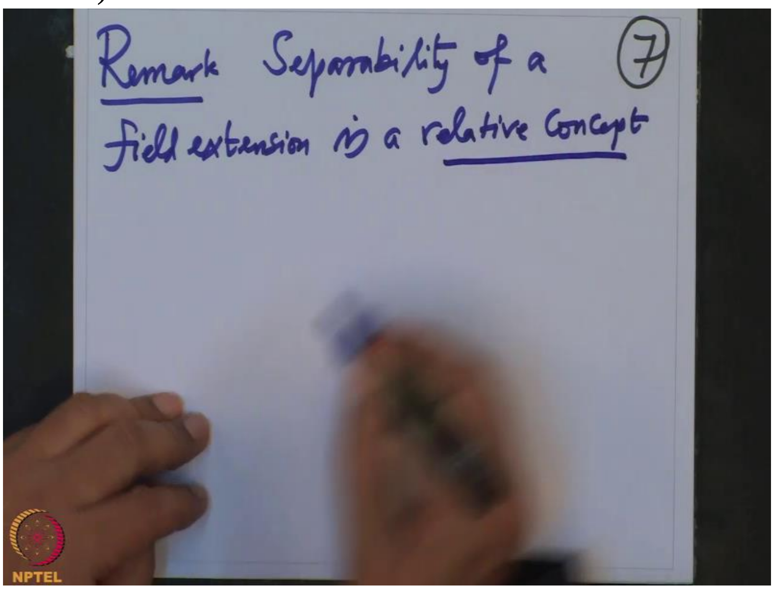

Is one way to check the number of zeroes equal to the degree of the polynomial. This is one possibility.

So I am going to enlarge on this. But before I do that I want to note one observation. So note that, this is remark.

This separability of a field extension, of a field extension is a relative concept. What does that mean?

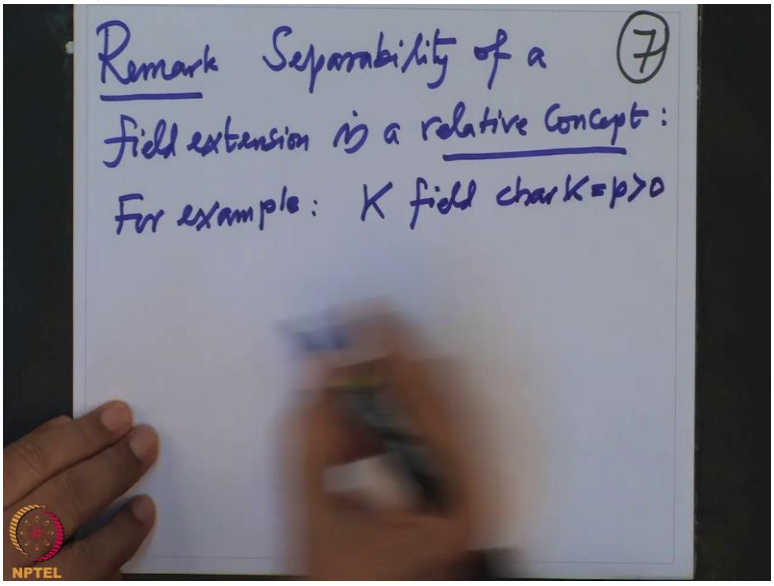
That means it depends

(Refer Slide Time 18:03)



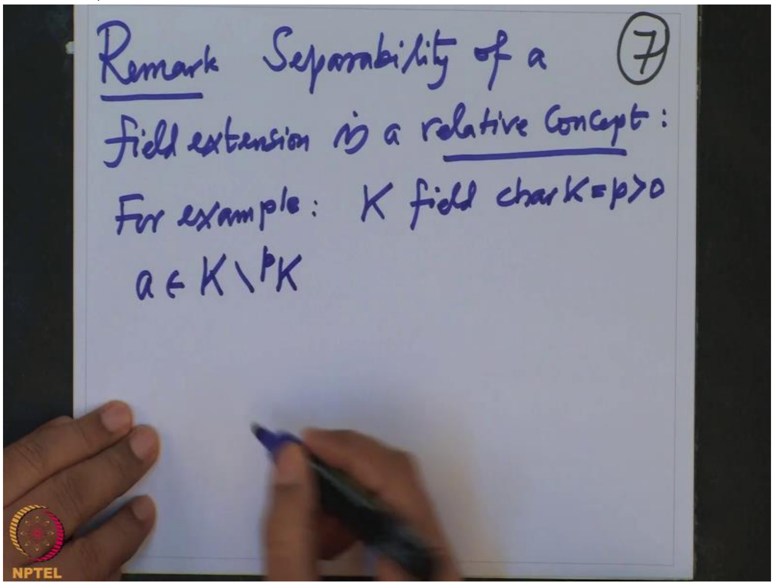
on the base field. So, so for example suppose K is field of characteristic p, positive and

(Refer Slide Time 18:23)




we have taken an element a in K minus pth powers of K.

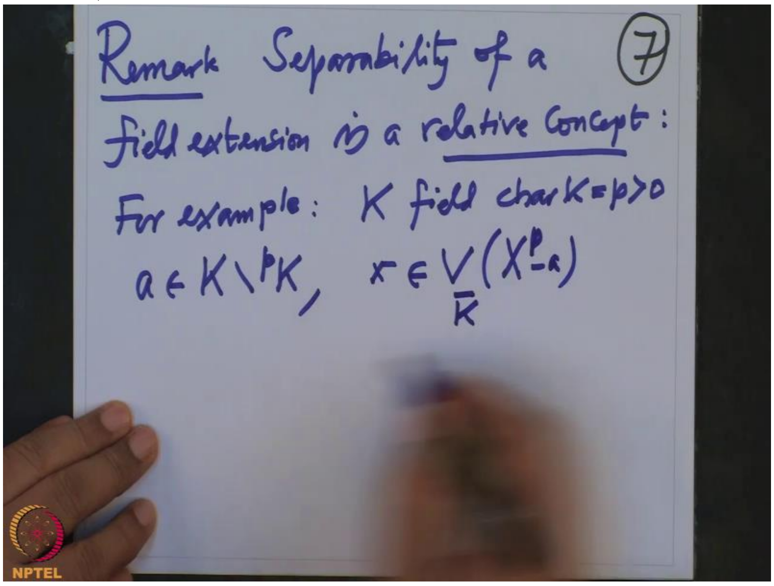
(Refer Slide Time 18:31)




This is a image of the Frobenius map.

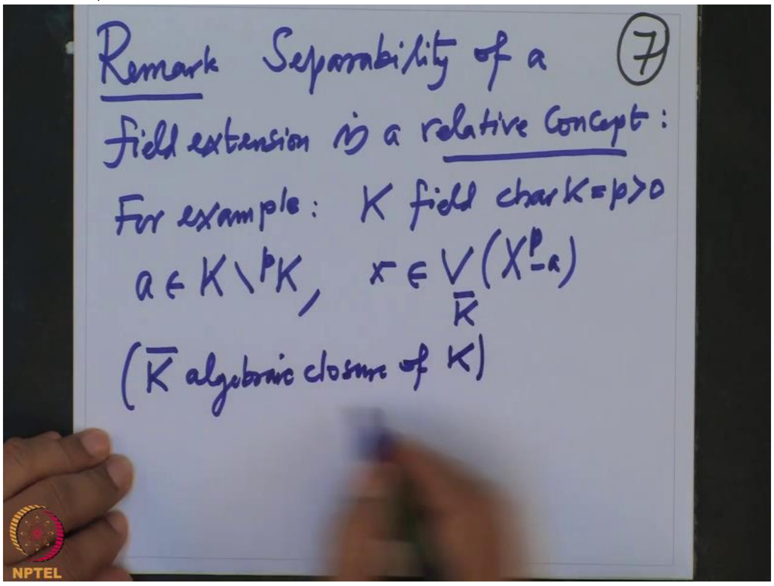
Suppose I have taken K. Like we have taken in one of the proof and suppose we have taken x is a 0 of X power p minus a. This 0 is in algebraic closure.

(Refer Slide Time 18:48)



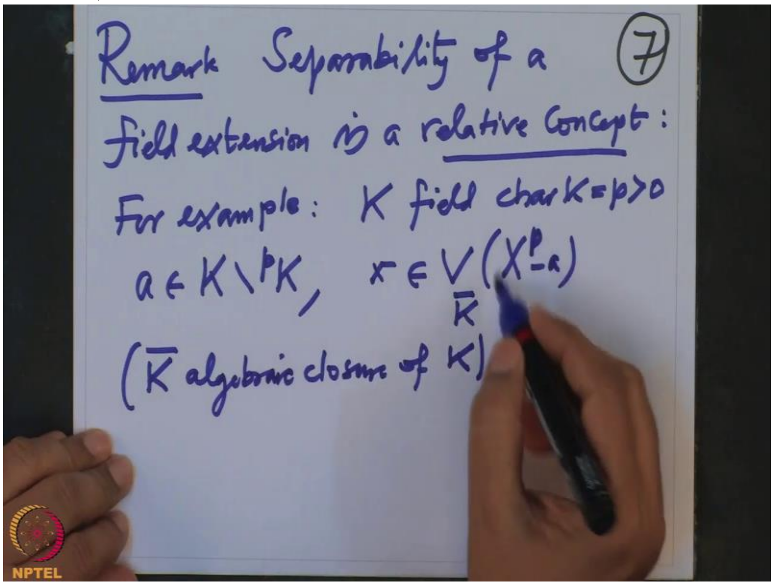

So K bar is algebraic closure of K.

(Refer Slide Time 19:00)




We choose an algebraic closure. We know it exists. And so

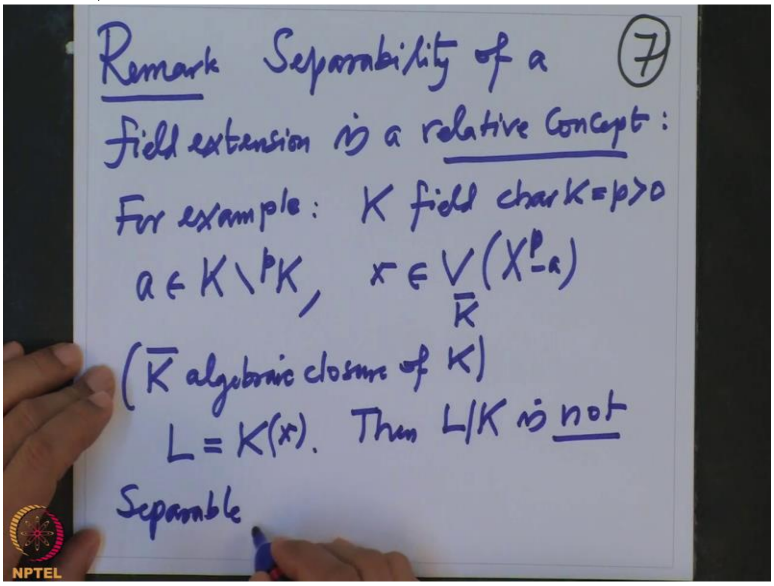
(Refer Slide Time 19:04)




this polynomial is a polynomial in K bar X and therefore it has 0, so I choose that 0. And now look at the simple extension L equal to K x. This K x, this is a simple extension.

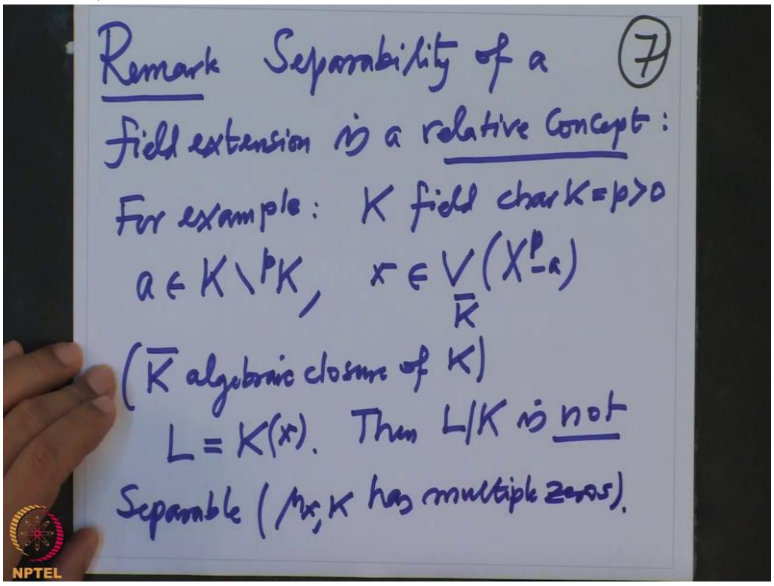
Then we know L over K is not separable. Because we have seen that

(Refer Slide Time 19:33)



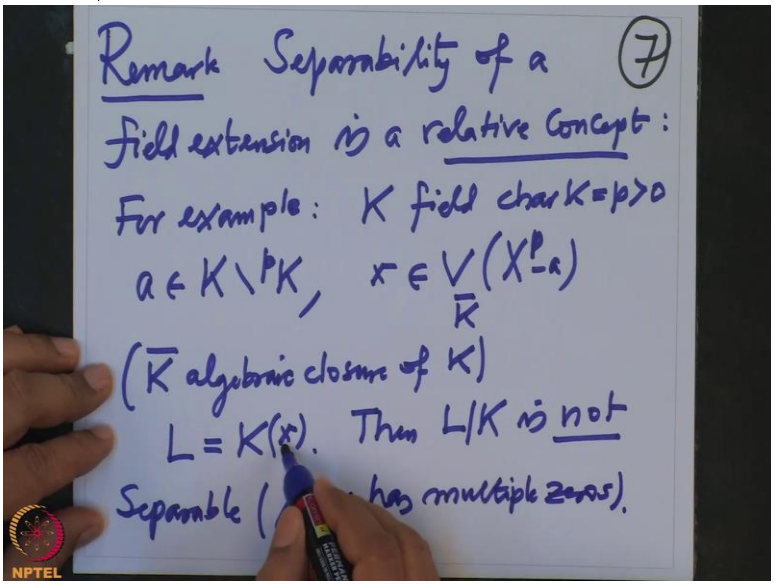

the minimal polynomial mu x over K has multiple zeroes.

(Refer Slide Time 19:45)



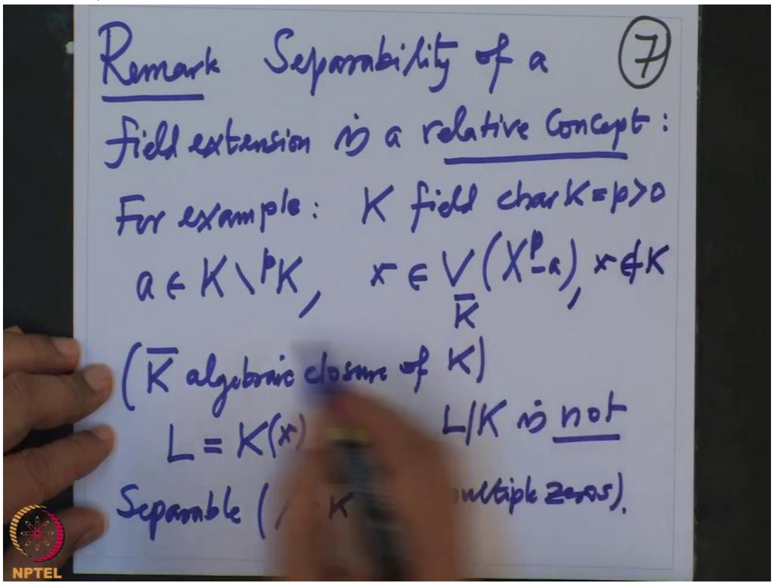

This x is not in K,

(Refer Slide Time 19:49)




this x; this x is not in K because

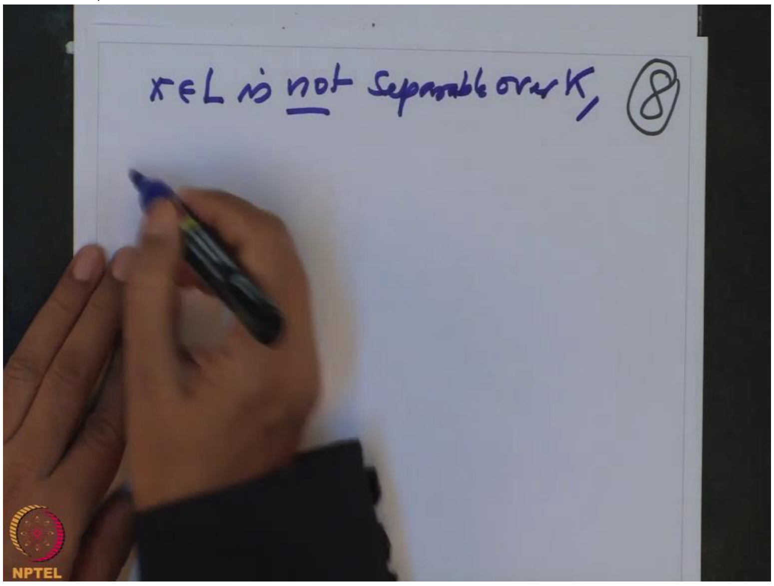
(Refer Slide Time 19:54)




it is not a pth root. a is not a pth root.

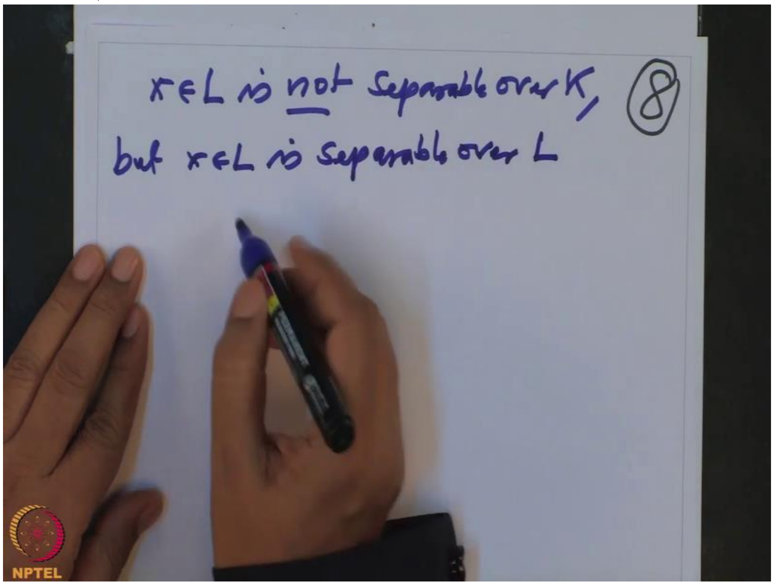
But now, so therefore this L over K is not a separable extension. Or an element x, so element x in L is not separable over K.

