

Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture -38
Characterizations of Solvability - Part I

Welcome back. In the last class, we looked at radical extensions, as well as the notion of being solvable by radicals. So, a simple radical extension is one, where it is generated by a single element, which is a radical; namely it is an n th root of an element of the base field. A radical extension is one, where it is, where, there are lots of simple radical extensions in the middle. The entire extension may or may not be a simple radical.

And then, we say that a particular element is solvable by radicals, or simply solvable, if it is inside a radical extension; and the extension itself is solvable, if every element is solvable. And a polynomial is solvable, if its roots are solvable. So, we looked at examples of simple radical extensions. Kummer cyclotomic extensions are simple radical, and we also looked at examples, which are radical but not simple radical. So, $\mathbb{Q} \sqrt[3]{2} \sqrt[3]{3}$, as well as splitting field of a polynomial with 3 real roots.

(Refer Slide Time: 01:26)

But $K \subseteq \mathbb{R} \cdot \sqrt[3]{X}$

Eg: $X^3 - 3X + 1$ is irr and has 3 real roots (exercise)

Theorem: Let K/F be a Galois extension of degree $[K:F] = 6$. Then K/F is solvable. (That is: every element of K is solvable over F).

(char $F = 0$)



So now, our goal today is to prove the following theorem, that splitting fields of cubic polynomials are in fact radical; need not be simple radical, but they are radical. So, the theorem, that I want to prove today, is let K over F be a Galois extension of degree 6; of degree 6, then K over F is solvable. That means K is solvable over; that is every element of K

is solvable over F . That is our goal. And I am going to assume characteristic is 0, just to avoid some, maybe complications in some specific examples.

(Refer Slide Time: 02:22)

Char $F=0$ K/F is solvable. (That is: every element of K is separable)

Prop Let K/F be a cyclic extension (i.e., K/F is Galois and $\text{Gal}(K/F)$ is cyclic)
 Let $\alpha \in L$ where L is an extn of K . Then $K(\alpha)/F(\alpha)$ is also a cyclic ext
 and $[K(\alpha):F(\alpha)]$ divides $[K:F]$.



Prop Let K/F be a cyclic extension (i.e., K/F is Galois and $\text{Gal}(K/F)$ is cyclic)
 Let $\alpha \in L$ where L is an extn of K . Then $K(\alpha)/F(\alpha)$ is also a cyclic ext
 and $[K(\alpha):F(\alpha)]$ divides $[K:F]$. $\alpha \in L$
 $\begin{array}{c} K(\alpha) \\ | \\ K \\ | \\ F(\alpha) \\ | \\ F \end{array}$ cyclic

Pf: $G = \text{Gal}(K/F)$.

(i) $K(\alpha)/F(\alpha)$ is Galois: K is the sp fld of a separable poly $f \in F[X]$.

Say $K = F(\alpha_1, \alpha_2, \dots, \alpha_r)$ where α_i are roots of f .

Then $K(\alpha) = F(\alpha)(\alpha_1, \dots, \alpha_r)$ and $f \in F[X] \subseteq F(\alpha)[X]$.

So $K(\alpha)$ is a sp fld of a sep poly over $F(\alpha)$.
 ... is Galois.



So $K(\alpha)/F(\alpha)$ is Galois.

(ii) $\text{Gal}(K(\alpha)/F(\alpha))$ is iso to a subgroup of $\text{Gal}(K/F)$: Let $\sigma \in \text{Gal}(K(\alpha)/F(\alpha))$.

So $\sigma(\alpha) = \alpha$. Restrict σ to K : $\sigma|_K: K \rightarrow K$ (because K/F is normal)

$K(\alpha) \xrightarrow{\sigma} K(\alpha)$
 $\downarrow \quad \downarrow$
 $K \xrightarrow{\sigma|_K} K$
 $\sigma|_F = \text{id}$

We get a gp homom: $\text{Gal}(K(\alpha)/F(\alpha)) \xrightarrow{\psi} \text{Gal}(K/F)$
 $\sigma \mapsto \sigma|_K$.

