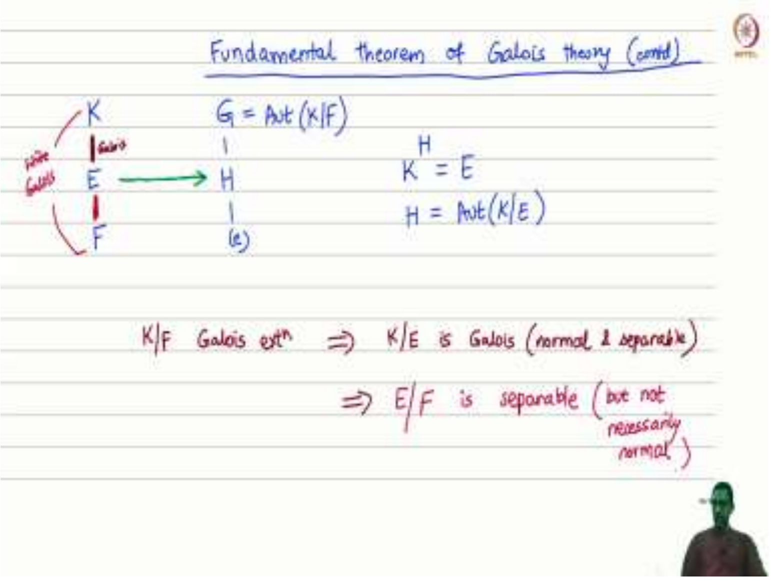
Algebra - II
Professor S Viswanath
Department of Mathematics
The Institute of Mathematical Science
Lecture 37
The Fundamental Theorem of Galois Theory - II

(Refer Slide Time: 00:14)



Fundamental theorem of Galois theory (contd)

$$\begin{tikzcd} K \arrow[d, dash, "\text{Galois}"] & G = \mathrm{Aut}(K/F) \arrow[d, dash] \\ E \arrow[d, dash] \arrow[r] & H \arrow[d, dash] \\ F & (e) \end{tikzcd}$$

$K^H = E$

$H = \mathrm{Aut}(K/E)$

K/F Galois ext^n $\Rightarrow$ K/E is Galois (normal & separable)

$\Rightarrow$ E/F is separable (but not necessarily normal)

To recall we talked about the fundamental theorem of Galois Theory. So what we will do is, say a few more things about it. So continued; so, observe that the following is really the main content of the theorem that if I have a Galois extension, K over F, so here is a finite Galois extension K over F, then the intermediate sub fields of this extension are in bijection with the, let us draw the group picture on the other side.

This is the automorphisms of K over F. This is the identity subgroup and I can look at subgroups of G. So subgroups by definition are necessarily subsets of G which contain the identity. So, these intermediate extensions e are in bijection with the subgroups of G and this map is sometimes called the Galois correspondence.

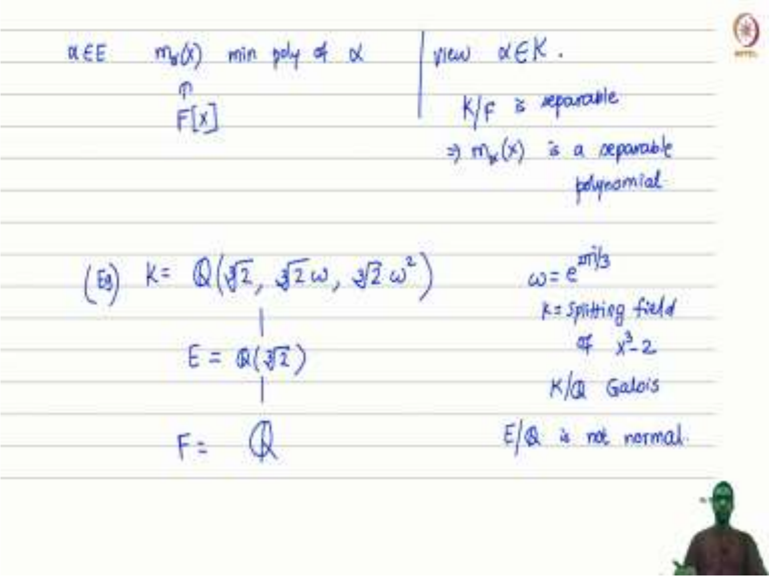
So, there are sort of maps in both directions. We know how to, given H is obtained as the fixed field of H and given E H is obtained as the automorphisms of K which are identity on E. Now, the one thing that we did say, as part of the proof of this, this bijective correspondence is that if K over F is Galois, then so is K over E.

So this is also automatically a Galois extension. And so, in fact let us just write this down K over F is a Galois extension implies in fact, this is true even if it is not finite K over E is

Galois and that just followed because of we use the normal and separable definition. We just have to check that, when you think of K as an extension of E, it continues to be normal and separable.

However the same is not true of E (kind) thought of as an extension over F. So this bottom extension here is not necessarily Galois but there is certainly one thing we can say about it, which is that it is always a separable extension but not necessarily normal. So separability is easy to see because what does separability mean?

(Refer Slide Time: 03:19)



$\alpha \in E$ $\quad m_\alpha(x)$ min poly of α

$\in F[x]$

view $\alpha \in K$.

K/F is separable

$\Rightarrow m_\alpha(x)$ is a separable polynomial

(Eg) $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$

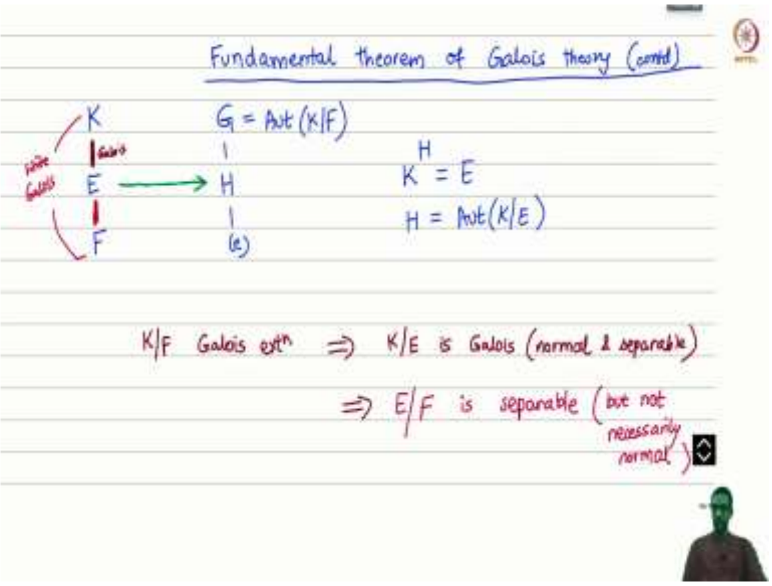
$$\begin{tikzcd} K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) \arrow[d, dash] \\ E = \mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash] \\ F = \mathbb{Q} \end{tikzcd}$$

$\omega = e^{2\pi i/3}$

K = Splitting field of $x^3 - 2$

$K/\mathbb{Q}$ Galois

$E/\mathbb{Q}$ is not normal



Fundamental theorem of Galois theory (contd)

$$\begin{tikzcd} K \arrow[d, dash, "\text{Galois}"] & G = \mathrm{Aut}(K/F) \arrow[d, dash] \\ E \arrow[r] \arrow[d, dash] & H \arrow[d, dash] \\ F & \{e\} \end{tikzcd}$$

finite Galois

$K^H = E$

$H = \mathrm{Aut}(K/E)$

K/F Galois ext^n $\Rightarrow$ K/E is Galois (normal & separable)

$\Rightarrow$ E/F is separable (but not necessarily normal)

It just says if you take any element of E, then it has to have its minimal polynomial must be a separable polynomial over F. So if you take an element alpha in E and look at its minimal polynomial m alpha of x, minimal polynomial of alpha over the base field, then this must be separable but observe that the minimal polynomial of alpha you know, you can think of alpha as another element of V or an element of K, the minimal polynomial over F is the same. It is still m alpha of x.

