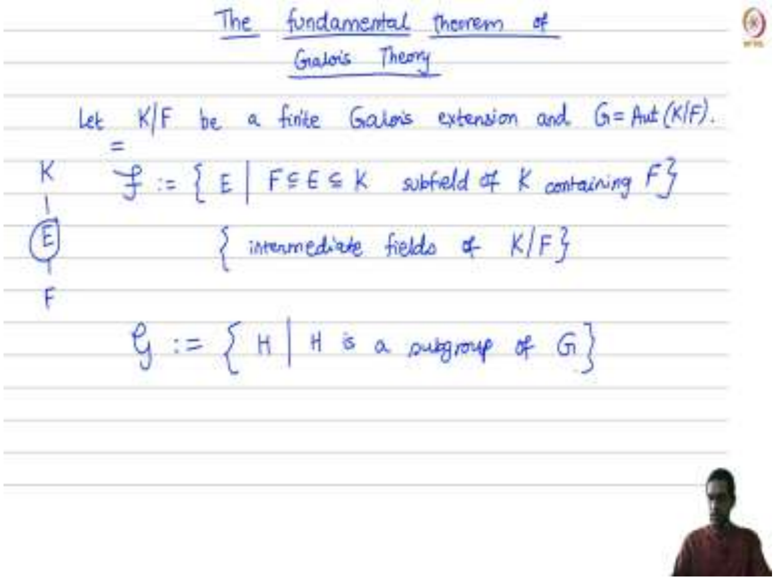
Algebra - II
Professor S Viswanath
Department of Mathematics
The Institute of Mathematical Science
Lecture 36
The Fundamental Theorem of Galois Theory - I

(Refer Slide Time: 00:14)



The fundamental theorem of Galois Theory

Let K/F be a finite Galois extension and $G = Aut(K/F)$.

$\mathcal{F} := \{ E \mid F \subseteq E \subseteq K$ subfield of K containing F $\}$

$\{$ intermediate fields of K/F $\}$

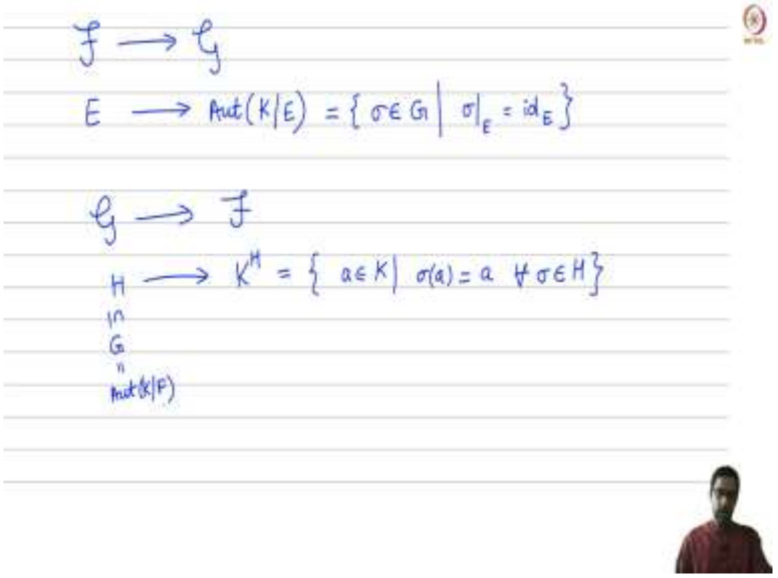
$$\begin{tikzcd} K \arrow[d, dash] \\ \boxed{E} \arrow[d, dash] \\ F \end{tikzcd}$$

$\mathcal{G} := \{ H \mid H$ is a subgroup of G $\}$

Let us talk about the fundamental theorem of Galois Theory. So we start with the Galois extension, let K over F be a finite Galois extension and we let the automorphism group, let G denote the automorphism group, K over F. So, we have two sorts of objects that are related by this fundamental theorem and they are on the one hand sub fields of K. So, let us call this F for field, script F is the set of all E, where E is a subfield of K, which contains F.

So, E is basically a subfield of K containing F and this is sometimes called the set of all intermediate fields of this extension. So K and F themselves are included in script F. So K, E is something that sits between K and F. So that is on the one hand. So the, such objects are in script F and in script G. So we will put, so script G is the other kind of object which has now subgroups.

