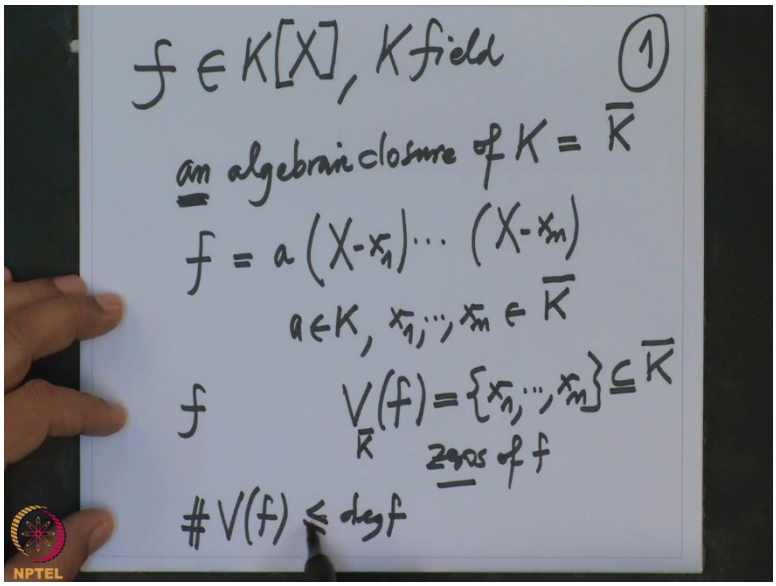
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture 54
Galois group of a polynomial

Alright, so like I was saying in the last lecture that we want to study polynomials, their zeros and also the groups together, so let us start with the polynomial f.

(Refer Slide Time: 0:47)

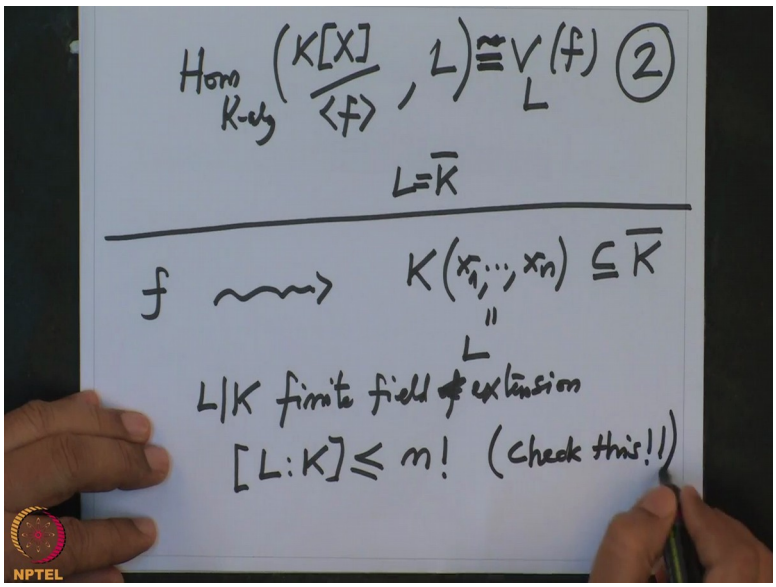


F is a polynomial with coefficients in field K, K is a field. And then we know now that every field has an algebraic closure so usually an algebraic closure of K this is denoted by $\overline{K}$ and we fix it, we fix that for like in one of the last lectures I commented that if you want to study this we will fix this. It is unique up to K algebra isomorphism but it may be different means it is not equal so therefore we fix that one and therefore in that field every polynomial with coefficients in K will split into linear factors.