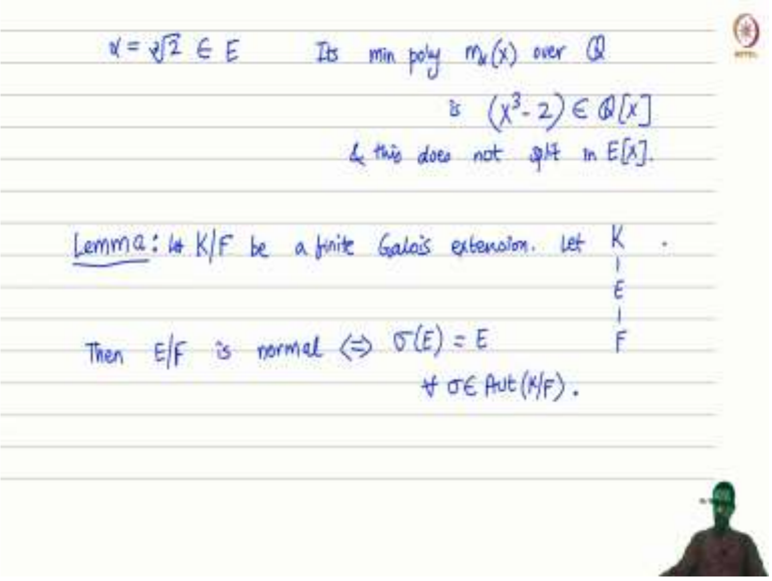
So, observe that if I view alpha as an element of K, then what do we know? Well, we know that K over the base field is separable and the minimal polynomial m alpha is the same whether you think of alphas belonging to K or E. m alpha of x is therefore a separable polynomial and that does the job.

So this is more or less a trivial consequence of the definition. So, separability sort of, is inherited by intermediate extensions but normality is not so and let us give an example where normality will not be there for an intermediate field and so here is a Q cube root of 2, cube root of 2 omega, cube root of 2 omega squared, omega being the cube root of unity.

Then observe that this is nothing but the splitting field so over Q, my base field is Q. So we looked at this example before, K is nothing but the splitting field of the polynomial x cubed minus 2 and it is therefore normal and it is a separable extension because we are over characteristic 0, where algebraic extensions are automatically separable.

So this is a therefore it is Galois because it is both normal and separable. So K over Q is definitely a Galois extension. But here is an intermediate field, which fails to be Galois. So we can just adjoin one of them, let us adjoin only cube root of 2, then if this is E observe that E over Q is not a normal extension.

(Refer Slide Time: 06:11)

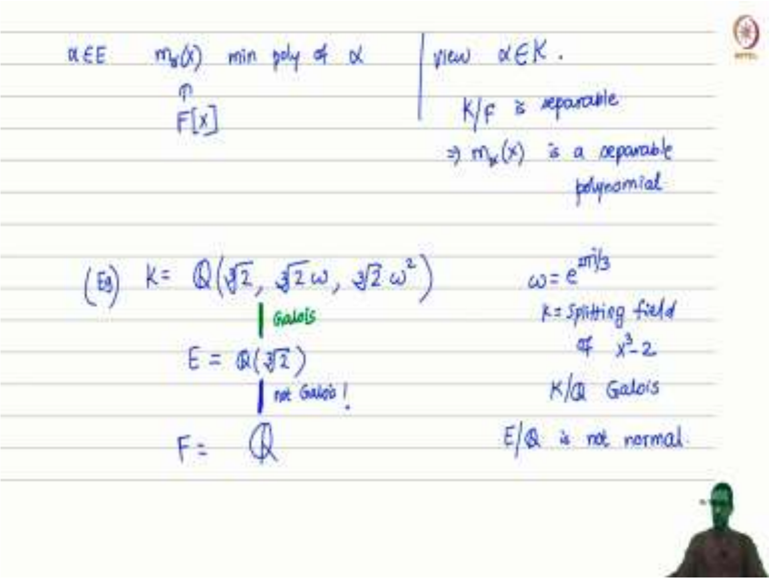


$\alpha = \sqrt[3]{2} \in E$ Its min poly $m_\alpha(x)$ over $\mathbb{Q}$ is $(x^3-2) \in \mathbb{Q}[x]$ & this does not split in $E[x]$.

Lemma: let K/F be a finite Galois extension. Let

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

Then E/F is normal $\Leftrightarrow$ $\sigma(E) = E$ $\forall\, \sigma \in \mathrm{Aut}(K/F)$.



$\alpha \in E$ $m_\alpha(x)$ min poly of α $\in F[x]$

view $\alpha \in K$. K/F is separable $\Rightarrow m_\alpha(x)$ is a separable polynomial

(Eg) $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$

$$\begin{tikzcd} K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) \arrow[d, dash, "\text{Galois}"] \\ E = \mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash, "\text{not Galois!}"] \\ F = \mathbb{Q} \end{tikzcd}$$

$\omega = e^{2\pi i/3}$

K = Splitting field of x^3-2

$K/\mathbb{Q}$ Galois

$E/\mathbb{Q}$ is not normal.

Why is that? Because recall, what does normal mean? If I take any element of E, it is minimal polynomial, over Q must split in E but in this case, if I take the element alpha equals cube root of 2 in E, it is minimal polynomial over Q. So what is the minimal polynomial over Q is, well, it is just x cube minus 2. We have shown that x cubed minus 2 is an irreducible polynomial in Q x and this polynomial, you know it does not split our E as we see.

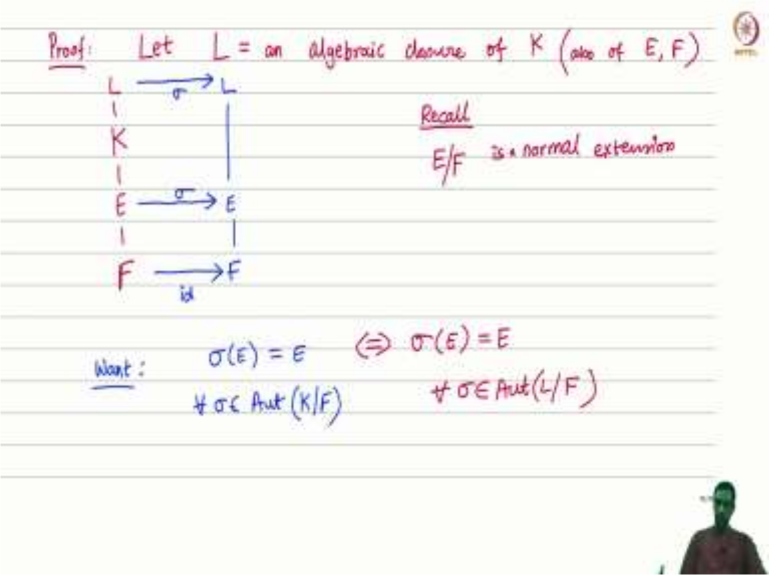
Its roots, all its roots do not lie in E, you have to go all the way to K to get so this polynomial is this and this does not split in E x. It does not split meaning; it does not, cannot be written as a product of linear factors. Therefore, E is not normal.