(Refer Slide Time: 02:15)



$\mathcal{F} \longrightarrow \mathcal{G}$

$E \longrightarrow \mathrm{Aut}(K|E) = \{\sigma \in G \mid \sigma|_E = \mathrm{id}_E\}$

$\mathcal{G} \longrightarrow \mathcal{F}$

$H \longrightarrow K^H = \{a \in K \mid \sigma(a) = a \ \forall \sigma \in H\}$

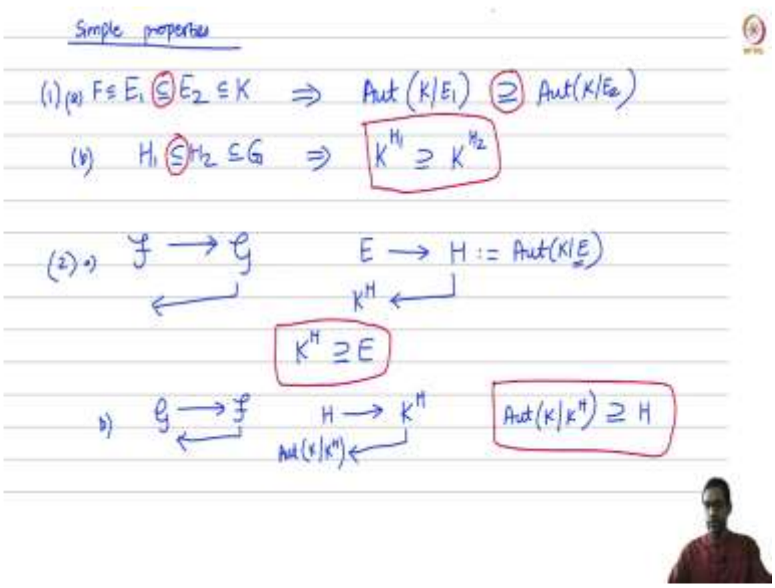
$H \subseteq G = \mathrm{Aut}(K|F)$

So this is the set of all H, such that H is a subgroup of the group G of all automorphisms and one has maps between these two sets. So, from script F to script G so given an intermediate field, E one associates, the set of all automorphisms of K, which are identity on E. So, observe this is just a set of all sigma, which is you can say it is all sigma and G. This G is automorphisms of K, which identity on F, but this is something extra is required of sigma.

Sigma restricted to E should also be identity on E. So sigma should also fix every element of E, not just every element of F. So that is one and the map in the other direction from G to script F is the following; given any subgroup H, you look at its fixed field, K H just the set of all elements of K such that sigma of a equals a for all sigma in H and as we have seen, this is a subfield.

It is, this subfield contains F definitely because the sigmas that we are looking at, the H that we are looking at is a sub of G. H is contained in G and G is all those automorphisms of K, which are definitely identity on F. So sigma will definitely fix F in this case. So these are maps in both directions.

(Refer Slide Time: 03:38)



Simple properties

(1)(a) $F \subseteq E_1 \subseteq E_2 \subseteq K \Rightarrow \mathrm{Aut}(K/E_1) \supseteq \mathrm{Aut}(K/E_2)$

(b) $H_1 \subseteq H_2 \subseteq G \Rightarrow \boxed{K^{H_1} \supseteq K^{H_2}}$

(2) a)

$$\begin{tikzcd} \mathcal{F} \arrow[r, shift left] & \mathcal{G} \arrow[l, shift left] \end{tikzcd} \qquad \begin{tikzcd} E \arrow[r] & H := \mathrm{Aut}(K/E) \arrow[dl] \\ K^H & \end{tikzcd}$$

$$\boxed{K^H \supseteq E}$$

b)

$$\begin{tikzcd} \mathcal{G} \arrow[r, shift left] & \mathcal{F} \arrow[l, shift left] \end{tikzcd} \qquad \begin{tikzcd} H \arrow[r] & K^H \arrow[dl] \\ \mathrm{Aut}(K/K^H) & \end{tikzcd} \qquad \boxed{\mathrm{Aut}(K/K^H) \supseteq H}$$

And here are some simple properties; the obvious properties are the following that these maps are inclusion reversing. In other words, if I have two fields, E 1, E 2 such that E 1 is contained in E 2, both contain F and are contained in K, then the fixed field, I am sorry, the automorphisms, so the group that you associate to E 1 versus the group that you associate to E 2.

