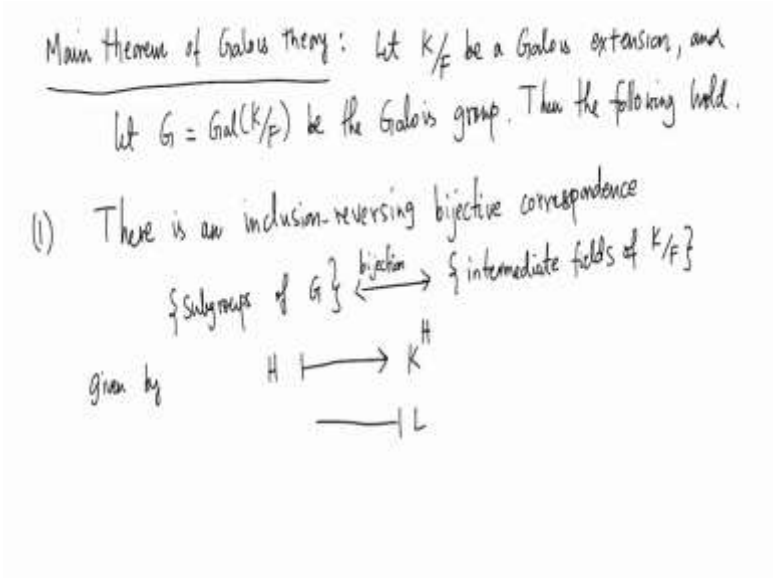
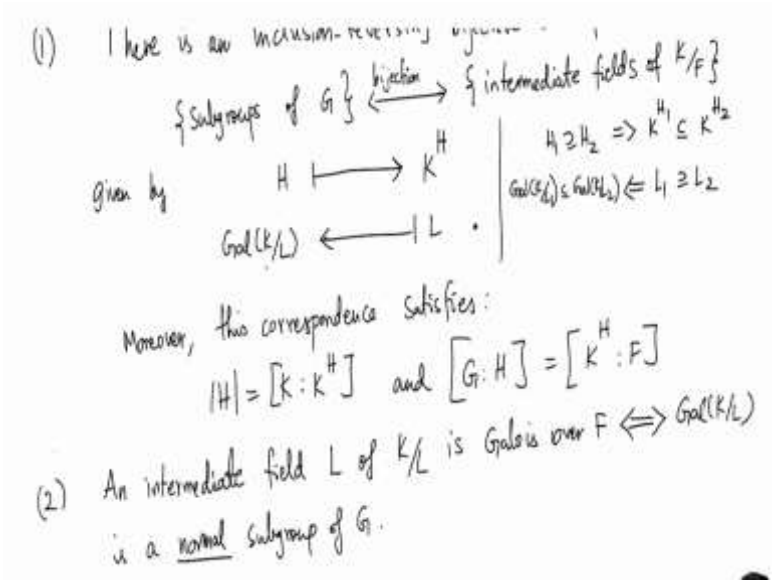
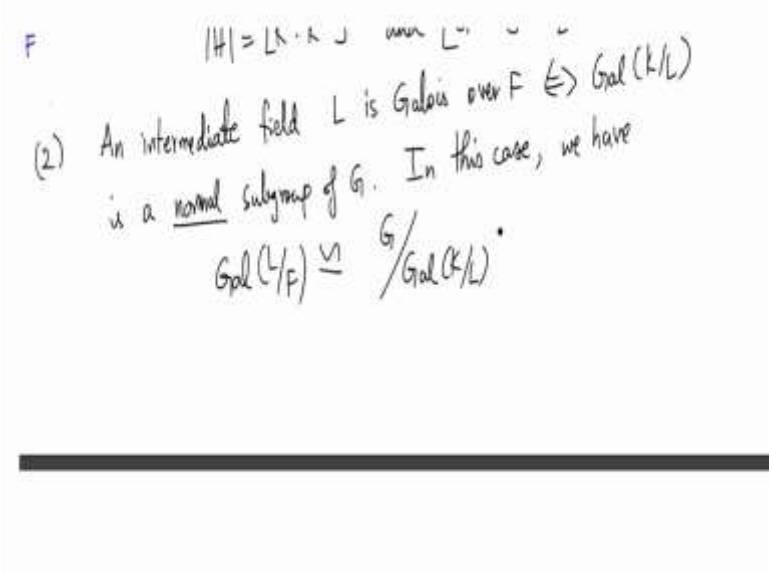
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture – 24
Main Theorem of Galois Theory – Part 1

