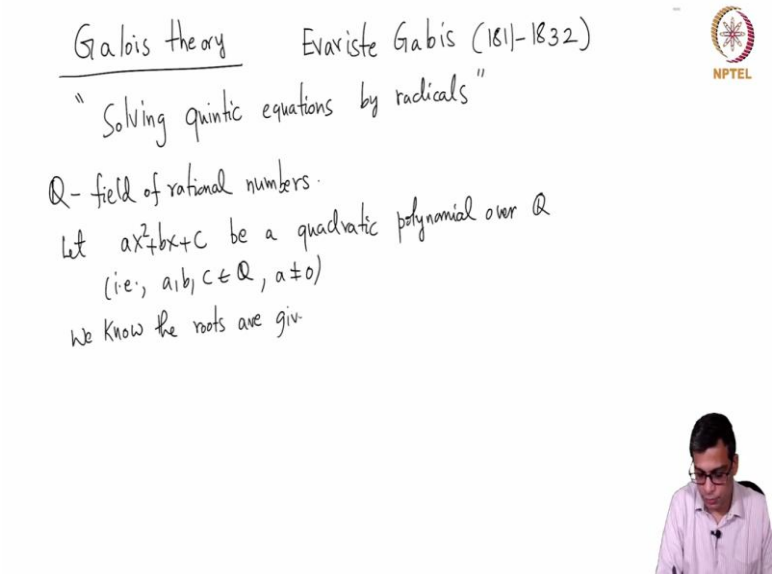
**Introduction to Galois Theory**
**Professor Krishna Hanumanthu**
**Department of Mathematics**
**Chennai Mathematical Institute**
**Motivation and Overview of the Course**

Hello, my name is Krishna Hanumanthu, and welcome to this eight week course on Galois Theory. In this course, we are going to learn this very beautiful topic that is named after a mathematician called Galois. And I will in the beginning the first few videos I will introduce the motivation for this subject as well as quickly recap some of the prerequisites that we need for the course.

(Refer Slide Time: 00:39)




So, the course is called Galois Theory. That is how you pronounce this name Galois is named after a French mathematician his name is Evariste Galois. And he lived in the 19th century and he died very young as you can see 21 years old and he was interested in a very important problem around the time that a lot of mathematicians were interested and in and famous mathematicians were trying to solve this.

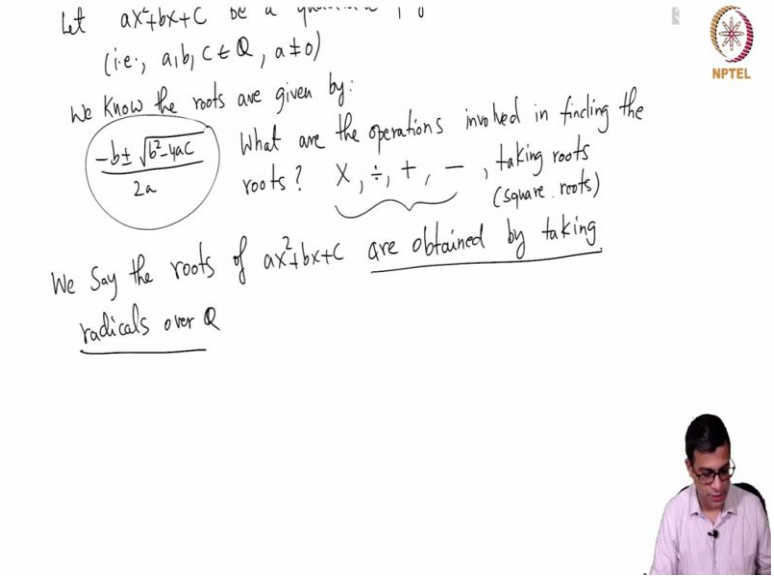
This is the question of whether you can solve Quintics by radicals. So, I will explain this to you now. So, the question that was in the minds of lot of mathematicians around the time was solving Quintic equations, my radicals, so, I will explain what I mean by this. And when Galois was the one who, along with Abel, who was another mathematician, Norwegian mathematician, who worked around the same time as Galois, and in fact proved this, a few years before Galois, but it

was Galois work that led to Galois Theory and that is now the standard way of understanding why you cannot solve Quintic by radicals.

So, before we come to all that, let me just introduce, in very simple terms, what we mean by solving by radicals. So I am going to denote by Q, the field of rational numbers, so we all are familiar with this. And I am going to look at polynomials over the field of rational numbers. So, let us take a quadratic polynomial, let ax square plus bx plus c be a quadratic polynomial, quadratic polynomial over the, full form now, over the rational number.

So, that means that I mean, only that a, b, c are in the field of national numbers and I want the class number here to be nonzero so that I have actually a quadratic polynomial if a is 0 I have linear polynomial or a constant. So I am assuming a is nonzero. We know from school, high school, the roots of this polynomial are given by, this is something that we are very familiar with.

