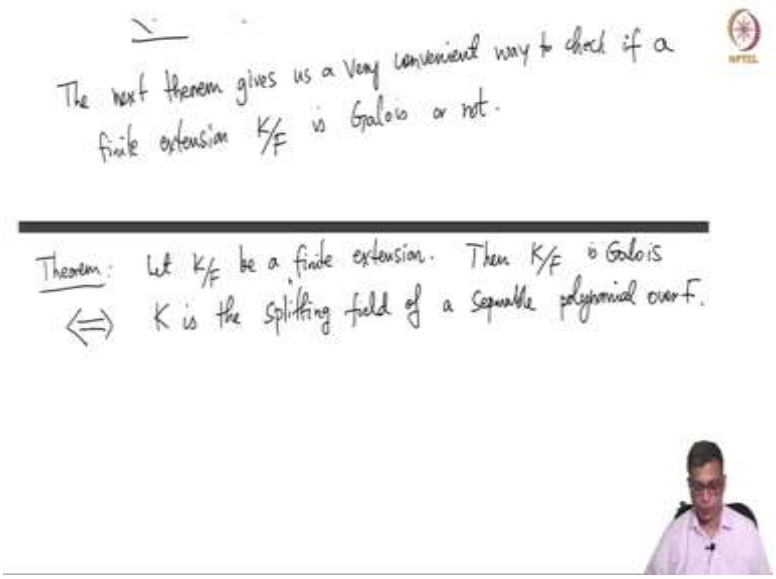
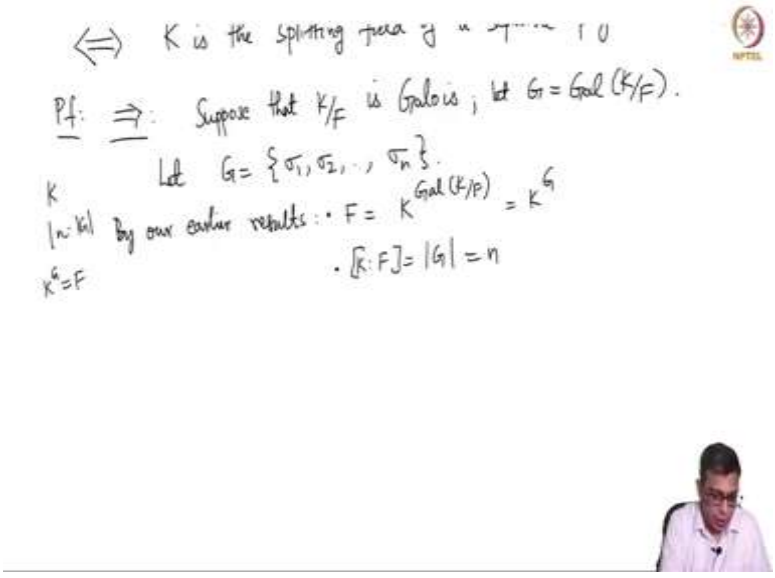
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 20
Characterization of Galois Extensions – Part 1

(Refer Slide Time: 00:23)