Since E 1 is smaller than E 2, the group associated to E 2 will be contained in the group associated to E 1 and this just follows from definition because if an element sigma fixes everything in E 2, it necessarily fixes everything in E 1. So that is one direction and the other direction is, so maybe we should call this a and b. So it is property 1 a and b is if I have two subgroups H1 and H2.

They are both subgroups of G, then the fixed fields are also have the opposite inclusion. Again for just reasons or definition H2 has more elements. So, elements of K which are fixed by every element of H2 will certainly fix I mean, those elements will certainly be fixed by every element of H1.

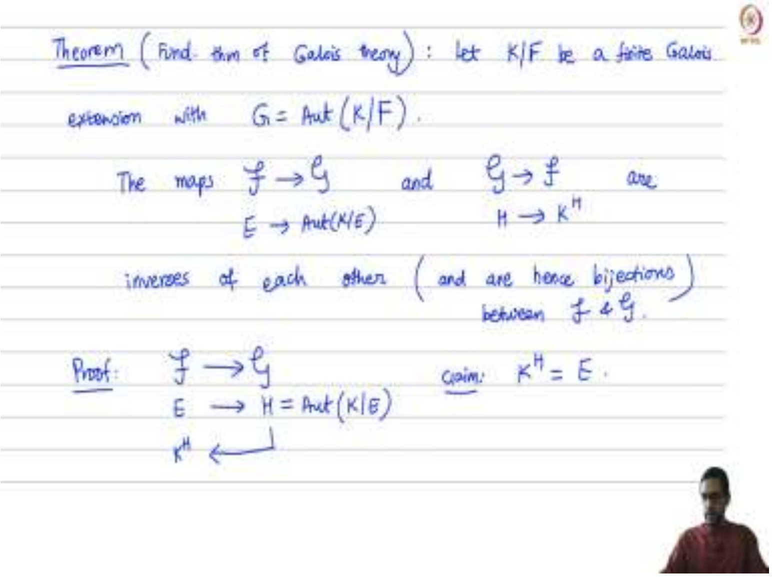
So, these are both obvious properties, property 2 here is what happens if you compose these maps. So, if I take F first go to G and then come back to F. So, what does this mean? I start with the intermediate field E, I look at the subgroup H, which is all automorphisms of K which are identity on E, then I come back, I take the fixed field of H. And the question is, what is the relationship between E and K H in general?

So, observe that the following holds that K H certainly contains E; again definition basically because elements of H already fix every element of E. So, the fixed field has to contain E. So, this is one statement is again 2 a, b is for the opposite. Start with G go to F and you go back, in other words, you start with a subgroup you form its fixed field, then you look at the automorphisms of K which fix this fixed field.

Then what is the relationship between that and the original subgroup H. So, the left hand side here is all automorphisms of K which fix every element of K H, definitely every element of H fixes every element of K H by definition. So, again you have this trivial you have this inclusion. So, these are the various facts, which are more or less obvious from a definition that these two maps F and G are inclusion reversing.

So, if the inclusion here goes one way, there it is the other way around E 1 sub of E 2 but here it is contained and what happens when you compose the maps? The final answer after composing the two is always bigger than the original. So, these are simple properties and the fundamental theorem of Galois Theory says really, that these two maps are inverses of each other.

(Refer Slide Time: 07:38)



Theorem (Fund. thm of Galois theory): let K/F be a finite Galois extension with $G = \mathrm{Aut}(K/F)$.

The maps $\mathcal{F} \to \mathcal{G}$ and $\mathcal{G} \to \mathcal{F}$ are

$E \to \mathrm{Aut}(K/E)$ $\quad$ $H \to K^H$

inverses of each other (and are hence bijections between $\mathcal{F}$ & $\mathcal{G}$.)

Proof: $\mathcal{F} \to \mathcal{G}$ $\quad$ Claim: $K^H = E$.

