

Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 34
Kummer Extensions - Part 3

(Refer Slide Time: 00:16)


Part of the previous lecture

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

(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, $a \in F$).

Handwritten notes in blue ink:
 Kummer \Rightarrow cyclic
 cyclic \Rightarrow Kummer




Welcome back. we are proving certain theorems about Kummer extensions. These are extensions which adjoin an n th root to a field that already contains a primitive n th root of unity. And so far we have proved that a Kummer extension is a cyclic extension meaning a Galois extension, whose Galois group is cyclic.

And today we are going to prove that a cyclic extension is a Kummer extension. So, if F is a field containing a primitive n th root of unity and you have a cyclic extension of degree equal to n , then K is the splitting field of an irreducible polynomial of the form $X^n - a$, which is to say that it is a Kummer extension. So, we just started the proof last time. So, let me continue now.

(Refer Slide Time: 01:00)

Pf of Thm 2: F, n as above; K/F is a cyclic ext. ($\alpha \in F$)
 Then K is the sp fld of an irr poly $X^n - \alpha$ over F
 Let $G = \text{Gal}(K/F)$. (Note K/F is Galois and G is cyclic)
 by assumption
 Let $\zeta \in F$ be a primitive n th root of unity.
 $|G| = n$, and G is cyclic $\Rightarrow \exists \sigma \in G$ be a generator of G



Let $\zeta \in F$ be a primitive n th root of unity. ($G = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$)
 $|G| = n$, and G is cyclic $\Rightarrow \exists \sigma \in G$ be a generator of G
 Then $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are all distinct F -auto of K .
 By our earlier results on independence of characters: $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are ind as functions $K \rightarrow K$



$|G| = n$, and G is cyclic
 Then $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are all distinct F -auto of K .
 By our earlier results on independence of characters: $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are ind as functions $K \rightarrow K$ over F .
 $1 + \zeta \sigma + \zeta^2 \sigma^2 + \dots + \zeta^{n-1} \sigma^{n-1} \neq 0$ (not identically zero as a function on K).



NPTEL

$$1 + \zeta \sigma + \zeta^2 \sigma^2 + \dots + \zeta^{n-1} \sigma^{n-1} \neq 0 \quad (\text{a function on } K).$$

There exists $0 \neq \beta \in K$ st

$$\alpha := \beta + \zeta \sigma(\beta) + \zeta^2 \sigma^2(\beta) + \dots + \zeta^{n-1} \sigma^{n-1}(\beta) \neq 0.$$

Then $\sigma \alpha = \sigma \beta + \zeta \sigma^2(\beta) + \zeta^2 \sigma^3(\beta) + \dots + \zeta^{n-1} \sigma^n(\beta)$

$$\Rightarrow \sigma \alpha = \sigma \beta + \zeta \sigma^2 \beta + \zeta^2 \sigma^3 \beta + \dots + \zeta^{n-1} \sigma^n \beta$$

$$\Rightarrow \sigma \alpha = \zeta^{-1} (\zeta \sigma \beta + \zeta^2 \sigma^2 \beta + \zeta^3 \sigma^3 \beta + \dots + \zeta^n \sigma^n \beta)$$

\parallel
 α

$$\Rightarrow \sigma \alpha = \zeta^{-1} \alpha$$

$\Rightarrow \sigma \alpha = \zeta^{-1} \alpha$

$\sigma^n = 1$
 $\zeta = \zeta^{-1}$
 $\because \zeta^n = 1$
 $\Rightarrow \zeta^{-1} \zeta = 1$
 $\Rightarrow \zeta = \zeta^{-1}$



So, let us say G is the Galois group of that extension and ζ is a primitive n th root of unity in F . So, since G is n , order of G is n and G is cyclic, we do know that there is a generator which will be of course of order n . So, let us take σ in generator G . Then we have $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are all distinct F automorphisms of K . In fact, they are all the automorphisms of K , F automorphisms of K , because G is exactly those powers of σ .

So, now, way back we proved that any collection of distinct characters is independent. So, by our earlier results on independence of characters, so I am going to use that now. We have used this, of course, to set up Galois theory now we are going to use this directly again by our earlier results on independence of characters $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are independent as functions from K to K independent over F .

