Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 42
Correspondence of Normal Subgroups and Galois sub-extensions (Contd)

(Refer Slide Time 00:25)

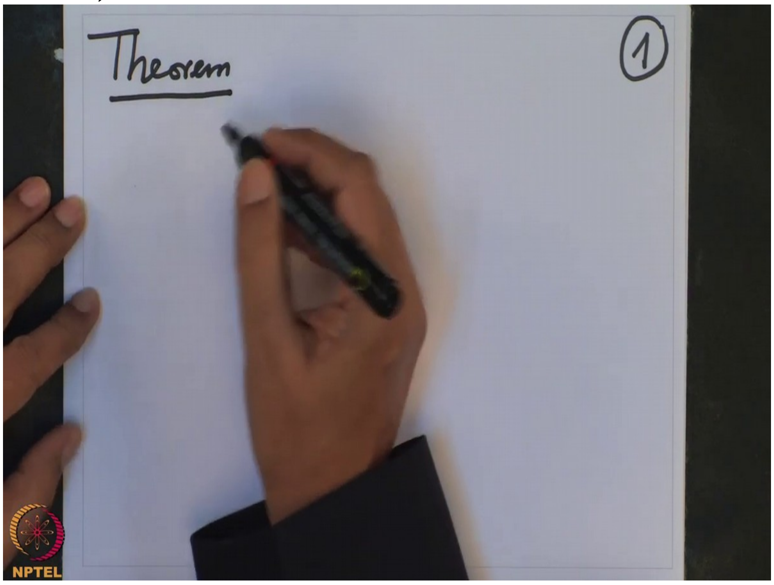
In the last lecture we have discussed very important theorem and we have proved it.

(Refer Slide Time 00:36)

However I want to state it more formally, the last time it was more of a discussion form.

So I want to state more formally what we have proved is the following theorem, so theorem this is one of the very important

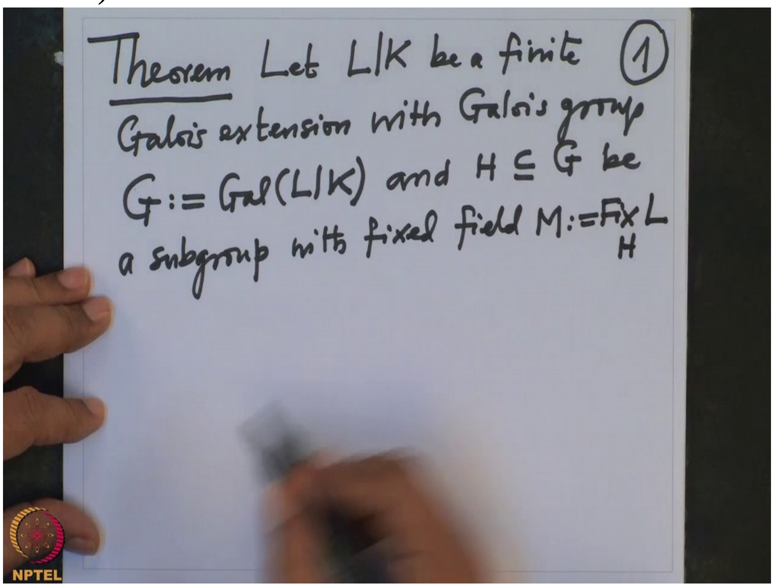
(Refer Slide Time 00:58)



steps in understanding the Galois theory, especially the Galois groups so on. Let L over K be a finite Galois extension with Galois group G which I am abbreviating for $Gal(L|K)$.

And let H contained in G be a subgroup and with fixed field M which is by definition $Fix_H L$.

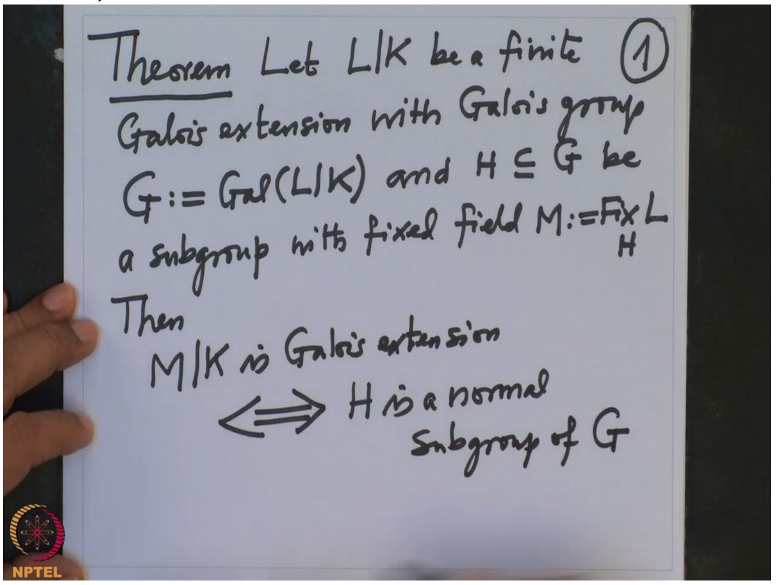
(Refer Slide Time 02:08)



This is under the natural action of Galois group on L. This is the fixed points of subgroups H, subgroup H Ok.

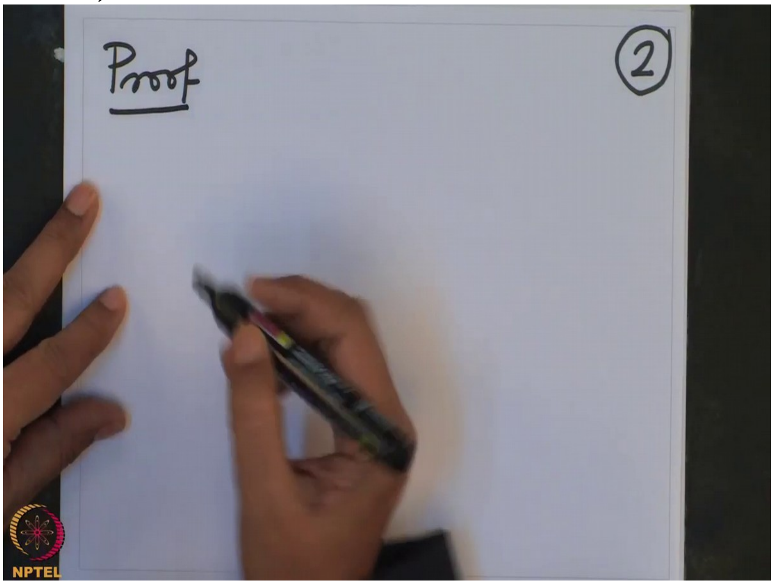
Now we are discussing when will M over K be Galois? Then, then M over K is Galois extension if and only if H is a normal subgroup of G.

(Refer Slide Time 02:54)



Alright so let me sketch the proof, the way we proved it. So we proved, first we proved, so proof. Proof, I am just

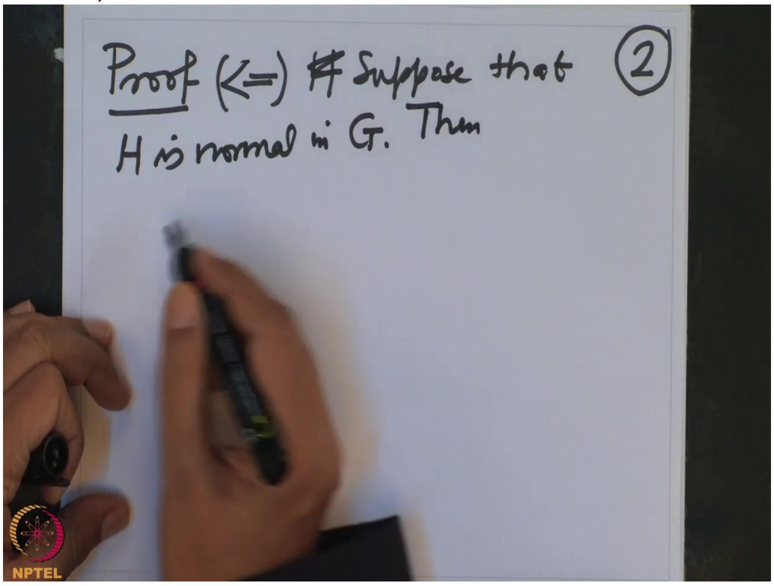
(Refer Slide Time 03:13)



writing the important steps which we checked last time, that first I am proving this way.

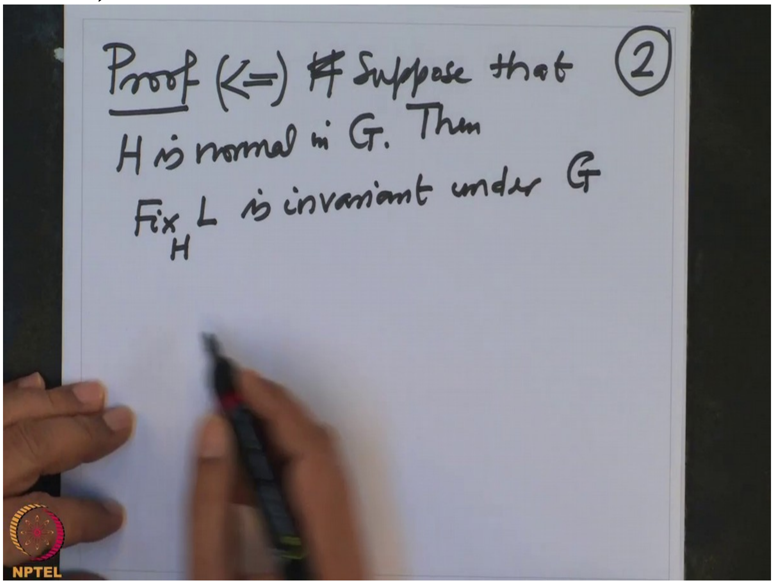
First we proved this way that is we are assuming H is normal. So H is normal, suppose that H is normal in G. Then we noted that, then

(Refer Slide Time 03:44)



this $Fix_H L$ is, is invariant under every element of G, invariant under G

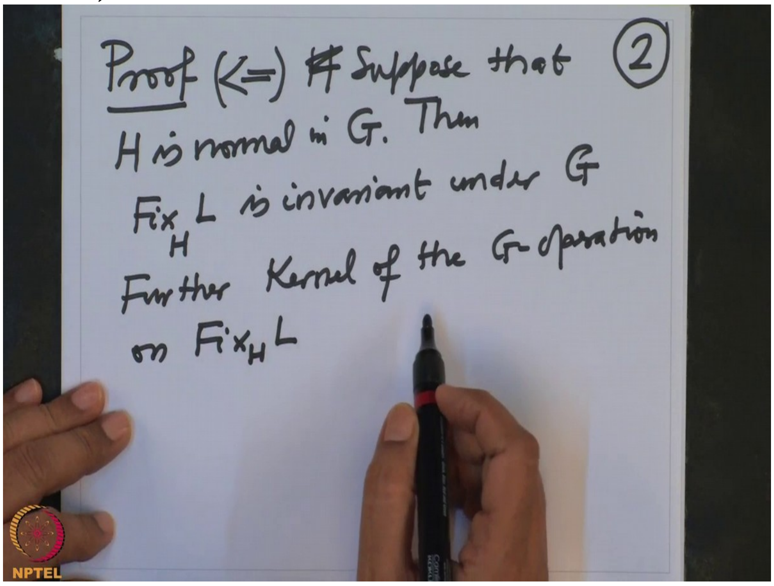
(Refer Slide Time 04:04)



so that means this is a G set, Ok.

That we have noted that and therefore we consider the restriction action of G on this. So further we noted that kernel of the G operation on this Fix, note that G operation is not arbitrary

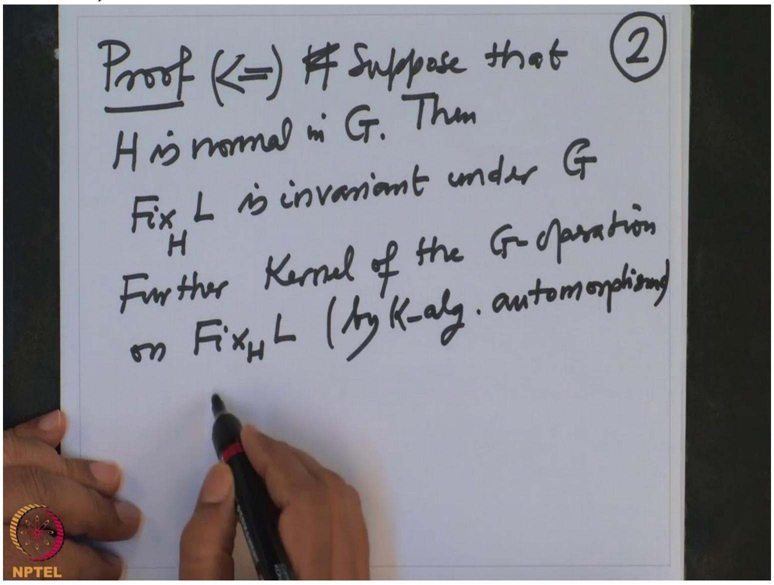
(Refer Slide Time 04:40)



G operation. It is induced on the operation of G on L which is by automorphism.

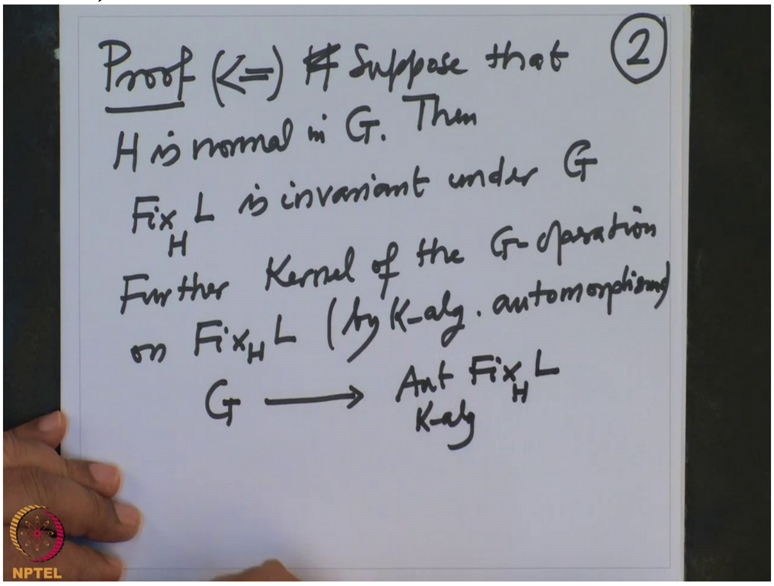
So therefore this G operation on this is by K-algebra automorphisms. That means

(Refer Slide Time 05:02)



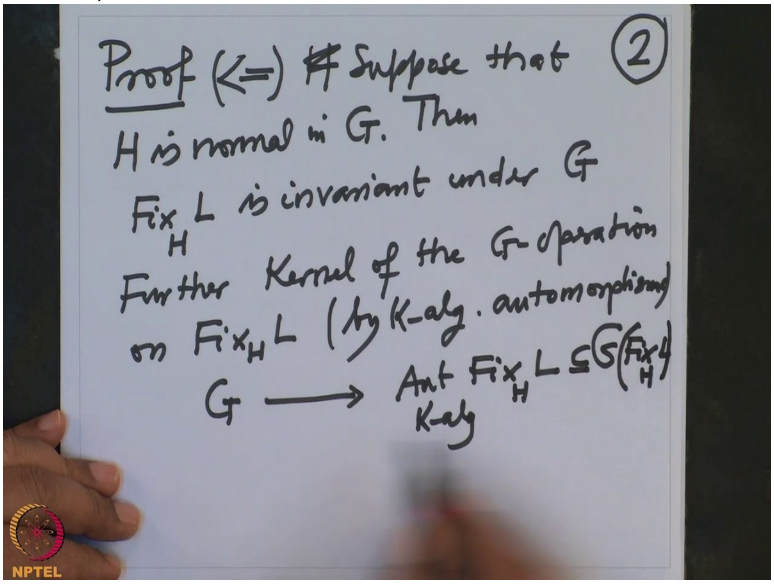
G to Aut K-algebra $Fix_H L$; we have

(Refer Slide Time 05:13)



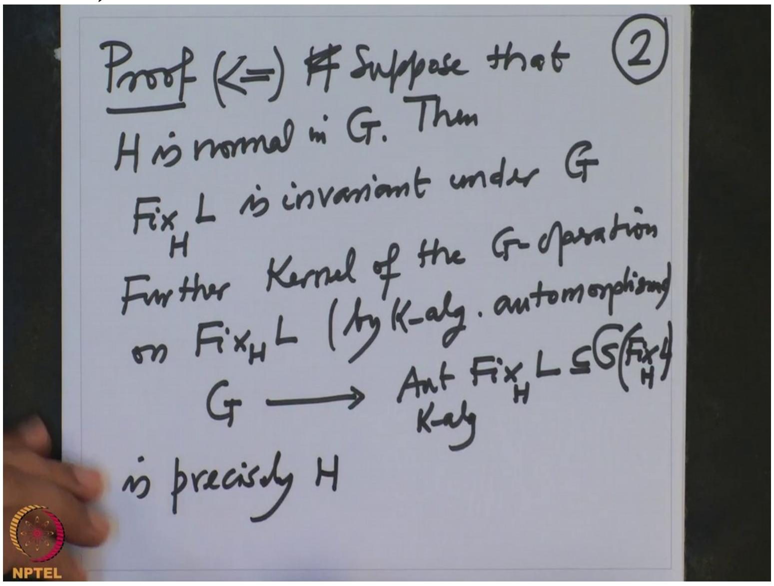
this operation on this which is sub of permutations on $Fix_H L$.

(Refer Slide Time 05:22)



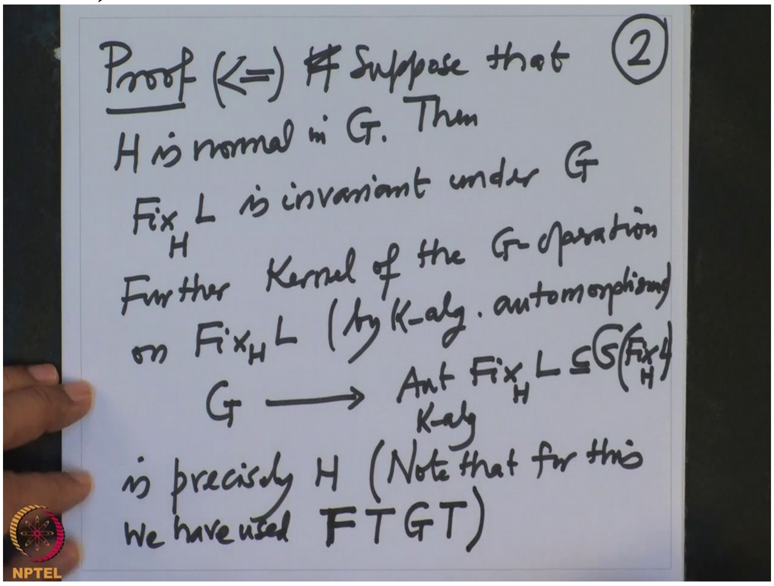
This operation, the kernel of this operation is precisely H.

(Refer Slide Time 05:36)



This, for this we have noted that, note that for this, for this we have used fundamental theorem of Galois Theory.

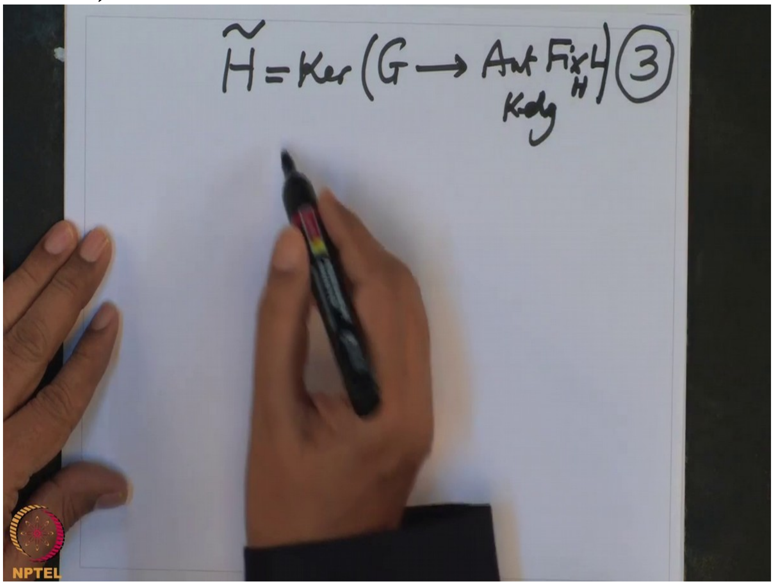
(Refer Slide Time 05:58)



So to check that we have used, so suppose, so let me indicate how did we check this. This we have checked as follows.

