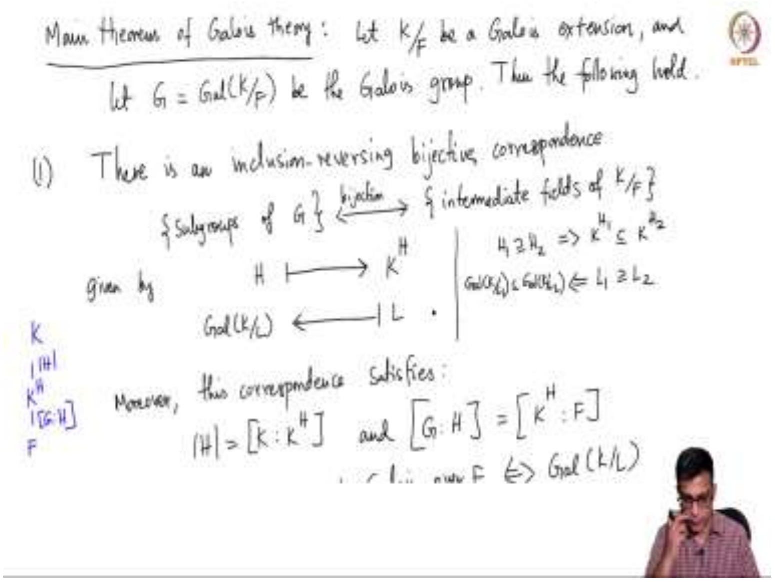
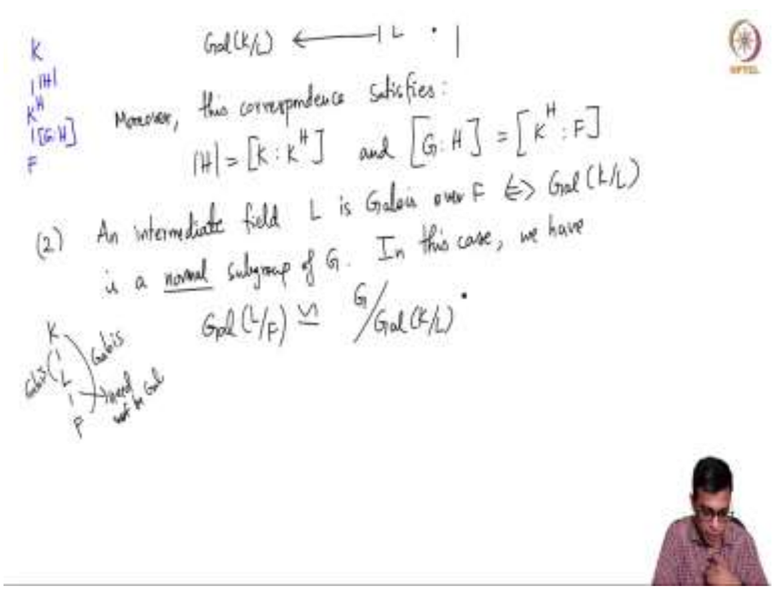
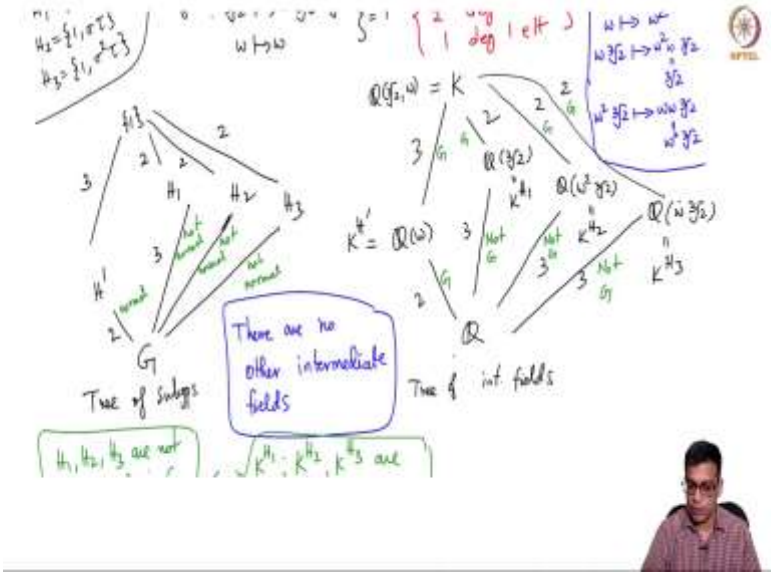
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 25
Main Theorem of Galois Theory – Part 2

(Refer Slide Time: 00:15)







Welcome back, we are in the middle of proving this main theorem of Galois Theory and this is really the first main result in this course. In fact, as the name itself suggests, this is the main theorem of Galois Theory. So, everything that we do later will build on this. So, this is a good point to take stock of the course and see that you are following everything.

