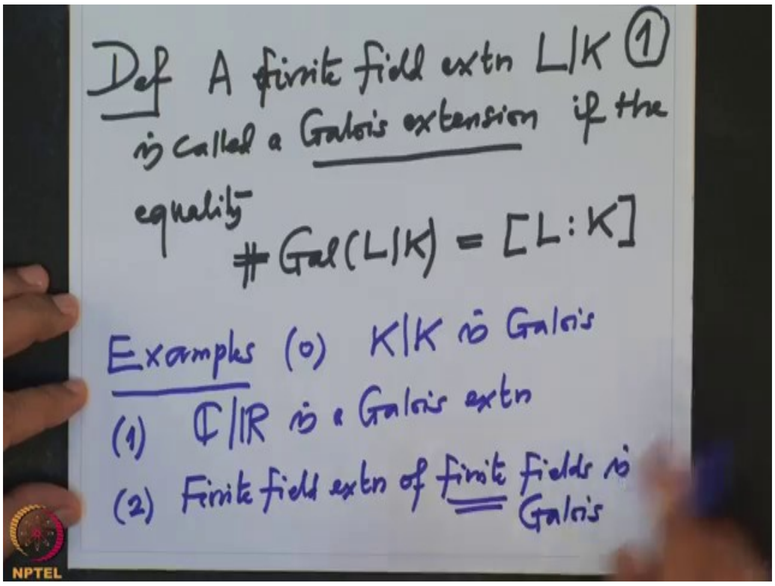
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics,
Indian Institute of Science, Bangalore.
Lecture No. 26
Galois Extension

Recall that in the last lecture, we have proved that, when we have a finite field extension, then the Galois group, the order of the Galois group is less equal to the degree of the field extension and this allows us to define a particular type of field extensions, what are so called a Galois extensions.

(Refer Slide Time: 0:57)



Def A finite field extn $L|K$ ① is called a Galois extension if the equality

$$\# \mathrm{Gal}(L|K) = [L:K]$$

Examples (0) $K|K$ is Galois

(1) $\mathbb{C}|\mathbb{R}$ is a Galois extn

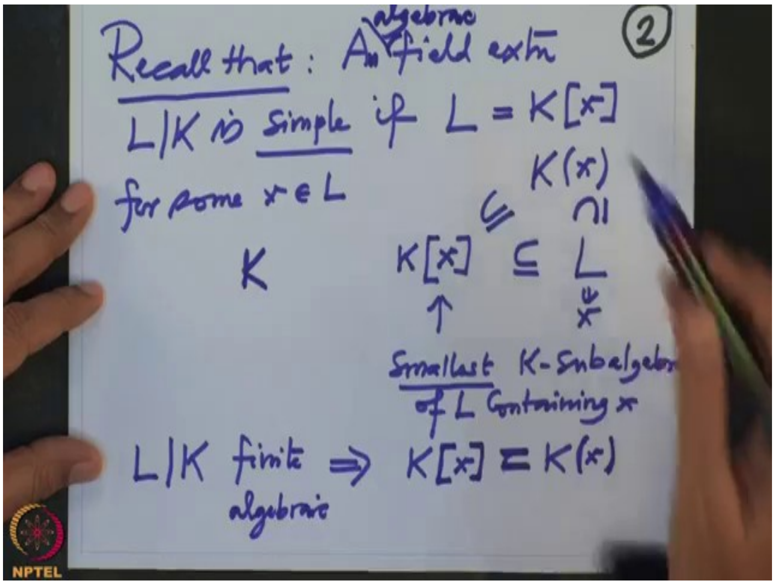
(2) Finite field extn of finite fields is Galois

So let me define properly, so definition. A finite field extension L over K is called a Galois extension, if the equality holds, the equality order of the Galois group equal to the degree of the field extension, such extensions are called Galois extensions, so first of all we have at least few examples, we know that, so obviously the trivial extension K over K is Galois extension, because the degree is one and the Galois group is trivial, so it is obviously Galois extension.

We have also seen that $\mathbb{C}$ over $\mathbb{R}$ is a Galois extension, because in this case, the group has two elements and the degree is also 2. If I have a finite field extension of finite fields is also Galois and in this case also we have immediate consequences the Galois group is cyclic, both the cases in example 1 as well as 2.

So now the next is I am going to analyse when can a simple extension be Galois, so let us recall what a simple extension means? And what?