(Refer Slide Time 20:17)



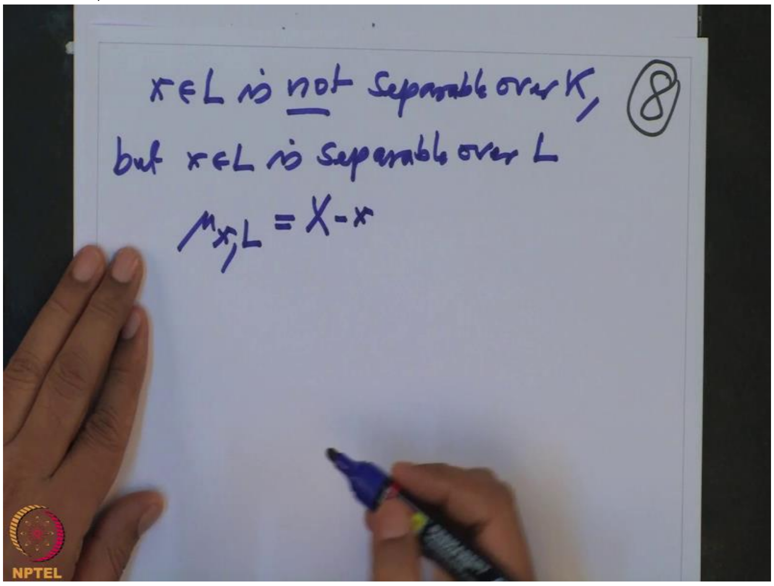

But the element x in L is separable over L

(Refer Slide Time 20:27)



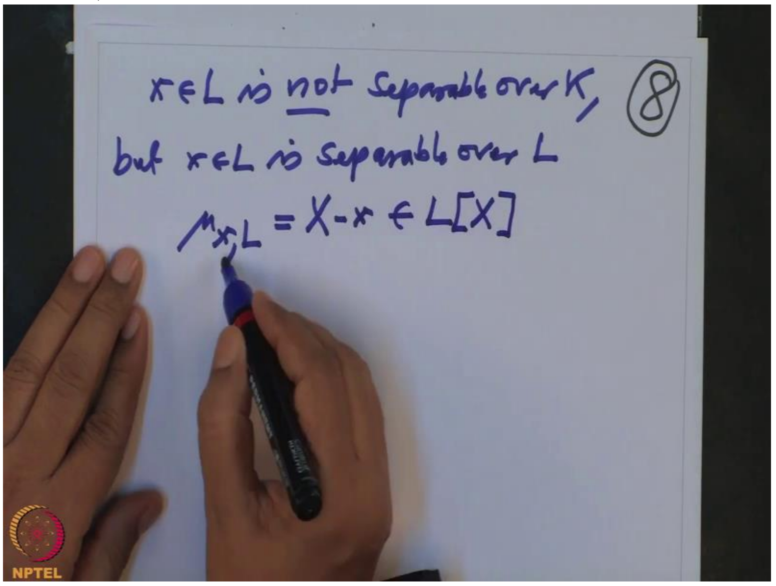

because what is the minimal polynomial of x over L? This is the simple X minus x

(Refer Slide Time 20:33)




polynomial only because X is, this is a polynomial in L X and this is a

(Refer Slide Time 20:38)



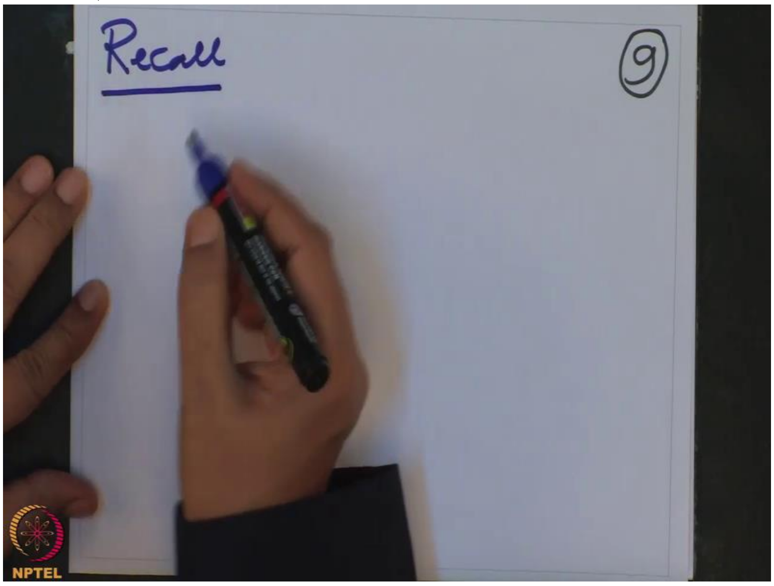

minimal polynomial of x over L which has only the simple zeroes.

So therefore element x is separable over L but the same element x is not separable over K. So this concept, separability of an element, it depends on the base field. It depends on the relative, so it is a relative notion.

So this was the comment I wanted to make, alright. Now to check the numerical criterion, I want; I am looking for easy checking condition which checks that the field extension is separable.

So for that I want to recall, recall that, so in earlier lecture we have considered

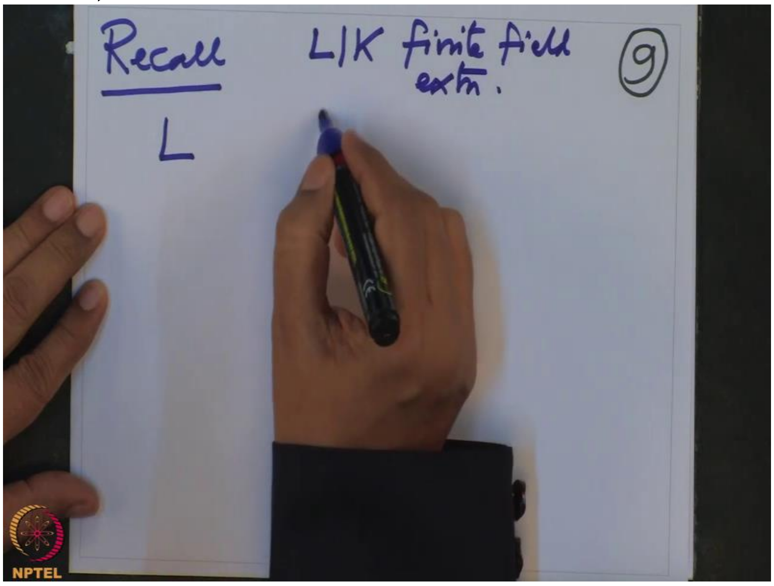
(Refer Slide Time 21:27)




embeddings, K embeddings.

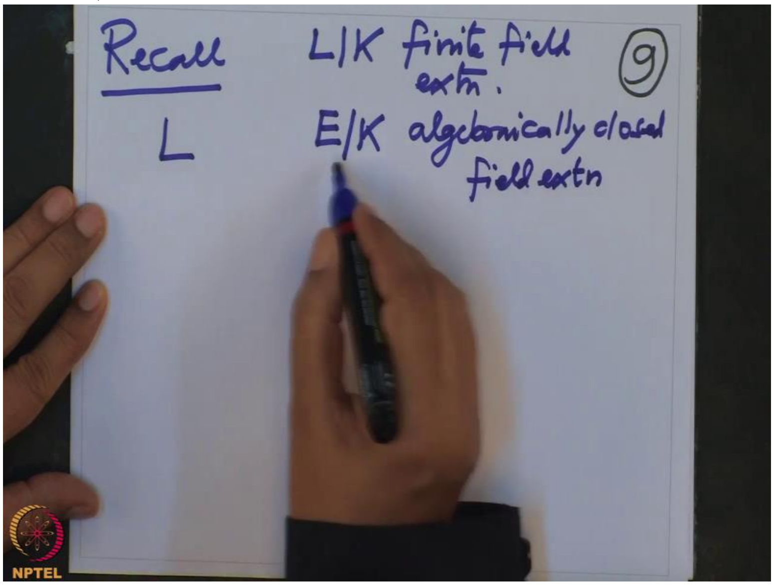
When we have a field extension L over K finite field extension, finite field extension, and

(Refer Slide Time 21:42)



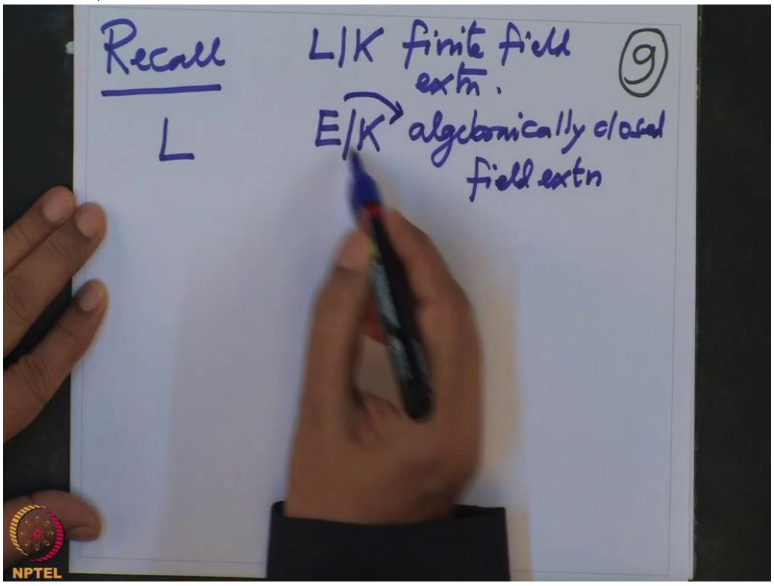

if we have any other extension E over K and E is algebraically closed, algebraically closed field extension.

(Refer Slide Time 21:58)



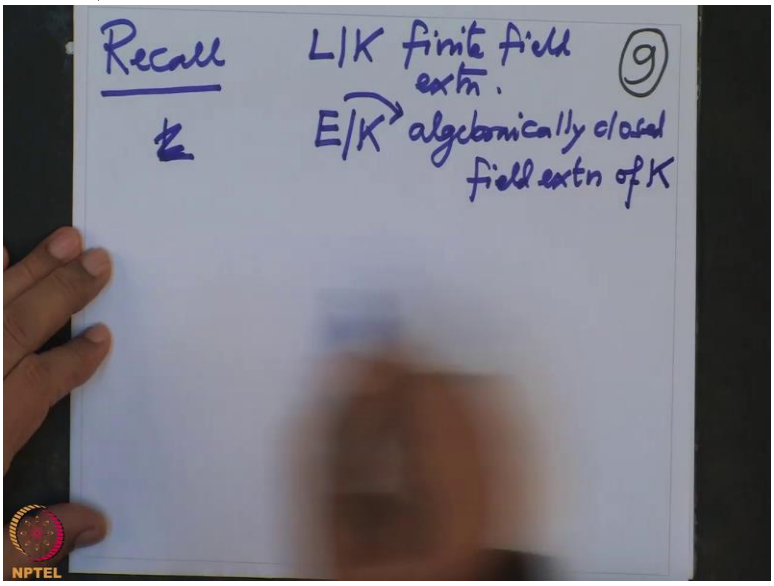

When I write like this that means E is algebraically closed and it is

(Refer Slide Time 22:02)




an extension of K. I am not saying E over K is algebraic, Ok so I will keep writing an algebraically closed field extension of K

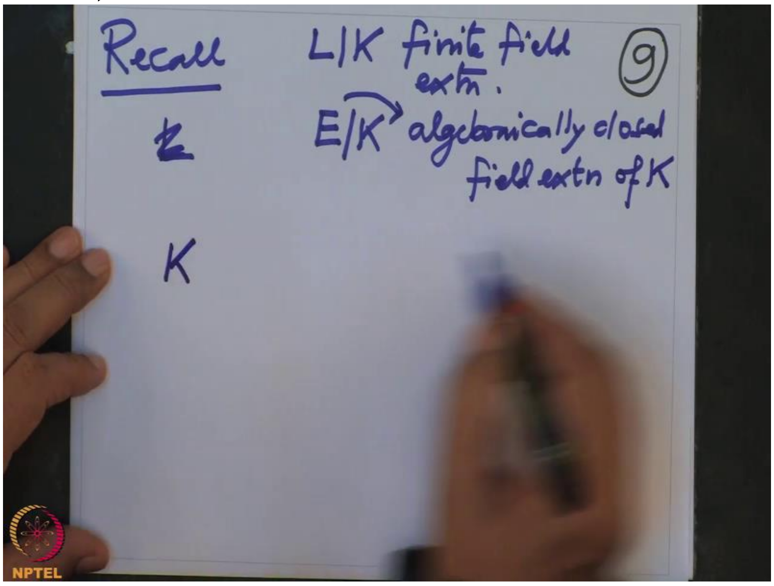
(Refer Slide Time 22:14)




that may not be algebraical closure.

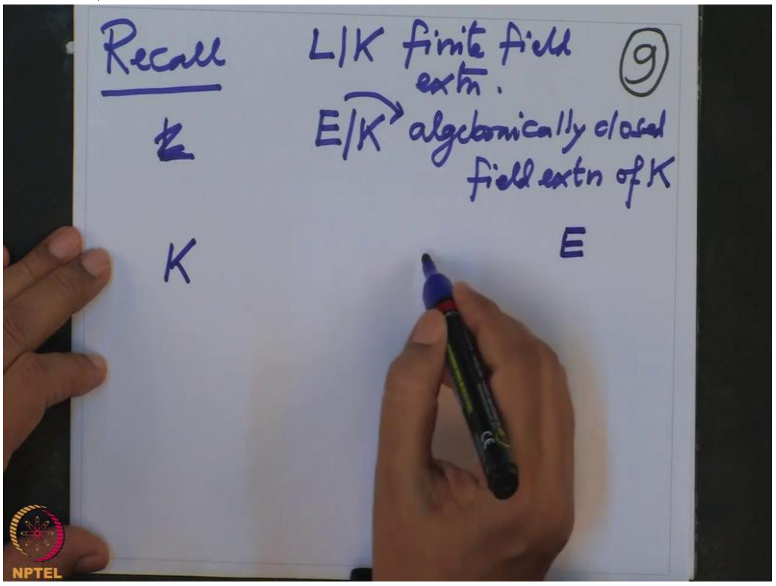
But definitely if I look at K is here,

(Refer Slide Time 22:19)



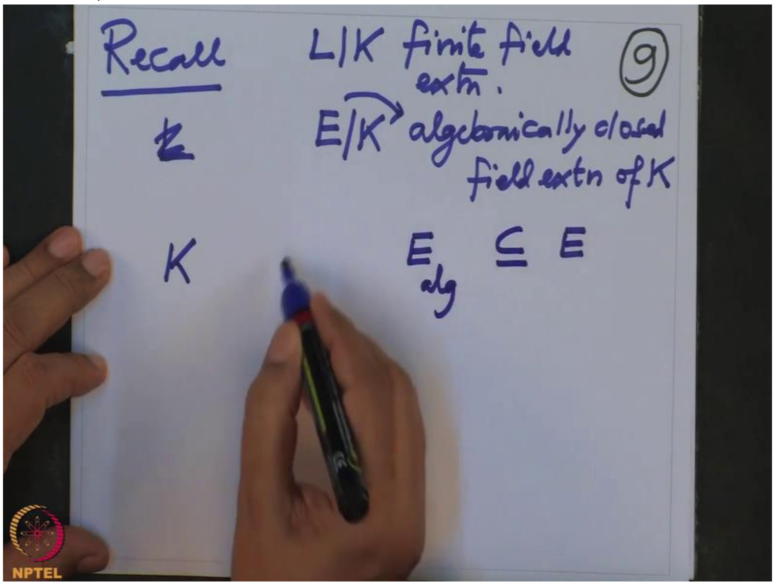

E is here

(Refer Slide Time 22:21)



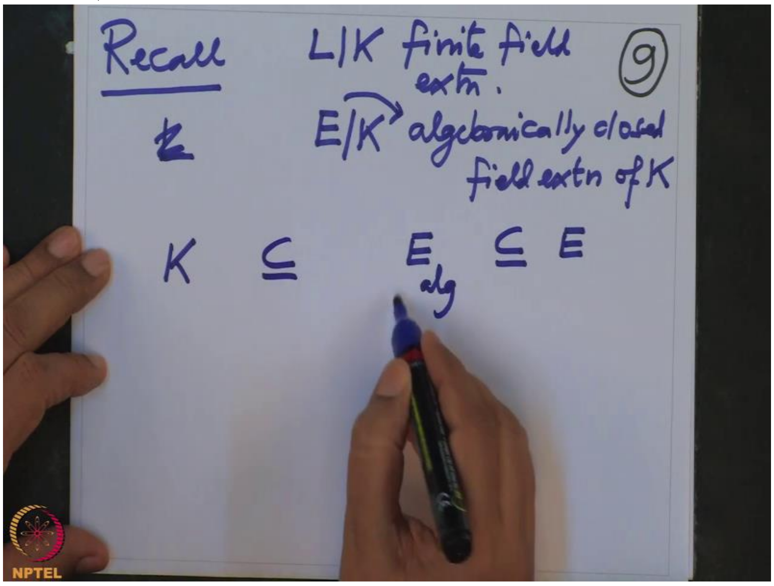

and if I look at the relative algebraic closure a l g, this is the set of

(Refer Slide Time 22:26)



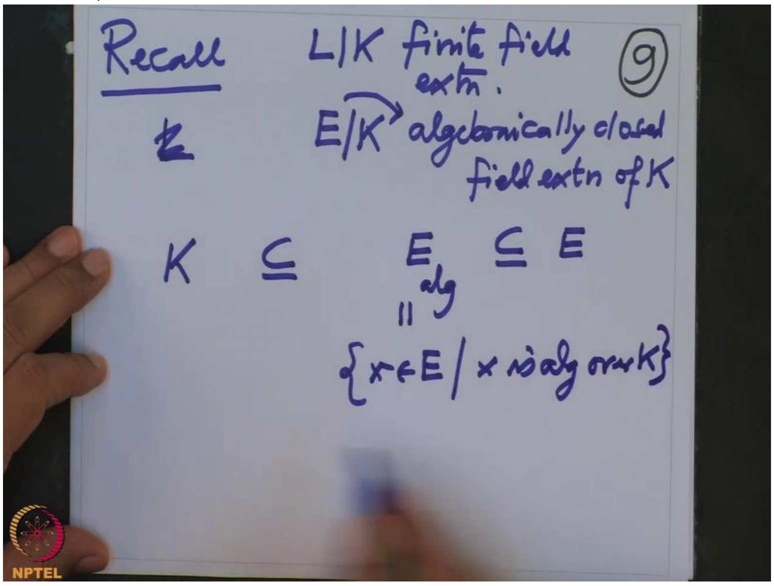

all algebraic

(Refer Slide Time 22:27)



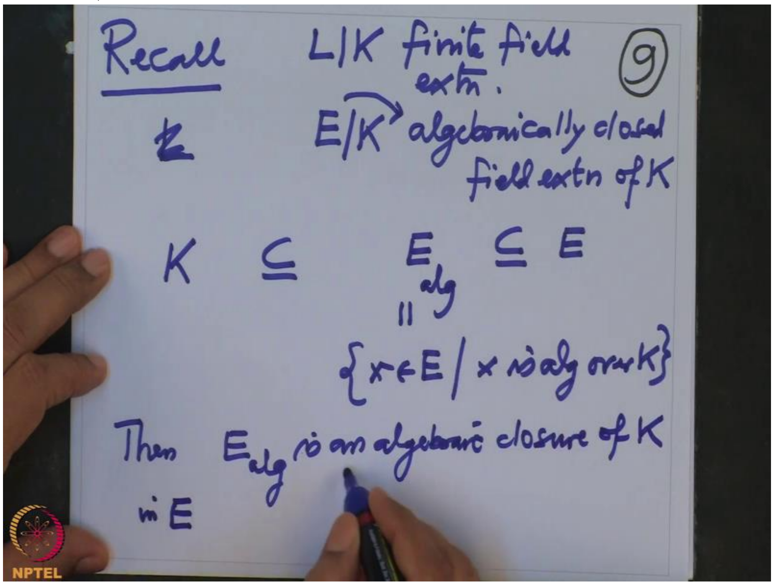

elements, all those x in E such that x is algebraic over K then

(Refer Slide Time 22:38)




this E a l g is an algebraic closure of K inside in E.

