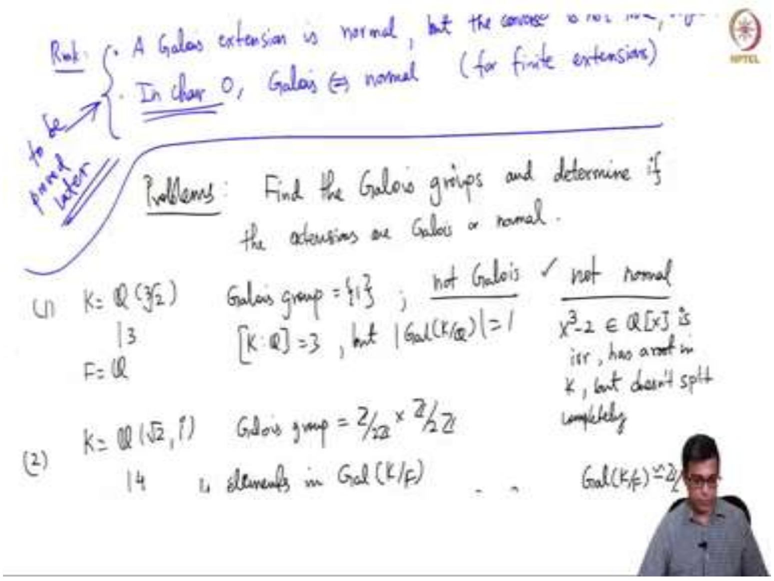
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 17
Problem Session 4

(Refer Slide Time: 0:23)



Okay, let us continue. In the last video we started doing some problems. So, let me do one more example. So, the problem asked us to find the Galois groups and determine if the extensions are Galois or normal. So, we did a few, let me do one more. And this is also an example that we discussed earlier, but I want to finish the example by proving various statements that I was making in the past.

(Refer Slide Time: 02:55)

6) $K = \mathbb{F}_{p^r}$ Recall: Frobenius homom: $\sigma : K \to K$
$|r$ (F-auto of K) $\sigma(\alpha) = \alpha^p$.
(p-prime, $r \geq 1$) $F = \mathbb{F}_p$

Checked: σ is a field homom, σ injective
So σ is surjective; $\sigma(a) = a \; \forall a \in \mathbb{F}_p$ } σ is an F-auto of K.

So $\sigma \in Gal(K/F)$.

Claim: order of σ in $Gal(K/F)$ is r.

(p-prime, $r \geq 1$) $F = \mathbb{F}_p$

Checked: σ is a field homom, σ injective
So σ is surjective; $\sigma(a) = a \; \forall a \in \mathbb{F}_p$ } σ is an F-auto of K.

So $\sigma \in Gal(K/F)$.

Claim: order of σ in $Gal(K/F)$ is r.

Pf. $\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\alpha^p) = (\alpha^p)^p = \alpha^{p^2}$. Similarly

$\sigma^i(\alpha) = \alpha^{p^i} \; \forall \alpha \; \forall i \geq 1$.

Suppose order of $\sigma = n$. $\Rightarrow \sigma^n = 1$.

$\therefore \sigma^n(\alpha) = \alpha \; \forall \alpha \in K \Rightarrow \alpha^{p^n} = \alpha \; \forall \alpha \in K$
$\Rightarrow \alpha$ is a root of $x^{p^n} - x$ in K.
$\forall \alpha \in K$

Since $\deg(x^{p^n} - x) = p^n$, $x^{p^n} - x$ has at most p^n roots in K.

But every elt of K is a root of $x^{p^n} - x$

So $|K| = p^r \leq p^n \Rightarrow r \leq n$.

But $\sigma^{p^r}(\alpha) = \alpha^{p^r} = \alpha$ ($\because$ elts of K are roots of

General statement: $f \in F[x]$, $\deg f = n$, f has at most n roots in F. F must be a field.

$f \in F[x]$, $\deg f = n$, f has at most n roots in F. F must be a field

So $|K| = p^r \le p^n \Rightarrow r \le n$.

But $\sigma^{r}(\alpha) = \alpha^{p^r} = \alpha$ ($\because$ elts of K are roots of $x^{p^r} - x$)

$\Rightarrow \sigma^r = 1$

$\Rightarrow \text{ord}(\sigma) \le r$, $\text{ord}(\sigma) = n$. Hence $\boxed{n = r}$ □

$\therefore$ The subgp gen by σ in $Gal(\mathbb{F}_{p^r}/\mathbb{F}_p)$ has order r.

$= \{1, \sigma, \sigma^2, \dots, \sigma^{r-1}\}$

in F. F must be a field

But $\sigma^{r}(\alpha) = \alpha^{p^r} = \alpha$ ($\because$ elts of K are roots of $x^{p^r} - x$)

$\Rightarrow \sigma^r = 1$

$\Rightarrow \text{ord}(\sigma) \le r$, $\text{ord}(\sigma) = n$. Hence $\boxed{n = r}$ □

$\mathbb{F}_{p^r}$ | r | $\mathbb{F}_{p^r}^G$ | $\mathbb{F}_p$

$\therefore$ The subgp gen by σ in $G = Gal(\mathbb{F}_{p^r}/\mathbb{F}_p)$ has order r.

