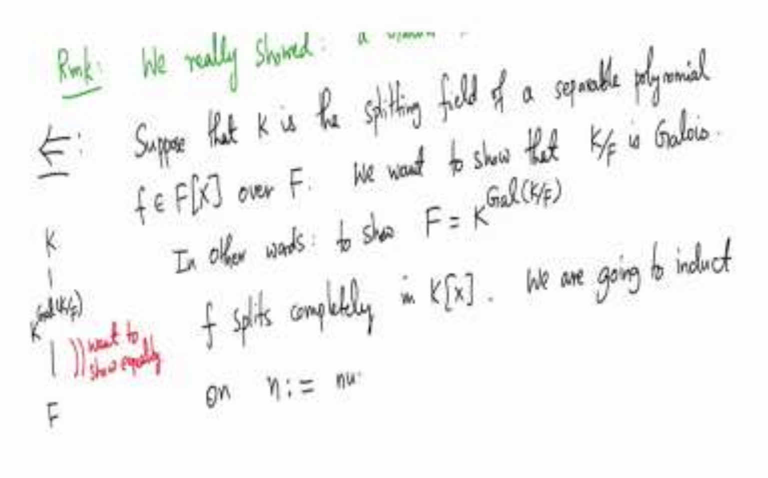
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture – 21
Characterization of Galois Extensions – Part 2

Welcome back, we are in the middle of proving this theorem about Galois extensions. We are trying to show that an extension is Galois if and only if it is a splitting field of a separable polynomial. And as I told you last time, this is a very convenient way of verifying if a given extension is Galois or not.

And we proved in the last video one direction of this. So, we assume that K over F is Galois and using some tricky involved arguments but still not very difficult but lengthy arguments, we showed that K is indeed the splitting field of a separable polynomial. In fact, in the process we really showed that Galois extension is always normal and always separable.

(Refer Slide Time: 1:05)



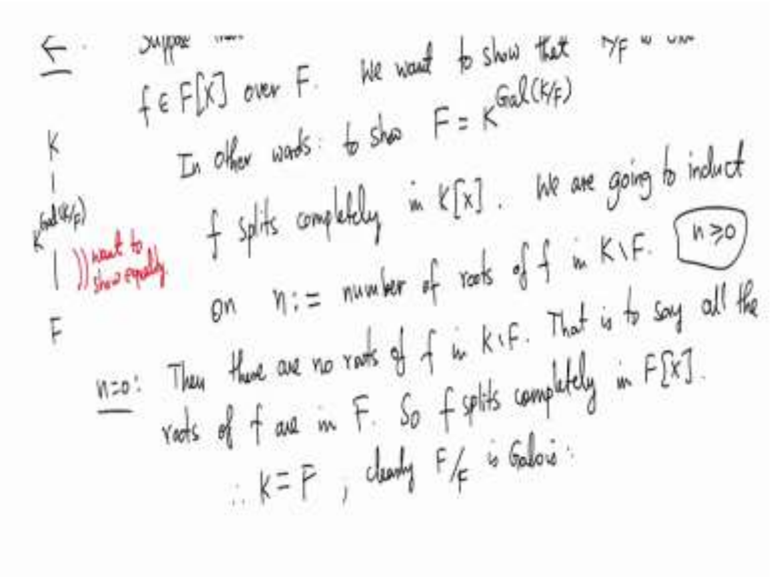
Rmk: We really showed: a [illegible]

$\Leftarrow$: Suppose that K is the splitting field of a separable polynomial $f \in F[X]$ over F. We want to show that K/F is Galois.

In other words: to show $F = K^{Gal(K/F)}$

f splits completely in $K[x]$. We are going to induct on $n :=$ nu

$$\begin{tikzcd} K \arrow[d, dash] \\ K^{Gal(K/F)} \arrow[d, dash, "\text{want to show equality}"] \\ F \end{tikzcd}$$



$\Leftarrow$: Suppose that ... We want to show that K/F is ...

$f \in F[X]$ over F.

In other words: to show $F = K^{Gal(K/F)}$

f splits completely in $K[x]$. We are going to induct on $n :=$ number of roots of f in $K \setminus F$. $\boxed{n \geq 0}$

K

$|$

$K^{Gal(K/F)}$

$|$ want to show equality

F

$\underline{n=0}$: Then there are no roots of f in $K \setminus F$. That is to say all the roots of f are in F. So f splits completely in $F[x]$.

$\therefore K = F$, clearly F/F is Galois.

So, now in this video we are going to prove the converse. So, I am going to assume that K is the splitting field of separable polynomial. K is the splitting field of a separable polynomial in capital FX. Let us call that polynomial f and it is of course splitting field over Capital F. So, what we have is K and F. And F is a polynomial in the base field and K is the splitting field. So, we want to show that K over F is Galois.

In other words, the definition of Galois extensions is that, to show F is equal to K power Galois K over F. So, you always know that K power Galois, K over F is an intermediate field for the given extension and our goal is to show this. We want to show equality of this. And we are going to induct on a strange number, so let me explain that.

