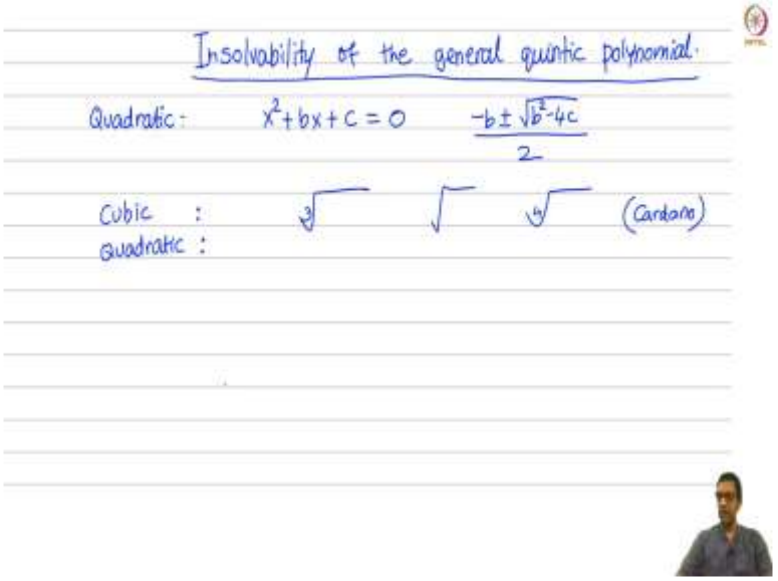
Algebra - II
Professor S Viswanath
Department of Mathematics
The Institute of Mathematical Science
Lecture 42
Insolvability of the General Quintic – Part I

(Refer Slide Time: 00:14)



Insolvability of the general quintic polynomial.

Quadratic: $x^2+bx+c=0$ $\quad \frac{-b\pm\sqrt{b^2-4c}}{2}$

Cubic : $\sqrt[3]{\ }$ $\quad \sqrt{\ }$ $\quad \sqrt[4]{\ }$ (Cardano)

Quadratic :

We are going to consider one of the historically, you know how Galois Theory really arose, which is from the efforts to solve polynomial equations for their roots. So for example, recall if you have a quadratic equation, then we have a formula for its roots, so x square, so let us assume it is monic, x square plus b x plus c equal to 0; the roots are given by minus b plus minus by 2.

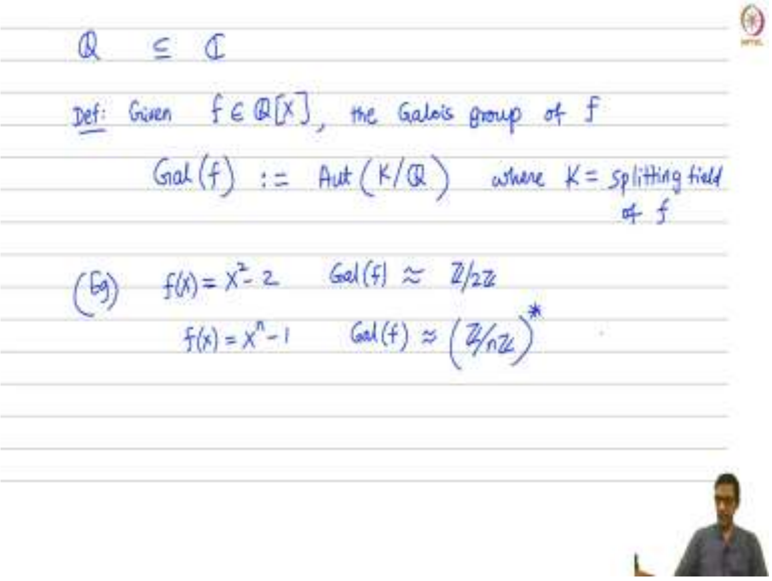
Now, similar formulas were known for both degree 3 and degree 4 equations and the formulas always involved you know, some closed form expression like this. So, maybe it was things like you know, something which involved cube roots or square roots or fourth roots and so on and often they were rather you know, complicated such expressions, but nevertheless, there was some closed form expression that people had managed to work out.

So, among the famous names associated to the cubic equation is Cardano. So, there is the Cardano solution to the cubic polynomial; so, degree 3 polynomial, degree 4 polynomial and of course, you know that brings the natural question up, which is can one do the same thing for all polynomials of all degrees?

And Galois sort of considered this problem as did some people before him but Galois theory really arose from his efforts to you know, understand the solvability of the roots for a general polynomial and it turns out that degree 5 polynomial, you know, a general one some of them can be solved but you can always find degree 5 polynomials whose roots cannot be expressed in such forms.

They can, you cannot find a formula for the roots. So what we are going to do over the course of the next few videos is to try and see how this is proved. Now, let me just define some of the notions that we will need.

(Refer Slide Time: 02:28)



$\mathbb{Q} \subseteq \mathbb{C}$

Def: Given $f \in \mathbb{Q}[X]$, the Galois group of f

$\mathrm{Gal}(f) := \mathrm{Aut}(K/\mathbb{Q})$ where $K =$ splitting field of f

(Eg) $f(x) = x^2 - 2$ $\mathrm{Gal}(f) \approx \mathbb{Z}/2\mathbb{Z}$

$f(x) = x^n - 1$ $\mathrm{Gal}(f) \approx (\mathbb{Z}/n\mathbb{Z})^*$

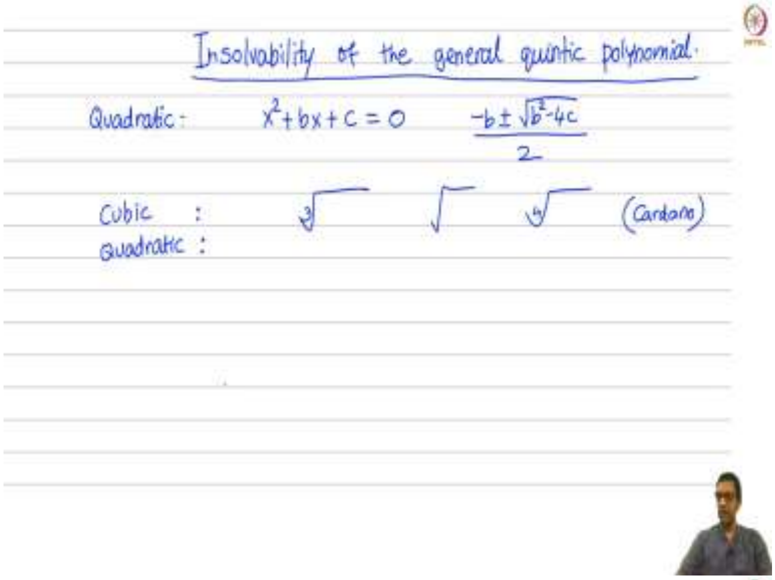
Now, given a polynomial; so here, now we are going to always look at the base field Q and we will, so we know that given any polynomial with coefficients in Q, it definitely has roots in the complex numbers. So we will sort of keep looking at Q and C throughout. I am not going to look at any other fields really.

