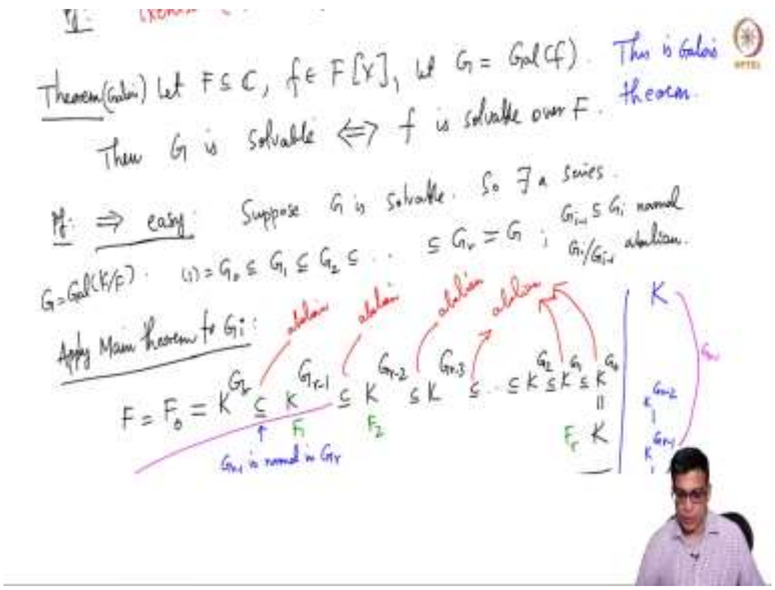
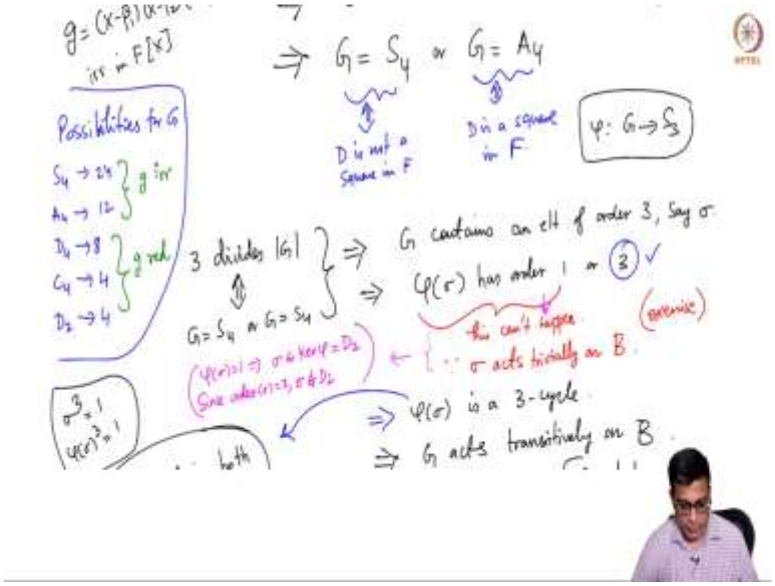
Introduction to Galois Theory
Professor. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No. 43
Solvable Groups – Part 2

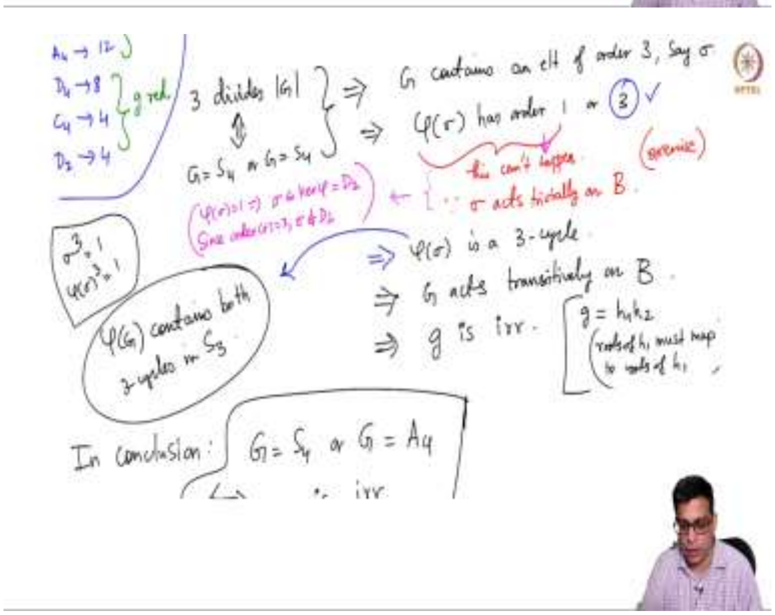
(Refer Slide Time: 00:17)



Welcome back, we are proving this important theorem of Galois; which says that a polynomial is solvable if and only if its Galois group is solvable, very simply speaking. So, this is the main achievement of Galois, and this is where we solved the problem of insolvability of context; in fact it did more than that. He gave a very group theoretic characterization of solvability of a polynomial. So, using this method we have the classical notion of solvability of polynomials, or expressing complex numbers using radicals. And he connected it to the modern notion of solvability of groups, which he in fact created. So, we proved one direction. Before we continue the proof let me quickly settle a issue that I last time had.