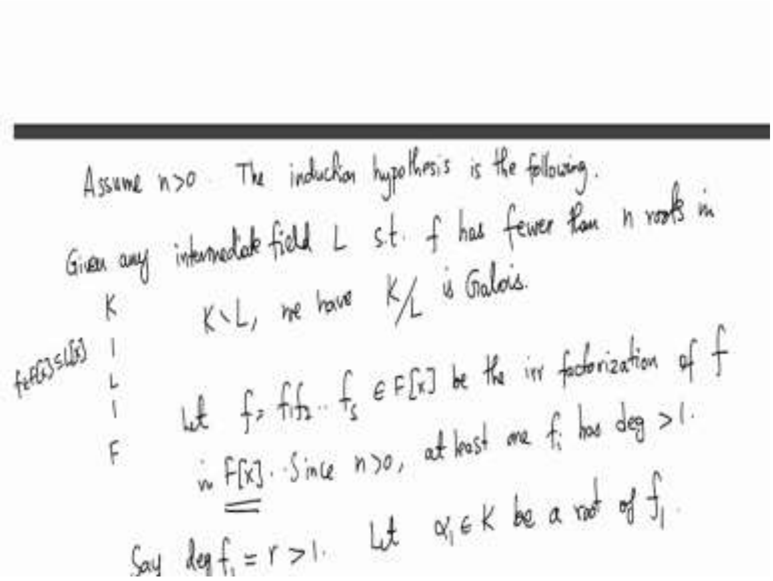
So, first we note that, of course, F splits completely in K, which used to say F can be written as a product of linear polynomials in KX, so all the roots of F is in K but we are going to induct on this number, which I will denote by n, it is a number of roots of f in K minus F. So, that gives a strange number to induct on, but this is what we will do. Just motivate what this number is and do also the base case, let us take n to be 0.

So, n of course is a non-negativity integers because it is a number of roots. So, if n is 0, then there are no roots of f in K minus F, because number of roots of f in K minus F is n and that is 0. But that is to say, all the roots of f are in K, sorry are in F. Remember all the roots of f are in K for sure because K is the splitting field.

But none of them are in K minus F that means they all are in F. So, F splits completely in FX itself because if it splits completely, if it is all the roots, then it will split completely. So, K must be equal to F, right? Because K is the splitting field of the polynomial and if the polynomial splits completely over the base field, splitting field is the base field and obviously, I am not sure, I said this explicitly before, but this extension is Galois.

An extension or trivial extension is always Galois because the Galois group is identity group, fixed field is that. So, various ways of clarifying this, the degree is 1, the Galois group cardinality is also 1.

(Refer Slide Time: 5:00)



Assume $n>0$. The induction hypothesis is the following.

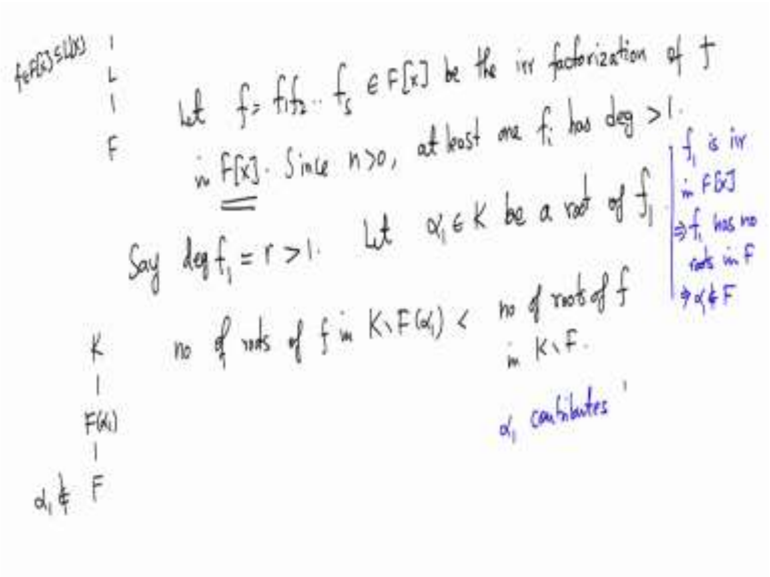
Given any intermediate field L s.t. f has fewer than n roots in $K \setminus L$, we have K/L is Galois.

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

$f \in F[x] \subseteq L[x]$

Let $f = f_1 f_2 \cdots f_s \in F[x]$ be the irr factorization of f in $\underline{\underline{F[x]}}$. Since $n>0$, at least one f_i has $\deg > 1$.

Say $\deg f_1 = r > 1$. Let $\alpha_1 \in K$ be a root of f_1.



$f \in F[x] \subseteq L[x]$

Let $f = f_1 f_2 \cdots f_s \in F[x]$ be the irr factorization of f in $\underline{\underline{F[x]}}$. Since $n>0$, at least one f_i has $\deg > 1$.

Say $\deg f_1 = r > 1$. Let $\alpha_1 \in K$ be a root of f_1.

