


**Introduction to Galois Theory**  
**Professor Krishna Hanumanthu**  
**Department of Mathematics**  
**Chennai Mathematical Institute**  
**Lecture 32**  
**Kummer Extensions - Part 1**

Welcome back. In the last video we did some problems. In fact, we had several problems sessions in the last few videos. And before that we proved the main theorem of Galois Theory, which was proved after developing the basic notions in Galois Theory and proving some preliminary results. So, we are now in the final stretch of the course.

And our goal now is to prove the famous insolubility of quintics by radicals, which was the original motivation for Galois. So, I want to head towards that. But on the way we want to discuss a couple of interesting topics, which are interesting on their own. And also they are critical for our study of polynomial equations solving by radicals.

(Refer Slide Time: 00:58)



---

Kummer extensions

either (1) char  $F=0$ , or  
 (2)  $p = \text{char } F > 0$  and  $p$  does not divide  $n$ .


*(C.A) standing assumption*

Def. An element  $\zeta$  in an extension  $K/F$  is called a "primitive  $n$ th root of unity" if  $\zeta^n = 1$  and  $\zeta^i \neq 1$  for any  $1 \leq i < n$ .

Eg. primitive 1st root of unity is 1, primitive 2nd root of unity =  $-1$ .  
 (there are 2 square roots of 1: 1,  $-1$ )  
 not primitive primitive

... 0, 1,  $\omega$ ,  $\omega^2$

← when we talk about primitive  $n$ th root of unity in a field  $K$ , we assume  $K$  satisfies the 2 condition



And the first topic, which I will start today is something about Kummer extensions. So, these are very interesting extensions that will play a role in later when we look at solving polynomials by radicals. So, let us set up the notation for this. So, let  $n$  be a positive integer, so I am going to now work with fields which have a certain property.

Now, I am not interested in all fields. So, let  $F$  be a field such that either characteristic of  $F$  is 0, in which case we have no further condition. Or characteristic of  $F$  is greater than 0, let us say  $p$ , then of course  $p$  is a prime number, in which case we want  $p$  not to divide  $n$ . So, we do

allow positive characteristic fields, but then we do not want the characteristic to divide  $n$ , So, we will fix such a field.

So, let me quickly define what is a primitive  $n$ th root of unity, I have been using that phrase repeatedly in the course and we will study them in more detail in the next topic. But for now, let me just say that an element  $\zeta$  in an extension field of  $F$  is called primitive  $n$ th root of unity. So, we will study this in more detail in a couple of videos, but for me, now, I will just define it in the following way, this is one of the equivalent definitions.

So, the primitive  $n$ th root of unity is  $1$  which is of course the root of unity if  $\zeta^n = 1$ , of course, and no smaller power is  $1$  for any  $i$ , you take any positivity is a strictly less than  $n$ ,  $\zeta^i$  is not equal to  $1$ . So, this is,  $n$  is the first power of  $\zeta$  which becomes  $1$ . So, as an example, primitive first root of unity is  $1$ , So, primitive first root of unity is  $1$  in any field that will exist. So, here remember, I said in an extension  $K$  over  $F$ , because  $F$  itself may not contain it but an extension field will contain it. So, I wanted to be precise and say that it is an extension of  $F$ .

What are primitive second root of unity? So, this of course is, there is only one such, minus  $1$ . So, because there are two, so second root is just another word for square root. There are  $2$  square roots, potentially  $2$  square roots  $1$  minus  $1$ . And of course, these will be different if the characteristic does not divide  $2$  which I am assuming. So, the point is, every time I talk about primitive  $n$ th root of unity, I assume the characteristic is not divisible by  $p$ .

So, just to emphasize this further. When we talk about primitive  $n$ th root of unity in a field  $K$ , we assume  $K$  satisfies one of these two conditions. So, either characteristic  $K$  is  $0$  or  $n$  is not divisible by the characteristic of  $K$ . So, this is a standing assumption I am going to make. Now, there are two square roots in one you assume that of  $1$ , and only one of them is primitive. So, this is primitive, this is not primitive because  $1$  actually a first root of unity, and so on. So, now, what primitive cube roots of unity for example in  $\mathbb{C}$  are, primitive cube root or 3rd root of unity in  $\mathbb{C}$  are  $\omega$  and  $\omega^2$ , there are three cube roots of unity one  $\omega$ ,  $\omega^2$ , out of which only two are primitive.

