

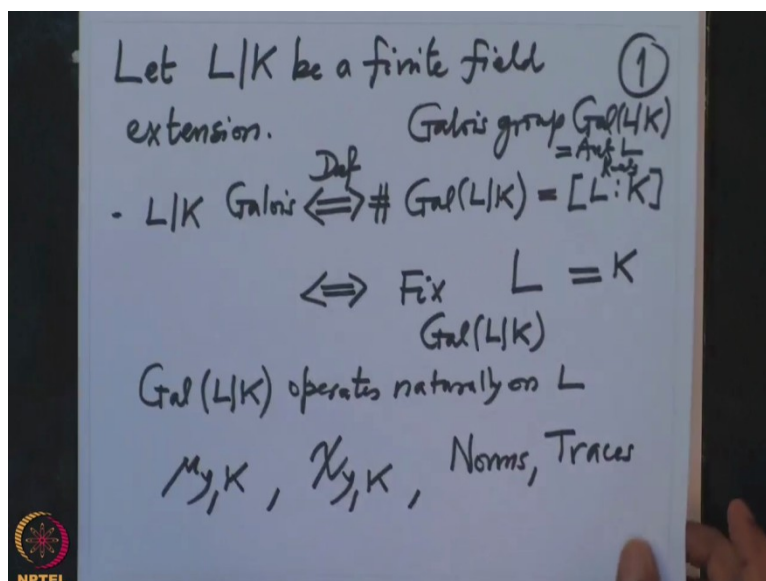
Galois Theory
Professor Dilip Patil
Department of mathematics
IISc Bangalore
Lecture 59

Equivalence of Galois extensions and Normal-separable extensions

Okay, so in the last couple of lectures we have been studying normal field extension and separable field extensions before that we have studied finite Galois extension. And also we have given equivalent characterizations of Galois extensions and now we will use normal and separable extension to give another characterization of Galois extension.

So let me begin with the notation, so we have been studying field extensions and in this course we have concentrated only on the finite field extensions.

(Refer Slide Time: 1:13)



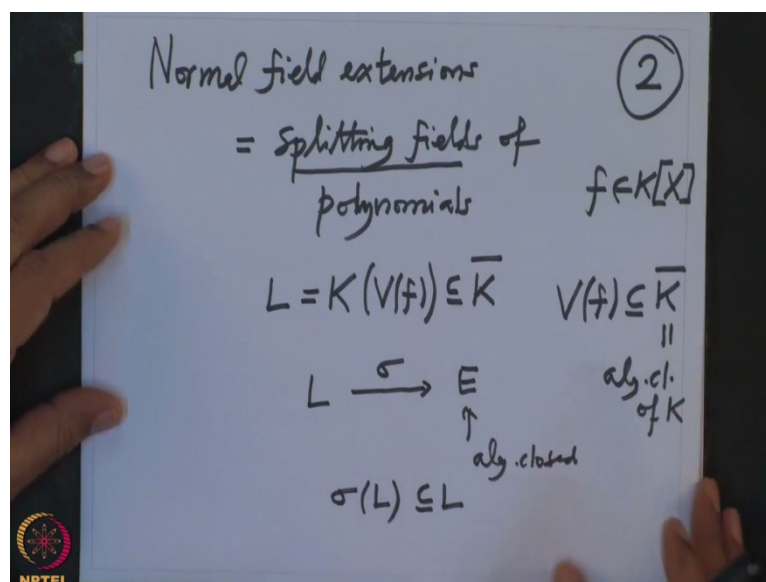
So let L over K be a finite field extension and let us summarize what we have done so far, so we have defined when L over K is Galois that was the definition was, this was the definition this is when the Galois group of L over K has order equal to the degree of the field extension, so the Galois group is $Gal(L/K)$ this is attached to any finite field extension and this is nothing but the Automorphism of L as K algebras.

So elements of the Galois group are also called symmetries of the field extension, so when the number of symmetry is equal to the degree of the field extension this is maximum possible because before this we have proved that the order of the Galois group is bounded by the degree of the field extension, this we got it using Dedekind-Artin's theorem.

So when the Galois extension has a maximum number of symmetries, the. So another thing we proved was, this is if and only if, this was proved that Galois group, so the Galois group operates on this and the , fix field of the Galois group action on L this is precisely the base field K, so here we have use the fact that Galois group of L over K operates naturally on L and we have computed the fix point of this action and that is precisely the base field then it is Galois extension.