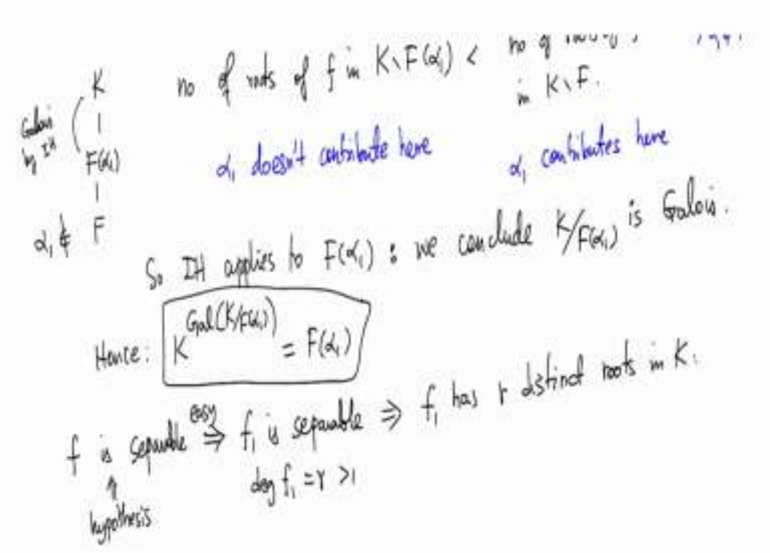
f_1 is irr in $F[x]$ $\Rightarrow f_1$ has no roots in F $\Rightarrow \alpha_1 \notin F$

no of roots of f in $K \setminus F(\alpha_1)$ < no of roots of f in $K \setminus F$.

α_1 contributes '

$$\begin{tikzcd} K \arrow[d, dash] \\ F(\alpha_1) \arrow[d, dash] \\ F \end{tikzcd}$$

$\alpha_1 \notin F$



K | $F(\alpha_1)$ | F — Galois by IH; $\alpha_1 \notin F$

no of rots of f in $K\setminus F(\alpha_1)$ < no of in $K \setminus F$.

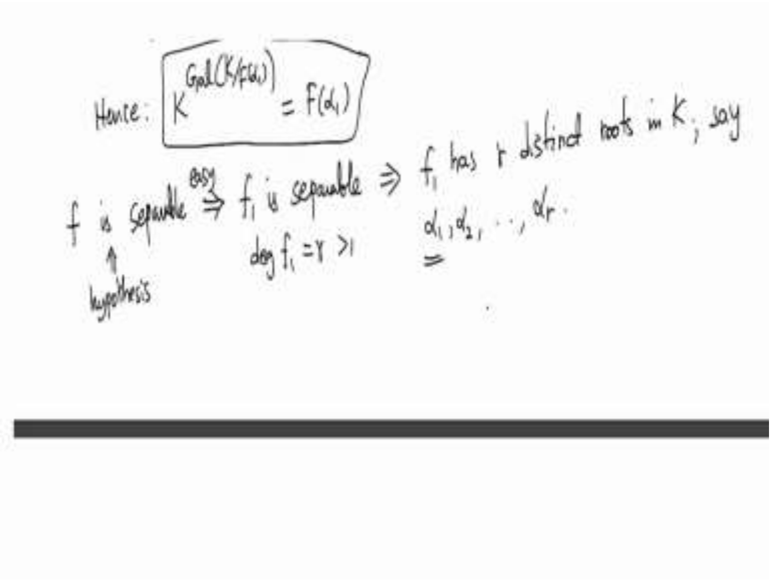
α_1 doesn't contribute here — α_1 contributes here

So IH applies to $F(\alpha_1)$: we conclude $K/F(\alpha_1)$ is Galois.

Hence: $\boxed{K^{Gal(K/F(\alpha_1))} = F(\alpha_1)}$

f is separable $\overset{easy}{\Rightarrow}$ f_1 is separable $\Rightarrow$ f_1 has r distinct roots in K.

↑ hypothesis — $\deg f_1 = r > 1$



Hence: $\boxed{K^{Gal(K/F(\alpha_1))} = F(\alpha_1)}$

f is separable $\overset{easy}{\Rightarrow}$ f_1 is separable $\Rightarrow$ f_1 has r distinct roots in K, say $\alpha_1, \alpha_2, \ldots, \alpha_r$. $\Rightarrow$

↑ hypothesis — $\deg f_1 = r > 1$

So, assume now, n is positive. And I am not going to explicitly write down what the induction hypothesis is, the induction hypothesis is the following. What is the induction hypothesis? It has the following… So, given any intermediate field L, that means we have K, F, K over F is the given extension, L is the intermediate field such that f has fewer than n roots in K minus L, we have K over L is Galois.

So, this is the induction hypothesis. Remember that, the original hypothesis is K over F is a splitting field of a separable polynomial namely F. That hypothesis also holds K over L because, f is in FX which is of course in LX. So, F is a polynomial over L and K will of course remain splitting field of F over L also. And if it happens that, the number of roots in K of f that are not in L is fewer than, that means strictly less than n, then that is Galois.

So, that we will assume. So, to proceed with the proof, let f equal to f1 times, f2 times, fs be the irreducible factorisation of small f in FX. We are given this polynomial f, it may very well not be irreducible so we can take its factorisation remember, this is in FX. Since, n is positive that means I does not split completely in F, at least 1 fi has degree strictly more than 1 because each Fi is degree 1 that means F splits into the product of linear polynomials which is to say, F splits completely, which means n equal to 0.

