Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 41
Correspondence of Normal Subgroups and Galois sub-extensions

(Refer Slide Time 00:25)

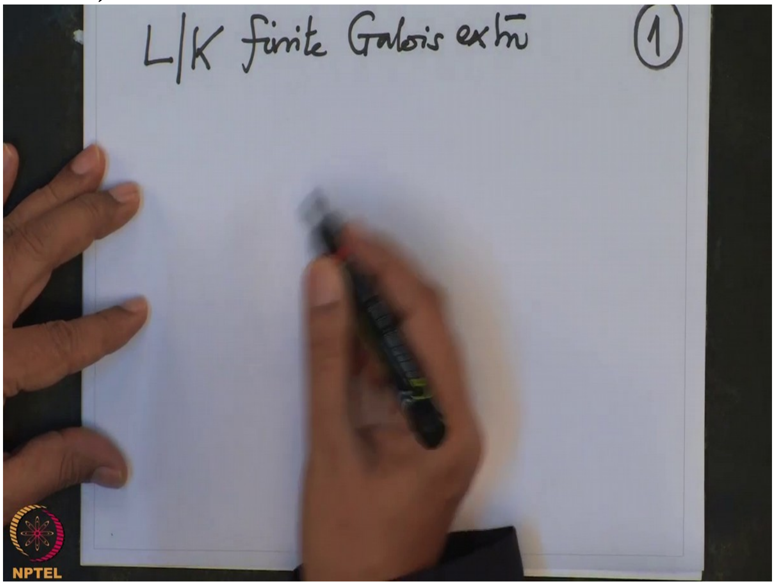
So last lecture we have observed some basic facts about the invariants

(Refer Slide Time 00:34)

of a subgroup, invariants of a subset when a group G is operating on the bigger set. And we want to apply those observations to our case when a Galois group is operating on a bigger field. So let us recall what I want to do.

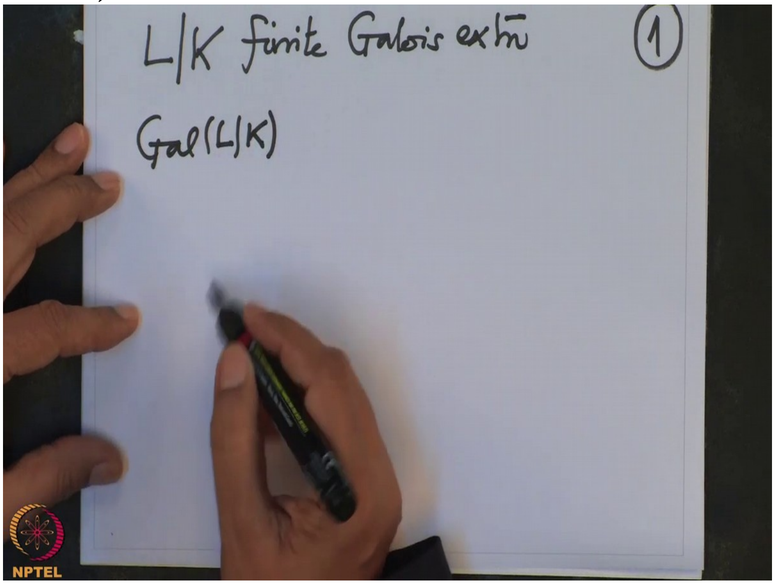
So we have a finite field extension L over K. This is finite Galois extension.

(Refer Slide Time 01:16)



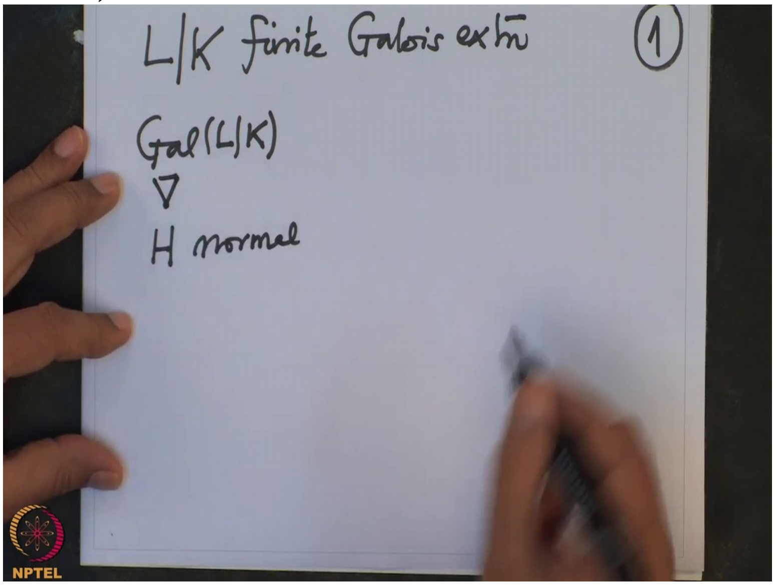
And so we have a group attached to that, that is the Galois group and

(Refer Slide Time 01:23)



we have given a normal subgroup H, H is normal subgroup, normal in this. So remember the notation was like this. This is a normal subgroup, it is a subgroup

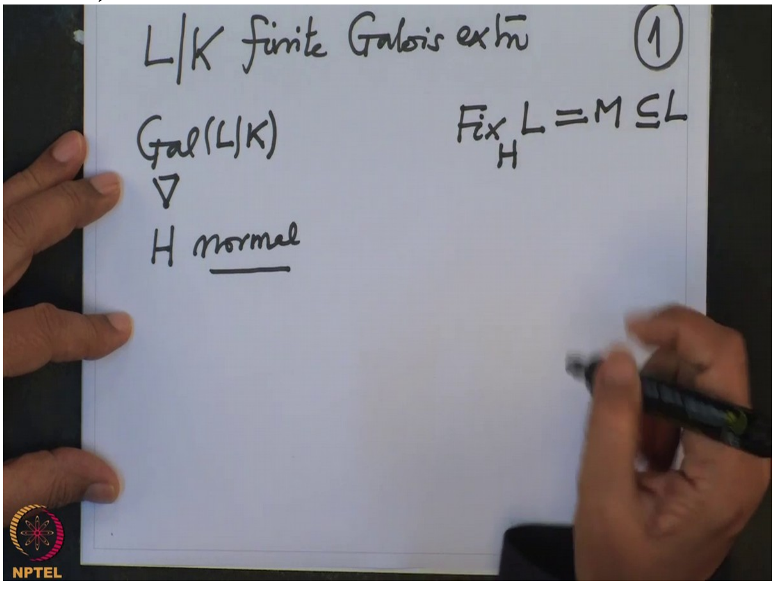
(Refer Slide Time 01:40)



and it is normal.

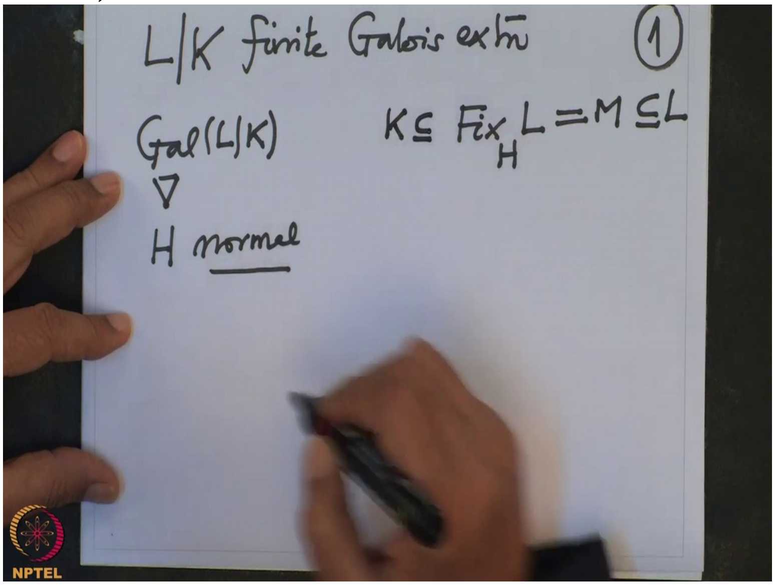
Then I want to study the fix field. So that means $Fix_H L$, this is M, this is a subfield of L

(Refer Slide Time 01:56)



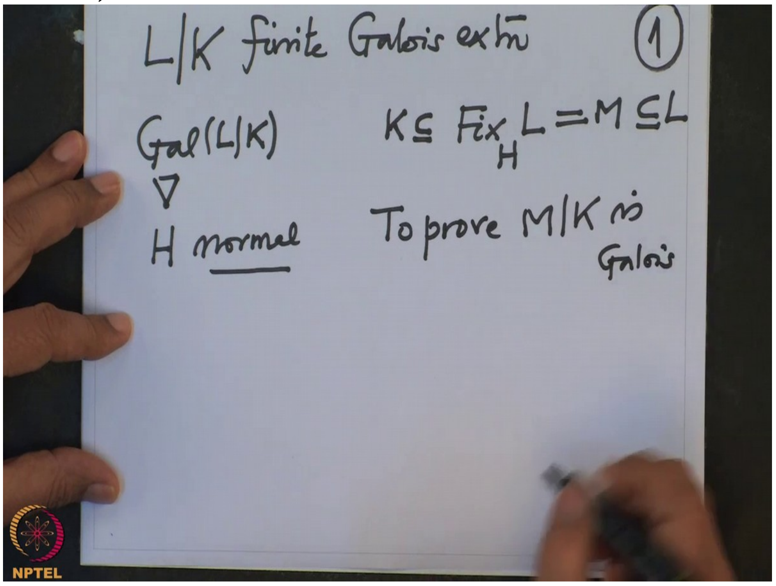
and I want to consider this M over K. It clearly contains K

(Refer Slide Time 02:03)



and I want to prove that this extension is Galois. So to prove M over K is Galois extension.

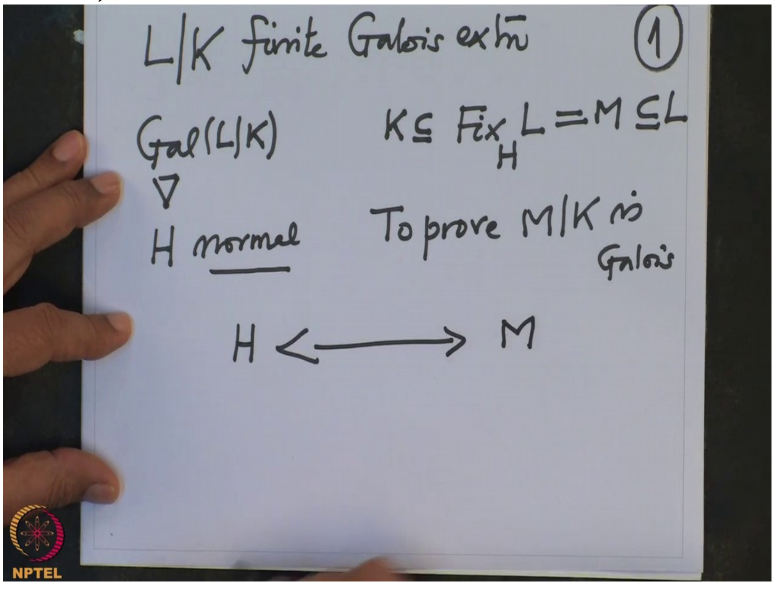
(Refer Slide Time 02:19)



In fact I want to prove if and only if. So first I will prove this is Galois and second I will prove that assuming this is Galois, I will prove this subgroup is normal.

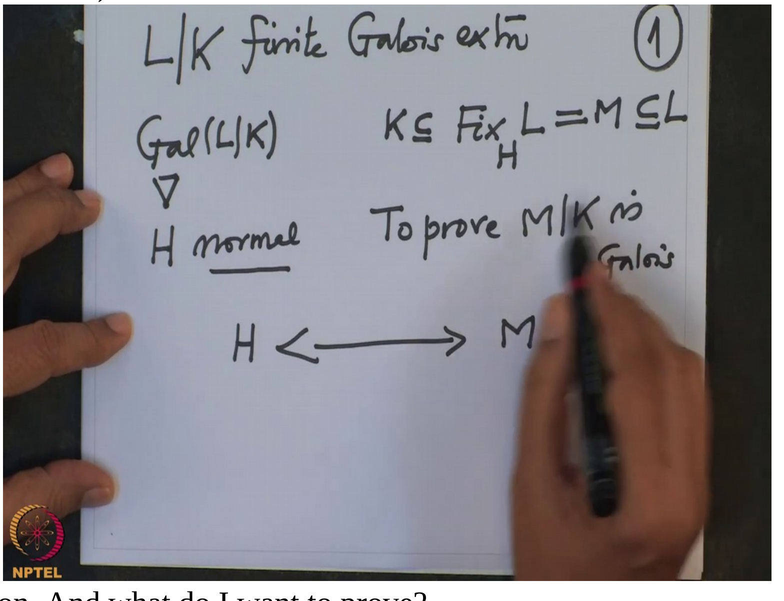
So now H corresponds to this field extension, this field M.

(Refer Slide Time 02:37)



So we want to prove M over K is Galois if and only if H is normal. So I am only proving the first part. So assuming H normal I want to prove M over K

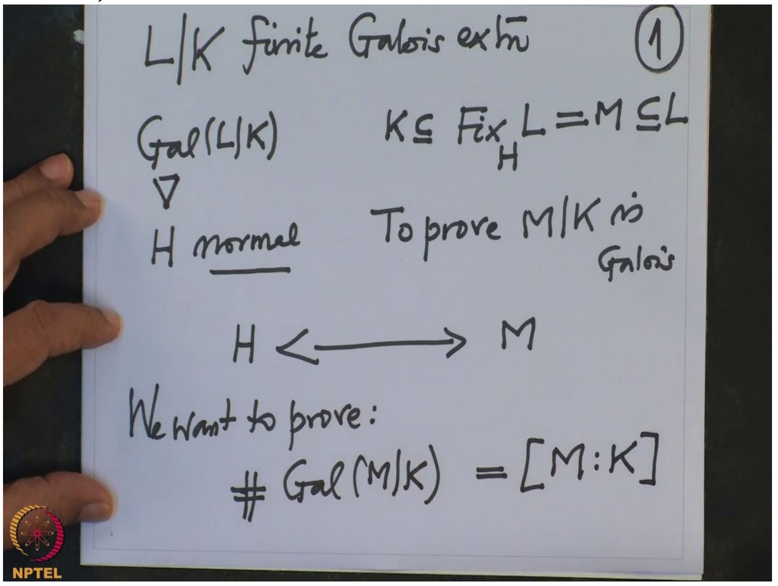
(Refer Slide Time 02:50)



is Galois extension. And what do I want to prove?

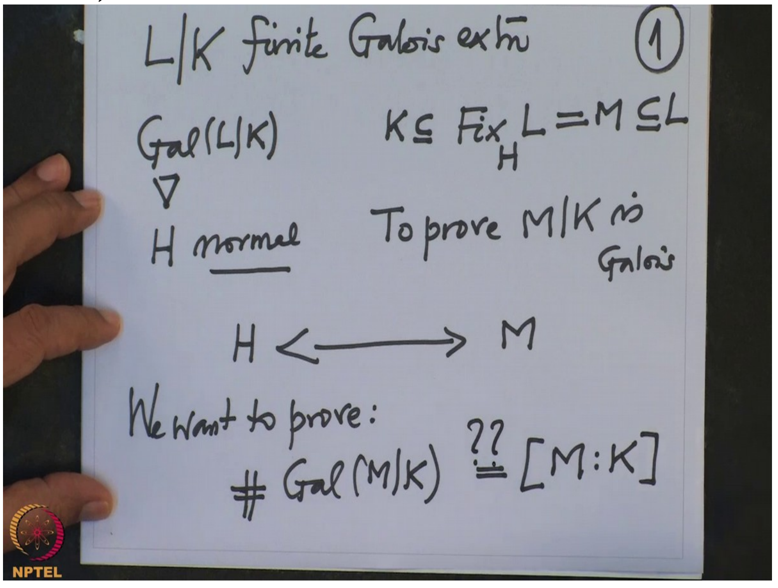
So that means we want to prove, we want to prove the order of the Galois group; $Gal(M|K)$, this order is nothing but the degree of M over K.

(Refer Slide Time 03:15)



This is what we want to prove. This is what

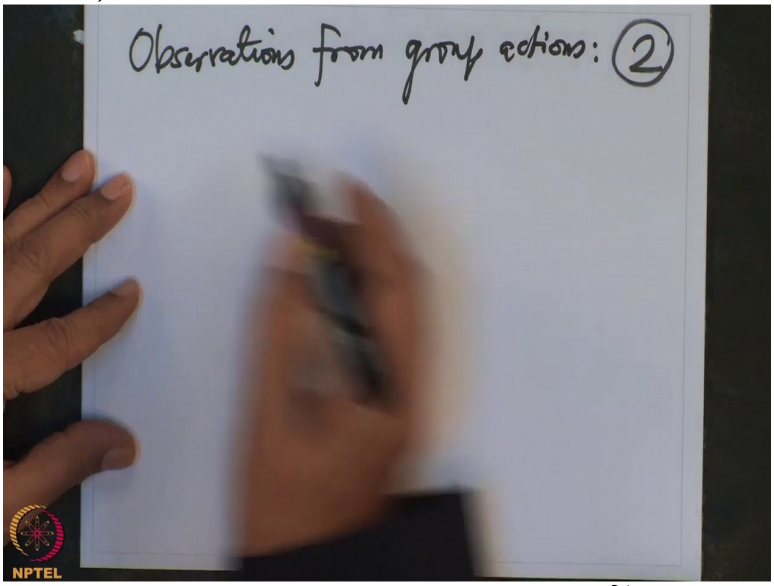
(Refer Slide Time 03:19)



we are heading to prove assuming H is normal, alright.

