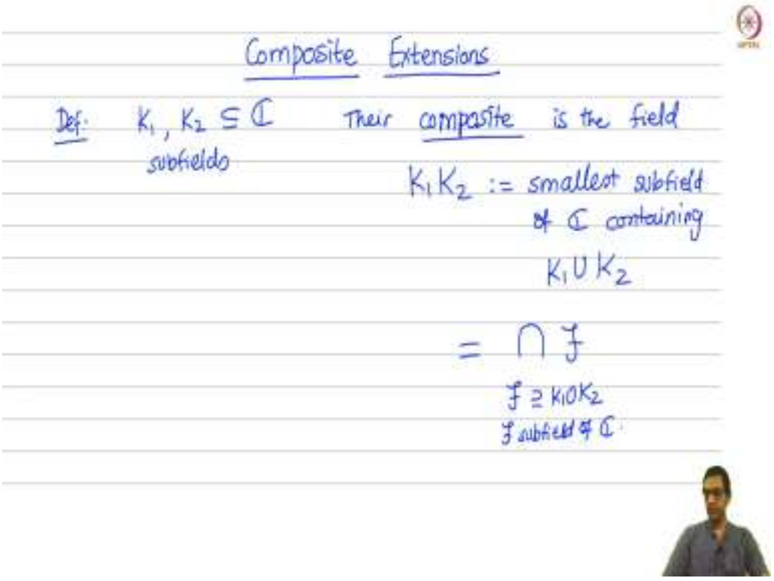
Algebra - II
Professor S Viswanath
Department of Mathematics
The Institute of Mathematical Science
Lecture 43
Insolvability of the General Quintic – Part 2

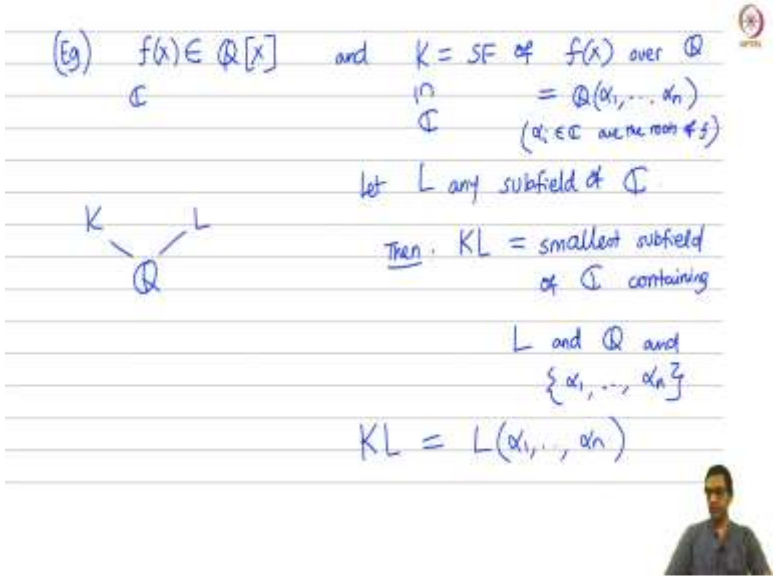
(Refer Slide Time: 00:14)



Let us talk about composite extensions. Now definition: suppose I have 2 subfields of C, so I will only worry about subfields of C. But of course, all these definitions are more general, given 2 subfields there composite, the composite field is the field it is usually denoted K 1, K 2 and it is just the smallest subfield of C which contains their union.

So, it contains both of them, the smallest subfield of C containing both K 1 and K 2. Another way of saying that, is to say you just take the intersection of F, script F so, what is F, F is a subfield which contains K 1 union K 2, F is subfield of C. So, this is called the composite of 2 given subfields of a larger field in general.

(Refer Slide Time: 01:31)



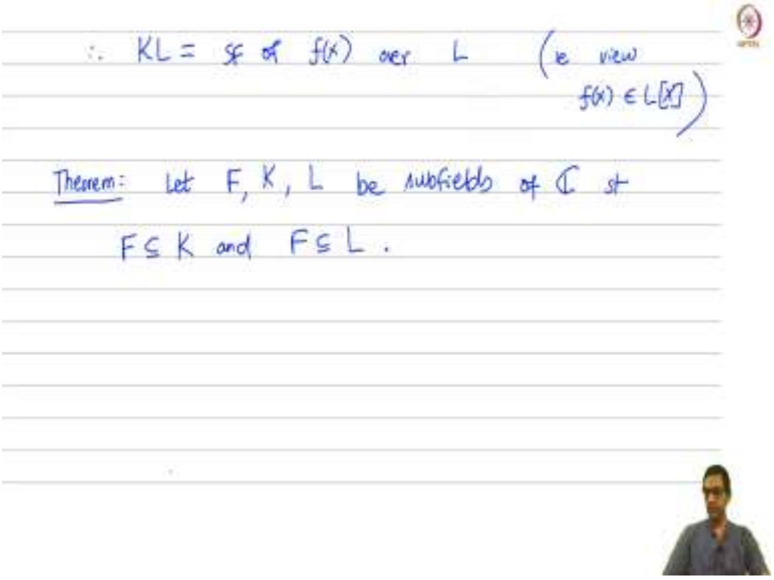
Now, the most important example of this, which you know is really the way in which it will arise is, if I give you a polynomial with rational coefficients and suppose K is the splitting field of this polynomial; so, is the splitting field inside the complex numbers. So, I have Q and I have K which is a splitting field of Q.

Now, suppose I just pick some arbitrary subfield of C, so all these are subfields of C. So, now let L be just any subfield, then the composite so, what does it mean to say K is a splitting field of F x? It just means that this is obtained from Q by adjoining the roots of F. So, alpha i in the complex numbers are the roots of this polynomial F.

So, you adjoin them to Q you get the subfield K. Now, if you take an arbitrary subfield L so, the key word here is it is a splitting field over Q. Now, the composite K L is well what is it? The smallest field which contains both K and L; so, now observe just by definition, this is the smallest subfield of C containing well, what does it contain?

