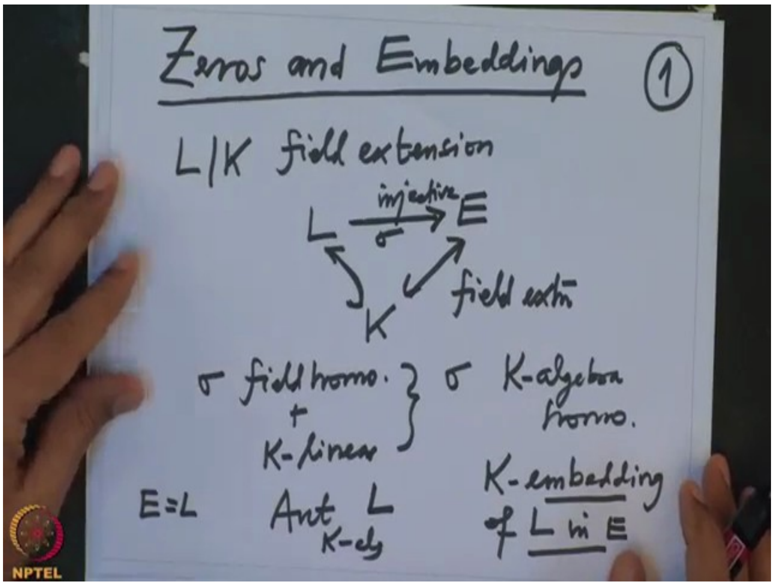
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 49
Zeroes and Embeddings

(Refer Slide Time: 00:52)

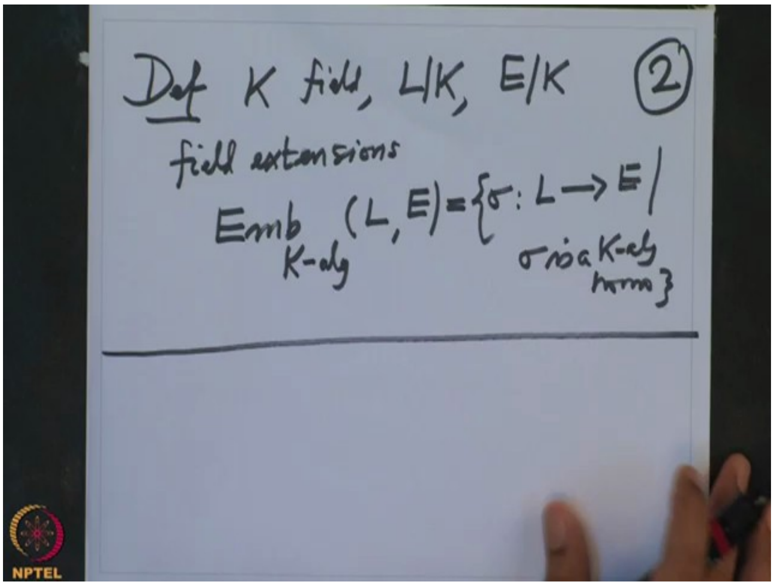


Now I want to begin a new study of field extensions which are so called normal extensions in general, we have seen already normality means splitting of a polynomial so we have to relate these normality property with the set of zeroes of polynomials so I want to study more generally the connection between the zeroes and so called embeddings, so what does this mean?

So let me first explain what is an embedding so suppose I have field extension L over K, field extension so that means we have L is a field and it contains K, this is an extension of K that means there is a inclusion map, now suppose I have another extension E, this is another field extension of, this is also field extension and if there is a field homomorphism here, field homomorphism means it should respect addition, it should respect multiplication and one should go to one, that is a field homomorphism because this L is a field, this will always be injective, this is always injective.

So I will call it, this σ, I will call it K embedding if it commutes with this, it is K-linear, if K is a sub field of E, K is also sub field of L and if this σ is field homomorphism plus K-linear, so remember all this together we have been saying this σ is a K-algebra homomorphism. So such a σ is called K-embedding of L in E, so for example we have been studying if E equal to L when E equal to L, this is precisely what we were considering the Galois group of L.