Now, definition given a polynomial, given polynomial f, with coefficients in Q, we say that the Galois group of f, so this is the definition, the Galois group of f and I will give it a name, Gal of F is the following. It is just the Galois group or the group of auto morphisms of K over Q, where k is a splitting field of f.

So look at the splitting field because it is a splitting field, it is normal. Q is of characteristic 0. So this is separable and so it is a Galois extension. So you have got this Galois group, the group of auto morphisms and we call that the Galois group of f. So, for example, if so we have seen many such examples before, if it is a quadratic x square minus 2, then the Galois group of this polynomial has cardinality 2.

So it is just isomorphic to the cyclic group, if I have x to the n minus 1, then the splitting field is the cyclotomic field of the nth roots of unity and we have seen that the Galois group of the cyclotomic extension is the value you take the rings at mod n Z and you look at the units in that ring, the elements which have multiplicative inverses and we have seen, so this cardinalities phi of n and so on; Euler's totient function.

(Refer Slide Time: 04:38)

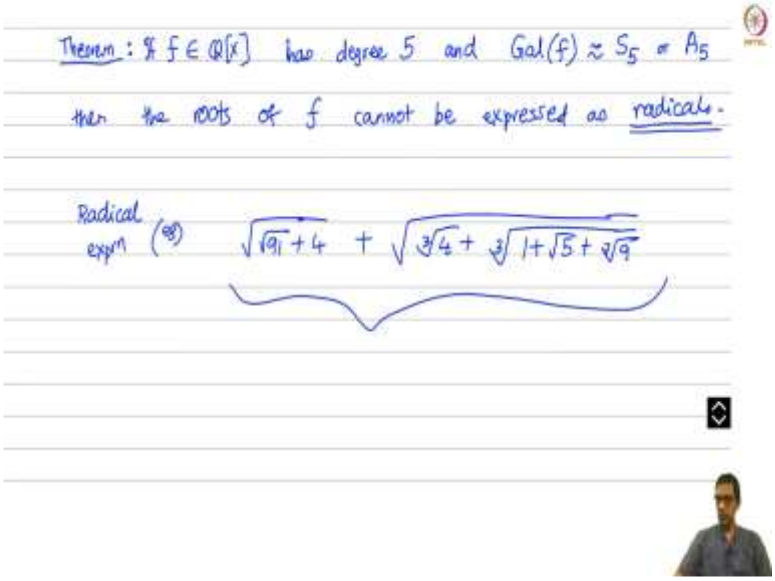


Insolvability of the general quintic polynomial.

Quadratic: $x^2+bx+c=0$ $\quad \frac{-b\pm\sqrt{b^2-4c}}{2}$

Cubic : $\sqrt[3]{}$ $\sqrt{}$ $\sqrt[4]{}$ (Cardano)

Quadratic :



Theorem: If $f \in \mathbb{Q}[x]$ has degree 5 and $Gal(f) \approx S_5$ or A_5 then the roots of f cannot be expressed as radicals.

Radical exp^n (eg) $\underbrace{\sqrt{\sqrt{91}+4} + \sqrt{\sqrt[3]{4}+\sqrt[3]{1+\sqrt{5}+\sqrt[4]{9}}}}$

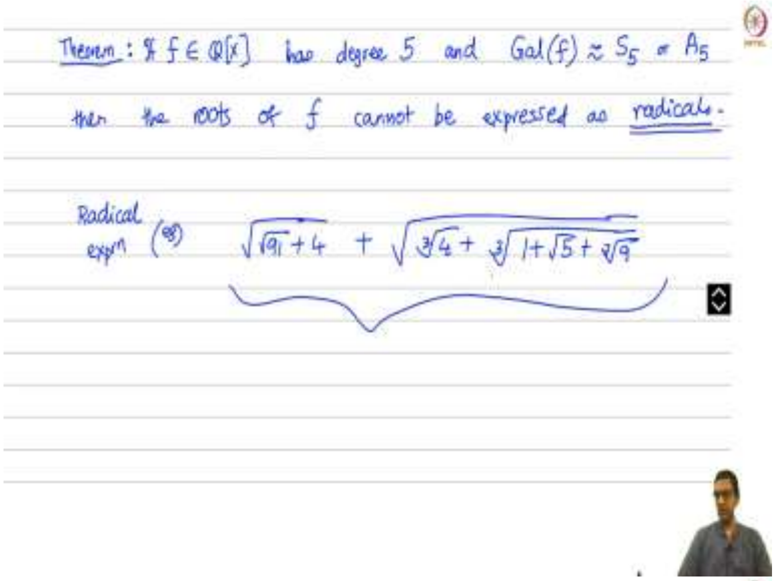
And so here is the eventual theorem that we are going to go towards, let me state it upfront and there are many intermediate steps which we will take up one by one. So given a polynomial with coefficients in Q has degree 5 and if it is Galois group is isomorphic to either the symmetric group is 5 or the alternating group a 5, remember that is the set of even permutations, then the roots of f cannot be expressed as radicals.

So, the key word here is radicals, we sort of know what that means in the quadratic and cubic cases. Radicals are things like this taking some nth roots of other expressions. So, what does an example of you know, what is the radical expression? So, here is a radical expression in terms of radicals.

I will give you an example. So, let us do something complicated I can take square root of square root 91 plus 4 something like that maybe plus square root of cube root of 4 plus cube root of maybe the seventh root of 9 and so on. So, you can you can imagine what I mean. So, I can have many layers of nesting; meaning I can take the square root of the cube root of some expression and so on and so forth.