ψ is a gp homom (easy)
 ψ is 1-1: $\sigma|_K = \text{id}, \sigma(\alpha) = \alpha \Rightarrow \sigma = \text{id on } K(\alpha)$

$|\text{Gal}(K(\alpha)/F(\alpha))|$ divides $|\text{Gal}(K/F)|$ \square

$[K(\alpha):F(\alpha)]$ $[K:F]$



(ii) $\text{Gal}(K(\alpha)/F(\alpha))$ is iso to a subgroup of $\text{Gal}(K/F)$

So $\sigma(\alpha) = \alpha$. Restrict σ to K : $\sigma|_K: K \rightarrow K$ (because K/F is normal)

$K(\alpha) \xrightarrow{\sigma} K(\alpha)$
 $\downarrow \quad \downarrow$
 $K \xrightarrow{\sigma|_K} K$
 $\sigma|_F = \text{id}$

We get a gp homom: $\text{Gal}(K(\alpha)/F(\alpha)) \xrightarrow{\psi} \text{Gal}(K/F)$
 $\sigma \mapsto \sigma|_K$.

ψ is a gp homom (easy)
 ψ is 1-1: $\sigma|_K = \text{id}, \sigma(\alpha) = \alpha \Rightarrow \sigma = \text{id on } K(\alpha)$

$|\text{Gal}(K(\alpha)/F(\alpha))|$ divides $|\text{Gal}(K/F)|$ \square

$[K(\alpha):F(\alpha)]$ $[K:F]$

Hint: ψ need not be onto. (eg. $\alpha \notin K$)

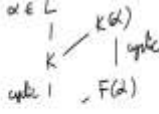


Eg: $X^3 - 3X + 1$ is ...

Theorem: Let K/F be a Galois extension of degree $[K:F] = 6$. Then K/F is solvable. (That is: every element of K is solvable over F).

Prop: Let K/F be a cyclic extension (i.e., K/F is Galois and $\text{Gal}(K/F)$ is cyclic). Let $\alpha \in L$ where L is an extn of K . Then $K(\alpha)/F(\alpha)$ is also a cyclic ext and $[K(\alpha):F(\alpha)]$ divides $[K:F]$.

so \dots



So, in order to prove this theorem, I am going to prove a very crucial result, that will be essential for everything that we do in the rest of the course. So, this I am going to call a proposition, this will be crucial for us. Let K over F be a cyclic extension. Remember, that means K over F is Galois, and the Galois group is cyclic. A cyclic extension is a Galois extension, whose Galois group is cyclic.

Let, α be, I mean so, in L ; where L is an extension of K . L is a completely irrelevant for us, but all I am really using L for is to get hold of an element, which is in L . So, L need not be, α need not be in K . So, L is irrelevant, except to provide us this element α . So, then the statement is $K(\alpha)$ over $F(\alpha)$ is also a cyclic extension. And moreover, the extension degree of $K(\alpha)$ over $F(\alpha)$ divides the extension degree of K over F .

So, what we have is, the picture is, I will draw it better. So, you have maybe here; L is some big field contained in K . There is an element α . So, you adjoin that to K , and $L(\alpha)$. So this is cyclic, implies this is cyclic. And the degree here, divides the degree here. It can very well be smaller, but it divides it. The proof is fairly simple. And it is crucial for all our arguments that follow.

So, first let us take the Galois group of the original extension to be G . So, I will first show that, $K(\alpha)$ over $F(\alpha)$ is Galois. Because remember, a cyclic extension is a Galois extension, whose Galois group is cyclic. So, I will first show that, it is Galois, then we will show that, its Galois group is cyclic.

So, by one of the characterizations of Galois extensions, we know that K is the splitting field of a separable polynomial. Separability comes of free, because we are in characteristic 0. But the crucial thing is, it is the splitting field of a polynomial. So, say K is $F(\alpha_1, \alpha_2, \dots, \alpha_r)$, where α_i are roots of f . So, this is trivial statement by the way, the whole proposition is easy; and this is even easier.