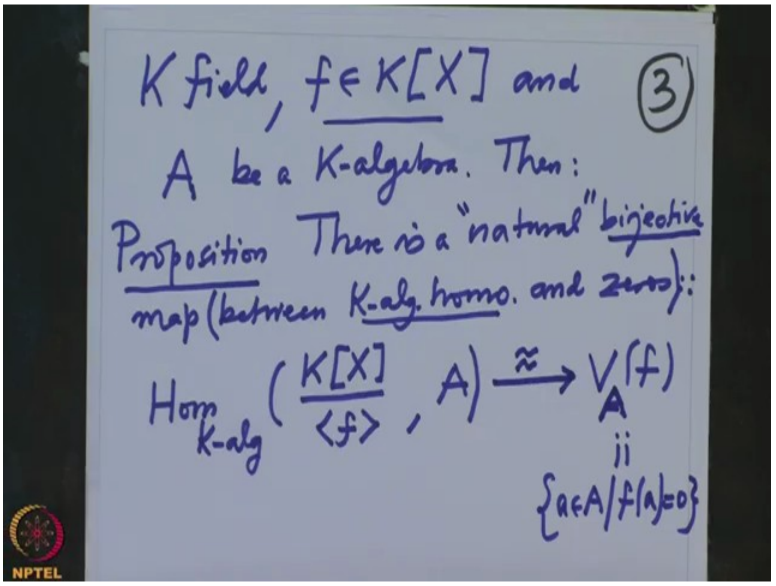
(Refer Slide Time: 03:54)



So now precisely we will put down the definition and then we will indicate its connection with the zeroes of polynomials. Alright in some sense this is more general than the Galois group so our notation, so definition K field and L over K and E over K, two field extensions then Emb, Emb for Embeddings, K as K-embeddings so I will not write KLG here that is, okay let us write K L to E, these are precisely, this is a set of all σ, σ is from L to E such that σ is a K algebra homomorphism.

So we want to study this set and as usual we will study it for finite L over K and decide how many elements this set has exactly like what we studied Galois groups alright so very simple cases I will do it first so this is what we want to study, we want to study this set. So let us do it little bit more general.

(Refer Slide Time: 05:14)

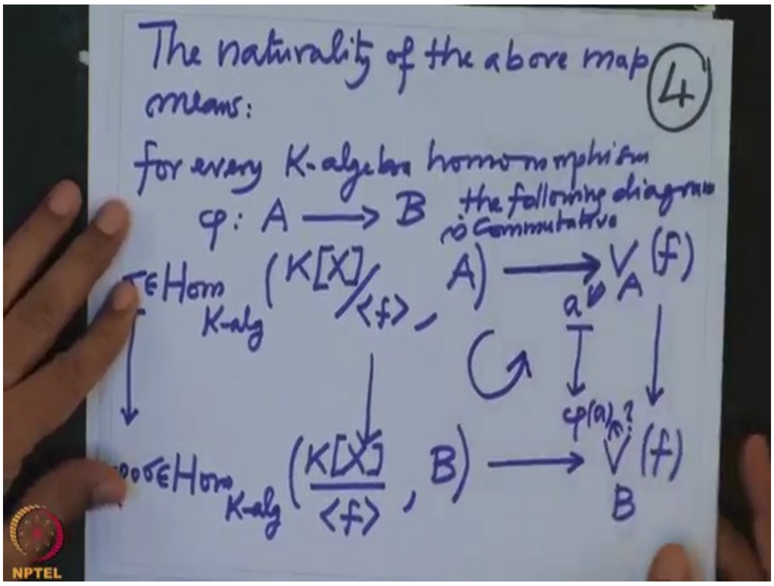


So suppose I have a field K, K is a field and I have a polynomial $f \in K[X]$ and I have A be a K-algebra, remember A need not be a field A is just a K-algebra, A could be polynomial algebra or A could be just K^n or quotient of the polynomial algebra and so on so A is any K-algebra then I want to write a proposition first, proposition, there is a natural bijective map from where between K-algebra homomorphisms and zeroes.