So, that means, in particular, $1 + \zeta \sigma + \zeta^2 \sigma^2 + \dots + \zeta^{n-1} \sigma^{n-1}$ is not identically 0 as a function on K . Because ζ , I mean, independence means non-trivial linear combination is 0, so ζ , of course, I mean you take 1 times 1 , ζ times σ and so on. So, this is a nonzero function, that means there exists a nonzero element β in K such that this function applied to β is nonzero. So, α which is defined to be $\beta + \zeta \sigma(\beta) + \zeta^2 \sigma^2(\beta) + \dots + \zeta^{n-1} \sigma^{n-1}(\beta)$ is nonzero. So, α is defined to be $\beta + \zeta \sigma(\beta) + \zeta^2 \sigma^2(\beta) + \dots + \zeta^{n-1} \sigma^{n-1}(\beta)$ is nonzero. So, α is defined to be $\beta + \zeta \sigma(\beta) + \zeta^2 \sigma^2(\beta) + \dots + \zeta^{n-1} \sigma^{n-1}(\beta)$ is nonzero.

So, it is not an identically zero function. That means, on some element in the domain it is nonzero. So, take a β on which it is nonzero and let us call the image α , so α is a nonzero element of K . Now, let us apply σ to α , then we are going to get a bunch of questions like this. So, let us apply σ to α , $\sigma \alpha$ is a homomorphism, and ζ

is fixed by sigma so I am going to write sigma square beta because sigma of sigma beta, sigma square beta, plus zeta square sigma cubed beta, all the way up to zeta n minus 1 sigma power n beta.

But what is sigma power n? So, I am going to write that here, sigma power n is identity. Because sigma is the generator of this group which has order n. So, this implies sigma alpha is sigma beta plus sigma square beta, zeta square sigma cubed beta, all the way up to zeta n minus 1 beta, because that sigma n beta is beta. So, now continuing this further, what we get is, and also note that zeta is an order n element also.

So, zeta power n minus 1 is another name for zeta inverse, this is because zeta n is identity, so zeta n minus 1 zeta is 1, that means zeta inverse is zeta n minus 1. Because zeta n minus 1 times zeta is 1 means, zeta n minus 1 is the inverse of zeta. So we can rewrite this as zeta inverse beta. So, now I am going to skip a step here. So, sigma alpha is equal to zeta inverse times zeta sigma beta, zeta square sigma square beta, zeta cubed sigma cubed beta, the previous term will be zeta n minus, so maybe I will write that here.

The previous term here is zeta n minus 2, sigma n minus 1 beta plus zeta n minus 1 beta, that was the previous talk. So, now I am factoring out zeta inverse. So, this will become zeta n minus 1, sigma n minus 1 beta plus beta. Zeta n minus 1 is just a scalar because it is in the base field, so I am pulling that out. So, you factor zeta inverse out, so zeta inverse which is of course, zeta power n minus 1, out.

So, here of course there is nothing, so it will be zeta inverse zeta. So, there must be, you have to increase the exponent of zeta in each place. So, zeta here, zeta square here. zeta cubed here, zeta n minus 1 here, and zeta power n here, that is 1. So, for this, if you just stare at this is, so let us see, what is this?

This first term is beta, I am going to put that here, this is exactly equal to alpha, because beta plus zeta sigma beta, zeta square sigma square beta, zeta cubed sigma cube beta, zeta n minus 1 sigma n minus 1 beta. So, this beta if you put here is exactly like alpha. So, this concludes the proof that sigma alpha is zeta inverse alpha, this is going to be used by us in a minute. So, this is a pure calculation, so there is nothing deep here and I hope the calculation is clear to you. So, sigma alpha is zeta inverse alpha.

(Refer Slide Time: 07:56)

claim: $\alpha^n \in F$. ✓

pf: $\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta \alpha)^n = (\zeta^n) \alpha^n = \alpha^n$
 $\Rightarrow \sigma(\alpha^n) = \alpha^n \Rightarrow \sigma^i(\alpha^n) = \alpha^n \forall i$.
 $\Rightarrow \alpha^n$ is fixed by $G \Rightarrow \alpha^n \in K^G = F$ $\hookrightarrow K/F$ is Galois

let $a_i = \alpha^{n_i} \in F$.

