Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 40
Digression on group action II

(Refer Slide Time 00:25)

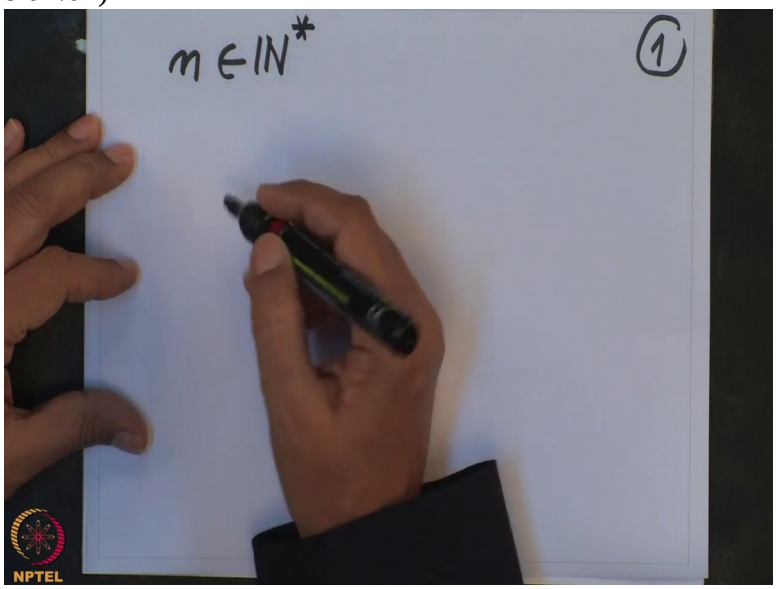
In the last couple of lectures we have been studying Galois groups of some examples of

(Refer Slide Time 00:33)

field extensions which are Galois extensions and particularly last 2 lectures we have spent on studying roots of unity in a extension of $\mathbb{Q}$ and also in a extension of finite fields.

So just let me roughly recall quickly that what we studied was, given any integer natural number n positive then we were

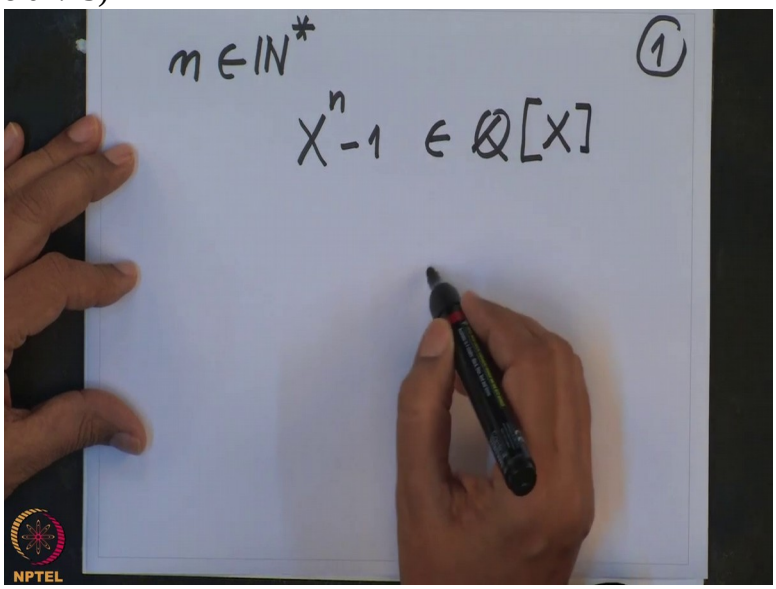
(Refer Slide Time 01:07)



studying this equation, roots of this equation $X^n - 1$.

So we have two cases, either characteristic 0, characteristic 0 case that is think of this as a polynomial in $\mathbb{Q}[X]$. That was the case 1.

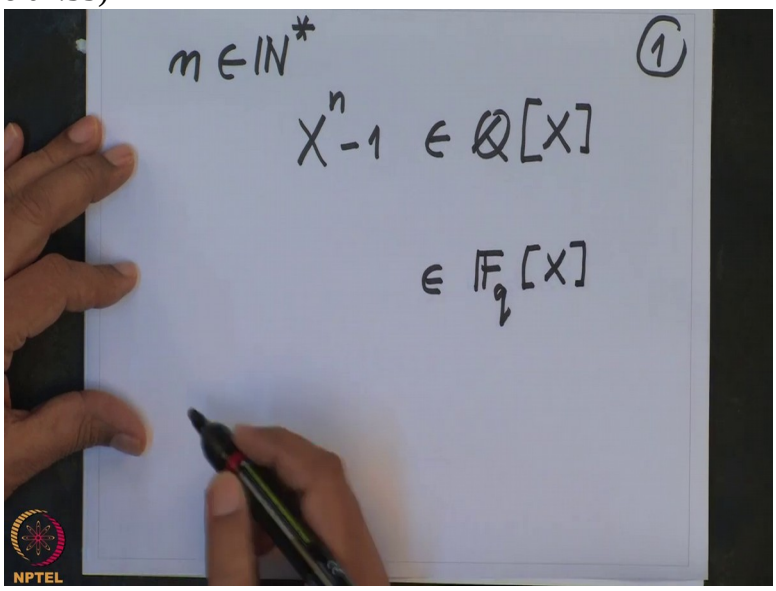
(Refer Slide Time 01:25)



Or think of this as a polynomial in the finite field with q elements.

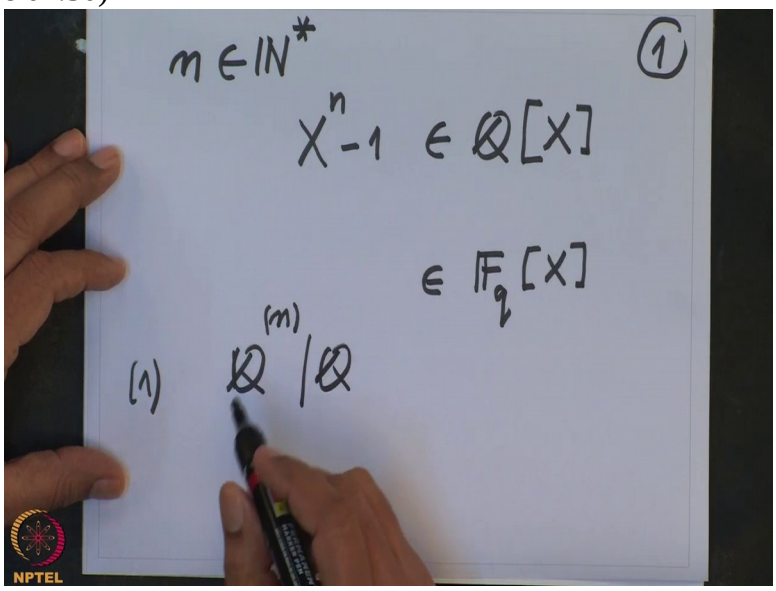
And then

(Refer Slide Time 01:33)



we consider in both the cases, in the first case the splitting field, that I have denoted by $\mathbb{Q}$ upper bracket round bracket n, this is the splitting field of this polynomial over $\mathbb{Q}$. We have checked that

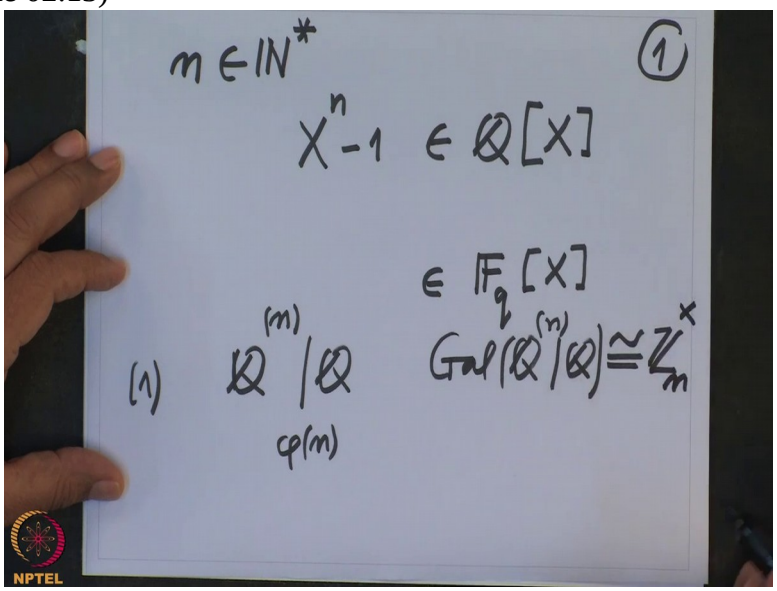
(Refer Slide Time 01:50)



this is a field extension of degree Φ_n where $\phi(n)$ is Euler's phi totient function.

And the Galois group, the Galois group of this extension is isomorphic to the unit group of the ring of

(Refer Slide Time 02:13)

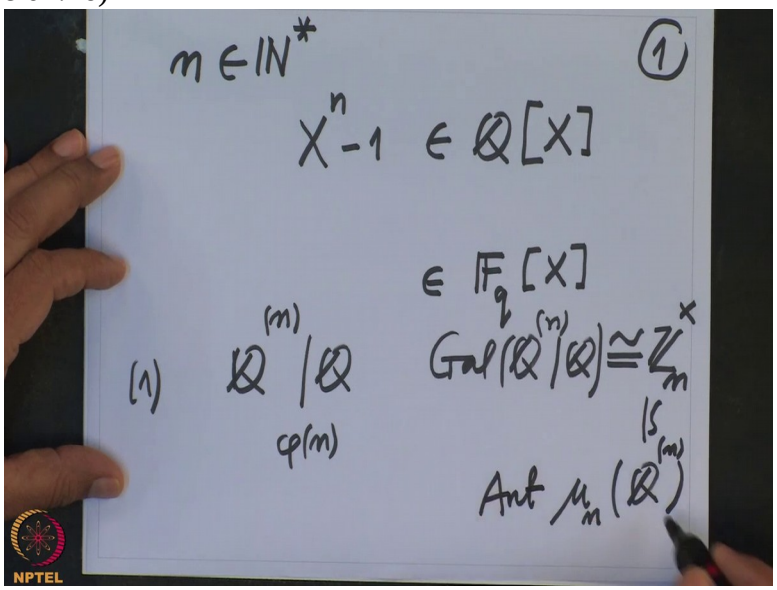


integers modulo n. This is what we proved.

And this is, we also in-between we proved that this is a Galois extension. So in this case the Galois group is actually the abelian group. It is the abelian group of order $\phi(n)$. This group we have identified it as that, the roots, the roots of unity in, in $\mathbb{Q}^{(n)}$.

This group is cyclic group of order n and automorphic group of that

(Refer Slide Time 02:46)

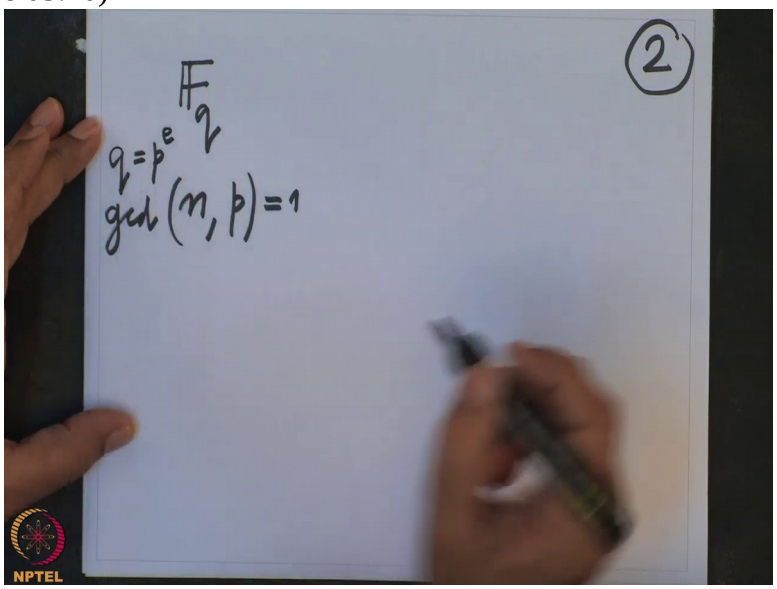


cyclic group is precisely $\mathbb{Z}_n^x$. This is what we are giving the identification. So that was a characteristic 0 case. And character p case we know that if you have a field with q elements F

q and we have to assume now, without loss we could assume this n and this q or p characteristic, this is co-prime.

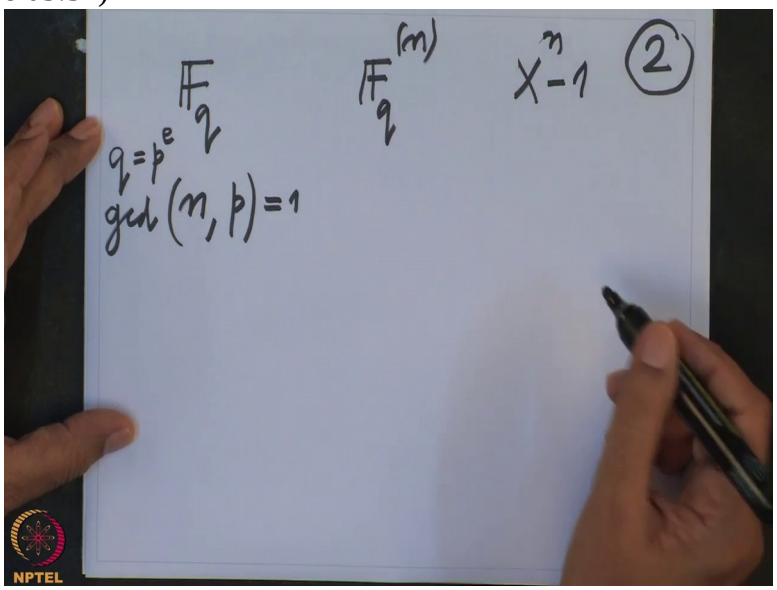
q is a power of prime, q is p^e ,

(Refer Slide Time 03:20)



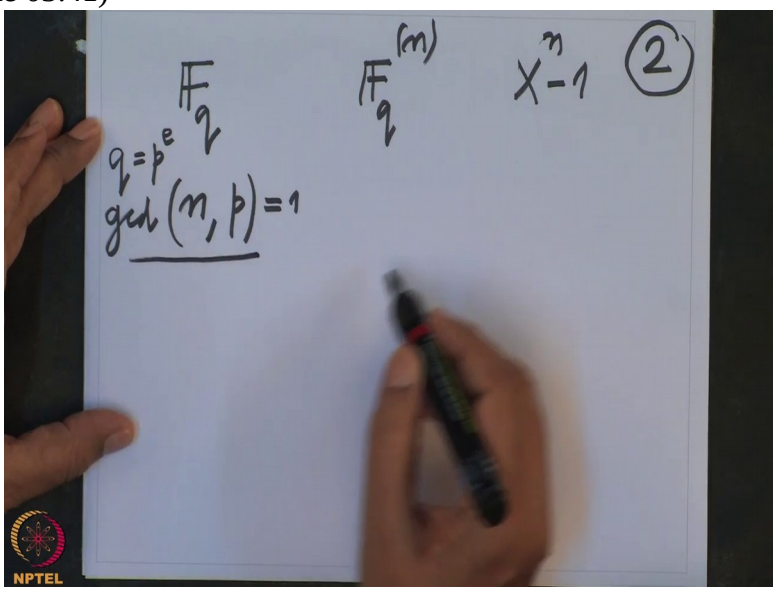
p is a characteristic and then we are looking at the splitting field of this polynomial $X^n - 1$,

(Refer Slide Time 03:31)



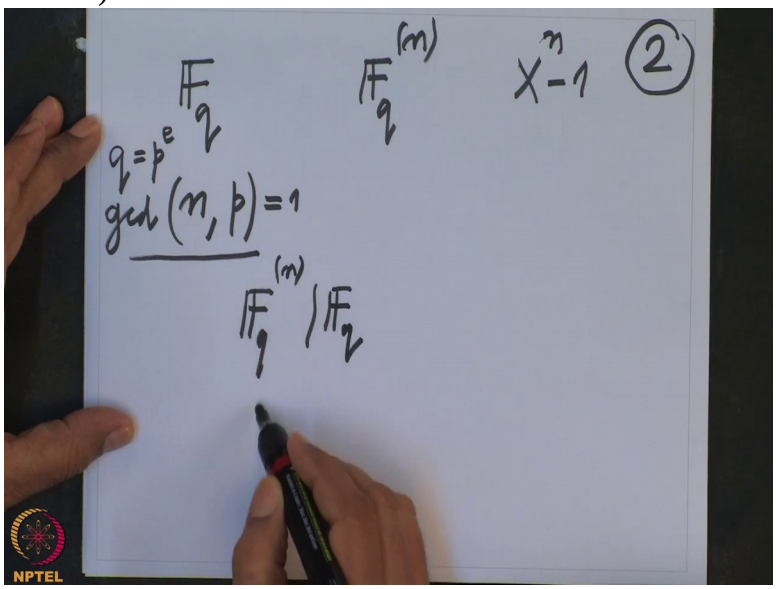
$X^n - 1$ and this polynomial is now, has simple roots because we are assuming this condition

(Refer Slide Time 03:41)



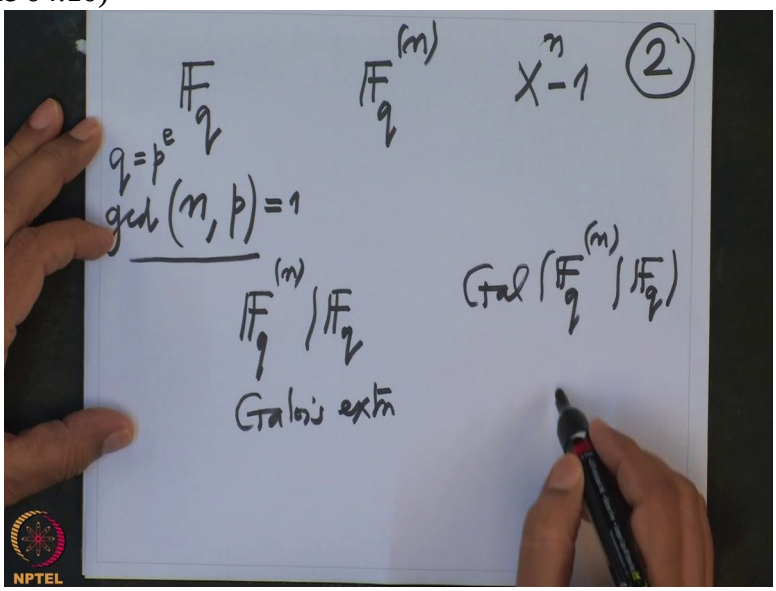
and therefore this extension is Galois extension.