So what is the map? So on one side we have Hom K-algebras from $\frac{K[X]}{\langle f \rangle}$ and A, now before I go on, this is also K algebra, this $K[X]$ is a K-algebra, polynomial algebra and modulo that this is also K-algebra, this is a simple K-algebra, it may not be a field because it may not be irreducible, I have taken arbitrary f so this may not be a field therefore I do not write M, I write Hom, homomorphism from as a K-algebra from this residue algebra to A, this is a set of homomorphisms, this is what I am referring to and to zeroes which zeroes, $V_A(f)$ and what is this by definition?

This is by definition all those elements $a \in A$ such that $f(a)=0$, these are the zeroes of f in A that is why this notation and there is a natural map here which is bijective that is the assertion, bijective and I have to explain in the word natural, this is what we want to prove, this is a first easy observation and as you see this observation is the same trick what I kept saying, this is the one trick which we will keep using in Galois theory again and again that means homomorphism and the zeroes.

(Refer Slide Time: 08:36)



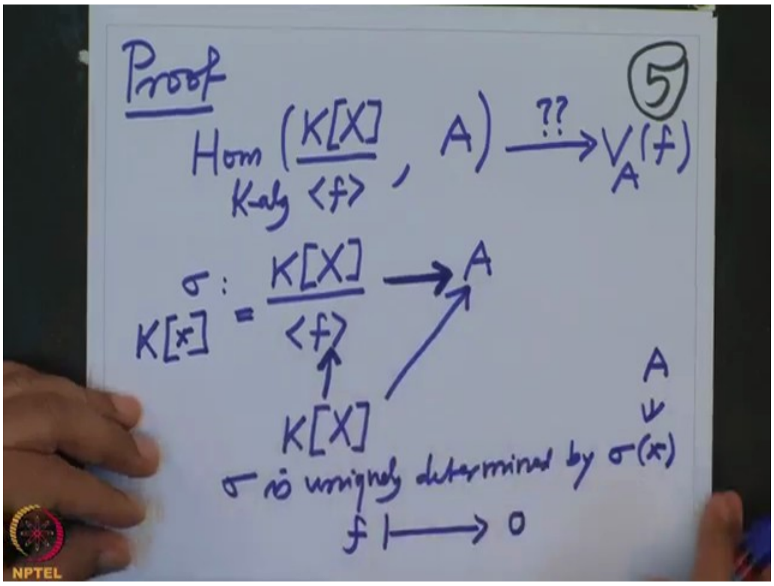
So now I will explain what the natural means okay, the naturality means of the above map means the following, whenever I have for every K-algebra homomorphism phi from A to B, now I have two, I will draw a diagrams so what we were considering was Hom K-algebra to A and $V_A(f)$ and these were the maps we wanted to define and on the other hand this algebra homomorphism is given algebra homomorphism will give us a map in this direction.

Hom K-algebra from the same $\frac{K[X]}{\langle f \rangle}$, B, what is the map, if I homomorphism here any σ whether this map goes this has to use this phi, that means I will take this σ and compose this σ is from this to this and $\frac{K[X]}{\langle f \rangle}$ from A to B, I can go so these I will map it to phi compose σ, this make sense which is an element here.

So this is also it will give me a map from V_B to f, this also I will define and this is the map we are defining so this diagram is commutative, now what should be this? This should be any a, any element a here, I should check that phi of a should belong here, this is what we need to check, so that this diagram is commutative right, so therefore this map in some sense it is very natural in this A, these are values in A, these are the zeroes in A, these are zeroes in B.

So naturality means for every K-algebra homomorphism phi the following diagram is commutative, this is a diagram of sets and maps and one says it is commutative when you know there is only one point here where you can go from here there is one way, other way is this, so this diagram should be commutative so usually it is denoted like that, this symbol is used, that means whether you go this way or that way it is same.