So now we are assuming n is not 0 so that means fi is, at least one fi has positive degree. So, we might assume without loss of generality that f1 has degree r, which is strictly more than 1. Now I am going to take, let alpha 1 in k be a root of f1 in K that means alpha 1 is in K. Remember that F splits completely in K that means f1 also splits completely. So, it is all the roots in K. I will take just 1, alpha 1 and now I am interested in this intermediate field.

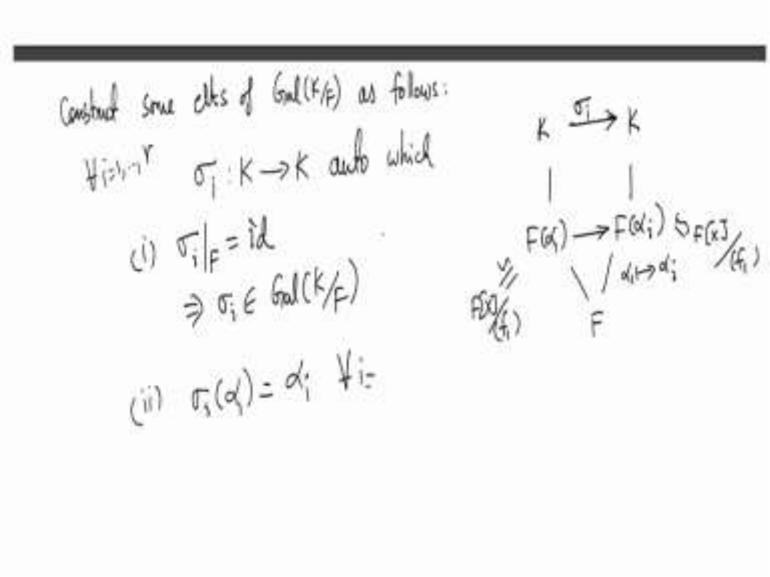
Now I want to note the following, the number of roots of f1 or f rather, in K minus f alpha 1, remember alpha 1 is not here. That is because, f1 is irreducible so I will just remark that here, f1 is irreducible in FX. This implies f1 has no roots in F because if it has the root then it cannot be irreducible. And its degree is positive, that is important. Because the only way, it will have a root and failed to be… and it is irreducible, is degree 1.

So, if the degree is greater than 1 and it has no roots… I mean if it is irreducible degree greater than 1, then it has no roots. So, in particular, alpha 1 is not in f. Now the number of roots of f in K alpha, K minus f alpha 1 is strictly less than number of roots of f in K minus F. This is clear because alpha one contributes to this number, alpha 1 is a root, that is not enough but alpha 1 is in f alpha 1… so alpha 1 does not contribute here. So, alpha 1 is in f alpha 1 so it is not in K minus f alpha 1.

So, the number of root and every other root will remain the same. So, the number of roots in f in K minus f alpha 1 strictly less than, at least 1 less. May be there are others also that are in f alpha 1. But we do not care. So, it is strictly less, so induction hypothesis applies to f alpha 1 and we conclude K alpha 1 is Galois. So, this is Galois by induction hypothesis. So, that is going to be crucial to us, in particular, hence, spelling out the meaning of been Galois, K power Galois K over f alpha 1 is F, alpha 1.

So, we will use this in a minute. So, now what we do know is, F is separable, this is hypothesis. This of course implies that f1 is separable, this is just the definition. If you have a separable, all its factors are separable. This means, degree f1 is of course r, so f1 has r distinct roots in K because F1 splits completely, all its roots are in K because it is separable there are r. Alpha 1 is something that we have already chosen. Alpha 1 is chosen here so alpha 1 is chosen here and the remaining roots are called alpha 2, alpha 3 up to alpha r.

(Refer Slide Time: 12:02)



Construct some elts of $Gal(K/F)$ as follows:

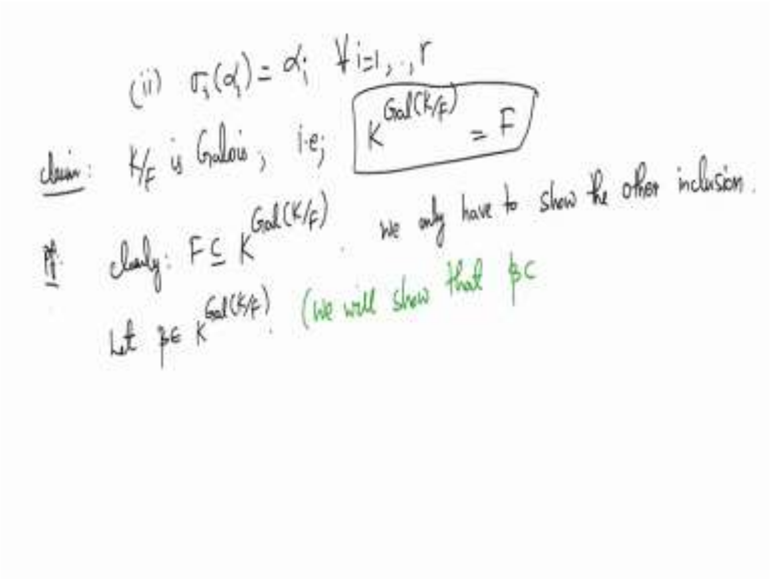
$\forall i=1,..,r$ $\sigma_i : K \to K$ auto which

