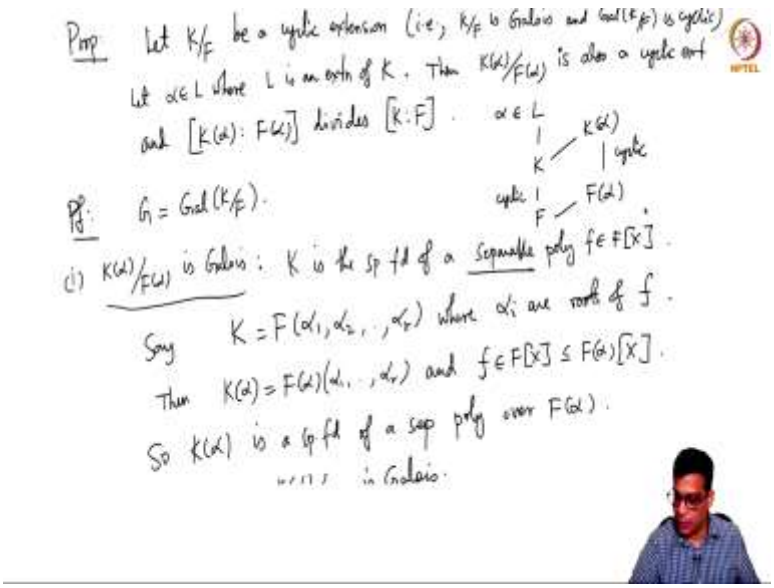
Introduction to Galois Theory
Professor. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture No. 39
Characterization of Solvability – Part 2

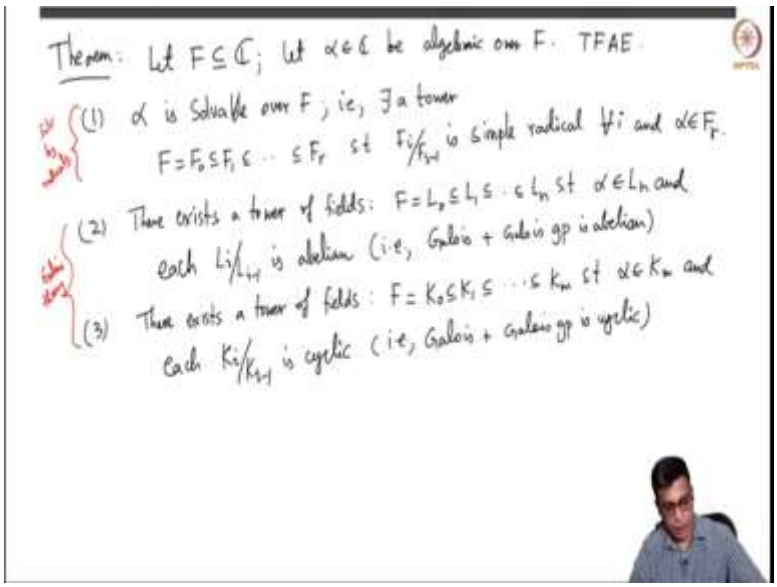
Welcome back. In the last class, we proved that Galois extension of degree 6 is always solvable.

(Refer Slide Time: 0:25)



Along the way we proved this important theorem, which says that if you have a cyclic extension and you are joined in alpha to both fields in the extension, you also get a cyclic extension and the degree of the new extension divides the degree of the old extension. So, the goal today is to the following theorem.

(Refer Slide Time: 00:43)



So, let me write down the theorem and we will spend the whole class proving this. Let F be field of, let F be a subfield of C, let alpha in capitals alpha be a complex number be algebraic over F So, then the following are equivalent. The 3 statements that I will make are all equivalent to each other. Alpha is solvable over F which is to say that is there exists a tower. I am going to write the tower as follows. So, F equals F0, F1, Fr such that Fi over Fi minus so, so let me write like this. A simple radical for all i and alpha is in Fr. So, it is simply saying that alpha is solvable over f means alpha is in a radical extension of F but that radical expression must be the end of a tower of simple radical extension. So, this is just the definition.