(Refer Slide Time: 12:20)

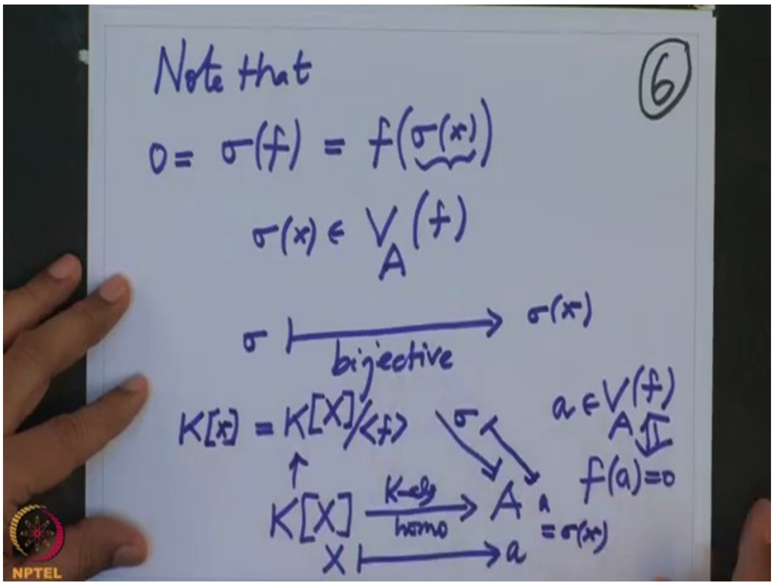


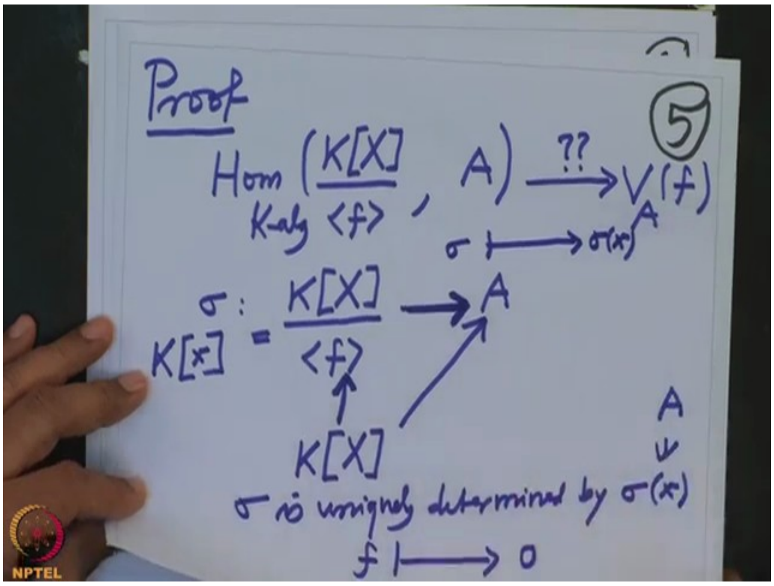
Now this is so easy you will see we have spent more time in the statement so proof is so clear okay so proof, so we want to give a map from Hom K algebra $\frac{K[X]}{\langle f\rangle}$ to that A, to A given this I want to get 0 out of this, so this I want to give a map, this to $V_A(f)$, I want to define a map here, so what do I have to do, that means suppose I have given σ, σ is K-algebra homomorphism from $\frac{K[X]}{\langle f\rangle}$ to A, this is given to us and I want to associate a 0 of that okay.

When this is given to us that means we have given from $K[X]$ there is a natural map here, this is natural surjective map that means I have given this and what is, this map is σ is given to us and I want to get 0 of that so that means what, so first of all note that this map is uniquely determined if I know values on X.

Therefore this map will be uniquely determined when I know it is value on if I denote the residue of capital X mod this f small x then it is enough, this σ is uniquely determined by σ of x. This σ of x is an element in A and this when should be this well-defined only when f should go to 0 there in A but where do f go that we will write on very precisely where do f go, once I know where x go, it is clear where f will go.

