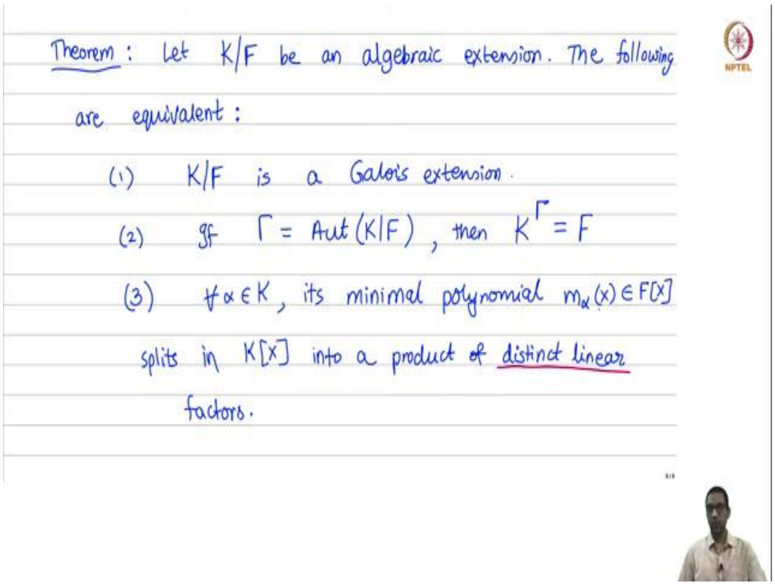
Algebra II
Professor S Viswanath
The Institute of Mathematical Sciences
Lecture 30
Characterization of Galois Extensions

(Refer Slide Time: 00:22)



Theorem: Let K/F be an algebraic extension. The following are equivalent:

(1) K/F is a Galois extension.

(2) If $\Gamma = \mathrm{Aut}(K|F)$, then $K^{\Gamma} = F$

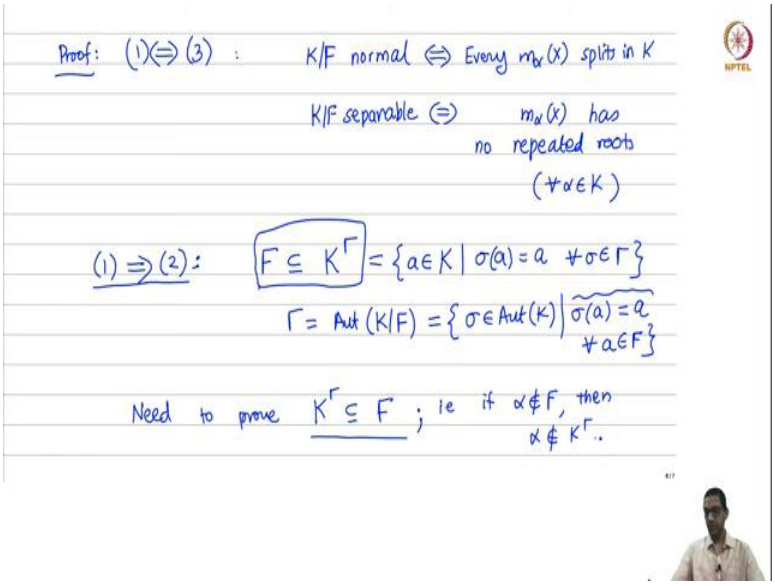
(3) $\forall \alpha \in K$, its minimal polynomial $m_\alpha(x) \in F[x]$ splits in $K[x]$ into a product of distinct linear factors.

And now we are ready to state our main theorem with all these things in place. Let me state the following characterization of Galois extensions. Let K over F be an algebraic extension, then the following statements are equivalent, the following are equivalent. 1, that K over F is a Galois extension. Property 2, if gamma denotes the group Aut K over F, F automorphisms of K, then the fixed field of gamma is exactly F.

And property 3, statement three, says for all elements alpha in K, it is minimal for each alpha in K, it is minimal polynomial m alpha of x. So, its minimal irreducible polynomial over the base field F splits into a product of linear factors, more than that the linear factors are distinct. So, it splits completely, but it does not have repeated roots in K. And this is really the characterization that we now want to prove.

Now, observe that, in some sense 1 and 3 are really, the same thing, we have, we talked about normality and separability; and observe that, to say that the minimal polynomial of every alpha in K splits completely was one of our equivalent characterizations of a normal extension. And the other fact that the minimal polynomial has is separable, meaning it has no repeated roots was exactly the characterization of separable extensions. So, quick observation here is that 1 and 3 are really equivalent to each other.

(Refer Slide Time: 03:13)



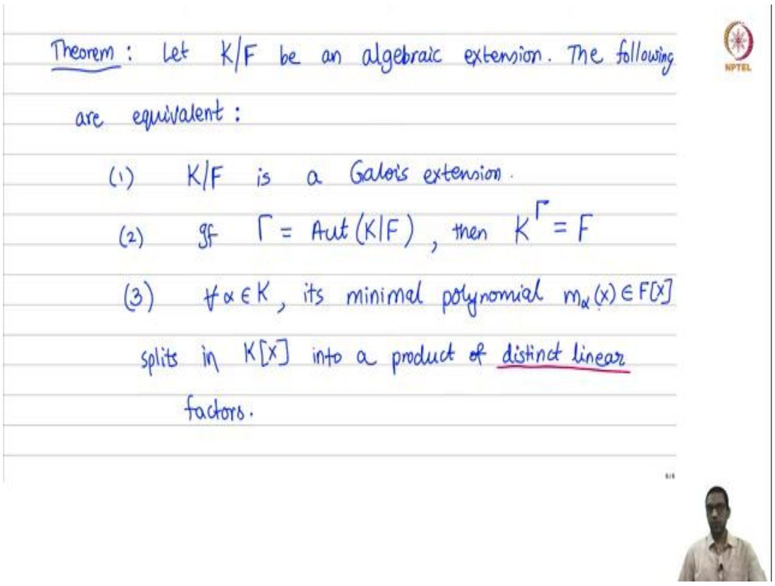
Proof: (1)$\Leftrightarrow$(3) : K/F normal $\Leftrightarrow$ Every $m_\alpha(x)$ splits in K

K/F separable $\Leftrightarrow$ $m_\alpha(x)$ has no repeated roots ($\forall \alpha \in K$)

(1) $\Rightarrow$ (2): $\boxed{F \subseteq K^\Gamma} = \{a \in K \mid \sigma(a) = a \ \forall \sigma \in \Gamma\}$

$\Gamma = \text{Aut}(K/F) = \{\sigma \in \text{Aut}(K) \mid \widetilde{\sigma(a) = a} \ \forall a \in F\}$

Need to prove $\underline{K^\Gamma \subseteq F}$; ie if $\alpha \notin F$, then $\alpha \notin K^\Gamma$.



Theorem: Let K/F be an algebraic extension. The following are equivalent:

(1) K/F is a Galois extension.

(2) If $\Gamma = \text{Aut}(K/F)$, then $K^\Gamma = F$

(3) $\forall \alpha \in K$, its minimal polynomial $m_\alpha(x) \in F[x]$ splits in $K[x]$ into a product of distinct linear factors.