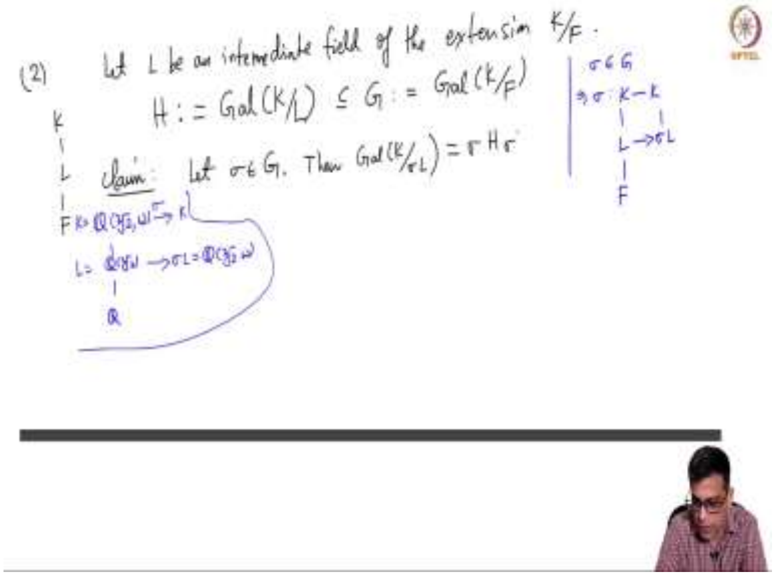
So, I in the last couple of videos, I recalled the basic things, and set up the main theorem by giving you a few examples and in the last video, we stated this and proved part of it. So, main theorem of Galois Theory tells you a lot about Galois extensions. And the first statement we proved last time is that there is a by bijection between subgroups of G and intermediate fields of the given extensions.

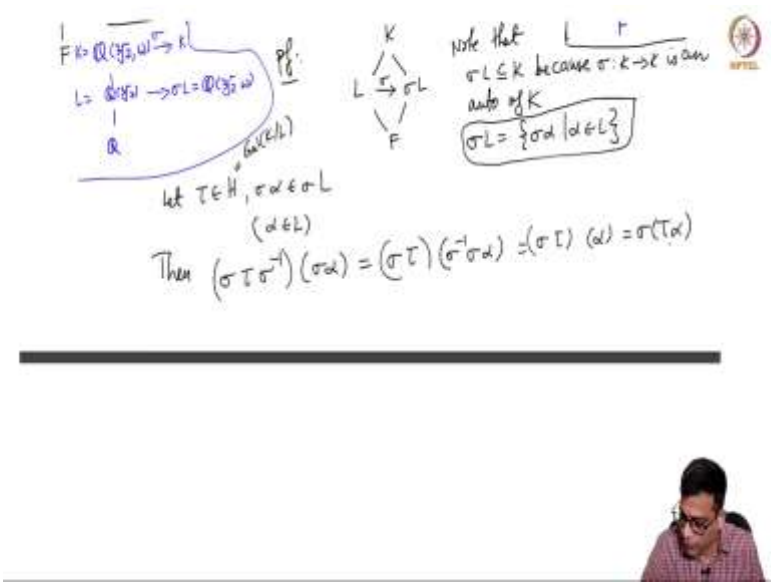
But G is of course, a Galois group. And this inclusion this bijective correspondence in fact, is an inclusion reversing one. And it you can completely determine the degrees of the extension fields using the order and the index of the subgroups in question. And now today we going to prove this second part.

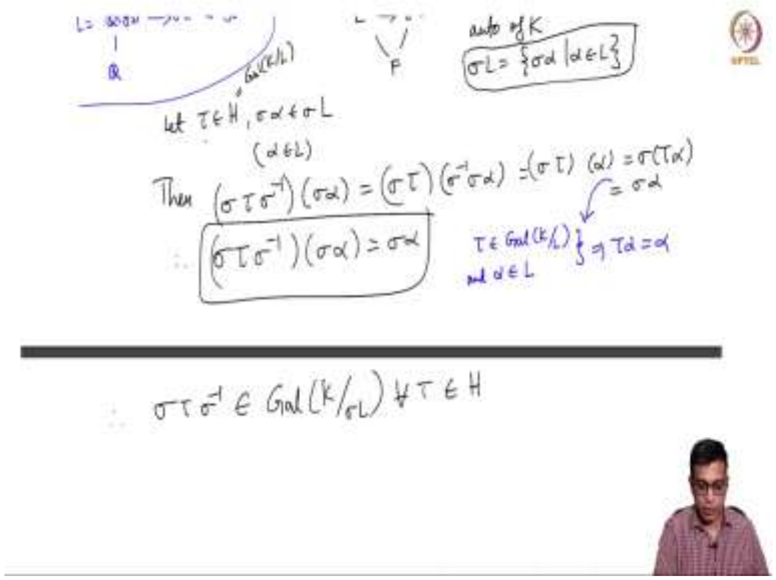
Second part tells us when the bottom part of the extension is Galois, in general, as we know, if you are given an extension, Galois extension K over L F and you take an intermediate field L, if this is Galois, this is Galois always, but this need not be Galois. As for example, the second example that we did here shows K or Q is Galois here; K is Q adjoined cube root of 2 omega but cube root of 2 over Q is not Galois.

