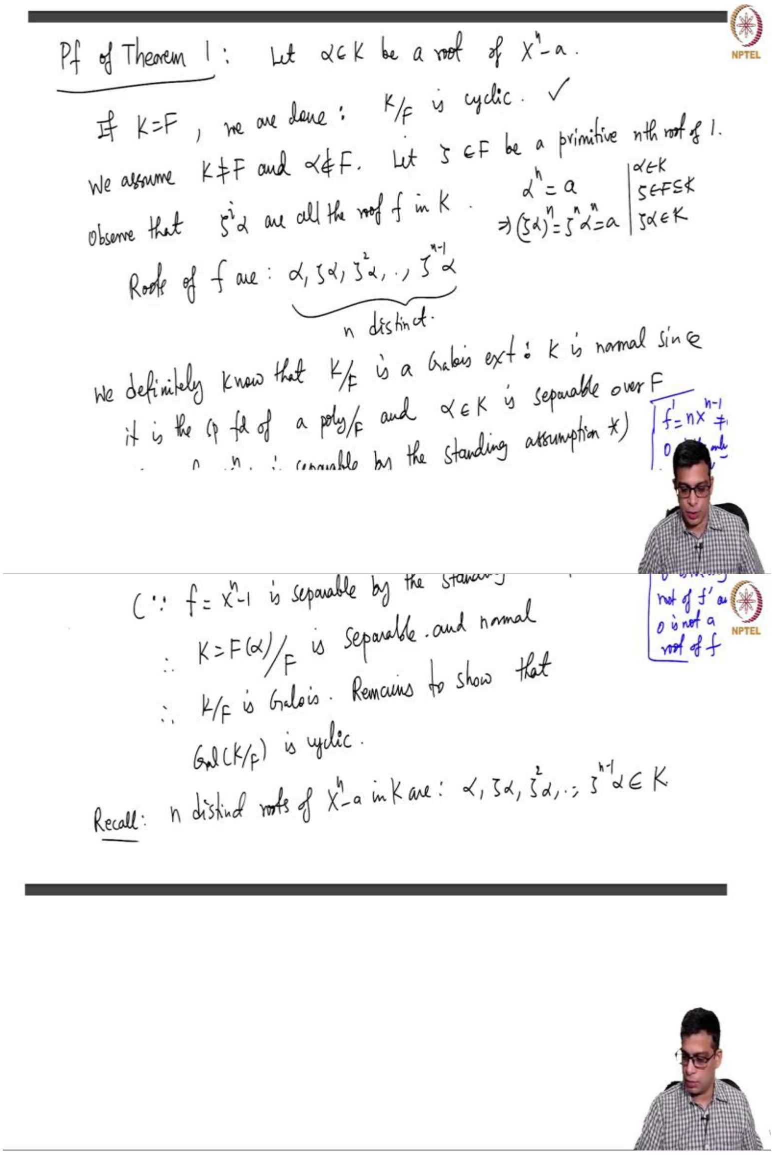
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 33
Kummer Extensions - Part 2

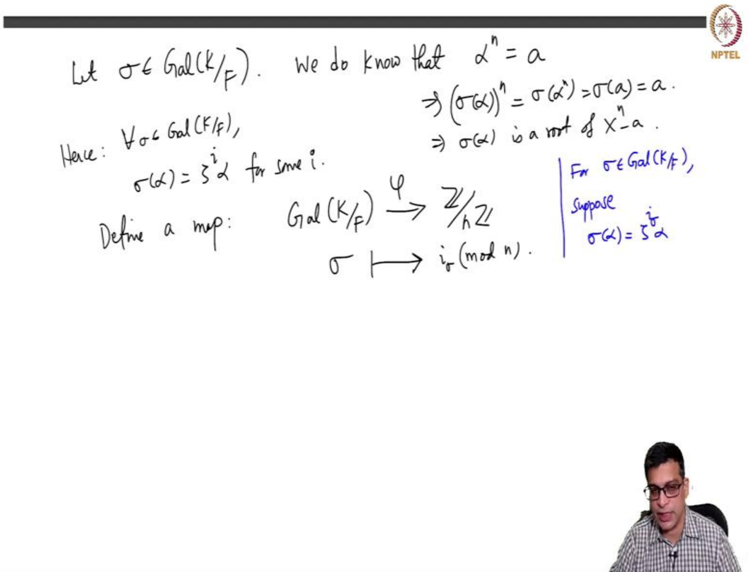
(Refer Slide Time: 00:16)