So that also gave us many examples how to construct Galois field extensions and also it gave us way to compute the minimum polynomials of the elements, minimal polynomials also it gave us way to compute the characteristic polynomials and also it gives us the concept of and trace and it also gave us a chance to use linear algebra to study finite field extensions, so that was what it.

(Refer Slide Time: 4:24)

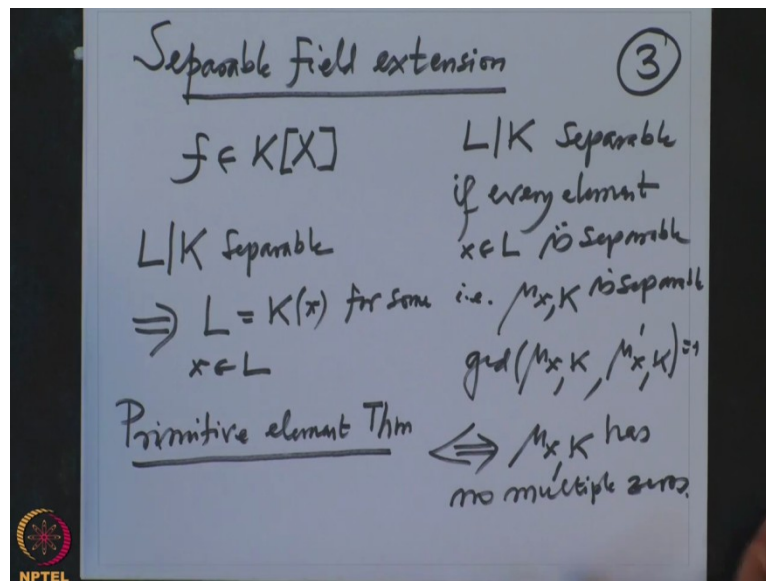


Now after that we have defined normal field extensions and we have characterize them and basically the normal will extensions are precisely the splitting fields, splitting fields of polynomials finite normal extensions they correspond to the splitting fields of polynomials. So splitting field of a polynomial is you have a polynomial F in the base field then we know by Kronicker theorem all the zeros of f delight in the algebraic closure of K, this is algebraic closure of K.

We approved their existence and also we have proved their uniqueness and then you take the subfield of \bar{K} generate it over K by the zeros of this polynomial and these are normal extensions and they have the property that if you call this as L every embedding of L into any

algebraically close field is algebraically closed, the $\sigma, \sigma(L)$ will be containing L that is the definition of normality.

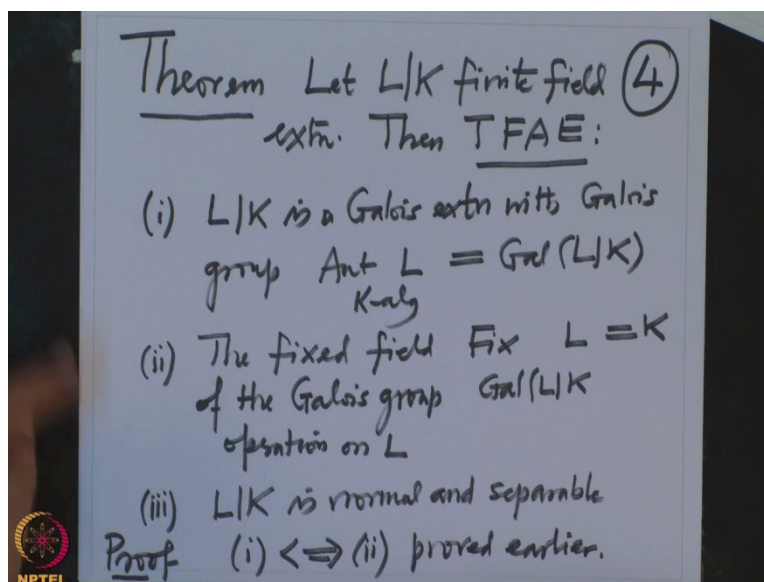
(Refer Slide Time: 6:04)



Okay, so that was normal extensions, now we came to separable extensions, so the most important property of the separable extensions which Galois use in that we develop that here that if I have a polynomial $f \in K[X]$ and I have , so first of all separable extensions means field extension is called separable if every element is separable. So separable if every element is separable $x \in L$ is available but that means that is the minimal polynomial of X over K is separable.