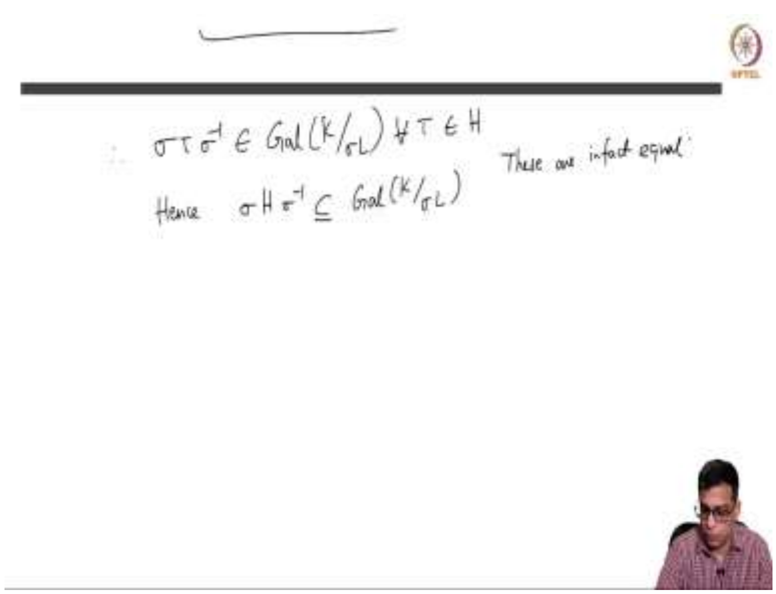
So, in general, you do not have L over F Galois, but main theorem of Galois theory tells us when it happens, it happens precisely when the corresponding subgroup in the bijection that we discussed in part 1 happens to be a normal subgroup of the Galois group and moreover, the Galois group is in fact, given as the quotient group of G with Galois group of K over L. So, let us prove all of these in the prove of second part,

(Refer Slide Time: 02:30)









So, let u take now, an intermediate field. Let L be an intermediate field of the extension, given extension K over F. So this L a priori is just an arbitrary extension, we do not arbitrary intermediate field, we do not know whether it is Galois or F or not. So, I want to define the corresponding group by H denote the corresponding group by H. So, K, L, F in the corresponding group is H. So, this is of course, a subgroup of G, which I will recall for you is the Galois group of the original extension and then, I claim the following.

So, I claim that let sigma be in G. So, G is the Galois group of the entire extension, then sigma remember, if sigma, so I will write that here sigma is in G means sigma is a function from K to K and L is here F is here, sigma fixes F pointwise. But L we do not know, sigma L is some other subfield. So, a priori sigma L is something else, for example, in the field, keyword joint cube root of 2.

Maybe I will write it here. So, Q adjoined cube root of 2 omega Q adjoined cube root of 2 Q, if you the call this L and you take a suitable sigma which sends cube root of 2 2 cube root of omega cube root of 2 sigma L will be Q adjoined cube root of 2 omega. So, sigma L is some other field. So, sigma L and it is some other extension, sorry, I should keep this as it is.

So, sigma L is another intermediate field. The statement that I want to say is that the Galois group of K over sigma L is sigma H, sigma inverse. So, this is the claim. So, let me prove this is an easy statement. So, the correct way to draw this picture will be I will keep it here. So, L is here, sigma L is here and F is here.

Why do I say that sigma L is a subfield of K? That is because note that sigma L is inside K so, that it is a subfield because K is Galois or more generally, I mean actually more precisely sigma is an automorphism of K. It may not be in L, but it is certainly in K because sigma maps K to K. So, we have this picture, I am saying that this Galois group here is this conjugate sigma H sigma inverse, you begin to see where normality of H will enter the picture.

Because this is a conjugate of H, H if H is normal this is equal to H. So, now, let us pick something in let us pick something in H let us a tau is in H and let us take an arbitrary element of sigma L that means, it is image of something in L sigma L is exactly things like this, by definition, it is the image of L under sigma.

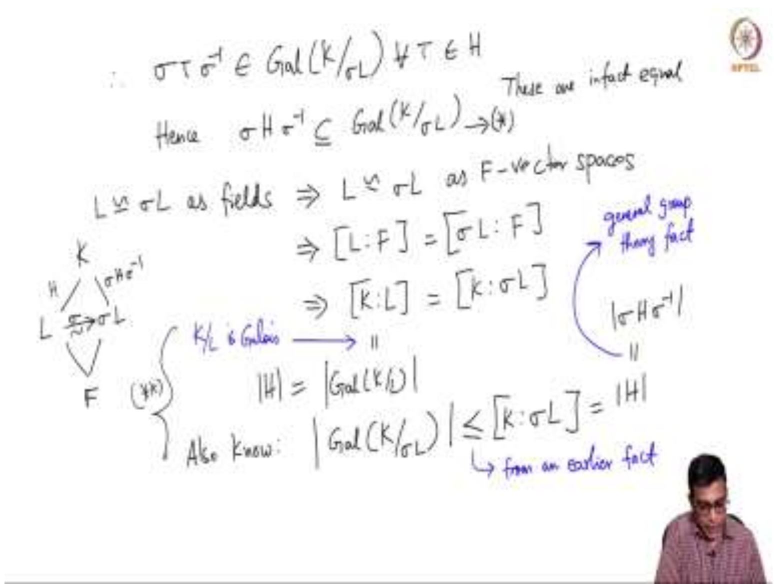
So, let us take an arbitrary element like this, then let us apply sigma tau sigma inverse to sigma L, then sigma tau sigma inverse applied to sigma L will be sigma tau sigma inverse, this is just a composition of functions. This is sigma tau of alpha, because sigma inverse sigma of alpha is this. But sigma tau alpha is this but tau is an H alpha is an L, where is tau this is the Galois group of K over L, H is by definition Galois group of K over L.

