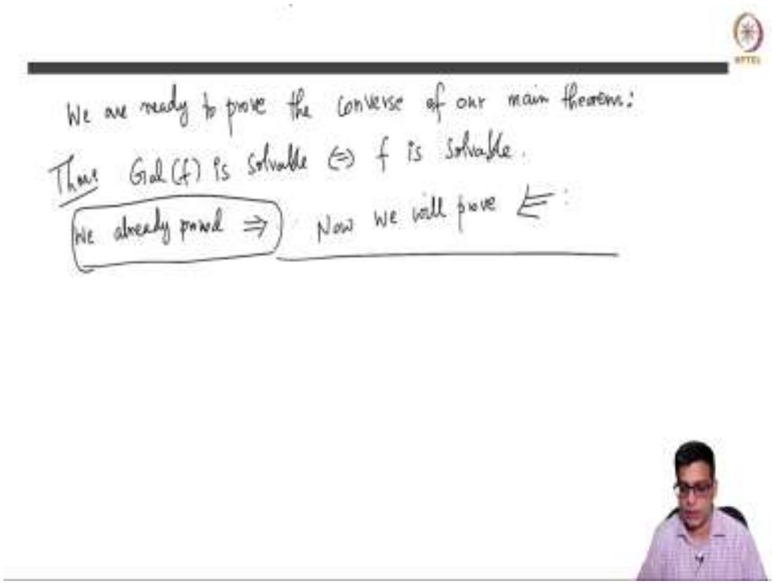
# Introduction to Galois Theory
## Professor. Krishna Hanumanthu
## Department of Mathematics
## Chennai Mathematical Institute
## Lecture No. 44
## Solvable Groups – Part 3

(Refer Slide Time: 0:17)



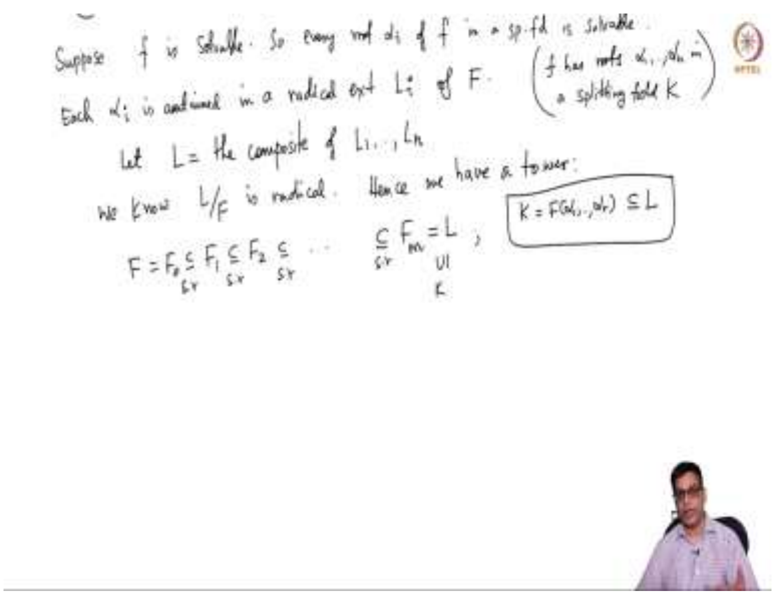
We are ready to prove the converse of our main theorem:

Thm: Gal(f) is solvable $\Leftrightarrow$ f is solvable.

$\boxed{\text{We already proved } \Rightarrow}$ Now we will prove $\Leftarrow$:

Welcome back, we are now ready to prove the converse direction of the theorem; that we are now doing in the last couple of videos. Namely, that Galois group of a polynomial is solvable, if and only if the polynomial itself is solvable.

(Refer Slide Time: 00:30)



Suppose $f$ is solvable. So every root $\alpha_i$ of $f$ in a sp.fd is solvable.

Each $\alpha_i$ is contained in a radical ext $L_i$ of $F$. ($f$ has roots $\alpha_1, .., \alpha_n$ in a splitting field $K$)

Let $L =$ the composite of $L_1, .., L_n$

We know $L/F$ is radical. Hence we have a tower:

$F = F_0 \underset{s.r}{\subseteq} F_1 \underset{s.r}{\subseteq} F_2 \underset{s.r}{\subseteq} \cdots \underset{s.r}{\subseteq} F_m = L$ , $\boxed{K = F(\alpha_1, .., \alpha_r) \subseteq L}$

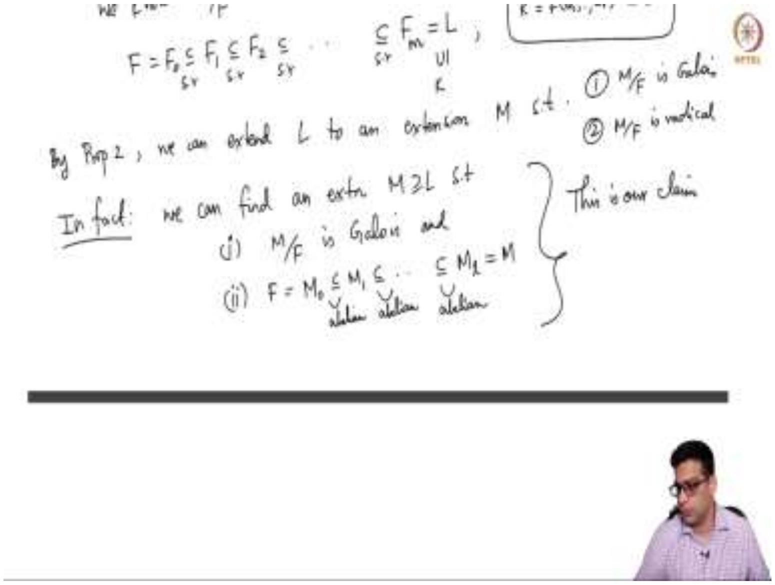
$\underset{K}{\cup\!|}$

So, suppose f is solvable; so this means by definition so every root of alpha i of f in a splitting field is solvable. So, this means I am not going to spell out exactly, so each alpha i; so alpha 1 through alpha n are the roots. So, each alpha i is contained in in an extension field in a radical extension; that is what it means to be solvable, radical extension Li of F. So, alpha 1 is contained in L1, alpha 2 is contained in L2, alpha n is contained in Ln, and Li's are all radical extensions of F. So, now let L be the composite of all of them, so f has roots alpha 1 through alpha n in a splitting field K; that is the set up.

So, remember I defined the composite of 2 fields, but of course now you can define the composite of 3 fields; 3, 4 fields and so on, for any finite set. So, let L be the composite of L1 through Ln, we know that L over F is radical by the previous class. We know that composite of radical extensions is radical; so, hence we have a tower as follows. We have F which is equal to F0 contained in F1, contained in F2, contained in Fr let say, which is equal to L. I am going to call it Fm, and the point is this is simply radical, this is simply radical, this is simply radical and this is simply radical.

This is the meaning of L being radical over capital F; that means L to F there is a tower of simply radical extensions. And of course, L contains K which is the splitting field; so K is contained in. So, K is the splitting field, so it is generated by alpha1 through alpha r up to over l. So, it is going to be contained in L, this is our situation.