(Refer Slide Time: 0:21)







Welcome back, so today we are going to state and start the proof of the main theorem of Galois Theory. So, in the last video I gave you a recap of whatever we have done so far about Galois Theory and I also gave you few examples to motivate the main theorem of Galois Theory. So, I am going to state now and see how much of it I can prove today. And the proof like I said, is fairly easy ones.

So, let K over F be a Galois extension. And I will only orally say here but Galois extension is always a finite extension. So, we are also assuming that K over F is a finite extension and in addition it is Galois extension. So, let K over F be a Galois extension and let G be the Galois group, so instead of writing G, A, L, K over F we are going to simply write G for this proof, for this theorem. So, let G is the Galois group, then the following statements hold.

The first one is the statement that I indicated in my examples in the last video which is a bijection between sub-groups of G and intermediate fields of the extension. So, more formally there is an inclusion reversing bijective correspondence between, so I will simply write the sets here, sub-groups of G, so this is the bijection and intermediate fields of.. remember intermediate fields means, it means sub-field L which contains F and it is contained in K, something like this.

So, the right hand side is all L, like this which includes K and F. So, intermediate fields of K over F. And it is given by, this is the point H cross to.. H is the sub-group; you simply send it to K power H. We will show, of course it is easy but we will expressively show that it is an intermediate field. On the other hand, if you take an intermediate field L, it is going to go through Galois K over F. We will see that, it is a sub-group of G.

So, this is the exact maths in both directions and it has a property that, if H1 is containing H2 that implies K H1 is containing K H2. This is the inclusion reversing part of the statement. Similarly if L1 contains L2, this implies Galois K over L1 contains is containing Galois K over L2. These are all part of the statement, if L1 is a bigger field its Galois group of K over L1 will be containing Galois group of K over L2.

Moreover, before that I will write, this correspondence satisfies the following equalities. The order of K H is the degree of the field extension K over KH and the index of H is the degree of the bottom extension. So, I want to draw a picture in a minute but that will clarify this. So, K over the intermediate field given by H is H, the degree. K over H or the base field is the index of that H. This is confirmed in the examples that we did in the previous video.

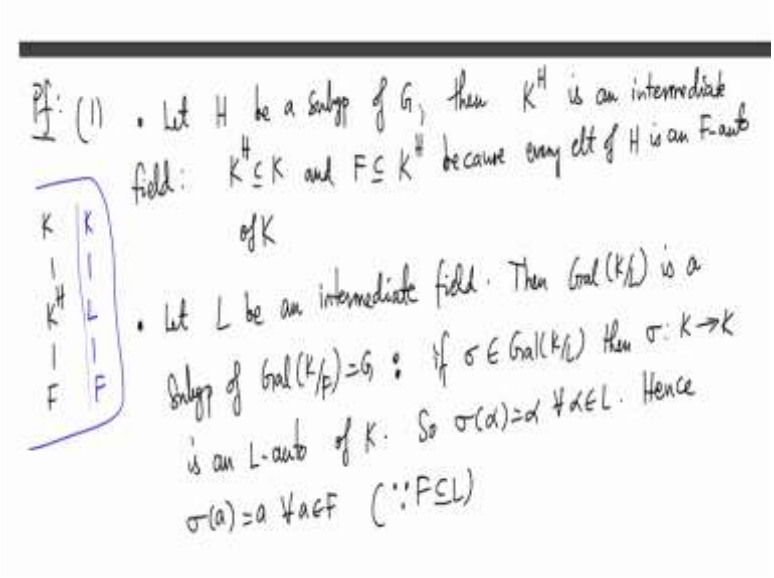
An intermediate field L of the extension is Galois over F if and only if Galois K over L which is the corresponding sub-group to L is a normal sub-group of G, it is a sub-group by this statement 1, L gives the sub-group Galois K over L. In general, it is merely a sub-group, if it is normal sub-group then L is Galois extension of F, maybe this is bit confusing so I will just simply write, an intermediate field L is Galois over F.