So, here is an example of an intermediate field of a Galois extension, which is not normal over the base field. So this is not a Galois extension. Of course, here you know, we can always say that the top will be always be this will be Galois for sure. So, that sort of comes for free. Now, what we need to do is for sort of for the second part of the fundamental theorem of Galois Theory, we really want to understand when an intermediate field would be normal over the bass field.

When do we have normality? So, let me state a lemma which allows us to understand this precise situation. So let K over F be a finite Galois extension, let E be an intermediate field. So, just denoted like this. Let E be an intermediate field, then E over F is normal. So, remember separable is always true. So, normality would then imply that it is a Galois extension.

E over F is normal, if and only if the following is true; that sigma applied to E gives you back E for all elements sigma in the group G of automorphisms of K over F. So, this is the statement that E stabilized by all automorphisms or by the entire Galois group of K over F. So, let us prove this. It is a easy lemma. In fact, you have seen something like this already, when we talked about normal extensions.

(Refer Slide Time: 09:11)



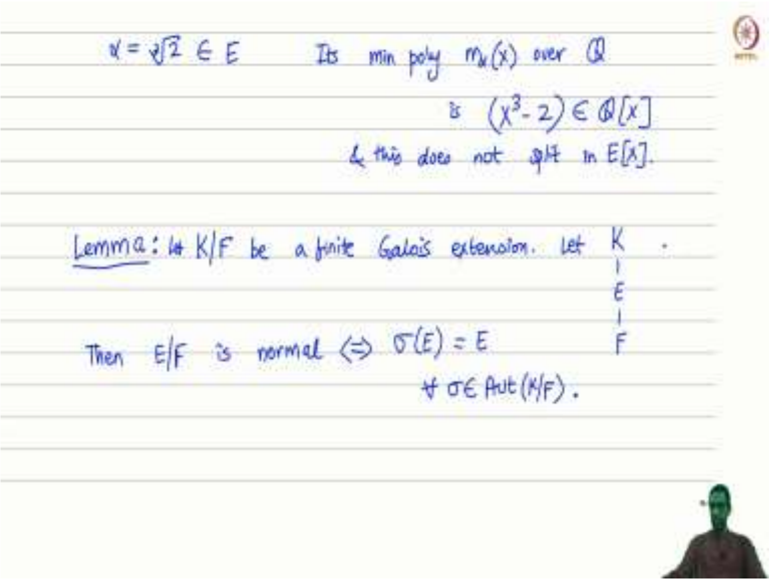
Proof: Let L = an algebraic closure of K (also of E, F)

$$\begin{tikzcd}
L \arrow[r, "\sigma"'] \arrow[d, dash] & L \arrow[dd, dash] \\
K \arrow[d, dash] & \\
E \arrow[r, "\sigma"] \arrow[d, dash] & E \arrow[d, dash] \\
F \arrow[r, "id"'] & F
\end{tikzcd}$$

Recall

E/F is a normal extension

Want: $\sigma(E) = E$ $\forall \sigma \in Aut(K/F)$ $\Leftrightarrow$ $\sigma(E) = E$ $\forall \sigma \in Aut(L/F)$



$\alpha = \sqrt[3]{2} \in E$ Its min poly $m_\alpha(x)$ over $\mathbb{Q}$

is $(x^3-2) \in \mathbb{Q}[x]$

& this does not split in $E[x]$.

Lemma: let K/F be a finite Galois extension. Let

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

Then E/F is normal $\Leftrightarrow$ $\sigma(E) = E$

$\forall\, \sigma \in \mathrm{Aut}(K/F)$.

So, recall that proof this this sort of statement should be familiar from our earlier discussion of normal extensions; so, we will introduce the algebraic closure. So let L be an algebraic closure of K, this be an algebraic closure of K. So I have K, now I also have L, there is E, there is F and of course, as we remarked earlier, an algebraic closure of K.

Since K is algebraic over E and F, L will also be algebraic over K, E and F and so an algebraic closure of K, it is just an algebraic extension of K which is algebraically closed. So this is also the algebraic closure. So you can also think of L as also an algebraic closure of E as well as of F. So we will take such an algebraic closure and what is it that we know about normal extensions?

So observe, recall other we have talked about this before; E over F is normal, it is a normal extension, is a normal extension that is a characterization of normality in terms of what automorphisms do to it, if and only if every automorphism sigma so if and only if sigma of E is E for all automorphisms of L of an algebraic closure, which our identity on the base field. Now the words, if I take L, F, take a map from L to L any automorphism sigma, which restricts to the identity map on F.

So, look at this take such a map, then under this map, the image of E will just be E itself. So this will actually go to E that is what we mean. and this is equivalent to being normal, E is normal over F, even only if this happens for every sigma, sigma E is equal to E and recall, we proved this fact from the definition of normality in terms of splitting fields and so on.

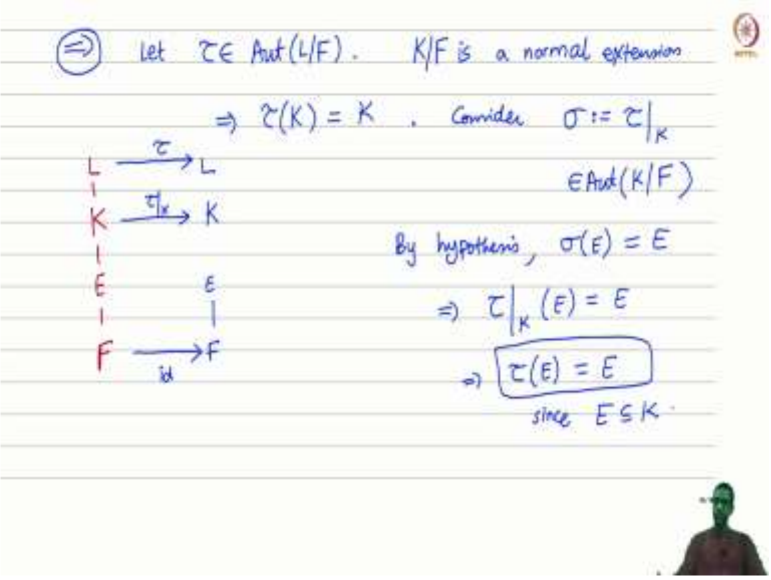
So this is the characterization we are going to use. So, what we want to prove is almost this. See we want to prove this not, I mean we want to prove it for K instead of L, L is the algebraic closure, we want to prove it for our normal extension. We want to prove it for K, which contains E, but K is normal that somehow the key point K is normal over F.

So let us actually do the proof now. We have to somehow replace L by K everywhere. That is the broad model. So let us prove the lemma. So, proof of lemma, let us prove this implication first, which is, if sigma E is E for all sigma in Aut K F, if I want to prove that E, F is normal. So what does that mean?

I have to show that sigma E is E for all sigma in Aut L F. So it is nice to, what we need to prove want to prove is really the following. We want to show that this, so this is exactly normality but we want to show that this is the same as, this is the same as sigma E is equal to E for all sigma in Aut K F.

This is exactly what we are trying to show. So let us prove one implication. So if it is true, over K so, I will now prove the forward implication. If it is true for K and show it is true for L. If it is true for L and show it is true for K.