(Refer Slide Time: 03:17)

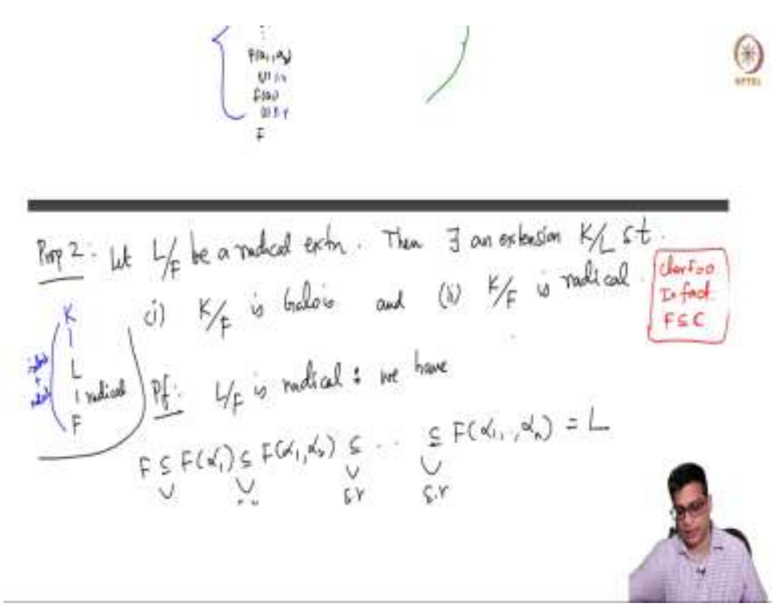


$F = F_0 \underset{s.r}{\subseteq} F_1 \underset{s.r}{\subseteq} F_2 \underset{s.r}{\subseteq} \cdots \underset{s.r}{\subseteq} F_m = \underset{\substack{\cup\!| \\ K}}{L}$ ;

By Prop 2, we can extend L to an extension M s.t. ① M/F is Galois ② M/F is radical

In fact: we can find an extn $M \supseteq L$ s.t.
(i) M/F is Galois and
(ii) $F = M_0 \underset{\text{abelian}}{\subseteq} M_1 \underset{\text{abelian}}{\subseteq} \cdots \underset{\text{abelian}}{\subseteq} M_l = M$

This is our claim



$F(\alpha_1,\alpha_2)$
$\cup\!|$ s.r
$F(\alpha_1)$
$\cup\!|$ s.r
$F$

Prop 2. Let L/F be a radical extn. Then ∃ an extension K/L s.t.
(i) K/F is Galois and (ii) K/F is radical.

char F = 0
In fact
$F \subseteq \mathbb{C}$

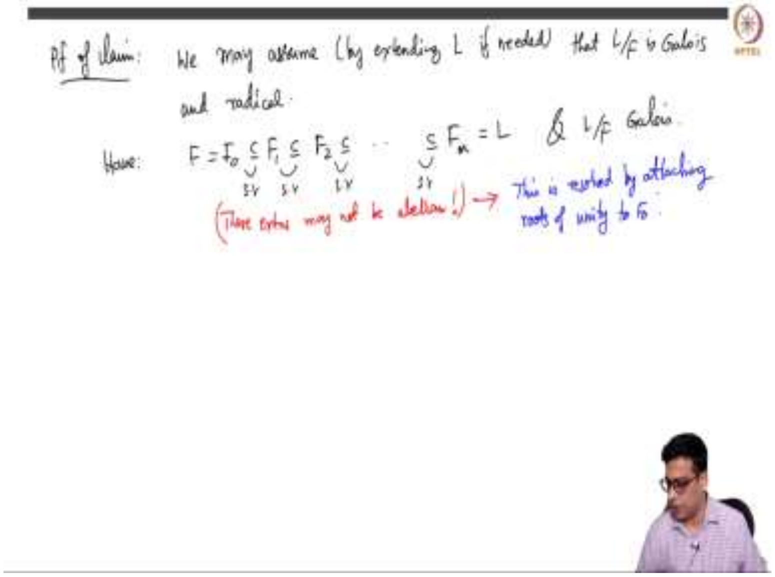
K
|
L
| radical
F

Pf: L/F is radical: we have
$F \subseteq F(\alpha_1) \subseteq F(\alpha_1,\alpha_2) \underset{s.r}{\subseteq} \cdots \underset{s.r}{\subseteq} F(\alpha_1,\ldots,\alpha_n) = L$

Now, by proposition 2 of the previous class we can extend L to an extension K; I mean so let me use some other letter, so I already used K. We may M over F such that 1: M over F is Galois; in 2: M over F is radical. So, I have to do over than this to conclude that the Galois group is radical; but what I will do now is the following. And this is just preposition 2 if you recall, given a radical extension you can always extend it further; so that the bigger extension is radical as well as Galois.

But, in fact what I want to do is in fact, we can find an extension M such that M contained in L. Such that 1: M over F is radical or rather M over F is Galois; and 2. So, there is a tower starting with F like this and ending with M, such that each of them is abelian; so that is my goal. So, let me first claim this, so this is our claim. I will prove the claim and then show that that will imply what we want.

(Refer Slide Time: 05:28)



Pf of claim: We may assume (by extending L if needed) that L/F is Galois and radical.

Have: $F = F_0 \underset{\text{s.r.}}{\subseteq} F_1 \underset{\text{s.r.}}{\subseteq} F_2 \underset{\text{s.r.}}{\subseteq} \cdots \underset{\text{s.r.}}{\subseteq} F_m = L$ & L/F Galois.

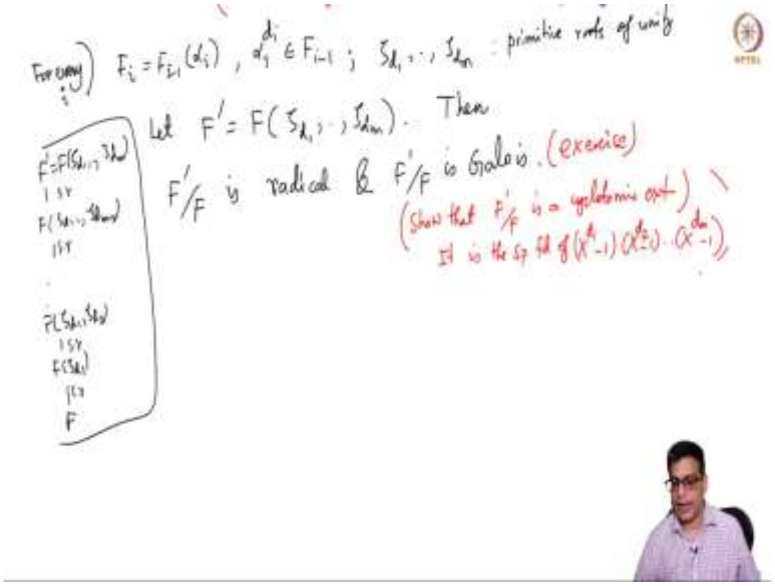
(These extns may not be abelian!) → This is resolved by attaching roots of unity to $F_0$.