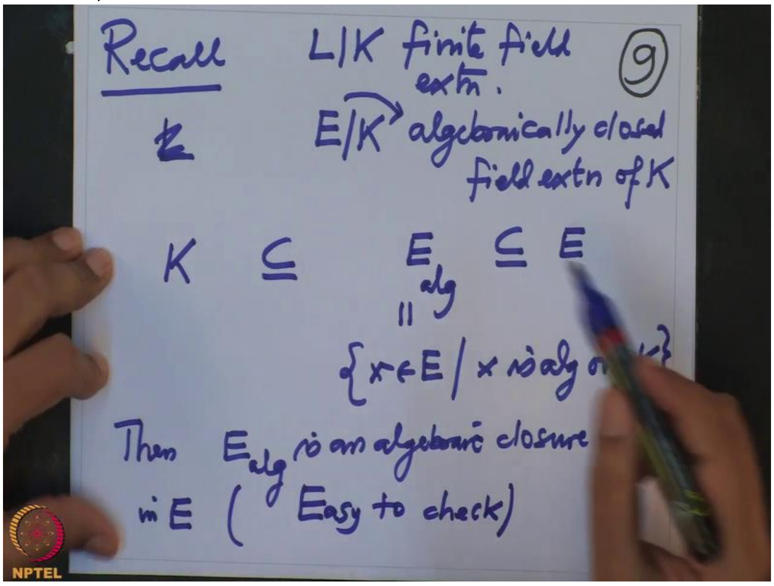
(Refer Slide Time 22:56)




So this is easy to check, so easy to check. So what do we need to check?

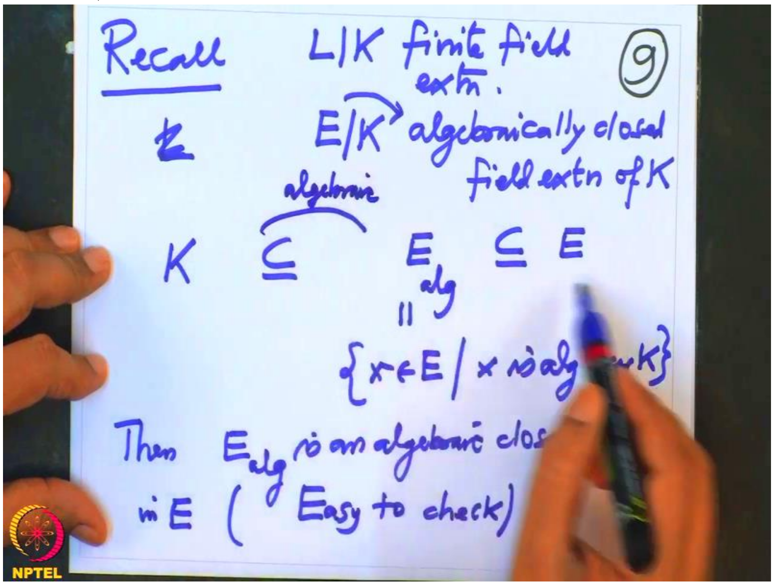
Let me spell out what do we need to check.

(Refer Slide Time 23:04)




First of all, because this extension is now algebraic, because I have taken only those elements which are

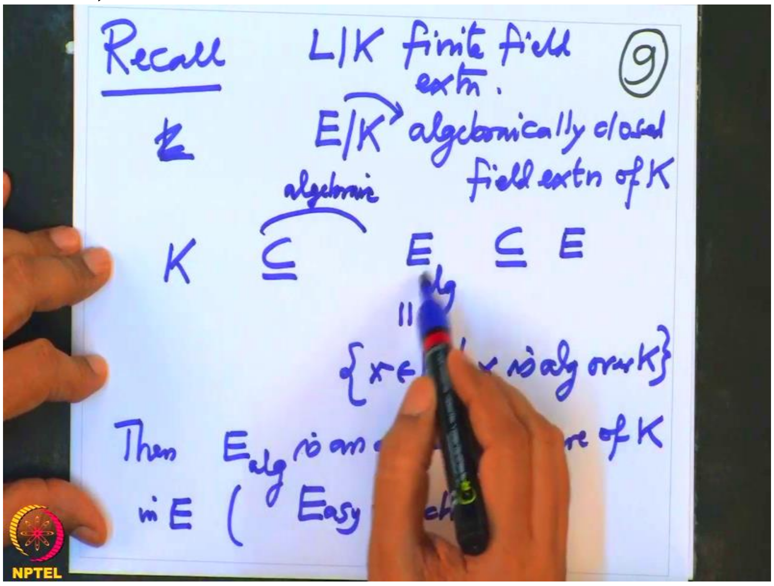
(Refer Slide Time 23:11)




algebraic over K. So this extension is algebraic.

All that we

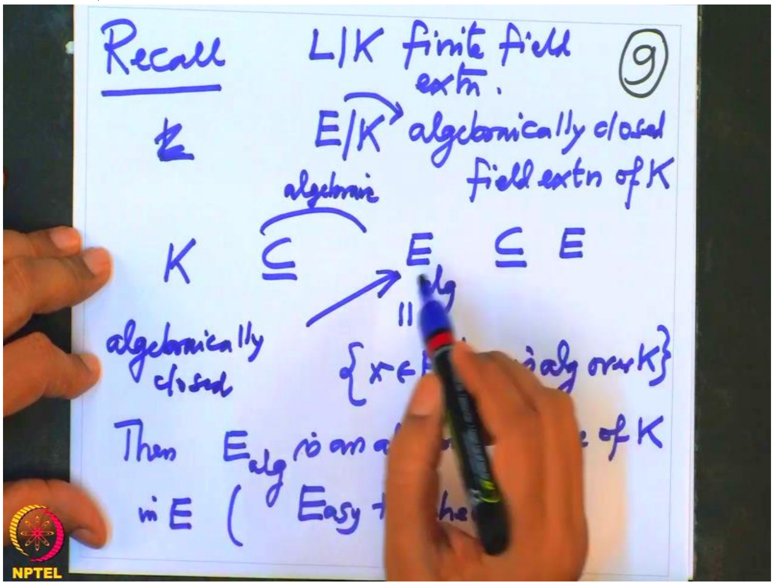
(Refer Slide Time 23:15)




need to check is that this field, this is a field also, we know. So this field is algebraically closed. That is what we need to check.

And how does one check the field is algebraically closed?

(Refer Slide Time 23:28)

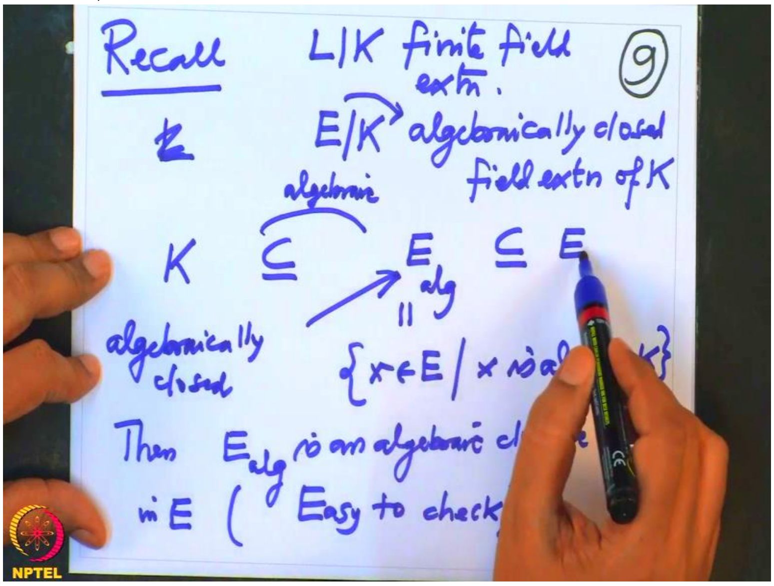



We take a polynomial with coefficients in that field. And we want to check that it has a 0 inside this field. That is enough to check.

Or in other words we want to check that any irreducible polynomial here is linear. So if you take any, any element here we need to check that, we need to check that this field is algebraically closed.

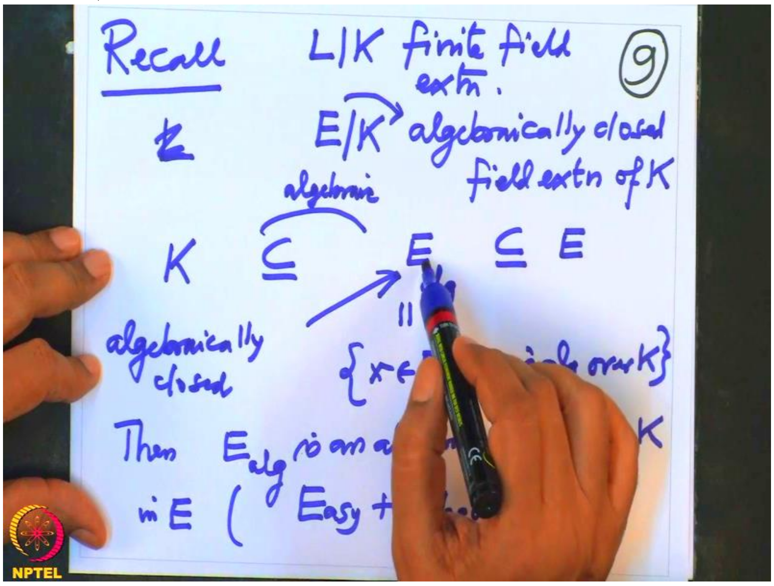
That means you take a polynomial f and consider that

(Refer Slide Time 23:57)




as an polynomial in with coefficients in E, so and E is algebraically closed. Therefore definitely that polynomial has a 0 here. We want to prove that, that 0 is

(Refer Slide Time 24:08)

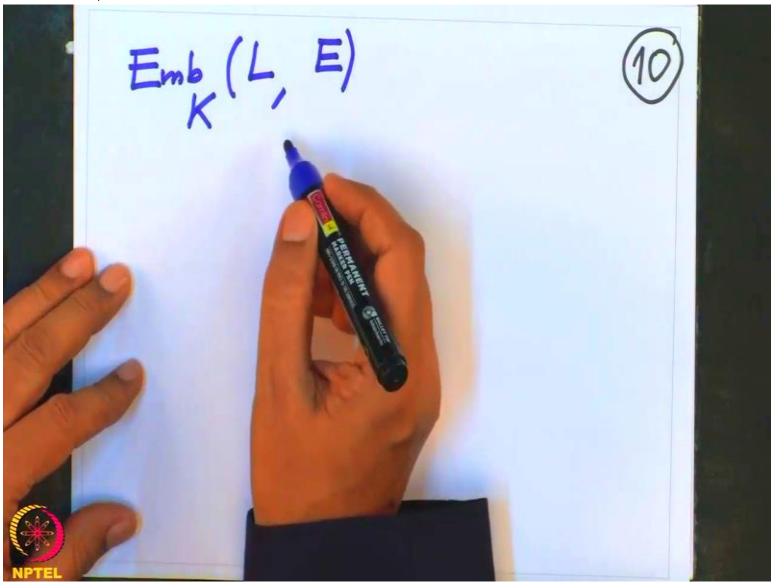



automatically here.

But that will follow from the transitivity of algebraic elements, so which I will not write down the proof here. This is easy to check that, this is one way to restrict it to algebraic closure of K, alright.

So now we want to do that? So we have considered the embeddings, embeddings of, K embeddings of L inside E. Remember E is algebraically closed.

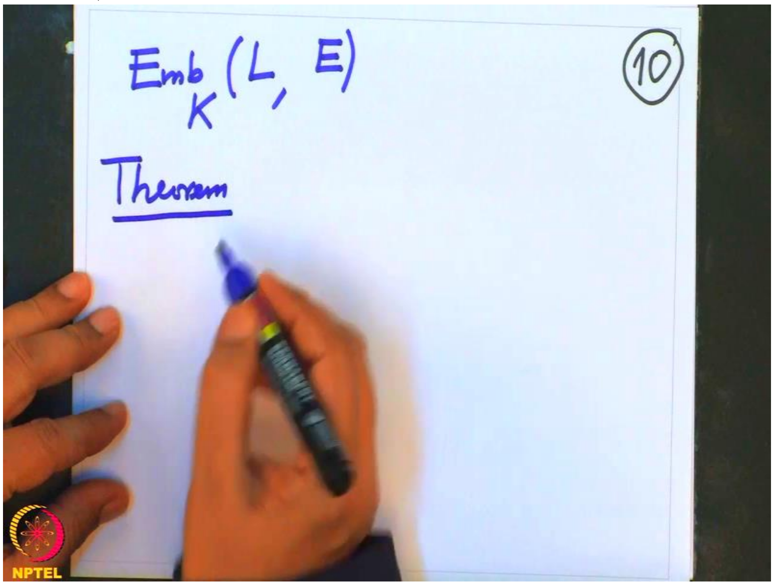
(Refer Slide Time 24:43)




So K embed, this set I want to, I want to prove the theorem, this theorem I want to prove.

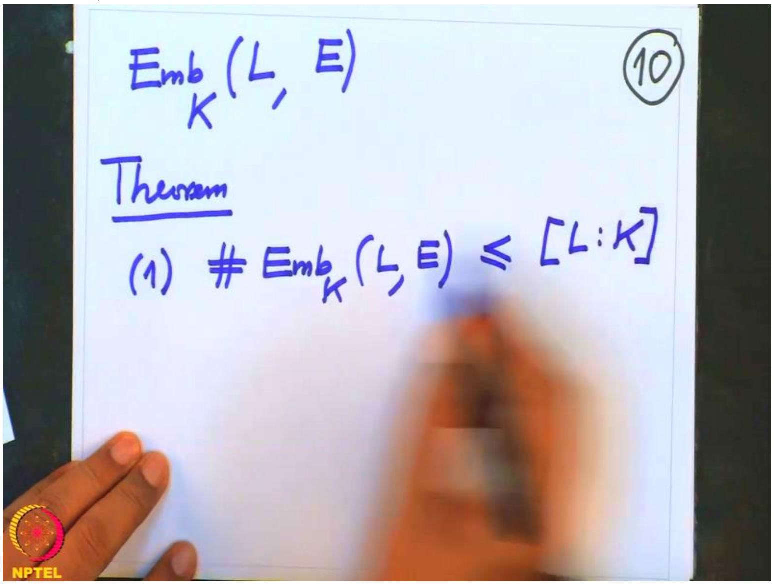
This theorem has

(Refer Slide Time 24:54)



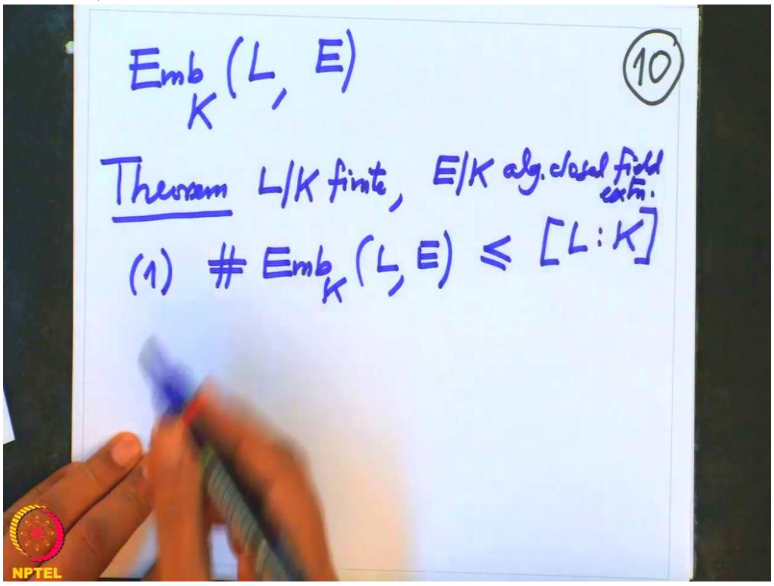

two parts. Part 1, the number of embeddings of L in E, this number smaller equal to the degree of L over K

(Refer Slide Time 25:13)



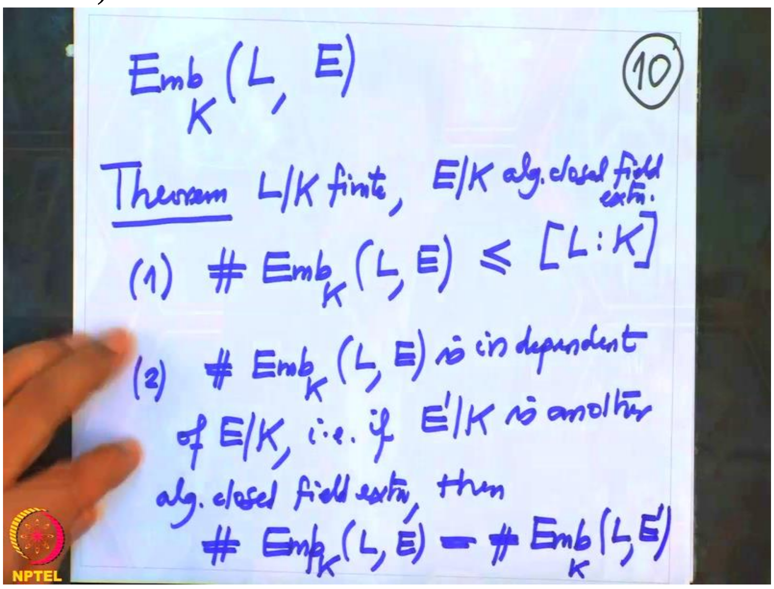

and this is L over K finite extension and E over K algebraically closed field extension. This is part 1

(Refer Slide Time 25:31)




And part 2, I want to show that this number, number of embeddings is independent of E over K. That means that is, if E prime over K prime is another algebraically closed field extension, then these two numbers are equal, number of K embeddings of L in E is same thing as number of K embeddings of L in E prime.