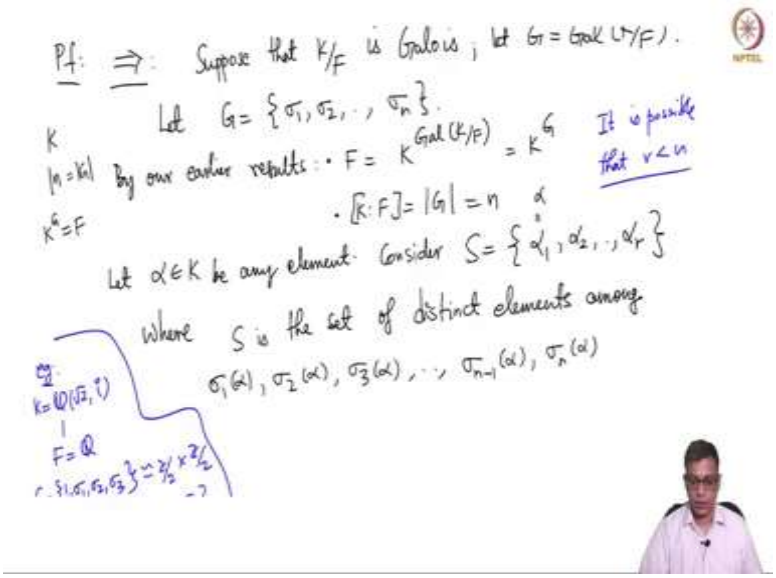


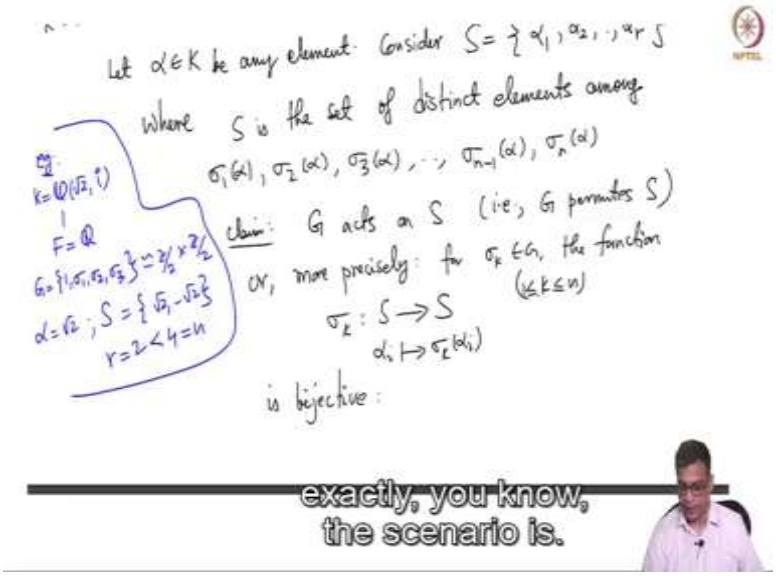
Welcome back, we are ready to prove this very important theorem about Galois extensions. And which as I said in the last video, which gives us a convenient way of verifying if something is Galois or not. So, let us get right to the proof. So, you have the statement that a given extension is Galois if and only if the extension field is a splitting field of a separable polynomial over the base field.

So, let us prove first the direction forward direction. So, suppose, so here we are assuming that suppose that K over F is Galois, we are going to show that it is a splitting field of a separable polynomials over capital F. So, suppose that K over F is Galois and let us for convenience called the Galois group G. So, G is the Galois group and write G as sigma 1, sigma 2, sigma n. So, this mean, it is a finite extension.

In fact, what we know is that, so by our earlier results before we did separability, when we talked about Galois extensions, and Kuru characters, and so on. So, we have this, so this is of course K power G, so this is the first statement, F is the fixed field of G, and also, the degree of the field extension is order of G, which I am calling n. So, you have a extension like this. And this n is also the cardinality of G. So, that is what we have.

(Refer Slide Time: 02:04)





So, now, I am going to consider an arbitrary element of capital K, let alpha be an element of capital K, be any element. So, I want to consider the set S to B alpha 1, which is alpha, alpha 2 and alpha r, where S is the set of distinct elements among all the elements that you get by applying G to alpha. So, sigma 1 alpha, sigma 2 alpha, sigma 3 alpha, sigma n minus 1 alpha, sigma n alpha, The point is some of these could be equal to each other.

So, I am going to just take the distinct ones among them and call this r. So, it is possible often that r is less than n. So, for example, I will do one example here. So the proof is very easy, but it is long. So just keep track of it with me and carefully follow the arguments. So, I will give you an example here of what is going on here. So we take a to b, Q root 2 comma i over F, which is q. So here G of course, is something that you have seen many times in the past, it is isomorphic to Z mod 2 cross Z mod 2.

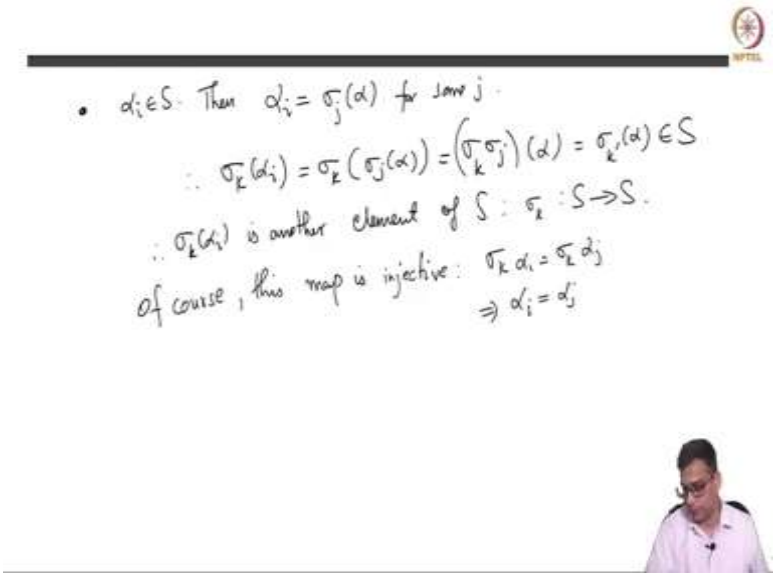
But if you take alpha to be root 2 the set S, you will simply get root 2 comma minus root 2. So r in this example is 2, which is less than 4 which is n. So for a particular element, for example, in this example, you get identity of alpha, which is root 2, sigma, 1 of alpha, I mean, the labelling is somewhat mixed up, but root 2 goes to root 2 under one of them, so that will not give you a new element, whereas in the second one it will go to minus root 2, in the third one, also go to minus root 2.