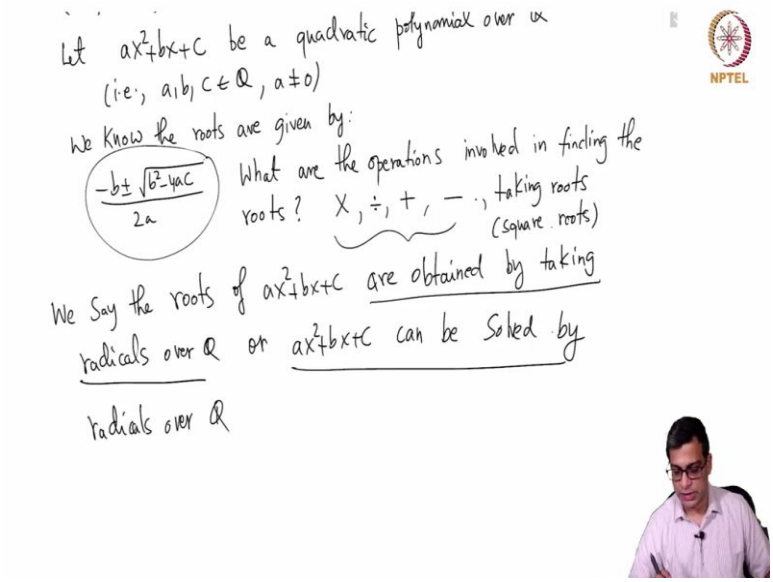
(Refer Slide Time: 03:12)




So, the roots are given by minus b plus or minus b square minus 4ac over 2a. So, this is the equation for the, this is the formula for the roots of this quadratic polynomial. And let us spend a couple of minutes on understanding how we can find the roots what are the operations involved in computing this. So, what are the operations involved in finding the roots. So, obviously, we can immediately see that we have to add, we have to subtract, we have to multiply and we have to divide. So, clearly, we need addition, multiplication, division, addition and subtraction.

So, these are the fundamental four operations in mathematics. So in addition, we also need taking roots because of this, we need the square root we need to take square roots. So in particular, we have to take square roots, so I am going to need also the operation of taking roots. So any number which can be obtained by performing the four fundamental operations and on extra namely taking roots, we say that is obtained by taking radicals. So, we say so, this is the important terminology roots of ax square plus bx plus c are obtained by taking radicals over Q. So, that is one way of saying this.

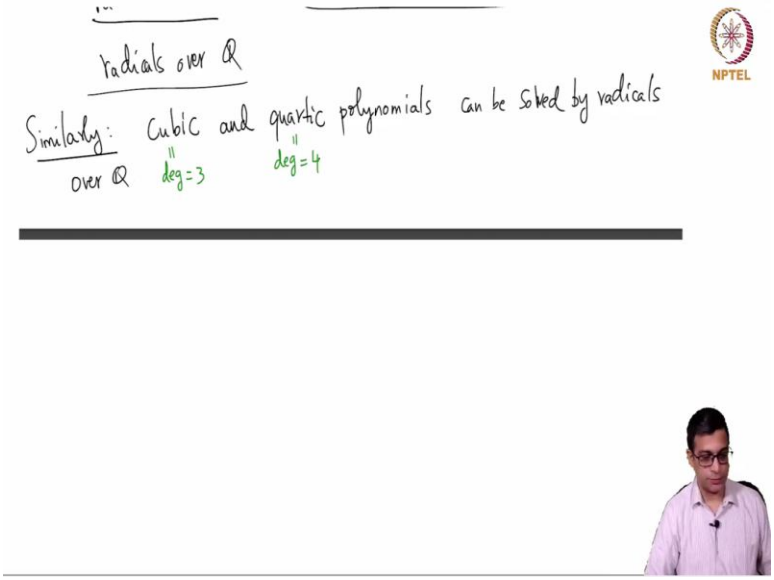
(Refer Slide Time: 05:26)




Another way of saying this or roots or we will say ax square plus bx plus c can be solved by radicals over Q. So, these are the terminologies that we use. So, we say that the quadratic equation, quadratic polynomial can be solved by radicals over Q or the roots of the quadratic formula can be obtained by taking radicals and this is a very simple notion.

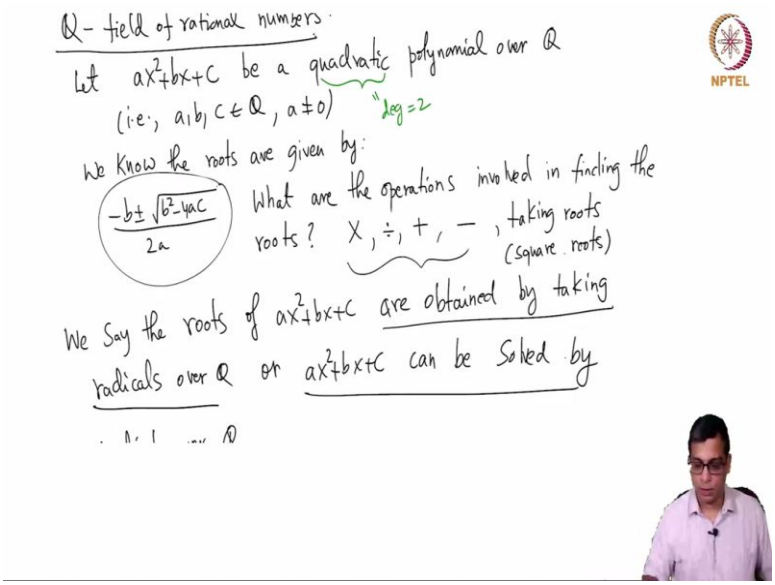
So, let me just repeat it again what do we mean, what do we mean by solving by radicals? It means that you take the coefficients of the polynomial which are rational numbers in this terminology they are a and b and c, they are three rational numbers. Starting with those three rational numbers, we can obtain all the roots of the polynomial by taking the four, by performing the four standard mathematical operations along with taking roots. So, we say that quadratic polynomials can be solved by radicals over the field of rational numbers.