So therefore f we will split, f may be some constant $(X-x_1)...(X-x_n)$ splits into linear factor where a is actually in the base K and x_1 to x_n these are the zeros of f, all zeros of f in $\overline{K}$, all of them lie in $\overline{K}$ and these are all maybe some of them are repeated etc, etc, but to this f we are therefore f we are writing this notation $V(f)$ we have been writing this, but this is all x_1 to x_n and this is a set of $\overline{K}$ and these are called as zeros of f without saying where, it is understood that it is taken in $\overline{K}$. So here also I could have written $\overline{K}$ but when I do not write that means it is assumed that it is in $\overline{K}$, in earlier lectures also that was the strategy.

And we know therefore the fundamental theorem of algebra says that this number this cardinality of $V(f)$ this is bounded by the degree and this is crude. So if you take them distinct and compute according to the multiplicity then also it will be exactly equal but I do not need it right now so we have the zeros and we want to study the zeros.

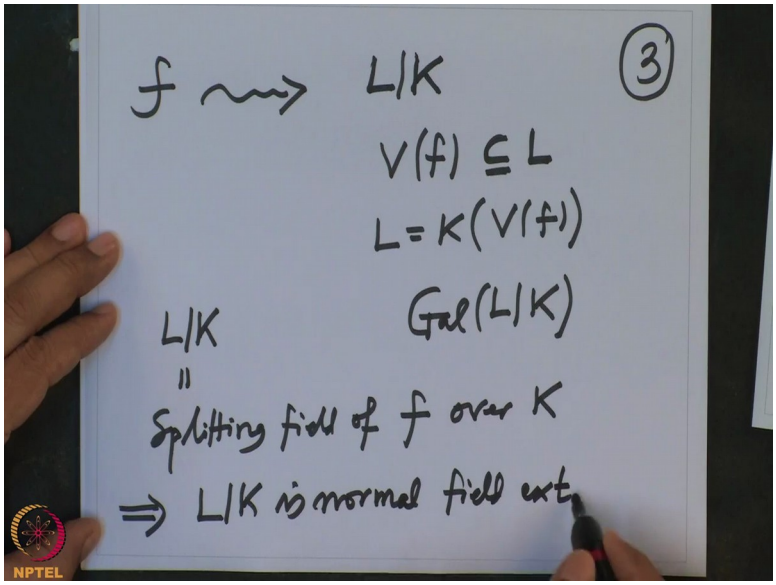
(Refer Slide Time: 4:03)



So note that the zeros we have seen in one of the earlier lectures that the zeros are embedding so if I want to embed so Hom K algebras of $\frac{K[X]}{\langle f \rangle}$ in some field L field extension L, these are precisely the zeros of f in L, this was seen these 2 sets are bijective, there is a bijection between these. So if I would have taken L = $\overline{K}$, I will take here all zeros so alright so this is it. Now to this as we are adjoining therefore we are associating a field of $\overline{K}$ that is generated over K by the zeros of f so this is X 1 to X n, this is a subfield here.

And not only that, this is a finite extension of K, if you call this as L, L over K is finite field extension, the degree also we know L over K degree is smaller equal to n factorial. This is also clear, this you do it by induction so I would simply say here check this. So we have got a finite field extension of degree S = $n!$.

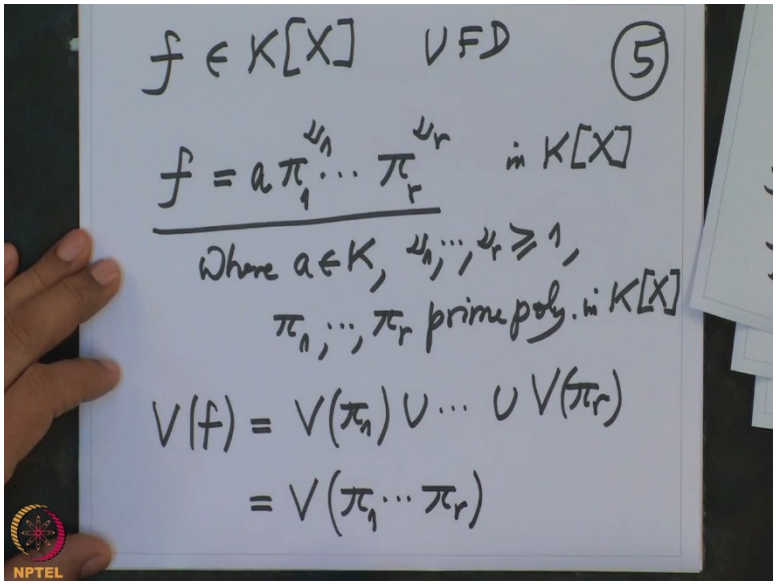
(Refer Slide Time: 5:50)