So, let us let us prove this. Start with the assumption. I mean, start with the observation that 1 and 3 are really the same thing. And why is that? Because normality according to what we proved in our lecture on normal extensions, is the following that every minimal polynomial every m alpha of x splits in K into linear factors. But at the moment, they could be repeated as well. But separability ensures distinctness of those linear factors. So separable says that every m alpha of x has, so I should say m alpha of x has no repeated roots. And this is true for all alpha in K.

So, looking back on what we have already proved normal and separable is exactly what statement three encodes. So that is done. What we are really looking for is this new property 2, the new characterization, which says that if you take the set of all F automorphisms, then the fixed field of that group is exactly the base field. So, let us prove that 2 is equal to 1 and 3. So, I will prove it as follows. Let me show first that 1 implies 2. So, if it is a Galois extension, then the fixed field of the group of F automorphisms is exactly the base field.

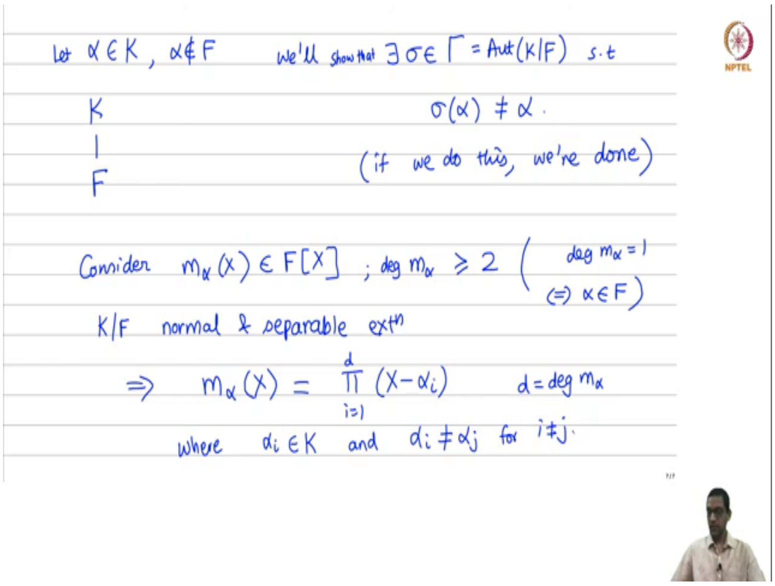
So first observe the base field is certainly contained inside the fixed field. So now I am just using the notation of the theorem, gamma is going to denote the set of all automorphisms of K, K over F, then we need to show K gamma is F. But one way is clear, F is always a subset of K gamma. Why is this? Because what is K gamma, it is a set of all elements of K, which are fixed by every element of gamma.

But gamma is the set of all F automorphisms of K. And what is an F automorphism? It was an automorphism, which is assumed to fix the base field pointwise, fix all those automorphisms such that when you restrict it to elements, so sigma a is definitely a, for all a in F, this is what restricting to F gives you identity means exactly this. So, it is clear that every element of the base field is going to be fixed by every element of gamma. So, this property is clear.

Now, what we need to really prove is that the other inclusion also holds, which is that K gamma is contained in F. So, we now need to show K gamma is also contained in F and we will prove this by contradiction. So, suppose not, well, what does that imply? It says that there is an element suppose not or maybe we should, well, so maybe we will prove it as follows. Let us pick an element of, well, maybe let me not just say contradiction here.

So, let me say I need to prove this K gamma is contained in F. So, I will pick an element that is not in F and show that it is not in K gamma. So, contra positive is really what I mean, I suppose here. So, we will prove this as follows, i.e., if alpha is not in F, then alpha cannot be in K gamma. That is what we will do.

(Refer Slide Time: 07:17)



Let $\alpha \in K$, $\alpha \notin F$ We'll show that $\exists \sigma \in \Gamma = \mathrm{Aut}(K|F)$ s.t $\sigma(\alpha) \neq \alpha$.

$$\begin{tikzcd} K \arrow[d, dash] \\ F \end{tikzcd}$$

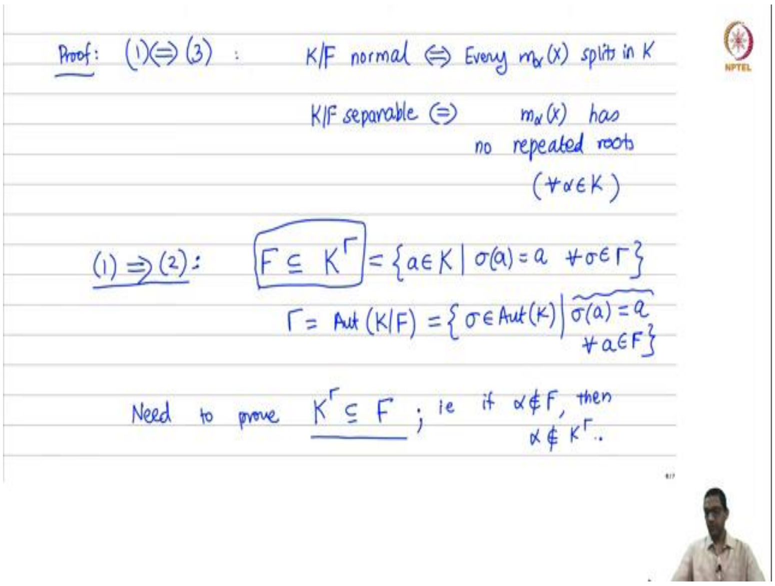
(if we do this, we're done)

Consider $m_\alpha(X) \in F[X]$; deg $m_\alpha \geq 2$ (deg $m_\alpha = 1$ $\Leftrightarrow \alpha \in F$)

K/F normal & separable ext^n

$$\Rightarrow m_\alpha(X) = \prod_{i=1}^{d} (X - \alpha_i) \qquad d = \deg m_\alpha$$

where $\alpha_i \in K$ and $\alpha_i \neq \alpha_j$ for $i \neq j$.



$\underline{\text{Proof:}}$ (1)$\Leftrightarrow$(3) : K/F normal $\Leftrightarrow$ Every $m_\alpha(x)$ splits in K

K/F separable $\Leftrightarrow$ $m_\alpha(x)$ has no repeated roots ($\forall \alpha \in K$)

$\underline{(1) \Rightarrow (2):}$ $\boxed{F \subseteq K^\Gamma} = \{a \in K \mid \sigma(a) = a \ \forall \sigma \in \Gamma\}$

$\Gamma = \mathrm{Aut}(K/F) = \{\sigma \in \mathrm{Aut}(K) \mid \widetilde{\sigma(a) = a} \ \forall a \in F\}$

Need to prove $\underline{K^\Gamma \subseteq F}$; ie if $\alpha \notin F$, then $\alpha \notin K^\Gamma$.

So let us do that. So let is pick an alpha. So, let alpha be an element of K, which is not in F. So, K, which is not in F, so K is an extension of F, I am taking something which is not in the base field. And I need to show that it is not going to be fixed by every element of gamma. So, so what do we need to show, we will show, we will prove the following, we will show that there exists at least one element of gamma, at least one automorphism such that, so, this is we will show that there exists an automorphism which maps alpha to something other than alpha.