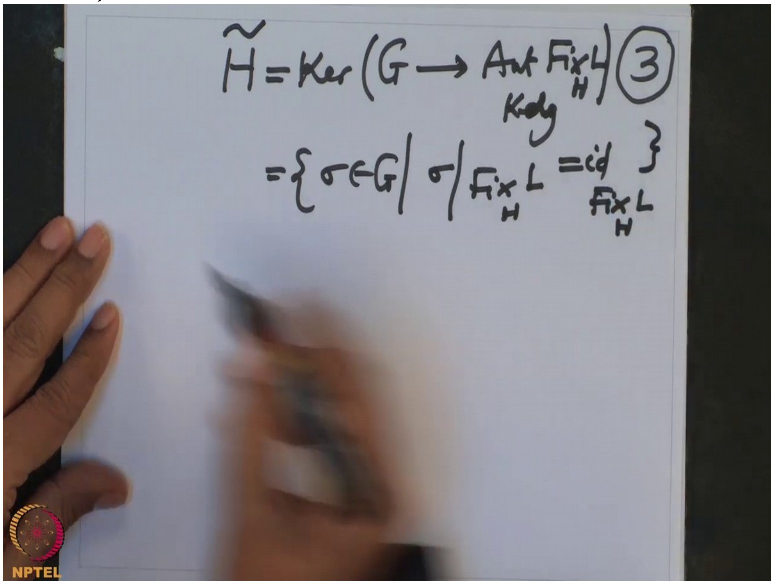
So let $\widetilde{H}$ be the kernel of G to this Aut K-algebra $Fix_H L$.

(Refer Slide Time 06:29)



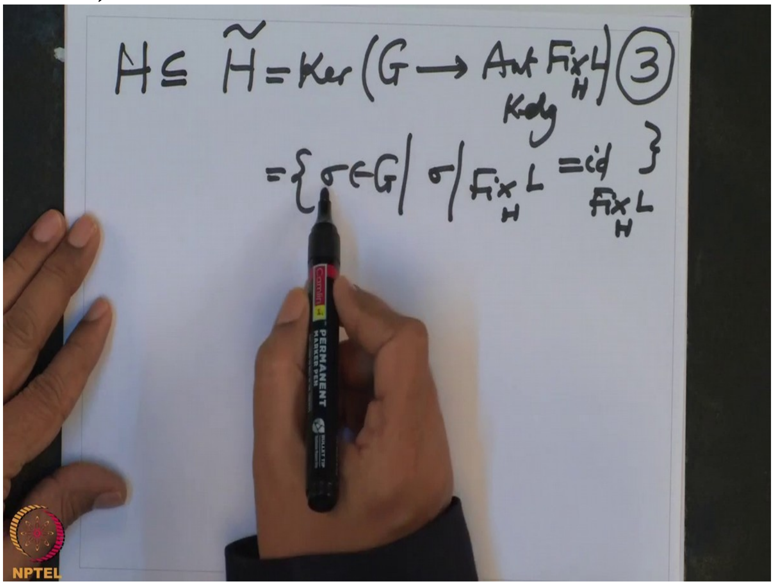
So that means this is all those elements σ in G such that σ restricted to the Fix field equal to the identity on the Fix field.

(Refer Slide Time 06:44)



And obviously it contains H because

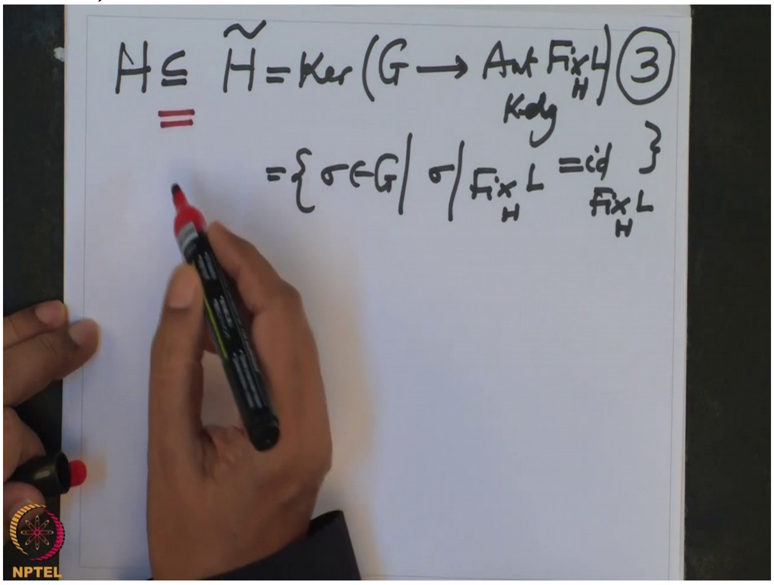
(Refer Slide Time 06:49)



every element of H fixes this point wise.

Therefore it is indeed here; conversely I want to prove that, to prove equality here. To prove the equality here,

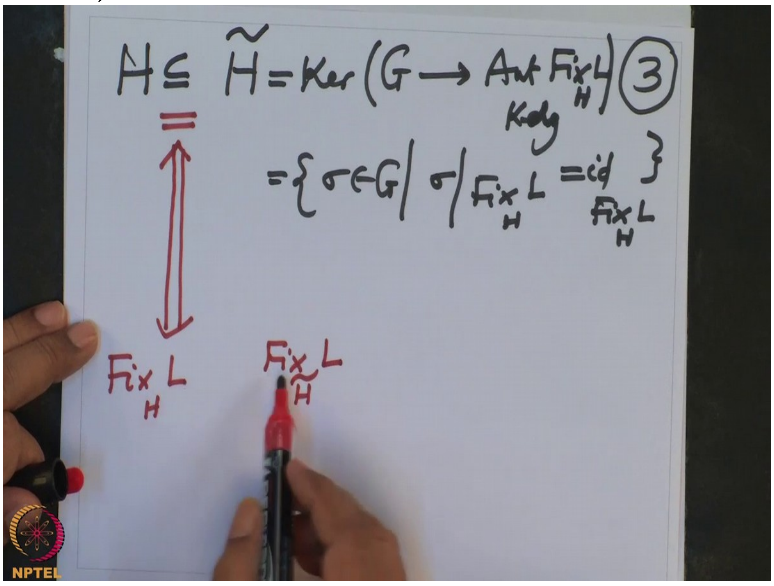
(Refer Slide Time 07:06)



how did we prove?

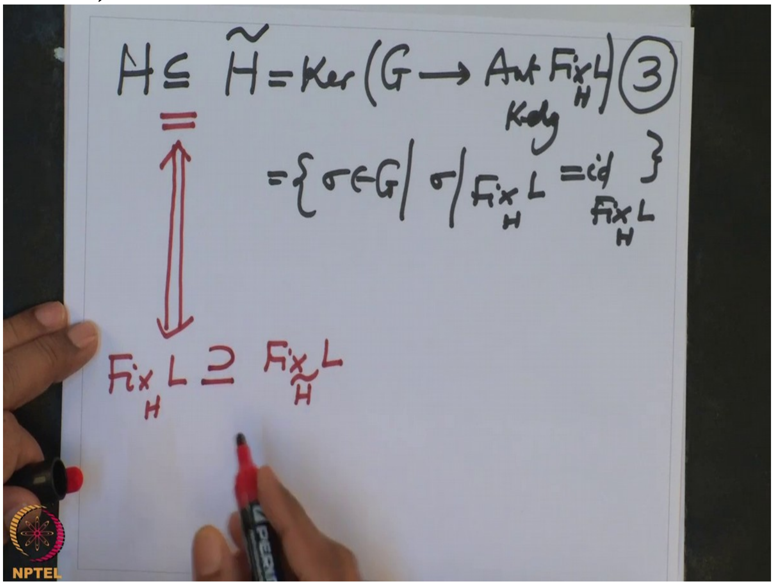
To check the equality here that is equivalent to checking the Fix fields are same but

(Refer Slide Time 07:20)



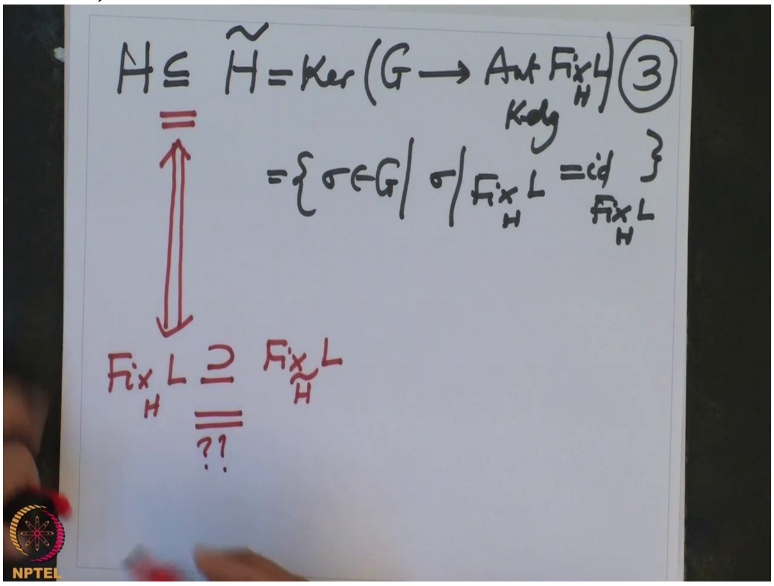
which is clearly bigger, this is smaller group therefore Fix field this is bigger, this is clear.

(Refer Slide Time 07:26)



But we want to check equality here.

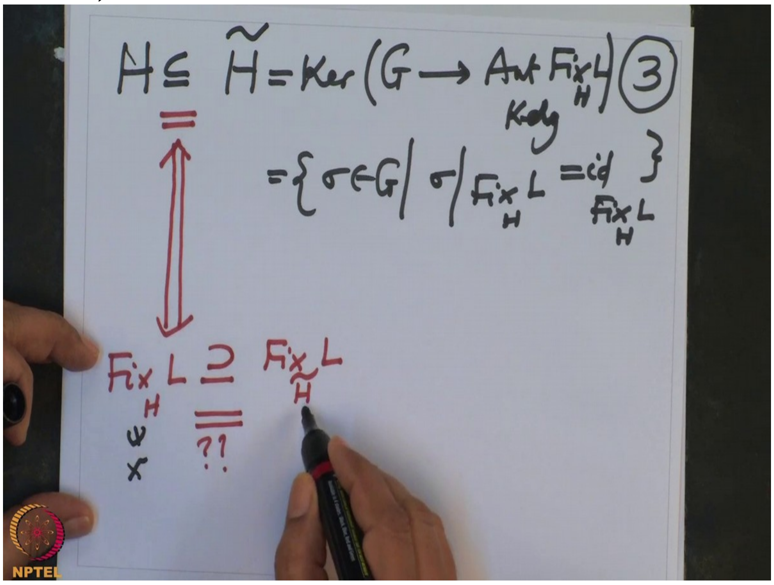
(Refer Slide Time 07:29)



And that we have checked as follows.

We have taken an element here x and we want to check it is here.

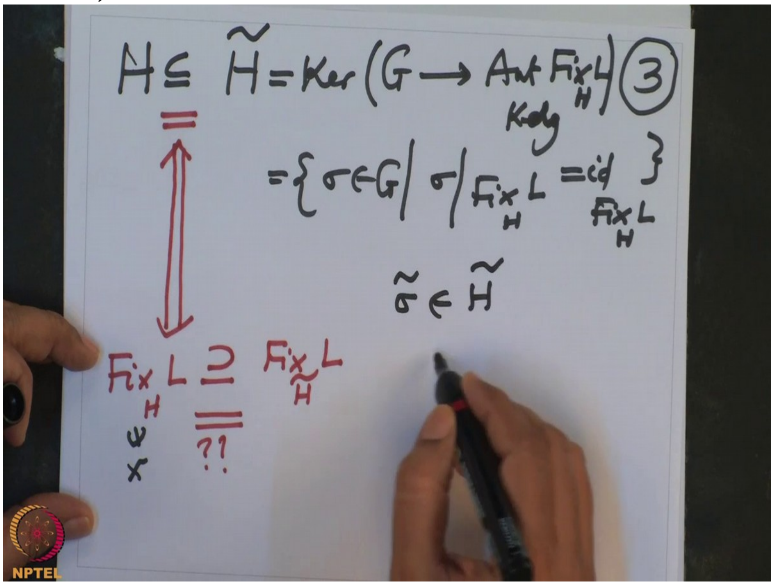
(Refer Slide Time 07:37)



So an element here is, H is an element here means, that means, and I want to check it here, so therefore we take any element in $\tilde{\sigma}$ in $\tilde{H}$.

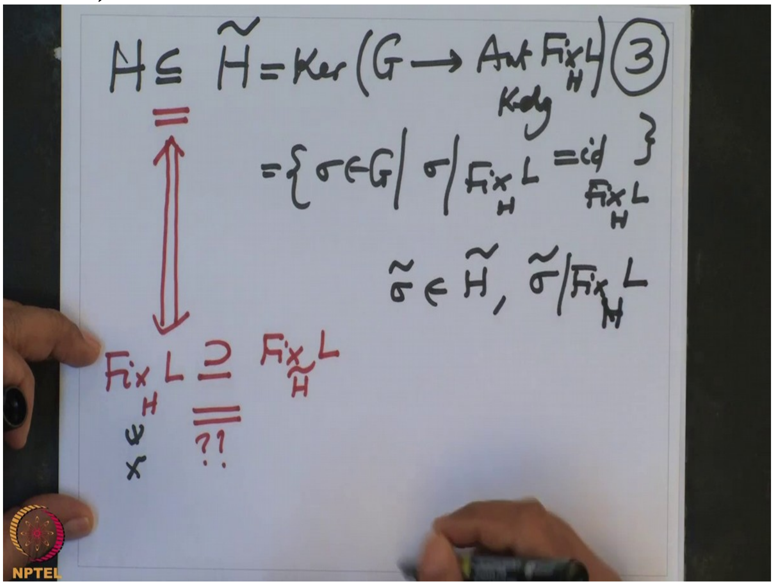
That is then by definition,

(Refer Slide Time 07:56)



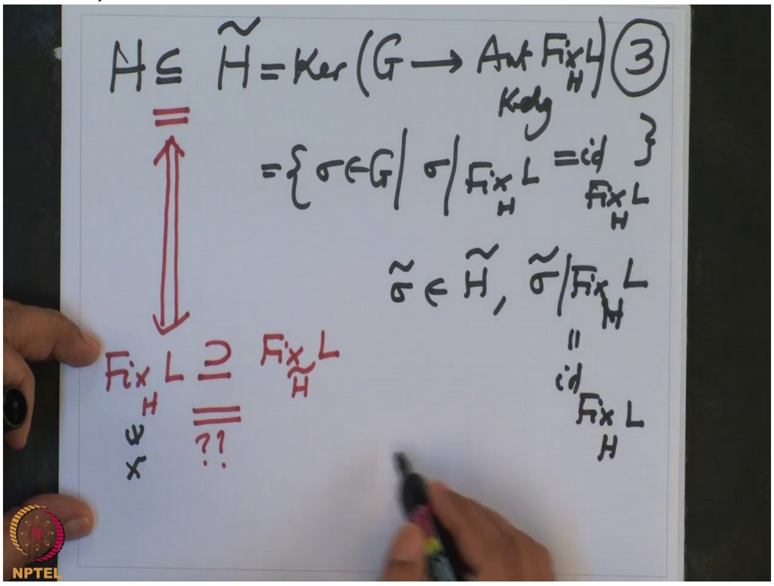
$\tilde{\sigma}$ is an element in G and $\tilde{\sigma}$ restricted to the Fix field of H,

(Refer Slide Time 08:06)



this is identity on the Fix field, in particular x is an element here,

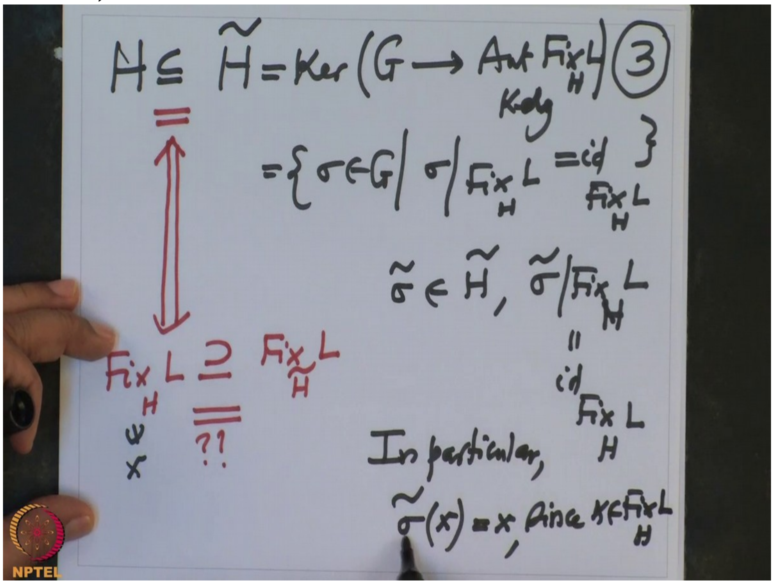
(Refer Slide Time 08:15)



therefore in particular $\tilde{\sigma}$ operated on x is same thing as x.

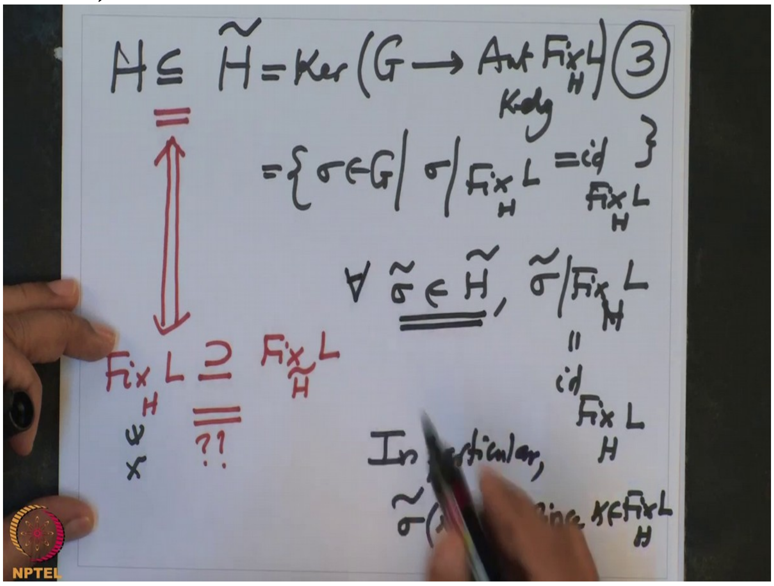
It is since we started with x in Fix field. Therefore

(Refer Slide Time 08:33)



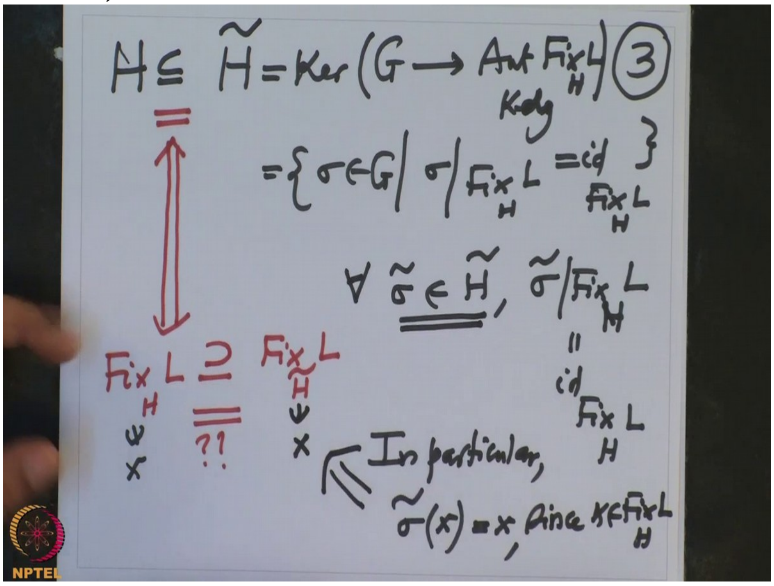
it is here, but that means, and that we have checked it for every $\tilde{\sigma}$

(Refer Slide Time 08:39)



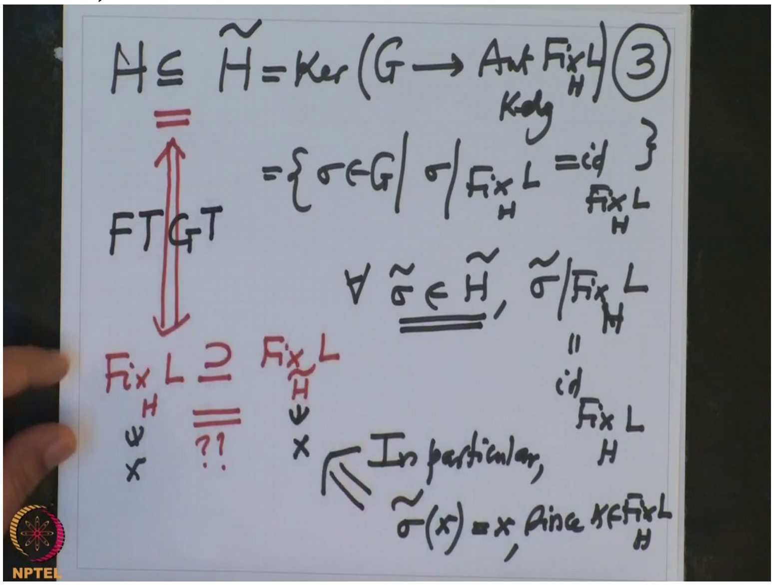
but that is precisely the meaning of x belonging to this.

