Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 58
Primitive Element Theorem

(Refer Slide Time: 00:25)

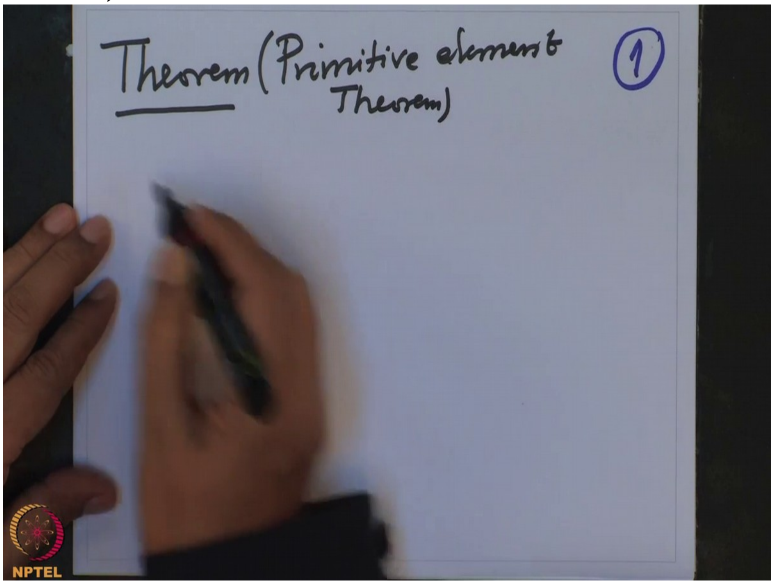
Ok so we have stated a Primitive Element theorem

(Refer Slide Time: 00:29)

for separable, finite separable extensions and we will prove it now.

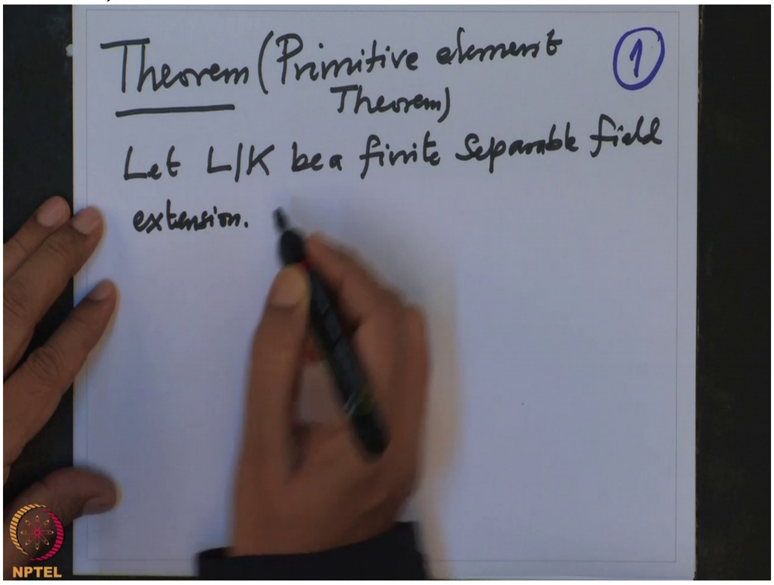
So the theorem we will prove is this is Primitive Element theorem.

(Refer Slide Time: 00:53)



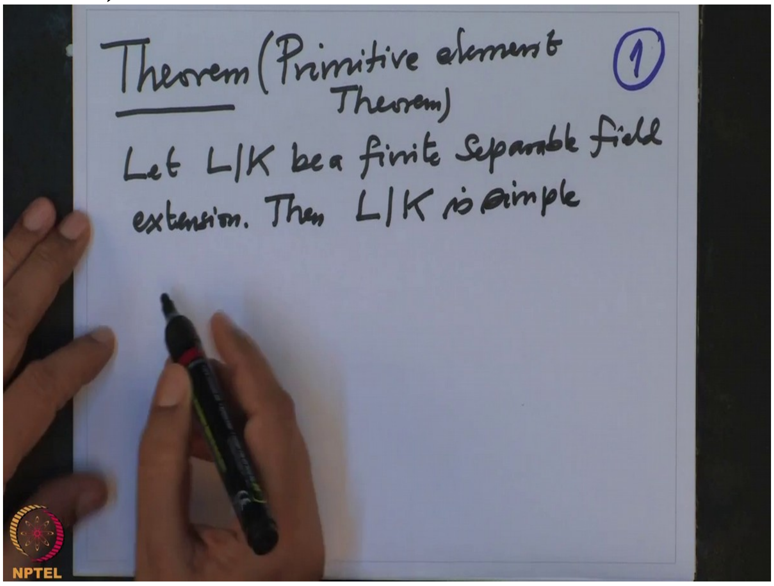
So let L over K be a finite field extension, finite separable field extension.

(Refer Slide Time: 01:11)



Then L over K is simple. This is what we want to prove.

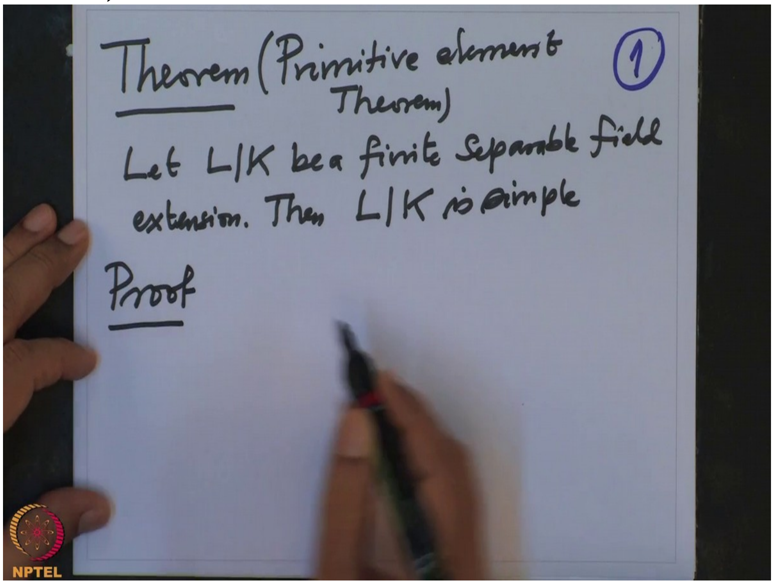
(Refer Slide Time: 01:20)



Proof

Let me just mention

(Refer Slide Time: 01:25)



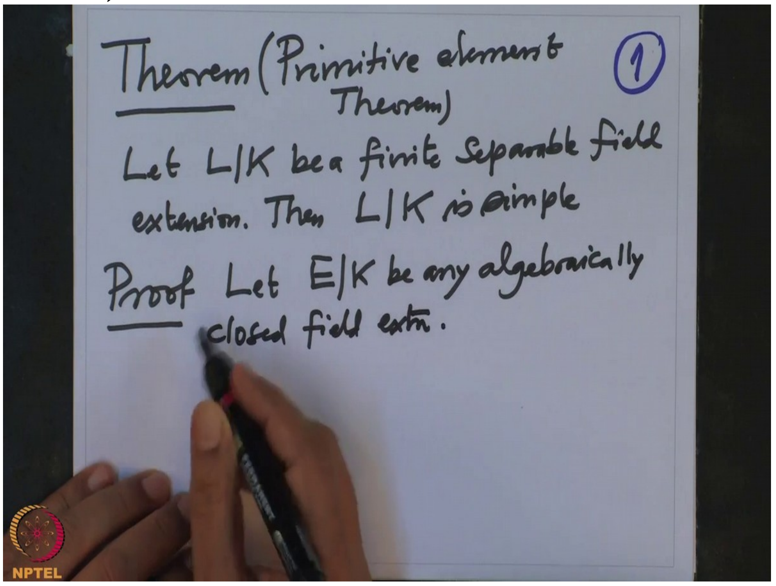
that this was the most important step in Galois Theory. Galois was looking for primitive element for a separable extension.

His, in his time, all extensions considered were characteristic 0 fields. They were characteristic 0 fields therefore all were separable and they were all the time looking for primitive elements.

And that is very, very important step in the Galois Theory.

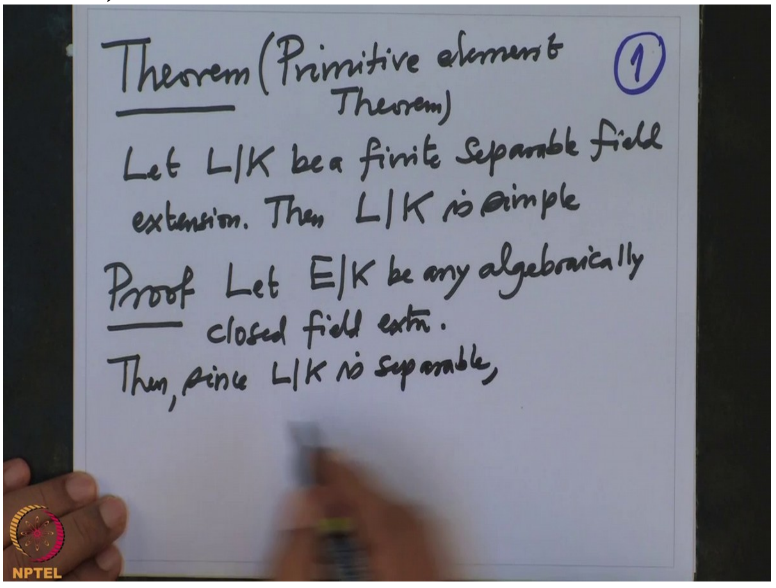
So, so let E over K be any algebraically closed field extension. Then what we have proved

(Refer Slide Time: 02:20)



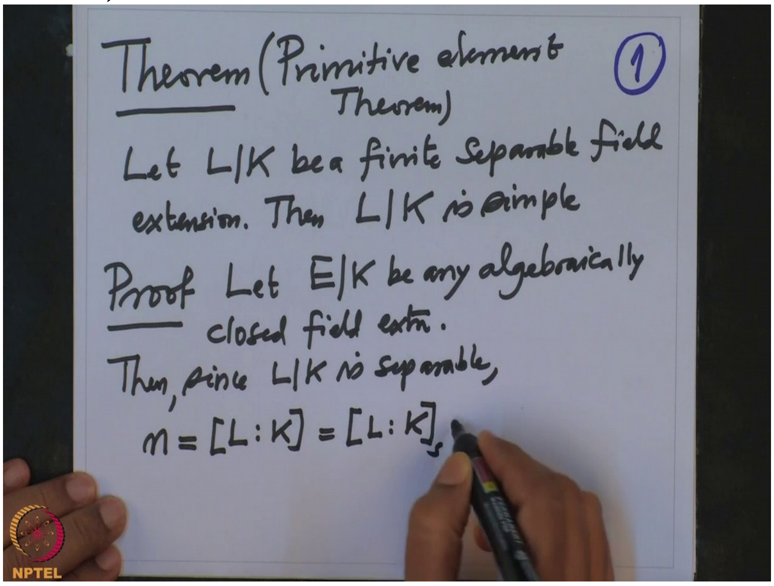
is then since L over K is separable, we know

(Refer Slide Time: 02:34)



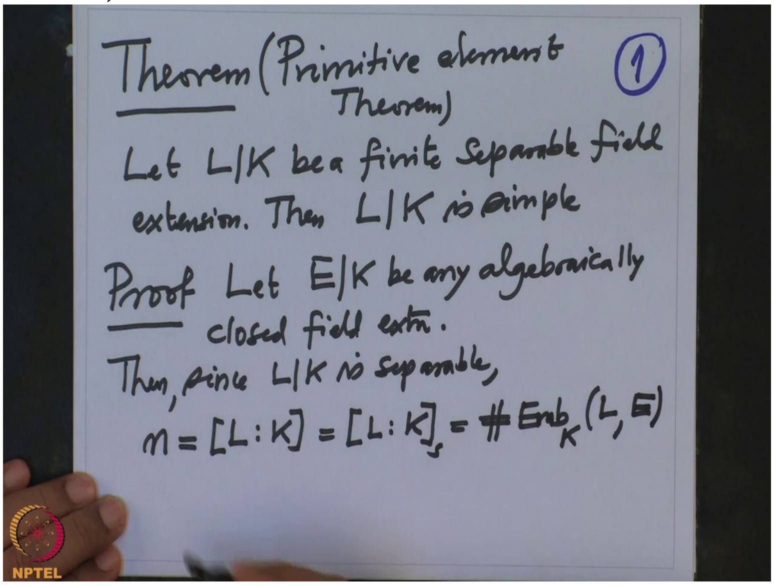
that if n is the degree of the field extension, this degree is also equal to the separable degree L over K S, and

(Refer Slide Time: 02:45)



separable degree is by definition, cardinality of the embeddings of L inside K, K embeddings of L inside K.

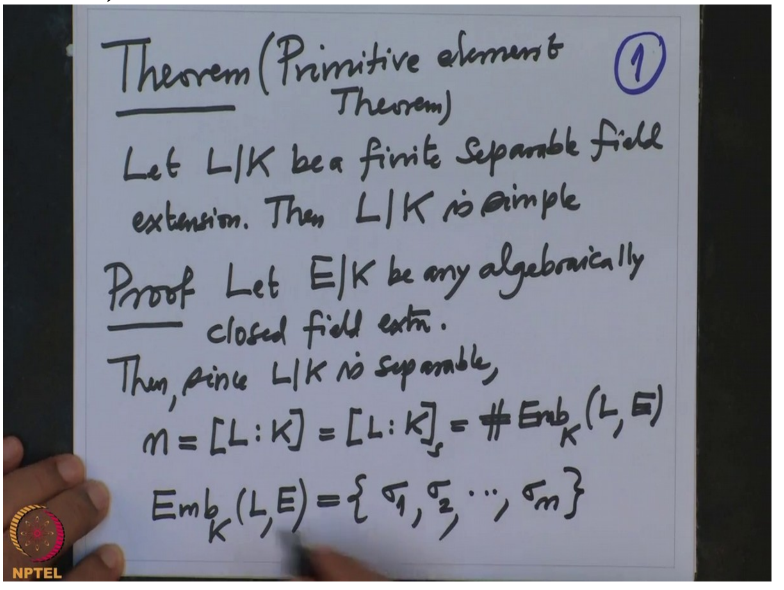
(Refer Slide Time: 02:53)



So let us say that, that means these embeddings, there are precisely n embeddings. So let embedding set L E, this be exactly equal to $\sigma_1, \sigma_2, \ldots, \sigma_n$.

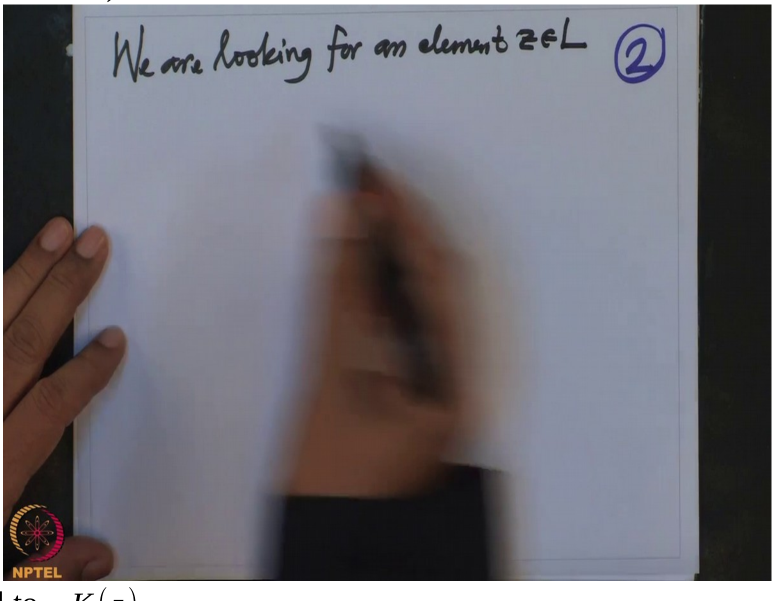
There are precisely n K embeddings

(Refer Slide Time: 03:17)



of L into E. And what are we looking for? We are looking for an element z, so we are looking for an element $z \in L$

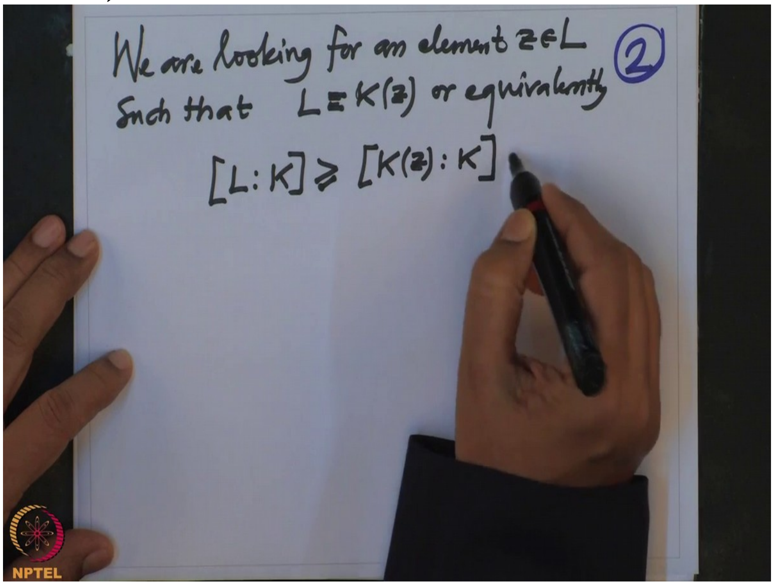
(Refer Slide Time: 03:43)



such that L equal to $K(z)$.

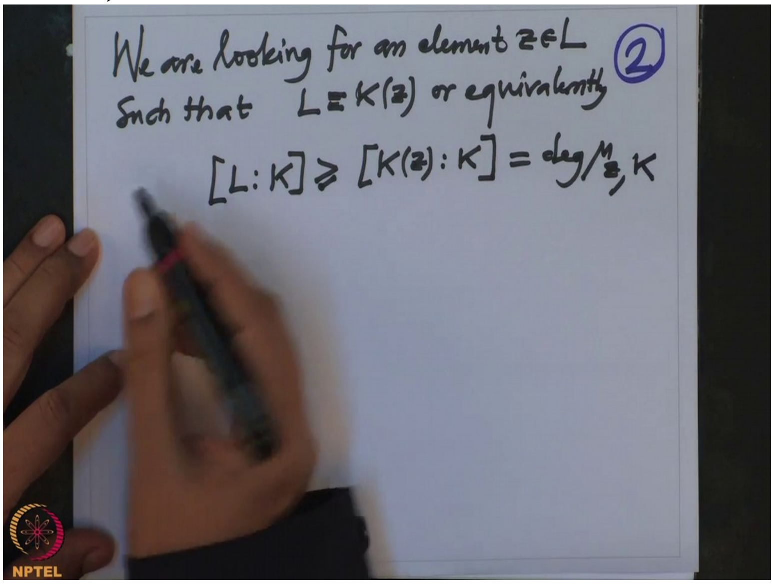
Or equivalently this equality here will also follow from this inequality L over K bigger equal to $K(z)$ over K

(Refer Slide Time: 04:18)



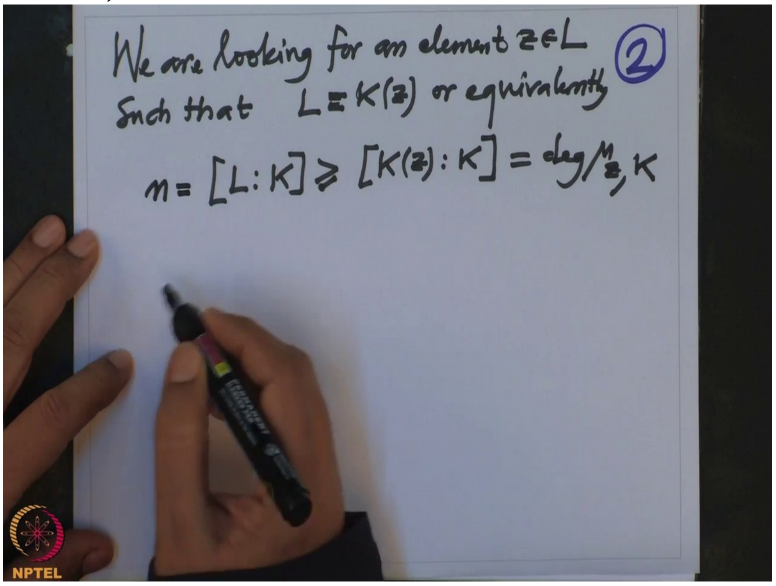
and this is equal to degree of $\mu_{z,K}$,

(Refer Slide Time: 04:24)



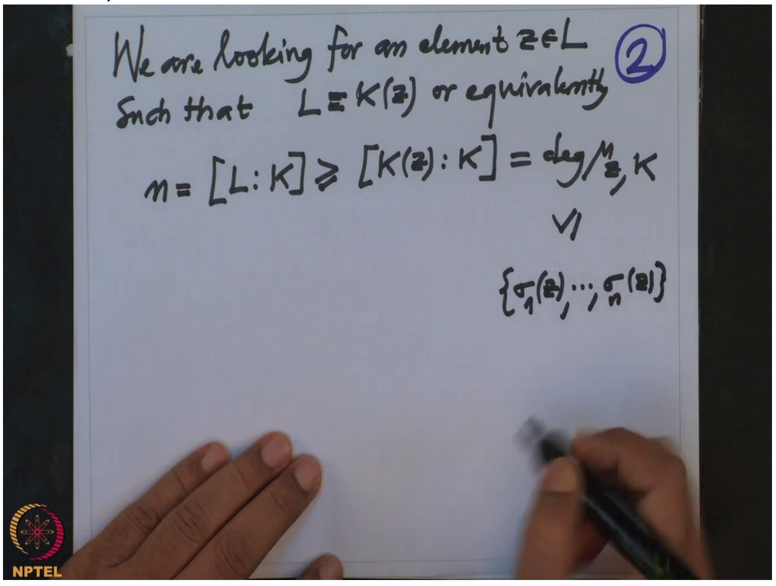
this is n

(Refer Slide Time: 04:28)



and this is bigger equal to, we have seen this degree is bigger equal to the zeroes, zeroes inside E but $\sigma_1(z),\ldots,\sigma_n(z)$, they are all zeroes

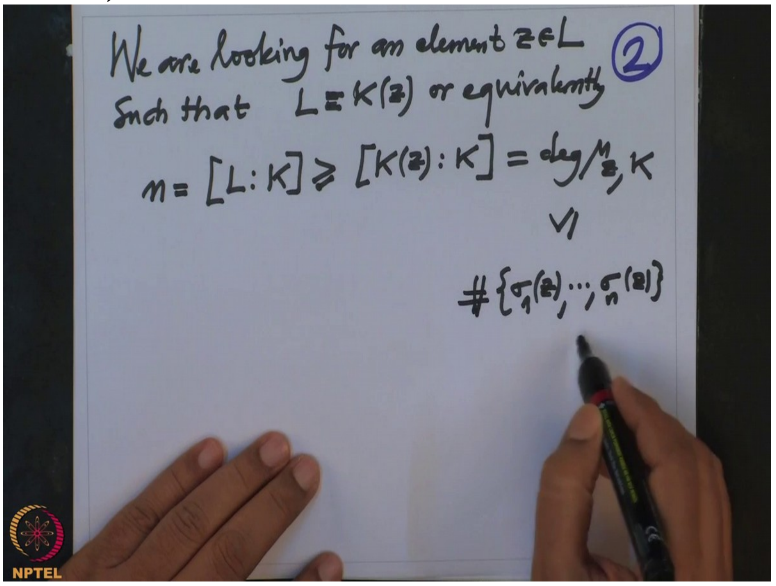
(Refer Slide Time: 04:48)



of mu, because the sigmas are K-algebra homomorphisms.