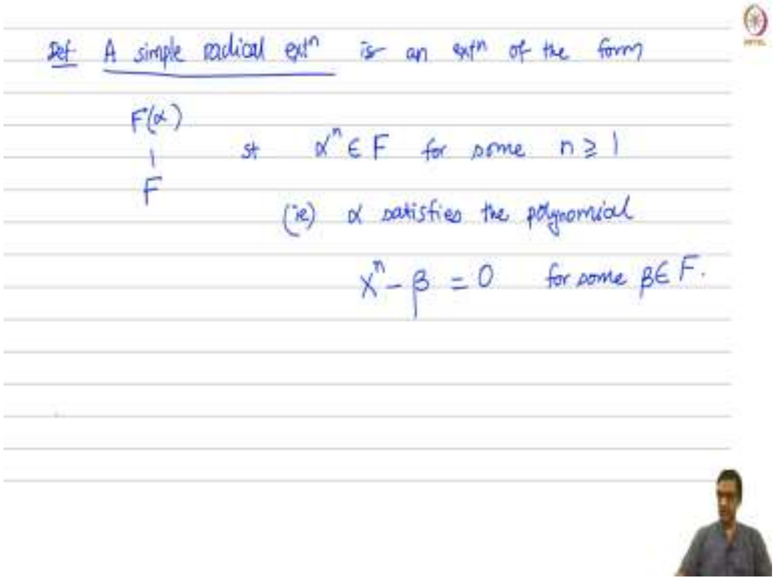
So, any such thing is what we would like to mean by a radical expression or an expression in terms of radicals. So, what this theorem says is that you cannot get a formula for the roots in in you know of this form, which we are able to do for quadratic, cubic and the quartic equations. So, sorry I called them quadratic again, this is what is called quadratic degree 4.

(Refer Slide Time: 06:56)



Theorem: If $f \in \mathbb{Q}[x]$ has degree 5 and $Gal(f) \approx S_5$ or A_5 then the roots of f cannot be expressed as radicals.

Radical exp^n (eg) $\underbrace{\sqrt{\sqrt{91}+4} + \sqrt{\sqrt[3]{4} + \sqrt[3]{1+\sqrt{5}+\sqrt[3]{9}}}}$



Def A simple radical ext^n is an ext^n of the form

$$\begin{tikzcd} F(\alpha) \arrow[d, dash] \\ F \end{tikzcd}$$

st $\alpha^n \in F$ for some $n \geq 1$

(ie) α satisfies the polynomial

$x^n - \beta = 0$ for some $\beta \in F$.

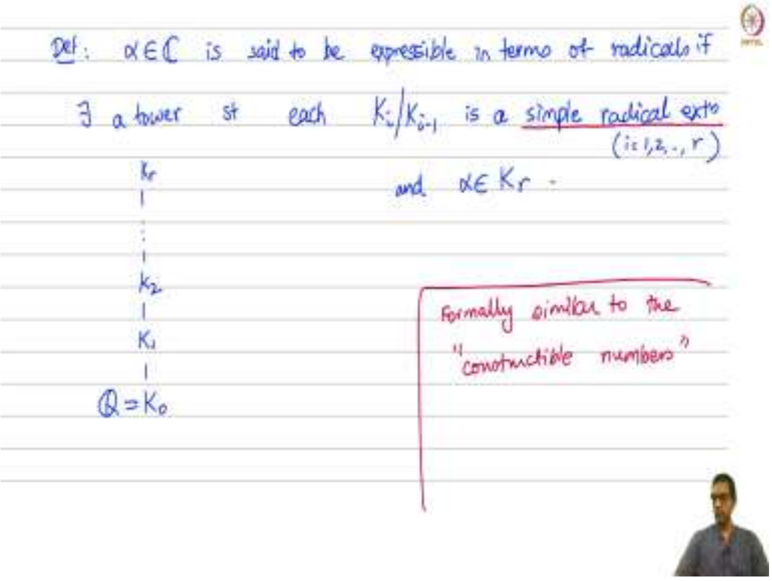
Now, let us see what how to formalize this a little bit better. So definition; what does it mean to take radicals? So simple radical extension; so I am going to define what is meant by a simple radical extension; is an extension of the following form, is an extension of the form, I have some base field and I have an extension F which is obtained by adjoining just a single element alpha to the base field such that what properties is alpha?

Some power of alpha belongs to the field, so for some n greater than equal to 1. In other words, i e alpha satisfies the polynomial, what will it satisfy? x to the n minus beta equal to 0 for some beta which belongs to the base field. So, it is another way of saying you take some element of the base field and you adjoin some nth root of that element.

So that is like what we are doing in in these examples. So, we sort of take some element of your base field. So maybe this is your element of the base field and then you are trying to take the cube root of that element. Of course, this element of the base field itself is obtained as you know, you first take root 5 you adjoin root square root of 5 to the rational numbers.

You get some field now, to that field you adjoin another element the seventh root of 9 and you get another further element and so on. So there are, we are not just doing you know, radicals in one step. So, this is what we have defined so far is what it means to just do a one-step radical. More generally, we have a definition.

(Refer Slide Time: 09:03)



Def: $\alpha \in \mathbb{C}$ is said to be expressible in terms of radicals if $\exists$ a tower st each K_i/K_{i-1} is a simple radical extn $(i=1,2,..,r)$ and $\alpha \in K_r$.

$$\begin{tikzcd}
K_r \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
K_2 \arrow[d, dash] \\
K_1 \arrow[d, dash] \\
\mathbb{Q}=K_0
\end{tikzcd}$$

Formally similar to the "constructible numbers"

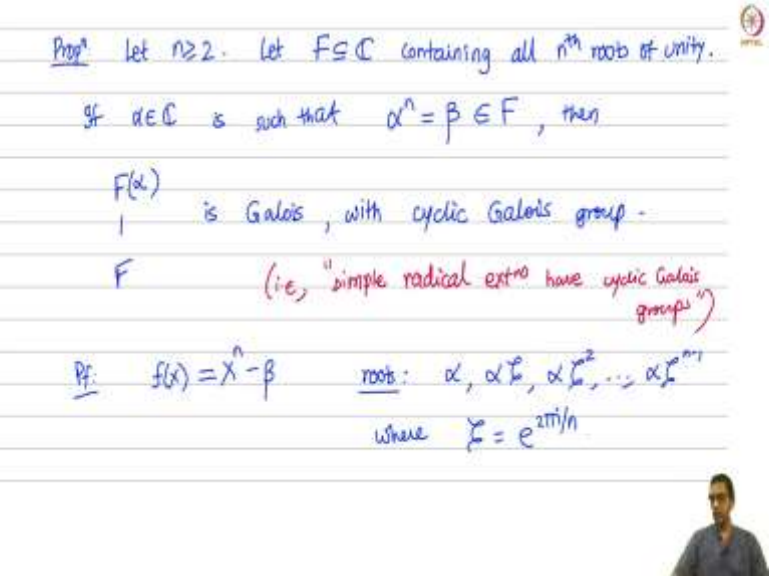
So, an element alpha in C, a complex number is said to be expressible in terms of radicals, you say it is expressible in terms of radicals, if there exists a tower of simple radical extensions. So, there should be a tower of the following kind that I start with the rational numbers.