(Refer Slide Time: 13:20)



($\Rightarrow$) Let $\tau \in \mathrm{Aut}(L/F)$. K/F is a normal extension

$\Rightarrow \tau(K) = K$. Consider $\sigma := \tau|_K \in \mathrm{Aut}(K/F)$

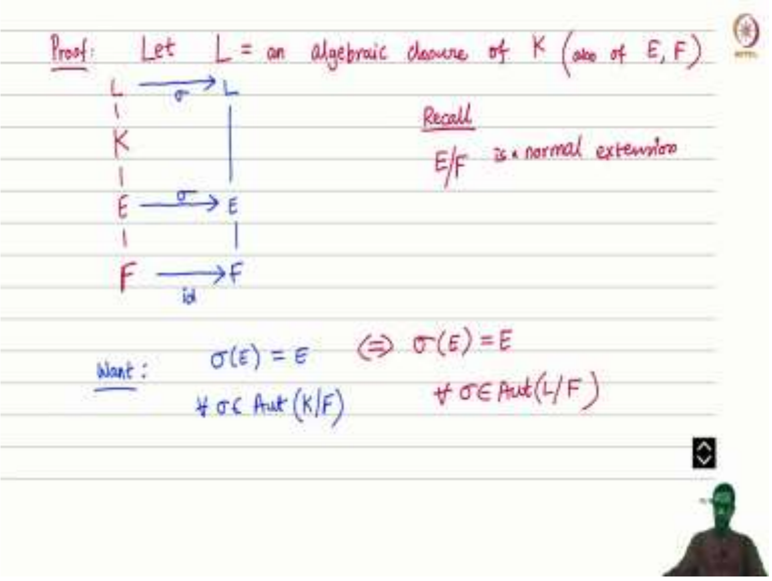
$$\begin{tikzcd}
L \arrow[r, "\tau"] \arrow[d, dash] & L \\
K \arrow[r, "\tau|_K"] \arrow[d, dash] & K \\
E \arrow[d, dash] & E \arrow[d, dash] \\
F \arrow[r, "id"'] & F
\end{tikzcd}$$

By hypothesis, $\sigma(E) = E$

$\Rightarrow \tau|_K (E) = E$

$\Rightarrow \boxed{\tau(E) = E}$

since $E \subseteq K$.



Proof: Let L = an algebraic closure of K (also of E, F)

$$\begin{tikzcd}
L \arrow[r, "\sigma"'] \arrow[d, dash] & L \arrow[dd, dash] \\
K \arrow[d, dash] & \\
E \arrow[r, "\sigma"] \arrow[d, dash] & E \arrow[d, dash] \\
F \arrow[r, "id"'] & F
\end{tikzcd}$$

Recall

E/F is a normal extension

Want: $\sigma(E) = E$ $\forall \sigma \in Aut(K/F)$ $\Leftrightarrow$ $\sigma(E) = E$ $\forall \sigma \in Aut(L/F)$

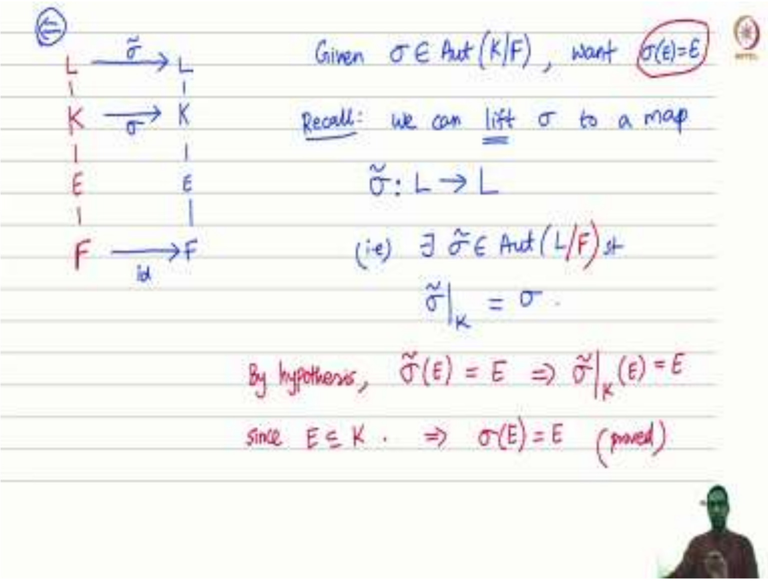
So forward implications, suppose it is true for K and we need to prove it for L. So what does that mean? Let us take an element tau, which is an automorphism of L over F and we need to look at what tau does to E. Now, observe K over F is normal. See, this is a normal extension, means I can sort of use the same argument for K.

What does that mean? In particular, it means that an automorphism of L, which is identity on F will send K to itself, this will stabilize K. Well, what does that say? It means that in this diagram that I was trying to draw here. When I, when I apply let us copy this diagram. So I take this diagram and so I started with a tau.

I need to understand what tau does to E. But I certainly know one thing, what tau does to K? What does tau do to K? Well, it maps K to itself. So let us call this tau restricted to K. So let us consider let us call it sigma, maybe sigma is the map tau restricted to K. This is now an automorphism of K and of course, it is identity continues to be identity on F because tau was identity on F.

So here is an automorphism of K which fixes F. Now by hypothesis, what did we hypothesize? Any such sigma maps E to E, this is what is given but then that just means that tau restricted to K maps E to E but well, tau restricted to K is just tau. So tau maps E to E. Why? Because E is furthers subset of K.

(Refer Slide Time: 15:40)



$$\begin{tikzcd} L \arrow[r, "\tilde{\sigma}"] \arrow[d, dash] & L \arrow[d, dash] \\ K \arrow[r, "\sigma"'] \arrow[d, dash] & K \arrow[d, dash] \\ E \arrow[d, dash] & E \arrow[d, dash] \\ F \arrow[r, "id"'] & F \end{tikzcd}$$

Given $\sigma \in Aut(K/F)$, want $\boxed{\sigma(E)=E}$

Recall: we can lift σ to a map

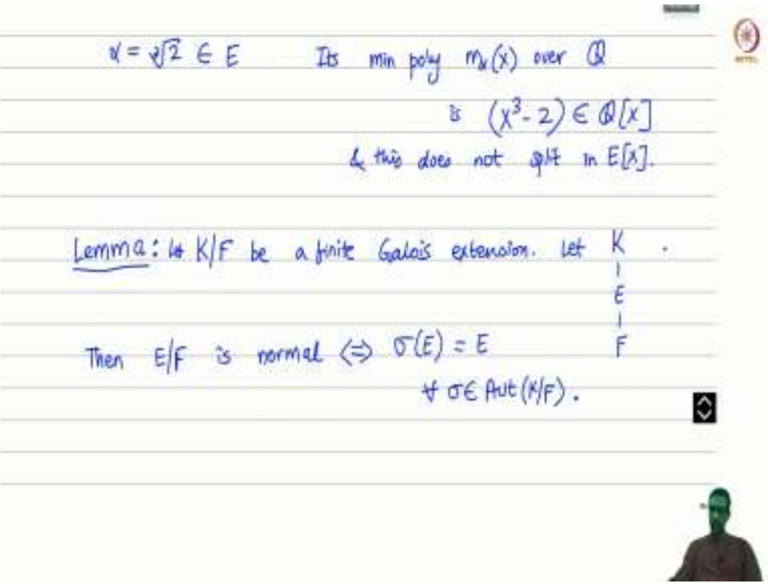
$\tilde{\sigma} : L \to L$

(i.e) $\exists\ \tilde{\sigma} \in Aut(L/F)$ st

$\tilde{\sigma}|_K = \sigma$.