(Refer Slide Time 03:49)



This is Galois and we already know finite extension, of a finite field is always cyclic, so this is Galois extension with Galois group cyclic, this is cyclic and this is only

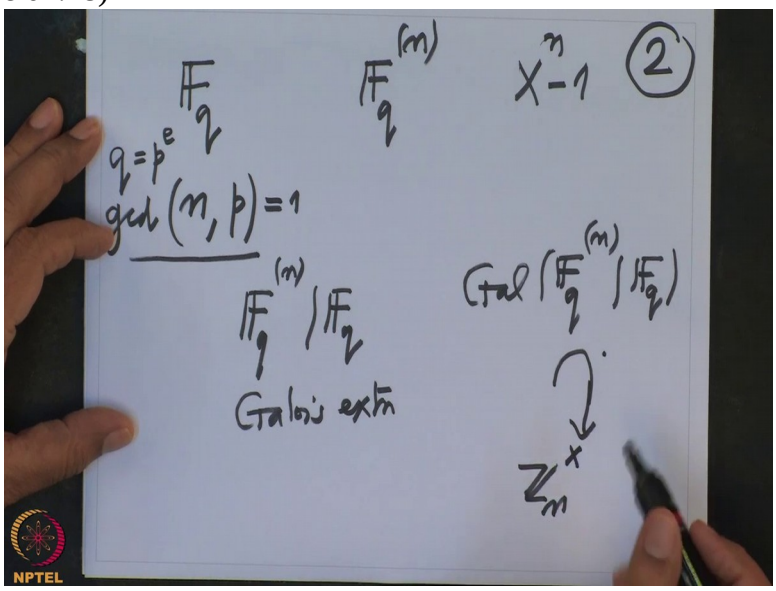
(Refer Slide Time 04:10)



a subgroup of $\mathbb{Z}_n^x$.

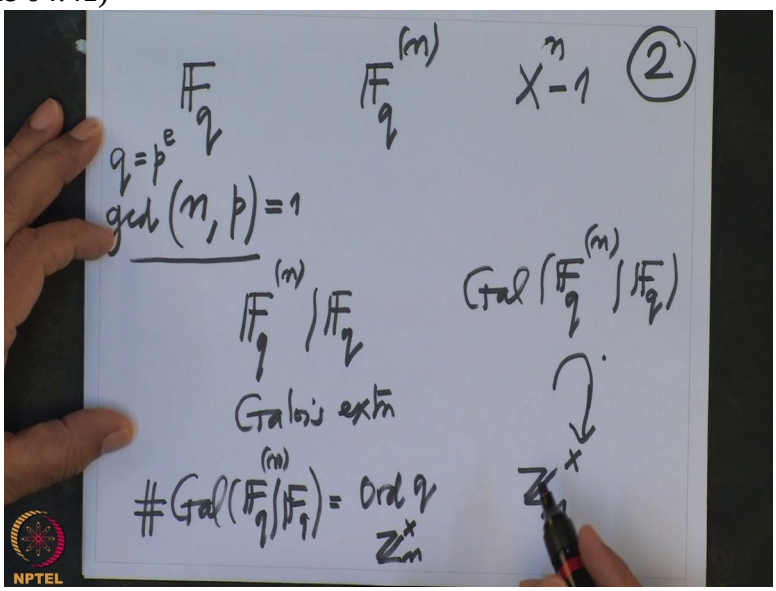
So

(Refer Slide Time 04:18)



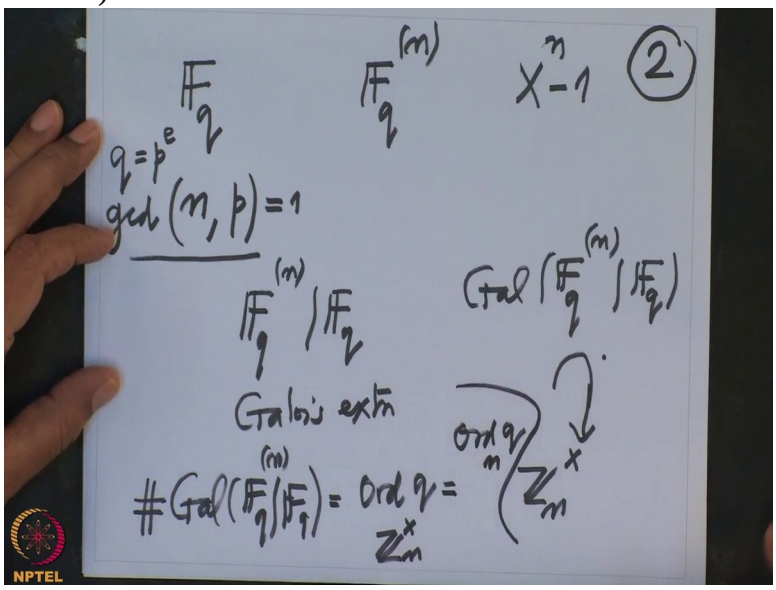
the order of this Galois group we computed, the order of the Galois group, order of this Galois group which is also order of the field extension, this order is precisely the order of the integer q in the group $\mathbb{Z}_n^x$

(Refer Slide Time 04:41)



So that is also, I denoted by order of q in mod n, in a multiplicative group.

(Refer Slide Time 04:50)

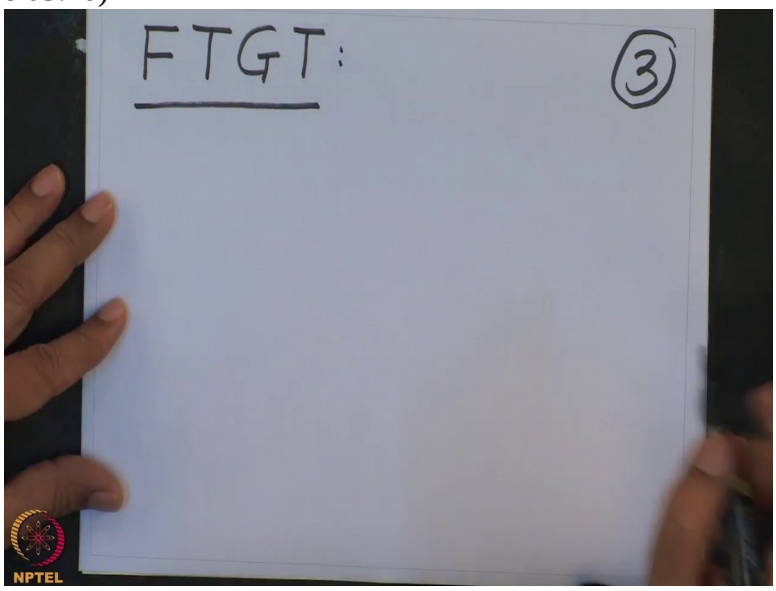


So we have fairly good understanding of this field extensions. Now I want to go on further little more intricate results which will tell us about which groups occur as Galois groups.

This is still vague. I will make it more and more precise when we go on. And we want to therefore, extend or do more finer study about the Galois correspondence. So let me recall quickly what is the Galois correspondence we did.

So this was a main theorem; that was a fundamental theorem of Galois Theory. So that I will abbreviate always as I said also, F T G T, this is the fundamental theorem of Galois Theory.

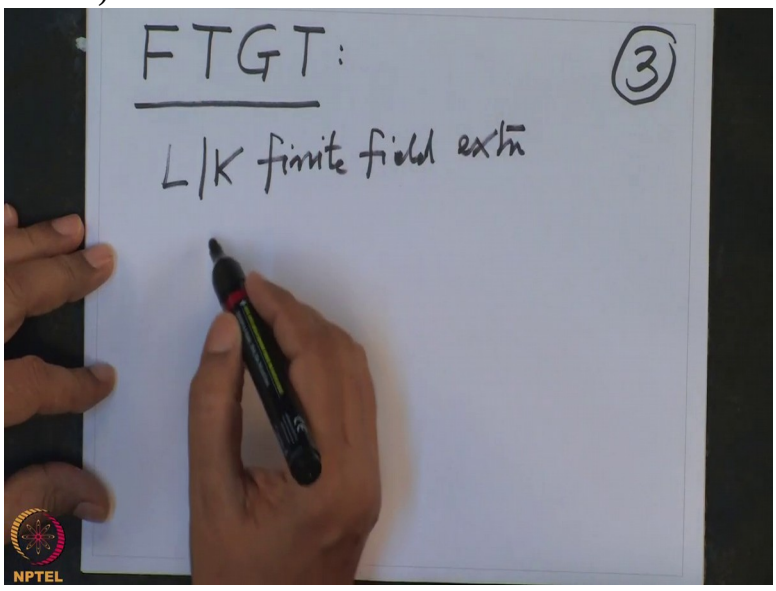
(Refer Slide Time 05:40)



And what we proved was when we have a field extension, we did it only for finite field extension and if time permits in this course I will go on to more general field extensions. Not even I do not even want to; I will assume that it is an algebraic extension, not even finite etc. But that will come probably at the end or if not, it will be in the further next course, alright.

So we have a field extension L over K, finite field extension, finite field extension and remember we called

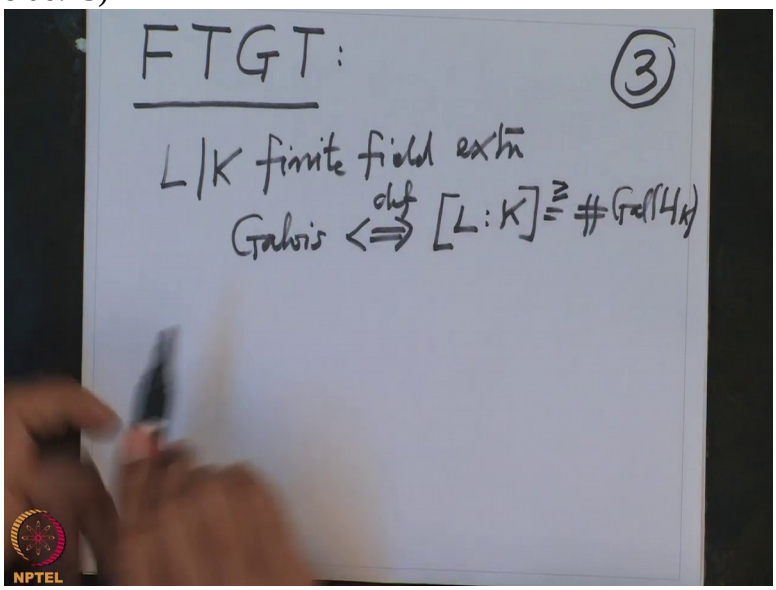
(Refer Slide Time 06:22)



it Galois extension. That was the definition was, that was the degree of the field extension equal to the order of the Galois group, $Gal(L|K)$.

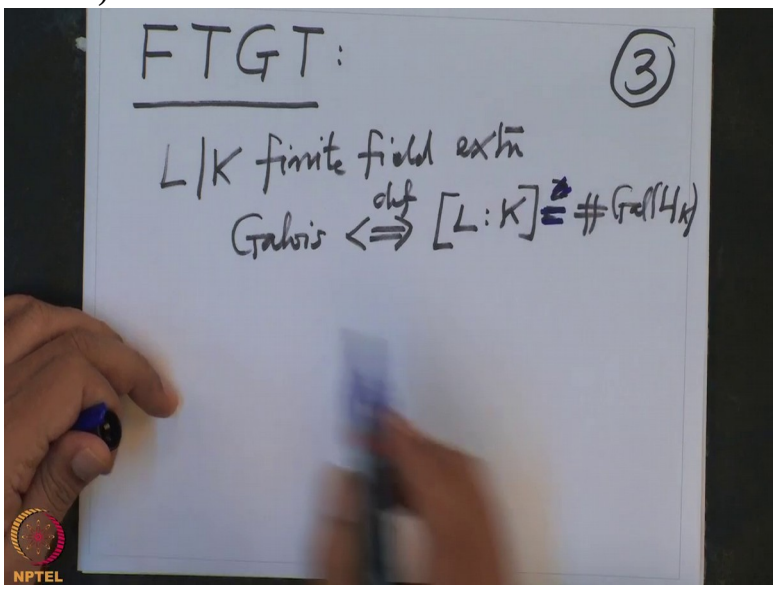
In general, the degree of the field extension is bigger equal to

(Refer Slide Time 06:43)



but when the equality holds we call the extension to be Galois extensions. We also proved that, so this is the equality; that is when

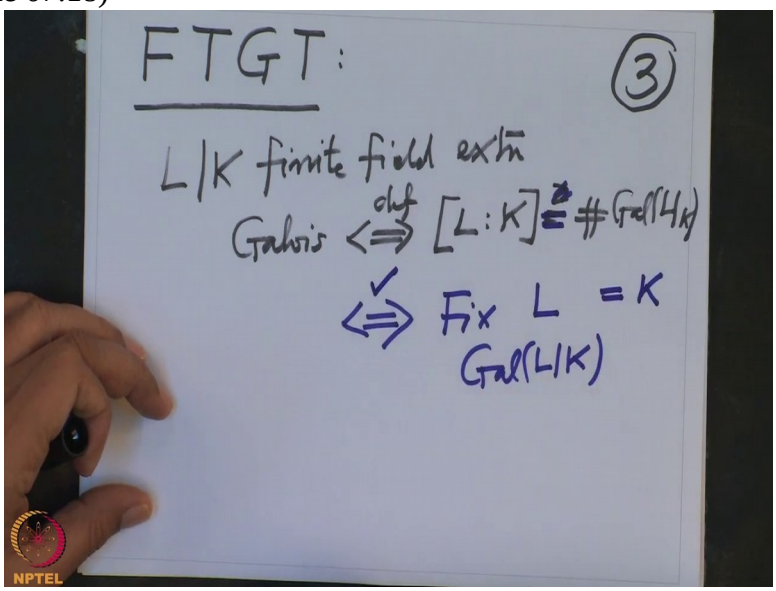
(Refer Slide Time 06:55)



you call the extension to be equal to be Galois extension.

We have also checked that this is equivalent to saying that the, the fixed points of the natural action of the Galois group on the field L; this fix point is the base field. This is also we have proved.

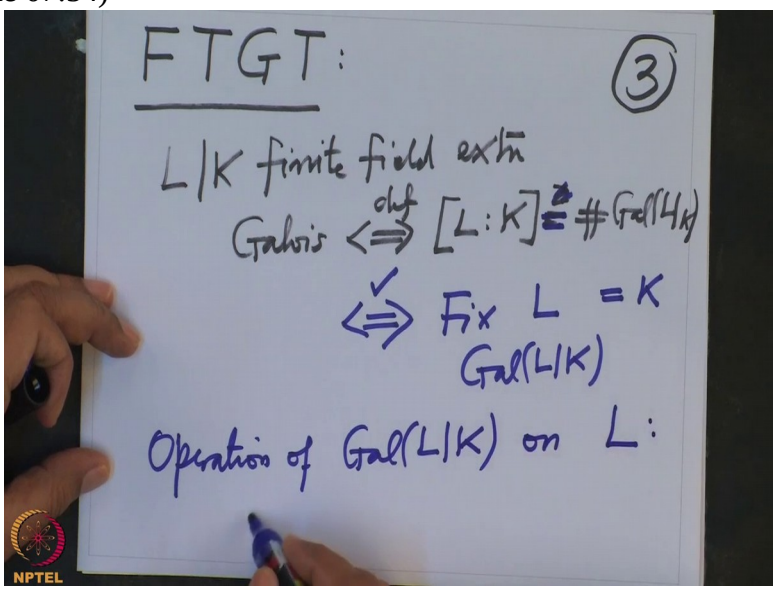
(Refer Slide Time 07:18)



So this is purely a numerical condition that order equal to the degree. This is not numerical condition but it is the, it involves the action of the Galois group. So the whole Galois Theory centers around studying the action or operation of the Galois group on the field L and this is a very natural action.

So the

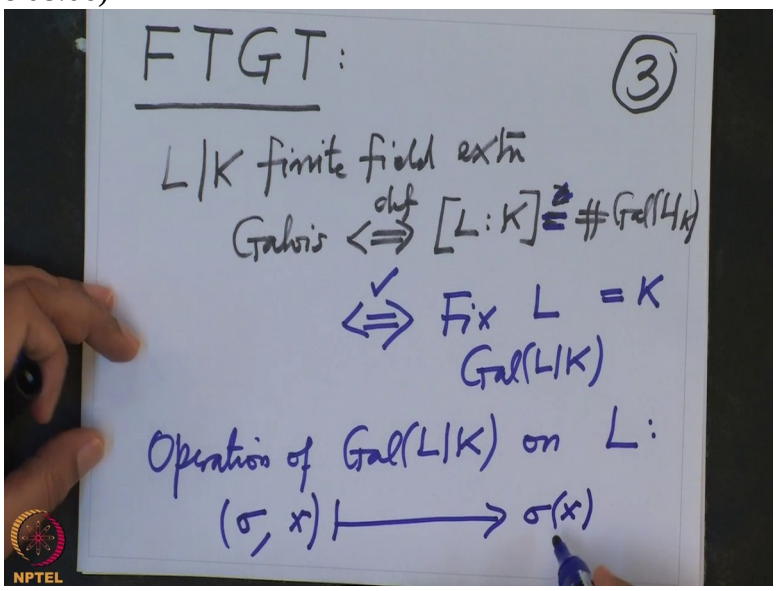
(Refer Slide Time 07:54)



action is given by, if you have an element in the Galois group σ and element in the field L, x that goes to σ evaluated at x.

And

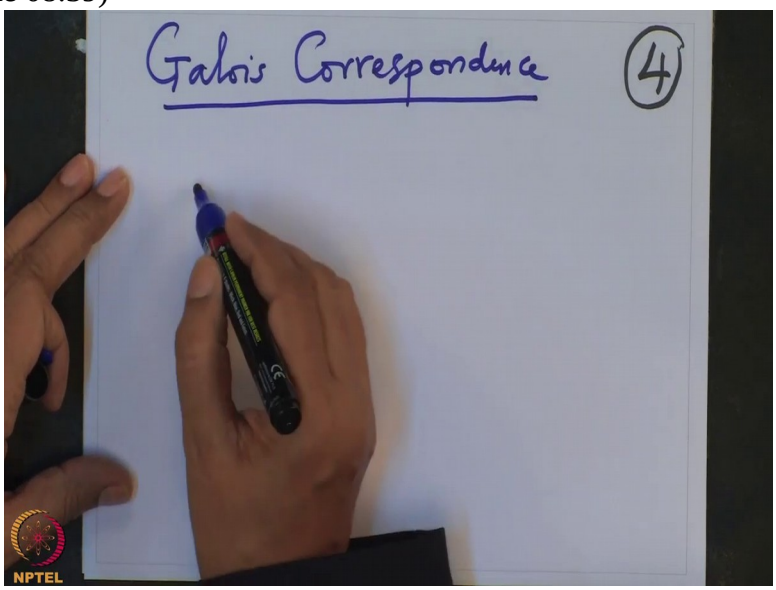
(Refer Slide Time 08:06)



as you see I will, today also study this action more carefully. Not just the basics but I will go little bit more deeper. So what is the Galois correspondence? Galois correspondence, so this is, I will keep referring these two Galois correspondence.