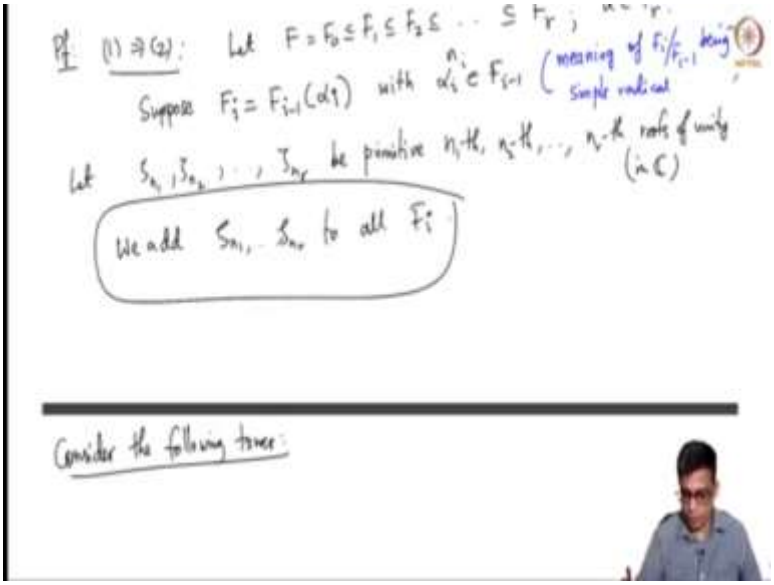
The second statement is, there exists a tower. So, in all 3 statements, there are towers with the differing properties. There exists a tower of fields. So, let us call this F equals L0 L1 contained in Ln such that of course, alpha is in the end of them and each of the extensions is abelian that is Galois plus Galois group is abelian as we know very well an adjective which is used for groups, if you use it for field extensions, that means that field exploration is Galois and the Galois group has that adjectives. So, in this case, it is the Galois and the Galois group is abelian.

In the third statement is exactly as to except that the word abelian is replaced by cyclic. There exists at tower of fields. It is a F again starting with F, now K0 K1, all the way up to Km, let us say such that of course alpha is in the last one and each Ki over Ki minus 1 is cyclic which is to say Galois plus Galois group is cyclic. So, that is the 3 statements. So, just stare at this. It is

important that you understand the first statement has to do with solvability by radicals as understood before Galois, as understood for hundreds of years before Galois, 2 and 3 have to do with Galois Theory, which is Galois' ingenious idea to connect field theory with group theory.

So, 2 and 3 are really group theoretic statements saying that there are towers of extensions, there with extensions being either abelian or cyclic. So, it is important that we prove this equivalence and then we will attack the possibility of solving quantics by radicals via 2 and 3. So, we have to settle once and for all the equivalent of these 3 statements.

(Refer Slide Time: 04:52)

