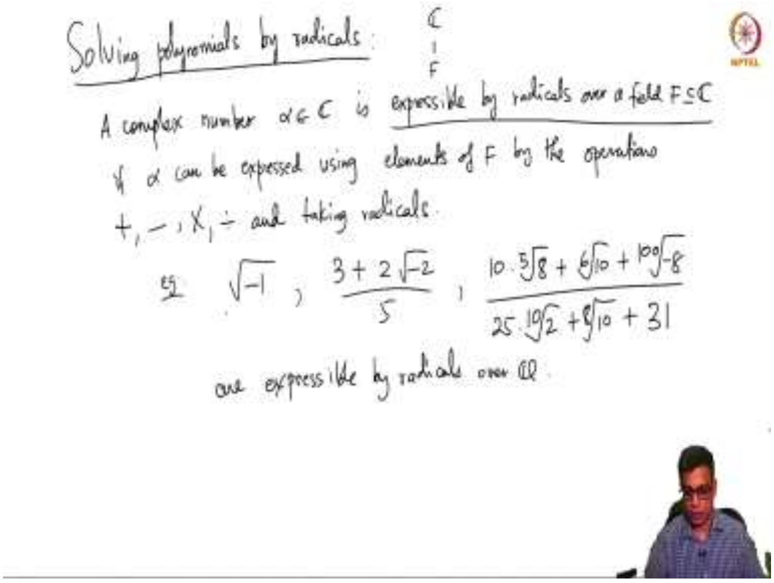
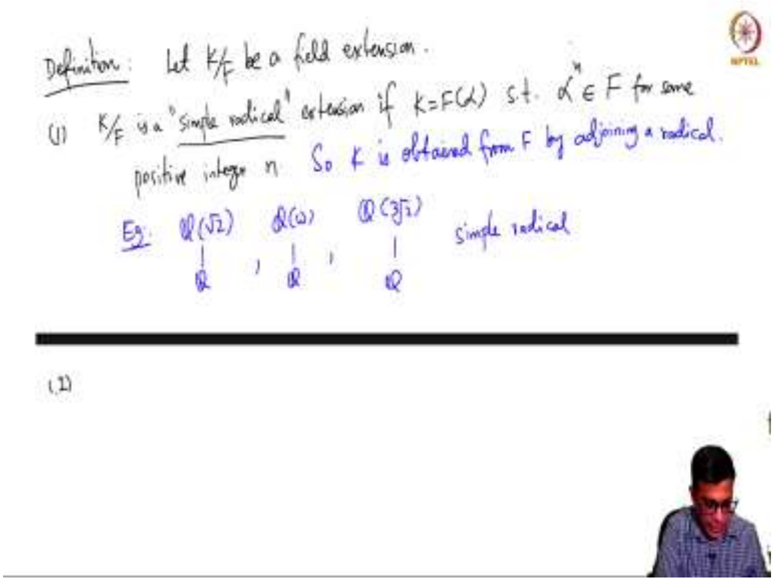
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture - 37
Solvability by Radicals

(Refer Slide Time: 00:27)





Welcome back. In the last video, we completed our discussion about cyclotomic extensions, and the topic now is the final topic of the course. So, the rest of the course is going to focus on solving polynomials by radicals. So, in the very first video I described, what we mean by this. So, let me quickly recall that, and then we formally will define, what this means. So, we can generally define; I am now going to stick to characteristics 0 fields for the rest of course. For simplicity, some of these statements will be true in some most characteristics.

But, I want to stick to complex numbers, because it is easiest to state it without any restrictions about characteristic. Let us take a complex number. We say that. So, I do not formally define as of now; but, a complex number alpha is expressible by radicals. So, I have to fix a base field. So, it is expressible by radicals over some fields. So, C contains F.

And we typically take F to be Q, if alpha can be expressed. So, this is not a formal definition, that will come in a minute. But I want to indicate, what we need, can be expressed using elements of F by the operations; of course, the standard operations; addition, subtraction, multiplication, division, and radicals, taking radicals.

So for example, root minus 1 is one such, 3 plus 2 times minus 2 by 5, or 10 times 5th root of 8 plus 6th root of 10 plus 100th root of minus 8 by 25 times 10th root of 2, I mean, I am just, as you can see, just randomly writing some numbers. These are expressible by radicals, over Q in fact.

Because each of these numbers is an expression involving rational numbers, and the 5 operations; addition, subtraction, multiplication, division, and you are allowed to take radicals that means taking roots of elements. So, you can take 10th root, 5th root, and so on. So, these are, this is roughly what it means to be, I mean this is loosely speaking the definition of being expressible by radicals.