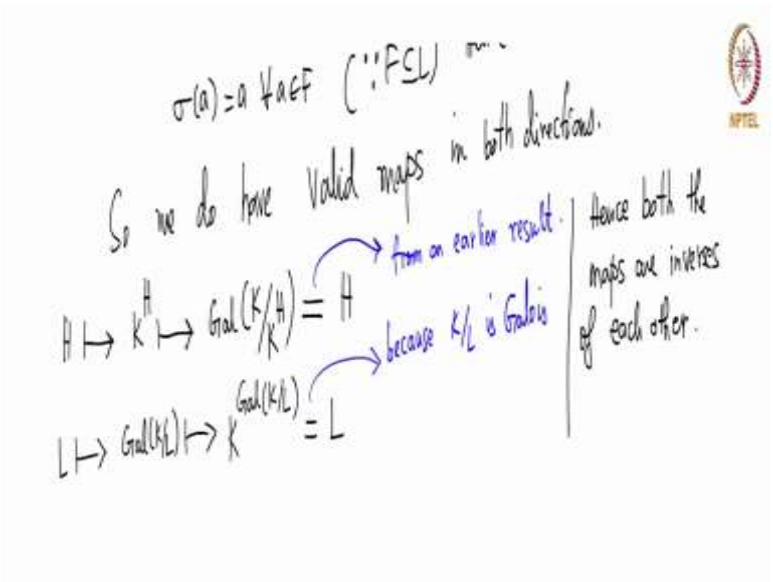
Of course it is an intermediate field of the extension, so if and only if Galois K over L is a normal sub-group of G. In this case, we have, the Galois group of the Galois extension L over F, is in fact, isomorphic to G mod Galois group of K over L. Galois K over L is a normal sub-group of G, by the first statement so you can take the quotient group. So, this is the statement of the main theorem.

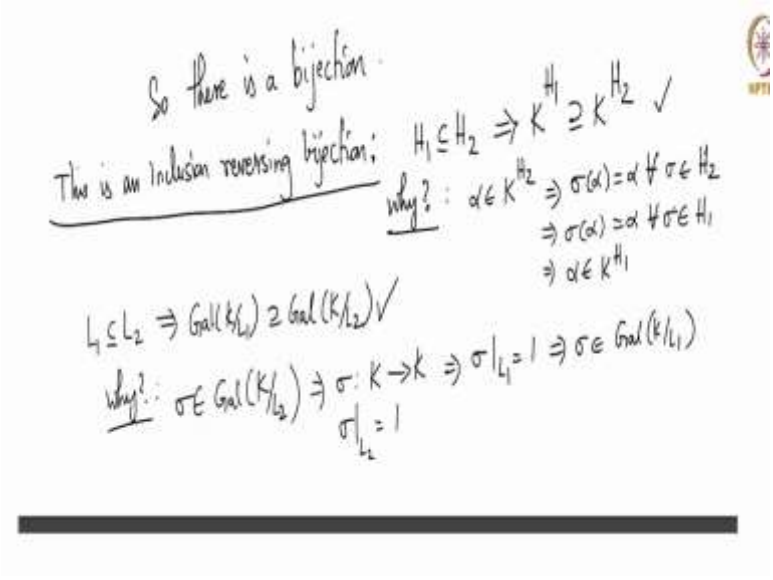
So, I cannot make whole thing appear but there are 2 parts so K over F is any Galois extension with Galois group G, that we have 2 statements. First is that, there is a bijection between sub-group of G and intermediate fields of K over F. So, this tells me by the way why in all these cases, there are no other intermediate fields, in these examples because there are no other sub-groups.