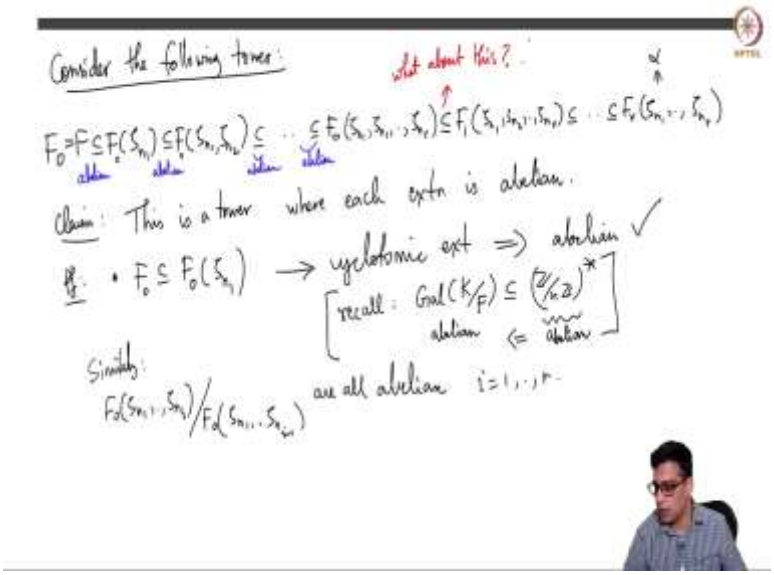


So, I will now prove the equivalence of this. Some of this is essentially coming from the previous class where we proved that cyclic extensions are solvable. So, let us see. So, we are assuming that, we are assuming that this is the new thing really, 1 to 2 is new, 2 to 3 is trivial, 3 to1 is essentially done by us. So, let us do 1 to 2 first because we new so we are assuming that alpha is solvable. So, let F contained in F1 contained in F2 contained in Fr.

So, alpha is in Fr and suppose each Fi because each Fi or Fi minus 1 is a simple radical extension suppose Fi is generated over a Fi minus 1 with by alpha i with alpha i power Ni in Fi minus 1. This is the meaning of the extension being simple radical. I am just giving names to the generators and the exponents because we have now our extensions so we have to keep track of the all the things. So, we say that F1 is generated over F0 by alpha 1 and alpha upon power n1 is in F1 or F0 and so on. So, this is the notation.

Now I am going to consider the following roots of unity. So, let, so remember we have n1 through nr and alpha 1 to alpha r coming from this tower. So, we take the corresponding n th roots of unity. Primitive n1, n2, nr th roots of unity. We can take them in C because we are working with subfield of C now. So, we have completely switched our characteristic to 0 here and subfields of C in fact. So, these are primitive. If n1 is 2, I take primitive second row which is minus 1, of course that is already in F but if n2 is 3, I will take omega, if n3 is 4, I will take i and so on. So, these are those roots of unity.

(Refer Slide Time: 7:41)



Now consider following tower. So, I am going to write down the tower and I will carefully look at this. So, first I will do F0. So, let me try to squeeze this here. I do F0 adjoint zeta n1, then F0 adjoined zeta n1 n2. So, maybe I will just go to the next page because I want to squeeze everything in the same page. So, consider the following tower. So, what I will start with F0 which is of course F. Remember the given tower is this. I am going to add all these nth roots to F0 because I want to use our original theorem about extensions.

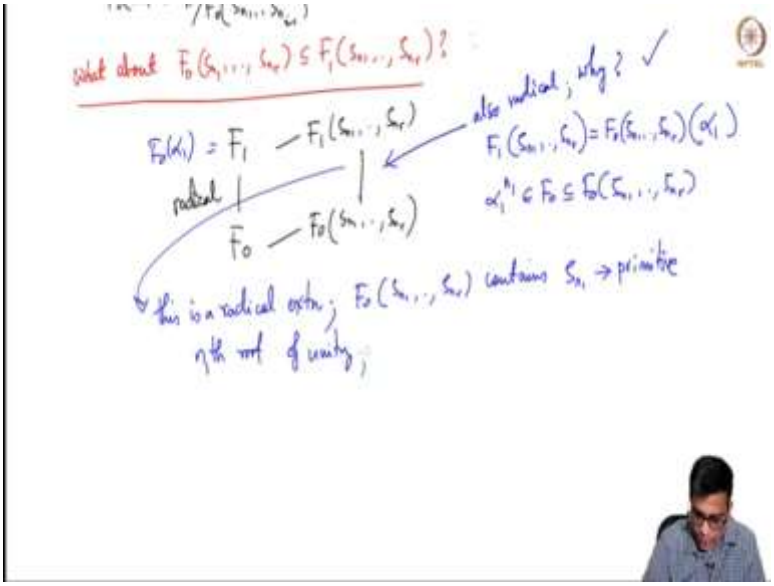
So, then I will do F zeta n1 F zeta n1 comma zeta n2, F0 and I will one by one attach all of them and finally attach zeta nr and now, I will put F1 zeta, remember F0 is contained in F1. So, I will just add all of them to F1 also and keep doing this and finally I will do Fr zeta n1 zeta nr. So, I have changed the original fields completely. So, originally, we have this. So, basically, we add zeta n1 to zeta nr to all fi. So, for the first one, I just break the addition into one by one.