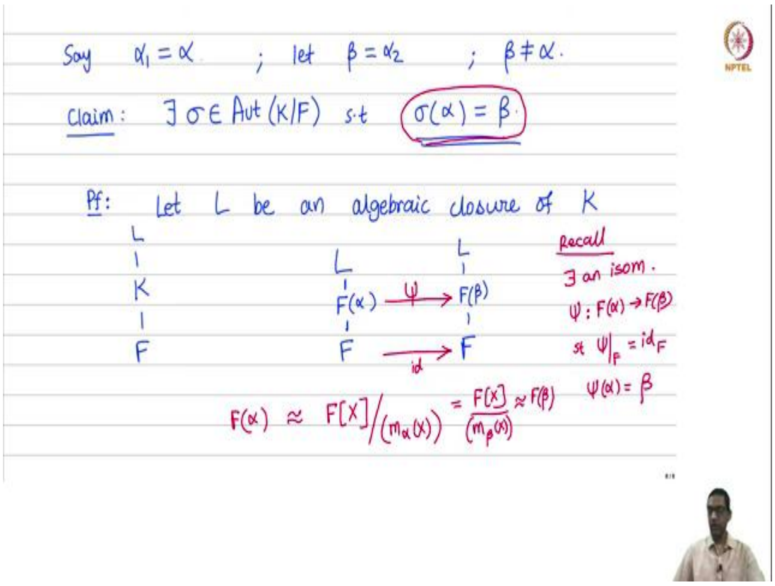
If you show this, then we are done. If we do this, then we are done. We would prove, what we want to prove, because this will tell you that alpha cannot be in the fixed field, at least one automorphism does not fix alpha. So, this is all we need to prove. So, how should we try and construct such an automorphism? So, observe that alpha is in K, but not in F means the following, consider its minimal irreducible polynomial m alpha of x, same notation as in the theorem, m alpha of x is the minimal irreducible polynomial of alpha over the base field.

This polynomial has degree at least 2, degree of m alpha is at least 2. Why? Because the degree 1 polynomials are exactly the, if m alpha had degree 1 then it would tell you that alpha is actually in the base field, because the polynomial would be of the form some linear polynomial, it looks like, it will look like x minus some constant, which means that alpha minus that constant is 0. So, alpha itself is that constant.

In other words, alpha is the base field. Because if degree m alpha is 1, then it just means that alpha is in the base field. In fact, it is an if and only if statement. Now degree is at least 2 means the following, well, what are we assuming? We are assuming 1, so we are assuming that the extension is normal and separable. So now here is an irreducible polynomial m alpha of x, look at its roots. So, look at K over F. I have assumed that it is Galois.

So, in other words, I know that this is a normal separable extension, which implies or you can think in terms of property 3, which is the same thing, it says that this polynomial m alpha of x, firstly splits completely, becomes a product of x minus alpha i's, i goes from 1 to d, where d the degree of this polynomial. So, d is the degree of m alpha, where the alpha i's are distinct numbers, that is the important thing here. The separability, where alpha i's are in K and alpha i not equal to alpha j for i not equal to j. In other words, you have a split into a product of distinct factors.

(Refer Slide Time: 11:02)



Say $\alpha_1 = \alpha$; let $\beta = \alpha_2$; $\beta \neq \alpha$.

<u>Claim</u>: $\exists\, \sigma \in \mathrm{Aut}(K/F)$ s.t $\underline{\boxed{\sigma(\alpha) = \beta}}$.

<u>Pf</u>: Let L be an algebraic closure of K

$$\begin{tikzcd}
L \arrow[d, dash] & & L \arrow[d, dash] & L \arrow[d, dash] \\
K \arrow[d, dash] & & F(\alpha) \arrow[r, "\psi"] \arrow[d, dash] & F(\beta) \arrow[d, dash] \\
F & & F \arrow[r, "id"'] & F
\end{tikzcd}$$

<u>Recall</u>
$\exists$ an isom.
$\psi : F(\alpha) \to F(\beta)$
st $\psi|_F = id_F$
$\psi(\alpha) = \beta$

$$F(\alpha) \approx F[X]/(m_\alpha(X)) = \frac{F[X]}{(m_\beta(X))} \approx F(\beta)$$

Now, so of course, alpha is one of the roots here. So, m alpha of x, of course, alpha is the root of this polynomial. Let me assume the first root alpha 1 is alpha, say, say, alpha 1 is your alpha. Now, let us look at the second root. So, recall, there is at least one more root because the degree is at least 2. So, let us call the second root as beta. So, let beta denote alpha 2, let beta be alpha 2, we know that, what do we know? We know beta is not the same as alpha certainly.

Now we will construct our automorphism as follows, there exists an automorphism, there exists sigma in gamma, gammas. There is an F automorphism of K, such that sigma maps alpha to beta. That is our claim. Now, once you prove this, you are done, because beta is not the same as alpha. Now, let us prove this claim. Again, it is an argument which we have seen before when we talked about normal extensions, and so on. So, for this, let us just bring in the algebraic closure.

So, it is convenient to have the algebraic closure here. So, let L be an algebraic closure of the field K. So, what I am doing here is looking at K, this is a base field F. And now I am putting L inside its algebraic closure. So, observe, again, algebraic closures, as you have seen before, are unique. In a certain sense there exists given any two algebraic closures there is always automorphism between them which restricts to an identity on the base field.

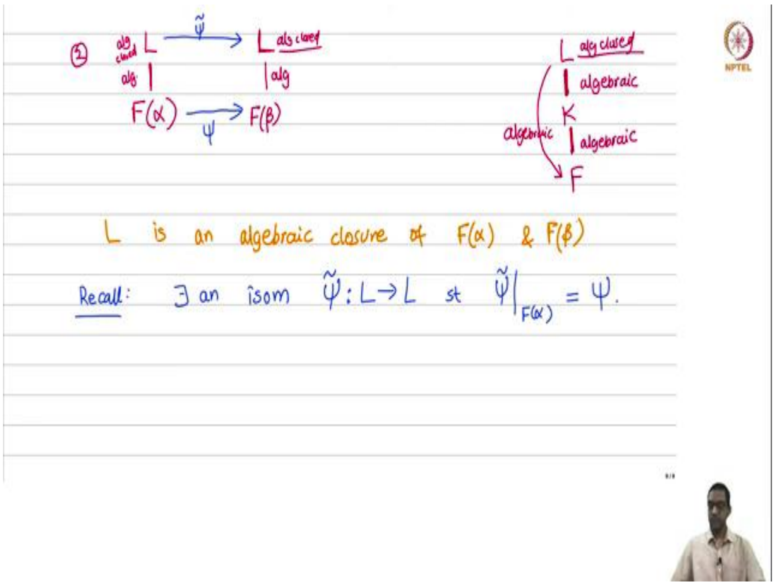
Now, so what do we know? Well, let us do the following, meaning we are trying to do this. We are trying to construct an a map, which takes alpha to beta. So, let us do the following for the moment, let us let us forget about K here. So, I have L, I have F and in between them, I am going to look at the intermediate field F adjoined alpha, this is a subfield of K. So, recall that alpha and beta are elements of K here. So instead of looking at all of K, I will look at a certain subfield which is F of alpha.

