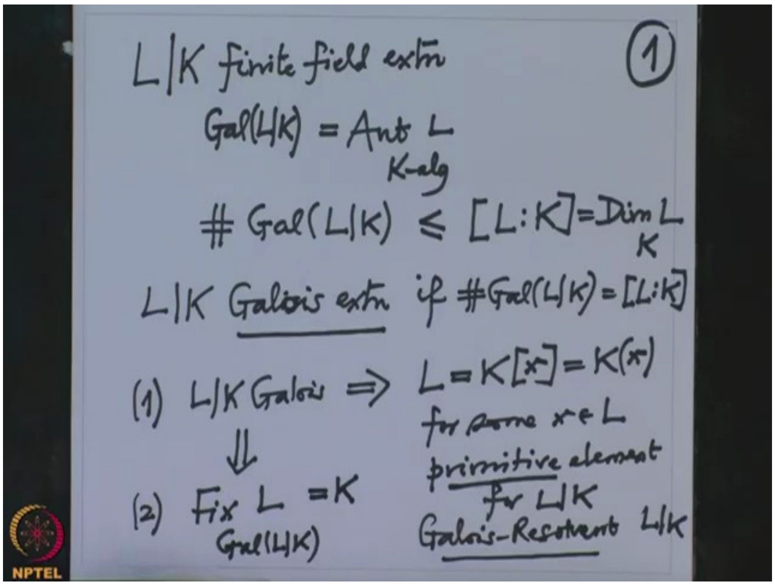
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 32
Fundamental Theorem of Galois Theory

(Refer Slide Time: 0:37)



L|K finite field extn ①

$\mathrm{Gal}(L|K) = \underset{K\text{-alg}}{\mathrm{Aut}}\, L$

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

L|K $\underline{\text{Galois extn}}$ if $\#\mathrm{Gal}(L|K) = [L:K]$

(1) L|K Galois $\Rightarrow$ $L = K[x] = K(x)$ for some $x \in L$ $\underline{\text{primitive element for } L|K}$ $\underline{\text{Galois-Resolvent}}$ L|K

$\Downarrow$

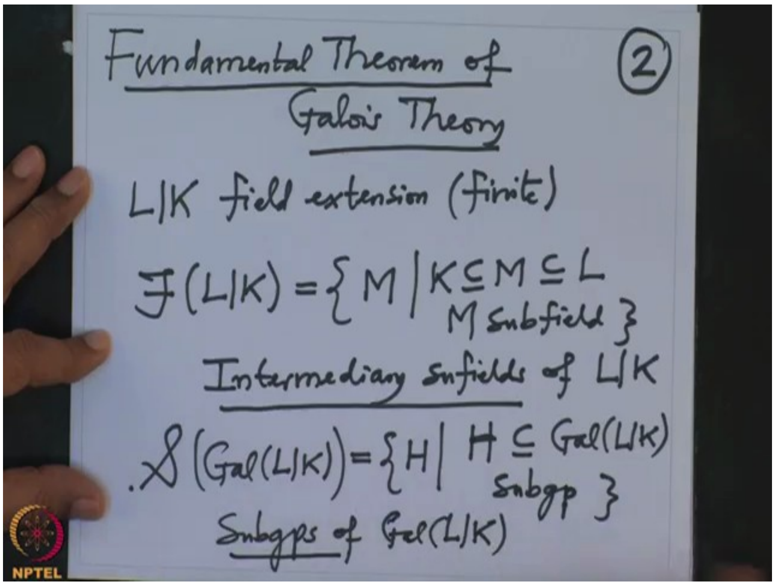
(2) $\underset{\mathrm{Gal}(L|K)}{\mathrm{Fix}}\, L = K$

Remember that in these lectures here are studying finite field extension along with its automorphism groups, so recall briefly what we have done so far if we have a field extension L over K finite field extension we have attached a group to this namely the automorphism groups of L as K algebra and this group is also called the Galois group of L over K. I want to stress again to define these groups we do not have to assume the field extension is a Galois extension after this we have noted that the order of this group is bounded by the degree of the field extension which is dimensional of L as K vector space and then we define L over K Galois extension if the equality holds that is order of the Galois group is equal to the degree of the field extension.

Remember this is only a numerical condition that is how we define Galois extension and 2 things we have proved that if L over K is Galois then L is simple over K, so L is $K[x]$ for some x which is K round bracket x this is because this is finite for some x, such an x is also called primitive element for L over K and there may be more than one primitive element. This is also called Galois resolvent for L over K, some people actually call not the element as a Galois resolvent but the minimal polynomial of x as a Galois resolvent.