We will call that K naught; there should be K 1, K 2 such a tower, such that each K i over K i minus 1 is a simple radical extension and alpha is in the topmost guy, alpha belongs to K r. So, when you say each of this I mean for i equals 1 to r. So, this is the formal way of encapsulating the idea that you keep doing multiple nth roots, you to keep taking multiple nth roots and observe just a quick aside that this is very, very reminiscent of what we have seen already in for constructible elements.

So, this is formally similar to the definition of constructible elements, to the what we call constructible numbers. There we said we had to start with Q and keep doing you know quadratic extensions and a real number there was said to be constructible if it can be realized as part of the topmost extension in a tower where, you know each successive thing is quadratic.

Now, here we do not demand it is quadratic instead we say it each of them should be a radical extension. It should be obtained by adjoining some nth root, may not be a square root. So, recall quadratic extensions are always realizable as adjoining the square root of some element from the base field in the sense that this is a generalization you can adjoin any nth root.

(Refer Slide Time: 11:27)



Prop^n Let $n \geq 2$. Let $F \subseteq \mathbb{C}$ containing all n^{th} roots of unity.

If $\alpha \in \mathbb{C}$ is such that $\alpha^n = \beta \in F$, then

$$\begin{tikzcd} F(\alpha) \arrow[d, dash] \\ F \end{tikzcd}$$

is Galois, with cyclic Galois group.

(i.e, "simple radical ext^ns have cyclic Galois groups")

Pf: $f(x) = x^n - \beta$ roots: $\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}$

where $\zeta = e^{2\pi i/n}$

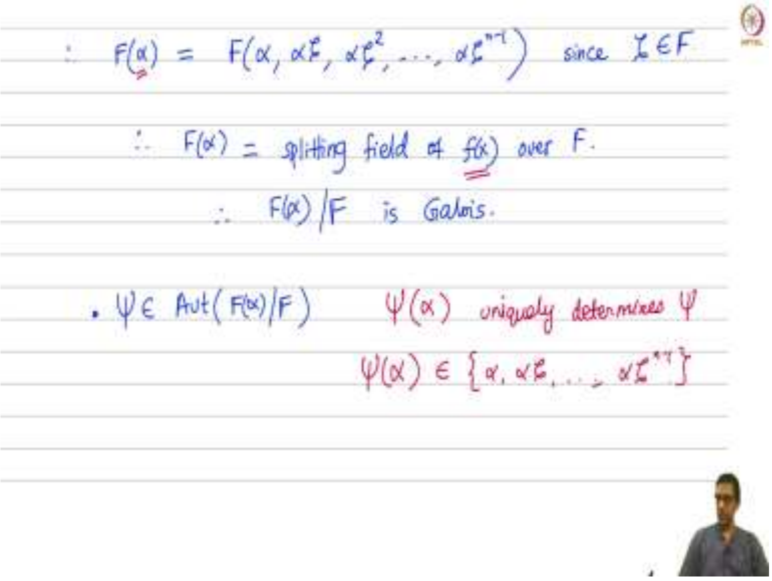
Good. Now, what is the key thing, key fact that one needs to know about this? So that is the following proposition. So, let n be at least 2, I mean adjoining the n equals 1th root of an element does not mean, does not give you anything new. Now, let F be a subfield of C containing all nth roots of unity, containing all nth roots of unity.

So, e to the 2 pi i by n and its square cube and so on. Now, if alpha in C is such that it is nth power belongs to F then the extension, so I have F and I adjoin alpha to it. The claim is that this extension is actually Galois, further with cyclic Galois group. So this is the key proposition. So, observe this is a simple radical extension.

So, what this means, in other words, i e simple radical extensions, i e, simple radical extensions and I am only talking about subfields of C here. So simple radical extensions have cyclic, are Galois and have cyclic Galois groups. So have Galois. That is just a quick way of remembering what this says. So let us prove this. So first, let us show that this is actually a Galois extension. Proof: so what are we doing here?

To show that F alpha over F is Galois, we need to show that this splitting field for example of a collection of polynomials. So here, it is very easy to see what polynomial we are talking about. Let us just take the polynomial x to the n minus beta. Observe that so, what are the roots of this equation? So the roots of this polynomial, one root we know is alpha itself but then the other roots are just alpha multiplied by the various nth roots of unity, alpha zeta to the n minus 1 where zeta is just this nth root of unity.

(Refer Slide Time: 14:07)



$\therefore\ F(\underset{\approx}{\alpha}) = F(\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1})$ since $\zeta \in F$

$\therefore\ F(\alpha) =$ splitting field of $\underline{\underline{f(x)}}$ over F.

$\therefore\ F(\alpha)/F$ is Galois.

- $\psi \in \mathrm{Aut}(F(\alpha)/F)$ $\psi(\alpha)$ uniquely determines ψ

$\psi(\alpha) \in \{\alpha, \alpha\zeta, \ldots, \alpha\zeta^{n-1}\}$

So, these are the roots but observe, we made an assumption that F, the base field already contains zeta, zeta square zeta cube and so on. So therefore, observe that if you take F and I just adjoin F alpha to it, so maybe I should say this first. If I take F and I adjoin alpha to it, that is the same as adjoining alpha zeta, alpha zeta square and all the other roots as well, because zeta is already in F, since, zeta and its powers are already in the base field by assumption.

So, adjoining just alpha will automatically give you all the nth roots, I mean all the n roots of that polynomial. So, what does that mean? That just tells you that F alpha is actually just a splitting field. Like this the definition splitting field should be the field generated by the roots of that polynomial over the base field.

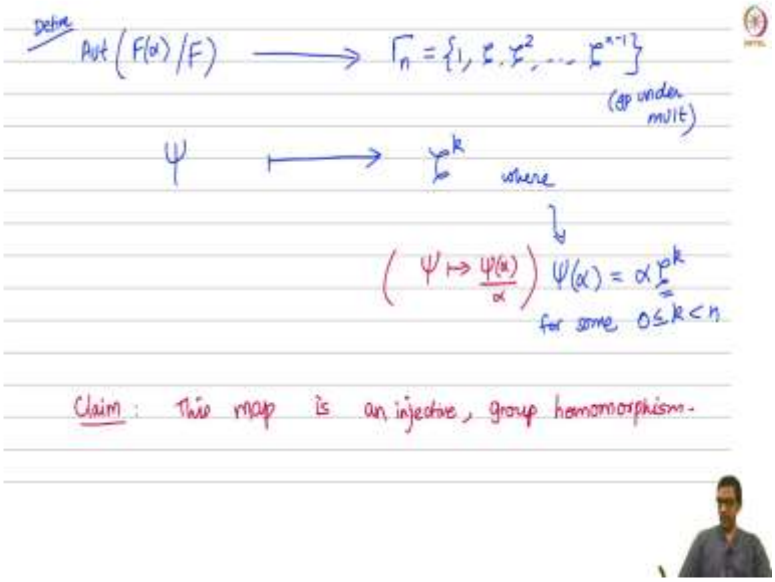
So this is a splitting field of this polynomial over the base field. Therefore it is Galois. Here characteristic is 0, so separability is not, it comes for free. It is normal therefore, Galois in this case. Good. Now, what about the Galois group? Where is the cyclicity of the Galois group going to come from?