(Refer Slide Time 08:45)



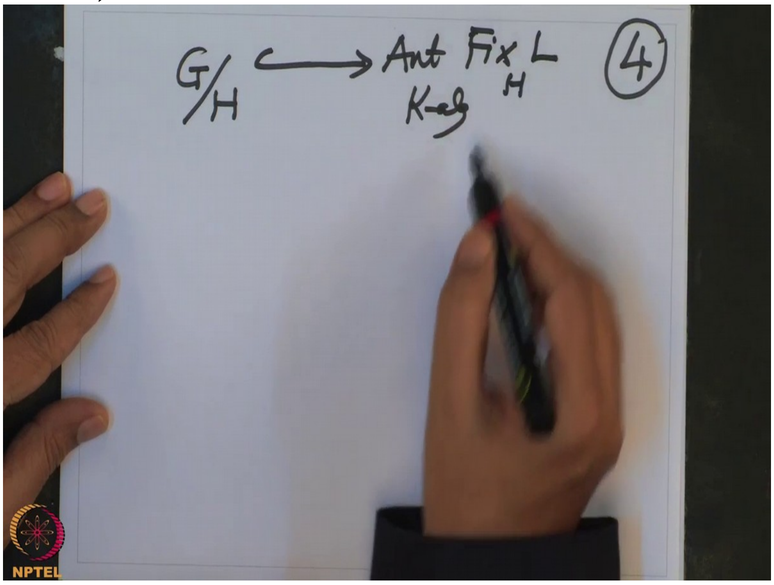
So that is how we proved the Fix fields are same. And once Fix fields are same we know there is one to one correspondence between the subgroup and the Fix fields. So this was precisely F T G T.

(Refer Slide Time 08:59)



So we have proved altogether that this kernel is precisely H but then once the kernel is H what do we get? Then we get an injective homomorphism from G/H to automorphisms as K-algebra of $Fix_H L$

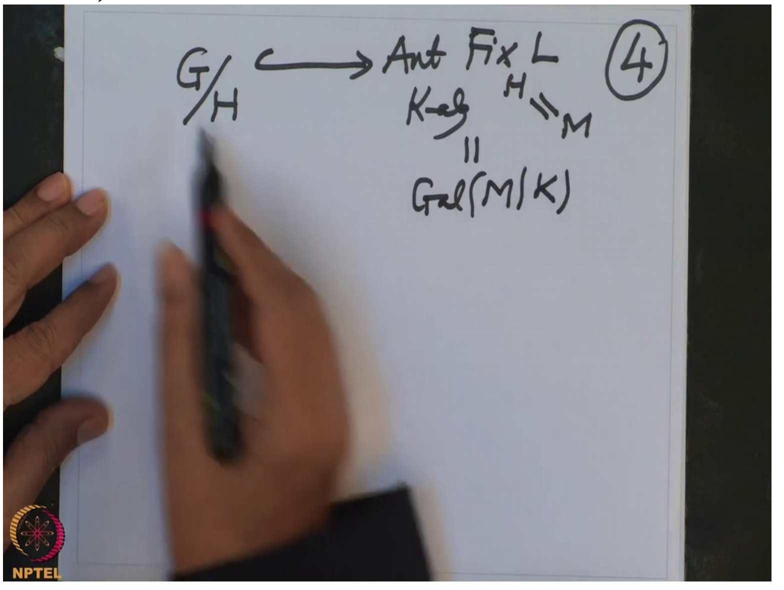
(Refer Slide Time 09:25)



but this is, this was in our notation this was M.

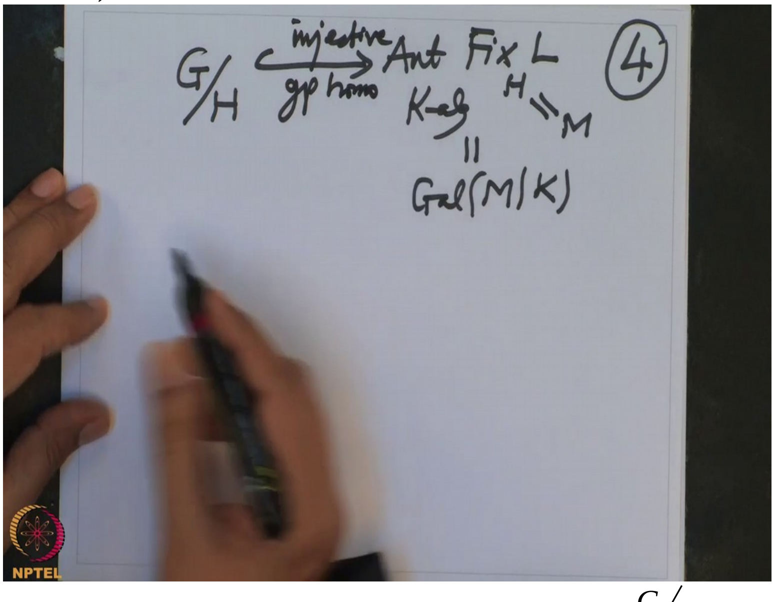
But this is nothing but the Galois group of M over K

(Refer Slide Time 09:35)



and then the group; this is injective group homomorphism because we went mod the kernel.

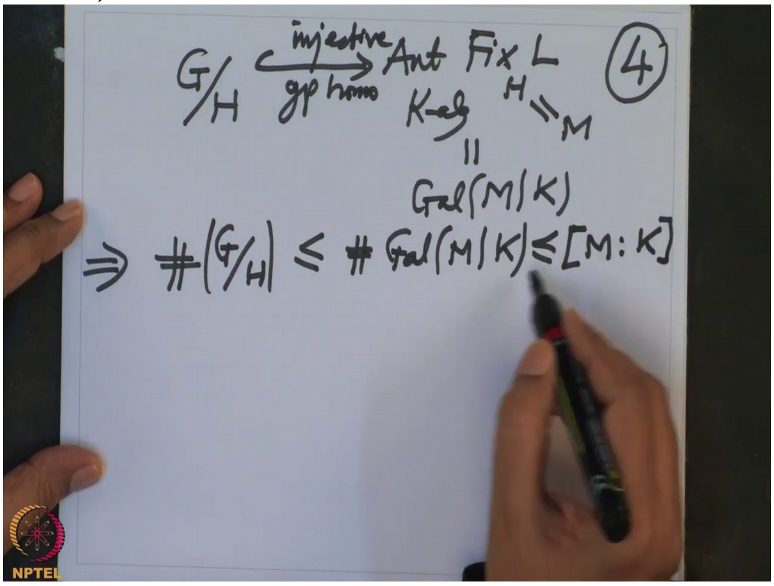
(Refer Slide Time 09:43)



So therefore we will get cardinality of this quotient group G/H is smaller equal to cardinality of the Galois group but this Galois group cardinality is smaller equal to degree M over K.

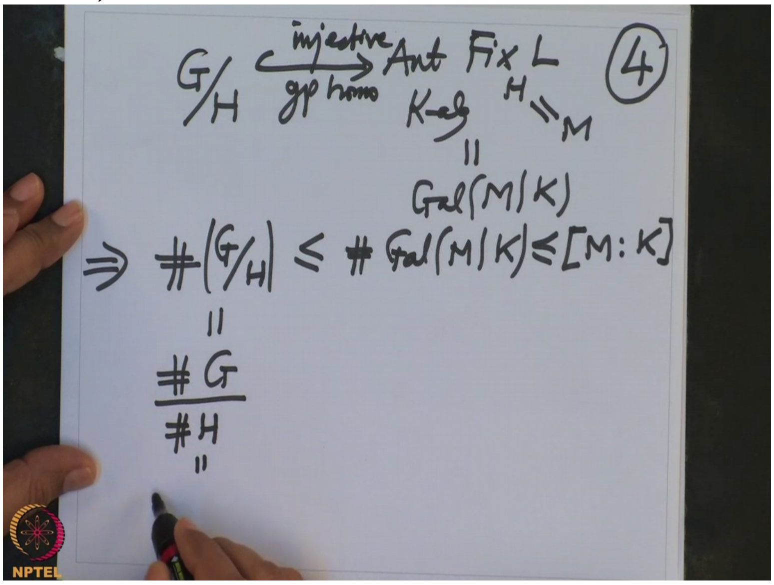
That is true for any

(Refer Slide Time 10:03)



field extension because we know this is by that Dedekind and Artin Theorem, long back we proved it, this quotient group therefore this is cardinality G by cardinality H but cardinality G is,

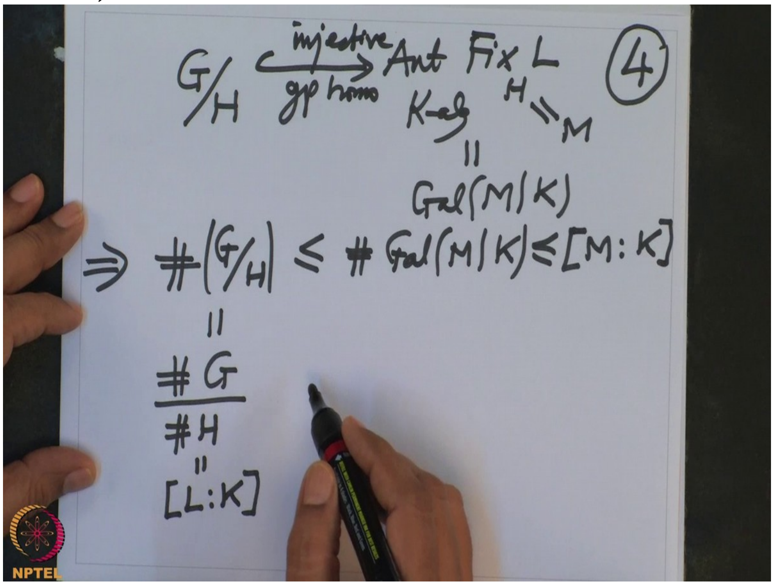
(Refer Slide Time 10:22)



cardinality of, this is the Galois group of L over K and L over K is Galois extension

Therefore this cardinality is L over K and H, cardinality of H, H was what, H was the group

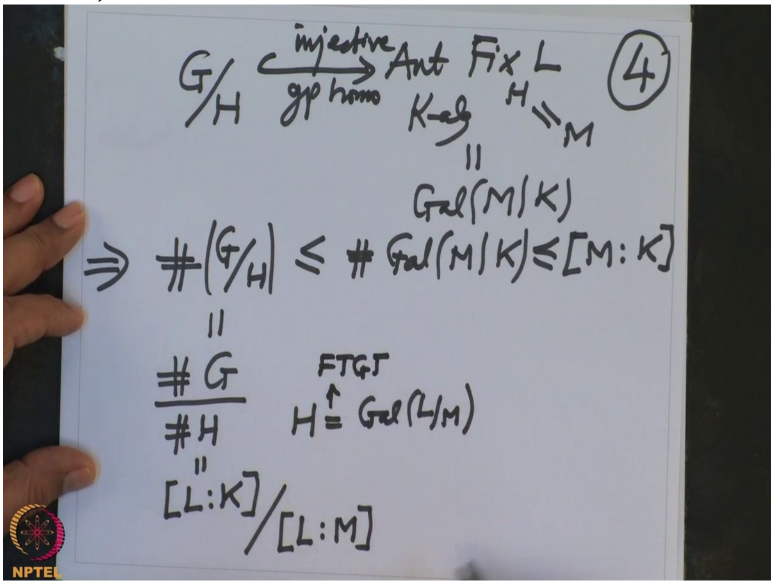
(Refer Slide Time 10:35)



$Gal(L|M)$, that is cardinality of this.

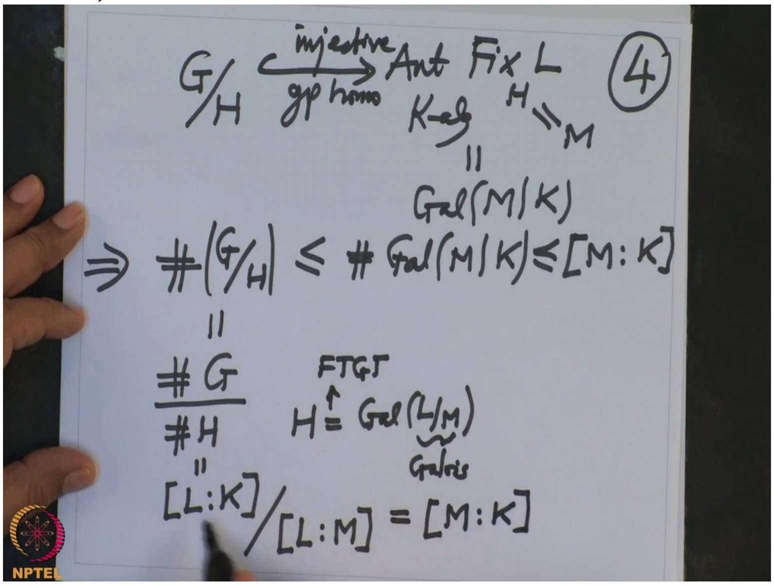
This is because H is $Gal(L|M)$. This is precisely, again this equality by F T G T if one likes,

(Refer Slide Time 10:59)



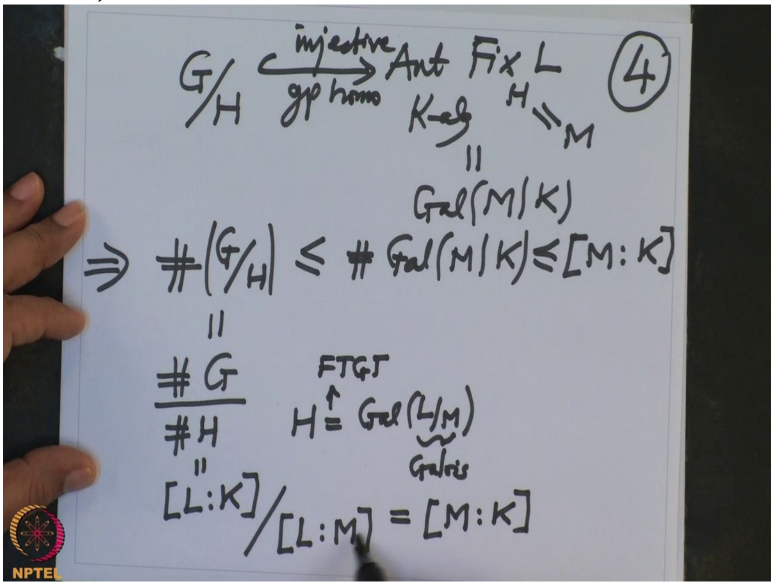
therefore and this extension is Galois, we have this equality here, therefore equality here but this one is same as M over K because

(Refer Slide Time 11:13)



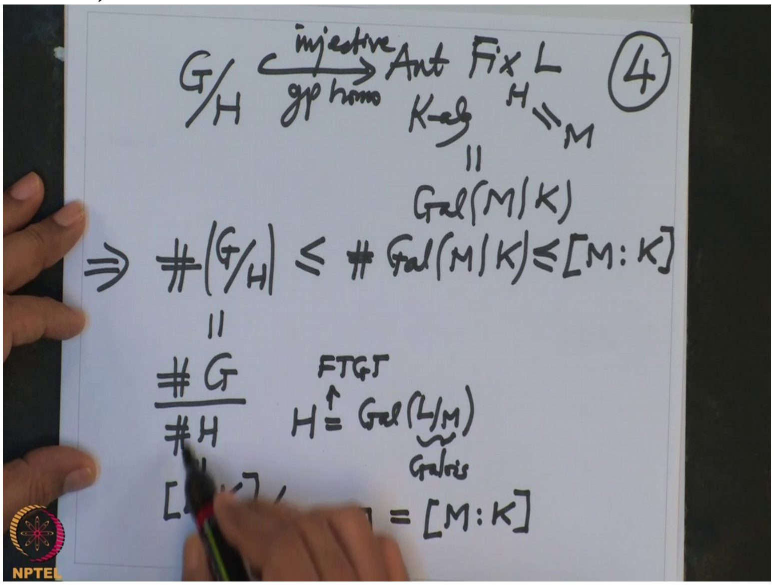
for intermediary field, so multiply this, you get L over K, so read from here, we have proved

(Refer Slide Time 11:20)



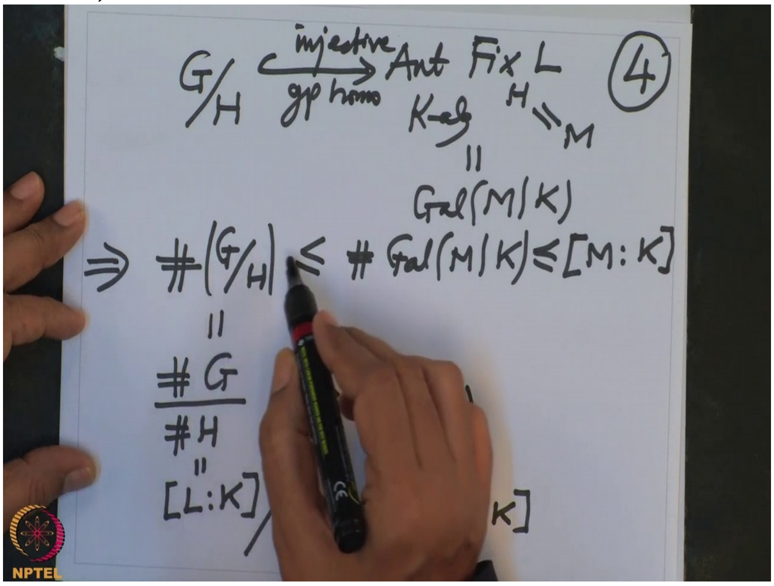
this equal

(Refer Slide Time 11:21)



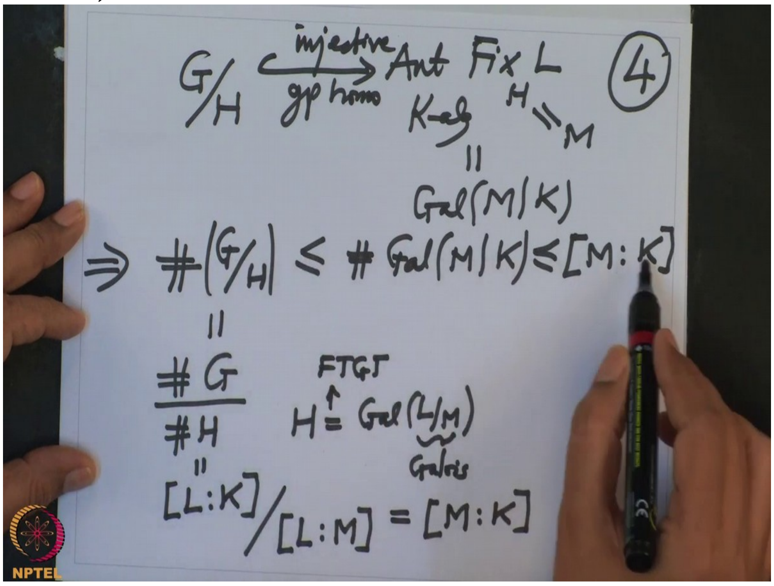
to this equal to this less equal

(Refer Slide Time 11:23)



to this less equal

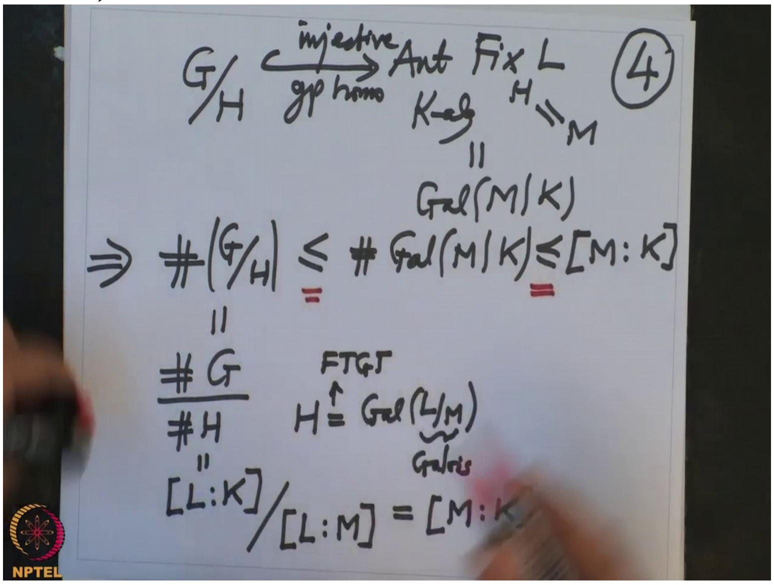
(Refer Slide Time 11:24)



to this.