So this is very important and 2^{nd} thing we proved was if L over K is Galois then the fixed field of L under the action of the Galois group is a base field, these 2 things we have proved. Actually we want to prove the converse also but today I will first state the fundamental theorem of Galois Theory which will give a interplay between the Galois group, its subgroups and the intermediary field extension.

(Refer Slide Time: 4:02)



Fundamental Theorem of Galois Theory ②

$L|K$ field extension (finite)

$\mathcal{F}(L|K) = \{ M \mid K \subseteq M \subseteq L \text{, } M \text{ subfield} \}$

Intermediary sufields of $L|K$

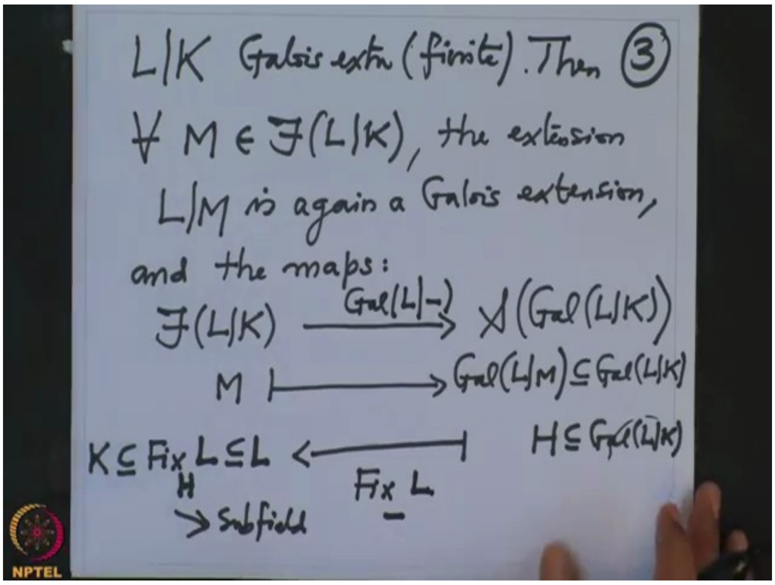
$\mathcal{S}(Gal(L|K)) = \{ H \mid H \subseteq Gal(L|K) \text{ subgp} \}$

Subgps of $Gal(L|K)$

So now I will only state fundamental theorem of Galois Theory. This is so fundamental that it connected 2 subjects one is theory of equations studying the roots or zeros of the polynomials then from this we get field extensions and from the field extensions get the Galois groups and we want to study this interplay, so let us fix to field extension L over K field extension, finite field extension and the set of all intermediary field extensions so that I am going to denote $F(L|K)$ these are subfields of L which contains K, so these are all M, K is contained in M, M is contained in L and M is a subfield.

These are also called intermediary subfields of L over K and also to this we have attached the Galois group and we are looking at the subgroup of this group, so S of this they are precisely the set of all H, H is a subgroup of the Galois group, H is a subgroup. So set of all subgroups, so this definitely has 2 elements one is the trivial element and the other is the whole group. Similarly this intermediary field has definitely 2 elements K itself and L itself this is the subgroups of $Gal(L|K)$ and we want to give a bijection between the 2 and actually we have… There are obvious so you get the map, so the statement of the fundamental theorem is following.

(Refer Slide Time: 6:52)



$L|K$ Galois extn (finite). Then ③

$\forall\, M \in \mathfrak{F}(L|K)$, the extension $L|M$ is again a Galois extension, and the maps:

$$\mathfrak{F}(L|K) \xrightarrow{Gal(L|-)} \mathcal{S}(Gal(L|K))$$

$$M \longmapsto Gal(L|M) \subseteq Gal(L|K)$$

$$K \subseteq \underset{H}{Fix}\, L \subseteq L \xleftarrow[\;]{Fix\, \underline{L}} H \subseteq Gal(L|K)$$