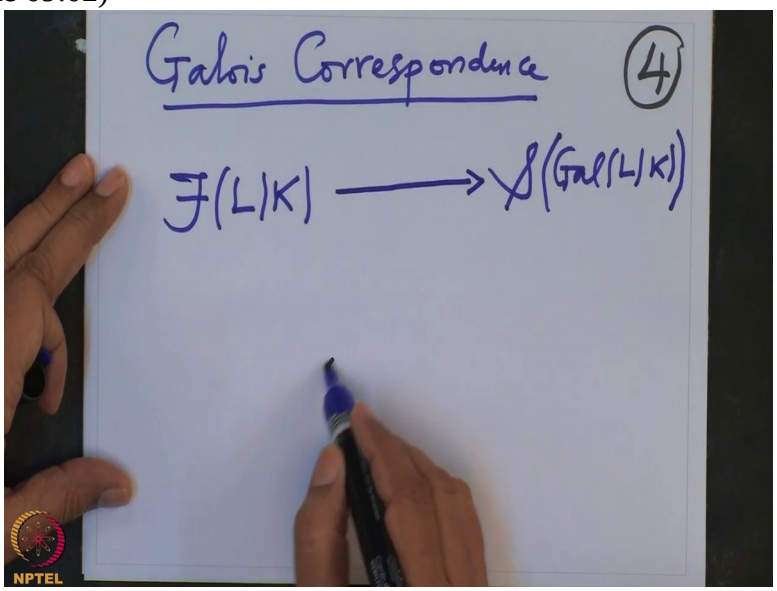
This is, these are the bijections between the intermediary

(Refer Slide Time 08:39)



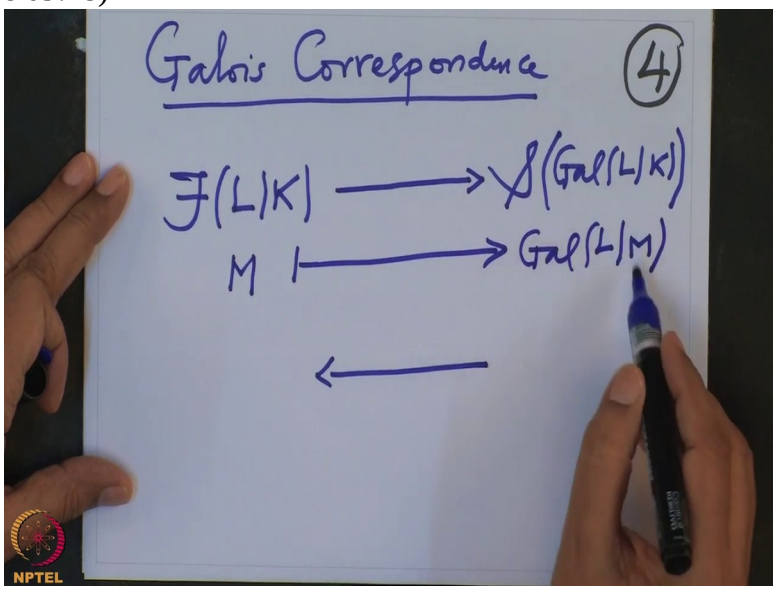
fields, intermediary fields of L over K that means they are subfields of L which contain K on one side. On the other side, the subgroups of the Galois group, these are the subgroups and we have given the map, one in this direction and the other in this direction.

(Refer Slide Time 09:02)



So this map is the, if you have a intermediary field M, then you just map it to the Galois group of L over M. This is clearly a subgroup

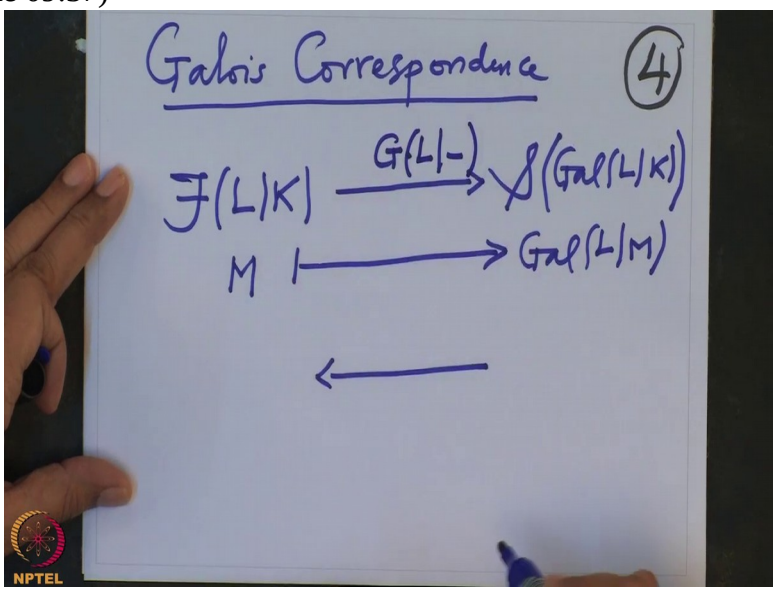
(Refer Slide Time 09:18)



here because these are only M linear maps and these are all K linear maps. So this is a subgroup here. So it makes sense.

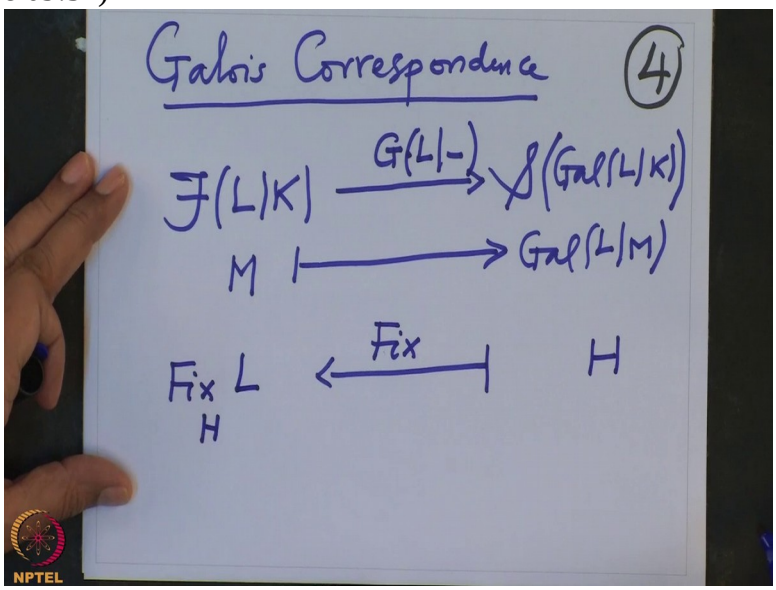
And this map I have denoted by, let us call today just $G(L|-)$.

(Refer Slide Time 09:37)



And this way map is a fix map. So this map is fix. So that is, given any subgroup H, given any subgroup H we mapped it to the fix field of H which is a subfield of

(Refer Slide Time 09:54)

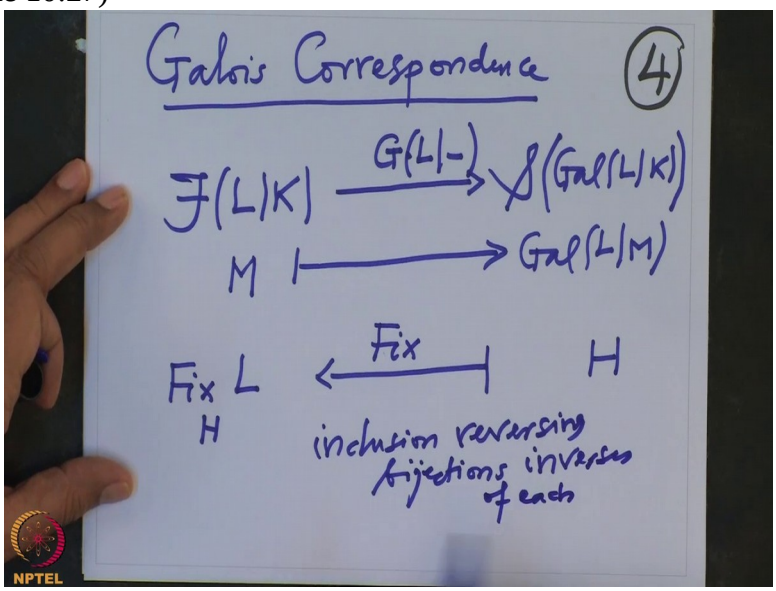


L clearly.

These are all fix points of all elements of H. So this correspondence we have checked that, they are inclusion reversing. They are bijections and not only they are bijections, they are inverses of each other.

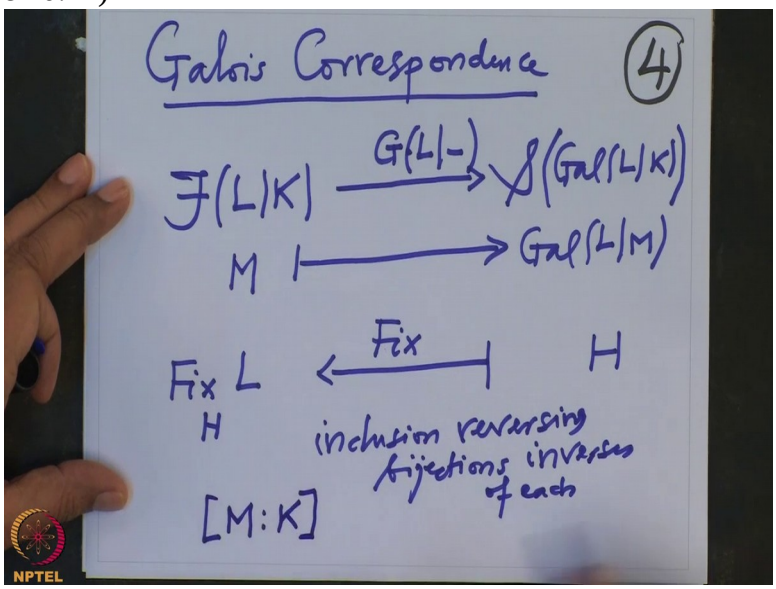
Now for example, now

(Refer Slide Time 10:27)



this also shows that, I am going to ask more questions regarding this correspondence. So for example, I know if we have a intermediary field then we can talk about its degree over K, M K

(Refer Slide Time 10:44)

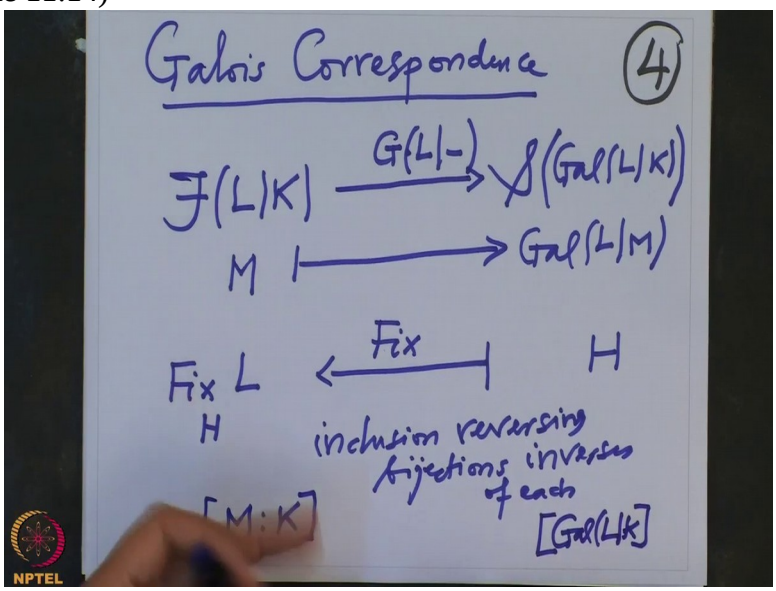


and also we can talk about the, the, this subgroup H, this is H. This is H.

So what is the relation between degree of M over K and H? So it is easy to see that this one will correspond to the index of the subgroup H in the Galois group.

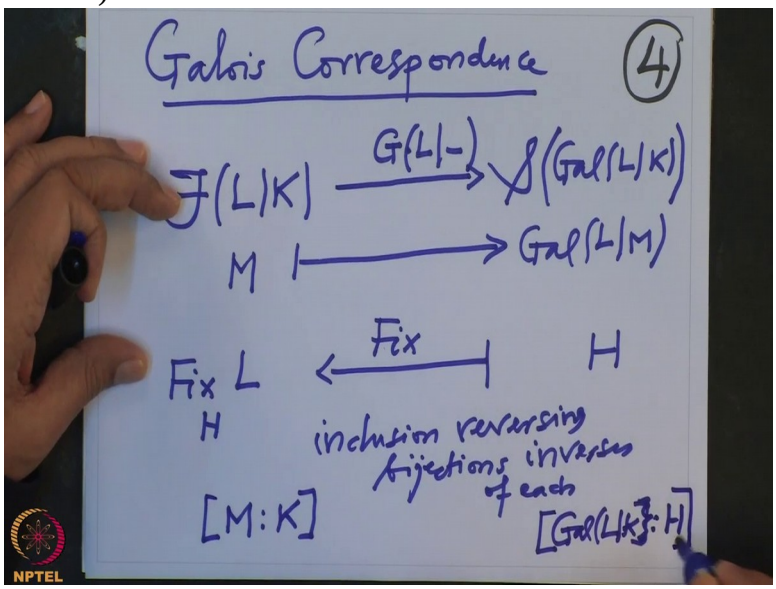
This we have, this is index,

(Refer Slide Time 11:14)



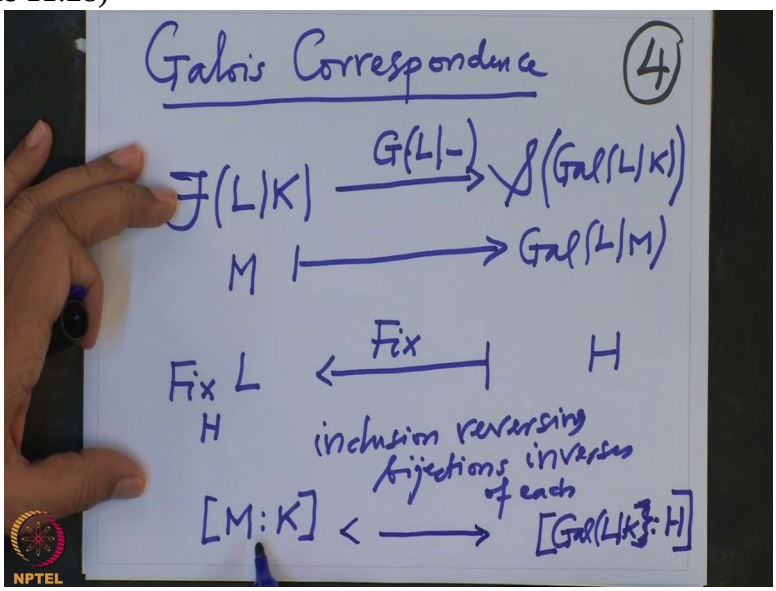
this whole double dot H. This is the

(Refer Slide Time 11:19)



index of H in the subgroup, in the bigger group, the Galois group of L over K. They correspond to each other because

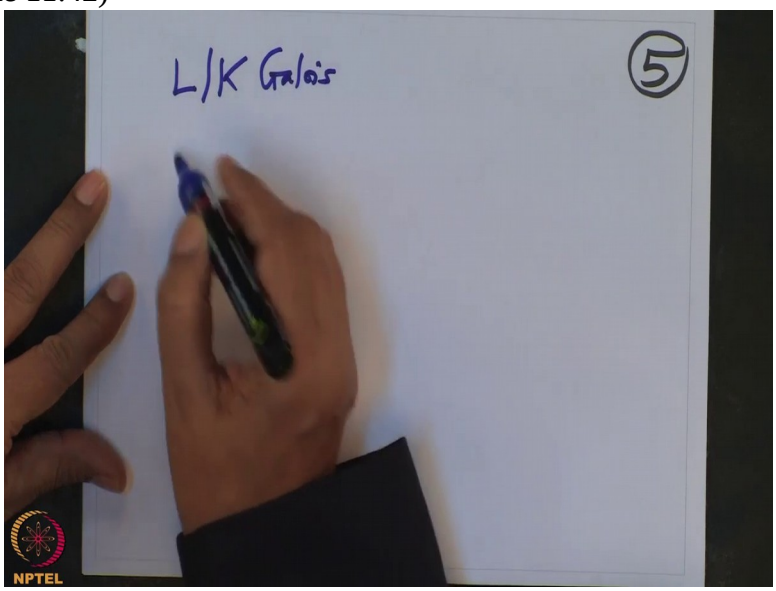
(Refer Slide Time 11:28)



we know that this is easy. I will just write the proof here in one line.

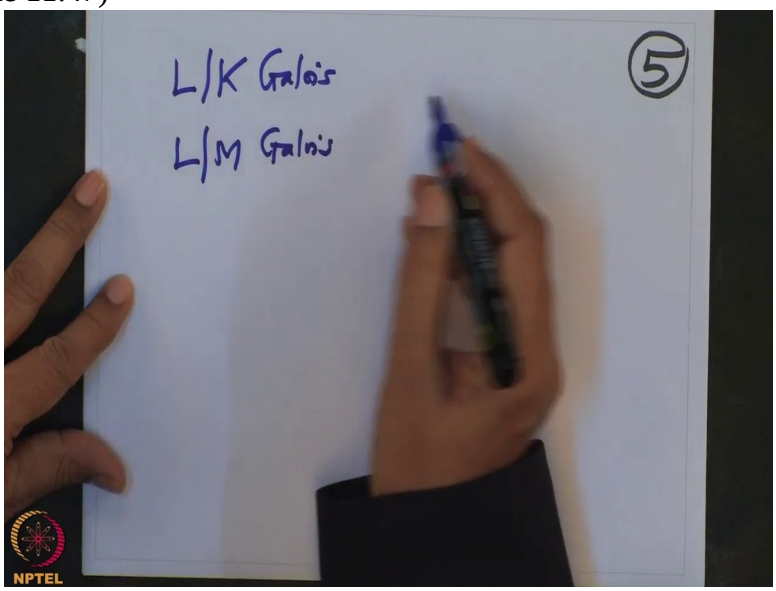
We know, because L over K Galois,

(Refer Slide Time 11:42)



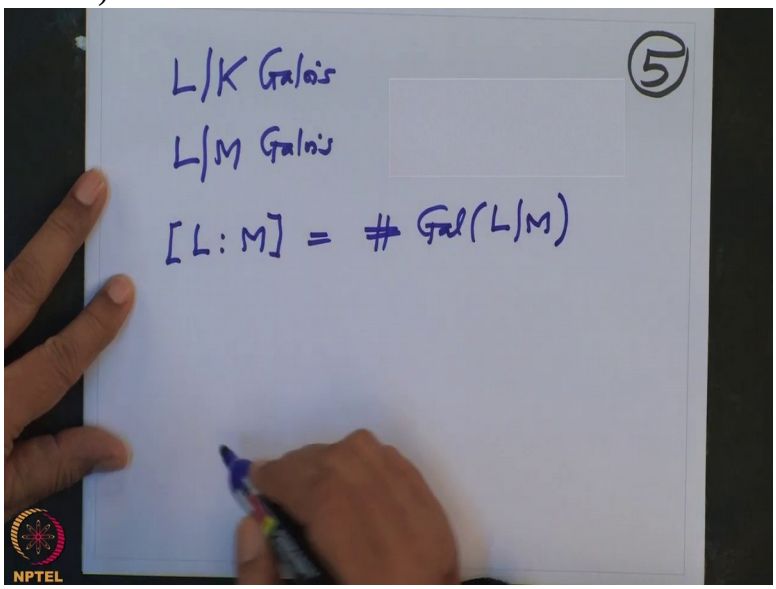
L over M is also Galois, this we have checked.