And separable polynomial means that the definition is gcd of μ_x and its derivative they are co-prime and this condition is equivalent to saying $\mu_{x,K}$ has no multiple zeros that means all zeros a simple, so that is a separability and then we have the most important fact Galois use was the separable extensions have primitive element then L is simple, L is of the form $K[x]$ for some x, this was the most important, this is called primitive element theorem and remember we have also proved a primitive element theorem for Galois extension, so that we have proved it very simple by using linear algebra.

(Refer Slide Time: 8:23)



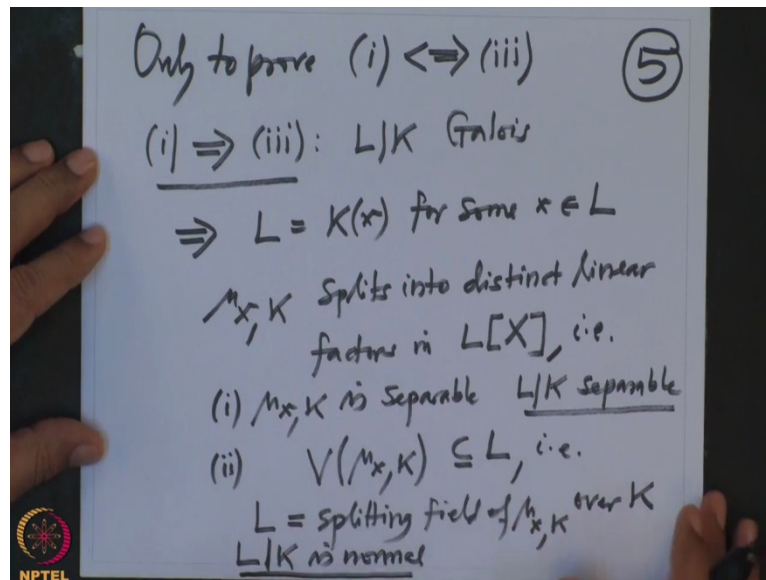
So now I want to state a theorem, so this is let L over K be a finite field extension then the following statements are equivalent 1, L over K is Galois extension with Galois group $\text{AUT } K$ algebras as L this you have the noted by $\text{Gal}(L \vee K)$. 2, the fix field $\text{fix } \text{Gal}(L \vee K)L$ equal to the base field, this is a fix field of the Galois operation, Galois group operation on L is precisely the base field. 3rd one L over K is normal and separable.

Note that in earlier course of lectures we have proved 1 if and only if 2 this was proved earlier, very beginning of course when we started we have proved 1 if and only if 2 and I want to make a few comments before I approve the equivalence of 1 and 3 or 2 and 3 that normally in the modern books 3rd condition is taken as a definition of the Galois field extensions.

But in my opinion it doesn't give a feelings for the subject because if you right away start directly with a definition of normality and separability but doesn't know where this conditions have come from and how did one thing about it whereas if we have defined Galois extension like I did it gave a natural feeling and it was indeed what Galois did it and we followed completely historically as it went on.

And this will complete now once we prove this theorem this will also complete our compatibility with the present-day courses. So therefore it is necessary to prove this theorem because otherwise one might feel that we are different from the world, no we are not different from the world but we have changed the order of studying and that is very important sometimes to study as it happens.

(Refer Slide Time: 11:53)