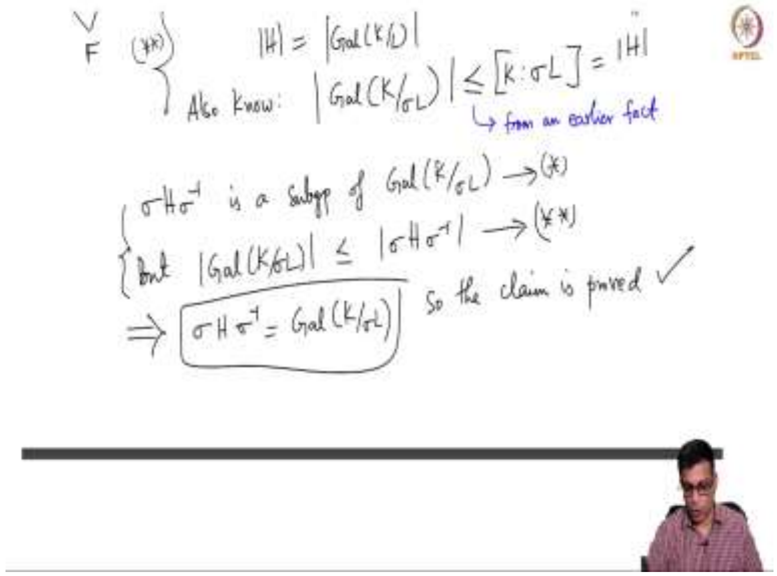
So, everything in H fixes everything in L. So, tau alpha is alpha. So, this is sigma alpha that means, sigma tau sigma inverse tau alpha sigma alpha is sigma alpha. So, sigma tau sigma inverse belongs to Galois K over tau L. Because, basically what I have done by this calculation is you give me anything in sigma L, you give me any element in sigma L, it must be of the form sigma alpha sigma tau sigma inverse we will fix it because sigma tau sigma inverse sigma alpha is sigma alpha and this step here, I will maybe highlight this this step here is because tau is in Galois K over L and alpha is in L.

So, by definition tau alpha is an alpha because alpha is an element of L tau fixes L. So, that is the statement. This is of course, now, true for all sigma in H. Because an arbitrary all tau in H, I am taking an arbitrary tau and proving this. So, that means, hence, sigma H sigma inverse is contained in the Galois group of K over tau L. So, it is contained in the Galois group of tau L.

But, now, I want to show that they are equal that is the claim, but that will follow essentially from counting the number of elements in this, but these are in fact equal. Why? The reason is the following.

(Refer Slide Time: 09:01)





So, note first that H note first that L is isomorphism tau L, because sigma is an automorphism homomorphism from L to sigma L it is injective because, any field homomorphism is injective it is surjective because it goes to sigma L by definition, sigma L is the image. So, this is isomorphic isomorphism of fields. This implies L is isomorphic to this as F vector spaces. This is isomorphism as F vector spaces but this means L colon F the degree is same as sigma L colon F.

So, the picture again I will go here K is here, L is here, sigma L is here, F is here is an isomorphism. This degree is same as this degree, but this implies of course, K L is equal to K is equal to K sigma L this is a triviality, because K over F is on the one hand L colon L times L colon F, on the other hand it is K colon sigma L colon times sigma L, colon F, but L colon F is same as sigma L colon F.

So, K L is equal to K colon sigma L and once this happens, this is of course, the order of K over L. So, this is order of H, because K over L is Galois. So, this is because K colon L is equal to the cardinality of the Galois group of K over L this of course, is equal to H because H is the Galois group of K over L.

So, this carnality is H, but on the other hand, we do know that this is less than or equal to, so, what do I want to say this. So, this so on the other hand, we also know so, this is something that I mentioned before the cardinality or the order of the Galois group of K over L is less than or equal to K colon sigma L. So, this is from an earlier fact. In fact, this was recalled in a video two, three videos back. In general, if every time you have an extension field extension, the order of the Galois group in fact divides the degree of the extension. In fact, this divides this, so, this is true.

So, now, this is equal to order of H, because this is equal to this this is equal to this this is equal to H, this is less than or equal to H. And on the other hand order of H, so, I am all over the place I am sorry is sigma H sigma inverse. So, this is a general group theory fact. If you take a subgroup and conjugate of it, they both are the same cardinality.