(Refer Slide Time 11:47)



Degree of L over M, this is equal to the cardinality of the Galois group of L over M.

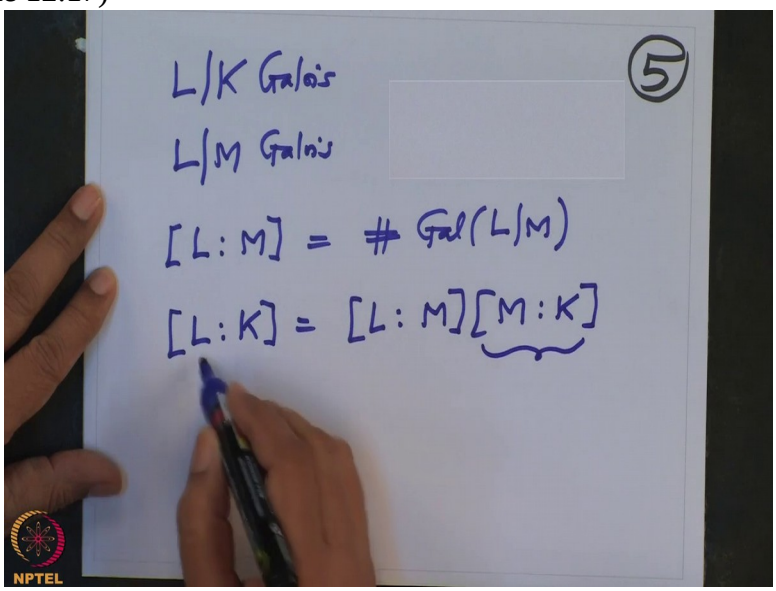
(Refer Slide Time 11:58)



And degree of L over M and degree of L over K, what is the relation?

Degree of L over K, this is degree of L over M times degree of M over K and we are interested in this number.

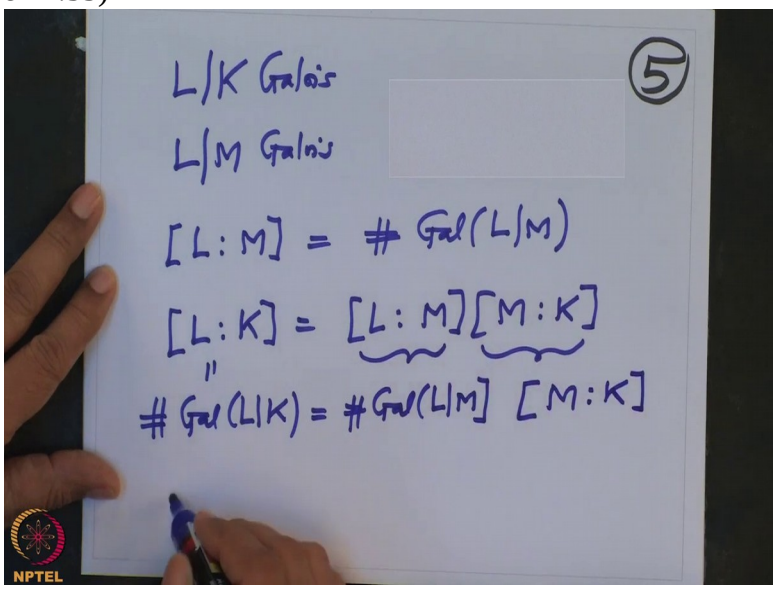
(Refer Slide Time 12:17)



This number I know, this number also I know, this is cardinality of $Gal(L|K)$, and this is cardinality of, cardinality of L over M. And this is what we want.

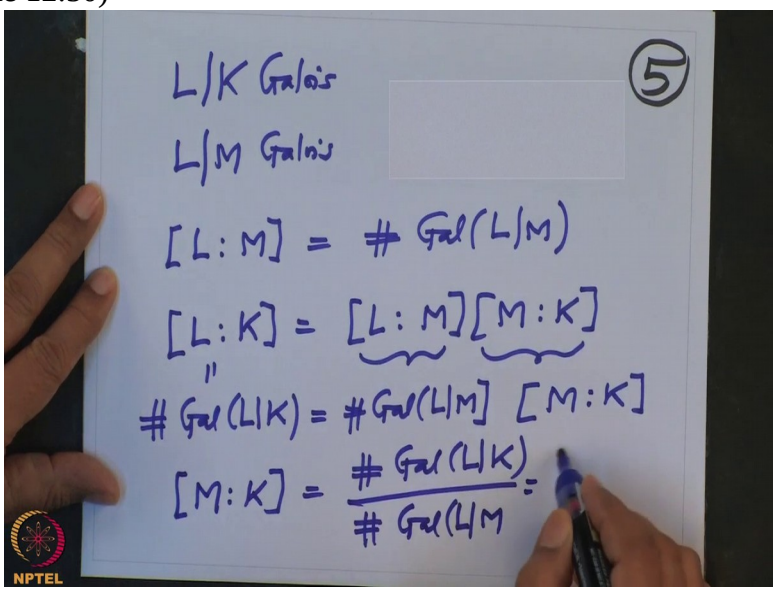
So therefore

(Refer Slide Time 12:35)



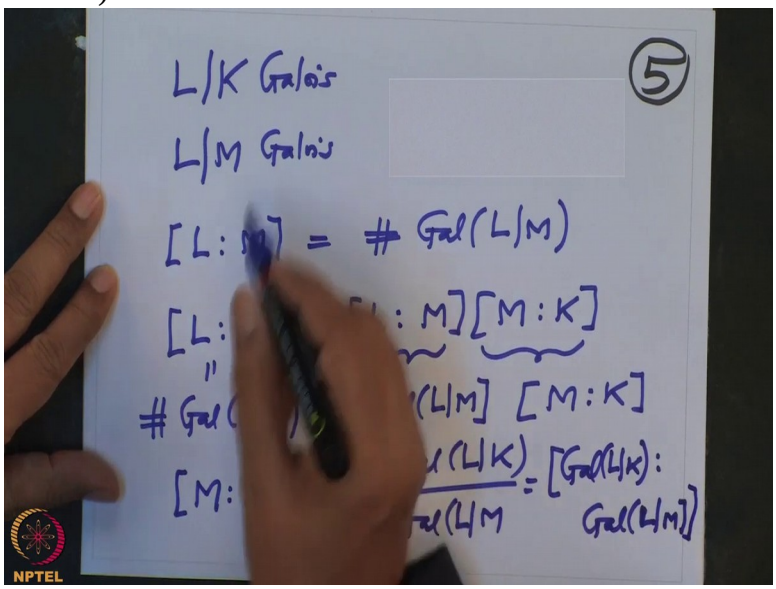
the degree of M over K is nothing but the order of L over K divided by order of L over M. This is

(Refer Slide Time 12:50)



precisely the index of L over M in the group L over K, Galois group of L over M. But this is

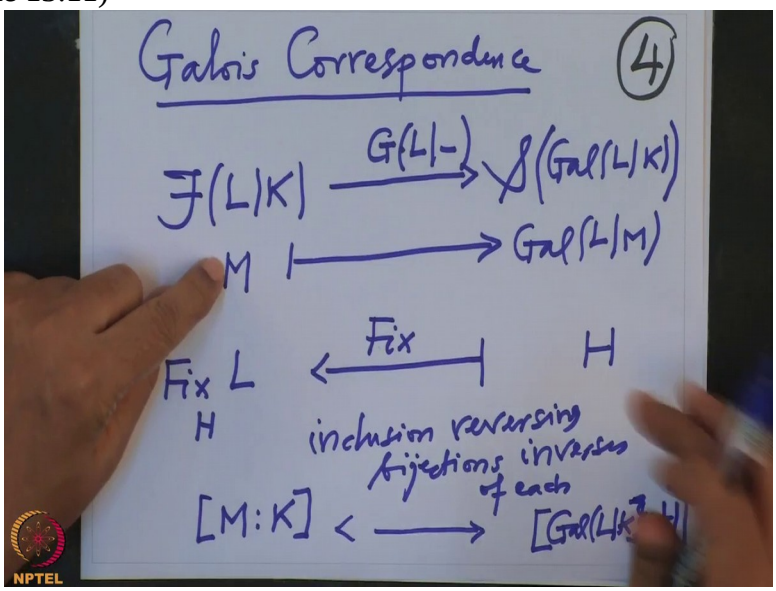
(Refer Slide Time 13:01)



what?

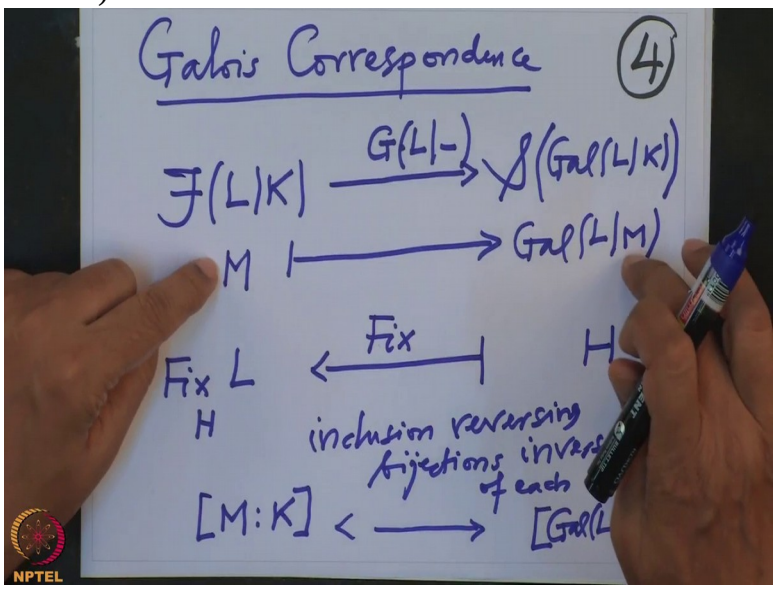
The correspondence is this is the corresponding group H. Therefore what we noted is when you have intermediary field,

(Refer Slide Time 13:11)



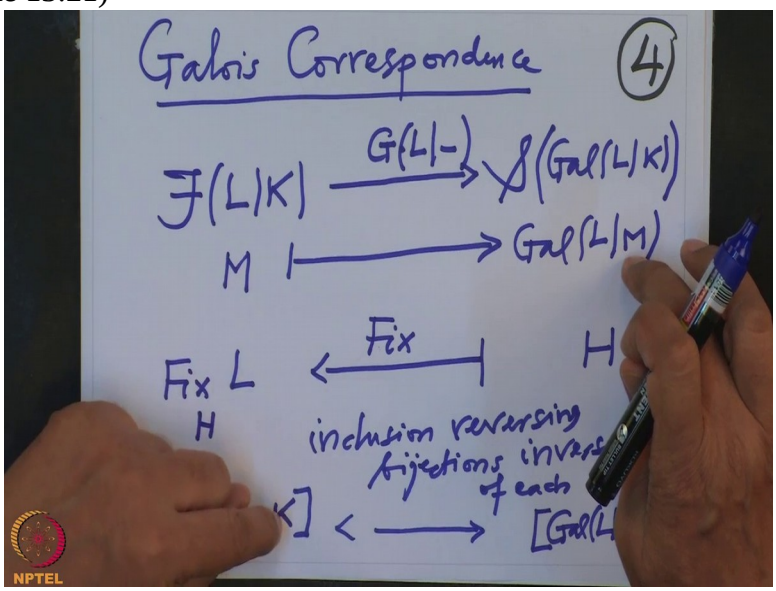
and the Galois

(Refer Slide Time 13:12)



group, this, the information about M, particularly the degree of M over K,

(Refer Slide Time 13:21)

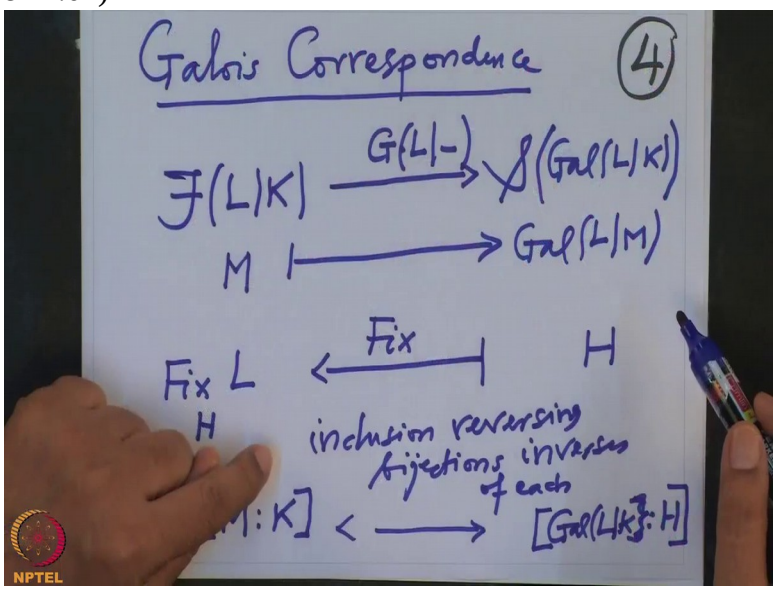


that is the index of the Galois group of L over M in Galois group of L over K.

So we have this extra information. Now I want to also ask questions. If H is some special group, some special subgroup or subgroup which has a special property, for example H is normal then what can you say about that intermediary field?

How do you read that normality of a subgroup in terms of the intermediary field? Or conversely we do not know in general, in general it is not true. We will see by example that M need not be Galois extension of the base field K.

(Refer Slide Time 14:07)

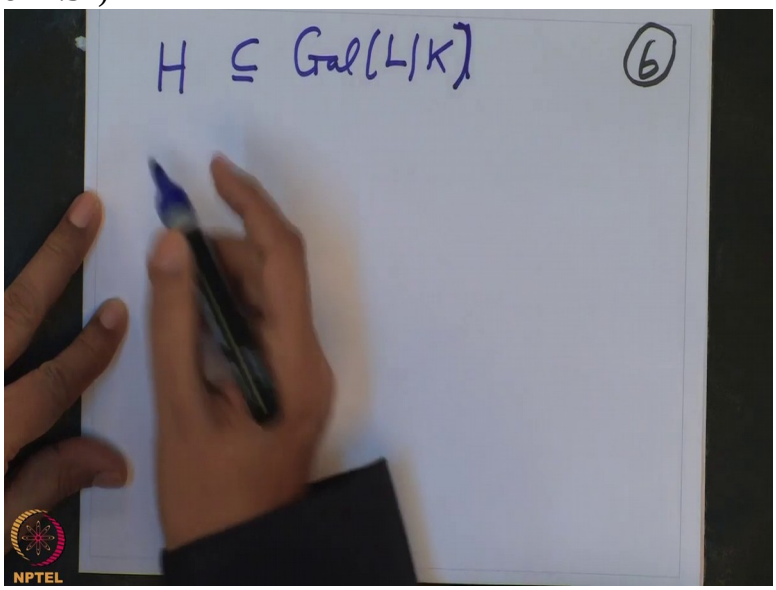


All we know is L is Galois over M but we do not know whether M is Galois over K.

And in general it is not true. We will see these by examples but then we can ask when exactly M over K is Galois extension? So that in terms of the group, so we will check, we will have some results which connects group theory and intermediary fields in a more intimate way.

So right now I want to assume, so the result I am aiming at, suppose H is the subgroup of the Galois group, $Gal(L|K)$ and

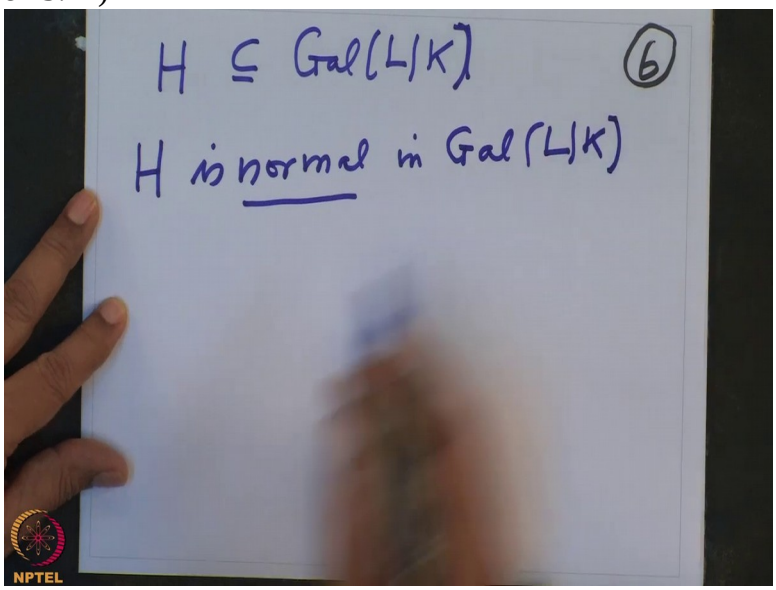
(Refer Slide Time 14:57)



we assume H is normal, normal in G Galois group of L over K.