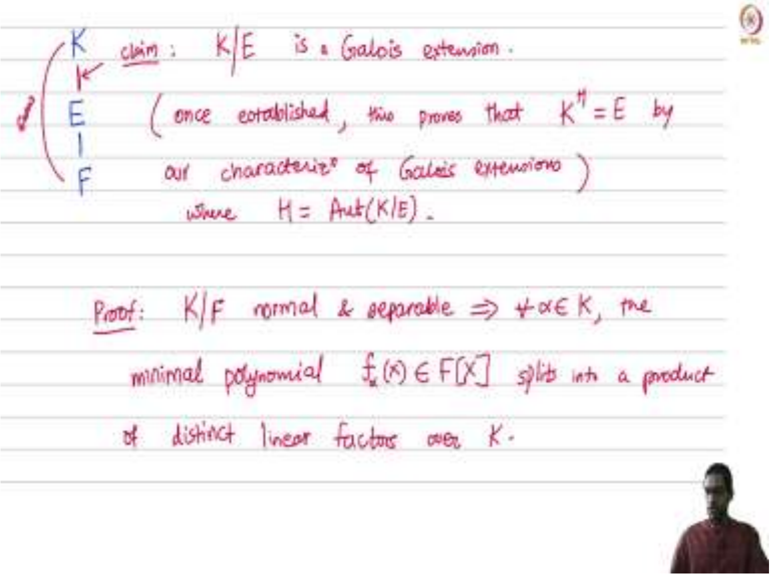
$$\begin{tikzcd} E \arrow[r] & H = \mathrm{Aut}(K|E) \arrow[dl] \\ K^H & \end{tikzcd}$$

So here is the theorem, which we call the fundamental theorem of Galois Theory, which is that, that K over F be a finite Galois extension with Galois group G. So this group of automorphisms is called the Galois group. Then the falling hold, the maps in some sense, that is really the only main content, the maps F to G, E going to aut K E and G to F.

These two maps are inverses of each other. So therefore, they are both bijections because they are both you know, they have inverses therefore and are hence by bijections. So this setup, these maps give you a bijective correspondence between the set of intermediate subfields and the set of subgroups.

Let us prove this. Most of the work required to prove it, we have already done by way of the various intermediate propositions that we approved so far. So here is the, let us prove one direction first. Let us show that F followed by G. So we said from F to G and back, K E, now let us go back to K H. So claim is that this fixed field K H is exactly the field E.

(Refer Slide Time: 10:23)



claim: K/E is a Galois extension.

(once established, this proves that $K^H = E$ by our characterizⁿ of Galois extensions) where $H = Aut(K/E)$.

Proof: K/F normal & separable $\Rightarrow \forall \alpha \in K$, the minimal polynomial $f_\alpha(x) \in F[X]$ splits into a product of distinct linear factors over K.

So that is one part of the, the theorem because it establishes that when you compose in this order, then you get the identity on F. So let us just draw the extension tower K, E, F and what is given? You are given that K over F is a Galois extension. So this is known to be a Galois extension or given to be Galois.

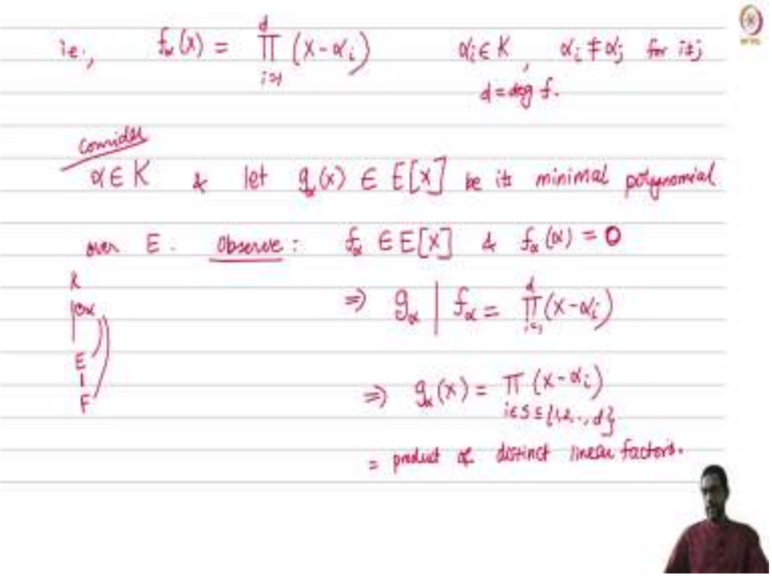
Now, the first claim, well in order to prove what is it that we needed to prove that K H is E, again, where H is the subgroup. So the, all we need to really prove is that this extension is Galois. So this is now going to be our claim. Claim; if K over F is Galois then K over E is also Galois, is a Galois extension. That is actually all we need to prove because let us just complete the proof assuming this claim.

