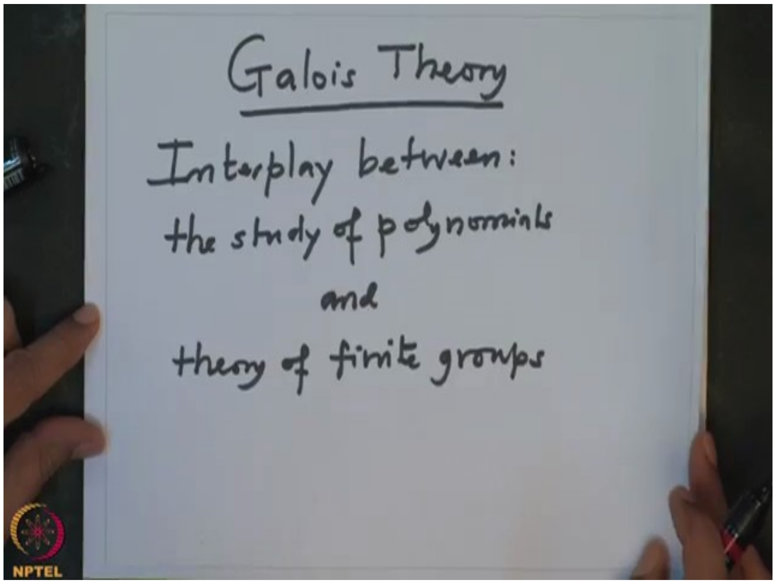
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 01 – Historical Perspectives

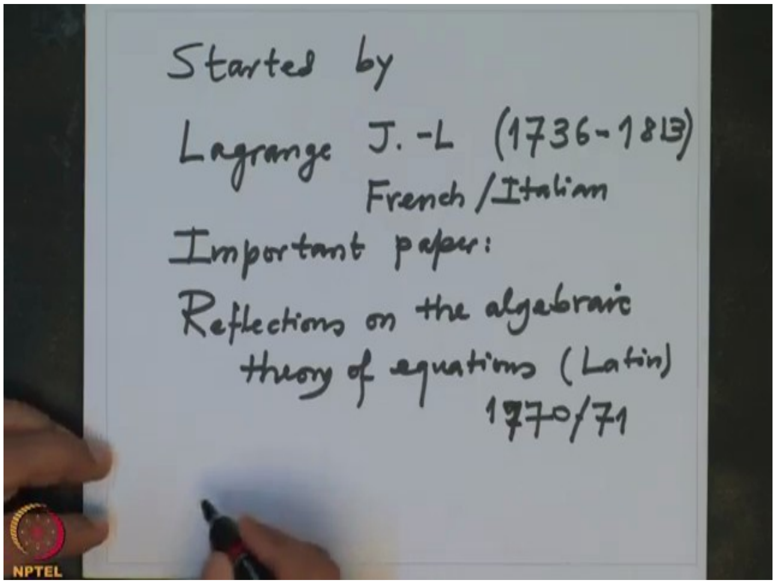
My name is Dilip Patil. I am from the department of mathematics, IIT Bombay. And actually originally I am from Indian Institute of Science, at present on the sabbatical leave from IISc.

(Refer Slide Time: 0:52)



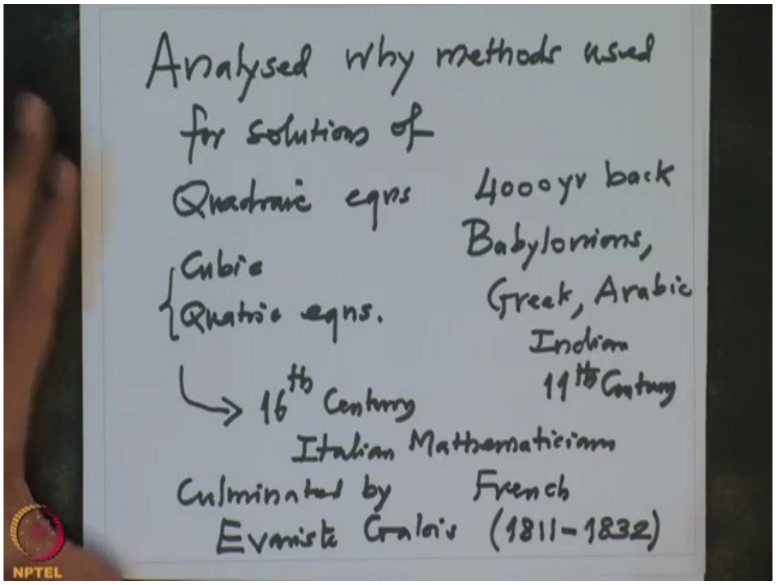
This is a course on Galois Theory. First let me briefly recall what the subject is about and what are the main contributors to this subject and then we will eventually go on to the details of the topics. So Galois Theory is an interplay between the study of polynomials and theory of finite groups. The subject is very old and it has taken many stages to go on. Now it has taken modern viewpoint and it has grown so much that we need many more courses on Galois Theory actually. But this is the first course on Galois Theory. So I will begin from the beginning really.