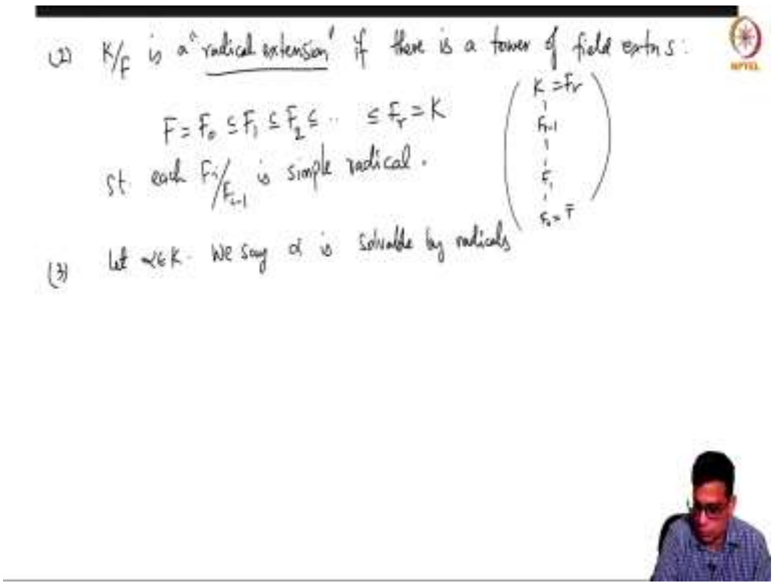
But, in order to give a formal definition and we will use field theory for this. I am going to define a series of statements here. I will give you a series of definitions. Let K over. So basically, I will fix, be a field extension, and fix an element in the bigger field. So, the first definition is that. So, these are crucial definitions.

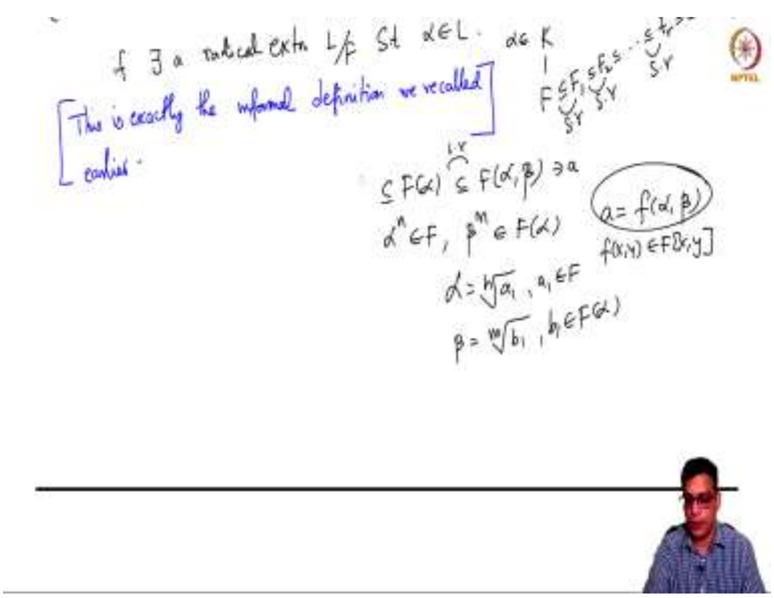
So, as I said, I want to formalize this notion that I am trying to define here, what it means for something to be expressible by radicals. So I need to say that, there is a tower of extensions from starting with F all the way to some field containing alpha, where each extension is a radical extension. So, that is going to be our formal definition.

So in order to do that, let me give you these definitions, is simple radical. So, this is the terminology. The extension is a simple radical extension; if K equals F alpha. So, let me not fix alpha here. So, I am starting with an arbitrary field extension. If K equal to F alpha, such that alpha power n equals, is in F for some positive integer n.

So, essentially what we are saying is that. So, that is. So, K is obtained from F by adding a adjoining, that is the correct term, a radical; by adjoining a radical. So, this is a simple radical extension, a trivial example. We will do more examples later, but. So, this is a simple radical extension. You are adjoining an nth root in general. Here, you are adjoining a square root. So, all your, they are all simple radical.

(Refer Slide Time: 06:17)





$\mathbb{Q}$, $\mathbb{Q}$, $\mathbb{Q}$

(2) K/F is a "radical extension" if there is a tower of field extns:

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r = K$$

s.t. each F_i/F_{i-1} is simple radical.

$F_r = K \supseteq_{s.r} F_{r-1} \supseteq_{s.r} \cdots F_1 \supseteq_{s.r} F_0 = F$

(3) Let $\alpha \in K$. We say α is "solvable by radicals over F" or (simply) "solvable" over F if $\exists$ a radical extn L/F st $\alpha \in L$.

α is solvable

[This is exactly the informal definition we recalled earlier.]

$\alpha \in K$, $F \subseteq_{s.r} F_1 \subseteq_{s.r} F_2 \subseteq \cdots \subseteq_{s.r} F_r = L \ni \alpha$

earlier.

(4) K/F is solvable if every element of K is solvable over F.

The question we want address: If $f(x) \in \mathbb{Q}[x]$, are the roots of f solvable over $\mathbb{Q}$?

(5) A polynomial $f \in F[x]$ is solvable over F if all its roots in a splitting field are solvable over F.

Re-phrasing the question: Given a poly $f \in \mathbb{Q}[x]$ is it solvable over $\mathbb{Q}$?

$+, -, \times, \div$ and taking radicals.

eg $\sqrt{-1}$, $\frac{3 + 2\sqrt{-2}}{5}$, $\frac{10 \cdot \sqrt[3]{8} + \sqrt[6]{10} + \sqrt[100]{-8}}{25 \cdot \sqrt[19]{2} + \sqrt[8]{10} + 31}$

are expressible by radicals over $\mathbb{Q}$.