Now let us do the same thing on the other side with beta in place of alpha, you look at F beta and I look at L. So, I look at these two extensions. Now, recall the following facts, again the same argument which we have seen before. So, recall, F alpha and F beta are actually isomorphic fields, there exists an isomorphism of fields isomorphism, they call it psi from F alpha to F beta such that with the following properties, psi restricted F is just the identity map on F and psi takes alpha to beta.

So, you have seen this before, and why this, why does there exists a map like this? Well, abstractly, because both F alpha and F beta, you can think of both of them as being given by well it is a symbolic adjunction. So, you think of F adjoined x, modulo the minimal polynomial, and now both alpha and beta have the same minimal polynomial, which is m alpha of x, because F alpha is this, but then well, that is, that is really the same as the minimal polynomial of alpha and beta are the same, the same polynomial F alpha of x.

So, you should think of this as also m beta of x. That is like F beta. So, this map if you just unravel this, this chain of maps what it gives you is a map from F to F, I mean a map from F alpha to F beta, which is identity on F and which takes alpha to beta So I am just recalling things you have seen before. So at least we have constructed sort of a map which has the property we want, which takes alpha to beta, but now recall a second fact.

(Refer Slide Time: 15:16)



②
$$\begin{tikzcd} \text{alg closed } L \arrow[r, "\tilde{\psi}"] & L \text{ alg closed} \\ F(\alpha) \arrow[u, dash, "\text{alg}"] \arrow[r, "\psi"'] & F(\beta) \arrow[u, dash, "\text{alg}"'] \end{tikzcd}$$

$$\begin{tikzcd} L \text{ alg closed} \arrow[d, dash, "\text{algebraic}"] \arrow[dd, bend right, "\text{algebraic}"'] \\ K \arrow[d, dash, "\text{algebraic}"] \\ F \end{tikzcd}$$

L is an algebraic closure of $F(\alpha)$ & $F(\beta)$

Recall: $\exists$ an isom $\tilde{\psi}: L \to L$ st $\tilde{\psi}|_{F(\alpha)} = \psi$.

So we need to recall a second fact here, which is when you have maps. So, observe that L is also the algebraic closure of F alpha. It was the algebraic closure of K, but it is actually also the algebraic closure of F alpha. Why is that? Because it is algebraic over, what is an algebraic closure? It is an algebraically closed field, which is an algebraic extension of the field you are looking for. So here, this is an algebraic extension and L is algebraically closed. This is what an algebraic closure is.

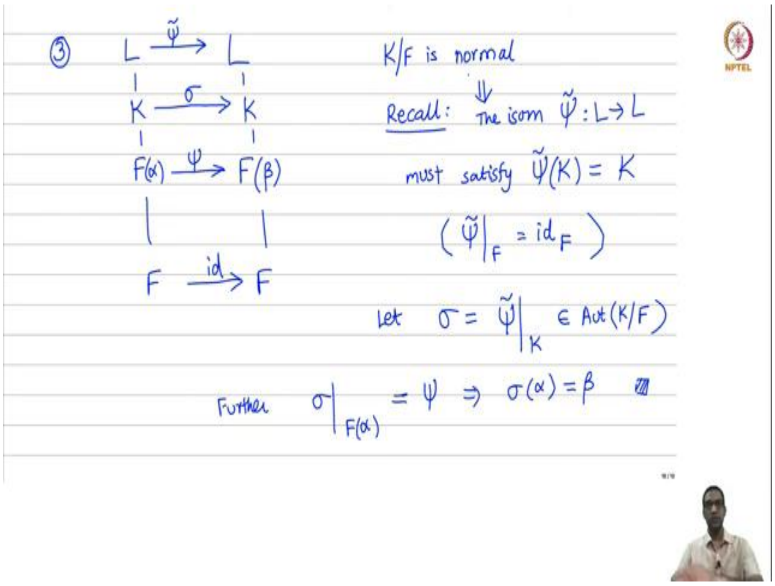
And why is L over F alpha algebraic? Well, L is in fact, algebraic over the base field F itself. So, recall, the original thing I had L, K, F. K over F, I had assumed to begin with was algebraic. L over K, well, L is an algebraic closure of K. So, in particular, L over K is an algebraic extension, L remember is algebraically closed. Now, a tower of algebraic extensions, algebraic over algebraic gives me something that is algebraic. So, this overall extension here is algebraic. So it is, in fact, an algebraic extension of F, so in particular, it is an algebraic extension of F alpha.

So, it involves sort of putting together many of these ideas that keep reoccurring in this business. So now again, F beta for the same reason, L is an algebraic extension of the base field F. So, in particular, it is an algebraic extension of the field F alpha. And L is an algebraically closed field on its own, so L is therefore the algebraic closure of F beta. So, what is the summary of this argument, it says that L is the or a if you wish, an algebraic closure of both F alpha and F beta.

And now the fact to recall is that if I have two fields, which are isomorphic to each other, so there exists an isomorphism between them, then there is a way to lift this isomorphism to an isomorphism of their algebraic closures. So, if the base fields are isomorphic, their algebraic closures are also isomorphic. But a little more than that, if you have a certain, given any isomorphism psi between the base fields, it extends or lifts to an isomorphism between their algebraic closures.

So, this is again, something you have seen before. So, recall the following fact, there exists an isomorphism of fields psi tilde from L to L, such that when you restrict psi tilde to the field F alpha, what you get is the original isomorphism psi. So where does this leave us? We are almost where we want to be.

(Refer Slide Time: 18:29)



③

$$\begin{tikzcd}
L \arrow[r, "\tilde{\psi}"] \arrow[d, dash] & L \arrow[d, dash] \\
K \arrow[r, "\sigma"] \arrow[d, dash] & K \arrow[d, dash] \\
F(\alpha) \arrow[r, "\psi"] \arrow[d, dash] & F(\beta) \arrow[d, dash] \\
F \arrow[r, "id"] & F
\end{tikzcd}$$

K/F is normal

$\Downarrow$

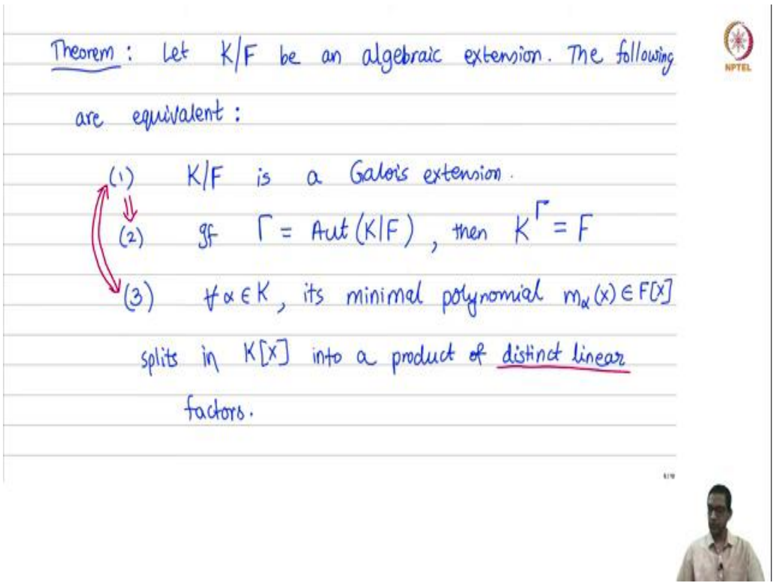
<u>Recall:</u> The isom $\tilde{\psi}: L \to L$

must satisfy $\tilde{\psi}(K) = K$

$(\tilde{\psi}|_F = id_F)$

Let $\sigma = \tilde{\psi}|_K \in Aut(K/F)$

Further $\sigma|_{F(\alpha)} = \psi \Rightarrow \sigma(\alpha) = \beta$ ▨



Theorem: Let K/F be an algebraic extension. The following are equivalent:

(1) K/F is a Galois extension.