Then (1) K is the sp. fld of $X^n - a$:
 roots of $X^n - a$ in K : $\alpha, \zeta \alpha, \zeta^2 \alpha, \dots, \zeta^{n-1} \alpha$
 and $K =$



Remember, our goal is to prove that K over F is a Kummer extension, that means K must be obtained by adding an n th root, I claim that α itself is that n th root, which is to say α^n is in F . The proof is clear, it is a one-line proof. So, the proof is that $\sigma(\alpha^n)$ is, of course, $\sigma(\alpha)^n$ this is because σ is an automorphism, but $\sigma(\alpha)$ is $\zeta \alpha$ because $\sigma(\alpha)$ is a n th root of a and $\sigma(\alpha) \neq \alpha$, so $\sigma(\alpha) = \zeta \alpha$, but $\zeta^n = 1$ because ζ is an n th root of unity. So, $\sigma(\alpha^n) = \alpha^n$. So, this is just α^n .

This means $\sigma(\alpha^n) = \alpha^n$, this means α^n is fixed by σ , so this of course implies that α^n is in the fixed field of G because every element of G which is of the form, G is exactly $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$, each of them fixes α^n . So, α^n is in K^G , but K^G is of course F , this is because K over F is Galois. So, K^G is F , so that means α^n is in F , so that proves the claim. So, now we are going to take, let a be α^n which is in F .

So then, the first point is, K is the splitting field of, and the reason for that is clear because roots of $X^n - a$ in K are $\alpha, \zeta \alpha, \zeta^2 \alpha, \dots, \zeta^{n-1} \alpha$ and K is generated by them. K of course is, I mean, so remember what is the α that we have? So, I am going to prove this in a minute, but I think we should prove that $F(\alpha)$ is the splitting field. So, maybe I should write that here. $F(\alpha)$ is the splitting field of $X^n - a$, this is the first statement, this is easy of course.

(Refer Slide Time: 10:58)


Let $a = \alpha^n$.

Then (1) $F(\alpha)$ is the sp. fld of $X^n - a$.

$X^n - a$ splits completely over $F(\alpha)$ because all the n roots of $X^n - a$ are in $F(\alpha)$, namely $\alpha, \zeta\alpha, \zeta^2\alpha, \dots, \zeta^{n-1}\alpha$. n of them.

$F(\alpha)$ is generated by α over F .


$\alpha^n = a = \alpha^n$
 $(\zeta\alpha)^n = a$
 $(\zeta^2\alpha)^n = a$
 \vdots
 $(\zeta^{n-1}\alpha)^n = a$



$F(\alpha)$ is generated by α .

(2) $f = X^n - a$ is irr over F .

$\sigma(\alpha) = \zeta\alpha$
 $\Rightarrow \sigma^2\alpha = \sigma(\zeta\alpha) = \zeta^2\sigma(\alpha)$
 $\therefore \sigma^i\alpha = \zeta^i\alpha + i$




So, let me prove this carefully. So, $F(\alpha)$ is a splitting field of $X^n - a$, this is because $X^n - a$ splits completely over $F(\alpha)$, this is because all the n roots of $X^n - a$ are in $F(\alpha)$, namely. What are the n roots? α is one of them because $\alpha^n = a$, which is α^n . Then $\zeta\alpha$ is also a root because $(\zeta\alpha)^n = \zeta^n\alpha^n = \alpha^n = a$.

Similarly, if $\zeta^{n-1}\alpha$ is a root. This implies the roots are $\alpha, \zeta\alpha, \zeta^2\alpha$ all the way up to $\zeta^{n-1}\alpha$, there are n of them. So, all the roots are there, it splits completely. And of course, $F(\alpha)$ is generated by α over F . So, $F(\alpha)$ is a splitting field. Now, we claim, second statement is that $f = X^n - a$ is irreducible over F , second statement is this and then that will tie up everything. So, why is this irreducible? And the reason is the following.

So, note that sigma alpha is that I have showed earlier. So sigma alpha is zeta inverse alpha. So, this is what we have, and then this tells me that sigma square alpha, maybe I will write it here. So, sigma square alpha is sigma of alpha, which is zeta inverse alpha, which is zeta inverse sigma alpha, which is zeta inverse alpha, so that is zeta power minus 2 alpha. So, similarly, sigma power i alpha is for all i, so sigma i alpha is that. Now, sigma power.