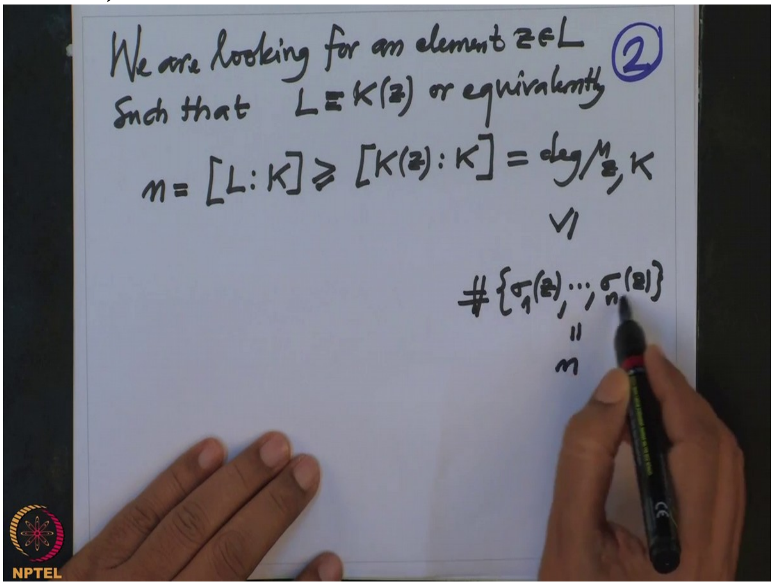
And this, this number,

(Refer Slide Time: 04:58)



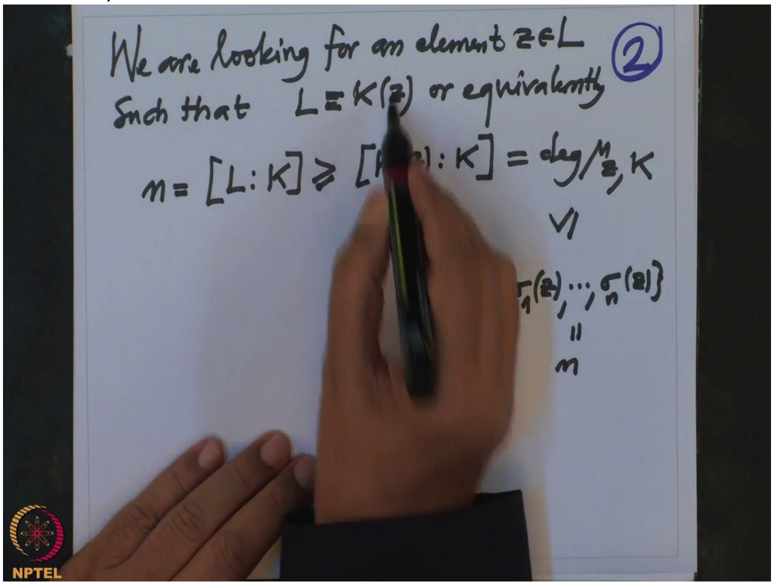
so this number is also n because

(Refer Slide Time: 05:02)



these sigmas are uniquely determined by z

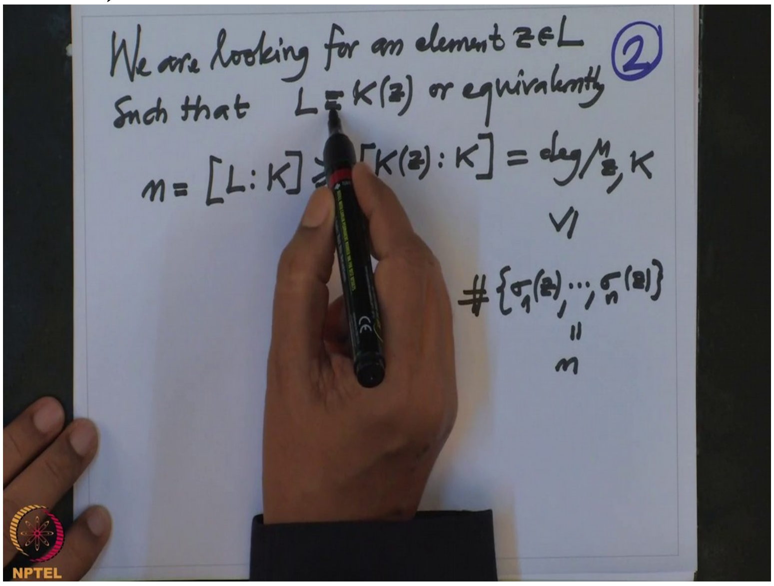
(Refer Slide Time: 05:07)



on L.

So therefore this number will be n. So therefore all these inequalities will be equalities and we will get equality here and we will get

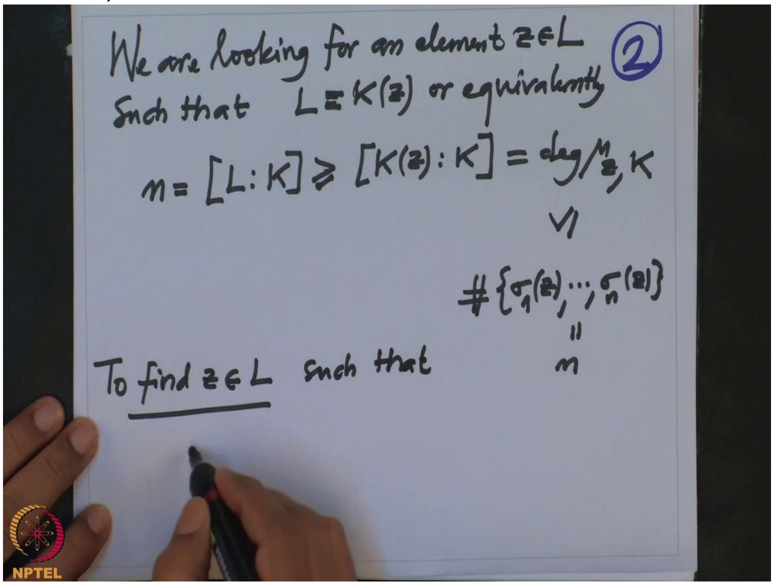
(Refer Slide Time: 05:19)



L equal to $K(z)$.

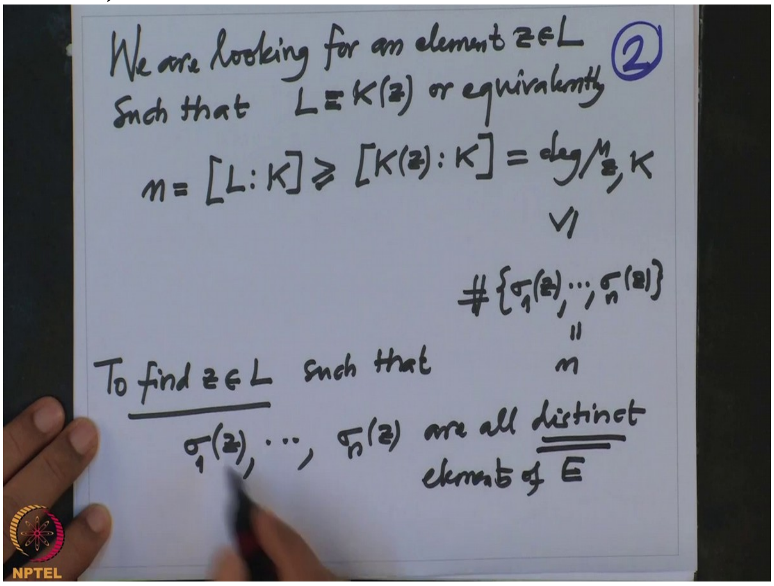
So I want to check that, so in other words I want to find z, to find $z \in L$ such that

(Refer Slide Time: 05:39)



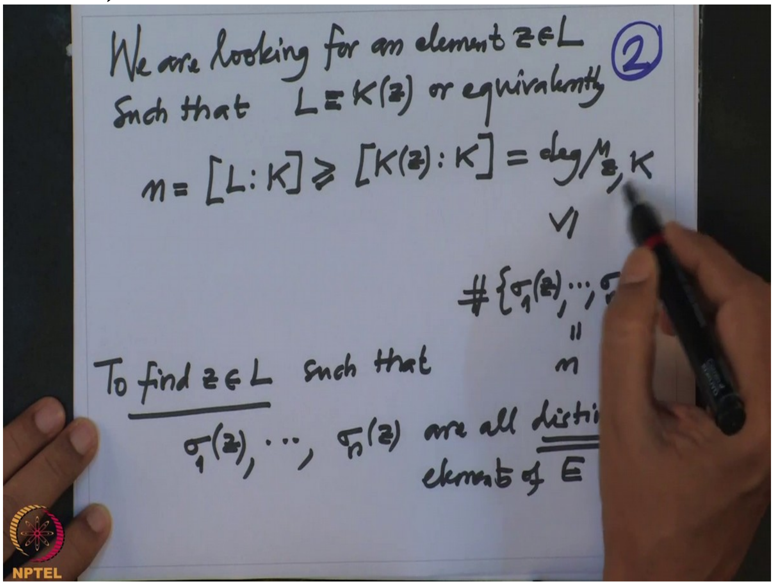
the $\sigma_1(z),\ldots,\sigma_n(z)$ are all distinct elements of E, they are elements of E, but the distinct is important.

(Refer Slide Time: 05:59)



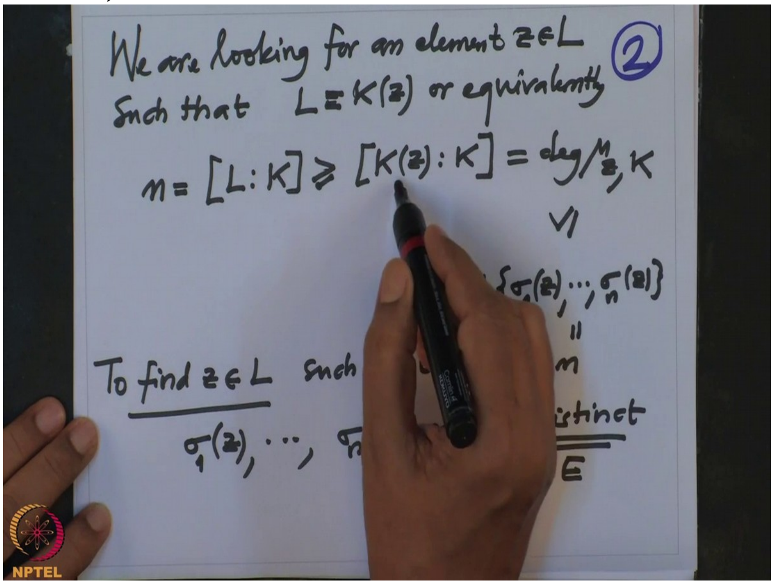
So once we achieve this then this number will be n and this μ, they are all zeroes of the minimal

(Refer Slide Time: 06:07)



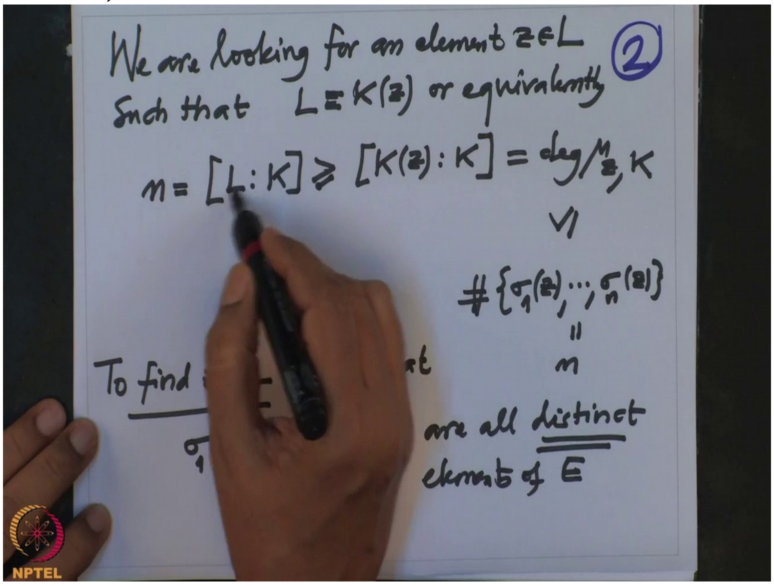
polynomial, therefore the degree of the minimal polynomial will be bigger equal to this. Degree of the minimal polynomial

(Refer Slide Time: 06:12)



is the degree of $K(z)$ over K and z is contained in L therefore this degree is smaller

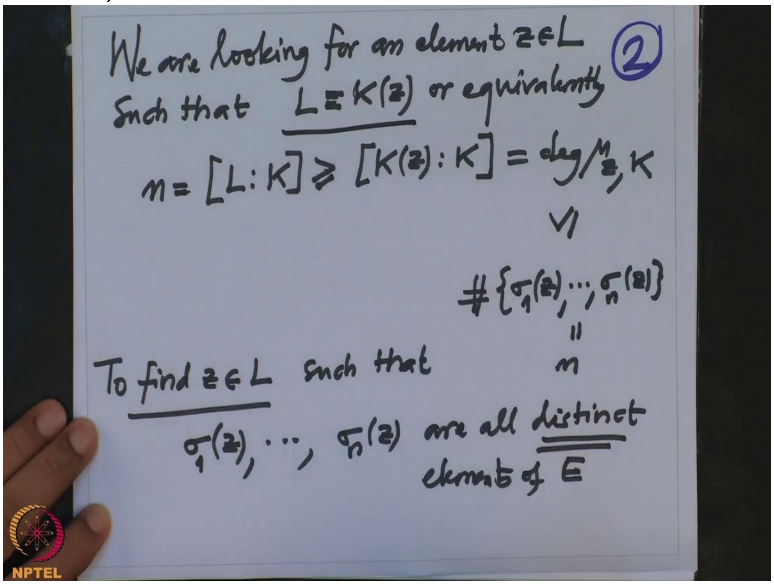
(Refer Slide Time: 06:18)



equal to degree of L over K.

But this is precisely n. Therefore if I prove that these are distinct then all will be equalities here and this will follow,

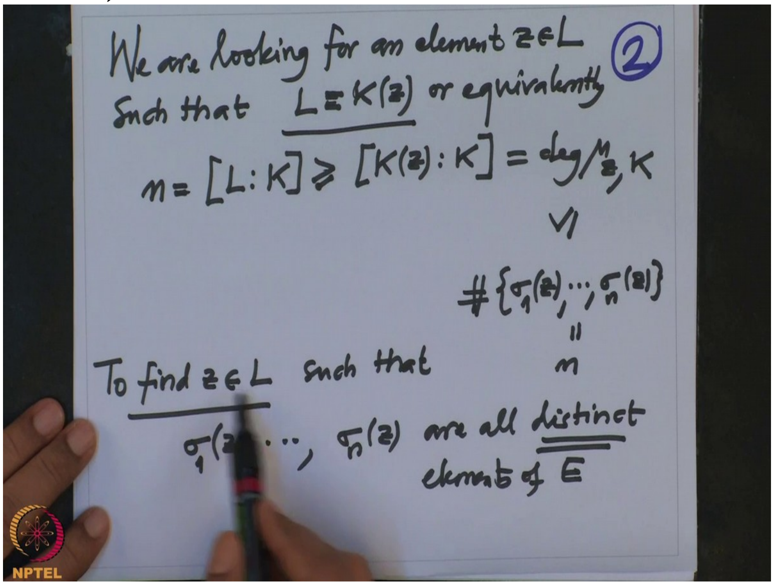
(Refer Slide Time: 06:29)



clear.

Therefore our problem is to find z

(Refer Slide Time: 06:35)

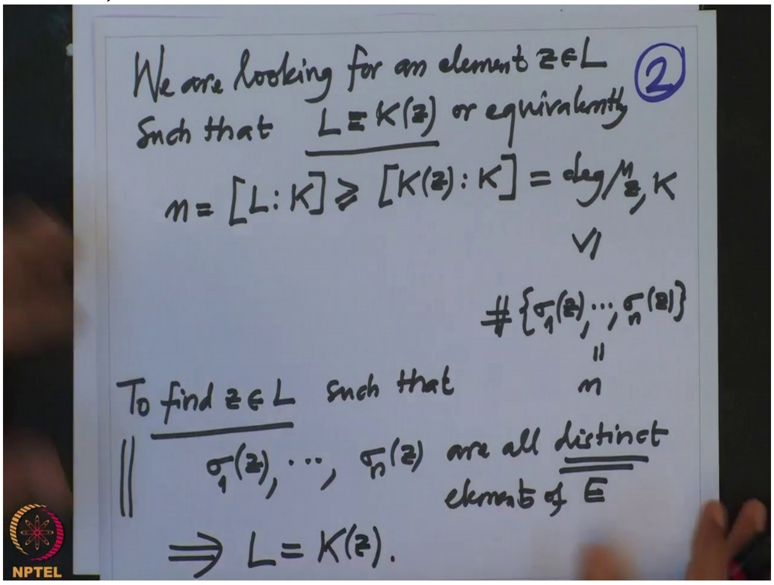


in L such that if I take, if I evaluate all embeddings of L into E at z the number should be different. Then all these elements should be different elements of E.

That is what we are looking for.

So this will imply L equal to $K(z)$.

(Refer Slide Time: 06:56)

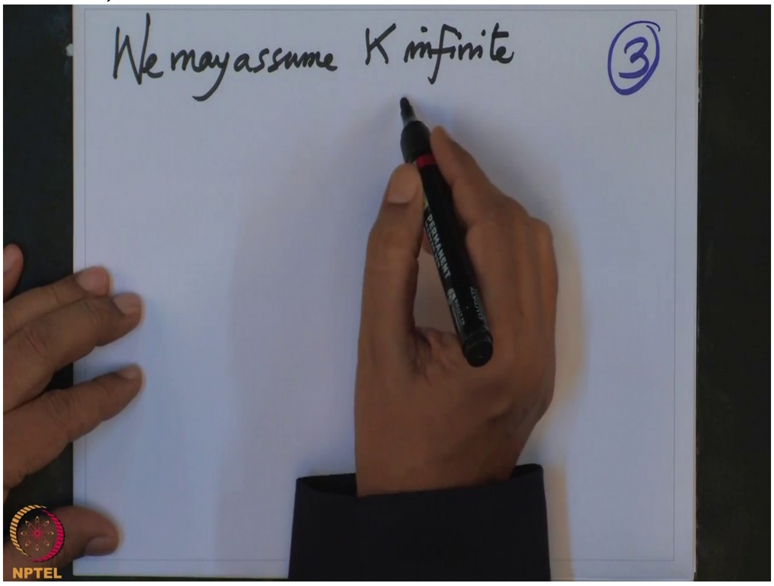


And we would finish our proof, Ok.

So how do we achieve that? I should have said in the beginning itself we may assume K is infinite.

Because if K

(Refer Slide Time: 07:10)

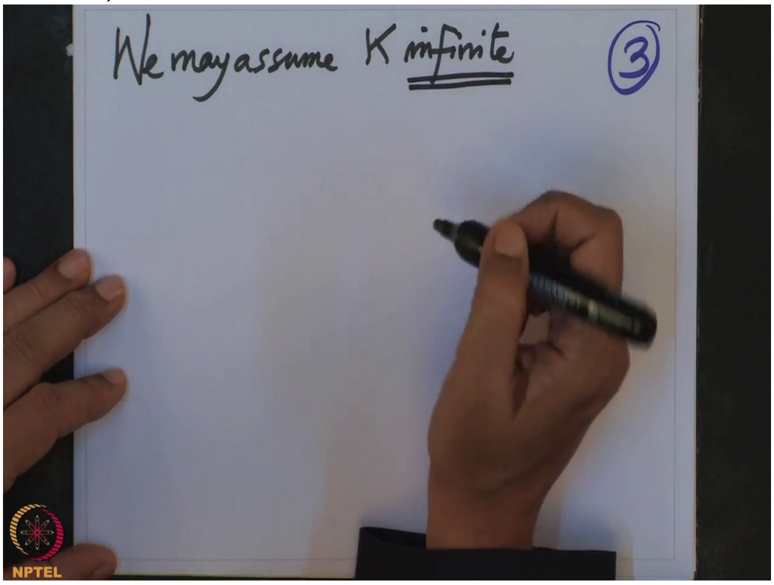


is finite and L over K is a finite field extension of a finite field then you already know that L cross is cyclic group.

And therefore L will be simple extension. So that is not a big deal.

So we are assuming

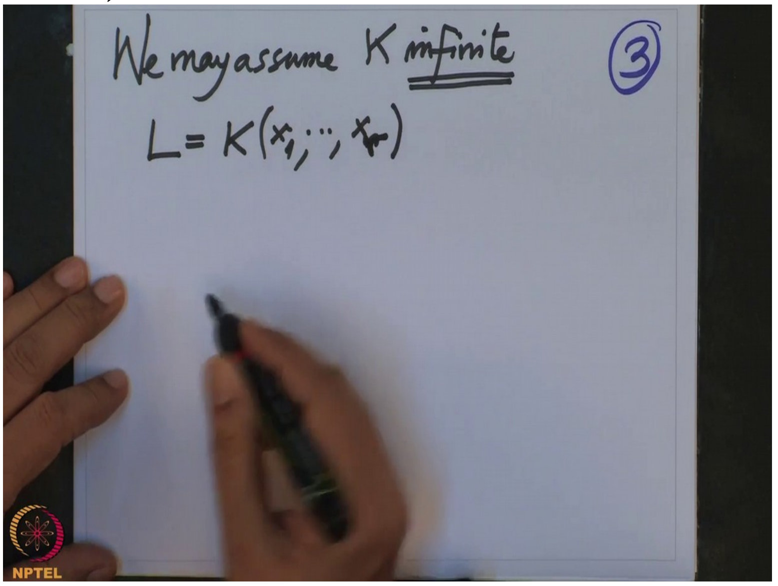
(Refer Slide Time: 07:27)



K is infinite field. And we will proceed the proof, so therefore L is a finite extension of K.

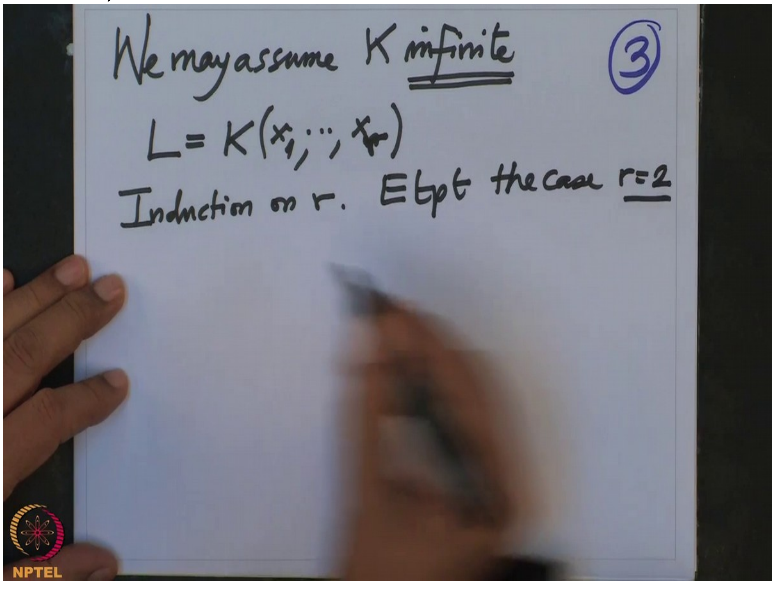
So L will generated by $x_1, \ldots, x_r$.

