

Algebra - II
Professor S Viswanath
Department of Mathematics
The Institute of Mathematical Science
Lecture 35
Finite Galois Extensions

(Refer Slide Time: 00:15)

Finite Galois Extensions

Theorem: Let K/F be a finite extension. Then K/F is a Galois extension $\Leftrightarrow [K:F] = |\text{Aut}(K/F)|$

Proof: $\Gamma := \text{Aut}(K/F) = \{ \sigma \in \text{Aut}(K) \mid \sigma|_F = \text{id}_F \}$

Observe: $[K:F] < \infty \Rightarrow |\Gamma| < \infty$

finite $\left\{ \begin{array}{l} F(\alpha_1, \alpha_2, \dots, \alpha_n) \\ F(\alpha) \\ F \end{array} \right. \Rightarrow K = F(\alpha) \text{ for some } \alpha \in K$

$\sigma: K \rightarrow K \quad \sigma \in \text{Aut}(K/F)$

Let us talk about finite Galois extensions. So recall, we have proved Artin's theorem and these are all now some nice consequences. So here is a theorem, which characterizes finite extensions, which are Galois. So let, K over F be a finite extension. Then K over F is Galois extension, if and only if the following degree criterion holds that the cardinality of the degree of extension K/F is the same as the cardinality of the group of F automorphisms of K .

So, let us prove this. So, recall what the group of F automorphisms was. So, $\text{Aut } K$ over F just meant, take all automorphisms of K which are identity on F and this of course appeared in our, so let me just call this group Γ . So this appeared in our earlier characterization of general Galois extensions.

Recall that an extension is Galois if and only if the fixed field of this group of automorphisms is the base field itself. So we will come to that, the course of the proof. So I have called this as Γ . So the first observation is that, observe the finiteness of this extension implies the finiteness of this group.

So why is this true? Well, what does a finite extension look like? So here is one way of thinking about a finite extension. I start with the base field, if there is at least one element

outside the base field, which belongs to my field K , then what I do is I adjoin that element. So if I can find one element in K which is not in F I adjoin it.

I get an intermediate field F of α_1 . If $F \alpha_1$ is still not everything, there is something more than I can adjoin 1 further element. I pick an element outside and adjoin and so on. So I keep going. Now, at every step, the extension that I have created has degree at least 2, like the degree of this extension is at least 2 because I have chosen α_1 that does not lie inside F .

So at every step, I have at least a degree 2 extension and the overall extension is finite which means that I cannot keep going on and on like this forever because recall that the degrees are multiplicative. So $[K:F]$ is just the degree of the product of the degrees of all the intermediate extensions. So therefore, this process has to stop. So, this means that in particular K is just obtained from F by finitely many adjunctions.

So, this has looked like $\alpha_1, \alpha_2, \dots, \alpha_s$ for some finite value s could be 0 even if K and F are equal. So, in other words, there are there are no α_s if K and F are equal. So, what does that mean? So, if I can obtain K from F by finitely many adjunctions, then the effect of an automorphism, so observe now that σ from K to K so, if σ is an automorphism of K over F .

(Refer Slide Time: 04:16)

σ is uniquely determined by the values $\sigma(\alpha_i)$ $i=1 \dots s$

$\sigma|_F = \text{id}_F$

$F(\alpha_1, \alpha_2)$
 \downarrow
 $F(\alpha_1)$
 \downarrow
 F

Result: $\alpha \in K/F$ & let $m_\alpha(x) \in F[x]$ be its minimal polynomial.

Then $\forall \sigma \in \text{Aut}(K/F)$, $\sigma(\alpha)$ is a root of $m_\alpha(x) \Rightarrow \sigma(\alpha) \in \{\text{roots of } m_\alpha \text{ in } K\}$

This σ is uniquely determined once I tell you what it does to the α . So, σ is uniquely determined by the values of σ by the values σ evaluated on these

generators. Why is that? Well, because sigma recall, sigma on F is already the identity I know how to evaluate sigma on elements of F. And then on other elements once I know the value on sigma alpha 1, this determines sigma uniquely on the first extension.

So, I just argue extension by extension. I know the value on F, its identity and I know the value on the generator alpha 1. So, that uniquely determines the value of sigma on F alpha 1. So, that that is like sort of an easy exercise and since I know the value on F alpha 1, then I adjoin just one more element and the value on of sigma on alpha 2 together with its value on the field F alpha 1 will generate, will tell me how to define, will uniquely determine sigma on F alpha 1 alpha 2 and so on.

So, I just go extension by extension and so, the (value) you know what it does is it determines sigma uniquely on K. All values on K are uniquely determined by just knowing the values on the generators, but observe that the possible candidate values for the generators are only finitely many.

In other words, so observe or recall the following fact; if I had an element alpha in this extension K over F then and say and let m_α denote its m_α of x in $F[x]$ be its minimal polynomial. So, this is the the minimal irreducible polynomial satisfied by alpha with coefficients in F, then so, let then observe for all sigma which is an auto morphism of K which fixes F sigma of alpha is also a root of the same minimal polynomial.