So, why can we do this proof of claim? So, the proof of claim is we may assume by extending L if needed that L over F is Galois and radical. So, that is because we can extend it by the preposition that I proved in last class; that you can extend it get a bigger extension which is Galois and radical. So, I might as well call the new thing L, and all the intermediate things I will call F1 through Fr. So, I will assume without loss of generality that L over F is Galois and radical. So, we have F equal to F0 contained in F1 contained in F2, contained in Fr or Fm, I called it Fm; I will just use the same notation.

So, this is radical, simple radical in fact, this is simple radical, this is simple radical, this is simple radical; and L over F is Galois. Now, what prevents this? Why I cannot take this itself and claim these 2 properties. The reason is of course I have Galois, but I do not necessarily have abelian. So, the problem is this, these extensions may not be abelian; in general simple radical extensions are not abelian.

However, if they become Kummer extensions, meaning if the base field for each successive extension contains a right root of unity, this becomes a Kummer extension and become cyclic and hence, abelian. So, this problem this is resolved by attaching roots of unity as required. So, just let me spell it out. We have done this earlier in our big theorem about equal n's of radical extensions with other kinds of extensions. But, let me quickly tell you what we do here.

(Refer Slide Time: 08:10)



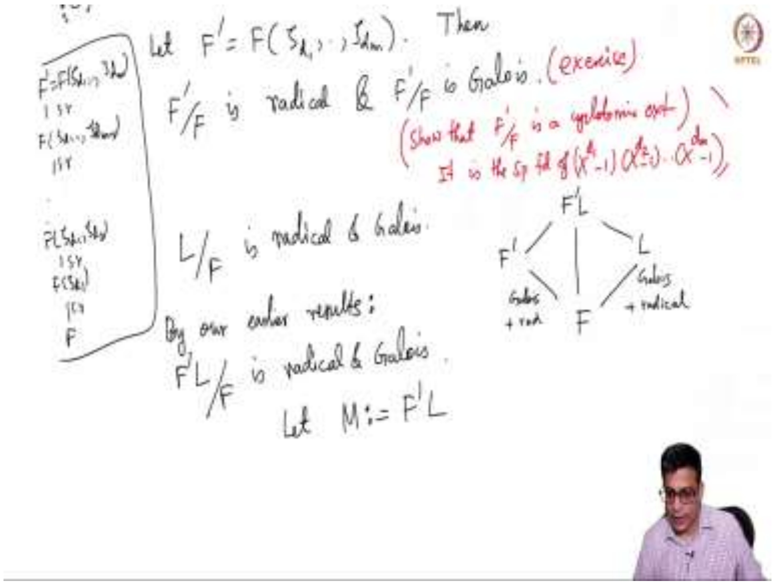
For every $i$) $F_i = F_{i-1}(\alpha_i)$, $\alpha_i^{d_i} \in F_{i-1}$ ; $\zeta_{d_1}, \ldots, \zeta_{d_m}$ : primitive roots of unity

Let $F' = F(\zeta_{d_1}, \ldots, \zeta_{d_m})$. Then

$F'/F$ is radical & $F'/F$ is Galois. (exercise)

(Show that $F'/F$ is a cyclotomic ext.) It is the sp fd of $(x^{d_1}-1)(x^{d_2}-1)\cdots(x^{d_m}-1)$

$F' = F(\zeta_{d_1}, \ldots, \zeta_{d_m})$
| SR
$F(\zeta_{d_1}, \ldots, \zeta_{d_{m-1}})$
| SR
⋮
$F(\zeta_{d_1}, \zeta_{d_2})$
| SR
$F(\zeta_{d_1})$
| SR
$F$



Let $F' = F(\zeta_{d_1}, \ldots, \zeta_{d_m})$. Then

$F'/F$ is radical & $F'/F$ is Galois. (exercise)

(Show that $F'/F$ is a cyclotomic ext.) It is the sp fd of $(x^{d_1}-1)(x^{d_2}-1)\cdots(x^{d_m}-1)$

$F' = F(\zeta_{d_1}, \ldots, \zeta_{d_m})$
| SR
$F(\zeta_{d_1}, \ldots, \zeta_{d_{m-1}})$
| SR
⋮
$F(\zeta_{d_1}, \zeta_{d_2})$
| SR
$F(\zeta_{d_1})$
| SR
$F$

$L/F$ is radical & Galois.

By our earlier results:
$F'L/F$ is radical & Galois.

Let $M := F'L$

$$\begin{tikzcd}
 & F'L \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\
F' \arrow[dr, dash, "\text{Galois + rad}"'] & & L \arrow[dl, dash, "\text{Galois + radical}"] \\
 & F &
\end{tikzcd}$$

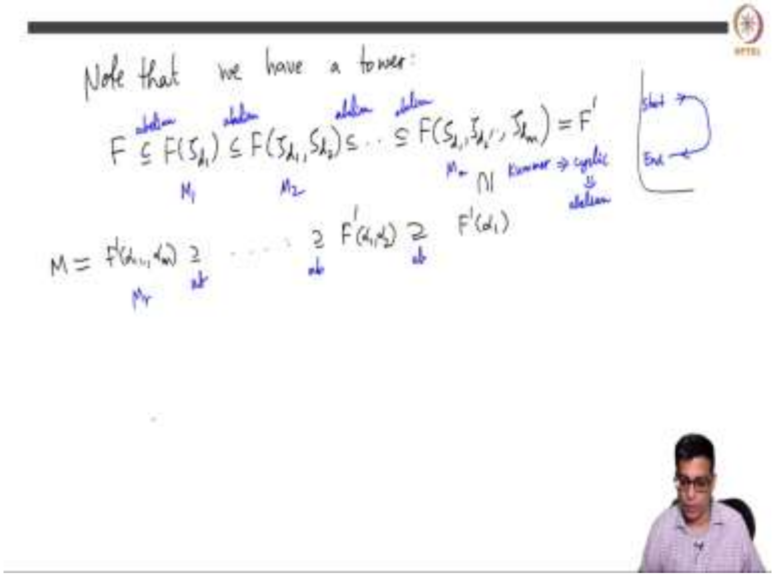
So, suppose Fi is Fi minus 1 adjoint something let say alpha, with alpha power di being in Fi minus. So, for every i we have this. Because each Fi is a radical extension of Fi minus 1, it is generated by a root; a particular single alpha i, whose dith power is this. So, now let us take zeta d1, zeta dm are primitive roots of unity; of course of the appropriate order. Zeta d1 is the primitive d1 is a primitive d1th root of unity; zeta dm is a primitive dmth root of unity. So, let F prime now be F adjoint zeta d1, zeta dm; so, this is a radical extension. So, now I claim that this is radical and Galois.

Because this is at F contains all the, so now basically what I want to say is that then F prime over F is radical of course. Because you can add one by one F prime, so is F adjoint all of them; you do zeta dm minus 1 and all the way up to F zeta d1, zeta d2, F zeta d1, F zeta or just F. These are all simple radical extension, adding them one by one; and I claim that and F prime over F is Galois. Think of this, this is an exercise for you; this is because this is a sequence of cyclotomic extensions. So, this F prime over F in fact is a cyclotomic extension, so you can show that.