(Refer Slide Time: 07:44)



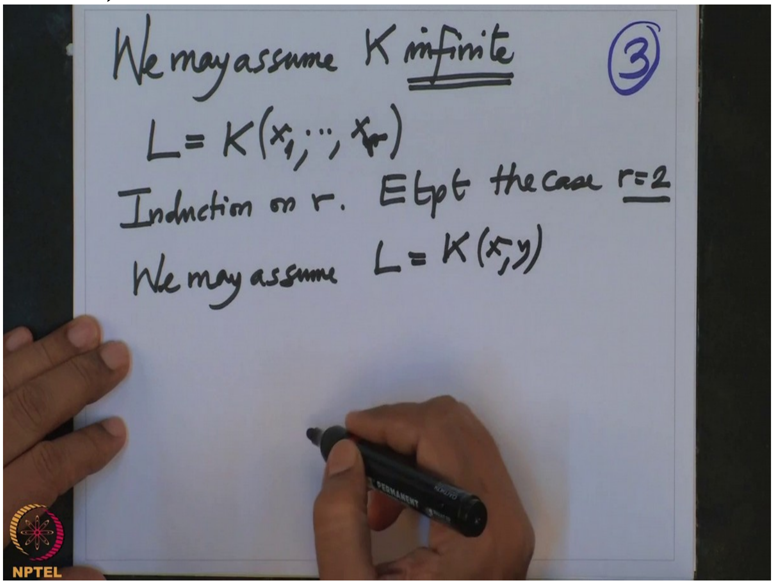
And by induction on r, induction on r, enough to prove that, enough to prove the case r equal to 2.

(Refer Slide Time: 08:02)



So that means what? We may assume L equal to, L is generated by 2 elements, now I will call them x and y.

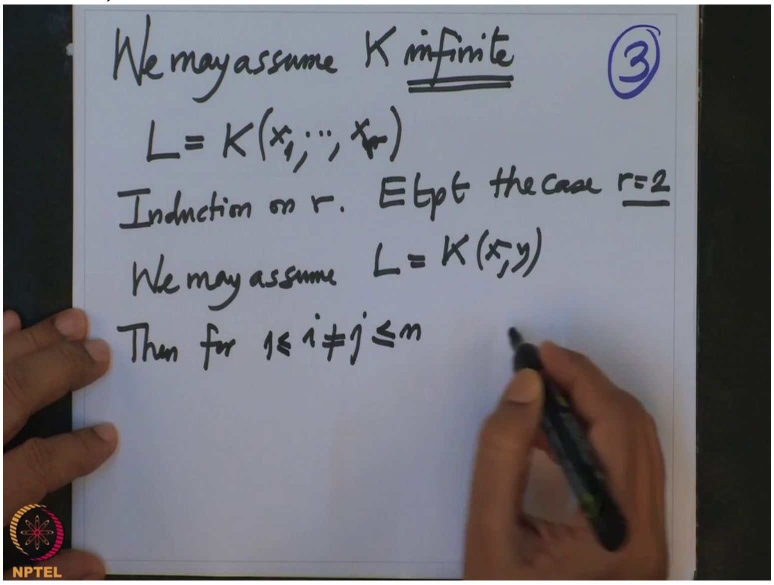
(Refer Slide Time: 08:17)



And I want to find an element z so that all values of different embeddings are different.

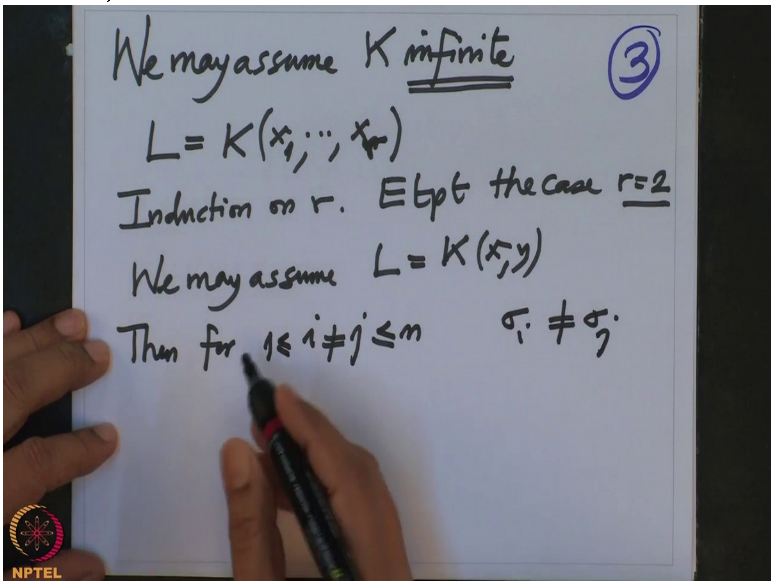
So then, for any indices i and j, i not equal to j but in-between n and 1,

(Refer Slide Time: 08:42)



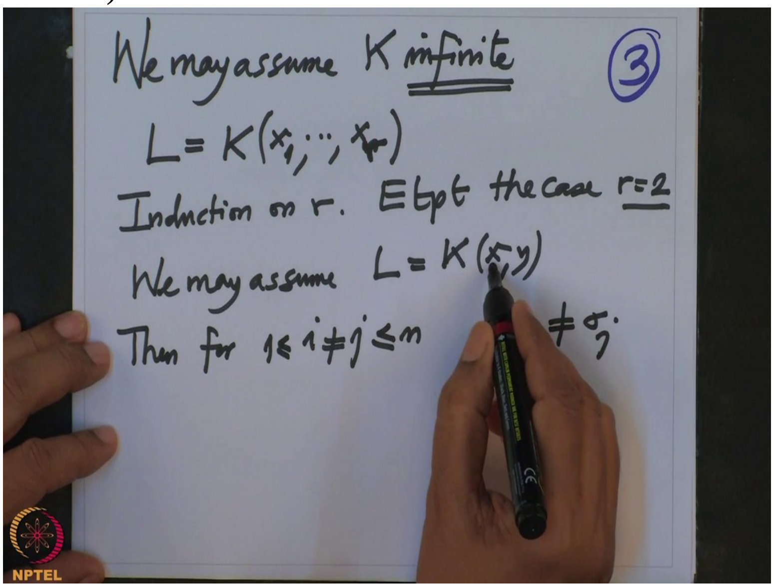
these embeddings we know they are different.

(Refer Slide Time: 08:46)



Therefore the values, these embeddings they are uniquely determined

(Refer Slide Time: 08:50)

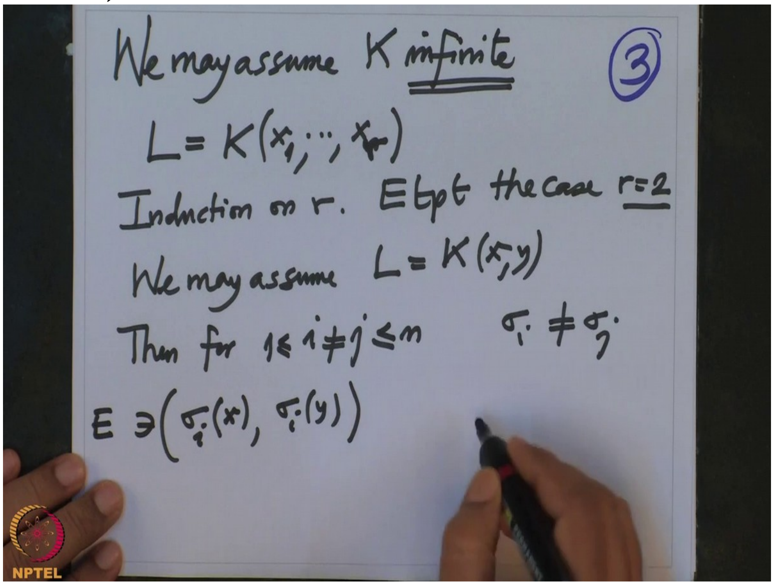


by x and y, their values and x and y.

If I know $\sigma(x)$ and $\sigma(y)$ then that is uniquely determined because this L is generated by x and y.

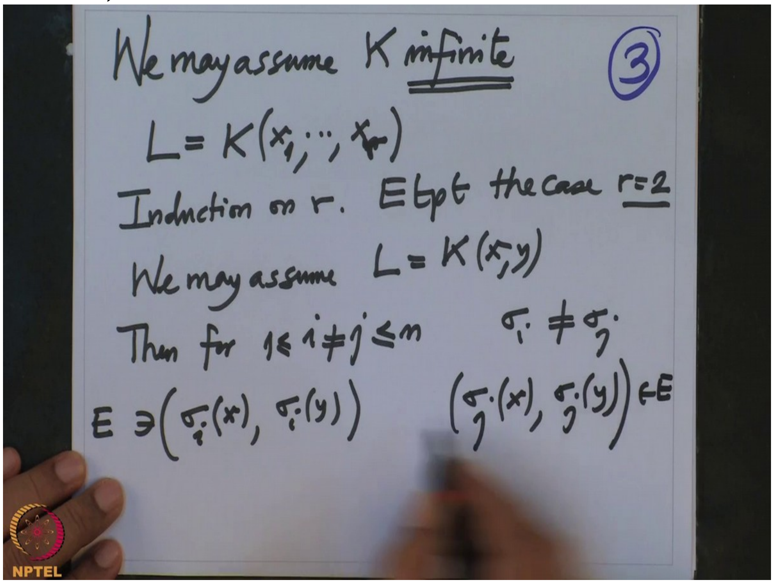
So if I look at $(\sigma_i(x),\sigma_i(y))$, this pair, this is a pair of elements in E.

(Refer Slide Time: 09:13)



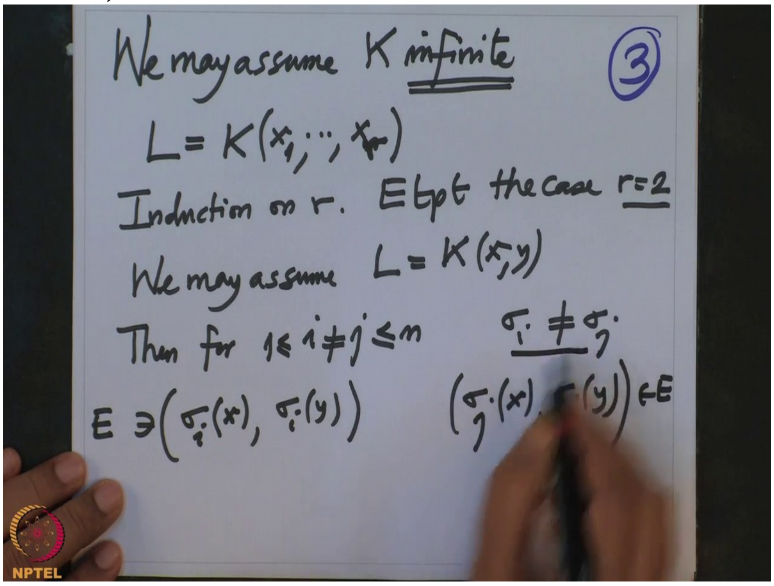
And we have this $(\sigma_j(x), \sigma_j(y))$, this is also pair in E.

(Refer Slide Time: 09:23)



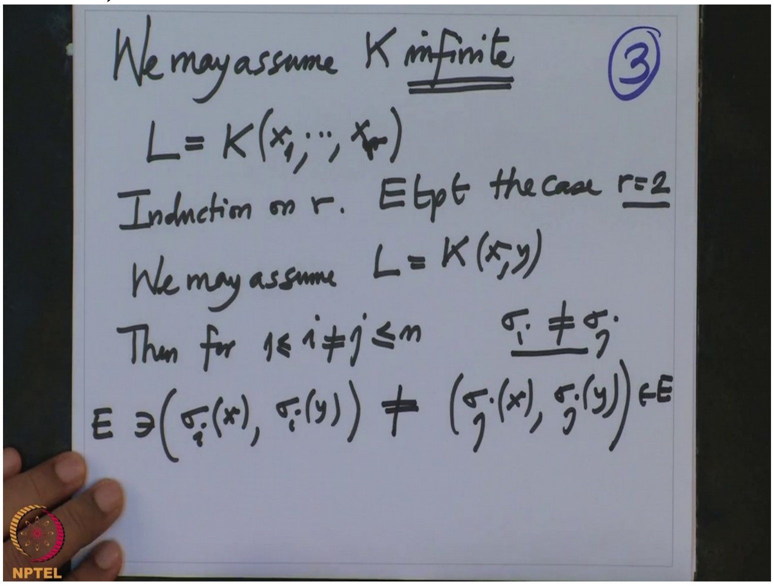
So if they are different

(Refer Slide Time: 09:25)



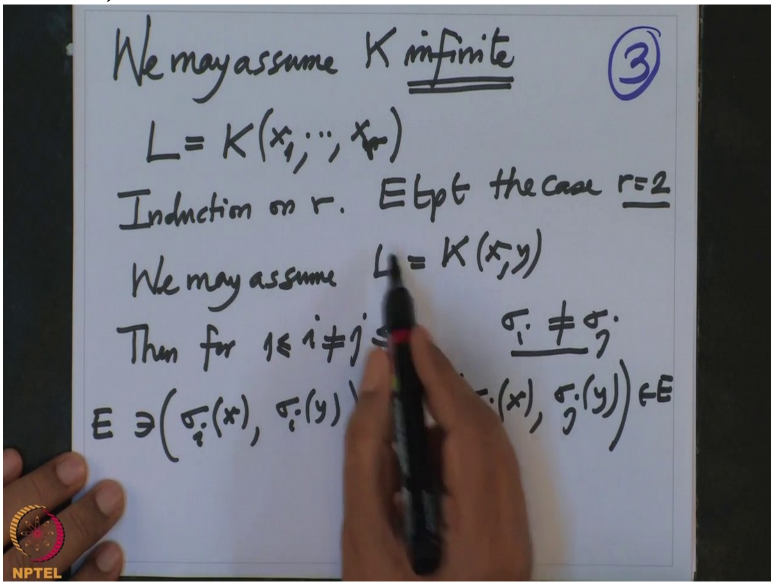
these are different.

(Refer Slide Time: 09:27)



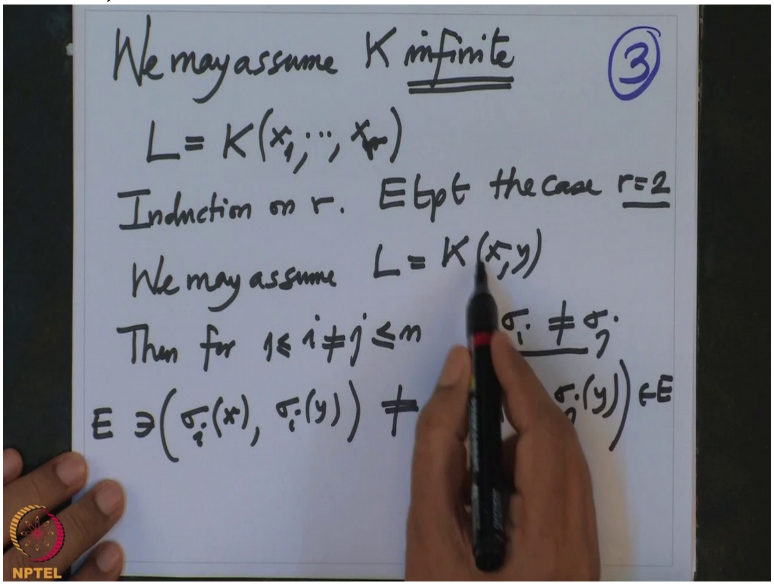
Because if they are equal, each, each element of L

(Refer Slide Time: 09:32)



is a combination

(Refer Slide Time: 09:33)

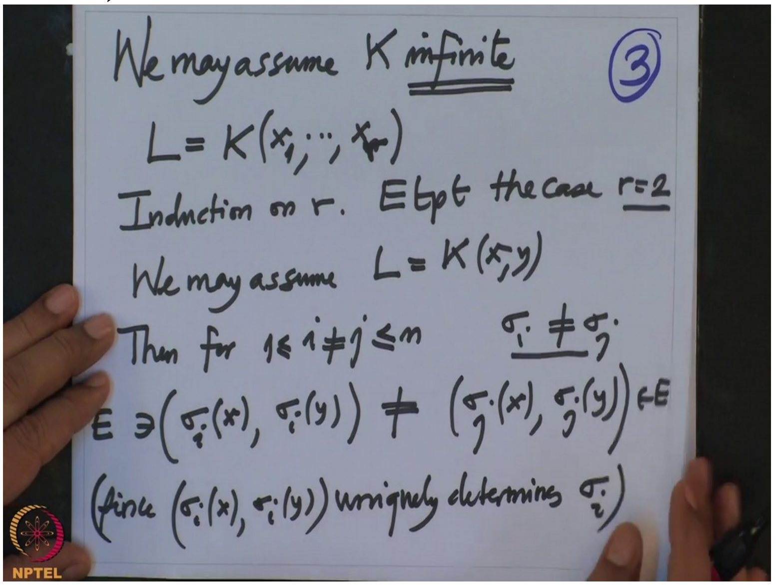


of x and y and therefore these two numbers will be equal, so they will be

So therefore for different i and j these pair of elements are different.

So this is since, $(\sigma_i(x), \sigma_i(y))$, this pair uniquely determines σ_i ,

(Refer Slide Time: 10:08)

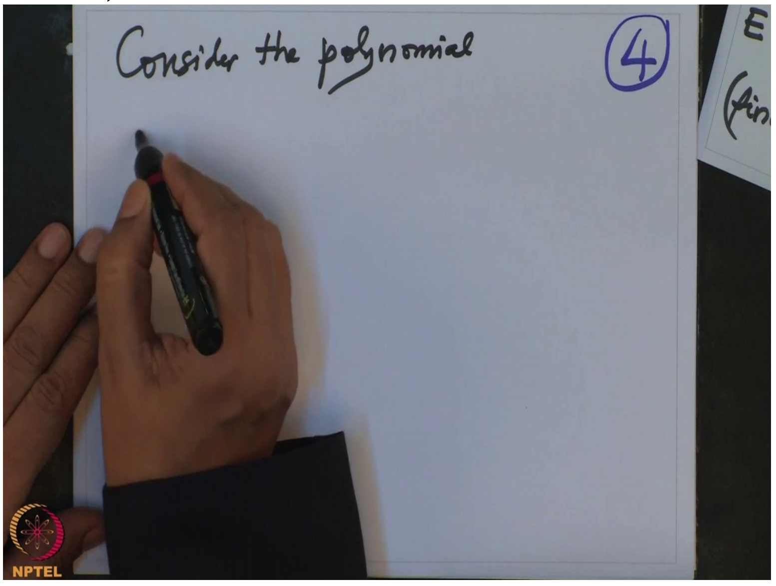


alright.

So now we have, to each embedding we have a pair. And now we consider a polynomial.

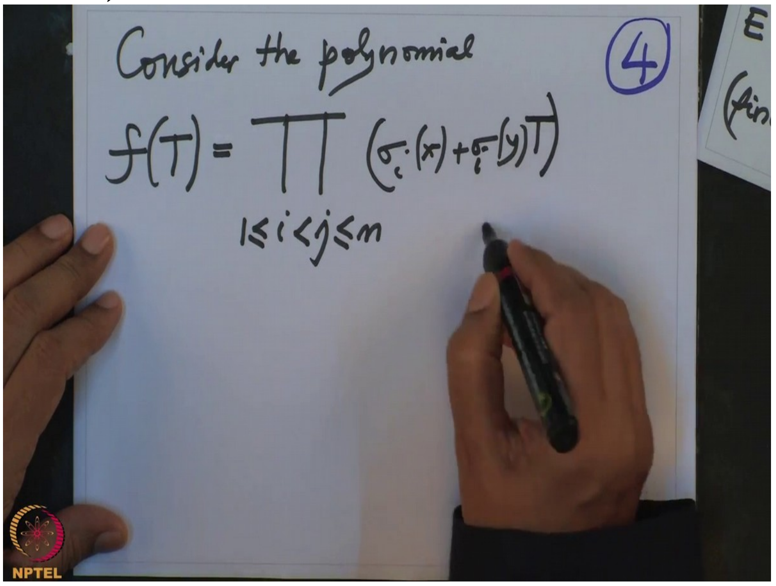
So consider the polynomial

(Refer Slide Time: 10:30)



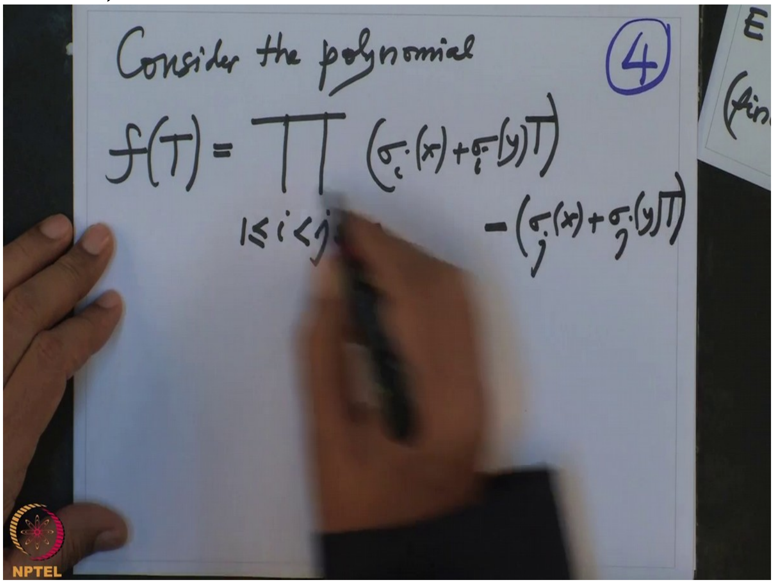
f T, this polynomial is product, product is running over pairs i comma j such that i is less than j. x is equal to n $\left(\sigma_i(x)+\sigma_i(y)T\right)$, this minus,

(Refer Slide Time: 11:00)



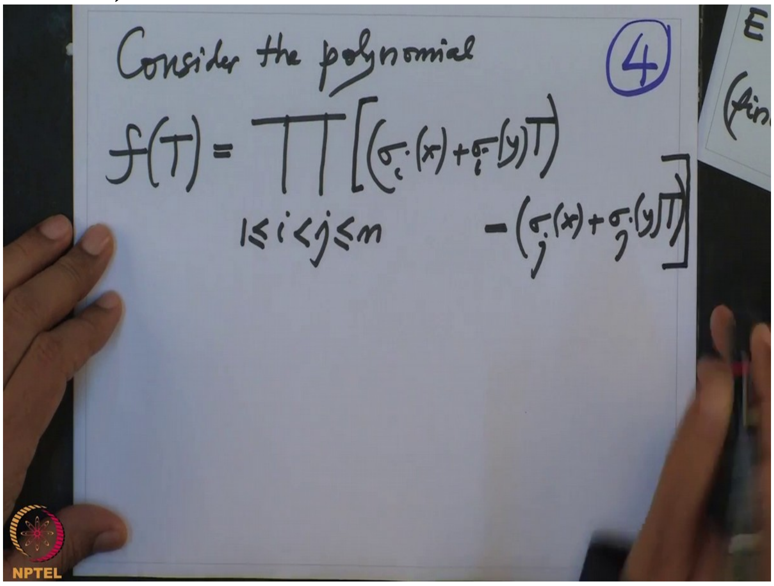
- $\left(\sigma_j(x)+\sigma_j(y)T\right)$.

(Refer Slide Time: 11:12)



And then this is running over the product, this is like this.

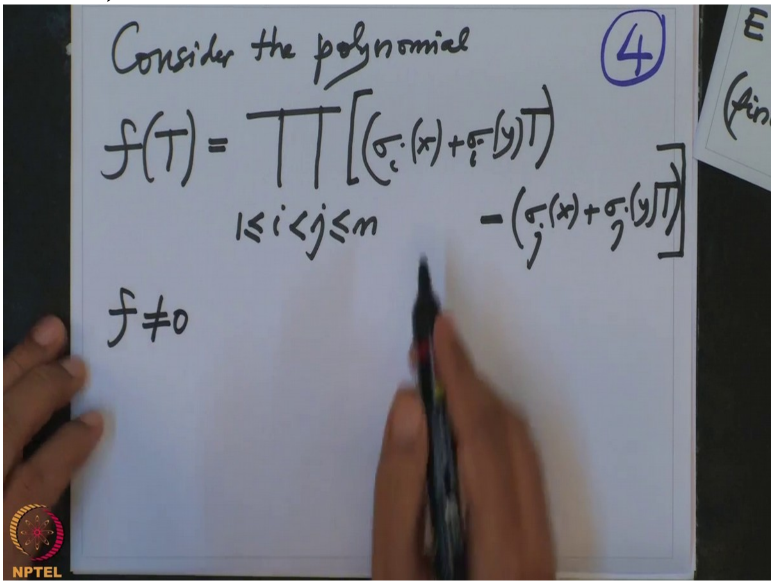
(Refer Slide Time: 11:17)



So just stare at this polynomial.