So, why is this Galois $K(\alpha)$ over $F(\alpha)$? So then, $K(\alpha)$ can be obviously written as $F(\alpha)$, adjoin α_1 through α_r ; and f of course is in $F[X]$, which is a subring of $F(\alpha)[X]$. So, $K(\alpha)$ is a splitting field of a separable polynomial over $F(\alpha)$. It is generated by the roots of the same polynomial. So it is a Galois; simple, right?

So, the same polynomial in capital $F[X]$, whose splitting field is K , will serve the job, role for us. We will do the job for us, because $K(\alpha)$ is a splitting field of same polynomial. Now,

we will just change the base field, and the polynomial is in the base field. So, there is no problem. So, this is Galois, and by the way, I do not think I need characteristic 0 here. So, separability is an assumption, but we are working in the same polynomial, so that is separable.

Second statement is Galois K^α over F^α is isomorphic to a subgroup of Galois K over F . So, this proves both statements that Galois K^α over F^α is cyclic, and this divides this. Because this order is $K^\alpha : F^\alpha$, this order is $K : F$. So, why is this? This is because of the following reason. So, let σ be in the Galois group of K^α over F^α . So, in particular σ^α is α .

So, we restrict to K . So, this means σ restricted to K is a function from K to K , because K over F is normal. So a priori σ is a function from K^α to K^α , which fixes F^α , and it fixes α . And then, you fix K in this. So, σ restricted to K a priori will land in K^α ; because K is normal, its image is again in K . So, it is an automorphism.

So, σ restricted to K is an automorphism of K over F ; of course, σ restricted to F is identity. Because, σ restricted to F^α is identity. So now, we get a group homomorphism from Galois K^α over F^α to Galois K over F , sending σ to σ restricted to K . This is the function. So, you take an automorphism of K^α , you restrict it to K .

So, ϕ is certainly a group homomorphism, because, I mean, you check this, because $\phi(\sigma \circ \tau)$ is $\sigma \phi$ of $\sigma \circ \tau$ is $\sigma \circ K \sigma$ restricted to $K \circ \tau$ restricted to K , but restrictions are really be the same thing. You are just taking elements from K . So, this is a group homomorphism is easy exercise. It is also easy to show that, it is 1-1. Because suppose, $\sigma|_K$ is identity, σ restricted to K is identity.

We also know that, σ^α is α . So, that means σ is identity on entire K^α because it fixes α by definition, because it is an automorphism of K^α , which fixes F^α . So, it means it fixes α . On other hand, if image of ϕ is identity that means σ restricted to K is identity. So now, what are elements of K^α .

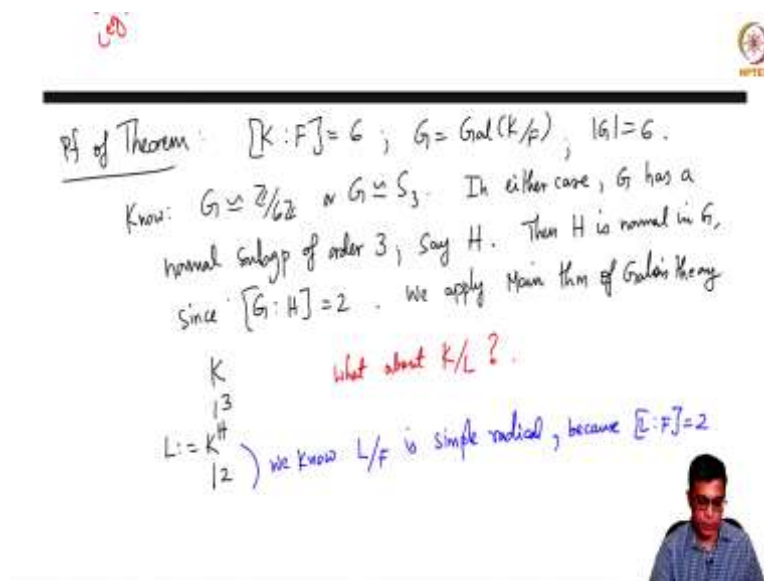
They are polynomials in α with coefficients in K . Every coefficient is fixed, because of this, α itself is fixed, so σ is identity. So, σ is an injective group homomorphism,

from Galois K^α over F^α to Galois K over F . That means, this is a subgroup of this. This is cyclic by hypothesis. So, this must be cyclic. Subgroup of a cyclic group is cyclic.