For example I am showing that if you take a primitive d1th root of unity, all the d1th roots of unity are there. So, zeta dm is a primitive dmth root of unity; so all the roots of dmth rots of unity are there. So, it is the splitting field of X power d1 minus 1, X power d2 minus 1; all the way up to X power dm minus 1. It is radical and Galois; on the other hand, we also L over F is radical and Galois. So, our situation is you have F, F prime Galois plus radical; you have L, which is Galois plus radical. Because L is by hypothesis, originally L is given to be radical extension. But, I have enlarged it if needed to make it Galois also.

Now, you take F prime L the composite; again take the composite in a algebraic closure. I do not want to tell you which ambient field; I do not care which it is. But, now by our earlier results L F prime L over F is radical and Galois; because composite of radical extensions is radical, composite of Galois extensions is Galois that this exercise; so composite of radical and Galois extensions is radical and Galois, so call this M. So, let M, we can find an extension M, such that which is Galois and radical.

(Refer Slide Time: 12:51)



Note that we have a tower:

$$F \overset{abelian}{\subseteq} \underset{M_1}{F(\zeta_{d_1})} \overset{abelian}{\subseteq} \underset{M_2}{F(\zeta_{d_1},\zeta_{d_2})} \overset{abelian}{\subseteq} \cdots \overset{abelian}{\subseteq} F(\zeta_{d_1},\zeta_{d_2},\zeta_{d_m}) = F'$$

$M_m$ $\cap\!|$ Kummer $\Rightarrow$ cyclic $\Downarrow$ abelian

$$M = \underset{M_r}{F'(\alpha_1,\ldots,\alpha_m)} \underset{ab}{\supseteq} \cdots \underset{ab}{\supseteq} F'(\alpha_1,\alpha_2) \underset{ab}{\supseteq} F'(\alpha_1)$$

Start →

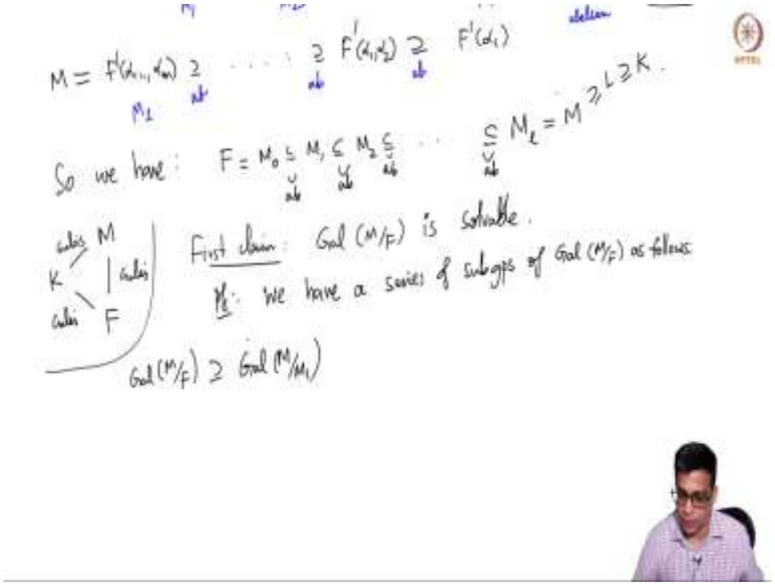
End ←

But, now we have a tower, now note that we have a tower; first you sort with F0 attached the roots of unity like so. So, have F of zeta d1, F of zeta d1, d2; you do all of them one by one. And now you do with this is what we called F prime, so this is F prime. And now do F prime alpha1, F1 is 0 alpha1; so I will do F prime alpha 1, F prime alpha 1, alpha 2. And all the way up to F prime alpha 1 through alpha m, and that is exactly equal to M. Because, M is the composite of F prime and L, this is by definition of composite; or rather by an easy observation about composite of fields, which I mentioned before; so you adjoint all of them.

But, now let us look at this, this this tower looks like this; I have written it like this, just to save space. So, so you start with here and end here; so now let us look at this. This is abelian because it is an cyclotomic extension; so we know that the Galois group is contained in Z naught d1 star, so this is abelian. So, this is recall from our cyclotomic extensions part, these are all abelian. But, now this is radical plus the bottom base will contains roots of this; so this is Kummer. Base will contains the required root of unity and its radical extension.

So, this this Kummer implies cyclic and, which implies abelian. This is also abelian, because it is Kummer which implies cyclic which implies abelian. So, this is abelian, this is abelian. So, thereby we got our result; so you have a tower of fields, so we called this M0, M1. This is M1, this is M2, this is I do not care Mm and so on, so all the way to Mr. So, we have a tower where each successive extension is abelian and the full extension is Galois. Now, continuing with the proof and what is our situation?

(Refer Slide Time: 15:58)



$M = F'(\alpha_1, \dots, \alpha_m) \underset{ab}{\supseteq} \cdots \underset{ab}{\supseteq} F'(\alpha_1, \alpha_2) \underset{ab}{\supseteq} F'(\alpha_1)$ abelian

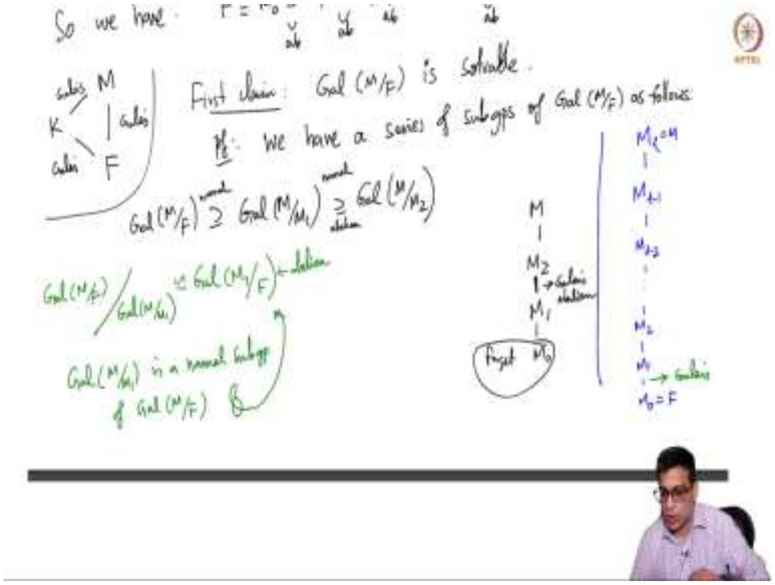
$M_1$

So we have: $F = M_0 \underset{ab}{\subseteq} M_1 \underset{ab}{\subseteq} M_2 \underset{ab}{\subseteq} \cdots \underset{ab}{\subseteq} M_\ell = M \supseteq L \supseteq K$.

First claim: $Gal(M/F)$ is solvable.