$= \{1, \sigma, \sigma^2, \dots, \sigma^{r-1}\}$ $\therefore$ Hence $|G| \ge r$.

$$r = [\mathbb{F}_{p^r} : \mathbb{F}_p] \ge [\mathbb{F}_{p^r} : \mathbb{F}_{p^r}^G] = |G| \ge r$$

$$\Rightarrow [\mathbb{F}_{p^r} : \mathbb{F}_{p^r}^G] = r \Rightarrow [\mathbb{F}_{p^r}^G : \mathbb{F}_p] = 1$$

$\mathbb{F}_{p^r}^G$ | $\mathbb{F}_p$

$\therefore$ The subgp gen by σ in $G = Gal(\mathbb{F}_{p^r}/\mathbb{F}_p)$ has order r.

$= \{1, \sigma, \sigma^2, \dots, \sigma^{r-1}\}$ $\therefore$ Hence $|G| \ge r$.

$$r = [\mathbb{F}_{p^r} : \mathbb{F}_p] \ge [\mathbb{F}_{p^r} : \mathbb{F}_{p^r}^G] = |G| \ge r$$

$$[\mathbb{F}_{p^r}^G : \mathbb{F}_p] = 1 \Rightarrow \mathbb{F}_{p^r}^G = \mathbb{F}_p$$

Hence $\mathbb{F}_{p^r}/\mathbb{F}_p$ is Galois and $Gal(\mathbb{F}_{p^r}/\mathbb{F}_p) \cong \mathbb{Z}/r\mathbb{Z}$ □

So, the first field is FPR and this is FP, so this is F. So of course, as usual, in this case, P is a prime number, R is a positive integer and FPR is the field of out P power R. FP is a field of out of P, and this degree R extension. So in this case, let us compute the Galois group. And let us see if it is Galois and if it is normal. So, in this case, potentially Galois and normal could be different, because this is not characteristic zero.

So, and we recalled earlier the Frobenius map that we defined, Frobenius homomorphism. So, this is, in fact, a F homomorphism of F automorphism in fact, of K, namely this is K to K, sends Alpha to Alpha P. For every Alpha you send it to its Pth power. What we have checked is, checked or earlier or at least remarked earlier that sigma is a field homomorphism.

This is because of the characteristic P, only real thing to check is alpha plus beta goes to alpha P plus beta P, which it does because of characteristic P, sigma is of course, injective being a field homomorphism. So, sigma is surjective also, because it is an injective map from a finite set to itself. So, it must be injective. So, it is a automorphism. And sigma of A is equal to A for all A in FP, because every element of F P has Pth power equal to itself.

So, this is the proof that sigma is an F automorphism of K. So far so good, that means, in the new language of Galois groups, what we can say is that sigma belongs to the Galois group of K over F. So, it is F automorphism of K. Now, let us see what the Galois group is, so it contains sigma, but let us see what more can it contain. So, I first claim that order of sigma in the Galois group as an element of the Galois group is r.

So, order means it is the least integers such that sigma power R is identity, least positive integer. First we note a few things, for example, what is sigma square of Alpha; sigma square of Alpha sigma of sigma Alpha, which is sigma of alpha power P. What is sigma of alpha power P? It is alpha p power p, so this is alpha P square.

So, similarly you can check, so similarly, this is, I mean I did one case, but similarly is we can check that sigma power i of alpha is alpha power P power i, for all alpha and for all i. Now, suppose order of sigma is n, we are going to show that it is equal to r, but suppose it is some integer n, but that means, sigma over n is identity, sigma power n is the identity element of the Galois group, which means it is identity automorphism.

So, sigma N of alpha is alpha for all alpha in K. So, this implies. So, maybe I will write it here that means, sigma n is alpha is alpha, P power n equals alpha, for all alpha in K. That means, alpha is a root of, so alpha is a root of that polynomial X power P power n minus X in K. Since, degree of X power P power n minus X is equal to P power n, X power P power n minus X has at most P power n roots.

See, this is a statement for any field. So, if you have a field, so this is a general statement. Let us say small f is a polynomial in capital FX, degree F is n. F has at most n roots in F, because you can, every time you have a root X minus alpha will divide, if you have a root alpha X minus alpha divides F. So, you can divide by it and get a degree n minus 1 polynomial, which will have induction at most N minus 1 roots.

So this is a statement that we generally have over a field. It is important that it is a field, it is not true for a ring, F must be a field. So, F must be a field. In this case it has P power n roots, on the other end every element of K is a root of X power P power n minus X that is the statement.

Alpha is a root of this for all alpha and K, because for all alpha and K, alpha power P power n is equal to alpha. So, that means the number of elements of K must be less than or equal to the number of roots of X power P power n minus X. So, that means number of elements of K, which is P power r which is less than or equal to the degree of the polynomial, which is P power n. So, that means r is equal – n is at least r.

So, that means, the order is at most order is at least r, but we do know that sigma power P power r of alpha is alpha power P power r, which is alpha, this is because elements of K are roots of, this is from the structure theorem of finite fields. So every element of K is a root of X power P power r minus X. So, it must satisfy alpha power P power r equals alpha.

So, this must be the case. So, this implies order of, so this implies sigma power r is identity. So, order is less than or equal to r. Order is the smallest positive integers such that this has property. So, which is n, so hence, N is less than equal to r as well as greater than equal to r. So order is equal to r by this analysis, so that proves the claim.