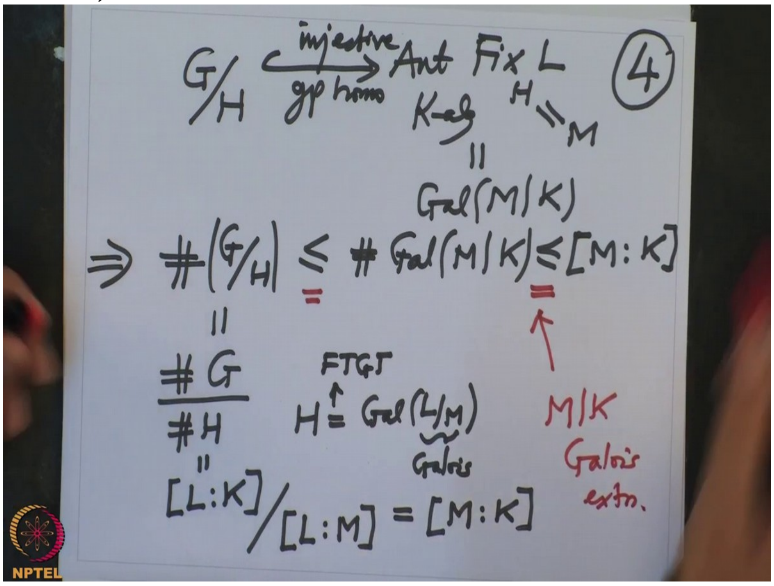
But this number and this number is same. So everywhere there is equality. Therefore we have proved equality here and equality here

(Refer Slide Time 11:35)



but equality here precisely means that M over K is Galois. This was what

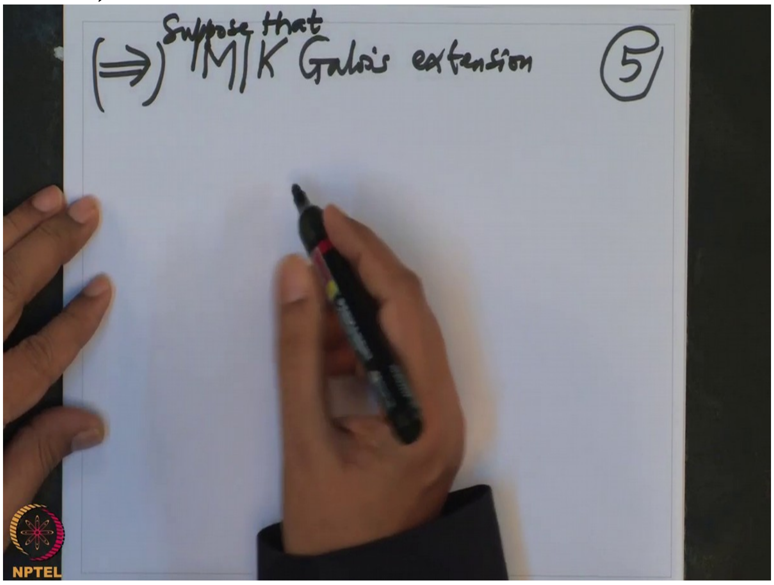
(Refer Slide Time 11:43)



one implication we had to prove.

Conversely what did you do? Conversely assuming that, so converse implication is so this way we are assuming M over K is Galois. So suppose that M over K is a Galois extension.

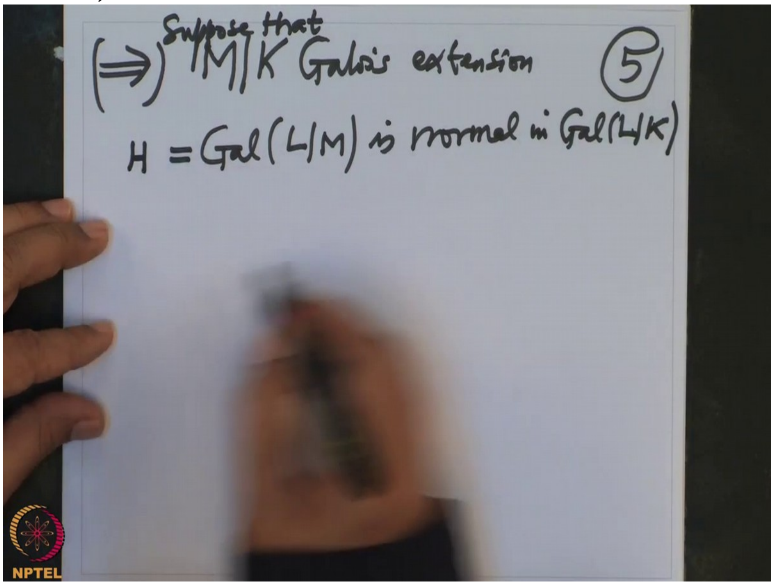
(Refer Slide Time 12:10)



Then I want to prove that the Fix field, the Galois group that is $Gal(L|M)$ is normal in $Gal(L|K)$.

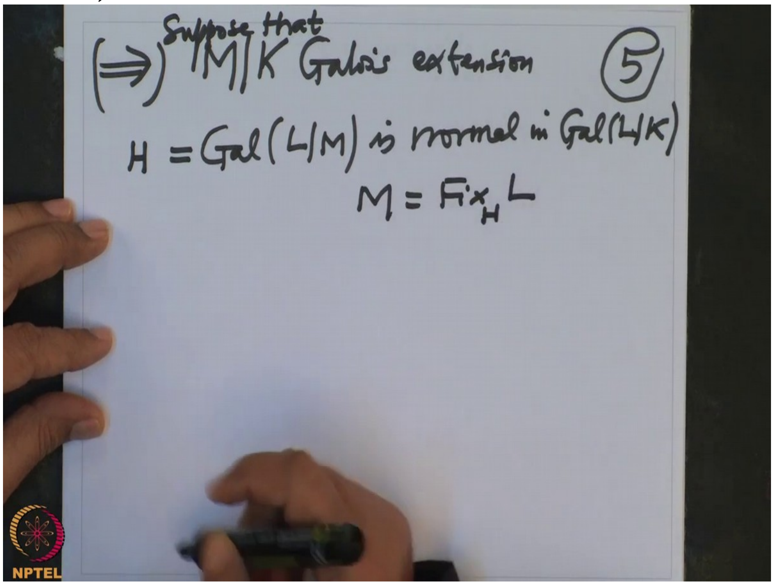
This is what I have to prove. This is our H.

(Refer Slide Time 12:30)



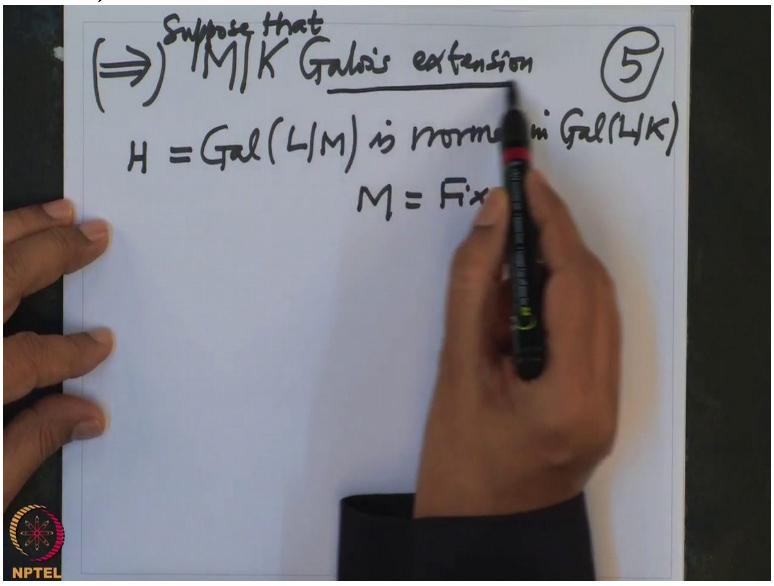
And M is precisely the Fix field of H. And

(Refer Slide Time 12:36)



we want to prove, assuming it is Galois extension

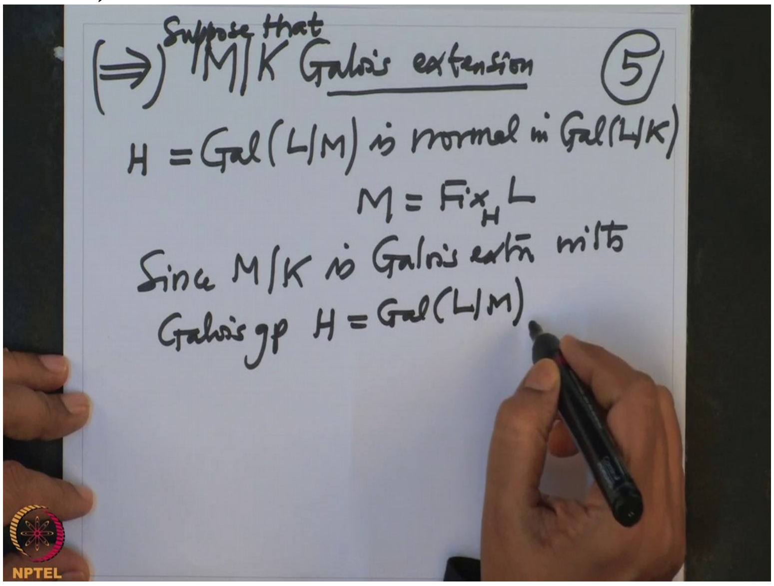
(Refer Slide Time 12:38)



we want to prove it is nor/normal, this subgroup is normal.

Alright we want to prove subgroup is normal, so I will, therefore I will, Ok so it is normal. So and we want to use the fact that M over K is the Galois extension so it has a primitive element. So since M over K is Galois extension with Galois group H which is $Gal(L|M)$,

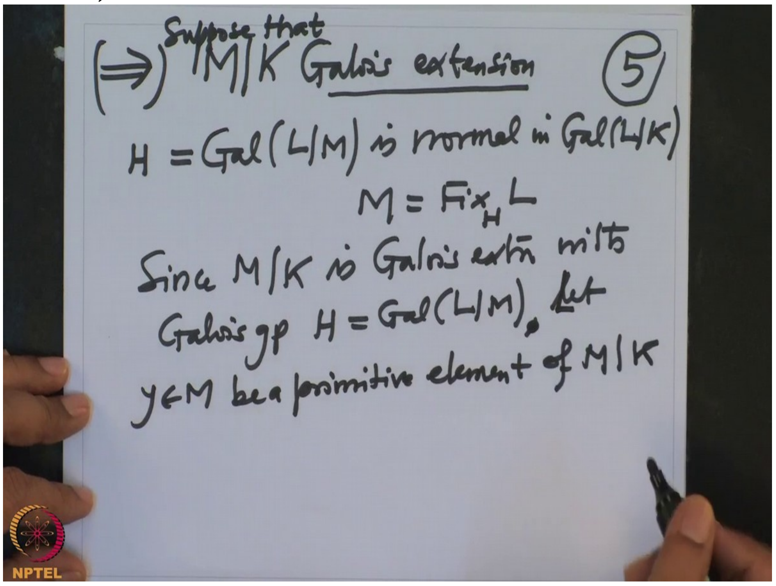
(Refer Slide Time 13:26)



it has a primitive element.

So let $y \in M$ be a primitive element of M over K.

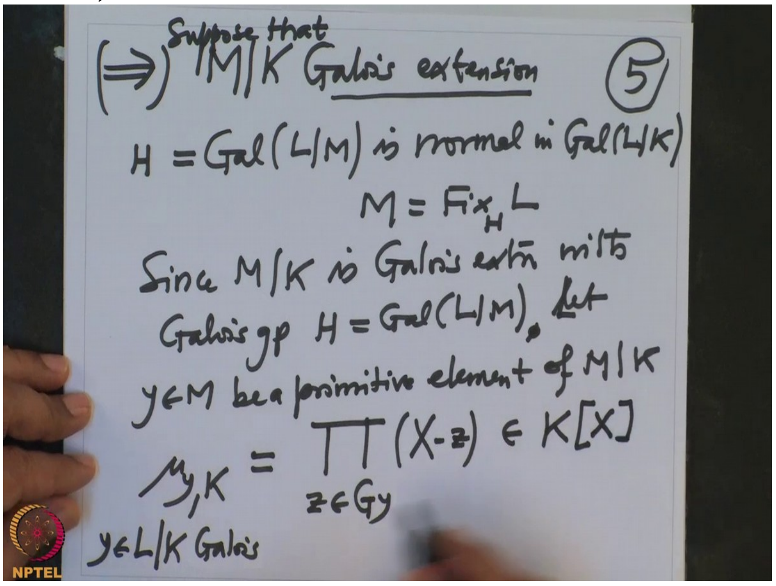
(Refer Slide Time 13:44)



So then we know the minimal polynomial of y over K, we noted in one of the lectures earlier, whenever this I am applying it to the, an element y, $y \in L$ which is Galois over K, in this situation we have noted the minimal polynomial is nothing but product z belonging to the orbit of y where $X - z$.

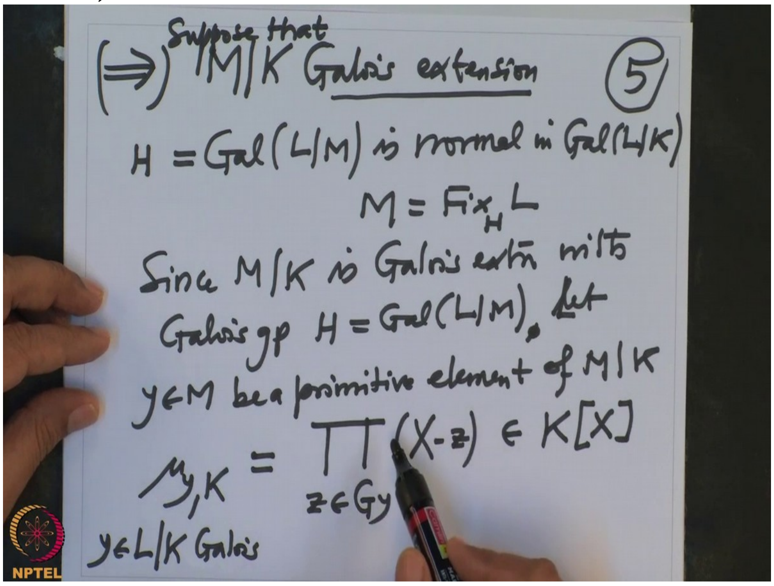
This is a monic polynomial in $K[X]$ and

(Refer Slide Time 14:20)



it is a minimal monic polynomial of y over K. y is one of the elements in the orbit so y is the root. But because it is a Galois extension and this y is a primitive element, this polynomial

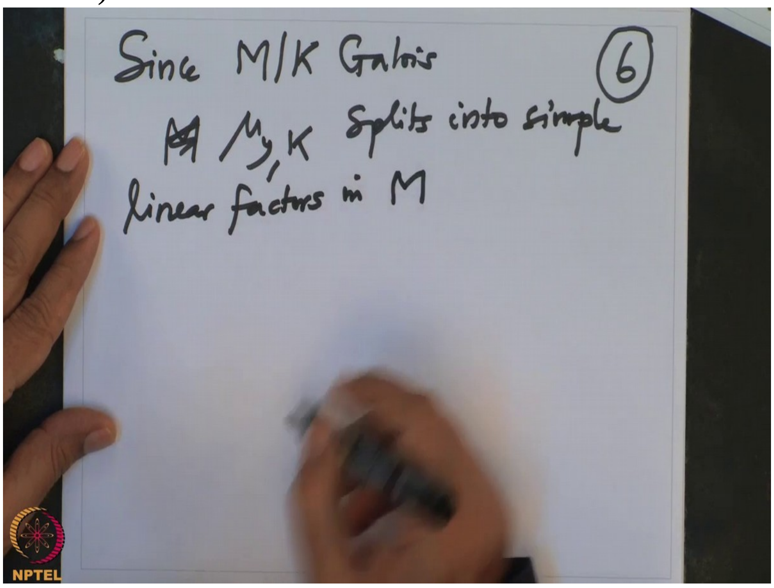
(Refer Slide Time 14:37)



splits.

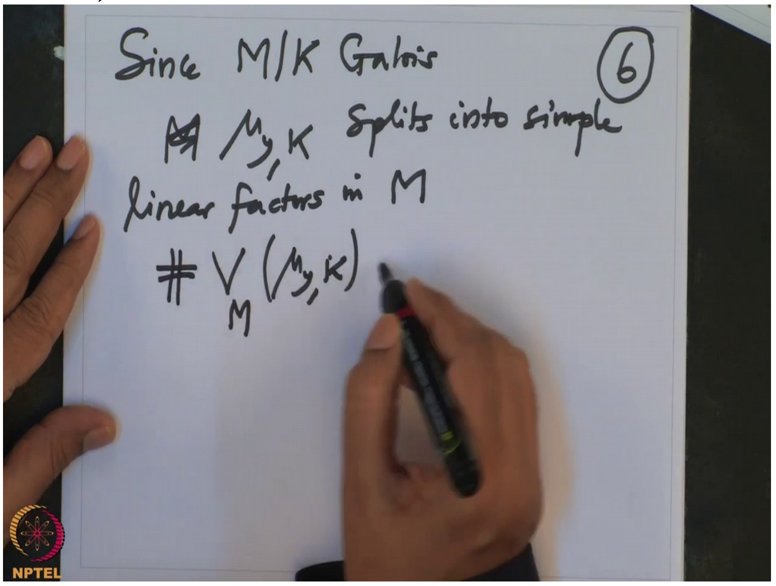
So since M over K is Galois, this is very important observation, that is why I wanted to repeat little bit. So since M over K is Galois, minimal polynomial, minimal polynomial of the primitive element splits into simple linear factors in M.