(Refer Slide Time: 14:43)





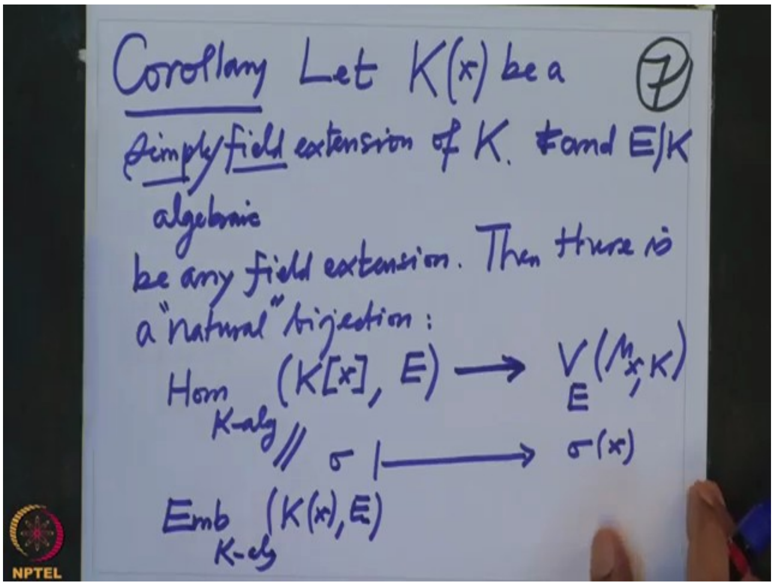
So note that f of, if I apply σ to f, what do I get this is the trick I am saying, this σ is a K-algebra homomorphism and f is a polynomial so that means this will be f of σ of x and this is 0 we know because the map is f should map to 0, so therefore this is given to us, that means what?

That means this σ X, this means σ X indeed belong to the 0 of f in A because this is an element in A therefore we have a natural map, this σ which maps to σ of X, this makes sense and that is a map this is so natural and I want to check that this is bijective, alright but that bijectivity is clear because it is uniquely determined by X, the value of X, see we have defined a map from here to here, this map is σ going to σ of X and this σ is uniquely determined by this, therefore this map is clearly injective and it is clearly surjective also, so this map is bijective.

Because if a were a 0, so injectivity is obviously clear because σ is uniquely determined by this that means the map is injective, to prove surjectivity if a is a an element in 0 element in this I could define a map from $K[X]$ first to A, this map is I have to give only for X, where does X go, X goes to a because this a is a 0 of f so that is f of a is 0 then this map, this K-algebra homomorphism obviously it will factor through $\frac{K[X]}{\langle f \rangle}$ to this, this is my σ there and this small x here will go to that given a, σ is going to a and a is $\sigma(x)$.

I am not saying this map is injective but whenever somebody is in the kernel you can go mod and you have a well-defined map from here to here and that gives you a surjectivity of this map, so this map is bijective, so therefore all together we have proved our statement, so it is one which relates the zeroes with K-algebra homomorphisms.

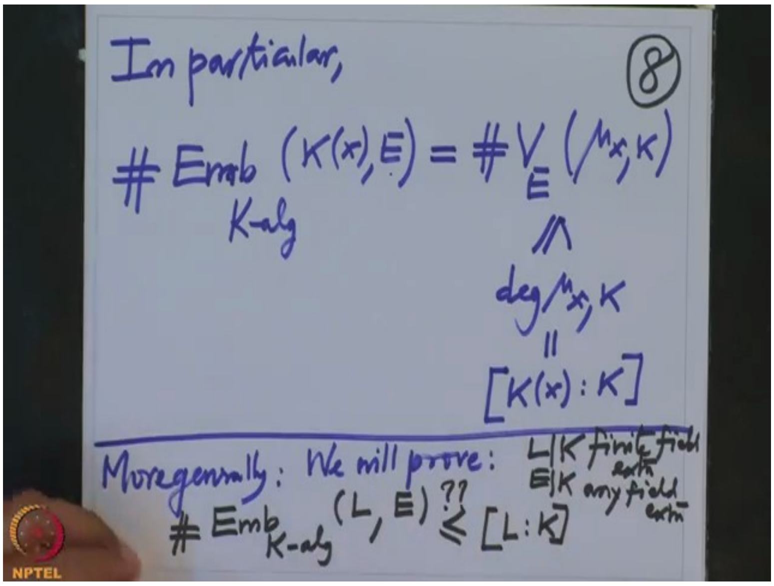
(Refer Slide Time: 18:02)



Now okay so some corollaries I want to write down from here, so corollary okay let $K[x]$ be a simple field extension of K and a simple algebraic I wanted to say, algebraic field extension of K then and E over K be any field extension then there is a natural bijection from where to where, that is Hom K-algebra $K[x]$, because it is algebraic whether I write square bracket or round bracket it is same and the values are in E to zero set of minimal polynomial of X over K in E this map there is a bijection and what is the bijection?