(Refer Slide Time: 1:05)



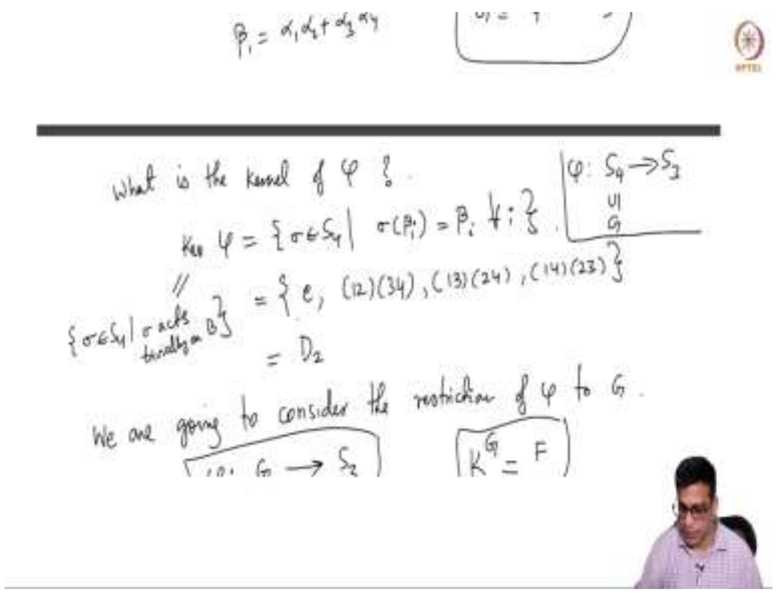


So, this I wrote it already here. So, if you remember we were discussing quartics, and analyzing them and proving that quartics are always solvable by radicals. I did not explain one point when I was doing this. So, I do not want to get into the details of the proof; but you can go and see that video. I think it was one or two videos ago. There we encountered a situation where G is a Galois group in question and it contains an element of order 3 by hypothesis. Because 3 divides order G, this is the assumption that we are making. And then we want to conclude that the polynomial in question or rather the resolvant cubic of the polynomial in question is reducible.

In order to do that we first note that G by hypothesis contains an element of order 3 called the sigma. And its image has this property, if sigma cubed is 1, phi sigma cubed is 1; so the order of phi sigma is either 1 or 3. If it is 3, our proof works and we conclude that it must be a 3-cycle; because it is 3, order 3 element in S3. So, it must be a 3-cycle, which in turn implies that G acts transitively on the set beta 1, beta 2 and beta 3; which in turn implies that G is reducible.

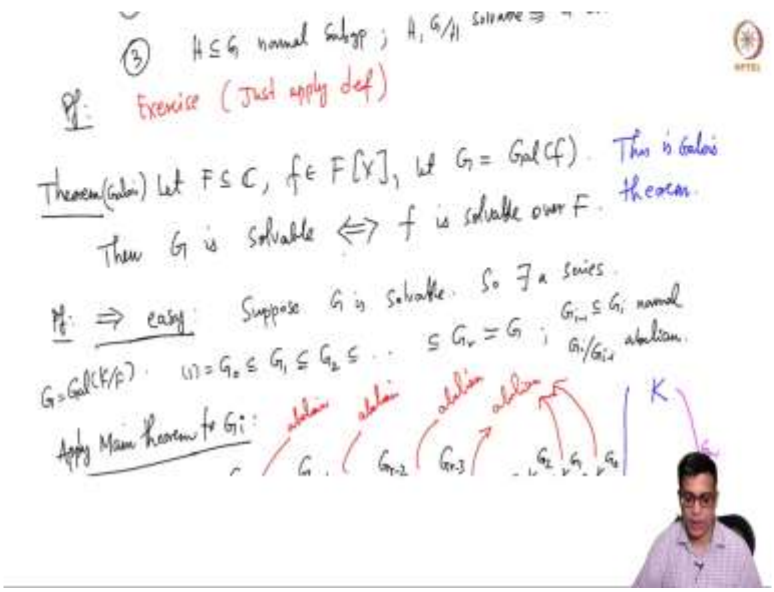
But we need it to rule out the possibility as that phi sigma has order 1; but if phi sigma has order 1 that means phi sigma is 1. The only element of order 1 in any group is identity element. If phi sigma is 1 that means sigma is in the kernel of the map phi. But, kernel of the map phi is D2, as I noted earlier in the proof.

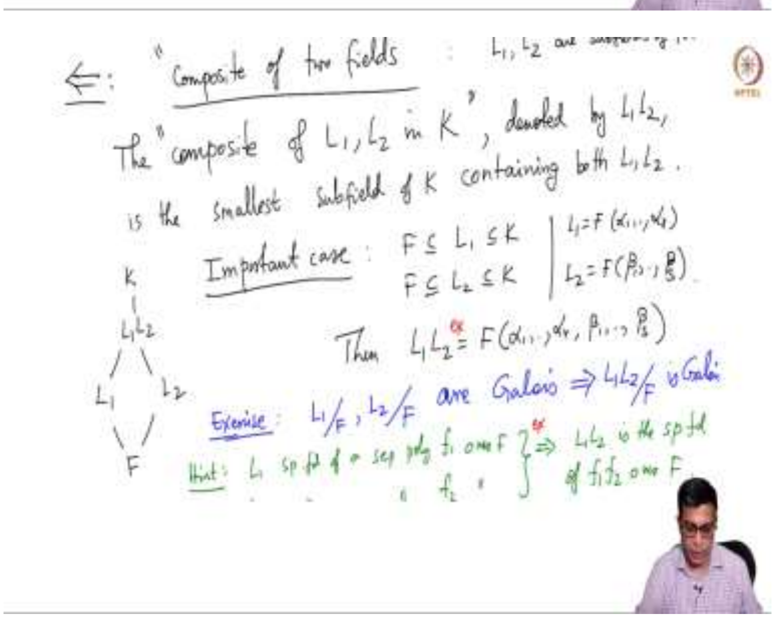
(Refer Slide Time: 02:44)