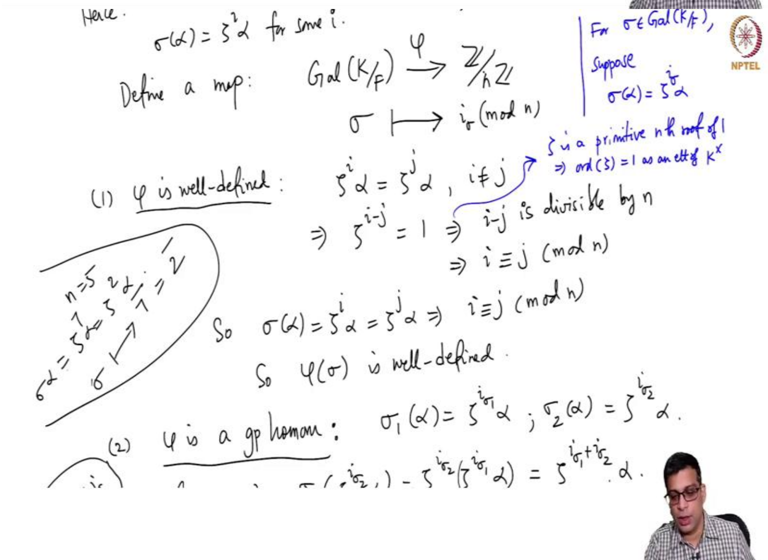


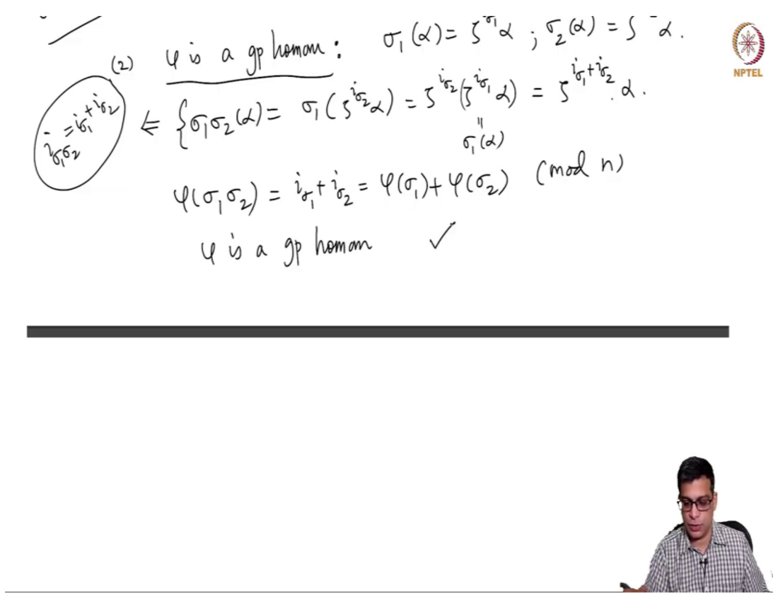
Welcome back, we are halfway through the proof of theorem 1, that I stated last time after defining the Kummer extensions. And our goal finally is to prove this main theorem about Kummer extensions, which say essentially that if you start with the kind of a field, which means it is a field containing a primitive nth root of unity, then a Kummer extension is really nothing but a cyclic extension. And equivalence is given with two theorems, and the first theorem is to show that Kummer extension is cyclic. So, we started with the Kummer extension we argued last time that it is definitely Galois.

Now, we are going to show that it is Galois group is cyclic. So, I also told you that the roots of, so recall, the n distinct roots of X power n minus a and K are, so you pick any root that you want first, then you take that root times the primitive nth roots of unity that exist in K. So, the primitive nth roots of unity are in F, so they are in K. So, the n roots are given by this, they are all distinct because a polynomial is separable. Now, we are going to show that the Galois group is cyclic by exhibiting a cyclic group which contains the Galois group as a subgroup.