(2) If $\Gamma = \mathrm{Aut}(K|F)$, then $K^{\Gamma} = F$

(3) $\forall \alpha \in K$, its minimal polynomial $m_\alpha(x) \in F[x]$ splits in $K[x]$ into a product of distinct linear factors.

So now it is time to put the field K back into the picture. So, we had the following. So, I have a map from L to L, which is psi tilde. This map has the following property when I restrict it to F, it just gives me back well, in fact, if I restrict it to F alpha, let us also put F alpha, it gives me psi, in psi remember when you restricted it to F, gave you identity. So, we have this. And now of course between F alpha and L, you got K, similarly between F as beta and L you have K. So, this contains both F alpha and F beta.

And now, recall, the K is normal. So far, we have not used the normality of K. So, K over F is a normal extension. So, we have only used so far, the fact that it is separable, because we said m alpha has, it must have distinct roots. So, if alpha is one of its roots, then there must be a different root beta, that is all we have used so far. Normality has not been used yet. And now it comes into play.

So, what do we know, if you recall what a normal (extension), one of the equivalent properties of a normal extension was, we proved that if K over F is normal, then any automorphism of the algebraic closure of K, any map psi tilde which restricts to identity on F must send K to K. So, recall from our lecture on normal extensions, this means recall the K over F is normal means the isomorphism psi tilde must satisfy the following property, that it must map K back to itself. It cannot send elements of K to elements which are not in K.

So, psi tilde map psi tilde of K is exactly K. And this is, to prove this, you need to know that psi tilde restricted to F is the identity. That is what makes this work, if you go back and look at the theorem for normal extensions. So, the K over F is normal means that any F automorphism of L must in fact preserve K. So, in other words, when you restrict psi tilde to

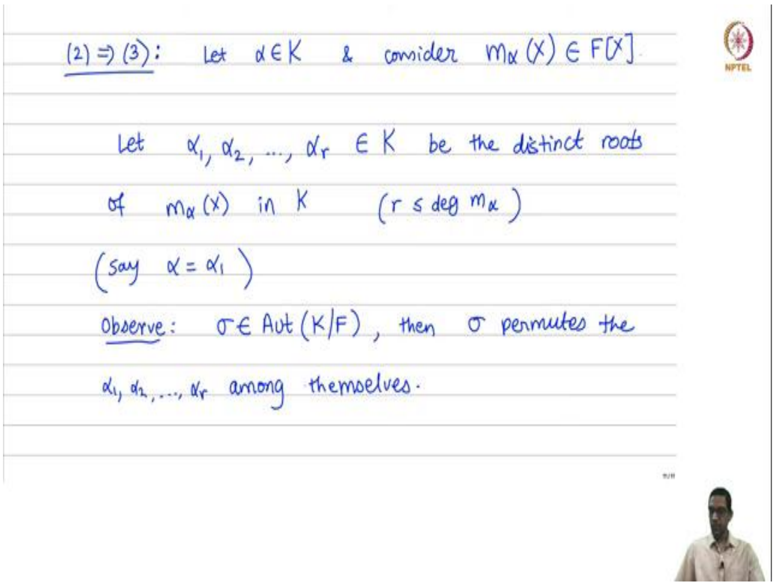
K, what you get is in fact a map which send K to itself. So, let us call this map as sigma. So, let sigma denote the restriction of psi tilde to K.

Now, what is this? Sigma therefore, is a map, it is an automorphism of K, which is identity on F, so it is an element of Aut K over F. Further what property does sigma have? Well, sigma when you restrict it to F alpha is the same as the original map psi. So, sigma when you restrict it to F alpha was the map psi. This means that, in particular, sigma must map alpha to beta. And that concludes the proof, because that is exactly what we were trying to construct an automorphism of K, an F automorphism of K which sends alpha to beta.

And notice that we have used many of the properties that we have studied until now. So, we sort of pass to the algebraic closure, we use this general theorem which says you can always lift maps between, you lift isomorphism of base fields to isomorphisms of their algebraic closures. And then you sort of descend to K again, by using the normality, isomorphisms, F isomorphisms of the algebraic closures must preserve the normal extensions, they must map K back to itself.

So slightly long-winded proof, but sort of a beautiful application of all the various ideas we have seen so far. So, let us see where we are. So, what is it that we needed to do? We needed to prove, so we said already that 1 and 3 are the same. So, we have now shown that 1 is the same, well, 1 implies 2, we have said 1 and 3 are the same. So, we just need to show that 2 implies 1, or which is the same thing 2 implies 3. That is all we need to show. So, let us prove that. So, let us try and show that 2 implies 3. So that is the last part of our proof.

(Refer Slide Time: 23:15)



(2) ⇒ (3): Let $\alpha \in K$ & consider $m_\alpha(X) \in F[X]$

Let $\alpha_1, \alpha_2, \ldots, \alpha_r \in K$ be the distinct roots of $m_\alpha(X)$ in K $(r \leq \deg m_\alpha)$

(say $\alpha = \alpha_1$)

Observe: $\sigma \in \mathrm{Aut}(K/F)$, then σ permutes the $\alpha_1, \alpha_2, \ldots, \alpha_r$ among themselves.

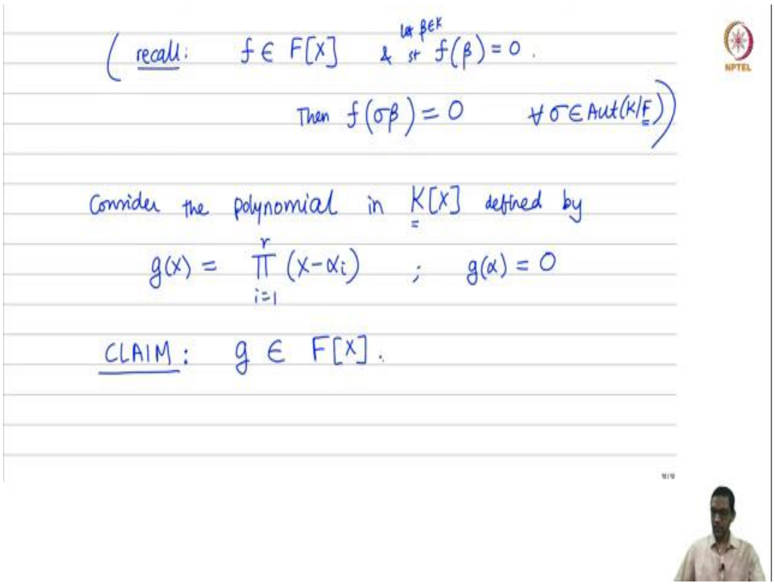
So, what do we need to do? We are going to assume that the fixed field of gamma is exactly F and using that we are going to show that every m alpha of x splits into a product of distinct linear factors. So, let alpha be an element of K. And consider its minimal irreducible polynomial m alpha of x. So, we need to show that this is going to be an element, it is going to be a product of distinct linear factors in K.