Obviously this polynomial f is non zero first of all.

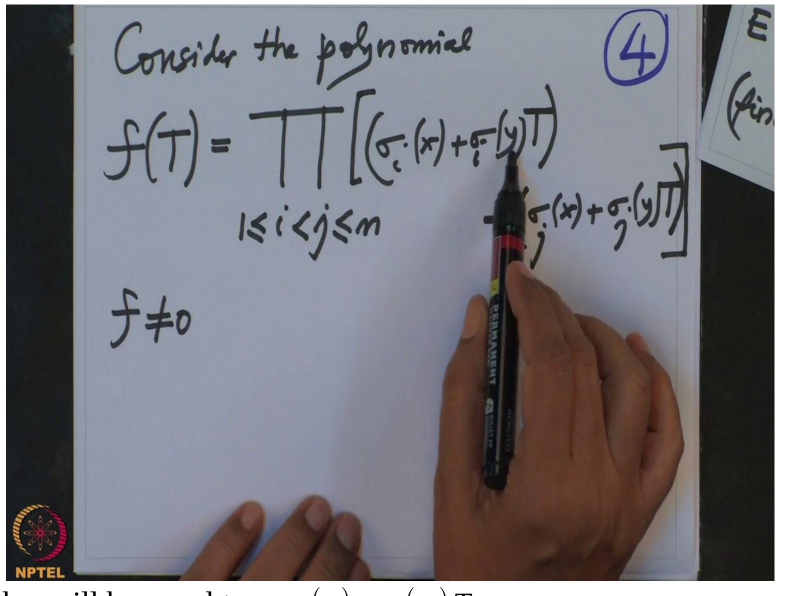
(Refer Slide Time: 11:27)



Because f 0 means what, at least one of the element in the product will be 0.

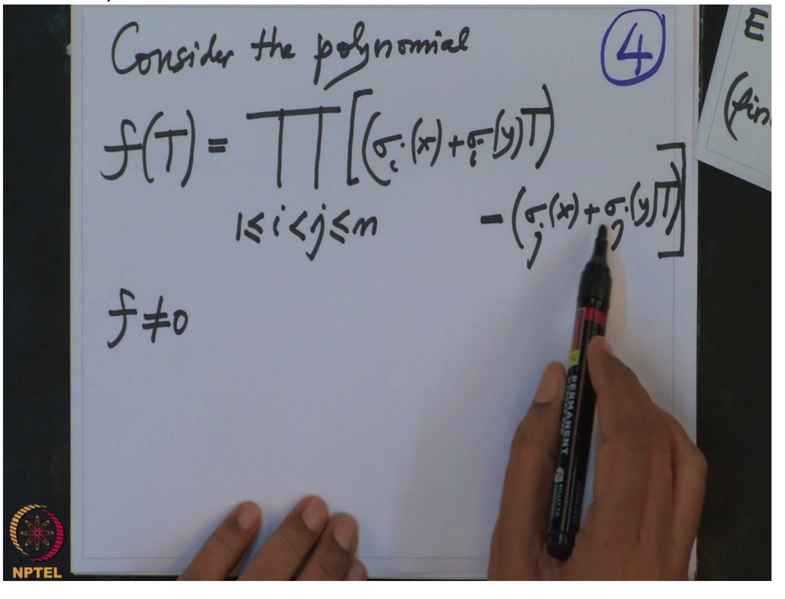
But if the element in the product is 0, that means this $\sigma_i(x)+\sigma_i(y)T$

(Refer Slide Time: 11:40)



will be equal to be, will be equal to $\sigma_j(x)+\sigma_j(y)T$

(Refer Slide Time: 11:44)



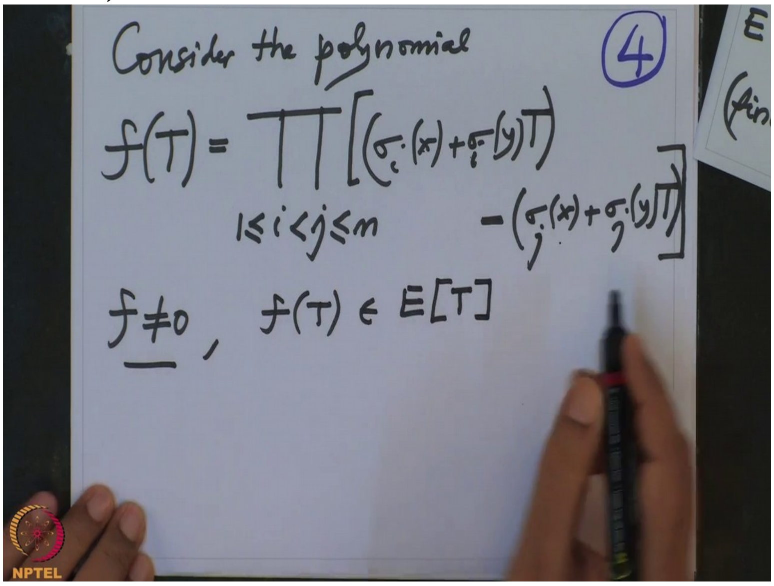
But as the polynomial in T, therefore $\sigma_i(x)=\sigma_j(x)$ and $\sigma_i(y)=\sigma_j(y)$ but i is different from j.

But that cannot happen. Because σ_i is different from σ_j.

Therefore f is non-zero.

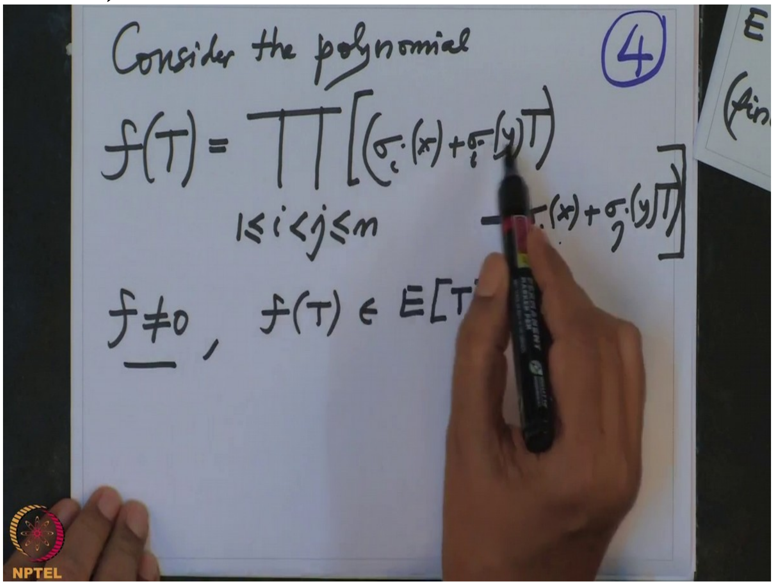
Where are the coefficients of f? They are in E T.

(Refer Slide Time: 12:09)



Coefficients of f

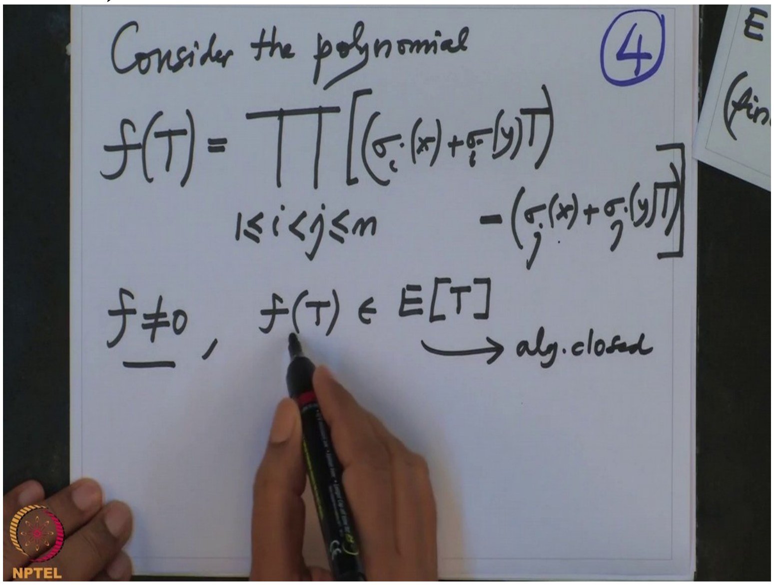
(Refer Slide Time: 12:11)



are this, they are elements, combinations of $\sigma_i \sigma(y)$ and $\sigma_j \sigma(y)$, all are elements of E therefore they are elements of T.

E is algebraically closed

(Refer Slide Time: 12:26)

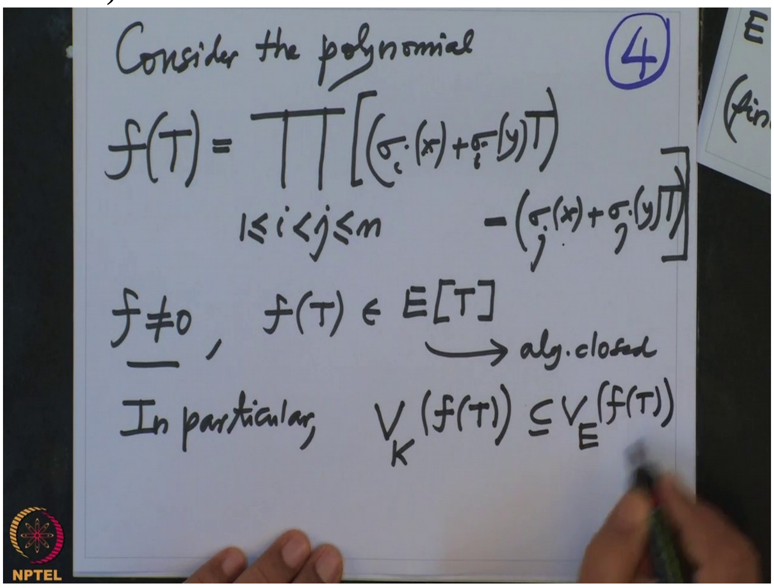


and we have a non-zero polynomial in algebraically closed field.

Therefore, therefore so in particular it has finitely many zeroes and all the zeroes are there.

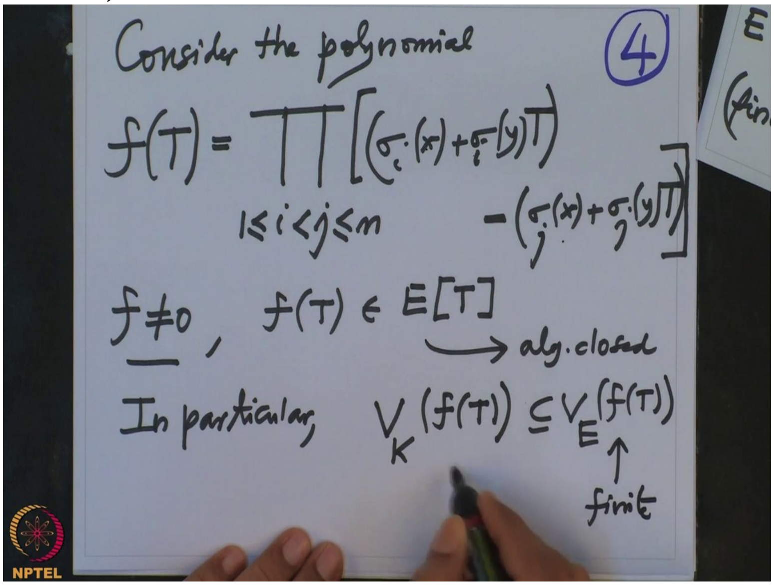
V K, how many zeroes are in, now I look at the zeroes of this in K but this is contained in $V_E(f(T))$

(Refer Slide Time: 12:57)



and this is finite,

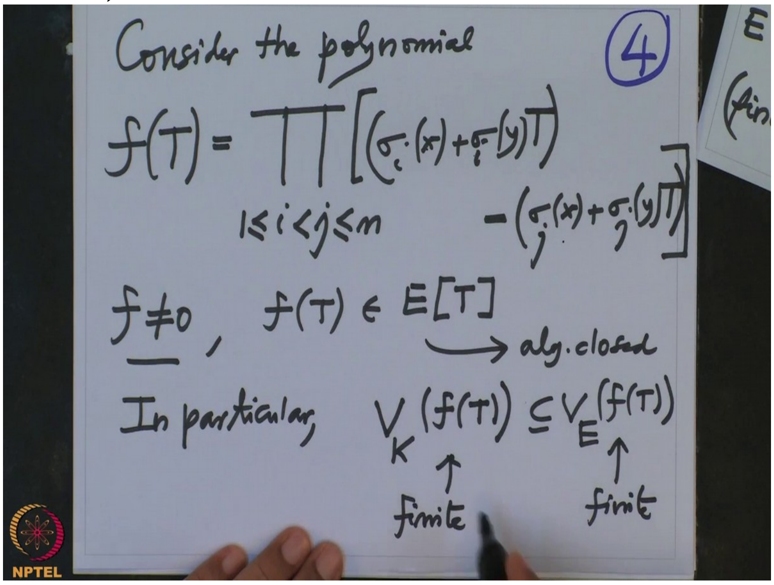
(Refer Slide Time: 13:00)



therefore this is also finite.

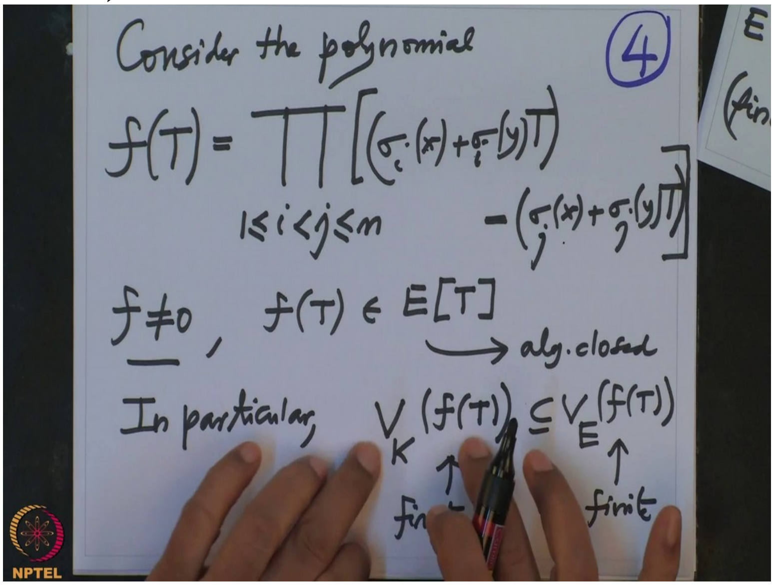
It may or may not have a 0,

(Refer Slide Time: 13:06)



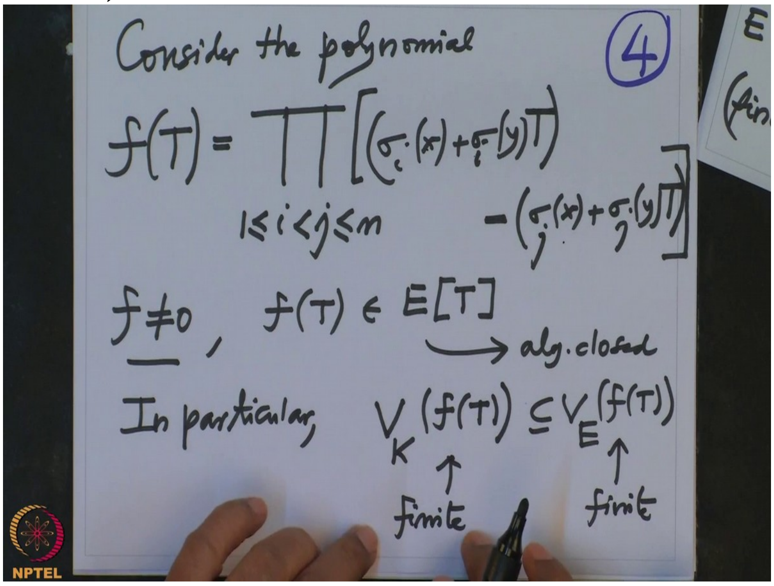
but in any case it is a finite set. It may be empty set

(Refer Slide Time: 13:10)



but it is finite,

(Refer Slide Time: 13:11)

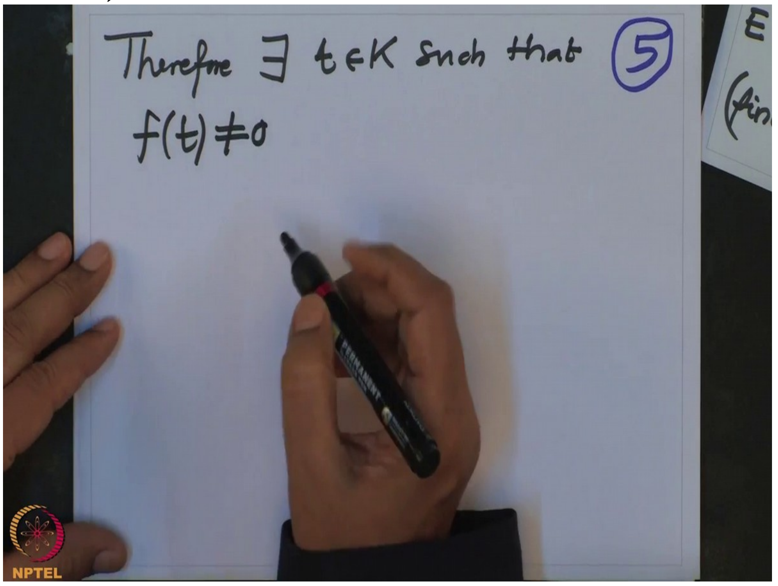


finite is important.

Now it is a finite set. So I can find an element which is outside that.

So therefore there exists an element t in K such that f of t is non-zero

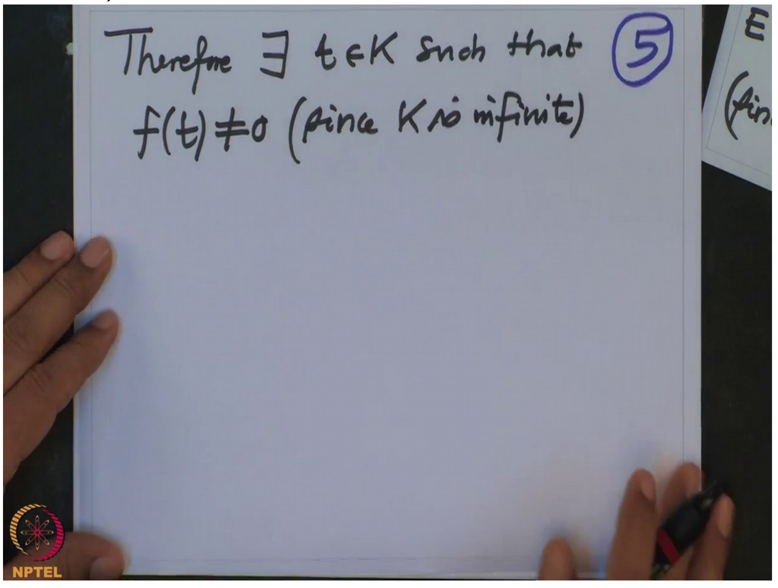
(Refer Slide Time: 13:36)



because since K is infinite.

Infinite field

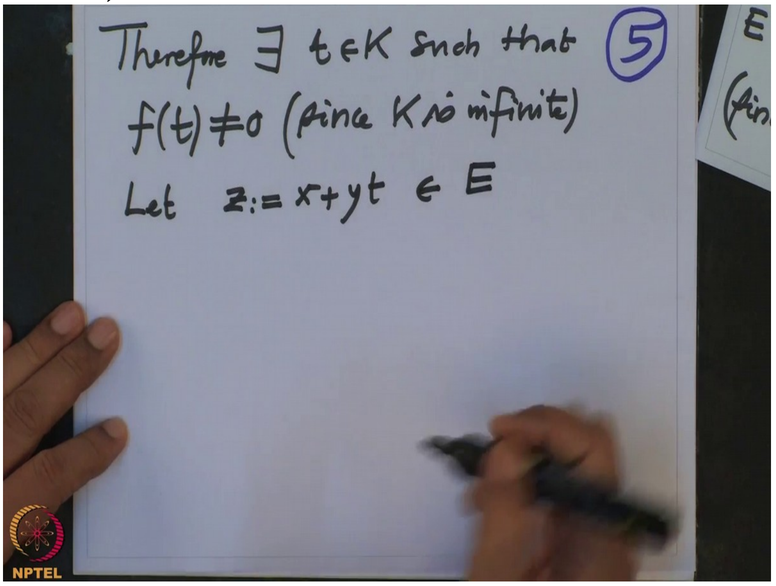
(Refer Slide Time: 13:46)



and a polynomial is non-zero therefore it has zero, not all elements it is zero so at least element it is non-zero.

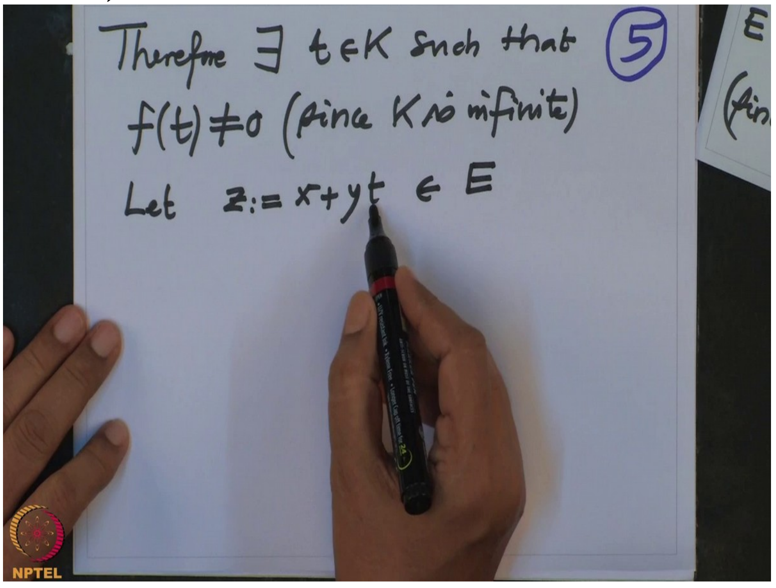
Now let $z = x + yt$. This is obviously an element in E,

(Refer Slide Time: 14:07)



because

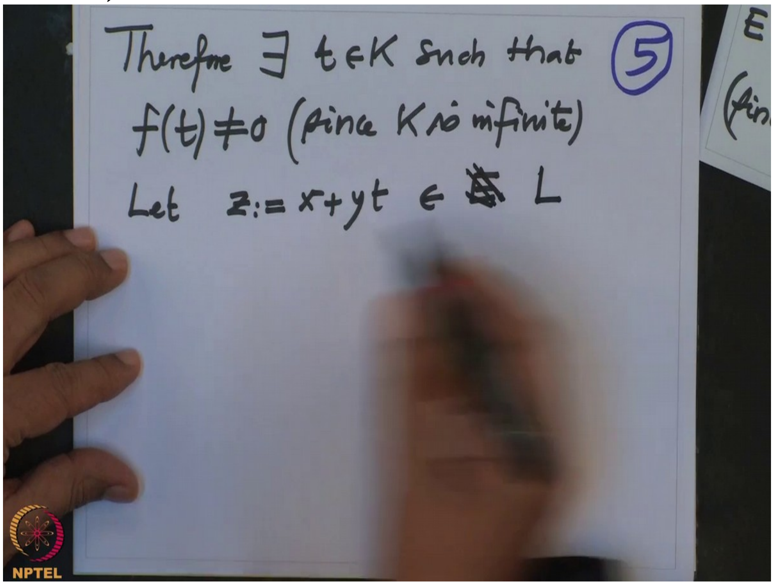
(Refer Slide Time: 14:09)



t is in K, K is a subfield of E and x and y are in L and therefore they are, there is embedding so they are in elements of E also.