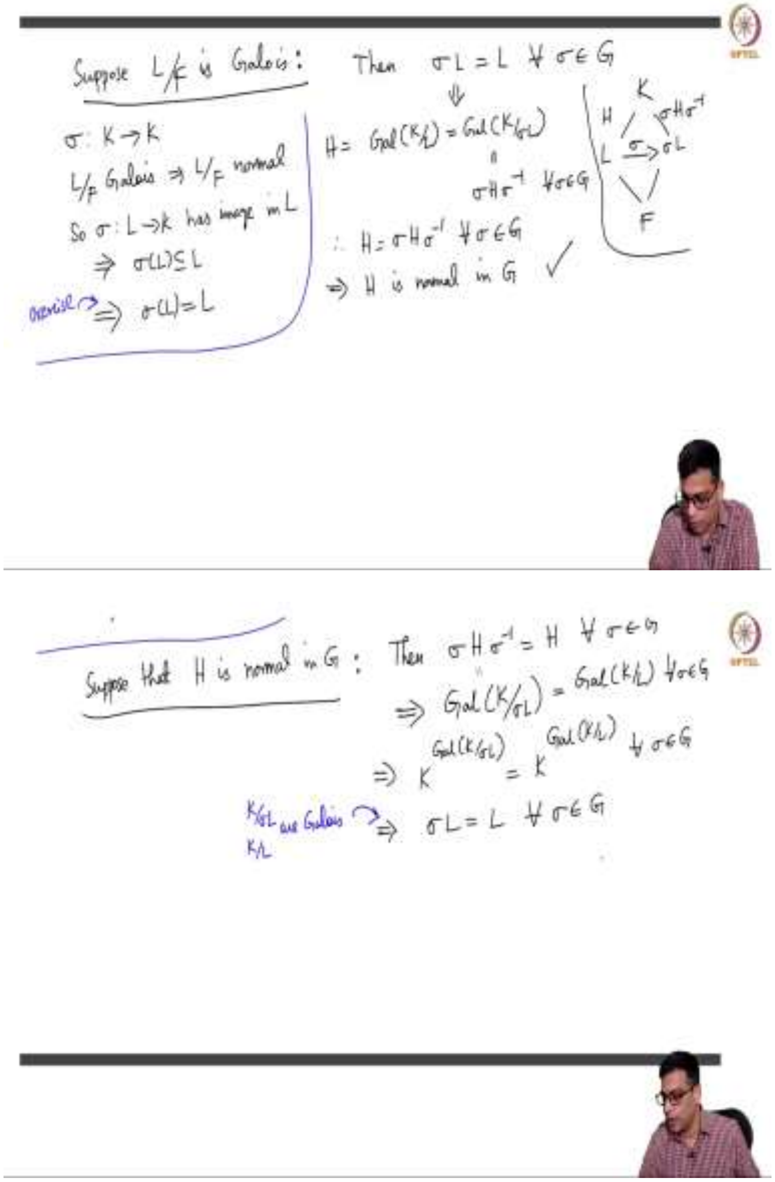
So, this is equal to this, but this is a subgroup of this. So, I am just using two facts sigma H sigma inverse is a subgroup of, so, maybe I will write it here, sigma H sigma inverse is a subgroup that is just this fact here, sigma H sigma inverse is a subgroup. Remember, if H is a subgroup sigma H sigma inverse is also a subgroup of G.

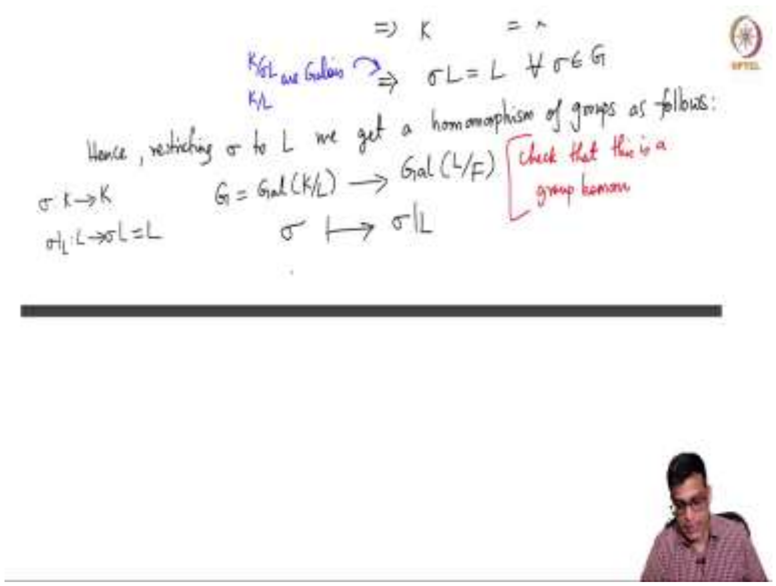
In fact, it is contained in Galois K over sigma L is what we have shown this here. So, it is a subgroup of this, but, the order of the bigger group is less than order of the smaller group. So, this is star star, so, that that is proved here and this is star and that is proved here. So, star star says that, order of the potentially smaller group thing is bigger than the order of the bigger group.

So, these two together imply sigma H sigma inverse is Galois K over L as required so, the claim is proved sorry, this is Galois so, the claim is proved. So, the claim was sigma H sigma inverse is the Galois group of K over sigma L. So, if the Galois group of this is H, this is sigma H sigma inverse, so, we are almost done there done with this proof. The crucial statement we have just proved.

So, if the Galois group of K over L is H, the Galois group of this which is also, remember a Galois extension always, because, if K over F is Galois and sigma L is an intermediate field K over sigma L is also Galois. So, this is the Galois group of this. So, sigma L that sigma also determines the Galois group here. So, that is the statement, which we have just proved. So, hopefully this proof is clear to you. If not please stop the video and just go back and go through this, this is a simple argument maybe I sort of made it more complicated than it should be.