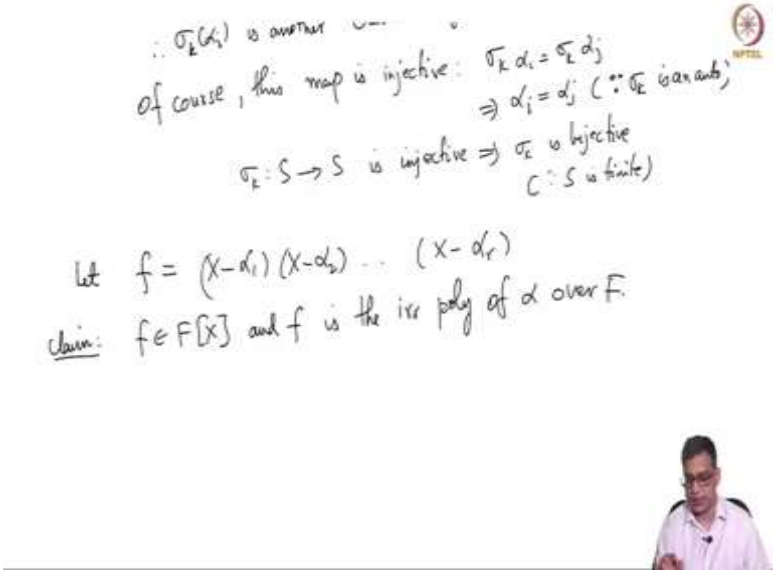
So remember, this, what we do know however, is that all these are conjugates of alpha, because their images under automorphisms, which fixed capital F. So these are distinct elements. So now in general, I have r less than n. So, let me continue the proof now, so I do not care what r is, but it is smaller than less than or equal to n.

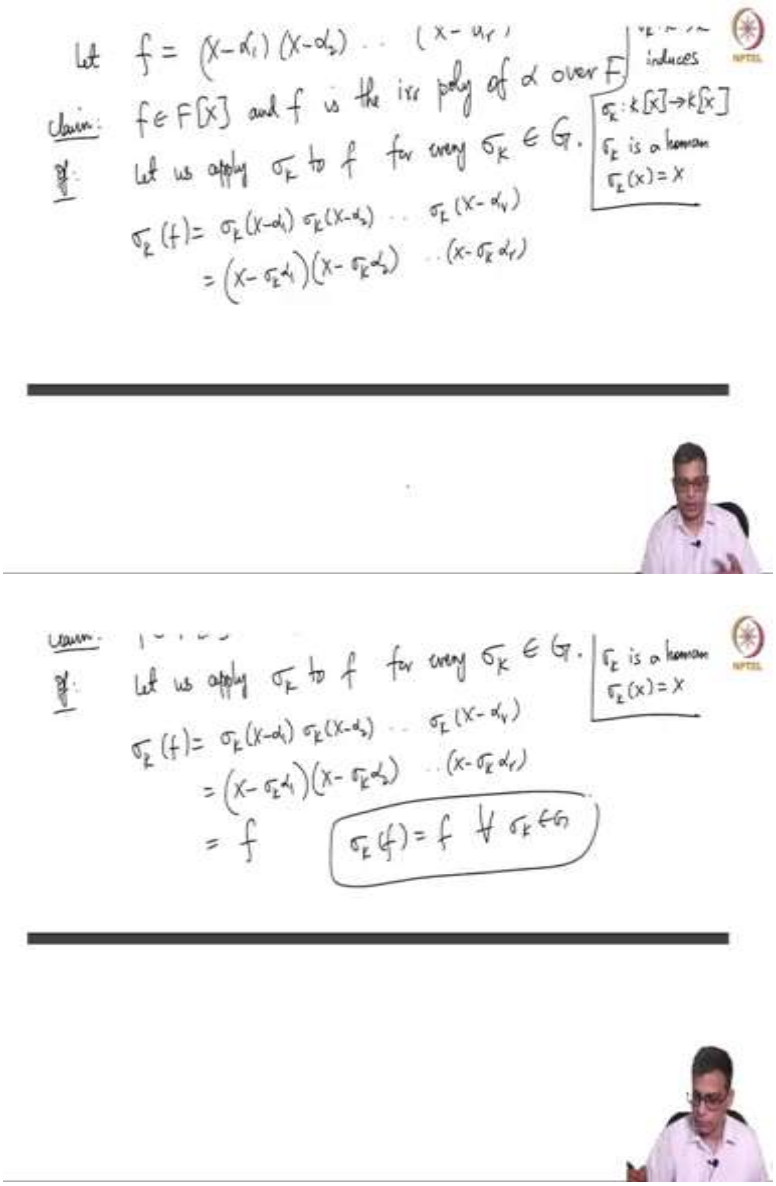
Now, we claim that g acts on us. So in the language of group actions that you would have seen, we said a G acts on S, that is G permutes S, that is another or more precisely for sigma K in G, the function sigma K from S to S with sends alpha i, two sigma K of alpha i is bijective. This is what my claim is. So, if you fix the sigma K, so G remember is sigma 1 through sigma n take any K between 1 and n.

So, you call that sigma K, then if you have operate sigma K on S, it fixes, it permutes S that means, it is a bijection of S. First of all, why does it even map to S.