(Refer Slide Time 15:13)



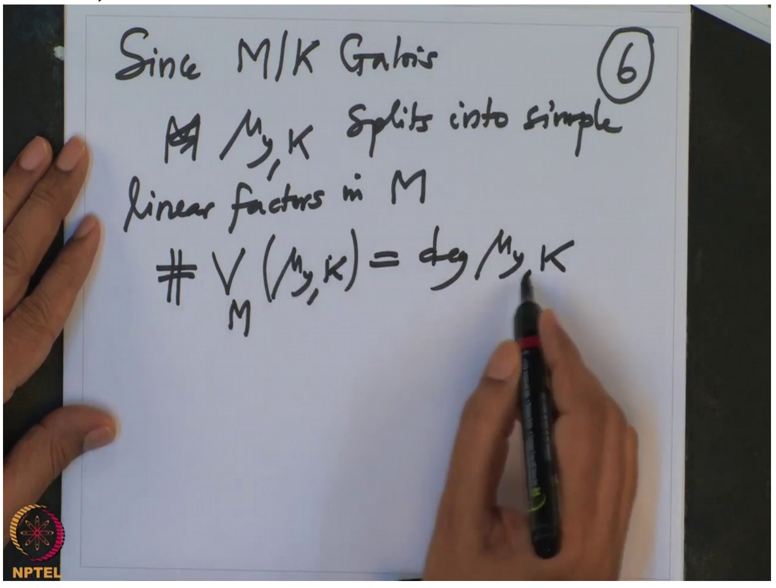
So but I know what are the, in particular all zeroes are simple and all of them, so the zeroes of $\mu_{y,K}$ in M, this cardinality

(Refer Slide Time 15:28)



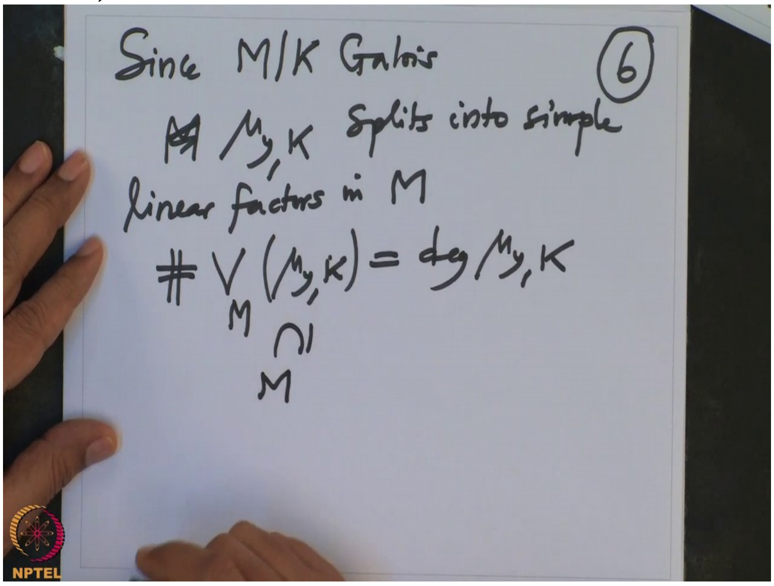
is equal to the degree of μ_y and

(Refer Slide Time 15:33)



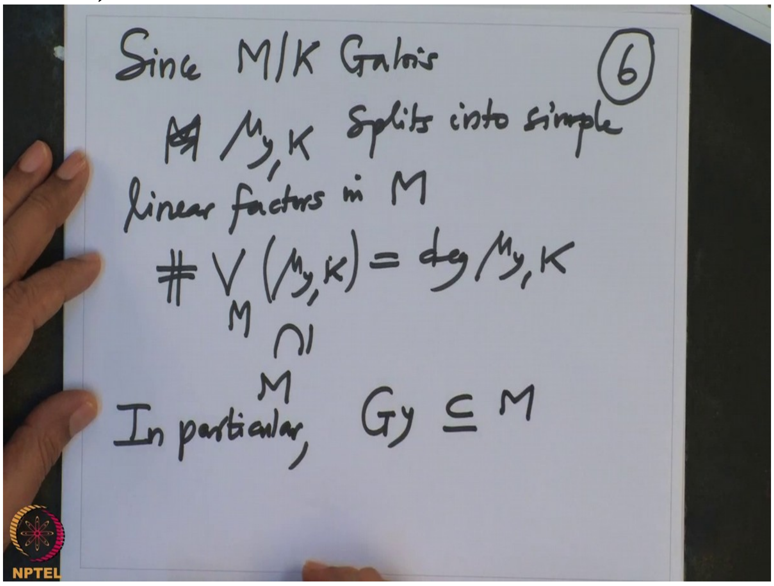
that means they are all simple and all of them lie inside M.

(Refer Slide Time 15:38)



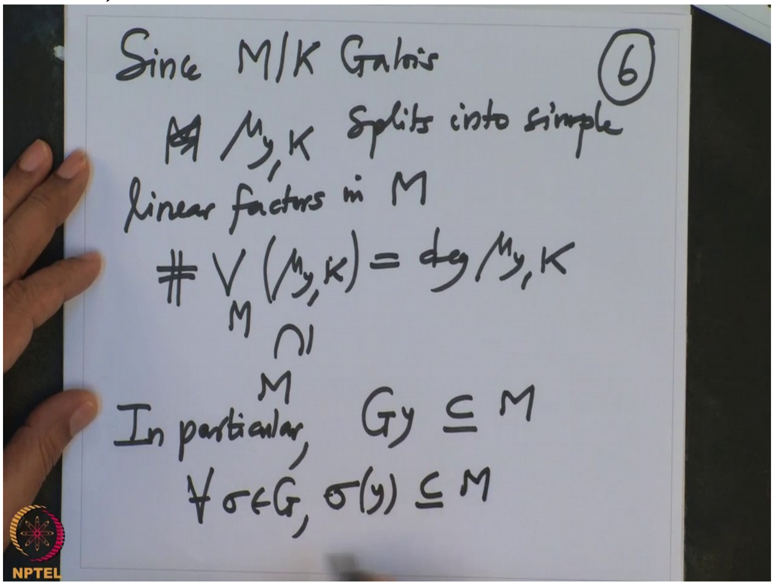
Therefore in particular, the whole orbit of y is contained in M.

(Refer Slide Time 15:53)



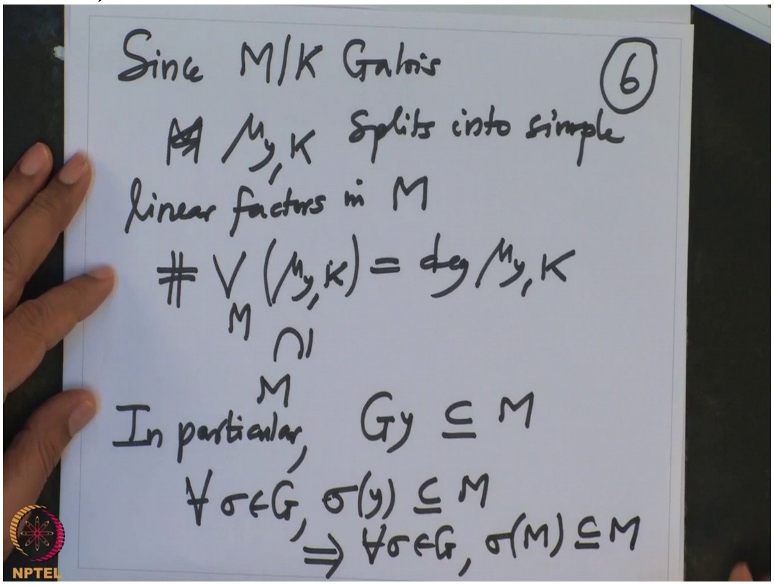
So therefore for every σ in G, $\sigma(y)$ is contained in M.

(Refer Slide Time 16:03)



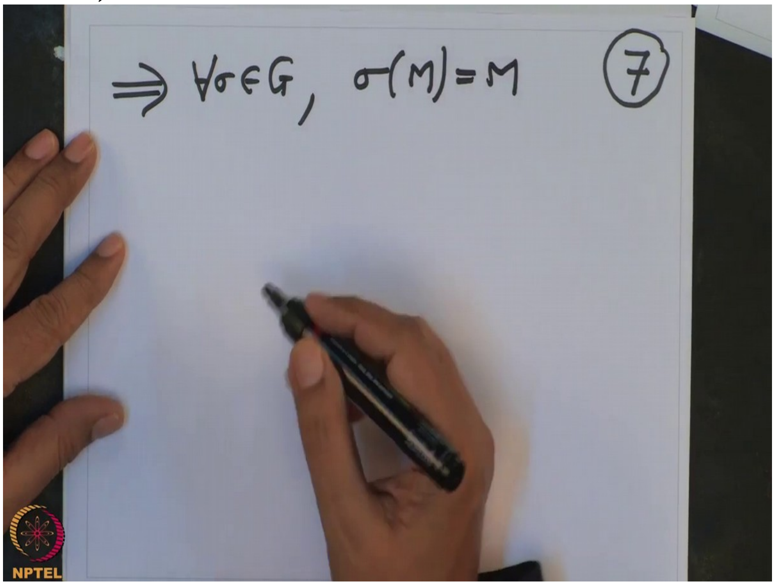
Therefore for every σ in G σ of M is contained in σ of M,

(Refer Slide Time 16:12)



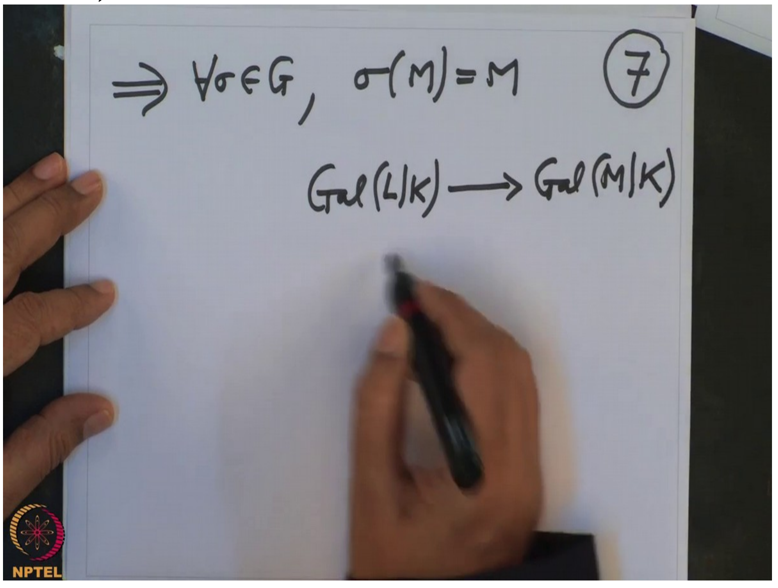
but then I can apply the same thing for the inverse. So that implies, for every σ in G σ of M equal to M.

(Refer Slide Time 16:26)



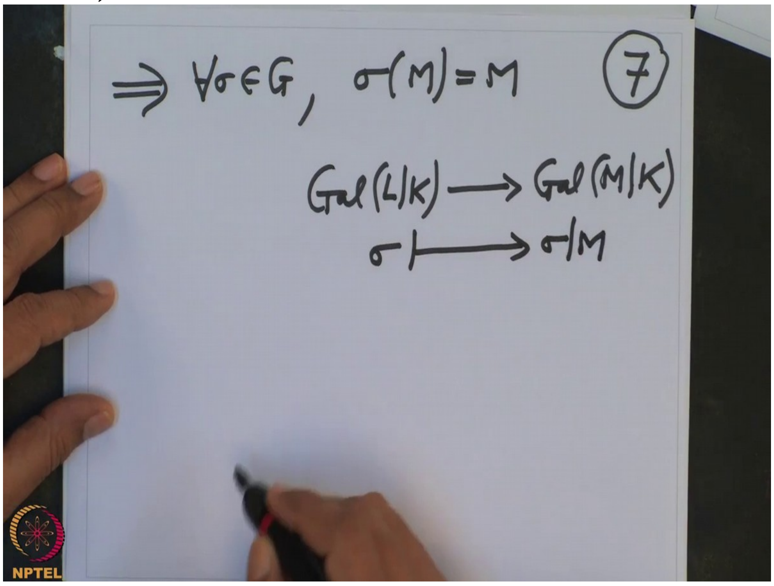
So therefore, therefore we have this map $Gal(L|K)$ to $Gal(M|K)$;

(Refer Slide Time 16:39)



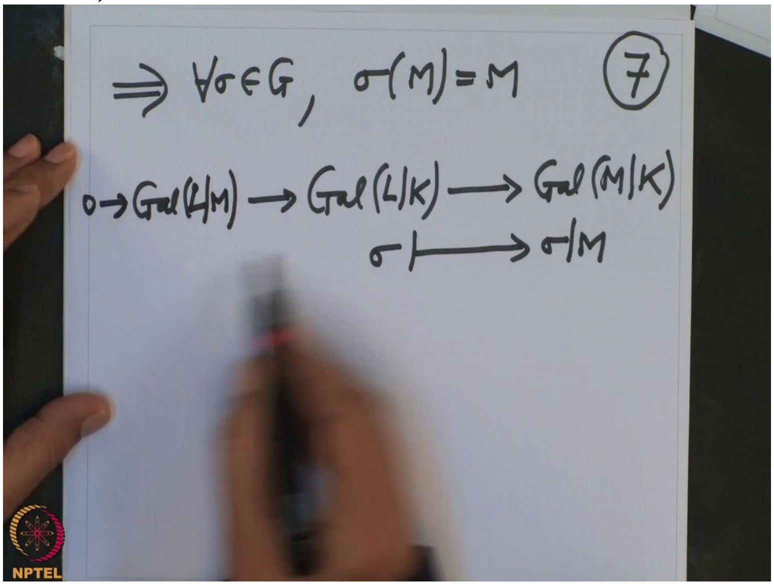
this is σ going to σ restricted to M.

(Refer Slide Time 16:44)



This makes sense. This is group homomorphism and kernel is precisely $Gal(L|M)$, this is a subgroup here

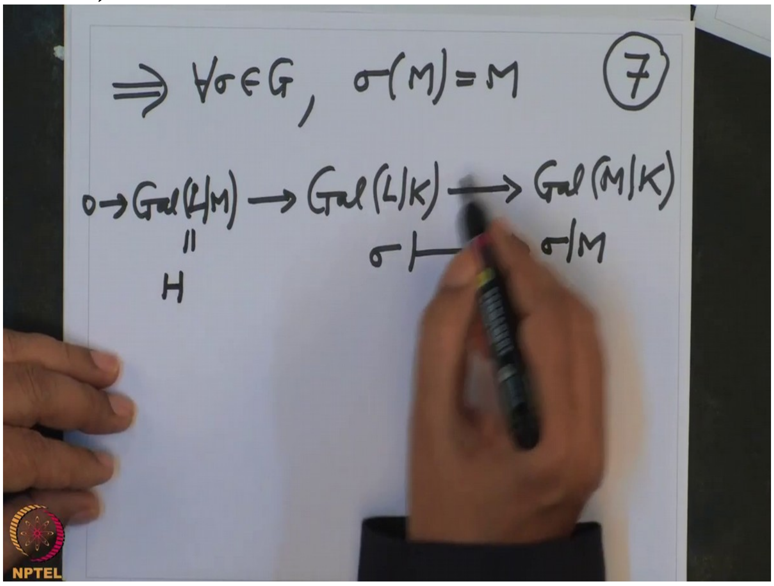
(Refer Slide Time 16:58)



so this sequence is exact means this kernel of this map is precisely this.

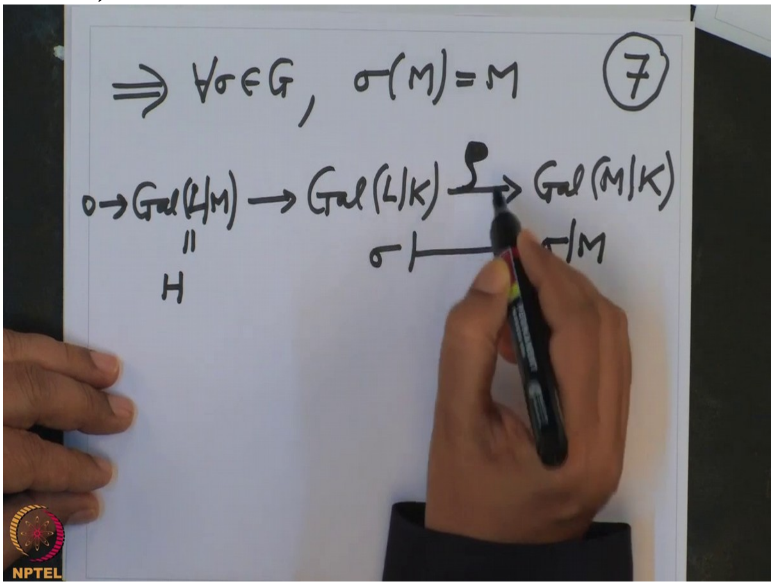
So this was our H. So if you call

(Refer Slide Time 17:08)



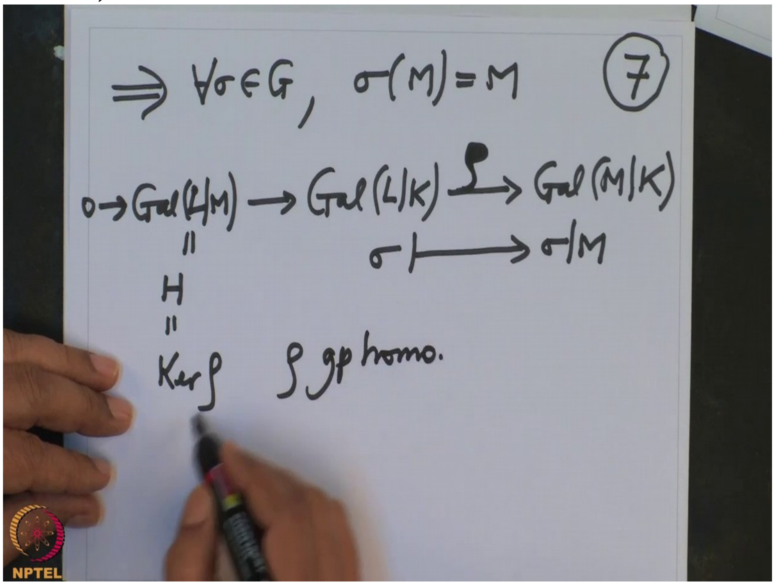
this map as, this is a restriction map. So this is r or rho.

(Refer Slide Time 17:16)



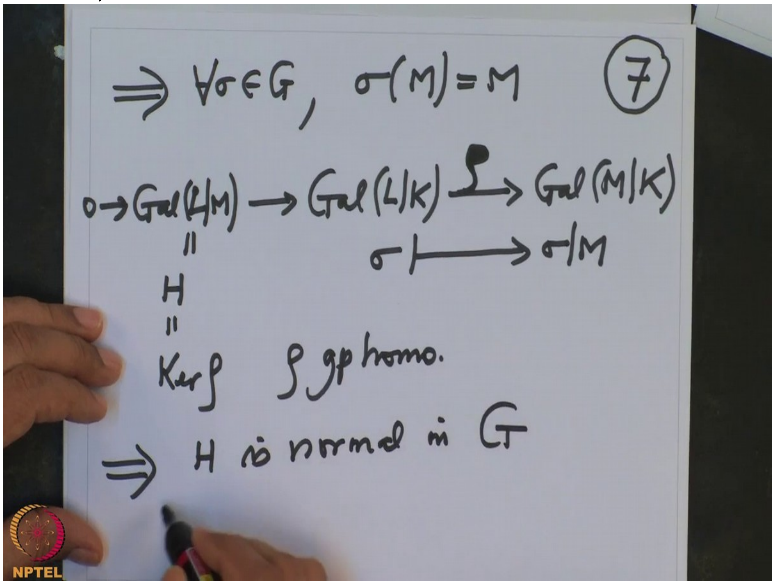
This rho is, so H is, we have proved H is kernel of rho, rho is group homomorphism.

(Refer Slide Time 17:25)



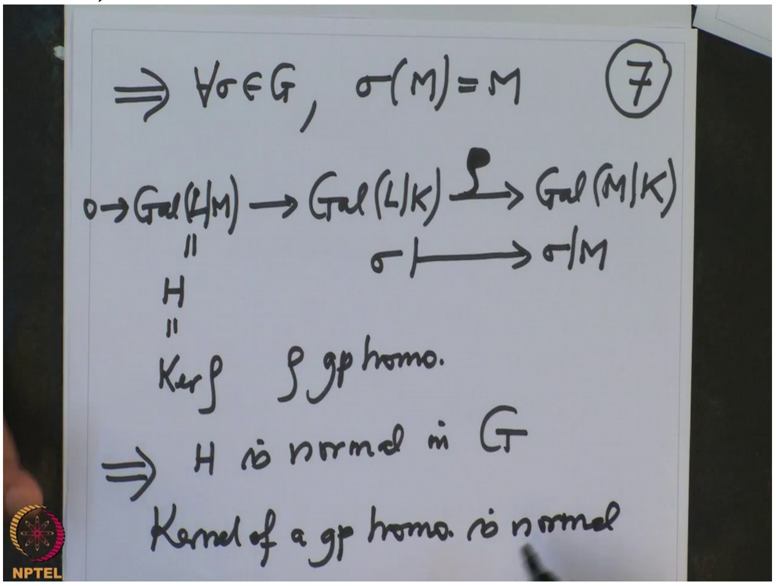
So therefore in particular H is normal in G because

(Refer Slide Time 17:33)



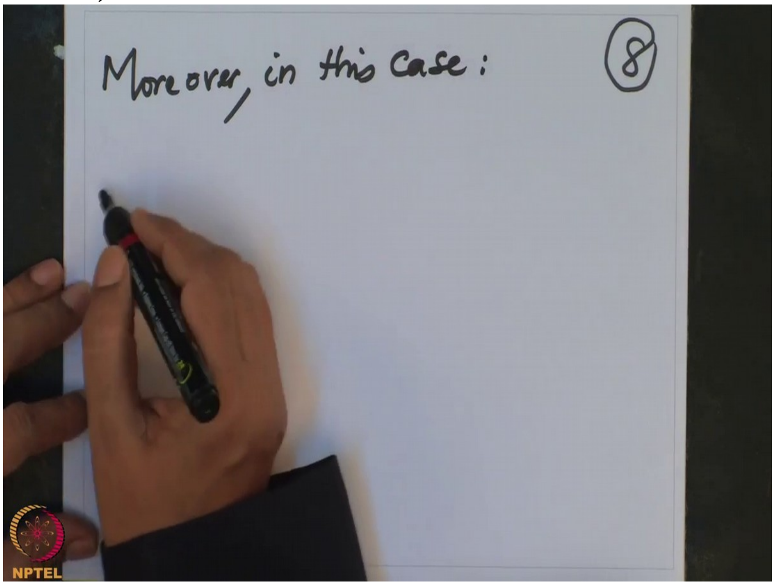
kernel of group homomorphism, group homomorphism is normal.