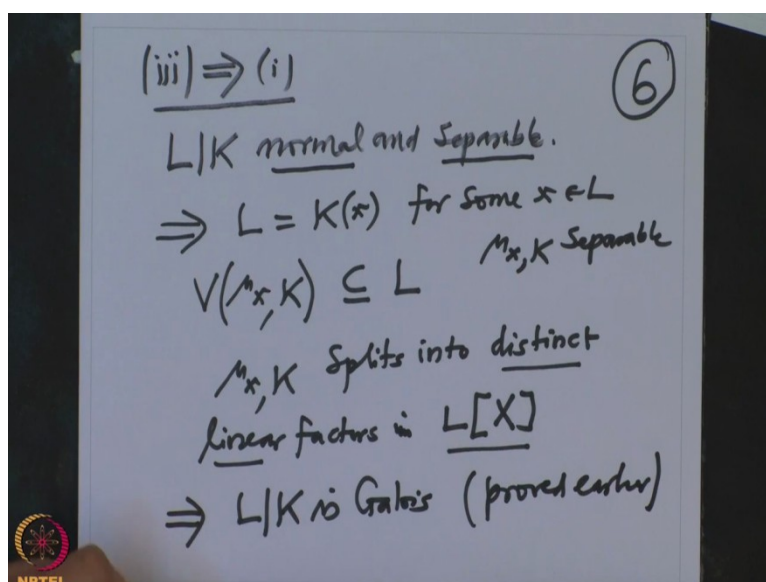


So only now, only to prove if and only if 3, all right. So first 1 implies 3, so I have a Galois extension and I want to prove L over K Galois given and I want to prove it is normal and separable, remember we have proved that Galois extensions have primitive roots, so therefore we know L is K of x for some x this we have proved earlier.

And also we have proved that the simple extension if it is Galois then the minimal polynomial μ_x, K splits into linear factors splits into distinct linear factors in LX , so this simply means, so in other words that is 1, μ_x is separable polynomial and 2nd all roots of μ_x they lie in L and this simply means L is a splitting field of μ_x over K but this means it is therefore L over K is normal and this condition 1 means L over K is separable.

So we have proved that if you have a Galois extension then it is normal and it is also separable, so that proves 3.

(Refer Slide Time: 14:08)



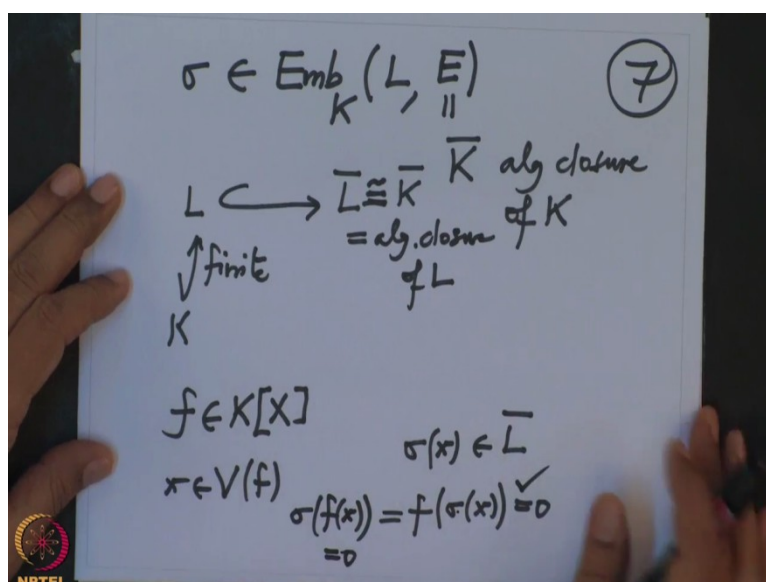
Now 3 implies 1, so we are assuming L over K is normal and separable and now I want to prove that L over K is Galois extension. So to prove L over K is Galois extension note that we have just couple of lectures, last lectures or couple of lectures back we have proved that if it is a separable extension then it is a primitive element, so L is as a primitive element and then because it is normal we know also it is a splitting field.

So normal, so μ_x, K this is minimal polynomial has one root in L therefore all roots of minimal polynomial should lie in this, so all the roots of this they are contained in L , so this means that minimal polynomial x over K splits into distinct because, the minimal polynomial is available because this extension is separable therefore this minimal polynomial μ_x, K is a separable polynomial therefore μ_x splits into distinct linear factors in $L[X]$.

But we know then we have characterized earlier how do you check that simple extension to be Galois? So the only easy way to test is that look at the minimal polynomial as a primitive element and it should split into distinct linear factors in $L[X]$ already, so this proves L over K is Galois this is proved earlier. So altogether we have finished the proof of this theorem that Galois if and only if normal and separable.

Now I want to highlight here 2 very important points which I want to use in further discussion and we have also used it many times earlier namely the following.