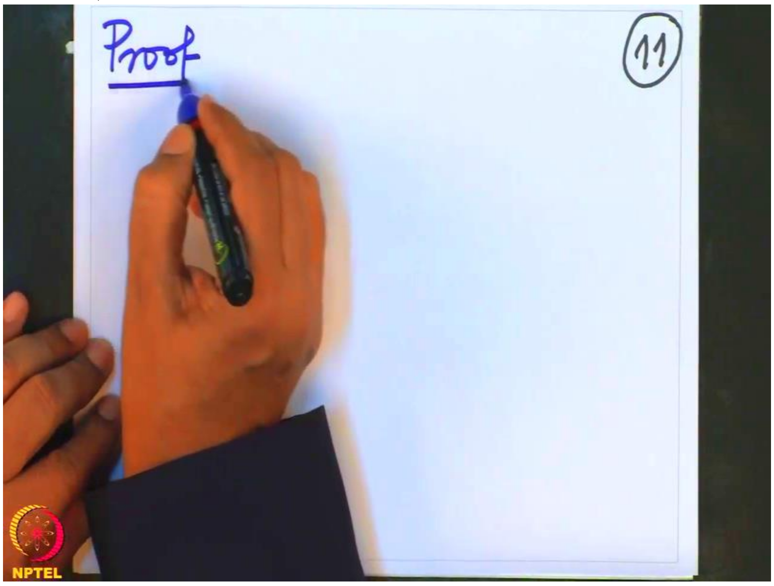
(Refer Slide Time 26:27)




And then that number is called the degree of separability of L over K if I prove this.

So let us prove at least first part. So it is very easy and proof, what I will use is

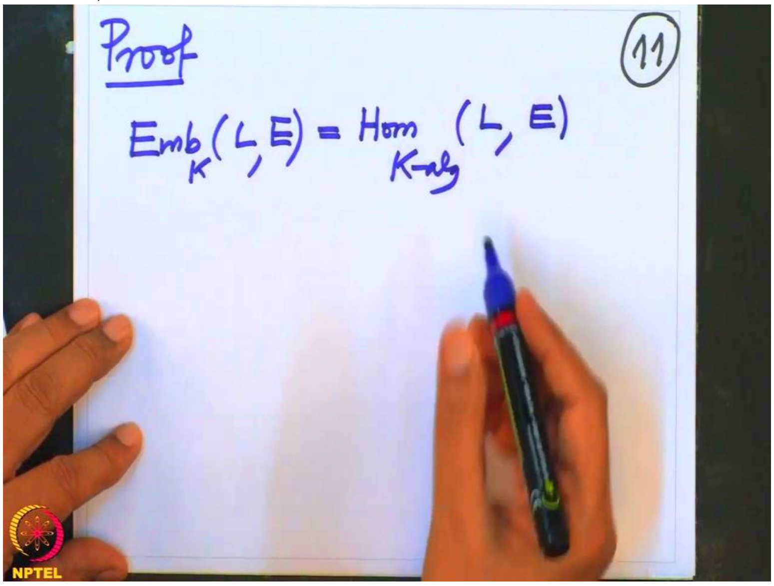
(Refer Slide Time 26:42)




old long time back we have proved Dedekind and Artin lemma and I will use that again here. So note that what are the embeddings.

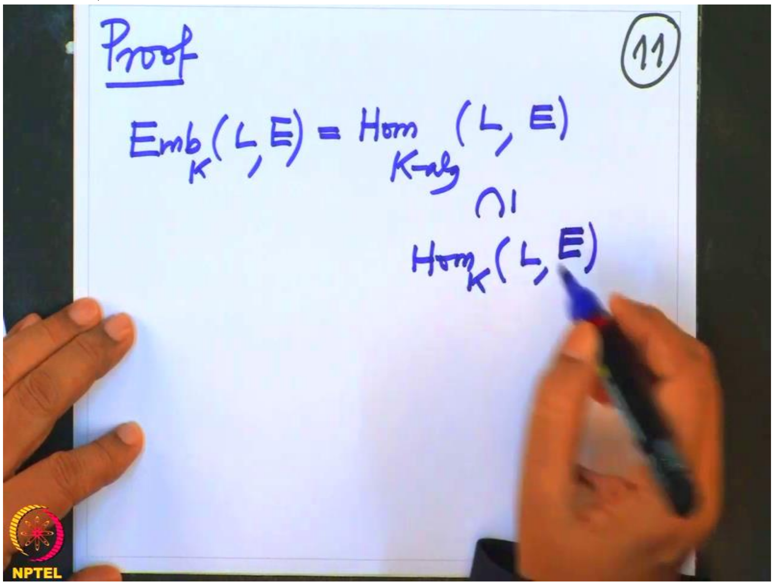
The embeddings of L in E, they are precisely the K-algebra homomorphisms from L to E

(Refer Slide Time 27:07)



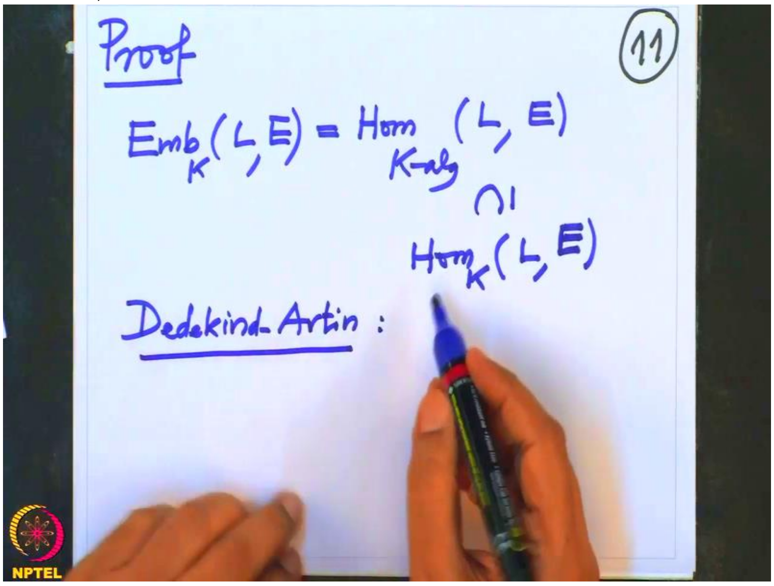

and this is a subset of K linear maps from L to E, because K-algebra means it is a ring homomorphism and K linear and this is just K linear map, they need not respect the multiplication.

(Refer Slide Time 27:22)



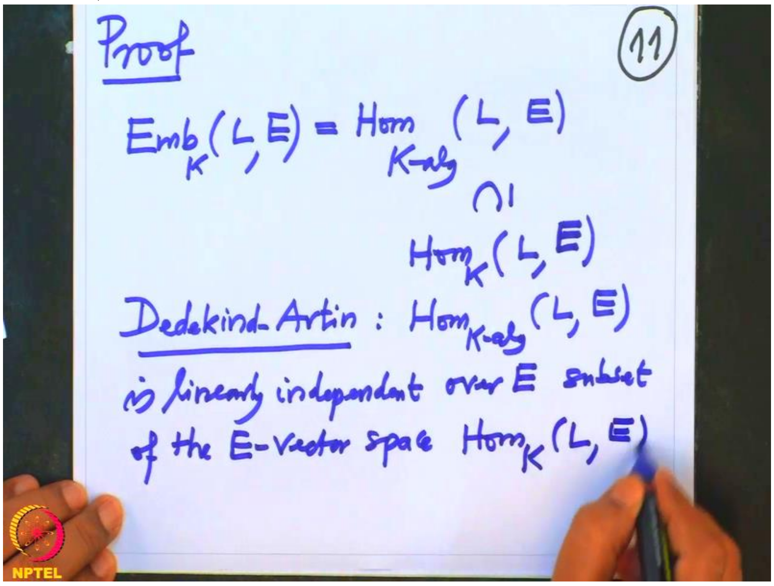

So this is clearly subset here and what Dedekind and Artin say? Dedekind and Artin say, Dedekind and Artin lemma, that says that

(Refer Slide Time 27:35)




this set Hom K-algebra of L in E, this set is linearly independent subset, linear independent over K, over E not over K, over E subset of the E vector space Hom K L E,

(Refer Slide Time 28:14)

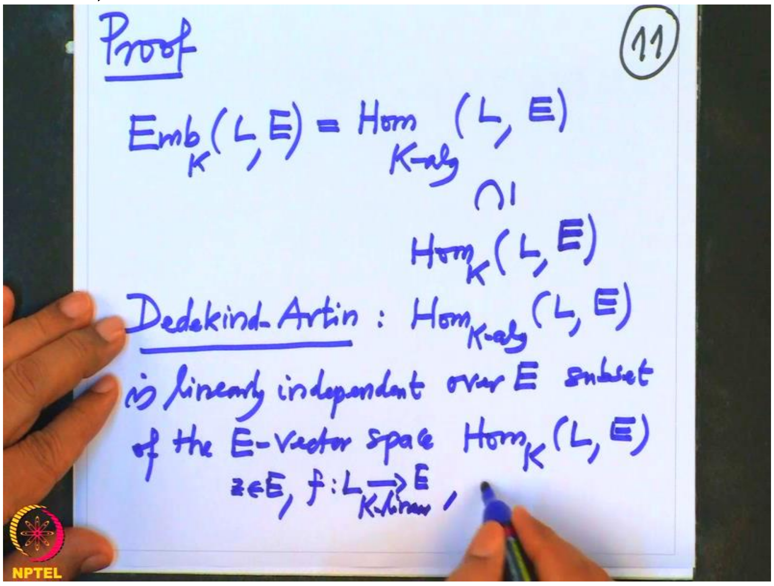



this.

This is E vector, not only K vector space, this is E vector space and what was the vector space multiplication?

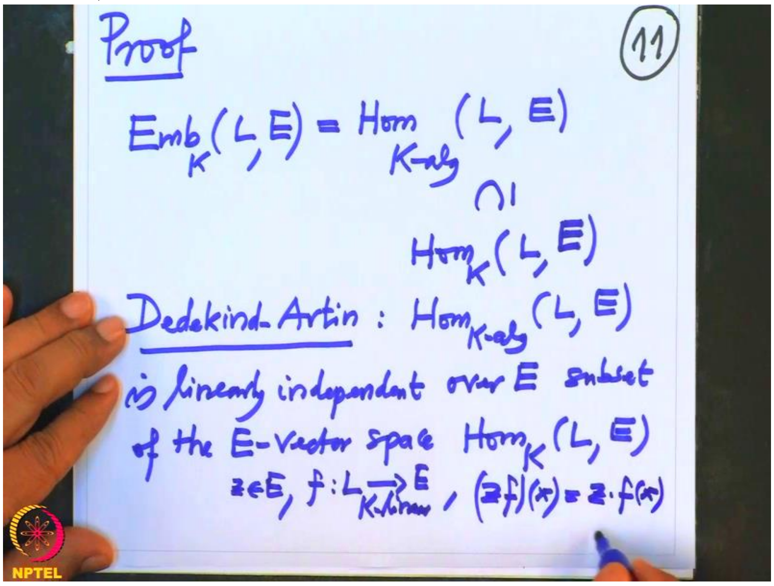
That is if I have z in E and a K linear map f L to E, K linear then how did we

(Refer Slide Time 28:35)



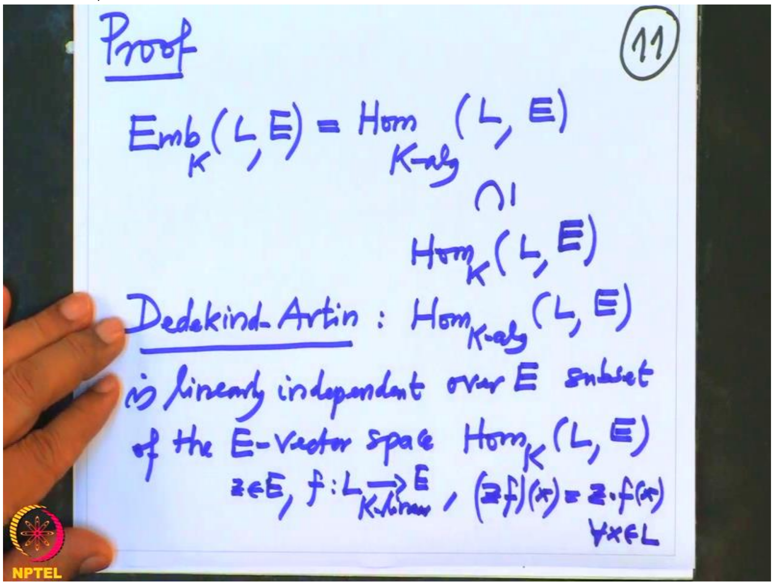

define z times f, this on only x in L? It is defined z times f x

(Refer Slide Time 28:43)




for every x in L. This is z is in E, x is in E therefore

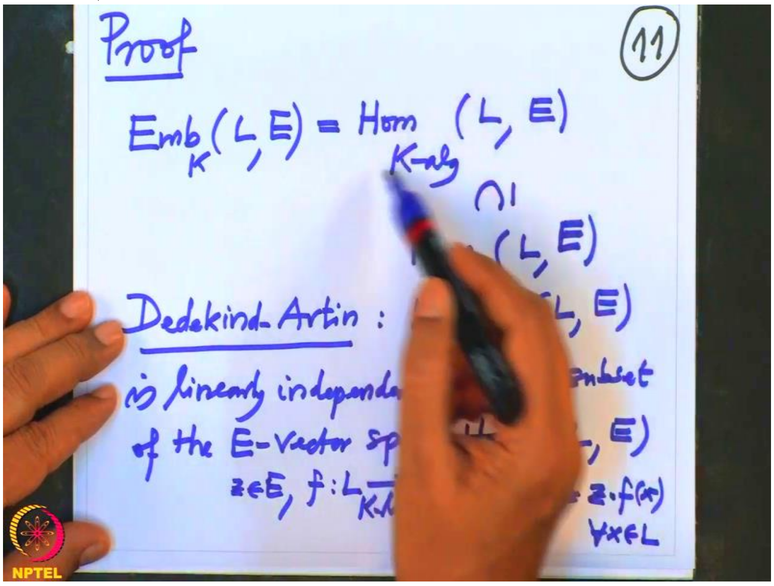
(Refer Slide Time 28:50)




this is defined with a multiplication in E.

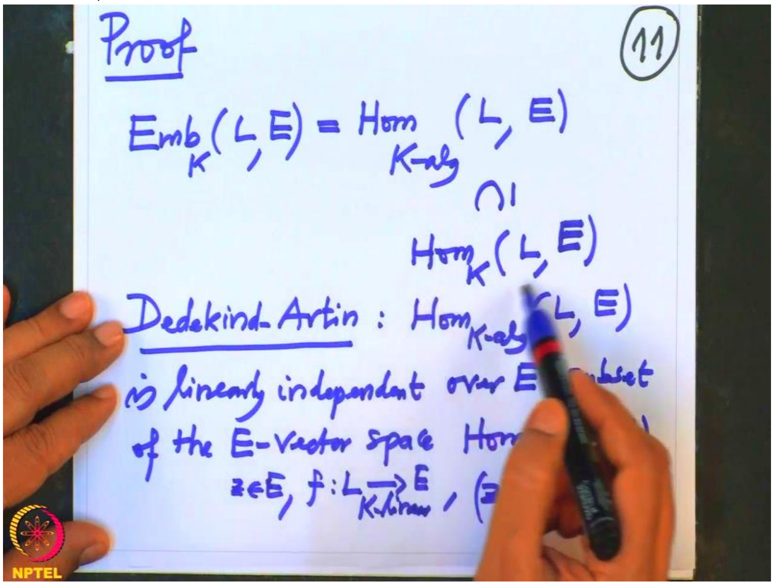
So these are linearly independent, particular the cardinality

(Refer Slide Time 28:57)




of this set will be less equal to

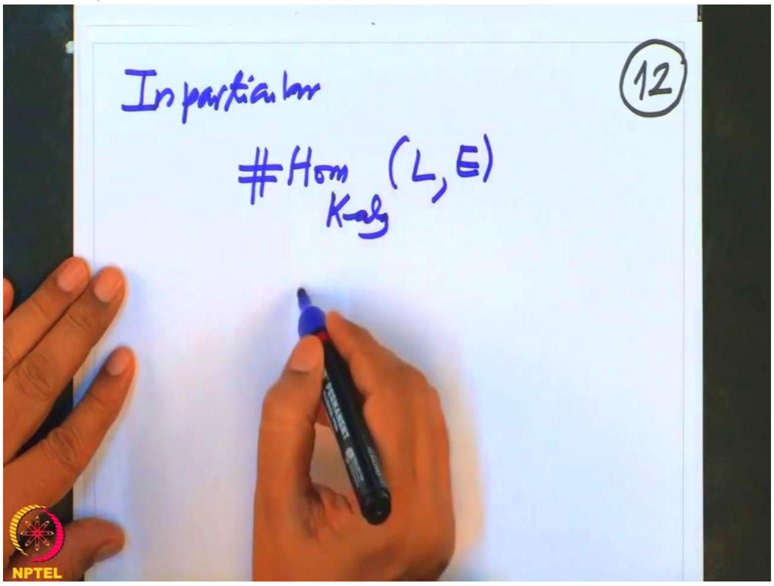
(Refer Slide Time 29:01)




cardinality, dimension of this vector space.