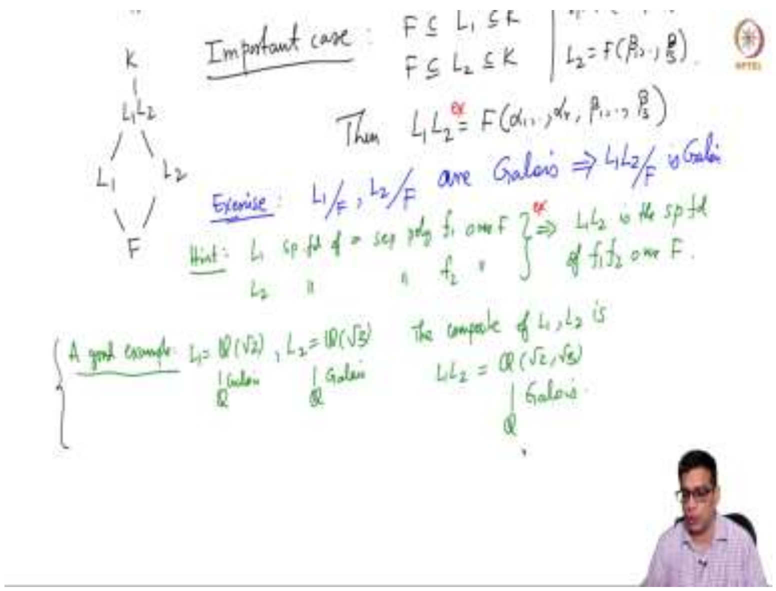


Kernel is those things that fixed beta I is; but that means that exactly consist of these permutations. But, this is a problem now, because D2 is the client for group; in particular it has order 4. But, order of sigma is 3; so n order basically what I am saying is that n order 3 element cannot be inside an order 4 group. So, phi sigma cannot be order 1. So, let me now get back to the main part of the proof; proof of the main theorem that we are doing. I hope that was clear. So, that I just wanted to fix that before proceeding; because that I left without proof last time.

(Refer Slide Time: 03:27)





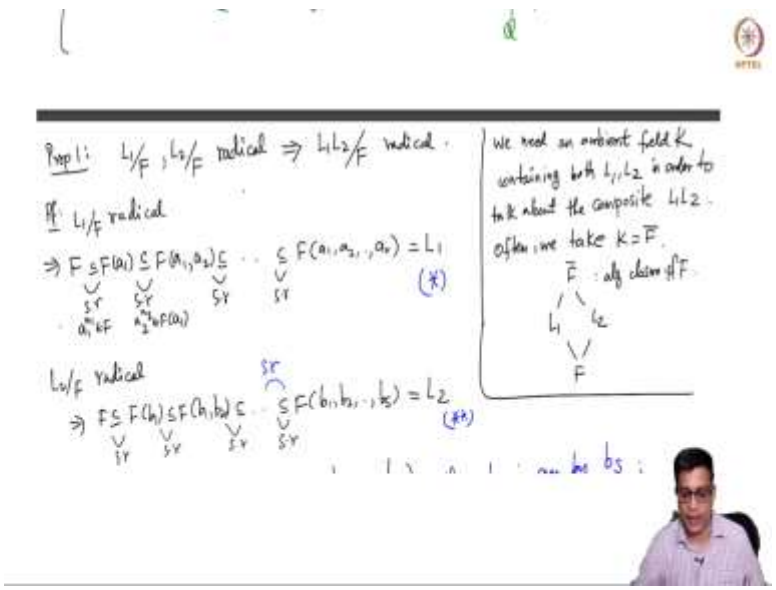


Now, let us get back to this; this is the main theorem that Galois proved towards solvability of polynomials. We proved already that the Galois group is solvable, the polynomial is solvable; this is sort of straightforward computation. We are now going to the prove the converse, and in order to prove the converse I need to introduce some notions about composite of two fields. And the composite is the is this smallest field containing both of them. So, we have to fix an ambient field K that contains both L1 and L2; composite is the smallest subfield containing both of them.

And the most important case for us is this situation; where both L1 and L2 actually are extensions of a fixed capital F, generated by alpha a's and beta j's. Then the composite is simply generated by the union of these things. I already wrote this, this is new, so a good example in fact this sort of the typical example that you have to consider, is if you have L1 is Q root 2, L2 is Q root 3. Then all you need to take for the composite is Q root 2 comma Q root 3.

So, this is the composite, it is just a fancy name for something your very familiar with this. And the last time I left as an exercise for you to statement that composite of 2 Galois extension is Galois. This is not difficult; this is just standard Galois Theory. So, in fact I gave you a hint which more or less solves the problem.