So, once this claim is established, what does this tell you? Well, it says that recall what the one of our equivalent characterizations of Galois extensions was. It said if K over something is Galois, then the fixed field of aut. So then once established, this proves that K H is exactly E by our characterization of Galois extensions.

So, this was one of those equivalent conditions that we proved, where h is exactly aut K E. So look back on that theorem, which we showed. So, if you chose Galois then you are done. Now, to prove this we will use the other characterization of a Galois extension, which is that it is normal and separable. So if K over F is normal and separable, we just need to show that the same is true of K thought of as an extension over E.

So let us do that. So K or F is normal and separable or if you look back on the same characterization of Galois extensions that we proved, we showed this. If it is normal inseparably, then of course it means that for every element alpha of K, the minimal polynomial; so let me call it F alpha now F alpha of x, coefficients in F x is, it splits into a product of distinct linear factors over K.

(Refer Slide Time: 13:48)



i.e., $f_\alpha(x) = \prod_{i=1}^{d} (x-\alpha_i)$ $\quad \alpha_i \in K$, $\alpha_i \neq \alpha_j$ for $i \neq j$

$d = \deg f.$

Consider $\alpha \in K$ & let $g_\alpha(x) \in E[x]$ be its minimal polynomial over E. Observe: $f_\alpha \in E[x]$ & $f_\alpha(\alpha) = 0$

$$\Rightarrow g_\alpha \mid f_\alpha = \prod_{i=1}^{d}(x-\alpha_i)$$

$$\Rightarrow g_\alpha(x) = \prod_{i \in S \subseteq \{1,2,\ldots,d\}} (x-\alpha_i)$$

= product of distinct linear factors.

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

In other words, when you think of it, i e, when I write F alpha of x, it expands like this; x minus alpha i 1 to d. Let us say alpha is are all elements of K alpha i not equal to alpha j or i not equal to j and d is just the degree of F. So it splits completely and these routes are all distinct. That is what separable t means and splits completely is the normality of the extension.

Now, all we need to show is that the same is true when you think of K as an extension over E. So let us do the following. So, now take the same element alpha, so take alpha that we are looking at in K and let, so I want to think of K as an extension of E. So I need to now look at the minimal polynomial. So let G alpha of x belong into E of x now, be its minimal polynomial over E

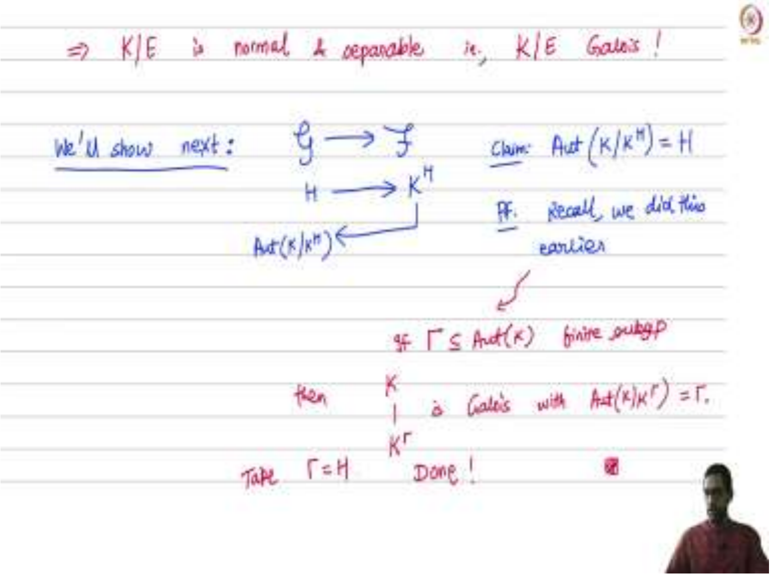
Meaning it is the unique smallest degree polynomial with coefficients in E that has alpha as a root. Now observe that, so this is our usual sort of argument. So, observe that F alpha is also in E x. It is actually in F x, but therefore, it is certainly in E x because E is bigger and F alpha has alpha as a root which implies that G alpha must divide F alpha. So, this is a general fact.