Take any σ and map it to $\sigma(x)$, this was the trick we were using it earlier also, it is a natural bijection and I have applied to the special case where a equal to the field actually E and now in this case this is also field because I am taking a simple field extension so therefore instead of writing this I will write Emb K-algebra $K[x]$ E, so this simple field extension embedded in this, how many are ways so that is this σ, so that to the 0 set of this and now in particular I will write down this obviously follows from the above very clearly.

(Refer Slide Time: 20:45)

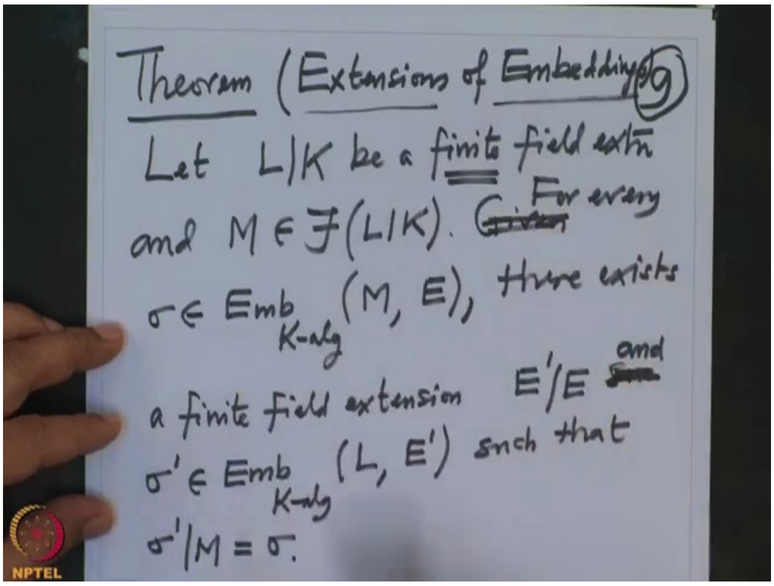


In particular if you have a bijection cardinalities are same, so cardinality of the number of embeddings, K-algebra embeddings from the simple extension $K[x]$ to E, this number is same as the number of zeroes of the minimal polynomial of x over K in E but this zeroes is definitely less equal to the degree of the minimal polynomial and this minimal polynomial degree is precisely the degree of the field extension $K[x]$ over K.

So you see the answer is very nice, so this bound you see here, this bound is not depending on this E, there is no E on this side that is in between so the number of embeddings from one field to the other field we would like to say that it is bounded by somebody like we said in case of a finite extension the cardinality of the Galois group is bounded by the degree of the field extension.

So therefore I would like to prove more generally I would prove so this was part of the corollary, more generally we will prove the following statement not now but later maybe couple of lectures above, so number of embeddings, K-embeddings of L to E where L over K is finite extension, if L over K finite field extension and E over K any extension, any field extension then I want to prove this number of embedding this is bounded by the dimension of L over K, this is what I want to prove later and what we have proved it today is for the simple extension, for simple extension we know this.

(Refer Slide Time: 23:31)