(Refer Slide Time 17:45)



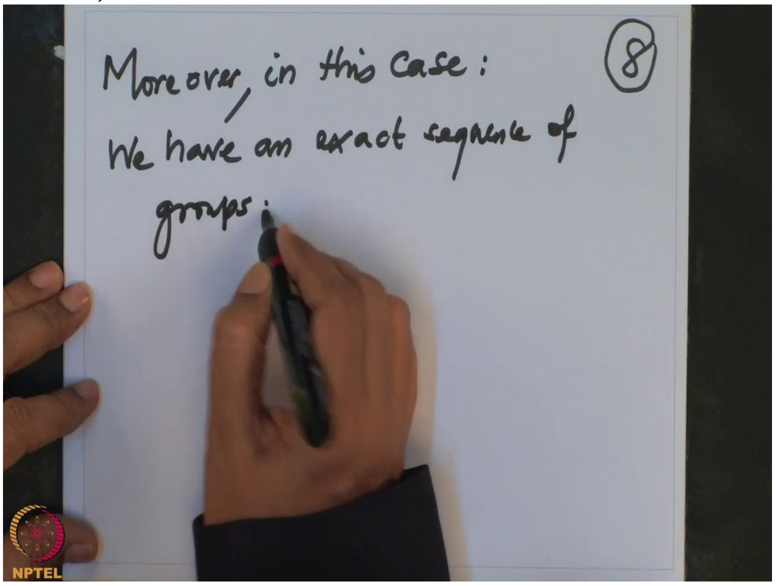
So we have proved that Galois group of L over M is normal if and only if M over K is a Galois extension. Moreover in this case, moreover in this case we have

(Refer Slide Time 18:03)



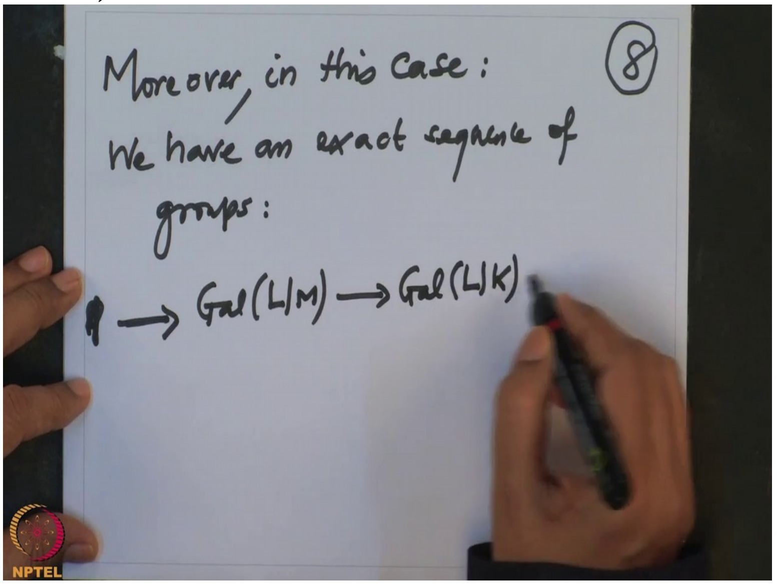
an exact sequence of groups. We have an exact sequence of groups, which one?

(Refer Slide Time 18:18)



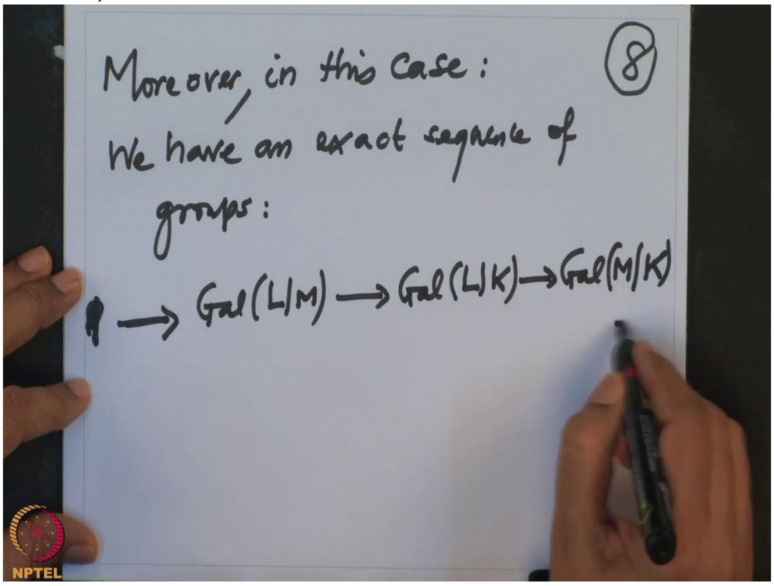
1, all the groups are written multiplicatively so 1 is identity. So this is a trivial group. Then $Gal(L|M)$, $Gal(L|K)$ to

(Refer Slide Time 18:33)



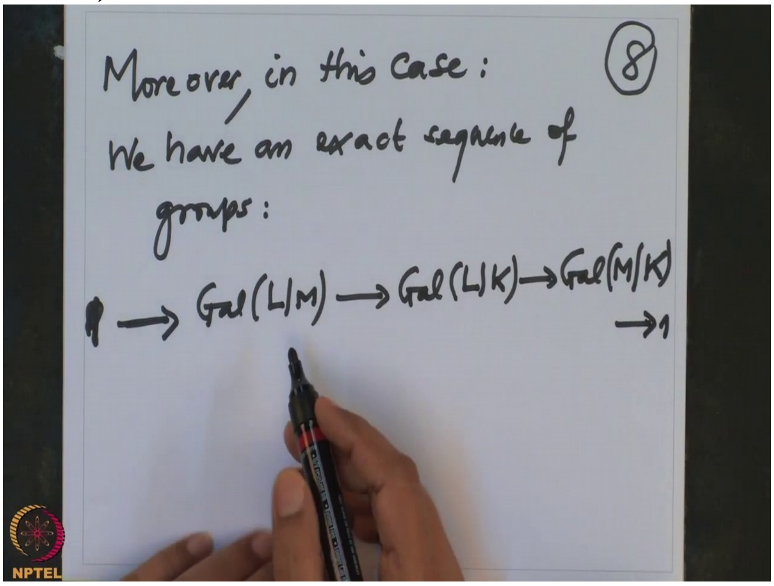
$Gal(M|K)$

(Refer Slide Time 18:38)



to 1. Now let me explain this

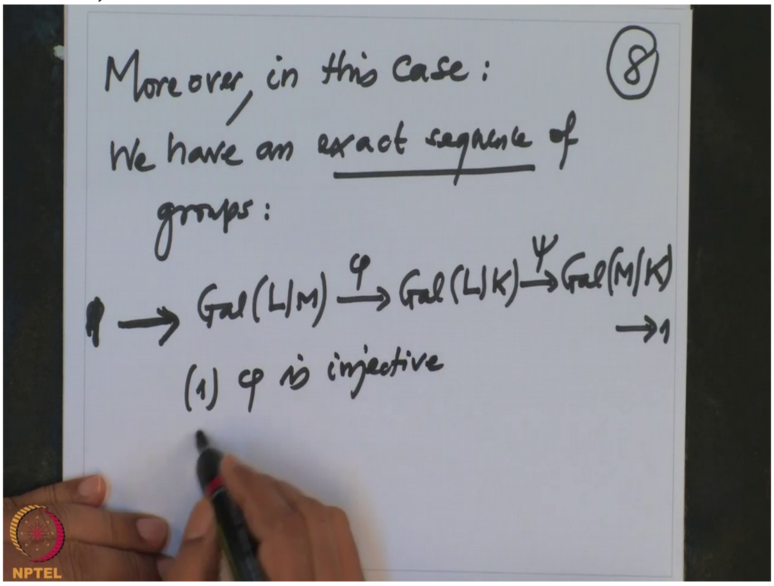
(Refer Slide Time 18:40)



terminology exact sequence. That means what, first of all that means, this means 3 things.

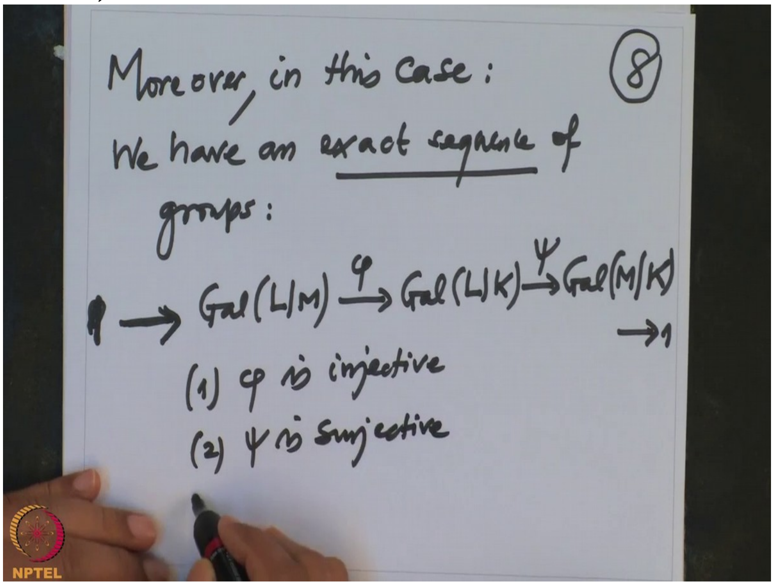
Number one, the first map is injective. So let me give the names now. This has, this is phi, this is psi. So phi is injective,

(Refer Slide Time 19:03)



two this psi is surjective

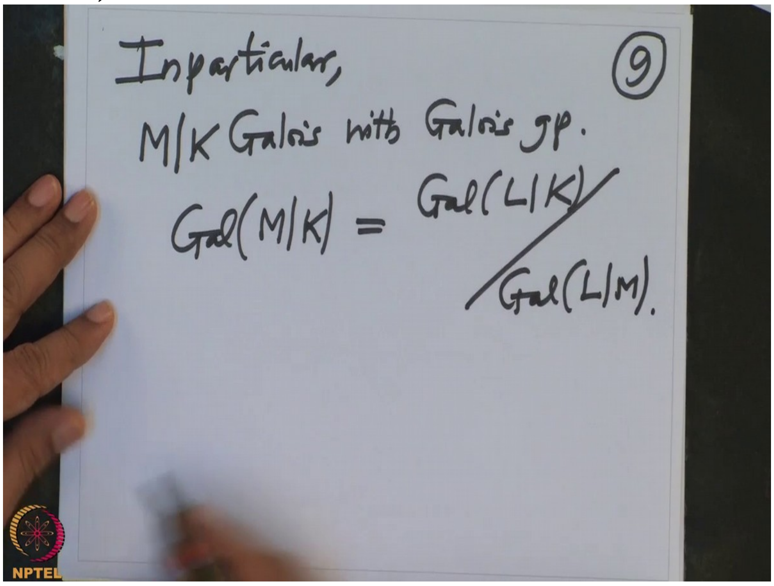
(Refer Slide Time 19:10)



and three the kernel here, kernel of psi equal to image of phi. These three things mean this sequence is exact.

So this, this is a quotient group of this, of this Galois group so in particular, so I will write in particular M over K Galois with Galois group this is $Gal(M|K)$ which is Galois group of L over K modulo the normal subgroup $Gal(L|M)$. This is what we have got.

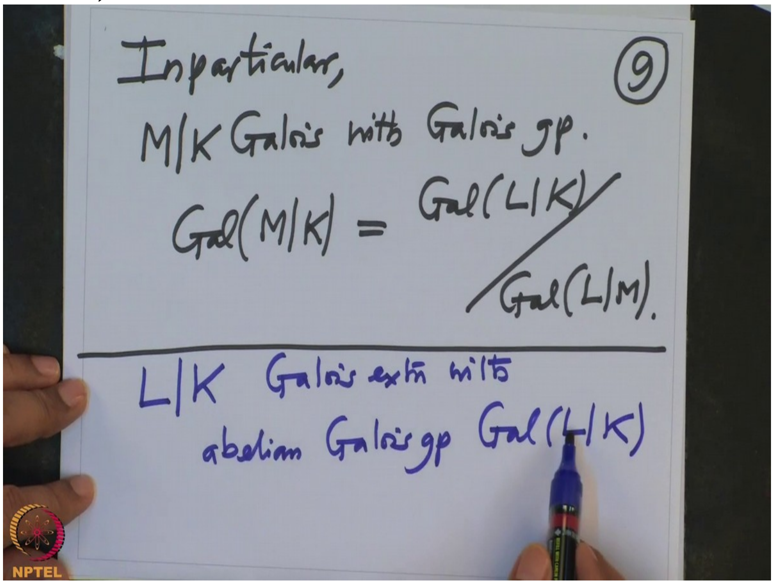
(Refer Slide Time 20:03)



This is very, very important. You will see I want to deduce many consequences from here. So in particular when can we apply this theorem? So in particular we will apply, we can always apply this theorem for Galois extensions, Galois extensions, finite Galois extensions always, with abelian Galois, $Gal(L|K)$.

Whenever the Galois group of the field extension, Galois extension

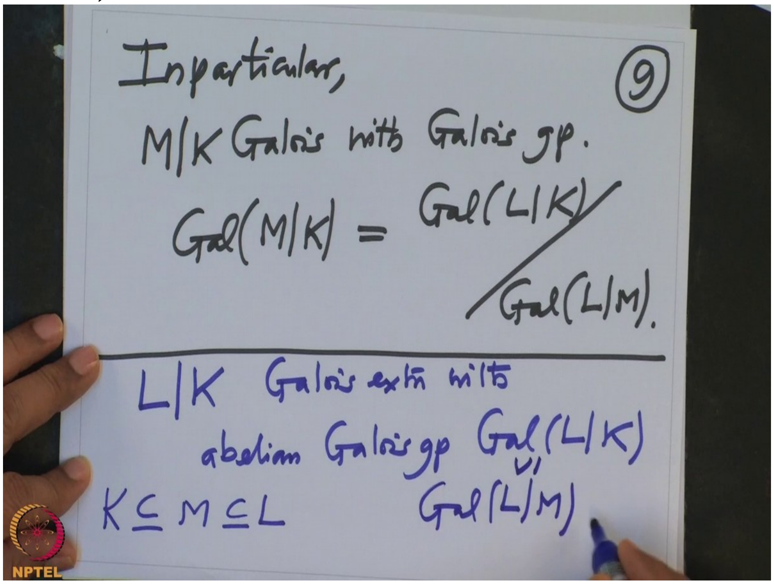
(Refer Slide Time 20:46)



is abelian then we can apply this theorem. Because in case of abelian group every subgroup is normal. Therefore, therefore every subextension will be Galois extension in this case and we can apply the above theorem.

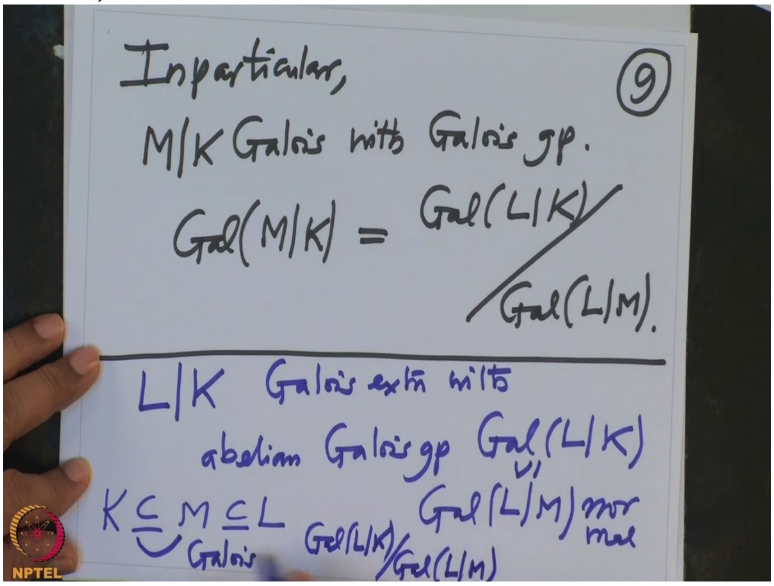
So for every subextension M in between, the Galois group of L over M, because this is a subgroup here,

(Refer Slide Time 21:14)



this is normal and therefore this extension is Galois and the Galois group will be the quotient group. Mod $Gal(L|M)$,

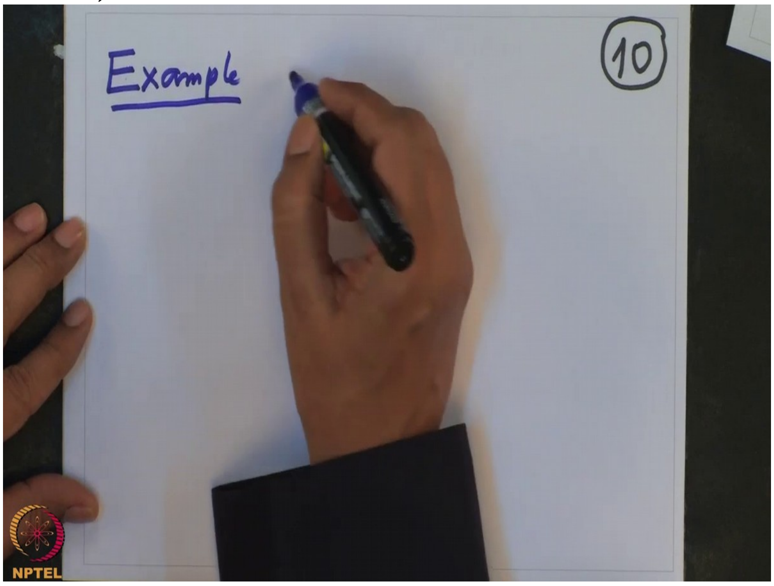
(Refer Slide Time 21:31)



this is precisely the Galois group of this extension. This is very important.

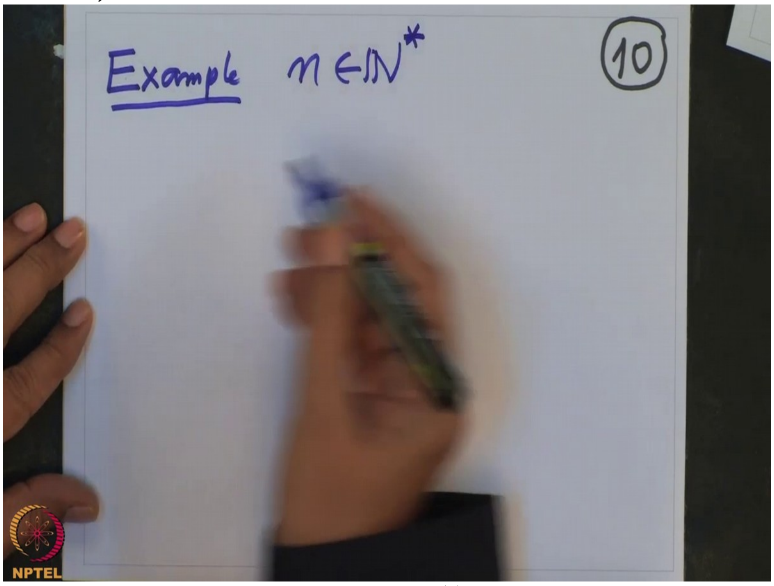
And now let me remind you we have readily one extension here, so let me write it as an example. Remember

(Refer Slide Time 21:51)



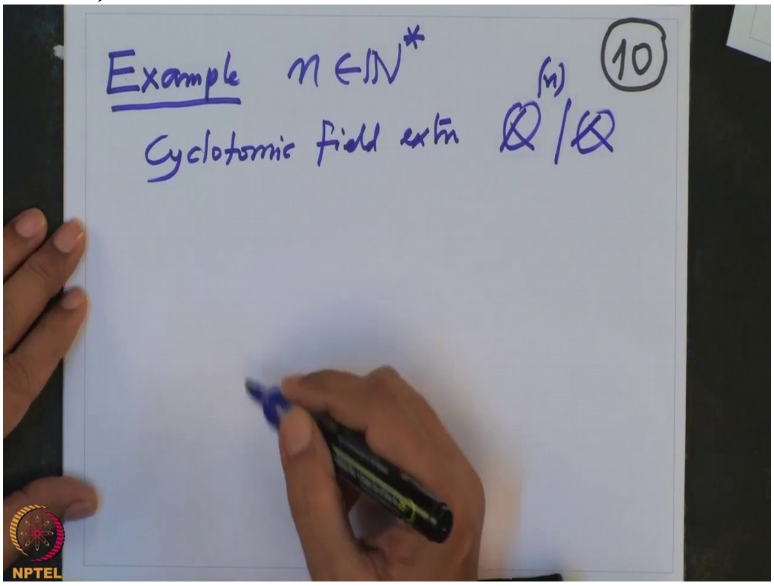
for a non-zero natural number n

(Refer Slide Time 21:55)



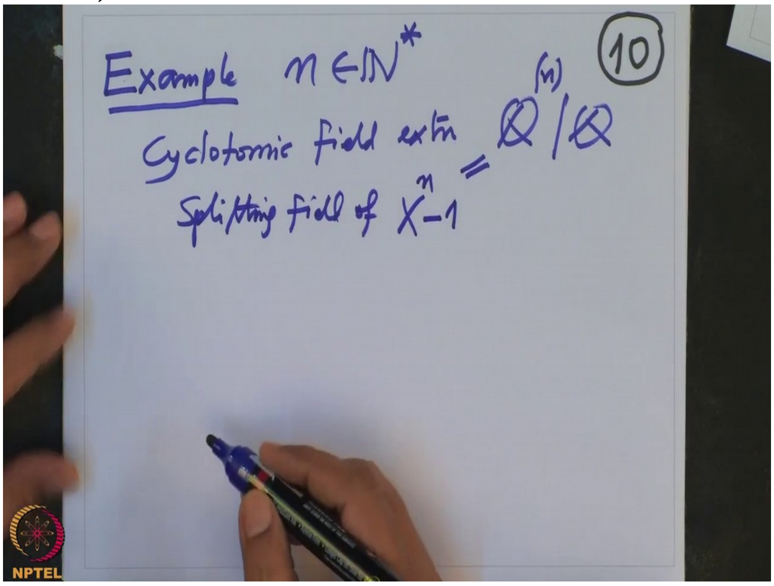
we have considered cyclotomic field extension $\mathbb{Q}^{(n)}$ over $\mathbb{Q}$.