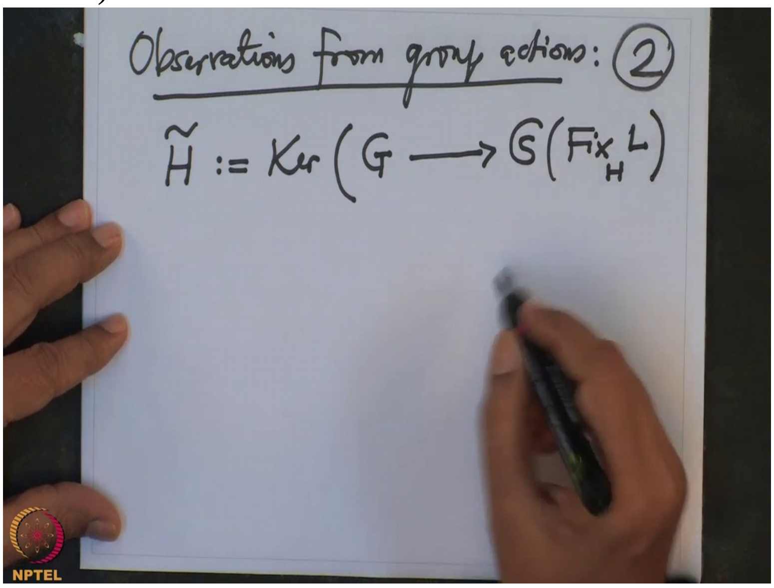
So here is what we have a situation. So when will H be normal? When H is normal, we know, we know from the observation from group actions, observations from group actions tells us

(Refer Slide Time 03:50)



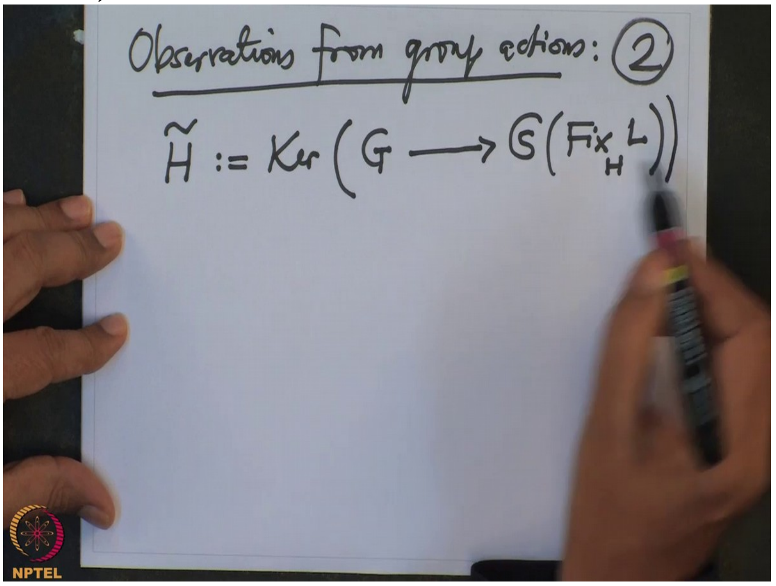
that if I want to check that, Ok so I want to check that, so $\widetilde{H}$, this is the kernel of the operation on G, we know that G operates on the fix field of H.

(Refer Slide Time 04:26)



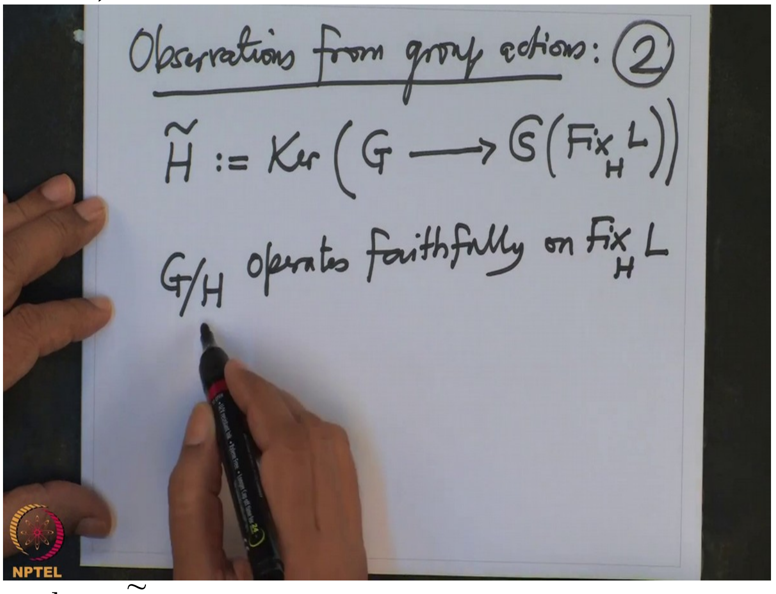
This we have checked that this is a fix elements of L under the action of H and we checked that this, because H is normal this fix H is invariant under all action of G and therefore we have a group homomorphism from G to this and the kernel

(Refer Slide Time 04:47)



of this group homomorphism is because, this kernel, so I want to check that G/H operates faithfully on $Fix_H L$, this we know

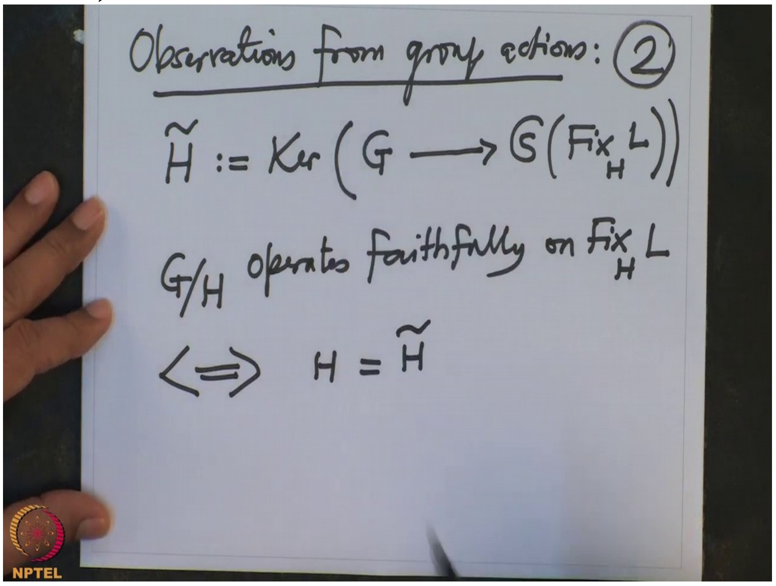
(Refer Slide Time 05:13)



if and only if H equal to $\tilde{H}$.

This is the observation

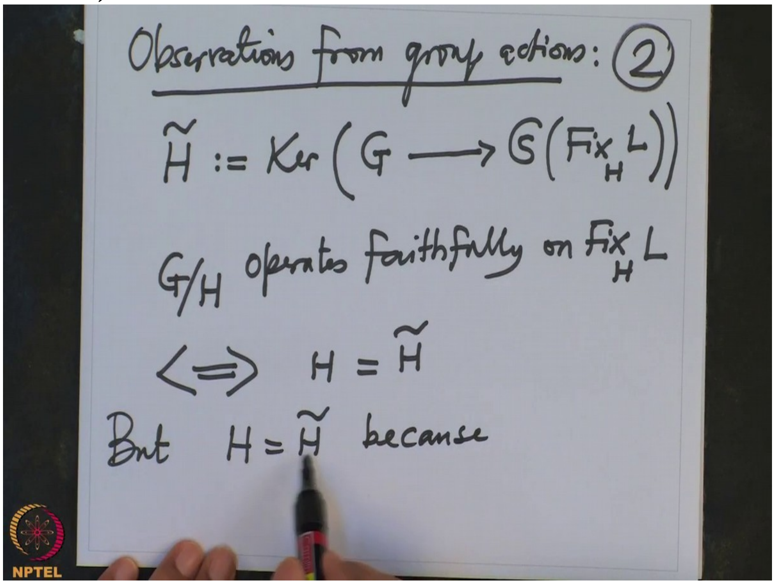
(Refer Slide Time 05:18)



from the group action we have made it, because H is normal, Ok. But if I, if I know that H equal to $\tilde{H}$, do I, if I know this equality then I will know that G/H operates faithfully on this fix field.

But I would say, if I want to, I want to check this, but H equal to $\tilde{H}$ because, see I want to prove the two sets

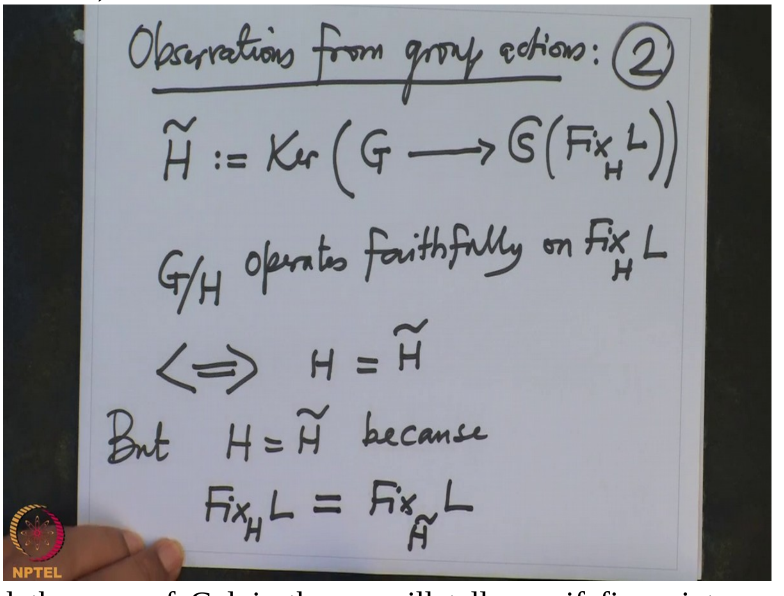
(Refer Slide Time 05:52)



are equ/equal, two subgroups, these are both subgroups and I want to check that they are equal.

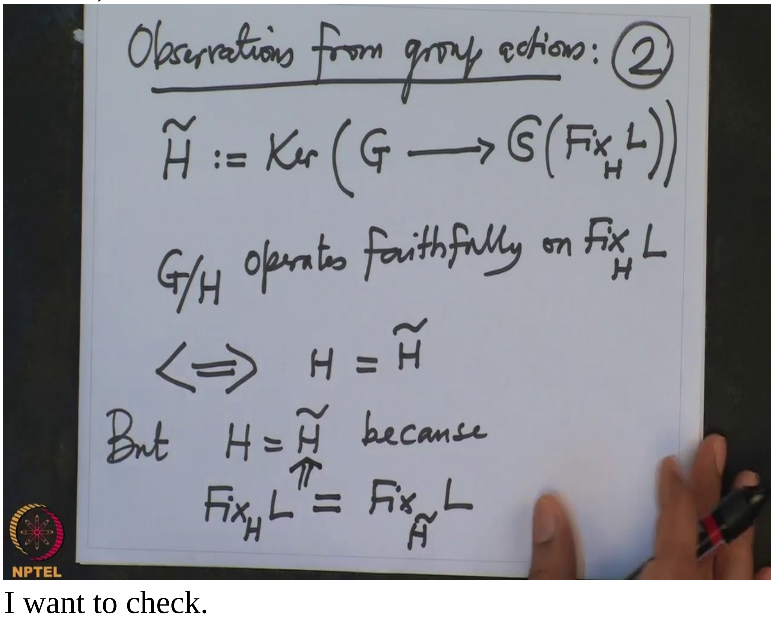
So I might check as well that their fix points are same. So this is because $Fix_H L$ and $Fix_{\tilde{H}} L$, if I take both these are equal

(Refer Slide Time 06:15)



then fundamental theorem of Galois theory will tell you if fix points are equal then the subgroups are equal. So this will be, this is what I want to check.

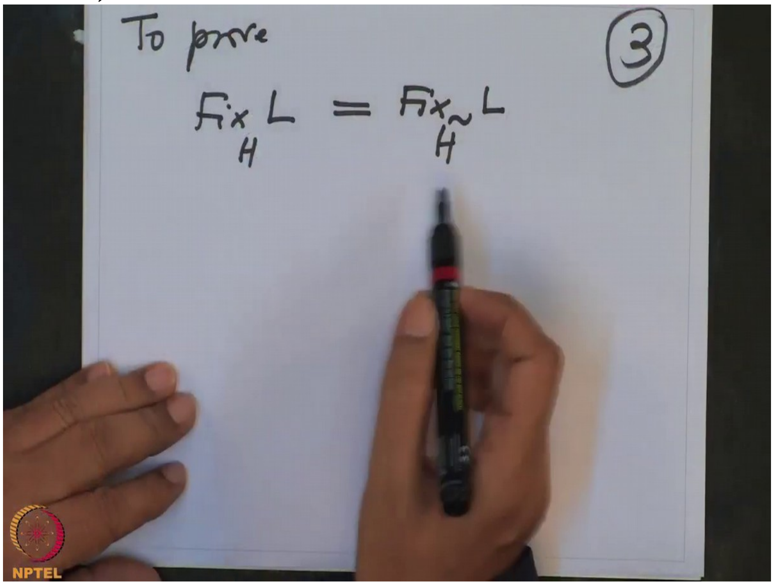
(Refer Slide Time 06:24)



This implication I want to check.

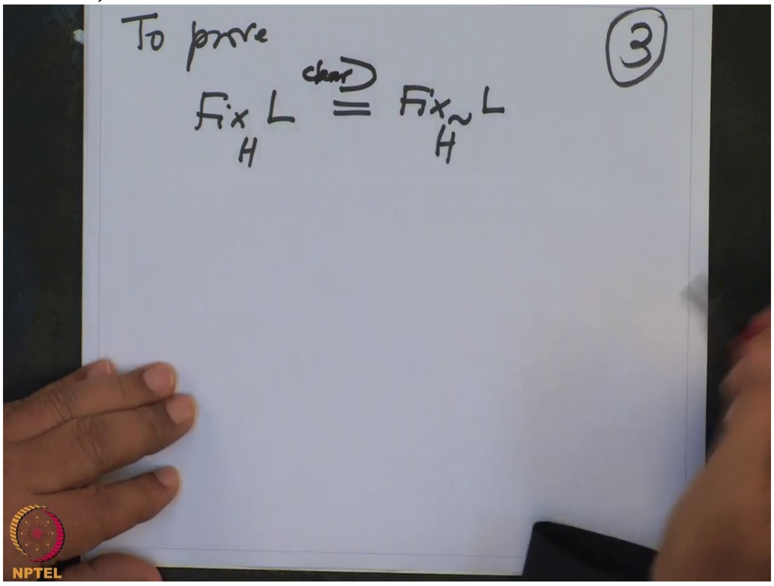
So to prove, to prove $Fix_H L$ is same thing as $Fix_{\tilde{H}} L$, this is what I want to prove.

(Refer Slide Time 06:42)



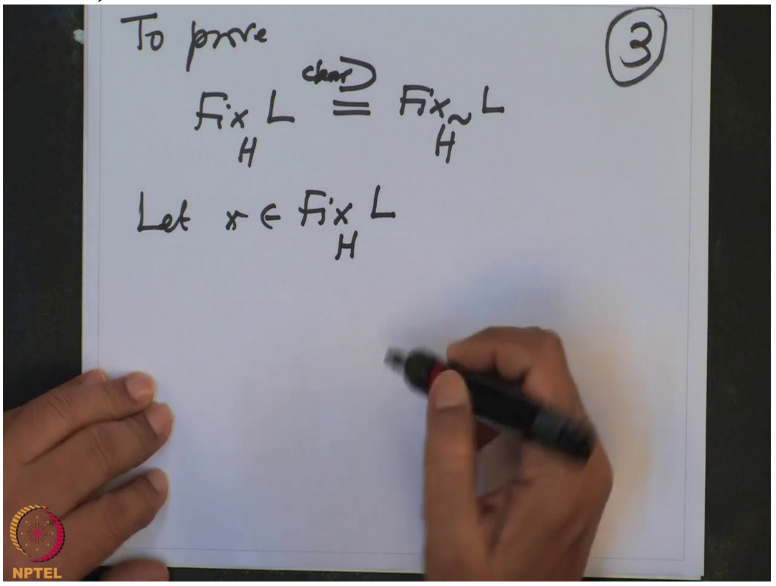
But what do we know? We know that H is always contained in $H^{'}$. Therefore this inclusion, H is smaller subgroup. Therefore fix field is bigger. Therefore this is clear, this inclusion is clear.