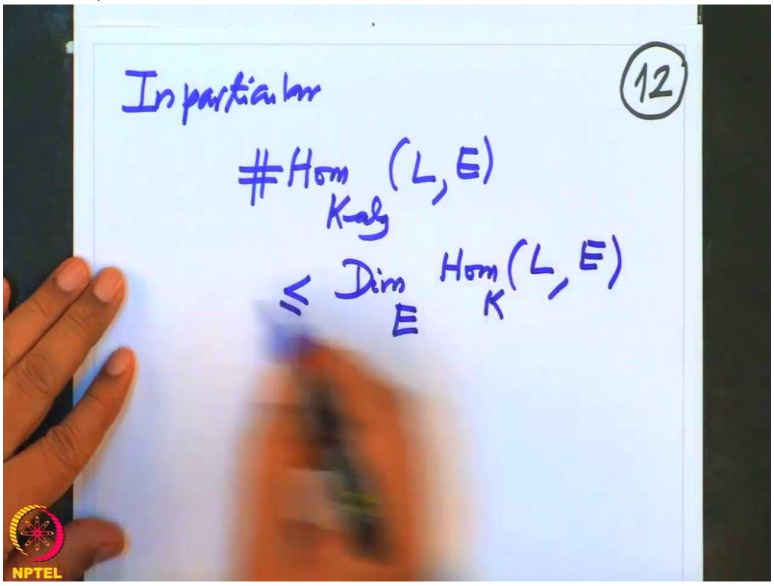
So in particular cardinality of Hom K-algebra L E, this cardinality

(Refer Slide Time 29:20)



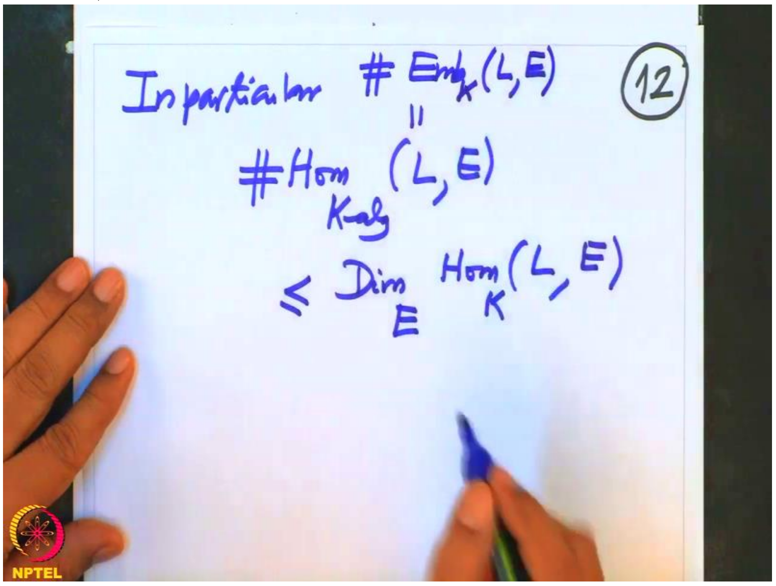

will be less equal to dimension of, E dimension of the vector space Hom K L E

(Refer Slide Time 29:33)



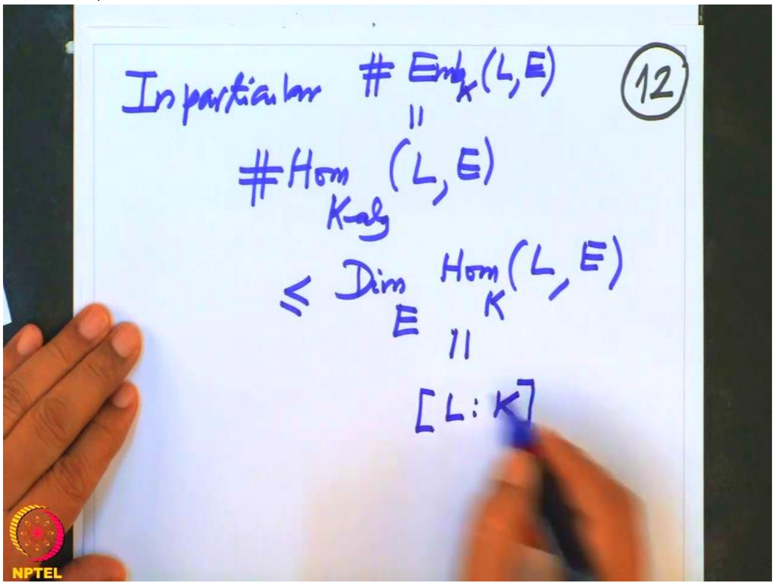

and this is precisely the number of embeddings.

(Refer Slide Time 29:43)



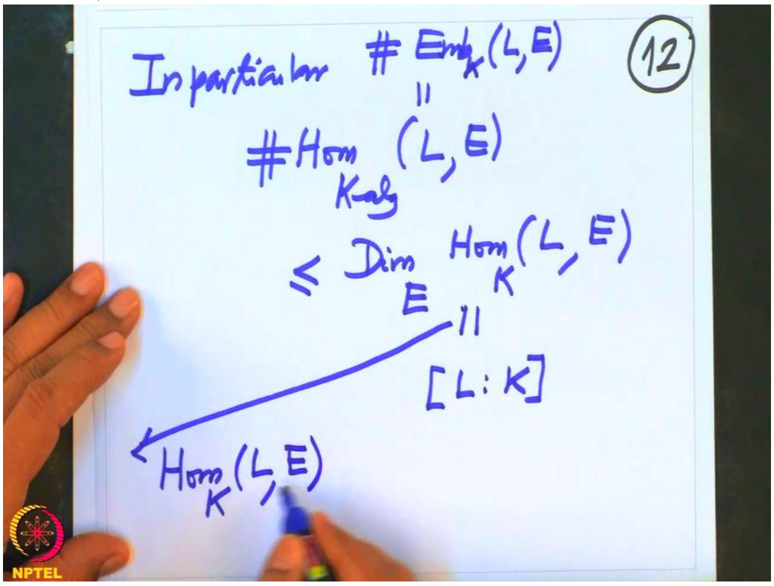

And this, what is this dimension? I want to compute. So let us compute this dimension, this is equal, I claim that this dimension is precisely equal to the degree L over K.

(Refer Slide Time 29:58)



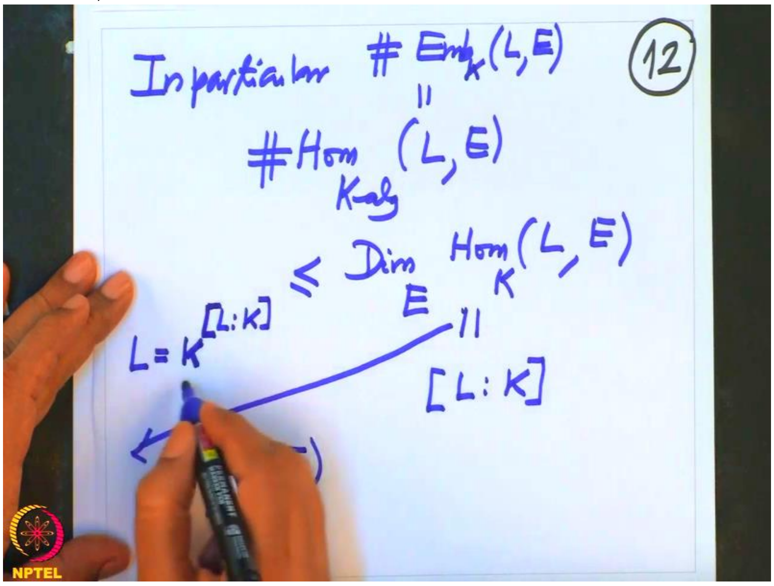

This equality follows from the following. So look at this vector space, Hom there are K linear maps on K to E.

(Refer Slide Time 30:08)




But E, L is a finite extension therefore L as a vector space is isomorphic to K power L, degree of L, degree of L over K because

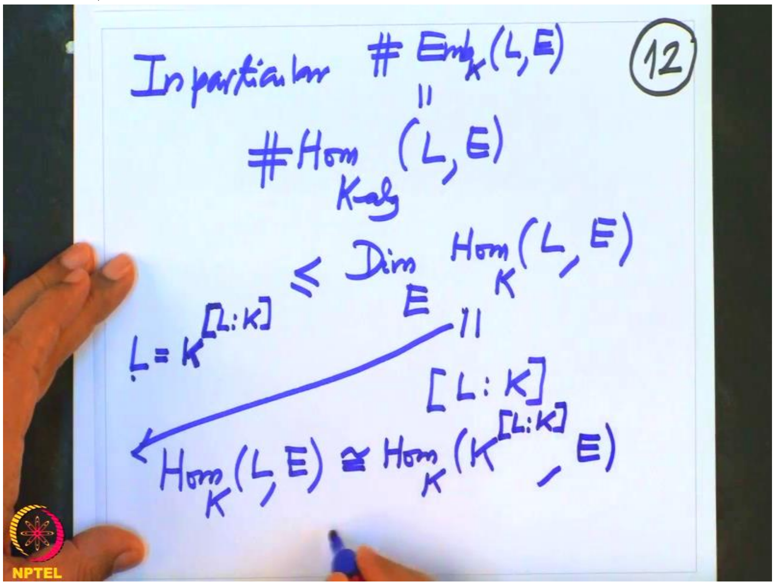
(Refer Slide Time 30:22)




this L is a vector space of this dimension.

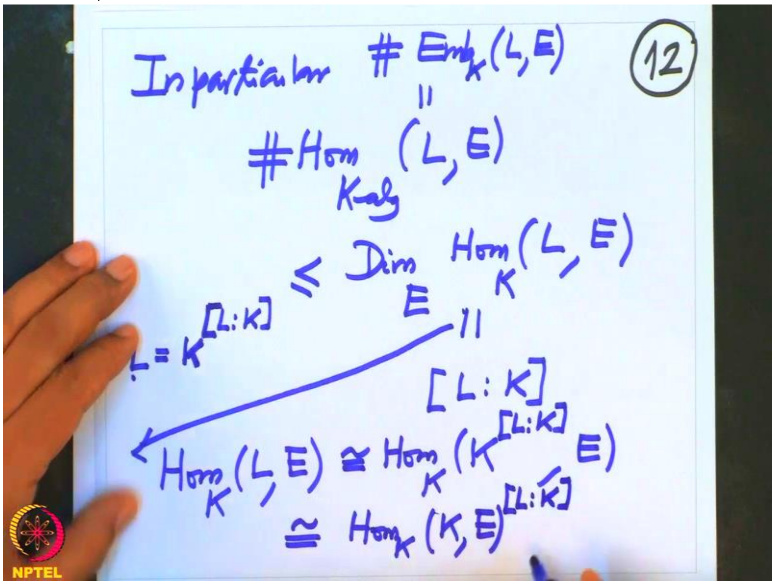
So therefore this is same thing as Hom K K power L over K E but

(Refer Slide Time 30:36)




this is isomorphic to, clearly this degree will come out. This is Hom K K E power L over K degree

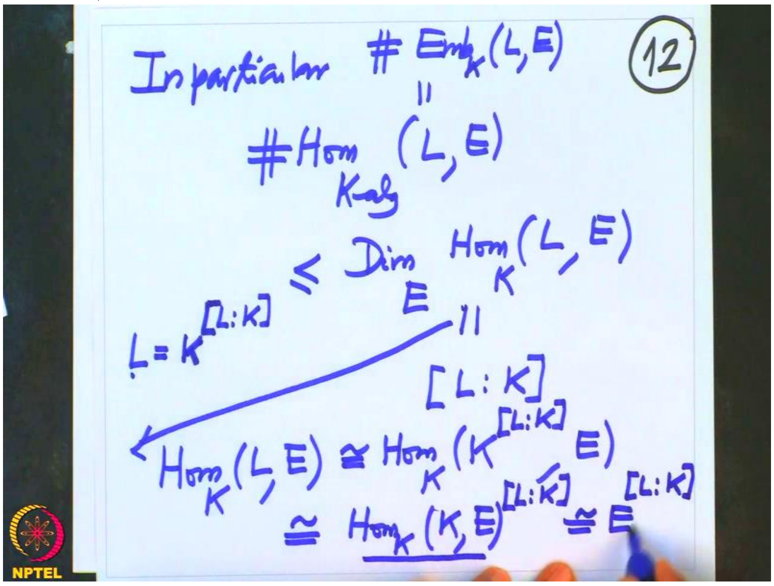
(Refer Slide Time 30:48)




but this is, this is isomorphic to E. So this is E power L over K

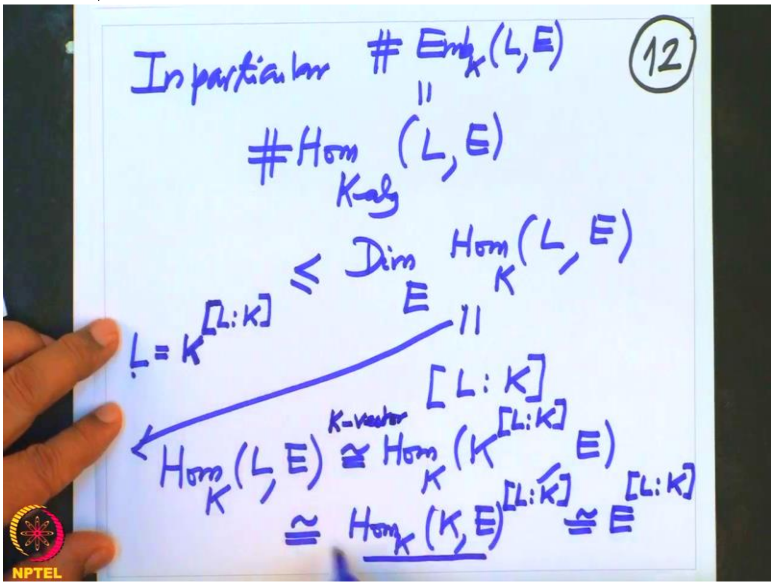
So it is

(Refer Slide Time 30:59)



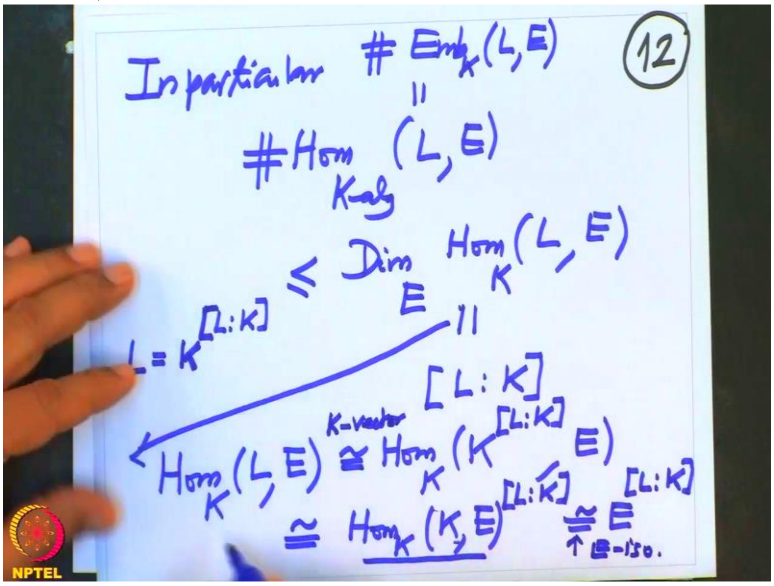

vector space E power, so all these isomorphisms are, isomorphism as, this is isomorphism as K vector spaces,

(Refer Slide Time 31:13)




and this is isomorphism as K vector space and the last one is E isomorphism. Therefore

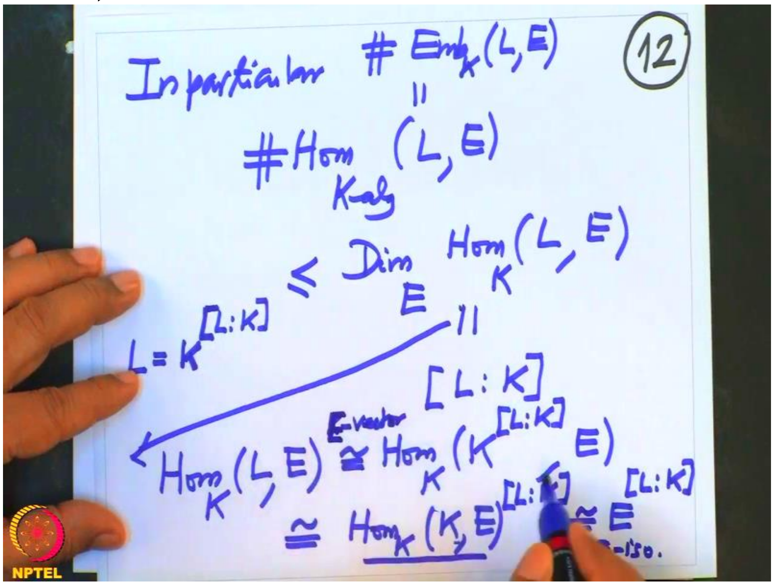
(Refer Slide Time 31:22)




altogether this will be all E isomorphism.