(Refer Slide Time 22:10)



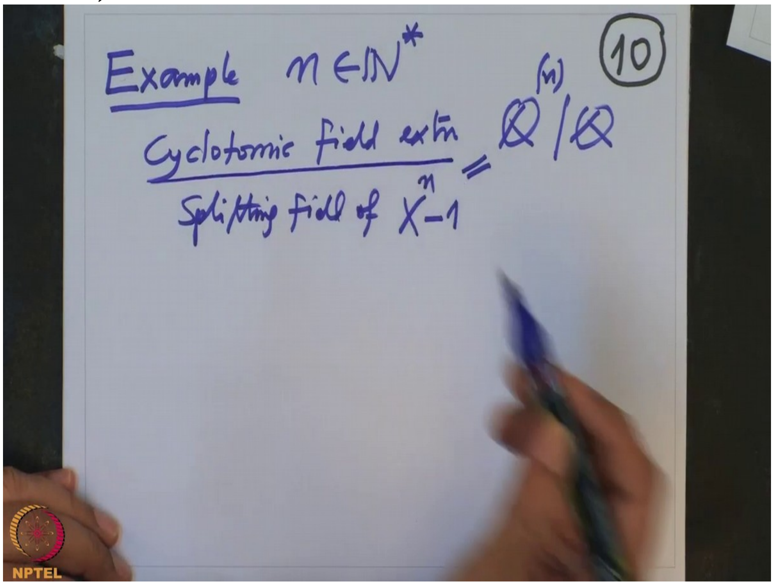
This is the splitting field of, splitting field of the polynomial $X^n - 1$.

(Refer Slide Time 22:22)



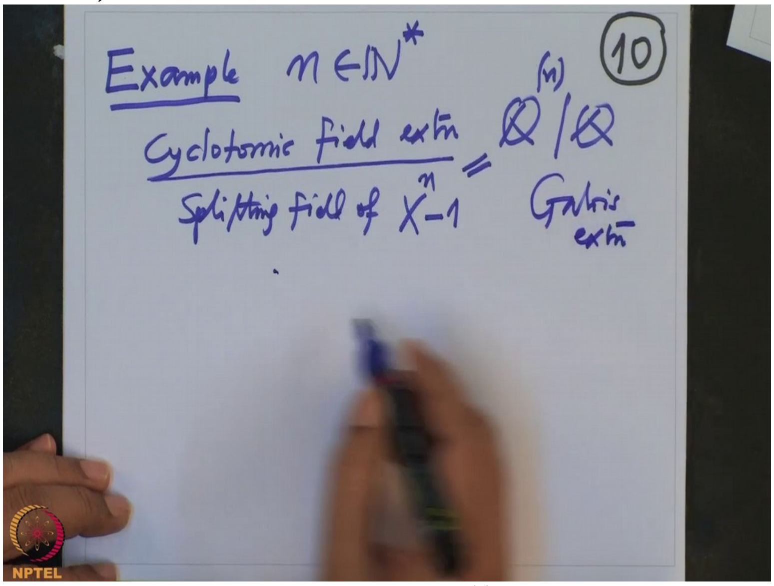
And the roots of this polynomial are precisely the roots of unity. That is why it is called as cyclotomic field extension.

(Refer Slide Time 22:30)



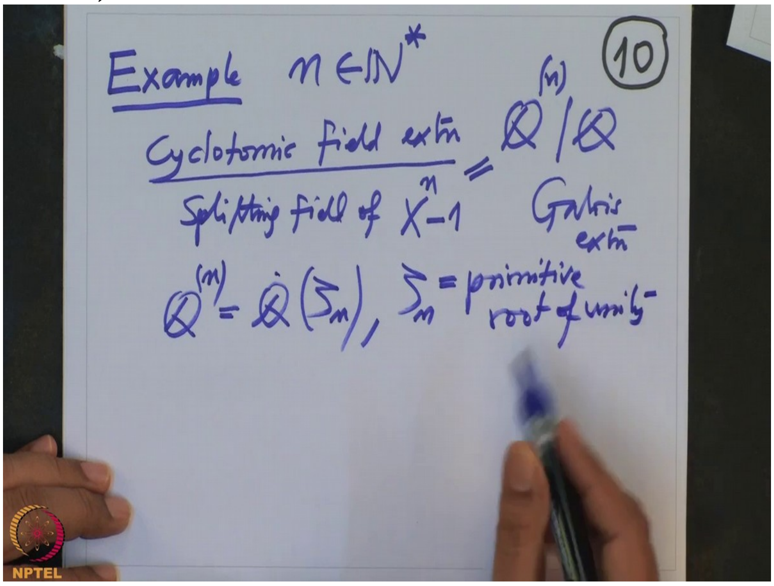
And we have seen that the Galois, this extension is Galois extension

(Refer Slide Time 22:38)



because it is simple, so this extension is simple, $\mathbb{Q}^{(n)}$ in fact is generated over $\mathbb{Q}$ by a primitive root of unity, ζ_n is a primitive root of unity

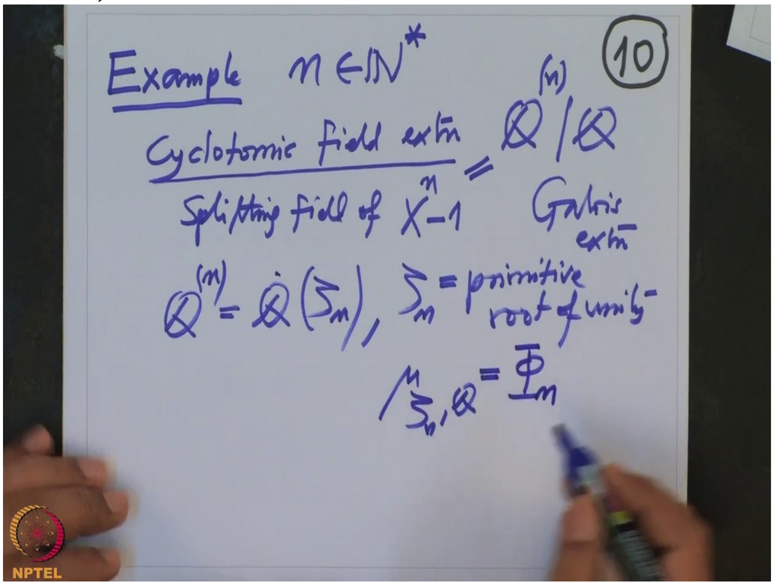
(Refer Slide Time 23:02)



which is, which has irreducible polynomial, minimal polynomial of ζ_n over $\mathbb{Q}$.

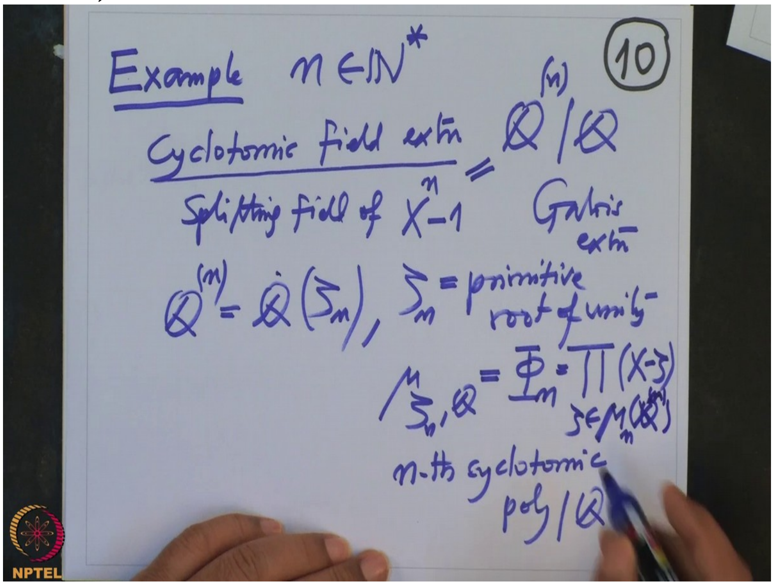
We have checked this is nothing but Φ_n. This is a n-th

(Refer Slide Time 23:13)



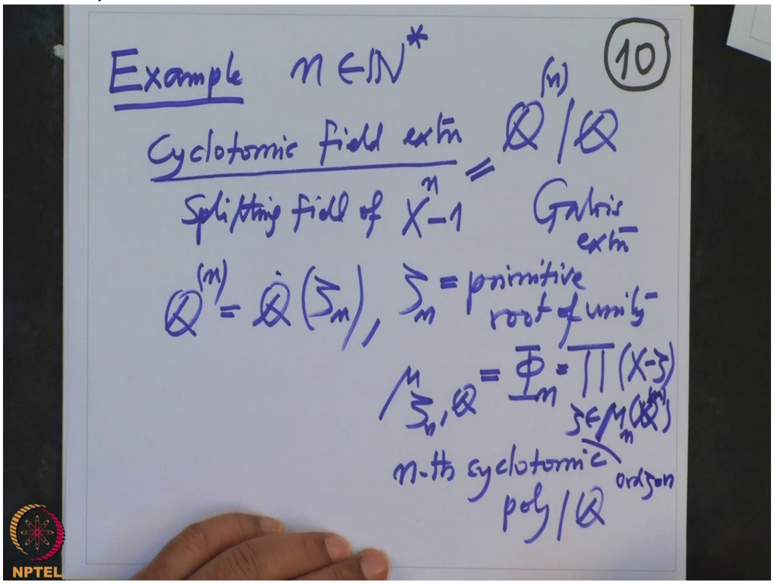
cyclotomic polynomial over $\mathbb{Q}$. This is nothing but the product of $X - \zeta$ where ζ running, of the, the root of this polynomial, it is an element in this group,

(Refer Slide Time 23:43)



and order of ζ in that group is n.

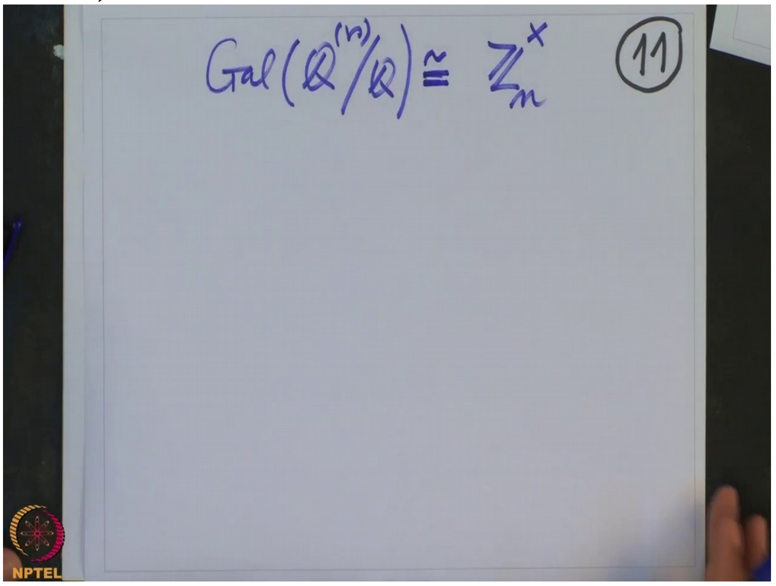
(Refer Slide Time 23:48)



And we know there are precisely $\phi(n)$ roots so degree of this Φ_n polynomial is Euler's number, Euler's number $\phi(n)$ and we have checked that the Galois group is precisely units in $\mathbb{Z}_n$. We have checked that. $Gal(\mathbb{Q}^{(n)}|\mathbb{Q})$ this is precisely units in the range $\mathbb{Z}_n$, isomorphic fields.

This is what we have checked.

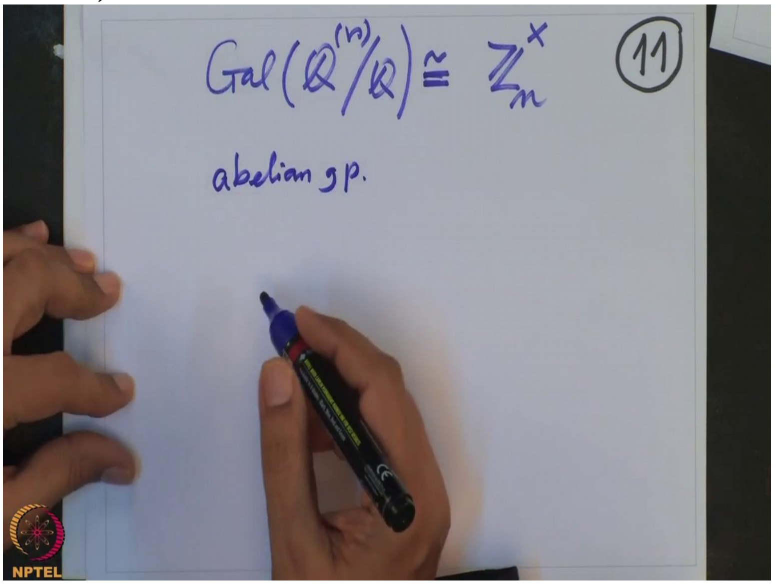
(Refer Slide Time 24:21)



For this checked we needed, we need to compute what is exactly the minimal polynomial of the primitive element of this extension over $\mathbb{Q}$ and we did it last time and then we proved that this is a group isomorphism.

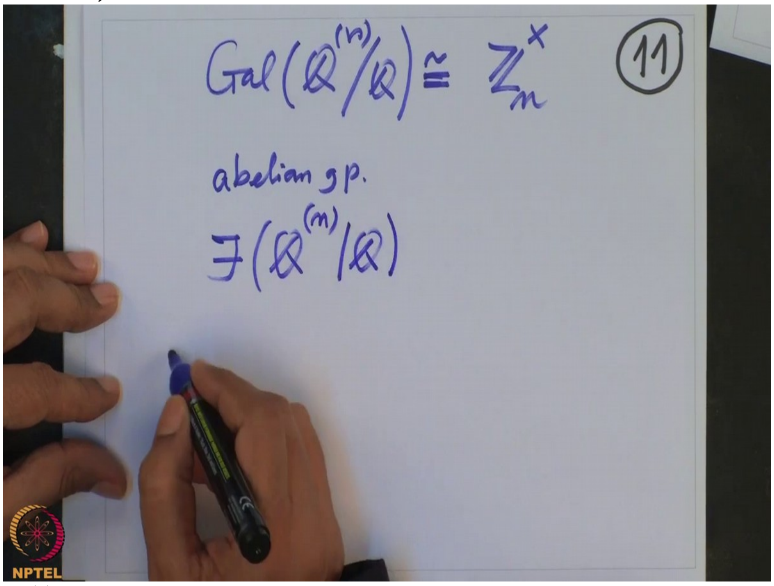
So this is an abelian group. Therefore if I take any

(Refer Slide Time 24:46)



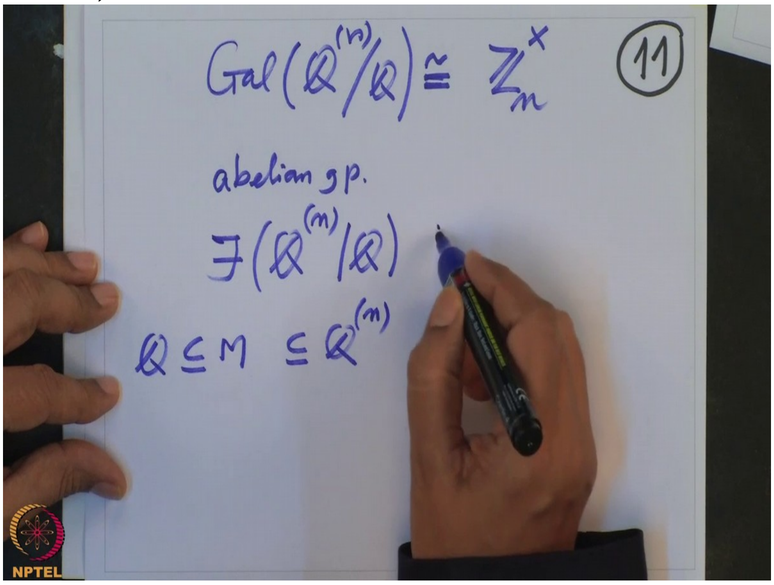
subgroup H, so now let us, let me remind you Galois correspondence in this case, that is we have here intermediary fields. So they are fields

(Refer Slide Time 25:02)



in between. So $\mathbb{Q}^{(n)}$ contained in this, they corresponds

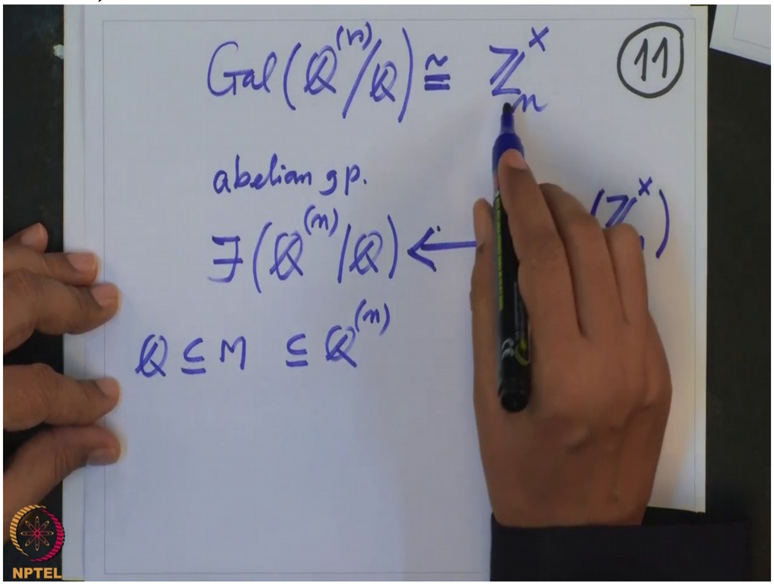
(Refer Slide Time 25:10)



to, they are both ways mapped. This is Galois correspondence.