(Refer Slide Time: 2:54)



So it is systematically started by Lagrange, Joseph Lagrange. This was 1736 to 1830, he was a French-Italian mathematician and started with very important paper which is titled as Reflections on the Algebraic theory of equations. This is actually written in Latin, published in 1770-71.

(Refer Slide Time: 4:40)



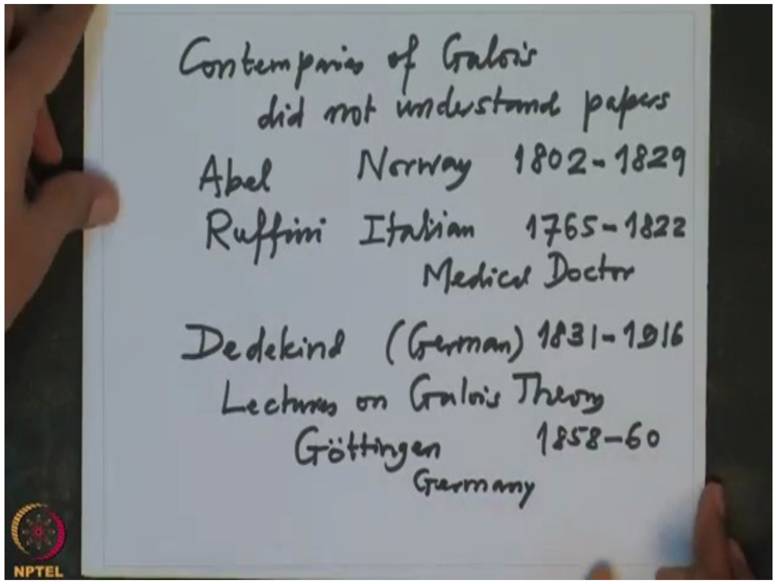
Lagrange analyzed the earlier methods, so he analyzed why methods used for solutions of quadratic, cubic and quartic equations. Actually the history of quadratic equations is very old, it is, it started with more than 4,000 years back. It started with Babylonians, also Greek, Arabs, Arabian Mathematics, and of course Indian. There is a very long history. I will recall briefly when I have the right time to do so. Right now I will only say that Babylonians look for the solutions of the quadratic equations in very particular cases.

And it was finally completed by the Indian mathematics by Brahmagupta in 11th century. And nowadays we learn these methods in school. I will recall it when I have enough time. Just now today's lecture I am going to just brief about the subject, how it progress. So cubic, so this was cubic and quartic equations solutions, there were only solved in 16th century by Italian mathematicians. And finally this was culminated by Évariste Galois which was a French genius boy actually. He died very young, 1811 to 1832.

And his whole theory is named after him because he really finished, he answered these, all these questions which ancient people were doing in a very satisfactory way. Galois was a French. But in all this process there was one thing which was not very satisfactory, namely the notations, definitions and way of expressing the results were very classical. And among various mathematicians there was lot of confusion.

And therefore in this course what I will do is I will uniformize all the notations, definitions and so on. I will use very modern language so that the participants of this course also can read further other courses. And at the same time I will keep telling in between the history and also the classical results. But my methods of proofs will be the algebraic. Okay. So more comments about this when, before we start actually formally writing down the notations and so on.