(Refer Slide Time: 17:01)

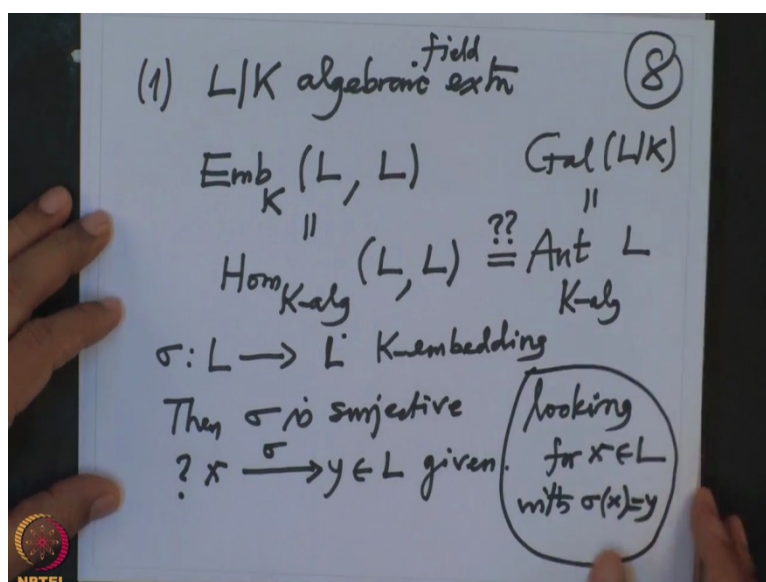


So this was always we have used, so whenever I have an embedding, so σ belonged to K embedding of L into any algebraically closed field E and we have seen that this embedding are independent of this E , so I could have simply taken this E equal to algebraic closure of K . So actually easier way to say is this L over K we have a finite extension.

And therefore finite therefore algebraic and instead of saying K algebraic closure of K I take the \bar{L} which is algebraic closure of L but this is same thing as \bar{K} because this extension is algebraic therefore \bar{L} equal to \bar{K} equal means what? Isomorphic, so better to take an algebraic closure of \bar{L} it will contain L and therefore it will contain K also. So therefore one writes equality here, so this is algebraic closure of L .

And if I have some polynomial of f in the ground field, coefficient in the ground field and if some 0 of that polynomial and if I have any embedding then $\sigma(x)$ this is an element in \bar{L} but it is also 0 of f and f of $\sigma(x)$ is 0 this fact we have used it many times this is simply because σ restricts addition and multiplication and also the K linearity will tell us this is the same thing as $\sigma(fx)$, the $\sigma(fx)$ is 0 therefore this is 0 .

(Refer Slide Time: 19:17)

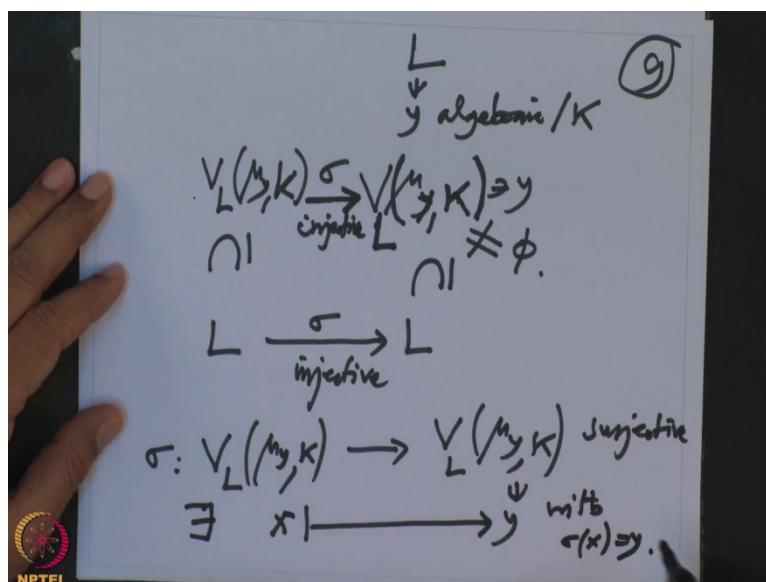


That is one I have repeated this many times but more than that I want to say something better, so the remark I want to make is the following. 1, if L over K algebraic extension not only finite but any algebraic extension and if I have a embedding, K embedding into L , so this is $\text{Hom } K$ algebra from L to L , so because L is a field algebraic field extension.

So L is a field therefore these here, these all embedding is our really injective mappings but apriori it is not clear why should they be surjective but yes it is true that I want to prove this equality in fact they are surjective also and so they are Automorphism of L as K algebra this is what we called it a Galois group of L over K and we are debating why this equality.