(Refer Slide Time: 14:48)





Now, we are ready to prove the second part. So suppose, L is normal in L is Galois over F so let me write it like this, suppose L over F is Galois we want to show that Galois K over L is normal in G. So, suppose L is normal in F that means, so, this is an observation that we made in the past. Because sigma is an automorphism from K to K, if you restrict sigma to L, it sigma is, so the reason is L over F is Galois implies L over F is normal.

So, the map from L to K has image in L, has image in L that means, sorry, so as image in L and hence, sigma L is in L, but because of an exercise we did, so this is an exercise, every time you have a algebraic extension L over F and you have an F auto F homomorphism from L to L, the image is always equal to L.

So, this implies that sigma L equals L. But this means, so in the picture that I had earlier which I will write here K L sigma L F, so if the Galois group here is H Galois group here is sigma H sigma inverse. So, if these are actually equal, then Galois of K over L is equal to Galois K over sigma L because they are the same fields.

So, the fixed Galois groups are also equal, but this is sigma H, this is H this is sigma H sigma inverse, this is true for all sigma in G. So, H equals sigma H sigma inverse for all sigma in G which is precisely the definition of normal subgroup. So, the one direction is proved. So, if so, let me just go back to the statement of the theorem and intermediate field is Galois if and only if

Galois K over L is normal in Galois K over F. So, assuming it is normal we have shown that its corresponding subgroup is normal.

So, now, suppose that H is normal in we are going to show that L is Galois over F, why is this suppose H is normal in G, then by definition of normality sigma H sigma inverse H is equal to sigma for all sigma in G, this implies Galois K over sigma L is equal to Galois K over L for all sigma in G, because sigma H sigma inverse is equal to Galois K over L, H is equal to Galois K over L. So, Galois K over L is equal to Galois K over sigma L for all sigma in G, but that means, by applying K power these are two groups.

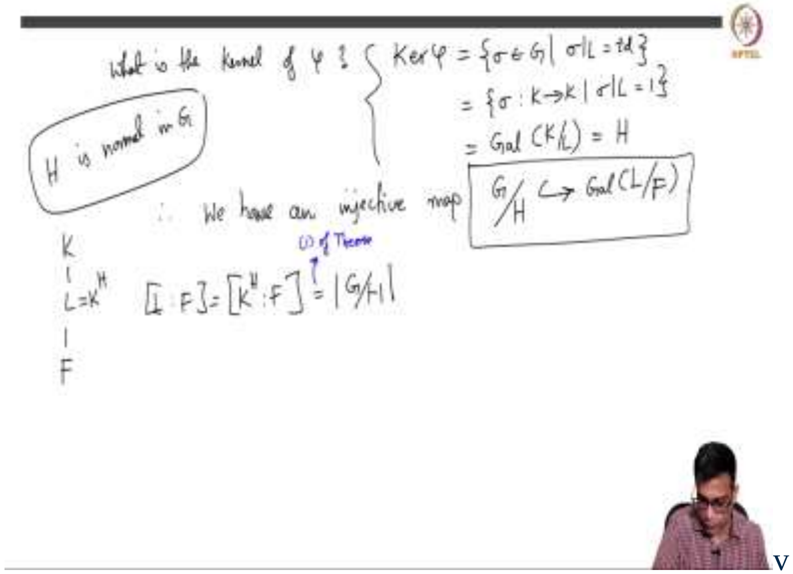
So, this straightforward if you have two groups, their fixed fields are equal. So, K power this is equal to K power this, but this because of the various facts that we have done in the past and recall several times is exactly sigma L, K power Galois K over sigma L is L K power Galois K over L is L, this is of course, because K over sigma L and K over L are Galois that is required for this implication.

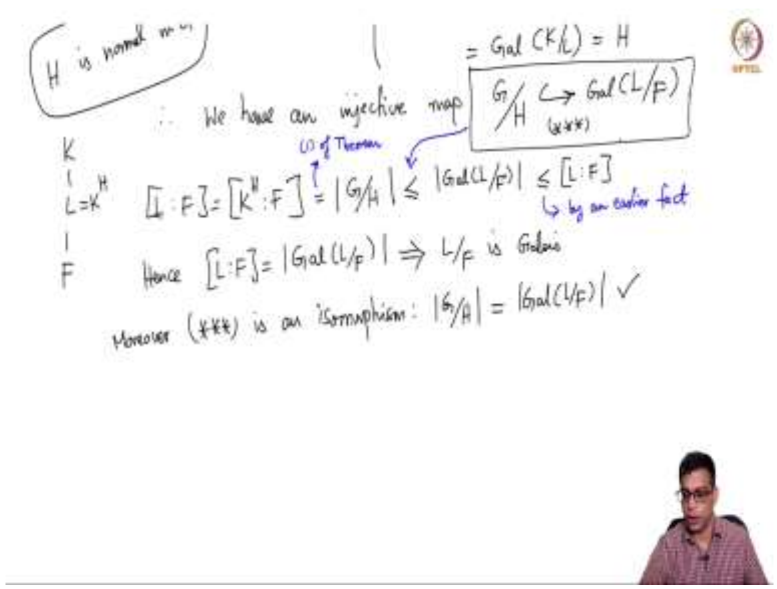
So, sigma L is equal to L for all sigma in G. So, sigma L is equal to sigma this basically proves that it is normal almost, but we want to do this in a way that gives the last statement about the Galois group of F over L in one shot, so, let us do the following. So, hence restricting sigma to L, we get a homomorphism of groups. And in any problem session some time ago I did talk about this restriction map.