(Refer Slide Time 06:56)



To prove the other inclusion I will take an element here and prove it is here. So let x be fix point of

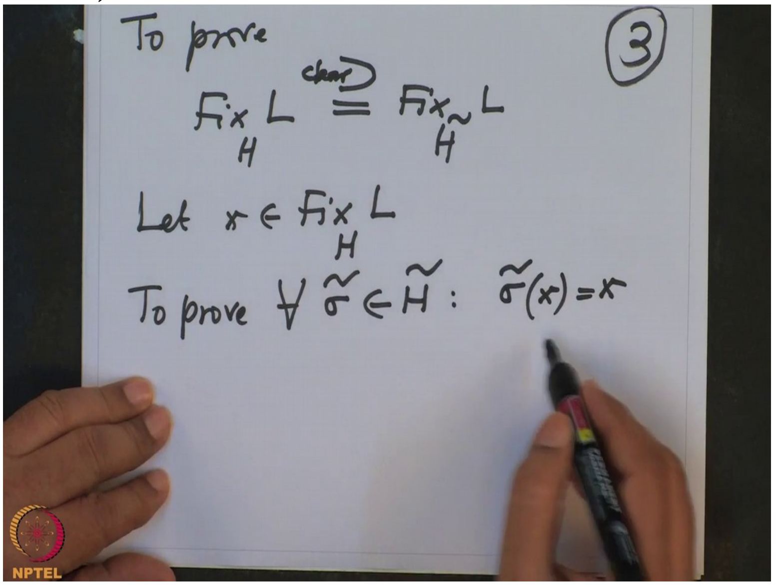
(Refer Slide Time 07:10)



L under H, then I want to prove that, so I want to prove that it is here. That means I want to prove that for any $\tilde{\sigma}$, so to prove, for every $\tilde{\sigma}$, $\tilde{\sigma}$ in $\tilde{H}$, to prove for every $\tilde{\sigma}$ in $\tilde{H}$ I want to prove what? I want to prove that $\tilde{\sigma}$ of x equal to x.

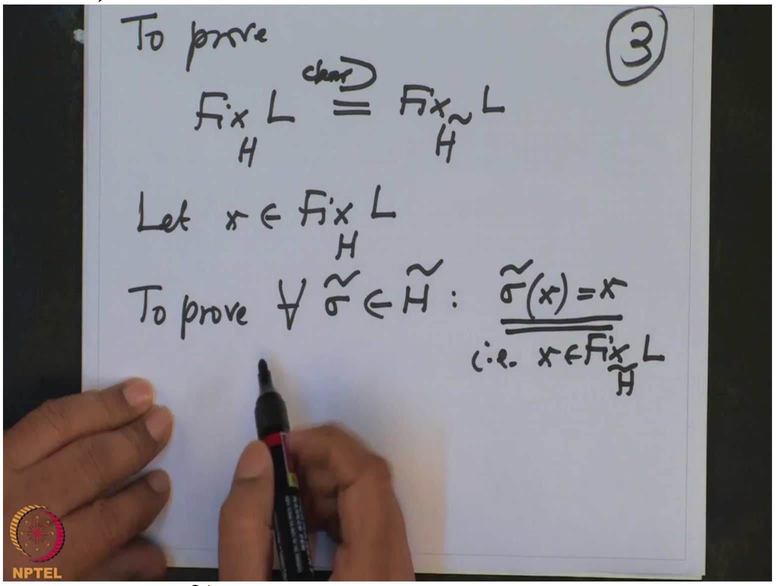
Then it will be here.

(Refer Slide Time 07:46)



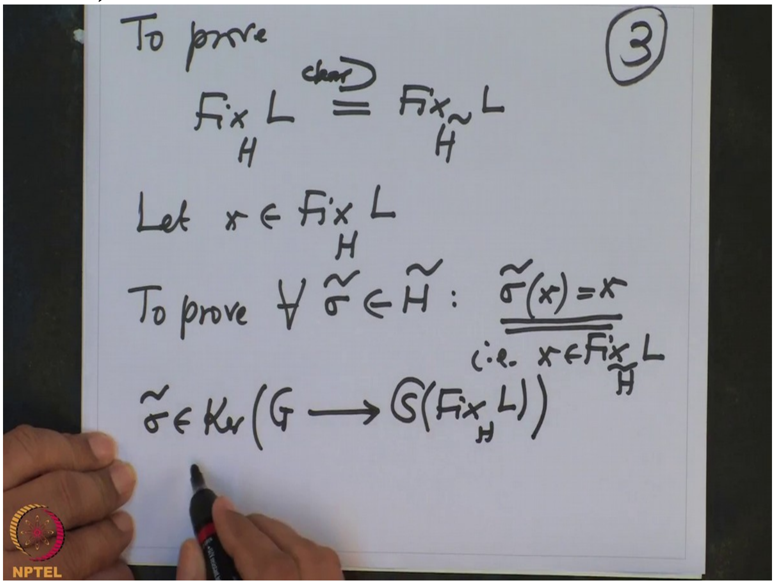
So that is, then, that is x will belong to $Fix_{\tilde{H}} L$. This is what I want to prove. But

(Refer Slide Time 07:58)



I have given that $\widetilde{\sigma}$ is in $\widetilde{H}$. What does that mean? That means this $\widetilde{\sigma}$ belongs to the kernel of the map of G to the permutation group on $Fix_H L$. This was,

(Refer Slide Time 08:15)

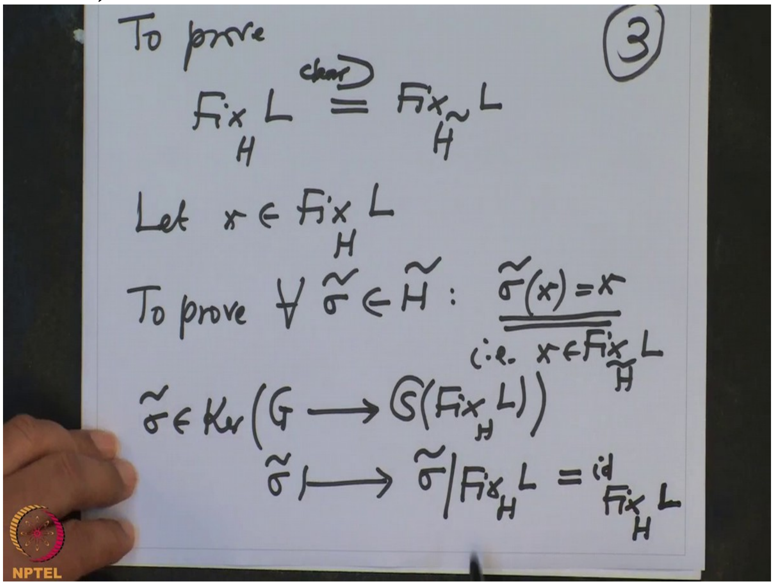


$\widetilde{H}$ was a kernel of this.

So and what does the kernel means? That means $\widetilde{\sigma}$ should go to, $\widetilde{\sigma}$ here, identity but this is $\widetilde{\sigma}$ is going to $\widetilde{\sigma}$ restricted to fixed points of H in L, this is identity on fix points of L with respect to H.

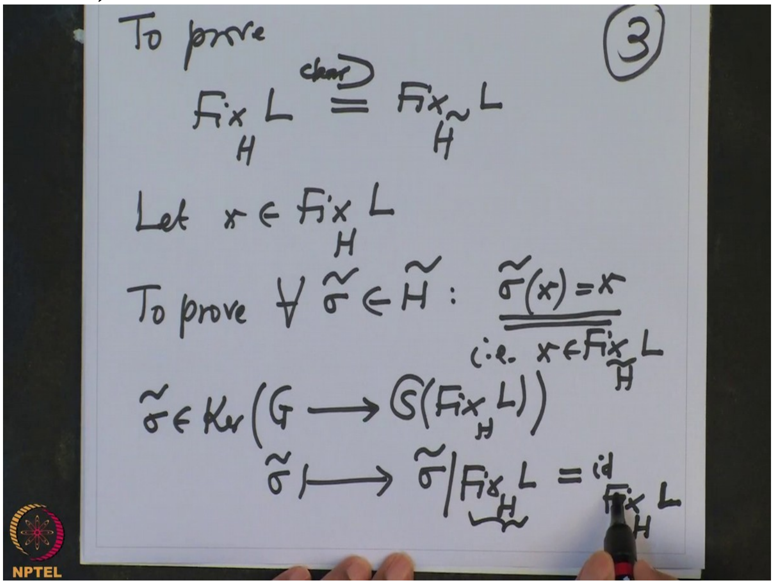
So

(Refer Slide Time 08:41)



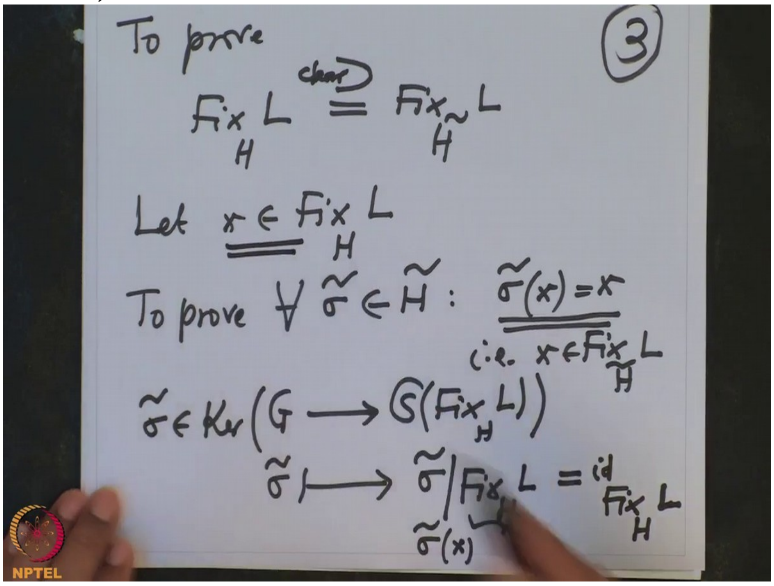
that means on every element of this, it behaves like identity

(Refer Slide Time 08:46)



but that simply means that $\tilde{\sigma}$ if I evaluate on an any element here and in particular this x is there,

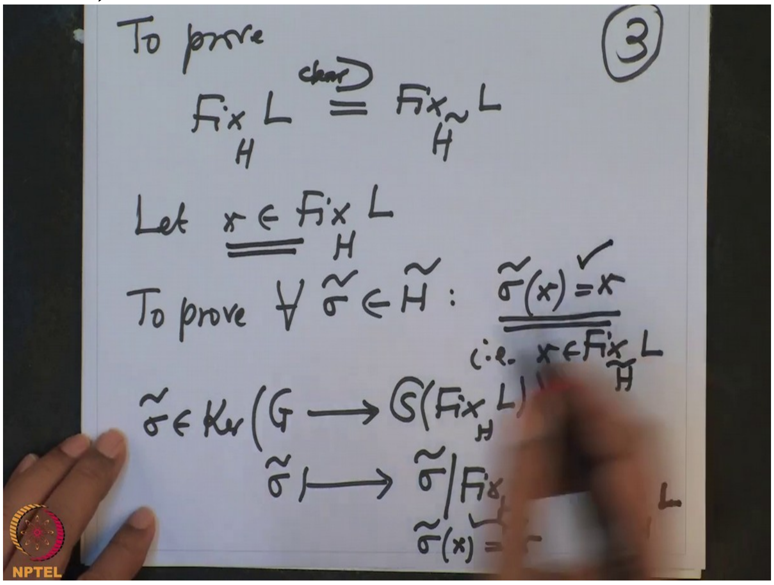
(Refer Slide Time 08:54)



therefore this is x.

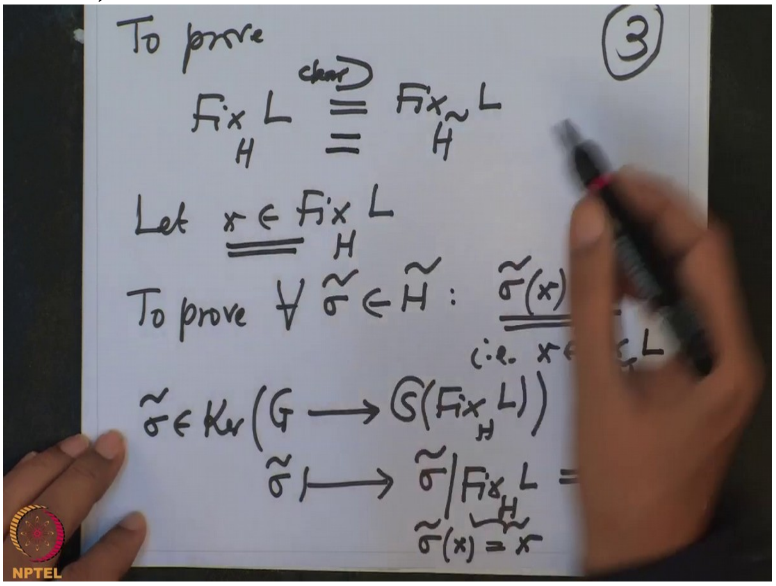
So that proves this equality

(Refer Slide Time 08:58)



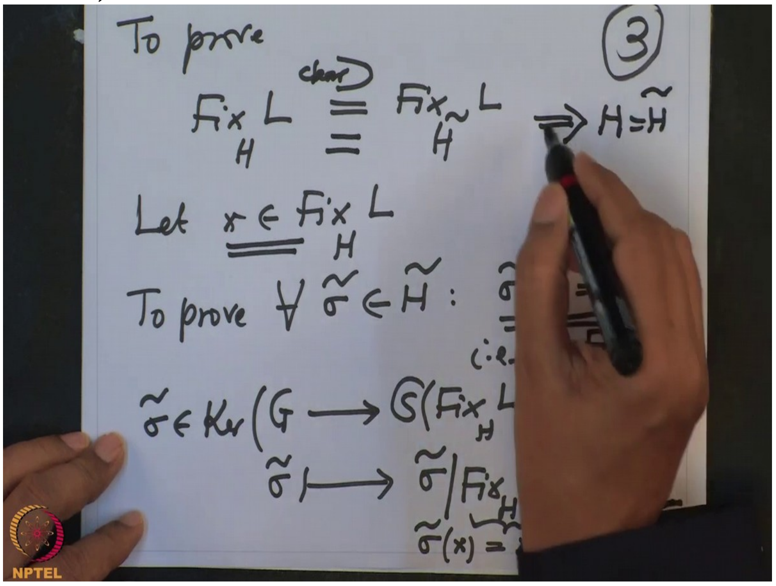
and that proves that this equality of the field extension and

(Refer Slide Time 09:03)



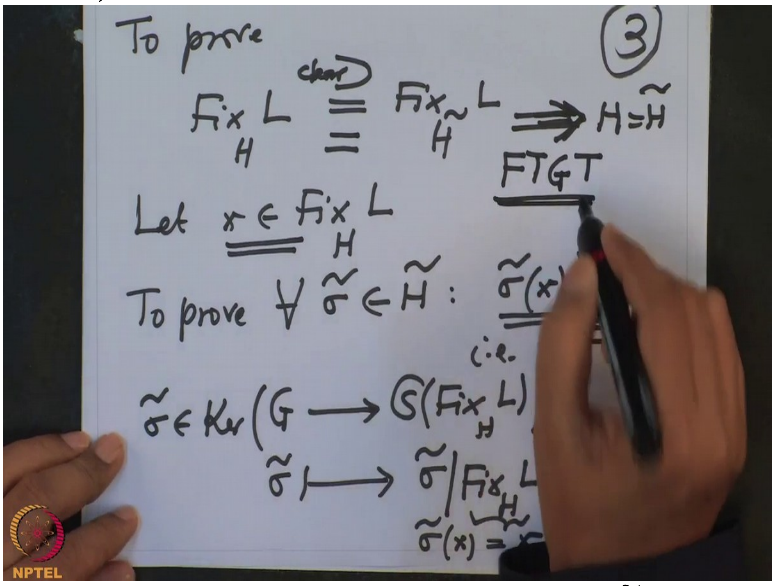
therefore by fundamental theorem of Galois Theory that shows that H equal to $\widetilde{H}$. This is very important.

(Refer Slide Time 09:10)



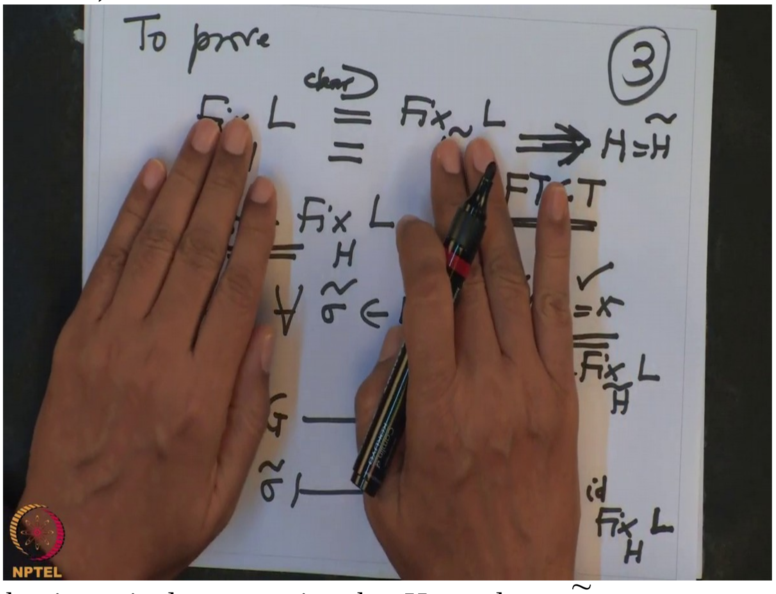
This is where we are using F T G T.