So, that is the statement and in fact, we know more about these correspondence. The order of the group is the index degree here. The index of the group is the degree here and this is normal, if and only if, sorry this is Galois, if and only if this is normal. So, all of this is confirmed in this examples but of course we have to prove this. So, just to draw the picture, we have K, KH, and H sorry F. This is order H and this is index H that is the statement here.

(Refer Slide Time: 7:43)







So, now let me start proving the theorem, so we will prove this, as I said the proof is easy given everything that we have done. So, we just have to carefully do all the steps. So, proof is as follows, first we take, first we will prove 1. So, let H be the sub-group of G, then KH certainly is an intermediate field. This is a trivial statement, right? Of course KH is contained in K because it is the sub-field of K consisting of element that are fixed by all of age.

And F contains, F is containing KH because every element of H is an F automorphism of K. So, every element of H is a F automorphism that means every element of H fixes F point wise. So, F is in the fixed field so KH is indeed an intermediate field. And now let us apply the, this is the first map, I am just saying the map going from H, K power H is in fact, a set map. You take a sub-group and give an intermediate field.

Other than that, if you take an intermediate field, then this is something that we have observed several times in the past but then we know that Galois K over L is a sub-group of Galois K over F, which is G. This is because if sigma is in Galois K over L, then sigma is an L automorphism of K. So, sigma of alpha equals alpha for all alpha in L and hence sigma of a is equal to a for all a in F. Since F is containing L, right?

So, here I am.. maybe I will just draw this here. K, L, F that is given to you. So, F is containing L so if an automorphism fixes L point wise, it fixes F point wise. And hence, sigma belongs to Galois K over L. And it is a group, so hence Galois K over L is a sub-group of G. So, this map is also well defined, so you take an intermediate field and you do get a sub-group. So, we do have valid maps in both directions.

So, give me a sub-group, I map it to an intermediate field via taking the fixed field which is an intermediate field as I argued here. On the other hand, if I take an intermediate field, I take its Galois group of K over that intermediate field, I do get a sub-group as I already argued here. So, we do have valid maps in both directions. So, to prove bijection all you need to check is that we have identity when we compose either way. So, let us start with H, next we want to show that the maps are inverse of each other.

So, let us start with H and go to K power H that is the map in the followed direction. Now go back in the opposite direction, what we get? By the map define here, L goes to Galois K over L. So, K over H, K power H goes to Galois, K over K power H. But this is exactly equal to H and this is, if you recall in the last video I gave you a bunch of formulas that I recalled, Galois group of K over K power G is G. For any automorphism groups G of K.

So, apply that to H, forget this. So, this comes from an earlier result so this is okay. So, that means you go from H to the fixed field and then come back, you do get H back. So, on the other hand, let us take L so now I am proving that, you start with L, take the group and then combine and look at its fixe field. So, L goes to Galois K over L. So, this is the map from intermediate fields to sub-groups. So, L goes to Galois K over L.

And now where does this go? This goes to K power Galois K over L because that is the map, H going to K power H. So, Galois K over L goes to K power Galois K over L and this is L and this follows because K over L is Galois. K over L is Galois so K power K over L is Galois. So, this is also recorded in the list of formulas that I wrote in the previous video.

So, K power Galois K over L is Galois that means… hence both the maps are inverses of each other. H going to K power H and then L going to Galois K over L are inverses of each other and hence… so there is bijection. So, the bijection part is clear right? So, we have 2 set maps between set a and set b, there is a map from a to be and there is map from b to a. Since that both compositions are identities, one identity on a and the other is an identity on b so a and b are bijections. A and b are bijective via those maps.

