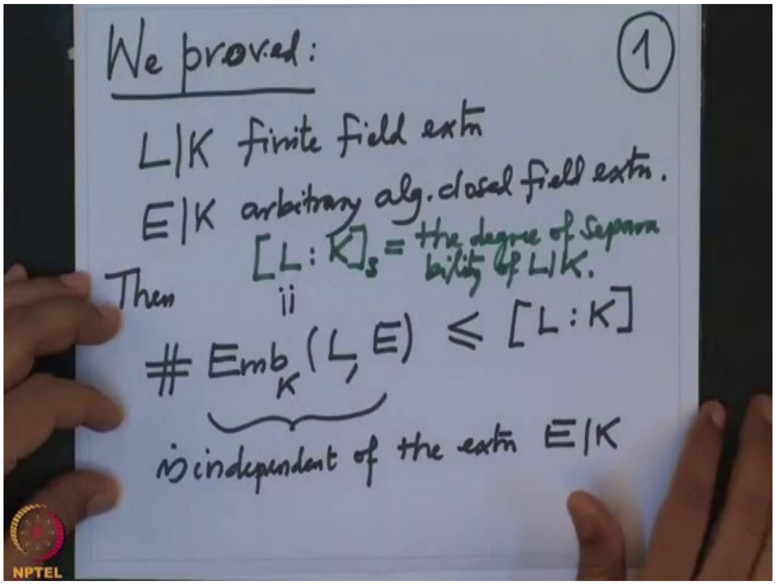
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 57
Characterization of Finite Separable Extension

In the last lecture we have seen that for every finite field extension the embedding of this field extension inside an arbitrary (clo) algebraically closed field extension this number the number of embedding is bonded by the degree of the field extension and this number is also independent of the choice of the algebraically closed field extension of $\mathbb{Q}$. So let me write in symbols what we have proved?

(Refer Slide Time: 00:56)



We proved: ①

$L|K$ finite field extn

$E|K$ arbitrary alg. closed field extn.

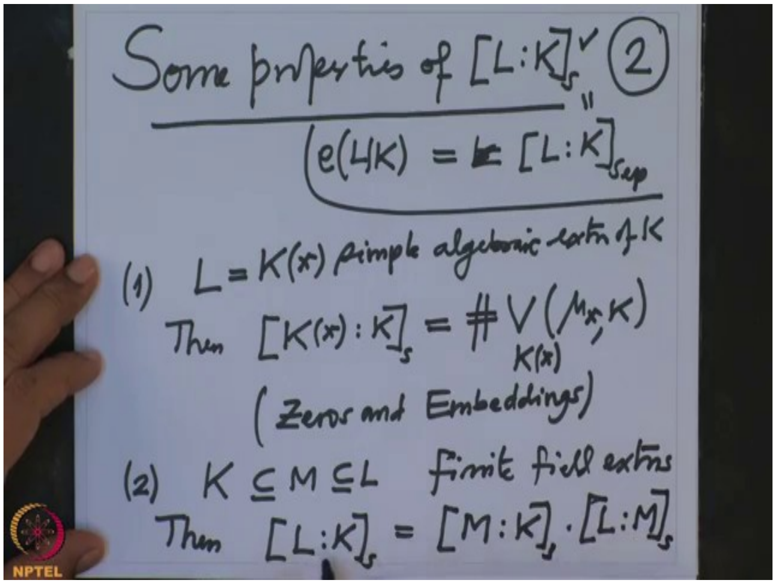
$[L:K]_s$ = the degree of Separability of $L|K$.

Then

$$\overset{\displaystyle [L:K]_s}{\overset{\shortparallel}{\underbrace{\# \operatorname{Emb}_K(L,E)}_{\text{is independent of the extn } E|K}}} \leqslant [L:K]$$

We proved if you have L over K finite field extension and E over K arbitrary algebraically closed field extension then the number of K embedding of L in E this number is bonded by the degree of the field extension and this number is independent of the extension E over K so this that means this number depends only on L over K and therefore this number we define this number to be seperability degree of L over K s, s in the notation here this is called the degree of seperability of L over K that is the definition of, now we will prove that we will observe some basic properties of this seperability degree or degree or seperability and we will prove that equality happens if and only if the given field extension L over K is separable that is what we will prove.