(Refer Slide Time: 01:45)







So, for this let us know the following. So, let us take the Galois group K over F and take an element of this. So, then we do know that alpha power n is a, so this means, sigma alpha over n is sigma alpha power n, which is sigma a. So, because a is in the base field, so a is fixed. So, this means sigma alpha is a root of X power n minus a.

So, hence the conclusion is, for all sigma in the Galois group, sigma alpha is some zeta i for some i, because the roots are all in front of you here. The roots of the polynomial are here, sigma alpha is a root of that polynomial, so sigma alpha is 1 of them. So, now, this allows us to define a map from the Galois group to the cyclic group Z mod n Z. What do we do with this? This is a map phi, so phi send sigma 2.

So, the notation here is, so I am going to try this. So, for sigma in G the Galois group let suppose, we know that sigma alpha is zeta power i times alpha, that zeta i, I will call, that i will depend on sigma, right. So, I will call that the exponent of zeta i sigma, so then I will simply send it to i sigma mod n. So, I have to be a little careful here because i sigma is an integer, so it is not in Z mod n Z a priori, but I can take its residue class modular n, then sigma will go to i sigma mod n.

So, we will prove some things about this. Phi is well defined, first. We will show that it is an injective group homomorphism and thereby Galois group of K over F is a subgroup of that Z mod n Z is isomorphic to a subgroup of Z mod n Z and hence Galois group will be cyclic. So, why is this well-defined? The problem might occur, if you have zeta i alpha is equal to zeta j alpha for different i and j, then via phi I will send sigma to, if sigma alpha is this, then I will send to either i mod n or j mod n.

So, I need to know that i and j are same mod n. So, suppose this happens, then we of course know that because sigma i minus j is equal to 1, so I can always multiply by sigma j alpha inverse. So, this is sigma i minus j 1. This will guarantee that i minus j is divisible by n. This part here is because zeta is a primitive nth root of unity, it is a primitive nth root of 1, because of that if sigma i minus j is 1, i minus j must be divisible by 1 because the order of zeta is 1. So, this implies order of zeta is 1, as an element of K cross.

So, its order is 1 because it is a finite order element, zeta power n is 1 and nothing less than n will make zeta 1. That means, after n the next one we will make, that will make zeta power that equal to 1 is 2n, then 3n, then 4n and so on. So, nothing in between can have that property. So, zeta power anything is 1 implies that power must be divisible by n. So, this is a simple group theory here nothing more than that.

That means, i is congruent to j modular n. So, if sigma alpha is zeta i alpha, which is also zeta power j alpha, then i is congruent to j mod n. So, sigma phi of sigma is well-defined. So, a priori you might write different integers. But when you look at the residue modular n you get the same answer. If you take Galois K over F to Z you will not get the same well-defined map because maybe n is 5 and then zeta power 7 equals zeta square alpha.

So, where will you send sigma to, so if this is sigma alpha, sigma will go to either 7 or 2. So, if the target is integers, this is not a well-defined map. However, if the target is Z mod phi Z, 7 bar equals 2 bar. So, there is no problem so I am just explaining too much perhaps, but this is a well-defined map. And that requires the fact that zeta is a primitive nth root unity. Second statement is phi is a group homomorphism, why is this?

So, of course, this is a group, so this is a group homomorphism. And this is rather easy because, suppose sigma 1 of alpha is zeta i sigma 1 alpha, and let us say sigma 2 alpha is zeta i sigma 2 alpha. So, then what is sigma 1, sigma 2 of alpha? Sigma 1, sigma 2 of alpha which by composition. So, this is zeta i sigma 2 alpha, then you apply sigma to this, zeta i sigma 2 is a constant because that is in the base field. So, that comes out and then sigma 1 alpha is i sigma 1 alpha.