(Refer Slide Time: 13:18)

$\therefore \sigma^i \alpha = \zeta^i \alpha + 1$


$K \xrightarrow{\sigma^i} K$
 $| \sigma^i |$
 $F(\alpha) \xrightarrow{\sigma^i} F(\alpha)$
 $| \text{Galois} |$
 F
 Each $\sigma^i \in \text{Gal}(F(\alpha)/F)$


$\sigma^i(\alpha) = \zeta^i \alpha \in F(\alpha) \Rightarrow \sigma^i(F(\alpha)) \subseteq F(\alpha)$
 $\Rightarrow \sigma^i$ restricts to an automorphism of $F(\alpha)$
 Moreover $\sigma^i \neq \sigma^j$ for $i \neq j$.
 Indeed: $\sigma^i(\alpha) = \sigma^j(\alpha) \Rightarrow \zeta^i \alpha = \zeta^j \alpha$
 $\Rightarrow \zeta^i = \zeta^j \Rightarrow i = j$

Hence: $n \leq |\text{Gal}(F(\alpha)/F)| = [F(\alpha):F] \leq [K:F] = n$

$\Rightarrow [F(\alpha):F] = n \Rightarrow F(\alpha) = K$

\therefore So $X^n - a$ is irreducible.

$f = X^n - a$;
 $\because \deg \alpha = [F(\alpha):F] = n$
 and $f(\alpha) = 0, \deg f = n$
 $\Rightarrow f$ is irr poly of α over F .



So, our situation is this, K is an extension of F alpha. And that is an extension of F. So, sigma is an automorphism of K, and sigma i sends alpha to zeta power minus i alpha which is an F alpha. So, each sigma i restricts to an automorphism of F alpha, because its image is contained again in F alpha. So, this implies sigma i of F alpha is contained in F alpha. Because once alpha has image in F alpha, capital F it is fixed.

So, for every polynomial in α with F coefficients, its image under σ^i is again in $F(\alpha)$. So, it is restriction automorphism, once it is contained in this because $F(\alpha)$ is an algebraic extension image is $F(\alpha)$. So, it is an automorphism of $F(\alpha)$. And moreover, σ^i is not equal to σ^j , for i not equal to j . Indeed, suppose $\sigma^i(\alpha) = \sigma^j(\alpha)$, if they are identical automorphisms of $F(\alpha)$, that means that they agree on α .

But that means, because $\sigma^i(\alpha) = \alpha^{p^i}$, and $\sigma^j(\alpha) = \alpha^{p^j}$, this implies. And here, of course, we are only taking i between i greater than equal to 0 but strictly less than n . But if $\alpha^{p^i} = \alpha^{p^j}$, this will guarantee that i equal to j . So, this is the proof of this. If i and j are different, σ^i cannot be equal to σ^j . I mean, this is another way of saying that σ has order n , as automorphism of K .

Because α separates powers of σ , they are distinct as automorphisms of $F(\alpha)$ also. So, hence, we are almost done now. The Galois group of $F(\alpha)$ over F has at least n elements because each σ^i , so the point is, each σ^i is in the Galois group of $F(\alpha)$ over F . So, that is the first statement here because it restricts automorphisms and the second statement is that they are all distinct.

So, there are at least n automorphisms in the Galois group of $F(\alpha)$ over F . But this is equal to $[F(\alpha) : F]$, if you want, because this is a Galois extension. Because it is a splitting field of a separable polynomial. I mean, it is splitting filled up this polynomial which is separable by characteristic assumption. But this is less than or equal to $[K : F]$, because $F(\alpha)$ is an intermediate field.

So, this degree is less than this degree, but this is of course n is by hypothesis, so that is part of hypothesis and hence, everything here is 1 equal. So $[F(\alpha) : F]$ is equal to n , this means $F(\alpha)$ is equal to K . So, I mean, the statement that X^n is irreducible, because if it is not irreducible then the degree of α over capital F , which is the extension degree is less than or equal to n , because α satisfies and if this is equal to n .

So, if this is equal to n is what we have just shown and $F(\alpha)$ is K , so I am sort of messing this up a little bit, but $F(\alpha) = K$, F is, of course, $X^n - a$. Then $F(\alpha)$ is K , degree $[F(\alpha) : F]$ is n and degree of the irreducible polynomial of α over F is n . So, that means F is the irreducible polynomial of α over capital F . That means, this is irreducible.

So this completes the proof that, so let us go back to the original statement of theorem 2.

(Refer Slide Time: 18:35)

$\text{Kt of the previous slide}$
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
 (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., $a \in F$).