(Refer Slide Time: 3:31)



Recall that: An algebraic field extn ②

L|K is Simple if $L = K[x]$ for some $x \in L$

K

$$\begin{tikzcd} & K(x) \\ K[x] \arrow[ur, phantom, sloped, "\subsetneq"] \arrow[r, phantom, "\subseteq"] & L \arrow[u, phantom, sloped, "\subseteq"] \\ \text{Smallest K-Subalgebra of L Containing } x \arrow[u] & x \arrow[u, phantom, sloped, "\in"] \end{tikzcd}$$

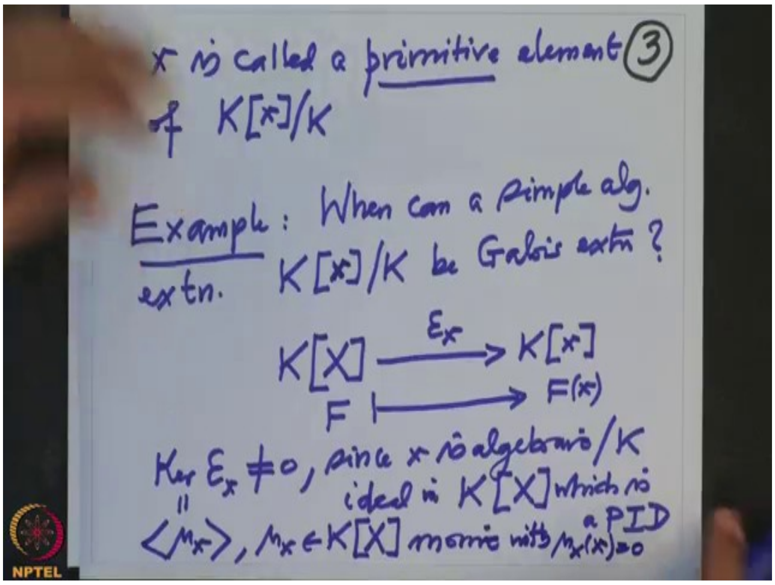
L|K finite algebraic $\Rightarrow K[x] = K(x)$

So first of all recalled that a finite field, in general a field extension L over K is simple, if $L = K(x)$, for some $x \in L$, so remember our notation L is a field here. It contains K and x is an element in L, then we take the smallest, this is a notation for the smallest K algebra that contains x, smallest K sub-algebra of L containing that element x and then we have seen, then all elements of this sub algebra are precisely the polynomials in that x, now the polynomial may not have unique coefficients because it is only a an element, it is not an, it may not be an indeterminate.

So, but now, strictly speaking we should consider K around bracket x, this is the quotient field of this and then, this also contained in L because this is a field and it is a smallest field that it contain this algebra, but L is one such, so this is a quotient field therefore it is contained here.

So simple extension means around bracket here, but why did I write a square bracket because we are assuming that the extension is, if you assume L over K is finite, then $K(x)$ is already a field and therefore it is equal to K round bracket x, this we have seen last time, because it is a finite extension, more generally actually algebraic enough, if I have an algebraic extension, then whether I have it square bracket or round bracket it is a same thing, this we have proved in earlier when we discussed about element wise characterisation of algebraic elements, so in general we are assuming a field extension is algebraic, so an algebraic field extension is called simple, if L is as a algebra over K, generated by one element at is a cyclic algebra and this x is called a generated of that algebra.

(Refer Slide Time: 6:58)



x is called a <u>primitive</u> element ③
of $K[x]/K$

<u>Example</u>: When can a simple alg. extn. $K[x]/K$ be Galois extn ?

$$\begin{tikzcd} K[X] \arrow[r, "\varepsilon_x"] & K[x] \\ F \arrow[r, mapsto] & F(x) \end{tikzcd}$$

$\operatorname{Ker} \varepsilon_x \neq 0$, since x is algebraic/K
$\overset{\shortparallel}{}$ ideal in $K[X]$ which is a PID
$\langle \mu_x \rangle$, $\mu_x \in K[X]$ monic with $\mu_x(x)=0$

So x is also called a primitive element of this $K(x)$ over K remember there may be more than one primitive element that we will see, primitive element are not necessary unique is exactly like a group, a group is called cyclic, if there is a generator and a generator of a group may not be unique as you know from several examples.