If I take the minimal polynomial of an element alpha over some field F, then I also look at its minimal polynomial over a larger field. So, all this is happening inside some ambient field, then the minimum polynomial over the, over E will divide the minimal polynomial of alpha over F exactly for this reason.

So G alpha divides F alpha, but F alpha already factors into a product of distinct linear factors. This is as we just said in K and now G alpha divides F alpha means of course, that what can G alpha look like? Well, it can only have, since it divides F alpha it has to be a product of some of these factors. So, G alpha is therefore a product x minus alpha i where i belongs to some subset, let us call it s, of 1 to d.

So, it has to run over some smaller subset of 1 to d possibly, but whatever it is G alpha of x again splits into distinct linear factors. This is, this is still a product of distinct linear factors over K. In other words, G alpha is also, it is a separable polynomial which splits over K. So that is exactly what we need to show.

(Refer Slide Time: 17:14)



$\Rightarrow$ K/E is normal & separable i.e., K/E Galois !

We'll show next:

$$\begin{tikzcd} \mathcal{G} \arrow[r] & \mathcal{F} \\ H \arrow[r] & K^H \arrow[dl] \\ \mathrm{Aut}(K/K^H) & \end{tikzcd}$$

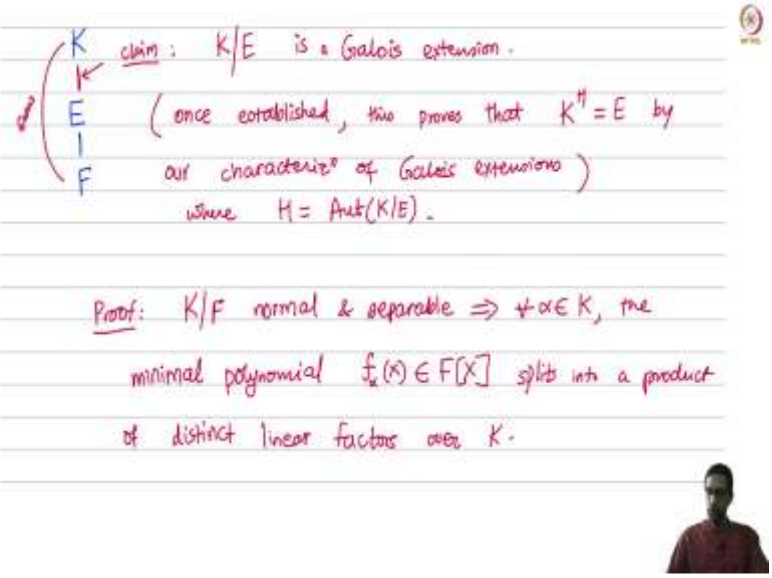
Claim: $\mathrm{Aut}(K/K^H) = H$

Pf. Recall, we did this earlier

If $\Gamma \leq \mathrm{Aut}(K)$ finite subgp

then $\begin{matrix} K \\ | \\ K^\Gamma \end{matrix}$ is Galois with $\mathrm{Aut}(K/K^\Gamma) = \Gamma$.

Take $\Gamma = H$ Done ! ■



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

claim : K/E is a Galois extension.

(once established, this proves that $K^H = E$ by our characteriz^n of Galois extensions) where $H = \mathrm{Aut}(K/E)$.

Proof: K/F normal & separable $\Rightarrow \forall \alpha \in K$, the minimal polynomial $f_\alpha(x) \in F[X]$ splits into a product of distinct linear factors over K.