So these are the elements in, no what I am saying is actually they are elements in L

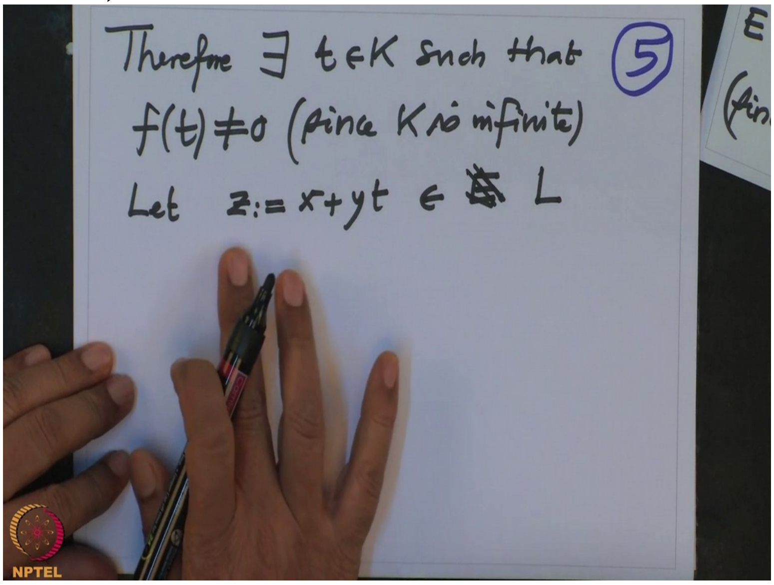
(Refer Slide Time: 14:30)



because x is in L, y is in L and t is in K therefore they are elements in L.

Now I want to check that this z is

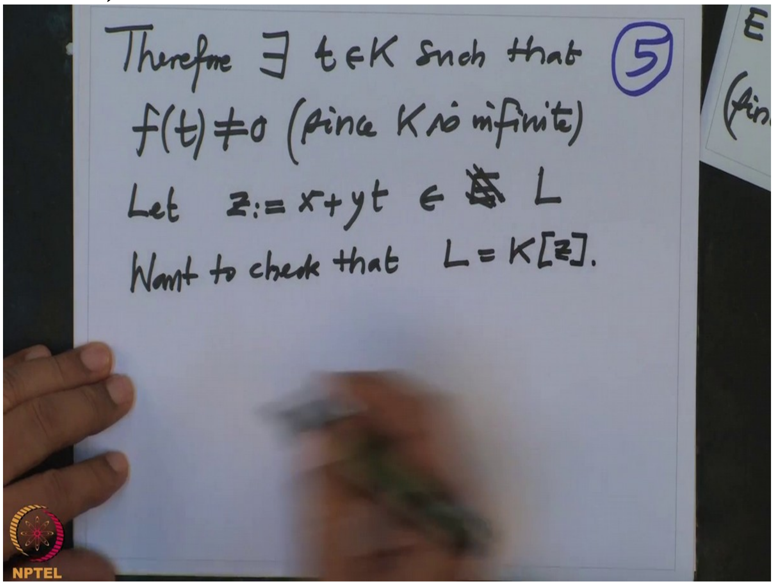
(Refer Slide Time: 14:38)



a required element.

So we may want to check, want to check that L equal to $K(z)$. And that

(Refer Slide Time: 14:55)

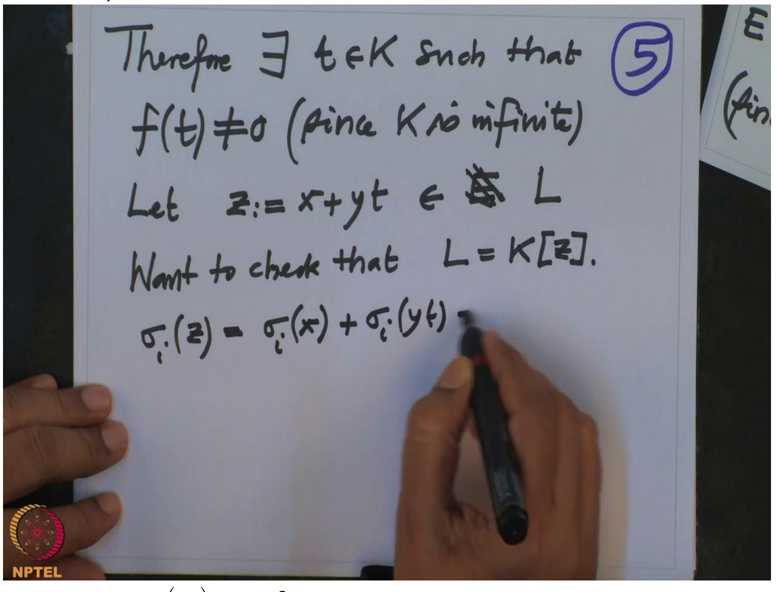


will finish our proof, alright.

So look at $\sigma_i(z)$ is, apply σ to this.

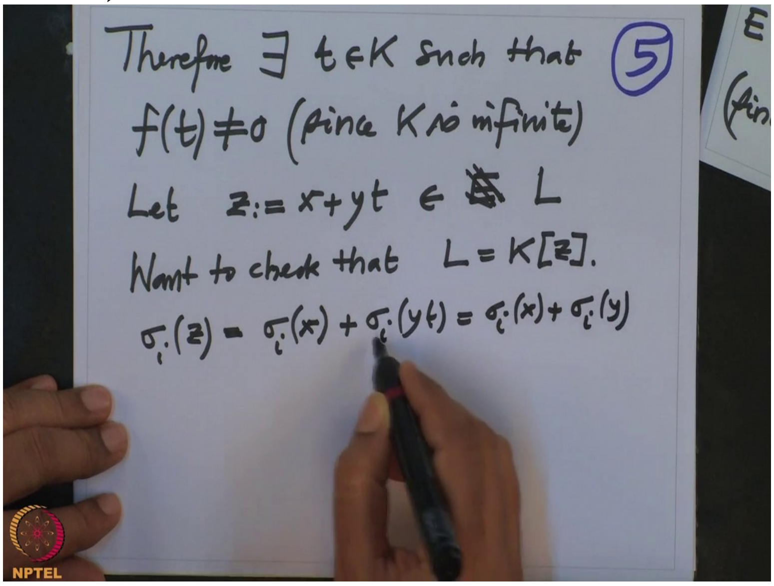
Because sigma is a K-algebra homomorphism so this is $\sigma(x)+\sigma_i(yt)$

(Refer Slide Time: 15:14)



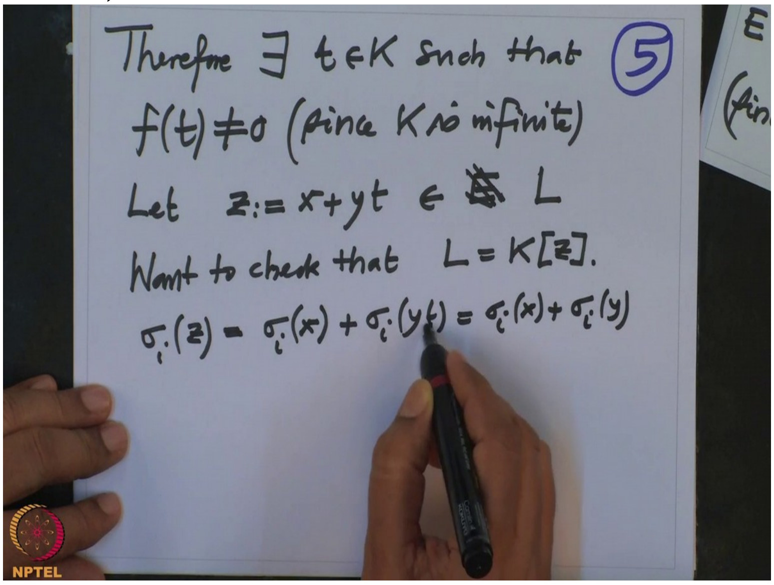
but $\sigma_i(yt)$ is same as $\sigma_i(y)$ and

(Refer Slide Time: 15:21)



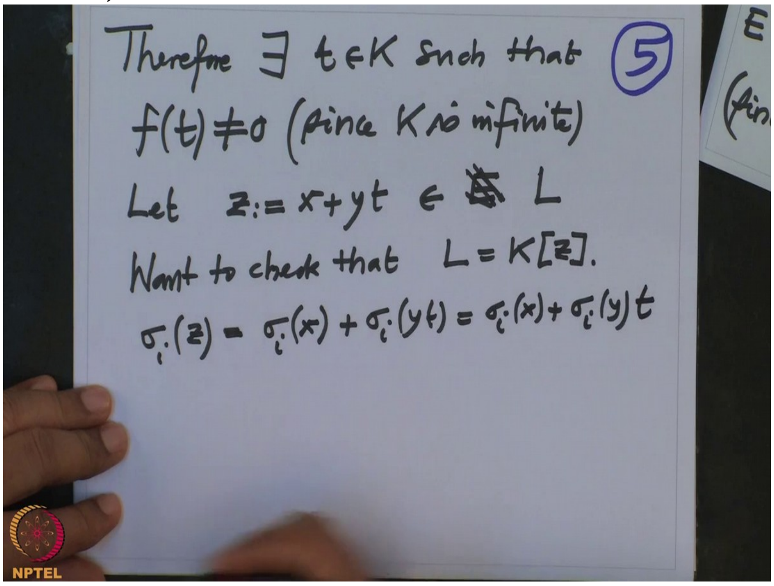
$\sigma_i(t)$ but σ is identity

(Refer Slide Time: 15:24)



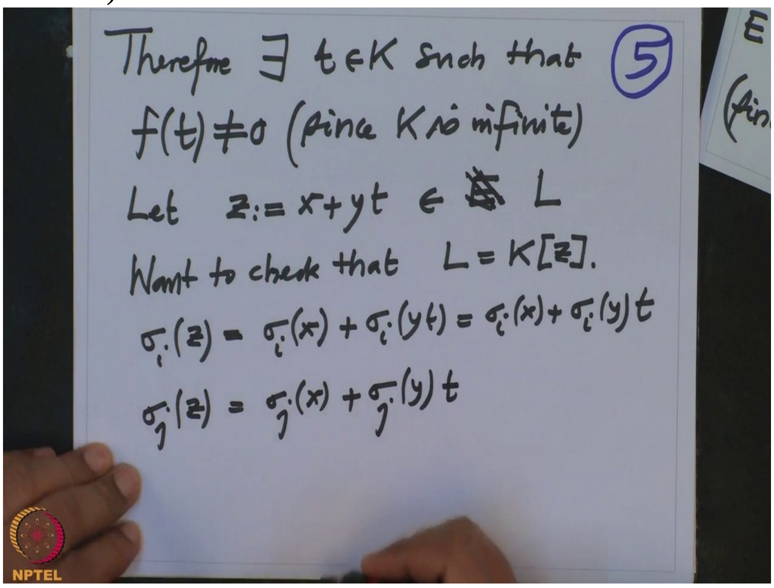
on K, therefore this is just t.

(Refer Slide Time: 15:27)



Ok, on the other hand, Ok when I apply $\sigma_j(t)$, $\sigma_j(z)$, what do I get? I get this is $\sigma_j(x)+\sigma_j(yt)$.

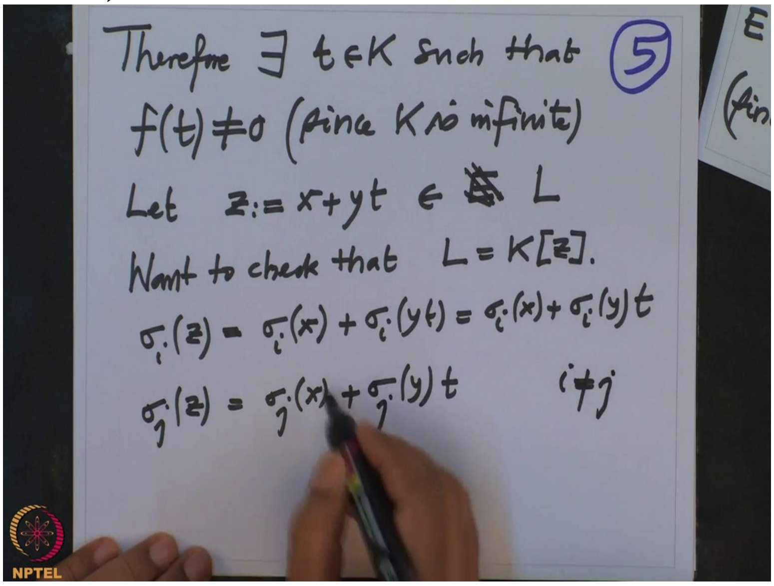
(Refer Slide Time: 15:50)



So i not equal to j.

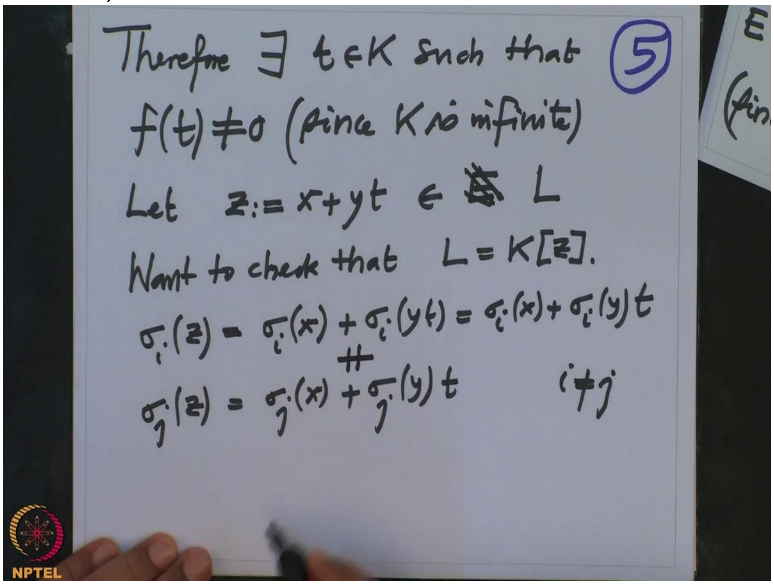
Ok, but now note that i is, if i is different from j

(Refer Slide Time: 16:07)



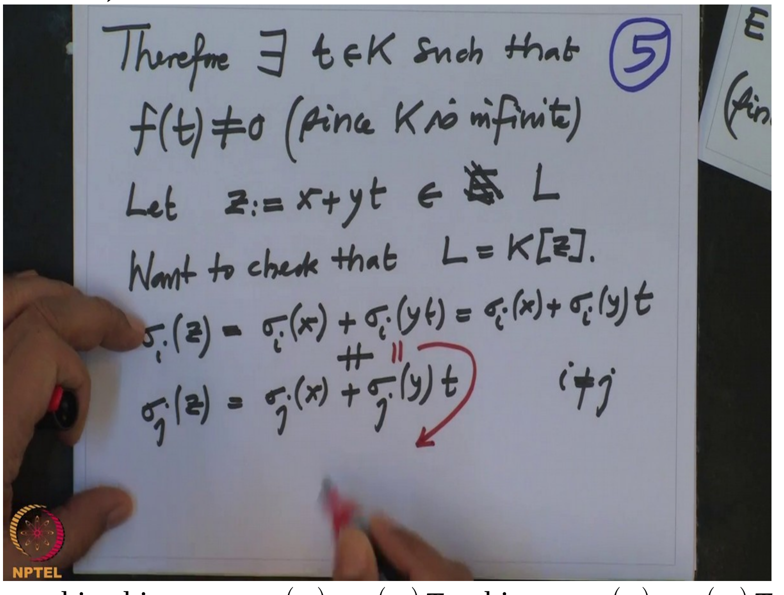
this cannot be equal to this. Both this cannot be equal to, so I claim that this is not equal,

(Refer Slide Time: 16:14)



because if it is equal then, if it is equal here, if equality so I want to write the another color, if equality here, then what happens?

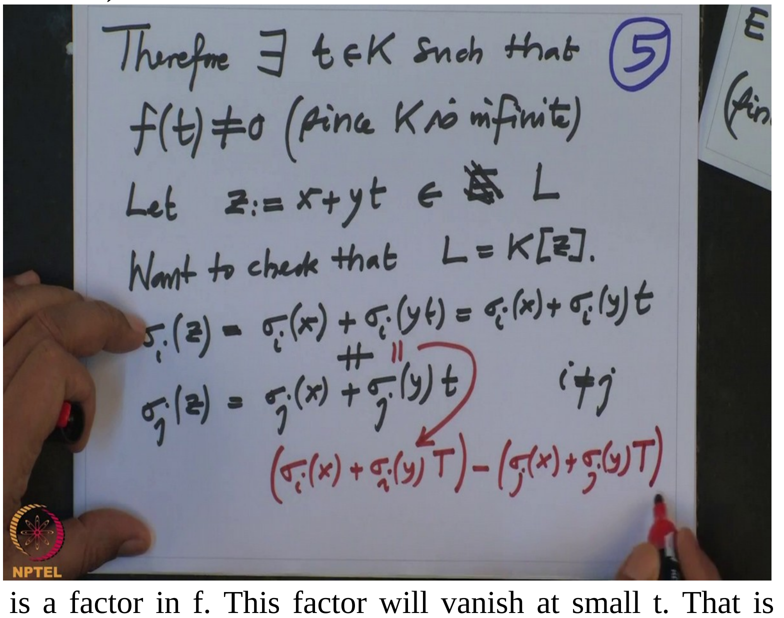
(Refer Slide Time: 16:31)



Then we get, we get this, this guy, $\sigma_i(x)+\sigma_i(y)T$ this $-\sigma_j(x)+\sigma_j(y)T$.

This is one of the

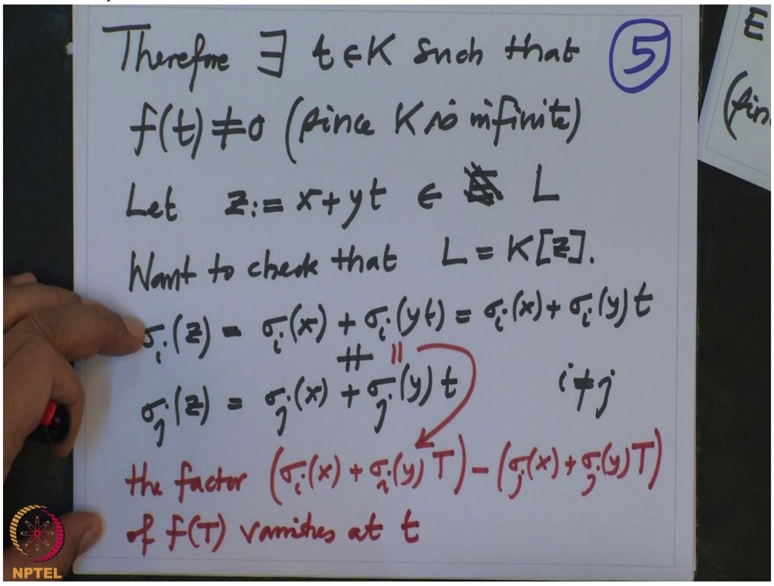
(Refer Slide Time: 16:51)



factor in f. This is a factor in f. This factor will vanish at small t. That is the meaning of equality here.

So this equality means the factor of f, $f(T)$ vanish, vanishes at t,

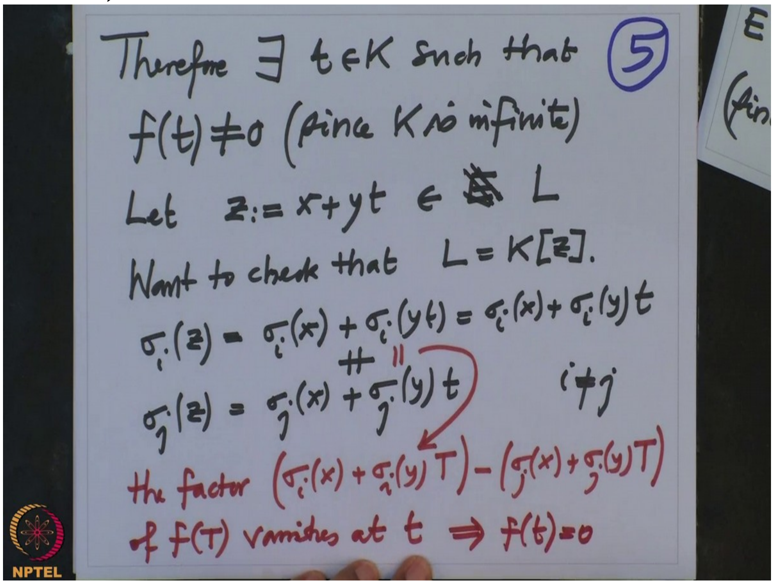
(Refer Slide Time: 17:20)



because equality here means when I evaluate it at T; that is equal here, so it is equal.

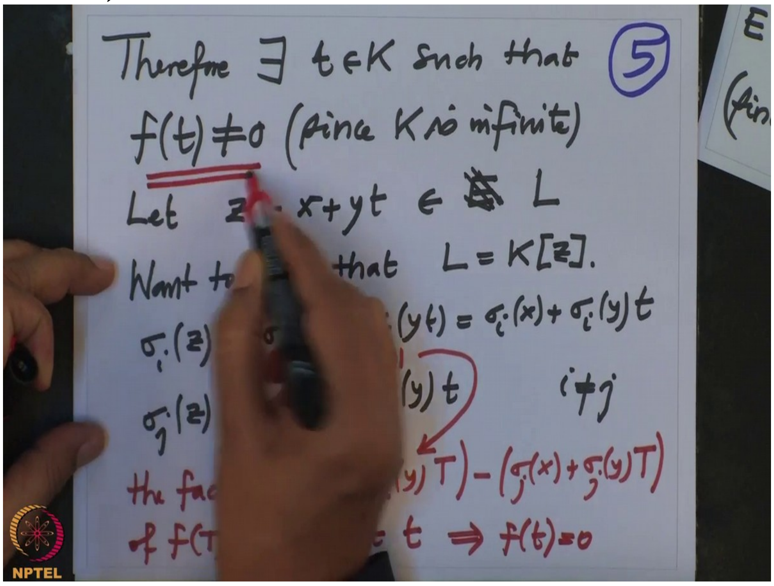
But that will mean if a factor vanish then f of t will be 0.