So therefore to this f we have attached the field extension L over K, where all the zeros of f they are contained in L, all zeros. In fact, L is generated by over K and generated by $V(f)$ is the smallest subfield of the algebraic closure which contains all the zeros so therefore we have Galois group $Gal(L|K)$. And also we know that this L over K this is a splitting field, this is a splitting field of the polynomial f over K therefore, L over K is normal field extension. What is the definition of normal?

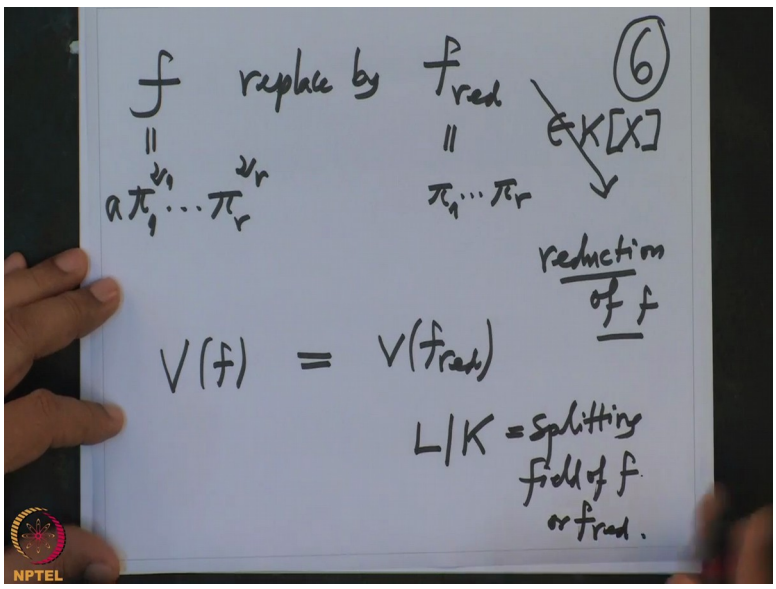
Let me recall it quickly, so we will say that field extension L over K is normal if I take any embedding K embedding if every K embedding from L to where… an algebraically closed field but that is I am taking $\overline{K}$ now… $\overline{K}$, every embedding maps L inside maps L into L so that is $\sigma(L)$ is containing it that is a normality definition alright that isthe field extension is normal we know. I also want to say that we can also assume it is we can to do this whatever we have done we started with any polynomial $f \in K[X]$ I wanted to claim that we may assume that f is a separable polynomial.

(Refer Slide Time: 8:51)