Sigma of alpha is a root of m_α of x . So, this argument has occurred many times before that if alpha is the root of some polynomial then sigma of alpha is also the root of the same polynomial over the base field, because sigma fixes the coefficients from the base field. So, given this, what does it imply in particular? m_α of x only can have finitely many roots in K.

(Refer Slide Time: 07:28)

Finite Galois Extensions

Theorem: Let K/F be a finite extension. Then K/F is a Galois extension $\Leftrightarrow [K:F] = |\text{Aut}(K/F)|$

Proof: $\Gamma := \text{Aut}(K/F) = \{ \sigma \in \text{Aut}(K) \mid \sigma|_F = \text{id}_F \}$

Observe: $[K:F] < \infty \Rightarrow |\Gamma| < \infty$

finite $\left\{ \begin{array}{l} F(\alpha_1, \alpha_2) \\ F(\alpha_1) \\ F \end{array} \right\}$ $\Rightarrow K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ for some $n \geq 0$.

$\sigma: K \rightarrow K \quad \sigma \in \text{Aut}(K/F)$

$\alpha_1 \begin{array}{c} \nearrow \sigma \\ \rightarrow \sigma \\ \searrow \sigma \end{array}$

$\alpha_2 \begin{array}{c} \nearrow \sigma \\ \rightarrow \sigma \\ \searrow \sigma \end{array}$

$\alpha_3 \begin{array}{c} \nearrow \sigma \\ \rightarrow \sigma \\ \searrow \sigma \end{array}$

$\Rightarrow |\Gamma| < \infty$

\Rightarrow Artin's theorem applies:

$(\Gamma \subseteq \text{Aut}(K))$
 \parallel
 $\text{Aut}(K/F)$
 \downarrow
 $F \subseteq K^\Gamma$

$\left(\begin{array}{c} K \\ | \\ K \\ | \\ K^\Gamma \\ | \\ F \end{array} \right) |\Gamma|$

$[K:K^\Gamma] = |\Gamma|$
Conclusion
 $[K:F] = |\Gamma|$
 $\Leftrightarrow [K^\Gamma:F] = 1$
 $\Leftrightarrow K^\Gamma = F$
 $\Leftrightarrow K/F$ Galois!

This means that sigma of alpha is only one of finally many possibilities. So, this belongs to the set of roots of m alpha in K. So, each sigma alpha i has finitely many choices. So sigma alpha 1, I can possibly map it to one of the many possibilities. So, sigma alpha 2, similarly there are only finitely many choices and so on. So, what does this mean? Finally, it means that, so maybe I should say alpha 1 can map under sigma to only one of the many choices and so on.

So, this finally implies that the possible values of sigma itself is only finitely many. So, this in particular implies that the possible choices for elements sigma of gamma itself is only finitely many. So, this is just the simple finite observation that if the extension is finite then the group of automorphisms which fix the base field is also necessarily a finite group.

Now, that means that we can now apply Artin's theorem. So, observe $\text{mod } \Gamma$ is finite implies Artin's theorem applies and what it Artin's theorem say? It said that if you take K and Γ was any finite so, what was the hypothesis here? Γ needed to be any finite subgroup of the group of automorphisms of K .

So, in particular we have taken Γ to be $\text{Aut } K/F$, that is known to be finite now case and Artin's theorem says that if you look at K as an extension of K/Γ so, then the theorem says that this extension has degree exactly equal to the cardinality of Γ . So, this is exactly Artin's theorem.

This is the (concept), this is the assertion of Artin's theorem. But in our case, Γ is something special. Γ is actually the group $\text{Aut } K/F$, which means it is the set of all automorphisms of K , which leave elements of F fixed pointwise. What does that mean? Well, that says that K/Γ actually contains F .

So this means in particular that F elements of F certainly lie inside the fixed field of Γ . That is how Γ is defined in this case. So that is, that is our case. So, what is this say? This says then, that this extension has degree $\text{mod } \Gamma$ according to Artin's theorem. So, well what is it that we want to conclude?

So, conclusion is that the full extension the overall extension from K to F also has degree $\text{mod } \Gamma$ if and only if the extension on the bottom $K/\Gamma/F$ has degree 1 because Artin's theorem already told you that the top bit has degree equal to $\text{mod } \Gamma$. So, this is what we have concluded, but this last conclusion just says that K/Γ is equal to F .

A degree 1 extension is just the base field itself. Now, K/Γ equals to F should be a familiar statement. So, recall this is exactly one of the characterizations of Galois extension. That if (Γ) if I take the group Γ to be the auto morphism group of K over F and I look at the fixed field of that group of automorphisms then it should be exactly F .

So, this recall from our earlier theorem on characterization of Galois extensions says exactly that K/F is Γ . So, that proves this rather nice characterization of finite Galois extensions. So, this is yet another characterization now, purely in terms of the degree of the extension, says that the extension degree must be the cardinality of the group of F automorphisms of K .