(Refer Slide Time: 17:33)



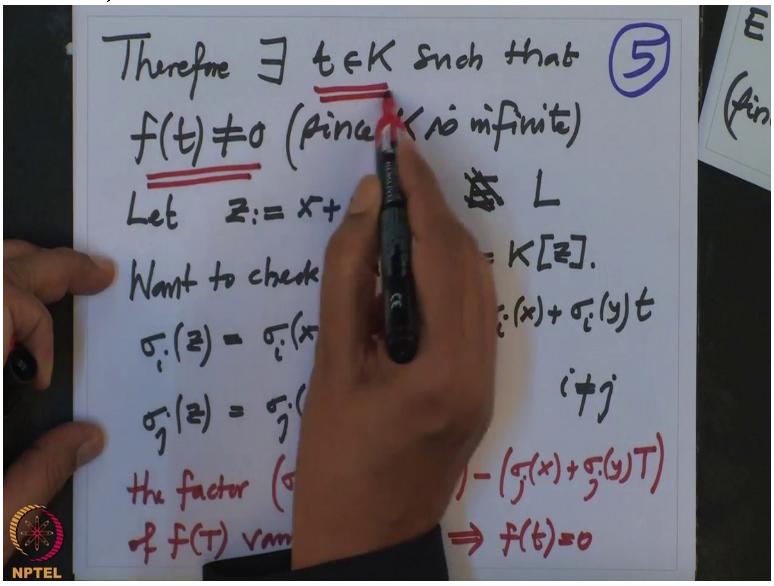
But I have chosen f of t, so that

(Refer Slide Time: 17:37)



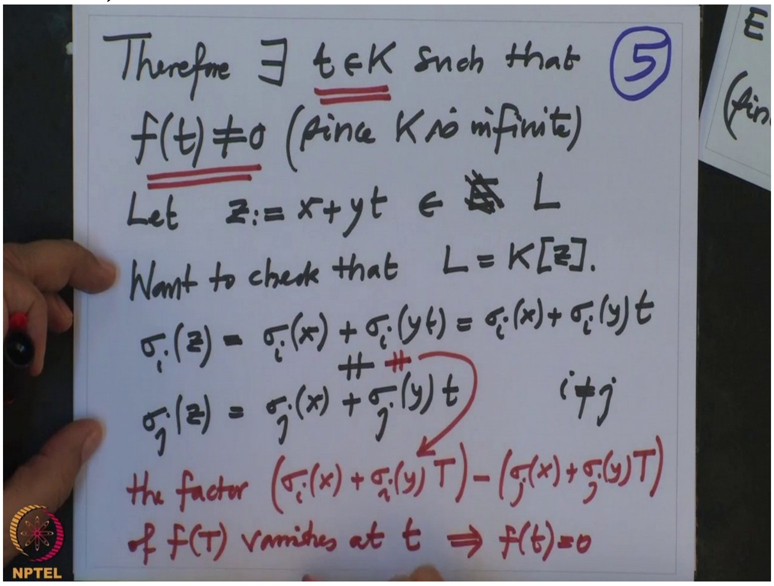
I have chosen t

(Refer Slide Time: 17:38)



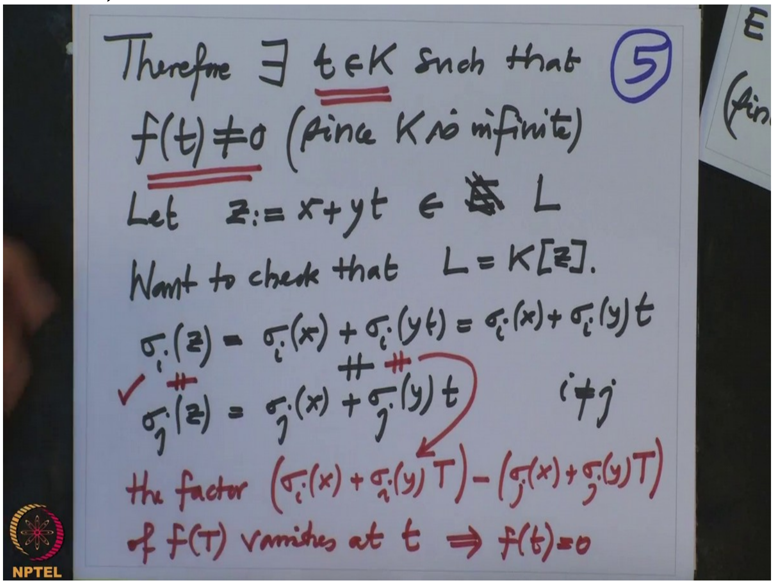
so that f of t is non-zero. So therefore this

(Refer Slide Time: 17:41)



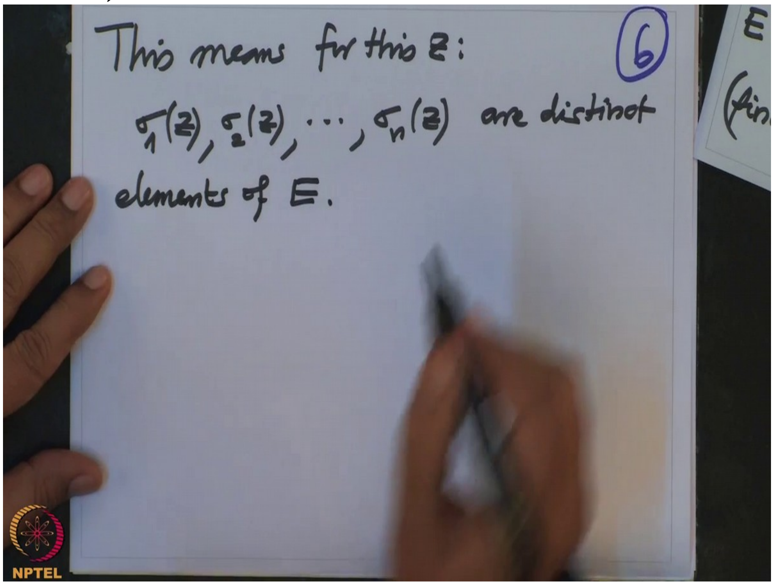
cannot be equal and therefore $\sigma_i(z)$ is not equal to $\sigma_j(z)$.

(Refer Slide Time: 17:47)



So I have done. That means I have chosen my z; so this means, this means, for this z $\sigma_1(z),\ldots,\sigma_n(z)$ are distinct elements of E and that is what we wanted

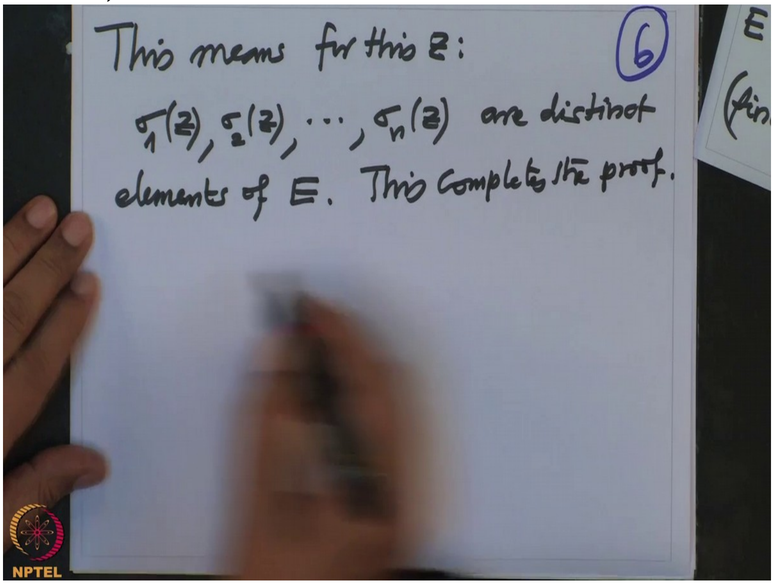
(Refer Slide Time: 18:26)



to prove.

And this finish, this completes the proof.

(Refer Slide Time: 18:37)

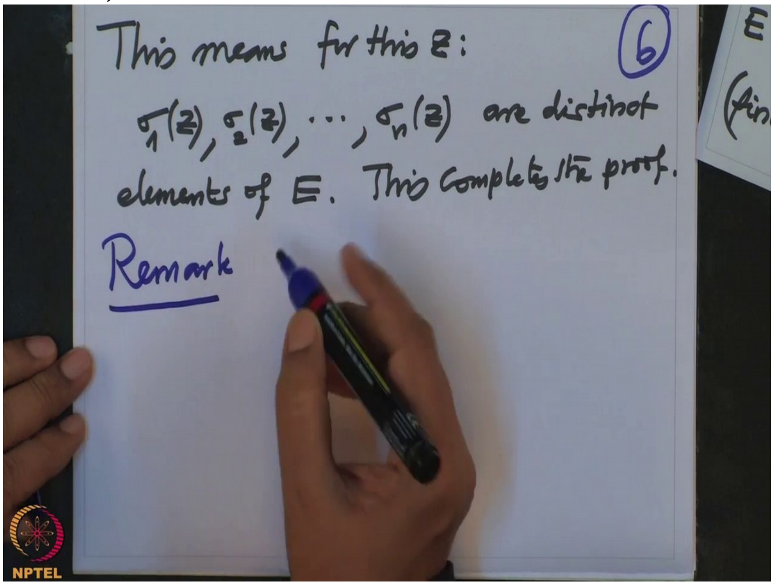


Now I want to indicate also that, this proof we have done it by induction on the number of generators of L over K. L is a finite extension of K and by the induction on the number of generators of L over K we have proved that L over K is simple.

But one can also avoid the induction and directly prove it. So I just want to indicate that direct proof.

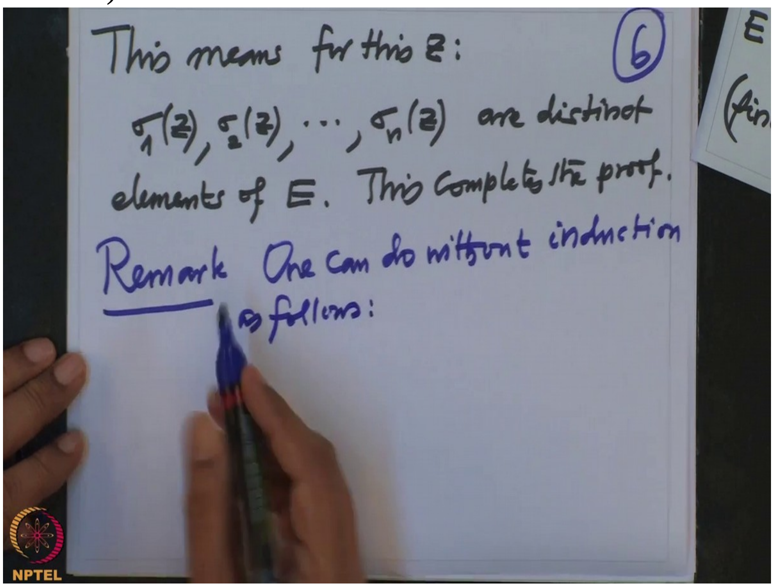
So another, so this is remark, this is remark,

(Refer Slide Time: 19:15)



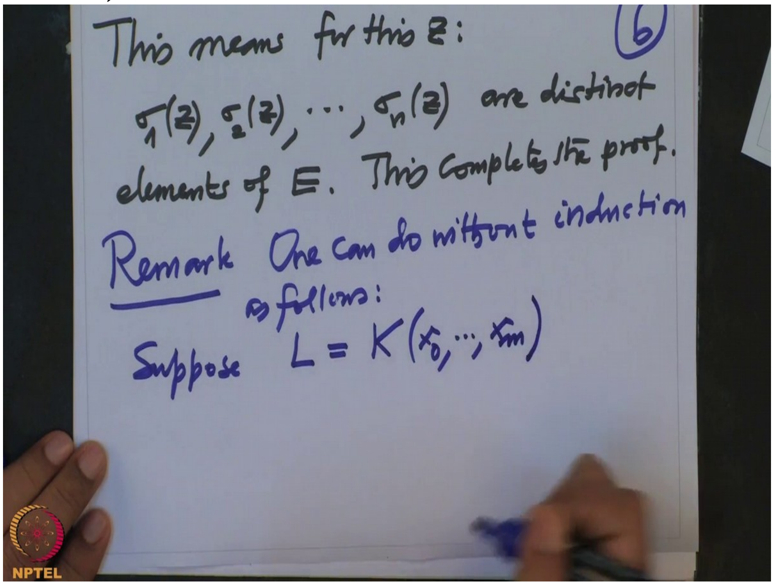
one can do without induction as follows.

(Refer Slide Time: 19:30)



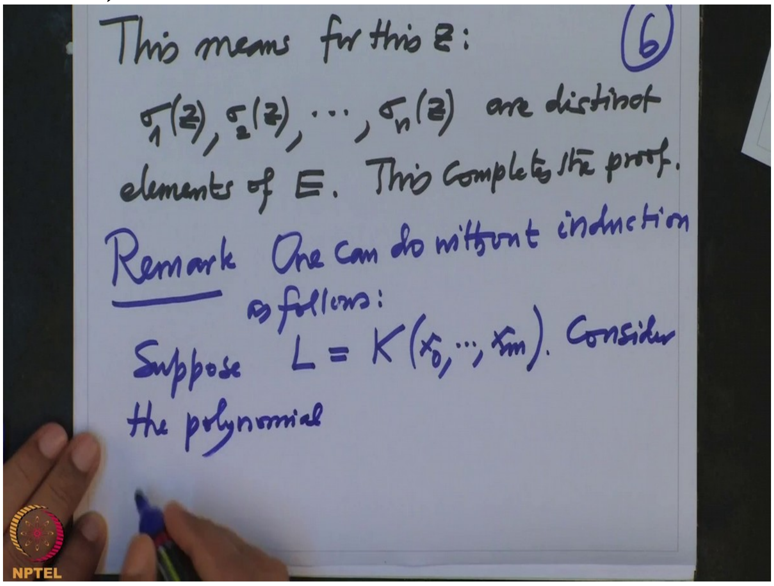
So, so suppose L is a finite extension of K, therefore let us say L is generated by $x_0, \ldots, x_n$.

(Refer Slide Time: 19:47)



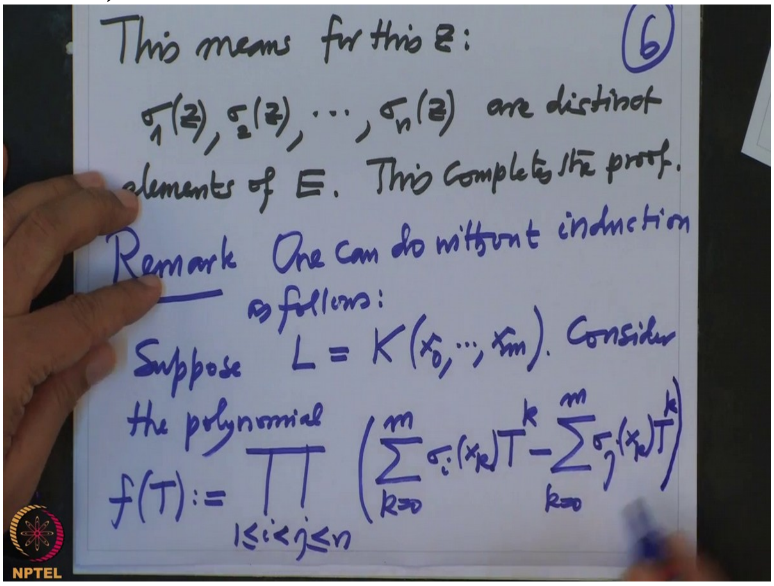
And now instead of, we can consider the following polynomial. Consider the polynomial

(Refer Slide Time: 20:02)



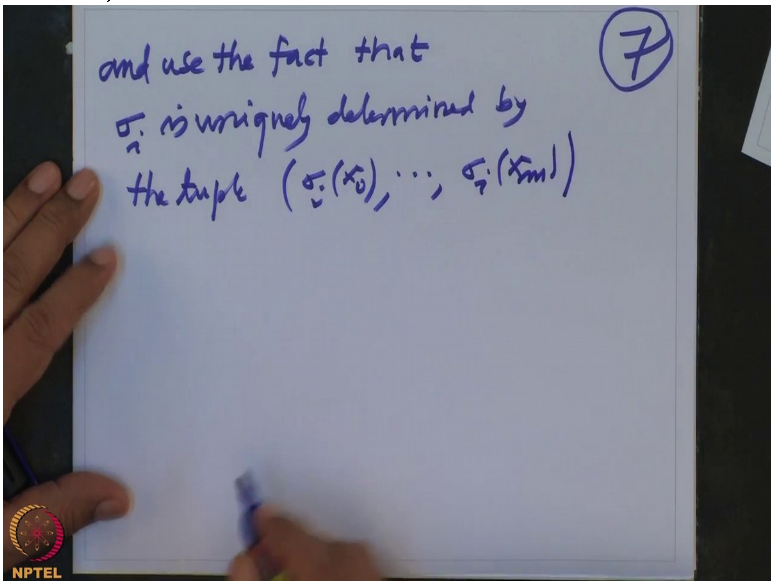
f, f T equal to product, 1 less equal to i less than j less equal to n and then the sum, sum is from k equal to 0 to m $\sigma_i(x_k)t^k$ minus summation k is from 0 to m $\sigma_j(x_k)T^k$.

(Refer Slide Time: 20:43)



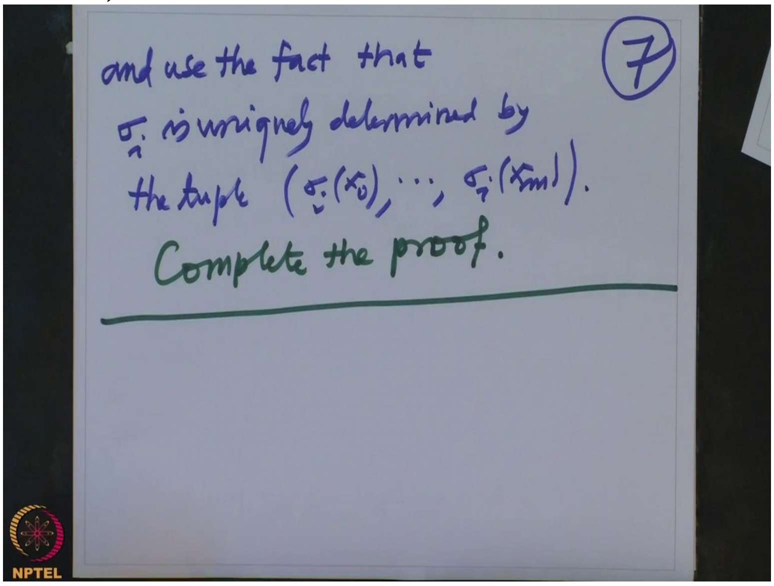
And do the same, do the same trick. So instead of, do the same trick and use the fact that σ_i and σ_j, I will write in the next page, and use the fact that σ_i is uniquely determined by the tuple $\sigma_i(x_0),\ldots,\sigma_i(x_n)$.

(Refer Slide Time: 21:32)



And same trick, so I will, so I would just say here, completed the proof, complete the proof. Is the same trick, no more extra trick is needed

(Refer Slide Time: 21:52)

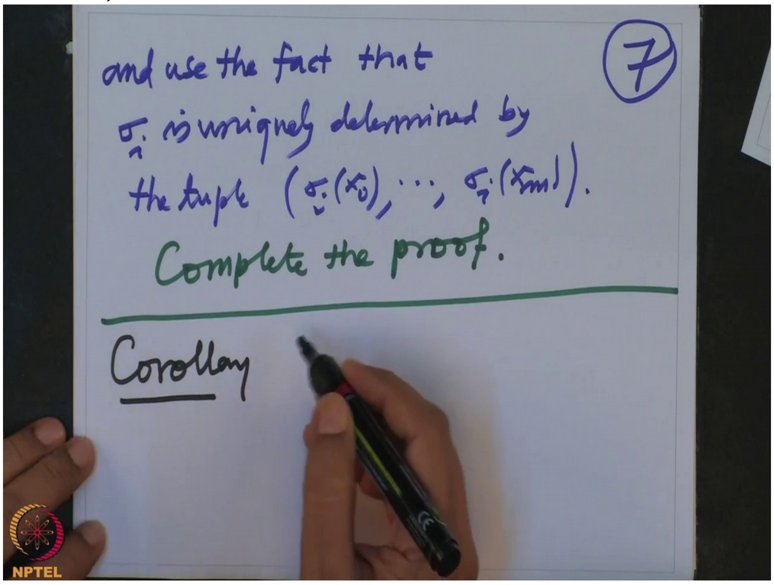


for this, so that was what.

Now let us deduce some consequences from here.

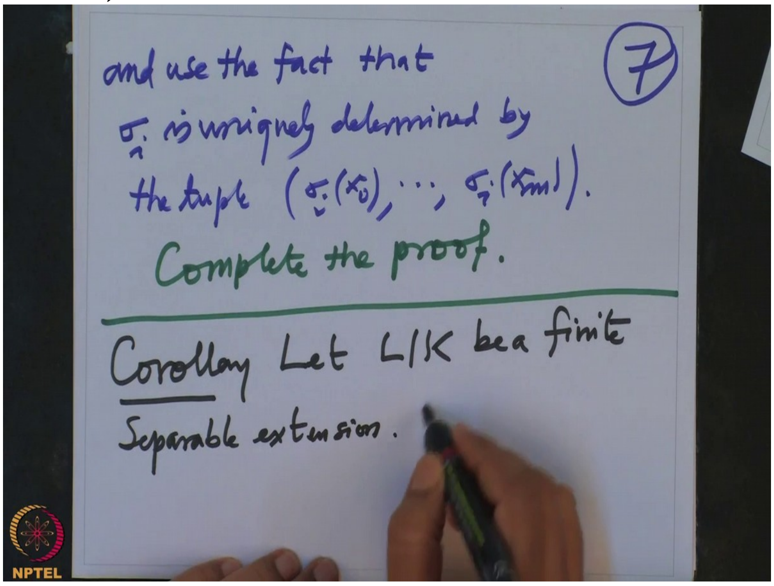
So the first important consequence, so corollary,

(Refer Slide Time: 22:06)



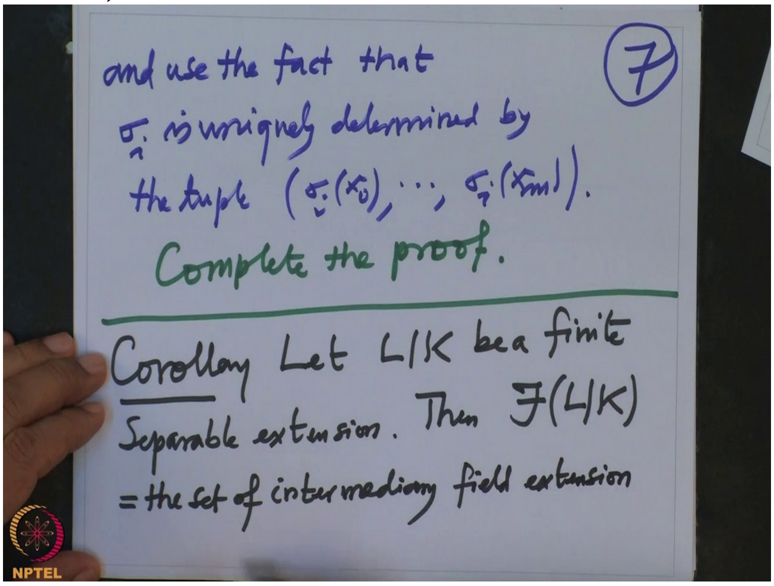
let L over K be a finite separable extension

(Refer Slide Time: 22:24)



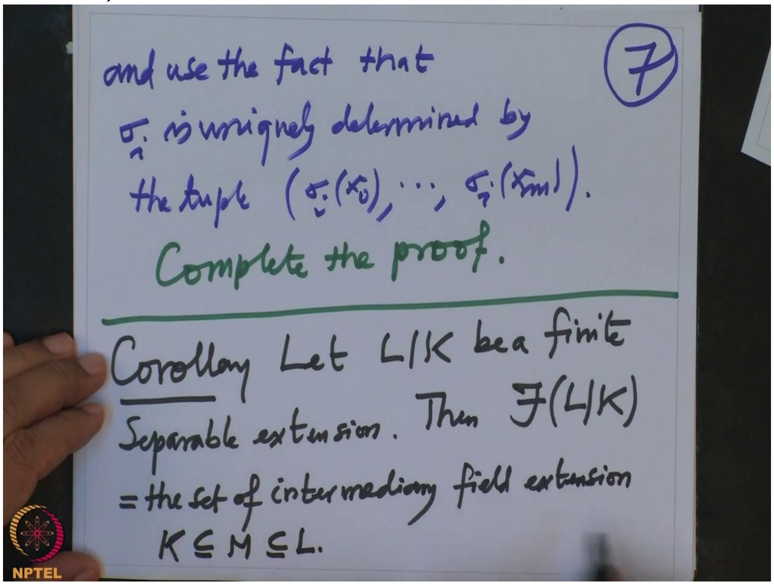
then f L over K, the set, this is the set of intermediary field extensions

(Refer Slide Time: 22:50)



K contained in M contained in L,

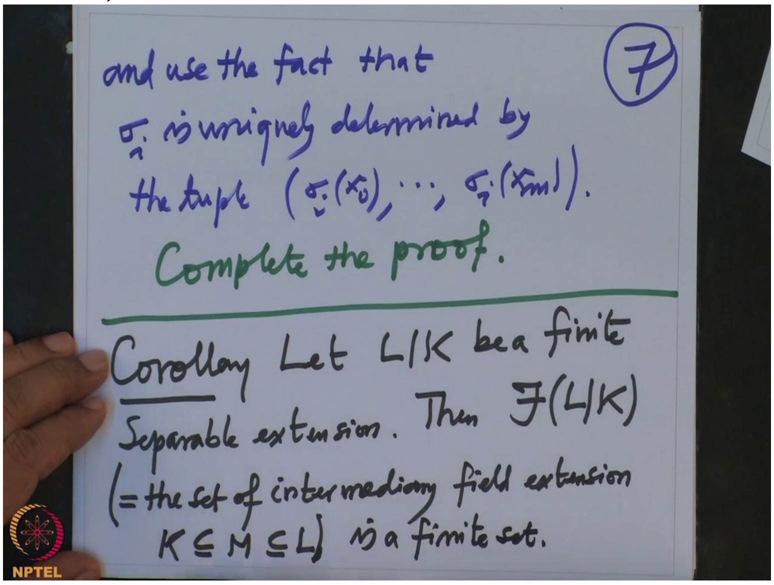
(Refer Slide Time: 22:55)



this set, so this is the definition of that set.