(Refer Slide Time: 3:21)



Some properties of $[L:K]_s$ ✓ (2)

$\parallel$

$(e(L|K) = [L:K]_{sep}$

(1) $L = K(x)$ simple algebraic extn of K

Then $[K(x):K]_s = \# V_{K(x)}(\mu_{x,K})$

(Zeros and Embeddings)

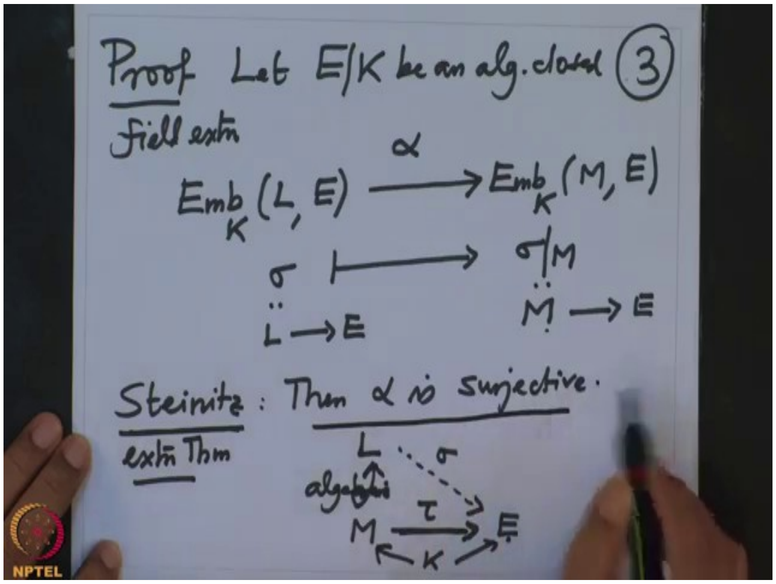
(2) $K \subseteq M \subseteq L$ finite field extns

Then $[L:K]_s = [M:K]_s \cdot [L:M]_s$

So we are aiming to prove this a numerical criterion for the extension to be separable, so some properties, some properties of this L over K (s) this symbol some people denote this symbol in a different way for example when notation is L over K sep for seperability or also one denotes it by simply by e L over K this e being for embedding cardinality of the embedding and so on but I will stick to this notation they are also used ok. So the first property we have already observed if proof L over K if L is simple a simple extension simple, finite simple ofcourse simple algebraic extension of K then this $K[x]$ over K this set s this is nothing but cardinality of the zeros of $\mu_{x,K}$ (in L) in $K[x]$ that is the number of distinct roots of the minimal polynomial in K.

This was precisely done when we did zeros and embedding so I want to recall now this is what we have done in the when we were discussing in the lecture zeros and embedding in that lecture. So that was one, second if you have field K contained in M contained in L finite field extensions then the L over K s is M over K s times L over M s this behave like a degree so like multiplicative , so let us prove this.

(Refer Slide Time: 6:27)



Proof Let E|K be an alg. closed field extn ③

$$\begin{tikzcd} \mathrm{Emb}_K(L,E) \arrow[r, "\alpha"] & \mathrm{Emb}_K(M,E) \end{tikzcd}$$

$$\sigma \longmapsto \sigma|M$$

$$\overset{..}{L} \to E \qquad \overset{..}{M} \to E$$

Steinitz extn Thm : Then α is surjective.