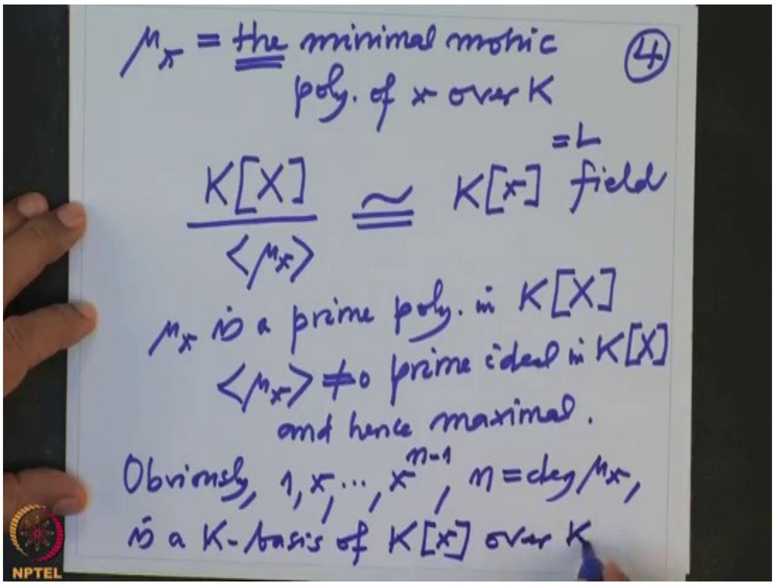
So simple extension is an algebraic extension, right now I am assuming only algebraic and algebraic extension is a simple, if it is, it has a primitive element and now I want to analyse in this example, when can such extension be Galois, so question is we are going to analyse this question, so let me write an example, in this example we are analysing, when can a simple algebraic extension $K(x)$ over K be Galois?

This is what I want to answer. Okay, now this x is an algebraic element in this, so therefore remember our substitution homomorphism for the polynomial algebra to this, this is a substitution homomorphism any polynomial F going to $F(x)$ and we are looking at the kernel of this is definitely nonzero, because since x is algebraic over K, so there is at least one nonzero polynomial in the kernel.

So therefore kernel ideal is a nonzero ideal and we know this is an ideal, ideal in the PID $K[X]$, which is a PID and therefore generated by a single polynomial and if you choose a monic generator, that monic generator is unique and that is called the minimal monic polynomial of X over K.

So this is generated by μ_x , where μ_x is a polynomial over K monic and it is monic with $\mu_x(x)$ is zero a minimal polynomial, minimal monic polynomial.

(Refer Slide Time: 10:13)



μ_x = $\underline{\underline{\text{the}}}$ minimal monic poly. of x over K 4

$$\frac{K[X]}{\langle \mu_x \rangle} \cong K[x] \overset{=L}{} \text{ field}$$

μ_x is a prime poly. in $K[X]$

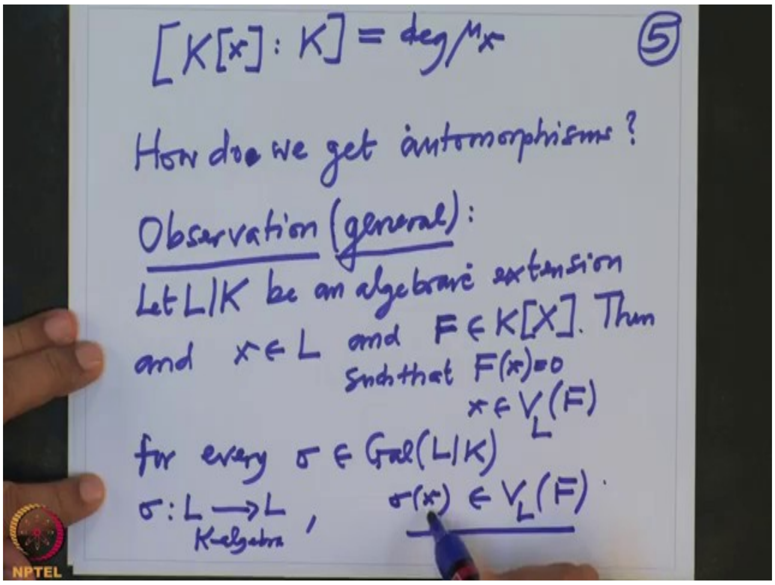
$\langle \mu_x \rangle \neq 0$ prime ideal in $K[X]$ and hence maximal.

Obviously, $1, x, \ldots, x^{n-1}$, $n = \deg \mu_x$, is a K-basis of $K[x]$ over K

So I write once more μ_x is the minimal, the because it is unique the minimal monic polynomial of X over K and we know from the above that, this $\frac{K[X]}{\mu_x}$, this module kernel, this is isomorphic to the image, image is everything here because a this map is surjective, so we have this isomorphism, and because this is a field therefore μ_x is a prime polynomial in $K[X]$, it is a maximal ideal, its generates a prime ideal, it generates a nonzero prime ideal μ_x is a nonzero prime ideal in $K[X]$ and hence maximal also.

So the divisional algorithm will tell, this is a field and I am going to write down a basis of these, this is our field, this is our L, so obviously we have seen earlier also, obviously $1, X, \ldots, X^{n-1}$, where n is the degree of μ is a K basis of this field $K[X]$ over K.

(Refer Slide Time: 12:35)



$[K[x] : K] = \deg \mu_x$ 5

How do we get automorphisms?