Now we want to claim that this is an extension where each, this is a tower where each extension is abelian. Thereby proving 2. So, of course, alpha is in here. So, alpha is in Fr. So, alpha is in F adjoined this. You are only enlarging the field. So, alpha will remain here and 2 says, there is a tower of abelian extensions with alpha being in the last one and here is the tower with alpha in the last one. So, why is this? Why is each of them abelian? So, one by one, let us check. What about F0 contained in F0 theta 1. This is a cyclotomic extension. So, abelian. So, this is covered in our class about cyclotomic extensions.

In general, every time you have a cyclotomic extension, recall from, so if you have cyclotomic extension, it is a the Galois group is isomorphic to a subgroup of Z mod nZ star. This is abelian. So, this is abelian. So, this is just, this is exactly the result we proved in the corresponding, I mean the theorem in cyclotomic extensions class. So, these is abelian. So, let me write that here. This is abelian. What about this? This is also abelian of course because this is also a cyclotomic extension. You are adding zeta into 2 F zeta n1. So, this is abelian. This is abelian. So, all of these are abelian. So, up to this everything is abelian.

So, similarly F zeta, F circle zeta ni over F circle n1, zeta ni minus 1 are all abelian. So, from i equal to 1 to r. So, these are all abelian. What about the next one? So, this, let us focus on this. What about this? I claim this is also abelian. Now here is where we will use Kummer theory.

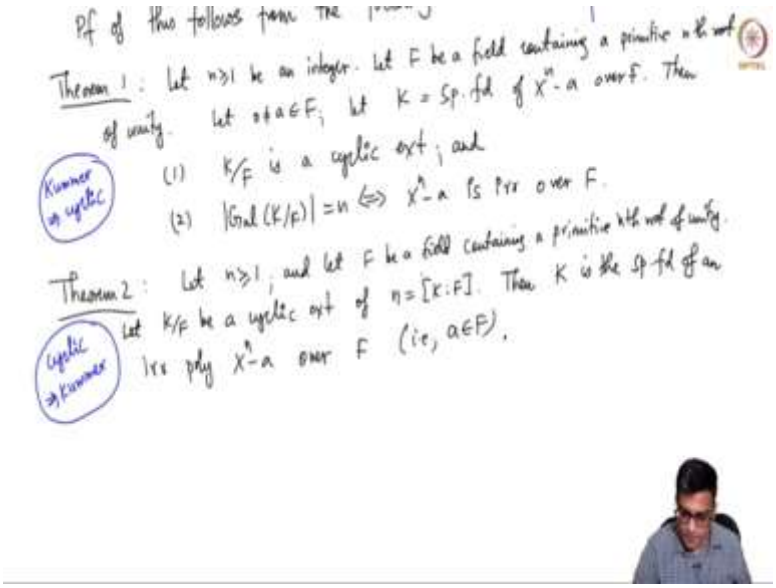
(Refer Slide Time: 12:44)



So, what about this? By the first observation what we have is F1 over F0, this is cyclic, this is radical. So, I now claim this is also, radical. So, why is that? So, think about this, why is that radical? That is radical because F1 is F0 alpha 1. So, F1 of zeta n1, zeta n r is F0 of zeta n1 zeta nr adjoined alpha 1. So, the same thing will generate this field over this field and alpha 1 power n1 is in F0. This implies, of course, it is in F0 power zeta n1 to zeta nr.

So, this is also a radical extension. So, that is okay, but now we have a radical extension so, this is a radical extension and what is a degree of that extension? So, this radical extension contains the base of this radical extension contains a primitive contains zeta n1 which is a primitive nth root of unity, n1 th root of unity.