(Refer Slide Time: 9:53)



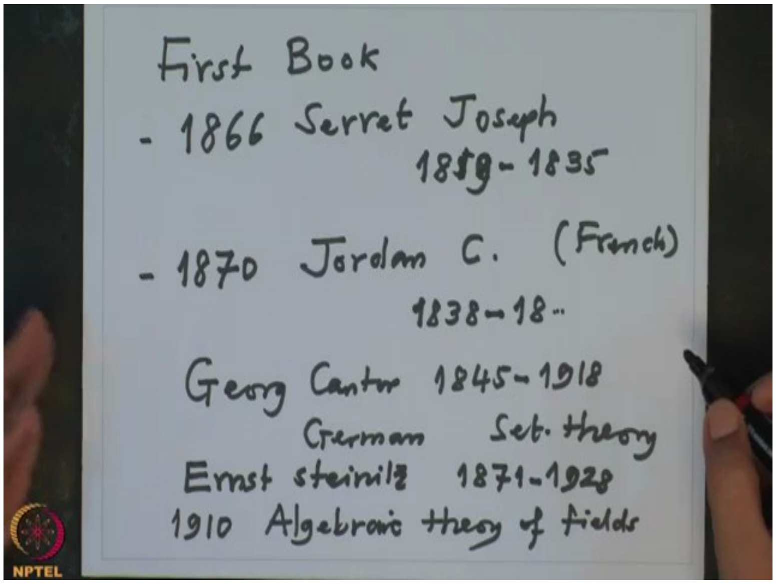
I will also mention what kind of prerequisites I will assume in this course. For example, the Galois Paper which appeared in 40 years later after his death because of so many, because essentially contemporaries of Galois did not understand his papers, so people have realized only after 40 years that what kind of papers are there and what kind of impact it has done on the mathematics.

Of course at the same time I should also mention that Abel and Ruffini, Abel was a Norwegian mathematician. He also died very young, it is 1802 to 1829. He died because of tuberculosis. And Ruffini was Italian, year 1765 to 1822. He was actually a medical doctor and in his spare time he was doing mathematics. And these two people, they were before Galois. They essentially changed the mindset of the people.

They started giving the different direction to the subject. And before them for example, Lagrange and others, they were actually trying to prove that one can solve the equations of arbitrary degree. This term which I use is solve the equations of arbitrary degree, this is somewhat still not very clear and vague. But I will make things soon precise

So Dedekind, so the real modern era of Galois Theory, it starts with Dedekind. He was a German mathematician, 1831 to 1916. He was the first to give lectures on Galois Theory. This was during 1858-60. This was in Göttingen, this is one of the old university in Germany. This is also known as Mecca of Mathematics.

(Refer Slide Time: 13:20)



And the first ever book published on the Galois Theory, first book that was by French mathematician, this was published in 1866 by Serret Joseph. This was a French mathematician, 1819 to 1835. Also soon after this there was a book again by French mathematician, 1870, this is Jordan C., French. This was 1838 to 18, I do not know the year here. But this book is very, very interesting. Jordan has developed lots of linear algebra for studying Galois Theory, it is very very important. That is where he has also proved Jordan canonical form, which is usually taught in any algebraic courses.