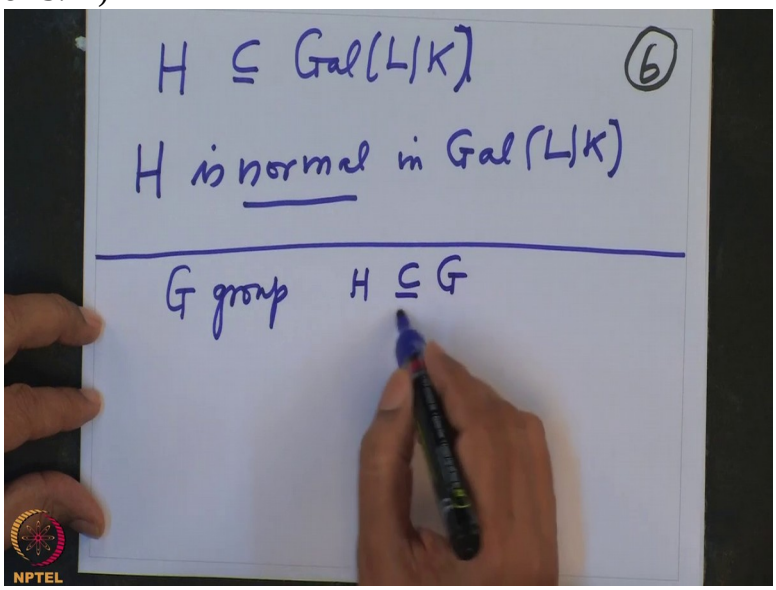
So in general,

(Refer Slide Time 15:11)



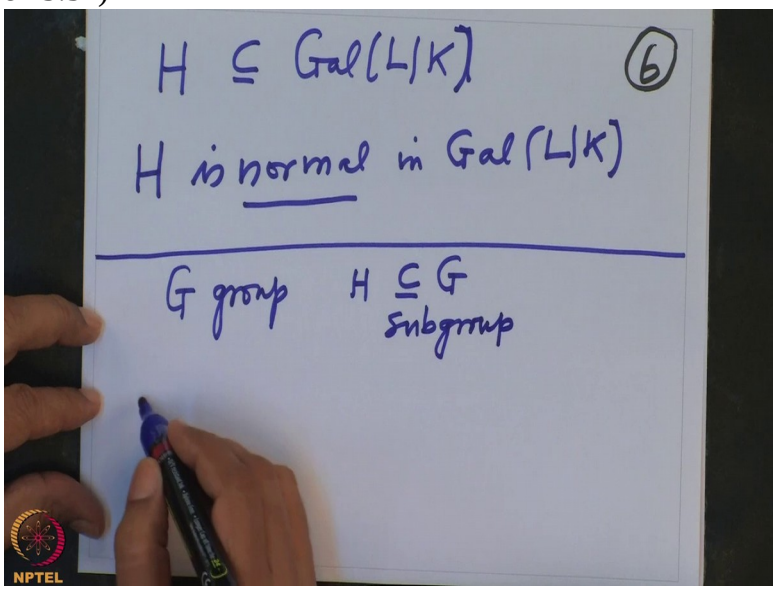
we will have to, I will recall, in general let us recall if G is a group, and H is a subgroup

(Refer Slide Time 15:27)



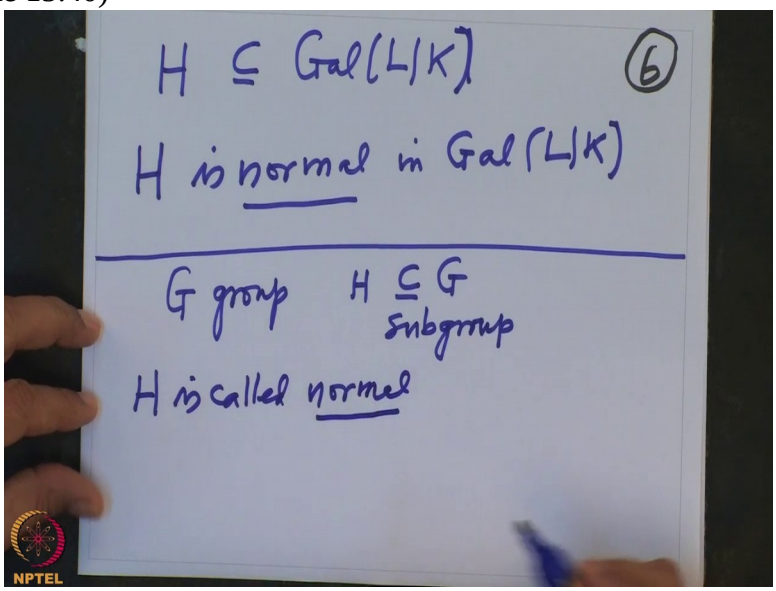
when do you

(Refer Slide Time 15:31)



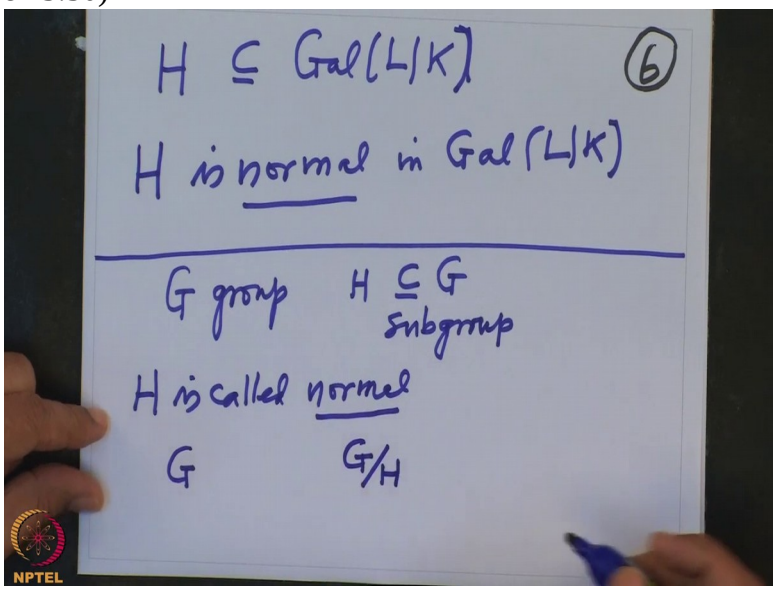
call the subgroup to be normal? H is called normal.

(Refer Slide Time 15:40)



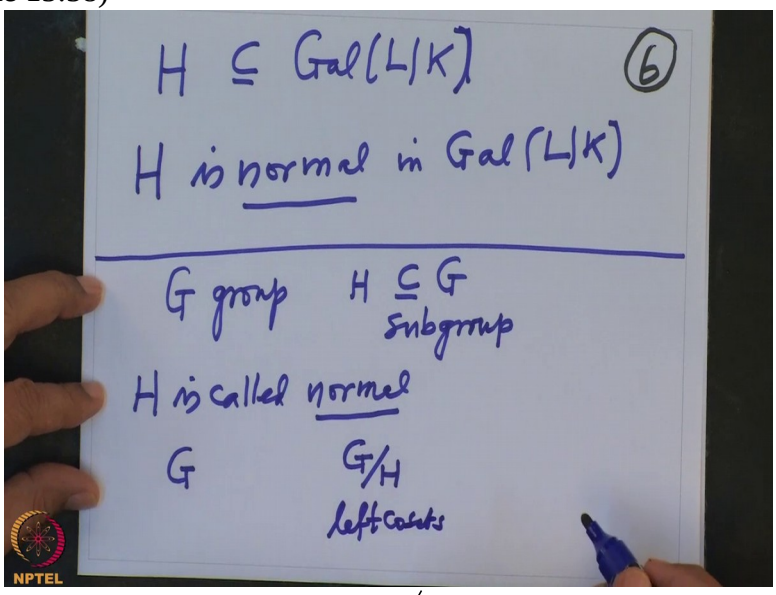
So we have given a subgroup H. So we have given G, this is subgroup of G. And we have given the cosets, so left

(Refer Slide Time 15:50)



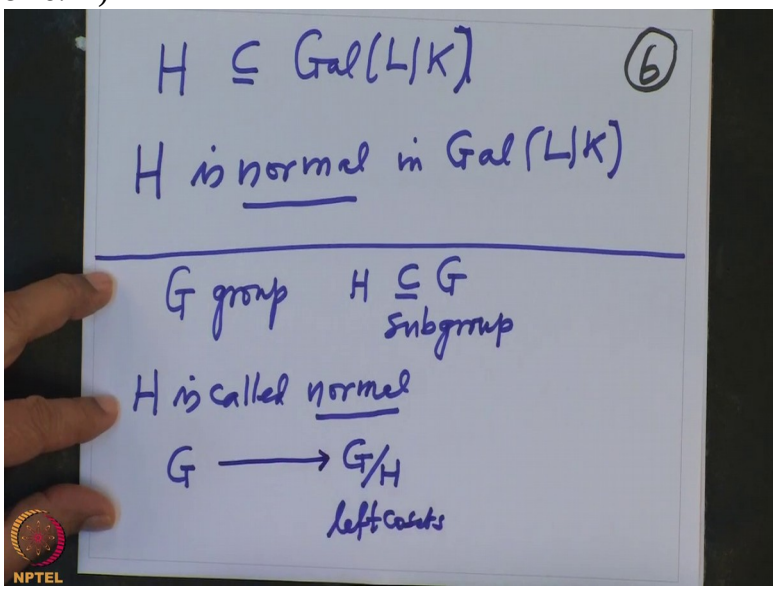
or right cosets. We will concentrate on the left coset. So this is the set of left cosets.

(Refer Slide Time 15:58)



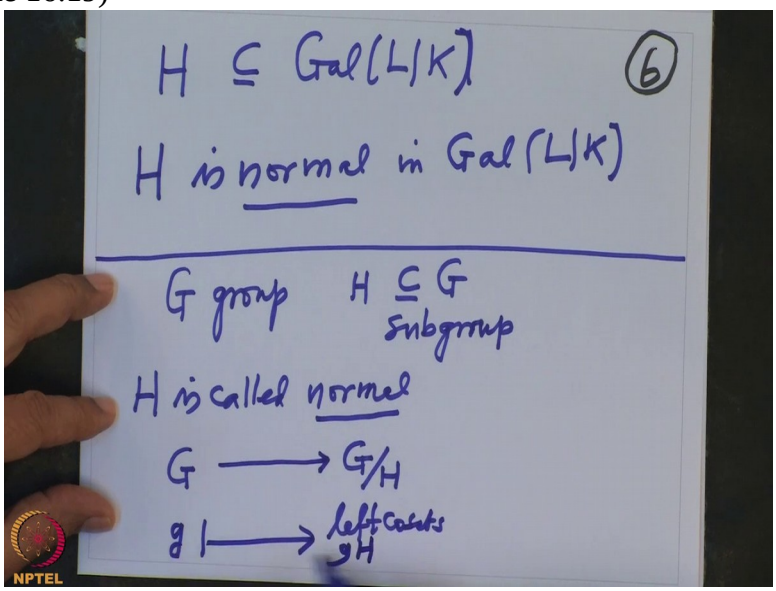
And one would like to know when will the G/H, the set of cosets when will it be a group again in such a way that we have a natural quotient map here.

(Refer Slide Time 16:11)



This quotient map is very clear. Any element g in G that goes to the coset of H defined by

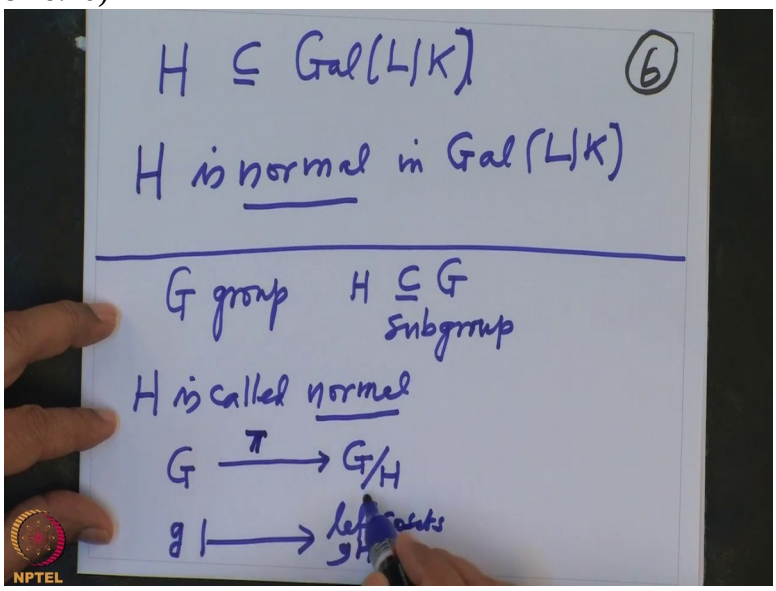
(Refer Slide Time 16:19)



that g H, all those g times H as H varies in the subgroup H. So this is the quotient map.

So we would like to know when can we put a group structure on the cosets so that this natural map, this canonical map, let us call it π , when this

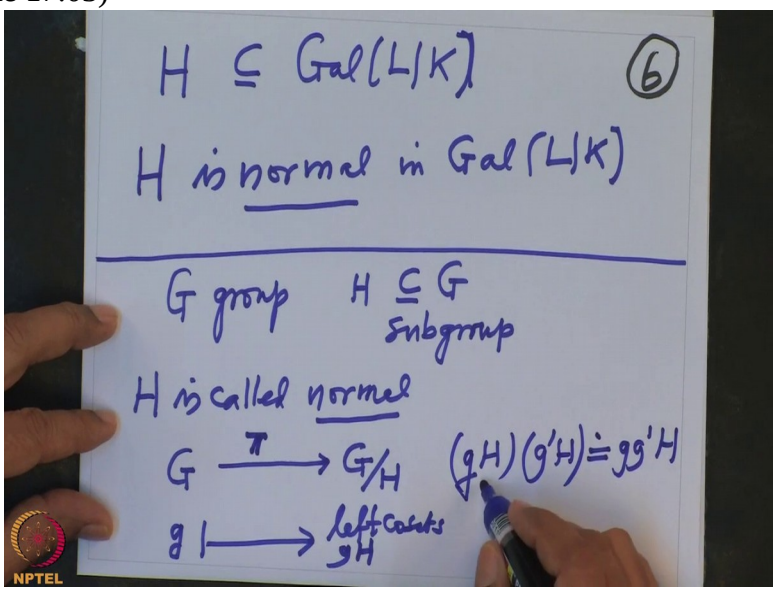
(Refer Slide Time 16:40)



is the group homomorphism? And that is if and only if, what do we know?

We get the group structure, here will be nothing but $(gH)(g'H)$, this will be defined by $(gg')H$. And if you want to define this we have to check that this definition is independent

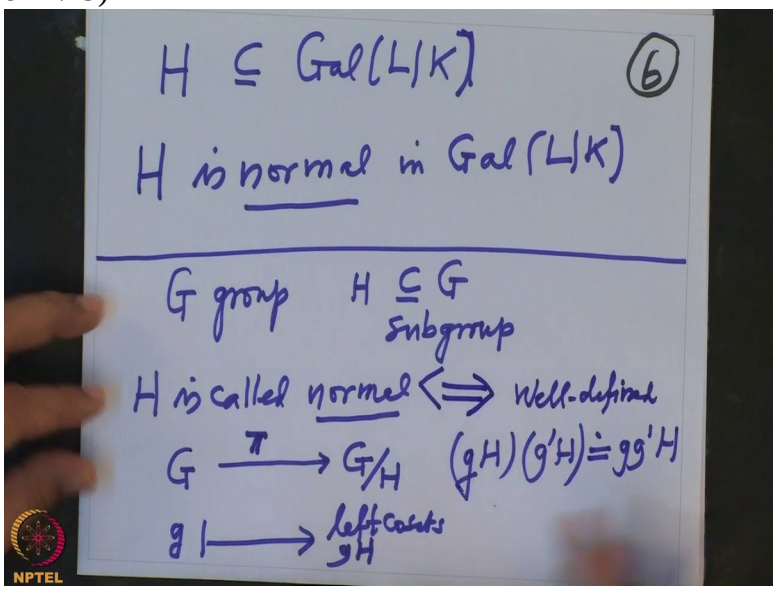
(Refer Slide Time 17:03)



of the representative g and g' of this cosets.

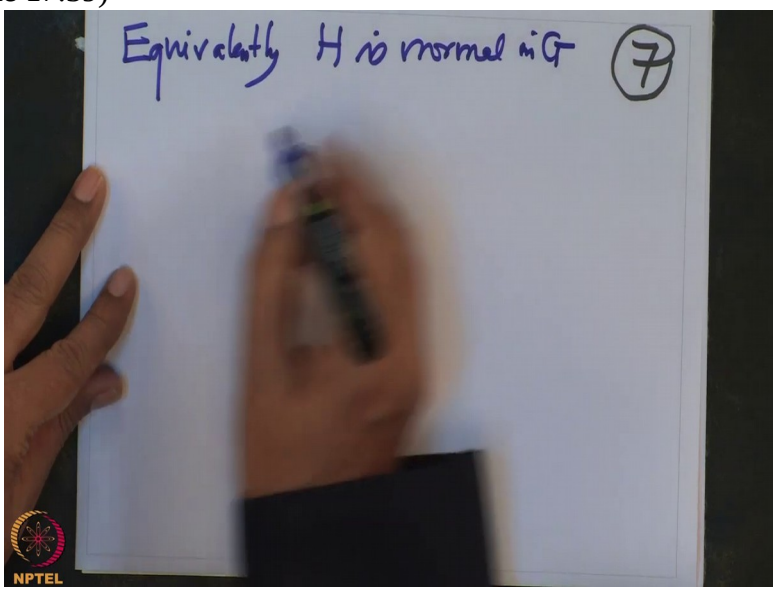
But that is equivalent to saying that subgroup H is normal. So this is well-defined, that is if and only if H is normal.

(Refer Slide Time 17:19)



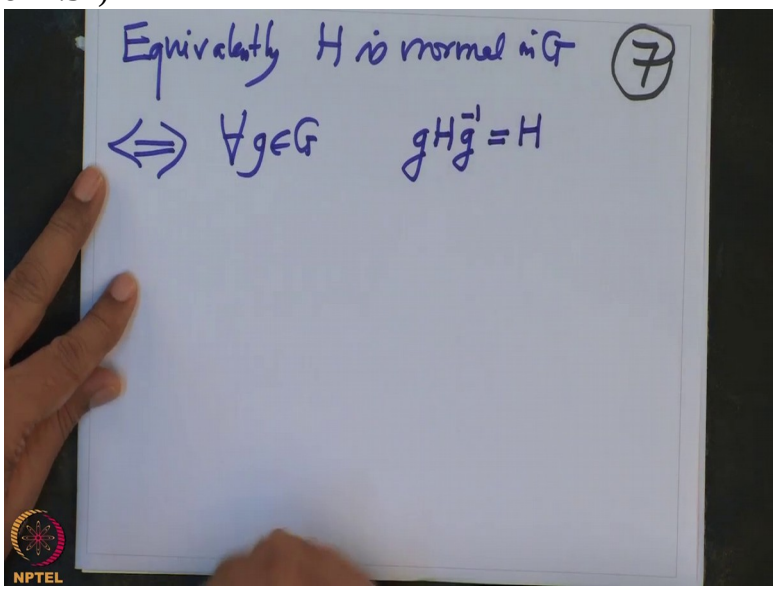
When you want to write down this more precisely, or more transparent way that is equivalent to saying, so equivalently H is normal in G, if and only

(Refer Slide Time 17:39)



if, for every element $g \in G$ the conjugate subgroup gHg^{-1} is H.