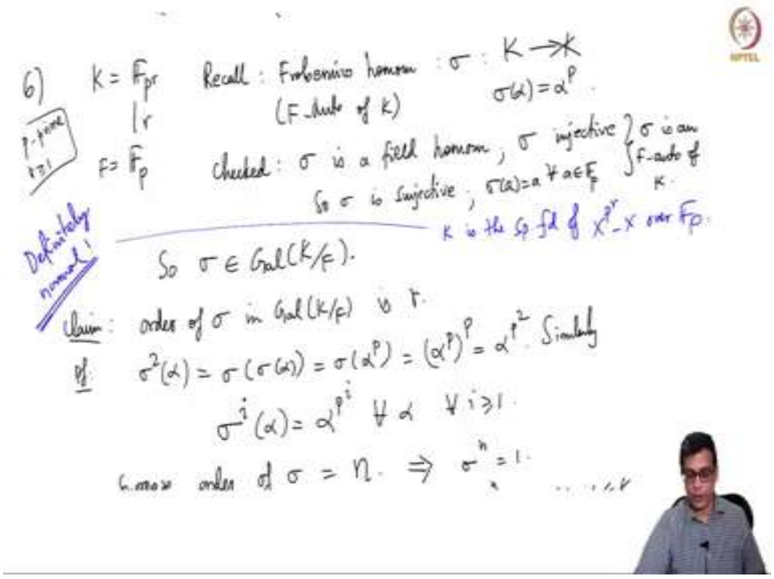
So that means the subgroup generated by sigma in the Galois group has order r. So, the if, you have an order r element, the subgroup generated by that is equal to 1 sigma sigma square and so on. And it will go up to sigma r minus 1, that has order r. So, this is order now, let us just see where we are. So, in particular, order of the Galois group, let us call this G for simplicity is at least r because it has a subgroup or not, so number of elements in r itself must be at least R.

So, now, let us write down this following set of inequalities. So, r we know very well is the degree of this field extension FPr or FP, but this is greater than or equal to the -- because FPr is here, the fixed field will be somewhere here and this is FPr, sorry FP. So, the fixed field always contains FP, FP being the prime field or more directly any automorphism in the Galois group must fix FP.

So, this is something we have, but this by the various theorems that we proved about fixed fields is precisely the cardinality of G, but that we know is at least r, so we have r, greater than equal to r, so everything in the middle is equal to r. So hence, the only possibility is FPr colon FPrG is r. That means FPr fixed field over FP is 1. So, if this is r, this is 1, because the whole thing is r.

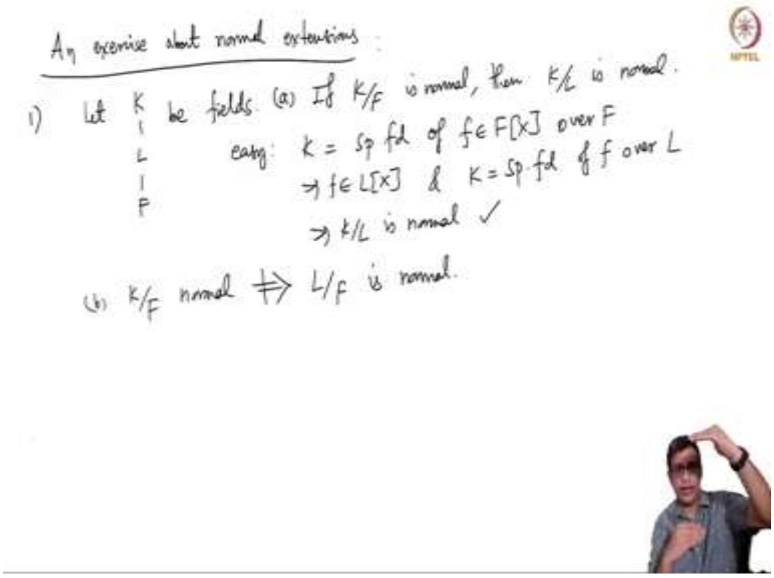
That means, any degree one extension means they are equal. So, the fixed field is FP. So, hence, it is not a Galois. So, it is a fixed field. So, the cardinality of the Galois group is r is in fact, more we can say it is the cyclic group generated by sigma. So, it is cyclic group of order r. And of course, it is always normal, I should have said this at the very beginning, this is normal.

(Refer Slide Time: 10:08)



This is normal because of the structure theorem, because this K is a splitting field of, let me just squeeze that here K is the splitting field of X power P power r minus X over FP. So, it is a splitting field of a polynomial. So it is normal, it is also Galois and its Galois group is cyclic, that is the observation.

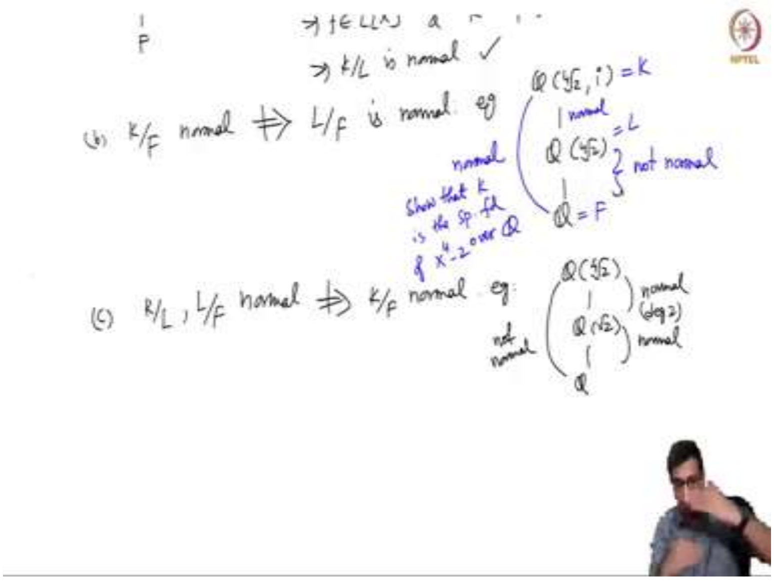
(Refer Slide Time: 10:44)



Now, let me do an exercise about normal extensions. So, I will give you a few properties of normal extensions in this exercise. So let me make a few statements and while we will prove that one by one. So, one, let KLF be fields, if K over F is normal, then K over L is normal. So, this is because this is the first point, a, let us say.