What about primitive cube root of unity in  $F_7$ ? So, these I claim are  $2$  and  $4$ . This came up in the earlier video, so  $2^3 = 8$ , which is  $1 \pmod{7}$ . Similarly,  $4^3 = 64$  which is also,  $1 \pmod{7}$ , so  $F_7$  has three roots of unity  $1$ ,  $2$ , and  $4$ , only two of them are primitive. So, this is a primitive  $n$ th root of unity. Of course, a given field may not contain it for example, rational

numbers do not contain primitive cube roots of unity, real numbers do not contain primitive cube roots of unity.

(Refer Slide Time: 06:59)

primitive cube (3rd) root of unity in  $\mathbb{C}$ :  $\omega, \omega^2$   
 $\mathbb{F}_7$ :  $2, 4 \in \mathbb{F}_7$ .  $\begin{cases} 2^3 = 8 \equiv 1 \pmod{7} \\ 4^3 = 64 \equiv 1 \pmod{7} \end{cases}$  (Note:  $\mathbb{F}$  satisfies)

Def. Let  $F$  be a field containing a primitive  $n$ th root of unity.  $(*)$   
 A Kummer extension of  $F$  is an extension  $K/F$  s.t.  $[K:F]=n$  and  $K$  is the splitting field of an irr poly  $X^n - a$  ( $a \in F$ ).  
 We say:  $K$  is obtained by adjoining an  $n$ th root.



Now, let us define the notion of Kummer extension. Let  $F$  be a field containing a primitive  $n$ th root of unity. So, I will not repeat this all the time, but there is a standing assumption here. So, there is standing assumption, which is to say that every time you talk about a field containing a primitive  $n$ th root of unity, its characteristic is either zero or its characteristic does not divide  $n$ .

So, in fact, you can argue that if you properly, rigorously defined primitive  $n$ th root of unity, a field containing a primitive  $n$ th root of unity must have this property but for now, I do not want to get into that. So, I will make that an assumption. So, note,  $F$  satisfies star. As I said, I will talk about primitive  $n$ th roots of unity later, this is one way to define it and other ways that the set of  $n$ th roots of unity in a field for this cyclic subgroup of the multiplicative group of nonzero elements of that field and primitive  $n$ th roots of unity of generators of that group.

So, I will come back to that in the lectures when we talk about cyclotomic fields. Now, let us get back to the definition. So, you have a field containing a primitive  $n$ th root of entity, that is an assumption. A Kummer extension of  $F$ , so that is an extension  $K$  over  $F$ , such that  $K$  is the splitting field of a polynomial, so let me even say reducible polynomial, that comes for free in some sense. Here is an extension, I will write them such that  $K$  over  $F$  is  $n$  and  $K$  is the splitting field of an irreducible polynomial of the form  $X$  power  $n$  minus  $a$ , for some  $a$  in  $F$ , so these are Kummer extensions.

So, Kummer extension, remember, is a base must contain a primitive  $n$ th root of unity and the extension must be of degree  $n$  and it must be obtained by adding an  $n$ th root. So, we say  $K$  is obtained by adjoining an  $n$ th root. So, we say that  $K$  is adjoined by adding an  $n$ th root, as we will explain. Because a root of this polynomial is an  $n$ th root of  $a$ . So,  $a$  is in  $F$ , so we adjoined an  $n$ th root to get that field, so then it is Kummer extension.


(Refer Slide Time: 10:40)

Example: ①  $F = \mathbb{Q}$ ,  $n = 2$ . Then  $F$  contains  $-1$  (which is the primitive square root of unity)

A Kummer ext is simply a quadratic ext:  $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ , where  $d \in \mathbb{Q}$ ,  $\sqrt{d} \notin \mathbb{Q}$ .  
 deg 2 ext ( $X^2 - d$  is irr)

②  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  is NOT a Kummer extn; because  $\mathbb{Q}$  doesn't contain a primitive 3rd root of unity.

(Such extensions are called "radical extns" and they are important to us when we study solving polynomials by radicals.)




So, let us quickly look at some examples and our goal in this class is to understand Kummer extensions. So, of course, you can take  $F$  to be  $\mathbb{Q}$  and  $n$  to be 2. So, then  $F$  contains minus 1, which is the primitive square root of unity. So, that part of the assumption is satisfied, because minus 1 is the primitive  $n$ th root of unity, second root of unity. So, then what are you looking for?