By hypothesis, $\tilde{\sigma}(E) = E \Rightarrow \tilde{\sigma}|_K(E) = E$

since $E \subseteq K$. $\Rightarrow \sigma(E) = E$ (proved)



$\alpha = \sqrt[3]{2} \in E$ Its min poly $m_\alpha(x)$ over $\mathbb{Q}$

is $(x^3-2) \in \mathbb{Q}[x]$

& this does not split in $E[x]$.

Lemma: let K/F be a finite Galois extension. Let $\begin{matrix} K \\ | \\ E \\ | \\ F \end{matrix}$.

Then E/F is normal $\Leftrightarrow \sigma(E) = E$

$\forall\ \sigma \in Aut(K/F)$.

So what does that imply? Well, we have shown that tau maps E to E. This is exactly what we needed to show. So we assumed that it is true for K and we have shown that it is true for L. Conversely, suppose it is true for L and we want to show it for K. So let us paste that picture again. So here is the converse. I will try to prove the opposite implication now. So know it for L and I need to prove it for K.

So let us start with so what are we given? We are given a map from K to K and so given sigma and automorphism of K over F, I want to prove that sigma maps E to itself. I know that this is true if sigma were a map from L to L. So, what I have to do is to lift sigma to a map from L to L and recall again that we have discussed this before, when we proved uniqueness of algebraic closures and so on.

So, recall we can lift sigma to a map, sigma tilde. So what is sigma tilde? It is now an automorphism of L. Sigma tilde as a map from L to L. So, what does lift mean here? So, I mean I e, there exists sigma tilde automorphism of L, it is an automorphism of L, such that it is an extension of, well, when I restrict sigma to sigma tilde to K, I just get back sigma.

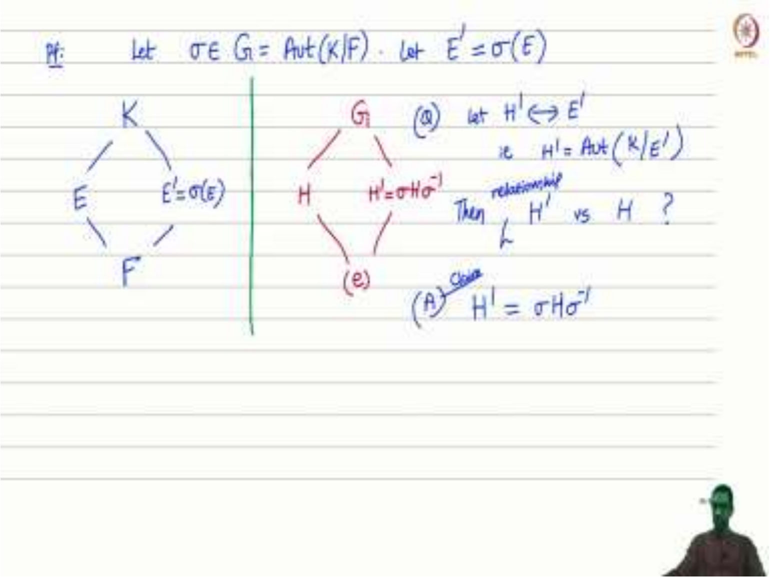
And recall this is because of the fact that L is algebraically closed. Any isomorphism of the base fields lifts to a isomorphism of the algebraic closures. This is not a unique isomorphism in general; there are many, many possible lifts. Let us pick one of them. But now we are in business because what do we know?

We know that what we want to prove is true for sigma tilde. So now by what we assumed by hypothesis? We know that sigma tilde maps E to E. Why is that? Well, because sigma tilde is an automorphism of L and I should have said it is a lift. Sigma tilde restricted to K sigma, which means that sigma tilde when you restrict to F will just be identity because sigma is identity on F.

So is sigma tilde, so for such sigma tilde we know E is mapped to E and so this implies in particular that sigma tilde restricted to K will map E to E because E is of course, a sub of K. It is the same sort of thing we said for the other part, since E is after all further inside K and that is all we need to prove.

Sigma tilde are restricted to K is exactly the original sigma. So sigma of E is equal to E. So proved; that proves the lemma here. So let us go up and see what the lemma stated. So essentially it said, for E F to be normal, all you need to do is ensure that the entire all elements of the Galois group of K the automorphisms of K over F, so this is what we usually call the Galois group.

(Refer Slide Time: 19:21)



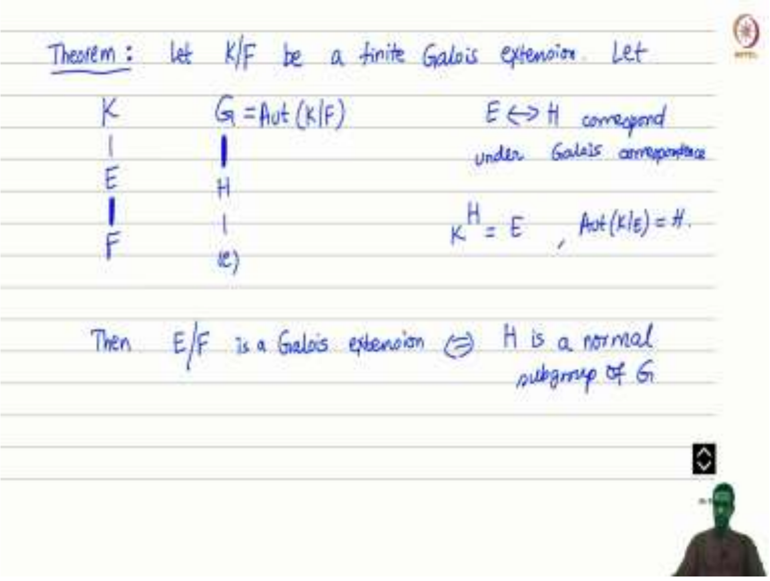
Pf: Let $\sigma \in G = \mathrm{Aut}(K|F)$. Let $E' = \sigma(E)$

(Q) let $H' \leftrightarrow E'$

ie $H' = \mathrm{Aut}(K/E')$

Then relationship H' vs H ?

(A) Claim $H' = \sigma H \sigma^{-1}$



Theorem: let K/F be a finite Galois extension. Let

$E \leftrightarrow H$ correspond under Galois correspondence

$K^H = E$, $\mathrm{Aut}(K|E) = H$.

Then E/F is a Galois extension $\Leftrightarrow$ H is a normal subgroup of G

All elements of the Galois group stabilize E, they send E to itself. So recall, I am not saying that it maps you know, it is not necessarily the identity map on E. It need not fix every element of E pointwise. It just sends E as a set to itself and now, we are ready to sort of state and prove a follow up theorem to the fundamental theorem of Galois Theory.

So, this says that, let K over F be a finite Galois extension. Then, and let us say E, so let us draw the usual figure, suppose E is an intermediate field and let G be the Galois group, G be the set of all automorphisms of K over F and H identity. So, let H, let E and H correspond to each other under the Galois correspondence.

Here what that means is of course, H K H is E automorphisms of K over E is H. They correspond to each other under the bijection then E is normal over F. So, the normality of E F is equivalent then E over F is normal or maybe I should say is Galois which is the same as saying it is normal is a Galois extinction if and only if, H is a normal subgroup of G.