This is easy, because K is a splitting field of, by one of the equivalent conditions for a normal extension, k is the splitting field of let us say F in FX over F, but that polynomial lives in FX. So, F is also in LX and K is the, K will continue to be the splitting field. There is no problem because it is generated by the roots over F, so it is also generated by the roots over L. So, this implies that K over L is normal. No problem, but it is not true, does not imply L over F is normal.

(Refer Slide Time: 12:22)



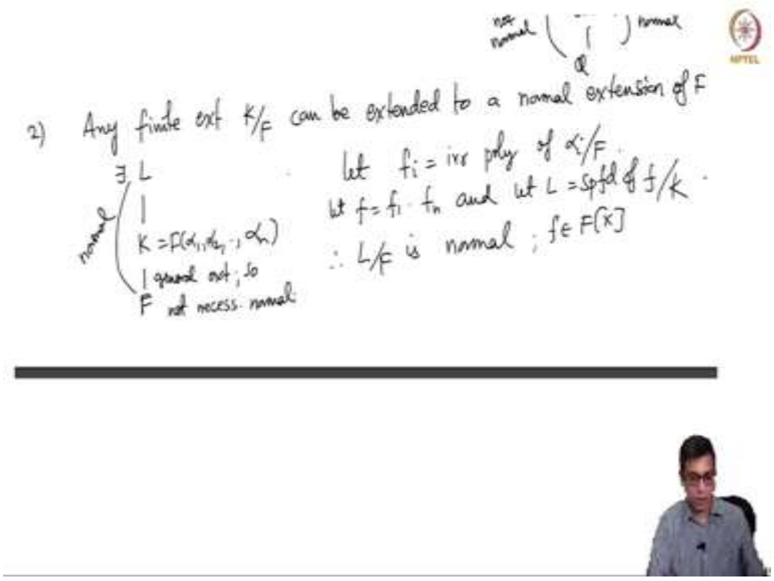
So, in general, if you have a tower of three fields, the bigger X, that top over bottom is normal implies, the top half is normal, bottom half is not in general normal. And the reason is example is you can simply take Q, adjoin fourth root of two comma i to Q adjoined fourth root of 2 to Q. So, this is not normal we know. This came up in the previous problem, because it is not a splitting field, rather X power 4 minus 2 has a root in this, but not all the roots, this is not normal, however, this is normal.

So, I will let you prove this for yourself. Show that, so here it is K, this is L, this is F, show that K is a splitting field of X power 4 minus 2 over Q. And the reason that L fails to be normal is because it is missing roots. And once you provide those roots it will become normal. So, in fact, every field extension can be extended to a normal extension as I do in a problem a little bit later.

So, the bigger top to bottom is normal and this is normal of course, by the first part, but this is not normal. So, that is – that can happen. And finally, if K over L is normal, and L over F normal, does not mean K over F is normal. So, if you have three fields, one above other, and the both halves of the tower are normal does not mean the entire tower is normal. And this example is you take Q adjoined fourth root of 2 over Q adjoined square root of 2 over Q.

This is normal by because it is a degree to extension. This is also normal, these are both degree 2. And by one of the properties of something I did in the previous set of problems, any degree to extension of fields is normal. So these are both normal, but this is of course not normal by that came up earlier also. So normal extension followed by another normal extension may not imply that the entire extension is normal.

(Refer Slide Time: 14:47)