(Refer Slide Time: 5:47)







So, take alpha i and s then by definition alpha is equal to, alpha is one of these elements. So, S is this, but each alpha i is an element of some sigma j of alpha, because alpha I, they are all elements, images of alpha under sigma j's, for some j, therefore, sigma K of alpha i, which is the image of this map, sigma K of alpha i is equal to sigma K of sigma j of alpha.

But this is same as sigma K times sigma j of alpha, by the property that you have a group G. This is a group operation. So, this means sigma K prime alpha, so this is equal to sigma K prime alpha, which is another element in this set. So, this must be an element in the set of sets S itself. So, it is not S prime. S consists of all elements like this. So, you apply sigma ''s and you get S. So, this must be another element of S. So, sigma K alpha i prime, alpha i is another element of S, maybe same element, but I do not care, it is an element of s.

So, sigma K maps S to S and of course, and of course sigma this map is injective, because sigma K of alpha is equals to sigma K of alpha j implies alpha i because sigma K is an automorphism. This is because is an automorphism, it is a field automorphism. In fact, any field homomorphism is injective. So, that is all I need here. So, sigma K is an injective map implies it is also bijective, because S is a finite set.

So, an injective map from S set to itself is bijective, meaning injectivity implies surjectivity and also we have a surjective map from a finite set to itself is also injective. So, to check bijectivity of a finite set map to itself, we need to check either injectivity or surjectivity. So, we check this.

So, this proves this claim sigma acts on, G acts on S. And now, we are able to prove the following statement. So, let f b x minus alpha 1, x minus alpha 2, x minus alpha r. So, remember again, let me remind you, S consists of these elements alpha 1 through alpha r, and they are the distinct set of elements among all the images of alpha under all elements of capital G. Again, this is what we are doing in the example.

So, in this example, f will be x minus root 2 times x plus root 2. I am not taking all the elements here, I am taking only the distinct elements here. So, the claim is, now this is the most important claim. Claim f is in fact, a polynomial over the base field and f is the irreducible polynomial of alpha over f. So, this is a very crucial claim.

In fact, it gives us more than what we are claiming in a theorem, it proves the theorem, one direction of the theorem, but it in fact, tells us how to compute irreducible polynomial of an arbitrary polynomial, of arbitrary element. So, why is this? So, first of all why is f in capital FX? So note that, so let us apply sigma K to f for every sigma K in G.

So now, I do not want to multiply f out and apply sigma, I want to keep f as it is and apply sigma. So what is sigma K of f? Because sigma k is a group, I mean automorphism sigma K, in fact, gives a map from K x to K x. Sigma K induces this, so I am being sloppy and using the sigma K, which is a function from K to K induces this.

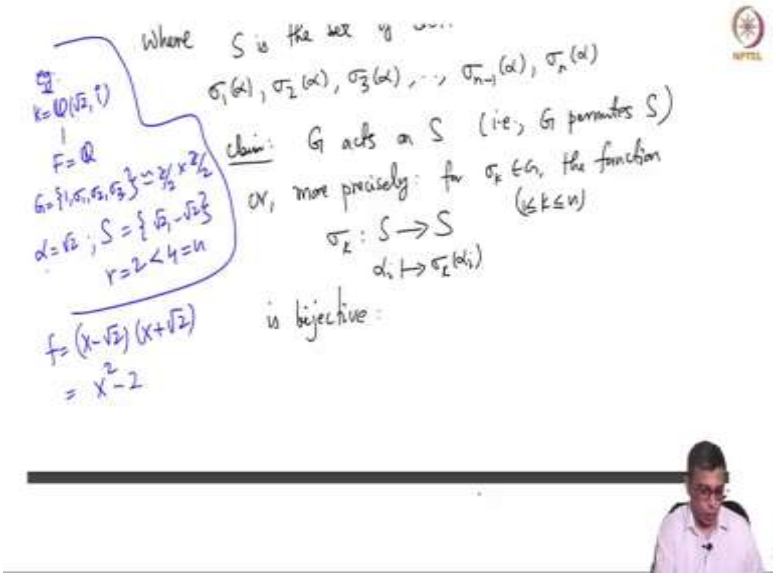
Every time you have an automorphism of fields, you get an homomorphism of the polynomial rings in one variable like this, x goes to x and co—efficient go to images of sigma K. So, this and sigma K is a homomorphism. So, sigma K of f is actually sigma K of x minus alpha 1 times sigma K of x minus alpha 2 times sigma K of x minus alpha r.

But sigma k of x minus alpha 1 again using the property that it is a homomorphism and sigma K x equals x, this will be simply x minus sigma k alpha one. Similarly, x minus sigma K alpha 2, dot dot dot x minus sigma K alpha r.

Now, just let us stare at this for a moment and use this claim, that G acts on S or more concretely, we have, this is a bijective map, that means, if you apply sigma K to alpha 1 through alpha r, we get a bijection, so, you are permuting the maybe, so if you apply this, this might be in some other, f is this right, this might be the second term, or this might be the first time and so on.