Then this is a finite set. That means there are only finitely

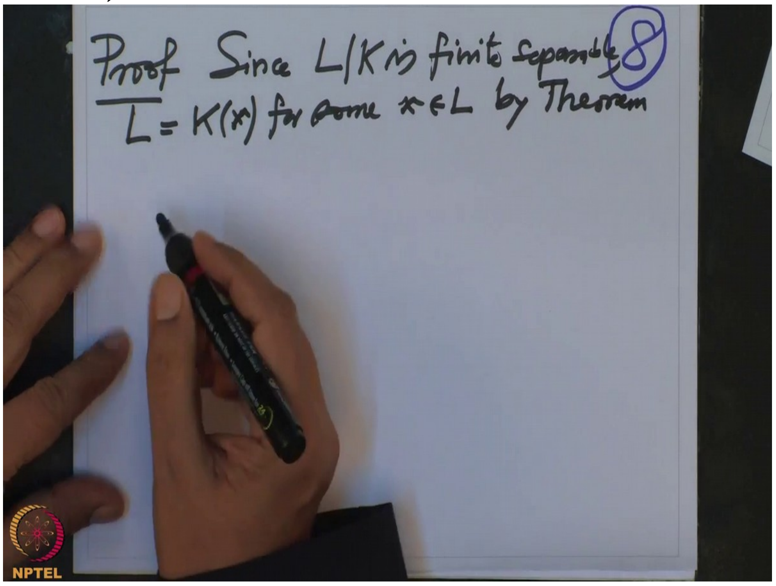
(Refer Slide Time: 23:07)



many intermediary extensions.

So proof, proof, since L over K is finite separable, L over K is finite separable, we know it is simple. L is $K[x]$ for some x by theorem.

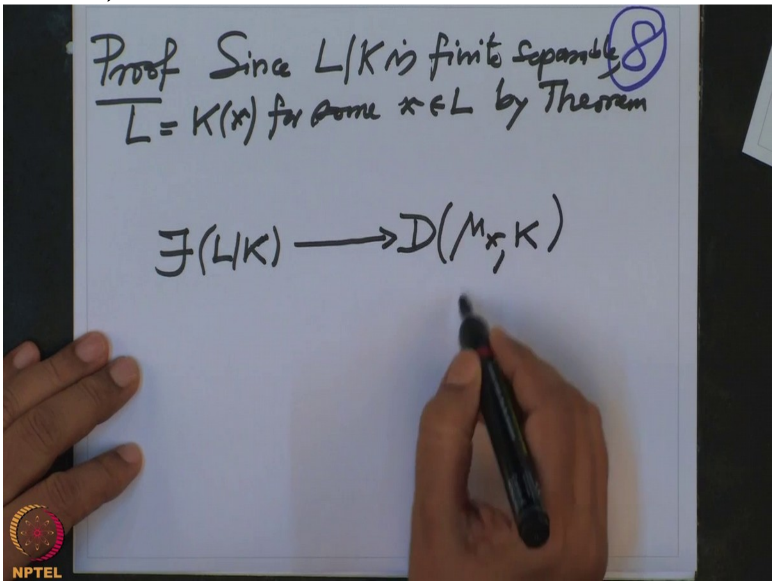
(Refer Slide Time: 23:48)



And we want to check that this is a finite set. I want to check this is finite.

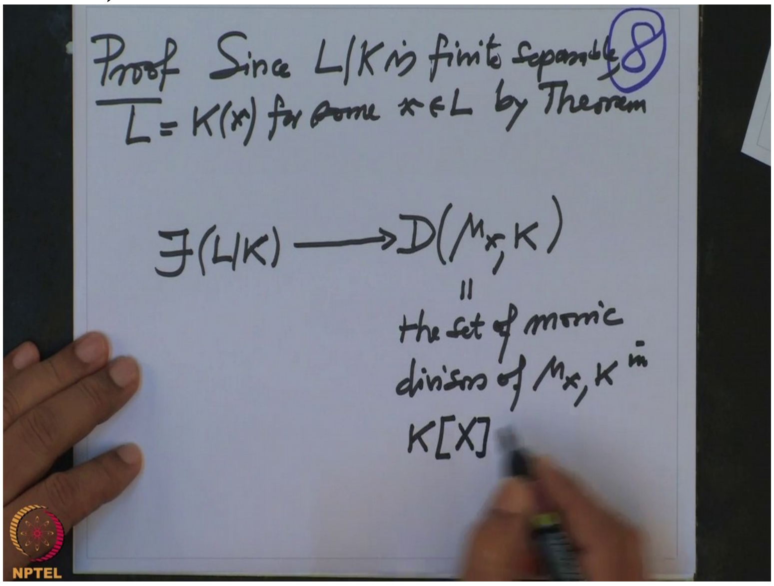
So I am going to give you a map from this set to divisors of $D(\mu_{x,K})$. What is $D(\mu_{x,K})$?

(Refer Slide Time: 24:08)



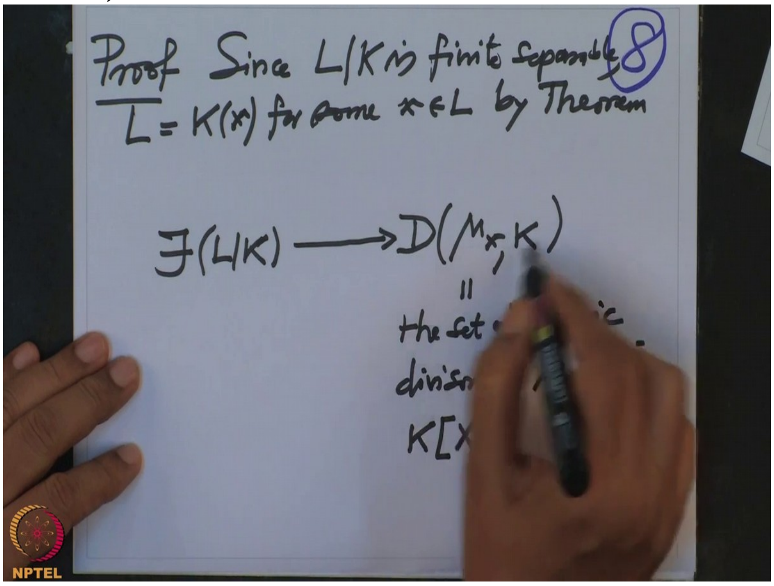
This is, these are, this is the set of monic divisors of $\mu_{x,K}$ in the polynomial ring, in $K[X]$.

(Refer Slide Time: 24:28)



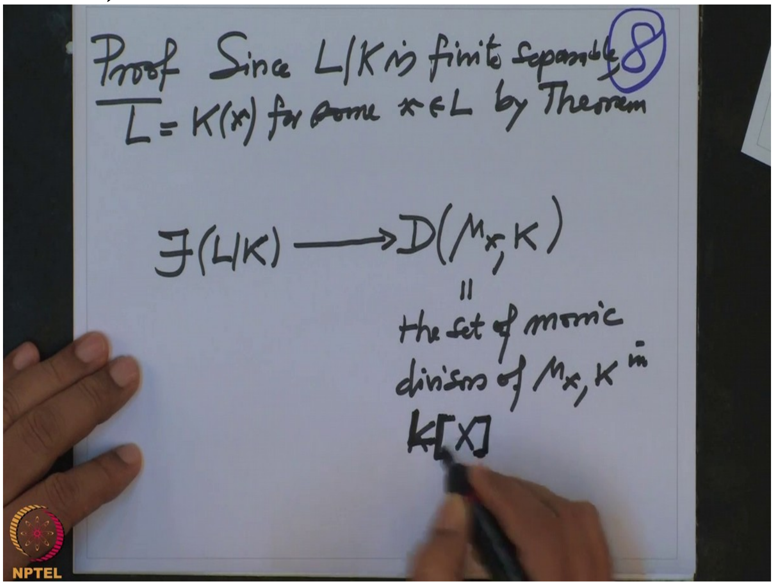
This is a monic polynomial,

(Refer Slide Time: 24:29)



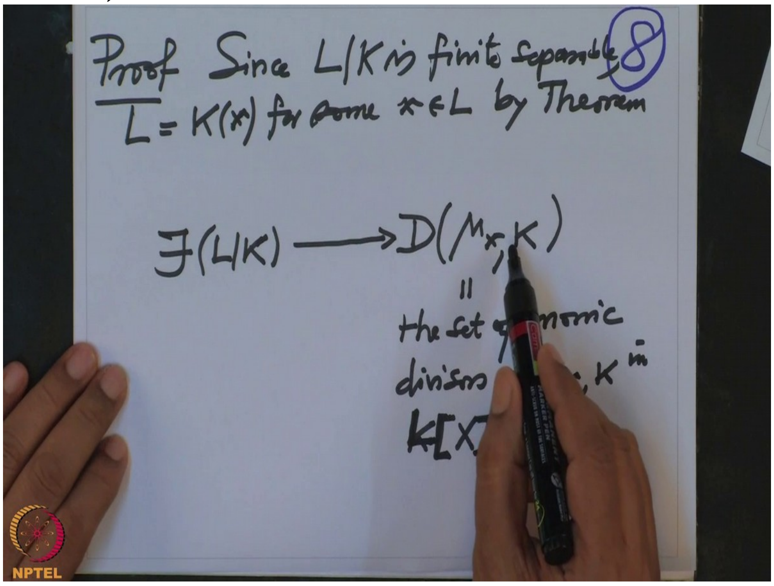
monic irreducible polynomial not in $K[X]$ but in $L[X]$.

(Refer Slide Time: 24:42)



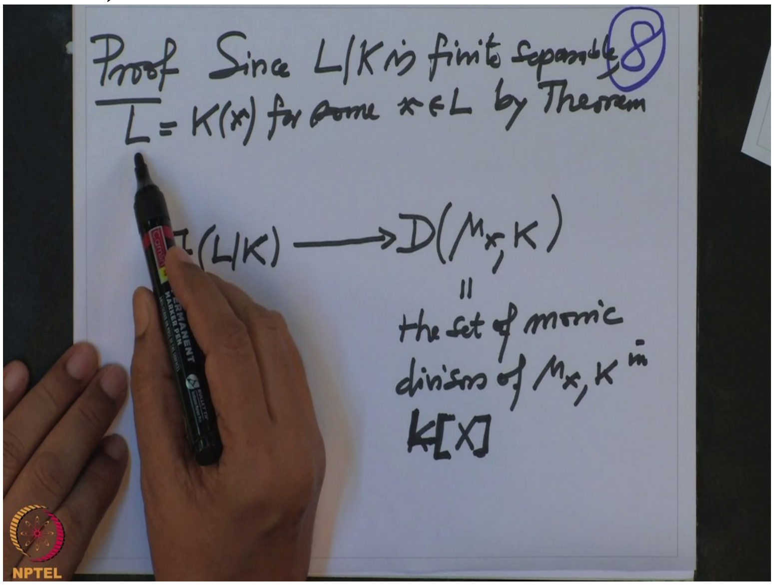
It is a

(Refer Slide Time: 24:45)



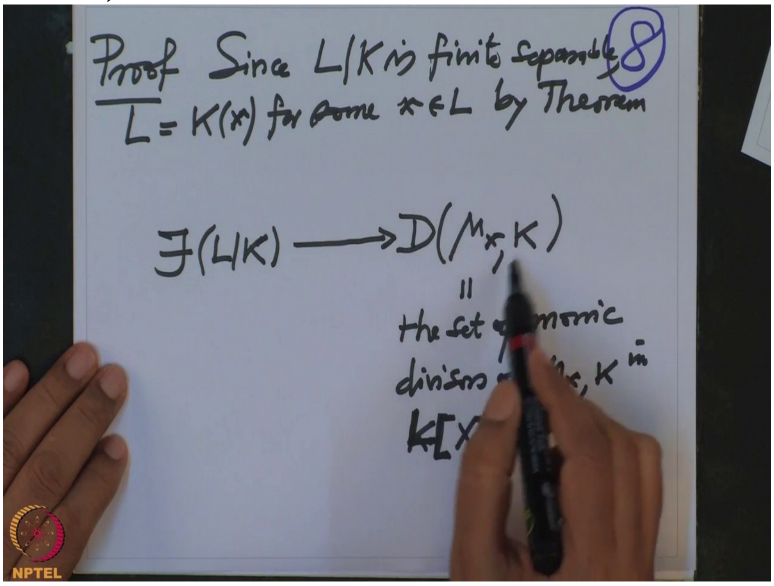
a irreducible polynomial in $K[X]$ but in

(Refer Slide Time: 24:49)



L, when you go to L, it has a 0 in x so definitely this polynomial

(Refer Slide Time: 24:56)

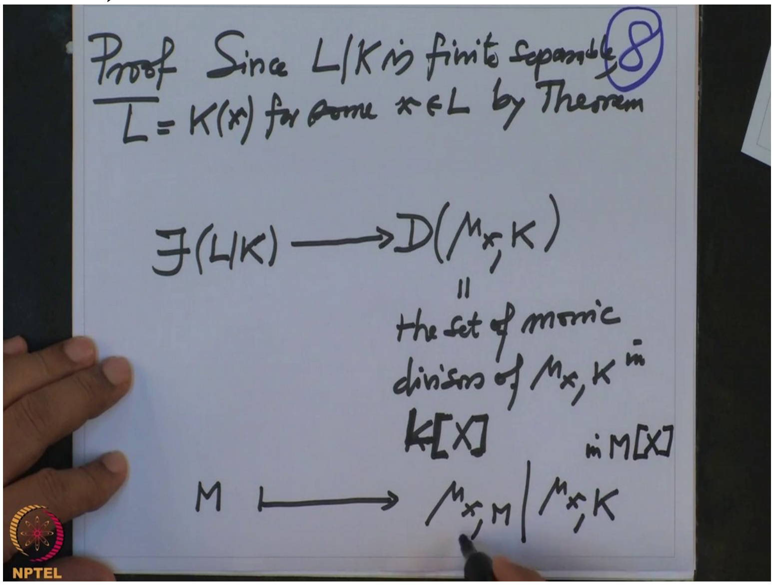


is not irreducible over $L[X]$ so I look at the monic divisors of that polynomial in $L[X]$.

And what is the map? Map is very simple. Take any M, intermediary field and look at the minimal polynomial of X over M.

This minimal polynomial of X over M and what is the relation between minimal polynomial of X over K, this divide this where in $M[X]$ but if

(Refer Slide Time: 25:30)



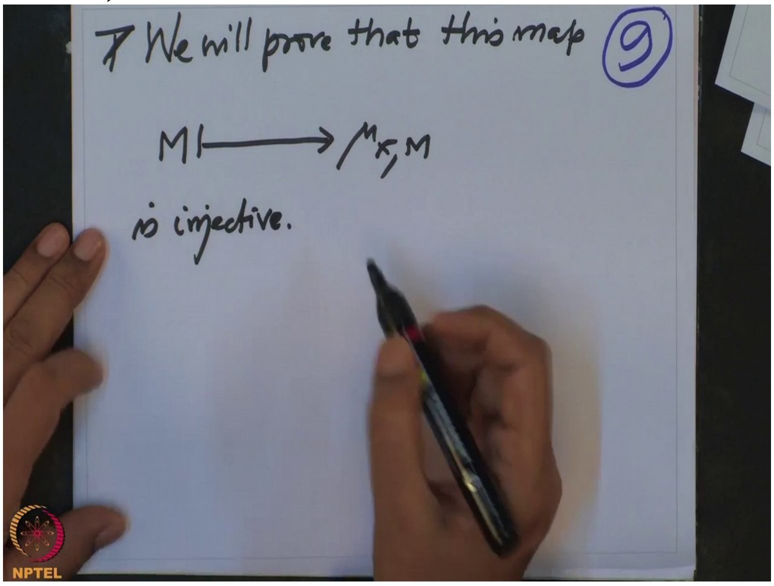
it divides in $M[X]$ then it will also divide in $L[X]$ because L is bigger field.

So our map is very simple, M going to the minimal polynomial of X over M. And I claim that this map is injective.

So the map we will check, we will prove, prove that this map, what is the map, M going to $\mu_{x,M}$ is injective.

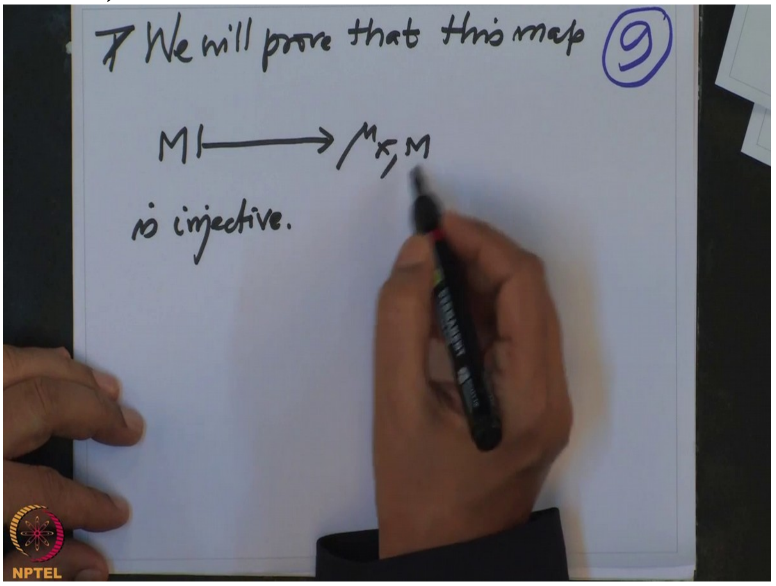
What does that mean?

(Refer Slide Time: 26:09)



How does one prove that map is injective? That means if I know this

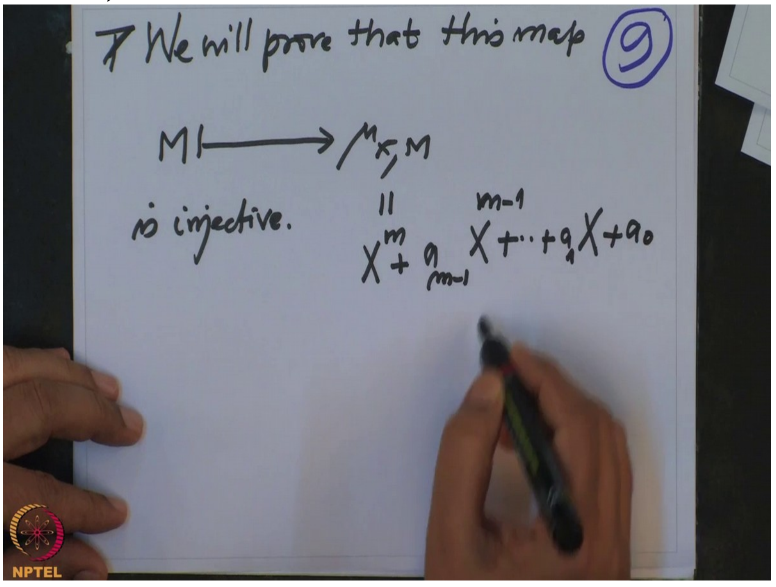
(Refer Slide Time: 26:13)



polynomial then I should get back this M.

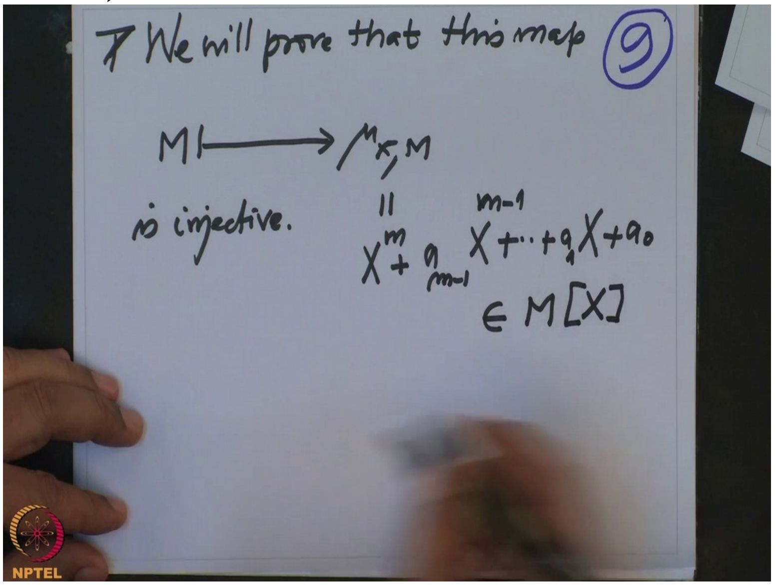
So let us write this polynomial. Suppose this polynomial where, where, this is a monic polynomial of some degree. So suppose it is $X^m + a_{m-1}X^{m-1} + ... + a_1 X + a_0$,

(Refer Slide Time: 26:38)



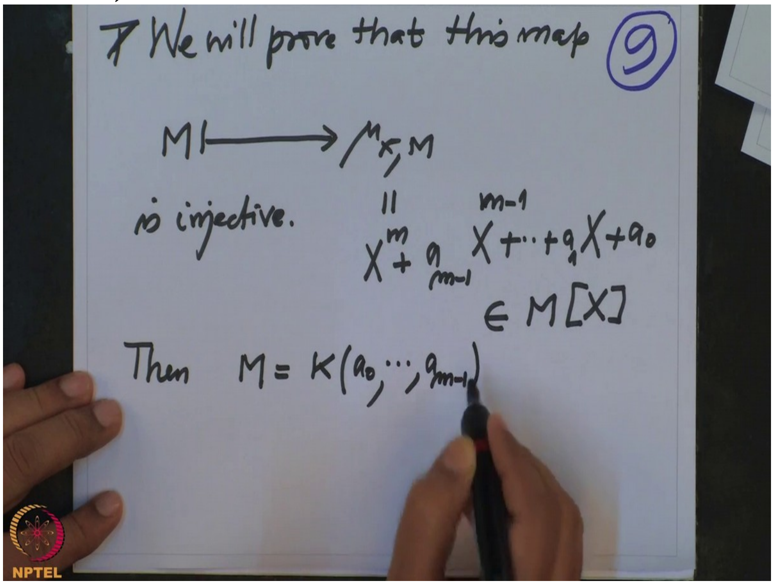
this is the polynomial in $M[X]$.