Strictly speaking, this is isomorphic to subgroup of this. This is cyclic. So this cyclic, not only that, because this is isomorphic subgroup of this, order of the Galois group of K^α over F^α divides order of Galois group over F , but order of Galois K^α over F^α divides order of Galois K over F . But this is $K^\alpha : F^\alpha$, and this is $K : F$; because both are Galois extensions.

So, this is done. So this proves this. This is a useful statement that we will use all the time in rest of the course. And I also want to remark finally about this proposition; ϕ need not be, need not be in general onto. For example, you can take α to be in F , α to be in K . So, if you take α to be in K , K^α is equal to K ; but F^α could be strictly bigger. So, this will be smaller than this. So, all we know is that, this is a subgroup of that.

(Refer Slide Time: 11:44)



$\text{Pf of Theorem: } [K:F] = 6; G = \text{Gal}(K/F); |G| = 6.$
 Know: $G \cong \mathbb{Z}/6\mathbb{Z}$ or $G \cong S_3$. In either case, G has a
 normal subgroup of order 3, say H . Then H is normal in G .
 Since $[G:H] = 2$. We apply Main thm of Galois theory.
 $\begin{matrix} K \\ |3 \\ L := K^H \\ |2 \end{matrix}$ what about K/L ?
 we know L/F is simple radical, because $[L:F] = 2$

$L = K^{\frac{1}{2}}$
 $|L:F| = 2$

we know L/F is simple radical, because $[L:F] = 2$

Know K/L is Galois with $\text{Gal}(K/L) \cong \mathbb{Z}/3\mathbb{Z}$

What we do now is important: If we knew K/L is a Kummer extn, then K/L is a radical ext and we are done ✓

But for K/L to be a Kummer ext, L must contain a primitive 3rd of unity. But in general it may not!



then K/L is a radical ext.
 But for K/L to be a Kummer ext, L must contain a primitive 3rd of unity. But in general it may not!
 We overcome this problem as follows:



Now, I will come back to the theorem that I started with. Proof of the theorem that I stated at the beginning of this class, so if you have a Galois extension of degree 6, sorry; K colon F here, if you have a Galois extension of degree 6. I want to show that, it is solvable. So, what do I do? So, K over F is degree 6 extension. Let us take the Galois group to be G , and we know, because the given extension is Galois, we have degree 6, order of G is 6.

So, let us take the following. So what we have is, we know this is irrelevant. But what we know is that, G is either $\mathbb{Z} \bmod 6\mathbb{Z}$; or G is S_3 , S_3 . Because that, those are the only 2 groups of isomorphism, which have order 6. In either case, what I said is this, it is irrelevant, which one it is. In either case, G has a normal subgroup of order 3. In the case of the cyclic group, it is abelian. So, every group is normal.

So, you take an order 3 subgroups, cyclic group. In S_3 also there is an order 3 subgroups, generated by 3 cycles; for example, generated by the 3 cycle. So, there is an order 3 subgroup, H . Then H is normal in G . Since it is a index 2 subgroup. I mean, you do not need the general result. You can make do with the specific statement, that in the case of $\mathbb{Z} \bmod 6\mathbb{Z}$, every group is abelian, subgroup is abelian.

In the case of S_3 , the order 3 subgroup is abelian; one can check directly. So now, we apply main theorem. So, we have $K \subset K^H$ and F . So, main theorem of Galois theory, I mean. So, we have this. And what are the degrees of these? So let us call this L , because the order of the group is 3, that is 3. Because index of the group is 2, this is 2. So now, in this I am going to assume the characteristic is different from 2.