Observation (general):

Let $L|K$ be an algebraic extension and $x \in L$ and $F \in K[X]$. Then such that $F(x)=0$ $x \in V_L(F)$

for every $\sigma \in \operatorname{Gal}(L|K)$

$\underset{K\text{-algebra}}{\sigma : L \longrightarrow L}$, $\underline{\sigma(x) \in V_L(F)}$.

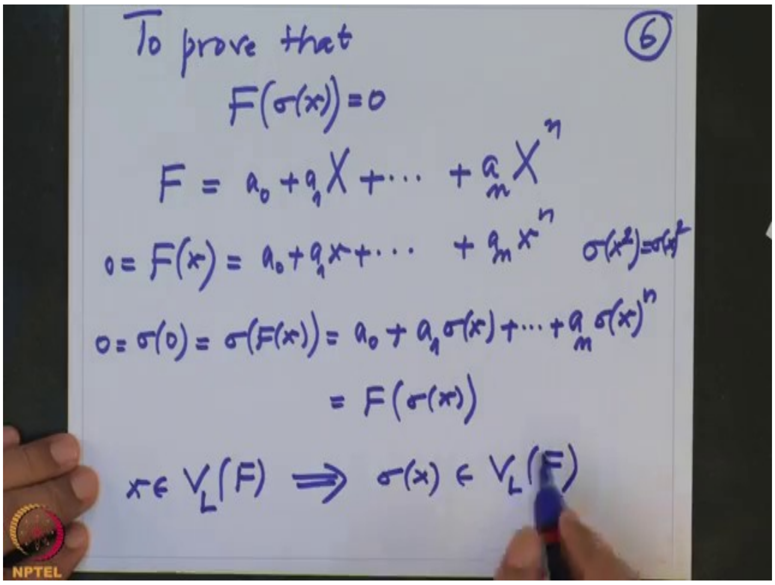
So this in particular shows that, we can compute the degree of the field extension, so this shows that degree, field extension, degree of the extension equal to degree of the minimal monic polynomial of x, now we want to compute the Galois group. Now take any automorphism, I want to compute, so we want to know now, how do we get automorphism? And then you want to count also and we want to see how many in which case, they will be equal to the degree μ_x .

So this is very important observation which will use again and again and this observation is general, in this observation I need not assume that it is a simple extension, so I want to write this observation, a general observation, which is used very often in Galois theory, so L over K be an algebraic extension and let us take and element $x \in L$ and a polynomial F in $K[X]$.

Then if I take any automorphism such that polynomial F, such that, so I want to assume also, polynomial F such that, if $F(x)$ is zero, so this one also one writes x belong to $V_L(F)$, remember our notation $V_L(F)$ is the set of all zeros of F inside the field L, this x may not be in K, so take such a thing.

Then and let us take σ , than for every σ an element in the Galois group of L over K, so Galois group of L over, σ belonging to that means σ is a K algebra homomorphism from L to L, K algebra homomorphism, so for every this $\sigma(x)$ is also zero of F, this is what I want to prove, so what should I prove, I should prove that, if I take F any valuated $\sigma(x)$ it should be zero.

(Refer Slide Time: 16:25)



To prove that 6

$$F(\sigma(x)) = 0$$

$$F = a_0 + a_1 X + \cdots + a_m X^n$$

$$0 = F(x) = a_0 + a_1 x + \cdots + a_m x^n \quad \sigma(x^2) = \sigma(x)^2$$

$$0 = \sigma(0) = \sigma(F(x)) = a_0 + a_1 \sigma(x) + \cdots + a_m \sigma(x)^n$$

$$= F(\sigma(x))$$

$$x \in V_L(F) \Rightarrow \sigma(x) \in V_L(F)$$

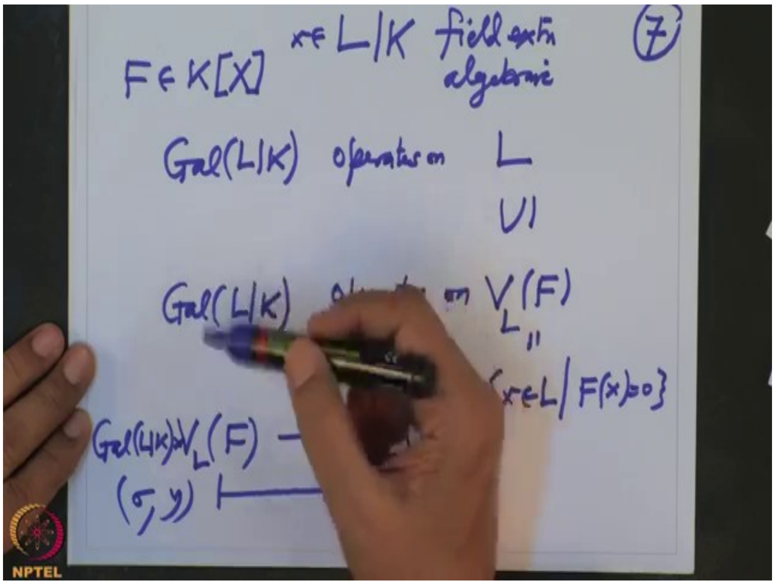
So I want to prove that, so to prove that, I will write, to prove that, $F(\sigma(x))$ is zero, then it will be a zero of $F \in L$ also, so remember $F(x)$ is zero given to us, so F is a polynomial like this, only once I have to write this and this is again and again use, so it is a polynomial like this $a_n X^n$, then what is $F(x)$, $F(x)$ is given to be zero, that means I have to put small, capital x equals to small x so such a combination is zero in L, now I apply σ to this equation.