Kummer \Rightarrow cyclic
 cyclic \Rightarrow Kummer



If you are given a cyclic extension, we did prove that K is the splitting field of an irreducible polynomial this we just showed over the base field which is to say a cyclic implies Kummer, Kummer implies cyclic. And hence, this theorem is proved, the theorem, main theorem which is to say Kummer, if and only if, cyclic. So, this is saying that Kummer if and only if cyclic. So, I have a few minutes left in this class. So, let me just tie up some loose ends and prove or at least to start studying something which will help us when we talk about solving polynomials by radicals.

(Refer Slide Time: 19:21)

Def: Let F be a field; K/F is an ext. and $\alpha \in F$. We say that α is "expressible by radicals over F " if there exists a tower of field exts:
 $F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_r$ s.t.
 (i) $\alpha \in F_r$

$\Rightarrow f = \text{irr poly of } \alpha \text{ over } F$

F_r
 $|$
 F_{r-1}
 $|$
 F_1
 $|$
 $F_0 = F$



Def: Let α be a number, $\alpha \in F_r$. We say that α is "expressible by radicals over F " if there exists a tower of field extns: $F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_r$ s.t.

- (i) $\alpha \in F_r$ and
- (ii) Each ext F_i/F_{i-1} is a "radical extn", i.e., $F_i = F_{i-1}(\alpha_i)$ with $\alpha_i^{n_i} \in F_{i-1}$.

Recall from the first class: α can be expressed using elts of F and $+$, $-$, \times , \div and radicals (taking roots)

$$F_r = F_{r-1}(\alpha_r)$$

$$F_2 = F_1(\alpha_2), \alpha_2^{n_2} \in F_1$$

$$F_1 = F_0(\alpha_1), \alpha_1^{n_1} \in F_0$$

$$F_0 = F$$



So, let me just give you a preview of what we are going to do later. So let us say F is a field and let us say K is some extension of F , and α is in F . So, we will come back and give these definitions formally later. But I wanted to use Kummer extensions that we just studied so that this will be fresh in your mind to indicate what we will do later.

So, we say that α is expressible by radicals over F if there exists a tower of field extensions. Let say F , which is F_0 , then F_1 , finally F_r . So, in our usual way, this is $F, F_{r-1}, F_{r-2}, \dots, F_1, F_0$ which is F . Such that a couple of things happen, one is that α is in F_r . So, this K that I started with is irrelevant for this, K is just given so that we need to talk about some elements that are in an extension field, so otherwise, K is not important.

And two, each extension F_i over here F_{i-1} is a radical extension. That is F_i equals $F_{i-1}(\alpha_i)$, so radical extension is one where it is obtained by adding a radical. So, what we are saying is that this is $F_0(\alpha_1)$ and a power of α_1 , $\alpha_1^{n_1}$ is in F_0 . So, F_2 will be, so maybe I will just use that here, $F_1(\alpha_2)$ where $\alpha_2^{n_2}$ is in F_1 and so on. So, all the way like that, and this will be $F_{r-1}(\alpha_r)$, where $\alpha_r^{n_r}$ will be in the previous field.

So, if you recall from the beginning, first-class in fact. In that language, α can be expressed using elements of F and addition, subtraction, multiplication, division and radicals. So, that means taking roots. Because α is in F_r , so it can be written as a polynomial with F_{r-1} coefficient with polynomial α_r . But α_r is the root of something in F_{r-1} . So, it becomes obviously very messy, but in principle you can do that.

(Refer Slide Time: 23:35)

Recall from the first class: α can be expressed using $+$, $-$, \times , \div and radicals (taking roots)



eg: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) \ni \alpha$

$$\alpha = a + b\sqrt{2} + c(\sqrt[3]{5})^2 + d(\sqrt[3]{5}) + e\sqrt{2}\sqrt[3]{5} + \dots$$

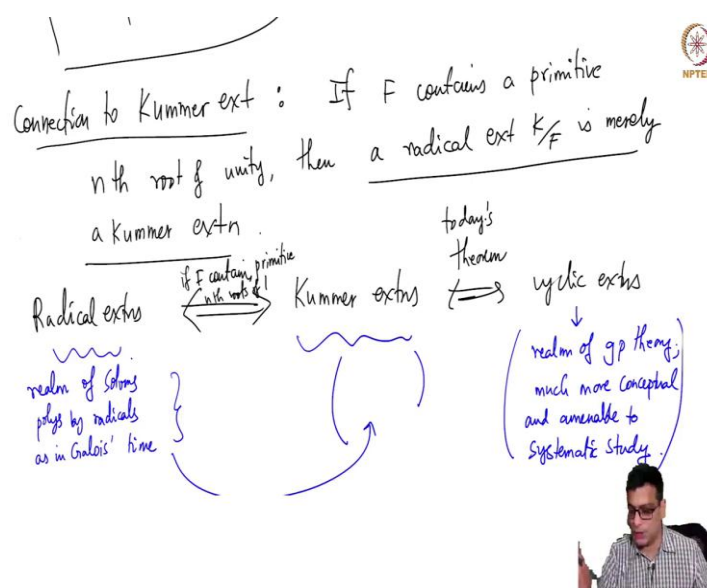
any elt of this can be expressed as a function of rational numbers using radicals.