It contains L as well as K, but K is nothing but Q and the n roots. So, if you just take the smallest subfield which contains all these 3 sets l q and the set of roots, then that is exactly K L, just by definition. So, of course, any field containing Q necessarily, so observe this is nothing but it is a smaller subfield of C, which contains L and the n roots of this polynomial. So here is the final conclusion. K L is nothing but L adjoin alpha 1, alpha 2, alpha n.

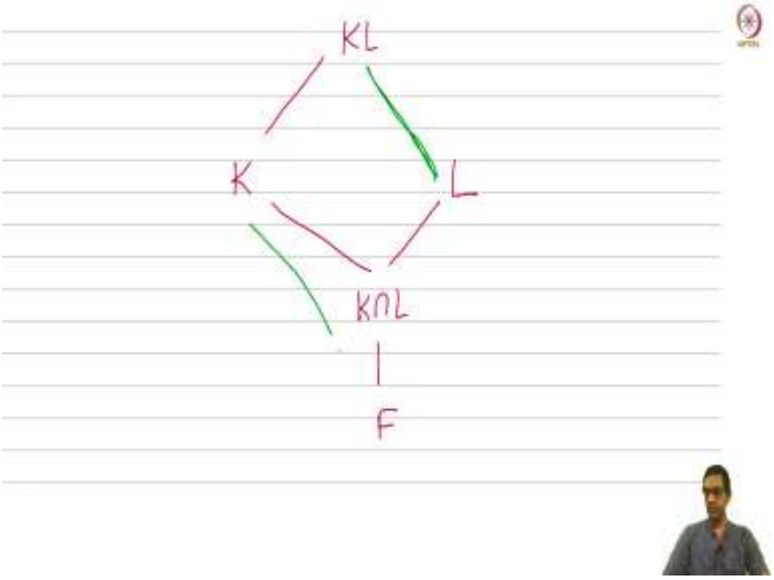
(Refer Slide Time: 03:48)

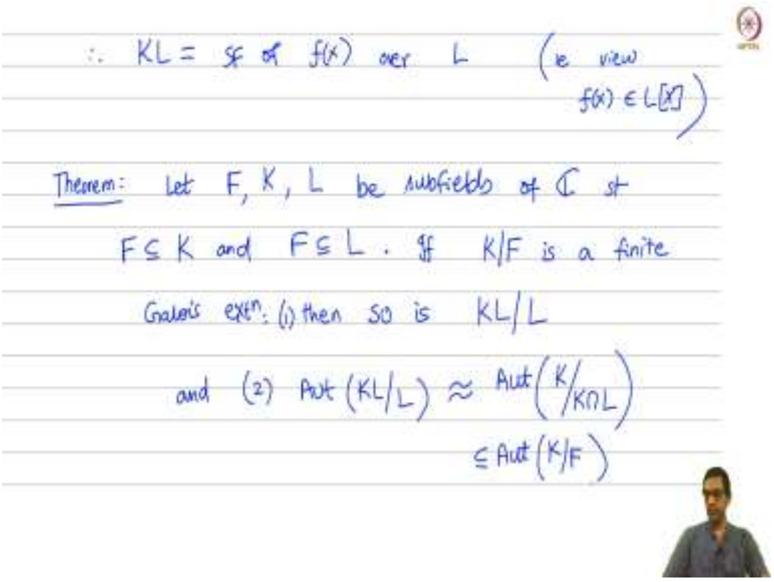


In other words, therefore this is exactly what you would call, this is the splitting field of this polynomial f x but thought of as a polynomial with coefficients in L x. When I say it is a splitting field of f x over L. i e, what I mean is you just view this polynomial as since it has rational coefficients, you can think of it as having coefficients in L, because L is bigger than Q.

And the splitting field over L is really L adjoin the n roots and so that is exactly the composite. This all this is just definition more or less. Now, here is the key theorem which allows us to work with composites. So it says; suppose I have subfields of C such that F is contained in both of them now if one of them is finite and Galois, so let us start drawing the picture maybe.

(Refer Slide Time: 05:07)





So let us go to the next page. So I have F now, F is contained in K; it is also contained in L. So in fact, F is contained in their intersection. So I have this feel K intersectional and F is contained in their intersection. So let me just draw these lines and of course, everything is contained in C. So I am not drawing C here.

Now, the field K L that we are talking about, which is the composite that certainly contains both K and L by definition so, it is bigger than both K and L and as I said, everything is inside C. So this is the picture. So, this is what is given. Now, given fields F sub set of K and L. Suppose I have the following assumptions, if K over F is a finite Galois extension, then so is K L over L.

So, this is the first part of the theorem says suppose K over F is a finite Galois extension. So, what is that? K thought off as an extension of F is Galois then K L over L is also Galois. So, I will just indicate anything that Galois by this. Maybe we will just put it in green. So when I put something in green that is the Galois extension.

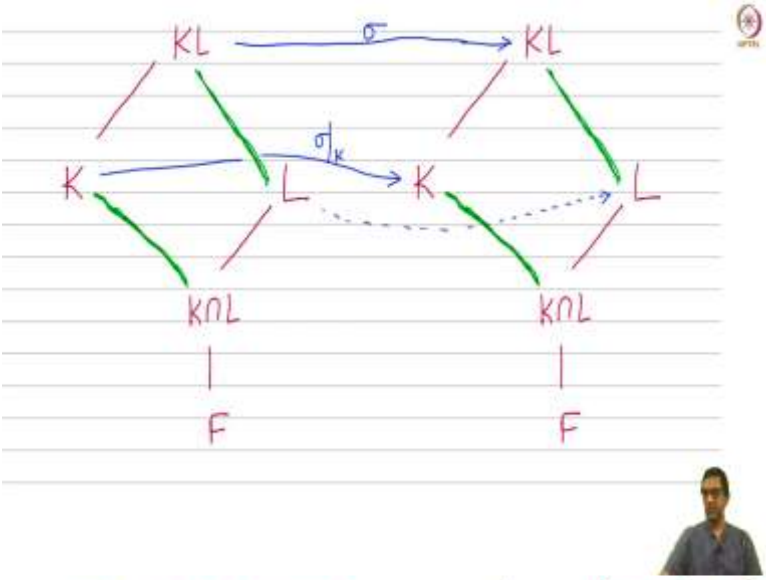
So here is the Galois extension. You are given that K over F is Galois. So that is the first part of the theorem. If K over F is finite Galois, then K L over L is finite Galois. Further, I can also say something about the Galois group itself. What is, how are the two Galois groups related? So the group of K L over L; well, it is not the same as the other group.