(Refer Slide Time 09:17)



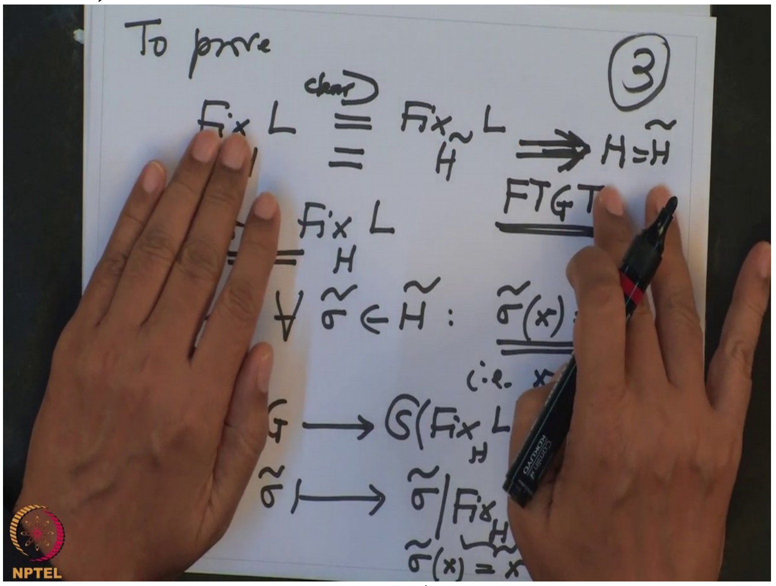
So what we proved is their fix point with respect to H and $\widetilde{H}$ are same. Therefore by fundamental theorem of Galois Theory, H equal to $\widetilde{H}$. And we have observed that this fact, two fixed

(Refer Slide Time 09:32)



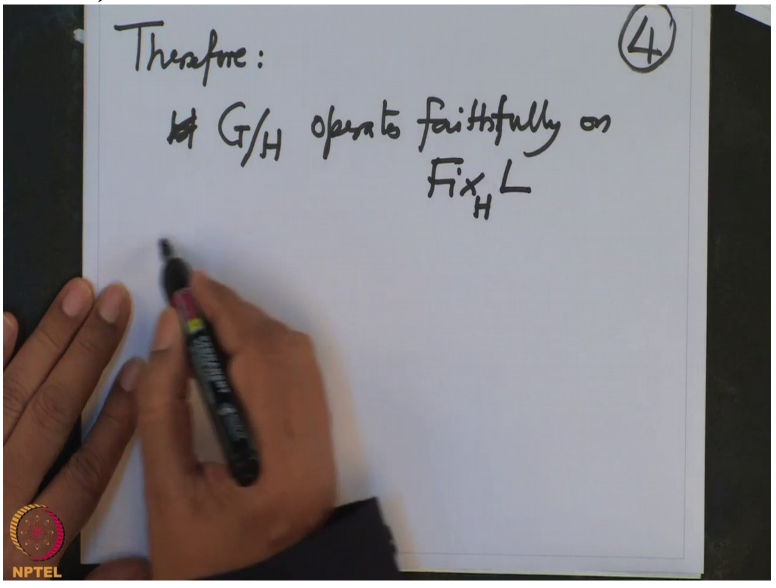
fields are equal, that is equivalent to saying that H equal to $\widetilde{H}$

(Refer Slide Time 09:38)



and H equal to $\widetilde{H}$ is equivalent to saying G/H operate faithfully on the fixed point set. So therefore what we proved is, therefore H, not H, G/H operates faithfully on this $Fix_H L$.

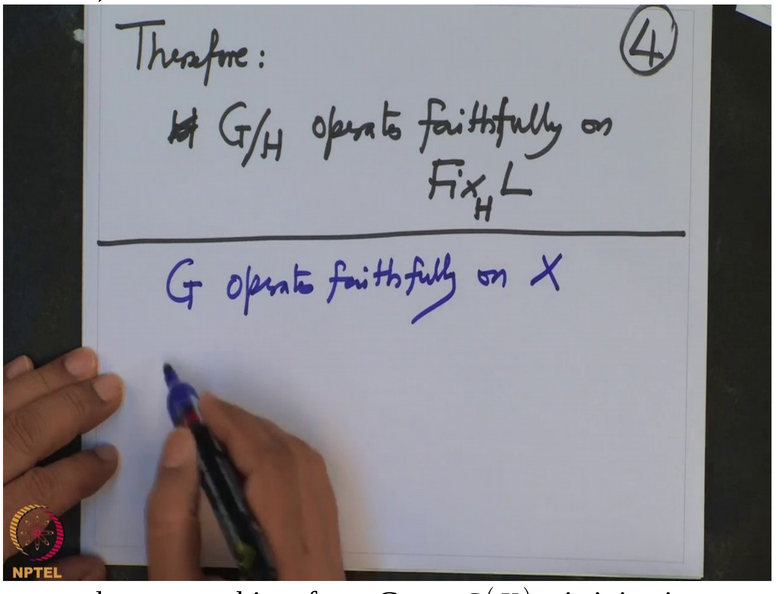
(Refer Slide Time 10:17)



Now let us recall what does this faithful action means. I, remember I want to conclude that this field is Galois over K. This is what I want to conclude. So coming back to understand what does the group operation faithful means?

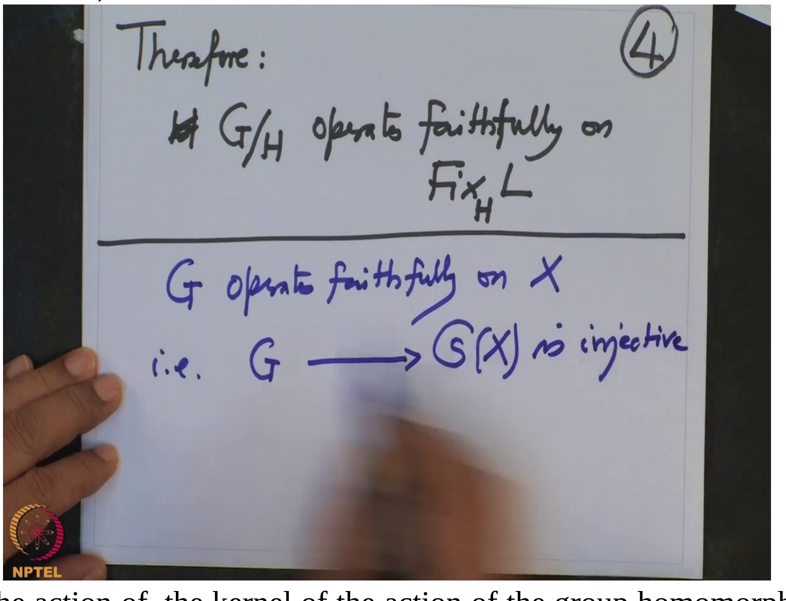
So let us take in general, G is a group and suppose this operates faithfully on a set X. That means

(Refer Slide Time 10:50)



by definition, the group homomorphism from G to $S(X)$ is injective.

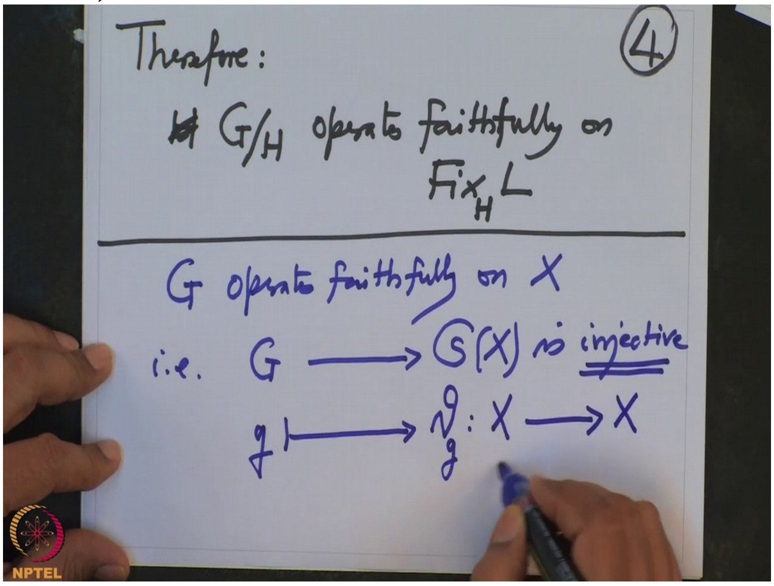
(Refer Slide Time 11:02)



Faithful means the action of, the kernel of the action of the group homomorphism is a trivial. So that means the group homomorphism is injective. So this is injective.

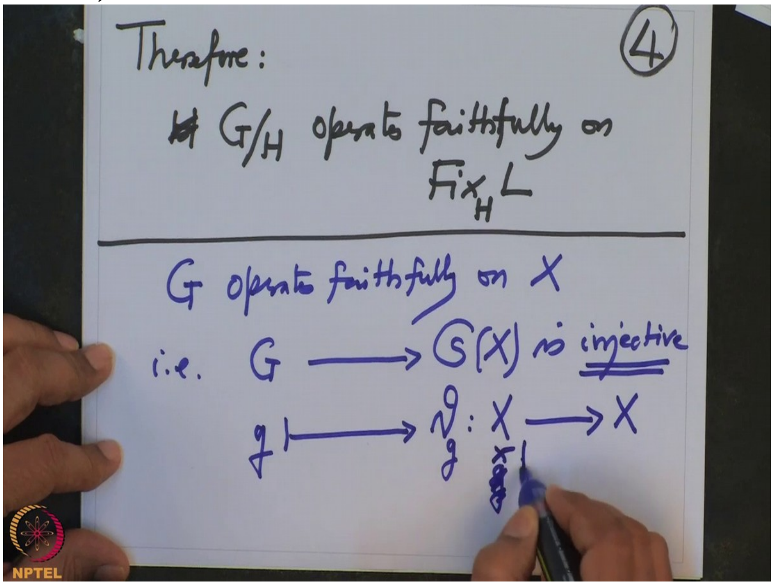
So therefore if I take any element g in G, where does it go? It goes to theta G, theta G is the multiplication on that set X.

(Refer Slide Time 11:23)



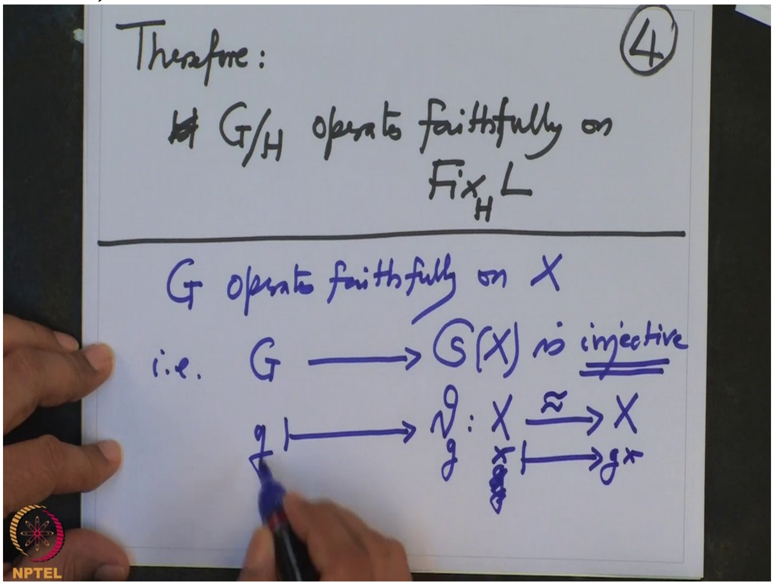
This is g going to, x going to

(Refer Slide Time 11:26)



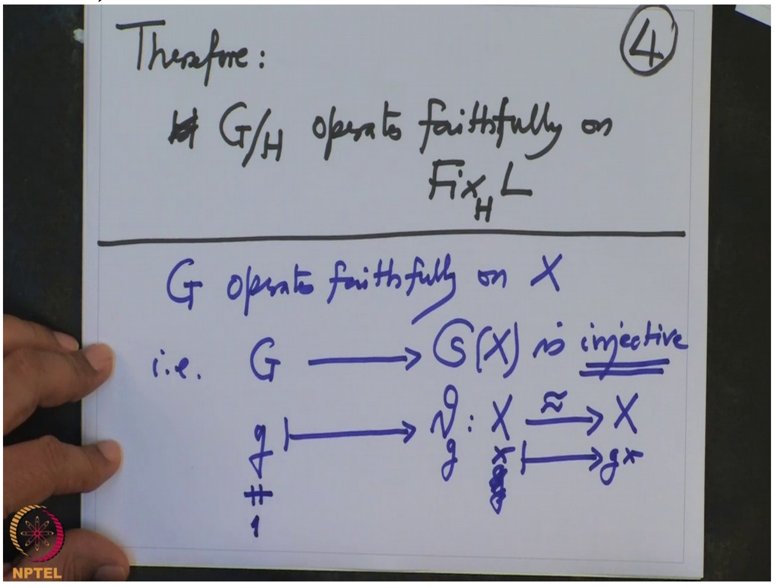
g x. this is the bijective map we know, and

(Refer Slide Time 11:31)



this G, so when g is not identity in the group, so I will denote identity by 1 without

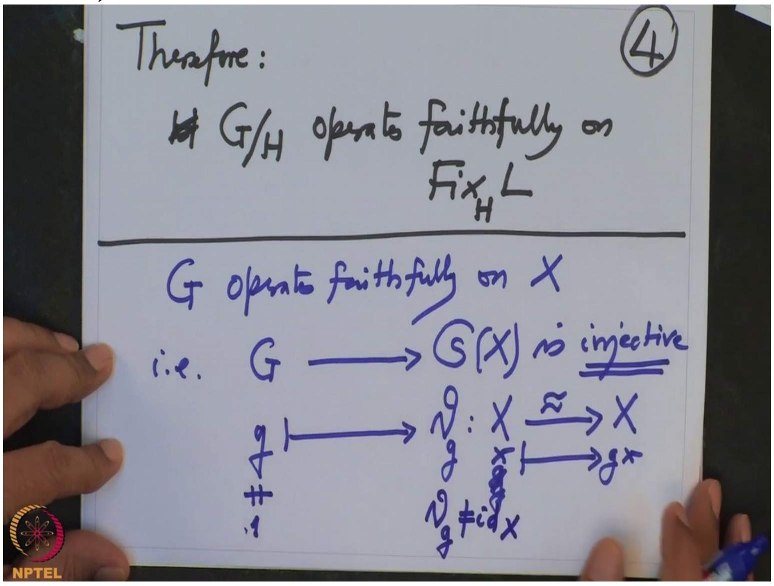
(Refer Slide Time 11:37)



much fuss, so this g if it is not identity then this is definitely not identity.

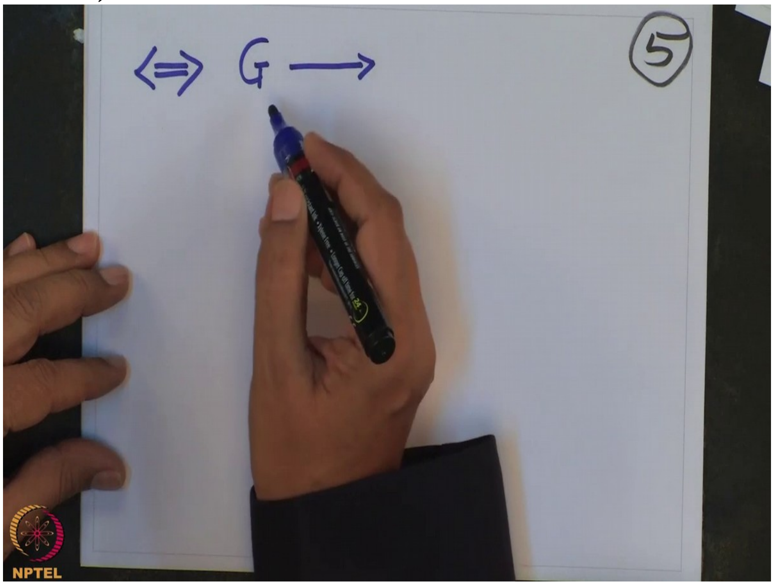
Because no non-identity elements will go to identity element because the kernel is trivial, so if g is not this then this theta g cannot be identity map of X.

(Refer Slide Time 11:59)



So, but then what is theta g? So that means equivalently this map from x to x is inject, the, the not-identity that means if I take this map from G to G, G to $S(X)$. So that means

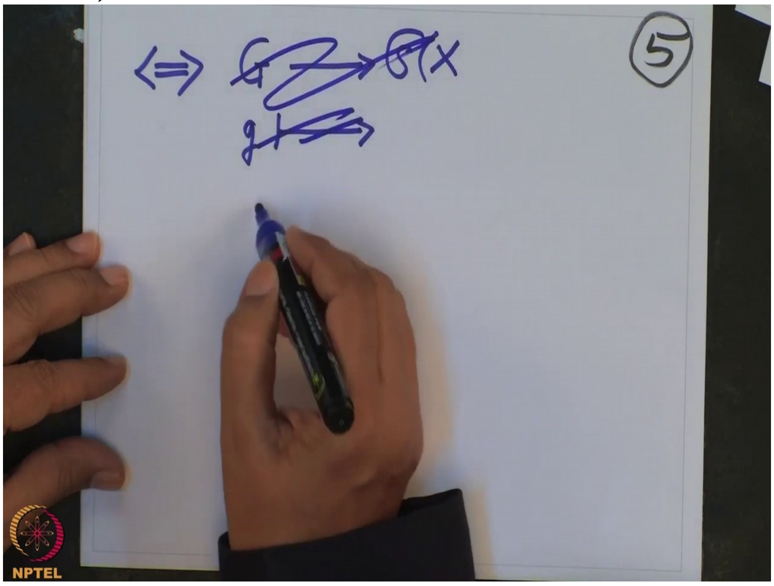
(Refer Slide Time 12:28)



g going to $S(X)$. So that means what?