So, recall, you know we have looked at this in the various examples and so on. What are the possible possibilities for an element of the Galois group? So, take an element now, sigma in the Galois group of this extension. So, as always you know it is, it is determined by what it does to this generator.

So if I know what psi does to alpha, so this uniquely determines if I specify this, this uniquely determines psi. You can work out what the images of the other elements are. Now, what can psi alpha be? Again, if you look back on our problems that we did, so what this says is that alpha can only be one of the roots of its minimal polynomial.

In particular, it I mean here, I do not quite know maybe what the minimal polynomial is, I do not know that this is irreducible. The polynomial I chose little effects, but whatever it is, since alpha is the root of F of x, psi alpha must also be root of F of x. So what are my possibilities? I already know what they are; so only one of these. So now point is, so let us just define a map.

(Refer Slide Time: 16:33)



Define $\mathrm{Aut}\left(F(\alpha)/F\right) \longrightarrow \Gamma_n = \{1, \zeta, \zeta^2, \dots \zeta^{n-1}\}$ (gp under mult)

$\psi \longmapsto \zeta^k$ where

$\left(\psi \mapsto \frac{\psi(\alpha)}{\alpha}\right)$ $\psi(\alpha) = \alpha\zeta^k$ for some $0 \le k < n$

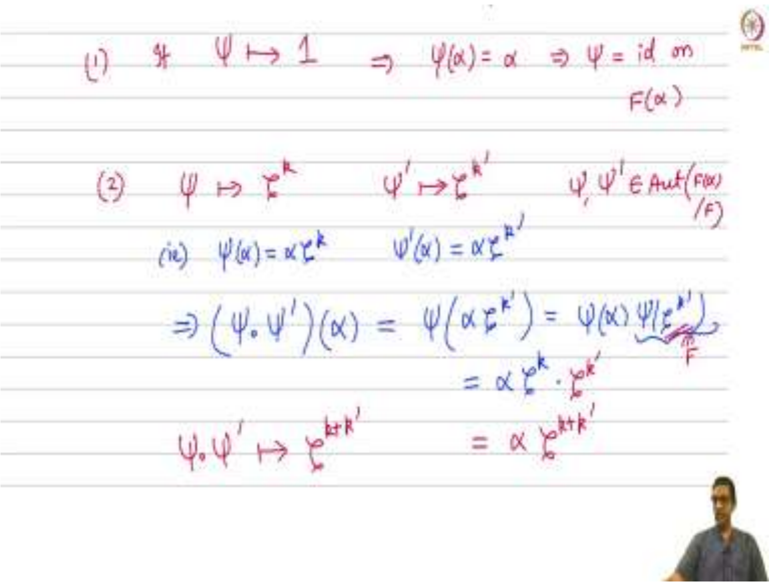
Claim: This map is an injective, group homomorphism.

Stick the map. So I am just going to take the nth roots of unity 1, zeta, zeta square, zeta to the n minus 1. So this is I am calling this gamma n, the nth roots of unity, this forms group under multiplication. So what we now do is? We will define a group homomorphism between these 2 groups. So this is a group under multiplication. What is the map?

Well, we just said take any psi, it is uniquely determined by what it does to alpha. So and what can psi do to alpha? Psi has to map alpha to an element of the form alpha into some power of zeta, it should look like alpha zeta power k for some k between 0 and n minus 1. So now, what you do is you just map it to that k. So psi will map to zeta power k, where what is k? k is that element such that psi alpha is alpha zeta power k.

This is the definition or if you if you wish to have something, you know which looks a little slicker; you just say psi maps to psi of alpha divided by alpha. That is really what this map is. Good. Now, we just have to check a few things. The claim is that this map is an injective group homomorphism. So claim: this map is an injective group homomorphism. So let us check the injectivity first.

(Refer Slide Time: 18:34)



(1) If $\psi \mapsto 1 \Rightarrow \psi(\alpha) = \alpha \Rightarrow \psi = id$ on $F(\alpha)$

(2) $\psi \mapsto \zeta^{k}$ $\quad \psi' \mapsto \zeta^{k'}$ $\quad \psi, \psi' \in Aut(F(\alpha)/F)$

(ie) $\psi(\alpha) = \alpha \zeta^{k}$ $\quad \psi'(\alpha) = \alpha \zeta^{k'}$

$$\Rightarrow (\psi \circ \psi')(\alpha) = \psi(\alpha \zeta^{k'}) = \psi(\alpha)\, \underbrace{\psi(\zeta^{k'})}_{\overset{\uparrow}{F}}$$

$$= \alpha \zeta^{k} \cdot \zeta^{k'}$$

$\psi \circ \psi' \mapsto \zeta^{k+k'}$ $$= \alpha \zeta^{k+k'}$$

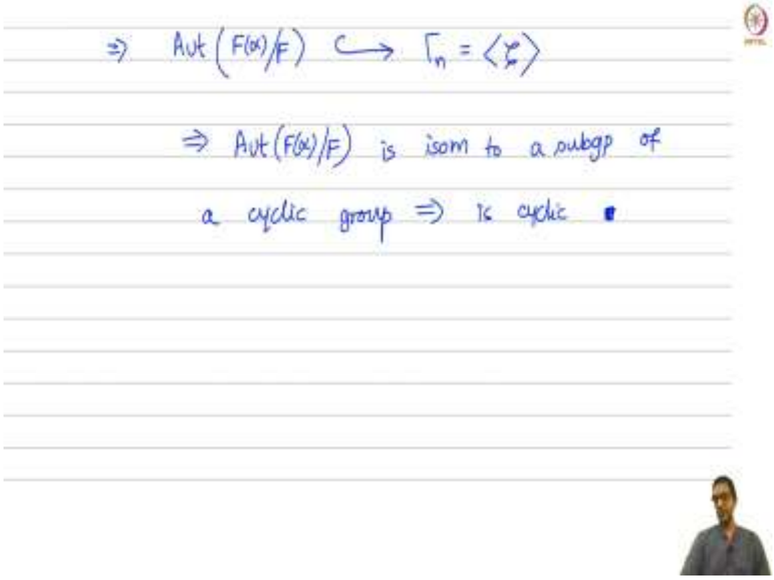
If something maps to the identity, so first, I will check injectivity; if psi maps alpha, so if psi maps to be the identity of the group gamma n, what does that mean? It means that psi of alpha is alpha. If psi maps to 1, it means that psi of alpha is alpha. Therefore, you know that automatically means that psi must just be the identity on the entire field F of alpha.