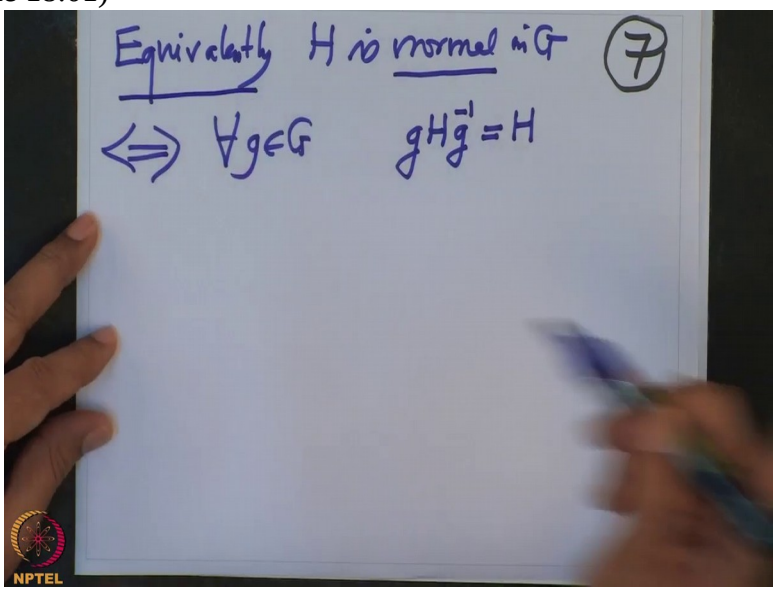
(Refer Slide Time 17:51)



Then we say it is normal.

So many people will take this as a definition. So this as a definition but that is equivalent to

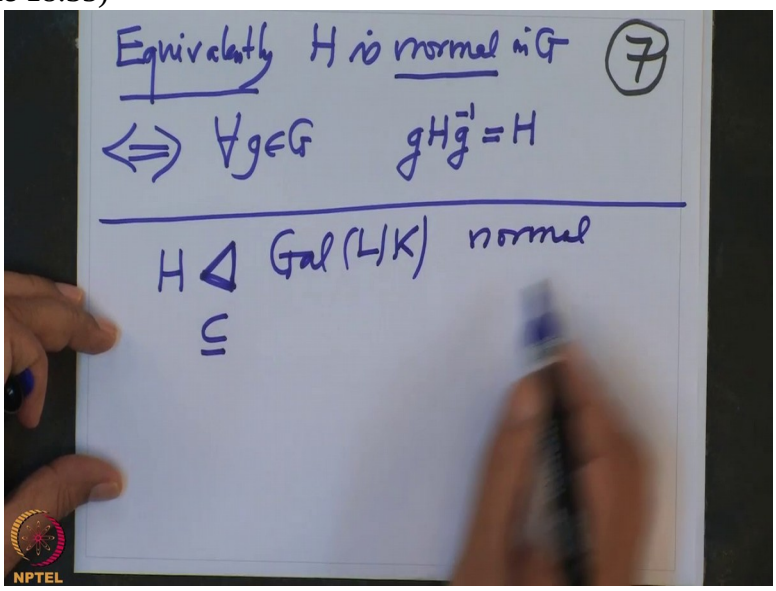
(Refer Slide Time 18:01)



what I said, that is more appealing, saying that when will the quotient g will be a group in a natural way so that the quotient map is a group homomorphism.

So that is normal. Now our problem is the following. We have a subgroup H which is, and normal subgroup is usually denoted by this notation, this instead of only this. So H is normal in the Galois group, normal and I will prove that

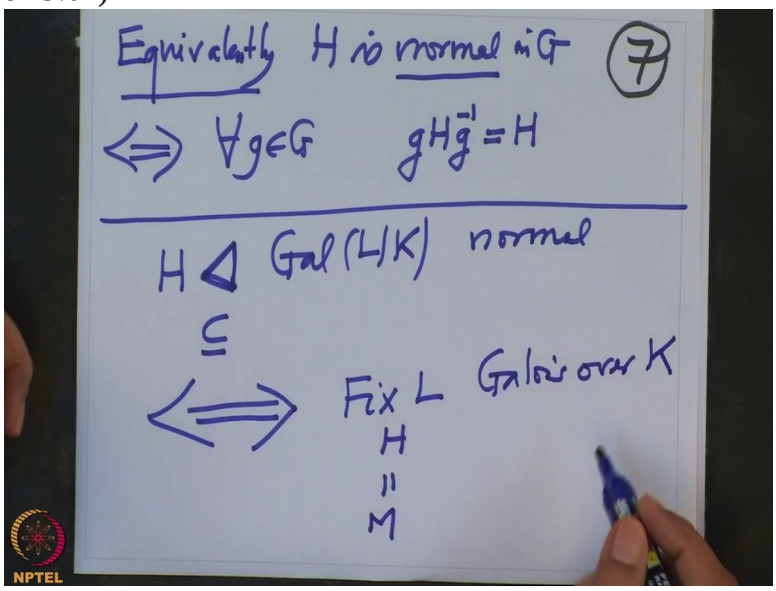
(Refer Slide Time 18:35)



this normality is equivalent to saying this H corresponds to the intermediary field M so this H, so that is fixed, fix L this, this is our M. This is Galois over K.

So that means

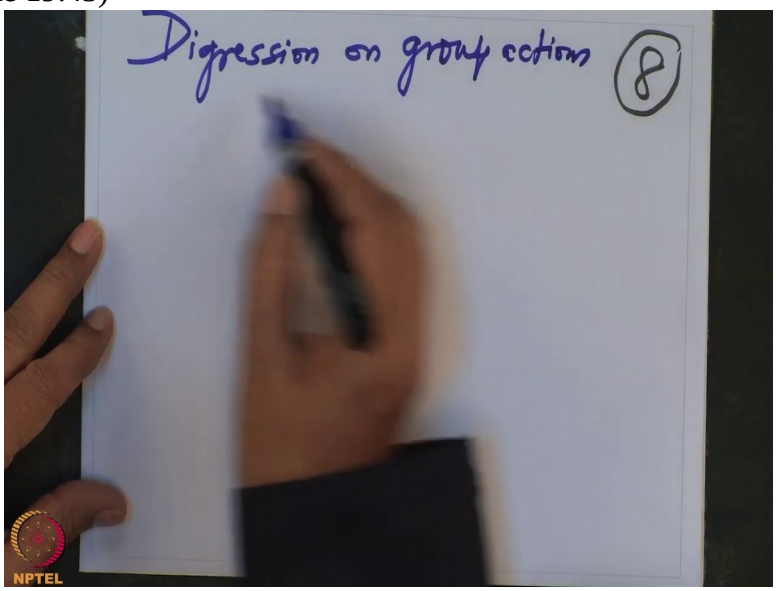
(Refer Slide Time 19:01)



under the Galois correspondence normal subgroups will correspond to Galois subextensions. That is the theorem we want to prove. And obviously this involves studying group actions more intimately and that is what I want to digress. What is this condition? When will this H be nor/ normal, when H is normal what happens to the fixed field?

That is what I want to analyze now. So this is a digression on the group actions. So this is digression on group actions.

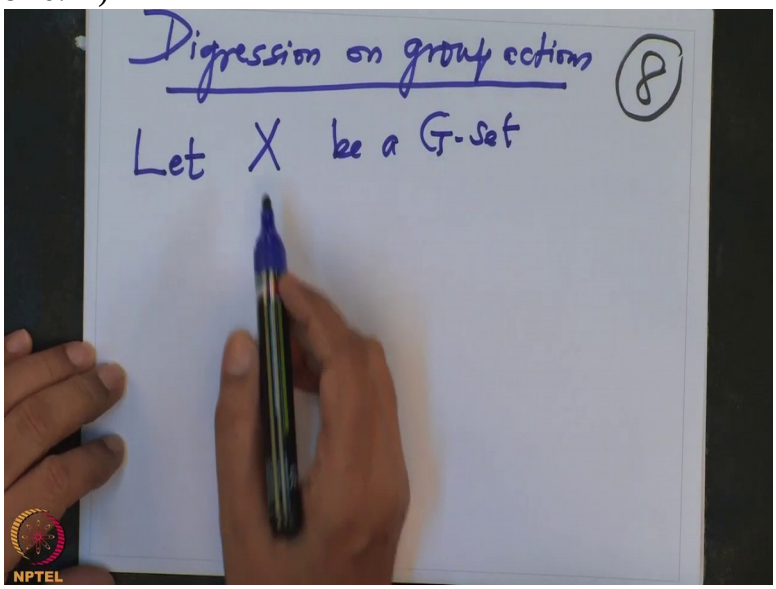
(Refer Slide Time 19:43)



And we will apply these results to our situation of the field Galois field extension and subgroup of that. This is what we are planning to do.

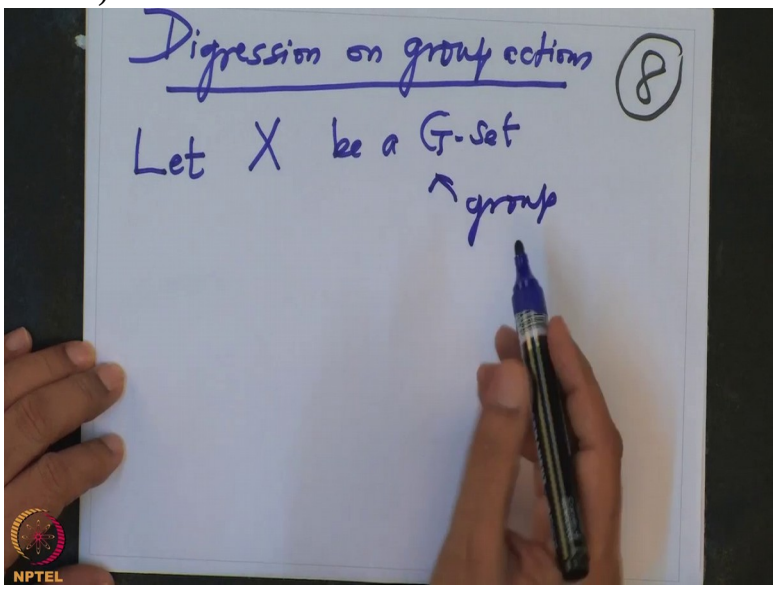
But before that we will understand little bit group actions in a more detail. So let us take in general, let X be a G-set. That means you remember, that

(Refer Slide Time 20:12)



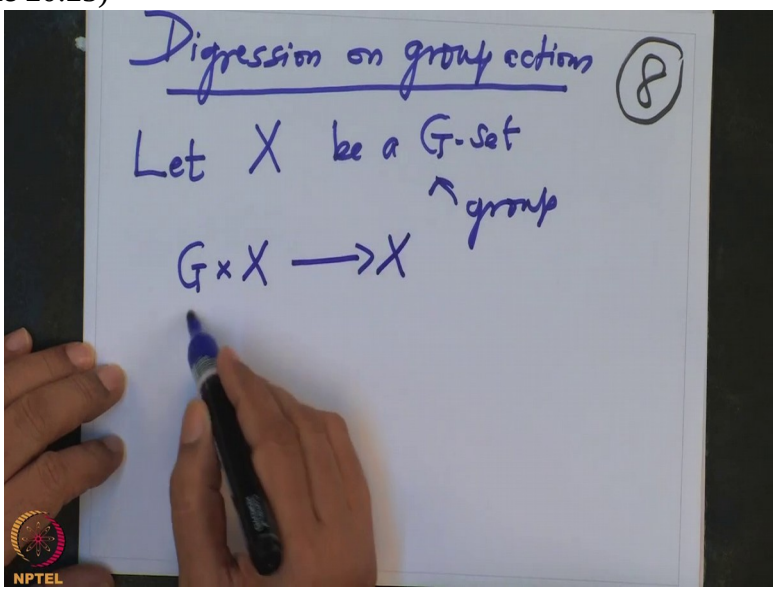
means X is a set and G is a group. And G is operating on X.

(Refer Slide Time 20:18)



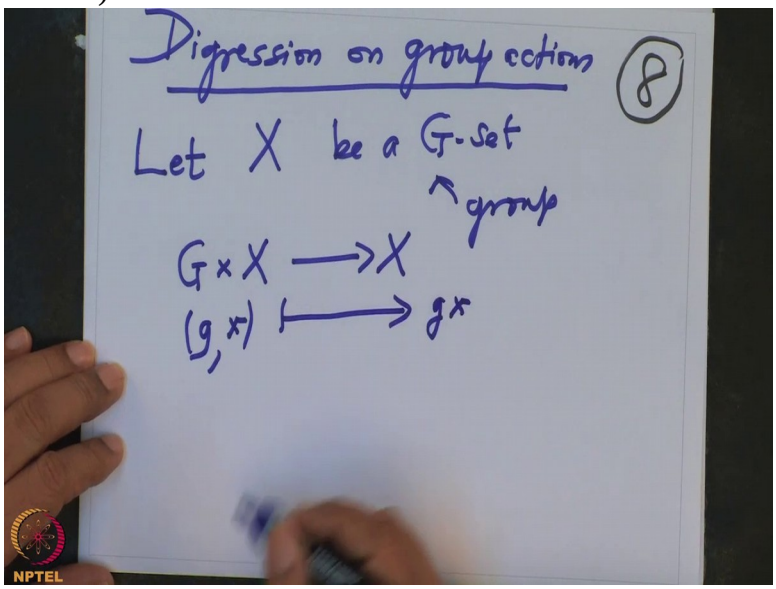
So the operation is the fixed operation, that is written like that,

(Refer Slide Time 20:25)



any g in G comma x that goes to the element g x. This is our notation.

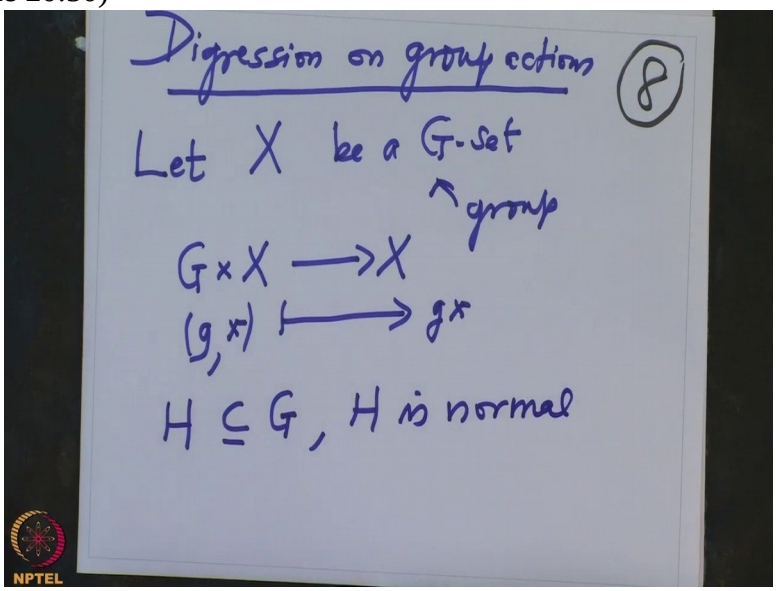
(Refer Slide Time 20:31)



So this is the operation of the group G on X.

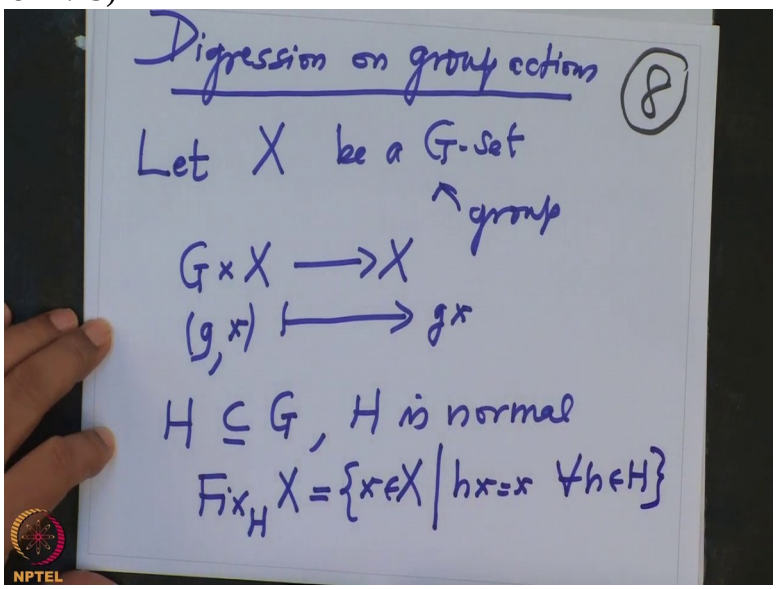
Whenever such a thing is given and suppose H is a, H is a subgroup, H is a subgroup of G. And suppose H is normal.

(Refer Slide Time 20:50)



That is given to us, alright. Now what do I say? And let us denote also the set fix H X, these are only the fix points of X with respect to H, that is these are all those points x in X, all those elements x in X such that h x equal to X for all h in H. These are the fix points

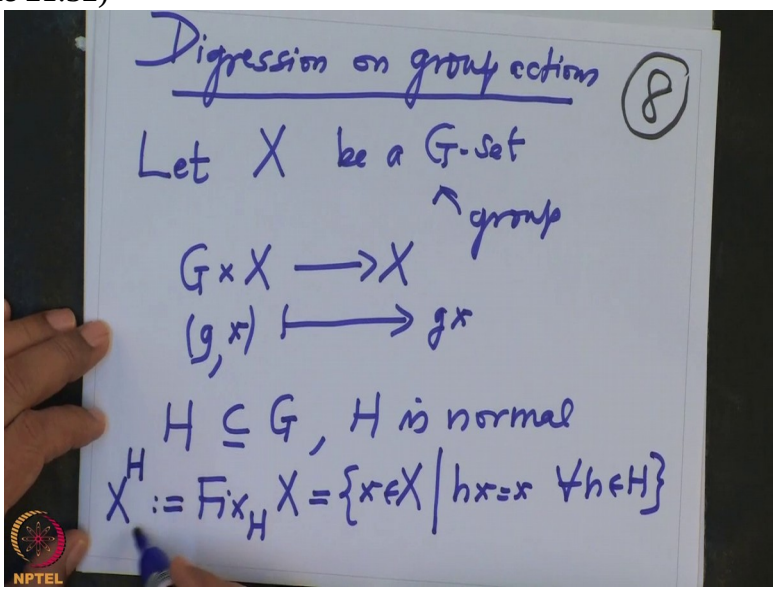
(Refer Slide Time 21:19)



with respect to H.