Pf: We have a series of subgps of $Gal(M/F)$ as follows

$Gal(M/F) \supseteq Gal(M/M_1)$



So we have:

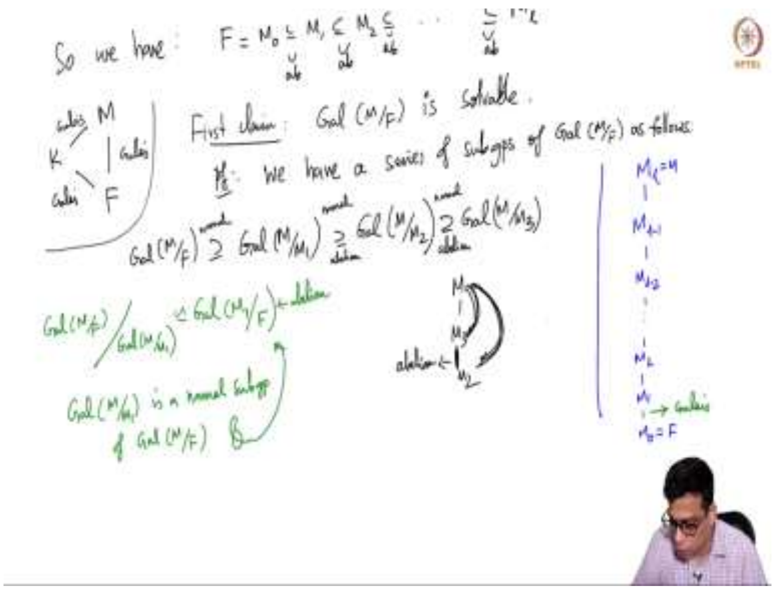
First claim: $Gal(M/F)$ is solvable.

Pf: We have a series of subgps of $Gal(M/F)$ as follows

$Gal(M/F) \overset{normal}{\supseteq} Gal(M/M_1) \underset{abelian}{\overset{normal}{\supseteq}} Gal(M/M_2)$

$Gal(M/F) / Gal(M/M_1) \cong Gal(M_1/F)$ ← abelian

$Gal(M/M_1)$ is a normal subgp of $Gal(M/F)$ &


So we have: F = M0 ⊆ M1 ⊆ M2 ⊆ ... ⊆ Ml
ab ab ab ab
Galois M
K Galois
abelian F
First claim: Gal (M/F) is solvable.
Pf: we have a series of subgps of Gal (M/F) as follows:
Gal (M/F) ⊵ Gal (M/M1) ⊵ Gal (M/M2) ⊵ Gal (M/M3)
normal normal normal
abelian abelian
Gal (M/F) / Gal (M/M1) ≅ Gal (M1/F) ← abelian
Gal (M/M1) is a normal subgp of Gal (M/F)
M3
M2
abelian
Ml=M
Ml-1
Ml-2
M2
M1 → Galois
M0 = F

So, our situation is the following. So, we have F which is equal to M0 contained in M1 contained in M2 contained in Mr; or I called it Ml which is M, where each of them is abelian. And remember, M contains L which contains K. So, what we have is forget L, M is an intermediate field of this. So, maybe rewriting this, what we have is just putting the extensions like this; so this is Galois, this is Galois of course and this is also Galois.

Now, I want to find first claim that Galois M over F is solvable, why is this? So, the proof of this claim. So, Galois L M over F is solvable; this is because we have a series. See, it is an easy observation which came up in the first part of the proof, in one of the directions of the proof. If you have a suitable tower of abelian extensions, by applying the main theorem we get the required series of a subgroups. We have a series of subgroups of Galois M over f as follows; so let me write down what that is.

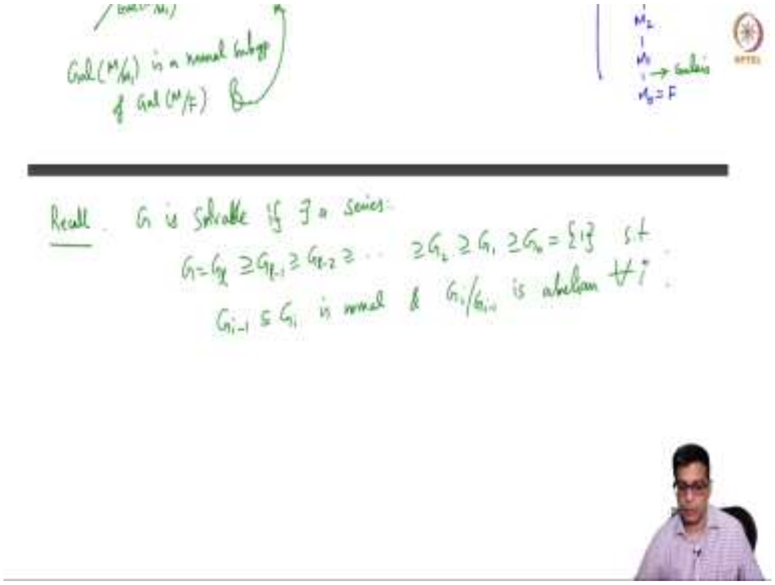
So, we have Galois L over F or m over F contained in; see this whole thing I am taking the Galois group. If you just take the Galois group of M over M1; this is a subgroup. So, maybe it is better for me to separately write this; so we have this here. So, we have M Ml, so it is M, Ml minus 1, Ml minus 2, M3 or M2, M1, M0 which is F. So, this whole thing is Galois M over F. but, if I just take this; that is of course a subgroup of the whole thing.

And moreover what is the kernel? What is the quotient of this? Because this is Galois, this is Galois remember; in fact this is abelian. So, the quotient of this Galois M over F quotient it with Galois M over M1, is by the main theorem isomorphic to Galois M over M1 over M0, which is

F. The Galois group of the whole thing modulo Galois group; forget all the other intermediate fields. You have M, M1, M0; Galois group of this mod Galois group of this is Galois group of this.

Because this is Galois, Galois this is a normal subgroup; so that should be first actually. So, Galois M over M1 is a normal subgroup of Galois M over F; and we have this, the quotient is this, but this is abelian. So, what now I am saying is that the tower that (())(20:16).

(Refer Slide Time: 20:18)



$\mathrm{Gal}(M/M_1)$ is a normal subgp of $\mathrm{Gal}(M/F)$

$M_2$ <br> $M_1$ → Galois <br> $M_0 = F$

Recall. $G$ is solvable if $\exists$ a series:

$G = G_\ell \geq G_{\ell-1} \geq G_{\ell-2} \geq \cdots \geq G_2 \geq G_1 \geq G_0 = \{1\}$ s.t

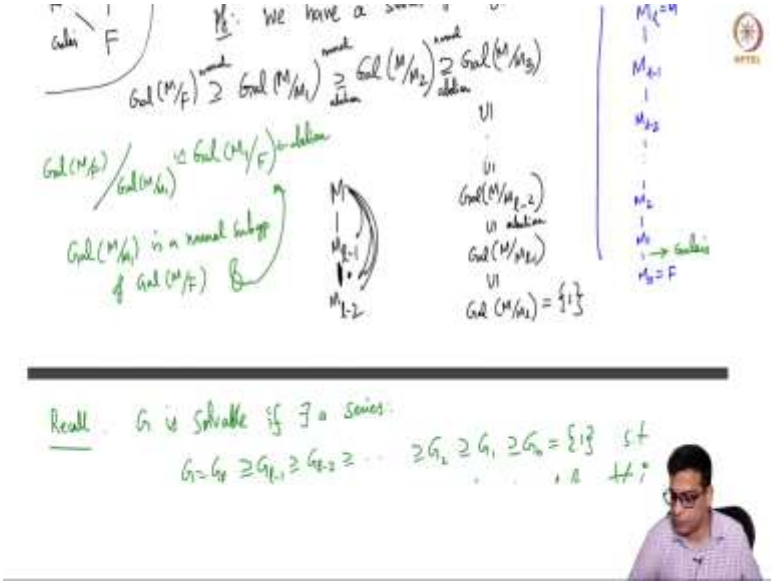
$G_{i-1} \leq G_i$ is normal & $G_i/G_{i-1}$ is abelian $\forall i$.