(Refer Slide Time: 04:59)



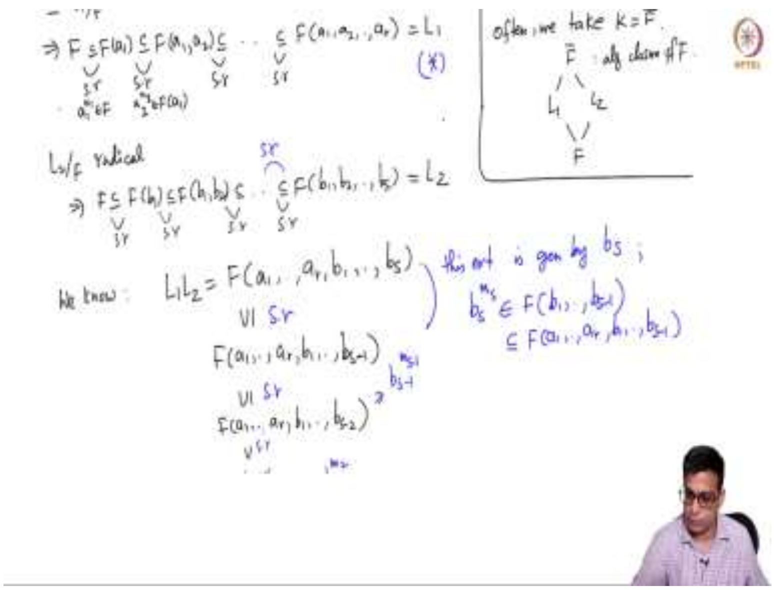
So, now let me do a couple of more prepositions which, which are needed for the converse of our main theorem. Suppose we have 2 radical extensions L1 and L2; I claim that their composite is also radical. So, now just I heard about that ambient filed, we always we need an ambient field K containing both L1, L2 in order to make sense of, in order to make sense of the composite. Because it without this ambient filed which contains both L1, L2; the composite does not make sense. But, otherwise the ambient field is relevant.

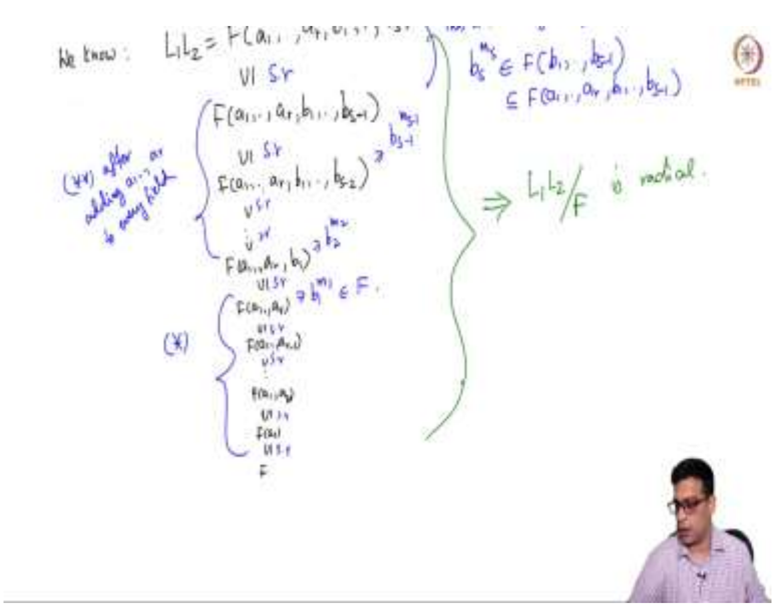
So, often we can take K is to be F bar. So, our main situation will be L1 L2 be infinite extensions of F. So, if you take F bar containing both L1 and L2; this is algebraic closure of course of F; that will play the role of this ambient field. So, in the prepositions that I am now going to write, I will mention this ambient field. But, you can work with any field that contains both of them; in particular you can take the algebraic closure, of all three of them will be the same. So, let us prove that composite of two radical extensions is radical.

Now, we know that L1 over F is radical means; there is a tower of simple radical extensions, where the last field in the tower is L1. So, I am going to write it like this. F contained in a1 contained in a1, f adjoint a1, a2 and all the way up to a1, a2, ar; this is L1. Now, what is the property? This is simple radical that means a1 power n1 is in F. This is also simple radical that means a2 power n2 is in F a1. So, this was something that we called F1 earlier; this we called F2, this we called Fr.

But, I do not want to introduce that kind of notation now; I want to keep track of this radical elements that we attached in this tower. So, we have a series of radical extension simple radical extensions standing with L1. So, similarly L2 F L2 over F is radical implies we have also similar tower; so F contained in F of b1 contained in F of b1 comma b2, and all the way up to bs which is L2. So, this is simple radical, this is simple radical, this is simple radical, this is simple radical. So, radical extension is simply by definition a tower of radical simple radical extensions, ending with whatever field you started with.