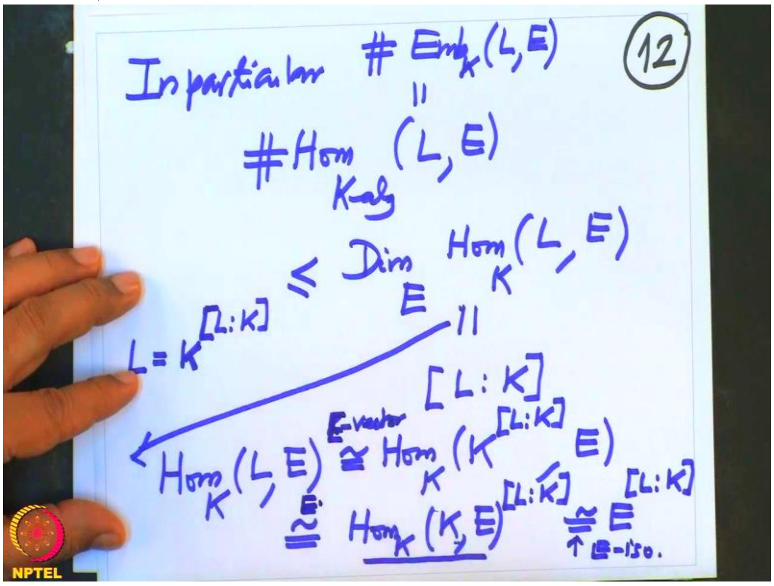
These are all E isomorphisms, sorry E.

(Refer Slide Time 31:28)



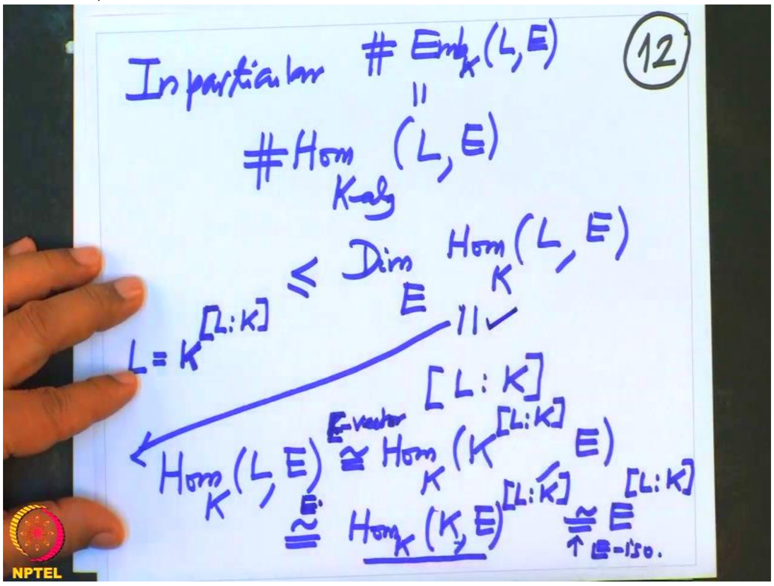

This is also E isomorphism,

(Refer Slide Time 31:31)




this is also E isomorphism therefore the, this dimension equal to dimension of this but which is clear that L over K,

(Refer Slide Time 31:41)

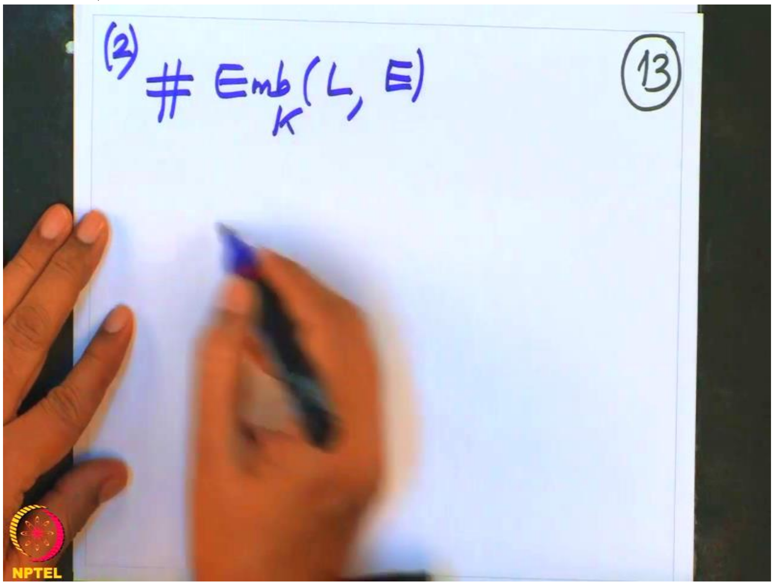



therefore we know this.

So therefore we proved the equality in, inequality in 1 and I will indicate the, inequality now 2. Remember we now want to prove that this is independent of E algebraically closed extension of K. So I want to prove that, so this is the proof of 2.

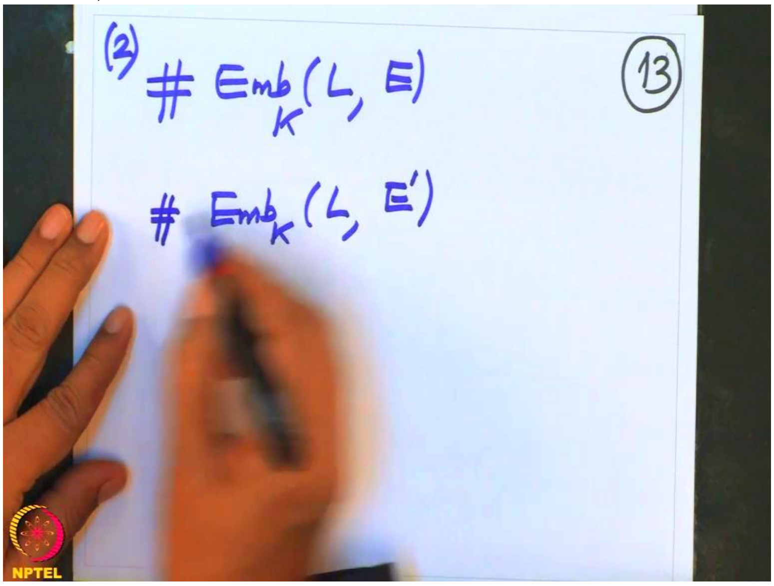
The cardinality of embeddings of L in E or

(Refer Slide Time 32:18)



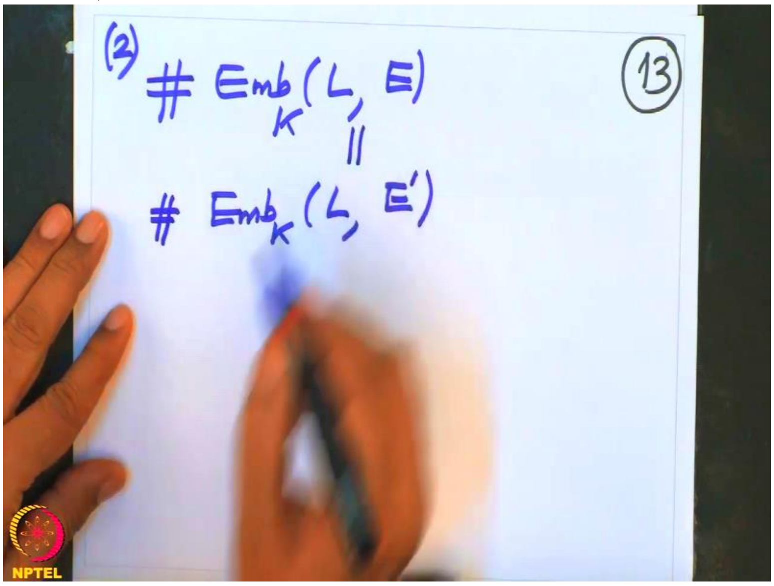

cardinality of the embeddings of L in some other algebraically closed extension; I want

(Refer Slide Time 32:25)




to prove these are equal,

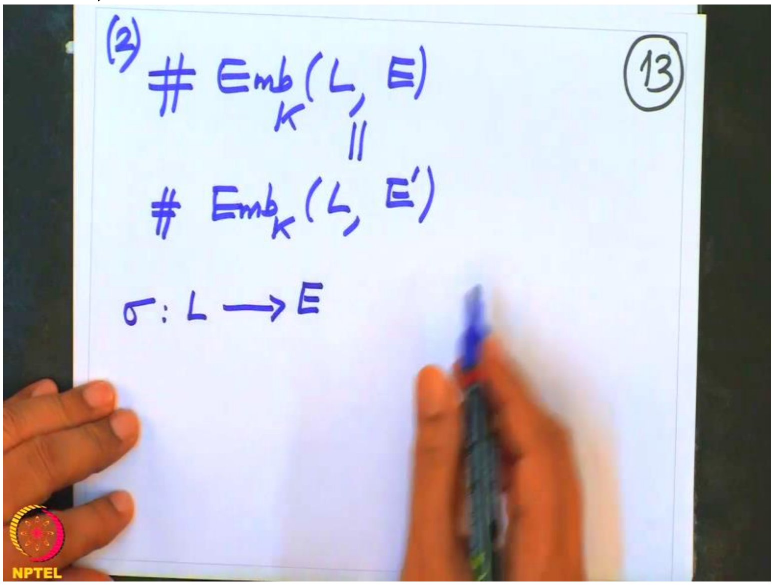
(Refer Slide Time 32:27)




Ok.

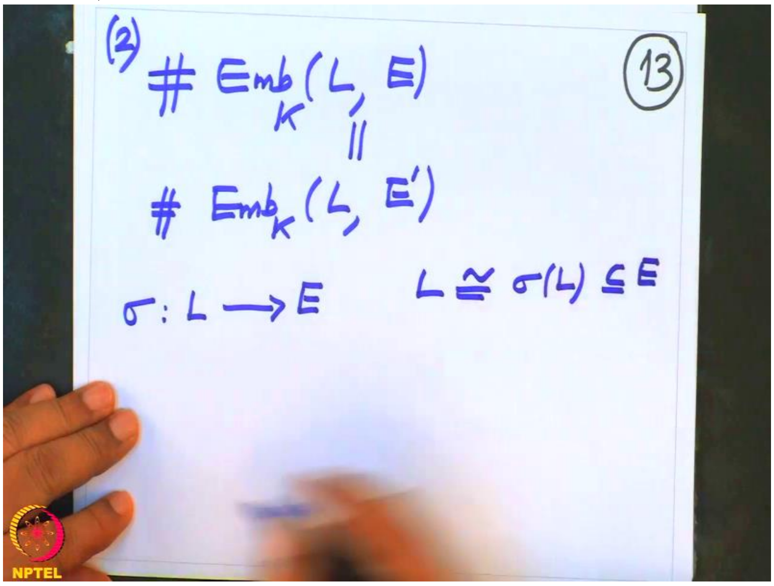
But that is also very simple because now look at the embedding sigma L in E. So

(Refer Slide Time 32:38)



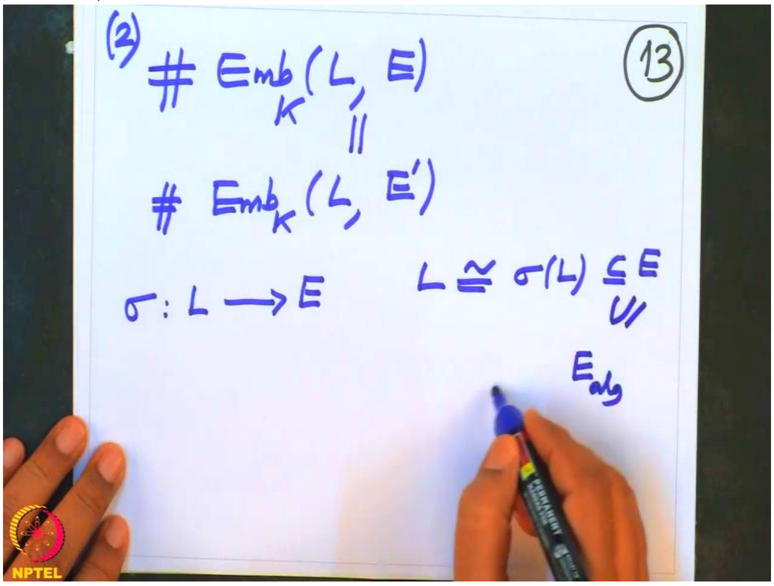

look at the image in sigma that is sigma L. So L is isomorphic to sigma L and this is contained in E.

(Refer Slide Time 32:48)



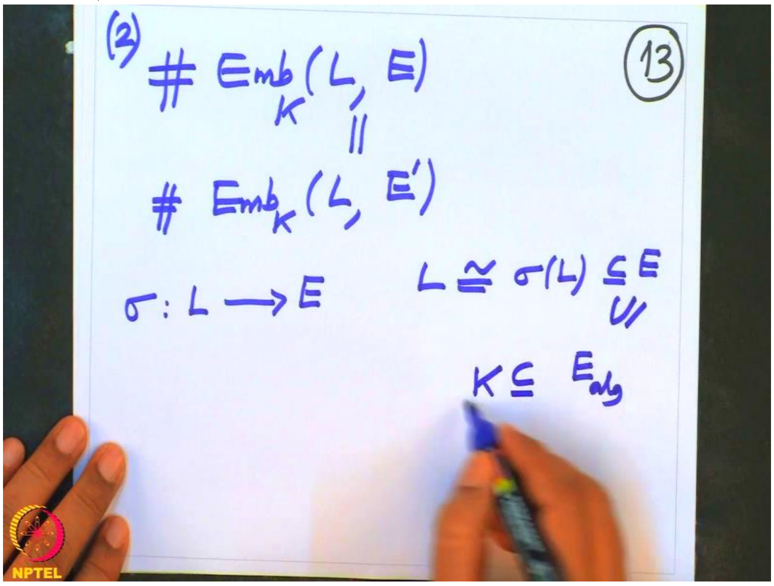

So I am going to replace and this one we have E a l g here, what is E a l g?

(Refer Slide Time 32:59)



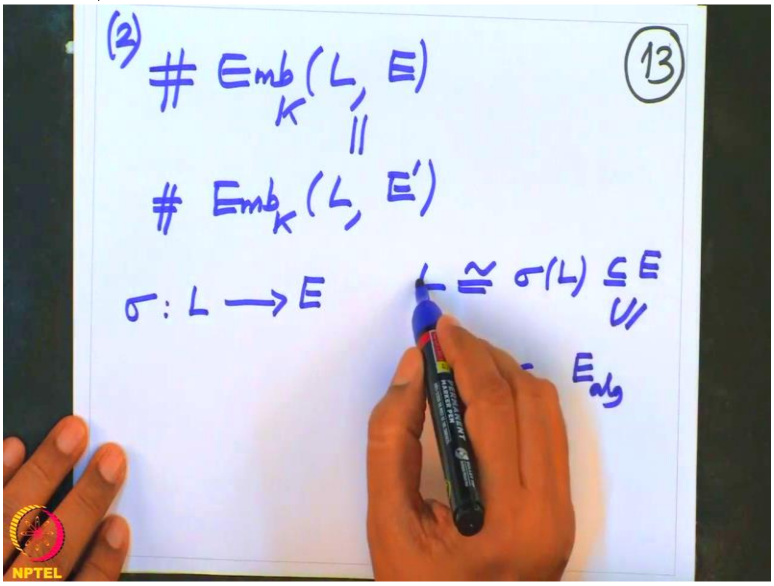

That is an algebraic closure of

(Refer Slide Time 33:01)



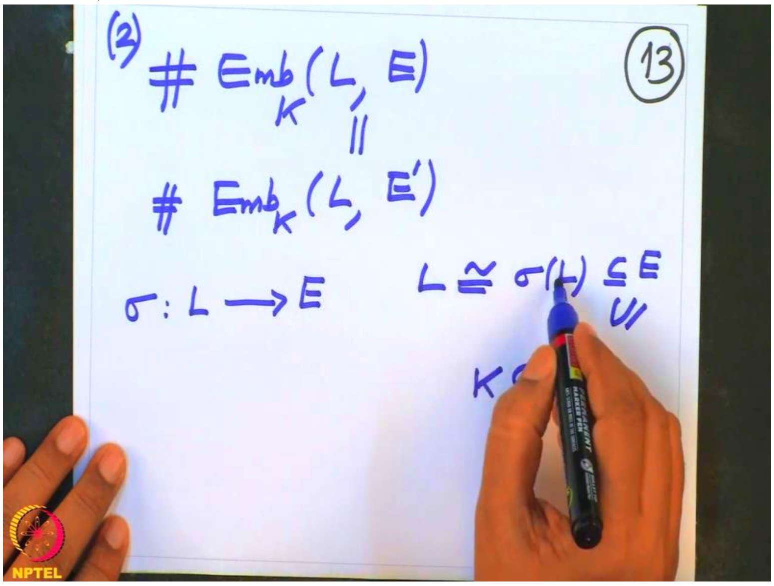

K in E. This is algebraic closure of K in E. We have considered it earlier also. Now because L is finite,

(Refer Slide Time 33:10)



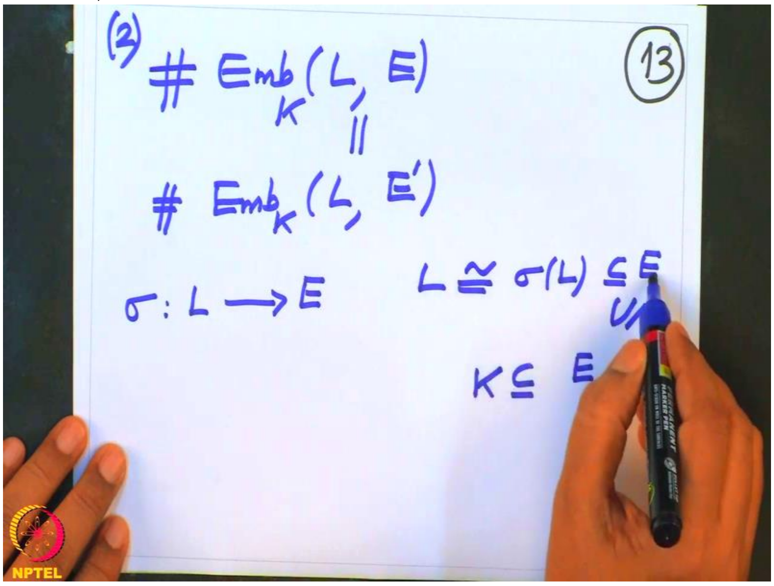

this is algebraic over K.