A Kummer Extension has to be of the form, is simply a quadratic extension, let us say  $\mathbb{Q}$  adjoined root  $d$  over  $\mathbb{Q}$ , where  $d$ , you can take  $d$  for example. So, in fact, one can prove that every Kummer extension is like this, this is something we did in a problem session. So, it is a quadratic extension like this where  $d$  and root  $d$  is not in  $\mathbb{Q}$ . If root is in  $\mathbb{Q}$ , of course, this is not a quadratic extension.

So, quadratic means degree 2 extension. So, a Kummer extension is simply a quadratic extension because you can always, I mean, then  $X^2 - d$  is irreducible. You are adding a square root that is first example. On the other hand, if you take cube root of 2 is not a Kummer extension, though it is obtained by adding a cube root it is adjoining a cube root but it is not a Kummer extension.

Why? Because  $\mathbb{Q}$  does not contain a primitive 3rd root of unity, the only 3rd roots of unity in complex numbers are  $\omega$  and  $\omega^2$ , neither of them is in  $\mathbb{Q}$ . So, this assumption here, that the field must contain a primitive  $n$ th root of unity is not satisfied. So, this is not a Kummer extension. These are important extensions, such extensions are called radical extensions and they are important to us.

Later, when we study solving polynomials by radicals, so I will come back to this later. So, these are preferably good extensions called radical extension. Radical extensions are those that are obtained by adjoining a radical or a root of some existing element. And when we talk about solving polynomials by radicals, we are looking to produce that, show that the root is contained in a radical extension, because then it will be expressed in terms of radicals. If you remember the first video of the course, where I motivated Galois Theory by explaining what solving polynomials by radicals is.

Now, with all the knowledge that now we now have, it is tantamount to saying that the root is in a radical extension. It need not be a single radical extension like this, but it can be inside a field which is at the end of a series of radical extensions. So, all this will be explained in detail later. But for us, the order of business today is Kummer extensions and this is not a Kummer extension because it fails to have 3rd root of unity.

(Refer Slide Time: 15:05)

when we study solving 1.0

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

$$F = \mathbb{Q}(\omega)$$

is a Kummer ext.


③  $K = \text{SP fld of } X^3 - 2 \text{ over } F_7$

$F_7$  is a Kummer ext.

$n=3$   
 $p=7$  (pt n)

(p does not divide n)

$F_7$  contains 2, 4 which are primitive 3rd roots of unity  
( $2^3=1, 2^2=4 \neq 1, 2^3=1$ )  
in  $F_7$




However, if you take  $\mathbb{Q}$  adjoined cube root of 2 comma  $\omega$  over  $\mathbb{Q}(\omega)$  is a Kummer extension. Because you have rectified this problem of the base field, not containing a

primitive cube root of unity by adding that, and then you are taking a cube root, so, this is a Kummer extension.

So, and finally, let me just give you a 3rd example, which I will write here, if you take  $K$  to be the splitting field of  $X^3 - 2$  over  $F_7$ , this came up in a problem session. We also recall today that  $F_7$  does have a primitive cube root of one, namely two, also four. And now you are adding cube root of 2 to this extension. So, this is a Kummer extension, so here, of course, 3 is the  $n$  that we are interested in,  $p$  equals 7. Here the field characteristic does not divide. So, that is good also. So, this notation here for me means  $p$  does not divide  $n$ .

So, the sentence short form is that  $p$  does not divide  $n$ . This refers to the fact that  $p$  divides  $n$  and when I put a bar that means it does not divide  $n$ . So, all the conditions are satisfied, I will simply write  $F_7$  contains 2 and 4, which are primitive 3rd roots of unity. Because 2 is not one, 2 square which is 4 is not 1, but 2 cubed is 1, this is in  $F_7$ . And same thing you can check for 4, 4 is not 1, 4 square which is 16 is not one, but 4 cubed is 1

(Refer Slide Time: 17:13)

$K = \mathbb{Q}(\sqrt[3]{2}, \omega)$   
 $F = \mathbb{Q}(\omega)$

is a Kummer ext.

Kummer exts are interesting by themselves; further they will be useful to us when we study polynomial equations.

③  $K = \mathbb{F}_7(\sqrt[3]{2})$  is a Kummer ext.

$F_7$   $n=3$   $p=7$  (pt  $n$ )

( $p$  does not divide  $n$ )

$F_7$  contains 2, 4 which are primitive 3rd roots of unity  
 $(2 \neq 1, 2^2 = 4 \neq 1, 2^3 = 1)$   
in  $F_7$




So, Kummer extensions are useful or interesting by themselves, as we will see in a minute, and further, they will be useful to us when we study for polynomial equations, so this will come up in a few videos. So, let me write down the theorem that I want to prove today, which completely characterizes Kummer extractions.


