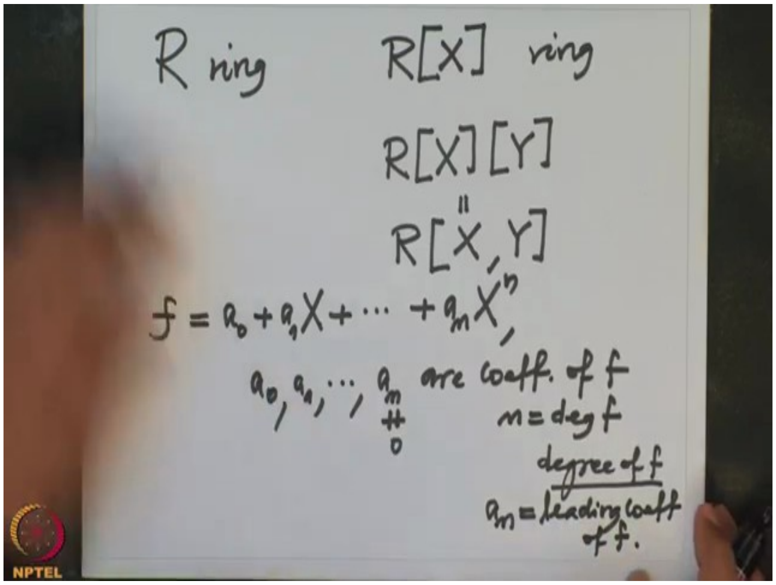
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 04 – Polynomial Rings

Welcome back to this second half of this lecture on the polynomials. Last half I have defined what a polynomial ring over a ring is. And I will continue with some basic properties of the polynomials which we will keep using in this course. I will still be little briefer and faster because in principle what I am doing now is a prerequisite for this course.

(Refer Slide Time: 1:04)



R ring R[X] ring

$$\begin{array}{c} R[X][Y] \\ \| \\ R[X,Y] \end{array}$$

$f = a_0 + a_1 X + \cdots + a_n X^n$,

$a_0, a_1, \cdots, a_n$ are coeff. of f

$a_n \neq 0$ $n = \deg f$

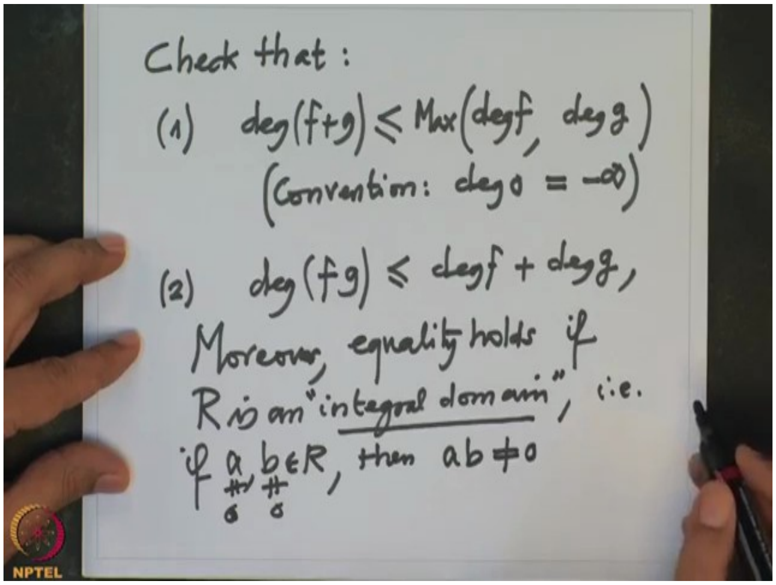
<u>degree of f</u>

a_n = leading coeff of f.

So remember we have a ring R and we have constructed a new ring R[X] called polynomial ring in, over R, or polynomial ring in one variable over R. And actually we can repeat this process. So we can, now we can take this ring R, R[X], polynomial ring and then we can consider a polynomial ring over this ring in the second variable Y. But this is same thing as a polynomial ring R[X,Y] now in two variables over R.

And this way we can construct polynomial rings in many number of variables. So note that for each polynomial f, this a_i are called the coefficients of f, $a_{0,}a_{1,}\cdots,a_n$, are called coefficients of f. And when this a n is non-zero, this n is called the degree of f, this is denoted by deg f, degree of f. And this coefficient a_n is called a leading coefficient of f. So important thing to note is immediately the formulas for the degrees.