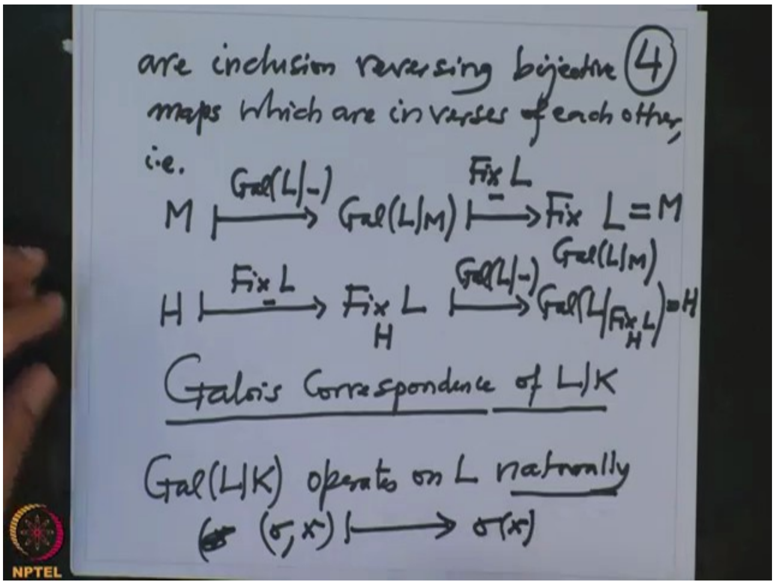
$\rightarrow$ subfield

So we are assuming now L over K is Galois finite always. When we have enough time in the course I will come back to the not necessarily finite extension but here are assuming it is finite extension. Then for every M intermediary field the extension L over M is again a Galois extension and the maps one is from $F(L|K)$ to subgroups of $Gal(L|K)$, the map is any M going to the $Gal(L|M)$ which is obviously subgroup of Galois group of L over K because if somebody is M linear these are all automorphism as a M algebra of L because M is bigger than K they will also be K algebra automorphism of L to L and because they are M linear they are K linear.

So therefore this is clearly a subset means clearly a subgroup that is clear, so the map make sense. So this is one way map and the other way map is, I have a map this way also, so what is the map? Given any subgroup H, H is a subgroup here we definitely have an intermediary field because we can take fix points of L under the action of H. This is clearly will contain K because K is fixed under every element of Galois group in particular every element of H.

So K is clearly contained in here and these are the fix elements of L therefore there is this and this is clearly a subfield that is very easy to see because elements of H are K algebra automorphism of L, so if an element is fixed under K algebra automorphism of L then it is fixed under the inverse of that also and if 2 elements fixed then the composition also fix the element, therefor this is clearly a subfield, so this is indeed a map from here to here. This map I am going to denote by $Gal(L|-)$ and this map I am going to denote by fix_L then what about these maps?

(Refer Slide Time: 10:36)



are inclusion reversing bijective ④
maps which are inverses of each other,
i.e.

$$M \xmapsto{Gal(L|-)} Gal(L|M) \xmapsto{Fix_{-} L} Fix_{Gal(L|M)} L = M$$

$$H \xmapsto{Fix_{-} L} Fix_{H} L \xmapsto{Gal(L|-)} Gal(L|Fix_{H} L) = H$$

Galois Correspondence of L|K

Gal(L|K) operates on L naturally

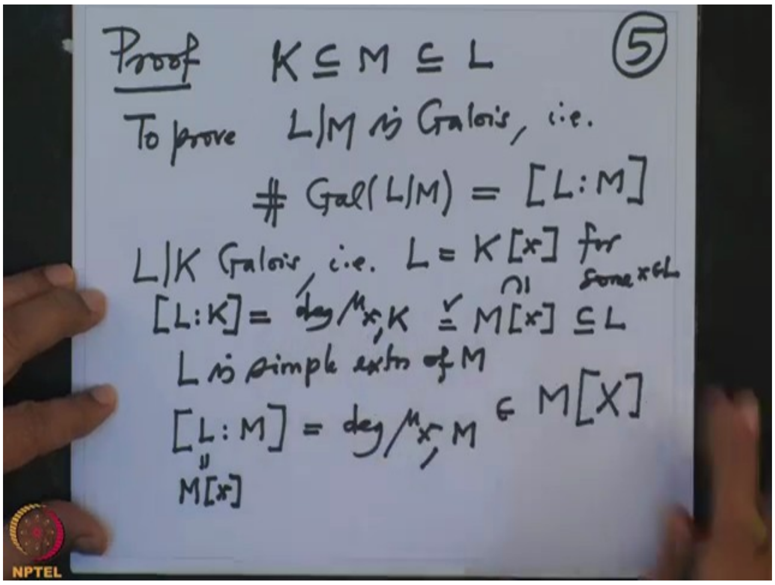
$$(\sigma, x) \longmapsto \sigma(x)$$

The assertion is the maps are inclusion reversing bijective maps which are inverses of each other that means what? That is if I start with M and then go to under this map $Gal(L|-)$ it goes to $Gal(L|M)$ this is my H now and then map these to $Fix_{Gal(L|M)} L$ and then I get back M that means the composite of this map fix… Composite of these 2 maps is an identity map. Also the other way that means I will start with H go Fix_L this goes to the fix field of H and then map it to $Gal(L|Fix_H L)$ then you get back H.