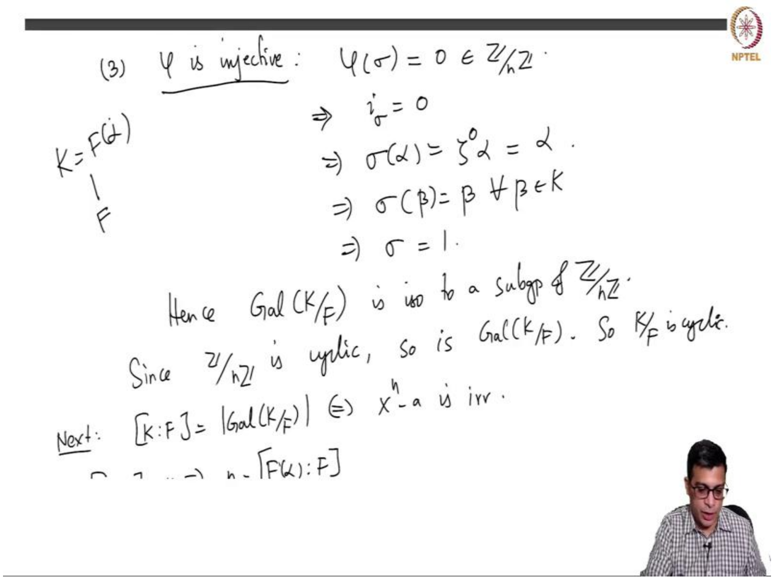
So, this is sigma 1 alpha. So, zeta power i sigma 2 comes out and then you get this. But this is nothing but zeta i sigma 1 plus i sigma 2 alpha. Now, if you go back to the definition of phi, phi will send anything to you simply apply sigma to alpha and then see what is the exponent of zeta. So, to find the image of sigma 1 sigma 2 under phi, you look at the image of alpha under sigma 1 sigma 2. And that is, so basically this entire calculation shows that i sub sigma

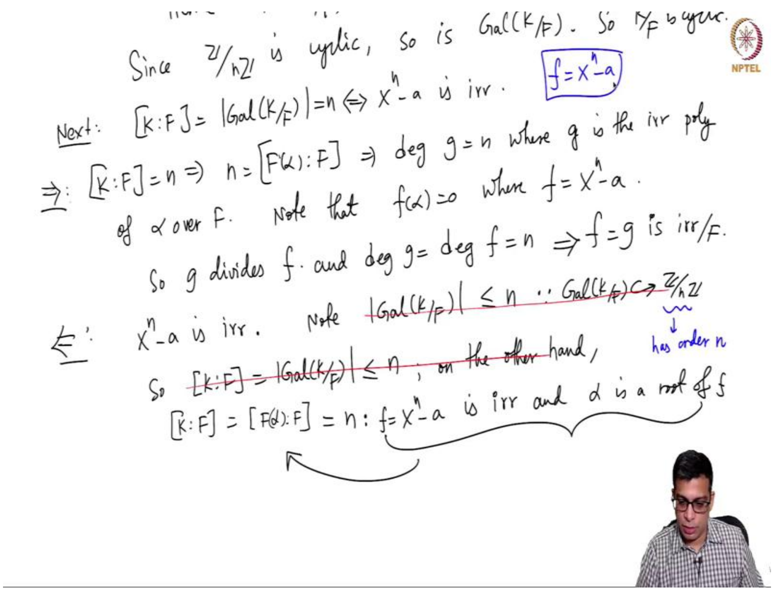
1 sigma 2 is i sigma 1 plus i sigma 2. So, maybe this is a bit confusing if you are seeing this for the first time.

And I am going maybe a bit fast, but just pause the video there, its really nothing more than notation here this is not Galois theory, this is just keeping track of the notation. So, phi sigma 1 sigma 2 is, you look at the image of sigma 1, sigma 2, and image of alpha sigma 1 sigma 2 and look at the exponent, because that is a root of X power n minus a, it must be a power of zeta times alpha and that power is this.

So, this is i sigma 1 plus i sigma 2. And by the well-defined, so I can take anything here, I mean any integer that has this property. So, of course, this is modular n, of course, because that is the group. So, this is a group homomorphism the operation of the left-hand side group is composition, the operation of the right-hand side group is addition. So, phi of sigma 1 composite sigma 2 is phi sigma 1 plus phi sigma 2. So, this a group homomorphism.