Definition: Let K/F be a field extension. Assume $[K:F]$

(1) K/F is a "simple radical" extension if $K = F(\alpha)$ s.t. $\alpha^n \in F$ for some positive integer n. So K is obtained from F by adjoining a radical.

Eg: $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(\omega)/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ simple radical

So now, a radical extension is one, which consists of its tower of simple radical extensions. K over F is a radical extension. So, I removed the word simple here, if there is a tower of field extensions. So this is the following. So, I am going to write it like this; F equals F0, containing, contained in F1, contained in F2, all the way up to F r, which is K. So, our usual way of denoting this. I just did this to save space.

This is our usual way of describing such a tower, such that each of these extensions is simple radical. So, K over F need not be simple radical, but it is made up of simple radical extensions. So, we will do examples of all of these things. So now, let alpha be in K. So, K over F is a fixed field extension a priori. We say, alpha is solvable by radicals. So, let me erase this. I will write it smaller.

So, F r is K, F r minus 1 F1 F0, which is F and this is simple radical. So, that is my short form, simple s r is simple radical. Each of them is simple radical. So now, let us come back to the third definition. Alpha, in case said to be solvable by radicals or simply solvable. Often, we will just use the word solvable, because we will only talk about solvable by radicals. If there exists a radical extension, I am not saying K over F is a radical extension.

I am only saying that there is a radical extension, L over F, such that alpha is in F. So. I am not, I mean, a priori you are given K over F, alpha is here. But then, you can construct a tower like this, containing alpha, and this is simple radical, this is simple radical, this is simple radical. So, this is the meaning of being solvable by radicals, and I will let you think about this; this is exactly the informal definition, we recalled earlier.

Informal definition being this, this is something for you to ponder. But, if alpha is in L and each of these is a simple radical extension, then it will become a very messy expression, of course depending on how many fields are in this tower. Nevertheless, it is possible to express alpha with starting the elements of F, and using only radicals, and of course the usual 4 operations. Because, if you have, let us say 2 things.

So, as I said, I will not. Let us say alpha n is in F, and beta m is in F alpha. This is simple radical, and this is simple radical. So, I am not giving you a formal definition, but just to indicate it. And now, you take some a in here; a can be written using, a can be written as a polynomial in f alpha, beta; where f is, f as coefficients in capital F. By definition that is the meaning. And alpha power, alpha is nth root of something in F.

Let us say, a1 and beta is an mth root of something in F alpha. So now, you can further write, b1 as a function, as a polynomial in alpha and each of those has coefficients in F, and alpha is already in nth root. So that ultimately anything can be expressed using, starting with elements of F, and using only radicals. So, I am sorry. I sort of did not explain this in detail, but this is the crucial definition, that we are going to take for our informal earlier definition, will be formalized by this third statement.

And finally, I will give you the meaning of an extension being solvable, K over F is solvable, if every element of K is solvable over F. So, I should really write here solvable over F that is part of this, over F. So, it is important to put that over F statement because solvability is a property over, once you fix the base field, because if you change the base field, something may be solvable or not. So for example, I mean, you can take.

So, pi for example is not even algebraic over Q. So, whereas it is solvable over, I mean, it is a simple example, but not over Q. So, it is not over Q, because it is not even algebraic. So, I really should take an algebraic extension. But I want to even assume that, it is a finite extension, for the last part at least.

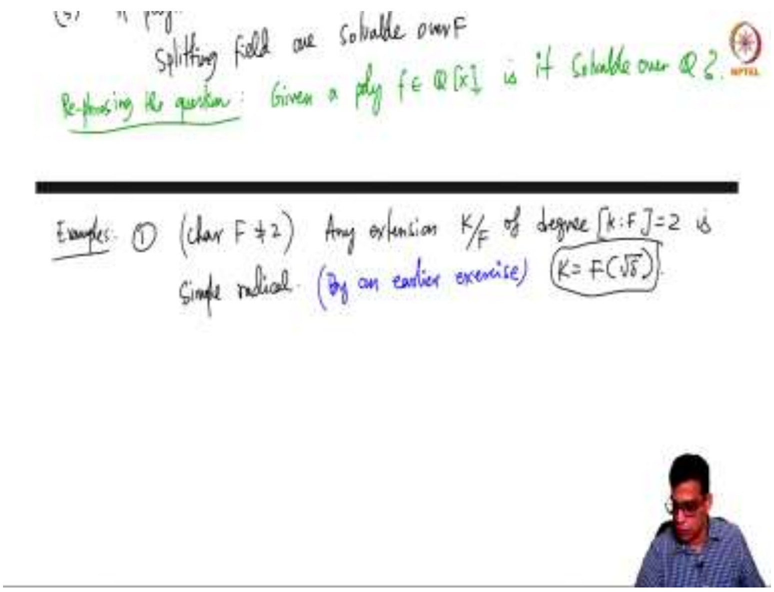
So for, 3 and 4, for 3, I assume alpha is algebraic over F; and for 4, K over F is algebraic. See, if you do not have an algebraic extension, the question of being solvable by radicals does not arise. So, 1 and 2 of course are general statements; but for 3 and 4, you need, for 3, you need alpha to be algebraic; for 4, you need the entire extension to be algebraic. So, let me give you some examples and then we will study this further.