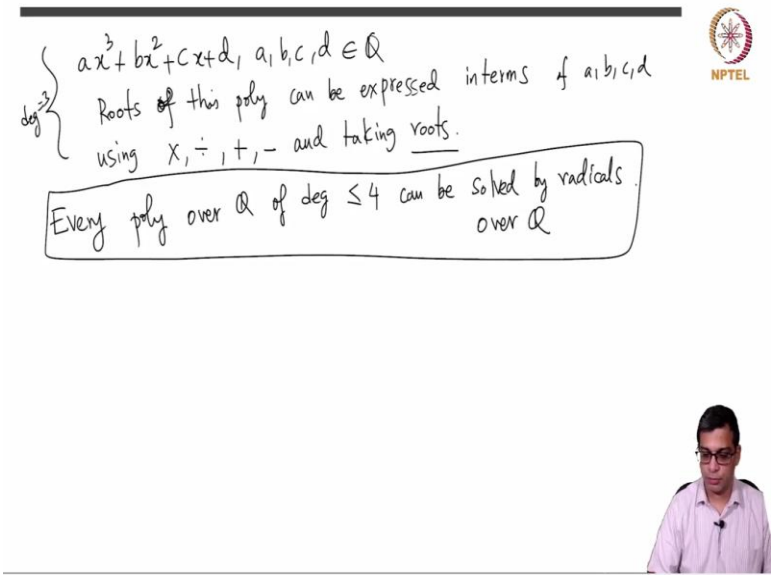
(Refer Slide Time: 06:41)




So, I will now, I will not be able to write the formula, but I will simply assert. Similarly, cubic and quartic polynomials can be solved by radicals over Q. So, just to recall cubic means degree 3 and quartic means degree 4.

(Refer Slide Time: 07:25)






And of course, quadratic means degree is 2. So, this is something that you are familiar with. So, given any degree 2 or degree 3 or degree 4 polynomial over the rational numbers, so, that is important, so, I am always going to work with polynomials defined over rational numbers. So, I can solve them by radicals, which means, you give me any cubic polynomial.

So, just to spell it out in a bit more detail, if you are given a cubic polynomial ax square plus b x, ax cubed plus bx square plus cx plus d, where a b c d are rational numbers roots of this, of this polynomial can be expressed in terms of a b c d and using let me write using the standard operations, multiplication division, addition, subtraction and taking roots.

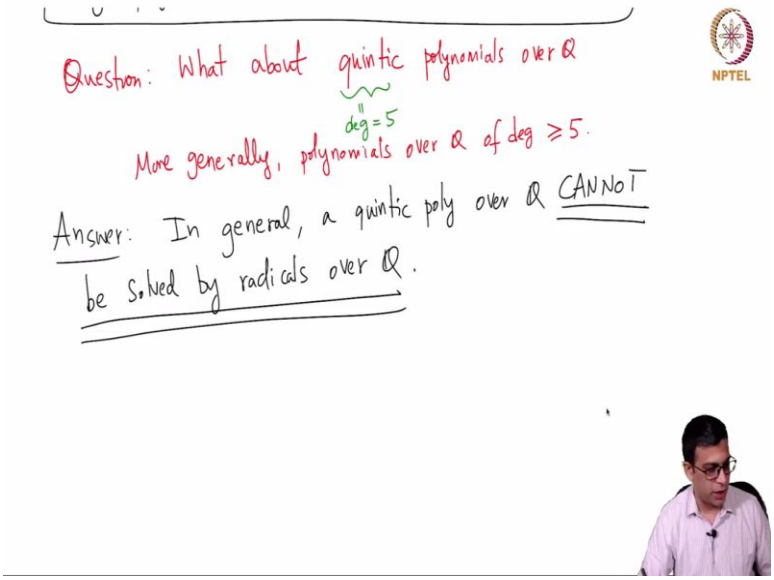
So, here it is not enough to take square roots as it was in the case of the quadratic equation.

Here of course, a cubic equation you have to take 3rd roots, but that is allowed so, I am allowed to take roots of rational numbers, any roots, any order roots, so, here I will not specify which roots so, if as long as I can take roots, I am happy.

So, this the formula is quite a bit complicated, but it does exist. So, just like in the quadratic equation case, cubic equation can be the roots of the cubic polynomial can be expressed using the four coefficients and taking roots and the four mathematical operations. So, and the same can be done for degree 4. So, this is degree 3. And same thing can, can be done for degree 4. So, I want to stress here that every, so here I am doing every polynomial over the rational numbers of degree less than equal to 4 can be solved by radicals. So, that is the important point for us.