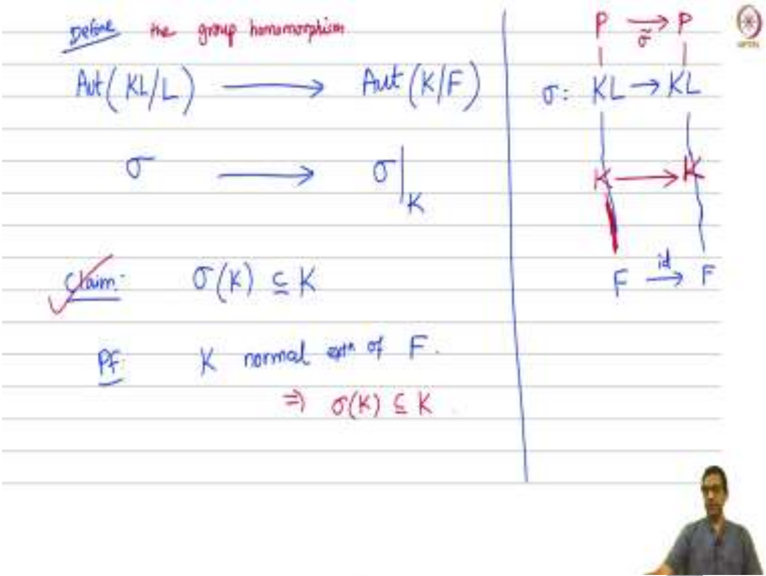
It is in fact only a subgroup and what subgroup is it? Well, you can actually identify it, it is the subgroup K over K intersection L. So this recall is always a subgroup of the Galois group of K over F. So what are we saying? We are saying the Galois group of this extension K L over L is the same as the Galois group of the extension, K over K intersectional.

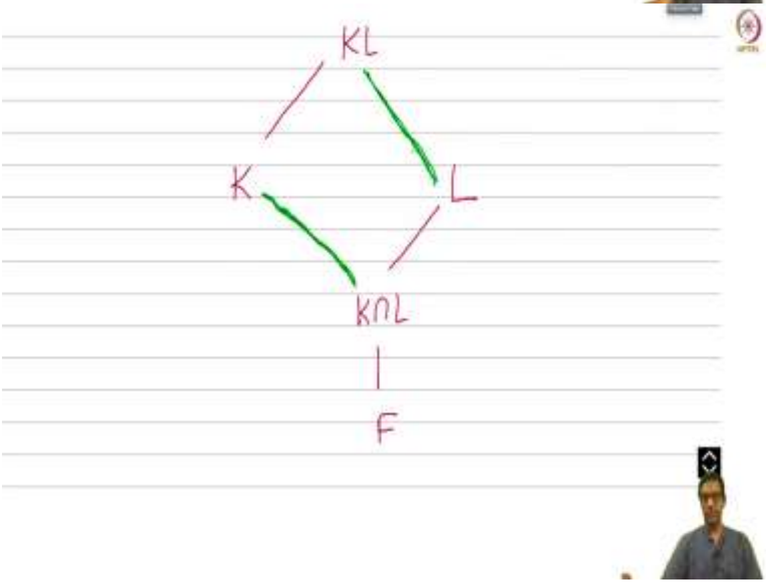
So recall that if K over F is Galois, then K over anything, any intermediate field between K and F is also Galois and Galois just means normal inseparable and those properties continue to hold when you think of K as an extension of anything between K and F.

So all these are Galois in fact, so now finally, what this theorem says is let us erase this green guy. So it is like saying these two opposite sides of the parallelogram are the same in some way. It says that the Galois group of K L over L is the same as the Galois group of K over K intersection.

(Refer Slide Time: 08:19)







So that is the content of theorem. So let us prove this. So first, let us try and see if we can define a map. So we know that, so first let us check that K over L is Galois. So that is easy. So remember, K over F is finite. Galois means of course, it is a normal extension. So it is a splitting field of a collection of polynomials in general. But if it is a finite extension, then you know you cannot have an infinite collection of polynomials.

It is got to be only finitely many polynomials of which this is the splitting field and you can multiply those polynomials together to get a single polynomial of which this is the splitting fee. So in other words, K because it is a finite Galois extension, this is the splitting field of some polynomial F x with coefficients in capital F of x.

This is just from normality and finiteness, since K is normal over F and finite over F and now we just now saw that what is K L? K L is just nothing but the splitting field of the same polynomial but over the field L. So think, if you think of F x as an element of L x then K L is the splitting field of F over L, which means again, by the same token, K L over L is normal and of course, everything here is a subfield of C. So it is characteristic 0 therefore it is Galois.

Good. Now, that is all now we just need to establish that the Galois groups of these two things are the same, the two green sides are had the same Galois group. So let us try and define a map now, between now from the top, Galois group which is K L over L to the Galois group of K over F, K over F not to K over K intersection F, is going to define a map to K over F. So the map itself is obvious. So, what is this map? This is just; take any element sigma in the Galois group of K L over L.

That means that what is sigma? It is an auto morphism of the field K L. So, sigma therefore recall is nothing but a map from K L to K L, the field on top such that sigma restricts to identity on L such that when you restrict sigma to L, you should get the identity map. This is what an element of the Galois group is.

So, in particular sigma is a map from K L to K L. So, let us go back up here. So, this is really your picture. So, let us take K L here make another copy of this diagram. So this is K L to K L and what is sigma? Sigma is just a map from K L to itself, such that when you restrict sigma to L, it is just the identity map.

So on L, it is the identity. So I will just put a dot there to save inside entity map. Now, how do I get a map? What do I need? I need a map from this to the set of auto morphisms of K over F. Well, how I get a map? I just restrict it to K. So just take sigma and you restrict sigma to K.