This is $Gal(L|-)$ so that means this maps are inverses of each other that means it gives us interplay between subfields, intermediary subfields and the subgroups of the Galois group, so one can study one to the other and the other way, so it is very important, then when we will prove this now and I am going to make this more finer. These are called Galois correspondence of L over K, now this is the first step I am going to make this more and more intermediate that means I am going to study what happens to the normal subgroups, where do they go? And which intermediary fields will give a normal subgroup?

All these we are going to analyse but first let us finish of the prove of this and as I said the most important thing that I am going to use which I have used in the earlier proves also named at the group $Gal(L|K)$ is group operates on L naturally, the action is so natural that an element of the Galois group, then automorphism and element of x so that operation is σ , x that is going to $\sigma(x)$ that is the operation map that is why it is so natural.

(Refer Slide Time: 14:18)



Proof $K \subseteq M \subseteq L$ (5)

To prove $L|M$ is Galois, i.e.

$\# \, Gal(L|M) = [L:M]$

$L|K$ Galois, i.e. $L = K[x]$ for some $x \in L$

$[L:K] = \deg \mu_{x,K} \overset{\checkmark}{\leq} \overset{\cap}{M[x]} \subseteq L$

L is simple extn of M

$[L:M] = \deg \mu_{x,M} \in M[X]$

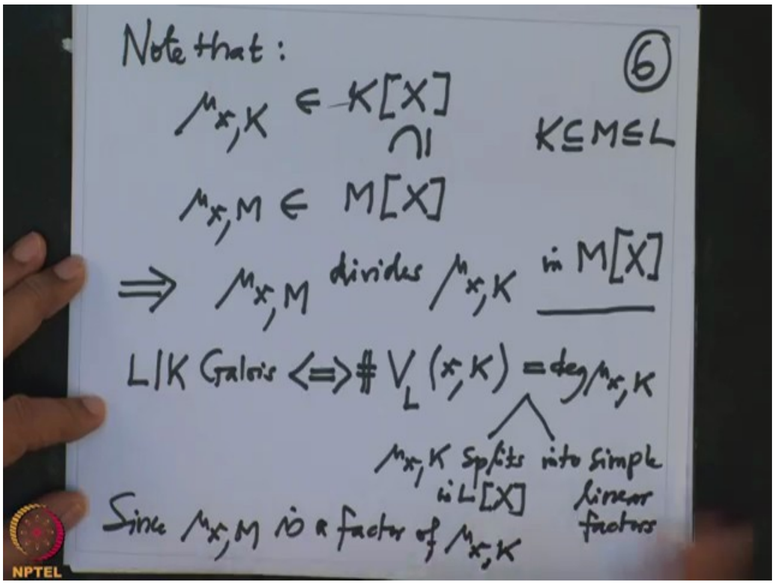
$\overset{L}{\underset{M[x]}{\parallel}}$

So let us prove the fundamental theorem, so proof first the first part that is I have given a subfield L, subfield intermediary, subfield M and I want to prove what? We want to prove L over M is Galois that is the first part of the statement and how do we prove some field extension is Galois so that is I want to prove that the order of the $Gal(L|M)$, this order is same thing as the degree, this is what we want to prove that means that L over M is a Galois extension. Alright, so what do we know? We have given L over K is Galois, so that means there is a primitive element or there is a Galois resolvent.

So that is L as $K[x]$ for some $x \in L$, so this is by definition is the smallest K sub algebra of L which contain x which is also a field because everything is algebraic extension, but then it will also be equal to $M[x]$ because in general if the field… this M is bigger then this is contained here but this is contained in L therefore they are equal, so therefore this is equal. So first of all M is a simple so that is L is simple extension of M and the same is a primitive element, same element x is a primitive element and therefore I know this side, what is L over M and therefore I know degree of L over M this is nothing but the degree of the minimal polynomial of x and I have to be careful because minimal polynomial of x over M.