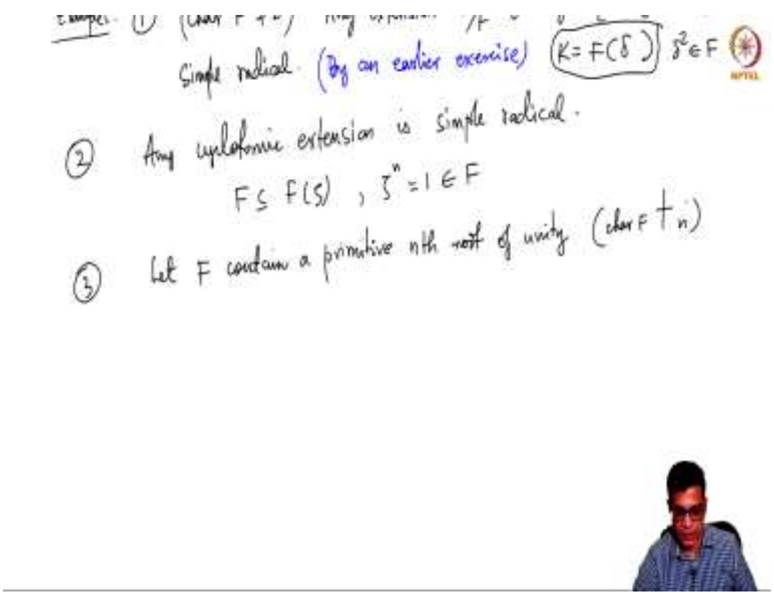
So the question, that we want to ask is, which complex numbers are solvable over rational numbers, most specifically, whether the roots of a given polynomial are solvable by radicals over Q. So, it starts with polynomial with rational coefficients. Can the roots be expressed using radicals, starting with Q? So, that is a question in the new language. Our question is. So the question, that we want to, want to address, is the following.

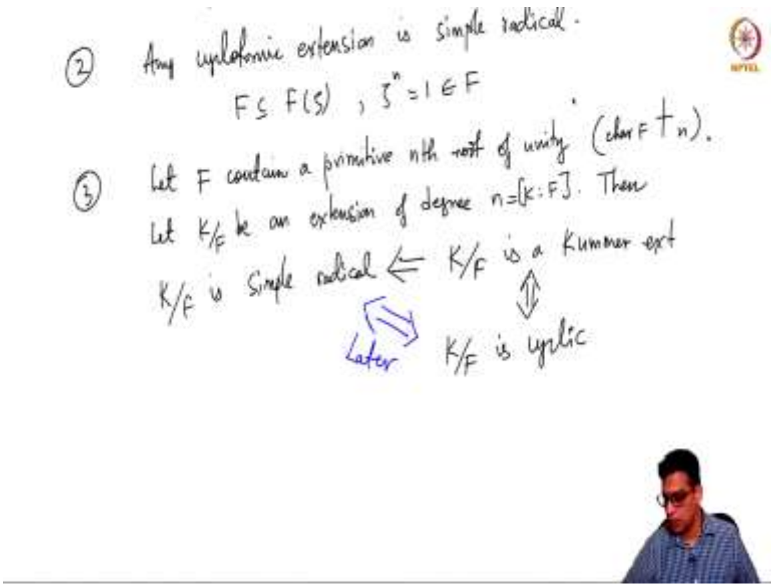
If f is a polynomial with rational coefficients, are the roots of f solvable over Q? So, that is a question that we want to address. This is the question that Galois solved. And u, is showed that for a degree 5 polynomial you cannot do this. And the final definition, let me write that here. A polynomial is solvable, if all its roots in a splitting field, of course F, capital F itself may not contain the roots, are solvable over F.

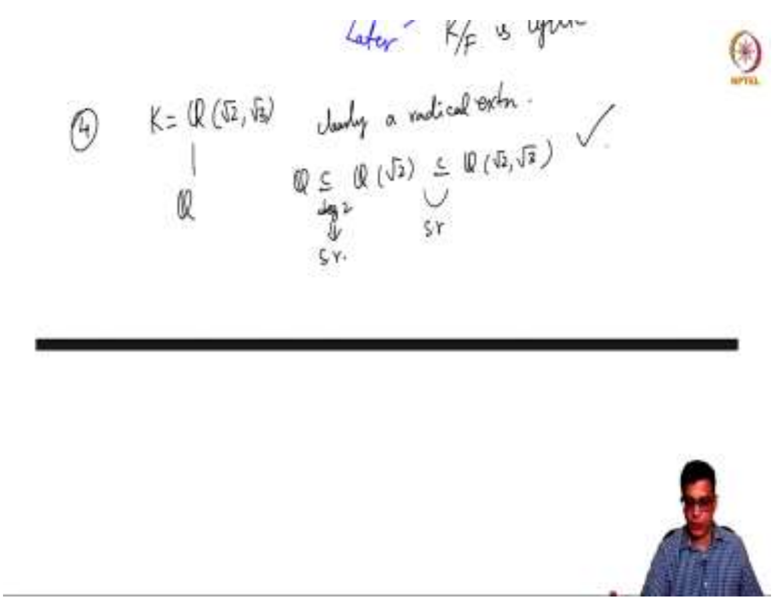
So again, I omitted the crucial thing here, solvable over F, if all its roots in a splitting field are solvable. So the question can be rephrased is as follows. So, rephrase the question. So, the rest of the course is going to be addressing this question. If given a polynomial f in Q X, is it solvable? So, we are going to develop the theory as Galois developed to answer this question.