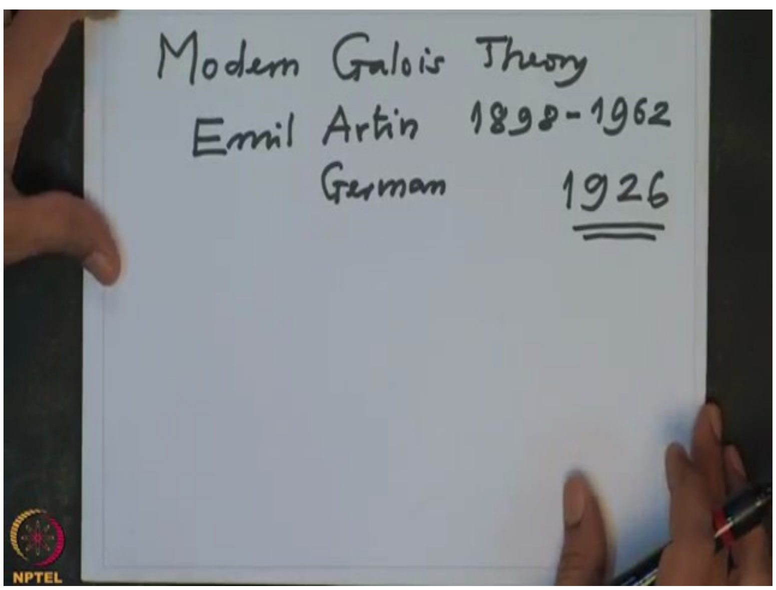
And it is very interesting to note that, Jordan actually proved Jordan canonical form for finite fields. Whereas today's curriculum about linear algebra, now one usually proves it for complex numbers. And one does not mention it for finite fields, what to do, what is the replacement for the finite field. But nowadays present applications of mathematics to the engineering side and also the digital technologies and so on, finite fields are very very important object to study. And you will see in this course also we will do finite, Galois Theory of finite fields as well.

All this still comes under the classical aspects of Galois Theory. The real one which started by Dedekind, it happened so, the main hurdle was the development of the Set Theory. And nowadays Set Theory is the medium of instructions, Set Theory is the language of mathematics. So without Set Theory one cannot study mathematics at all. And I just want to mention that Georg Cantor, 1845 to 1918, was a German mathematician and he had done the Set Theory very rigorously and today it is used without saying much with, all the mathematics courses assume Set Theory.

But again contemporaries of Cantor did not accept lot of, proposed theory and he was attacked by many mathematicians. He had to even spend 8 to 10 years of his life in hospital. So after Georg Cantor's Set theory when it was done, then another young mathematician, Ernst Steiner, German again, 1871 to 1928, he has written in 1910. He has written one very important paper, Algebraic, I will write in English, Algebraic theory of fields.

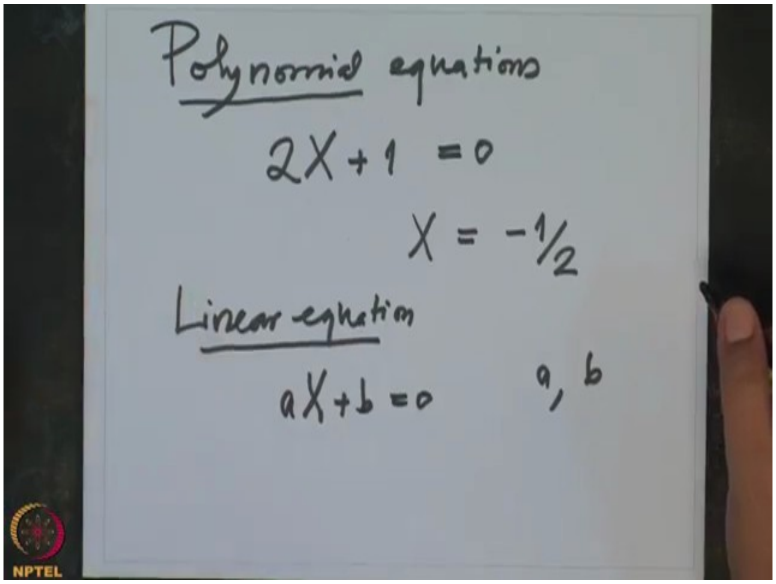
This paper is essentially, one can say this is the beginning of Algebra in a very precise way. And this paper also gave more examples of fields. Soon I will come to the examples of fields. This paper provided abstract platform for studying fields. And he has converted lot of classical earlier results in a modern way and this is very very important reference.

(Refer Slide Time: 18:58)



Now finally the modern incarnation of Galois Theory, this is very modern. That started by Artin, 1898-1962. He was also German mathematician originally but because of, after the war he had to go to US. There was trouble in Germany, so he migrated to America and there he had modernized this Galois Theory which was, which is abstract. And many classical results he proved in a different, more elegant methods. So this was, this happened around 1926.