So σ of zero, which is zero obviously, because σ is a group homomorphism from the identity groups, so this is $\sigma(F(x))$ but then, this is σ of this sum, but the sum, the σ respects sum and σ respect the scalar multiplication and σ also respect the multiplication, so therefore when I want to apply σ to this, I will apply separately plus and σ of a not is a not because σ is K linear on the elements of K it is same.

The next one is σ of this a x, but the $a_1 x$, but a_1 will come out because it is K linear, so this is $\sigma(x)$, a_1 I will take it out, $a_1 \sigma(x)$ and so on and the last term will be a_n will come out and $\sigma(x)$ I will repeatedly take out, so this is nothing but $\sigma(x^m)$, that is because it is respect the multiplication, so we have used repeatedly $\sigma(x^2)$ equal to $\sigma(x)^2$, this is why we have used again and again.

So therefore on the other side is this, so this is zero, but this is nothing but F evaluated at $\sigma(x)$, so therefore we have proved that, $F(\sigma(x))$ is zero, that means you have proved that whenever x is then $V_L(F)$, then we have proved that $\sigma(x)$ is also in $V_L(F)$.

(Refer Slide Time: 19:02)



$F \in K[X]$ $x \in L|K$ field extn algebraic

7

$\mathrm{Gal}(L|K)$ operates on L

$\cup\!\mid$

$\mathrm{Gal}(L|K)$ o[illegible] on $V_L(F)$

$\{x \in L \mid F(x) = 0\}$

$\mathrm{Gal}(L|K) \times V_L(F) \longrightarrow$

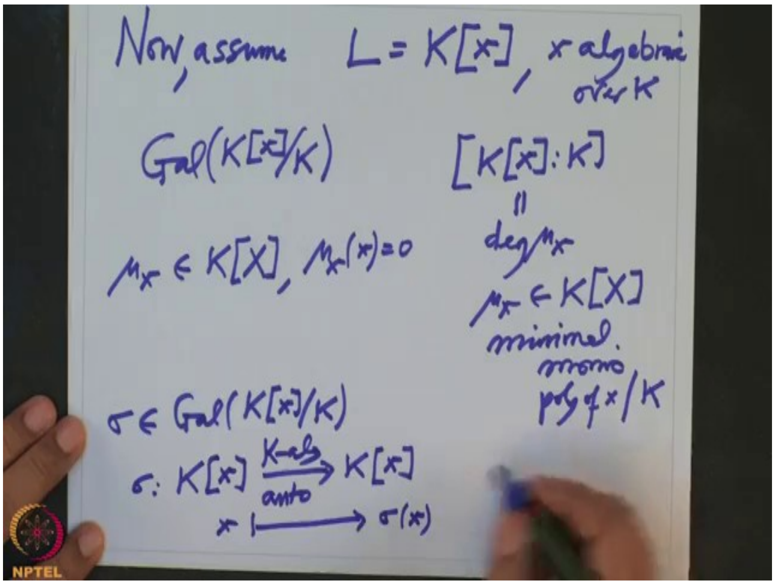
$(\sigma, y) \longmapsto$

So these simply means, now let me get back to the, that means, see here you have L over K was the field extension algebraic and I have an element of x here and I had this L and we have this Galois group of L over K and we have noted that these group operates on L in a natural way, and but I have a smaller subset here now, $V_L(F)$, F is a any polynomial, F is a polynomial in $K[X]$ I have this zero set of F in, so these are all elements in $x \in L$ such that $F(x)$ is zero, remember, it may not have all the zeros inside L given a polynomial F, it may not have all the zeros there unless that L where L contains all the zeros of F, but anyway does not matter

This set, this is a subset of L and we have checked that these group actually, this group operates on this, on the zero set of polynomial and this operation is nothing but a restriction of this operation is the same operation as it operates on L, the same operation $V_L(F)$, Galois group of L over K^x this to $V_L(F)$, the map is the same map, evaluation maps, (σ, y) goes to $\sigma(y)$, we have checked that this is indeed an element here.