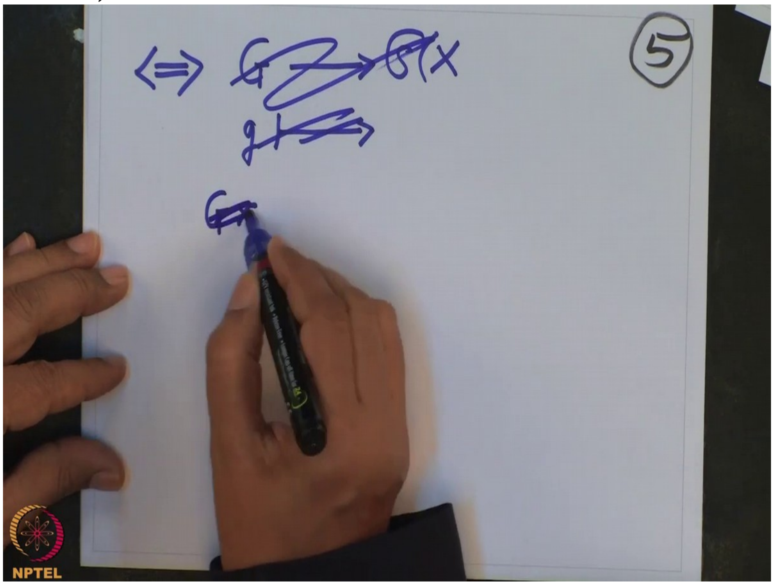
I want to write in terms of the orbit. That means

(Refer Slide Time 12:39)



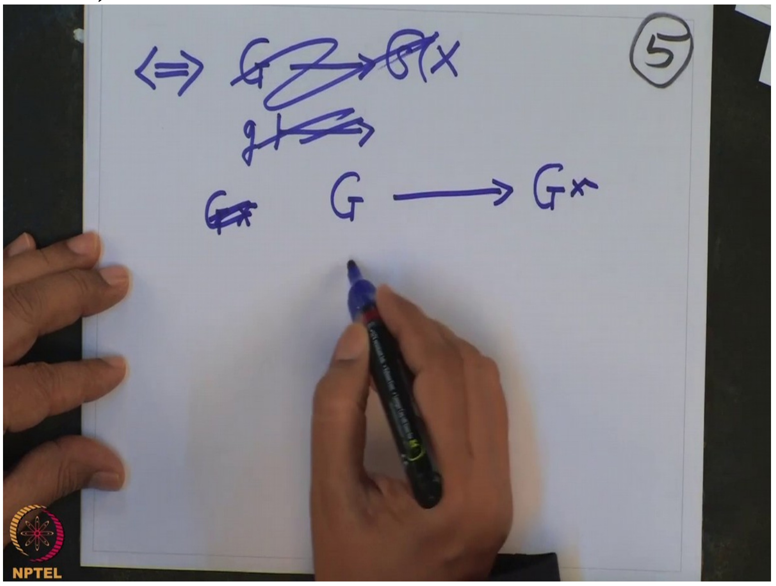
if I take any x and orbit of x, we have a natural map

(Refer Slide Time 12:45)



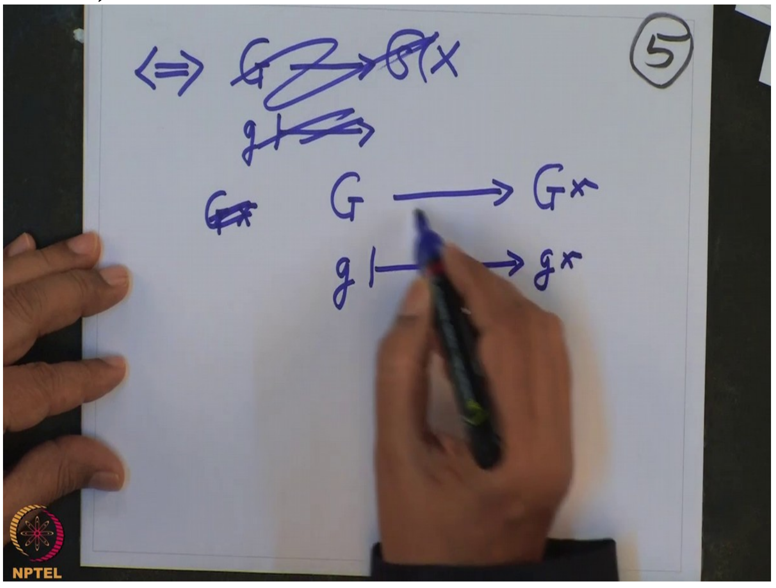
from G to orbit of x,

(Refer Slide Time 12:50)



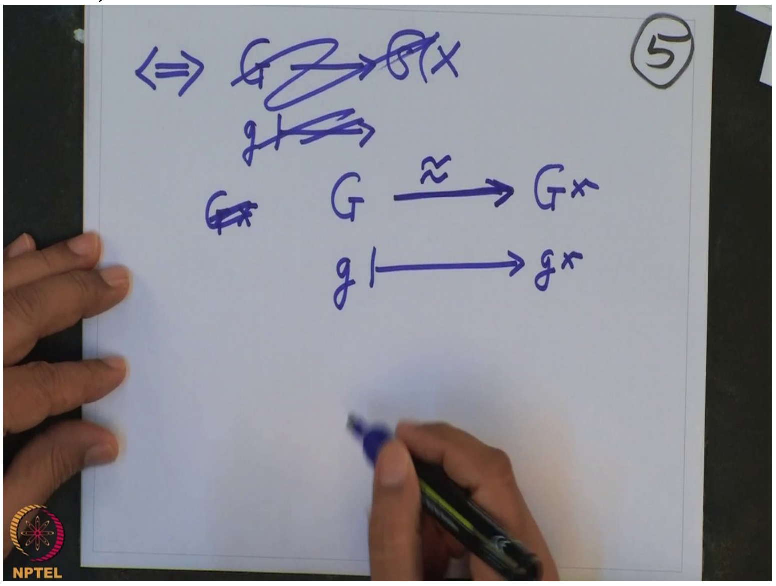
namely any g going to g x, this map

(Refer Slide Time 12:54)



is a bijection

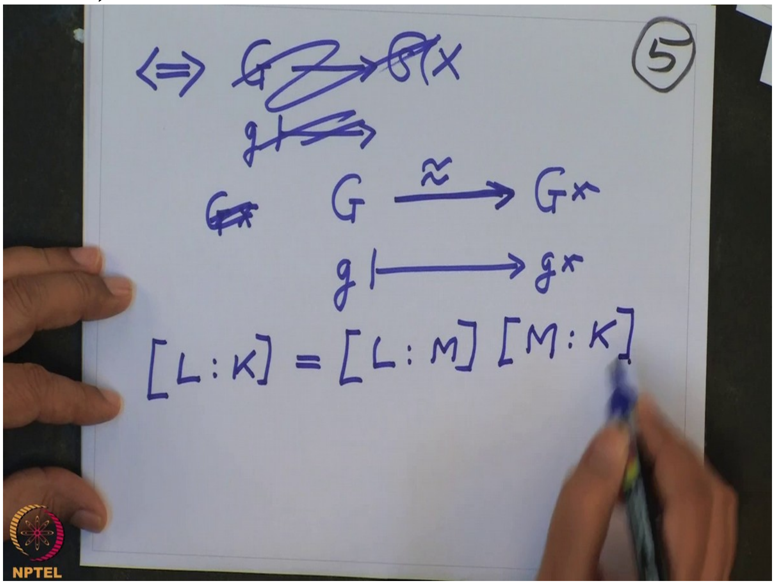
(Refer Slide Time 12:58)



because 2 different gs cannot map to the same. So that means the orbit is the full orbit.

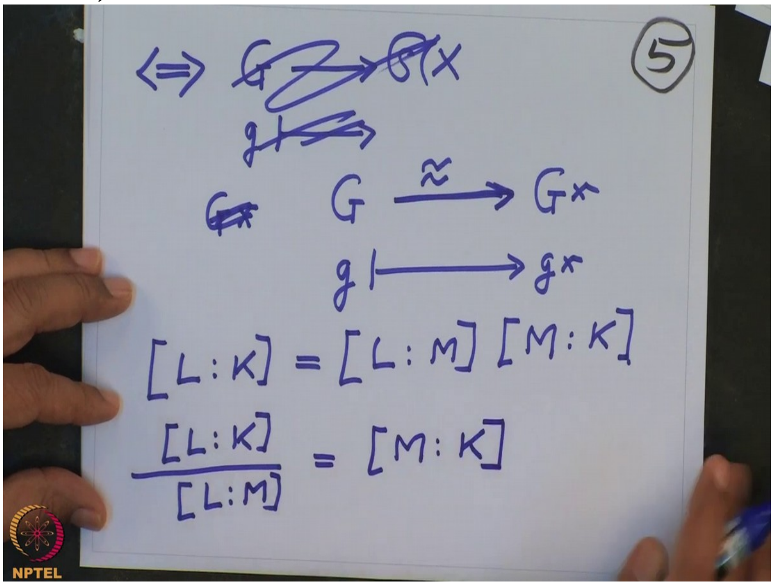
That means that, that the action faithful means, Ok, so that means that the cardinality, so I want to check that this is now equivalent to checking that what happens to the fix point. So that means we know L over K, this degree we know. This is degree of L over M, this is degree of M over K.

(Refer Slide Time 13:39)



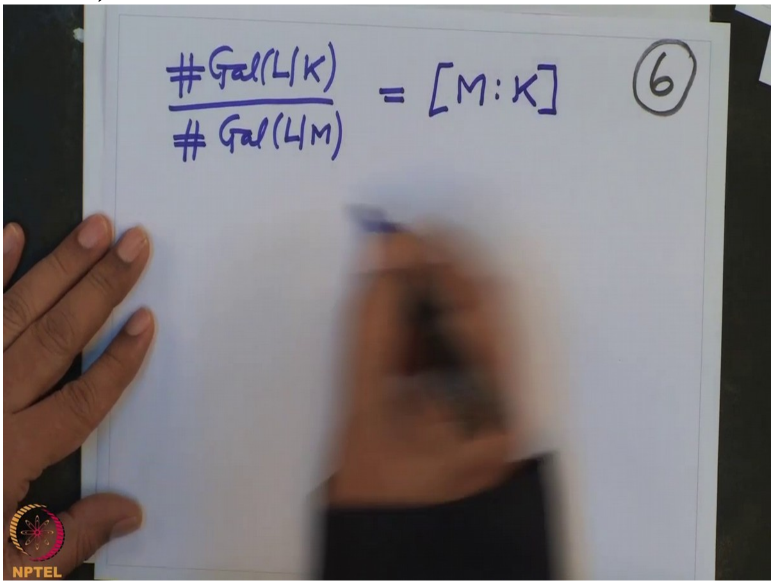
But this M over K, I want to shift this to that side. So that means L over K divided by L over M, this is M over K.

(Refer Slide Time 13:56)



And this means what? Now the other side, this side I know. This means the cardinality of the Galois group of L over K divided by cardinality of Galois group of L over M, this cardinality is same thing as M over K.

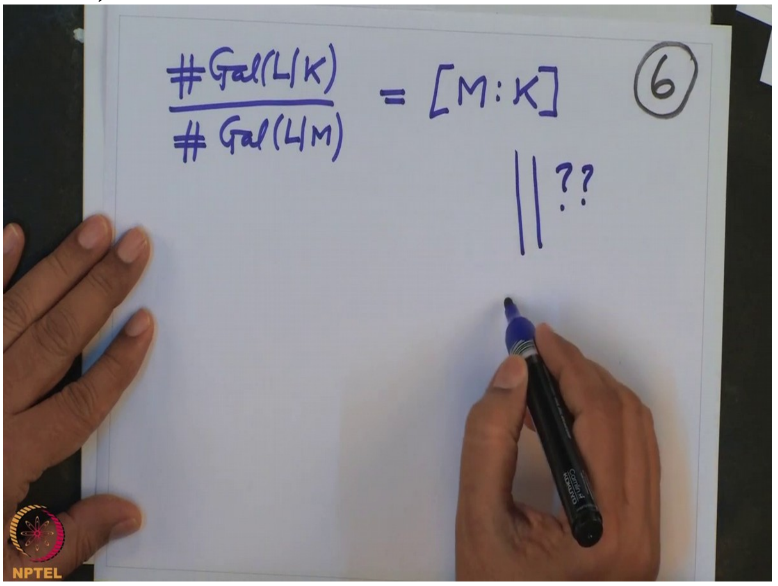
(Refer Slide Time 14:18)



And I want to check what?

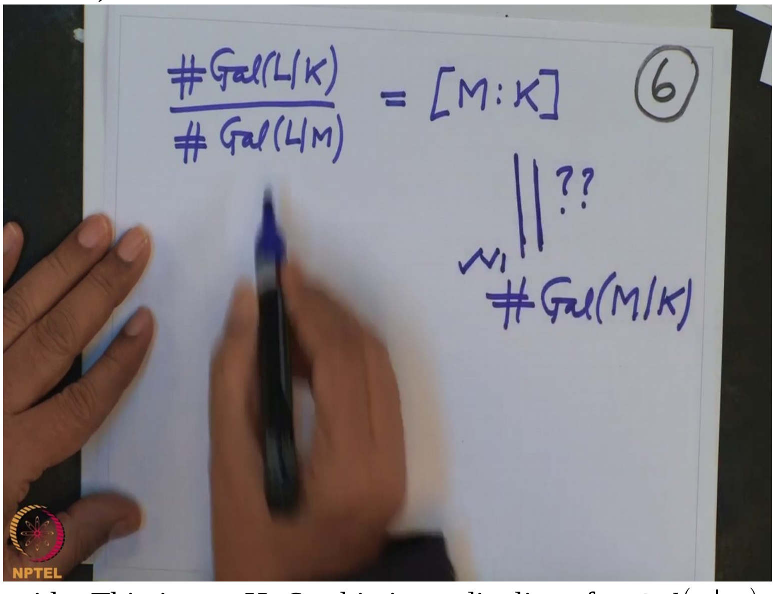
I want to check that this is what we are looking for. This is what we want to check, that

(Refer Slide Time 14:26)



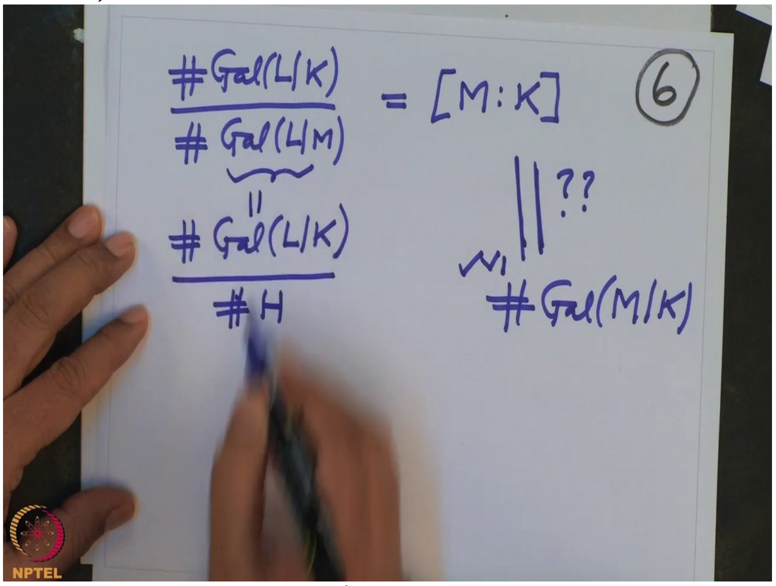
this is the cardinality of Galois group of M over K. Now all that we know is, this less equal to this, we know. But we want to check equality

(Refer Slide Time 14:39)



here. I know this side. This is our H. So this is cardinality of $Gal(L|K)$ and modulo H, cardinality of H. But this is same thing as,

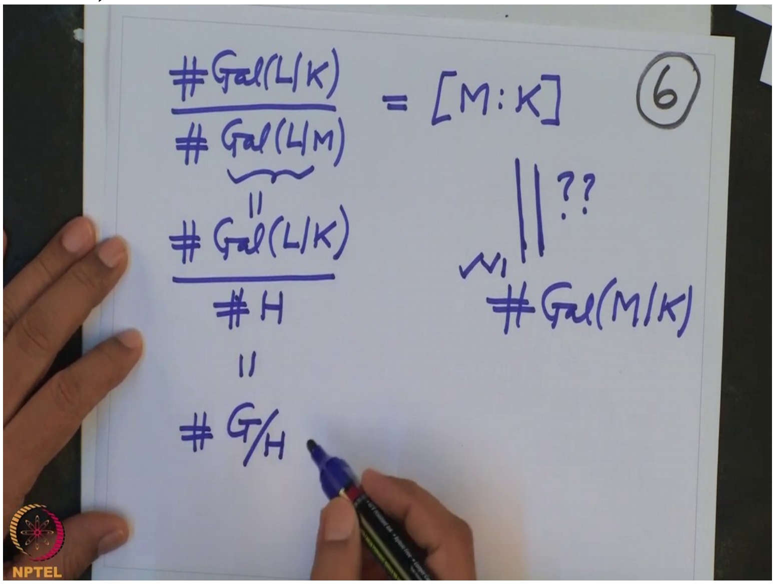
(Refer Slide Time 14:56)



this is same thing as cardinality of the G/H.