(Refer Slide Time: 15:24)

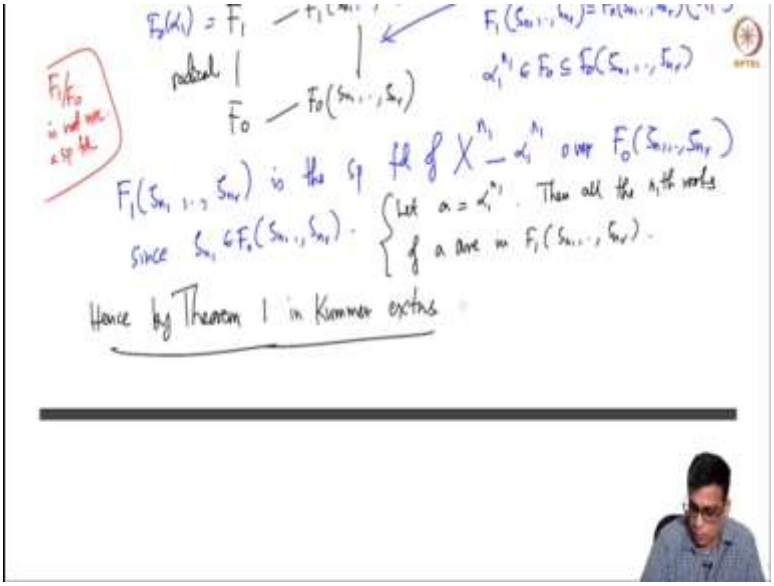


So, now here is some general facts. So, the, I claim that so what we have now shown is so let me go back to the Kummer extension theorem that we proved it. So, let me explain how we use that. I think I went way back. So, this is the Kummer extension theorem. So, let us look at the main theorem and in fact, I wanted to look at the theorem 2. So, if you have field containing a primitive nth root of unity and N is the extension of that, then K is the splitting field of that but okay, actually I do want theorem 1.

So, you have a field containing primitive nth root of unity and K is splitting field of X power n minus A. Then it is cyclic. So, what I want is this. So, I want this statement. So, if I claim that in our situation the hypothesis is satisfied. F is a field containing a primitive nth root of unity. K is

the splitting field of x power n minus a. Then that extension is cyclic. So, primitive n1 th root of unity and this is the splitting field of x power n1 minus. So, I so let me just rewrite this.

(Refer Slide Time: 17:38)



So, F1 that adjoin zeta n1 to zeta nr is the splitting field. This is clear because F1 is the splitting field of, F1 is the is a radical expression. It is not necessarily splitting field. So, F1 over F0 is not necessarily splitting field extension, not a normal extension. However, it is obtained by adjoining a root n1 th root of alpha 1 but now in this new extension, you have adjoined n1 th root of alpha 1 power n1 and hence you attached because zeta n1 is there in the base field.

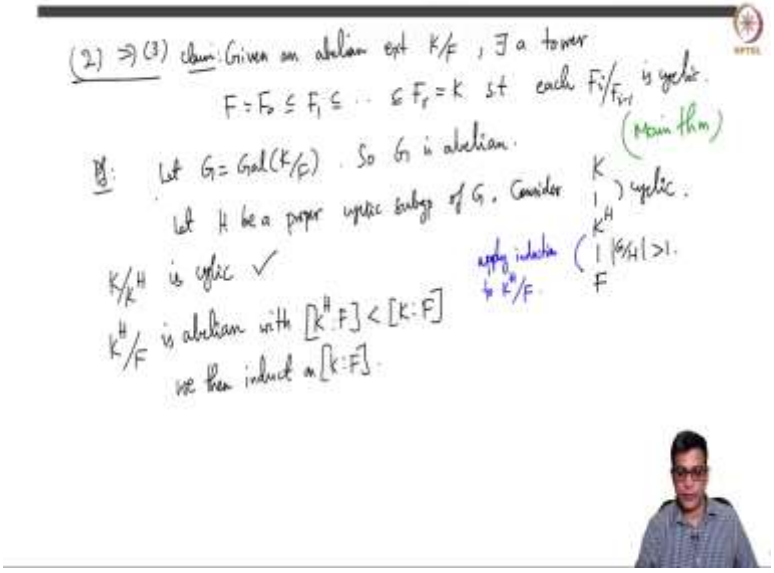
Once you attached, so basically what I am saying, is that let a be alpha n power n1, then all the n1 th roots of a are in F1 zeta n1 zeta nr. So, it is a splitting field and the base field contains sub 0 zeta n1. Hence by theorem 1, in Kummer extensions class: F1 zeta n1, zeta nr over F0 zeta n1, zeta nr is cyclic and hence abelian. So, basically, my goal has always been to use the theorem 1 but in order to use that, I need my base field to have roots of unity, which I have achieved by adding them a priori. So, I hope this is clear.