(i) $\sigma_i|_F = id$

$\Rightarrow \sigma_i \in Gal(K/F)$

(ii) $\sigma_i(\alpha_1) = \alpha_i$ $\forall i=$

$$\begin{tikzcd}
 & K \arrow[r, "\sigma_i"] & K & \\
F[x]/(f_1) \arrow[r, phantom, "\cong"] & F(\alpha_1) \arrow[u, dash] \arrow[r] & F(\alpha_i) \arrow[u, dash] \arrow[r, phantom, "\cong"] & F[x]/(f_1) \\
 & F \arrow[u, dash] \arrow[ur, dash, "\alpha_1 \mapsto \alpha_i"'] & &
\end{tikzcd}$$

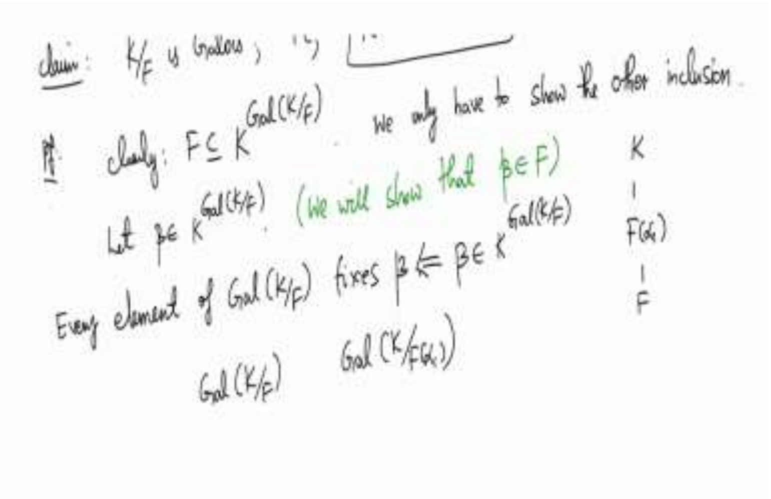


(ii) $\sigma_i(\alpha_1) = \alpha_i$ $\forall i=1,..,r$

claim: K/F is Galois, i.e; $\boxed{K^{Gal(K/F)} = F}$

Pf: clearly: $F \subseteq K^{Gal(K/F)}$. we only have to show the other inclusion.

Let $\beta \in K^{Gal(K/F)}$. (we will show that $\beta \in$



claim: K/F is Galois, i.e.

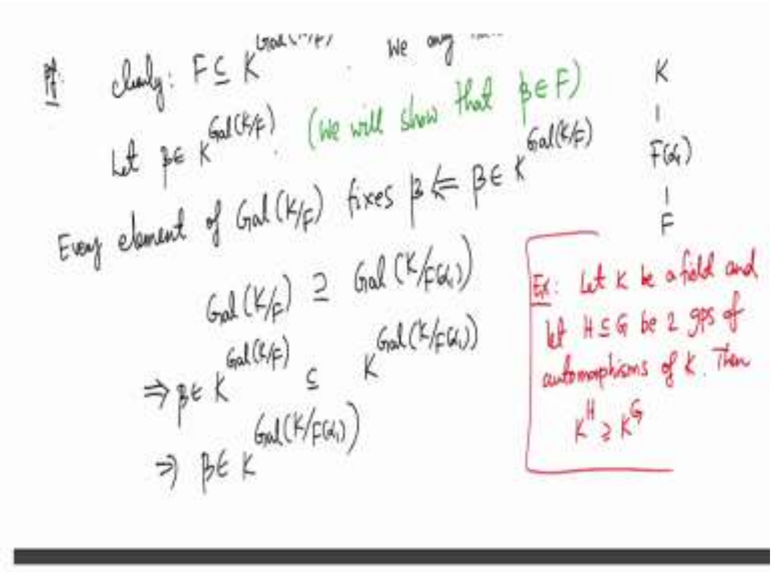
Pf. clearly: $F \subseteq K^{Gal(K/F)}$. We only have to show the other inclusion.

Let $\beta \in K^{Gal(K/F)}$. (We will show that $\beta \in F$)

Every element of $Gal(K/F)$ fixes $\beta \Leftarrow \beta \in K^{Gal(K/F)}$

$Gal(K/F) \quad Gal(K/F(\alpha_1))$

$$\begin{tikzcd} K \arrow[d, dash] \\ F(\alpha_1) \arrow[d, dash] \\ F \end{tikzcd}$$



Pf. clearly: $F \subseteq K^{Gal(K/F)}$. We only

Let $\beta \in K^{Gal(K/F)}$. (We will show that $\beta \in F$)

Every element of $Gal(K/F)$ fixes $\beta \Leftarrow \beta \in K^{Gal(K/F)}$

$Gal(K/F) \supseteq Gal(K/F(\alpha_1))$

$\Rightarrow \beta \in K^{Gal(K/F)} \subseteq K^{Gal(K/F(\alpha_1))}$

$\Rightarrow \beta \in K^{Gal(K/F(\alpha_1))}$

$$\begin{tikzcd} K \arrow[d, dash] \\ F(\alpha_1) \arrow[d, dash] \\ F \end{tikzcd}$$

Ex: Let K be a field and let $H \leq G$ be 2 gps of automorphisms of K. Then $K^H \supseteq K^G$

Now, I am going to construct some elements of Galois K over f as follows. And this one is the direct application of extension theorem so I will go fast over this. So, you have a math from f alpha 1 to f alpha i. So, these are the extensions of f, this is simply because this is FX, I mean this is triviality. This is isomorphic to FX not f1 and so is this. Here the point is alpha 1 goes to alpha i. So, this is true for all i equal to 1, 2 r.