So if we go here, sigma is defined on the big set. So all I do is I restrict sigma and you know, to K, I just think of it as a function on K. Now, the point is if I restrict sigma to K, the key observation is that the image will again being K. The restriction of sigma to K will map K to itself. So there are lots of nice parallelograms in this figure. So why is this? Observe for this to be well defined, if I restrict sigma to K. The claim is that, well sigma maps K to itself.

Proof: Well, if you go back and look at the various things we proved, about normal extensions and so on, recall that K is a normal extension of F. Now, I can think of sigma as a map from K L to L. So if it is identity on a K L to K L, if it is identity on L, in particular it is identity on F because F is even smaller than L.

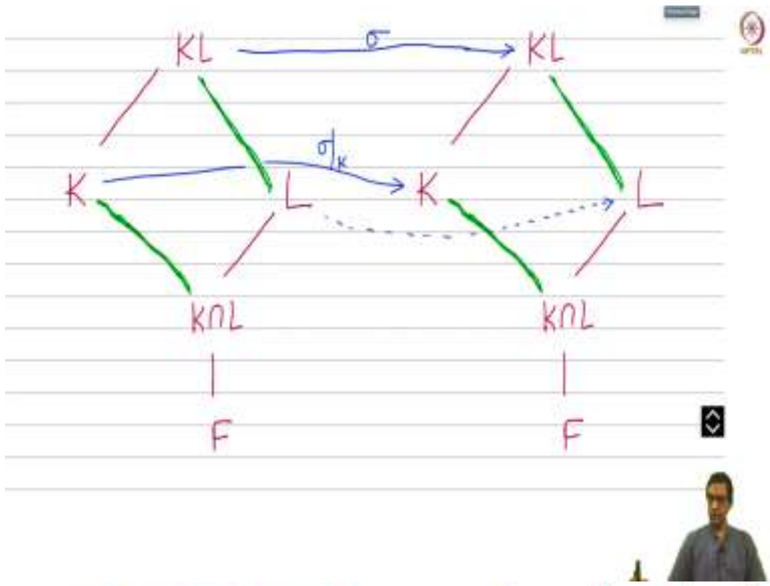
So I just think of sigma is a map from K L to K L, which is identity on F. So let us erase the thing in the middle. It is just a map like this, this identity on F. Now, the normality of K; now the point is K is a normal extension. So K sits in the middle and K over F is normal, then one of the equivalent conditions we proved about normal extension is that if you have sort of a map of the algebraic closures, then that map restricts to a map of K.

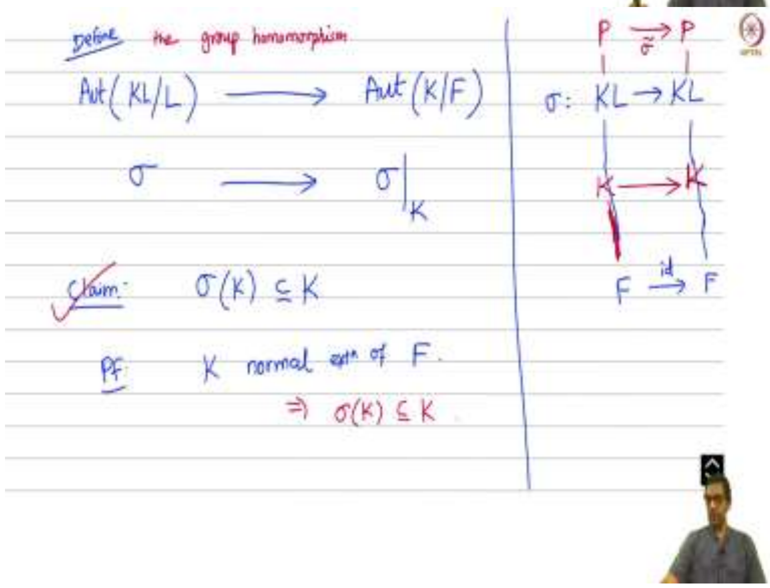
And here, K L is bigger than K you know, you can always extend this to some larger algebraic closure. So, recall by the theorem on algebraic closures, if P is an algebraic closure of L L, any map sigma from K L to K L can always be extended to some map from P to P and I mean we have used these arguments before. So, the restriction of sigma tilde to K will map K to itself definitely. Therefore sigma maps K to K by the property of normal extensions.

Good. So, that at least it allows us to define a map and it is easy to see that this map is a group homomorphism because we have done nothing we have just restricted you are given a map on a larger field. You are just restricted to a smaller field and you know so compositions of maps go to compositions of maps.

So it is a group homomorphism. So define the group homomorphism like this. So for well-defineness we need to check this claim and this claim comes from the normality of K over F. Let us see, where are we now what do we need to do? We need to prove two things, we need to first show that this map is a one to one map and secondly, its image is exactly the subgroup that we claimed in the theorem.

(Refer Slide Time: 15:13)





So we need to prove two claims. So let us go claim 1 that this map is, this restriction map is injective. First claim; second claim its image, let us call its image as something H, it is a certain subgroup of the auto morphism group. It is image H is exactly the set of auto morphisms of K, which are identity on K intersection L.

So this is the second claim that we need to make. If we prove these two claims, then the theorem is proved. Now let us, so H by the way, is just a name that I am giving to the image here. It is nothing. It is not a new subgroup here. I am just giving and calling the image as H. Let us prove it is injective first.