So, every polynomial, you give me a polynomial of degree 1, 1 of course is trivial, its root is a rational number, but, more interestingly, if you take a degree 2, 3 or 4 polynomial over the rational numbers, it can be solved by radicals over Q. So, that is the point so, you can solve it by taking the coefficients of the given polynomial and performing the 5 operations, multiplication, division, addition, subtraction, and taking roots. So, this is something that people knew this was known, well, before Galois, and the question that mathematicians before Galois, were interested in.

(Refer Slide Time: 10:50)



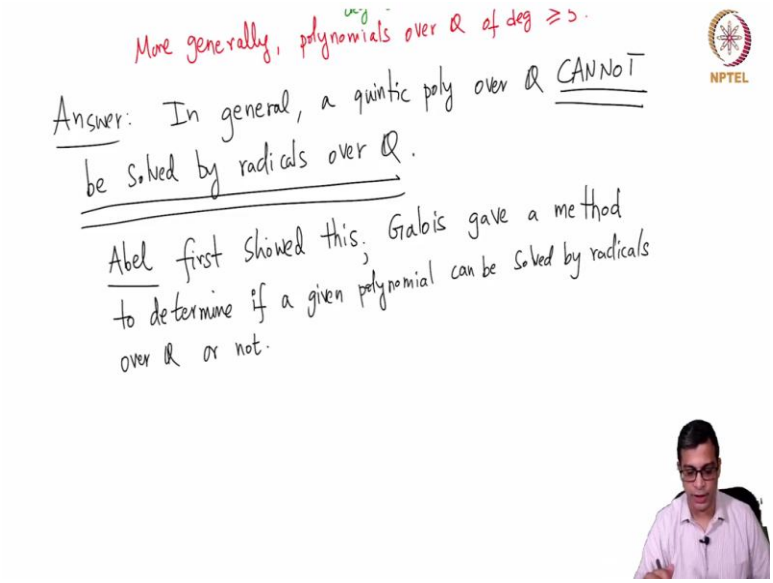

What about, so question, what about quintic polynomial over Q? So, quintic means degree 5, so quintic means degree 5 and more generally for all higher degrees polynomials over Q of degree at least 5. So, it was the problem of solving cubic, quadratic cubic and quartic polynomials was solved and it was not that difficult quadratic is very easy, cubic and quartic requires some work, but it was possible to do, but people are not able to do for degree 5.

So, naturally the question arose, is it possible to do, can you solve a degree 5 polynomial by radicals? And obviously, the question is what about all higher degrees, degree 5, 6 and so on. So, there was some work about this before Galois and the answer is in general a quintic polynomial over Q cannot be solved by radicals over Q. So, again, I mean, I am going to stress this, that means, there is a quintic polynomial.

So, in general, I am not saying that every quintic polynomial cannot be solved by radicals, I only mean that there are quintic polynomials, which cannot be solve by radicals over Q, which is to say, if you spell it out, there is a degree 5 polynomial with rational coefficients, such that its roots cannot be expressed using the coefficients of that polynomial with addition, subtraction, division, multiplication and taking roots.

And this involved quite a bit of work. And as you can imagine, to give a formula for finding the roots is a fundamentally different kind of problem than to show that it cannot be done. Because, just because you fail to find a formula does not mean that nobody else can find a formula. So, this is a new kind of theorem to establish that it cannot be solved. It is important to find a conceptual reason, why you cannot do this, just because you tried 1000 methods and they did not work does not mean that you cannot do it. So this is very different from what happened for degree 2, 3 and 4. So you cannot do this.

(Refer Slide Time: 14:03)



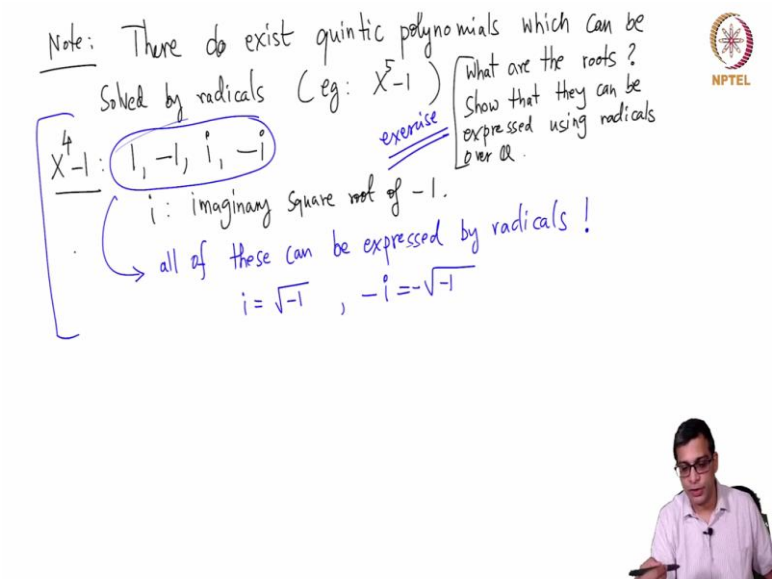

And it was done. Just before Galois did this by Abel. He is a, he was a mathematician. Around the same time as Galois. He also actually died very young, his life overlapped with Galois, and he is Norwegian. And he proved though his proof is somewhat different from Galois proof and we do not study his proof nowadays, we mainly look at Galois because Abel showed that a general quintic polynomial cannot be solved by radicals.