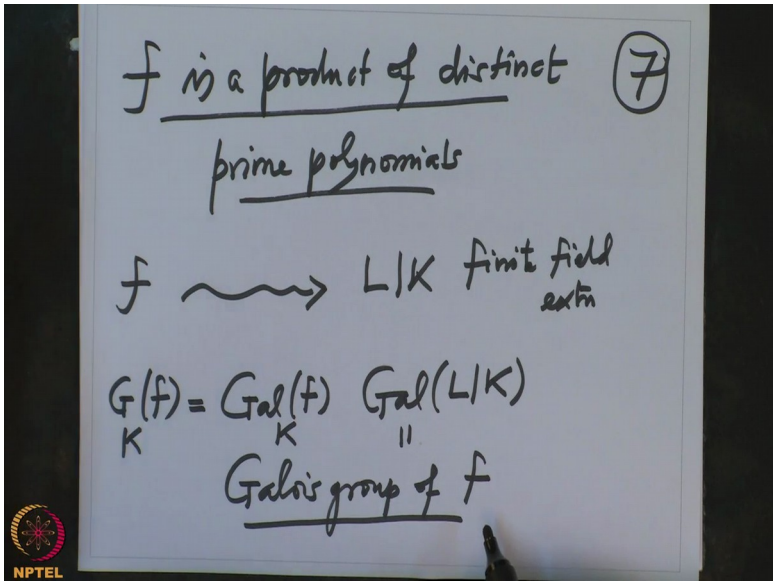
What is a separable polynomial? It does not have repeated zeros, zeros are distinct but you see that I can achieve by so we have f, f was arbitrary polynomial in $K[X]$ and this f therefore because we know every this polynomial ring over a field is a UFD so therefore this F definitely I will factor the prime factorisation of f in $K[X]$ will look like this, some constant $\pi_1^{\mu_1} \ldots \pi_r^{\mu_r}$, where this a is actually constant in K, $\mu_1, \ldots, \mu_r$ are nonzero natural numbers and $\pi_1, \ldots, \pi_r$ are prime polynomials in $K[X]$ that is the prime decomposition of f in $K[X]$. And as far as the zeros study of zeros, $V(f)$ is same thing as $V(\pi_1) \cup \ldots \cup V(\pi_r)$, and this is same thing as $V(\pi_1 \ldots \pi_r)$.

(Refer Slide Time: 10:13)



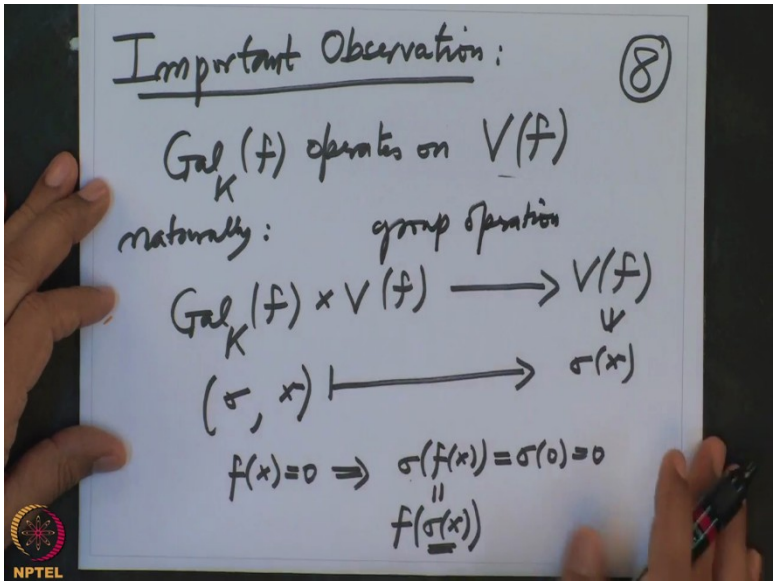
So, I could have simply replace f, this was f replace by f_{red} , reduction of f it is called induction of f, this is simply $\pi_1 \ldots \pi_r$ product, this is called reduction of f, this is also a polynomial in $K[X]$ only, so our 0 set did not change and then now with the splitting, field will also not change because of all the zeros so L over K is the same, this is a splitting field splitting field of f or f_{red} the same alright.