Now, let us do the following. Let, so observe at the moment, we know almost nothing about the extension. We do not, we have just assumed something strange about the fixed field of the automorphism, that is all. We do not even know for example, that m alpha of x has any other root other than alpha in the extension K. We do not know that it splits, we do not know that, it is separable. If it splits, does it have distinct roots, we know nothing about m alpha really. So, it may not even have any other roots other than alpha, for all you know, so but anyway, let us write those roots down.

Let, it has some number of roots alpha 1, alpha 2, alpha r, belonging to K be the distinct roots. Let these be the distinct roots of this polynomial m alpha of x in K. So, observe r is at most the degree of m alpha, we do not know that it has now exactly the degree number of roots, it probably has fewer. Also, the first root, definitely it has one root which is alpha definitely. So, let us again say that the first guy is alpha. Let us call, let us assume that alpha 1 is your alpha.

Now, the key observation, so, how do we bring in the automorphisms? Observe the following fact, that if I take an automorphism sigma of K over F, then sigma permutes the alpha i's among themselves. When I say alpha i, I mean permutes this set of roots alpha 1, alpha 2, alpha r among themselves.

(Refer Slide Time: 26:00)



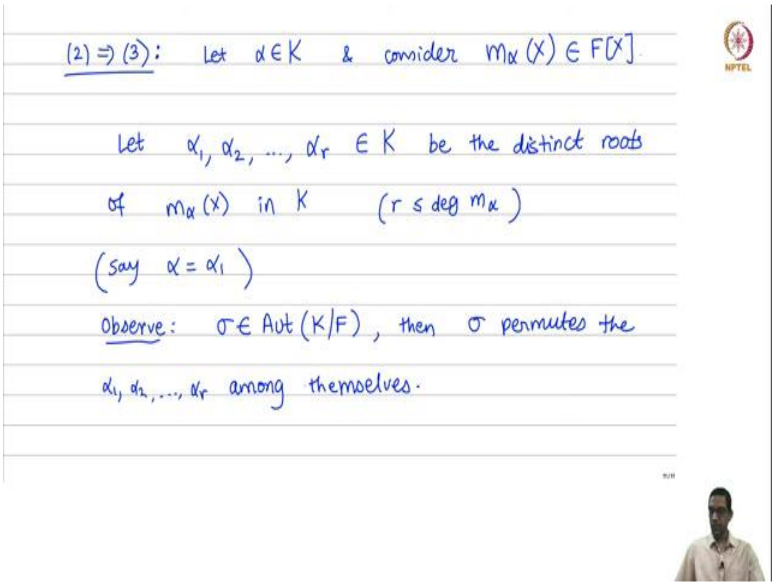
(recall: $f \in F[X]$ & let $\beta \in K$ st $f(\beta) = 0$.

Then $f(\sigma\beta) = 0$ $\forall \sigma \in Aut(K/F)$)

Consider the polynomial in $K[X]$ defined by

$$g(x) = \prod_{i=1}^{r} (x - \alpha_i) \quad ; \quad g(\alpha) = 0$$

CLAIM: $g \in F[X]$.



(2) ⇒ (3): Let $\alpha \in K$ & consider $m_\alpha(x) \in F[X]$

Let $\alpha_1, \alpha_2, \dots, \alpha_r \in K$ be the distinct roots of $m_\alpha(x)$ in K ($r \leq \deg m_\alpha$)

(say $\alpha = \alpha_1$)

Observe: $\sigma \in Aut(K/F)$, then σ permutes the $\alpha_1, \alpha_2, \dots, \alpha_r$ among themselves.

Why is this? Again, something that you have seen before, if in general when I have a polynomial. So, recall this fact again, if I have a polynomial coefficients in F, and let us say f of some beta is 0. So, let beta be a root, some beta. So maybe I should write it as let beta be an element of K, such that f beta is 0, then if I look at sigma beta, which is, say what is sigma here? Sigma is an automorphism of K over F.

So, if I take any sigma and automorphism, and look at sigma beta, then sigma beta is also root of the same polynomial. And we proved this, all you have to do is just write the polynomial F out and apply sigma to it, just look at f beta 0, you apply sigma to the equation, the coefficients will not change, because sigma fixes the field F, you have assumed sigma as an automorphism of K over F.

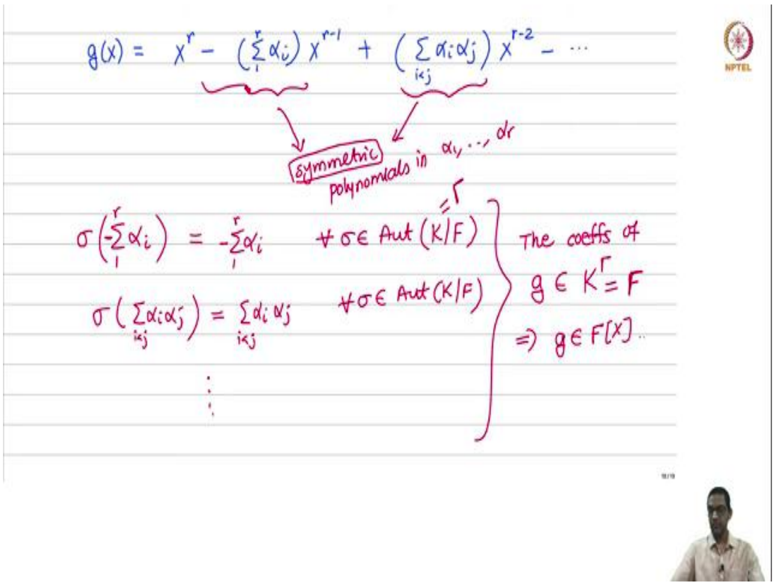
So, sigma fixes the coefficients, the beta powers will all become now sigma, powers of sigma beta instead, and that will show that f of sigma beta as well. Now in other words, if beta is the root of f, then sigma beta is also root of f, therefore, sigma must permute the roots of f. That is exactly the fact we are looking at here. So, we know for sure that sigma must permute the alpha 1 through alpha r among themselves.

So now let us do the following. Let us consider the polynomial in Kx, it is now got coefficients in K, define by the following define by, we can call it g of x is just the product of the x minus alpha i's, i goes from 1 to r. Observe this is not necessarily the same as m alpha of x because m alpha of x may not factor completely, it may have some higher degree irreducible factors and so on. gx is only the product of the distinct linear factors which occur inside m alpha of x.

So, it is a priori, something sort of smaller than m alpha. So, one thing we know for sure is, of course, that alpha is equal to alpha 1. So, g, certainly alpha is certainly a root of g. Now, here is the very surprising claim, in some sense, that well, at the moment, g only has coefficients in K. We cannot say anything more than that, because the alpha i's are only elements of K.