(Refer Slide Time: 08:17)





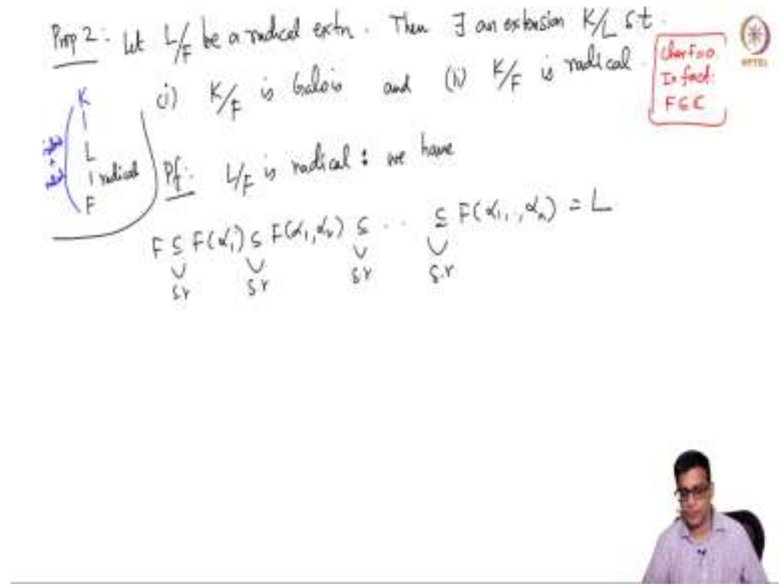
Now, we know by the analysis that I did in a previous slide and in the last class, the composite is simply F adjoint the union of these generators. So, I claim that this is radical over F and the tower of simply radical extension is staring right in front of you. So, what do we do? We do first V1 through bs minus 1; so this extension is generated by bs, because all the other things are common. So, if you take this as the base field, this field is generated over this base field by bs. And we know that bs power some ms is in right; this is by definition. Because this is simple radical that means bs is the last attach element; so, it is power is in the previous field which is that.

But, of course this is contained in this bigger field, which is exactly what you see here; so this is simple radical. So, now we leave a1 through ar as they are; but remove bs minus 1 from this; so, this is also simple radical because bs minus 1 generates this, this over this and this belongs to this; now you keep going like this. So, do not disturb a1 through ar; so the previous one will be generated by b2, and some power of that will be in this. So, this is simple radical also; so all of these are simple radical. Now, you consider this, I claim that this is also simple radical; because b1 power m1 belongs to F.

So, it is certainly belongs to this, so this is simple radical. And now, you just put this tower underneath this. So, just to spell it out I get a1 through ar minus 1; a1, a2, a1, a, F. All of these are simple radicals; of course this part, this part is just this part, this is just star. This is if we call this the second one star star; this is star-star after adding a1 through ar to every field. So, you take star-star and add a1 through ar.

So, if you take a radical extensions tower of simple radical extensions, attached some say common elements to all the fields in question, it will remain simple radical; so that means so the conclusion of all this is. So, conclusion of all this is L1L2 over F is radical as we need. So, this is just an easy observation; but it is good to make this and repeatedly use them. So, composite of simple radical extensions is simply radical.

(Refer Slide Time: 11:53)

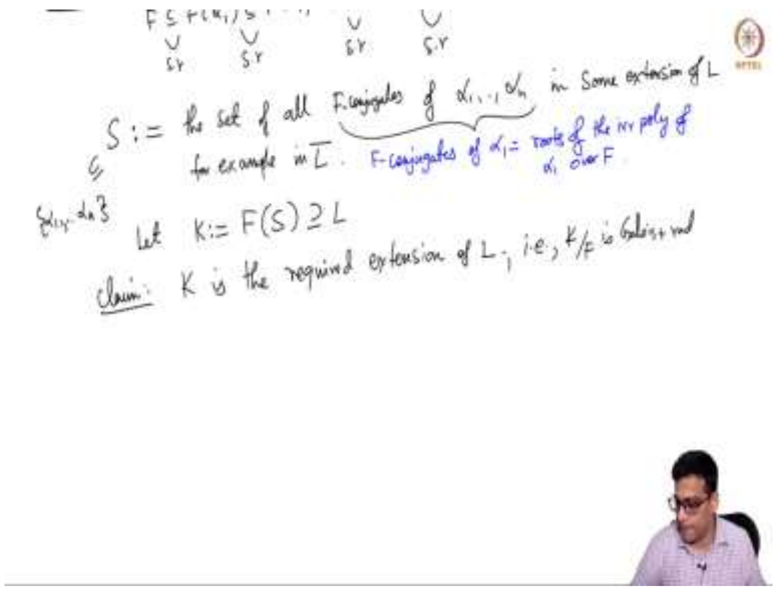


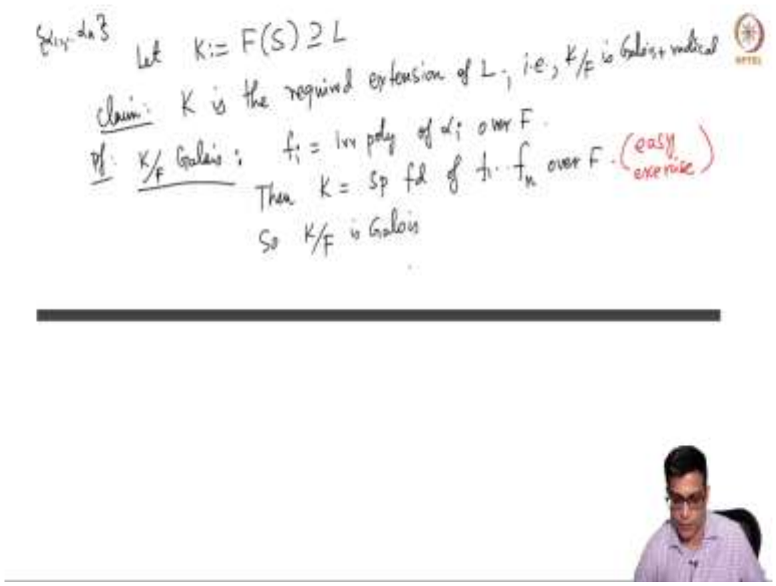
Let me do one more proposition, this is a very important proposition that we will often use. So, let L over F be a radical extensions, let L over F be a radical extension. Then, there exist a an extension K over L such that two things are connect. K over F is Galois and K over f is radical. So, any radical extension can be extended further to get remain radical; but now the new thing will be Galois. So, this is given L over F is given, you can construct one which is Galois plus radical. So, and this is going to be very useful to us and often we will apply this; because often we want to work with Galois extensions.