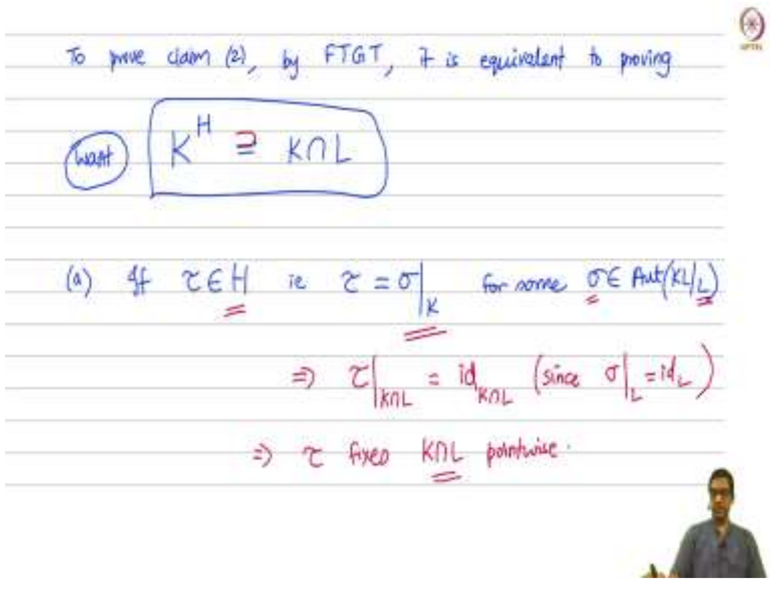
So what was a map? It takes any element sigma of from Aut K L. So let us copy the map. This is the map here. So here is, here is a map. Now, why is this injective? To show injectivity if sigma restricted to K is the identity on K, then we need to show sigma itself is the identity. Now, what does that mean?

Well, on K, it is already identity; observe sigma on L is definitely the identity because sigma came from this subgroup. It was identity on L already, which implies that sigma is necessarily the identity on K union L. Its identity on both of them, but what is K L? K L is just the smallest subfield of C which is generated by the union of K and L.

So if sigma is identity on the union, then it sort of follows easily that sigma is identity on K L. Since K union L generates, so that is all you need to show injectivity. So the first claim is down. Sigma, if sigma K is identity, then sigma K L itself is identity. Now the second claim is slightly trickier. So let us, let us try and prove that.

The claim is that the image H is exactly this subgroup. So let us go look at the diagram again. So, we need to show that the image is the subgroup of auto morphisms of K which are identity on K intersection L. Now, here we will use the fundamental theorem of Galois Theory. So to prove the second claim, how do you show that two subgroups are the same?

(Refer Slide Time: 18:25)



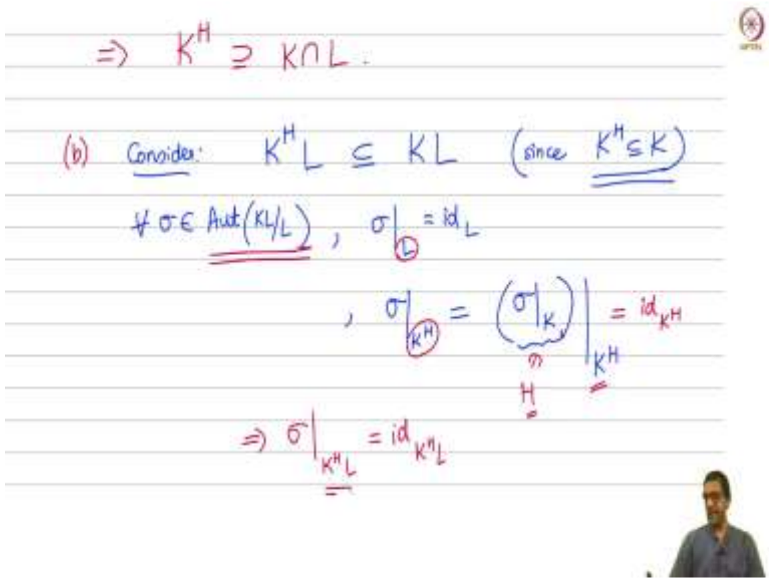
They are both subgroups of the group of auto morphisms of K over F. So to show two subgroups are the same, it is enough to show that there are fixed fields are the same. So to prove claim 2 by the fundamental theorem of Galois Theory, it is equivalent to proving the following some assertion that the fixed field of H is the same as the fixed field of the other group, which was K intersection L in this case.

So, we need to say that these two things are exactly the same. Now, how does one show that K H is K intersection L? So well, let us let us actually see, you know there is there is a one-way containment. So, this is what we will now try and prove. First observe that elements of H. So if sigma belongs to H, what is what does that mean?

i.e, why we should not call it sigma if tau belongs to H, what does that mean? That means tau is of the form the restriction of sigma for some element coming from the Galois group of K L over L. So what does this mean? Well, tau is sigma restricted to K. Now, sigma here fixes all elements of L. So sigma fixes L pointwise. So, the restriction of sigma to K will fix K intersection L pointwise.

So this means that tau on K intersection L is just identity map and why is this? Because sigma was the identity sigma on L was identity map. So what does that mean? This means that tau fixes K intersection L pointwise, therefore the fixed field so tau fixes so, what does this mean?

(Refer Slide Time: 21:00)



At least one way containment; we have shown that every element of H fixes K intersection L. So the fixed field, K H certainly contains K intersection L. So that is what we have proved. So let us say that this means that the fixed field of H just the elements which are fixed by every element of H. This certainly contains K intersection L.

Now, we need to prove the converse. Now the converse is the slightly tricky calculation. So, let us do the following for the converse. Let us do something slightly non-obvious. So, let us take a look at K H. So, it is some subfield H. So, what is K H? It is some subfield of K. So, therefore, K H L is some subfield of K L can since K H is some subfield of K.

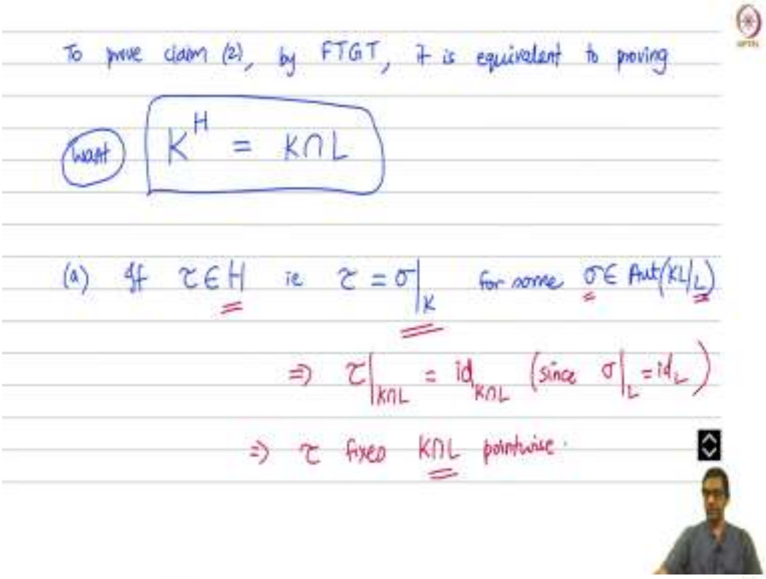
Now, let us do the following. Let us take all elements of the big Galois group. Now all elements, what do they do? Well, sigma fixes L pointwise. In other words, sigma on L is of course identity on L this, we know by definition, but we also know something that if you take sigma restricted to K H, then what is this?