But the claim is g actually has coefficients in F. Even though it does not look like it, it actually has coefficients in F. And to prove that we are going to use our hypothesis that the fixed field of the set of automorphisms is exactly F. So, let us prove this. So, what are the coefficients of g? So, let us expand g out and see what the coefficients look like.

(Refer Slide Time: 29:27)



$$g(x) = x^r - \underbrace{\left(\sum_1^r \alpha_i\right)} x^{r-1} + \underbrace{\left(\sum_{i<j} \alpha_i\alpha_j\right)} x^{r-2} - \cdots$$

$\boxed{\text{symmetric}}$ polynomials in $\alpha_1, \ldots, \alpha_r$

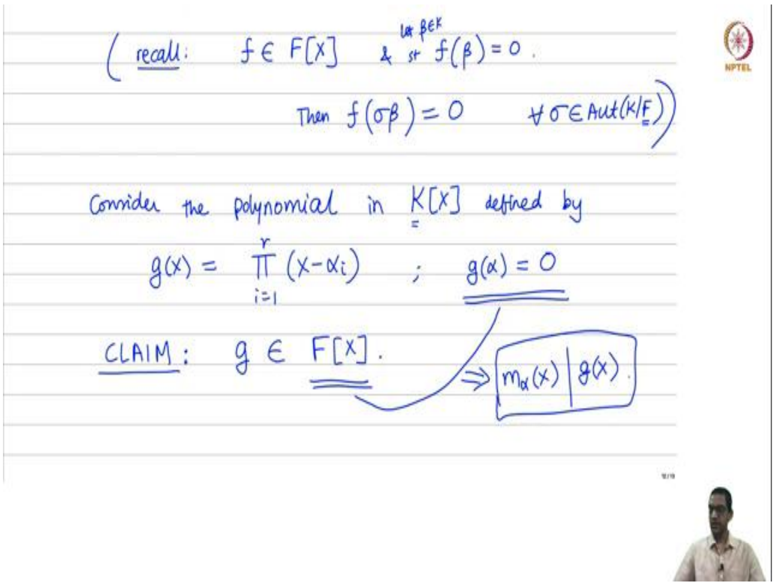
$$\sigma\left(-\sum_1^r \alpha_i\right) = -\sum_1^r \alpha_i \quad \forall \sigma \in \overset{\Gamma}{\overset{\shortparallel}{\mathrm{Aut}(K/F)}}$$

$$\sigma\left(\sum_{i<j} \alpha_i\alpha_j\right) = \sum_{i<j} \alpha_i\alpha_j \quad \forall \sigma \in \mathrm{Aut}(K/F)$$

$\vdots$

The coeffs of $g \in K^\Gamma = F$

$\Rightarrow g \in F[x]$ ..



($\underline{\text{recall}}$: $f \in F[X]$ & $\overset{\text{let } \beta \in K}{\text{st}}$ $f(\beta) = 0$.

Then $f(\sigma\beta) = 0$ $\forall \sigma \in Aut(K/\underline{F})$)

Consider the polynomial in $\underline{K}[X]$ defined by

$$g(x) = \prod_{i=1}^{r} (x - \alpha_i) \quad ; \quad \underline{g(\alpha) = 0}$$

$\underline{\text{CLAIM}}$: $g \in \underline{F[X]}$. $\Rightarrow \boxed{m_\alpha(x) \mid g(x)}$

So, gx now looks like x power r minus summation of all the alpha i's alpha i alpha j x to the r minus 2 and so on, so this is overall i less than j. So, recall this is how one expands polynomial and these coefficients here are exactly the various elementary symmetric functions if you wish. So, these fellows are all symmetric functions of the roots, symmetric polynomials if you wish or symmetric functions.

They are symmetric polynomials in the alphas. In other words, when you permute, the alphas, these things do not change, these coefficients do not change. And in fact, they are what are called the elementary symmetric functions, if you know what they are. But for us, the key word here is symmetric, that these coefficients do not change if you permute the alphas among themselves.

Now, what does that mean? It says that, if, for example, let us take the first coefficient summation alpha i here, if I apply any one of the sigma's, any automorphism sigma of belonging to K over F, then, sigma only permutes the alphas among themselves. So, this will give me the same answer for every alpha. So, for every sigma in automorphisms of K over F.

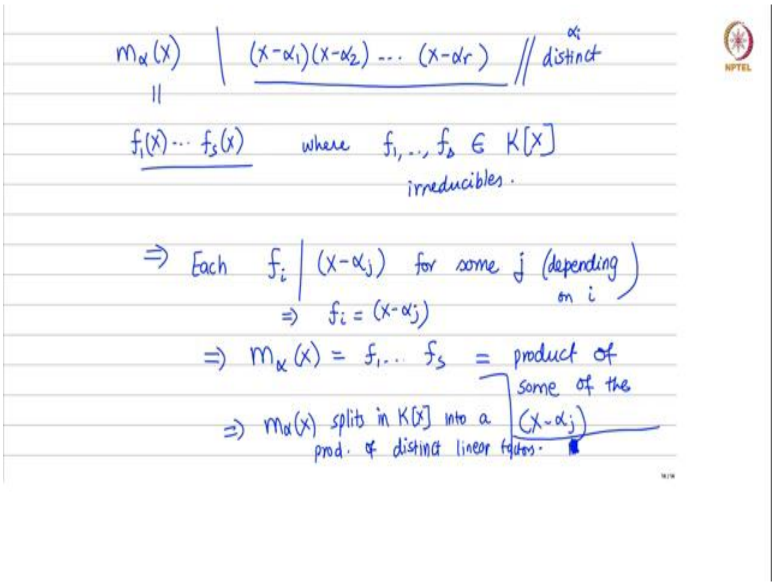
Similarly, if I take the second coefficient, so in first coefficient has a minus in front, the second coefficient does not. So, these are all twofold products, the alphas, just gives me back alpha i alpha j. Why? Because the only possible action of sigma is to permute the alphas, it will map each alpha i to some other alpha j. But then this final combination remains the same. This is again true for all sigma in Aut of K over F. So, what does that imply? Well, and so on, so you can see this is true for all the coefficients.

So that means that the coefficients, so the coefficients of g, therefore, all belong to K gamma, remember gamma is the Aut KF. It belongs to the fixed field of the group of automorphisms, F automorphisms of K. But the assumption, the hypothesis we started out with is that the fixed field of, the fixed field K gamma is exactly F, it is the base field. So that proves what we want. So, therefore, the coefficients of g are in fact in the base field.

Why is that? Because, well they are really symmetric functions of the roots and automorphisms necessarily permute the roots. Now, why is that useful? Because, if you look at g here, so, we have shown that g is a polynomial in FX, and g is a polynomial on which alpha vanishes. So, what does this mean?

These two things imply that m alpha of x, remember m alpha is the minimal irreducible polynomial, I mean, it is the minimal degree polynomial in FX, which has alpha as a root. Now, g is another candidate polynomial, it is another polynomial which has alpha as a root, then this just means that m alpha of x must divide g of x. The minimal polynomial always divides any other polynomial of in FX, which has alpha as a root. Now, why is that, what we want? Well, let us just analyze this a little bit.