(Refer Slide Time: 12:00)



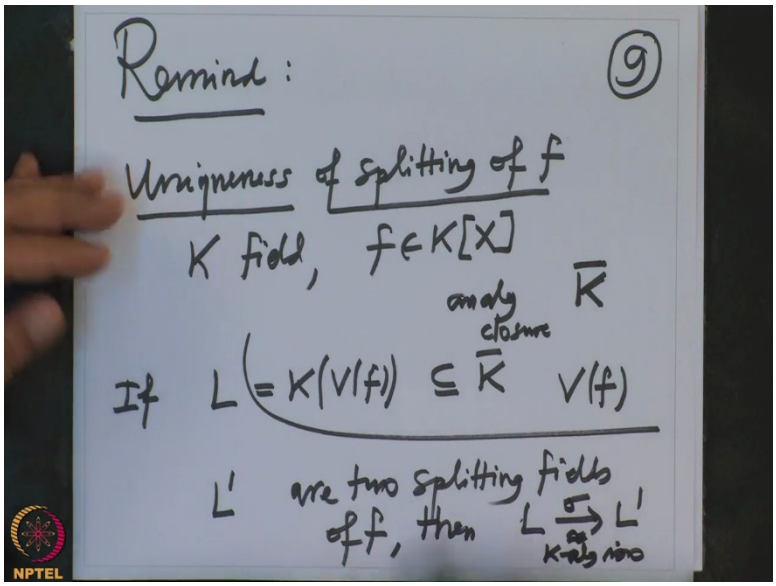
So we can assume always in the study we will always assume the polynomial is separable or polynomial at least separable I have not done very formerly yet but we may assume that f is a product of distinct prime polynomials that is what we will assume. So going back to f I have attached a finite field extension L over K, finite field extension and we have the Galois group, this Galois group I want to call it a Galois group of f and I will therefore denote by $Gal_K(f)$ or sometimes I will simply right $G(f)$ and to study the zeros of f. I will study this Galois group. So for example, I will write down what are the orbits, I will say what are the stabilisers and so on so that group action alright.

(Refer Slide Time: 13:09)



And also we know that the most important observation we have used so many times, important observation this we have used sometimes. $Gal_K(f)$ operates on Zero set of f naturally, so what is the operation? This is my set where this group is operating so $Gal_K(f) \times V(f) \to V(f)$, what is the map? Take any σ and take any Zero of f and map it to σ also, so this is a 0 means f of x is 0 and we are applying to this σ , σ is very isomorphism so σ of 0 is 0. And also it is collinear and it respects the multiplication therefore this is nothing but f of $\sigma(x)$ that means σ indeed belongs here. And it is clear that if σ is identity, this is X only and if I have σ and τ and so it is a group operation, this is a group operation.

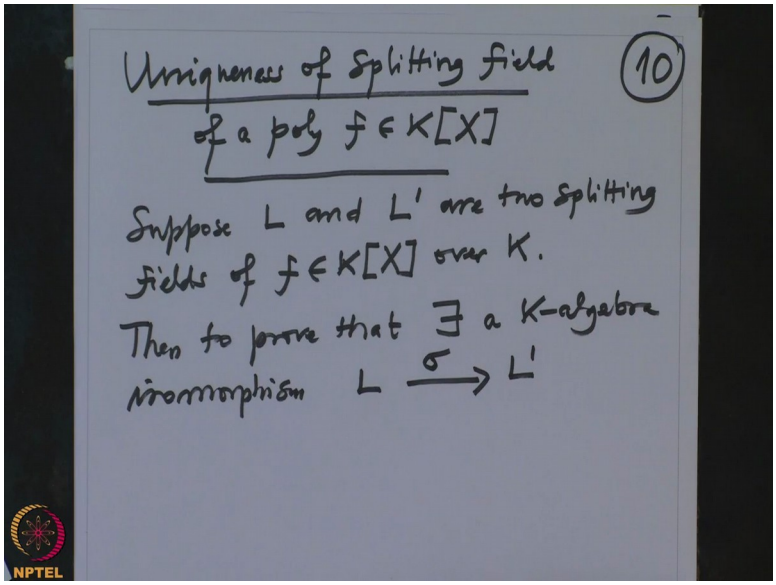
(Refer Slide Time: 14:56)



Okay so our aim will be to study this group action more and more intuitively. Okay before this we will do it in coming lectures but I want to remind you that we need to prove something about spitting field which I have not formally proved it so what if what if that thing I want to prove that if I have… So we need to prove the uniqueness of splitting field and what should uniqueness means? Uniqueness of splitting field of polynomial f. So what is that? Why is it necessary to prove? Remember what we have done, we have a field K and a polynomial $f \in K[X]$ and we have chosen we have fixed an algebraic closure, $\overline{K}$ is an algebraic closure of K.