(Refer Slide Time: 16:09)









So in order to do that, we need to rephrase radical extension, before I state that, let me give you examples. So, first example is if character. So, this is only. I mean here, this is very general. Of course, I am assuming characteristic of F is 0. So, this condition is no condition, but this statement is true; for any field, provided its characteristic is different from 2. Any extension, K over F of degree 2 is simple radical, is a simple radical extension.

Why is that? This is an exercise; we did, by an earlier exercise. What we did was, we selected an element alpha, which generates K over F, because you can take any alpha not in F. Then you take the irreducible polynomial of alpha, it is a degree 2 polynomial, and you simply notice that, if you take the discriminant of that and attach its square root, you get K. So, K is obtained by attaching a square root.

So, K is F adjoin root delta. So, it is a simple radical extension. The first definition is an extension, is simple radical, if it is generated by an element, a power of which is back in F. So of course, so delta is the root, so delta square is in F. So, delta is the square root of the discriminant; b square minus 4 a c. So, those are simple radical extension.

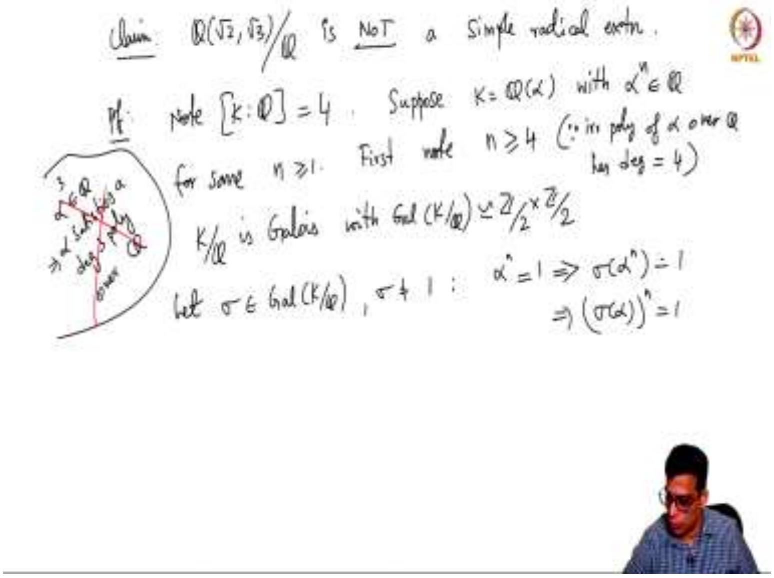
Any cyclotomic extension is simple radical obviously because it is generated by a primitive nth root of unity. So that means, it is of the form F zeta, where zeta power n is in F. So, this is also clear. What about Kummer extension? So, let me state the following. Let F contain a primitive nth root of unity. So, here I assume characteristic of F does not divide n. In fact, that is a consequence of this statement, but I did not do that.

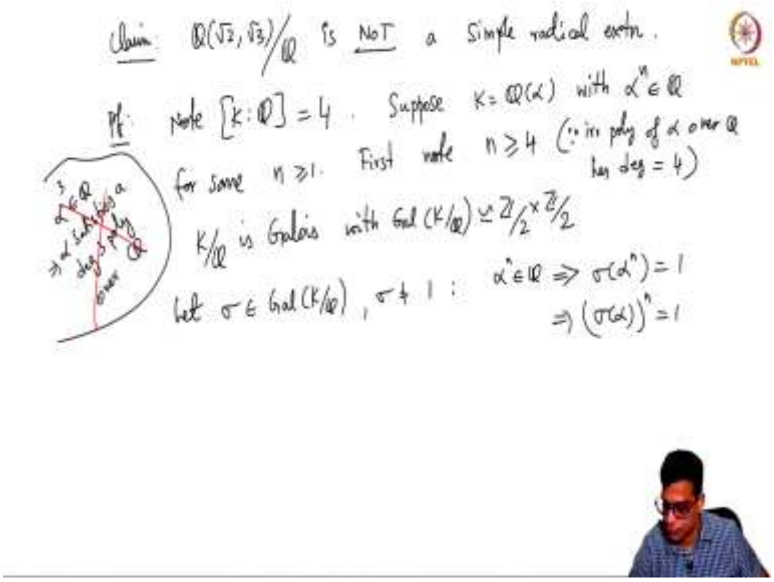
So, I am going to assume this. Again, our main focus will be in characteristic 0. So, where this condition is irrelevant, so let F contain a primitive nth root of unity where that is all. So that is sentence there. Then, let K over F be an extension of degree n. So then, K over F is simple radical. So, this requires some work this much. K over F is a Kummer extension. So in general, Kummer extensions are simple radical extension.