(Refer Slide Time 33:12)




Sigma L is an element,

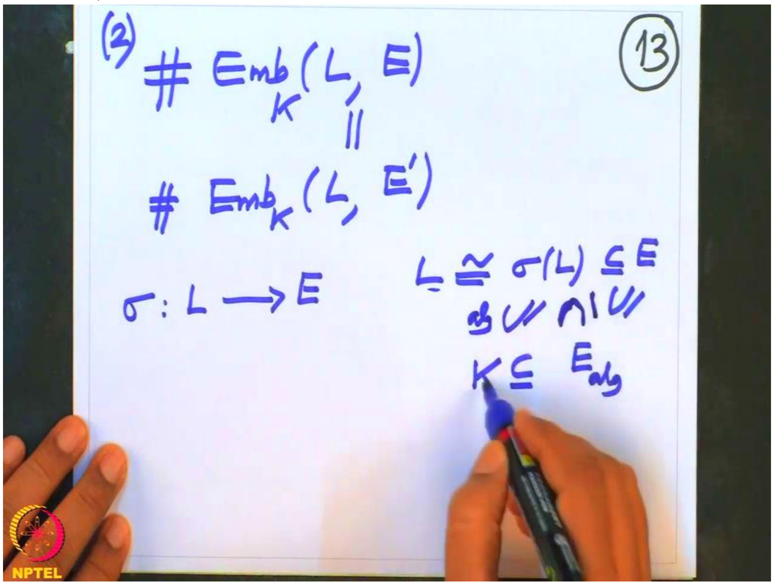
(Refer Slide Time 33:14)




elements of E which are algebraic over K because the elements of L are algebraic over K, this extension is algebraic.

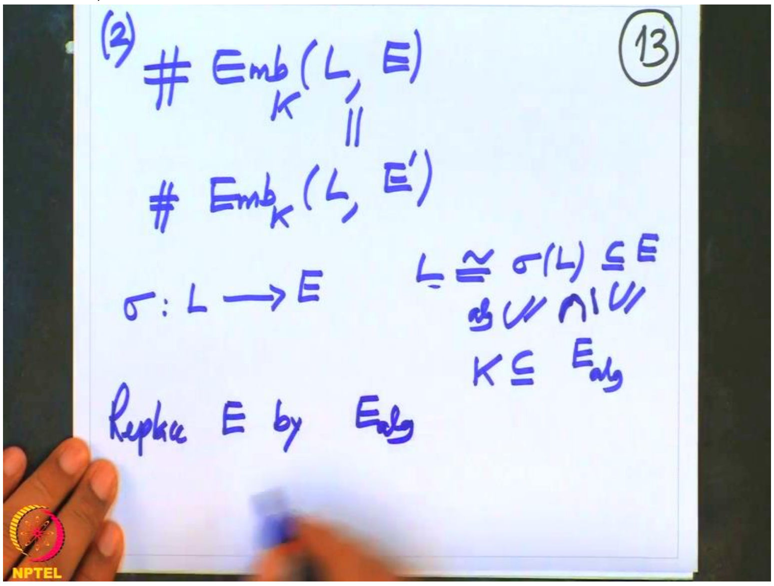
Therefore this element, this sigma L is actually contained here.

(Refer Slide Time 33:28)



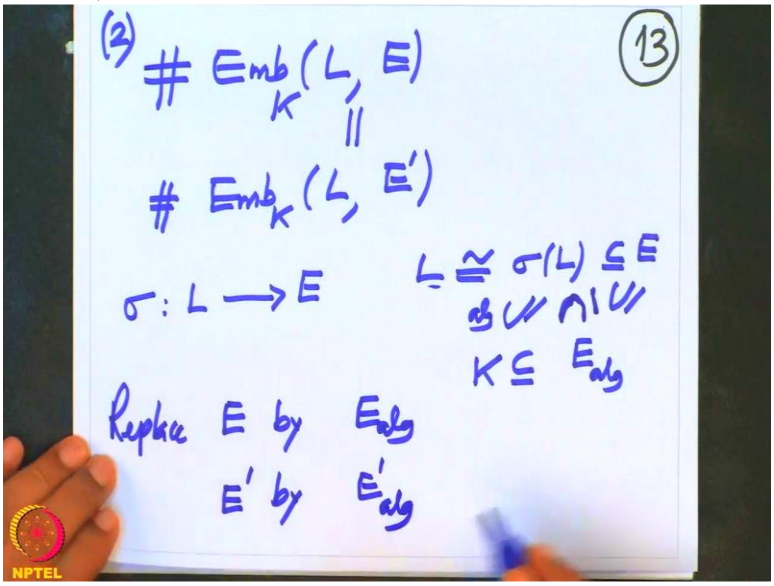

Therefore I am going to replace, this is true for every sigma. So replace E by E a l g

(Refer Slide Time 33:41)




and E prime by E prime a l g.

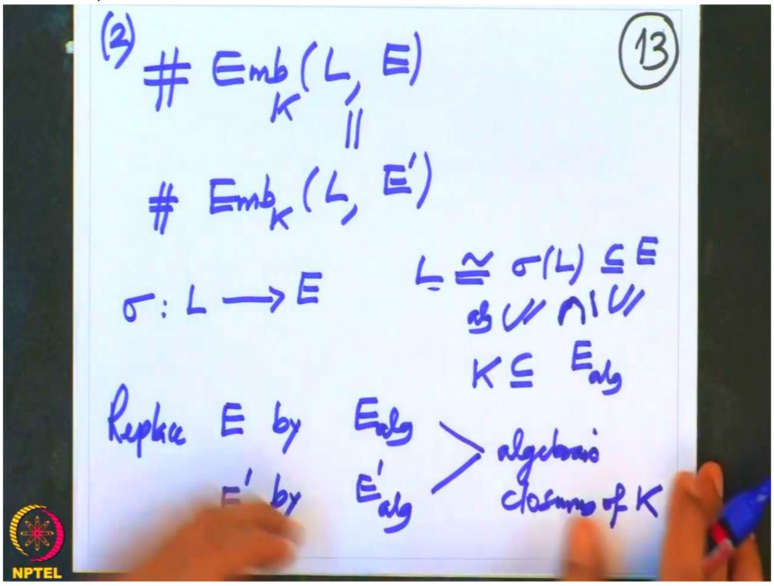
(Refer Slide Time 33:47)




The advantage is now these are algebraic closures of K.

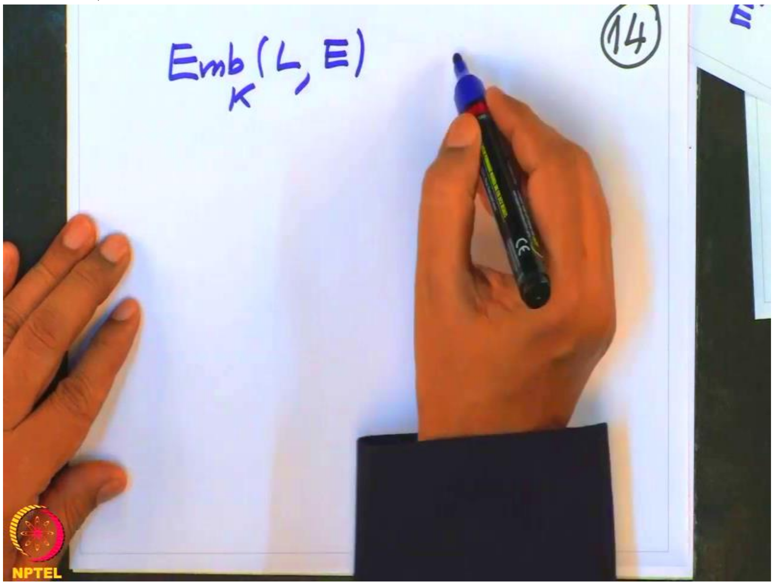
These are algebraic closures of K and

(Refer Slide Time 33:58)



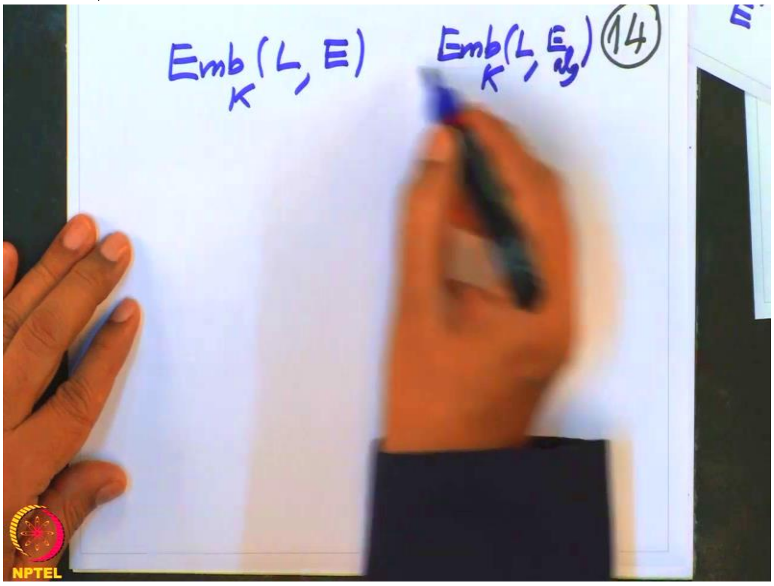

also the embeddings, the number of embeddings I have not changed. And also note that E embeddings, K embeddings of L in E

(Refer Slide Time 34:10)



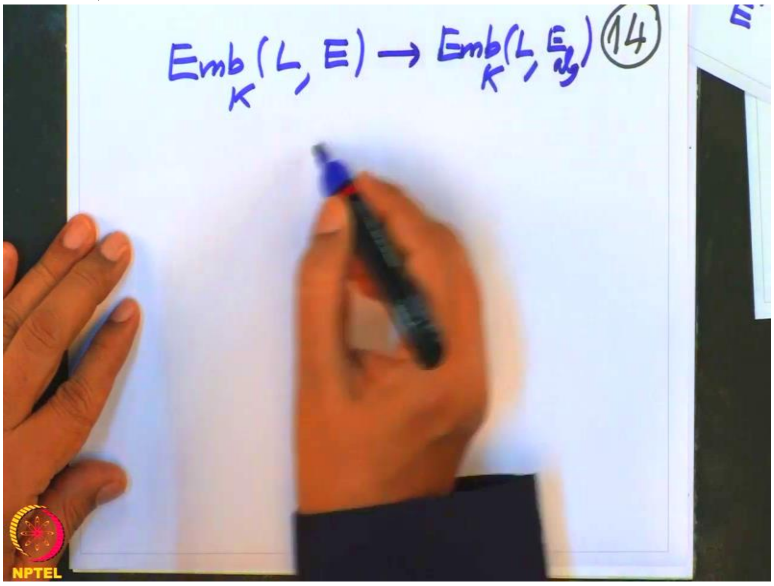

and K embeddings of L in E a l g,

(Refer Slide Time 34:20)



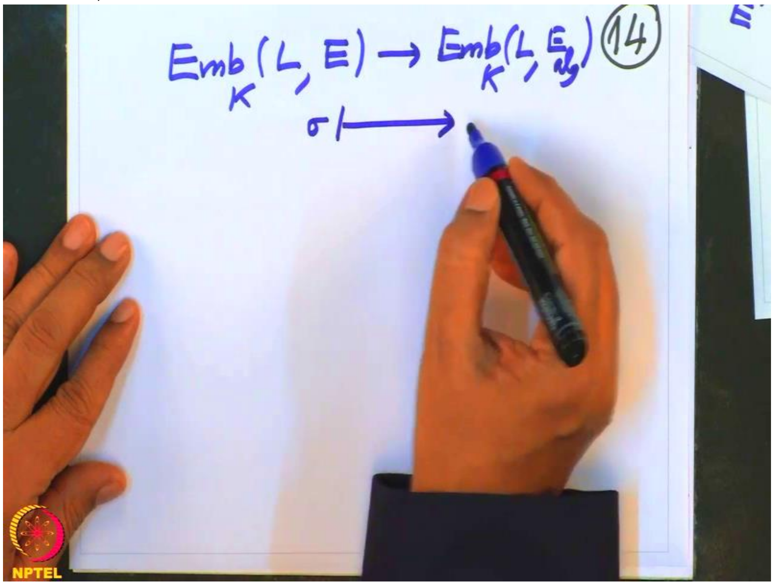

this is just a

(Refer Slide Time 34:21)



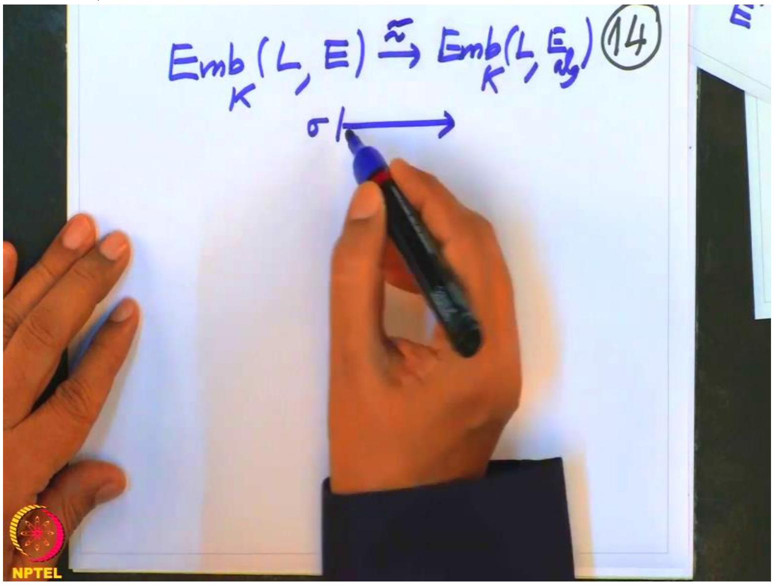

restriction, this sigma going to the restriction.

(Refer Slide Time 34:24)



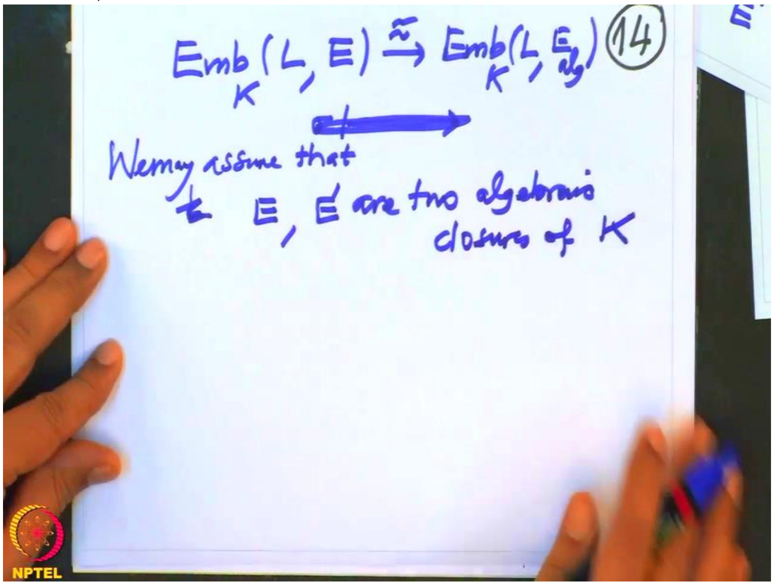

Now this is the other way. So this is, these are bijectives.

(Refer Slide Time 34:28)



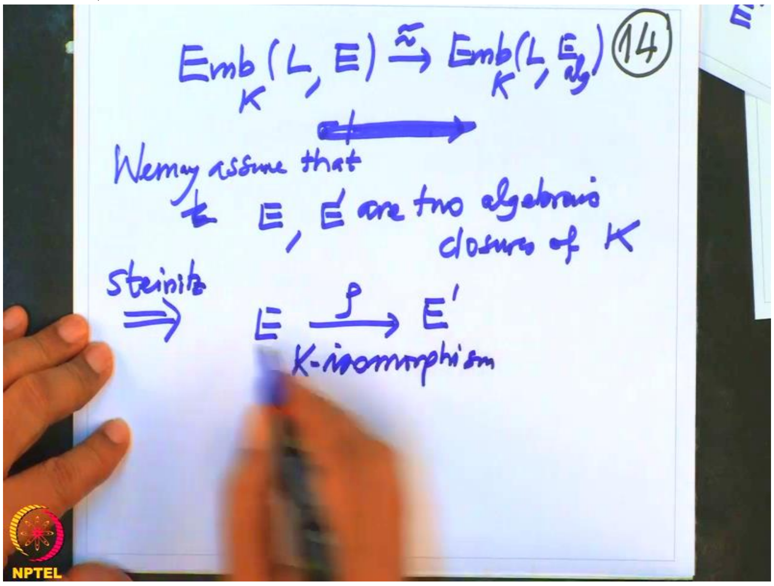

This has not changed. Similarly the other. So I can assume E, so we may assume, what is the advantage? We may assume therefore that E and E prime are two algebraic closures of K.