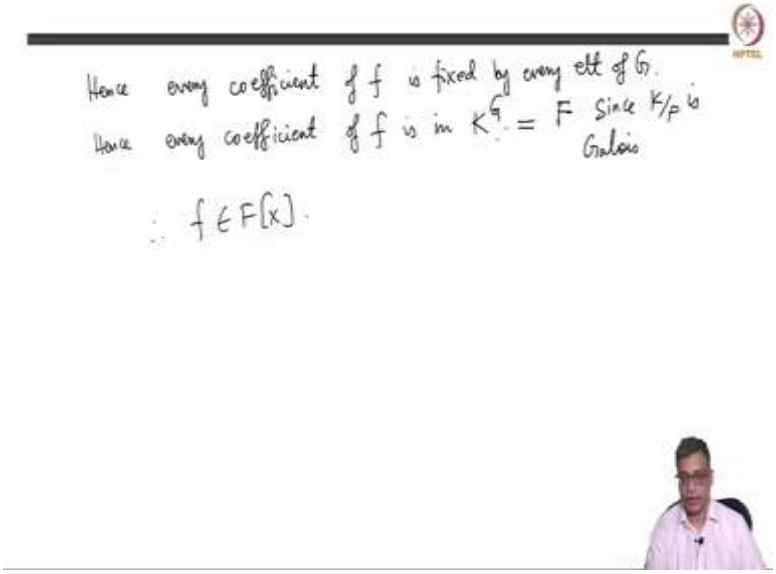
So, I do not care in which order I get, multiplication is abelian. So, this is nothing but f that is a point. So, this is exactly same as f because I get all the factors again. So, sigma K of f is f and of course, this is true for all sigma K in G. So, this is because this I am taking an arbitrary sigma K and f.

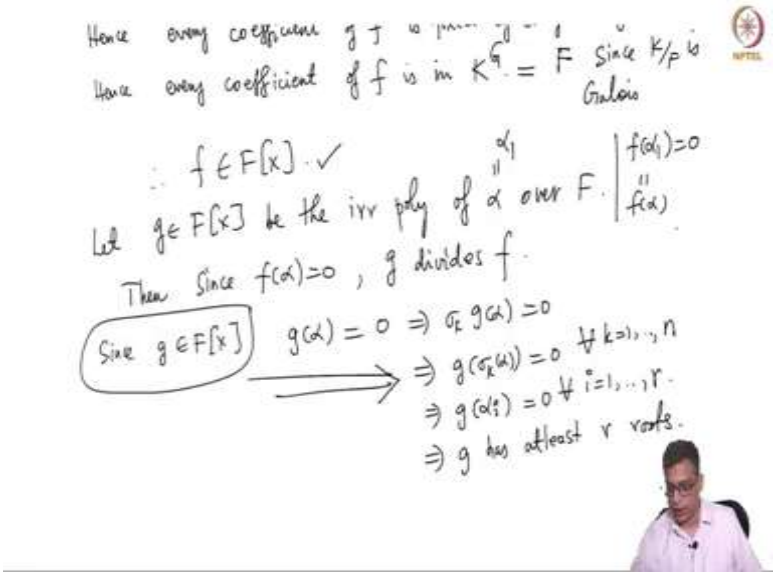
(Refer Slide Time: 12:20)



So, now, if you go back to this example, and apply sigma K to this, I mean this actually, it is useful to expand this out in this particular example, what you get is x square minus 2, which remember is the irreducible polynomial of root 2 over and the claim is then proved for this example, but the point is if you apply any of these 4 elements of the group you get that polynomial back.

(Refer Slide Time: 12:47)





Let $g \in F[x]$ be the irr poly of α over F. $\Rightarrow g \mid f(x)$

Then since $f(\alpha)=0$, g divides f.

Since $g \in F[x]$: $g(\alpha)=0 \Rightarrow \sigma_k g(\alpha)=0$

$\Rightarrow g(\sigma_k(\alpha))=0 \quad \forall k=1,\dots,n$

$\Rightarrow g(\alpha_i)=0 \ \forall i=1,\dots,r$.

$\Rightarrow g$ has atleast r roots.

$\Rightarrow \deg g \geq r$.

$\deg f = r$ and g divides f. $\therefore \deg g \leq r$.

$\Rightarrow \deg g = r$

$\Rightarrow g = f$.

$\deg f = r$ and g divides f. $\therefore \deg g \leq r$.

$\Rightarrow \deg g \geq r$.

$\Rightarrow \deg g = r$

$\Rightarrow g = f$. ✓

This proves the claim.

This is a useful way to find the irr poly of an elt in a Galois ext.