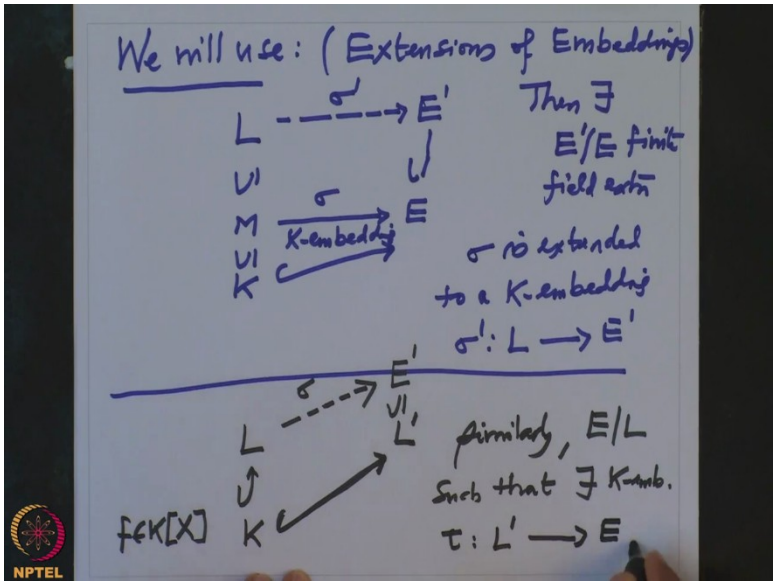
And now we have chosen we look at the 0 set her, $V(f)$ is here and the splitting field is L, L is K of $V(f)$. But see this is the finite extension of K and it is a subfield of $\overline{K}$ so somebody changes $\overline{K}$, somebody picks up another model for the algebraic closure then one will come across some other L'. So if L and L' with this preamble if L and L' are two splitting fields of f then we should prove that they are isomorphic over K then L and L' there is a K algebra isomorphism , this is needed to proof. Okay let me indicate the proof of this, already we have proved it but I only have to tie the things.

(Refer Slide Time: 17:19)



So prove uniqueness of splitting field of a polynomial $f \in K[X]$, so that means we want to prove that if I have so suppose L and L' are two splitting fields of a polynomial $f \in K[X]$ over K then we want to prove that there exists a K algebra isomorphism from L to L' σ, this is what we want to prove, alright. But for this we are going to use so we will use what we did about so we will use the following observation.

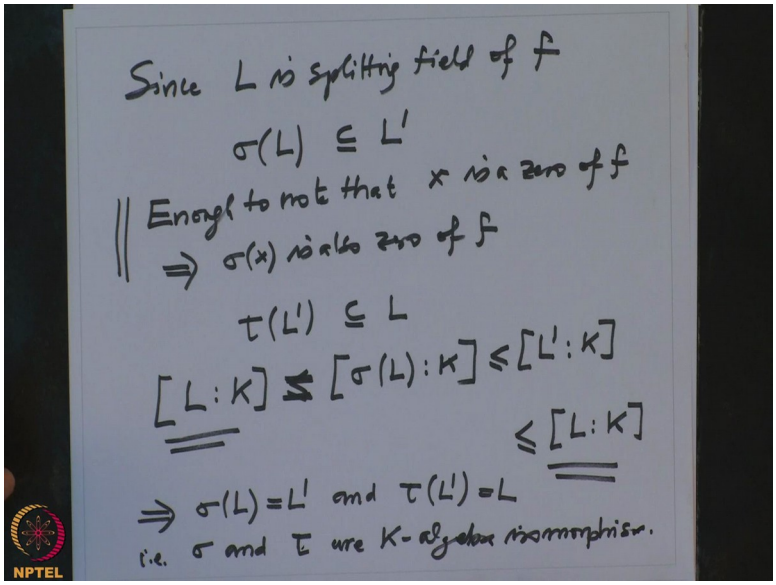
(Refer Slide Time: 18:56)