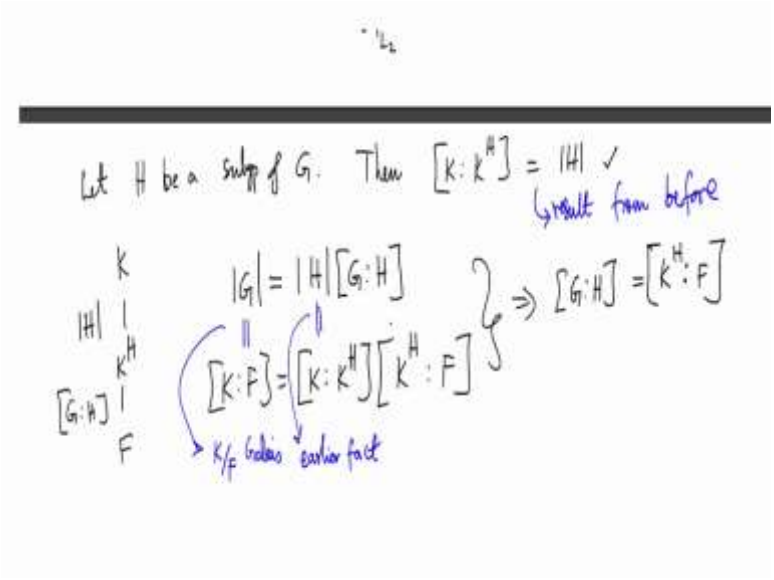
So, now why is this inclusion reversing? So, this is a triviality so I will not spend too much time on this but this is clear, right? If H1 is containing H2 K power H1 contains H power H2. So, why is this? So, let us take something in K power H2, so let us say, alpha is in K power H2 that means sigma of alpha equals alpha for all alpha in H2. But that means, sigma of alpha equals alpha for all..

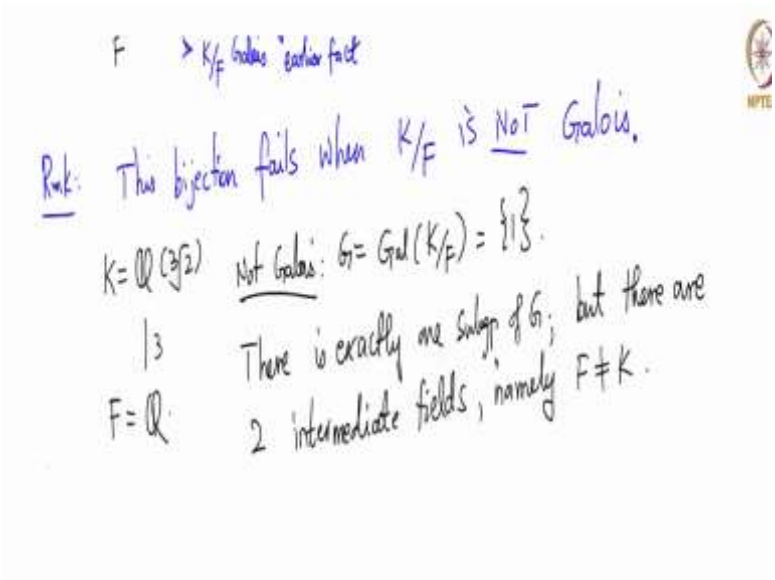
This is sigma in H2 so this must be true for every sigma in H1 because you gave me a sigma in H1, it is in H1 so it is also in H2 so alpha has the property. So, that means alpha is in K power H2, H1. So, that is okay. So, essentially I am proving this. So, now on the other hand suppose L1 is containing L2, I claim that Galois K over L1 contains Galois K over L2, so why is this?