K ... $|n=kl|$ By our earlier results: $F = K^{Gal(K/F)} = K^{G}$ ... that $r \leq n$

$K^G = F$

$\cdot [K:F] = |G| = n$

Let $\alpha \in K$ be any element. Consider $S = \{\alpha_1, \alpha_2, \dots, \alpha_r\}$

where S is the set of distinct elements among

$\sigma_1(\alpha), \sigma_2(\alpha), \sigma_3(\alpha), \dots, \sigma_{n-1}(\alpha), \sigma_n(\alpha)$

Eg: $K = \mathbb{Q}(\sqrt{2}, i)$, $F = \mathbb{Q}$, $G = \{1, \sigma_1, \sigma_2, \sigma_3\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $\alpha = \sqrt{2}$; $S = \{\sqrt{2}, -\sqrt{2}\}$, $r = 2 < 4 = n$

Claim: G acts on S (i.e., G permutes S)

Or, more precisely: for $\sigma_k \in G$, the function ($1 \leq k \leq n$)

$\sigma_k : S \to S$

$\alpha_i \mapsto \sigma_k(\alpha_i)$

So, the conclusion is hence every coefficient of f. So, now if you expand f out and look at coefficients they must be fixed by every element of G that means, every coefficient of f is in the fixed field of G. A priori f is a polynomial in K x that means, every element coefficient of f is in K, but we just argued that because sigma K f f is equal to f.

Remember f is a n x n plus a n minus 1 x minus actually r, it is a degree r polynomial, sigma K f is sigma K a r, x r and so on. But these are equal that means, sigma K a r equals a r. So, every question of f is fixed by every element of j that means, every coefficient of f is in KG, but KG is equal to f, since K over F Galois.

So, this is the statement that the assumption that K over F is Galois we are going to use that here. So, that means, f is in FX, if every coefficient of f is in the fixed field and the fixed field is capital F that means, the polynomial itself is in capital FX. So, this is the first part of the claim. Now, I claim that it is in fact the irreducible polynomial, this is easy.

Let G be the irreducible polynomial of, so it is a algebraic elements it is, it must have an irreducible polynomial, let us call that G. Then of course, since, f alpha is 0, remember alpha is equal to alpha 1 and alpha 1 is a root of f. So, f of alpha 1 is 0. So, g divides f because irreducible polynomial divides every polynomial that has alpha as a root. So, so far we have concluded that g divides f, but now what can be the degree of g.

So, note that since g has coefficients in FX, g alpha equal to 0 implies sigma K g alpha is equal to 0. This is not the reason, I will write what this gives, this is a triviality sigma K of a 0 element is the 0 element, but this is g of sigma K of alpha, this is the reason because sigma K fixes all the questions of g you can bring sigma K inside, so g sigma K alpha is 0 that means, g of alpha i is 0 for all i from one to r.

What are alpha i’s, let us go back to the beginning of the proof, alpha i's are just the distinct set of elements from sigma 1 alpha, sigma 2 alpha, sigma n alpha, g of sigma n alpha, sigma K alpha is 0 for all K from 1 to n. But some of them are equal. So, g of alpha is equal to 0 for all, every i from 1 to r, that means, g has at least r roots.

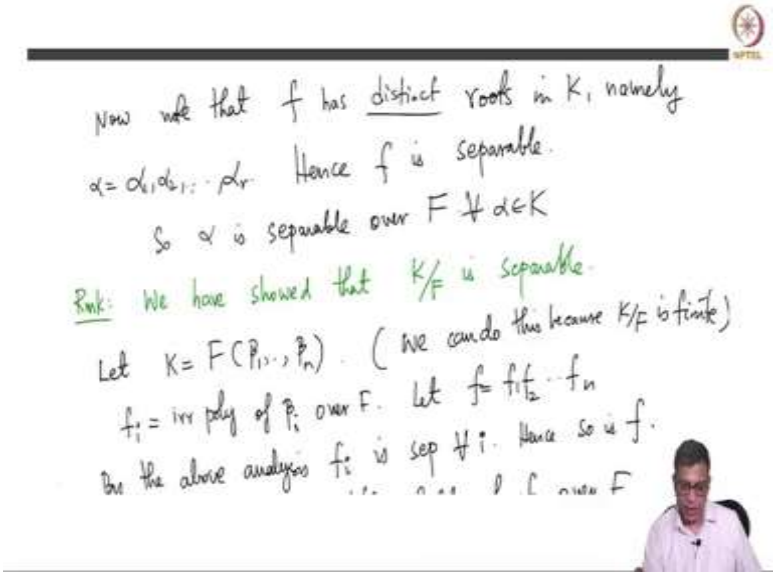
Remember also that alpha i's are distinct by choice, sigma K alphas may not be distinct like in this example, but alpha i's are distinct root 2 minus root 2, because we are only taking distinct ones among these. So, g has at least our roots, that means degree g is at least r,

because a polynomial which has a roots in a field must have at least degree, but degree of f is r and the g divides f.

So, degree of g is less than or equal to r, but it is also greater than equal to r by which we argued, but that means g is equal to f, because irreducible polynomial is a unique Monic polynomial, which has a least degree, which has alpha as a root, f is Monic, g is Monic so they are equal. So, this proves the, this proves the claim and in fact, let me comment here that this is a useful way to find the irreducible polynomial of an element in a Galois extension.