So let us prove this. So we more or less set up everything we need to prove this. So, proof. So let us look at, let us let us do the following. Let us look at a slightly more general situation. So suppose sigma is an element of the Galois group. So G is the automorphisms of K over F. Let me draw the falling picture for you.

So I have K and F, and E is my intermediate field. Let us do the following; let us call E prime to be the image of E under sigma, so E prime is another intermediate field. So, here is probably how the picture looks. Both E and E prime are intermediate fields between K and F. Now, the question is the following; I know what H, what E corresponds to.

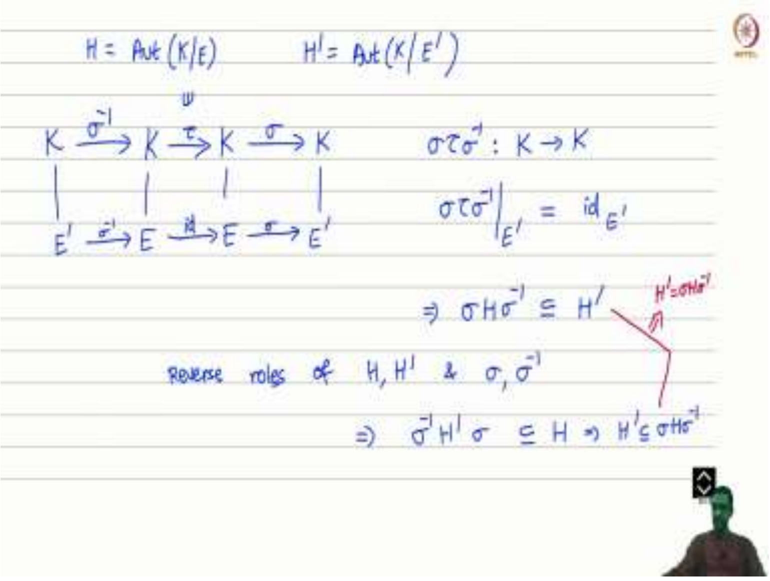
H is a subgroup that corresponds to E. The question is what is the subgroup H prime corresponding to E prime? So question; let H prime correspond to E prime under the Galois correspondence, i e H prime is just the automorphisms of G which are sorry, K which are identity on E prime.

Then the question is, how is H prime related to than H prime versus H? What is the relationship then relation? So, the natural question, so E prime remember is just sigma of E this case and the answer is rather beautiful. So, let us, let us answer this question. To do this, we'll just draw a similar looking figure on the other side.

So, let G be the group maybe I will draw it right next to this. So, let G be the full Galois group, E is the identity H is the subgroup corresponding to E and the subgroup H prime turns out to be just the conjugate subgroup sigma H sigma inverse. So, remember E prime is the conjugate sigma of E in this case.

So, just like E prime, I mean, we usually call this the conjugate field. So, just like E prime is obtained from E by applying sigma, H prime is obtained from H by conjugating by sigma. So, let us prove this. It is a rather easy proof. So, claim H prime is just the conjugate sigma in sigma inverse.

(Refer Slide Time: 24:12)



$H = \mathrm{Aut}(K/E)$ $\qquad H' = \mathrm{Aut}(K/E')$

$$\begin{tikzcd} K \arrow[r, "\sigma^{-1}"] \arrow[d, dash] & K \arrow[r, "\tau"] \arrow[d, dash] & K \arrow[r, "\sigma"] \arrow[d, dash] & K \arrow[d, dash] \\ E' \arrow[r, "\sigma^{-1}"] & E \arrow[r, "id"] & E \arrow[r, "\sigma"] & E' \end{tikzcd}$$

$\sigma\tau\sigma^{-1} : K \to K$

$\sigma\tau\sigma^{-1}\big|_{E'} = id_{E'}$

$\Rightarrow \sigma H \sigma^{-1} \subseteq H'$

$H' = \sigma H \sigma^{-1}$

Reverse roles of H, H' & σ, σ^{-1}

$\Rightarrow \sigma^{-1} H' \sigma \subseteq H \Rightarrow H' \subseteq \sigma H \sigma^{-1}$

Proof: more or less straightforward. So, what are H and H prime? H is all automorphisms of K which are identity on E; H prime is all automorphisms of K which are identity on E prime. How do you relate these two sets of automorphisms? Well, suppose I have an automorphism of the first kind; a map from K to K.

Suppose tau is like this. It is an automorphism of K which is identity when you restrict it to E. So, when I restrict tau to E, I get an identity. So, from such a tau, how do you manufacture a tau prime which belongs to the other set which is identity on E prime rather than on E? Well, here is what you do.

Remember, E and E prime are isomorphic. They have the map sigma connecting them. Sigma is E prime is exactly sigma of E. So from E to E prime, I have a map sigma from E prime to E; I have the inverse map sigma inverse and so let us do the following. Let us just apply sigma and sigma inverse to both sides.

So now when you restrict this map, so consider the following diagram, I look at sigma inverse the map from K to K, its restriction to E prime is exactly going to map E prime to E. That is the definition more or less and then I look at the next map tau, its restriction to E is the identity and then the map after that is sigma whose restriction to E is now the map sigma, which takes it to E prime.

So now observe that sigma tau sigma inverse, is this automorphism from K to K. How does it restrict sigma tau sigma inverse when you restricted it to E prime? Well, it is just the composition of these three maps, which is the identity map again. It is just going to take an element of E prime back to itself.

So, what does that mean? So, what we have shown is that if we take H and I conjugate it by sigma, the answer is definitely an H prime and now, what we have to do is just to reverse the roles of H and H prime. So, reverse the roles of H and H prime meaning repeat the same argument and change sigma to sigma inverse.

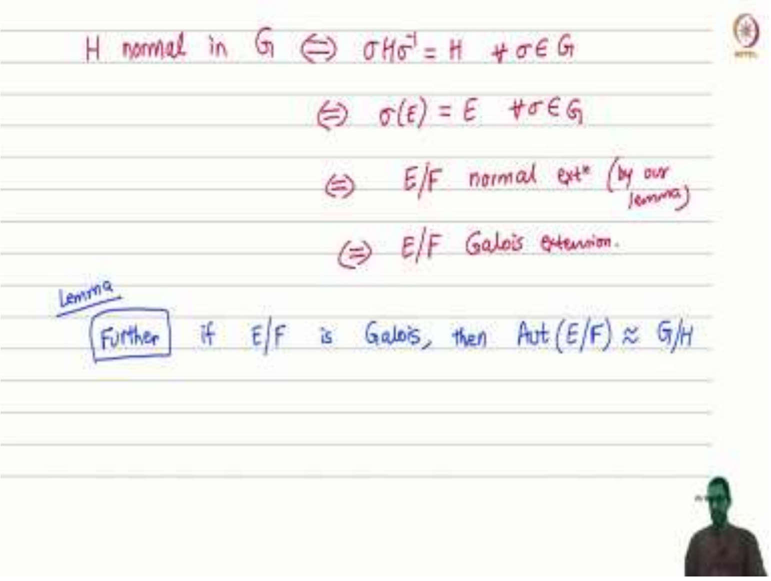
Reverse the roles of sigma and sigma inverse as well and do the same thing you will just get sigma inverse H prime sigma is contained in H and that just means you can conjugate by sigma on both sides, containment stays the same and which means if you look at these two final equations, this implies that the two are equal. This means H prime is sigma, sigma inverse.