So, G which is Galois K over L to Galois L over F, sigma goes to sigma restricted to L that is the restriction map. So, sigma is a function from K to K. So in general, if you restrict to L, you only go to sigma L, but I have just shown using the H is normal, I have shown this L. So, it is in fact an automorphism of L. So, sigma going to sigma L does map to Galois L over F. Remember sigma a priori is a (())(20:27) automorphism.

So, it will fix F pointwise. So this is a group homomorphism, which is a trivial statement, check that this is a group homomorphism. There is really nothing to show here. Because sigma composed with sigma prime restricted to L sigma restricted to L composed with sigma prime restricted to L that is all. Because sigma restricted to L is just sigma is just that you are only applying it to elements of L. So this is a trivial exercise.

(Refer Slide Time: 21:07)





F Hence $[L:F] = |Gal(L/F)| \Rightarrow L/F$ is Galois

Moreover $(***)$ is an isomorphism: $|G/H| = |Gal(L/F)|$ ✓

Hence $G/_{Gal(K/L)} \simeq Gal(L/F)$

This completes the proof of (2) and the theorem □

Suppose that H is normal in G: Then $\sigma H \sigma^{-1} = H$ ∀ ...

$\boxed{H = Gal(K/L)}$

$\Rightarrow Gal(K/\sigma L) = Gal(K/L)$ $\forall \sigma \in G$

$\Rightarrow K^{Gal(K/\sigma L)} = K^{Gal(K/L)}$ $\forall \sigma \in G$

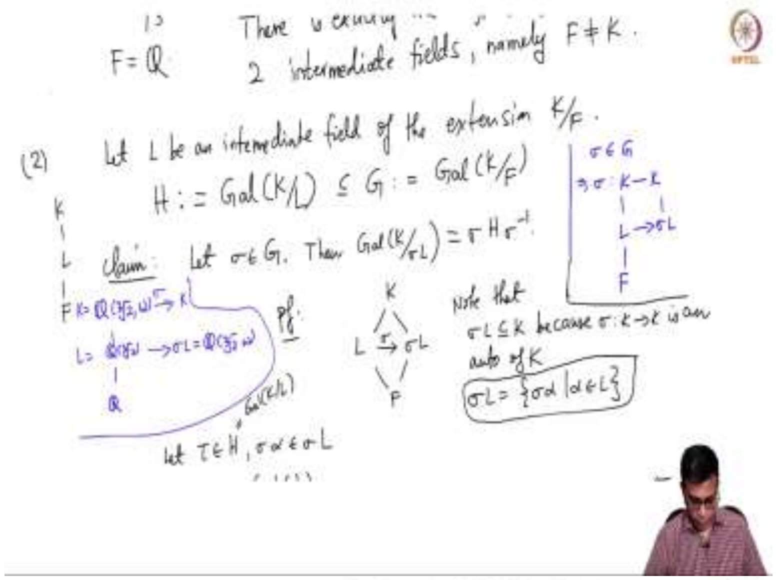
$K/\sigma L$, K/L are Galois $\Rightarrow \sigma L = L$ $\forall \sigma \in G$

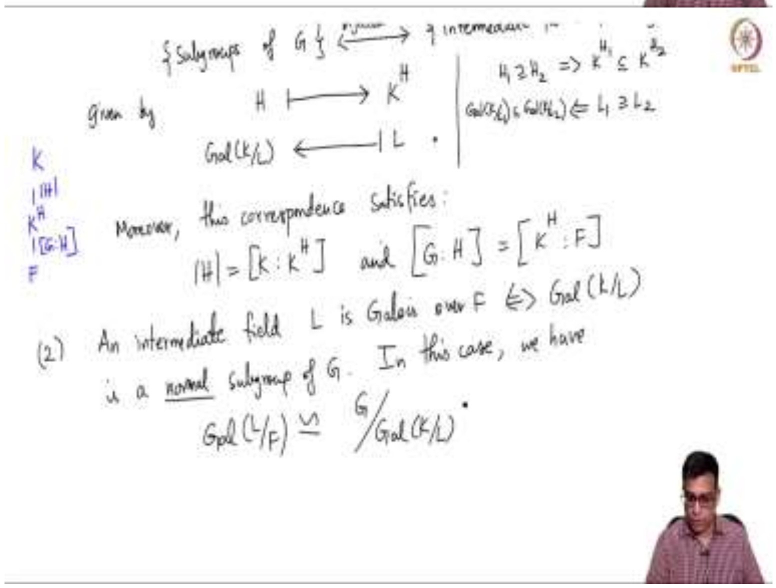
Hence, restricting σ to L we get a homomorphism of groups as follows:

$\sigma: K \to K$ $\quad G = Gal(K/L) \xrightarrow{\varphi} Gal(L/F)$ [check that this is a group homom ✓

$\sigma|_L : L \to \sigma L = L$ $\quad \sigma \mapsto \sigma|_L$

$Ker \varphi = \{\sigma \in G \mid \sigma|_L = id\}$





Now, what is the kernel of this? Let us say that, what is the kernel of phi? I claim that kernel of phi consists of all homomorphism's it is I am not claiming this is the truth. Such that sigma identity. So, that means sigma is an automorphism from K to K such that sigma L sigma restricted to L is 1, but this is precisely Galois K over L.