This is a polynomial with coefficients in M where X is 0 and the small x degree polynomial because this L is $M[x]$ and I want to show that this degree is nothing but the order of the $Gal(L|M)$. Okay and we know that what is the degree of L over K? Degree of L over K is because L is simple, x is a primitive element of L over K this is also the degree of minimal polynomial of x over K, now it is therefore necessary to write in our notation which minimal polynomial you are talking. So and what we know?

(Refer Slide Time: 17:59)



Note that: ⑥

$\mu_{x,K} \in K[X]$

$\qquad\qquad\quad \cap|$ $\qquad K \subseteq M \subseteq L$

$\mu_{x,M} \in M[X]$

$\Rightarrow \mu_{x,M}$ divides $\mu_{x,K}$ in $\underline{M[X]}$

$L|K$ Galois $\Leftrightarrow \# V_L(x,K) = \deg \mu_{x,K}$

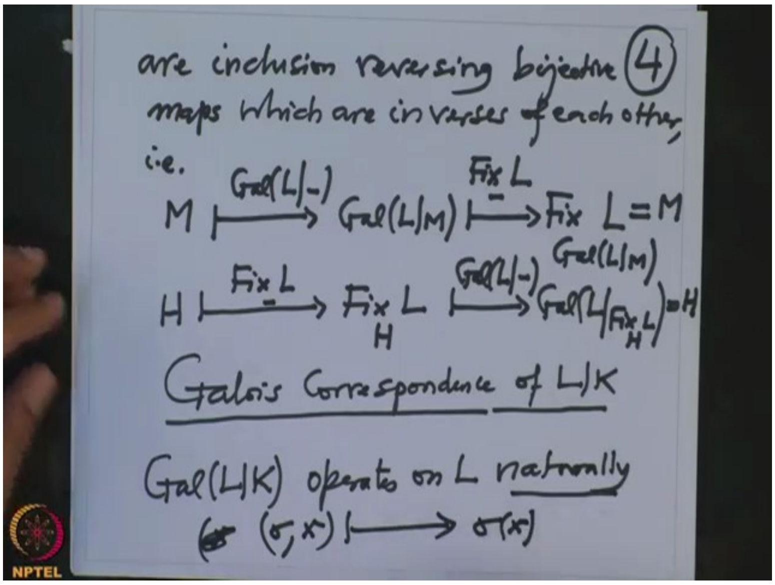
$\mu_{x,K}$ splits into simple linear factors in $L[X]$

Since $\mu_{x,M}$ is a factor of $\mu_{x,K}$

So note that…see $\mu_{x,K}$ this is minimal polynomial of x over K. This is actually polynomial with coefficient in K and $\mu_{x,M}$ this is a polynomial with coefficients in M and these polynomial ring is contained here because K is contained in there and L is contained in there, so this is the polynomial with coefficients in M and this is also polynomial coefficients in M, this is a minimal polynomial over M, this is one polynomial in $M[x]$ where x is 0 therefore obviously by definition of $\mu_{x,M}$, $\mu_{x,M}$ divides $\mu_{x,K}$ where?

In $M[X]$ because this is one polynomial where x is a 0 this is a minimal one and therefore this has to divide in $M[X]$. It is very important to write such things. Alright but we know that because L over K is Galois this is if and only if what, all zeros of $\mu_{x,K}$ this number equal to the degree of μ_x because it is a Galois extension. This means all the zeros of $\mu_{x,K}$ lie in L and they have the same number that means number of zeros equal to that that means all zeros are simple, right? So this is included in this equality, so this means 2 things $\mu_{x,K}$ splits in $L[X]$ into simple linear factors but this is the factor of that. Since $\mu_{x,M}$ is a factor of $\mu_{x,K}$ this was also factor into simple linear factors. So 1st of all this is a factor therefore all of zeros are the zeros here and all are simple.

(Refer Slide Time: 21:14)



are inclusion reversing bijective (4)
maps which are inverses of each other,
i.e.