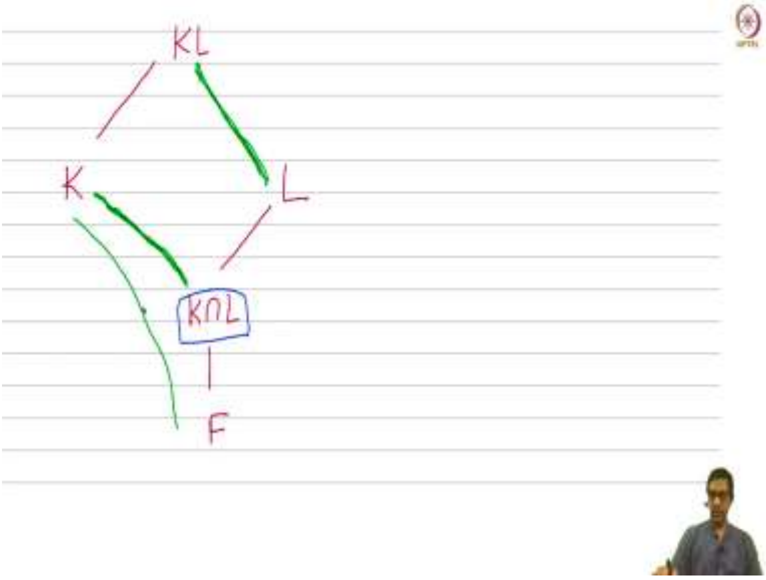
K H is remember, a sub of K. So, how do I restrict sigma to K H? I can do the following; I will first restricted to K, K is still bigger than K H and think of that as being further restricted down to this this subfield K H. Now, what do we know? Sigma restricted to K is exactly the elements those are the elements in the image.

So, this is this is like a tau. So, this fellow here belongs to my subgroup H, because that is the image of a sigma and of course, elements of H, how do they act on K H? By definition this is a fixed field of H. Therefore, elements from H will necessarily act as identity on their fixed fields.

So, this is a slightly tricky argument that one has to work through to understand, but the basic idea is that sigma restricted to K H is like some element of H acting on K H. So that is identity. Now, the same argument that we use before if an element acts as identity on both L and K H on two fields, then it acts as identity on their union and therefore as identity on their composite.

(Refer Slide Time: 23:59)





So same argument as before: so, what does this mean? This says that, you know every element here in K L over L; it also fixes K H L. So, this means that K H L is pointwise fixed by every element of the Galois group but then what does this mean? What is the, what does the fundamental theorem of Galois Theory tell us?

It says that, if I if I have the Galois group, so this means that K H L this field is contained in the fixed field of the entire Galois group. So, if you call this group G, the full Galois group, then this is contained in the fixed field of the Galois group of K L, but the fixed field of the Galois group is always the just the field the base field L.

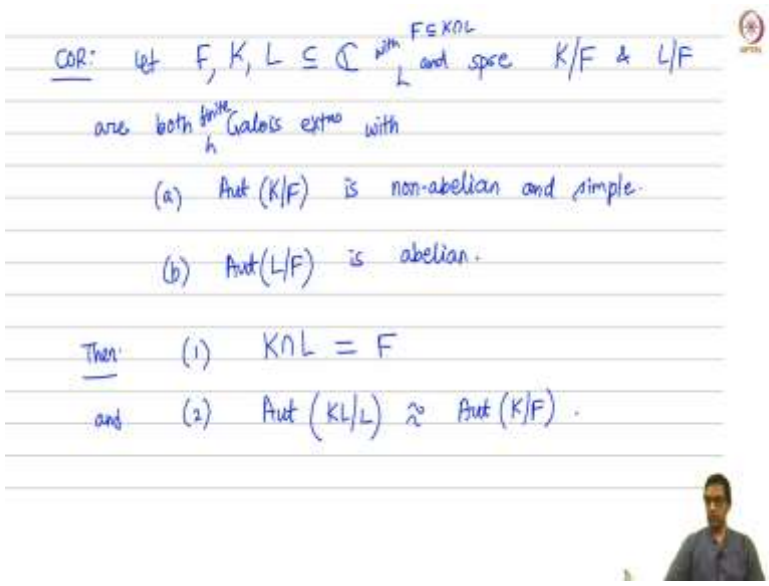
By Fundamental Theorem of Galois Theory and we are also using you know, since K L over L is a Galois extension. So we are using the fact that K L over L is Galois and therefore, the fixed field over the full Galois group is has to be the base field. So what does that mean? It says K H L is a subset of L that is a strange thing, because L is already there, what it says is if you take the composite of L with this other field, you do not get anything more than L, you just get L itself.

That means that K H in particular, this means K H union L is contained in L. This means that K H itself is contained in L. So, what does that mean? K H is contained in L also K H by definition is contained in K. Therefore, together it gives us what we want says that K H is therefore contained in K intersection L.

So, we have shown the other way inclusion therefore, we have shown both inclusions K H contains and is contained in K intersection L. Therefore, K H is equal to K intersection L. So, it is a somewhat tricky proof, but we have managed to do it. So, what this means is that the composite extensions, so let us go back and see what the theorem said.

If I have you know, if F is a subfield, let us get rid of this now. So, if I have that, so here is the statement if K over F is Galois, then so, if this whole thing is Galois, then so is this so is K L over L. Further the Galois group of K L over L is the same as the Galois group of K over K intersection L.