So, if we have a given radical extension, it may not be radical; but we can always extend and get Galois plus radical. So, in proofs that will come later given a radical extension, we might as well assume that this is Galois, without loss of generality. So, the construction of K that will do job for us is fairly straightforward. So, I should also remark here that; I am going to assume characteristics 0 throughout for the rest of the course. So, in fact going to work generally with subfields of C; every field that we consider is subfield of C, and their finite extensions. So, they also will be contained in C.

So, now let us go ahead and prove this; this is also sort of easy application of the previous two previous prepositions, and the exercise that I gave here. So, what do we do here? So, first L over f is radical; so we can write just like in the previous theorem proposition. We have F contained in F of let me call alpha 1, F of alpha 1, alpha 2; all the way up to F of alpha1 let me call that alpha n, which is L. So, the point is this is simple radical, this is simple radical, this is simple radical, this is simple radical. Simple radical remember, let me remind you is that alpha1 is some root of an element of F. So, that means alpha1 power some n1 is in F; alpha 2 power n2 is in this field and so on.

(Refer Slide Time: 15:01)





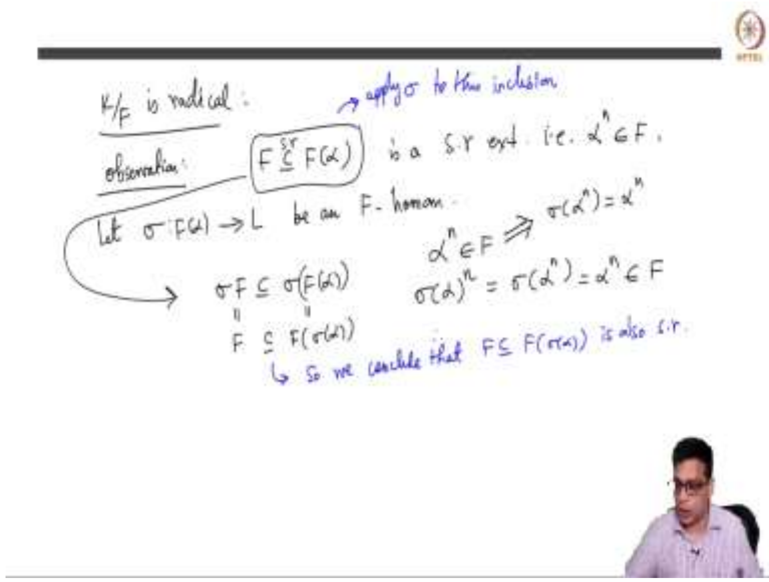
Now, we are going to take basically so let write me like this; so let S be the set of all conjugates in some larger field in some extension of L, for example in L bar. So, you can take L bar the algebraic closure of L and conjugates. What is the meaning of conjugates? So conjugates of alpha 1 are the roots. So, it really should say F conjugates F conjugates; conjugates of alpha 1 or

F conjugates of alpha 1 or roots of the irreducible polynomial of alpha 1 over F. So, you do that for all alpha 1, you do that for all alpha 2; and you do that for all alpha n, every one of them. So, it is a finite set, alpha 1 may have 25 conjugates, alpha 2 may have 31 conjugates, alpha 3 may have 5 conjugates. You take all of them and call S.

So, now let K to be F adjoint S; so attach all of them. So, I claim that so we claim that K is the, so of course K contains L; because L so alpha I is. So, S is a superset of rather I should try to write like this. If in fact, FS equal to L that means all conjugates of your alpha is already in L, which will imply that L is already Galois over F; so, we do not need to do anything. But, in general we have to add the extension, conjugates; it is the required extension. So, that k if I put that means K over F is Galois plus radical; so let us prove why that is the case, and that proves of course the proposition.

First I want to show that it is in fact radical, why is it radical, or actually is it maybe radical? Requires a little bit work Galois is easy. It is Galois because let say fi is the irreducible polynomial of alpha i over F. Then, K is the splitting field of f1 through fn I think I called over F. This is easy because you take the polynomial f1 through f1 times f2 times fn; this splits completely in K. Because you have attached all the roots of these polynomials to K; in fact k is generated over capital f by those roots. So, this is certainly the splitting field, so being a splitting field of a polynomial. Here we are in characteristics 0, so it is Galois; so this much is ok.