(Refer Slide Time: 17:53)

Theorem: Let  $F$  be a field containing a primitive  $n$ th root of unity  
 $(F \text{ satisfies our standing assumption } (*))$ . Let  $K/F$  be an extn of  
 degree  $n = [K:F]$ . TFAE:  
 (1)  $K/F$  is a Kummer ext; i.e.,  $\exists a \in F$  st.  $X^n - a$  is irr and  
 $K$  is the sp. fld of  $X^n - a$  over  $F$ .  
 (2)  $K/F$  is a cyclic extn; i.e.,  $K/F$  is Galois and  $\text{Gal}(K/F)$  is cyclic

Pf of this follows from the following 2 theorems.

Theorem 1: Let  $n > 1$  be an integer. Let  $F$  be a field containing a primitive  $n$ th root  
 of unity. Let  $a \in F$ ; let  $K = \text{Sp. fld of } X^n - a \text{ over } F$ . Then





So, let  $F$  be a field containing a primitive  $n$ th root of unity. Let me repeat again,  $F$  satisfies our standing assumption, which I wrote at the beginning of today's class, which is that either characteristic of  $F$  is 0, or if the characteristic is not 0, then the characteristic does not divide  $n$ . So, we fix a positive integer  $n$ , return we talk about Kummer extensions, we fix a positive integer  $n$ .

So, let  $K$  over  $F$  be an extension of degree  $n$ , so  $K$  colon  $F$  is 1. So, then the following are equivalent, TFAE remember, represent statement that the following are equivalent. So, the first is that  $K$  over  $F$  is a Kummer extension. So, in other words, there exists  $a$  in  $F$  such that  $X^n - a$  is irreducible and  $K$  is the splitting field of that polynomial. This is the definition of a Kummer extension. So, Kummer extension is an extension of degree  $n$  and it is the splitting field of an irreducible polynomial  $X^n - a$ .

Second statement which is much more Galois theoretic or more in the flavour of what we want to do. What we do in this course is that  $K$  over  $F$  is a cyclic extension. Remember that cyclic means, that is  $K$  over  $F$  is Galois. Cyclic represents two facts, that  $K$  over  $F$  is Galois and the Galois group is cyclic.

So, in particular what we are saying is that Kummer extensions are cyclic or Galois and Galois group is cyclic. And moreover, you give me any Galois extensions whose Galois group is cyclic, it is a Kummer extension. I want to emphasize again that we are assuming that  $F$  contains a primitive  $n$ th root of unity. So, we want to prove this, our goal is to prove this theorem and we will do this by essentially proving two different theorems, which give the two directions of this theorem.

(Refer Slide Time: 20:36)

(2)  $K/F$  is a cyclic extn; i.e.,  $K/F$  is Galois and  $\text{Gal}(K/F)$  is cyclic

Pf of this follows from the following 2 theorems.

**Theorem 1:** Let  $n \geq 1$  be an integer. Let  $F$  be a field containing a primitive  $n$ th root of unity. Let  $a \neq 0 \in F$ ; let  $K = \text{Sp. fld of } X^n - a \text{ over } F$ . Then

- (1)  $K/F$  is a cyclic ext; and
- (2)  $|\text{Gal}(K/F)| = n \Leftrightarrow X^n - a$  is irr over  $F$ .

**Theorem 2:** Let  $n \geq 1$ ; and let  $F$  be a field containing a primitive  $n$ th root of unity. Let  $K/F$  be a cyclic ext of  $n = [K:F]$ . Then  $K$  is the sp. fld of an irr poly  $X^n - a$  over  $F$  (i.e.,  $a \in F$ ).

NPTEL



So, the first theorem is the following. So, the way I wrote the proof is, break up the proof into two different theorems. The first theorem is the following, so theorem 1. So, the proof of this follows from the following two theorems. So, maybe I will write down those two theorems now and then we will prove them. So, theorem 1 is the following, I want to write down the full setup so that we have a record of this, when you just look at this theorem you know everything.