Now, what does that give us? We have managed to prove our claim that H prime is just sigma H sigma inverse. Now, what does this mean? So, remember this Galois correspondence is a bijection between subfields and subgroups on the other hand. So, we conclude, so since, so by the fundamental theorem of Galois Theory, since the Galois correspondence is a bisection, one concludes the following that E and sigma E prime, so E equals E prime.

In other words E equals sigma E can only happen if and only if H equals the subgroup corresponding to E prime and this is true for all for all sigma. So E equal sigma E if and only if H equals sigma H sigma prime. This is true for every sigma in the group G.

So, what does this mean? In particular, it says if H is normal which means H equals sigma H sigma inverse for every sigma in G, then it implies that E is sigma E for every sigma in G right. So, therefore, we conclude the following; H, maybe we should do this on the next page.

(Refer Slide Time: 28:27)



$$H \text{ normal in } G \iff \sigma H \sigma^{-1} = H \quad \forall \sigma \in G$$

$$\iff \sigma(E) = E \quad \forall \sigma \in G$$

$$\iff E/F \text{ normal ext}^{n} \text{ (by our lemma)}$$

$$\iff E/F \text{ Galois extension.}$$

Lemma

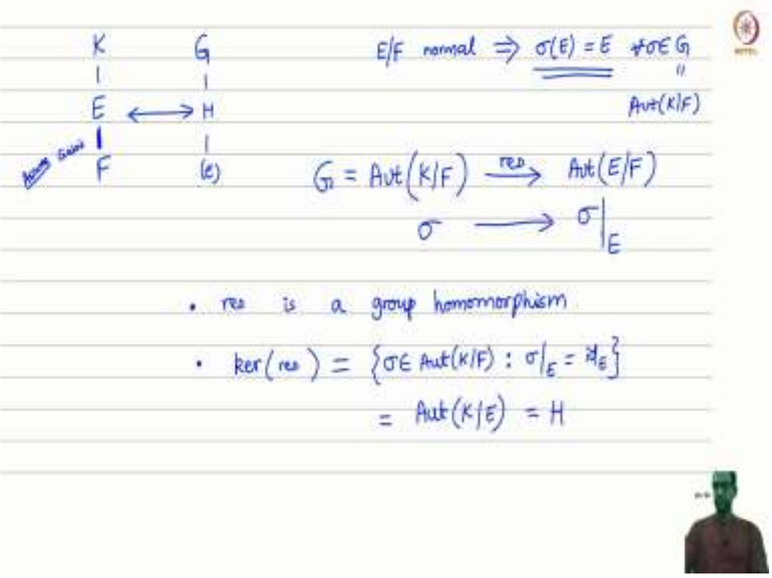
$\boxed{\text{Further}}$ if E/F is Galois, then $Aut(E/F) \approx G/H$

So let me write our final conclusion here. So, saying that H is normal in G means it has all conjugates of H coincide with itself for all sigma in the group G but from what we said, the corresponding subfields then conjugate mean the sub fields corresponding to the conjugate is this for all sigma in the group G and observe that this was exactly our lemma.

So, with said that this means that this is if and only if, in fact, E over F is a normal extension. This is the little lemma that we proved by our lemma and finally, the observation we made that separability anyway comes for free. So, normality is enough to say that E over F is a Galois extension. So, that completes the proof of this the second part.

In fact, we can say a little bit more, further if E over F is normal, with the same as Galois, is Galois. Then, we know something about the Galois group, then the Galois group, the automorphism group of E over F is in fact isomorphic to the quotient group G over H. So H remember is normal, so G over H is actually a group. So this is the last little bit of this theorem. So maybe I will make this into a separate lemma as well and how do we prove this?

(Refer Slide Time: 30:06)



$$\begin{tikzcd}[row sep=small] K \arrow[d, dash] & G \arrow[d, dash] \\ E \arrow[r, leftrightarrow] \arrow[d, dash] & H \arrow[d, dash] \\ F & (e) \end{tikzcd}$$

E/F normal $\Rightarrow \underline{\underline{\sigma(E) = E}} \ \forall \sigma \in G$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \| $

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathrm{Aut}(K/F)$

$$G = \mathrm{Aut}(K/F) \xrightarrow{\text{res}} \mathrm{Aut}(E/F)$$
$$\sigma \longrightarrow \sigma|_E$$

- res is a group homomorphism
- $\ker(\text{res}) = \{\sigma \in \mathrm{Aut}(K/F) : \sigma|_E = id_E\}$
$\quad\quad = \mathrm{Aut}(K/E) = H$

Well, we more or less proved it along the way. So if you see, what do we know? So I am going to use the same notation as the proof. So I have K, E, F. I have G H identity and I am assuming that E and H correspond to each other under the Galois correspondence. So and further, the assumption here is that E over F is a normal extension. In other words, it is a Galois extension.

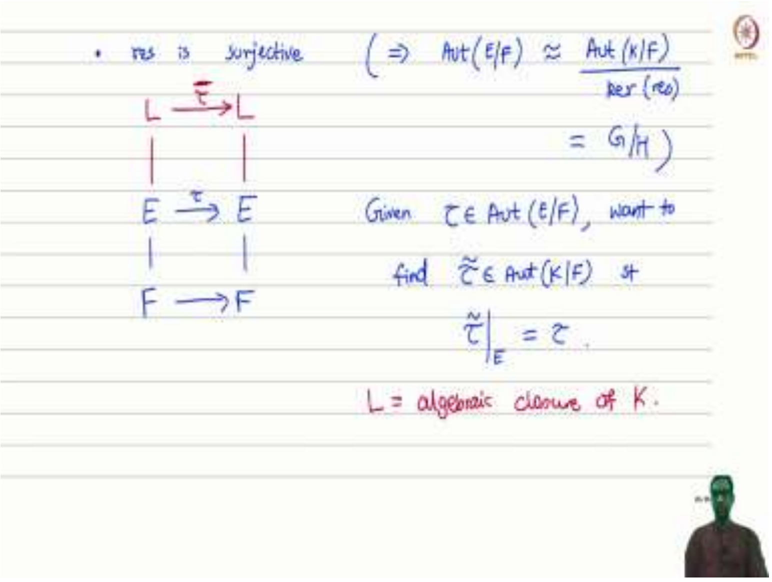
So we are assumed, assume this to be a Galois extension as well. So now observe the following. What does it mean to say E over F is Galois or normal? If and only if all elements of, this is the lemma we proved earlier, for all sigma in the group G. It is all automorphisms of K over F.

Now, what that tells us is the following. I can take the group automorphisms of K over F and to each element sigma there, I can associate its restriction. So there is a restriction map. So let us call it res for restriction. I can restrict any such sigma to the subfield E and what that gives me is of course, an automorphism of E.

That is what this lemma tells me. So this implies that so sorry, E over F is normal. So I just want one implication implies this is true. So there exists a restriction map, which looks like this, it gives me a map from Aut K, F to Aut E, F. Now observe that this restriction map has kernel. So this is a group homomorphism. So what are the properties of res? res is a group homomorphism.

That is easy to check because it is, it is doing nothing, it is only restricting it to a smaller subset. Property 2; is that it is kernel. So what is the kernel of this map? Well, that is all those elements of sigma whose all sigma in Aut K F, whose restriction to E is the identity and that by definition, is Aut K E. That is your H. Good. So we are already getting close. So the kernel of this map is H and so it is a map from G and the claim is that the rest is an onto map.