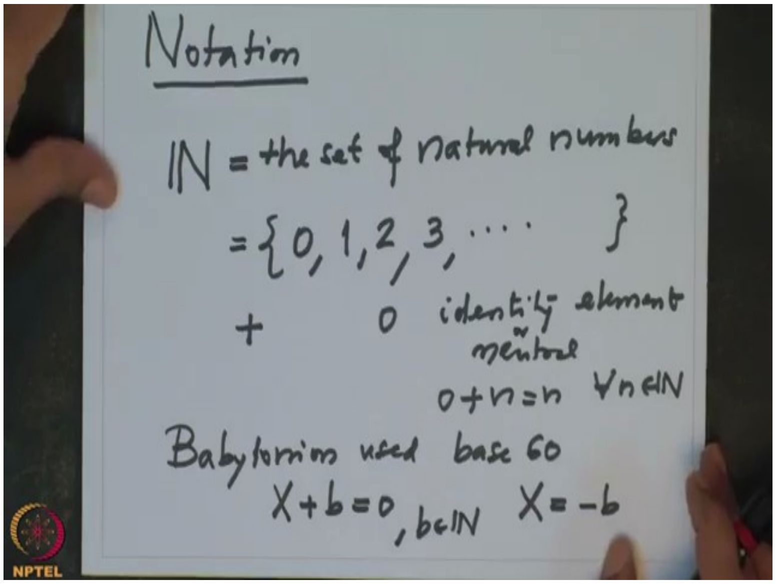
(Refer Slide Time: 20:31)



So now I will slowly start, so what is the problem? As many of us know that lot of problems in our daily life, one can formulate them in terms of equations and solve the equations. So what does one mean by equation? So in this we are only, in this course we are only considering polynomial equations. Polynomial equations, so something like this: $2X+1=0$. And we are looking for a solution. That means we want to solve for X. In this case, $X=-1/2$. This is the only solution.

This equation is a polynomial equation and the highest degree of X appearing is called the degree of the polynomial equation. For $2X+1=0$, the degree of $2X+1$ is 1, so it is also called a linear equation. So, it is clear from this example how do we solve the general linear equations. General linear means $aX+b=0$, where, a and b are where? See normally in the formal days in the historically they did not mention where the coefficients are but it was always assumed that they are natural numbers. And later on when time progressed, later on then, we say integers, later on rational numbers, then real numbers, then complex numbers. So this was a hierarchy I want to mention.

(Refer Slide Time: 22:11)



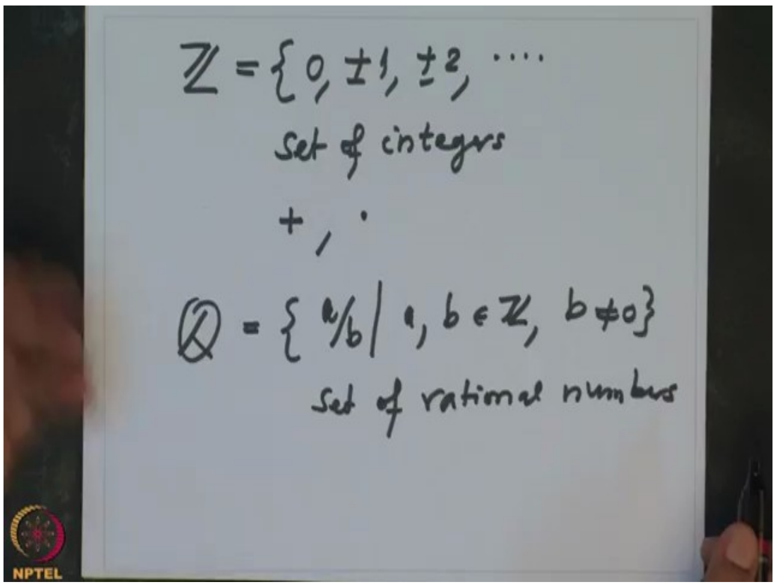
And I will also make this opportunity to, take this opportunity to introduce some notation. So throughout this course I am going to use this notation. So this is $\mathbb{N}$, the set of natural numbers. So this was started with a counting. When human being started counting, people knew how to count but still there were controversies. Like for example, even today in the school books usually it is said 1, 2, 3, et cetera. That is the set of natural numbers. It started with counting. Somebody has one object, somebody has two. But also one should mention that 0 is also natural number.