This is from extensions of embedding so what I want to use is the following assertion. So whenever I have an intermediary feel of the finite field extension L over K and suppose I have a K embedding of L in an extension E of K, this is K embedding then there exists finite field extension E' over E, finite field extension so E' over E you can find this finite extension and then this σ I can extend it to this σ'. So σ is extended to a K embedding σ' from L to E', this is what I want to use in the proof.

So how it is used? So we have L here and we have, this is a splitting field L of this is a splitting field of a polynomial f in $K[X]$ okay and L' is another splitting field of the same polynomial. Now we take this this natural inclusion map as an embedding and now this is, so this says that this embedding I can enlarge this field L' to E', this is a finite extension so that this natural inclusion map is extended here so that I want to call it σ. And similarly interchanging the rules of L and L' we have an embedding so similarly we have τ so similarly we have a finite extension E over L such that there is a K embedding τ from L' to E.

(Refer Slide Time: 22:15)



Now note that because this L is a splitting field, this image of so since L is a splitting field of f, $\sigma(L)$ is actually contained in L' that is because all that we have to check that E is for this. It is enough to note that if X is a zero of f then $\sigma(x)$ x is also 0 of f and similarly τ of L' is contained in L same observation. This observation is so very important, we have used it several times in the course, namely if x is a 0 of a polynomial then and if σ is embedding then $\sigma(x)$ is also zero of the same polynomial f.

So all this together shows that if I take L over K this degree, this degree is smaller equal to, this degree is same as σ L over K but this is smaller equal to L' over K because Sigma L is contained in L' and by the same argument this L' over K is smaller equal to L over K, this means interchanging the rules of L and L' . So because of this, this and this are equal and therefore all are equal so that shows that so that shows that Sigma L is actually L' and similarly τ of L' is actually L. So in other words, the σ and τ so that is σ and τ are K algebra isomorphism. So that proves that L and L' in particular they are isomorphic over K. So we have proved that any 2 splitting fields are isomorphic.

Note that this σ and τ are Isomorphisms but they may not be inverses of each other because there is no connection between σ and τ because σ and τ are obtained by extending the natural inclusion and that may not be compatible with each other so therefore we cannot say that σ and τ are inverses of each other but definitely σ and τ are isomorphism that is what we wanted to prove.

If we have a splitting field of a polynomial single polynomial, it is a finite extension and this finite extension is uniquely determine up to K isomorphism therefore, the group we have attached to that is isomorphic so therefore when we fix algebraic closure there is no ambiguity because the algebraic closure are not equal in general but they are isomorphic. For this reason I had to make this remark and this I should have made it that time only that when we studied zeros and embedding of field.

Okay so with this now from next time onwards we will concentrate more on studying the Galois group of a given polynomial and given polynomial will give you field extension and in order to achieve better results we will have to assume the polynomial is separable. Right now we only are assuming that the polynomial is the product of distinct prime factors. So but now it might happen that the prime factors may be separable or not that we have to analyse, for this reason next time I will define what is a separable field extension and then we will analyse when irreducible polynomial will be separable or not. And normally the problems will not arise in characteristic zero fields but when the characteristic is positive then many problems may crop up but that we will have to carefully study and decide when can a indivisible polynomial be separable or not, or what are the examples of non-separable polynomials. Okay this we will do it next time, thank you very much.