For example, simple example, let us say you have \mathbb{Q} , contained in $\mathbb{Q}(\sqrt{2})$, containing $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. So, anything here can be expressed in terms of radicals and rational functions. For example, cube root of 5, so any element of this can be expressed using the usual operations but radicals. So, the point is, you take this, I mean any functional element here will be something, some root 2, a plus root 2, b root 2 plus C times cube root of 5 plus d times cube root of 5 whole square, plus e times root 2 times cube root of 5, I mean it can be something complicated.

I do not care how complicated it is, but it can be done is the point. So, the Galois theorem is used to show that roots of a quintic polynomial cannot be expressed like this. The main achievement of Galois theorem is that, there is a quintic polynomial whose roots cannot be expressed by radicals that means you cannot construct a tower of fields like this.

(Refer Slide Time: 25:16)



Let me quickly tell you how to connect this to Kummer extensions. If F contains primitive n th root of unity, then a radical extension is merely or simply a Kummer extension, so this is the important thing. So, remember radical extension, this is the crucial property that we are seeking in solvability of quintic. And Kummer extensions are like that, except that you need to have a primitive n th root of unity and a suitable radical extension, not any radical extension but a radical extension where you only adjoin n th roots.

And Kummer, if and only if cyclic, assuming that F contains a primitive n th root. So, bas what I am really saying is that, this is in the realm of solving polynomials by radicals, this is something that mathematicians were trying to do 200 years before Galois. So, this is brute force expressions of roots. So, think of Kummer extensions, so maybe I will write down radical extensions if and only if Kummer extensions, I mean equivalent to Kummer extensions equivalent to cyclic extensions.

So, this is our theorem today and this is if F contains primitive n th roots. So, this is not, in general, true, but this is in the realm of solving polynomials by radicals as in Galois' time. And this is, of course, the same thing. So, this is like this, because if F contains primitive n th roots, but most of the time it will not, right, because Galois was interested in solving polynomials over \mathbb{Q} , which will not contain, we will know how to address that later.


So, this is the same as this, but this is not doing by brute force, but this is in the realm of group theory. So, this is much more conceptual and amenable to systematic study. So, now, the point of Galois is he translated the problem of messy formulas for roots which existed for

cubic's and cortex, and of course, quadratic formula also. And people are trying to see whether such a formula existed for quantic.

That becomes very messy. And if you search online for cardinal's formula, for cubic's, and similar formulas for quadratics, they become extremely messy, and in fact, you do not know how to use them. And it was just hopeless to see if there is such a thing existed for quintic using such methods. Galois really translated the whole problem into a much more systematic and conceptual problem using group theory, and this is a crucial bridge, we converted Kummer extensions to cyclic extensions.

And hence this theorem, today's theorem, or the theorem of the last two, three videos is hence very important for us it allows us to compare radical extensions to cyclic extensions. And modular these simple remains, this slight worry that we have that Kummer extensions are not just radical, but radical extensions where the base will contain primitive nth roots of unity. But that we will easily solve the problem.

(Refer Slide Time: 30:05)



We will see later: $F \subseteq K \quad \alpha \in K.$

Cond I $\{ \alpha \text{ is expressible by radicals over } F \} \iff$ If F contains primitive roots of unity this is already follows from our theorem on Kummer extns.