Because i is already identity on F and psi of alpha is also alpha, so psi must be identity. So that shows that this is an injective map definitely. But let us check that it is a group homomorphism. Now group homomorphism is, well suppose psi maps to zeta power k. I take another map psi prime which maps to zeta power k prime, psi n psi prime are elements of the Galois group, (())(19:53).

Then what can I conclude? So what does this mean? In other words, psi of alpha is alpha zeta power k, psi prime of alpha, so let us compute what the composition maps show, psi composition psi prime. Well, it is value on alpha by definition is, I first applied, psi prime. Psi prime is zeta power k prime, which is psi of alpha into psi of zeta power k prime.

Now, on the other hand, while I know something more; I know that psi of alpha is alpha times zeta power k and psi on zeta power k prime observe, zeta power k prime by definition, this this element here was assumed to be in the base field and psi acts as identity on the base field. So this just maps it back to itself. It does nothing to it. Psi of zeta power k prime, is it upper k prime? So the final answer therefore is alpha zeta power k plus k prime, which means that psi composition psi prime is going to be mapped to zeta power k plus k prime which means it is a group homomorphism because that is the group on the right hand side.

(Refer Slide Time: 21:24)



$\Rightarrow \mathrm{Aut}(F(\alpha)/F) \hookrightarrow \Gamma_n = \langle \zeta \rangle$

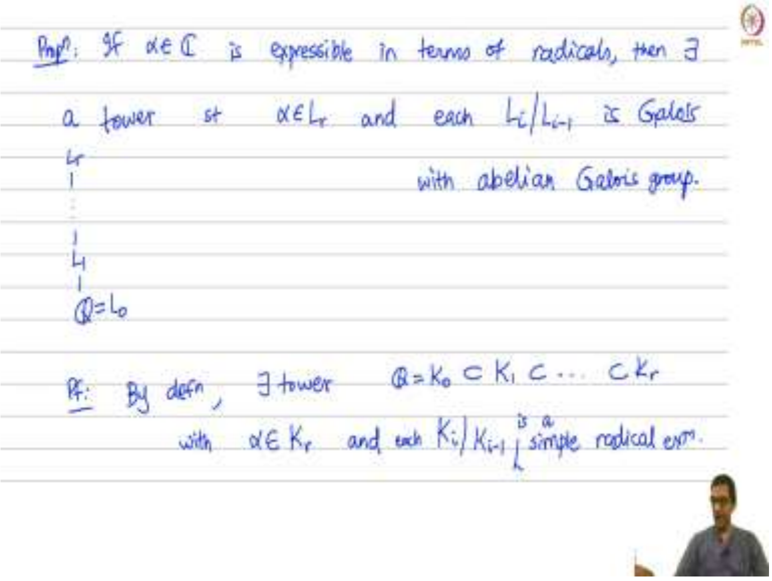
$\Rightarrow \mathrm{Aut}(F(\alpha)/F)$ is isom to a subgp of a cyclic group $\Rightarrow$ is cyclic ∎

So we managed to prove both parts that it is an injective group homomorphism, which means that, the Galois group is isomorphic. So the Galois group, see there is an injective map to an abelian group. So observe that gamma n, the multiplicative group of the roots of unity, it is after all an abelian group there.

And it is in fact cyclic. So, this is actually a cyclic group, this is cyclic generated by zeta, powers of zeta give you everything. So, this is a, this is really a subgroup of an abelian group, it is isomorphic to a subgroup, of a cyclic group. So therefore, this is also cyclic, therefore Aut of F alpha over F, you can think of it as it is isomorphic to a subgroup of a cyclic group.

And the only subgroups of cyclic groups are cyclic; therefore, it is already cyclic. So that is the end of the proof. So, what we managed to show is that simple radical extensions are necessarily Galois and have cyclic Galois groups and now the key thing about you know, a tower of extensions or about expressing numbers in terms of radicals.

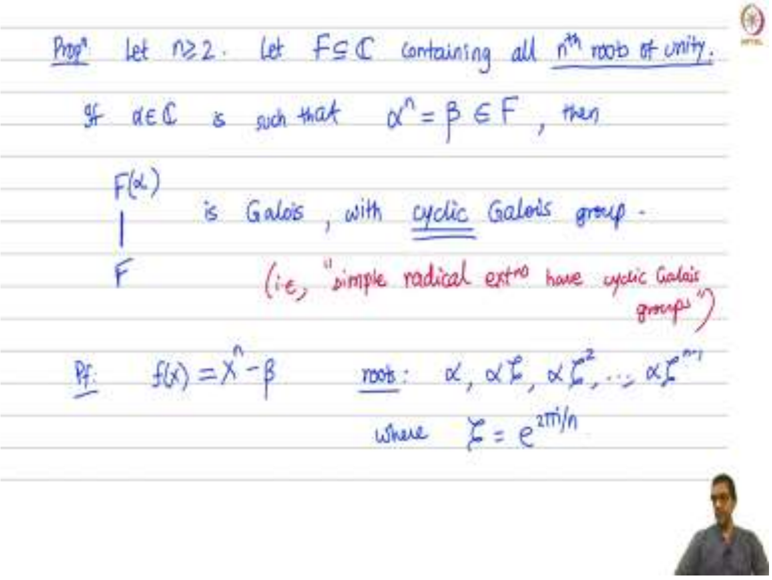
(Refer Slide Time: 22:46)



Prop^n: If $\alpha \in \mathbb{C}$ is expressible in terms of radicals, then $\exists$ a tower st $\alpha \in L_r$ and each L_i/L_{i-1} is Galois with abelian Galois group.

$$\begin{tikzcd} L_r \arrow[d, dash] \\ \vdots \arrow[d, dash] \\ L_1 \arrow[d, dash] \\ \mathbb{Q}=L_0 \end{tikzcd}$$

Pf: By defn, $\exists$ tower $\mathbb{Q}=K_0 \subset K_1 \subset \cdots \subset K_r$ with $\alpha \in K_r$ and each K_i/K_{i-1} is a simple radical ext^n.



Prop^n Let $n \geq 2$. Let $F \subseteq \mathbb{C}$ containing all n^{th} roots of unity. If $\alpha \in \mathbb{C}$ is such that $\alpha^n = \beta \in F$, then

$$\begin{tikzcd} F(\alpha) \arrow[d, dash] \\ F \end{tikzcd}$$

is Galois, with cyclic Galois group.