So this is, and this is a finite set L may not be finite, but this is a finite set and if you assume you are field extension is finite, then we also know this is a finite set, so therefore comminatory argument will help us to decide many things about field extension as well as the Galois group, so that is a trick,

(Refer Slide Time: 21:31)



Now, assume $L = K[x]$, x algebraic over K

$Gal(K[x]/K)$

$[K[x]:K]$ $\|$ $\deg \mu_x$

$\mu_x \in K[X]$, $\mu_x(x) = 0$

$\mu_x \in K[X]$ minimal mono poly of x/K

$\sigma \in Gal(K[x]/K)$

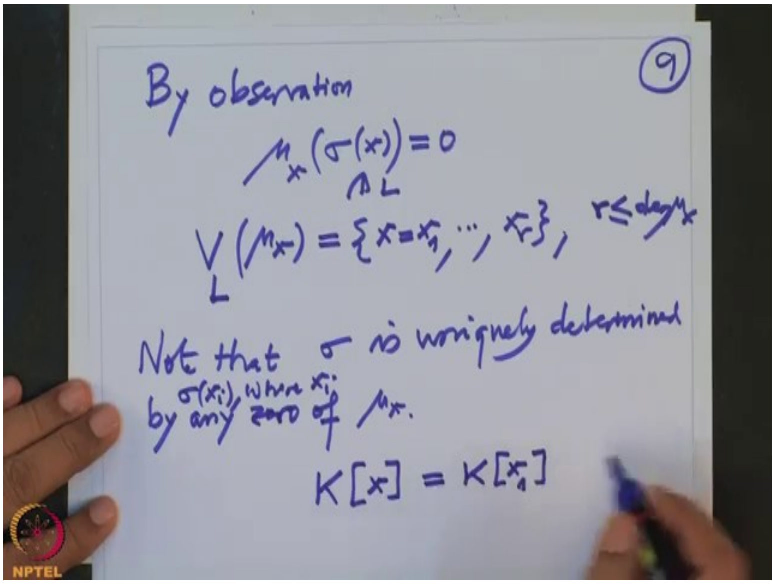
$\sigma : K[x] \xrightarrow[\text{onto}]{K\text{-alg}} K[x]$

$x \longmapsto \sigma(x)$

Now resuming back to our simple case. Now, assume you are L is a simple extension and X is a primitive element, then we have seen an x is algebraic over K, then we have noted that this degree is nothing but the degree of the minimal polynomial of x over K, μ_x is monic polynomial in $K[X]$, minimal monic, this we have just noted x over K and now you want to decide, what is the Galois group? And when can equality happens? This and when can the order be equal to exactly this, this is what I want to do.

So look at μ_x, this is a polynomial in $K[X]$ and x is zero of mu, because it is a minimal polynomial of x, so I want to apply the general observation that we noted about, that this if σ is in element of the Galois group, then and if I apply any, so then we look at $\sigma(x)$, that means is K algebra automorphism from $K(x)$ to $K(x)$, this is σ K algebra automorphism, so x here then it goes to $\sigma(x)$, but we have noted it if this x is a zero of some polynomial, then this $\sigma(x)$ is a zero of the same polynomial.

(Refer Slide Time: 23:57)



9

By observation

$$\mu_x(\underset{\in L}{\sigma(x)}) = 0$$

$$\underset{L}{V}(\mu_x) = \{x = x_1, \dots, x_r\}, \quad r \leq \deg \mu_x$$

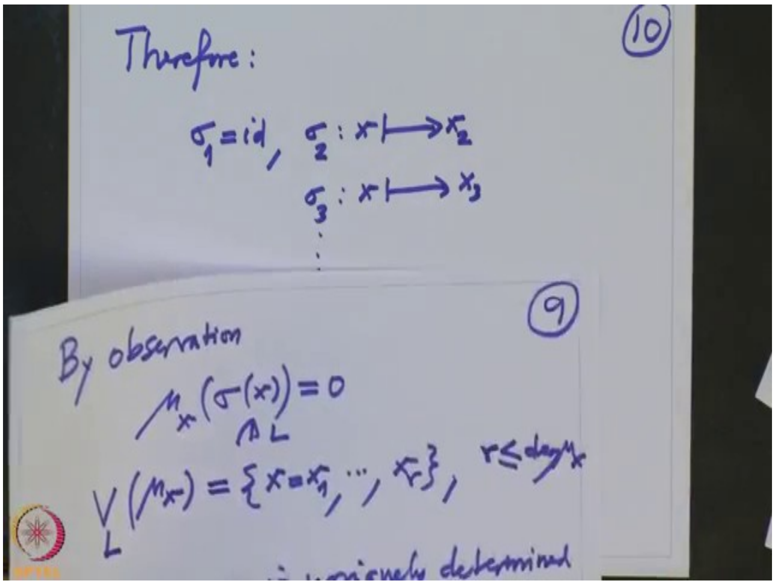
Note that σ is uniquely determined by $\sigma(x_i)$, where x_i any zero of μ_x.