So, I should remember recall the definition of G solvable, if there exists a series like this; so, G equal to Gr contained in Gr minus 1. So, let me call it l here which is contained in Gl minus 2, contained in G2, contained in G1 contained in G0; which is the identity, such that Gi minus 1 is normal and is normal in Gi; and Gi mod Gi minus 1 is abelian. This is the definition of a solvable group; I want to show that Galois M over F is solvable. And I have just started with constructing the first subgroup; this is normal and quotient is abelian, so far so good; so, I have done the first step.

Now, I will do Galois, next one I will do Galois M over M2. So, now I am only interesting in M over M2, which contains M1; so forget M, forget this part M0, forget M0. I look at this Galois M over M1; sorry first of all this is Galois. And the corresponding group subgroup for this intermediate field is Galois M over M2, which is a subgroup of Galois M over M1. And because this is Galois this is normal, and this is normal as I noted earlier. And this quotient is this, this is in fact abelian also that is the whole point of constructing this; so, we have abelian at every stage. This Galois and the Galois group is abelian; so, the quotient is abelian here.

So, I have done the one more step; I hope this is clear. I probably doing more than what I heard, but you see now what I will do. I will do Galois M over M3; so M over M3 over M2. This Galois group is contained in this Galois group; so this contained in this, but this is abelian. That means Galois and Galois group is normal, Galois group is abelian; so this is normal subgroup by the main theorem. Not only that the quotient is abelian, because quotient is a Galois group of this extension. So, I have next step in this.

(Refer Slide Time: 22:58)



Pf: We have a

$Gal(M/F) \overset{normal}{\supseteq} Gal(M/M_1) \underset{abelian}{\overset{normal}{\supseteq}} Gal(M/M_2) \underset{abelian}{\overset{normal}{\supseteq}} Gal(M/M_3)$

$\supseteq \cdots \supseteq Gal(M/M_{l-2}) \underset{abelian}{\supseteq} Gal(M/M_{l-1}) \supseteq Gal(M/M_l) = \{1\}$

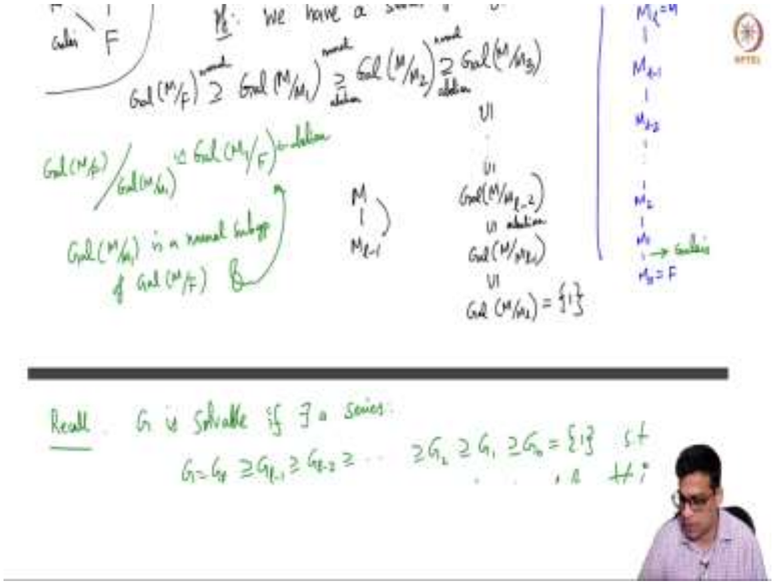
$Gal(M/F) / Gal(M/M_1) \cong Gal(M_1/F)$ ← abelian

$Gal(M/M_1)$ is a normal subgp of $Gal(M/F)$

$M_l = M$, $M_{l-1}$, $M_{l-2}$, ⋮, $M_2$, $M_1$ → Galois, $M_0 = F$

Recall: G is solvable if ∃ a series:

$G = G_l \supseteq G_{l-1} \supseteq G_{l-2} \supseteq \cdots \supseteq G_2 \supseteq G_1 \supseteq G_0 = \{1\}$ s.t. $\forall i$;



Galois F

Pf: We have a ...

$Gal(M/F) \overset{normal}{\geq} Gal(M/M_1) \underset{abelian}{\overset{normal}{\geq}} Gal(M/M_2) \underset{abelian}{\overset{normal}{\geq}} Gal(M/M_3)$

VI ⋮ VI

$Gal(M/M_{\ell-2})$

VI abelian

$Gal(M/M_{\ell-1})$

VI

$Gal(M/M_\ell) = \{1\}$

$Gal(M/F) / Gal(M/M_1) \cong Gal(M_1/F)$ ← abelian

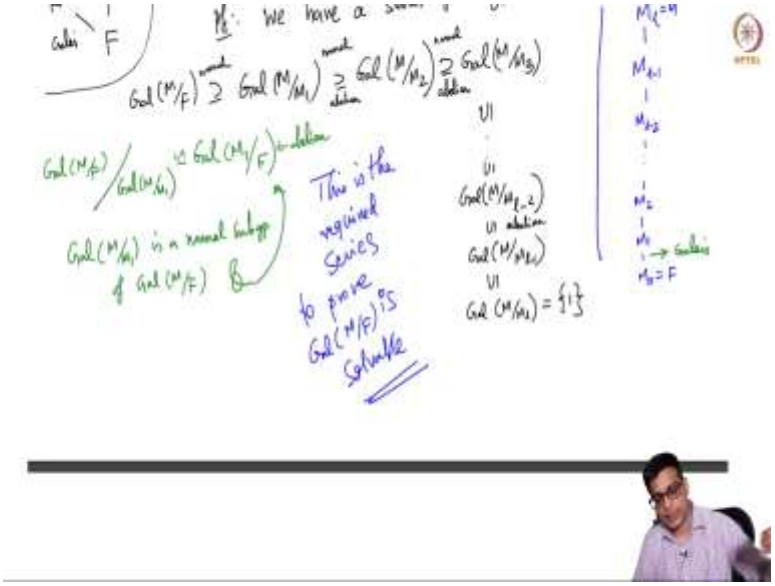
$Gal(M/M_1)$ is a normal subgp of $Gal(M/F)$ B

$M$ | $M_{\ell-1}$

$M_\ell = M$ | $M_{\ell-1}$ | $M_{\ell-2}$ ⋮ $M_2$ | $M_1$ → Galois | $M_0 = F$

Recall. G is solvable if ∃ a series:

$G = G_\ell \geq G_{\ell-1} \geq G_{\ell-2} \geq \cdots \geq G_2 \geq G_1 \geq G_0 = \{1\}$ s.t. ... ∀i



Galois F

Pf: We have a ...