(Refer Slide Time: 33:29)



$m_\alpha(x) \mid \underline{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)}$ // α_i distinct

$\parallel$

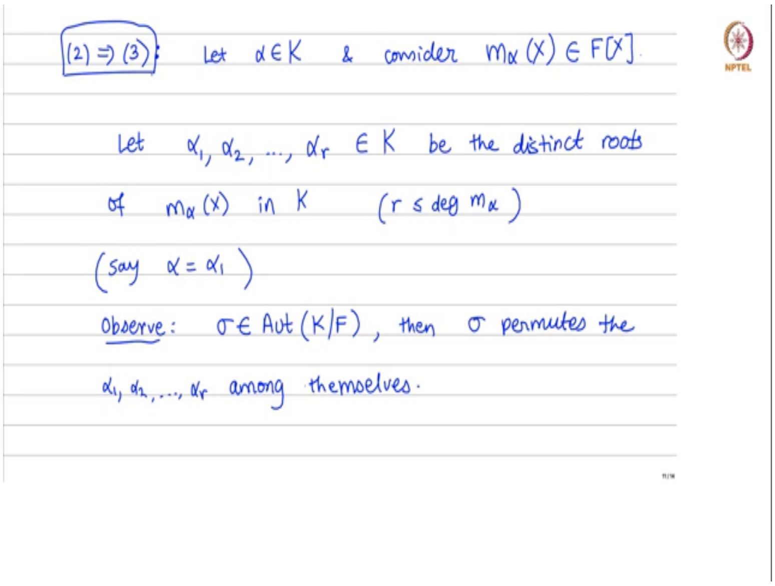
$\underline{f_1(x)\cdots f_s(x)}$ where $f_1,\ldots,f_s \in K[x]$ irreducibles.

$\Rightarrow$ Each $f_i \mid (x-\alpha_j)$ for some j (depending on i)

$\Rightarrow f_i = (x-\alpha_j)$

$\Rightarrow m_\alpha(x) = f_1 \ldots f_s$ = product of some of the $(x-\alpha_j)$

$\Rightarrow m_\alpha(x)$ splits in $K[x]$ into a prod. of distinct linear factors.



$\boxed{(2) \Rightarrow (3)}$: Let $\alpha \in K$ & consider $m_\alpha(x) \in F[x]$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_r \in K$ be the distinct roots of $m_\alpha(x)$ in K $(r \leq \deg m_\alpha)$

(say $\alpha = \alpha_1$)

Observe: $\sigma \in \mathrm{Aut}(K/F)$, then σ permutes the $\alpha_1, \alpha_2, \ldots, \alpha_r$ among themselves.

So, if you look at m alpha of x on the one hand, and g of x on the other, g of x is just the product. So, what is this? So, let us write gx out, this is now x minus alpha 1 x minus alpha 2. So, observe g is now a product of distinct linear factors and m alpha of x divide such a product. Now, so let us write this m alpha of x, say a product of irreducible, f1 of x, f2 of x, some fs of x, where f1, f2, fs are polynomials in Kx, which are all irreducible. So, I have factorized m alpha into a product of irreducible in Kx.

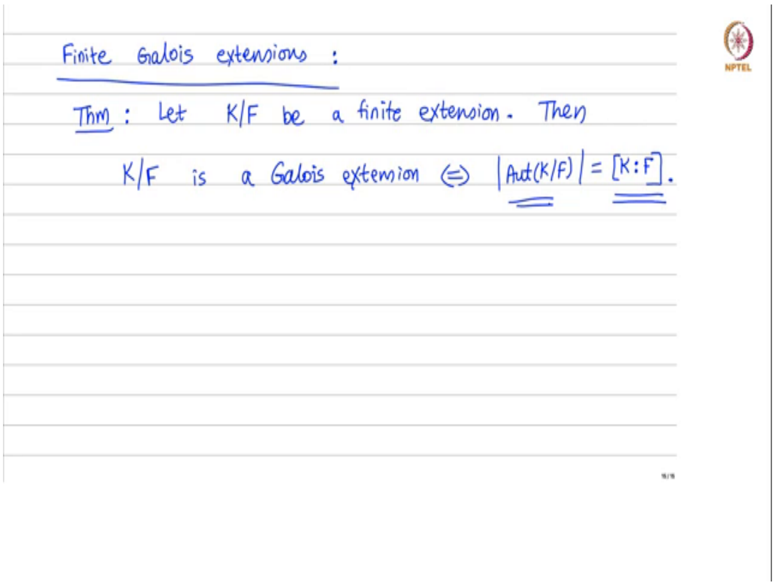
And this product of irreducibles divides this product of irreducibles, it divides the product of the linear factors. This means that each fi, so each irreducible. So, look at any given fi, it divides the product of the x, x minus alpha j's, that means, it must, well it must divide at least one of those factors. So, each fi had, has to divide at least one of the x minus alpha j for some j, some j depending on i of course. So, each fi will potentially divide a different x minus alpha j depending on i.

So, what does this mean? Well, this means that if you write out m alpha of x, which is a product, well fi is irreducible. And x minus alpha j is also irreducible a linear term. This just means that fi has to equal x minus alpha j, there is no other way out. This x minus alpha j is not divisible by any other irreducible. So, this means that m alpha of x, which is the product of f1, f2, fs, is therefore the product of terms of the form x minus alpha j. It is a product of some of the x minus alpha j's.

Some of the terms x minus alpha j, may not be all of them, only s of them are involved say. So, it is a product of some of these x minus alpha j's, but then that is exactly what we care about. This means, in particular, that m alpha of x splits in Kx into a product of distinct linear factors. Because to begin with, all these terms here are all distinct. The alpha i is remember that distinct to begin with. So, it splits in Kx into a product of distinct linear factors. And that is exactly what needed to prove.

So that that that completes the proof here. I mean, this is really 2 implies 3. So that is what we set out to prove. So, we wanted to show that each m alpha of x splits as a product of distinct linear factors. So that is somewhat interesting argument again. So, we start with what looks a priori, like a strange assumption, or at least a weaker assumption that the automorphism group F automorphisms of K has F as its fixed field. And that is actually enough to show that the extension is both normal and separable. So rather remarkable statement.

(Refer Slide Time: 37:15)



Finite Galois extensions :

Thm : Let K/F be a finite extension. Then

K/F is a Galois extension $\iff$ $|\underline{\underline{\mathrm{Aut}}}(K/F)| = [\underline{\underline{K:F}}]$.

And let us just quickly end with this remark about finite Galois extensions. So, far everything we have said works in general, could be infinite, as well. But here is a little theorem well, rather important theorem that we will prove, so that K over F be a finite extension, be a finite extension, observe finite extension automatically means algebraic. Then, here is yet another characterization, then K over F is a Galois extension if and only if the following holds; if and only if the cardinality of the automorphism group is the same as the degree of the extension.

So, this is a yet another criterion for when an extension is Galois. And again, it is a completely new sort of criterion you wish in terms of the degree of the extension. So, it says that the extension degree should be exactly equal to the number of automorphisms that are available, that are there. And so, to prove this requires, some more ideas and so we will take a short detour through the notions of linear independence of characters and theorem of (()) (38:48) and so on to and then come back and prove this statement.