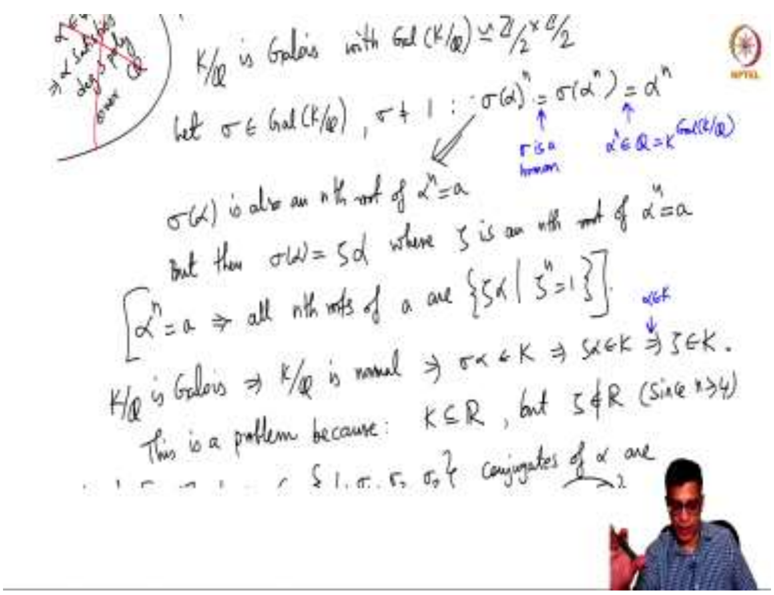
So that is what, if it is a Kummer extension that means K is generated by alpha; such that alpha power n is in F. And this of course is, if and only if K over F is cyclic. So, we will prove later something about this. So, this is our crucial observation, that simple radical extensions and cyclic extensions are sort of identical. I mean, one implies the other. I mean. So our, the extensions, that we have studied, namely cyclotomic and Kummer extensions are simple radicals, simple radical extensions.

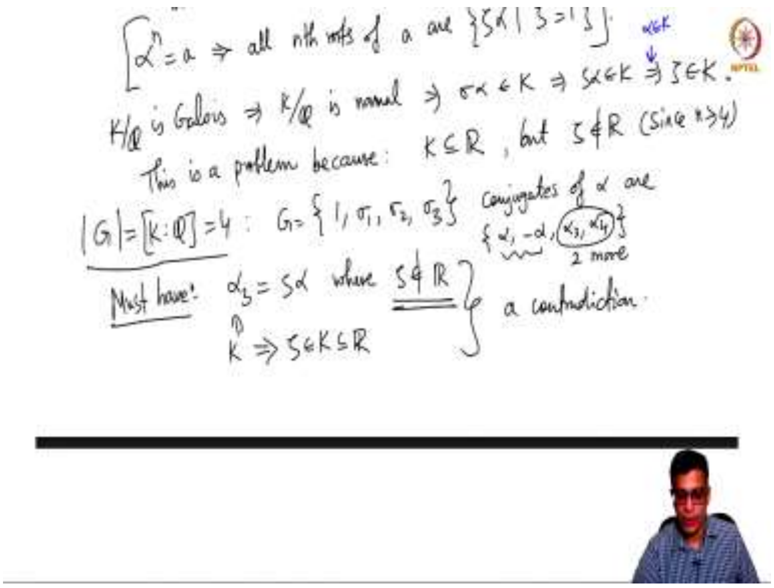
So, let us do one more examples. Let us take K to be Q root 2 and root 3 over Q. This is of course a radical extension. This is radical, because you can put Q first in Q root 2, and then in Q root 2 root 4. This is degree 2, implies simple radical. Of course you can immediately see that root power 2 is in Q. This is also because simple radical, because root 3 is the generator of this extension and root 3 whole square is there. This much is clear.

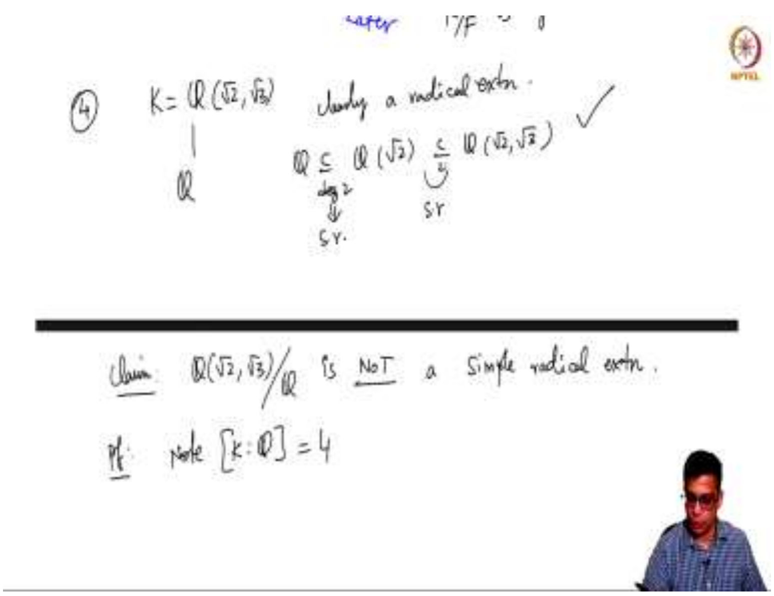
(Refer Slide Time: 21:35)











But the claim, I want to now prove, is that; Q root 2, root 3 Q is not a simple radical extension. It is a radical extension of course, because there is a tower of simple radical extensions, like this. But, it is not generated by a single radical. Why is this? This is a nice proof. So, note K colon Q is 4 of course that we know, because each of these is degree 2.