(Refer Slide Time: 26:42)



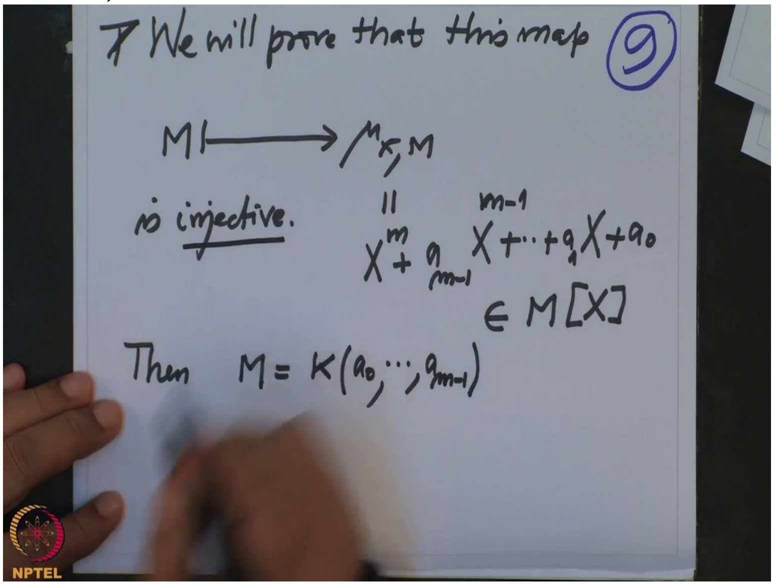
Then I say, then I want to prove M has to be equal to generated over K by these coefficients $a_0, \dots, a_{m-1}$.

(Refer Slide Time: 27:00)



If I prove this then injectivity

(Refer Slide Time: 27:03)

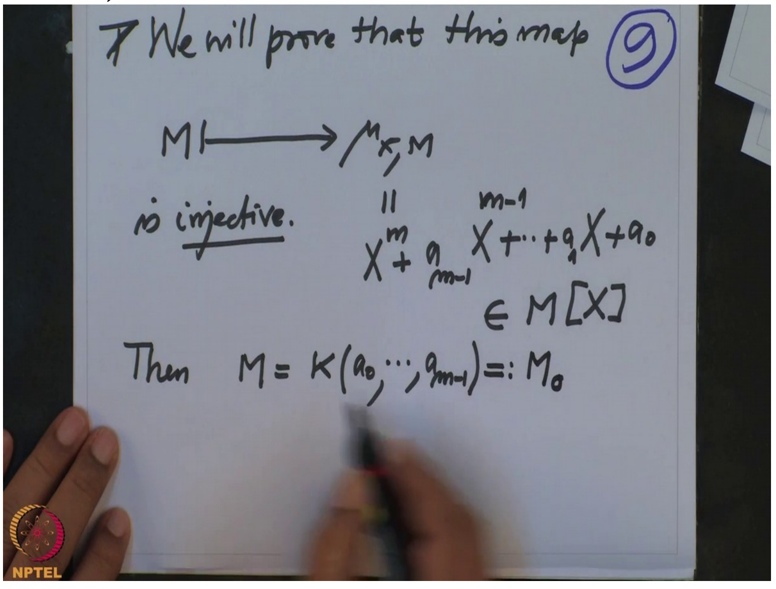


will follow because if I know the polynomial, I can get that my field M.

So I have to prove this equality.

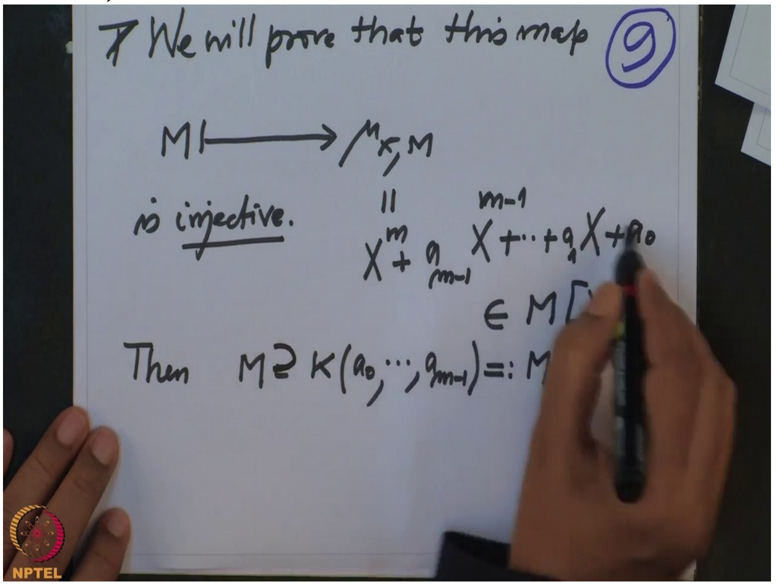
But to prove this equality, let us call this as M_0

(Refer Slide Time: 27:16)



and obviously this is contained here because this polynomial

(Refer Slide Time: 27:19)



has coefficients in M.

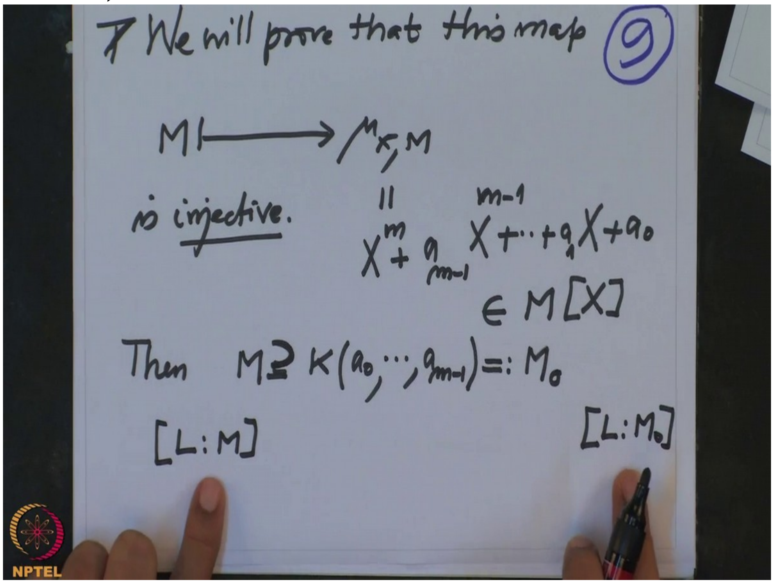
So this is ob/obvious, so this is clear. So I have to prove the other way.

So to prove the other way I just have to compute this, this, this, everything is a subfield of L.

So I want to compute L over M and also I want to compute L over M_0.

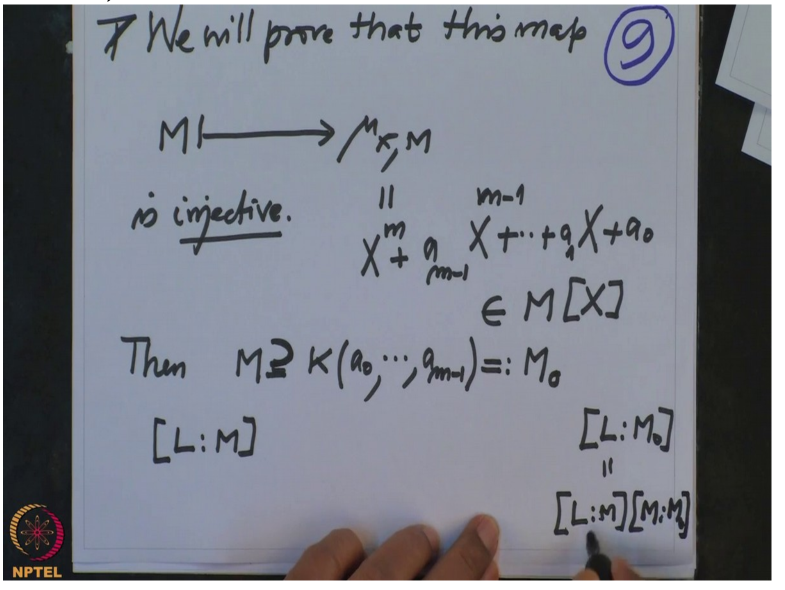
And I want to show they are equal.

(Refer Slide Time: 27:46)



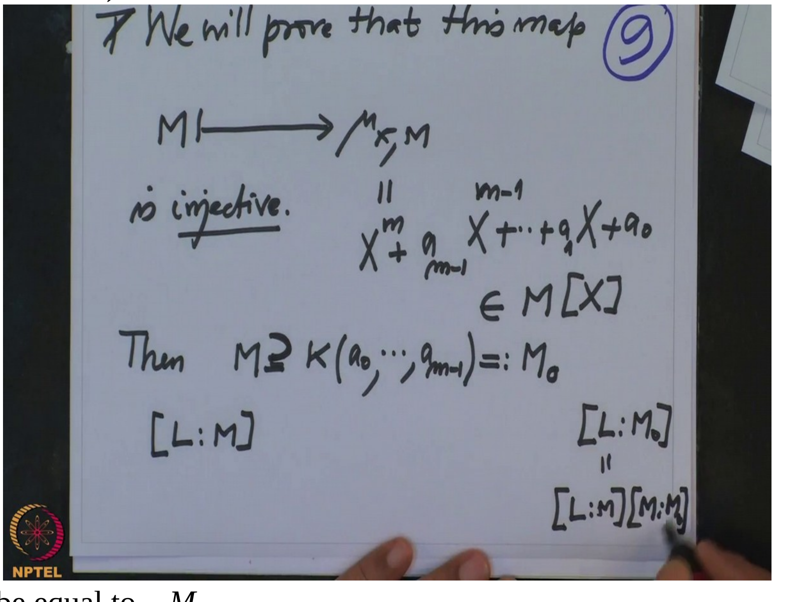
If I show they are equal then M will be equal to M_0 because this is a subfield, therefore this, this equal to L over M over, now times M over M_0, this I know.

(Refer Slide Time: 28:04)



So if I prove that this equal to this, then M over M_0

(Refer Slide Time: 28:08)

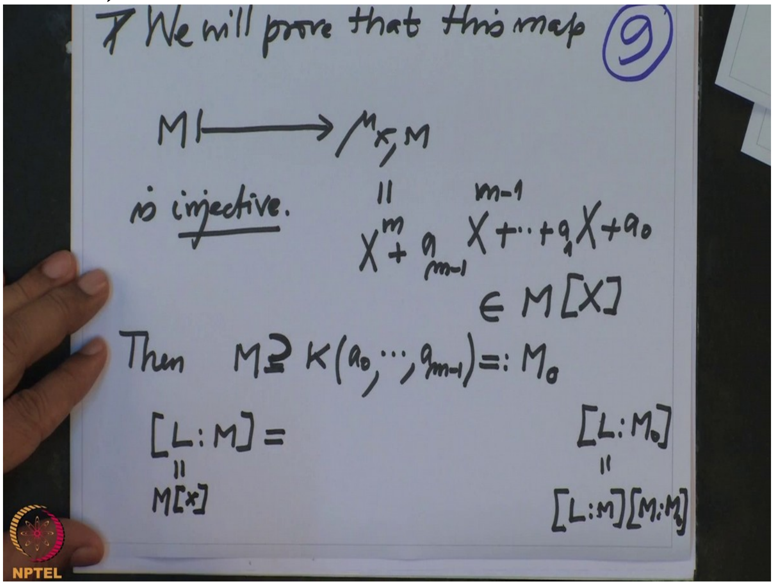


is 1, and M will be equal to M_0 .

So I am aiming to prove these are equal.

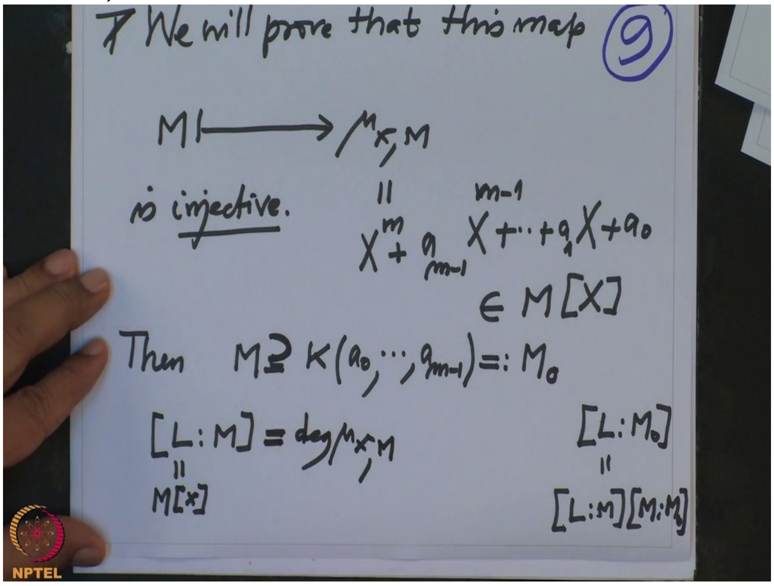
But, Ok what is this? This is L is generated by x over K therefore M is also generated by x over M.

(Refer Slide Time: 28:25)



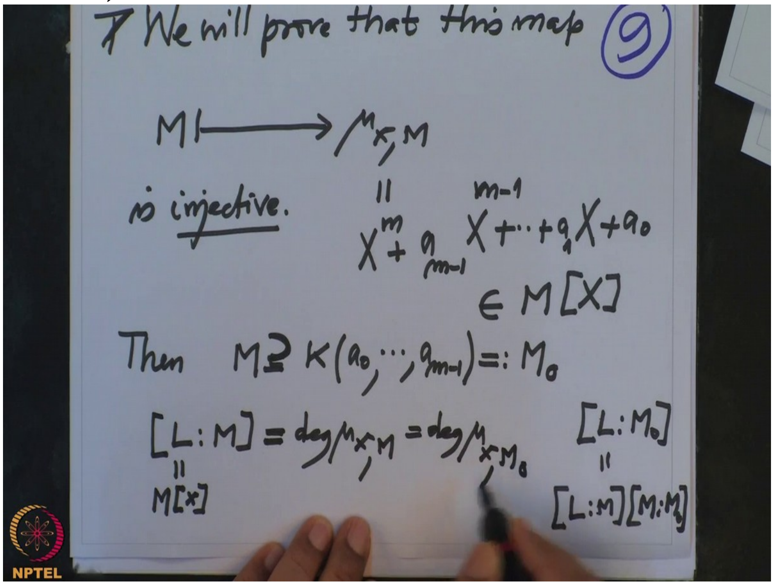
Therefore this equal, degree of this, this is a simple extension over M. So this is the degree of $\mu_{x,M}$.

(Refer Slide Time: 28:38)



But $\mu_{x,M}$, this is same thing as degree of μ_{x,M_0} because

(Refer Slide Time: 28:49)

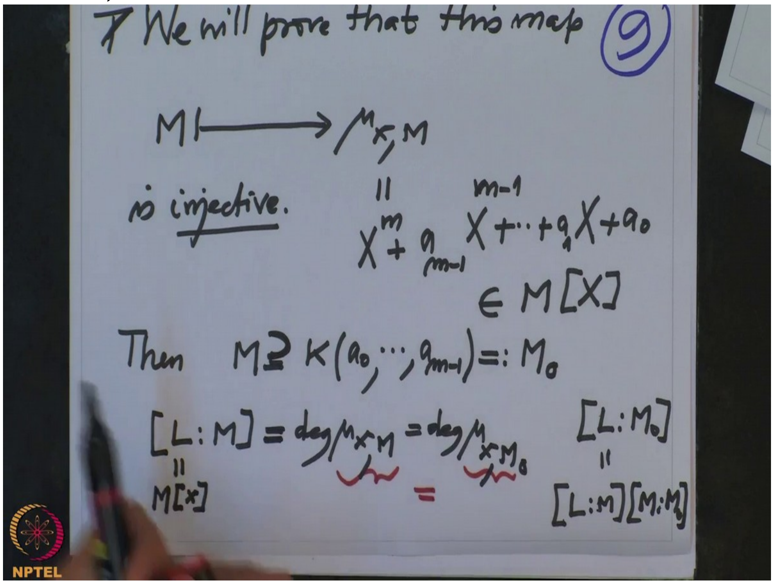


these two polynomials are same, because the coefficients are same.

Therefore these two polynomials are same. These polynomials individually, they are same.

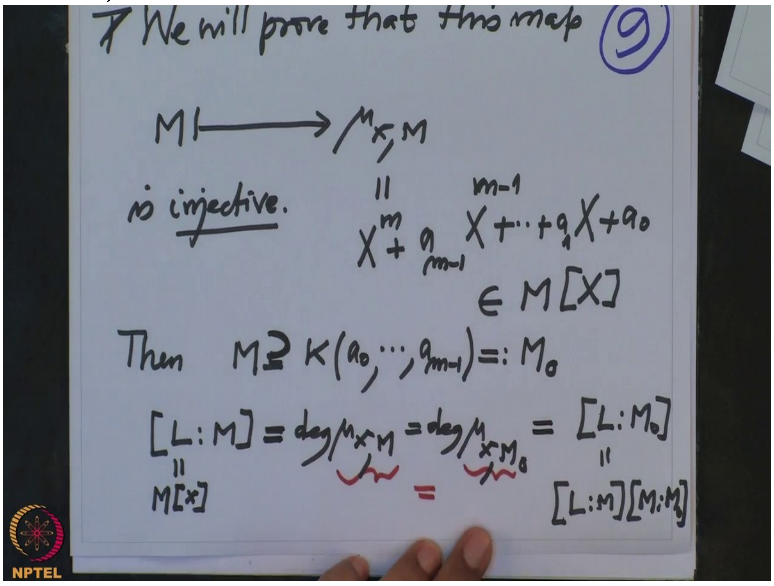
This polynomial and this polynomial are equal therefore their degrees are equal.

(Refer Slide Time: 29:02)



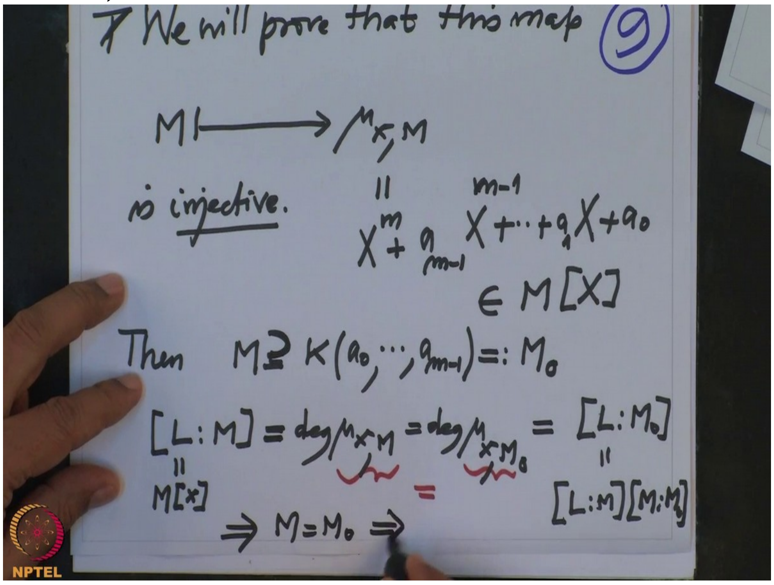
And by the same argument this equality,

(Refer Slide Time: 29:07)



therefore these are equal. Therefore from here you conclude M equal to M_0 and therefore

(Refer Slide Time: 29:15)

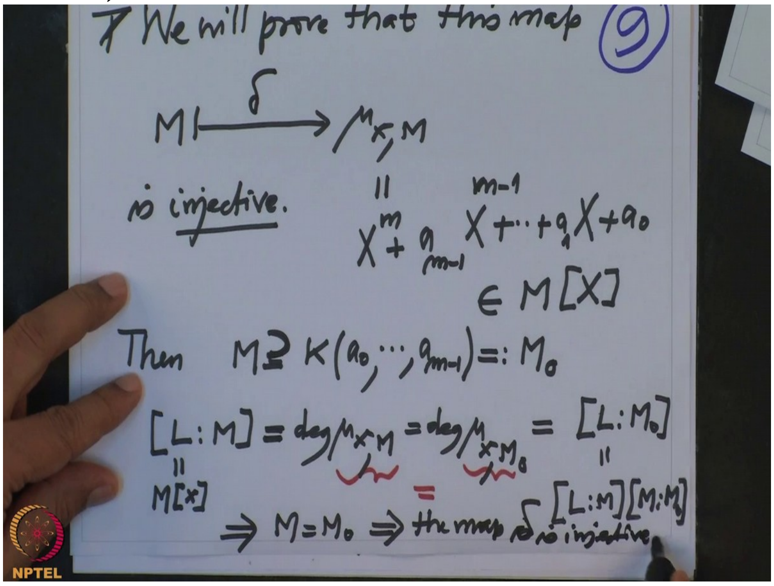


we conclude the map is injective.

The map is injective.

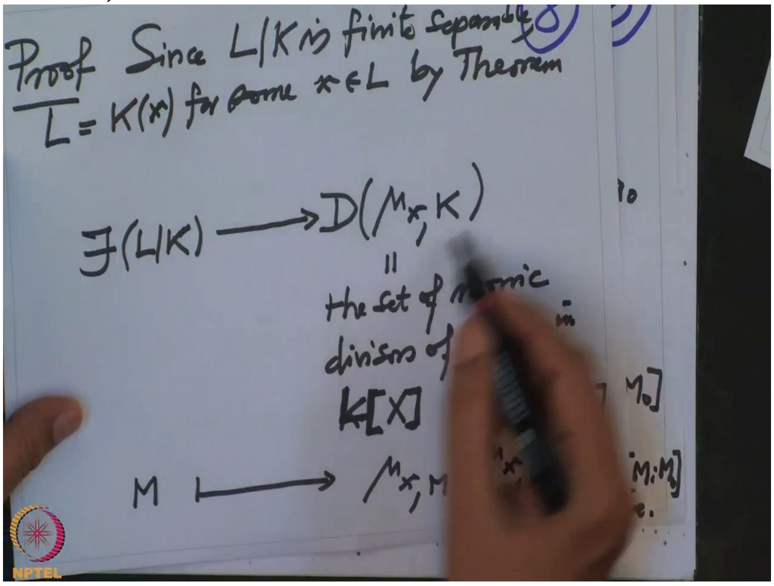
So if you want to give the name δ, the map δ is injective.

(Refer Slide Time: 29:33)



So that proves that, so if you have a injective map from some set to a set where the bigger set is finite, this is a finite set

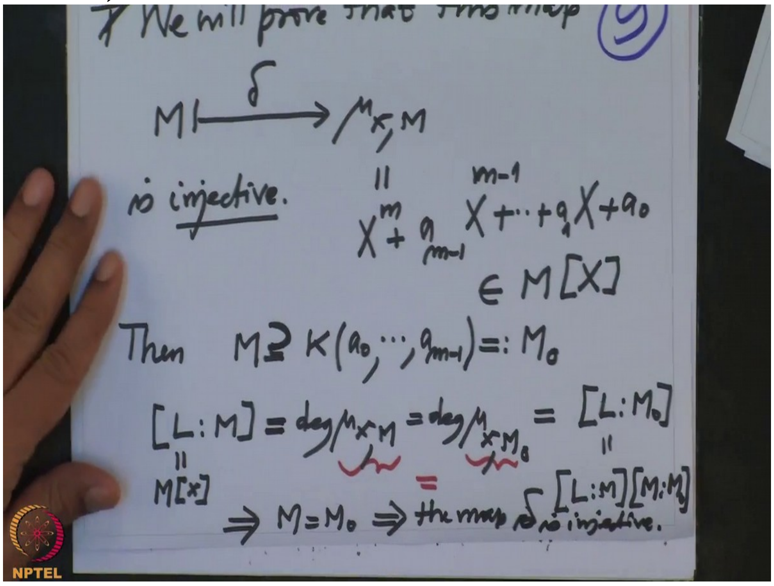
(Refer Slide Time: 29:44)



because this is a monic polynomial of some degree and therefore the number of divisors, monic divisors will be also finitely many.

Therefore

(Refer Slide Time: 29:55)



we finish the proof and next time we will continue therefore the consequences of this very important theorem,

(Refer Slide Time: 30:04)

and we will also use this to compute some examples of some Galois groups. So thank you and we will continue next time.