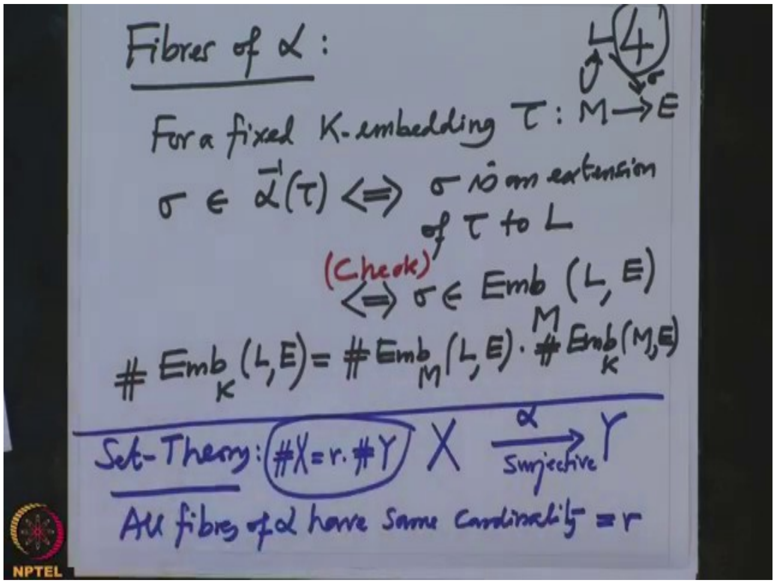
$$\begin{tikzcd} L \arrow[rd, dashed, "\sigma"] & \\ M \arrow[u, "\text{algebraic}"] \arrow[r, "\tau"] & E \\ & K \arrow[ul] \arrow[u] \end{tikzcd}$$

So proof of proof, let E over K be an algebraically closed field extension then we want to understand what is an embedding, how many embedding are the K embedding are there from L to E and what is that relation with embedding of K M to E this and obviously embedding of M to E(L to E) lets see we want to understand this two sets and we want to relate their cardinalities.

So first of all look there is an natural map here this remember embedding is a K algebra homorphism from L to E this are K algebra homorphism from M to E all are fields and this numbers will not depend on the algebraically closed field that we have chosen that we have seen already. So the σ is from L to E this maps to σ restricted to M because if σ is from L to E then it just say restrict means this is from M to E and this is obviously surjective because if I have an embedding from M to E I just ok, so by remember by Steinite’s Theorem that tells if you call this map I want to call this map what I can call it alpha the map alpha is surjective, how does it follow let us indicate that, that is due to Steinite's Theorem you see here we have M here, M to E we have and they are K embedding they are K linear that means this diagram is commutative so we have given this say τ and L is here this is and this extension is finite therefore algebraic and Steinite's extension theorem says that whenever I have algebraic extension and K algebra homorphism inside an algebraically closed field then I can extend it (a σ).

That precisely means this whenever I give an embedding of M in E I can extend to L so that means this map is surjective that is from Steinite's extension theorem. Now if both are finite sets both this are finite sets because their cardinalities bonded by the degree of the lower K and this cardinality is bounded by M over k and L over K is finite extension therefore both are finite sets and subjective map and therefore I want to infer about their cardinality I should know what are the fibers, so what are the fibers?

(Refer Slide Time: 10:03)



Fibres of α :

(4)

$$\begin{tikzcd} L \arrow[dr, "\sigma"] & \\ M \arrow[u, hook] \arrow[r] & E \end{tikzcd}$$

For a fixed K-embedding $\tau : M \to E$

$\sigma \in \alpha^{-1}(\tau) \Longleftrightarrow \sigma$ is an extension of τ to L

(Check) $\Longleftrightarrow \sigma \in \mathrm{Emb}^{M}(L, E)$

$\# \mathrm{Emb}_K(L,E) = \# \mathrm{Emb}_M(L,E) \cdot \# \mathrm{Emb}_K(M,E)$

Set-Theory: $\boxed{\#X = r \cdot \#Y}$ $X \xrightarrow[\text{Surjective}]{\alpha} Y$