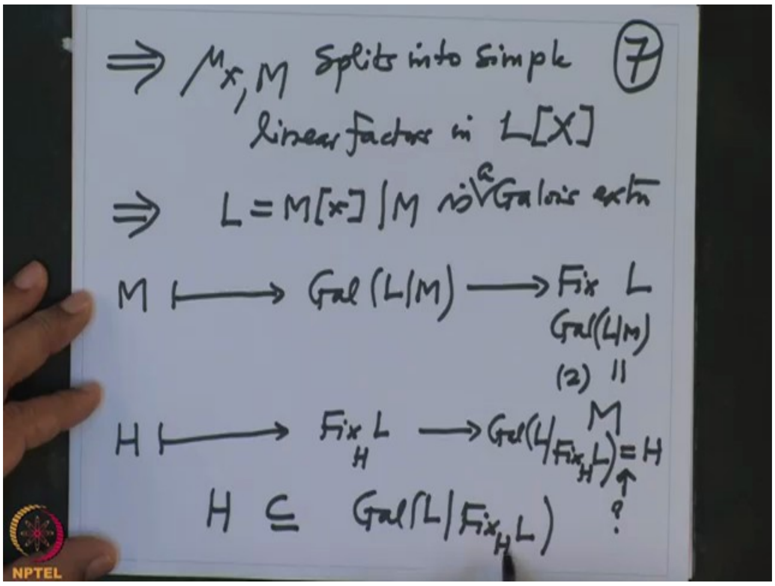
$$M \xmapsto{Gal(L|-)} Gal(L|M) \xmapsto{\underline{Fix} L} \underset{Gal(L|M)}{Fix} L = M$$

$$H \xmapsto{\underline{Fix} L} \underset{H}{Fix} L \xmapsto{Gal(L|-)} Gal(L|\underset{H}{Fix} L) = H$$

Galois Correspondence of L|K

Gal(L|K) operates on L naturally

$(\sigma, x) \longmapsto \sigma(x)$



$\Rightarrow \mu_{x,M}$ splits into simple (7)
linear factors in $L[X]$

$\Rightarrow L = M[x] | M$ is a Galois extn

$$M \longmapsto Gal(L|M) \longrightarrow \underset{Gal(L|M)}{Fix} L \overset{(2)}{=} M$$

$$H \longmapsto \underset{H}{Fix} L \longrightarrow Gal(L|\underset{H}{Fix} L) \overset{?}{=} H$$

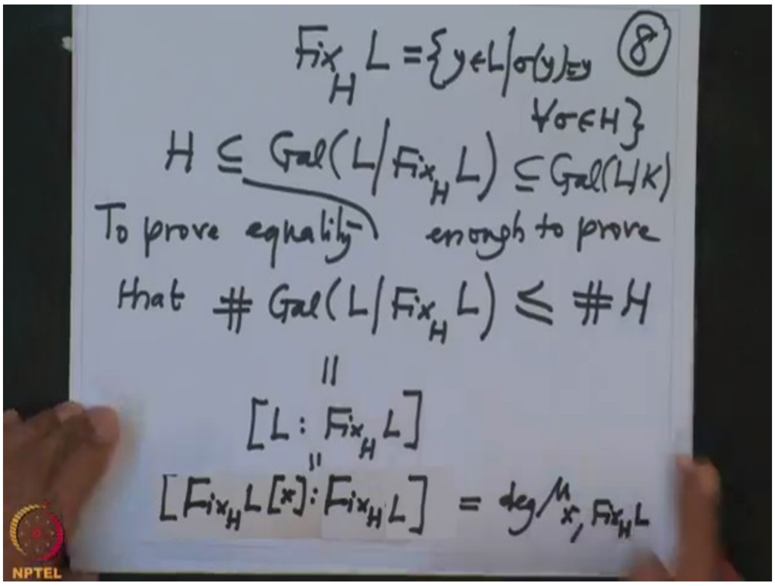
$H \subseteq Gal(L|\underset{H}{Fix} L)$

So that shows that implies $\mu_{x,M}$ splits into simple linear factors in $L[X]$ but that means L which is $M[x]|M$ is a Galois extension, so that was the first part we have to prove. Now we want to prove 2 things namely… I will take this page we want to show that if I start with M go here and then go to the fixed field then I get back M this is what I want to prove alright. So we have noted that L over M is Galois so we started with M then we go to $Gal(L|M)$ and then we go to the fix field of L of this but remember just now we have proved this is a field this extension is Galois and this is its Galois group.

So if I take the action of this Galois group on L the fixed points are precisely a base field, the base field is M and this is precisely the fixed point of L with respect to this Galois group, so this is clearly M because we proved whenever we have a Galois extension if I take the fixed point of the action of the Galois group on a bigger field you get a base field, so because of that… This was the statement 2 which I stated in the beginning of this lecture, so therefore this is obvious, this is going to this is obvious.