(i.e, "simple radical ext^{ns} have cyclic Galois groups")

Pf: $f(x) = x^n - \beta$ roots: $\alpha, \alpha\zeta, \alpha\zeta^2, \dots, \alpha\zeta^{n-1}$ where $\zeta = e^{2\pi i/n}$

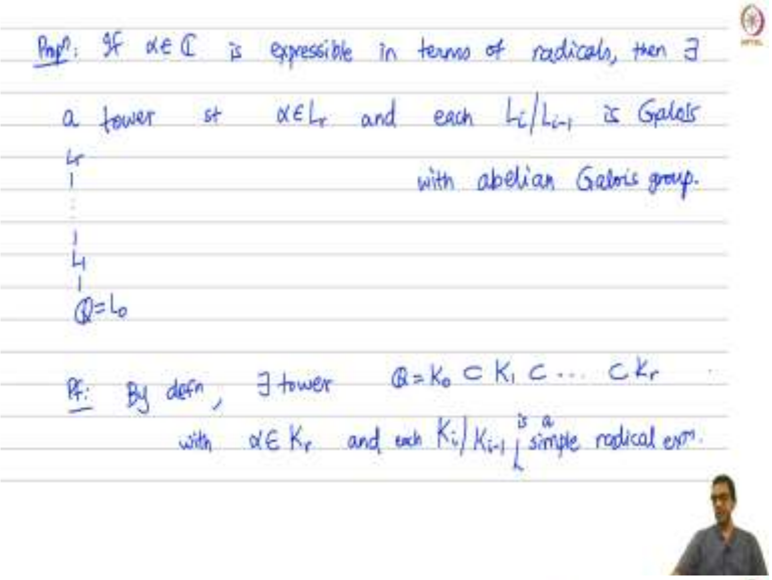
So, here is the proposition; if you can express alpha, if an element alpha is expressible in terms of radicals, then what it means is that then there exists, the proposition says, there exists at tower as follows: Q, it is called Q is L 0, L 1, L 2, L r such that alpha belongs to the last fellow Lr and each L i by L i minus 1 is Galois with an abelian Galois group.

So, you might wonder that you know, did not we prove something more? Did not we already say that every simple radical extension is cyclic? Well, we did that is exactly what the earlier proposition said. That you know, the simple radical extension F alpha over F is, has cyclic Galois group, but we made an assumption that F contains all the nth roots of unity.

So now we are trying to state it without that assumption and so there is just one little step that we need to do; which is we have to adjoin the nth roots of unity to our initial field Q. And once you do that, then everything works the same way. And that one step is what is going to give you an abelian group.

So you can actually n fact, say there is one guy which is a billy and the rest are cyclic and so on, but for us abelian is all that will be required for our later arguments. So, Proof: by definition of expresibility in terms of radicals, what we know is that exists at tower Q equals, so now write a tower like this K naught, K 1, K r with alpha belonging to K r and each extension is simple radical, each K i by K minus 1 is a simple radical extension.

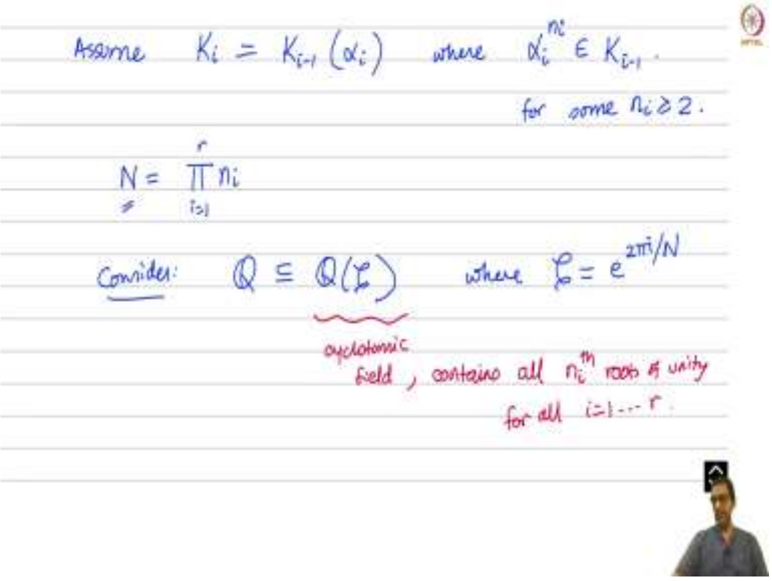
(Refer Slide Time: 25:32)



Prop^n: If $\alpha \in \mathbb{C}$ is expressible in terms of radicals, then $\exists$ a tower st $\alpha \in L_r$ and each L_i/L_{i-1} is Galois with abelian Galois group.

$$\begin{tikzcd} L_r \arrow[d, dash] \\ \vdots \arrow[d, dash] \\ L_1 \arrow[d, dash] \\ \mathbb{Q}=L_0 \end{tikzcd}$$

Pf: By defn, $\exists$ tower $\mathbb{Q}=K_0 \subset K_1 \subset \cdots \subset K_r$ with $\alpha \in K_r$ and each K_i/K_{i-1} is a simple radical ext^n.



Assume $K_i = K_{i-1}(\alpha_i)$ where $\alpha_i^{n_i} \in K_{i-1}$ for some $n_i \geq 2$.

$N = \prod_{i=1}^{r} n_i$

Consider: $\mathbb{Q} \subseteq \underbrace{\mathbb{Q}(\zeta)}_{\text{cyclotomic field}}$ where $\zeta = e^{2\pi i/N}$

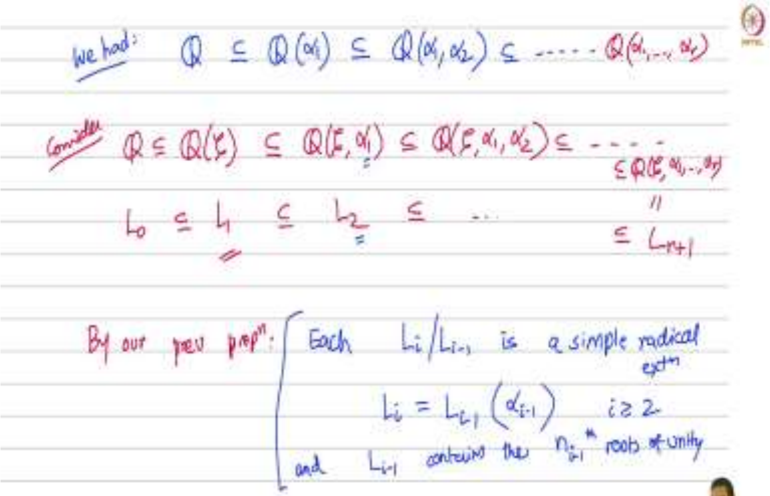
cyclotomic field, contains all n_i^{th} roots of unity for all $i=1\ldots r$.