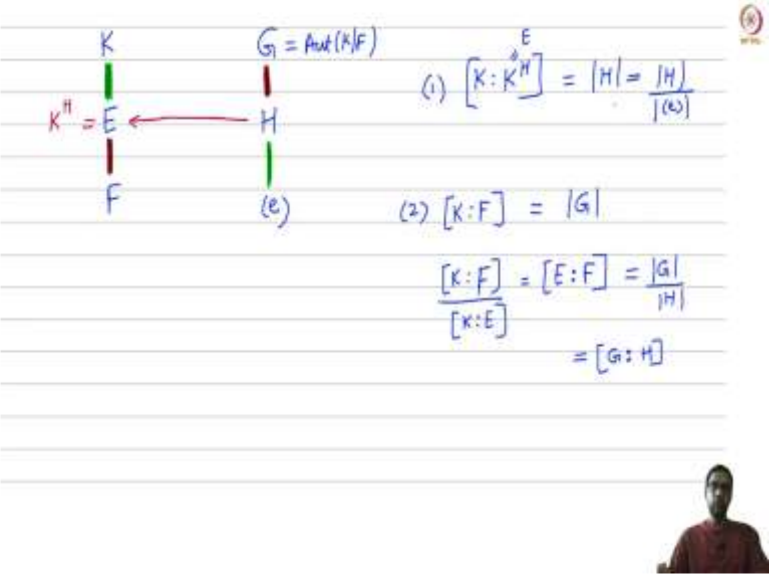
This implies by K over E is again normal and separable. Since this holds for all alpha in K, i e is Galois. So, notice how we sort of used all the various characterizations of Galois here to prove that F and G are I mean the maps between F and G are inverses of each other. We need you know, we use this characterization of Galois extension but to show that when K over F is Galois then K over E is Galois.

It is actually more convenient to use the other definition in terms of normality and severability. Okay, good. So that establishes that one of the two compositions is the identity. So now, what is the other thing that is left? We claim next, we will show next that the other compositions outside entity, you take G then go to F, which means I take a subgroup H, I form its fixed field, then I come back and take the set of automorphisms of K which fix K H.

So, then claim is that automorphisms of K over K H is exactly H. But recall this is exactly what we proved as a one of the corollaries of our Artin's theorem. So, proof recall we have already done this. In fact, what did, what was the thing we said; we said if I have some more generally we made the following statement; we said if gamma is a finite subgroup of the automorphism group, finite subgroup then we showed the following; that K over k gamma is Galois, is a Galois extension with the Galois group aut K over K gamma, equal to gamma.

This is the one of the propositions we show. So, now just use this preposition just apply it to H. That is all. So, take gamma equals H and what it shows exactly is that if I take automorphisms of K or K H then that is exactly the group H that we started. So this is done. So that proves the second half of the Galois correspondence or the fundamental theorem of Galois Theory. So that finishes the proof.

(Refer Slide Time: 20:16)



(1) $\left[K : \overset{E}{K^H}\right] = |H| = \frac{|H|}{|(e)|}$

(2) $[K : F] = |G|$

$\frac{[K:F]}{[K:E]} = [E:F] = \frac{|G|}{|H|}$

$= [G:H]$

So, I just want to make one last remark before, before we end this discussion which is that; so on the one hand, I have these extension fields K, E, F and on the other hand, I have the group G, which is aut K F and well I have various subgroups H and it is sort of useful from a symmetry perspective to put an identity there. So, sort of so that it looks the same and now observe something more, the Galois (correspondence).

So what does the Galois correspondence say to each H, if I associate the field E, which is the fixed field of H, K H, then that is the bijection? That is the correspondence from groups to subfields and now, again, we have a map in the the other direction also. But this correspondence has a following very nice property; the dimensions have a nice property, which is; if I look at the degree of this extension from K to K, E.

So if H and E correspond to each other, then the degree of this extension K E is just the cardinality of H. So recall, so this is also Artin's theorem, you wish, K, K H, degree of the extension is exactly the cardinality of H and I mean, just for symmetry, again think of the cardinality of H as just being H by 1.

So, it is the cardinality of H by the cardinality of identity. So what does that say? Well, that is like the cardinality of H divided by the cardinality of E or the index of the identity in the subgroup H. So that is one; further what about the other guy? So, if I if I look for this and this for instance, so observe there is just multiplicative here of degrees.

So this is one observation to make about the cardinalities of the subgroup and the degree of the extension. Now observe that K F similarly is therefore the cardinality of the group G and if you divide this one equation by the other that is just going to give you a K F by K E. So this is my E in my figure.

So K F by K E because degrees of extension, so when you have a tower, the degree is just multiply. So this is just the degree of the extension E F and so that is just the cardinality of G over the cardinality of H, which we could also write as the index of the subgroup H in the subgroup G.

So you should you should think of, you know, there is also symmetry in the other direction. So, this index of H in G or the quotient of their cardinalities is the same as the degree of the extension E over F. So we will talk about sort of the second part of the Galois correspondence, which sort of asks or answers the question as to when this brown extension E over F is Galois.