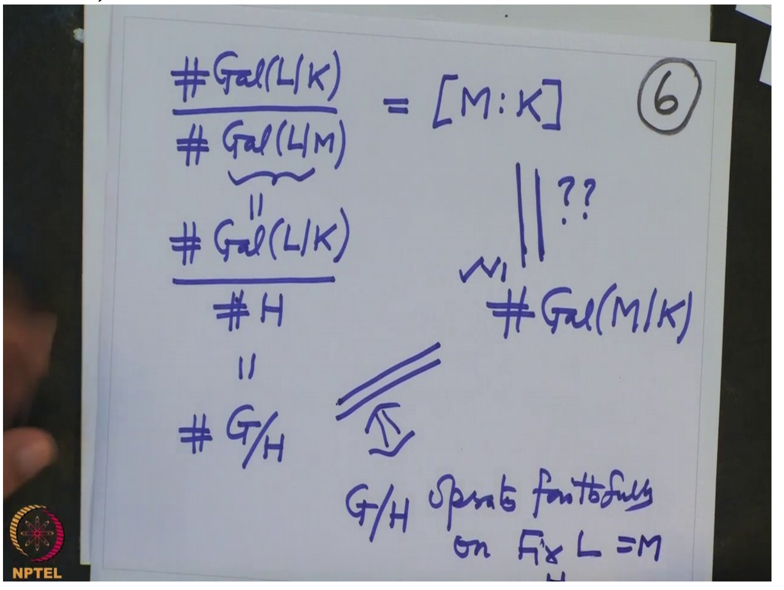
Remember we are

(Refer Slide Time 15:03)



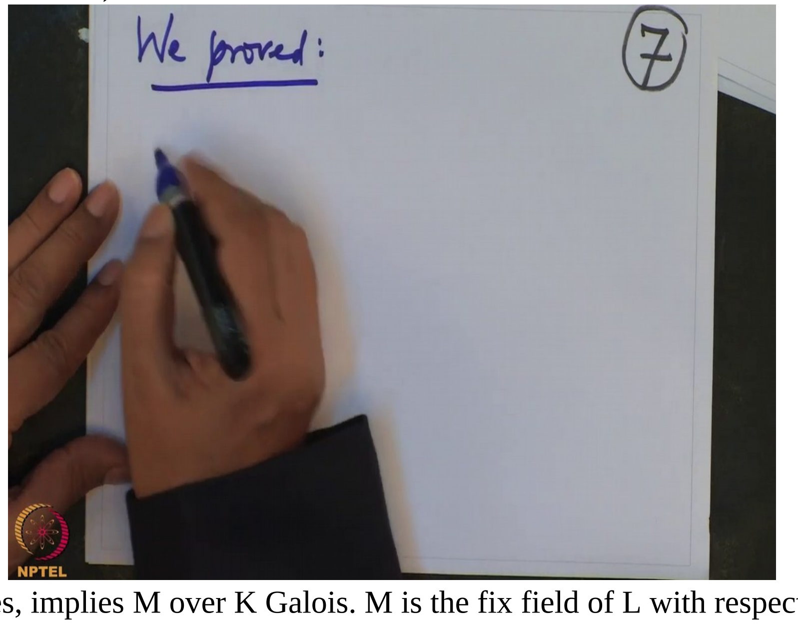
assuming H is normal therefore this is actually a group. And what do we want to check? This cardinality equal to the cardinality of this, this is what we want to check. But we will check that this, this action is faithful is equivalent to saying this equality here, this equality. This is because if and only if G/H operates faithfully on fix H. This is our M in the notation.

(Refer Slide Time 15:42)



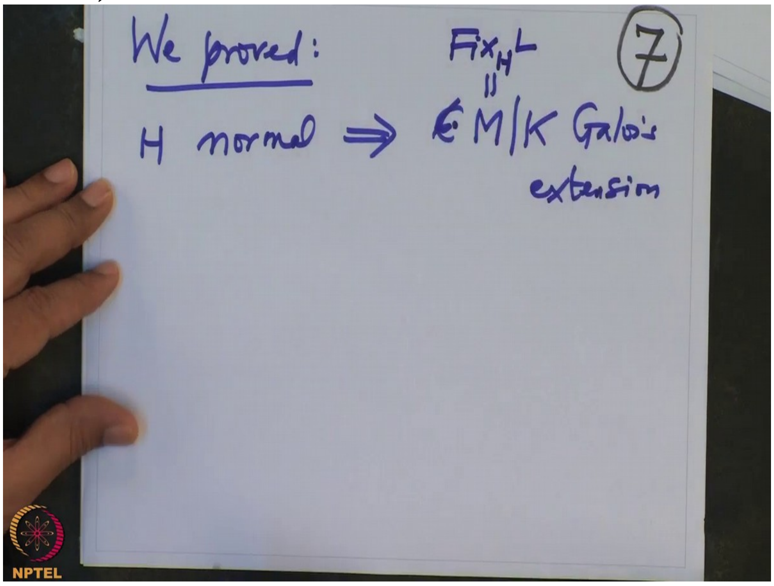
Because it operates faithfully the degree, the dimension will be equal to the cardinality of this group because this is precisely the orbit. So that follows, therefore, therefore we have proved the assertion that, we have proved, I will just recall. We proved

(Refer Slide Time 16:14)



H normal implies, implies M over K Galois. M is the fix field of L with respect to H.

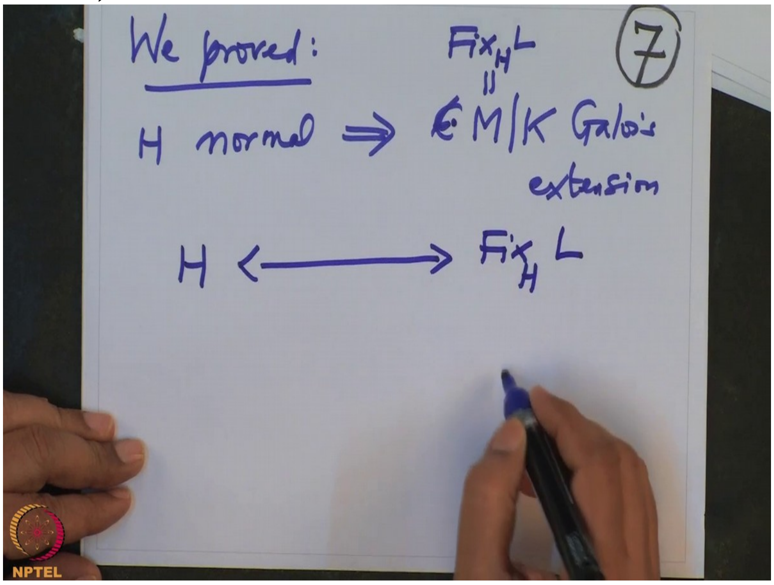
(Refer Slide Time 16:36)



This implication we have proved.

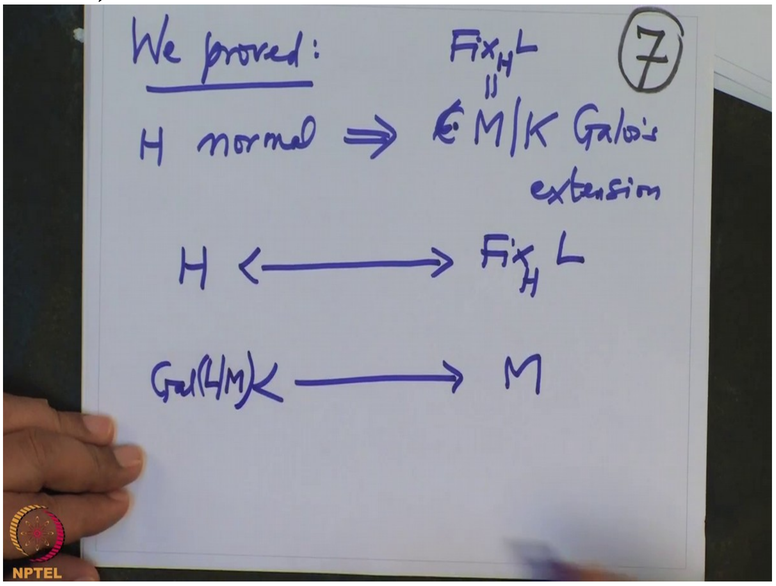
Now we want to prove the other way, namely if M over K is a Galois extension then the corresponding subgroup is normal. This is what we want to prove. And the corresponding subgroup is what? It is, so we are given M over K. So this, what is the correspondence? H corresponds to $Fix_H L$

(Refer Slide Time 17:04)



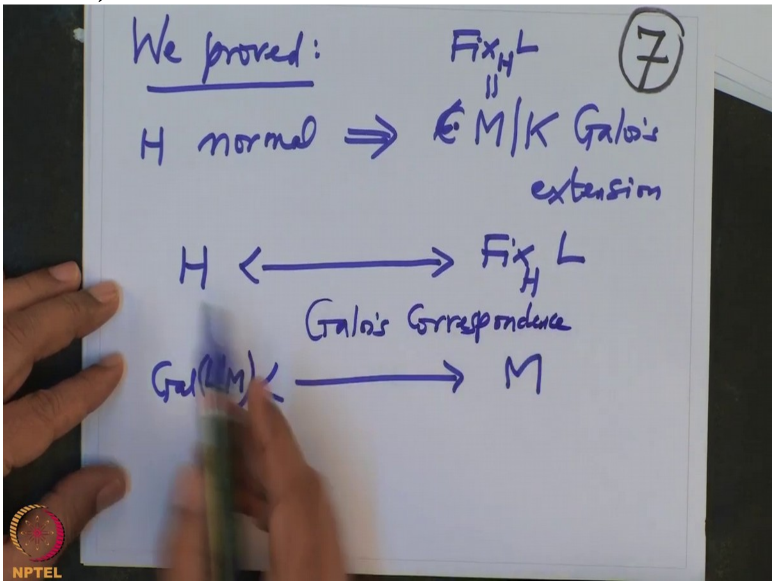
or if I have M here, that corresponds to whom? $Gal(L|M)$.

(Refer Slide Time 17:13)



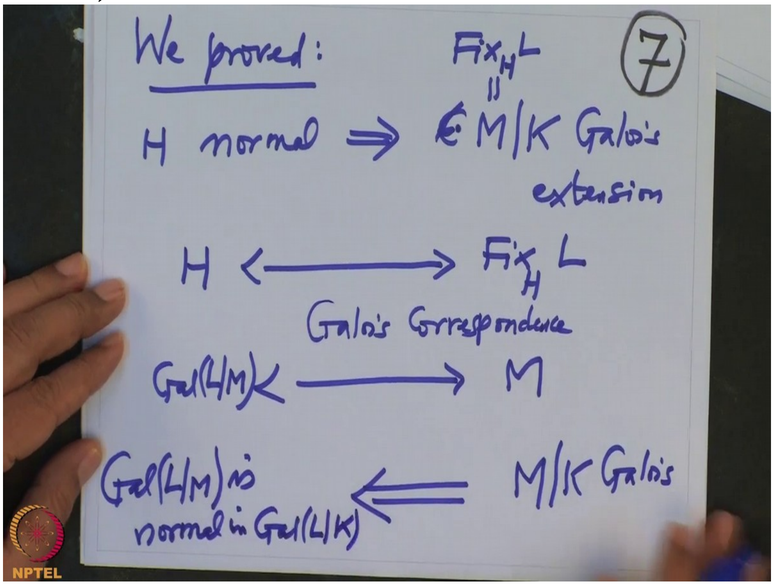
They correspond to each other. So this is the correspondence. This is under the Galois correspondence. This is precisely the Galois correspondence.

(Refer Slide Time 17:29)



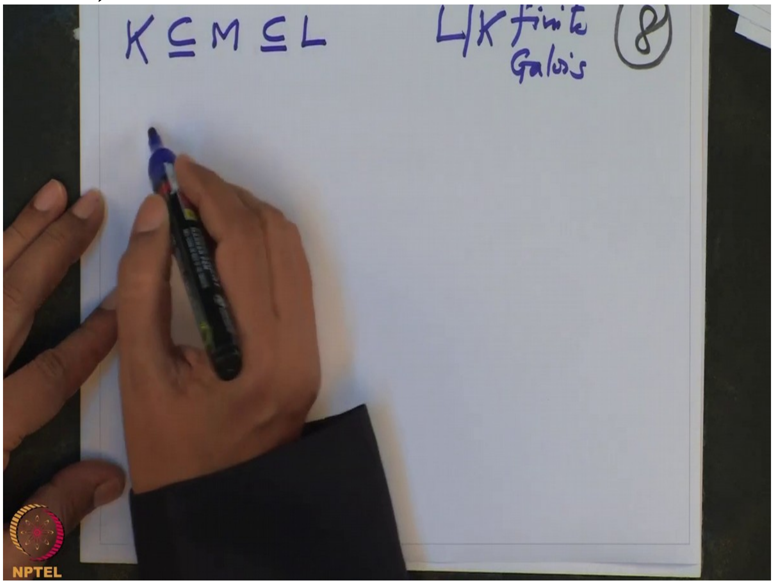
So we have proved that if H is normal, this fix field is Galois over K. Conversely I want to prove that if this subfield, intermediary field M is Galois over K, so I want to prove M over K Galois then I should prove that this subgroup $Gal(L|M)$ is normal in the Galois group L over K. This is what I want to prove.

(Refer Slide Time 18:02)



Alright, so we will prove that. So now we will, we have given, so let us recall what we want to prove. So we have given L over K finite field extension, finite Galois. And we have given a intermediary field

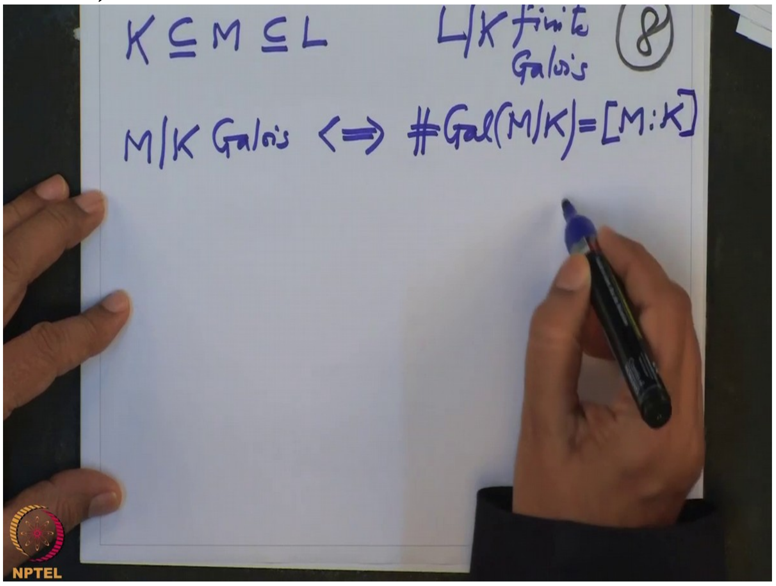
(Refer Slide Time 18:29)



and we have also given that M over K is Galois, that is given.

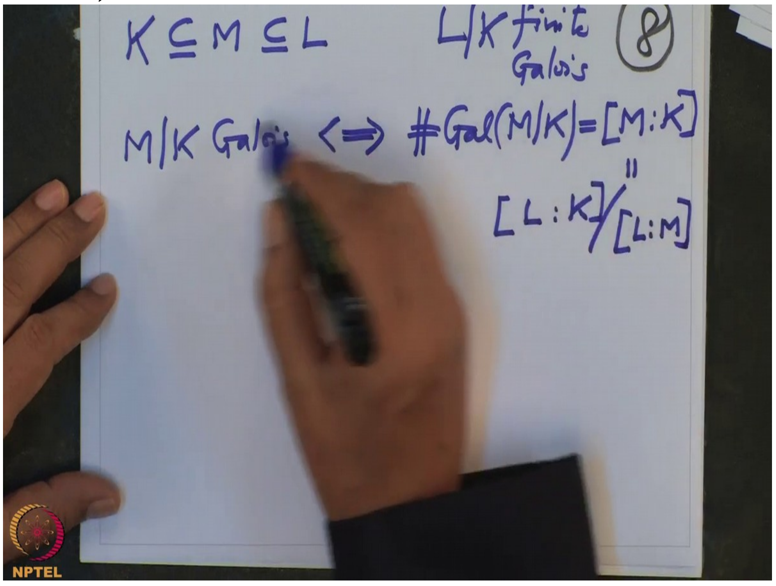
That is equivalent to saying the cardinality of the Galois group $Gal(M|K)$ this is equal to degree M over K. And degree M over K

(Refer Slide Time 18:50)



is same thing as degree L over K divided by degree L over M, this is what we have given. This equality we have given,

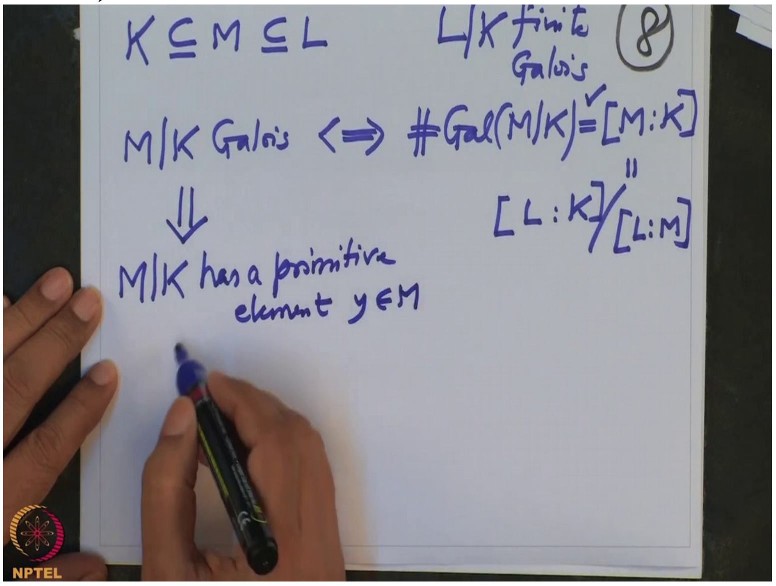
(Refer Slide Time 19:02)



this is given therefore we have given this. What more things we have given? We have given this is Galois. L over K is Galois. So this means it has a primitive element. We have proved that we have a Galois extension.