Now, the point is if instead of Q we had also a field which had all the nth roots of unity, then you know we could have concluded that the simple radical extensions are of have cyclic roots. So, what we will do is, we will just adjoin those nth roots. So let us assume that each K i is just, you get from K i minus 1 by adjoining some nth root, some alpha i, where let us say alpha i to the n i, it is the n ith root of some element in K i minus 1, for some n i, you can see assume they are all at least 2.

So you get each successive step by adjoining some n ith root of an element of the previous field to that field. So, suppose this is the case. So I have these numbers n i, I know all of them, so I will just take their product and what I will do is, I will adjoin, so now consider. So I want to adjoin all the n ith roots of unity, I can do it in one step by just adjoining the nth root of unity, capital nth root.

So let us do the following. Let us take the cyclotomic extension, Q zeta, where zeta is e to the 2 pi by capital N. Observe that if you have this, this is the capital Nth root of unity. But this field also contains all the n ith roots of unity. So this is a cyclotomic extension. This is a cyclotomic field and further it contains all n ith roots of unity because capital N is a multiple of n i for all i.

(Refer Slide Time: 27:54)



We had: $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\alpha_1, \alpha_2) \subseteq \cdots \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$

Consider $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\zeta, \alpha_1) \subseteq \mathbb{Q}(\zeta, \alpha_1, \alpha_2) \subseteq \cdots \subseteq \mathbb{Q}(\zeta, \alpha_1, \ldots, \alpha_r)$

$L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_{r+1}$

By our prev propⁿ: Each L_i / L_{i-1} is a simple radical extⁿ

$L_i = L_{i-1}(\alpha_{i-1}) \quad i \geq 2$

and L_{i-1} contains the n_{i-1}^{th} roots of unity

Now, what does that mean? Well, that means now that I can instead of this tower that I had K naught, K 1, K r, I will just construct a somewhat larger tower. So now define a new tower as follows. Let us define L i as, so this is instead of K i minus 1, so let us do it in steps maybe. So I had Q, L naught containing K 1 is, I adjoin alpha 1 to it.

Then K 1, I adjoin alpha 2, so this I called as K 2 and so on. So I keep adjoining successive elements. Now, let us just define L 0 to be Q. So, let us define L 0 maybe to be Q of, Q of zeta and now let us say L 0 is contained in maybe we should not call this as L 0. So this is one, one additional step that we need.

So let us say I have so instead of the tower Q, Q, alpha 1, Q, alpha 1 alpha 2 and so on. This was the original tower that we had. Now, we will define a new tower in which we will also adjoin that zeta. So, now instead of Q look at; start with a larger field Q zeta and to Q zeta you adjoin alpha 1 to Q zeta alpha 1, you adjoin alpha 2 and so on.

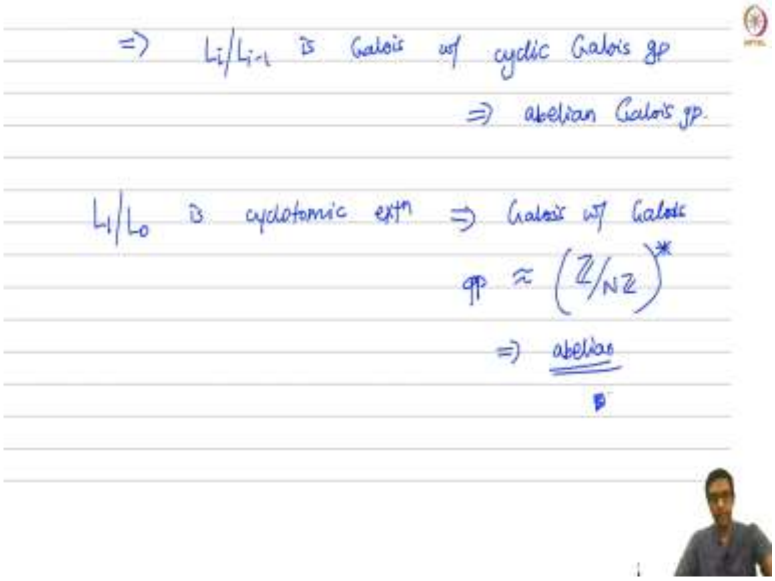
So, consider this new tower and of course, Q is contained in Q zeta. Now, I call these as my Ls, this is L 0, L 1, L 2 and so on. Now, this last step is some Q of have alpha 1, alpha 2 alpha r, this is Q of zeta comma alpha 1, alpha 2, alpha r. So, this guy is well unfortunately because of the way my numbering meant this is L r plus 1 rather than L r.

But does not; matter my key point finally is that I can construct a new tower in which all the n ith roots of unity are guaranteed to exist in the base field, they all exist in L 1 itself. Now we just use our previous proposition; by our previous proposition, observe that each step is a simple radical extension, observe that each L i over Li minus 1 is a simple radical extension and further, L i minus 1 contains all the n ith roots of unity definitely.

So contains all the required roots of unity. So maybe we should just be slightly more careful here. So L i over L i minus 1, what is it really? L i is L i minus 1 adjoin. So there is a slight numbering thing here, L 2 is obtained by adjoining alpha 1. So it is L i minus 1 adjoin alpha i minus 1 now. So this is for i at least 2.

Now, so what do I know? So, this is a simple radical extension and the base field which is L i minus 1 contains the n i minus 1th roots of unity, which is what I need for my earlier proposition. So these hypotheses are satisfied for earlier proposition.

(Refer Slide Time: 31:56)



⇒ L_i/L_{i-1} is Galois w/ cyclic Galois gp

⇒ abelian Galois gp.

L_1/L_0 is cyclotomic extn ⇒ Galois w/ Galois gp $\approx (\mathbb{Z}/N\mathbb{Z})^*$

⇒ $\underline{\underline{\text{abelian}}}$

■

So we conclude from our previous proposition that L i over L i minus 1 is Galois with a cyclic Galois group, cyclic is of course, abelian. Now, this only deals with extensions from the second stage onwards that is, this has cyclic Galois group, this has cyclic Galois group and so on. But we still have to worry about the very first step in the tower L 1 over L 0 but recall L 1 over L 0 is just a cyclotomic extension and we know what the group of a cyclotomic extension is.

So, this is of course just a cyclotomic extension which we have studied. Therefore, it is Galois we know that with well what is the Galois group? It is Z mod, whatever it is capital N Z, the group of units of that ring. So therefore, it is definitely abelian. So the first step is some abelian group; the remaining steps are definitely cyclic, in fact. So that proves the theory.