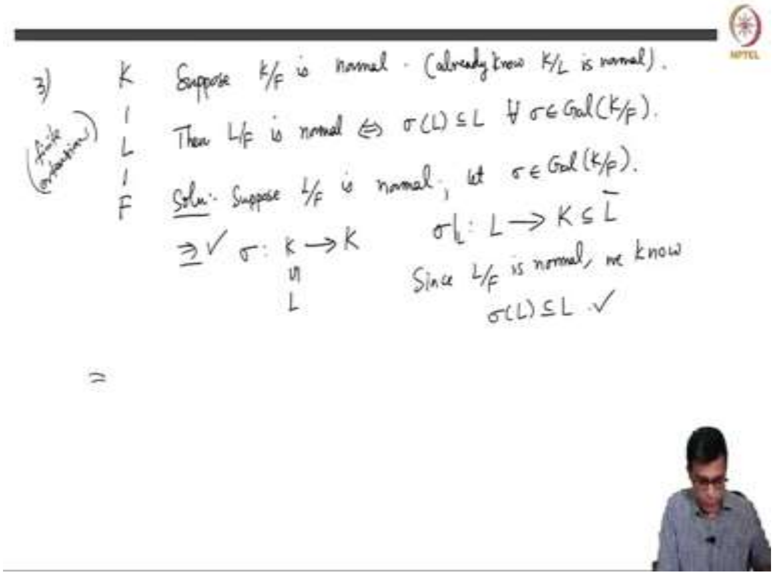


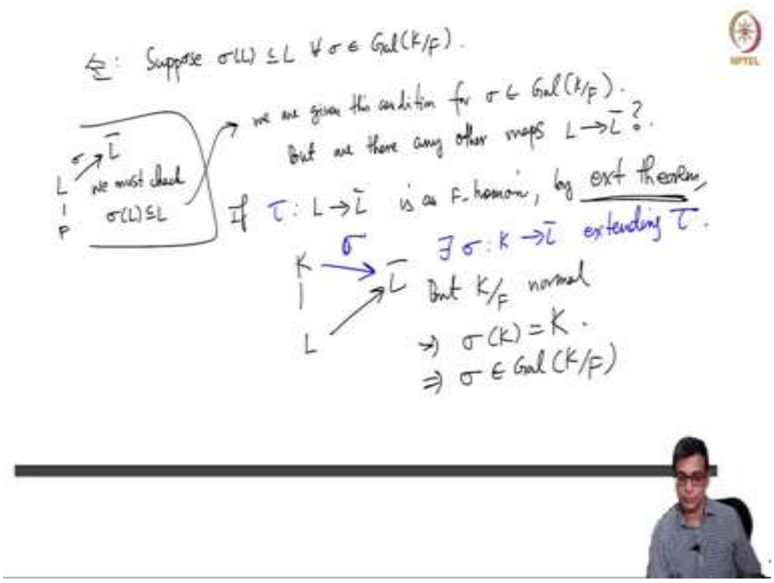
So, let us analyse these a little bit more to see what we can say about a normal extension. So but let me first get the following clear. So, any finite extension K over F, can be extended to a normal extension, by which I mean. So, if you are given a -- So, let us say K over F is given. So, write K as F of alpha 1, alpha 2, alpha r or alpha n.

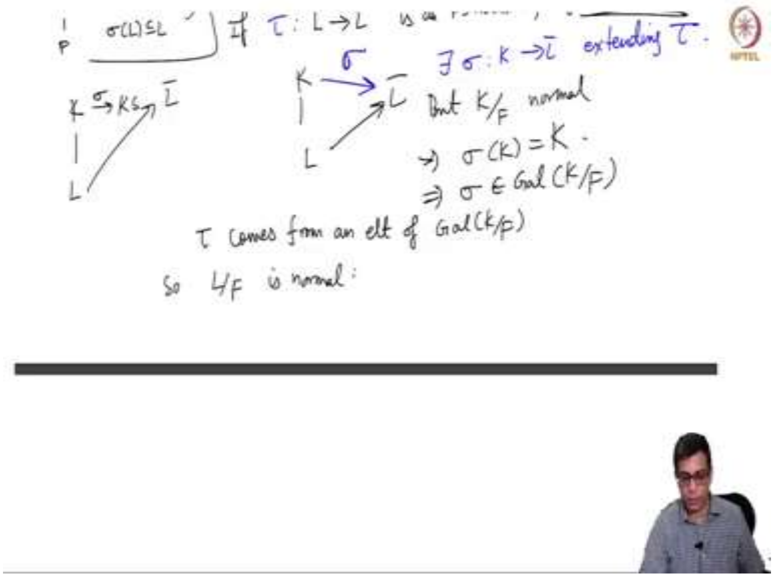
So, take fi to be the irreducible polynomial or let I should write, let fi be the irreducible polynomial of alpha i over F. So, when I say I can extend it I mean that you can find a bigger field L, which is normal over, so there exists L is what I am saying, normal extension of F. So, then you take F to be F 1 times F n and let L be the splitting field of F over capital F.

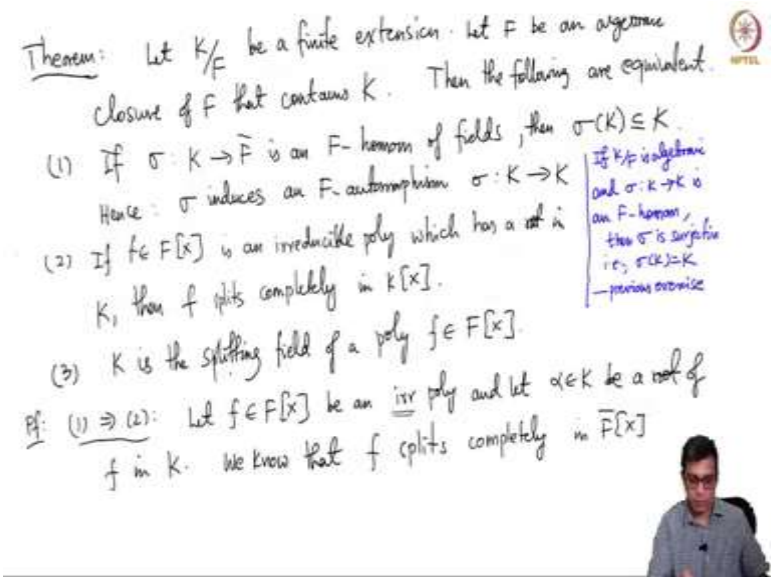
Because or you can take over capital K, no problem. So, it is a splitting field over capital F. So, then L over F is normal because it is a splitting field of the small f over capital F, because f is a polynomial in FX and it is generated by the roots. So, any extension can be extended to, this is not, this is a general extension, so not necessarily normal. So, this is not necessarily normal, but you can always put it inside a normal extension.

(Refer Slide Time: 17:00)









23:01, 23:24So now finally, let me do one more feature of Galois extensions. So, let us take a tower of fields, let us take K L over L over F. So, these are extensions and let us suppose that K over F is normal. And let us take. So, what I want to say is that suppose this, so suppose K over F is normal, we already know, K over L is normal. But in general L over F is not normal, but when is it normal? So, that is what I want to say.