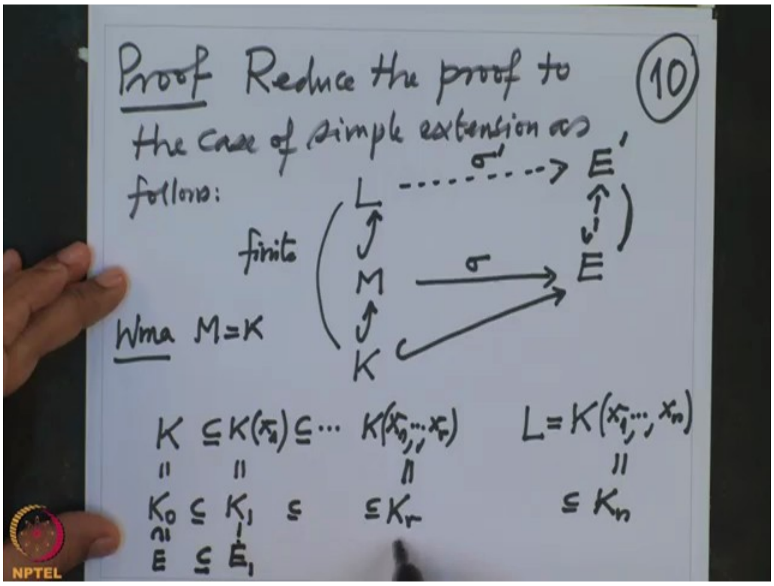


The theorem I want to state to which will support this claim, prepare this inequality, so theorem I want to state is the following that is this is extensions of embeddings, so the situation is the following, let L over K be a finite field extension, finite is I am assuming and later on we can also draw finite and replace it by algebraic but that I do not want to do it now because essentially this course we are dealing with finite field extensions.

But then when you want to drop this you will have to do better cardinal arithmetic alright and M be a intermediary field extension that is M is a field in between okay and we have given an element σ belonging to the embedding, K-algebra embedding of M to E and I would like to extend it to L to E and how many waves, so that is what I want to analyze the problem, so given this.

So given σ this there exist or let me write it, for every embedding σ there exists a finite field extension E' over E such that okay and finite field extension E' over E and σ' belonging to embedding of, K-algebra embedding of L to E' such that if I restrict this σ' to M, I get back that σ, statement is very easy, we will prove it immediately alright, so before I go on to the proof, remember the title Extensions of Embedding, so this σ is given to me embedding and I want to extend it to a bigger field L that is why extensions of embedding, this is very easy okay.

(Refer Slide Time: 26:46)



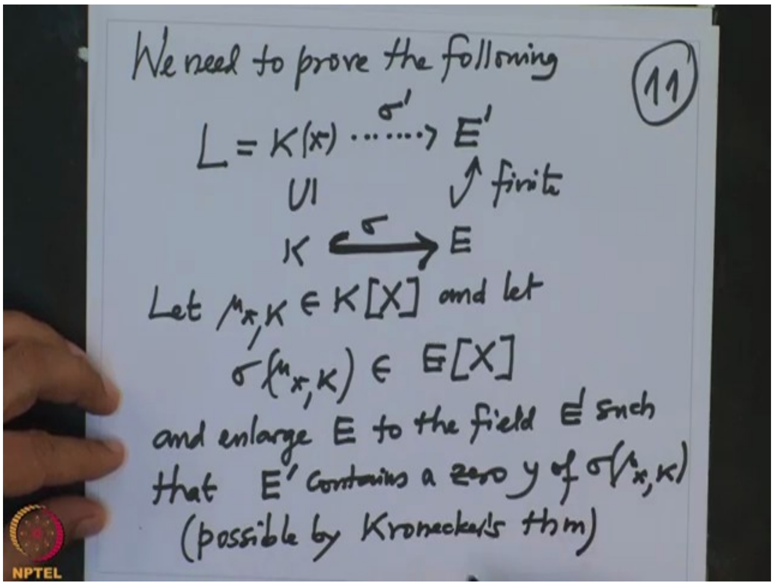
So proof, so reduction to the I will reduce the proof to the simple extension, reduce the proof to the case of simple extension as follows, alright so what to do, we have given L over K, L over K is given, let me draw a diagram so L over K is given to us and M is here in between and there is a map from M to E and this is K linear, this is given to a σ, this is contained here, this is contained here and this diagram is commuted to that is precisely the meaning that σ is K linear.

Alright and this is our extension here and we are looking for $E^{'}$ so that this is contained here so I will draw that dotted, we are looking for this and we are looking for this extension $\sigma^{'}$, this is what the problem is, we want to find $E^{'}$ which is also should be finite extension such that this we should be able to extend it here, alright so we know that this is finite given to us.