(Refer Slide Time: 10:30)





Finally, phi is injective. Why is this? So, this is also easy, suppose, something is in the kernel that means, it is image is 0, which is the identity element of this, but this means, i sigma is 0, this means, sigma alpha is the 0th power of zeta times alpha. But that means sigma alpha is equal to alpha. Once sigma alpha is alpha, now, recall that K is F alpha. Because once you adjoin alpha, all the routes are already contained, so, the splitting field is generated by alpha.

So, if sigma fixes alpha, so sigma of, if you want beta is equal to beta, for all beta in K. Because, of course, sigma fixes capital F, it fixes alpha, so it must fix every polynomial in alpha, that means sigma is identity element, so it is injective. So, that means, Galois group is isomorphic to a subgroup of Z mod n Z. Now, since Z mod n Z is cyclic, so is the Galois group.

So, this proves the first statement of the theorem 1, K over F is a cyclic extension. Now, we will you get to the second statement, but we can conclude now, so K over F is cyclic. So, now next we have to prove, I will write it down. K colon F is, which is the Galois group because it is the Galois extension, the degree of the extension is same as the order of the Galois group, if and only if X power n minus a is irreducible. So this is what we want to show so now let us show this.

So, K colon F equals n implies because K is F alpha. So, K column F is n means F alpha colon F is n. This means degree of g is n, where g is the irreducible polynomial of alpha over F. If you have a primitive extension like this generated by a single element, the degree of that extension is simply the degree of the irreducible polynomial of that primitive element. So, if g is irreducible polynomial, degree of g must be n.

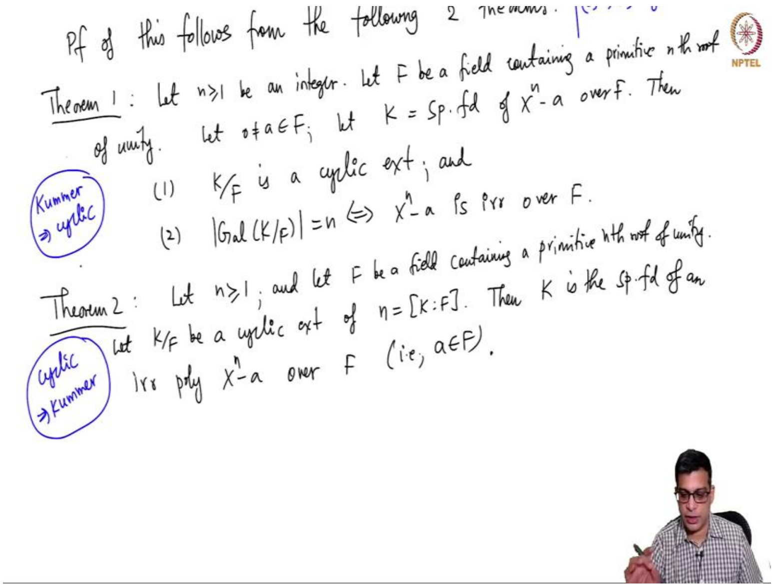
On the other hand, note that F alpha is 0, where F is our polynomial whose splitting field we have started with. So, f is X power n minus a, then F alpha is 0. So, g divides f, and degree g equals degree f equals n, F is already a degree n polynomial. That means, f is g is irreducible, in other words, it is irreducible over F. So, if K colon F is equal to n, then F must be irreducible, so F is this. Because the irreducible polynomial of alpha, whatever that is, must have degree n, F is a polynomial which has alpha as a root, so F better be the irreducible polynomial and of course, that means F is irreducible.

On the other hand this is one direction. So I did not write this completely, I mean this, if the degree of the extension or the order of the Galois group is n, that is irreducible. Now, suppose, this is irreducible. This, of course, means that degree of, so this implies, this is what I am assuming. But note that the order of the Galois group is less than or equal to and, this is because the Galois group is contained in the group Z mod n Z and this has order n.

So, if you have this order n, as a subgroup this will have order at most n. Now this implies, so the degree of the extension, which of course is the Galois group order because the extension is Galois, is less than equal to n. On the other hand, K colon F is F alpha colon F, so is what am i assuming, it is irreducible, so it is equal to n. So, I did not need to do all this, because what is the irreducible polynomial, X power n minus a hat is irreducible by hypothesis and alpha is a root.