All fibres of α have same cardinality $= r$

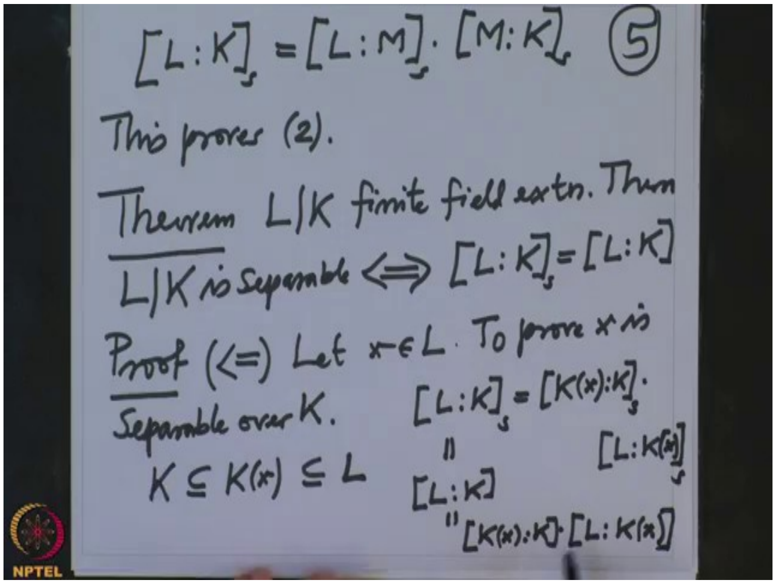
So fibers of alpha what do that mean? That means if I fix τ (so fix) for a fix τ for a fixed embedding K embedding τ from M to E I want know how many extensions are there.

So that one for a fixed τ and σ belongs to the fiber of τ that is if and only if σ is an extension of τ to L so in the diagram that means given this I have L here and extend it to here that is σ so the number of σ i have to count ok but therefore the cardinality of the fiber is precisely extensions from M to L, so that is if and only if this σ belongs to embedding over M of L to E if I fix this τ then this σ so is uniquely determined by so this means what?

This means ok so we have so this means now note this is from Set-theory I want to recall, this means so suppose we have two sets X and Y and a map between them alpha and suppose this alpha is surjective and all fibers of α have same cardinality both are finite sets and suppose the fiber all fibers of the same cardinality equal to r how do you compute the (cardinality) what is the relation between the cardinality of X and cardinality of Y? then we know cardinality of X equal to r times cardinality of Y this is very easy to see and we are in the similar situation we know that this alpha is surjective, alpha is surjective and I want to relate the cardinality of these two sets that is why I wanted to know what are the fibers.

But fibers are in one to one correspondence if the embedding of L to E over M and therefore we know cardinality of embedding of L into E this is same thing as cardinality of the fiber that is cardinality of embedding of L over M in E times cardinality of the image where it is, so embedding of M into E that this are precisely what are this precisely?

(Refer Slide Time: 14:32)



$[L:K]_s = [L:M]_s \cdot [M:K]_s$ (5)

This proves (2).

Theorem L|K finite field extn. Then L|K is separable $\iff [L:K]_s = [L:K]$

Proof ($\Leftarrow$) Let $x \in L$. To prove x is separable over K.

$[L:K]_s = [K(x):K]_s \cdot [L:K(x)]_s$

$K \subseteq K(x) \subseteq L$

$\| [L:K]$

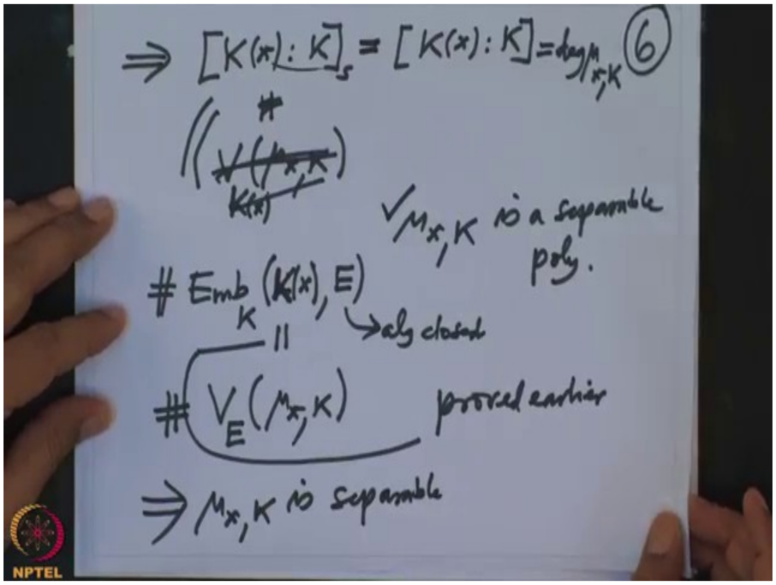
$\| [K(x):K] \cdot [L:K(x)]$

This are precisely L over K s equal to that is L over M s times M over K s so that proves this proves 2, I just want to remind you here that though I wrote this if and only if σ belongs to the embedding over the so this is quite it is little bit this is little bit abuse of notation because all that we know is σ is an embedding of τ to L.