Then there are all finite extensions. By the way, everything I am doing is finite extensions. Sometimes it may be true in general, but I do not want to deal with infinite extension. So, everything I am doing is a finite extension, normal Galois extensions for me are always finite, then L over F is normal if and only if the following happens, sigma L is contained in L for all sigma in the Galois group of K or F.

So, this is what I want to show. So, why is this? I want to show that L over F is, so in general L over F is not normal as this example shows here, but it is normal if this condition is satisfied. So, let us check this. So, suppose L over F is normal, suppose L over F is normal, then let us take sigma in the Galois group of K or F.

So, then if you restrict, so sigma is a function from K to K, but L l is here, so you can restrict to L, that will be a function from L to K, we do not know a priori that L image of something in L again in L but it is in K. However, remember the one of the conditions for a normal extension, which I did way back is that any map from K to F bar has the property that image lands again in K.

So, sigma restricted to L is a function from L to L bar because K obviously is contained in L bar. Since L is normal over F we know sigma L is contained in it. So because this is the equivalent condition for normality, so this is okay now, so let us prove this condition. This is exactly the same condition. Because suppose sigma L is contained in L for all sigma to prove, this is normal, let us do the following. So, what am I supposed to do? Yeah, so this is normal, but this any.

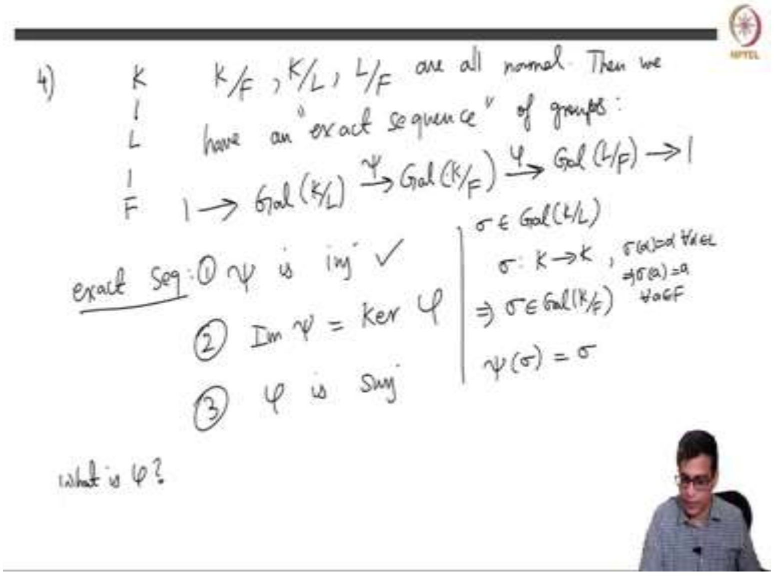
So, to check normality, what we have to check is you give me any map from L to L bar, we must check, yeah, so this is essentially given any such maps, we must check sigma L is contained in L. So, what we are given is that, we are given this condition for sigma in Galois group, but can we show this for any map from L to L bar? So, let us take, but are there others, I will write.

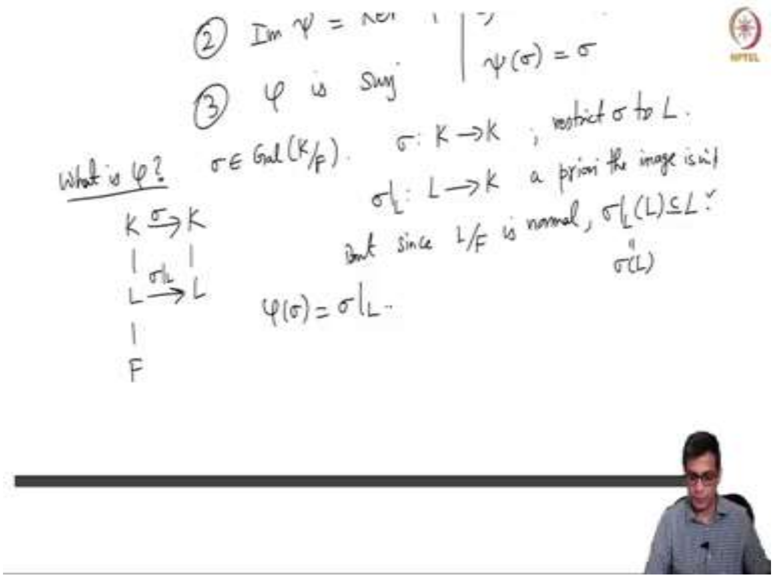
Are there any other maps from L to L bar, I claim there are none, because if tau from L to L bar is a field homomorphism, is F homomorphism by extension theorem. So, L to L bar is given, and K is a finite extension this there is an extension like this. There exists tau, this is sigma K to L bar extending tau, but this is by extension theorem, but K over F is normal implies tau of K is contained, in fact equal to K.