So, F is irreducible and alpha is a root of f, and hence, so this follows, so this entire thing here implies this. So, K colon F is equal to n, which is what we wanted to prove, so I did not really need this. Those are of course, correct segments, but I do not need any of those directly we can argue this because X power n minus a is irreducible, so that is a polynomial whose root is alpha. So, the irreducible polynomial must be that and hence the degrees n. So, this completes the proof of, this proves theorem 1 and hence it proves the one direction of theorem main theorem. So, this is the main theorem.

(Refer Slide Time: 17:31)

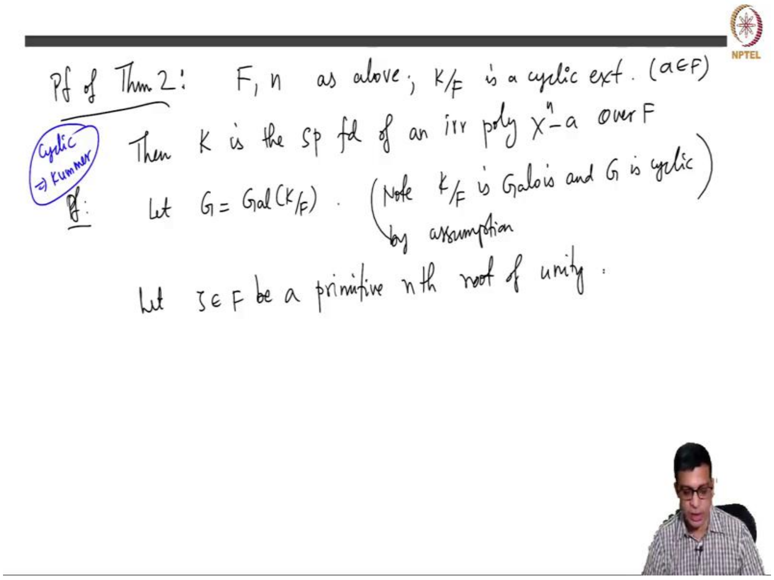


Remember 1 implies 2 is theorem 1, so this completes the proof of the first part, which says that if you have a Kummer extension, then it is a cyclic extension. So, basically think of this, there is a lot of stuff here, but think of theorem 1 as Kummer implies cyclic and think of theorem 2 as cyclic implies Kummer. This is just a short way to remember but remember also that it is not an I mean, it is there is a lot of additional hypothesis here that F is a field containing a primitive nth root and so on.

So, if you remember all that, a convenient way of remembering theorem 1 is, Kummer implies cyclic and convenient way of remembering theorem 2 is cyclic implies Kummer. So, we now proved Kummer implies cyclic and theorem is that Kummer if and only if cyclic. So, we are done with 1st theorem. Theorem 1 has a little more data than just Kummer imply cyclic, but that is a crucial thing for us. So, I wanted to highlight that.

Now, let us go ahead and start the proof of theorem 2.

(Refer Slide Time: 18:41)



So, theorem 2, I will write down just for, so that I do not need to go back to that slide, F and n as above that means, n is a positive integer, F is a field with the characteristic assumption star and that F contains primitive nth root of unity, K over F is a cyclic extension. So, that is a part of hypothesis K over F is a cyclic extension, then the statement is K is the splitting field of, so then K is a splitting field of an irreducible polynomial X power n minus a over F. So, of course, a is an F.

So this is the statement. So, this of course, as I said is saying that cyclic implies Kummer. So, these things will in fact be useful for us later, these are not just of intrinsic interest, which they are, but they will be useful to us later also. So, let me start the proof, I may not have time to finish it in this class, but I will prove for some time and then we will stop. So, let us see. So, let me start the proof and then see how much we can do.

So, let G be the Galois group. So, note that K over F is Galois is by assumption and G is cyclic. So, that is the assumption that it is a cyclic extension. So, now, our goal is to produce a small a in capital F, whose nth root will generate K. So, let us also fix a primitive nth root of unity in F, because F contains an nth root of unity, I will just take one of them. So, let me maybe, I am not sure I can finish the proof in 10 minutes. So, I am going to stop this class here and then, we will use the next class to prove this theorem. Thank you.