So, it is not easy to find the answer for a given polynomial. But Galois gave a more Galois studied this. And in fact, he gave a more concrete construction and gave a method to determine for any given polynomial whether it can be solved. So I will write this gave a method to determine if a given polynomial can be solved by radicals all over Q, again I am going to stress this a given polynomial over Q can be solved over Q or not.

So, Abel showed that this cannot be done in general. So, what happens for degree 2, 3, 4 is just not true for degree 5 there do exist polynomials, which cannot be solved with radicals over Q but Abel was not did not give a specific example of a polynomial which cannot be solved by radicals he said a general polynomial of degree 5 cannot be solved by radicals.

Galois, in fact, gave a method which of course, you cannot always apply, it is a conceptual method, but he developed a lot of theory to determine just by looking at the polynomial whether it is solved by, whether it can be solved by radicals or not. So, by the way, Abel is a mathematician after whom Abelian groups were named. So, that was just an interesting fact. So, I want to stress here that

(Refer Slide Time: 16:26)




There do exist quintic polynomials which can be solved by radicals. We can simply take an example, which is a simple example is x over 5 minus **one**. So, these are fifth roots of unity and the roots are all given by so, this is a good exercise for you to write down what are the roots and

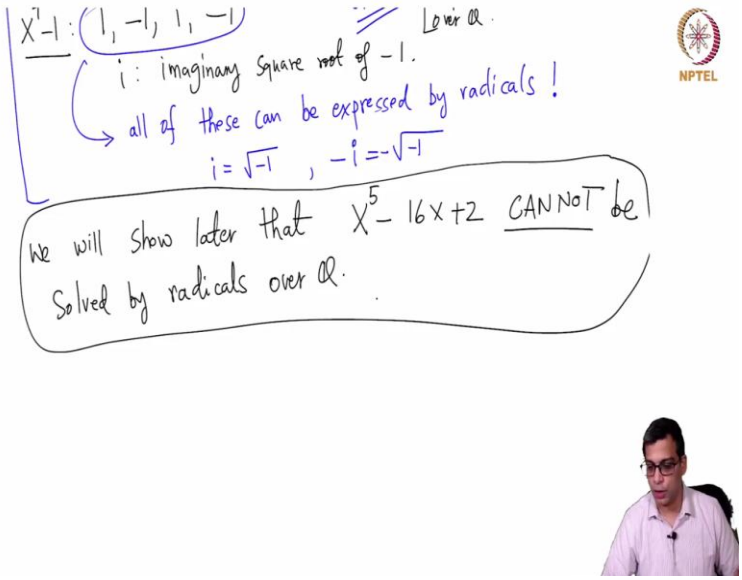
show that they can be expressed using radicals over Q. So this is an exercise for you. So, for example, i is not a root of this, but if you take x power 4 minus 1 then i is the root.

What are the roots? So, I mean I want to do is I want you to do x power 5 minus 1, but I will do x power 4 minus 1 which is not degree 5 but to illustrate the idea. So, this is the, i is the complex or imaginary square root of minus 1. So, all of these as you can see can be expressed by, all of these can be expressed by radicals clearly, clearly, because 1 is of course, a rational number so it is expressed by radicals, so, is minus 1. i is the only one you have to think about.

So, that is square root of minus 1. So, here, you are allowed to use radical symbols, square root symbol, so, these can be expressed by radicals. So, this is degree 4 of course, but it is easier to express I use that, but write down x power five minus 1 it is a good way for you to motivate yourself into this course, what are the roots of x power 5 minus 1 these are the fifth roots of unity and try to see that they can all be expressed by radicals.

So, now, what Abel and Galois did is that they do exist. So, we are not saying that, we are not saying that every quintic polynomial is not solvable by radicals, we are only saying that there are quintic polynomials, which cannot be solved by radicals.

(Refer Slide Time: 19:27)



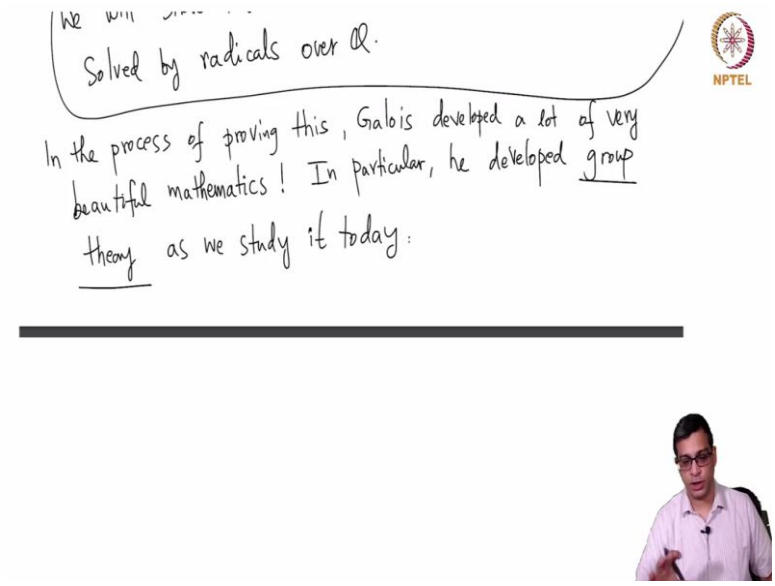

So, for example, we will show later. In fact, towards the end of the course, that there are several polynomials, so, I am going to write one here, x power 5 minus 16x plus 2 cannot be solved by it

is a rational polynomial, but it cannot be solved by radicals over Q. So, this is going to be the end goal or one of the end goals of this course. So, we have to develop a lot of theory.