So I want to prove that given any σ K embedding I want to prove it is surjective then σ is surjective. So to prove σ is surjective let y be in L given and what am I looking for? I'm looking for x which is going to y under σ . So I'm looking for x in L with $\sigma(x)$ equal to y this is what we want to prove.

(Refer Slide Time: 21:14)



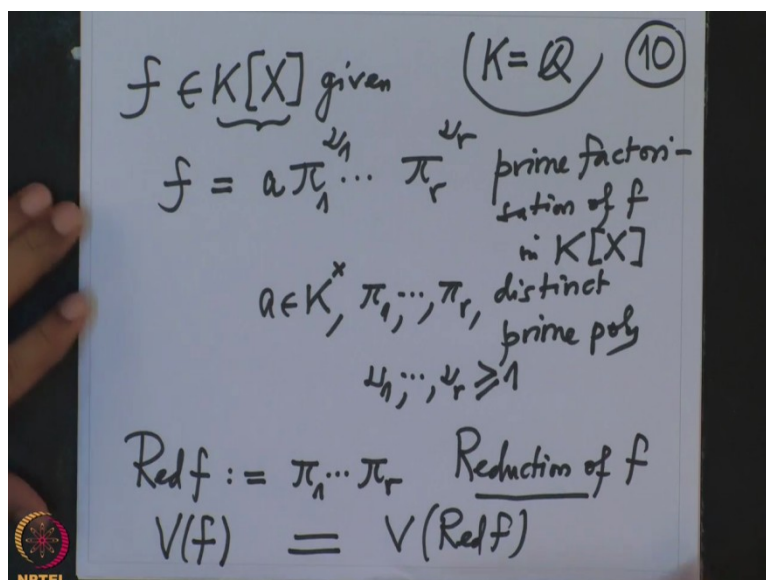
But well we have given y , so we have given and y is in L , y is algebraic over K therefore it has a minimal polynomial μ_y , K this is a polynomial with coefficients in K and therefore I have the zeros set, this zero set lies in and I look at the zeros of this minimal polynomial inside L , this is inside L and definitely y is here therefore this is a nonempty set. This is a nonempty set and we have the σ here L to L and now look at what do we know?

The zero set of the minimal polynomial contains y . I want to restrict the σ to this zero set, so the restriction will map the zero set to itself. That's what our earlier observations say. The zero set goes inside the zero set under the embedding, so this goes inside, so I gate the map. I don't do it by the same letter. I have a map on the finite set, same set to same set. σ is injective therefore the restriction is also injective and now it is a finite set.

Same set to same set injective mapping. Pigeon hole principle will tell you this is surjective, so therefore y is here therefore it is coming from somebody, so σ this map, this map is surjective and y is an element here therefore it has to come from x , so there exists x with $\sigma(x)$ is y that is what we wanted to prove.

So it is very simple the only observation is F you apply embedding to a zero of some polynomial it is a zero of the same polynomial again, okay. So that is what this observation I want to use it again and again, okay. So now I want to recall, I have defined it earlier but I want to elaborate on what is Galois group of a polynomial?

(Refer Slide Time: 24:02)



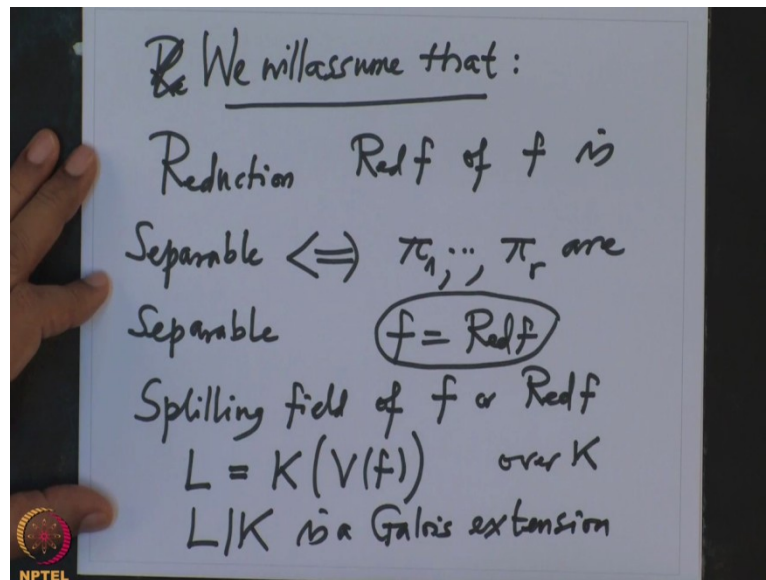
So the original problem what Galois was considering was given a polynomial $f \in K[X]$, so in the Galois time the only field was they were considering was \mathbb{Q} , so they were not even thinking about finite fields and characteristic positive fields and so on. But anyway we have now developed the theory for arbitrary field and we have a polynomial. Now this polynomial f we have proved that this is polynomial ring is a unique factorization domain.