Remember that we have r of them. So, there is nf homomorphism from f alpha 1 to f alpha i, sending alpha 1 to alpha i. And of course K are the extensions of this. And using extension theorems, we can extend sigma… this map is sigma i. So, sigma i is the function from K to K automorphism which fixes f so, which is to say, which fixes f, that means, this is because, this is f extension map so here every element goes to itself, alpha 1 goes to alpha i, so when you extend it, it will continue to fix Capital F.

So, that means by definition, these are f automorphisms of K so that means they are in the Galois group. And second point is, sigma i f alpha 1 is alpha i. And this is true for all i equal to 1 to r. So, that means we have r constructed automorphisms of K now, f automorphisms of K which send alpha 1 to alpha i. So, so far so good. Now I want to claim, the conclusion that we want to prove and prove it.

So, we show, basically K F is Galois, that is, K power Galois K over f, is F. So, that is our thing to prove. And the proof is as follows, remember clearly, this is something that we mentioned little earlier in the video, f is certainly containing the fixed field because here all the elements are f automorphisms so we only have to show the other inclusion. Meaning K power Galois K over f is in F. So, now let us take a beta in this, let us take a beta in the Galois group and I am going to argue very soon that, beta is in fact, in F.

So, now the first point that I want to argue is, so this is an exercise, maybe I will write a bit more and then I will write the exercise. So, every element of Galois K over f fixes beta, by definition because beta is in the fixed field of Galois K over f. Now, where are we, we have the picture that I had a earlier, I will read it, K contains K power.. sorry, K contains f alpha 1 which is an extension of f. So, this is simply because beta is in K power Galois K over f. That implies every element of Galois, K over f fixes beta.

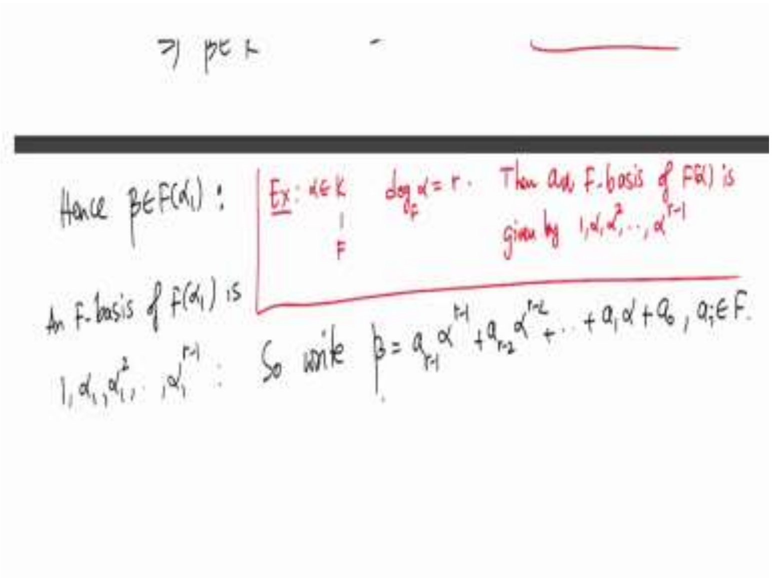
But now what is the relation between Galois K over f and Galois K over f alpha 1. Just think about it. This in fact, came in a problem section earlier, so what is an element of left hand side here. It means, it is an f automorphism of K, that means it is an automorphism of K, that fixes every point of f. And what are the elements here? This is an f alpha 1 automorphisms of K that means it is K auotmorphism that fixes every element of f alpha 1. But if it fixes every element of f alpha 1, it certainly fixes every element of f.

So, this is what we have, this is a simple statement, every element of, every K automorphism of, every automorphism of K which fixes everything in f alpha 1, is a K automorphism which fixes everything in K. So, this is an automorphism of K which fixes everything in F, so, this is a triviality. Now I claim, let us look at the fixed field of these, so, now these are things that are fixed by every automorphism of K… this is the thing which is fixed in K by every F automorphism of K.

These are the things in K that are fixed by every f alpha 1 automorphism of K. So, now because this is a smaller group, if a bigger group, every element in a bigger group fixes an element, it is automatically fixed by everything in a smaller group. So, this is the exercise that I want to give, it is a triviality. Let K be a field and let H and K be 2 groups of automorphims of K, H and G. So, that means K is a group of automorphisms and H is a sub-group.

So, then K power H contains K power G. Here is the triviality because everything in G fixes something here, so that means the element is fixed by everything in G. But if everything is fixed in G, it is fixed automatically by everything in H. So, it is in fixed field of H. But now, coming back to the proof, beta was chosen to be here so that means beta is in K power Galois K over f alpha 1. But now induction hypothesis told us what? All the way back, I wrote it here, this is the induction hypothesis, right? K power Galois, K over f alpha 1 is f alpha 1. So, that means, this is equal to f alpha 1.