And as I highlighted earlier, you should think about this to prove a statement like this that it cannot be solved by radicals, it is not a question of computing or doing lot of calculations, it is a question of developing enough theory to and find out some other properties which characterize whether something is solvable by radicals or not. And then show that this polynomial does not have those properties.

So, this is the genius of Abel and Galois, and that is what they have done, and which we are going to learn in this course, and at the end, we want to convince ourselves that you cannot solve this particular polynomial by radicals, in fact, we will show that there are a lots of polynomial which cannot be solved by radicals. So, this is the goal of this course.

(Refer Slide Time: 20:52)

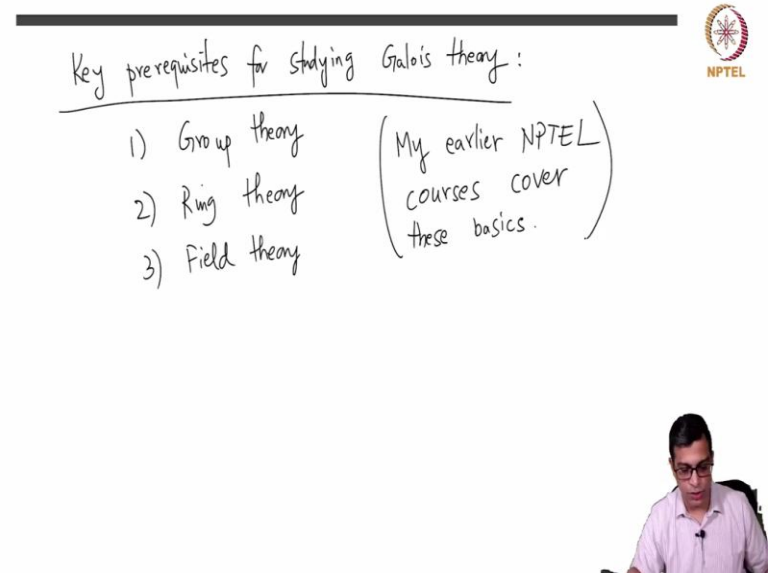



So, in the process of proving this, proving this fact and lots of related facts, Galois developed a lot of very beautiful mathematics. In fact, as you saw in the beginning, he died at a very young age at 20 years old. He wrote some of these work as letters to various people and only after he died, people realize that, there is a lot of deep mathematics in those letters and people publish them, and then we were studying all these things for the last 200 years.

So, this is the goal of the course, and in particular, I want to, he developed what we now call Group theory. So, Galois is usually considered one of the beginners of group theory as we study today, so, he did not really use these words, but he developed a lot of what we now study as Group theory. As we studied today, to solve this question, he developed group theory and a lot of other important and beautiful notions.

And the approach towards Galois theory nowadays, following work of lot of mathematician including Emi Latina and so on is through fields. So, we are going to study Galois theory as a study of field extensions. So, what I want to do in the rest of today's video, and in the beginning week, first three, four videos is to introduce the basic prerequisites for this course, which I will not dwell in at length, but quickly recap the key notions that we use before we start studying Galois theory in more detail.

(Refer Slide Time: 23:02)




So, the key prerequisites for studying and in fact, as we now study any algebra sequence in undergraduate or master's courses. We do this in the, in this following order. So we first do Group theory, which as I commented earlier, really started with Galois work to solve this question. Ring theory. And then we finally will need Field theory, because Galois theory is real, Galois theory is really a continuation of Field theory.

And as you can see any sequence of Algebra courses in any program usually start with Group theory, then Ring theory, and Field theory. We do not need all the concepts that we learn in a full