(Refer Slide Time: 11:48)

Proposition: let K be any field and $\Gamma \subseteq \text{Aut}(K)$ be a finite subgroup. Then (i) K/K^Γ is a finite Galois extension


(ii) $\text{Aut}(K/K^\Gamma) = \Gamma$

Proof: let $F := K^\Gamma$ and $G = \text{Aut}(K/K^\Gamma) = \text{Aut}(K/F)$

Observe: $\Gamma \subseteq G$ by definition since elts of Γ fix K^Γ pointwise.

$\Rightarrow K^\Gamma \supseteq K^G \supseteq F \Rightarrow K^G = F = K^\Gamma$

$\Rightarrow K/F$ is Galois (thm of Galois)



Now, let us also write out another corollary, sort of along the same lines of Artin's Theorem. So, let me call this proposition, this proposition says the following; let K be any field and γ a finite subgroup of the group of automorphisms. This is the same hypotheses as in Artin's theorem. Then two statements number one; K over K^γ , because this is a finite extension because Artin's theorem tells you that it is the cardinality, the degree of the extension is the cardinality of γ .

But we want to claim more than that. This is finite Galois extension, finite is already done by Artin. So, we are just trying to prove the Galois bit now. And statement 2; the group of automorphisms of K which leave K^γ fixed is exactly γ . So let us prove this. So let us give this a name. Let us call this fixed field as K^γ and let us call this group of automorphisms as G .

So, we need to say something about F and G . This theorem the two parts; so, observe that with these definitions, what do we know that firstly, that F so, F is K^γ so, observe G is definitely more than γ . So, γ is a sub of G . So observe, γ is actually a subgroup of G . Why? Well by definition because let us see if I take elements of γ then by definition they fix the elements of K^γ more or less this is by definition.

Since elements of γ certainly fix K^γ pointwise. That is how K^γ is defined and what is G ? G saying; take all automorphisms which fix elements of K^γ pointwise. So the original elements of γ are certainly part of this part of this. So, γ is

definitely a subgroup of G . But what does that imply in particular? It says that the fixed field of γ , so γ is smaller than G . So the elements of K which are fixed by γ is definitely a superset of the elements of G elements of K , which are fixed by G .

So, when you have a larger group, it fixes fewer elements in general. So, I know this K γ contains K G , but here is something that we know, what is G ? G is just the space of all automorphisms of K which fix F . So, remember F is the same as K γ for me. So, this just says that elements of G certainly fix F .

So, the fixed field of G certainly contains F in our case but so, you know, so what is on the left hand what is on the other end are actually the same. This is also F and that is also F . So, we conclude from this that the fixed field of this potentially larger group G is actually the same as the fixed field of the smaller group γ .

So, this is the first, this is the first conclusion and further; this statement here that K G is actually equal to F . What does this say? Just like we did in the previous part, this just says that the fixed field, so what is G ? G is exactly the group of automorphisms of K over F . And if the fixed field of this group is F , this exactly means that K over F is Galois is the, this is the equal and characterization.

So this is our previous theorem, characterization of Galois or Galois extensions, in terms of the fixed fields. So that is proved the first part because finite, we already knew. So now let us do the second part. We need to check that the auto morphism group is exactly γ . So, what do we know?

(Refer Slide Time: 17:17)

(ii) By our previous theorem, $[K:F] = |G| = |\text{Aut}(K/F)|$

||

$[K:K^\Gamma] = |\Gamma|$ (by Artin's theorem)

$\Rightarrow G \supseteq \Gamma \text{ \& } |G| = |\Gamma| \Rightarrow G = \Gamma$.

Proposition: Let K be any field and $\Gamma \subseteq \text{Aut}(K)$ be a finite subgroup. Then (\Leftarrow) K/K^Γ is a finite Galois extension

(ii) $\text{Aut}(K/K^\Gamma) = \Gamma$

Proof: Let $F := K^\Gamma$ and $G = \text{Aut}(K/K^\Gamma) = \text{Aut}(K/F)$

Observe: $\Gamma \subseteq G$ by definition since elts of Γ fix K^Γ pointwise.

$\Rightarrow K^\Gamma \supseteq K^G \supseteq F \Rightarrow K^G = F = K^\Gamma$

$\Rightarrow K/F$ is Galois (char of Galois)



Part to prove the second part. So, we therefore know so because we have just shown it is Galois. So by our previous theorem, that we just which characterizes finite Galois extensions. We know the following that the degree of the extension must be equal to the cardinality of the Galois group. So this is cardinality of $\text{Aut } K$ over F .

But well recall, K over F , on the other hand is K over K^Γ . That is how I first defined. And this by Artin's theorem K , over K^Γ is mod Γ by Artin's theorem. So what is this say? Well, it says G and Γ had the same cardinality and G contains Γ to begin with. Here is that Γ subset of G .

So this means that γ contains, γ is a sub of G and they have the same cardinality means they must be equal to each other. So the key point here is really the following; that we a priori, potentially have a larger group G , it could be bigger than γ , but the fixed fields are the same. That is what we are able to prove from this.

And the fact that they have the same fixed field then also implies this case that the groups themselves are the same. So all of these arguments, so this is sort of a, maybe a small argument split out of this broader thing of Galois theory. We will soon see that this, forms part of what is called the fundamental theorem of Galois theory. So that is, that is going to be what we will do next.