So, the crucial thing is theorem 1 in Kummer theory. In order to apply theorem 1, we need the base field to contain primitive nth roots of unity, which I achieved by adding this. So, this is abelian. So, this is abelian. What about this? Exactly the same reason. This is also abelian except that we work with N2 now because this is an extension a priori where in n 2 roots is attached. So, you perform the same logic F2 or F1 but F2 adjoined all the roots, F1 adjoined all the roots, the

relevant thing is only zeta n2 that is there. So, by theorem 1 of Kummer extension that is cyclic and hence abelian. So, everything is abelian.

So, this tower is a tower where each expression is abelian and hence 2 is proved. I hope this argument is clear. What we do is, take the original tower where every extension simple radical but figure out which roots of unity are required which come from the powers, the radicals which are attached in this simple radical extensions, attached the roots of unity for those nis and then argue the initial cyclotomic extensions are all abelian by our cyclotomic extension theorem and after that, after F0 after you attach all of them, you use Kummer Theory to argue that are all abelian. So, that proves 2.

(Refer Slide Time: 21:54)



Now 2 implies 1 is trivial because remember what is 2. 2 is that there is a tower where the end field contains alpha and each is abelian. So, 2 is not trivial, 2 to 1 is not trivial. So, let me, so we have to prove something. So, we will show that given an abelian extension K over F, there exists a tower such that each Fi by Fi minus 1 is cyclic. So, this is more or less trivial because what do we do? So, claim is this. Prove so let G be the Galois group of the original abelian extension. So, this G is abelian. K over F is abelian so it is Galois with Galois group abelian. So, let H be a proper sub group, G proper cyclic subgroup of G.

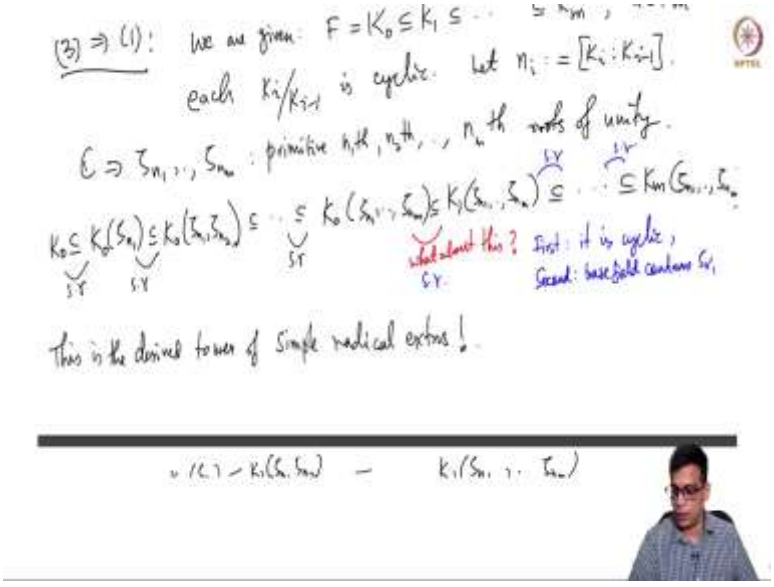
Of course, G is cyclic then we are done. If G is cyclic then we are done because K over F is a cyclic extension. So, then we consider K, K power H and F. Remember this is cyclic. So,

actually what I mean is, I do not need proper cyclic subgroup of G, proper cyclic proper cyclic subgroup. So, this G, this is Galois extension, I mean everything is abelian. So, this is Galois extension with Galois group G mod H, and this is strictly more than 1 because it is a proper subgroup. So, by induction, so apply induction to this.