(Refer Slide Time: 19:02)

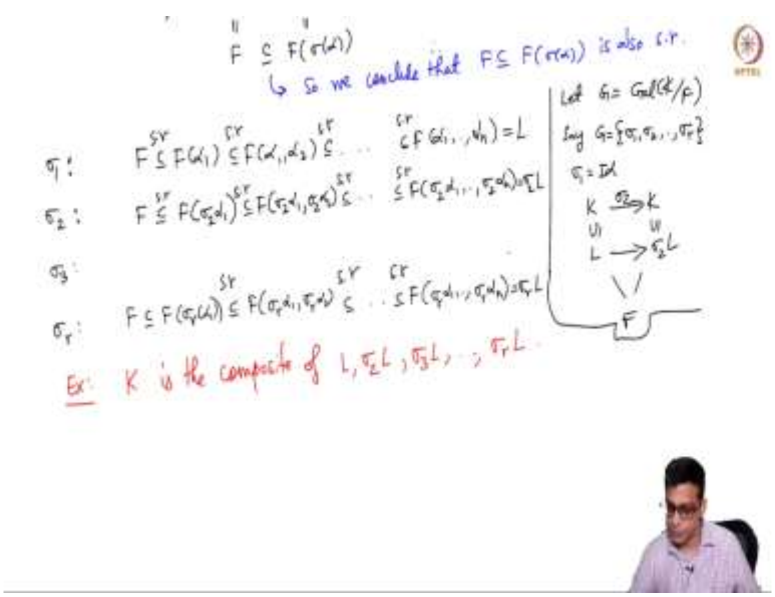


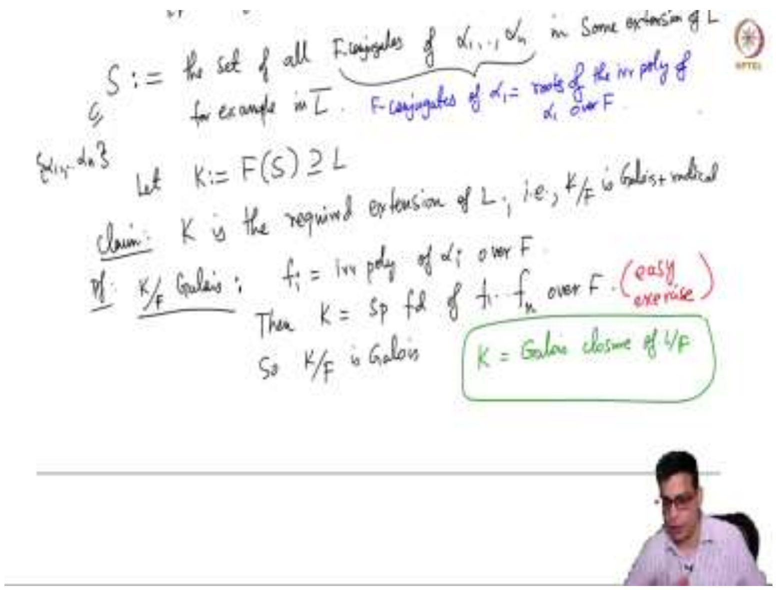
Next we want to show that K over F is radical; this is done in the following way. So, I want to produce a first of all let us look at the following, so simple observation. So, we first want to make an observation; so, suppose you have so what I want to observe is the following. Suppose you have F inside F alpha is a simple radical extension; so that is alpha power n is in F let say. So, forget the earlier notation I am just writing the simple radical extension with this property. Now, let sigma so suppose I will take this is contained in L; so now let F alpha be in L and sigma from L to L, sigma from L to actually I do not care what that is.

So, let say sigma is a function from F alpha to some L be an F homomorphism; so, it fixes F but it sends alpha to something. Then apply sigma to this inclusion; what do we get? What we get is sigma F contained in sigma of F alpha. But, this is F of course, because sigma is an F automorphism; so this is F. So, this is nothing but F of sigma alpha; because again F is fixed point. So, the extension is generated over F by sigma alpha. So, now sigma alpha, alpha power n is in F; but what is sigma alpha power n? This is sigma alpha power n. But, alpha power n is in F, so this is in F.

So, in fact sigma alpha power n is equal to alpha power n. So, sigma of alpha power n is again in F. So, this the conclusion I want to draw to your attention to is given that this simple radical; this is also simple radical. So, we conclude F contained in F of sigma alpha is also simple radical; so, this is the crucial observation. Now, let us get back to the proof that K over F is radical.

(Refer Slide Time: 22:13)





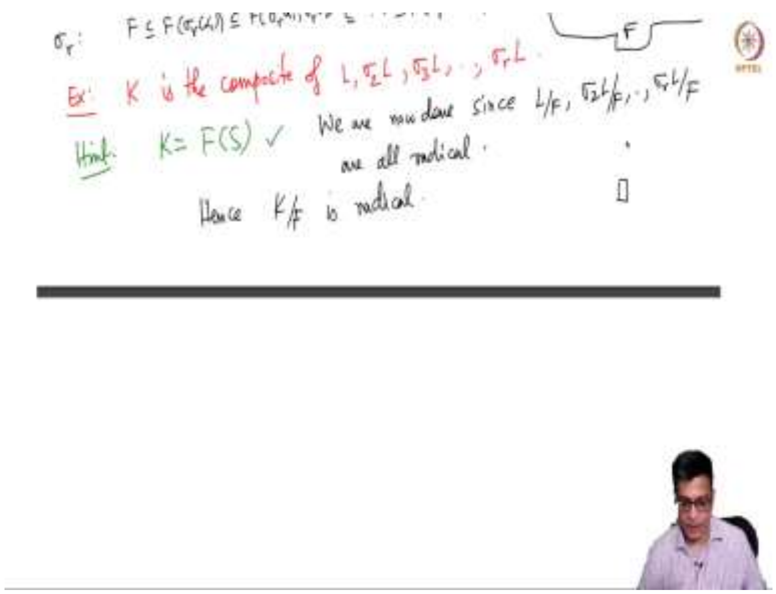
So, you have now let me write this now. F is contained in F alpha1 contained in F alpha 2, F alpha 1 comma alpha 2; and all the way up to alpha1 through alpha r or alpha n, which is our L. And now let G be the Galois group of K over f; K is already proved to be a Galois extension of F. Let us take the Galois group of that extension; so, G is sigma1, sigma2 some sigma r. So, some collection of in automorphism; so it is an extension of degree r. So, apply so this is sigma 1 identity; so think of this as the one with sigma 1. Apply sigma 2 to this inclusion, apply sigma 2 to this inclusion; what do we get? Sigma 2 is an F auto morphism.