So we can do like this, so K is here, L is here and L is generated by finitely many elements over $K\left[x_1,\ldots,x_n\right]$ and there is a chain here, this is contained in $K\left[x_1\right]$, etc. etc. this is, so if you call this as K_0, this is K_1, this is K_n and in between they will be generated suppose it is generated by $x_1,\ldots,x_r$, this is K_r, this is what we have given and I want to slowly so without loss first of all I can assume M equal to K because I will replace M by K.

So first of all we may assume M equal to K because this part is not doing anything there, all these are extension so in M equal to K case I have this chain and I am going to find here for this step I have to find E is given to us, E is an extension of this K, I will find $E^{'}$ which is a finite extension and then lift this map here and keep doing it. So therefore with this we only have to prove the following.

(Refer Slide Time: 30:11)

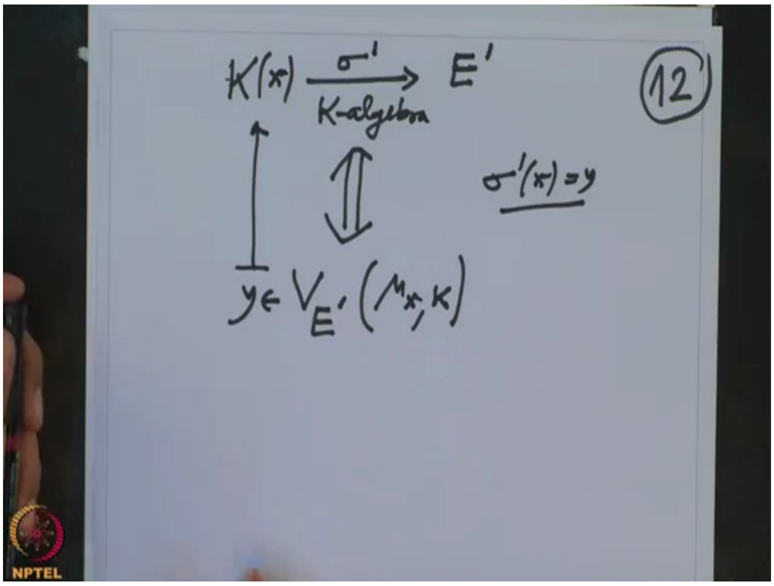


We have to prove that, so we need to prove the following, so L is my simple extension over K and I had a finite, I had another extension, this is field extension and I had that, not the infusion map but I had the embedding, this is my σ and here I want to find $E^{'}$ such that this is finite extension and I want to extend this σ to this $\sigma^{'}$ that is the problem.

Alright so what do we do, so take let, so this extension is uniquely determined by that μ_x, $\mu_{x,K}$, this is the minimal polynomial of x over K which is a polynomial with co-efficients in K and let, so therefore this polynomial also has without loss I can assume this is injective so therefore think of look at the image of μ under this map so $\mu_{x,K}$ this is a polynomial in $K[X]$ and apply σ to this, this is a polynomial in $E[X]$, this is simply, what you do is you take the co-efficient of the minimal polynomial and apply σ to them.

So this is a polynomial here and therefore I can enlarge this field E to field $E^{'}$ such that so let and enlarge E to the field $E^{'}$ such that $E^{'}$ contains zero y of this$\sigma(\mu_{x,K})$, this such a field exist and in fact we can choose a finite field extension I do not need all the zeroes, I only want 1 zero to be contained in $E^{'}$ such a thing is possible by Kroneckers Theorem.

(Refer Slide Time: 33:10)



Once I have that then we are done because how do I extend, how do I give the homomorphism from E to $E^{'}$ to give such a $\sigma^{'}$, K-algebra homomorphism in the beginning lemma only we saw that this is equivalent to giving $a_0 V^{'}$ of the minimal polynomial of x but that is what we have chosen y here, so this y will correspond to $\sigma^{'}$ and this $\sigma^{'}$ will map x to y.

So this $\sigma^{'}$ maps x to y, so therefore there exists $\sigma^{'}$ and therefore our problem is solved therefore that shows that given any embedding I can always extend to the bigger fields and I want to use that again and again so this will also, this is also related to what is called the extensions are normal extensions, so this is what I will study in the next onward, next time I will study precisely what are normal field extensions and use this prerequisite to that normal extension, so with this I will stop and we will continue next time, thank you.