So, note that KH, so K over KH is cyclic. This is okay. KH over K or KH over F is Galois, with abelian Galois because G's abelian is important here. So, every group is subgroup is normal. So, every intermediate field over the base field is Galois. So, the main theorem is required here. So, this is abelian with the degree strictly less than the original extension, so we then induct. So, this can be populated by a series of cyclic extensions. You attach one more to get the desired cycle extension.

So, this implies 1 because if you are given a tower of abelian extensions, you expand this tower by putting in lots of subfields where each extension is cyclic. Similarly, you do that for L1 contained in L2. Ln minus 1 contained in Ln and you get a much bigger tower but with each of the intermediate extensions being cyclic. So, 2 implies 3, this is not 2 implies 1. I am trying to prove 2 implies 3. So, given an abelian extension, it is rather easy to get a tower of cyclic extensions. So, you do that for each abelian extension and you have done.

(Refer Slide Time: 26:04)



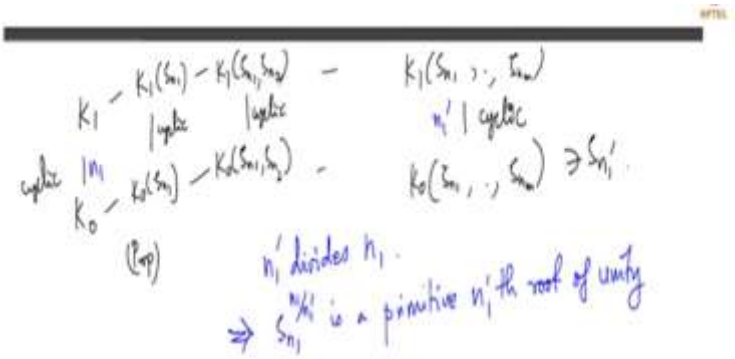
Finally, 3 implies 1 and this is something that we have done essentially in a special case in the previous video where we prove that a Galois extension about 6 is solvable. So, this is crazy

because the idea is that we are given so let me just summarize the method. So, F0 is, f is K0, K1, Km or n, Km such that alpha is in Km. Each Ki over Ki minus 1 is cyclic. So, what do I do here? So, what we do here is we let ni be the extension degree of Ki and Ki minus 1 and let us choose zeta n1 to zeta nm, primitive they are all complex numbers, primitive n1, n2 th, nm th, roots of unity and then attach all of them to K0.

So, first we do K0, adjoined K0 zeta n1 and K0 zeta n1, zeta n2, K0 zeta n1, zeta nm and then you do, K1 zeta n1, zeta nm, all the way up to Km, zeta n1, zeta nm, just like in the first case 1 implies 2. Here, the only difference is the ni we have chosen are the degrees of the extensions. In 1, we have chosen the ni to be the radicals we needed to take So, now you claim that this is the desired tower of simple radical extensions. Why is this?

Of course this is simple radical because it is a cyclotomic extension. Zeta n1 power n1 is 1 so that is in K1 K0 this is simple radical. This is simple radical because these are all obtained by adding an nth root of unity. A primitive nth root of unity ni th root as ni. So, do they do not present any problem. What about this and here is where the hopefully the Galois group extension of order 6 will be recalled to your mind now.