Now I have to prove that if I start with H sub group take the fix field $Fix_H L$ and then take the Galois group $Gal(L|Fix_H L)$ then I get back H this is what I want to prove but let us see which thing is obvious, so these are the elements….so let me write $Gal(L|Fix_H L)$ these are automorphism of L which fixes this field, so I say H is contained here that is obvious because take any element of H that is an automorphism of L over K but this automorphism fixes and I want this fix field is precisely all those elements of the Galois group of L over K which fixes H but I already started with element in H, so they have already fixes all these elements because these are elements which are fixed under all elements of H.

(Refer Slide Time: 24:59)



$Fix_H L = \{y \in L / \sigma(y) = y \ \forall \sigma \in H\}$ (8)

$H \subseteq Gal(L/Fix_H L) \subseteq Gal(L/K)$

To prove equality enough to prove that $\# Gal(L/Fix_H L) \leq \# H$

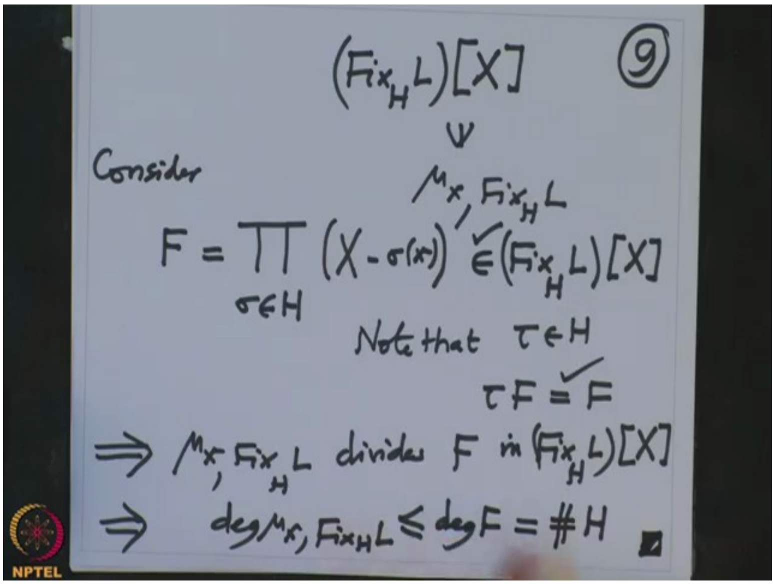
$$\begin{aligned} &\# Gal(L/Fix_H L) \\ &\quad \| \\ &[L : Fix_H L] \\ &\quad \| \\ &[Fix_H L[x] : Fix_H L] = \deg \mu_{x, Fix_H L} \end{aligned}$$

Therefore H is clearly contained here, so I just write here to remind you that fix field of H L is precisely all those elements $y \in L$ such that $\sigma(y) = y$ for every $\sigma \in H$ therefore which is clearly contained in the $Gal(L|Fix_H L)$. Now I want to prove the converse, so this is a sub group this is also sub group of $Gal(L|K)$ all are finite, so I will prove their orders are equal so to prove equality here enough to prove that the order of H this order is smaller equal to order of H.

Order of Galois group of L over fix, this order is smaller equal to order of H. If I prove this then this has to be equality here both are finite sets and this cardinality is more than this, so it has to be equal and this is smaller so this is enough but what is the cardinality of this field? Just now I prove that if I take any intermediary field then the extension is Galois and that will mean that the order of the Galois group equal to degree of the field extension, so this is equal to degree of L over $Fix_H L$ but what is this?

This is nothing but, L is nothing but the same x is a primitive element of this, primitive element of L over this, so this is same thing as $Fix_H L$ are join with x over… $Fix_H L$ but this is nothing but the degree of the minimal polynomial of x over this fix field over $Fix_H L$, so I want to show that the degree of the minimal polynomial is bounded by H and then we are done.

(Refer Slide Time: 27:49)



9

$(Fix_H L)[X]$

$\rotatebox{90}{$\in$}$

Consider

$\mu_{x, Fix_H L}$

$$F = \prod_{\sigma \in H} (X - \sigma(x)) \overset{\checkmark}{\in} (Fix_H L)[X]$$