Let  $F$  be a field containing primitive  $n$ th root of unity. Now, I will not write any more that it satisfies the standing assumption star, it does of course, that is given. Let  $a$  be a nonzero element in  $F$ , let  $K$  be the splitting field of  $X$  power  $n$  minus  $a$  over  $F$ . Then two things, one,  $X$  power  $n$  minus  $a$  is irreducible, so maybe I will write it here as I have here then  $K$  over  $F$  is a cyclic extension.

So, this gives me the one-directional global theorem and the order of the Galois group is  $n$  if and only if  $X$  power  $n$  minus  $a$  is irreducible over  $F$ . So, this is on the face of it a slightly more general result than what we need. So, maybe before I start to prove I will also write theorem 2. So, that I have everything on one slide. So, then I can try to, so let  $n$  as above and let  $F$  be a field containing a primitive  $n$ th root of unity as above.

So, capital  $F$  and  $n$  in this entire class will be standard notation,  $n$  is a positive integer,  $F$  is a field containing a primitive  $n$ th root of unity, either the characteristic of  $F$  is 0 or its characteristic does not divide  $n$ . So, then let  $K$  over  $F$  be a cyclic extension of degree  $n$ . So, this is the second statement here,  $K$  over  $F$  is a cyclic extension of degree  $n$ , then  $K$  is a splitting field of an irreducible polynomial over  $F$ .



So, of course, that means  $a$  is in  $F$ , the polynomial is in  $F$ . So, now I can't show you the full slide in one screen, but to prove now 1 implies 2, we use theorem 1. So, basically what I am saying is 1 implies 2, by theorem 1 because you are assuming that  $K$  is a Kummer extension of  $F$  and then you are concluding that it is a cyclic extension. That is exactly 1 implies 2. And 2 implies 1, in theorem 2, we are taking a cyclic extension and concluding that it is a Kummer extension, so by theorem 2.

So, this is the way I want to break up the proof so that the different results that we are proving are clearer in your head. So, the global theorem about Kummer extensions is that, remember this as basically saying that if you start with a field containing a primitive  $n$ th root of unity, then an extension of that field is a Kummer extension if and only if it is a Galois extension with cyclic Galois group, that is all. So, now, maybe I will try to prove theorem 1 today. And then we will postpone the next theorem to next class.


(Refer Slide Time: 25:27)

Pf of this follows from the following 2 theorems. (2)  $\Rightarrow$  (1) by Thm 2

**Theorem 1:** Let  $n > 1$  be an integer. Let  $F$  be a field containing a primitive  $n$ th root of unity. Let  $a \neq 0 \in F$ ; let  $K = \text{Sp. fld of } X^n - a \text{ over } F$ . Then

- (1)  $K/F$  is a cyclic ext; and
- (2)  $|\text{Gal}(K/F)| = n \Leftrightarrow X^n - a$  is irr over  $F$ .

**Theorem 2:** Let  $n \geq 1$ ; and let  $F$  be a field containing a primitive  $n$ th root of unity. Let  $K/F$  be a cyclic ext of  $n = [K:F]$ . Then  $K$  is the sp. fld of an irr poly  $X^n - a$  over  $F$  (i.e.,  $a \in F$ ).




So, proof of theorem 1. So, what is the proof of theorem 1? Theorem 1 is right here. So, we are given that it is the splitting field of a polynomial of the form  $X^n - a$ , and we are also given that  $F$  contains a primitive  $n$ th root of unity. And we are going to prove that it is a cyclic extension and that if the degree of the extension is  $n$  if and only if it is an irreducible,  $X^n - a$  is an irreducible polynomial. So, now, let us start with the proof.

(Refer Slide Time: 26:07)

NPTEL

Pf of Theorem 1: Let  $\alpha \in K$  be a root of  $X^n - a$ .

If  $K = F$ , we are done:  $K/F$  is cyclic. ✓


We assume  $K \neq F$  and  $\alpha \notin F$ . Let  $\zeta \in F$  be a primitive  $n$ th root of 1.

Observe that  $\zeta^i \alpha$  are all the roots of  $f$  in  $K$ .  $\alpha^n = a \mid \alpha \in K$   
 $\Rightarrow (\zeta \alpha)^n = \zeta^n \alpha^n = a \mid \zeta \alpha \in K$

Roots of  $f$  are:  $\alpha, \zeta \alpha, \zeta^2 \alpha, \dots, \zeta^{n-1} \alpha$   
 $n$  distinct.

We definitely know that  $K/F$  is a Galois ext:  $K$  is normal since it is the sp. fld of a poly/ $F$  and  $\alpha \in K$  is separable over  $F$  (separable by the standing assumption \*).