And particularly in India, actually 0 is an invention of Indians and that is very very important. I will keep showing in this course that it is very important to say 0 is a natural number. Because with that notation, the usual addition what we learn in the school is, 0 is an identity element for that addition, a neutral element. That means when you add 0 to anybody, that quantity does not change. 0+n=n, for every $n \in \mathbb{N}$.

And that is one of the reasons when Babylonians were trying to solve quadratic equations, they had lot of trouble. And another comment I want to make here is nowadays whole world is using decimal system to denote the numbers. In Babylonian time they were using base 60, so Babylonian used base 60 for calculation. That is also little bit more complicated but that time it was very practical.

And one can see one example where base 60 is used in the calculation, is our analog watches uses base 60, that is where we have every hour has 60 minutes and every minute is 60 seconds and so on. But as I said, now the whole world is normalized to use, stabilized to use the decimal system. So the set of natural numbers is this. And if you have equation or natural numbers like this: X+b=0, then what is X? X=- b. That is where it was felt that if you want to solve linear equations, you need to enlarge the set of natural numbers to the integers.

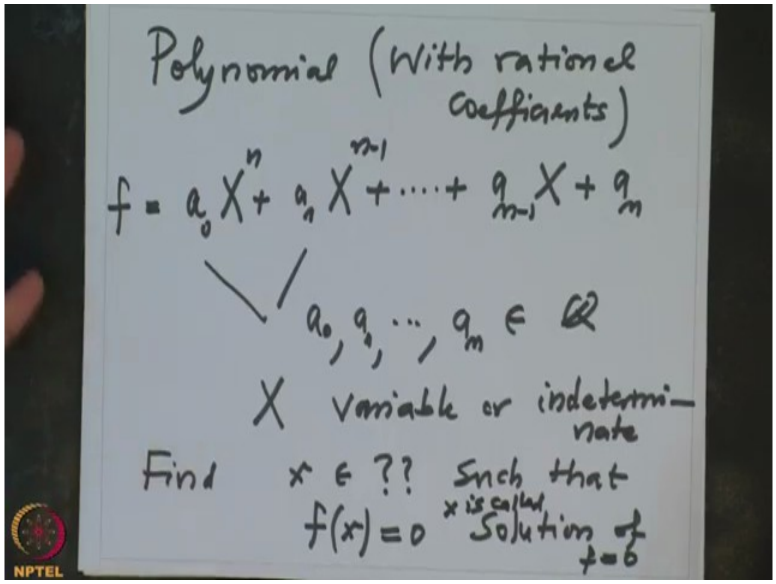
(Refer Slide Time: 25:39)



And that is where we have now the set of integers, $\mathbb{Z}=\{0,\pm 1,\pm 2,...\}$. So this is the set of integers. This set has two operations, + and $\circ$, even the natural numbers has two operations, + and $\circ$. $\mathbb{Z}$ has also has addition and multiplication. And then whole school, up to elementary school we study the properties of natural numbers, integers, and also the rational numbers.

Rational numbers now add fractions, so they are of the form, $\frac{a}{b}$, where a, b are integers and b is non-zero. This is a set of natural numbers, a set of rational numbers. So when in former time, when people were trying to solve equations, polynomial equations, solve means finding the zeros, or finding their solutions, then one usually assumed that the coefficients we are taking are from rational numbers.

(Refer Slide Time: 27:07)



So typically when I say polynomial with rational coefficients, this typically mean an expression like this: $a_0 X^n + a_1 X^{n-1} + \ldots + a_{n-1} X + a_n$. This is a polynomial equation where $a_{0,} a_1, \ldots, a_n \in \mathbb{Q}$. And this X is called variable or indeterminate. And one want to solve the equation, means find their zeroes. So if you call this as f, then we wanted to find x, where in earlier days it was not mentioned very explicitly, such that when f(x)=0.

That means when instead of X when I put x, then it should become 0. These are called solutions of f, so then x is called a solution of f equal to 0. x is called solution of f(X)=0. And there may be many solutions. Then the question comes how many equation, how many solutions and how do we find and are there formulas and so on. So this was a classical one. Then when the time progressed, so now the next, after the break I will tell more about this, what happened in the progress. Thank you.