So this is actually one should write it here that it is embedding of this doesn't depend on the τ so it is independent of the τ, so all fibers have the same cardinality. So I will just caution here saying that check this, ok so we have proved that the degree of seperability behaves like a degree. Alright now theorem I want to prove is so theorem I want to prove is let L over K be a finite field extension then L over K is separable if and only if L over K is equal to L over K so equality hold so this side right side is just a numeral, two numbers are equal and that is seperability which is define in terms of every element, so that is advantage.

So proof, alright so first let us prove this side, so we want to prove that as shown in this equality we want to prove that every element is separable. So let X be an element in L we want to prove it is separable, to prove X is separable over K alright now we know that so look at we are in this situation K is here, $K(x)$ is here contained in L is here so we have this tower of field extensions therefore we know L over K is equal to $K(x)$ over K s times L over $K(x)$ s this property 2 I am using and this I know it is equal to L over K given and this we know it is $K[x]$ over K times L over $K[x]$, now this equality is given so from there I infer that the equality holds each one of them.

(Refer Slide Time: 18:49)



$\Rightarrow [K(x):K]_s = [K(x):K] = \deg \mu_{x,K}$ ⑥

$\#\left(\cancel{V(\mu_{x,K})}\right)$ $K(x)$

✓ $\mu_{x,K}$ is a separable poly.

$\# \underbrace{\mathrm{Emb}_K(K(x), E) \overset{\text{}}{=} \# V_E(\mu_x, K)}$ proved earlier

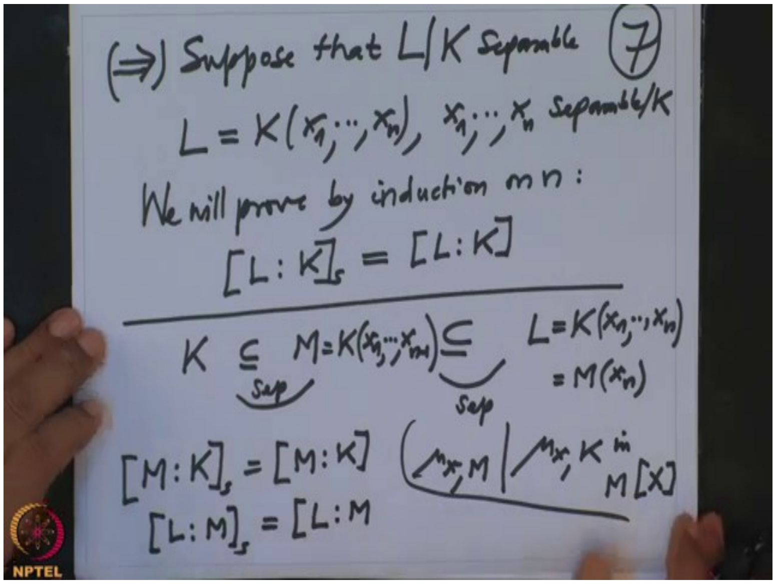
→ alg closed

$\Rightarrow \mu_{x,K}$ is separable

So therefore k x set s equal to $K[x]$ over K simply because we know this is small or equal to this and this is also small or equal to this so if it is both of them have to be equal to this because if one of them is smaller then the corresponding product will be smaller so therefore this and we know what is this, this have proved this is nothing but the number of zeros so this is $V(\mu_{x,K})$ L this is $K[x]$ so that means this is the number of zeros of the polynomial μ_x in this but that will mean that the number of zeros so what do we want to prove that this (numb) they are distinct so we want to check that so to check that x is separable we should check that $\mu_{x,K}$ is a separable polynomial that means it has the number of zeros is exactly if you take an algebraic closure the number of zeros of $\mu_{x,K}$ is precisely the degree of that but this is the degree of $\mu_{x,K}$ and this seperability degree is what?