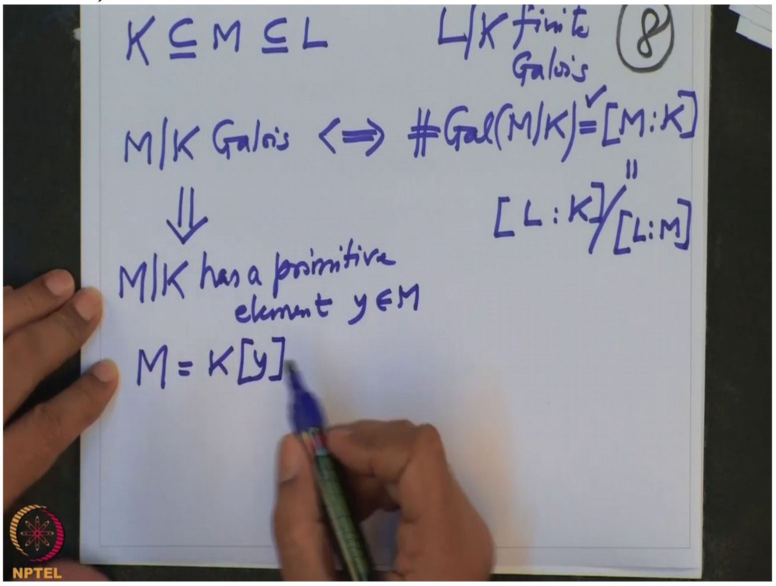
Then M over K has a primitive element, has a primitive element. Let us say $y \in M$. So that means

(Refer Slide Time 19:30)



we have given that M equal to K y, the smallest subfield

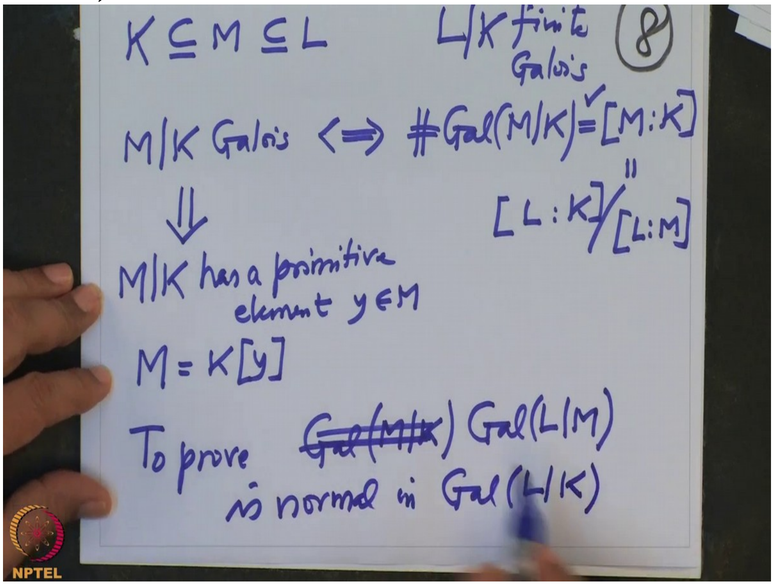
(Refer Slide Time 19:36)



or the smallest K-algebra which contain y. So we have given this equality. That is all we have given.

And what do we want to prove? To prove, we want to prove that the corresponding field extension, this group is normal in $Gal(L|K)$. This is what we want to prove because

(Refer Slide Time 20:05)

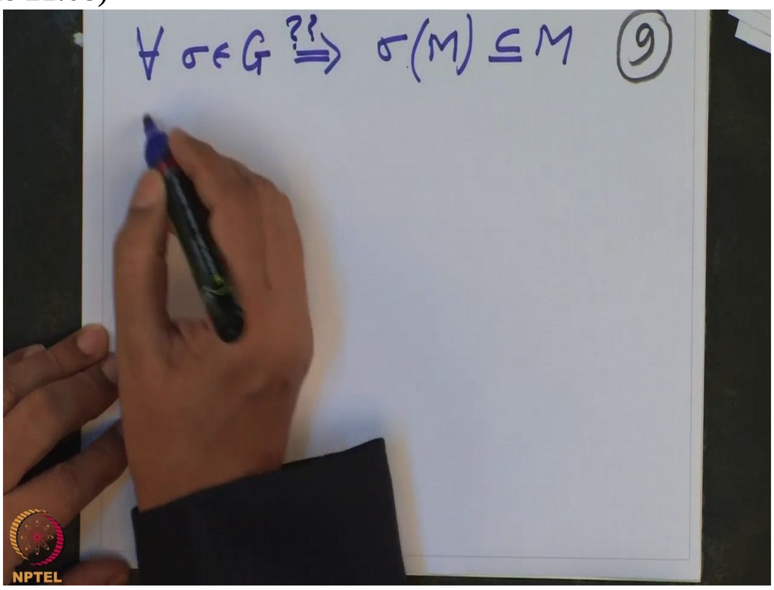


this M corresponds to this subgroup. This is what we want to prove.

So once you understand what needs to be proved, things are easy. So we want to prove this subgroup is normal here, alright. So that means what? Alright, Ok so that means that I want to check that what do we want to prove? That is Ok. First of all, note that that, first of all note the following.

That, for every σ in G I want to check that, that implies σ keeps M invariant. This is what I want to check. This I want to check from the assumption that M over K is Galois. Ok, so to check this it is enough to check, so this is what I am checking;

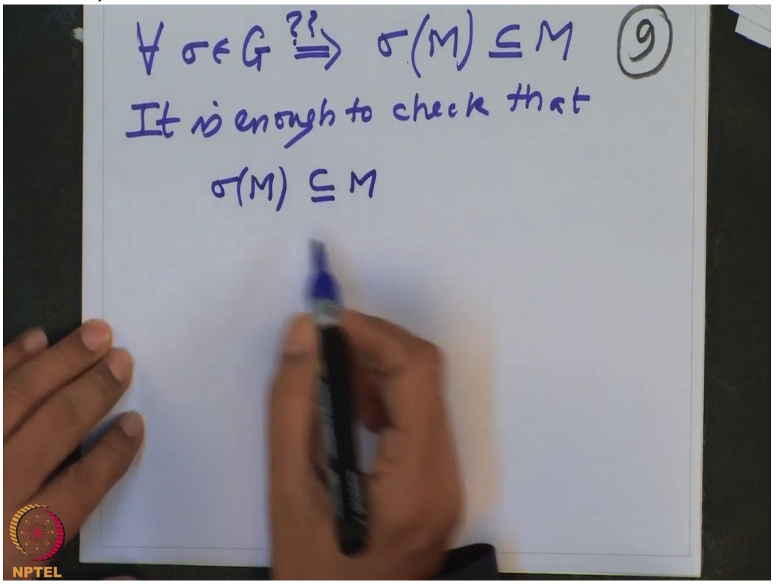
(Refer Slide Time 21:08)



it is enough to check that σ of M is contained in M.

Because once I check σ M is contained in M

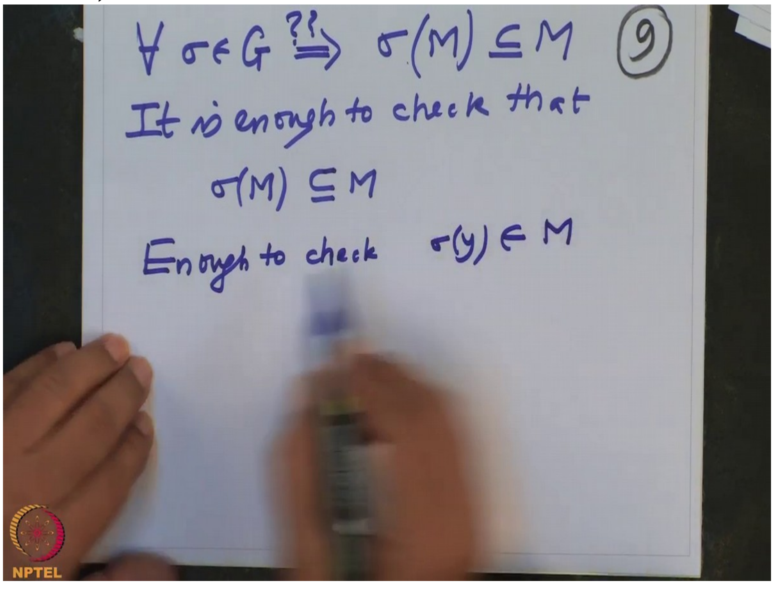
(Refer Slide Time 21:27)



then also this is valid for σ^{-1} because we are checking it for every, and then when I apply σ^{-1} then M will be contained in, so it is enough to check this.

Or in other words the degrees of this over K are same. So once you check this that is enough because this is another field whose degree will not change. So it is enough to check this. And to check this, it is enough to check, enough to check σ y is in M.

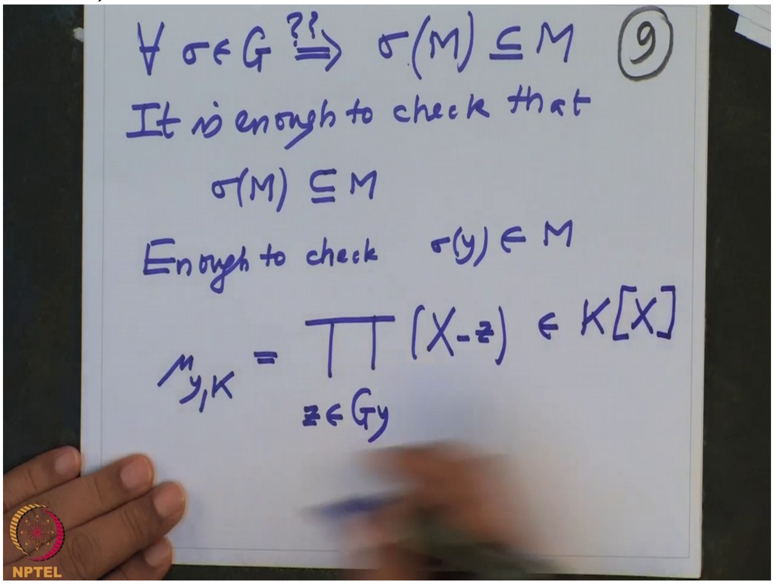
(Refer Slide Time 22:05)



Because $\sigma(y)$ is in M, because y is a primitive element, so will b $\sigma(y)$ e a primitive element of, so it is enough to check that $\sigma(y)$ belongs to M, alright. So this is what I want to check. But remember that we have given the formula for the minimal polynomial of Y. So remember that minimal polynomial of y over K is nothing but a product, product is running over the orbit of y now, G y $X-z$.

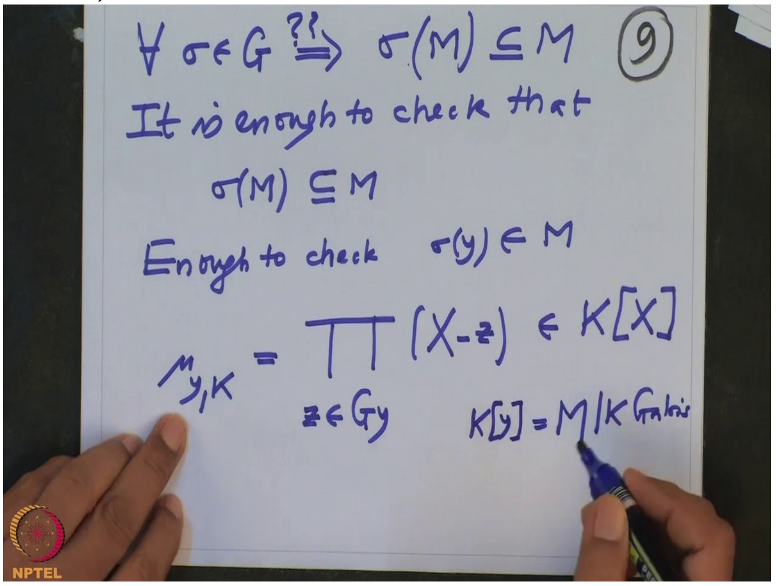
This is the polynomial in $K[X]$

(Refer Slide Time 22:48)



and, and this is the minimal polynomial of the element y over K. And we have given that M over K is Galois. And remember this M is a, this y is a primitive element for this. So when we have analyzed

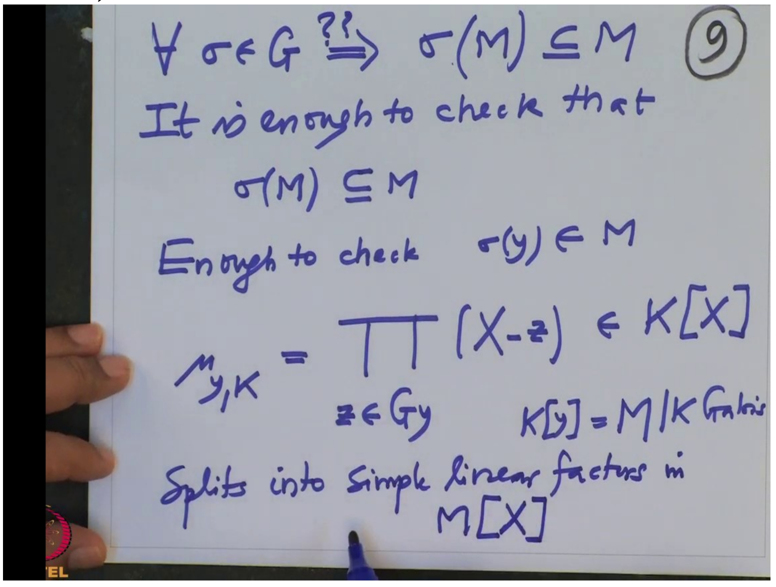
(Refer Slide Time 23:08)



when the simple extension be Galois, we only have to check the minimal polynomial should split into linear factors over K and into simple, simple linear factors over M.

So this polynomial, we know this splits into simple linear factors in M of X. We know that.

(Refer Slide Time 23:47)

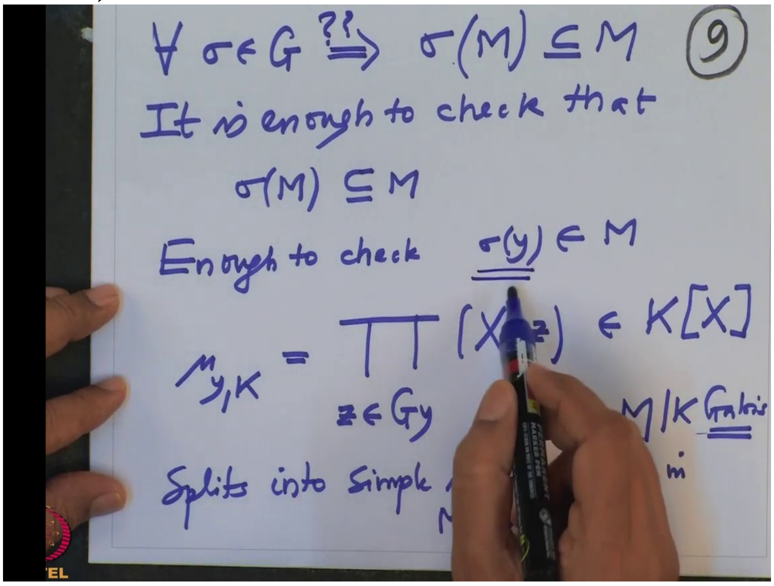


That is because this is Galois; this M over K is Galois.

Therefore this minimal polynomial splits into simple linear factors in this. In particular all elements in the orbit of y, they are there because this polynomial has, this is the product of mu into the linear factors. All these linear factors should lie in M, $M[X]$ and all of them should be different.