Note that $\tau \in H$

$$\tau F \overset{\checkmark}{=} F$$

$\Rightarrow \mu_{x, Fix_H L}$ divides F in $(Fix_H L)[X]$

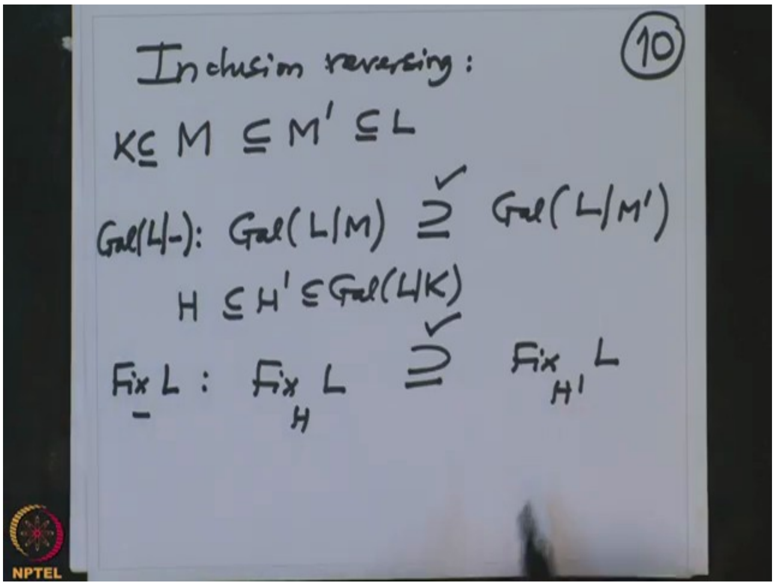
$\Rightarrow \deg \mu_{x, Fix_H L} \leq \deg F = \# H$ ■

So I will actually compute what is the minimal polynomial? So remember I want to know the polynomial over the fix field I want to know what is the degree of the minimal polynomial? So minimal polynomial of x over fix field of this is an element here, on the other hand I will give another polynomial F, so consider a polynomial F which is product σ varies over H so that $X - \sigma(x)$, so first of all note that these polynomials have coefficients in the fixed field of H this, why that? Because how do I check a polynomial as coefficients in the fixed field?

I just have to take any element of H and I apply there, so for this note that if I take $\tau \in H$ then tau of F which is F this is very easy to check apply tau to this product, push τ inside τ is not doing anything to x but it goes here but then use the fact that H is a subgroup therefore this is clear, therefore this is clear, so this is one polynomial with fix field where x is 0 and the minimal polynomial also has x as a 0, so therefore by definition of the minimal polynomial, minimal polynomial will divide this polynomial x.

So minimal polynomial of x over the fix field divides F in this polynomial but in particular that degree of this minimal polynomial will be smaller equal to this, so therefore degree of the minimal polynomial μ_x over fix field of H this is smaller equal to degree of F and degree of F is clear. Degree of F is nothing but the cardinality of H, so what we have proved is degree of the minimal polynomial is smaller equal to this but as I said that is enough because this degree is…so that finishes the proof here that is what we wanted to prove. So that proves that this you get back, so this compose it is identity in both ways so we have checked that both are inverses of each other. Now it was very clear check that their inclusion reversing that means smaller the subgroup bigger the fix field but that is also clear and similarly…

(Refer Slide Time: 31:04)



Inclusion reversing : (10)

$K \subseteq M \subseteq M' \subseteq L$

$\mathrm{Gal}(L|-)$: $\mathrm{Gal}(L|M) \overset{\checkmark}{\supseteq} \mathrm{Gal}(L|M')$

$H \subseteq H' \subseteq \mathrm{Gal}(L|K)$

$\mathrm{Fix}_{-} L$: $\mathrm{Fix}_{H} L \overset{\checkmark}{\supseteq} \mathrm{Fix}_{H'} L$

So only thing to note is inclusion reversing, that will follow from the following of reason, when M and M' are 2 subfield intermediary then what do you want to check? We want to check that $\mu_{x,K}$ and $Gal(L|M')$ which should be bigger inclusion reversing, so this should be clear. This is clear because somebody M' linear then it will be M linear, so this is clear. Similarly if H and H prime are 2 sub-groups of the Galois group then $Fix_H L$ and $Fix_{H'} L$, what is the relation?

Smaller the subgroup bigger the fix field, so this is also clear. So that means this map $Gal(L|-)$ map reverses the inclusion and similarly the fix map reverses the inclusion, so they are inclusion reversing bijection, so that proves all the statements what we made and we will continue improving this correspondence because we will analyse what happens to the normal subgroups for instance and some more things and normal subgroups corresponds to what fields under the intermediary fields, so we will check that the normal field extension precisely give what is called normal field extensions, so we will continue this in the next half.