(Refer Slide Time: 32:44)



• res is surjective $\left(\Rightarrow \operatorname{Aut}(E/F) \simeq \dfrac{\operatorname{Aut}(K/F)}{\ker(\text{res})} = G/H \right)$

$$\begin{tikzcd}
L \arrow[r, "\tilde{\tau}"] \arrow[d, dash] & L \arrow[d, dash] \\
E \arrow[r, "\tau"] \arrow[d, dash] & E \arrow[d, dash] \\
F \arrow[r] & F
\end{tikzcd}$$

Given $\tau \in \operatorname{Aut}(E/F)$, want to find $\tilde{\tau} \in \operatorname{Aut}(K/F)$ st $\tilde{\tau}|_E = \tau$.

L = algebraic closure of K.

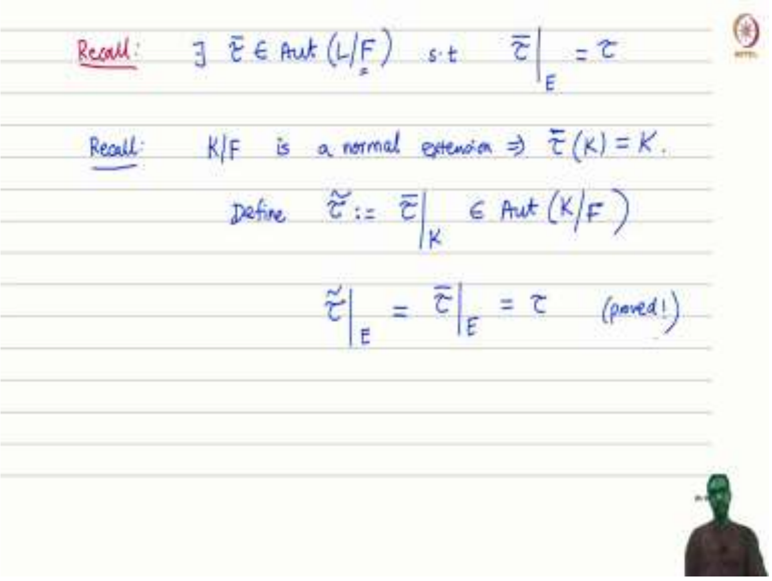
If we do that, then we are done. So, the last claim is that res is surjective and if we prove this then we are done. So, assuming the claim of this would imply then that the automorphisms of E over F is isomorphic to Aut K over F, modulo the kernel of the restriction map, which is just G over H and that would that would do the job.

So, why is this surjective? So, what does surjectivity mean? It says, if I give you an automorphism of E, so let us say I give you a map tau from E to E, which is identity on F, then you should be able to find a map from K to K such that tau is the restriction of that map. So that is what ontoness of res will meet.

So given tau from in E, F want to find an element? Shall we call it it tilde maybe, in Aut K F such that the restriction of tau tilde to E is tau. Now, well I do not offhand know how to do this extension to K. But there is something that I know how to do and that is our theorem on algebraic closures, which says, given a map, a E given a map from E to E, I can always lift it to its algebraic closure.

So let us take the algebraic closure L. So again, I am using the same notation that we used earlier in the in the lemma. So L now is the algebraic closure of K if you wish. So I can certainly lift tau there. So let us call that map as tau bar, maybe. The lift of tau I mean, there are many possible lifts but there definitely exists one lift.

(Refer Slide Time: 34:53)

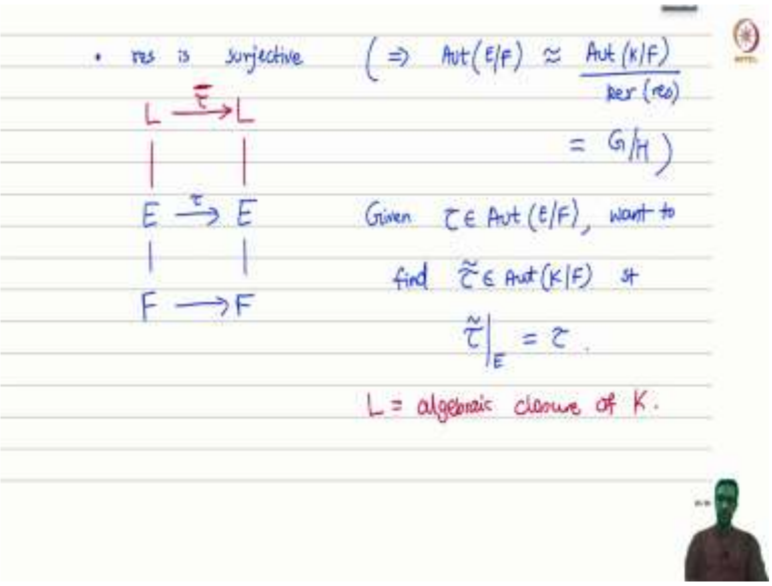


Recall: $\exists\ \bar{\tau} \in \mathrm{Aut}(L/F)$ s.t $\bar{\tau}|_E = \tau$

Recall: K/F is a normal extension $\Rightarrow \bar{\tau}(K) = K$.

Define $\tilde{\tau} := \bar{\tau}|_K \in \mathrm{Aut}(K/F)$

$\tilde{\tau}|_E = \bar{\tau}|_E = \tau$ (proved!)



- res is surjective $\left(\Rightarrow \mathrm{Aut}(E/F) \approx \dfrac{\mathrm{Aut}(K/F)}{\ker(\mathrm{res})} = G/H \right)$

$$\begin{tikzcd}
L \arrow[r, "\bar{\tau}"] \arrow[d, dash] & L \arrow[d, dash] \\
E \arrow[r, "\tau"] \arrow[d, dash] & E \arrow[d, dash] \\
F \arrow[r] & F
\end{tikzcd}$$

Given $\tau \in \mathrm{Aut}(E/F)$, want to find $\tilde{\tau} \in \mathrm{Aut}(K/F)$ st $\tilde{\tau}|_E = \tau$.

L = algebraic closure of K.

So recall the following fact about algebraic closures that there exists a map tau bar which is an automorphism of the algebraic closure L and of course it is you know, it fixes the base field. There exists this such that, tau bar restricted to E is tau because it is restriction to E is tau, that is the reason why it fixes the base field because tau fixes the base field.

But how do they get tau tilde? We do not want to go all the way to the algebraic closure; I want to get a map from K to K. Now observe this will come from the normality of K. So, now I can think of K as being in the middle and now observe K is a normal extension of F and what does normality give you?

It gives you precisely this that any automorphism of the algebraic closure will map this K to itself. So again, so we sort of are using all the various facts we have seen before. Recall K over F is a normal extension, will tell you the following that tau bar must map K to itself and now we are in business.

That is exactly what we need. So let us take this tau tilde now to be just the restriction of tau bar to K. So that will that will finish the job. So now define tau bar, sorry tau tilde to be take tau bar and just restricted to K. So we know it maps K to K. So you can restrict it to K. So what is this? This is now an automorphism of K for sure.

When you restrict tau tilde further to E, well it is the same as tau bar, restricted E. Tau tilde is really the same as tau bar when you restrict to K. So, definitely when you restrict further to E but this is just tau by definition. So again, because it is tau it fixes the base field pointwise. So that is exactly what we wanted to prove. So that is the end of proof. So this completes all the various parts of the fundamental theorem of Galois Theory.

So we will look at some applications next.