$$K[x] = K[x_1]$$

So therefore by the observation μ_x of $\sigma(x)$ is also zero, so that means $\sigma(x)$ is another group, so that means that this, the zero set of μ_x, L and it should be also in element in L, so if this is equal to say one, zero we know that is x, let us call x equal to x_1 and let us call all other zeros to be $x_1, \dots, x_r$ and we definitely know they are zeros of μ, therefore the number of zeros will not exceed the degree of μ, because we are over a polynomial over a field, so therefore what we noted that, σ will be uniquely determined by the zeros because once we know the zero.

So note that σ is uniquely determined by any zero of what I mean is. Okay, zero, uniquely determined by any zero of μ_x, because if I know σ is uniquely determined by I should say $\sigma(x_i)$, where x_i is any zero of μ. What does that mean? That means if I know, for example if I know value of $\sigma(x)$, then I know all σ, because our field is $K[x]$ but that is also same as $K[x_1]$, because both of them the same minimal polynomial, so therefore these fields are equal, so therefore all that together, altogether what we have done is.

(Refer Slide Time: 26:26)



Therefore:

$$\sigma_1 = id, \quad \sigma_2 : x \longmapsto x_2$$

$$\sigma_3 : x \longmapsto x_3$$

$$\vdots$$

(10)

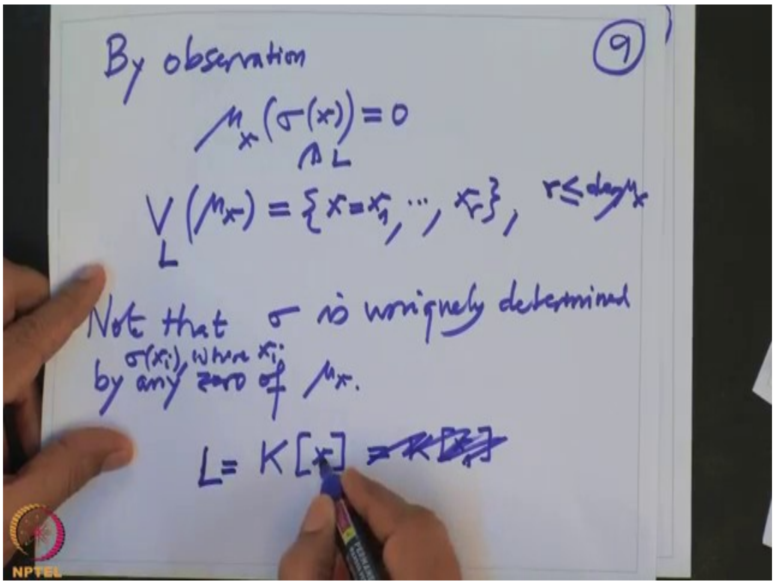
By observation

$$\mu_x(\underset{L}{\underset{\cap}{\sigma(x)}}) = 0$$

$$V_L(\mu_x) = \{x = x_1, \dots, x_r\}, \quad r \leq \deg \mu_x$$

(9)

... uniquely determined



By observation

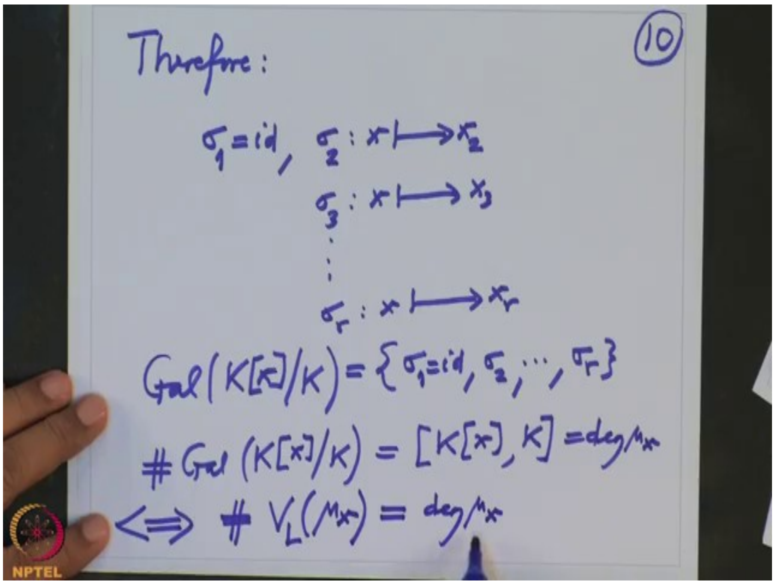
(9)

$$\mu_x(\underset{L}{\underset{\cap}{\sigma(x)}}) = 0$$

$$V_L(\mu_x) = \{x = x_1, \dots, x_r\}, \quad r \leq \deg \mu_x$$

Not that σ is uniquely determined by $\sigma(x_i)$, where x_i any zero of μ_x.