(Refer Slide Time: 3:00)



Check that :

(1) $\deg(f+g) \leq \mathrm{Max}(\deg f, \deg g)$

$(\text{Convention: } \deg 0 = -\infty)$

(2) $\deg(fg) \leq \deg f + \deg g$,

Moreover, equality holds if R is an "<u>integral domain</u>", i.e.

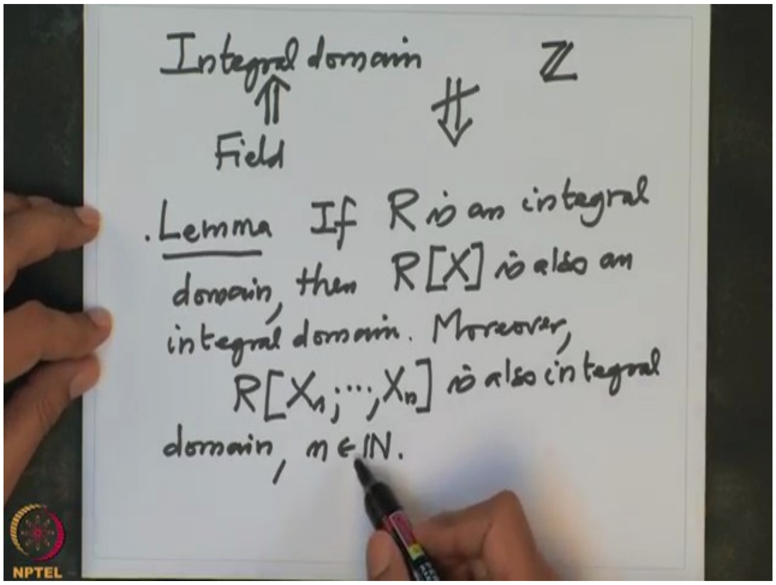
if $\underset{\neq 0}{a}, \underset{\neq 0}{b} \in R$, then $ab \neq 0$

So for example, what happens, when I add two polynomials, what happens to their degrees? So I will only say check, I am going to prove this, but check that. 1, if I take f and g, two polynomials and then look at the degree of f+g, that is less equal to degree f, degree g and take their maximum. Remember less equal to, it is not equal, it is less equal to because I could take f equal to -g.

And then this will become, is not defined. So some people define also let us say for its convention, it is defined but make a convention that degree of a zero polynomial is - ∞. And you will see why this $-\infty$ and why not - 1. Why this convention is made? Because of the following second formula: the second formula is very very important. Degree of the product is less equal tot degree f + degree g.

Moreover, equality holds if R is an integral domain. What is an integral domain? Integral domain is a ring which is free from 0 divisors. And what is 0 divisor? That means, so that is, I will just spell out, that is if a and b are two elements in R, both are non-zero, then their product ab is also non-zero. Then it is called an integral domain. For example, field is always an integral domain.

(Refer Slide Time: 5:40)



Integral domain $\Uparrow$ Field $\not\Downarrow$ $\mathbb{Z}$

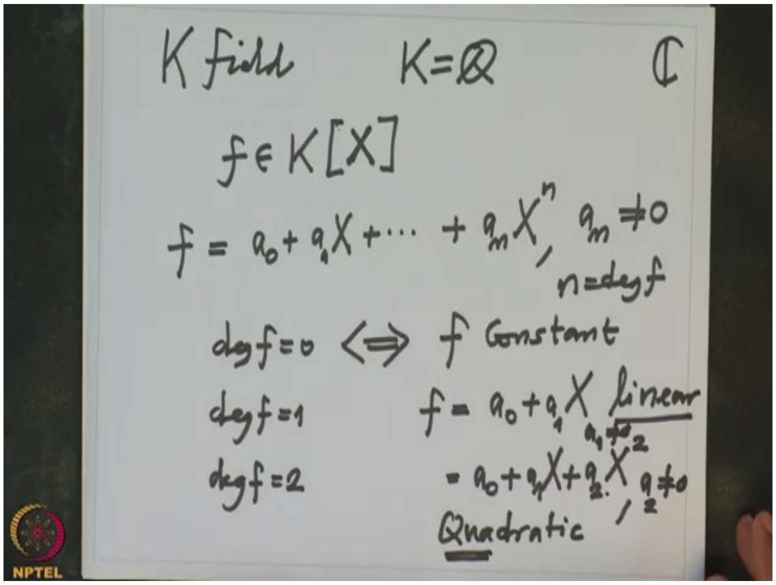
. Lemma If R is an integral domain, then $R[X]$ is also an integral domain. Moreover, $R[X_1, \cdots, X_n]$ is also integral domain, $n \in \mathbb{N}$.