So every polynomial has a unique set factorization, so factorization will look like some constant $a \pi_1^{u_1} \cdots \pi_r^{u_r}$ where this is a prime factorization of $f \in K[X]$, so this means this a is a constant f may not be monic, so I have taken it out that constant is π_1, \dots, π_r a distinct prime polynomials, prime polynomials are the monic polynomials which are irreducible they don't factorize further.

And is u_1, \dots, u_r are natural numbers bigger equal to 1 this is a prime factorization, so if I want to study the zeros of f I might as well forget this a and also I forget this u_1, \dots, u_r because the 0 set will not change, so that I consider the red reduction of f this is by definition π_1 this product of distinct factors, this is called reduction of the polynomial f , so instead of studying a 0 set of...

So note that 0 set of f and 0 set of reduction of f they are same they have not changed only the multiplicity they have changed but they are not bothered about multiplicities because our main aim was to find formulas for the zeros of a given polynomial. So this is we have achieved.

(Refer Slide Time: 26:38)

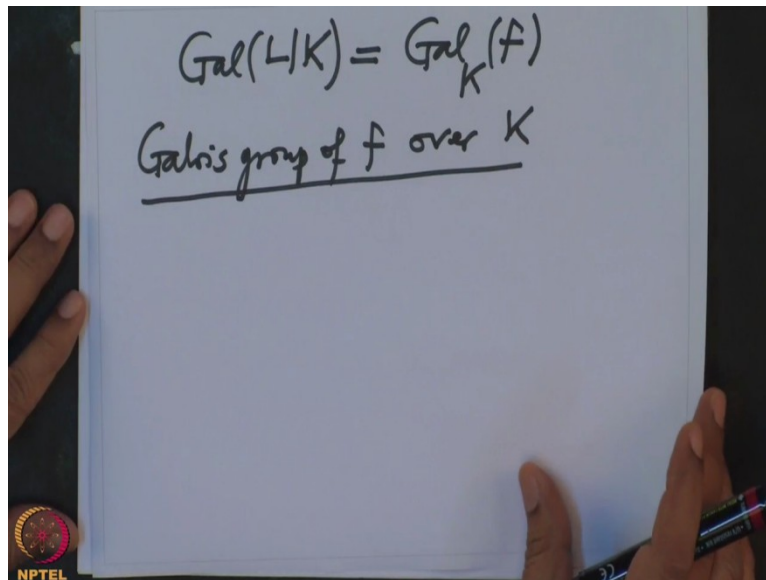


And now even further I want to assume that this is red, we will assume that this reduction that I will denote red f of f is separable polynomial. Separable means it has only distinct zeros but this is equivalent it is taking that this prime factors π_1 to π_r are separable, so we will assume that, this we will assume. And now I consider the splitting field.

So the splitting field of the reduction, , so the splitting field of f or the red f they are the same, so that I will denote by L . So this L is nothing but K adjoin all zeros of F and without loss I will assume now f equal to red f this we will assume, so I don't have to keep writing it every time. So this is a splitting field of f over K and because it is a splitting field it is normal and therefore it is a normal extension.

And because the polynomial is separable it is a normal and separable extension therefore L over K is a Galois extension. And in order to get the formulas or not formulas for a roots zeros of f we have to study this Galois extension more intimately and that is what I will study in this couple of lectures.

(Refer Slide Time: 28:50)


$$\text{Gal}(L/K) = \text{Gal}_K(f)$$

Galois group of f over K

So we want to study this Galois extension and this Galois extension I am going to denote this Galois group I'm going to this is called the Galois group of the polynomial f over K this only depends on f , so this is called Galois group of f over K and we will study this Galois group carefully little bit intimately and I will calculate this Galois group for some specific f in the next half of this lecture.

So with this I will stop and they will continue this calculation in the next lecture, thank you.