(Refer Slide Time: 19:22)



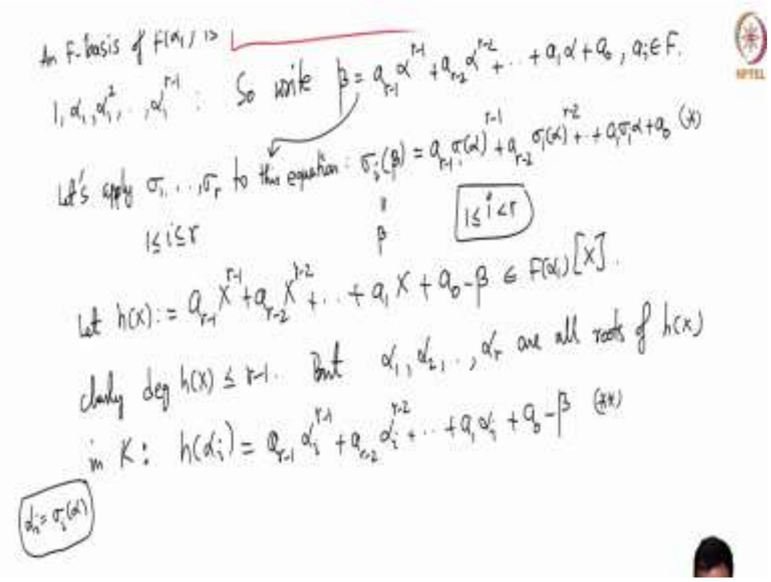
$\exists \beta \in K$

Hence $\beta \in F(\alpha_1)$:

Ex: $\alpha \in K$ $\deg_F \alpha = r$. Then an F-basis of $F(\alpha)$ is given by $1, \alpha, \alpha^2, \ldots, \alpha^{r-1}$

$\begin{array}{c} K \\ | \\ F \end{array}$

An F-basis of $F(\alpha_1)$ is $1, \alpha_1, \alpha_1^2, \ldots, \alpha_1^{r-1}$: So write $\beta = a_{r-1}\alpha^{r-1} + a_{r-2}\alpha^{r-2} + \cdots + a_1\alpha + a_0$, $a_i \in F$.



An F-basis of $F(\alpha_1)$ is $1, \alpha_1, \alpha_1^2, \ldots, \alpha_1^{r-1}$. So write $\beta = a_{r-1}\alpha^{r-1} + a_{r-2}\alpha^{r-2} + \cdots + a_1\alpha + a_0$, $a_i \in F$.

Let's apply $\sigma_1, \ldots, \sigma_r$ to this equation: $\underset{\beta}{\sigma_i(\beta)} = a_{r-1}\sigma_i(\alpha)^{r-1} + a_{r-2}\sigma_i(\alpha)^{r-2} + \cdots + a_1\sigma_i\alpha + a_0$ (*)

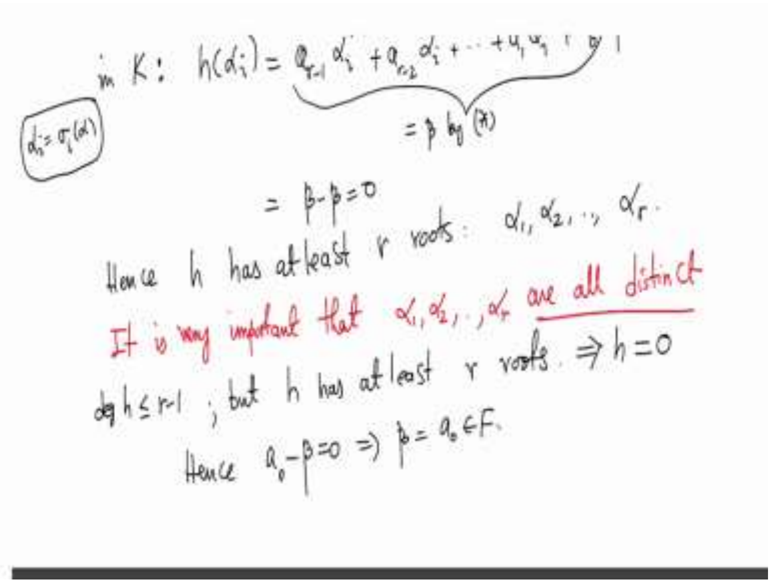
$1 \le i \le r$ $\boxed{1 \le i < r}$

Let $h(X) := a_{r-1}X^{r-1} + a_{r-2}X^{r-2} + \cdots + a_1 X + a_0 - \beta \in F(\alpha_1)[X]$.

clearly $\deg h(X) \le r-1$. But $\alpha_1, \alpha_2, \ldots, \alpha_r$ are all roots of $h(X)$

in K: $h(\alpha_i) = a_{r-1}\alpha_i^{r-1} + a_{r-2}\alpha_i^{r-2} + \cdots + a_1\alpha_i + a_0 - \beta$ (**)

$\boxed{\alpha_i = \sigma_i(\alpha)}$



in K: $h(\alpha_i) = \underbrace{a_{r-1}\alpha_i^{r-1} + a_{r-2}\alpha_i^{r-2} + \cdots + a_1\alpha_i + a_0}_{= \beta \text{ by } (*)} - \beta$

$\boxed{\alpha_i = \sigma_i(\alpha)}$

$= \beta - \beta = 0$

Hence h has atleast r roots: $\alpha_1, \alpha_2, \ldots, \alpha_r$.