Because what you do you take that element and you take the Galois group and you look at all its images and among the images, you take the distinct set and you simply take x minus the first one, x minus the second one, x minus the last one and multiply it out by this claim that will be a polynomial in capital FX and it will be the irreducible polynomial. So, that is a side remark. So, what did we show? We showed that f is the irreducible polynomial. So, we are almost done now with forward implication.

(Refer Slide Time: 18:40)



Rmk: We have showed that [illegible]

Let $K = F(\beta_1, \ldots, \beta_n)$. (we can do this because K/F is finite)

f_i = irr poly of β_i over F. Let $f = f_1 f_2 \cdots f_n$

By the above analysis f_i is sep $\forall i$. Hence so is f.

Claim: K is the splitting field of f over F.

Pf: Know that irr poly of β_1 over F is

$(X-\beta_1)(X-\beta_{12}) \cdots (X-\beta_{1r_1}) \in F[X]$, where

each $\beta_{1i} = \sigma_k(\beta_1)$ for some $\sigma_k \in Gal(K/F)$.

Pf: Know that irr poly of β_1 over F is

$(X-\beta_1)(X-\beta_{12}) \cdots (X-\beta_{1r_1}) \in F[X]$, where

each $\beta_{1i} = \sigma_k(\beta_1)$ for some $\sigma_k \in Gal(K/F)$.

But $\sigma_k : K \to K$ is an auto. So $\sigma_k(\beta_1) \in K$

Of course, this map is injective $\Rightarrow \alpha_i = \alpha_j$ ($\because \sigma_k$ is an isom, $\sigma_k : S \to S$ is injective $\Rightarrow \sigma_k$ is injective ($\because S$ is finite)

Let $f = (X-\alpha_1)(X-\alpha_2) \cdots (X-\alpha_r)$

Claim: $f \in F[X]$ and f is the irr poly of α over F

Pf: Let us apply σ_k to f for every $\sigma_k \in G$.

$\sigma_k(f) = \sigma_k(X-\alpha_1)\,\sigma_k(X-\alpha_2) \cdots \sigma_k(X-\alpha_r)$

$= (X-\sigma_k\alpha_1)(X-\sigma_k\alpha_2) \cdots (X-\sigma_k\alpha_r)$

$\sigma_k : K \to K$ induces $\sigma_k : K[X] \to K[X]$, σ_k is a homom, $\sigma_k(X) = X$

$f = a_r X^r + a_{r-1} X^{r-1} \cdots$

$\sigma_k f = \sigma_k(a_r) X^r + \cdots$

$\Rightarrow \sigma_k(a_r) =$

[illegible] $\forall \sigma_k \in G$

So, hence, now note that g has distinct roots, let me use f, f is irreducible polynomial, it has distinct roots in K, namely alpha 1, alpha 2, alpha is of course alpha 1, alpha r and hence by the definition of separability that I gave in the last video, f is separable. So, hence, alpha is separable over K, rather f.

Because we remember started with an arbitrary alpha in K and we concluded that series D, we concluded that its irreducible polynomial is separable, its irreducible polynomial over capital K is separable. So, alpha is separable over F, though we do not read this for this particular theorem. What we actually, when we will use this in a corollary later, we have showed that K over F is separable.

So, we have started with the Galois extension and we have showed that it is separable because every element is separable. Now, we are not quite done. So, we have to produce a separable polynomial whose splitting field is K. So, now let K is a finite extension of F that is given to us. So, now, let us choose some beta 1 through beta n, such that K is equal to, we can do this because K over F is finite that is our global assumption.

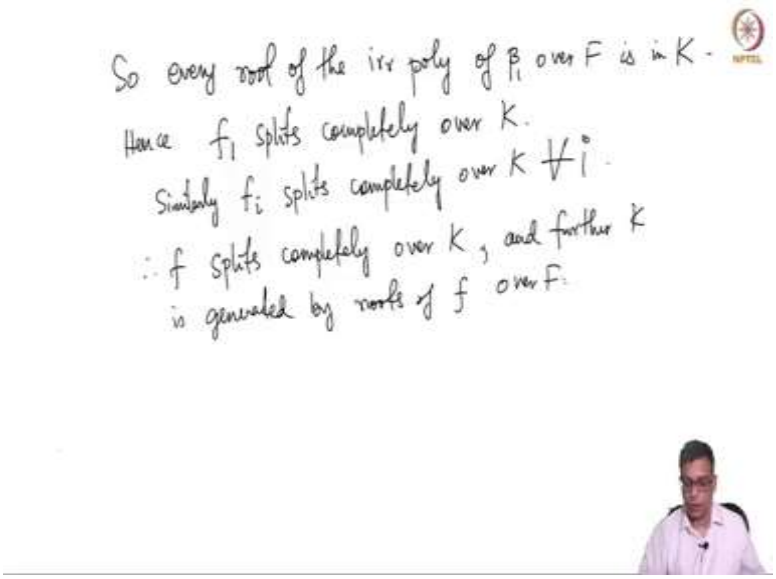
So, we have this, by and let us say f 1, f i is the irreducible polynomial of beta i over capital F and let small f be f 1, f 2 times f n. By the above analysis fi is separable for all i, because irreducible polynomial of any element in capital K or F is separable. So, fi being the original polynomial of beta i is separable hence, so is f because f has irreducible factors just f 1, f 2, fn and each of them is separable.