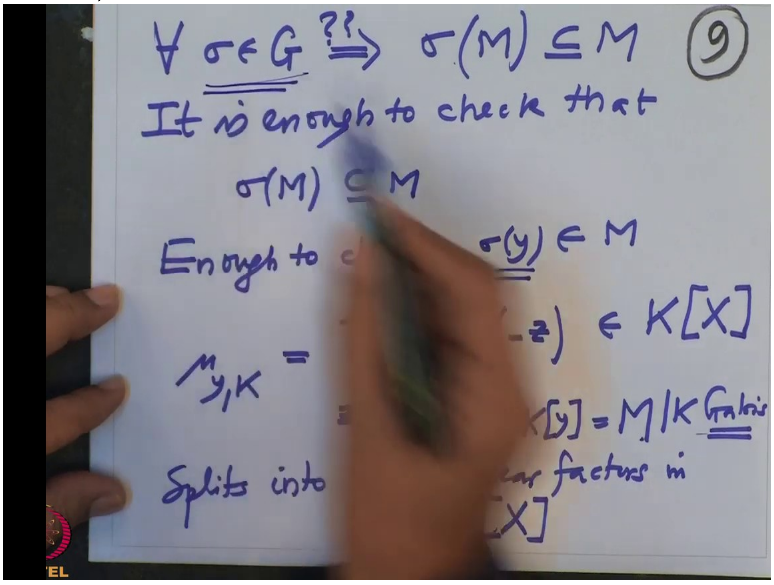
But that will mean that all, all elements in the orbit, they lie in M but $\sigma(y)$

(Refer Slide Time 24:25)



is one of the, so one of the element in the orbit and that is true for every σ because all the orbit elements are here. Therefore for all σ in G,

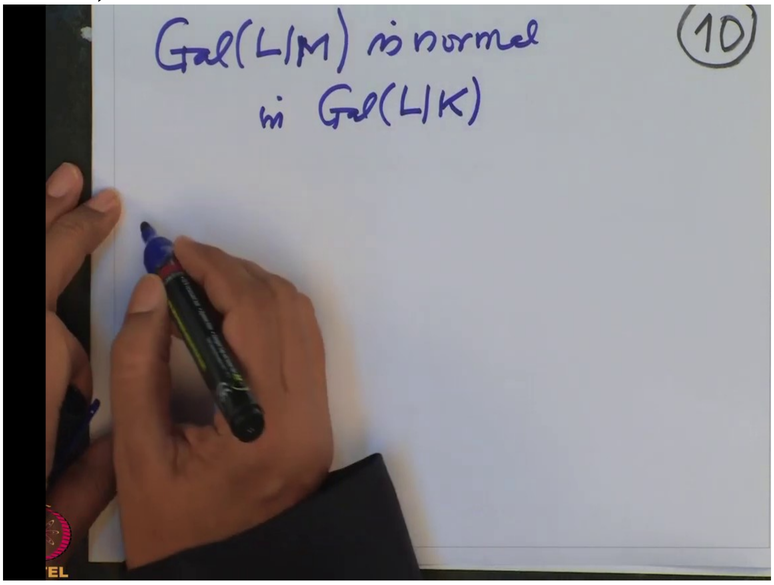
(Refer Slide Time 24:40)



all these elements they lie in M but that we know that is equivalent to saying σ of M is contained in M and that is equivalent to saying that σ of M equal to M actually.

So that shows that, what do we want to show? That means the whole orbit is contained in y but that precisely means the group is normal. Because what is the group then? This is the group, $Gal(L|M)$. I want to show that now this follows that this is normal in this. So how do you prove it is normal in this?

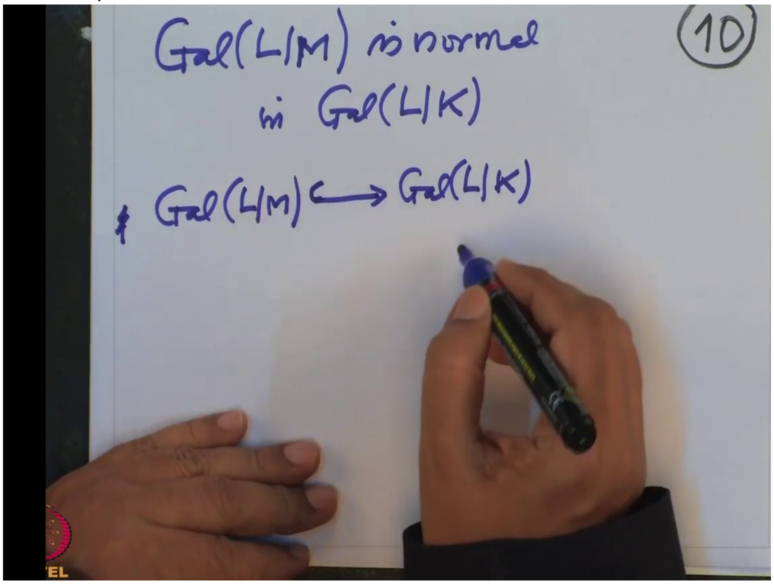
(Refer Slide Time 25:21)



It is very easy.

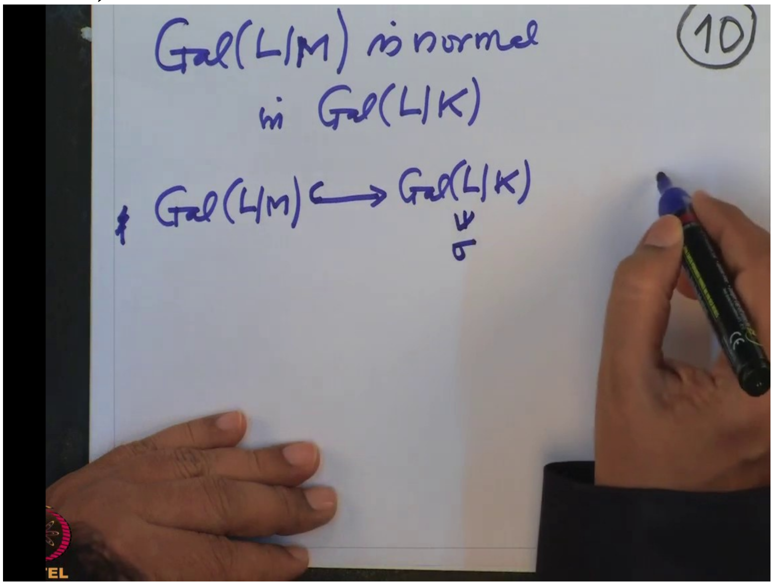
So it is a subgroup and we have an injective map here L M to Galois L over K, and, so this is injective map

(Refer Slide Time 25:37)



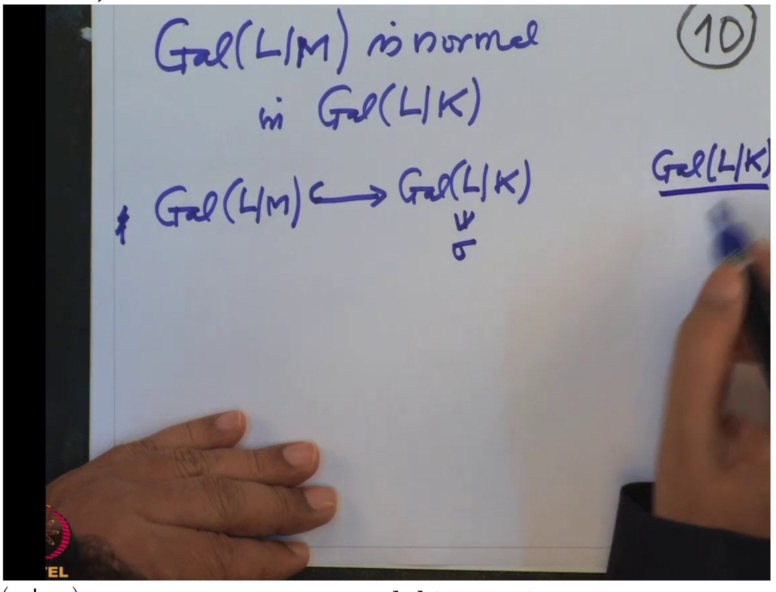
and we have given a map. So any σ , we have checked that any σ if I take

(Refer Slide Time 25:41)



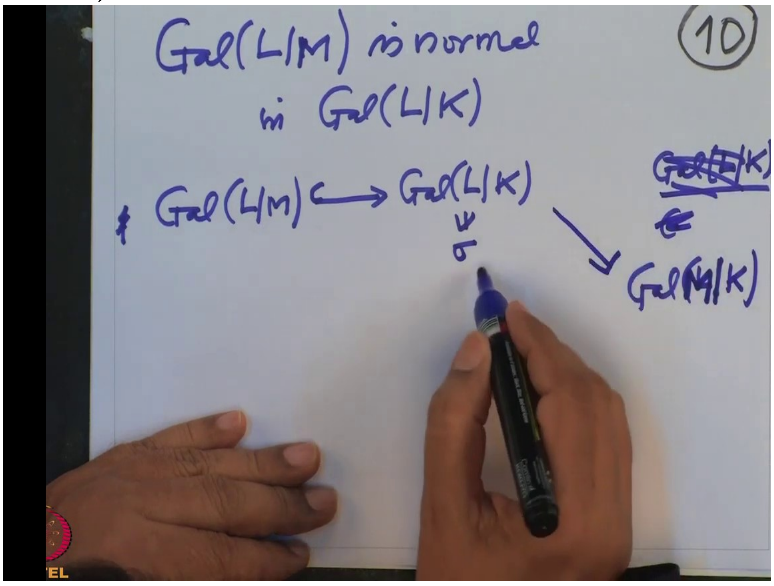
and restricts to M, it maps M inside M. So that means I have given a map from L over K modulo

(Refer Slide Time 25:55)



or directly $Gal(L|M)$, L over, M over K and this map is

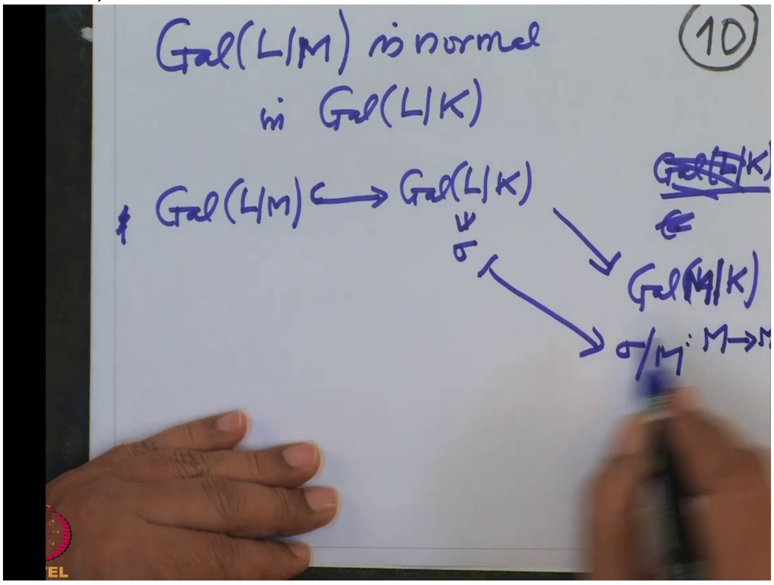
(Refer Slide Time 26:09)



σ going to σ restricted to M.

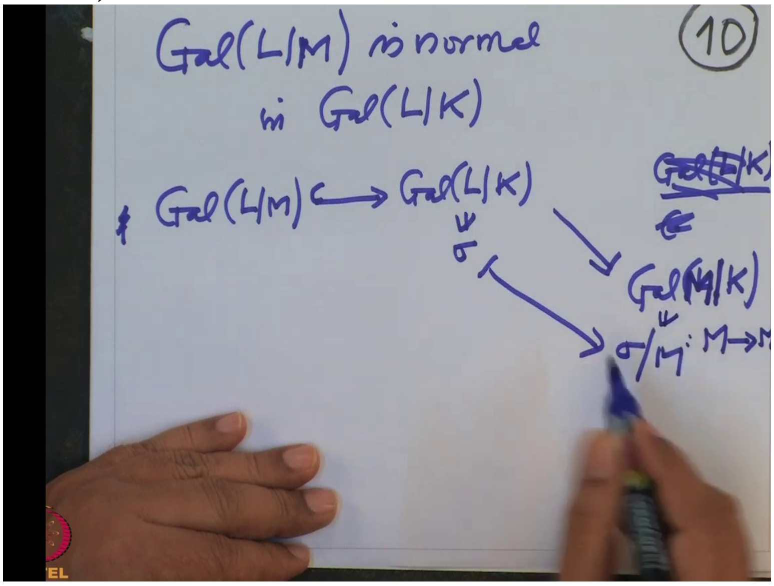
This makes sense. It is a homomorphism from M to M. It is algebra homomorphism from M to M. That is what we have checked

(Refer Slide Time 26:21)



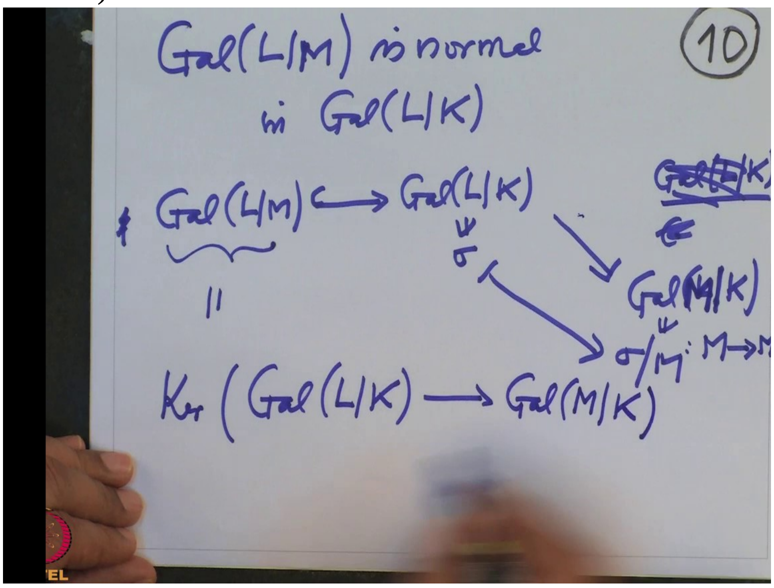
for every σ in the Galois group of L over K, if I restrict that to M, it goes M inside M and therefore it is an algebra automorphism of M. So that means it is an element in this Galois group.

(Refer Slide Time 26:33)



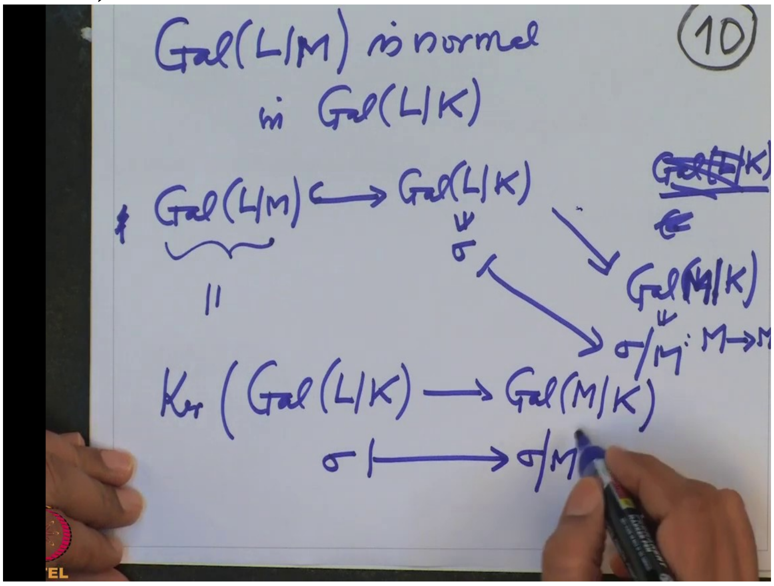
And when will this be identity? So what is the kernel of this map? Kernel of this map is precisely this subgroup. So this subgroup is therefore kernel of the restriction map. This is a restriction map. Kernel of $Gal(L|K)$ to $Gal(M|K)$,

(Refer Slide Time 26:57)



this map is any σ going to σ restricted to M. That makes sense because

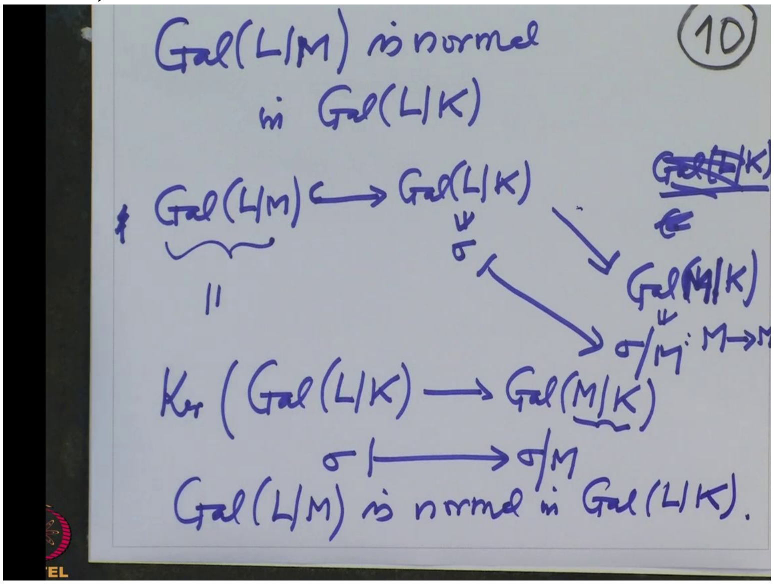
(Refer Slide Time 27:04)



this extension is Galois extension. That is what we checked.

And kernel is precisely this one. And that shows that this is, so that proves that $Gal(L|M)$, it is normal in Galois group of L over K.

(Refer Slide Time 27:23)



So we, remember that how do we check some subgroup of group is normal? That is if and only if it is kernel of a group homomorphism. Therefore it is normal. So we have proved altogether the statement, the normal subgroup will correspond to the Galois extension, Galois extension, Galois subextension will correspond to the normal subgroup.

So we have improved the Galois correspondence little bit better because we know which normal subgroups, where do they go? Or in other words when the Galois, when the intermediary field extension is a Galois extension. So we will continue this improvement more and more and that will enhance our understanding of the Galois groups using the Group Theory.

And that is what the main aim of this course is, to understand Galois extensions by using Group Theory. And conversely understand Group Theory by using Galois extensions. And then we will concentrate on the polynomials and the zeroes of the polynomials.

So polynomials will give us Galois extensions and Galois extensions will give us a group and then we will try to extract information about the

(Refer Slide Time 28:48)

of the polynomial by using the Group Theory.

So this is what plan is. We still have many more steps to go. But we will try to accumulate as much as possible, thank you.