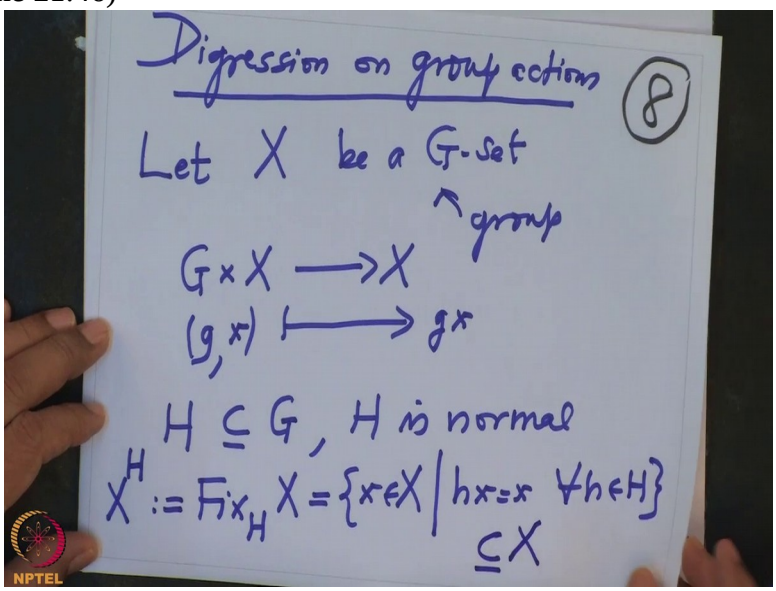
And I will also denote this fix point set by X^H . This is not a good notation but today I will

(Refer Slide Time 21:32)



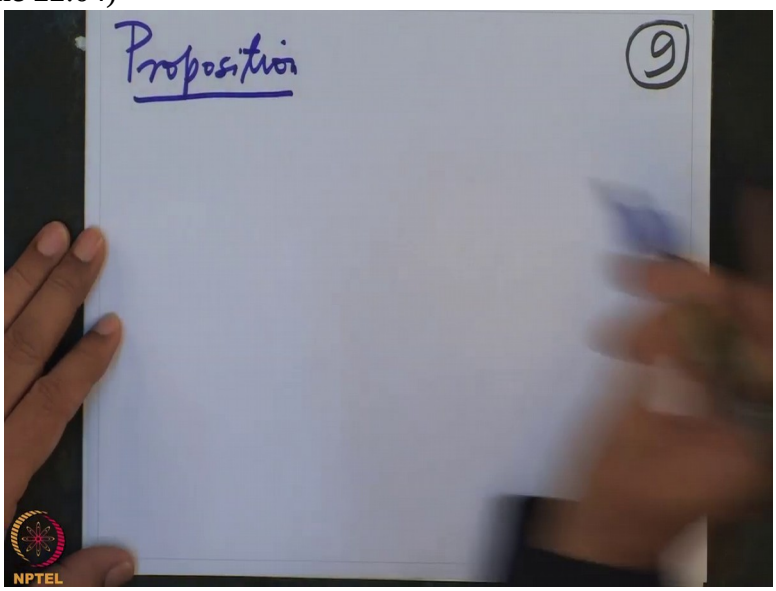
denote this. When there is no confusion we will denote this. Otherwise we will usually denote it by this, so X^H . So this is a subset of X.

(Refer Slide Time 21:46)



so first observation I want to denote is, so observe that, so let me write the proposition. So proposition,

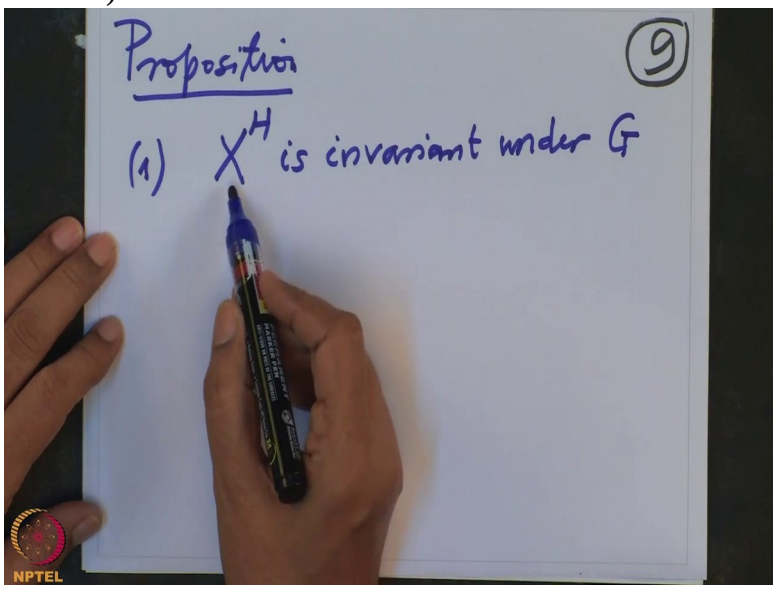
(Refer Slide Time 22:04)



with the notation as above, the first one X^H is invariant under G. What does that mean?

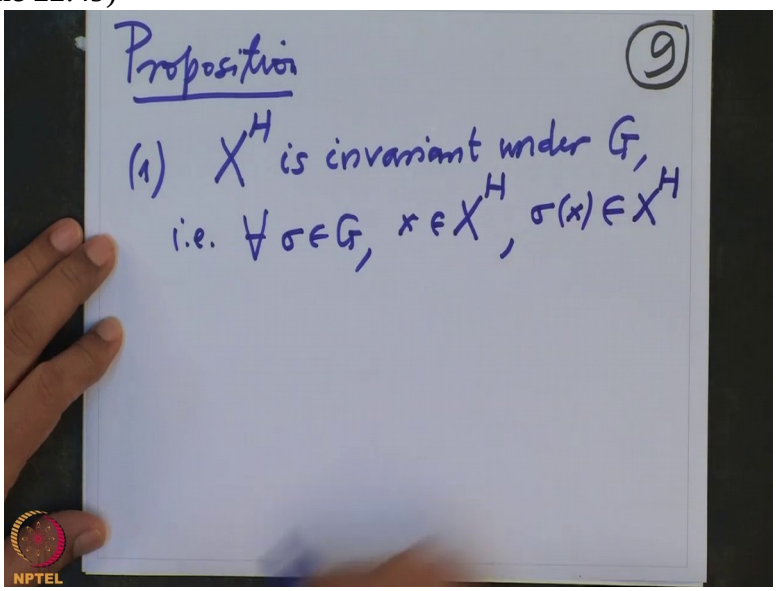
That means if I take any, any element of G and apply

(Refer Slide Time 22:28)



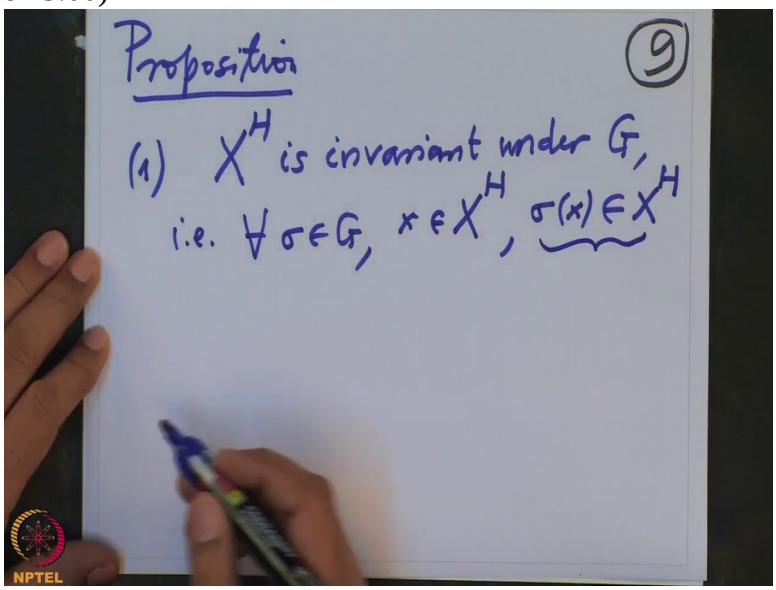
to any element of X^H then it will come back again in X^H. So that is, that is for every σ in G and every $x \in X^H$, σ of H again lies in X^H.

(Refer Slide Time 22:49)



Alright, let us finish off the proof now only. So that means I want to prove this. So I want to prove this means what? This is what to be proved.

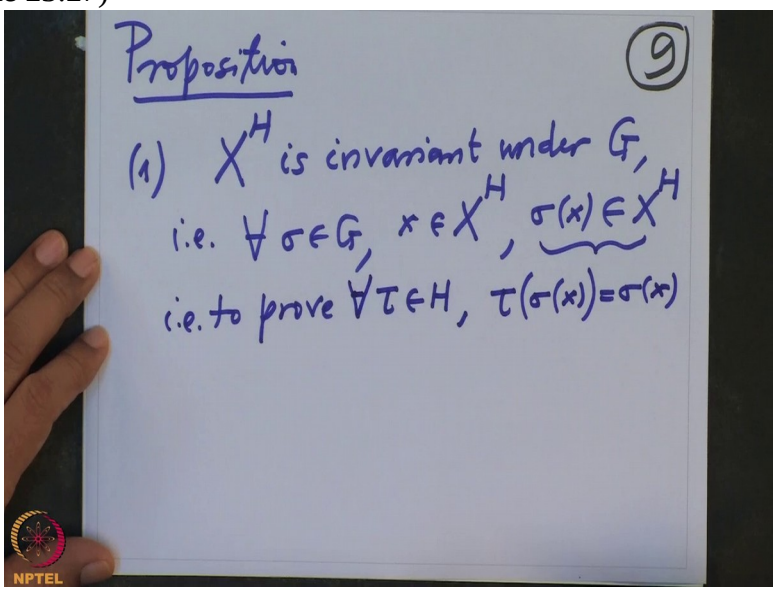
(Refer Slide Time 23:00)



So that means given any element, I want, that means this element $\sigma(x)$ is invariant under all elements of H.

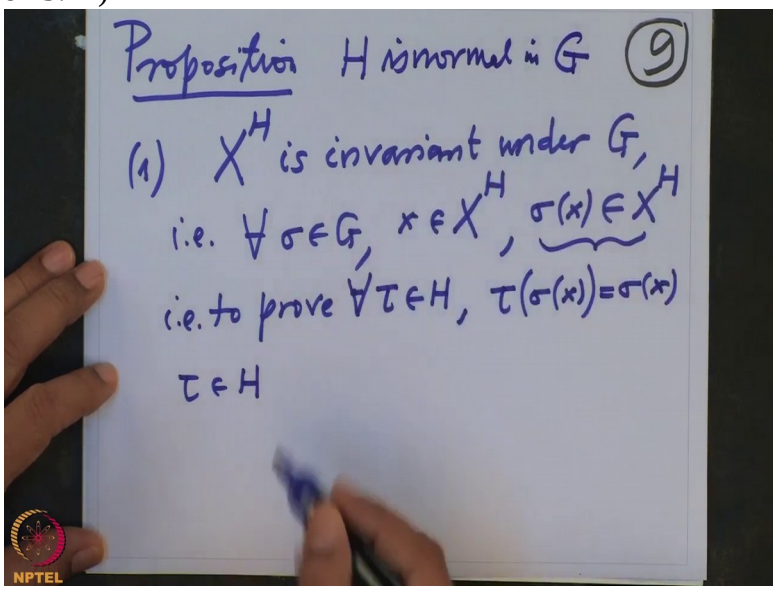
So that is, to prove, if I take any $\tau \in H$, $\tau(\sigma(x))$ should be $\sigma(x)$ only. This is for every τ

(Refer Slide Time 23:27)



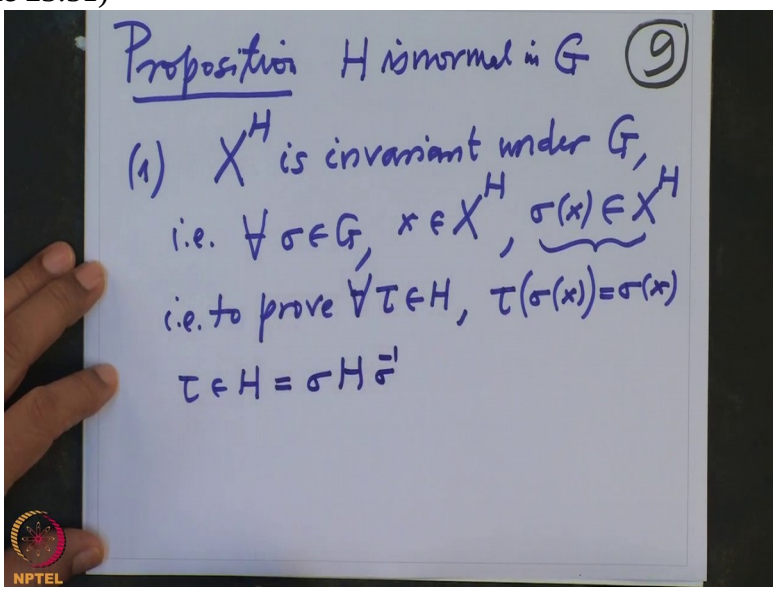
I have to prove, alright. But tau is in H and we are assuming, remember H is normal. That is what we are assuming. H is normal in G.

(Refer Slide Time 23:44)



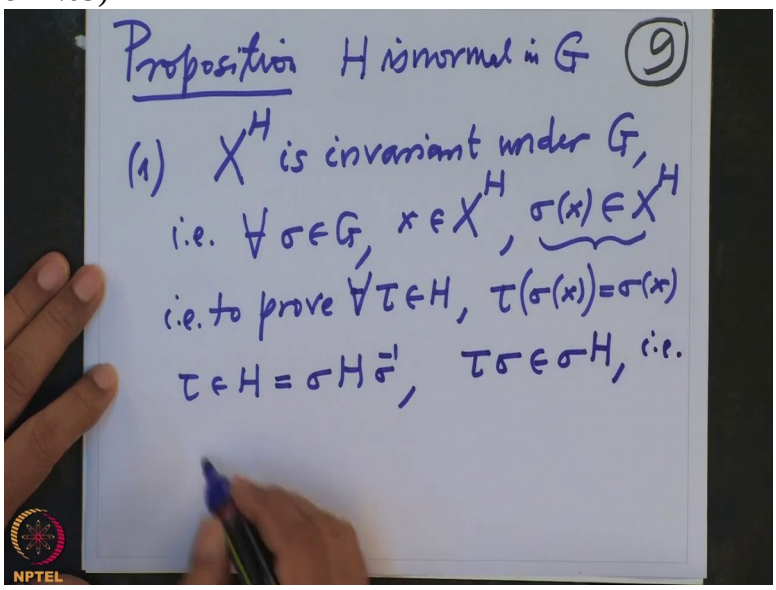
So tau is in H but H is also same thing as the conjugate subgroup this.

(Refer Slide Time 23:51)



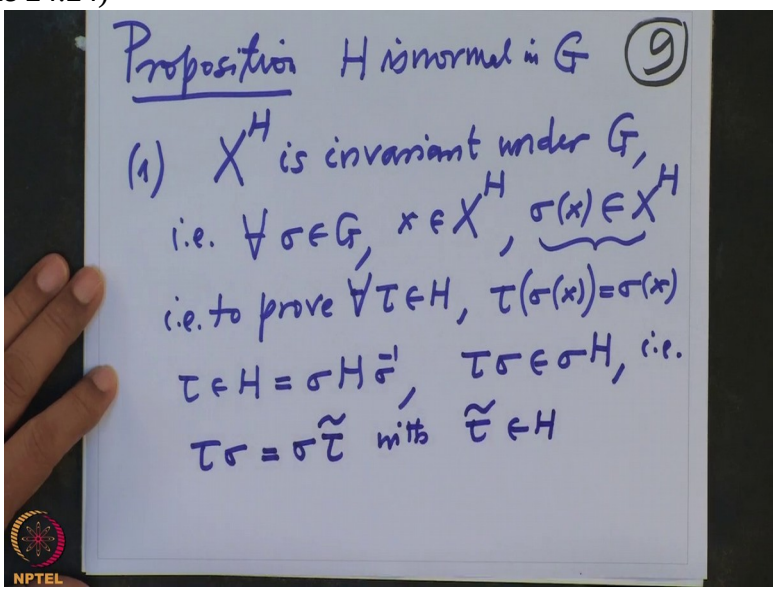
So therefore every tau is also an element of this. So that is tau I can write, so that means I multiply σ from the, this side so that is tau σ becomes to the coset σ H, so that means

(Refer Slide Time 24:09)



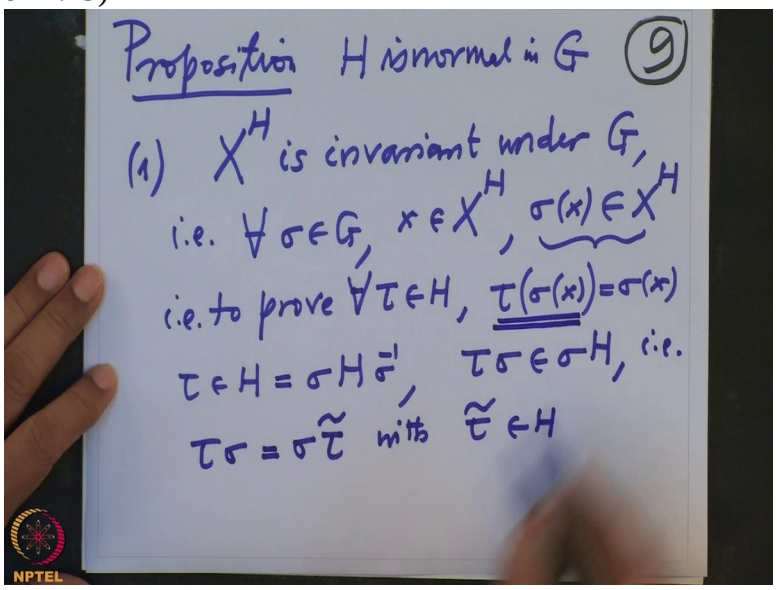
$\tau\sigma$ will be an element of this coset, so that will look like $\sigma\tilde{\tau}$ with $\tilde{\tau}$ belonging to H.

(Refer Slide Time 24:24)



And now what do we want? I want to check that this element is $\sigma(x)$ only.

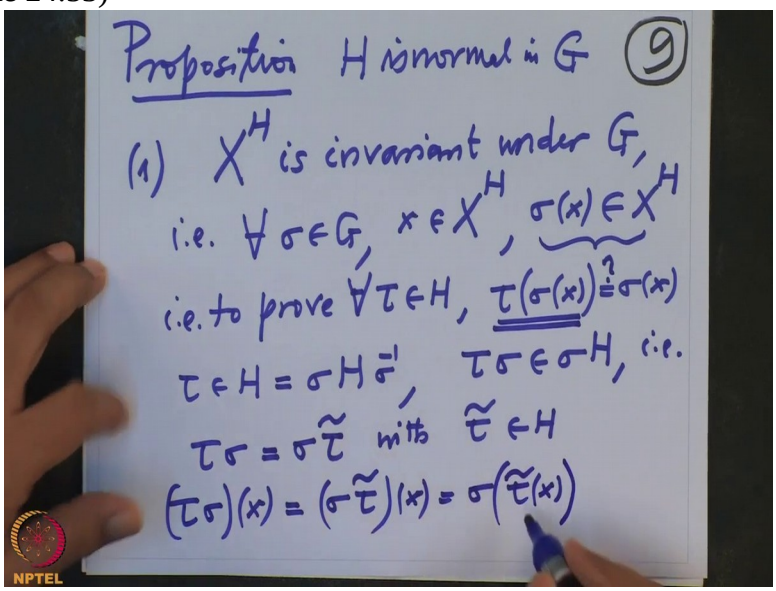
(Refer Slide Time 24:29)



This is what we want to prove. So start with, apply, evaluate both sides on x. So τ σ evaluated at x, this is what we are interested in.