So for integral domain, degree of the product equal to sum of the degrees. So integral domain field, fields are integral domain. Field implies integral domain but obviously not this way. Because we have an example here, integers, ring of integers. This obviously is an integral domain. It is the two integers if I take non-zero, their product is also non-zero. But it is not a field, $\mathbb{Z}$, it is not a field.

So there are many examples of integral domain which is not a field. In fact, one simple observation I will note here. If R is an integral domain, then the polynomial ring R[X] over R is also an integral domain. This is very important fact. We will keep using it. And nothing special about one variable, I could repeat this argument. So moreover, $R\left[X_1,\ldots,X_n\right]$ is also an integral domain for any n in natural numbers.

And actually not necessarily for rational numbers. But anyway I will not need it in this course. Even if you take polynomial ring in many many variables, number of variables could be also uncountable and so. That will also be an integral domain because any polynomial will involve only finitely many variables. And therefore if you have two polynomials, they altogether will involve finitely many variables. But ultimately therefore argument will come down to the polynomial ring over R in finitely many variables. So that is one.

(Refer Slide Time: 8:28)



K field $\quad K=\mathbb{Q} \quad \mathbb{C}$

$f \in K[X]$

$f = a_0 + a_1X + \cdots + a_nX^n, \; a_n \neq 0$

$n = \deg f$

$\deg f = 0 \iff f$ Constant

$\deg f = 1 \quad f = a_0 + a_1X$ linear

$a_1 \neq 0$

$\deg f = 2 \quad = a_0 + a_1X + a_2X^2, \; a_2 \neq 0$

Quadratic

So we are going to take a field. So K is a field and ancient day it was taken K to the ℚ. This was when Babylonians or, Babylonians did not even take ℚ, they only took natural numbers. So let us say in reasonable time, that is 16th century that people took ℚ. They did not even know complex numbers correctly.

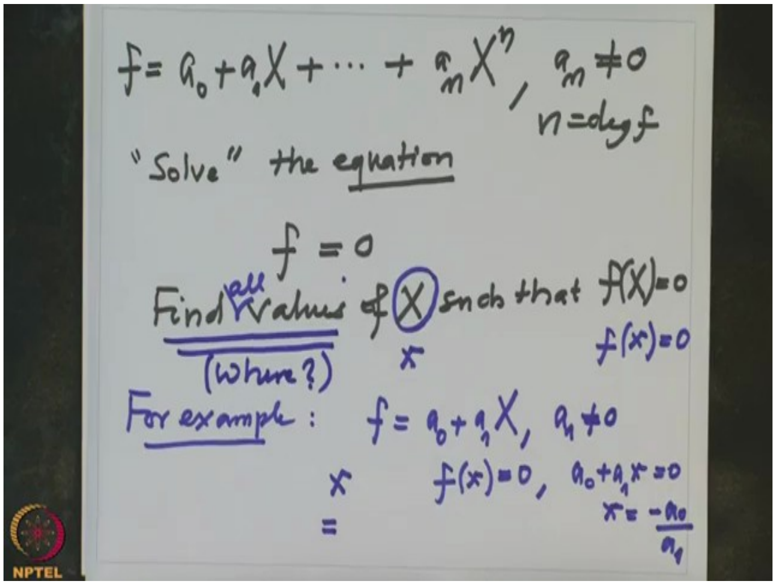
So take ℚ and then we would take a polynomial. So we are considering the polynomial over a field. So I will keep writing general field but specialized to this strength. So I have this polynomial ring over K in one variable. So elements of these are precisely the polynomial with coefficients in K. So f is a polynomial. So f will look like $a_0+a_1X+...+a_nX^n$. And this a n is non-zero. And this n is therefore the degree of f.

So the simplest one obviously the constant polynomial. So that is all this has, so the degree is 0. Degree is 0, means precisely degree of f is 0 if and only if f is a constant polynomial. So this only, there is nothing to, nothing much to study in this. So if degree is 1, then we have, f will look like a_0+a_1X. So this is called a linear polynomial. Linear, this is, degree is 1. Degree f equal to 2, that will, f will look like $a_0+a_1X+a_2X^2$. This a 1 is non-zero obviously, here a_2 is non-zero.

So that is also called quadratic. Qua is 2. And degree 3 cubic, degree 4 quartic or biquadratic; degree 5, quantic; degree 6, sextic and so on. That is how the Greek started calling them. All these words also coming from Latin. So what was the problem?