So, suppose it is a simple radical extension, suppose K is Q alpha with for some positive integer. So this is a. So I am assuming, the contrary. Suppose, it is a simple radical extension; that means, K is generated by Q alpha with a power of alpha landing in Q. So first note that, n is at least 4. So, it is clear because the irreducible polynomial of alpha over Q has degree equal to 4. That means, any polynomial, that alpha satisfies, has degree at least 4.

So, if alpha cubed is in Q, for example. This implies alpha satisfies a degree 3 polynomial over Q. But that of course cannot happen; because it is least degree polynomial, that it satisfies degree 4. So, n is at least 4. And now, we bring in some Galois theory here. K over Q is Galois, that we know very well because, it is normal. Root 2 has all its conjugates there, root 3 has all its conjugates there; namely, minus root 2 minus root 3.

So, it is a normal extension. It is certainly a separable extension, so it is Galois. So, that means in fact with Galois group, it is relevant for us; but it is this. So, for sigma in the Galois group; that is not identity. What is sigma of alpha? Sigma of alpha must be. So, let us take this. Then, alpha power 4, n is 1. If alpha power n is 1, sigma alpha power n is 1. This means, sigma alpha whole power n is 1. So, sorry.

So, not this; this is not correct; alpha power n in Q. So, I have to be careful here. So what I really want to say is that, sigma alpha power n; sorry, sigma alpha whole power n is sigma alpha power n. This is sigma alpha, this is alpha power n; sorry. So this is what, I wanted to say. So this is because, sigma is a homomorphism. And this is because, alpha n is in Q, and which is the fixed field of this.

So, everything I mean of course, sigma is in Q automorphism. So, it fixes this. So, sigma alpha; so this implies sigma alpha is also an nth root of alpha power n. But then, sigma alpha must be something like this; zeta alpha, where zeta is an nth root of alpha power n. Because, if alpha power n is a, all nth roots of a are alpha, zeta i alpha,; where i is equal to, where zeta is basically, I will simply write this.

I mean, this is a standard calculation, if you get hold of a 1 nth root of a; all other nth roots of a will be simply nth roots of 1 times alpha. So, this is the reason for, if sigma alpha is also an nth root of alpha power n, which I am calling a, then all other roots of a, nth roots of a, are zeta alpha. But now, we are in business. So since, K over Q is Galois, it is normal. This implies sigma alpha is in K, because it is normal.

Every conjugate of an element is again in K that means zeta alpha is in K. But then, zeta is in K, because alpha is in K. So this is because, if alpha is in K, you can multiply by alpha inverse. But this is a problem, because, remember K is in R. K is a real field, because root 2 and root 3 are real fields, but. So, what I want to say is that, zeta cannot be inside complex numbers, because n is at least 4.

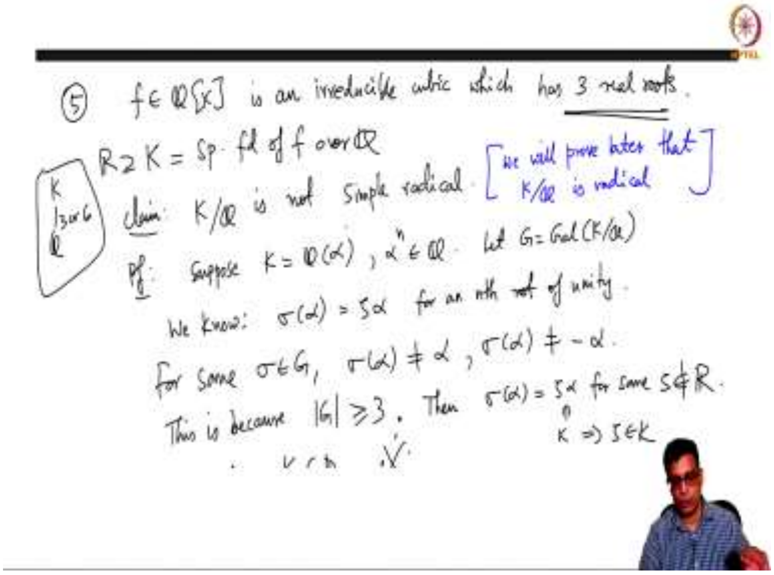
And, we have to take an nth root of a. So, what I really want to say is that, all the nth roots are there. So, I should really add here. So, there are, there is a primitive. So, I am sorry. So, the last point is I can, I am forced to have a non common, non real nth root of 1; because G consists of 4 elements because G is the, the degree of this extension. So G can be thought of as 1; sigma1, sigma2, sigma3.