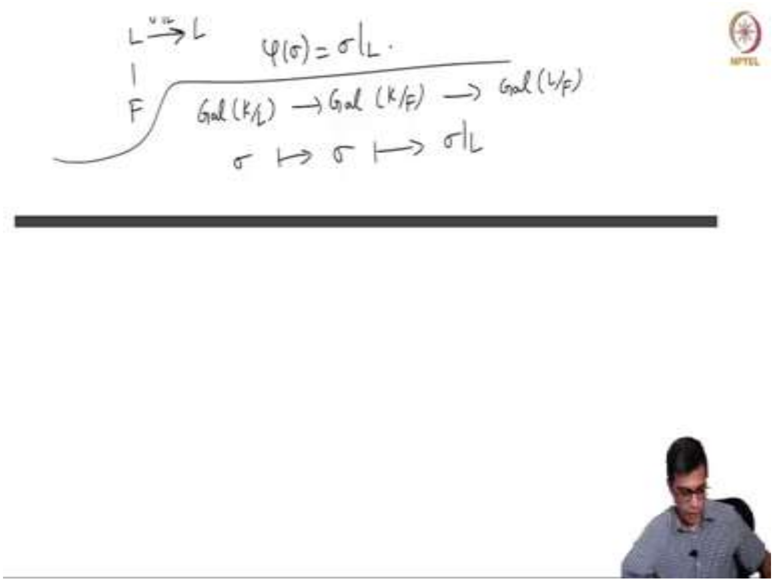
Because normal Extension has that property, any map from K to an algebraically close field must have this equal image, must be equal to K. So, that means sigma must be a priori an element of the Galois group. So tau must come from, so tau comes from an element of, I am sorry, I am going on this very fast. But I want to do one more example. So, I wanted to quickly finish this, but please play pay close attention.

If you have any math from L to L bar, it must come from, it must come from a Galois group element. So, and for those, we have this condition, so that means L over F is normal, again by our main theorem about normal extensions. So, in general, if you take a tower of fields, in the top to bottom is normal, the bottom half is not necessarily normal and this gives you a condition for checking the normality.

(Refer Slide Time: 23:44)







Now, let me do one final thing. And I want to sort of go over this fast, because I am running out of time. But I will set it up for you to complete this. So, suppose these are normal and everything in the in view is normal. So suppose we have these normal, all of them are normal, then we have an exact sequence. So I do not want to, I mean, maybe this is something that you are not seen before, but exact sequence of groups.

So, let me explain what this is and then we will, I mean, I will explain everything. So, what we have is, I will explain what I mean by an exact sequence. What is an exact sequence? So, I mean that let us give these names. So let us call this phi and let us call this sigma not psi. So, exact sequence means psi is injective, image of psi is equal to kernel of phi. And finally, phi is surjective. First of all, what are these maps?

I need to define this. You take an element in the Galois group of K over L. So that means it is a function from K to K, which fixes L point wise. But then it implies, it fixes everything in F point wise. No problem. Everything in L is fixed point wise, so obviously everything in K is fixed point wise. So, that means, sigma belongs to the Galois group, it is a k automorphism, automorphism of K which fixes everything in F.

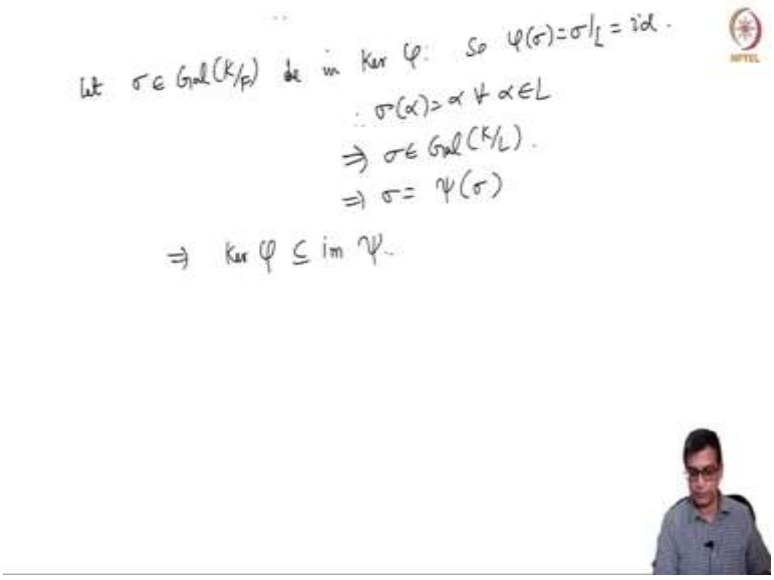
So, that means, psi of sigma is actually just sigma, because an element here is an automorphism of K, but it must fix L point point wise. Here these are automorphisms of K that fix F point wise, but if something fixes L point wise, it definitely fixes F point wise. So, psi is simply an inclusion and it is certainly an injective map, because if psi is non-zero, non-trivial map that means it is not identity, its images sigma itself.

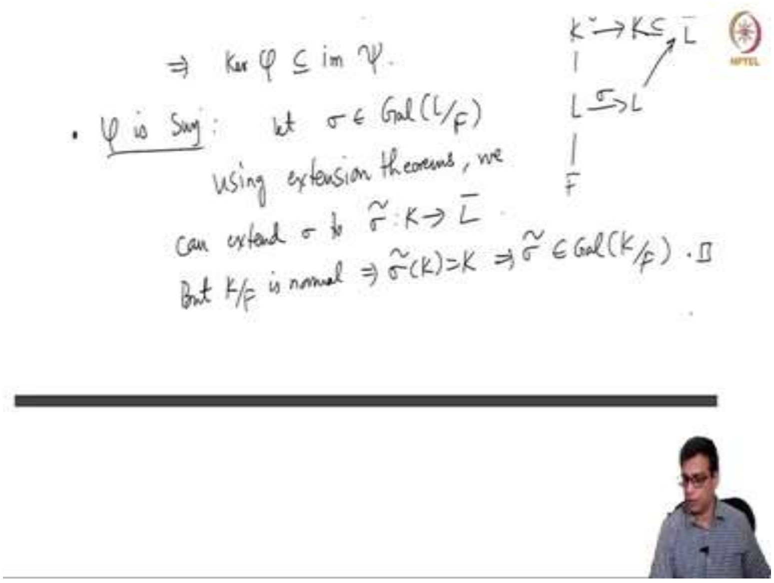
So, it is not identity. If sigma is not identity, its image, which is again sigma is not identity. So, that is okay. What is phi? So, for phi we start with an element of Galois K over F, that means, it is a function from K to K, so restrict sigma to L. So, you have K here, K to K here, L here, F here. So, restrict sigma to L, a priori it is to K, the image is K, but since, this is the previous problem, L over F is normal, sigma L of L is contained in L.