So, Galois K over L is and this is H of course, H is Galois K over L as I should keep reminding you. So, that we fixed at the beginning, L is Galois H is Galois K over L. So, then what we have is H is the kernel of this map that I just defined. Because if something is in the kernel H, then clearly sigma restricted L is identity, if something is in the kernel sigma will be in K. So this is trivial.

So, that means we have an inclusion and note that H is normal in G that is hypothesis. So, we have an inclusion or rather to be precise, and injective map, G mod H to Galois L over F. Let us, stare at this and see what we get. So, we have an injective map because this is an isomorphism theorem of groups. You have a map from one group an another, if you go mod (())(22:43) the kernel, it becomes an injective map.

So now, let us just play with this. So, K, L, F of course, that is what we have and L is the intermediate field that we started with. So, L colon F, L is K power H, L colon F is KH colon F this is by the equality of L and KH, this is the order of G mod H, this is the statement by part one of the theorem.

The theorem that we are now proving the main theorem because if you go back to the statement of the theorem, K colon K power H is H but K colon H power F is G colon H, which is order of G mod H because H is a normal subgroup I can talk about G mod H. So, G mod H is this, but then this is less than or equal to because of this inclusion the order of L over F, that is because of this.

Because G mod H is a subgroup of this, so this subgroup will have smaller order than the bigger group. So, the order of G mod H is less than or equal to order of Galois group of L over F, but then by another application of something that we know, order the Galois group of any extension in general is less than the degree of the extension, this by an earlier fact.

We know very well that cardinality of the Galois group is at most the order of degree of the extension and that is inequality if and only if the extension is Galois. So, now we have L colon F on the left hand side L colon F on the right hand side. So, everything in the middle is equal. So, hence in particular L colon F is Galois L over F. This already implies that L over F is Galois as required.

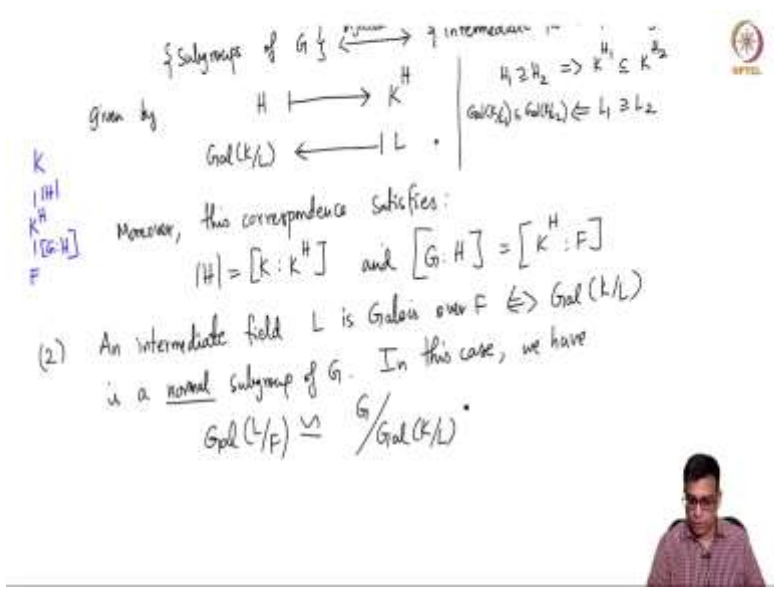
Remember, this is an equivalent condition for Galois extensions that I recall in a previous video. So, if the extension degree is equal to the order of the Galois group, the extension is Galois, but moreover, the star here, how this map triple star that we have here is an injective map. Moreover, triple star is an isomorphism.

Because order of the group G mod H is equal to the those are some other things that we pair here G colon H G mod H is here Galois L over F, if is this this an inequality. So, this is an isomorphism. So, you have an injective map of finite groups, which have the same order then that must be an isomorphism inclusion map. So, these are finite groups, so, that must be an isomorphism.

So, this is also going to prove the. So, this completes the proof of we got the final statement also, final statement told us that if you do have an fact that L is Galois over F Galois L over F is isomorphic to G mod Galois K over L which is exactly what we have. So, so maybe before I write that, I will simply say hence, G mod H, which is I have written that somewhere here Galois K over L is isomorphic to Galois over F. This is exactly the last statement of the theorem.

So, this completes the proof of 2 and the theorem. So, let me stop the video here. And what we want to do in the next videos is to apply this main theorem. So, we will spend one video or two videos giving you some nice applications of this and then we will go back to the most serious applications, which involve showing the insolubility of quintics by radicals and studying some other special kinds of Galois extensions.

(Refer Slide Time: 27:43)



So, in this video, I completed the proofs of the main theorem of Galois theory, which says that if you have a Galois extension, there is a bijection between the subgroups of the group and intermediate fields of the extension and moreover, if you are given an intermediate field, that is Galois over the base field if and only if the corresponding sub group is a normal subgroup of the Galois group of the original extension.

And if that is the case, we also do know how to find the Galois group of the extension L over F using the Galois group of the original extension and the Galois group of the top extension. So, let me stop this video here, and we will continue with applications in the next video. Thank you.