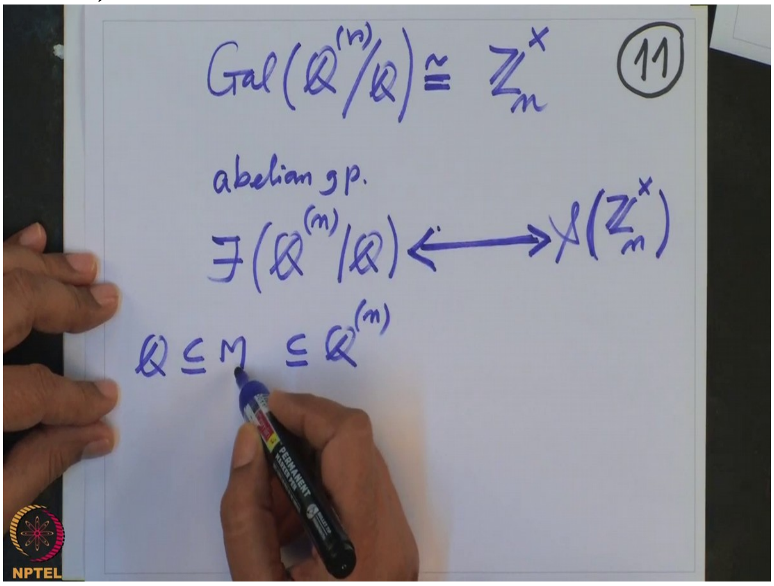
This is the subgroups of this group now, $\mathbb{Z}_n^x$. Remember this group

(Refer Slide Time 25:25)



may not be cyclic but it has subgroups. So this correspondence given any,

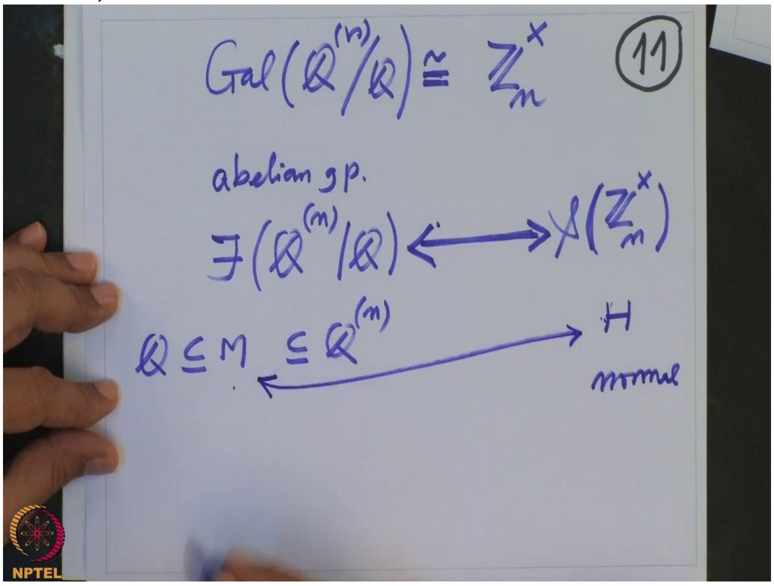
(Refer Slide Time 25:33)



because we know this is an abelian group. Therefore all subgroups H, these are normal and the subgroups H will correspond to this subextension.

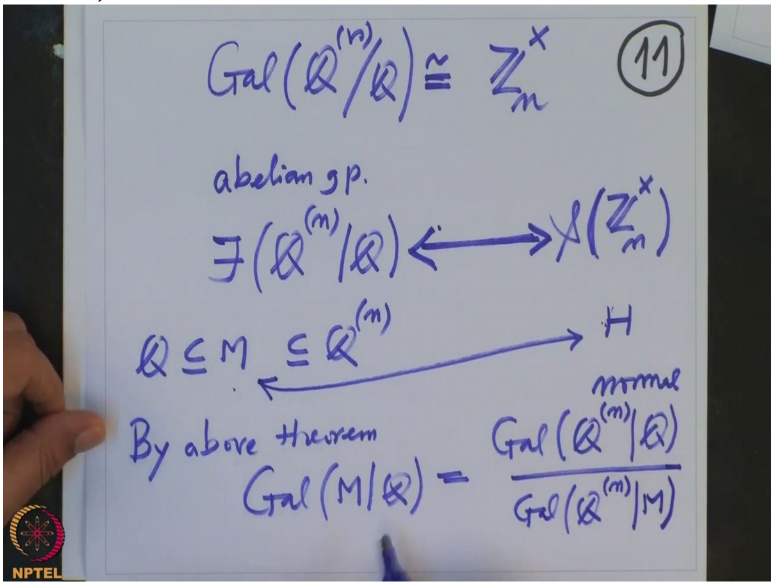
So therefore

(Refer Slide Time 25:50)



I know by above theorem Galois group of M over Q this is precisely the quotient group, $Gal(\mathbb{Q}^{(n)}|\mathbb{Q})$ modulo the group $Gal(\mathbb{Q}^{(n)}|M)$.

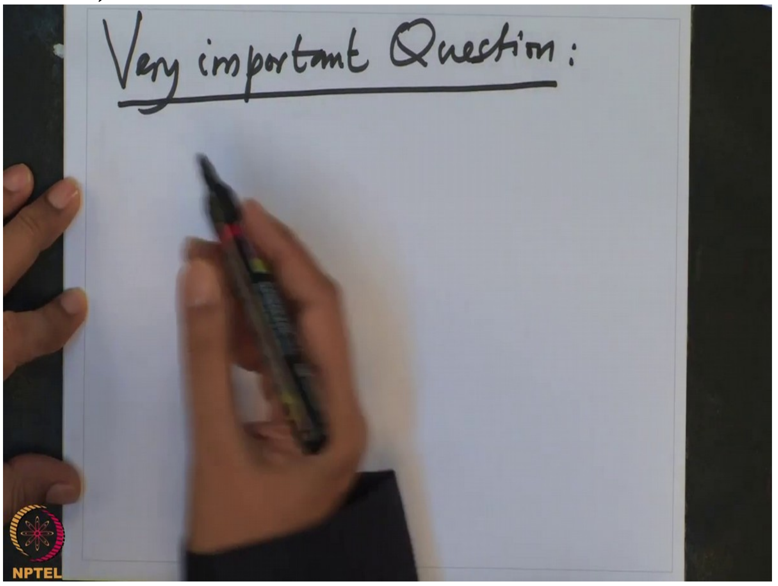
(Refer Slide Time 26:25)



So this, therefore we got it as a quotient group of this group.

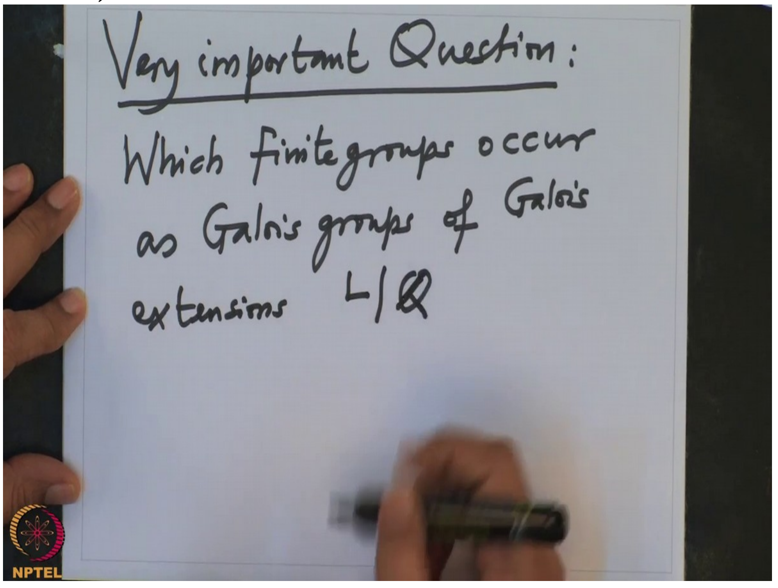
I want to use this to understand the following problem. So now this is a very, very important problem. This is in fact very important question.

(Refer Slide Time 27:07)



Which groups, which finite groups occur as Galois groups of Galois extensions L over Q, over

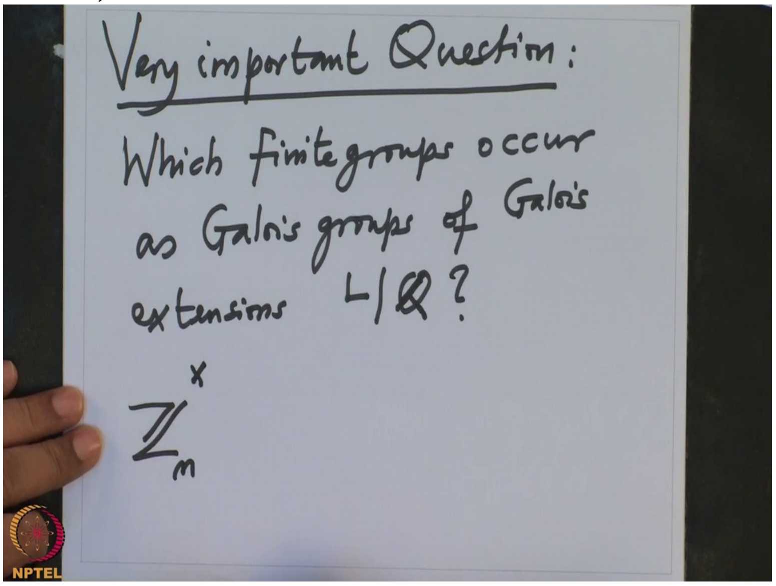
(Refer Slide Time 27:41)



Q?

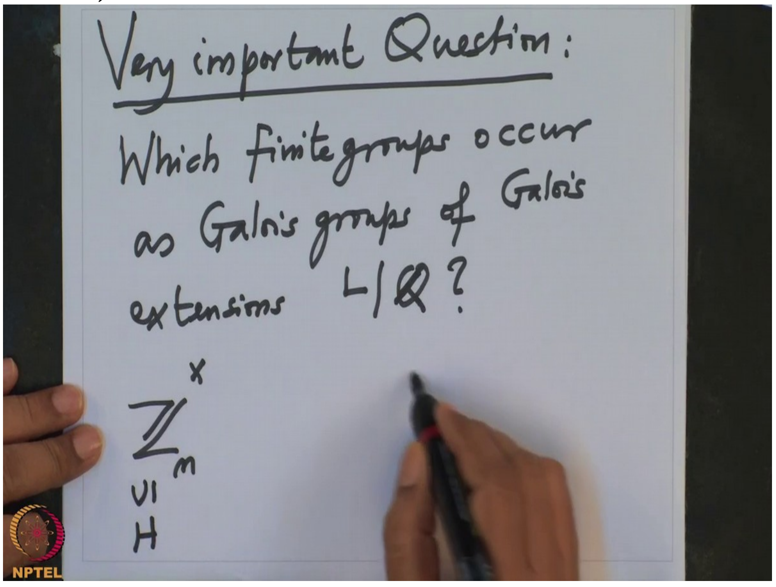
So, so far we only know all cyclic groups occur as a, no that also we do not know. Of course we know that this, this group for example $\mathbb{Z}_n^x$,

(Refer Slide Time 28:01)



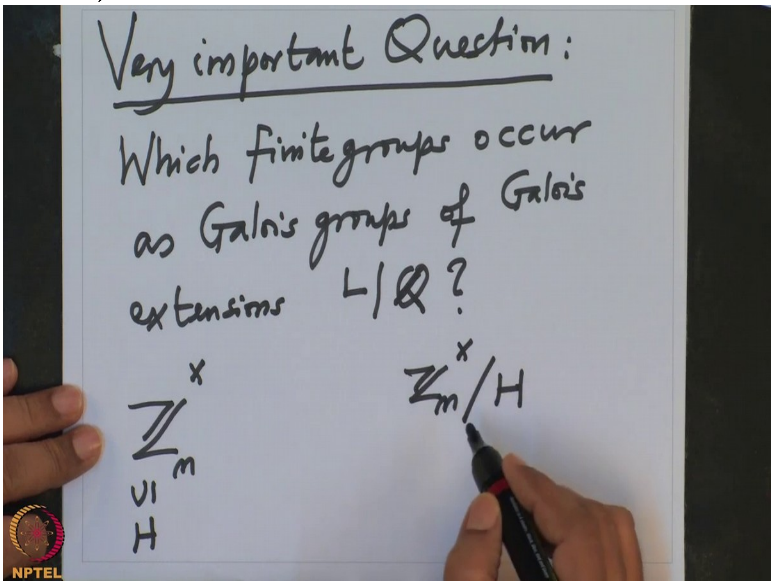
this occurs as a Galois group and also we know that the subgroups of this, we do not know, we only know that if I take any subgroup H here,

(Refer Slide Time 28:16)



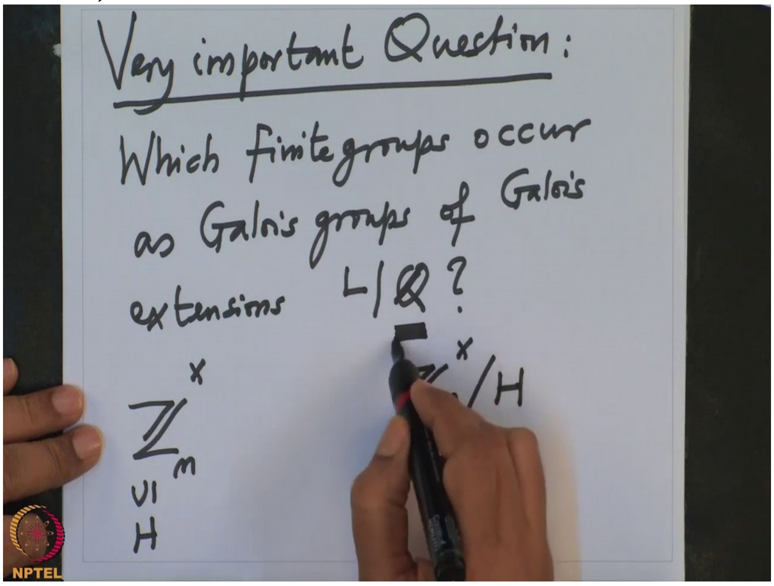
then this quotient group, that occurs as a Galois group of, Galois extension of $\mathbb{Q}$,

(Refer Slide Time 28:24)



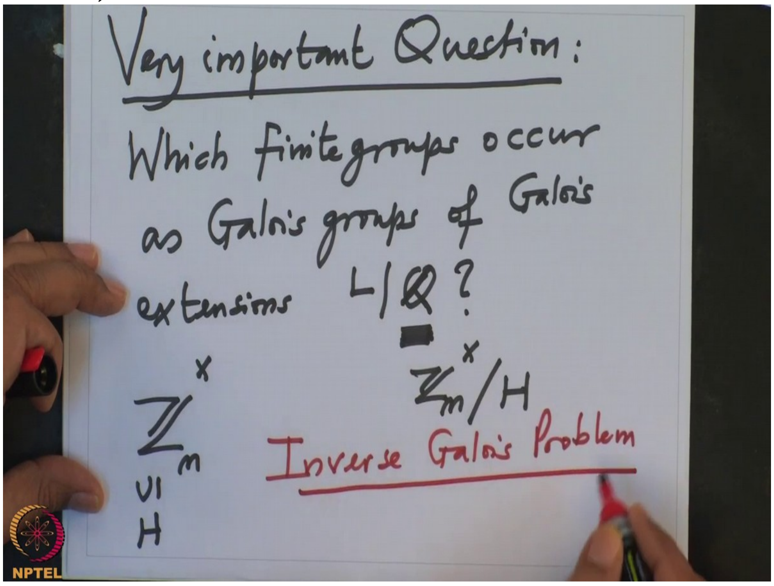
over ℚ is very important.

(Refer Slide Time 28:26)



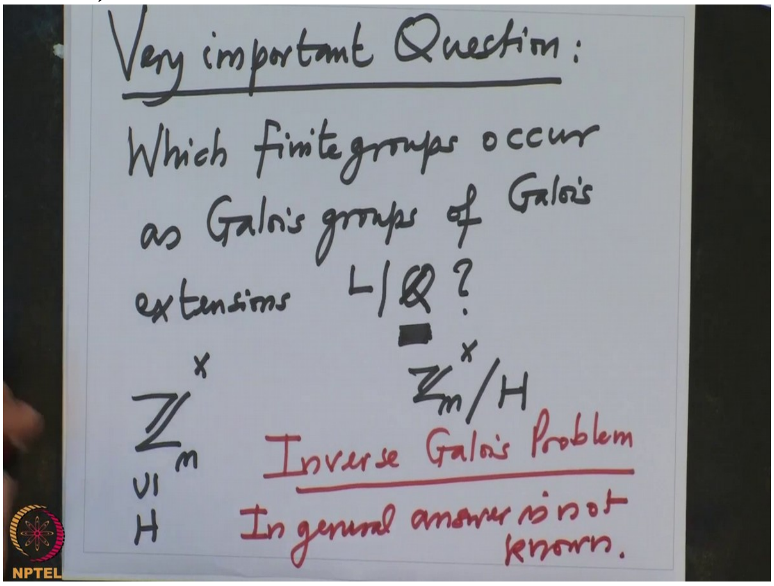
And let me tell you this, this problem is known as Inverse Galois Problem. And

(Refer Slide Time 28:44)



complete answer to this is not known. In general answer is not known but some

(Refer Slide Time 29:05)



particular cases are known.

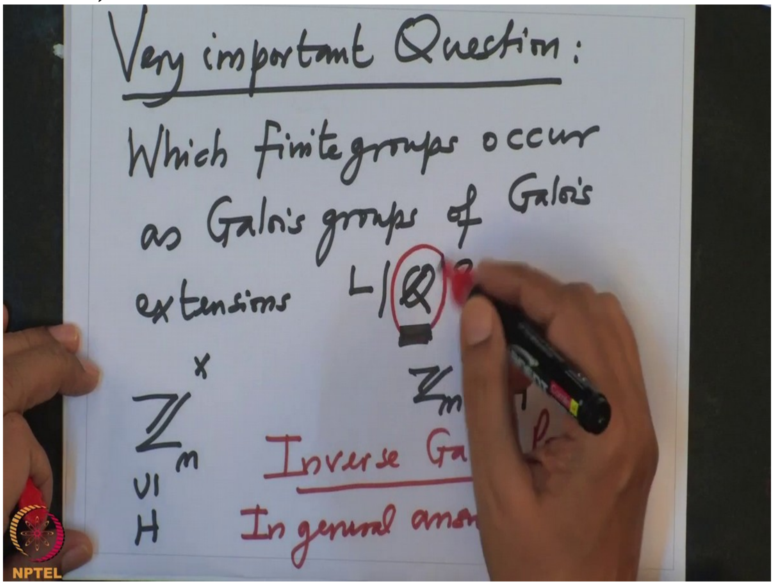
In fact this problem is one of the main, one of the frontline research problem in this field and it not only involves Galois Theory, it also involves the other subjects like number theory, algebraic topology, algebraic geometry and commutative algebra.

So this problem is considered to be one of the very difficult problems but also it is a very good frontline research area for the young researchers. This is not, this cannot, I cannot say this is a Ph D thesis problem.

This is much more than that but this is certainly worth studying this because of its many, many applications and many connections with the different fields of mathematics.

So with this I will stop and next time I will start preparing to show you how we can realize arbitrary abelian, arbitrary finite abelian group as a Galois group of L over $\mathbb{Q}$, over $\mathbb{Q}$ is very important. I will show you also

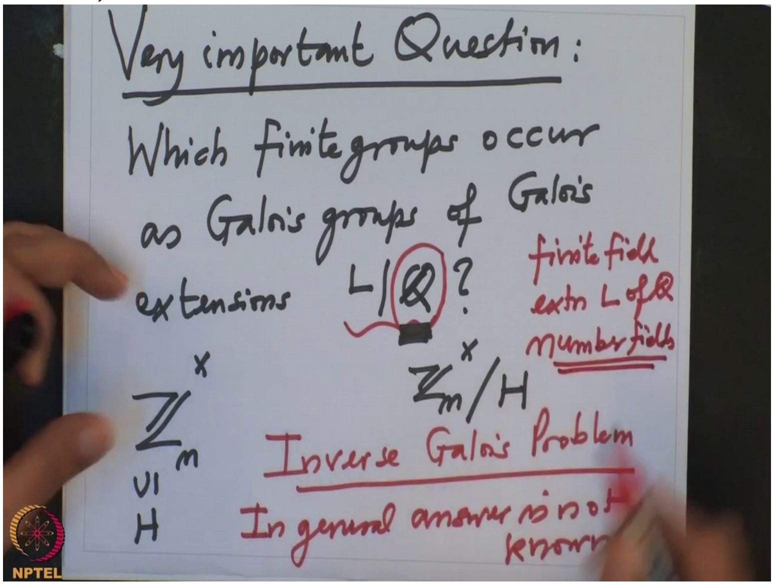
(Refer Slide Time 30:22)



that if you do not demand this base field to be $\mathbb{Q}$, then it is not so difficult.

But for $\mathbb{Q}$ it is more difficult and such fields are also called number fields. So these are called finite extension, finite field extension L of $\mathbb{Q}$, they are called number fields.

(Refer Slide Time 30:51)



So when can finite abelian group, when can arbitrary finite group be a Galois group of a number field; that is the main question.

And I will show you that every finite abelian group is, we already have enough machinery to show you that every finite abelian group is a Galois group of a number field over $\mathbb{Q}$.

And I will show you the other groups like symmetric group S_n or the alternating group A_n , they are also Galois groups of number field over $\mathbb{Q}$. This I will show you explicitly in coming lectures.

That will require

(Refer Slide Time 31:36)

some preparation but it is well within this course and we shall do it. So with this I will stop this lecture and continue working on this next time, thank you.