As I said, our primary case is, characteristic is 0, but some of these results are generally true. So, we know K, L over F is simple radical. This is simple radical, because its degree 2, and F has characteristic different from 2. Any degree 2 extension of a field, which is of characteristic different from 2, is simple radical. It is obtained by a degree, adding a square root. But now, what about K over L ?

So, we will analyse K over L here. We know that, K over L is Galois. This is the usual statement. It is the trivial statement; if K over F is Galois, K over L will be Galois, for any intermediate field with Galois group, because the only group of order 3 is a cycling group of order 3. So Galois group of K over L is $\mathbb{Z} \bmod 3\mathbb{Z}$. So now, this is the tricky thing, this is important. So what we do now is important.

So, pay close attention to this, because we use this idea essentially to prove our next theorem. So, this is a simple example of what I want to do in the general theorem, that I will do next. If we knew, K over L is a Kummer extension, then K over L is a radical extension, and we are done. If it was a Kummer extension, we know that, it will be generated by a radical over L . So, but what stops it from being a Kummer extension?

But for, K over L to be a Kummer extension, it is a degree 3 extension. So for, it to be a Kummer extension; L must contain a primitive third root of unity. But in general, it may not. Say, we are working with an arbitrary field extension, K over F . So, and we constructed L along the way. So, there is absolutely no reason to think that, L will contain a cube root of unity.

And, if it does not as our examples earlier show; and if you think about this example, the reason that, this fails to be simple radical, is because Q does not contain a primitive 4th root of unity. So here, if L does not contain a primitive third root of unity; we are in a problem. Because, we are faced with a problem, because then it will not be simple radical.

However, remember our goal is to not show that, this is simple radical; our goal is to show that K over f is solvable. So, we are allowed to deviate from the given tower. We overcome this problem as follows.

(Refer Slide Time: 18:15)

Let ω be a primitive 3rd root of unity in an extn of K .

we have
 $\begin{array}{c} N \\ | \\ K \xrightarrow{K(\omega)} \text{ s.v.} \\ | \\ L \xrightarrow{L(\omega)} \\ | \\ F \end{array}$

K/L is cyclic $\xRightarrow{\text{Prop}}$ $K(\omega)/L(\omega)$ is cyclic

Now $L(\omega)$ does it contain a primitive 3rd of unity?


$K(\omega)/L(\omega)$ is cyclic $\xRightarrow{\text{Kummer}}$ $K(\omega)/L(\omega)$ is a simple radical extn.

If $L(\omega)$ contains ω

Now consider: $F \subseteq L \subseteq L(\omega) \subseteq K(\omega) \xrightarrow{K} K$

$\xRightarrow{2} \text{ s.v.}$ $\xRightarrow{\omega^3 \in L} \text{ s.v.}$ $\xRightarrow{\text{s.v.}}$

$\Rightarrow K(\omega)/F$ is a radical extn. and $K \subseteq K(\omega)$



$\begin{array}{c} N \\ | \\ F \end{array}$

$K(\omega)/L(\omega)$ is cyclic $\xRightarrow{\text{Kummer}}$ $K(\omega)/L(\omega)$ is a simple radical extn.


If $L(\omega)$ contains ω

Now consider: $F \subseteq L \subseteq L(\omega) \subseteq K(\omega) \xrightarrow{K} K$

$\xRightarrow{2} \text{ s.v.}$ $\xRightarrow{\omega^3 \in L} \text{ s.v.}$ $\xRightarrow{\text{s.v.}}$

$\Rightarrow K(\omega)/F$ is a radical extn. and $K \subseteq K(\omega)$

Hence every elt of K is Solvable over F , hence so is K . I



A more general result: Let K/F be a cyclic ext. Then K/F is solvable.
 (Assume $\text{char } F \neq 2$)

Prp: $n = [K:F]$ let s be a primitive n th root of unity in an ext. of K .
 K/F cyclic $\xrightarrow{\text{Prp}} K(s)/F(s)$ is cyclic
 \downarrow
 $K(s)/F(s)$ is S.R.
 $F \subseteq F(s) \subseteq K(s) \Rightarrow K(s)/F$ is radical. \square
 \downarrow
 (solvable) \downarrow (S.R.)