(Refer Slide Time: 29:15)



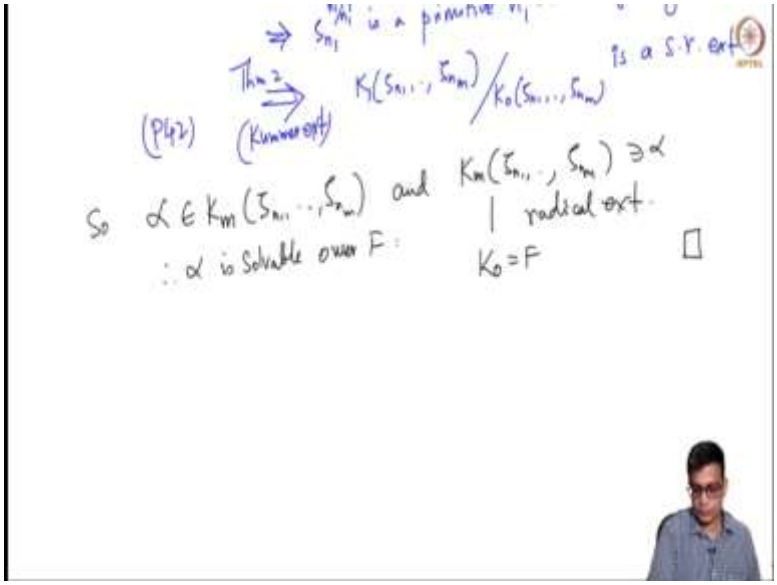
So, we have K1 over K0 is cyclic. That is given to be that case. So, this is cyclic. Adjoined all of these so basically, I will argue just for complete clarity. So, this is cyclic by the preposition. Remember the proposition we proved. So, if your cyclic extension you attach something, it will

remain cycling and you attach 1 more, this is also cyclic because this is cyclic, you apply the preposition and finally K1 zeta n1, zeta nm over K0 zeta n1, zeta nm, they are all cyclic. So, this is cyclic. So, this is cyclic.

First, it is cyclic. It is cyclic, but the base fields contains zeta n1 and base field contains, second argument is, based field contains zeta n1 which is the primitive nth root of unity, and now remember this is extension of degree n1. So, this is a divisor of n1 by the proposition that we proved. So, this, whatever this n1 prime is, n1 prime divides n1 So, this implies some power of zeta n1, I think it is n1 by n1 prime is a primitive n1th prime root of unity. So, I will write this here. So, this is an extension of degree n1 prime where the base field contains degree zeta n1 prime because once you have a primitive eighth root of unity, some power of it will be a primitive fourth root of unity.

So, once you have a primitive and n th root of unity, a suitable and n1 prime divides n1, suitable power of the primitive n 1 root of unity will be a primitive n 1 prime root of unity. So, this is a cyclic extension of degree n1 prime with base field containing a primitive n1 prime root of unity. So, now let us go back to one final time the lectures on cyclotomic extensions, Kummer extensions and let us look at theorem 2. So, we have a field containing a primitive nth root of unity and an extension containing a cyclic extension of that degree n where will contains an nth root of unity. Then K is the splitting field of some polynomial like this. That means K over F is irreducible. K over F is simple radical.

(Refer Slide Time: 33:03)



So, by theorem 2 Kummer extensions, so I think page 42 in this notes, K adjoined, K1 adjoined is a simple radical extension because it is obtained by adding n1 th power of n1 th root of some element of this field. So, similarly, so this is simple radical, this is simple radical, this is simple radical. So, everything is simple radical. So, alpha which is in, of course alpha is in here in Km and so I will just write it one more time over F0 K0 which is F is a radical extension. So, alpha is here and these radical extensions because this is a radical extension of this because there is a tower starting with this, ending with this and where each extension is a simple radical extension. This is radical extension containing alphas so, alpha is a solvable over F.

So, this proves the theorem that I started this class with and now we are ready to attack the question of solving polynomials by radicals. More precisely given a polynomial, is it solvable or not, we want to address and in the next video, we are going to settle the case of degree 1, 2, 3, 4 and then after that we will tackle the case of degree 5. So, let me stop today here and in the next class we continue with solving polynomials by radicals. Thank you.