$$L = K[x] ~~= K[x_1]~~$$



Therefore: (10)

$\sigma_1 = id, \quad \sigma_2 : x \longmapsto x_2$

$\sigma_3 : x \longmapsto x_3$

$\vdots$

$\sigma_r : x \longmapsto x_r$

$Gal(K[x]/K) = \{\sigma_1 = id, \sigma_2, \cdots, \sigma_r\}$

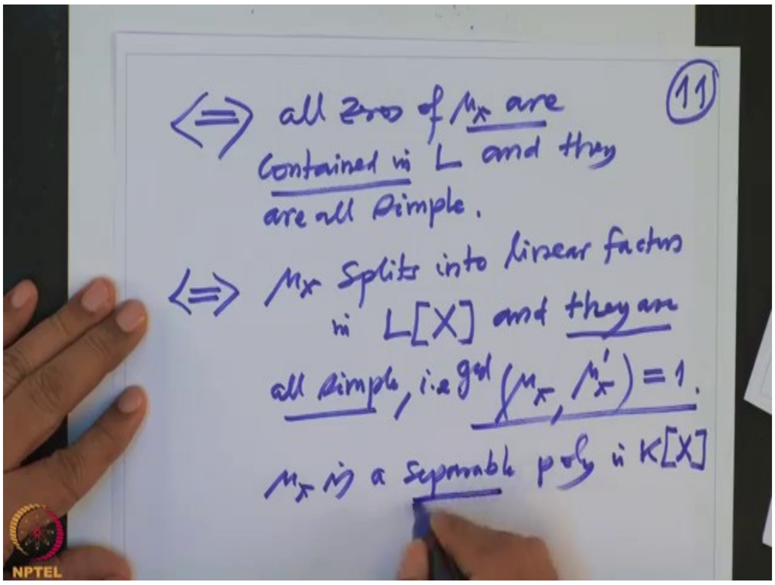
$\# Gal(K[x]/K) = [K[x], K] = \deg \mu_x$

$\Longleftrightarrow \# V_L(\mu_x) = \deg \mu_x$

So I will write a result that, therefore, σ one is the identity σ two means the one which map x to x, σ three the one which map x to x_3 and σ_r is the one x which maps to x_r, these are all automorphisms because x has to go to some route, where it can go, it can go to x_2, it can go to x_3 and so on and I know do not need this equality also, because all that I need is this, these are uniquely determined by their values on x only because is simply because L is $K[x]$ because this L equal to $K[x]$, if I know the value of any automorphism on x then, I know whole automorphism because this algebra L is generated by x.

So therefore what we have proved is the Galois group of $K[x]$ over K is precisely σ one which is identity because in this case x goes to x, then σ_2, and so on σ_r, as many as the number of zeros of the minimal polynomial of inside the field $K[x]$, so therefore when can the equality, so when, so therefore the order of the Galois group $K[x]$ over K equal to this which is the degree μ, this equality happens if and only if the cardinality of the zero set of μ_x in L is precisely degree of μ, that means it has all the zeros are inside L and all are distinct, so all our simple zeros.

(Refer Slide Time: 28:54)



11

$\iff$ all zeros of μ_x are contained in L and they are all simple.

$\iff$ μ_x splits into linear factors in L[X] and they are all simple, i.e gcd$(\mu_x, \mu_x') = 1$.

μ_x is a separable poly in K[X]

So this is equivalent to saying I will note it and then, so this is if and only if all zeros of μ_x is are contained in L and they are all simple, no repeated zero, then only the equality can happen. Okay, now this are two concepts, so this means, so I will then, this is, if and only if that means μ_x splits into linear factors in $L[x]$, that is a meaning that all zeros lies inside L, that is a meaning of this, that is this part and they are all simple, that simply means, so that is μ_x and the derivative μ_x they do not have any gcd, because if there is a gcd that will be the factor of μ and therefore it will have a zero in L and μ_x also will have a zero in L, so there will be common zero and that will not be simple zero, so this condition is also called, they are all simple, this condition can be restated as μ_x is a separable polynomial in $K[x]$, that is a definition of separability.

So we will continue in the, so we a know now when the simple extension is Galois, you only have to take the minimal polynomial and test whether all the zeros are inside that field and whether all the zeros are simple and simplicity is tested without finding zeros because you just have to find that whether the derivative and these original polynomial have common zero or not. Okay, thank you we will continue.