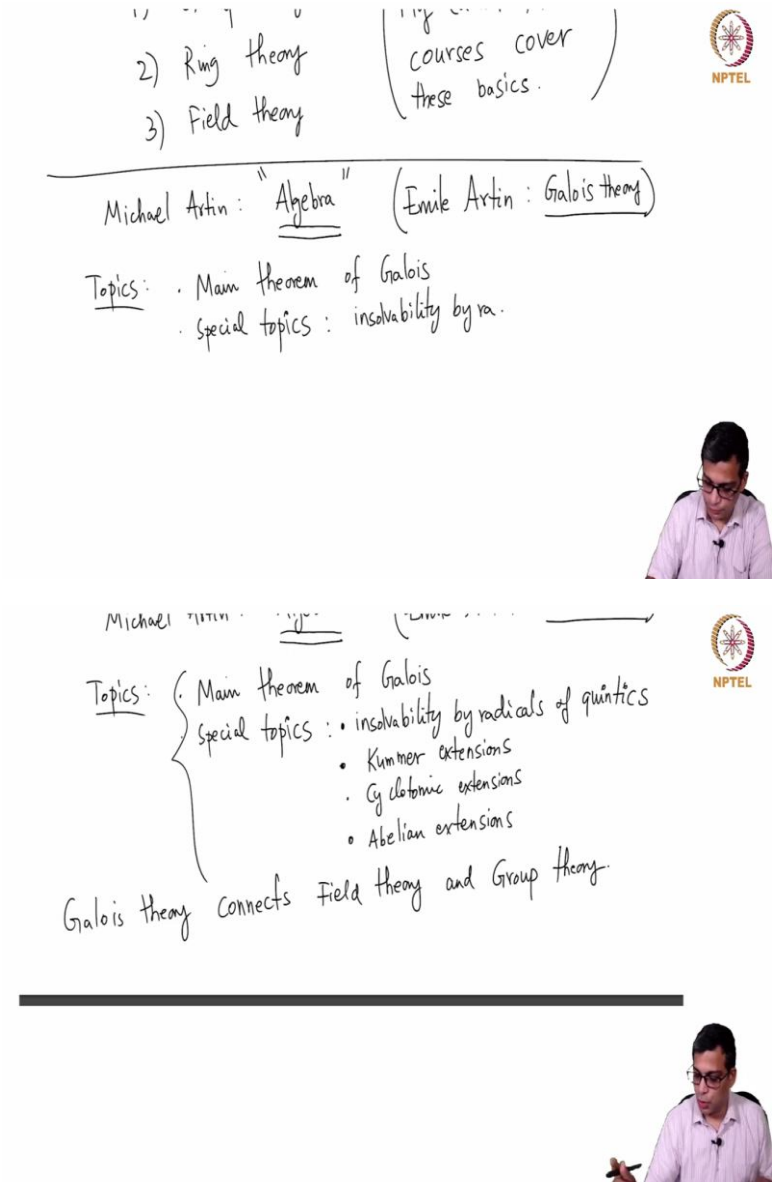
fledge course on any of these subjects. Certainly not one and two field theory is, of course, very critical. So I am going to spend first few videos of this course recalling the key concepts and as we go along and start learning Galois theory.

I will come back to important notions though I may not be able to prove the relevant factors because there is not a course on Group theory, Ring theory or field theory. But always revise them enough so that you can understand what I am doing in the course. So these can be learned from any standard books in algebra. And in particular, I have taught earlier, some courses on NPTEL.

So, I did one course on Group theory and one course on Rings and Fields, cover these basic, these basics. So one option for you is to go through those, but as I said any other source and in fact, I am going to list some of the important topics that we do need. So, the course will be structured as follows. In the first few videos, we will learn about the key concepts in Group theory, Ring theory, Field theory that we are going to use repeatedly, so I am not always explain them, but I will do once recall the basic notions and then we will keep using them without further explanation.

That will take me most of the first week and then we will get to Galois theory proper and the course will be eight weeks long. And every week at least once I will do a problem session where I will give you exercises and work them out in detail. Because one way to in fact, the only way to learn mathematics is to work on lots of exercises, which I want you to do a lot. So as a training for you, I will just do some basic problems, give you problems and solve them in my videos and you should build on that and solve lots and lots of problems.

(Refer Slide Time: 26:07)




The basic reference that I want to use is the book of Michael Artin. As we go along, I will mention some other courses, other books, Michael Artin's Algebra, it has comprehensive introduction to basic algebra, including the prerequisites group theory, ring theory, field theory. And I will mainly use the chapters on Galois theory in his book also. Michael's father, Emil Artin, has wonderful notes on Galois theory, wonderful little book, which I will also occasionally use.

These are the basic references and in fact, Galois theory is such a basic subject that any basic algebra book will cover it. So you are welcome to look at various books and as we go along, I

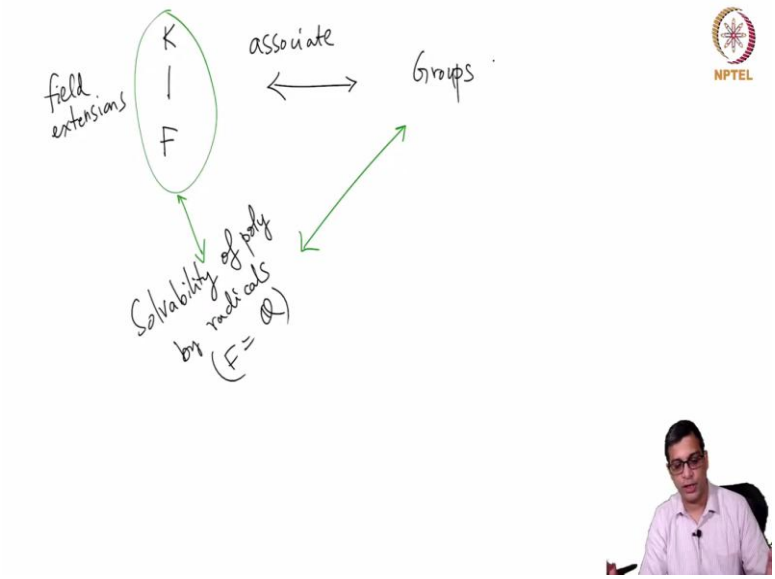
will mention some of them and solve exercises from all these books. So the main topics that we will cover are, so there is something called main theorem of Galois theory. It will take us some time before we get to this main theorem of Galois theory. This is one of the highlights of the course. And then we will do topics like special topics like which is the motivation I mentioned at the beginning of this video insolvability by Radicals, Insolubility by radicals of Quintics.