So, you get F sigma 2 of F is F, but you get sigma 2 alpha 1 F of sigma 2 alpha 1, sigma 2 alpha 2; f of sigma 2 alpha 1, sigma 2 alpha n; this is actually nothing but sigma 2 L. So, k it is an automorphism of K; L is contained in this; so it will go to sigma 2 L. L is of course not normal, so it will potentially be some other field. But, the point that we can now conclude using this observation that I gave here is these are simple radicals by hypothesis. But, now we conclude that this is simple radical; because some power of this is here. Some power of sigma 2 alpha 2 is here, same power in fact.

So, now you can apply these to all of them sigma r finally. So, you get F contained in F of sigma r alpha, contained in F of sigma r alpha 1 sigma, r alpha 2. All the way up to F contained in sigma r alpha 1, f adjoint sigma r alpha 1, sigma r alpha n, which is of course sigma r L. The same logic tells you that these are all simple radical extensions; because sigma2 sigma r alpha 1 power something lands here, sigma r alpha 2 power something lands here. Similarly, sigma r alpha n power something lands in the previous field. So, now this is an easy exercise for you.

K is actually the composite of, so I will let you do this; if you take this called the Galois closure. So, this is in some sense the smallest the smallest Galois extension containing L. So, because you have to attach all the conjugates of alpha here have no choice, in order to get Galois extension. So, Galois closure is nothing but the conjugate of these.

(Refer Slide Time: 25:46)

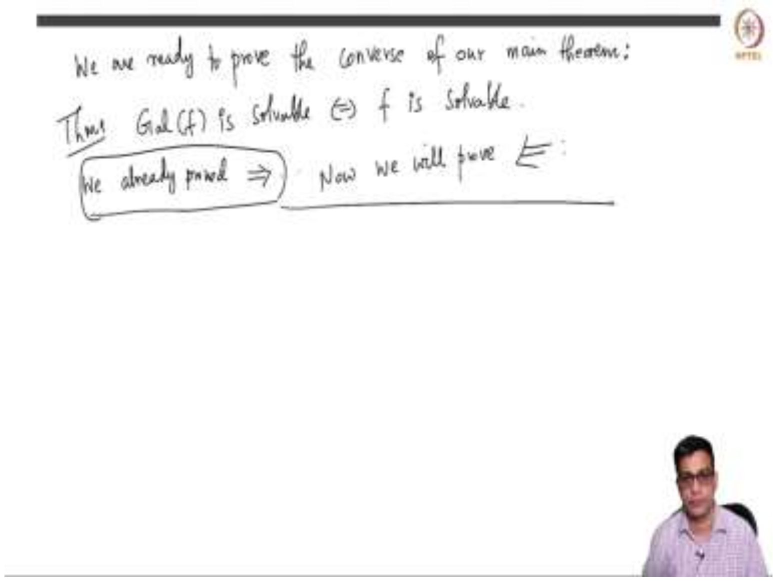


Because remember K is equal to hint F S. What is F? What is S? S consists of alpha1 through alpha n, sigma 2 alpha 1 alpha n; 1 to sigma 2 alpha n, sigma r alpha 1 to sigma r alpha n. All the conjugates, so this is as an easy observation; because the conjugates of all these fields is F adjoint union of this, this, this and this; that is same as this.

Now, we are done. So, since we are now done since L over F sigma 2 L over F, sigma r L over f are all radical; because by the way we constructed this. Sigma 2 L is radical because it is there is a tower of simple radical extension; ending with sigma 2 L, similarly sigma r L is radical. So, this is because of these towers; so they are all radical and composite of radical’s extensions is radical. I proved that composite of 2 radical extensions is radical; but one can quickly check that composite of 3 radicals extensions is radical. That is you do too and then do one more; that is triviality.

So, after you compose, take the composite of all of them, you get K; and hence K over F is radical. We already showed that K over F is Galois; so given a radical extension we can extend the extension to preserve radicalness; but add Galois. So, given that we have now a radical Galois extension.

(Refer Slide Time: 27:40)



Now, we are ready to prove the converse of our main theorem, and recall that what is the main theorem we are trying to prove. We are trying to prove that G Galois group of polynomials is solvable if and only if f is solvable. So, we already showed, so this is our theorem; strict of all the notations. So, I will go to the missed statement of the theorem for the notation. Capital F is the subfield of C, small f is a polynomial over capital F and then we have this; we already proved this. We already proved that if Galois group of the polynomials is separable, solvable; the polynomial is solvable.

Now, we will prove this direction; so let me just make sure that this simplication correct. So, G solvable if and only if f is solvable; assuming f is solvable, we showed that f is solvable. Now, we are going to show that if f is solvable, the Galois group is solvable. So, let me end the class here; in the next class we will complete this proof. And then see what kind of implications it will have. Thank you.