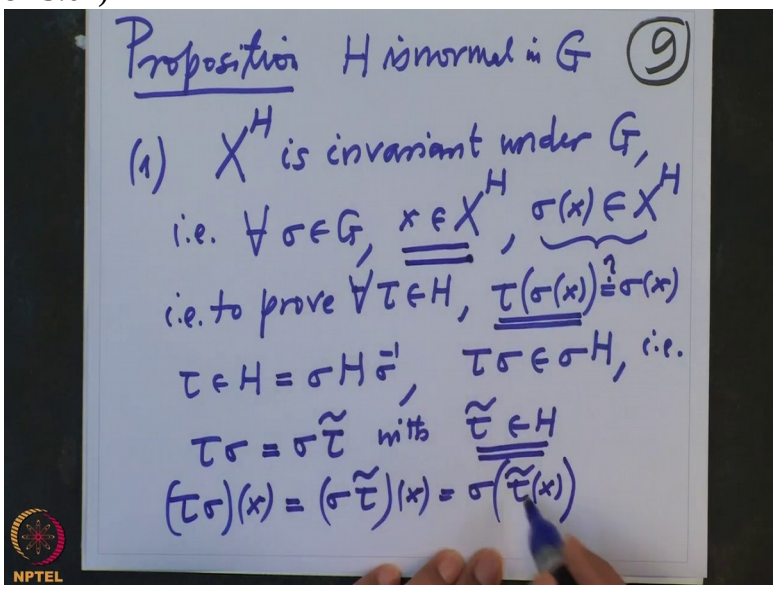
This is same thing as $\sigma\tilde{\tau}$ evaluated on x but this is $\sigma\tilde{\tau}$ of x but

(Refer Slide Time 24:53)



$\tilde{\tau}$ is in H and this x was element in X^H that means x is invariant under all elements of H,

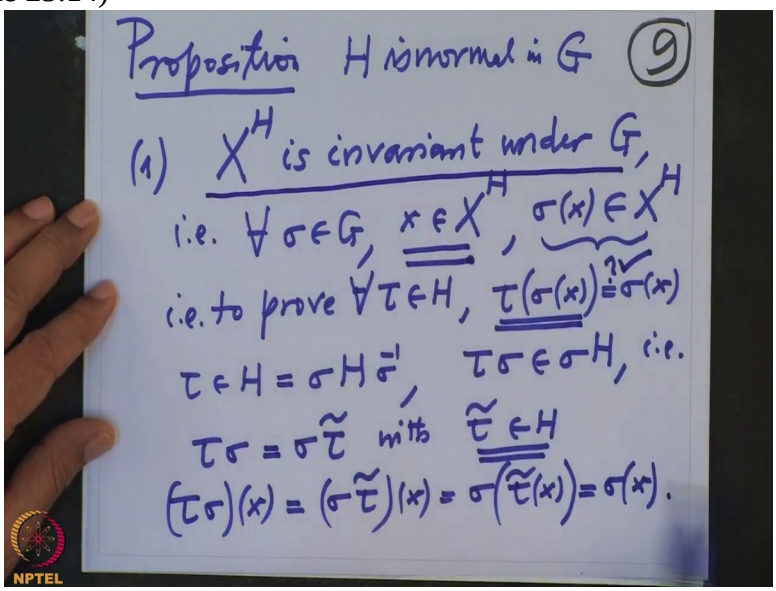
(Refer Slide Time 25:02)



in particular of $\tilde{\tau}$ so this is σ of x, this is what we wanted to prove.

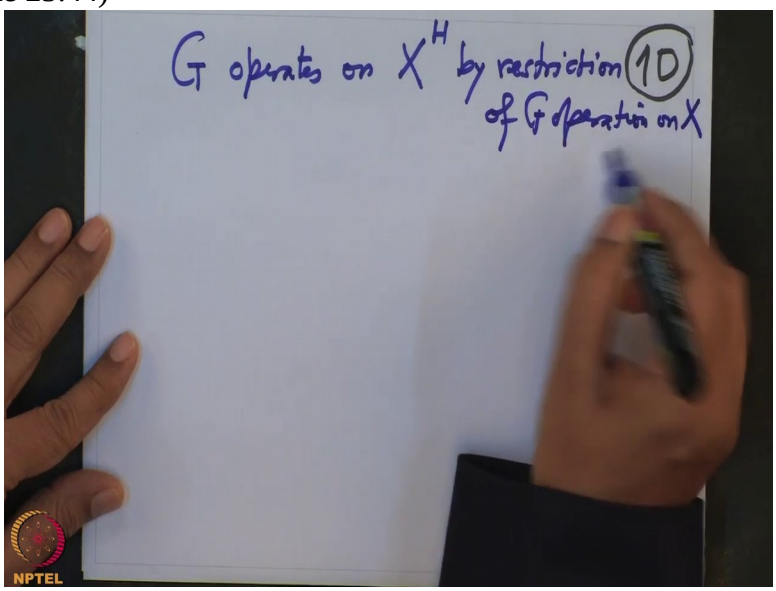
So we have proved this. So that means we have proved that X^H is invariant under G.

(Refer Slide Time 25:14)



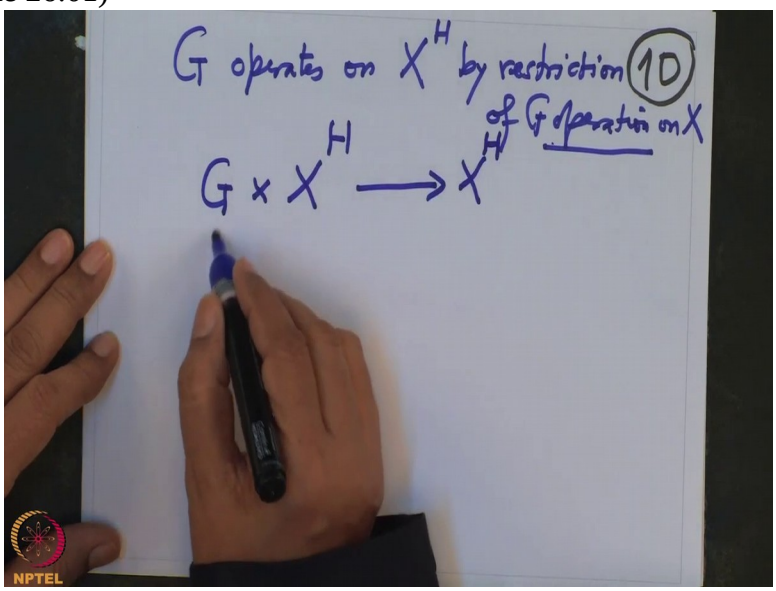
This is a subset which is invariant under G. So that means this G operates, so therefore G operates on X^H by restriction of G operation on X.

(Refer Slide Time 25:44)



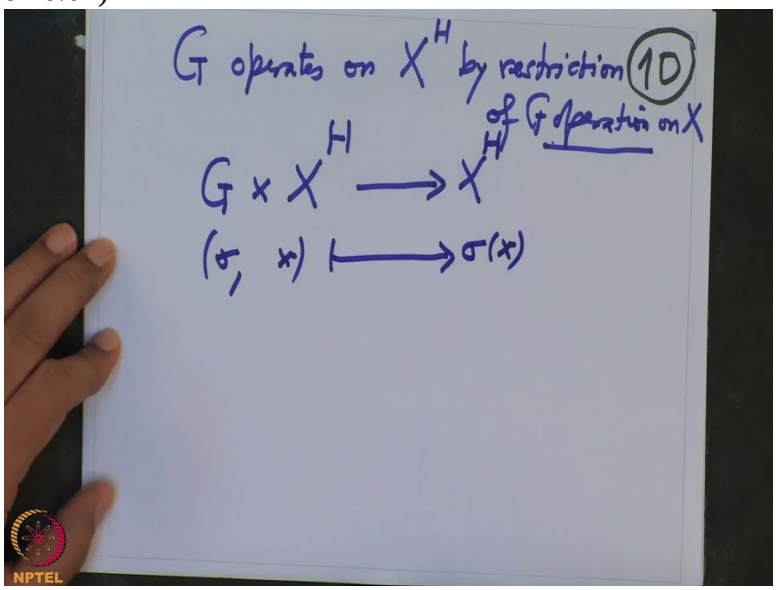
That was given to us and I will restrict that G operation to X^H. That means we have a map from G cross X^H to X^H

(Refer Slide Time 26:01)



that means any σ , x, that goes to σ of x. This makes sense. That is what we have checked

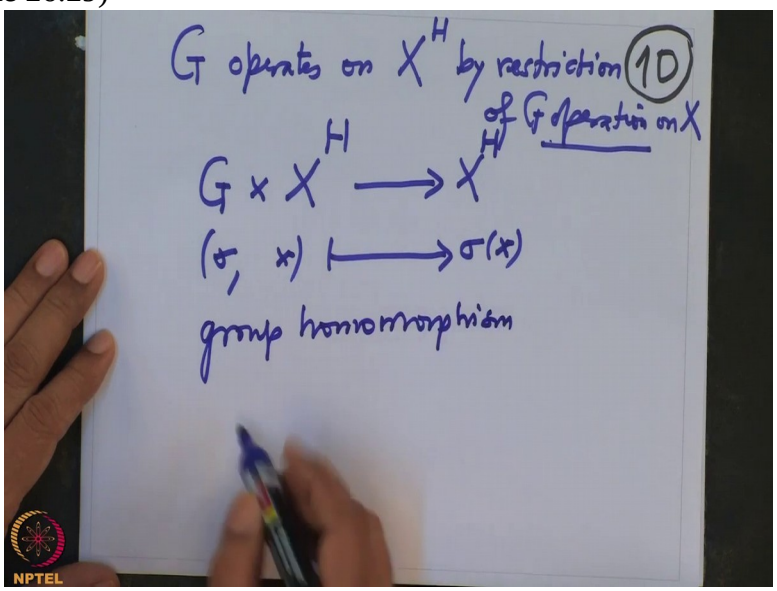
(Refer Slide Time 26:07)



in 1. But I want to say something more.

Now this operation is, will give you an action homomorphism. That means you have homomorphism. So this will give us a group homomorphism

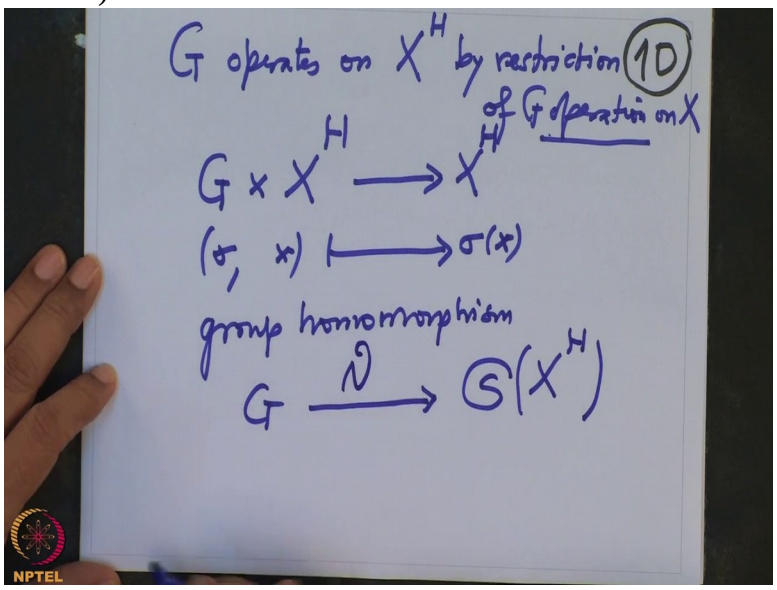
(Refer Slide Time 26:29)



from G to the permutation group on this set X^H bijections.

And therefore we want to know what is the kernel, so this is the Θ map

(Refer Slide Time 26:42)

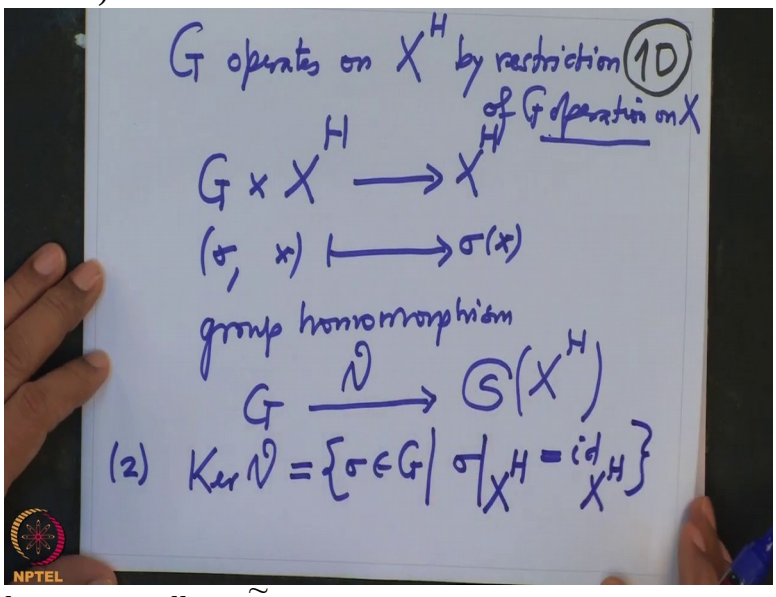


and we want to know what is the kernel of this group homomorphism. So this, now this second, this says something of the kernel of this group homomorphism.

So kernel of theta, because it is the kernel of a group homomorphism, it is a normal subgroup. So this is what, what is a kernel by definition? All those elements σ in G such that σ, when I send it here as a map from X^H to X^H, that should be identity map.

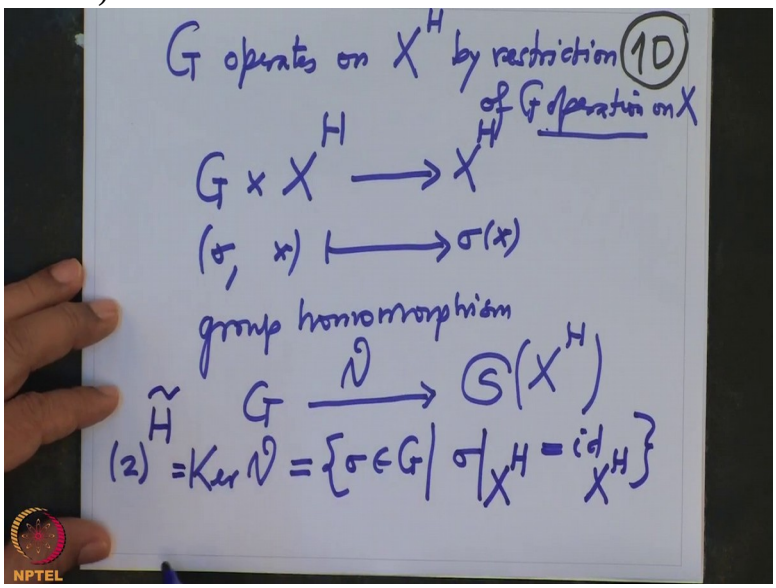
So we have restricted this to this σ , restricted to X^H is identity map on X^H . That is precisely the kernel of this group homomorphism.

(Refer Slide Time 27:27)



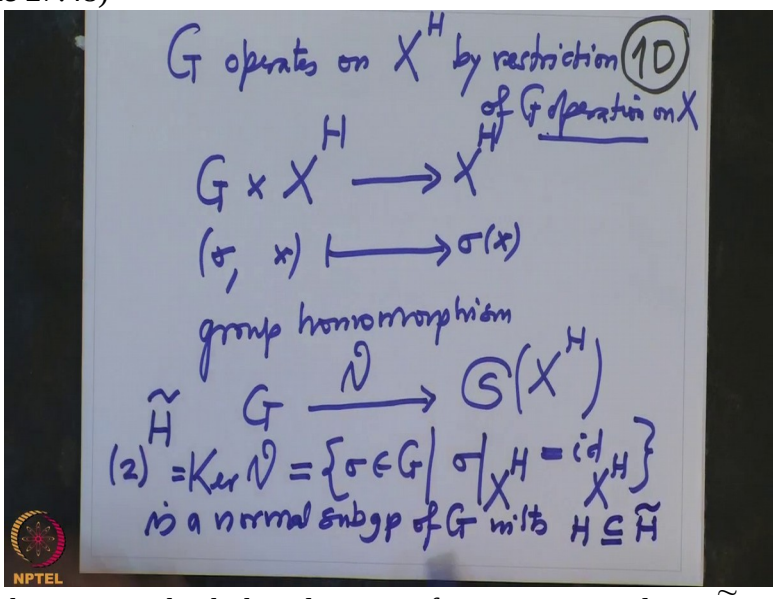
This is a non, and I want to call it $\widetilde{H}$

(Refer Slide Time 27:31)



so this is a normal, it is a normal subgroup of G with, H is contained clearly in $\widetilde{H}$.

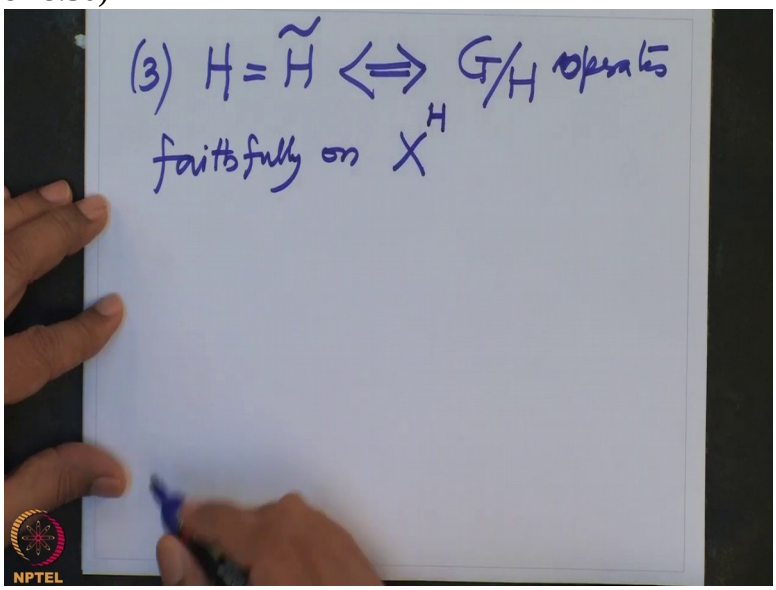
(Refer Slide Time 27:48)



This is also clear because to check that elements of H are contained in $\tilde{H}$ means that every element H in, $\tau \in H$ should, when I restrict to X^H, it should be identity on X^H but they are all elements of H, so they keep all these guys invariant. That means on that subset it is identity. So this is very clear.

Now what is more important I want to say is when will exactly this kernel be equal? So that is a statement third, H equal to $\tilde{H}$ if and only if G/H, now G/H makes sense because H is normal. This operates, operates faithfully on X^H,

(Refer Slide Time 28:50)



alright.

So that is, that is very easy to check but I want to use this. When will this be equal? When it operates, both ways are clear that is essentially the, when do you say group operating faithfully on the set, that means that the kernel is trivial.

So I want to use this information to our situation in the Galois field extension case. This I will do it after the break.