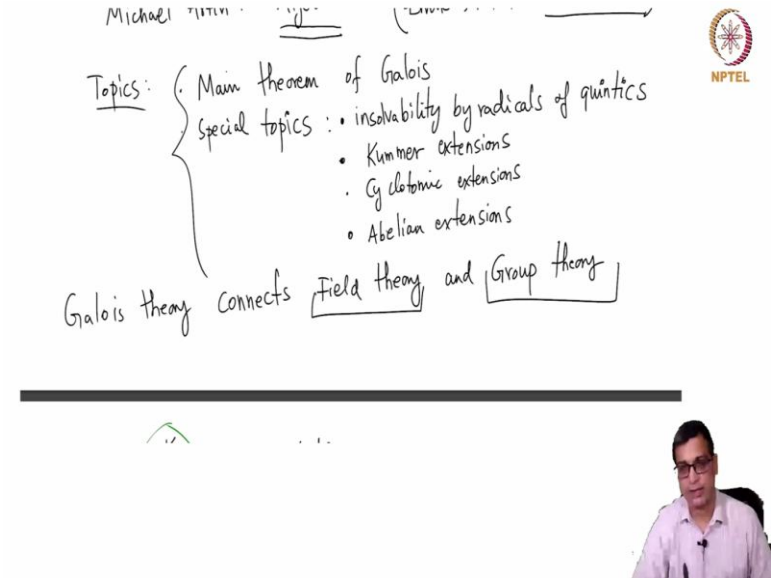
I will talk about what are called Kummer extensions, Cyclotomic extensions and Abelian extensions. So, as we go along, I will define all these things, it will take some time before we come to this, but I wanted to give you a basic preview of the topics. This is not an exhaustive list, but these are some of the topics that we are going to study.

So, just to recall beginning week, first few lectures, we will do recall revision of the basic ingredients of this course, which are Group theory, Ring theory, Field theory. Before After that will get into the heart of the topic and introduce the Notions of Splitting fields, Fixed fields, and then get to Galois theory. And then we will do some basic and important applications of Galois theory.

So, in the remaining one or two minutes, I want to summarize what Galois theory is, Galois theory essentially connects what we now call Field theory and Group theory and what we now call Group theory. So, the goal of the Galois theory or the methods of the Galois theory function by connecting these two topics. So, we want to Galois Field theory and Group theory.

(Refer Slide Time: 29:21)



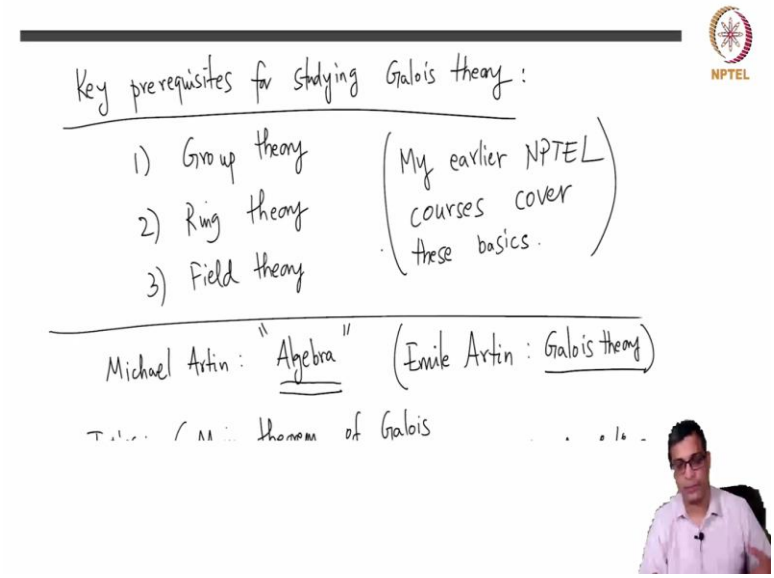




So, given the field extensions, given field extension like this, so, this is a Field extension, I will recall these notions in a few lectures, we want to associate groups. So, for Field extensions will be associated to groups in order to understand Field extensions. We are going to associate a group and understand groups and we are going to connect this, so we are going to connect this side of the picture to solvability by of polynomials.

So, this is the connection that typically we take F to be Q or some extension of Q. So, and then there will be connection to the side. So, whether a polynomial solvable by radicals or not will be a property of the field extension at the same time it will be a property of the group. And then

putting all this together we answer the that Galois answered that quintics cannot be solved by radicals and then developing further we are going to study all the other topics that are listed here. And the emphasis of the course will be to solve lots of problems it will be very hands on so every week at least one video will be purely problem solving.

(Refer Slide Time: 31:00)




And then I will give lots of examples throughout the course. And recall all the notions that we use to keep the course as self contained as possible. So, let me stop this video here. In the next video, we are going to start revising the basic notions of Group theory, Ring theory and Field theory. Thank you.