It is very important that $\alpha_1, \alpha_2, \ldots, \alpha_r$ are all distinct

$\deg h \le r-1$; but h has atleast r roots. $\Rightarrow h = 0$

Hence $a_0 - \beta = 0 \Rightarrow \beta = a_0 \in F$.

So, beta is in f alpha 1, hence beta is in f alpha 1. But now, another exercise for you, if K over f is some algebraic extension and alpha is here, let us say degree of alpha is r, then an f, f bases of f alpha over f is given by… f alpha is vector space over capital F and the basis is given by 1 alpha, alpha square, up to alpha power r minus 1. This is because, to begin with every element of f bracket alpha is a polynomial alpha.

So, in general it requires all powers of alpha but because degree is r, any power alpha r, alpha plus 1, alpha power 2 and so on can be expressed in terms of these using the polynomial which has alpha as a root. So, applying this exercise, we know that an f basis of f alpha 1 is 1, alpha 1, alpha l square up to alpha 1 power r minus 1. So, write beta is equal to a r minus 1, alpha r minus 1, a r minus 2, alpha r minus 2, a 1 alpha is 0 where of course the point is a, e, f. So, it can be represented by a f linear combination of these elements.

In fact, these are unique expression. Now let us apply.. so recall the automorphisms which we constructed, sigma i's. These are the elements of Galois group, right? Of K over F and what are the properties of sigma is? They send alpha 1 to alpha i. So, let us apply sigma 1 upto sigma r to this equality, this equation. So, what do I get? Because beta is fixed by the Galois group, by hypothesis, and sigma i is are in the Galois group, so beta will be fixed by sigma.

So, this is beta, so I want to take 1 less than… i less than equal to r. This is going to be… because a i are also in F, sigma is going to fix that also, so I am going to simply write this as sigma i alpha r minus 1, r minus 2 sigma i alpha r minus 2 plus dot dot dot.. a1 sigma i alpha plus a0 because sigma fixes it. So, this is what we have, so we have in fact, r equations, for every i, from 1 to r we have these equations.

Now the last step, we are almost done, let us consider the polynomial HX to be ar minus 1 X power r minus 1, ar minus 2 x power r minus 2, a1 x plus a0, I will subtract beta from this. So, this is a polynomial in F alpha 1 bracket X. Remember that, this is a priori not in FX because while ar minus 1, ar minus 2, 1 a0 are in F, beta is adjust point only in F alpha 1. We will show, it is in F but we are not yet there, so beta is in F alpha 1, so there is a polynomial in F alpha 1 bracket X so degree of, so clearly, degree of H is r minus 1.

So, ar minus 1 is certainly non-zero or degree is at most r minus 1. So, then that alpha 1, alpha 2, alpha r, are all roots of hx in K. So, they are in K, why are the roots of this because if you take h of alpha, you got ar minus 1 alpha r minus 1, alpha ir minus 1, ar minus 2, alpha ir minus 2, a1 alpha i plus a0 minus beta. But now let us see, what is in our screens, alpha i is actually nothing but sigma i of alpha. Alpha i is sigma i of alpha.

So, let us compare star and double star. So, compare star here and double star, I claim that, they are exactly the same equations, ar minus 1, ar minus 1. Sigma i alpha power r minus 1 but sigma i alpha is alpha i, alpha i power r minus 1. Sigma i alpha is alpha i power r minus 2, a1 alpha i plus a0, star is written…as this is equal to beta so this is equal to beta by star. So, that means we have beta minus beta.

And hence h has at least r roots, mainly alpha 1, alpha 2 up to alpha r. And it is very important for us to hear that, it is very important that alpha 1, alpha 2 upto alpha r are all distinct because, otherwise we cannot say it has at least r roots and that is the point here. So, it is crucial that alpha 1, alpha 2 up to alpha r are distinct and this is where separability comes into place. So, these are r different elements of all roots of h, so h has degree, r minus 1 but h has at least r roots. But this is a problem, right?

Because our field is polynomial and can have at most as many roots as its degree. Here you have a degree r minus 1 or less polynomial but it has at least 6 roots. The only resolution for this problem is h is 0 but if h is 0, each coefficient is 0. Polynomial is 0 means all coefficient are 0. So, a0 minus beta is 0 that means beta is equal to a0 which is an f. So, beta is in f as we wanted to show.

So, this is a very nice clever proof and it shows that, it is quite long so we may have lost track of time here but it shows that, if you have an extension which is the splitting field of a separable polynomial then it is Galois. So, this proof is several pages long, in the previous video we proved one direction and in this video we proved that if we have K, splitting field of separable polynomial over base field F then it is Galois extension.

So, let me stop this video here, I wanted to derive some analysis for this but we will postpone that to next video because this is already a lot of material to cover in a single video. So, let me stop this video here and we will continue with consequences of this theorem in the next video, thank you.