The last time I saw that then we want to solve these polynomials. Solve this means what? Equate them to 0, and you get equation, so it is a polynomial equation. One should really say it is a polynomial equation. A polynomial, you cannot say, so this writing it was allowed in the formal days because the language was not so established. But as I said last time that created also lot of confusion among people and that led to many errors and so on.

(Refer Slide Time: 12:02)



$f = a_0 + a_1 X + \cdots + a_n X^n$, $a_n \neq 0$, $n = \deg f$

"Solve" the equation

$f = 0$

Find all values of $\boxed{X}$ such that $f(X) = 0$

x $f(x) = 0$

(Where?)

For example: $f = a_0 + a_1 X$, $a_1 \neq 0$

$x =$ $f(x) = 0$, $a_0 + a_1 x = 0$

$x = \frac{-a_0}{a_1}$

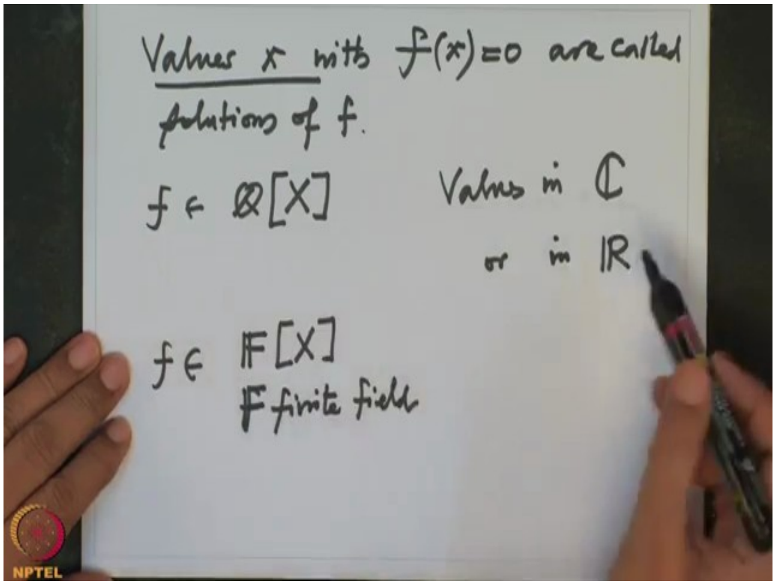
So if I have a polynomial of degree n, $a_0 + a_1 X + ... + a_n X^n$, a n is non-zero, so this n is the degree f. And then what are we doing? So we want to solve, again this is not so very precise, solve the equation. Now it is equation, f = 0. So what does that mean? That means in this expression, in this polynomial, all this $a_{0,} a_1, \ldots, a_n$, they are known quantities, they are given to you. And X is unknown. X is a variable, so it is unknown.

So when you say solve, means find all values of X so that this equality holds. Find, so find values of X such that f(X) equal to 0. Now I cannot write X because X is a variable. So I cannot, so instead of this when one writes, I could have used x. We will write like this. Find values of, find all values in fact, find all values of x such that when I write X=x, it is f(x)=0.

For example, suppose I have only linear polynomial, so that means my polynomial f is $a_0+a_1 X$. Then obviously the only x, so that f of x is 0, that is nothing but the only one value. That is, you see, last time you said, this means $a_0+a_1 x=0$. That means x equal to $\frac{-a_0}{a_1}$. So this was linear polynomial, so a 1 is non-zero. So therefore we are allowed to divide it by a_1. And not only that, that means you need actually a field. Because if I take a ring of integers for example, and a_1 is 2, then I cannot divide it by 2, then the solution, so this x is called a solution of f.

This x will be then out of $\mathbb{Z}$, so it is very very important when you say find all values where, where are you looking for values. This information is also very very important. So in former days, up to 16th century people have tried to solve of course, linear, quadratic, cubic and bi-quadratic and found the formulas for these values of solutions. So these values are called solutions of f. So let me write that also.

(Refer Slide Time: 16:11)



Values x with $f(x)=0$ are called solutions of f.