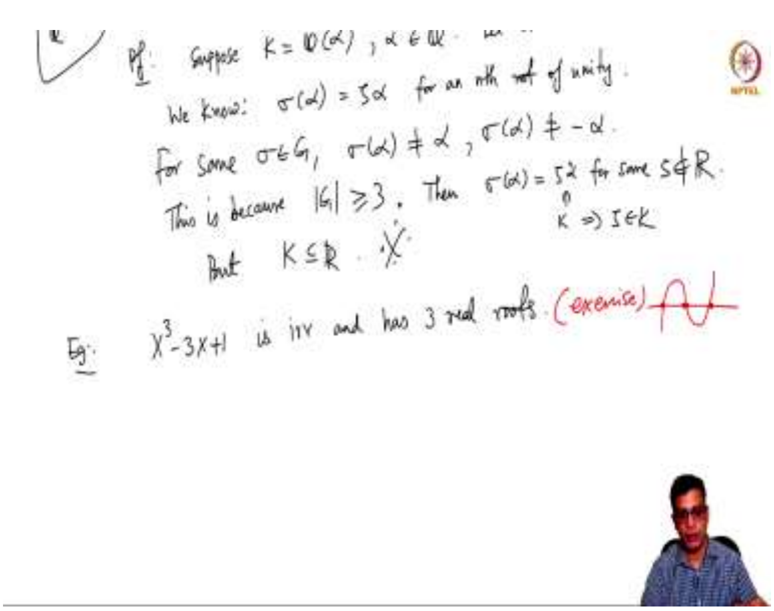
So, where sigma1 changes to root 2; let us say, where sigma2 changes root 3; and sigma3 changes both of them. So then, the conjugates of our potential radical element are alpha, of course 1 of alpha, there will be minus alpha; but there will be 2 more. So, maybe zeta, whatever these are. So alpha3, alpha4. So, these must be something like this, where we must have; because of only roots of unity, that are in real numbers, are 1 and minus 1.

So, that is already taken care of here. So, the third and fourth conjugates of alpha must be some complex non real root of unity times alpha. So that means, and now we use this argument here. Because, this is in K. So, this implies zeta alpha is in K, but zeta is in K, which is in R. So, that is your contradiction. So, I am sorry. I went rather fast about the last part. But this proves that K is not a simple radical extension.

Because if it varies simple radical extension, if there is a radical element alpha, it will have 4 conjugates, 4 different conjugates. One of them will be a non real root of unity times alpha. But that will force that non real root of unity to be in K, but K is a real field. So that is a contradiction. So, this shows that, this is a radical extension, but it is not a simple radical extension.

(Refer Slide Time: 31:12)





So, let me give you one more example, which is exactly similar to this. So, let us say f is an irreducible cubic, which has 3 real roots. So, we know that it has 3 complex roots and at least one real root. But, I am taking an example, where all 3 roots are real. So let us take k to be the splitting field of f over Q. So now I claim that, K over Q is not simple radical.

We will prove later that, it is radical. So, I am going to; I was going to simply say that, the proof is exactly similar to this. But let me quickly tell you, why it is not simple radical; maybe in the process this will become more clear to you. So, suppose K over Q is simple radical. That means, you have this, K equals to Q alpha. Then, such that alpha power n is Q. So then, what we know is, we know sigma alpha is equal to this, for.

So, let us take the Galois group to G. We know actually from our analysis earlier that, G is either a cyclic group of order 3, or G is S3. So, take that, because K over Q is 3 or 6. So, it depends on the polynomial, which; the polynomial determines which case occurs, but its either 3 or 6, for a root of unity. Because for, in fact an nth root of unity. This is clear; because alpha power n is in Q.

So, alpha is in an nth root of that element, sigma alpha must also be an nth root of that element. That means the only possibilities are zeta alpha. I claim that, there is one of; for at least 1. So this is the point, that I for, that I sort of messed up earlier. But what I want to say is that, for some sigma in G, sigma alpha is not alpha and not minus alpha. Why is this? Because, this is because, sigma the order of G is at least 3.

So you will, I mean, you can say, sigma alpha is alpha, sigma alpha is minus alpha, for two of them. But, the third one will be something else; because you are forced to have; I mean, if alpha, sigma alpha determines the entire sigma because, K is generated by alpha. So this is because, there is at least 3 elements. One element may send alpha to alpha; in fact, one element will send alpha to alpha.

The second element may send alpha to minus alpha. But, the third will have to send alpha to something else. Then, sigma alpha will be zeta alpha for some root of unity, which is not R; which is not R because, the only roots of unity that are in R, are 1 and minus 1. So, you are forced to have a different one. But again, as before by our hypothesis that, the polynomial has 3 real roots; we know that K is contained in R.

So, this is a problem; because, this is in K, this implies zeta is in K. So, that is the contradiction. So, this tells you that, if you take any reducible cubic with 3 real roots; its splitting field is not simple radical, It is however radical, as we will show later. So, let me just quickly give you an example of a polynomial, which has this property. So, is irreducible, you can use Eisenstein criterion here, not directly, but by changing X to X minus 1.

And you can also show that, it has 3 real roots, by just computing some roots and plotting its graph. So, its graph will look like this. So, it will cross X axis in 3 spots. So, for this polynomial, if you take this splitting field, it is not simple radical. So, let me stop this video here.

In the next video what we will do is, we will show for example that, if you take any reducible cubic its splitting field will be radical, and more generally we want to understand how to go from radical extensions to cyclic extensions as I have indicated here. Let me stop this class here. In the next class we will continue with radical extensions. Thank you.