(Refer Slide Time 35:00)




But then we know by Steinitz Theorem that there is an isomorphism. So therefore by Steinitz Theorem, E and E prime, they are isomorphic over K; that is there exists a K isomorphism rho

(Refer Slide Time 35:27)

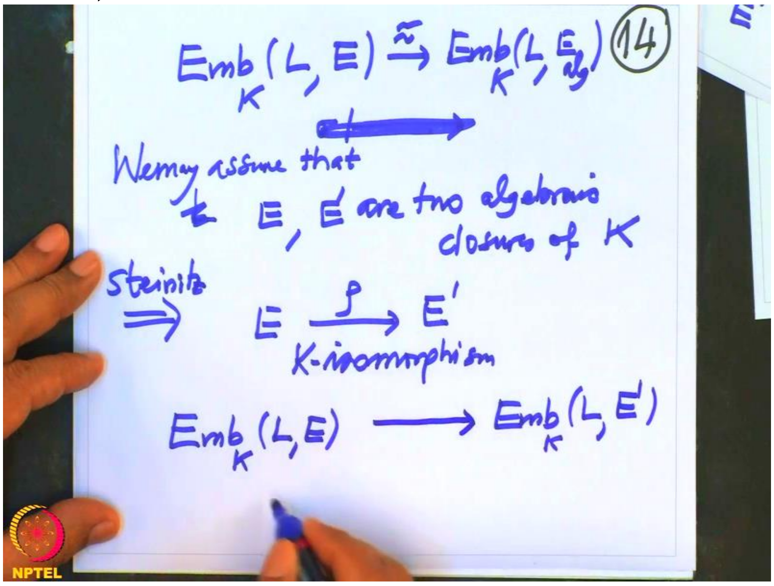



from E to E prime.

This we know rho. But then we can give a bijective map from embeddings of L in E to embeddings of L in E prime.

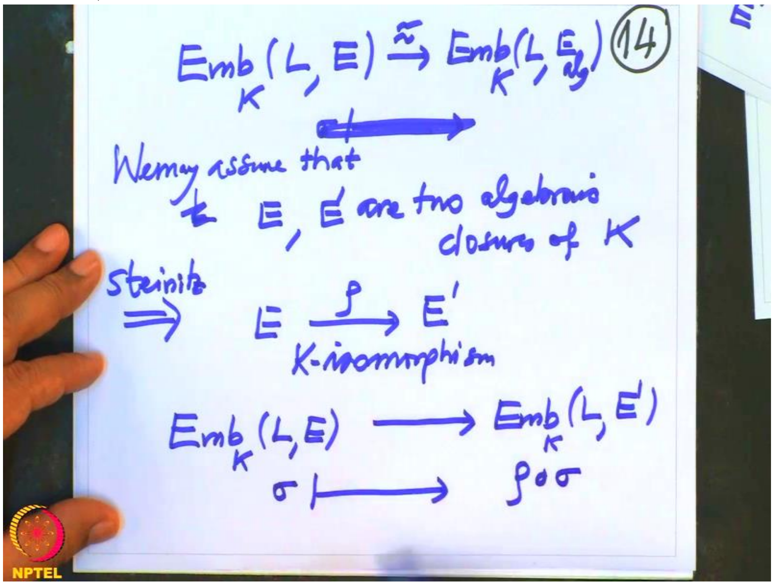
This is just a map,

(Refer Slide Time 35:45)



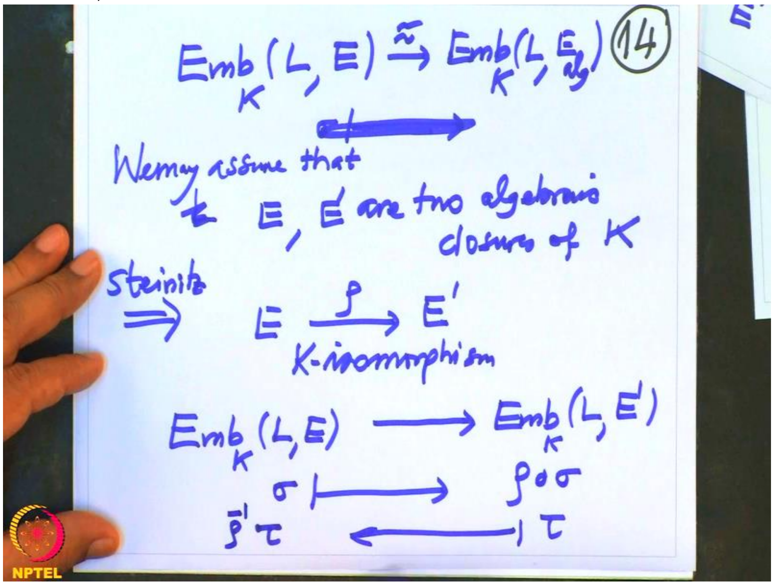

any sigma here going to rho compose sigma.

(Refer Slide Time 35:51)



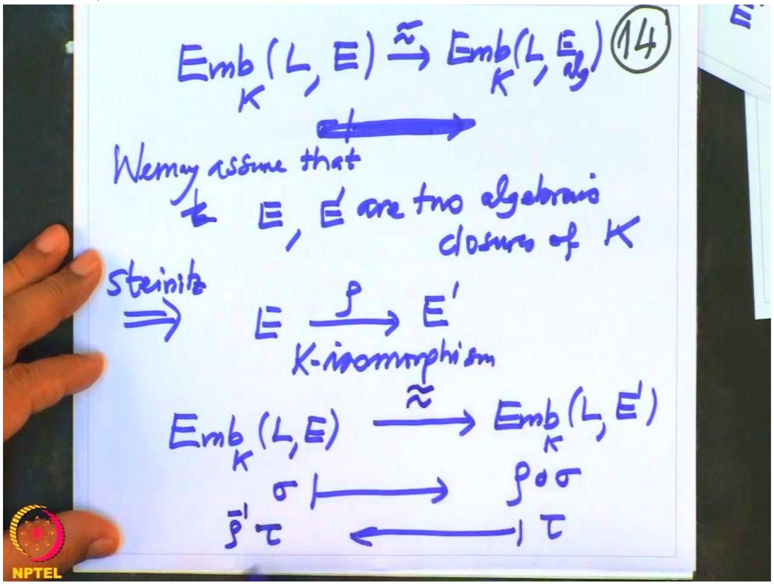

And obviously it is bijective because other way map is if we have tau here; that will be tau inverse, tau of, rho inverse of tau.

(Refer Slide Time 36:05)




This is therefore bijective

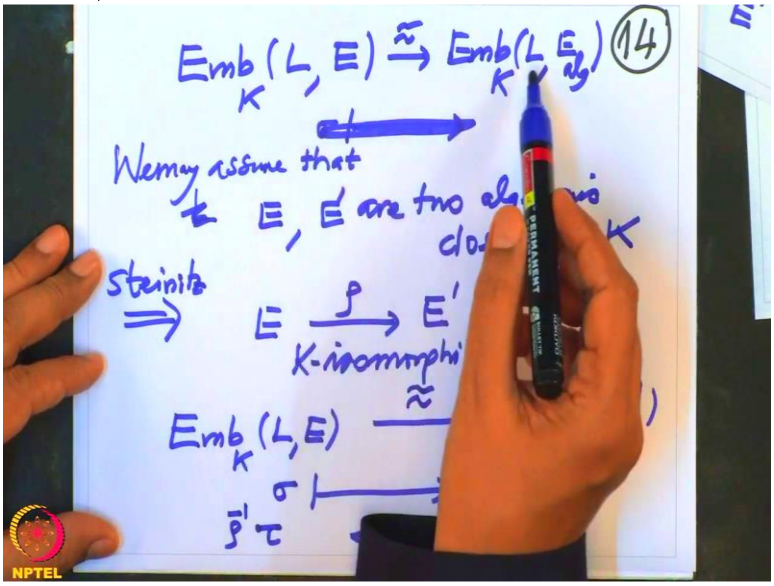
(Refer Slide Time 36:07)




map. Therefore in particular their cardinalities are equal. That is what we wanted to prove.

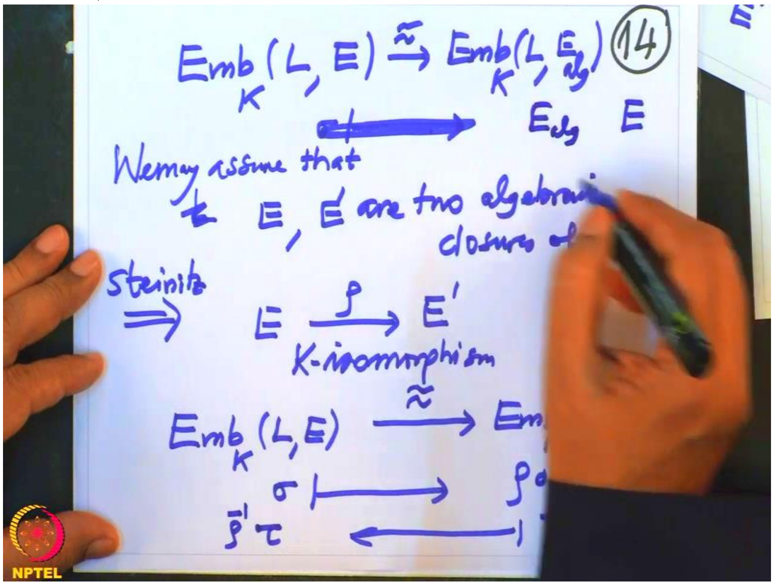
And note that this is isomorphism

(Refer Slide Time 36:14)



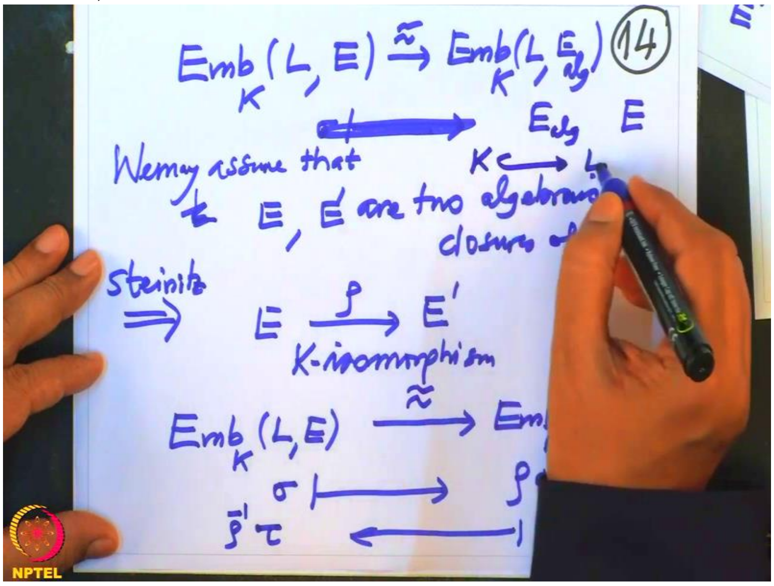

because, you know, because this, this E is here, and E a l g is here

(Refer Slide Time 36:23)



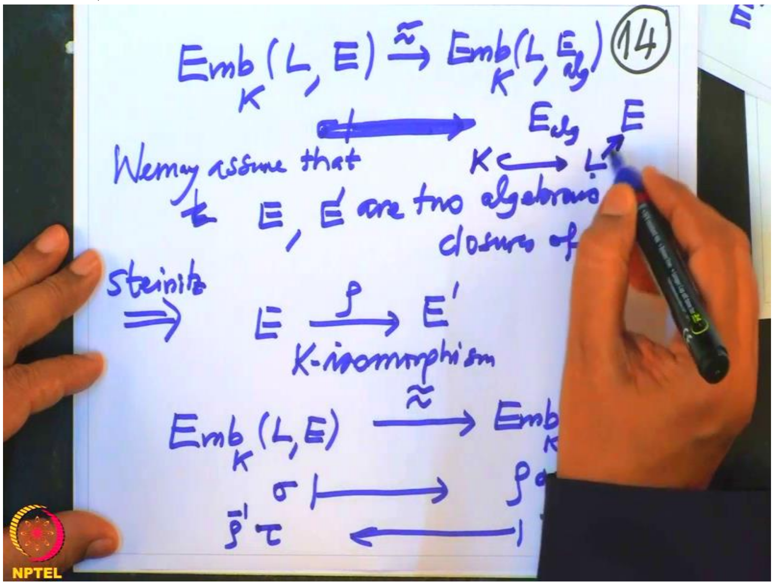

L is here and K is here, so whether you take

(Refer Slide Time 36:29)



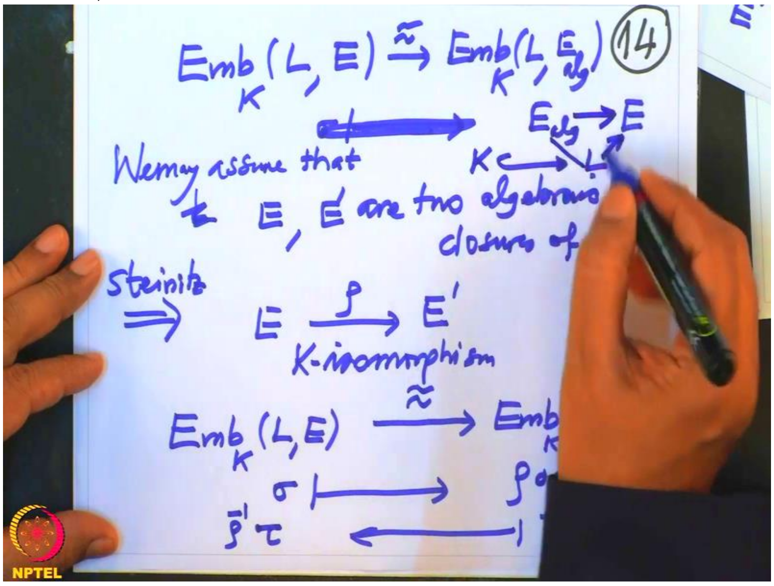

embedding, all embeddings of L in

(Refer Slide Time 36:34)




E they will already factor through this

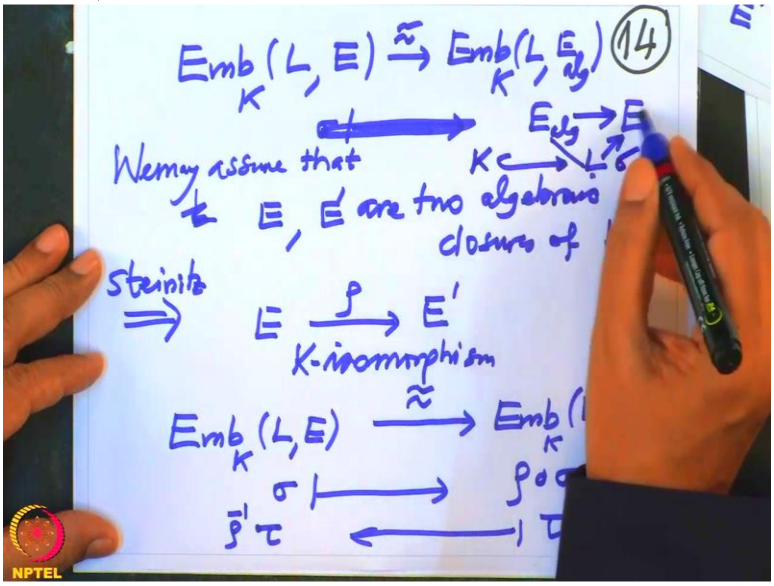
(Refer Slide Time 36:38)




because elements of L are algebraic, therefore elements of sigma L also algebraic.

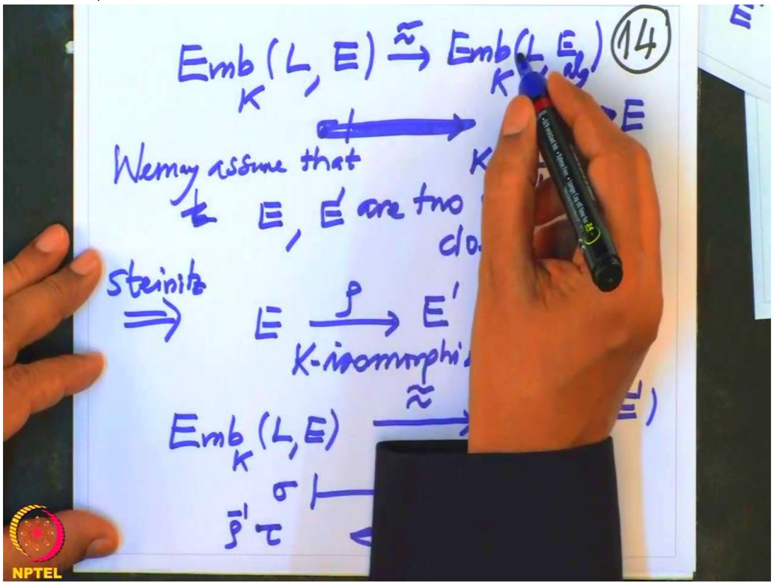
Therefore the images of sigma,

(Refer Slide Time 36:46)



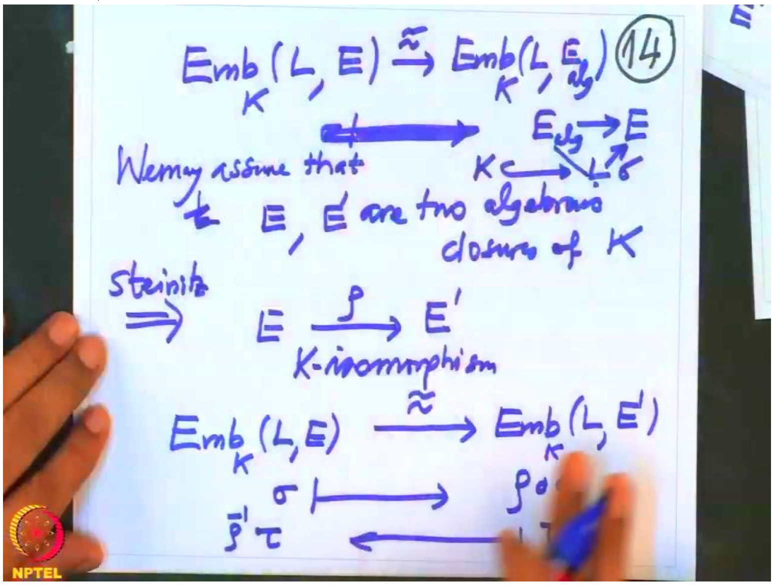

they will factor through this. Therefore you can identify elements of this as elements of this, so therefore this is a bijective map.

(Refer Slide Time 36:53)




Therefore we can replace E and E prime by the algebraic closures of K in them and therefore by Steinitz Theorem we have replaced, we know that E and E prime are isomorphic and that isomorphism will give us a bijection

(Refer Slide Time 37:09)




So we have therefore proved completely that the number of embeddings is a good invariant

(Refer Slide Time 37:17)


of the finite field extension L over E and now we will use this fact to prove that separable extensions have primitive elements so that we will do it in the next lecture. Thank you very much.