$f = X^n - a$   
 $0$



Let  $\alpha$  in  $K$  be a root of  $X^n - a$ , remember in the theorem,  $K$  is the splitting field of  $X^n - a$ . So,  $X^n - a$  contains all the roots of that polynomial. So, let us take 1 of them. So, if  $K = F$ , we are done because  $K$  over  $F$  is, of course, Galois and cyclic. So in fact, let me write cyclic, it is cyclic and Galois group is not, I mean the second statement does not quite apply because that we will come to in a minute, I mean, here we are taking  $X^n - a$  basically. So if this is done, we are okay.

So, we assume  $K$  is not equal to  $F$  and  $\alpha$  is not in  $F$ , because  $K$  is generated by the roots of the polynomial,  $K$  is generated by the roots of the polynomial  $X^n - a$ . So, if all the roots are in  $F$ , then  $K = F$ , in which case we are done. So, we are assuming that there is a root that is not in  $F$ . And we are also given that  $F$  contains a primitive  $n$ th root of unity, let us take one of them. So, primitive  $n$ th root of 1 is  $\zeta$ .

So, now, observe that  $\zeta^i \alpha$  are the roots of  $f$  in  $K$ . In fact, are all the roots of  $f$  because  $\alpha^n = a$ , that means  $\zeta \alpha$  which of course is in  $K$ , so  $\alpha$  is in  $K$ ,  $\zeta$  is in  $F$ , so  $\zeta \alpha$  is in  $K$ . And this is  $\zeta^n \alpha^n = a$  which will continue to be  $a$  because  $\zeta^n = 1$ . So, the roots of  $f$  are  $\alpha, \zeta \alpha, \zeta^2 \alpha, \dots, \zeta^{n-1} \alpha$  and there are  $n$  distinct ones. Because  $\zeta$  is a primitive  $n$ th root of unity.

And in fact, we know also, that this polynomial by the assumption of the characteristic of  $F$  is separable. So, actually we definitely know that  $K$  over  $F$  is a Galois extension, this is because  $K$  is normal since it is a splitting field of a polynomial over  $F$ , and  $\alpha$  in  $K$  is separable over  $F$ . The last statement is because  $f$  which is  $X^n - a$  is separable by the standing assumption.

(Refer Slide Time: 29:38)


Roots of  $f$  are  $\alpha_1, \alpha_2, \dots, \alpha_n$   
 $n$  distinct.

We definitely know that  $K/F$  is a Galois ext:  $K$  is normal since  
 it is the sp. fld of a poly/ $F$  and  $\alpha \in K$  is separable over  $F$   
 ( $\because f = x^n - 1$  is separable by the standing assumption  $\chi$ )

$\therefore K = F(\alpha)/F$  is separable and normal

$\therefore K/F$  is Galois. Remains to show that  
 $\text{Gal}(K/F)$  is cyclic.

$f = x^n - 1$   
 $0$  is the only  
 root of  $f'$  as  
 $0$  is not a  
 root of  $f$




Namely, the characteristic is either 0 or the characteristic does not divide  $n$ , if the characteristic is nonzero, the  $f$  prime is nonzero. So,  $f$  prime is nonzero and is only 0 as the root because  $f$  prime is  $n x^{n-1}$ . So, only root of  $F$  prime is 0, but 0 is certainly not a root of  $f$ . So,  $F$  and  $F$  prime have no common roots. So, I will just record that here,  $F$  prime is  $n x^{n-1}$  and it is not 0.

So, 0 is the only root of  $f$  prime which is  $n \cdot 0$  is not a root of  $f$ . So, 0 is not a root of  $F$  and hence  $F$  and  $F$  prime have no common roots, so it is separable. So,  $\alpha$  is separable and hence,  $K$  which is  $F(\alpha)$  is separable. So, this is a property of separable extensions. So, if  $\alpha$  is separable every polynomial in  $\alpha$  is separable, so this is a separable extension and it is normal. So,  $K$  over  $F$  is Galois, it remains to show that Galois group is cyclic.

So, that is what remains to show and that is what I am now going to show. Because remember, the first part of the theorem is to show that  $K$  over  $F$  is a cyclic extension, which is to say, it is Galois plus Galois group is cyclic, that it is Galois is clear so that we have just shown, So, next step is to show that the Galois group is cyclic.

So, it is already 30 minutes. So, let us stop now and we will continue with the proof in the next video, and then we will also prove the second theorem. Thank you.