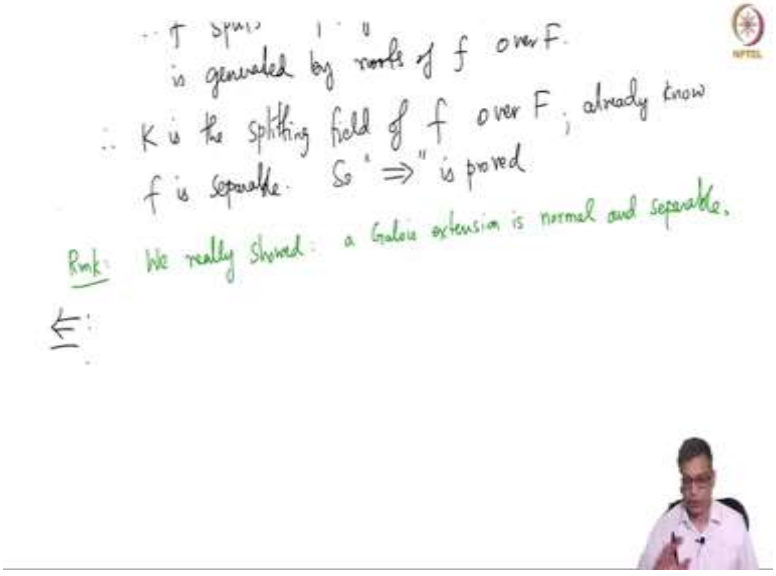
So, f is separable and clearly K is a splitting field, of f over capital F. Because clearly, so now this, I should not say clearly, I will say claim, K is a splitting field. So what is the proof? We know that f is separable. So now we want to show that K is a splitting field. So, we know that irreducible polynomial of beta 1 over capital F is of the form x minus alpha, x minus beta 1, x minus beta 1 1, let us say or 1 2 times x minus beta 1 r 1, I mean the indexing will get quite tricky here, but there will be some number of factors, I do not care what they are.

So, r 1 factors is what I am calling this is because where each beat i, so let me write that here, where so beta 1 i is sigma K, beta 1 for some sigma K in the Galois group. That is exactly this claim. And this claim is extremely important for us. This claim says that, if you take the conjugates of alpha via capital G, take a distinct set among them and construct this polynomial x minus alpha 1, times x minus alpha 2, and x minus alpha r, what you get is the irreducible polynomial.

So, for beta 1, it would be x minus beta 1, x minus beta 1 2, I mean I do not want to use beta 2 because that is already here, that is all, but some things which are images of sigma K, but sigma K is a function from K to K. So, sigma k of beta 1 is in K, this is the most important statement.

(Refer Slide Time: 23:50)





So, every root of the irreducible polynomial of beta 1 over capital F is in capital K, because this is the irreducible polynomial of capital beta 1 over capital F and its other roots are simply images of sigma K's, as you vary sigma K in Galois group, but sigma K is an automorphisms that means, beta 1 2 is in capital K, beta 1 3 is in capital K, beta 1 r 1 is in capital K, hence f 1, so by the way this is f 1 in my notation, f 1 is the irreducible polynomial of beta 1.

So, f 1 splits completely over capital K that is the crucial statement because other roots of capital, other roots of f 1 are images of beta 1 under the Galois group elements. So, f 1 splits completely. Similarly f i splits completely. So I hope this is clear. I may have gone over this a little fast, but please go over this carefully and understand if you have questions, you can ask in the discussion forum.

So each f i split is completely over capital K, so that means f i split, F splits completely because f is the product of f 1 through f n, f 1 splits completely up to 2, f 2 splits completely, f n splits completely, so f does. And remember that you cannot drop any roots of F, K is generated by it is generated by roots of F, because I am going to assume a priori that you can drop none of any of the Bi's.

If you drop any of the Bi's, you get a smaller field, that is an implicit assumption here. So that means K is the splitting field of f over capital F and we already showed that that f is separable. So this direction is proved. So we assumed that you have a Galois extension and we proved that K is a splitting field of separable polynomial over the base field.

This is a crucial proof, statement is important, but lot of stuff is going on in this proof. So, I will stop this video in the next video, we will prove the other direction, but what we have really showed here, I want to isolate here is, we really showed that a Galois extension is normal and separable. So, Galois extension is normal and separable, because we have showed here that it is separable and we have just shown below that that it is a splitting field of some polynomial. So it is separable, it is normal rather.

So Galois extension is normal and separable. So in the next video we are going to go the opposite direction, where we are going to suppose that it is a splitting field of a separable polynomial and show that it is a Galois extension. Thank you.