$Gal(M/F) \overset{normal}{\geq} Gal(M/M_1) \underset{abelian}{\overset{normal}{\geq}} Gal(M/M_2) \underset{abelian}{\overset{normal}{\geq}} Gal(M/M_3)$

VI ⋮ VI

$Gal(M/M_{\ell-2})$

VI abelian

$Gal(M/M_{\ell-1})$

VI

$Gal(M/M_\ell) = \{1\}$

$Gal(M/F) / Gal(M/M_1) \cong Gal(M_1/F)$ ← abelian

$Gal(M/M_1)$ is a normal subgp of $Gal(M/F)$ B

This is the required series to prove $Gal(M/F)$ is solvable

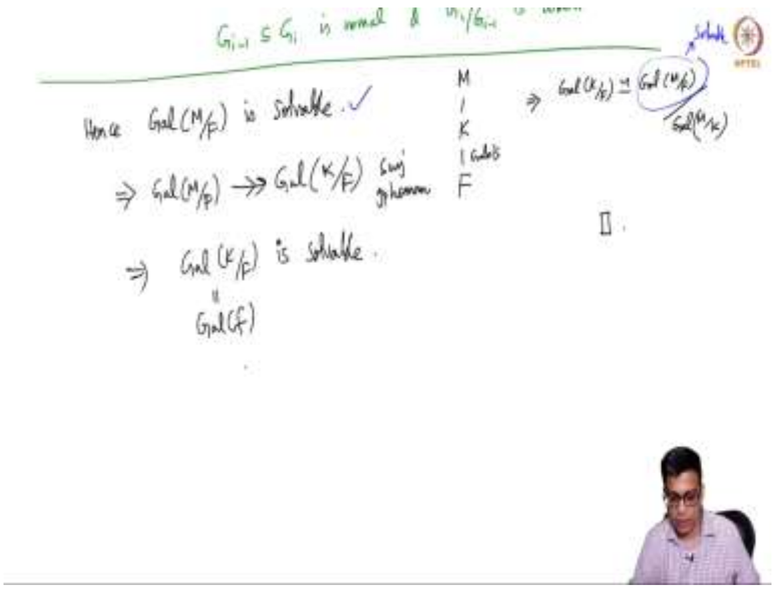
$M_\ell = M$ | $M_{\ell-1}$ | $M_{\ell-2}$ ⋮ $M_2$ | $M_1$ → Galois | $M_0 = F$

And then I continue like this all the way up to Galois M over Ml minus 1; so the last but one step. So, Ml minus 1 is normal subgroup of this which is a previous step; so maybe I will write this. This is here and that is normal in this; because this is an abelian, this is a Galois extension. Not only is it a Galois extension, it is a Galois extension with Galois group abelian; that means this quotient is abelian, normal and quotient is abelian. And finally you will do Galois M over Ml which is of course trivial.

So, if you do M over M minus 1, this is abelian extension; so Galois group is abelian of this extension. So, this quotient it by this is just this; it is abelian. So, this is the required series to prove Galois M over F is solvable. So, the definition is here. We have started with Galois M over

F and we have constructed is series of normal subgroups, with successive quotients abelian. And the whole point is we have done this because we had the right kind of field extensions; we have right end of tower of field extensions.

(Refer Slide Time: 24:54)



$G_{i+1} \leq G_i$ is normal & $G_i/G_{i+1}$ is abelian

Hence $\mathrm{Gal}(M/F)$ is solvable. ✓

$\Rightarrow \mathrm{Gal}(M/F) \twoheadrightarrow \mathrm{Gal}(K/F)$ surj grp homom

$\Rightarrow \underset{\mathrm{Gal}(f)}{\overset{\mathrm{Gal}(K/F)}{\shortparallel}}$ is solvable.

$$\begin{tikzcd} M \arrow[d, dash] \\ K \arrow[d, dash, "\text{Galois}"] \\ F \end{tikzcd}$$

$\Rightarrow \mathrm{Gal}(K/F) \cong \mathrm{Gal}(M/F) / \mathrm{Gal}(M/K)$

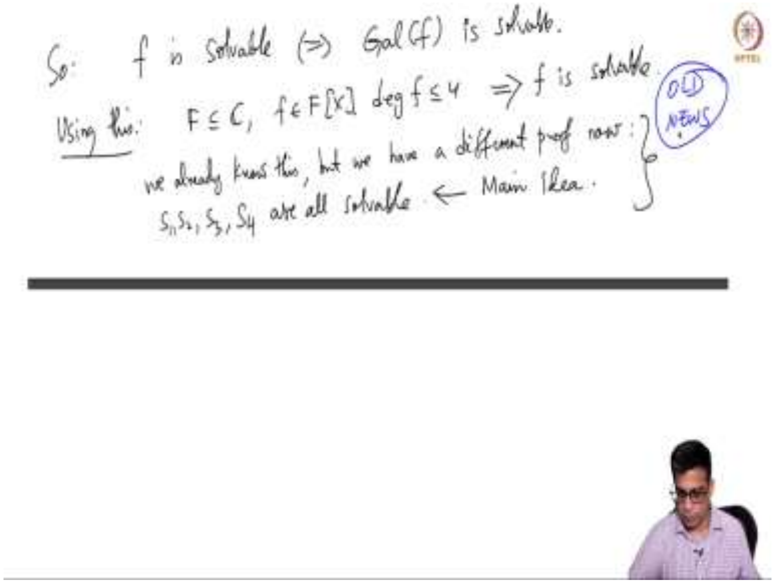
solvable

$\square$.

So, now we proved hence Galois M over F is solvable; remember this is not I want. I want Galois K over F is solvable; but we are there already. Now we get it because we have M contained in K contained in F; so this is Galois. So, this implies Galois K over F is isomorphic to Galois M over F quotiented by Galois M over K. Again the main theorem is used left right and center here; so this Galois group is a Galois group of this, modulo the Galois group of this. So, now this is solvable that is what I said here. This is Galois, so this is a normal subgroup of that solvable group; and we have already shown that image of a solvable group is solvable.

So, we have a surjective map of like this; so this an onto group of homomorphism, surjective group of homomorphism. So, this implies Galois K over F is solvable, so that is all; so we are done. So, we started with the statement that F is solvable and we concluded that the Galois group of f is solvable. Of course, this is Galois group of F; because K is a splitting field. So, Galois group of F by definition Galois group of K over F.

(Refer Slide Time: 26:44)



So: $f$ is solvable $\Leftrightarrow$ $Gal(f)$ is solvable.

Using this: $F \subseteq \mathbb{C}$, $f \in F[x]$ $\deg f \leq 4$ $\Rightarrow f$ is solvable.