(Refer Slide Time: 27:04)

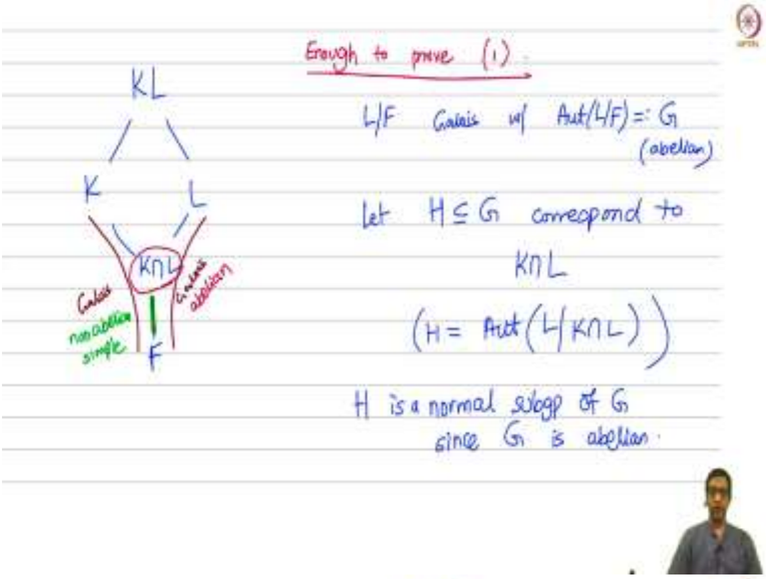


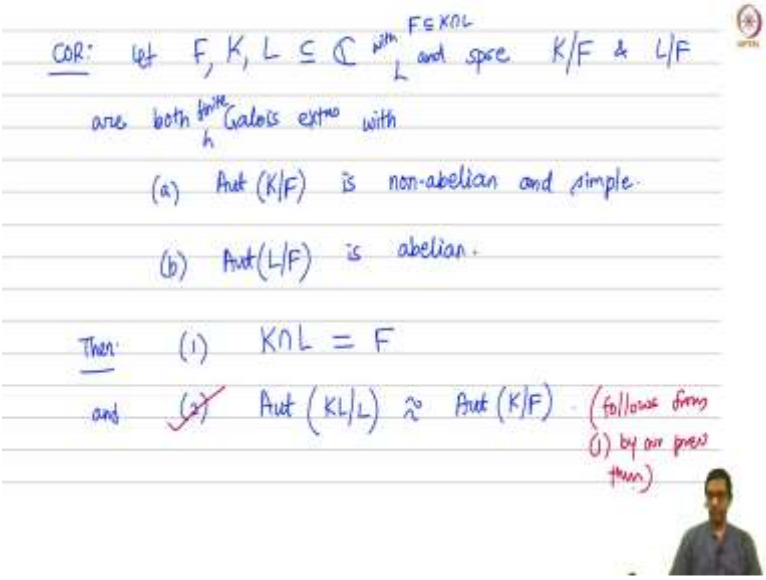
Now, let us just finish this up with a little corollary which is going to be very useful to us. Says the following corollary; let F K L be sub fields of C and suppose both are normal both K, well, I also want F to be contained in both of them. Suppose K F and L F are both Galois extensions, finite Galois extensions, are both finite Galois extensions with the following property that the Galois group so, the group of K over F is non-abelian and simple.

So, recall a simple group means the only normal subgroups of that group are the identity group and the full group and b the other guy is abelian. One of them is non-abelian simple, the other is abelian. So, they are somehow very different, widely different behaviour then, the conclusion is that K and L cannot really have any intersection other than F.

So, I have assumed to begin with that F is contained in both K and L; with I should say F is inside both K and L. But what we are concluding is that K intersection L has to equal exactly F and statement 2, that the auto morphism group of K L over L is isomorphic to the auto morphism group of K over L.

(Refer Slide Time: 29:24)





So, again to draw that picture, it says I have K L, I have K L F, but the assumptions here are that both are Galois K intersection F is a Galois extension, L over F is a Galois extension, but they sort of have these you know, somewhat different behaviour. The Galois group is non-abelian. Simple whereas, the other side it is abelian, this Galois group is abelian.

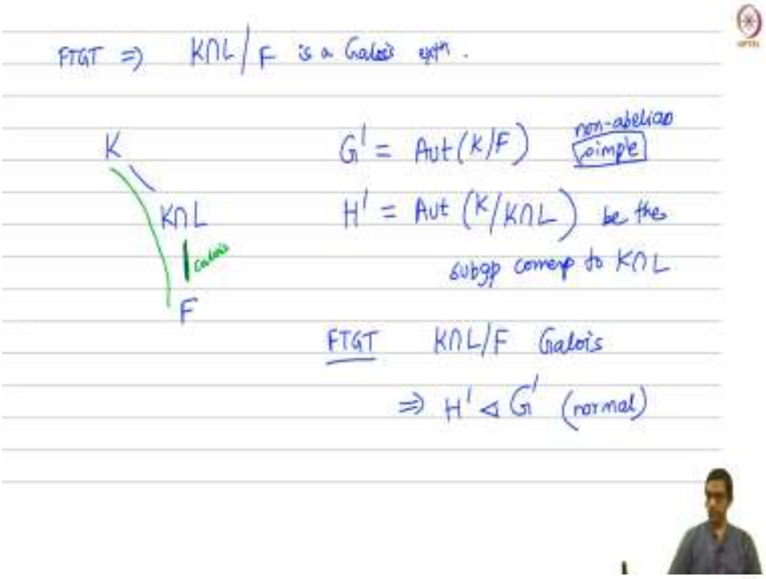
So we have this behaviour, then the theorem says that K intersection L cannot be anything other than F itself and the second part of the theorem observe is a corollary to the first one. So this follows from 1 by our previous theorem, this follows from 1 by our previous because the previous theorem said that the auto morphism group of K L over L is exactly the auto morphism group of K over K intersection L.