eg: $n = 6$

Theorem: Let K/F be a Galois extension of degree $[K:F] = 6$. Then K/F is solvable. (That is: every element of K is solvable over F).
 (char $F \neq 2$)
 (char $F \neq 3$)



Prp: Let K/F be a cyclic extension (i.e., K/F is Galois and $\text{Gal}(K/F)$ is cyclic).
 ... if L is an ext. of K , then $K(s)/F(s)$ is also a cyclic ext.



primitive 3rd of unity. that in general we overcome this problem as follows.

(Assume $\text{char } F \neq 2, \neq 3$)



Let ω be a primitive 3rd root of unity in an ext. of K .

N
 \downarrow
 K
 \downarrow
 L
 \downarrow
 F



Theorem: Let F be a field containing a primitive n th root of unity ζ_n . 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 . Kummer \Leftrightarrow cyclic
 - (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 $a \in F$, let $K = \text{Sp. fld of } X^n - a \text{ over } F$. Then



Theorem: Let F be a field containing a primitive n th root of unity ζ_n . 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 . Kummer \Leftrightarrow cyclic
 - (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 $a \in F$, let $K = \text{Sp. fld of } X^n - a \text{ over } F$. Then



(5) $f \in \mathbb{Q}[X]$ is an irreducible cubic which has 3 real roots.

$\mathbb{R} \supset K = \text{Sp. fld of } f \text{ over } \mathbb{R}$
Claim K/\mathbb{Q} is not simple radical. [we will prove later that K/\mathbb{Q} is not radical]

Pf: Suppose $K = \mathbb{Q}(\alpha)$, $\alpha \notin \mathbb{Q}$. Let $G = \text{Gal}(K/\mathbb{Q})$.

We know: $\sigma(\alpha) = s\alpha$ for an n th root of unity.

For some $\sigma \in G$, $\sigma(\alpha) \neq \alpha$, $\sigma(\alpha) \neq -\alpha$.

This is because $|G| \geq 3$. Then $\sigma(\alpha) = s\alpha$ for some $s \in \mathbb{R}$.

But $K \subseteq \mathbb{R}$.

$\therefore \dots$ has 3 real roots. (exercise)



So let us denote, ω be a primitive third root of unity in an extension of K . So again, let me draw the picture here. We have $L \subset F$ this is degree 2 this degree 3, and we have some large extension M , if you want, that contains ω . This M is relevant. All I need to know is that, there is a begin of extension that contains a primitive third root of unity. So, as I can see here, I want characteristic of F to be different from 3 also, in order to talk about primitive third roots of unity. So, this, I think, will hold in all other characteristics.

So, we will assume characteristic of F is different from 2, and different from 3. So, we do have an extension, which contains a cube root of 3, now, I adjoin that to ω $K(\omega)$; $K(\omega)$, and same I adjoin to this. Now, by, so we do know that, K over L is Galois. In fact, K over L is Galois with cyclic Galois group. So, K over L is cyclic. Because K over L is Galois with Galois group $\mathbb{Z}/3\mathbb{Z}$, so it is cyclic. Now, this is the important thing.

So, this is by the proposition. Proposition says that, if you have a cyclic extension; you attach an element to the bigger field, and same element to the smaller field; what you get is a cyclic extension. So this is a cyclic extension. And now, $L(\omega)$ does contain a primitive third root of unity by the very construction. So, $K(\omega)$ over $L(\omega)$ is cyclic, and $L(\omega)$ contains ω . This implies, go back to the videos, where we did Kummer extension.

This says that, $K(\omega)$ over $L(\omega)$ is a simple radical extension. So in that theorem, we did not necessarily use the word simple radical, but we did say that, it is generated by a single element; such that, the power of that is in $L(\omega)$, so maybe, I will quickly show this to you. So, I do not remember how long ago it was. So, this is a Kummer extension. So maybe, this is good. So, let F be a field containing a primitive n th root of unity, K over F is an extension of degree n . Then, the following are equivalent. K over F is a cyclic extension, apply this.