So, let us say, sigma in Galois K over L2, so I want to show that it is containing Galois K over L1. This means sigma is an automorphism of K such that sigma is restricted to L2 is identity. So, let me write 1, that is the meaning of an L2 automorphism of K, so sigma is automorphism of K which fixes 1, every element of L2. But this means, sigma restricted to L1 is also identity because L1 is containing L2.

So, sigma of alpha equals alpha, for every alpha in L2 that means sigma of alpha equals to alpha for every alpha in L1. This means sigma is in Galois K over L1 also. So, you took something here and showed that it is in this. So, it is an inclusion reversing bijection. So far so good, so what we have shown is, there is a bijection reverses inclusions.

(Refer Slide Time: 16:35)





Now let us prove the last part, this is also trivial. Let H be sub-group of G, then the index of K or K power H is equal to order of a H1 this is a fact from before. Or result we can say as we have proved it. So, this is recalled for you earlier, so this is the first statement there. So, this is the first statement, so you have K. K power H and F.

So, this is exactly the order of H. But now we do know certain things, so order of G, because of the product rule for group theory, in the group theory that you have learned; when you have learned group theory. So, order of a finite group G is equal to order of the sub-group H and index of the sub-group. On the other hand we also know K over K, the degree of K over F is equal to the degree of K over KH times degree of KH over F.

So, this is equal to this times this. We have both facts that we have studied in the respective courses. This is from group theory and this is from field theory. Now what we know if that, this is equal to this because it is a Galois extension; this is because K over F is Galois. And this is equal to this, this is the fact that we just recalled, earlier fact, so then this 2 better be equal. So, this implies… G colon H is KH colon F. So, this is G colon H, KHF, so this is exactly the last statement of part 1.

So, this is actually a consequence of this, so once you prove this, this follows. So, this is the nice, even the statement 1 is nice structured theorem of Galois extensions. Every time we have a Galois extension, you have a complete knowledge of all the sub-group, all the intermediate fields of the extension, just using what we know about Galois group and its sub-group. And we further know about, the degrees of the various field extension.

So, before we prove number 2, let me just go back to the examples that we looked at in detail. So, here you have sub-groups of order 2 hence these are order 2. This sub-groups also have index group so these are also degrees 2. And in this example, H prime is a sub-group of order 3 so K colon K power H1 is order 3, degree 3. H1, H2, H3 are sub-groups of order 2 hence K is degree 2 of the corresponding fixed fields.

And hence the index of H prime is 2 so this is 2. Index of H1, H2, H3 are all 3 so these are all 3. And of course there is no inclusion relationship between H primes and H1's so there is no inclusion relationship between these 4 sub-fields, these 4 intermediate fields. Similarly, there is no inclusion relation between L1, L2, L3. However in the finite fields case, there would be.. I did not analysis this fully because it is going to be messy to draw the tree here.

But there will be inclusions of the sub-groups here and hence there will be inclusions of the intermediate fields here and inclusion reverse in things here. So, let me actually stop this video here because I do not have to go fast over the second part and it will take me more than 10 minutes. So, what I want to do is to just remark that this bijection fails when K over F is not Galois. So, let me quickly give you a simple example and then we will stop this video.

So, what is the reason or example this fails, let us take K to be Q adjoin cube root of 2 and F to be Q. So, in this case, this is not Galois as we know very well, as we have several times mentioned this. And what is the Galois group here? It is just the identity. So, there is exactly 1 sub-group of G but there are 2 intermediate fields namely F and K, there are not different, they are distinct, right?

F and K are distinct field, this is the degree 3 extension, and they are distinct fields so there are 2 intermediate fields, here there are 2 elements in this set and in this set there is only 1. So, the bijection fails, so the assumption that K over F is Galois is extremely important. And it is a good exercise for you to go back to the proof and identify all the points where we used Galois property. So, K over L is Galois because K over F is Galois.

And this is not just the only place; there are several places where bijection will require the fact that it is a Galois extension. So, let me just stop this video here, I will continue with the proof and prove the second part in the next video. Thank you.