Cond II $\{ \exists \text{ a tower of fields } F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_m \text{ s.t. } \alpha \in F_m' \text{ and each } F_i'/F_{i-1}' \text{ is a cyclic extn.} \}$


Cond I

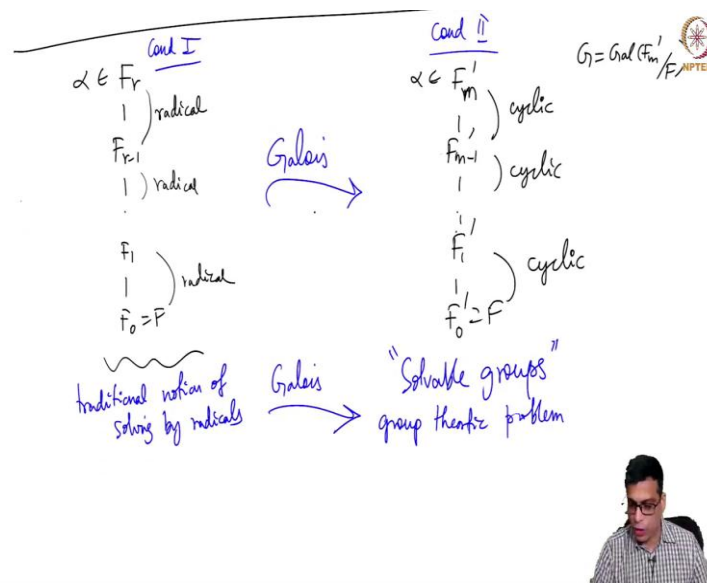
$\alpha \in F_r$
| radical

Cond II

$\alpha \in F_m'$
| cyclic

$G = \text{Gal}(F_m'/F_r)$





So, we will see later that F is any extension, any field and K is an extension field and α is in K , α is expressible by radicals over F if and only if. So the definition is this, where there is a tower, so this means, I will write it here, so this condition 1 and I will write condition 2 here. But condition 1 is really saying that there is a tower like this, such that α is in the last one, such that each of them is a simple radical extension, meaning it is obtained by taking an n th root.

As I said, that is messy and it is not easy to deal with such definition. Whereas, the second condition is, there is a tower of field, let us say F equals F_0 prime, F_1 prime, F_2 prime or F_M prime such that α is in F_M prime and each F_i prime over F_{i-1} prime is a cyclic extension. So, basically this is condition 1 and this is condition 2. The condition 2 says, this very complicated looking tower is replaced by a very beautiful, simple and conceptual tower, where the last one contains α , as always, but this is nothing, it is not messy like what is the radical extension but it is simply a cyclic extension.

So, now, it is not clear at all in this world, any information about the group that you have can say nothing about whether such a tower exists or not. Whereas, the group, any such tower has very strong restrictions on the group because. For example, if you take the Galois group of the extension F_M prime over F , there is something called a composition series or there is a chain of subgroups, right, because there is a cyclic subgroup of G such that the quotient has such an expression.

So, this is related to the notion of solvable groups. So, what I am trying to say here, is just an indication of what is to come, this is the traditional notion of solving by radicals. So, this is the traditional notion. Galois converted this into a group theoretic problem, this is the

contribution of Galois. And then you can argue all of this we will do later, basically you can argue that S_5 is not solvable.

And hence, if not any polynomial degree 5 polynomial, he constructed certain degree 5 polynomials whose roots, if they can be solved by radicals, then there is a corresponding picture like this, which would imply that S_5 is solvable, but it is not. So, this is the crucial theorem that makes it work and this is a crucial data which connects Galois theory, which connects classical problem of solving by radicals into groups, problem in group theory. And all of this, I am saying it today because it is connected to Kummer extensions.

So, this will be used, Kummer extensions will be used when we prove this. If F contains the final remark, let me, I have taken too much of your time already, but final remark I will make is that if F contains primitive roots of unity, I will not say which primitive, n th roots for various n , I mean, because it depends on what our degrees of these. If F contains primitive n th roots of unity, this equivalence, this already follows from our theorem on Kummer extensions.

So, that is what I want to end today with. Basically if F contains primitive n th roots of unity, then radical extensions are nothing but Kummer extensions, and Kummer extensions are cyclic so you can just take the same thing at each stage, this is Kummer, so this is cyclic. But F may not contain primitive n th roots of unity. In fact, the most interesting case for S is when F is \mathbb{Q} , which will not contain primitive n th roots of unity, except when n is 1 and 2. So, we will need to figure out what to do with that, but that is a simple trick that will solve that problem, and that is the place where we have to deal with cyclotomic extensions which we are going to do in the next video.

So, the next next one or two videos will do cyclotomic extensions and after that, we will get to the business of the course, which is to show that quintic polynomials cannot be solved by radicals in general. So, let me stop today here, and then we will continue with cyclotomic extensions in the next class. Thank you.