So, apply these to; I write this for now, but I will erase this. In our situation, apply this to $K(\omega)$ over $F(\omega)$. That is a cyclic extension by the proposition. The base field does contain a primitive n th root of unity. So K over F ; in this case, $K(\omega)$ over $F(\omega)$ is a Kummer extension, that means there is an a . Such that, $K(\omega)$ is a splitting field of $X^n - a$; that means K is F adjoin n th root of a . So, we are done.

So this is the result, that we will apply to conclude that, this is a simple radical extension. Now, K over L is not in general simple radical, but this is. So, this is simple radical. Now, we are done. So now, consider the following. So I am going to write it horizontally. So that it

is. I save some space here. So, I have F over L , L contained in L^{ω} , L^{ω} contained in K^{ω} . Now, each of these extensions is simple radical, I claim.

This is degree 2, so simple radical. This is simple radical, because ω^3 is in L . It is generated by an n th root of unity. So, this is a cyclotomic extension. So, it is simple radical, and this is simple radical by the argument, that I just gave you. So, this is simple radical. So now, and we note now that K is contained in this. So that means, every element of K . So basically that means, K^{ω} over F is a radical extension.

Because, K^{ω} . Remember, we are not saying that, K over F is a radical extension. This is an important point. We are only saying that, it is a solvable extension. So, K^{ω} over F is radical extension. Because there are, there is a tower of simple radical extensions, ending with K^{ω} . But, K is contained in a radical extension, so every element of K .

So hence, every element of K is solvable over F , because every element of K is in a solvable extension of F , is in a radical extension of F . So, let me show the definition, I gave in the last class. So, an element is solvable, if it is contained in radical extension. So here, every element of K is contained in K^{ω} , which is a radical extension of F . So, every element of K is solvable over F , and hence so is K .

So, this completes the proof of the theorem, which we started with today. That K over F is a Galois extension of degree 6; that means, K over F is solvable. I may have a sort of; So, I can see that, this is wrong; it is not necessarily radical, it is solvable. So, it need be radical in general. So however, it is solvable, as we showed here.

So, this idea that, we can extend our. So, this is a crucial step to go from a given extension with cyclic Galois extension, cyclic Galois group to something like this, by adjoining any roots of unity, that may require it to get a simple radical extension. So using this idea, we are going to show later, that we can prove, that radical extensions are essentially cyclic extensions.

So, let me end this video by more, stating a more general result, that comes out essentially from the same proof, is the following. Let K over F be a cyclic extension. Then K over F is solvable. What is a proof? The proof is very simple. So, assume here that important, that assume characteristic is 0. Because I mean, I can generalise this by

saying that, characteristic does not divide the degree. But I do not want to get into such technicalities. So, assume characteristic is 0. So, the same picture.

So, let us say, n equal to the degree of this extension. So, let ζ be a primitive n th root of unity in an extension field of K . So then, we have. So, we have some L contain in K contain in $F(\zeta)$ is here. Then I take $K(\zeta) = F(\zeta)$. L will go away now. L is only required to construct a n th root of unity. So, this is cyclic by assumption. So, K over F is cyclic. By the proposition, I proved in today's class. $K(\zeta)$ over $F(\zeta)$ is cyclic also.

And the base contains a primitive n th root of unity. So, this is simple radical. So, the tower of simple radical extensions, that we going to consider now, is F adjoin $F(\zeta)$ contained in $K(\zeta)$. So, this is a cyclotomic extension implies simple radical. This is simple radical, because it is Kummer. And K is contained in this. So, every element of K is contained in a radical extension.

So, this basically implies that, $K(\zeta)$ over F is radical. So, every cyclic extension is solvable. This is something that we will do. We will use, essentially this is the crucial idea in the proof of the next theorem. But let me stop this class here today. In the next class, we will discuss more properties of radical extensions. Thank you.