OLD NEWS

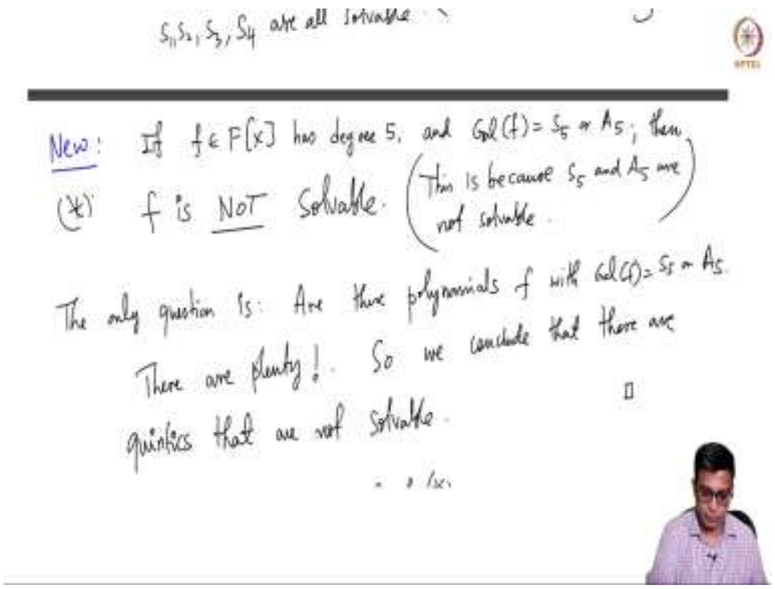
we already knew this, but we have a different proof now:

$S_1, S_2, S_3, S_4$ are all solvable $\leftarrow$ Main Idea.

So, we have shown that f is solvable implies if and only if Galois of f is solvable. So, now let me just take stock of the situation, because this is essentially proves the main result that I wanted to prove in this course. So, we can use this using this, in fact using the direction we already shown. If degree so F is inside C and small f is in capital FX; and degree of f is less than 4, implies f is solvable. This is old news; we have already proved this directly even without using this theorem. But, using this theorem we can get a different proof; we already know this, but we get a different proof; but we have a different proof.

What is the proof? The proof is that S4, S1, S2, S3, S4 are all solvable; this is the main idea. Because the Galois group of F polynomial of degree at most 4 is a subgroup of either S1, S2, S3, or S4; or you can just say it is a subgroup of S4. Because all of these are already subgroups of S4; and S4 is solvable. We have produced a series for S4 which shows the solvability of S4; so degree less than equal to 4 polynomials are solvable. But, this is old new, we have proved this.

(Refer Slide Time: 28:34)



$S_1, S_2, S_3, S_4$ are all solvable .

New: If $f \in F[x]$ has degree 5, and $Gal(f) = S_5$ or $A_5$, then

(*) f is NOT solvable. (This is because $S_5$ and $A_5$ are not solvable.)

The only question is: Are there polynomials f with $Gal(f) = S_5$ or $A_5$.

There are plenty! So we conclude that there are quintics that are not solvable. □

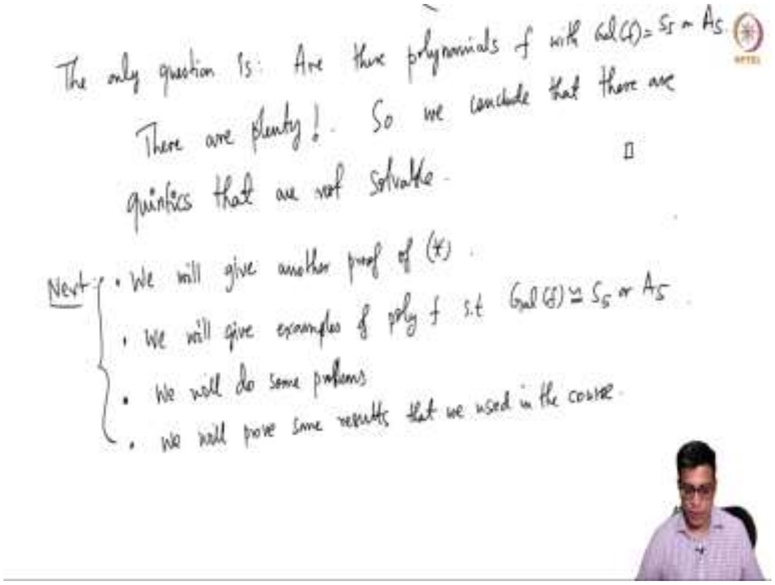
But, what is new? New is that If there exists a polynomial has degree 5, and Galois group of F is S5 or A5, then F is not solvable. This is new and for this direction we needed the, this statement we needed the direction we proved today. Because if Galois if F is solvable, then its Galois group would be solvable; but S5 and the A5 are not solvable. A5 is not solvable because it is normal and not a abelian; so a non-abelian a simple group A5 is simple, non-trivial and non-abelian. So, it cannot be solvable because if it is solvable, it must have a proper non-trivial normal subgroup, which it does not.

And once A5 is not solvable, S5 cannot be; because A5 is a subgroup of S5. So, because S5 and A5 are not solvable, any polynomial which has Galois group of S5 or A5 is not solvable. So, now the only question is are there polynomials f with Galois group f is S5 or A5? The answer is there are plenty. There are plenty as we will show later in the course; but this satis the issue of solving quintics by radicals. So, we conclude that there are quintics that are not solvable by radicals, or simply not solvable. Remember this is the first video of the course. I said Galois main achievement is proving that there are quintics, which are not solvable; and he gives specific examples.

And the way that he did this is more than what people before indeed, where they proved that in general you can have a general quintic is not solvable. But, that stops short of producing specific polynomials which are not solvable. In fact, it does not even tell you how to check if a given polynomial is solvable. Galois proved this theorem, so he sort of gave a very conceptual characterization of solvability. F solvable is the way people thought about this still that point was using some complicated roots and radicals as in quadratic formula or cardano's formulas.

But, Galois converted the whole problem into a very beautiful conceptual problem, about solvability of some groups. And in fact he showed this theorem, which showed that in principle you have a method to check any given polynomial is solvable or not. You simply computed Galois group and see if it is solvable or not. Checking that for groups is a more conceptual and easier problem; so we can do that, so we have done that. We have now finished this proof, we have given one proof.

(Refer Slide Time: 32:01)



The only question is: Are there polynomials f with $Gal(f) = S_5$ or $A_5$.

There are plenty! So we conclude that there are quintics that are not solvable. □

Next
- We will give another proof of (*).
- We will give examples of poly f s.t $Gal(f) \simeq S_5$ or $A_5$.
- We will do some problems
- We will prove some results that we used in the course.

So, the next we are almost at the end of the course; next will give you a different proof. Remember I wanted to give 2 proofs for every statement of about solvability. So, now I have given 2 statements for this, 2 proofs for this statement. We have directly proved that any polynomial of degree at most 4 is solvable; and now you have proved it using solvable groups. We have proved that a polynomial of degree 5 is Galois group S5 or A5 is not solvable. But, will give you another proof of this of star; and we will give examples of polynomials f such that Galois group of f is S5 or A5.

And after that we will do some problems, and will also cover some will prove some results that are not quiet in Galois Theory. But, if time permits that we used in the course; so I hope to do this last part also, like primitive element theorem. The fact that A5 is simple and so on so will come to this. So, this is the goal for the remaining classes of the course. So, let me stop this, so there is lot of stock in this class; please make sure that you go through the video again if needed. And understand this crucial thing; this is really the crux of the course.

We have proved that, we did not quiet proved that there are quintics that are not solvable. Because we need to produce polynomials with Galois group as S5 or A5; but that will do later. But, we have shown that if a polynomial has Galois group A5 or S5; it cannot be solve by radicals. Let me stop this video here and in the next classes we will address these topics. Thank you.