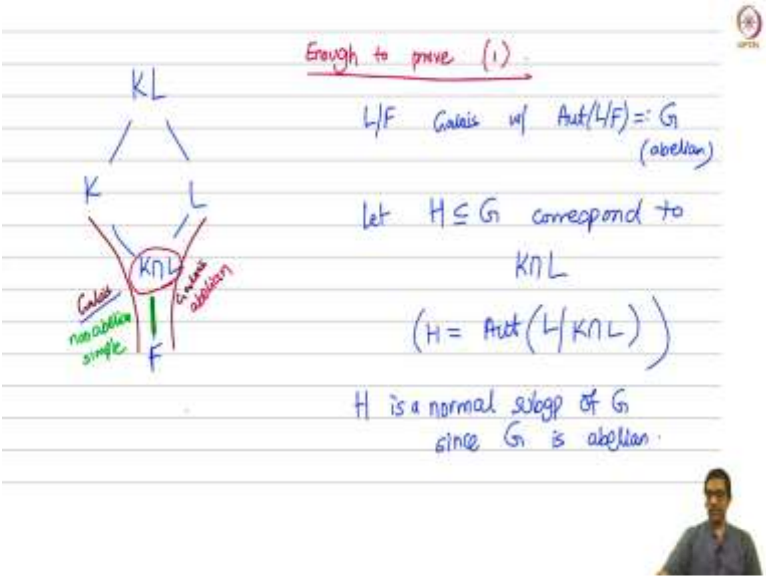
Good. So, we just need to somehow establish this. So, it is enough to prove 1. So that is the first observation, it is enough to prove the first part of the theorem. So let us prove it. Now, let us maybe give these Galois groups a name. So L over F we know it is Galois with let us say the Galois group. Let us give it a name G.

Now, G is an abelian group, G is what is given to be abelian and let us look at the subfield K intersection L. It is an intermediate field and therefore that subfield will correspond to some subgroup. So, let H subgroup of G, be correspond, so the fundamental theorem of Galois Theory there is some you know, one to one correspondence.

So this subfield K intersection L corresponds to a subgroup H and we know what H is. It is actually the group of auto morphisms of L, which are identity on K intersection L. Now, the key point here is that G is an abelian group and H is a subgroup therefore, H is automatically normal, H is normal, H is a normal subgroup of G since G is abelian and the fundamental theorem of Galois theory had something to say about this.

(Refer Slide Time: 32:26)





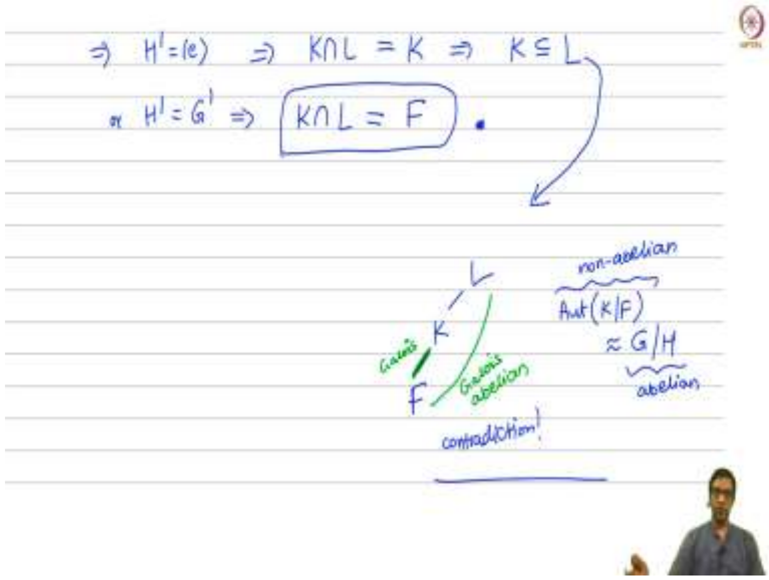
If you have a normal subgroup, then it says that the extension here is also Galois. So again, let us use the fundamental theorem says that K intersection L over F is a Galois extension. Now in fact, we know the Galois group is isomorphic to G mod H and so on. But let us just for the moment, do the same thing from the other side.

So let us look at the other fellow which is K over F is Galois. So, let us consider that that leg of the diagram K, K intersection L F, now by again by the fundamental theorem of Galois Theory. So, what do I know here? I have concluded by using this other side that this is Galois. I already know that this whole thing is Galois.

Now, by the fundamental theorem again, so on this side, so sorry, I should do the same thing on the side. So, let me call this group as G prime, the group of K over F and let us call the group corresponding to H prime as corresponding to K intersection L as H prime, be the group, subgroup corresponding to K intersection L.

Now, again fundamental Theorem of Galois Theory says that, since K intersection L over F is known to be Galois by other means, this automatically means that the subgroup has to be a normal subgroup. That was a if and only if statement; this has to be a normal subgroup of G prime. Now, that is a problem because we have assumed to begin with that G prime is a non-abelian well non-abelian, it is not the key.

(Refer Slide Time: 34:31)



It is it is simple, which means that it is got no subgroups other than, no normal subgroups other than the identity and the whole subgroup. So this means that are, well there are only two possibilities, which implies either H prime is the identity or H prime is the whole. Now, what do these two things mean?

If H prime is the whole, then the corresponding field that it corresponds to has to be the base field, that is the correspondence and on the other hand if it is identity, then the field K intersection L has to be the big field which in this case is K. So, there are only these two possibilities. But observe K intersection L is K will mean that K is a sub of L.

So, K is a, K is actually a sub extension of L. Now, what does this mean? This means that the diagram that we drew actually looks like this. There is F, K comes somewhere in the middle and then L comes somewhere further up. But then observe L over F was given to be Galois, this is Galois and with abelian Galois group so, again by the same argument that we gave before K intersection F, I mean K intersection L is K this is this is also a Galois extension.

And the Galois group if you remember, Galois group of K over F would have to be, it is a quotient. So, this would be in our earlier notation, this is the quotient G mod H. But whatever it is G is abelian so, G mod H is abelian, but we are also given that the auto morphism group of K over F is non-abelian.

So, we use both hypotheses is that it is non-abelian as well as simple. So, what does that mean? So, that is a contradiction. So, this this case cannot arise, tells you that K cannot be a sub of L. Therefore, the only option is this one which is K intersection F is K intersection L is F itself. Now, you know there are various modifications of this which will be relevant in that we will look at the next video.