Seperability degree is precisely so don't use this , this seperability degree is the number of embedding of $K[x]$ inside an algebraically closed field this is algebraically closed and how many embedding are there? There are precisely the number of zeros in $\mu_{x,K}$ number of zeros of $\mu_{x,K}$ in E that is because so the each zero you can define them at I am conversely each this we have proved earlier this is proved earlier therefore this cardinality is equal to this cardinality of the embedding which is by definition seperability degree and seperability we have proved this equality but this is a degree therefore this numbers equal to degree so that means $\mu_{x,K}$ is separable, that means this $\mu_{x,K}$ has so many roots in E.

(Refer Slide Time: 22:11)



($\Rightarrow$) Suppose that L/K Separable ⑦

$L = K(x_1, \dots, x_n)$, $x_1, \dots, x_n$ Separable/K

We will prove by induction on n:

$[L:K]_s = [L:K]$

$K \underbrace{\subseteq}_{Sep} M = K(x_1, \dots, x_{n-1}) \underbrace{\subseteq}_{Sep} L = K(x_1, \dots, x_n) = M(x_n)$

$[M:K]_s = [M:K]$ $\left(\mu_{x,M} \mid \mu_{x,K} \text{ in } M[X]\right.$

$[L:M]_s = [L:M$

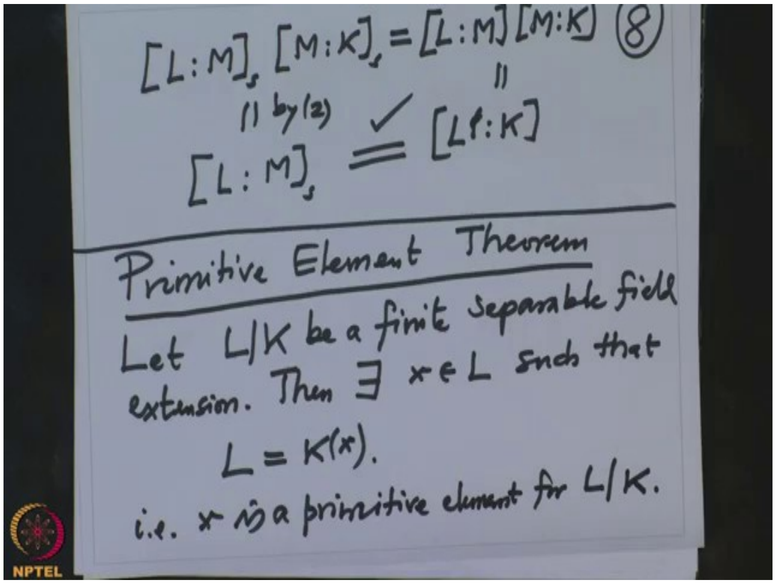
So we have proved this, so therefore we have proved one way that if it is a if equality holds then it is a separable extension conversely so this way conversely we have suppose that L over K is separable then I want to prove that the equality degree so seperability equal to the field extension degree. Alright so L is finite separable so therefore L is generated by finitely many elements $x_1, \dots, x_n$ and each $x_1, \dots, x_n$ is separable over K all elements are separable because the field extension is separable and the finite extension therefore it is generated a finitely many of them and now I am going to prove this assertion by induction on this n.

So I will prove by induction on n what we will prove? That this L over K set equal to L over K, this is what we want to prove, so look here K is here L is here $K[x_1, \dots, x_n]$ and then we have

M inside M is just one less $K[x_1,\ldots,x_{n-1}]$ and this. Now I have the tower of filed extension and this L is M over x_n. Now this is separable therefore this extension is also separable and this also is separable because x_n is separable over K therefore x_n is separable over M because $\mu_{x,K}$ and $\mu_{x,K}$ what is the relation in general?

If I have field in between then this divide this in $M[x]$ that is the relation. So divisor of a separable polynomial is always separable so because of that both this extension are separable therefore by induction I would have had proved that M over K s equal to M over K is by induction and also L over M s equal to L over M and then you multiply them all.