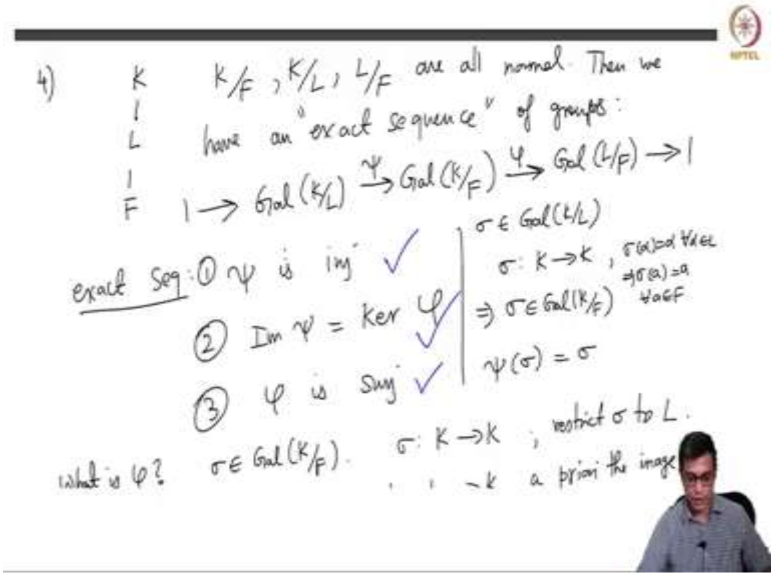
This is of course, same as sigma L. So, this also goes to L. So, this is the property that it is normal, so it is L over F is normal. So, image of any element of L must go to a conjugate but once I, element irreducible polynomial has one root in L, it has all the roots. So, all the conjugates are also in L. So, this holds. So, phi of sigma is simply sigma restricted to L.

So, this is just to rewrite everything now, what we have is Galois K over L to Galois K over F to Galois L over F, automorphism of K which fixes L pointwise goes through itself and then it goes to sigma restricted to L. This exact sequences have this one at the bottom at the left hand right hands, that is just a notational issue, it simply says that this is injective This is subjective and the at the middle your kernel equals image.

(Refer Slide Time: 28:19)







So, now, we have checked that phi is injective and let me quickly tell you how to check kernel of phi equals image of psi. So, suppose, sigma is an image psi. So, really there is not much here, it is just a matter of keeping track of the notation. That means, it comes from an element of the Galois group of K over L. So, sigma restricted to L is identity because it fixes L point wise. So, sigma restricted L is identity that means, phi of sigma is identity. So, image phi is contained in kernel phi. So, if something comes from psi, it must map to identity.

So, that means, it is in the kernel of this map. So, on other end, suppose something is in the kernel of, so let sigma be in the image of, sorry, sigma be the Galois group of K over F, be in the kernel of phi. So, phi restricted to L, which is exactly, sorry, phi of sigma which is sigma restricted to L is identity. That means, if you spell that out, sigma of alpha equals alpha for all alpha in L. So, sigma is in the Galois group of K over L. So, sigma is equal to psi of sigma.

So, this implies in a kernel of phi is contained in image of psi, image of psi is contained in kernel of phi.

So, the second condition is also okay. Finally, we have to check the third one which is that phi is surjective and this is just a extension theorem statement. So, let sigma be in the Galois group of L over F. So, that means it is a function from L to L, but then anything like this, of course, maps to L bar which is K bar, so you can extend it to K. But this extension, because K is normal over, F must land this. So, using extension theorem and this guy sort of came in the previous part.

We can extend, so this is sigma tilde, sigma to sigma tilde from k to L bar a priori, but k over L is normal or K over F is normal, because remember everything here is a F homomorphism. So, base field is important, K over F is normal implies sigma K is K. So, sigma tilde is an element of, remember because it is an F homomorphism it fixes F point wise, so it is an element of the Galois group of K over F.

So, everything so, that and further let me write one more line. So, phi of sigma tilde is sigma implies phi surjective. So, this proves that phi is surjective. This is a nice thing to keep in mind. We have, this tells you if you have a tower of three fields, how the three Galois groups in question, you have Galois group of the entire thing, Galois group of the top extension, Galois group or the bottom extension.

So, there is an exact sequence where the middle thing is the Galois group of the entire extension, top to bottom, left is a Galois group of the top most extension, right side is the Galois group at the bottom extension, and they fit in in this nice picture. So, I wanted to do this because it is important for us when we start talking about main theorem of Galois theory.

So let me stop this video here. I hope these two problems sessions gave you an idea of how to solve problems about Galois extensions, normal extensions. In particular, we learned about several Galois extensions, several extensions when and computed their Galois groups and determined whether they are Galois or not, and whether they are normal or not. And then we learned about some properties of normal extensions. So, let me stop this video here. In the next video, we will continue our study of Galois extensions. Thank you.