(Refer Slide Time: 25:12)



$[L:M]_s\,[M:K]_s = [L:M]\,[M:K]$ (8)

(1 by (2) ✓ $\|$

$[L:M]_s = [L:K]$

Primitive Element Theorem

Let L/K be a finite separable field extension. Then $\exists\ x \in L$ such that

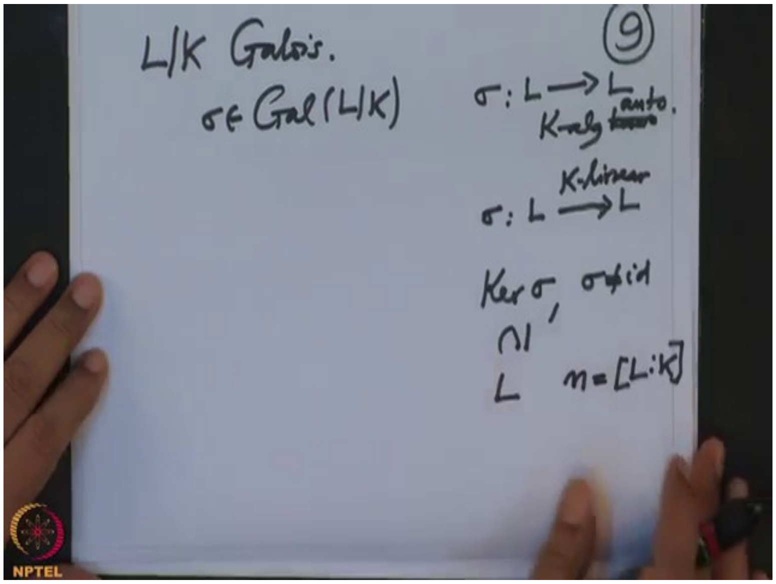
$L = K(x)$.

i.e. x is a primitive element for L/K.

If I multiply this all we have proved a property that this product is same thing as so L M s times M over K s this is equal to L over M s this is by property 2 we have checked and this is by induction it is L over M times M over K but this is L over M, L over K.

So therefore this equal to this we have proved and therefore we have proved theorem that the extension is separable if and only if degree of seperability equal to the degree of field extension alright. Now I want to prove so called primitive element theorem, so Primitive Element Theorem actually we have proved a weaker theorem than this we have proved a primitive element theorem for Galois extension but we don’t have the assumption that extension is Galois but we only know the extension is separable. So let L over K be a finite separable filed extension then we want to prove that then there exists $x \in L$ such that L equal to $K[x]$. So that means that is x is a primitive element for the field extension L over K it is a simple extension alright. So how I am going to prove this?

(Refer Slide Time: 27:50)


9
L/K Galois.
$\sigma \in Gal(L/K)$
$\sigma : L \to L$ auto.
K-alg ~~isom~~
$\sigma : L \xrightarrow{K\text{-linear}} L$
$Ker\,\sigma$, $\sigma \neq id$
$\cap|$
L $n = [L:K]$
NPTEL

Well I am going to prove this by using the embedding I will use embedding to choose this element x correctly I may recall that in case of Galois extension we have also use elements of the Galois groups we thought them as a linear maps and then so what was the proof for Galois in if L over K is Galois I just want to recall that I want to imitate the ideas if this was Galois then we looked at the Galois group $Gal(L|K)$ this is a finite group so if you have any element σ in this so that means the σ is K algebra homorphism from L to L, K algebra auto-morphism actually and therefore it is a linear map from L to L, k linear map in a finite dimensional vector space.

So we look at the Kernel's of this σ and they are if σ is not identity (σ is not identity) this are proper subspaces of a finite dimensional vector spaces L this is a n dimensional vector space where n is the degree of a field extension and we have chosen an element out so the unions of this Kernel and that give the primitive element so similar thing I am going to do it for the embeddings so this we will do it after we take a break we will continue this proof and as a consequence we will prove that an extension finite field extension is Galois if and only if it is separable and normal, this was what the another equivalent definition of the Galois extension, so we will do this after the break, thank you.