$f \in \mathbb{Q}[X]$ Values in $\mathbb{C}$

or in $\mathbb{R}$

$f \in \mathbb{F}[X]$

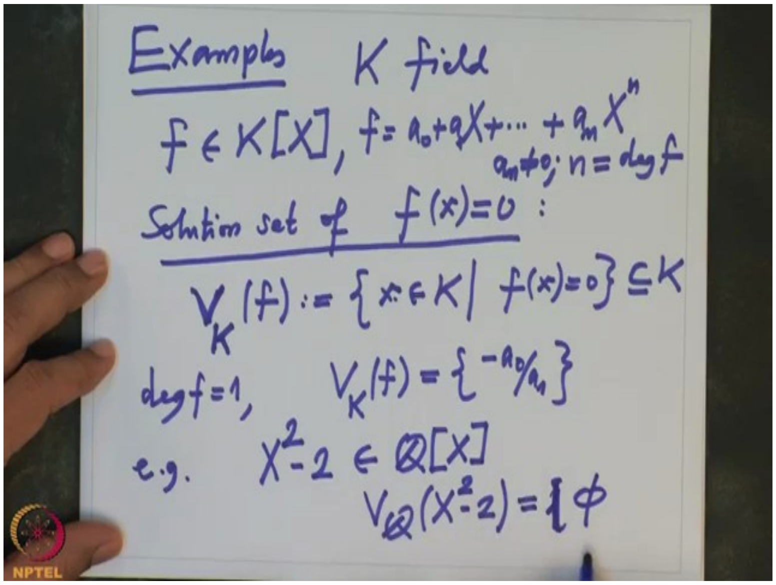
$\mathbb{F}$ finite field

So the values x with f(x) equal to 0 are called solutions of f. And now where are taking? So initially, formerly when, in the former days f were taken in the field $\mathbb{Q}$ with coefficients in $\mathbb{Q}$. Coefficients in $\mathbb{Q}$ were taken because we have realized that even taking coefficients in $\mathbb{Z}$ will not lead to solutions in general. So therefore, $\mathbb{Q}$ was the smallest possible field one could take that time and then the values we are taking in complex numbers $\mathbb{C}$. Values in complex numbers, they knew sort of complex numbers, what complex numbers are exactly, or sometimes real numbers.

But we need to specify when, where we were taking the values. And nowadays it is very very important in many engineering applications and many other science applications. They depend on the polynomial f, and coefficients are not in ℚ but over a finite field F, a finite field is double line F, the finite field. Then we are looking for solutions where? Again, so we are looking for solutions, this ℚ may not have, we will, I will, immediately after this I will give some examples.

Given polynomial, there may not be any solution in ℚ. So again the same problem. So we have to enlarge. So that means we have to consider a bigger field. Bigger field means you are extending the operations of plus and multiplication so that it become a field and same operation. So it is a subfield. So let us see some examples first and then we will come back to general theorem.

(Refer Slide Time: 18:41)



Examples   K field

$f \in K[X]$, $f = a_0 + a_1X + \cdots + a_nX^n$
$a_n \neq 0$; $n = \deg f$

Solution set of $f(x) = 0$:

$V_K(f) := \{x \in K \mid f(x) = 0\} \subseteq K$

$\deg f = 1$, $V_K(f) = \{-a_0/a_1\}$

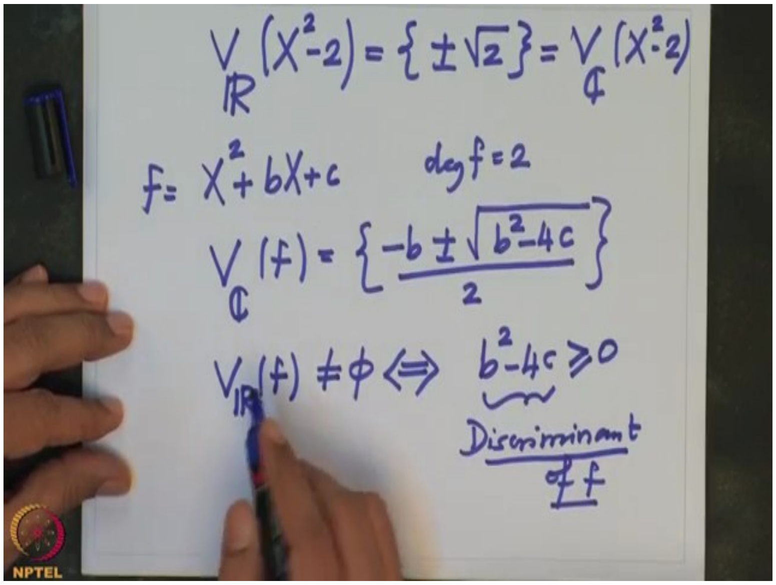
e.g. $X^2 - 2 \in \mathbb{Q}[X]$
$V_{\mathbb{Q}}(X^2 - 2) = \{\phi$

So examples. So first note that linear polynomial, there is nothing much, there is only one solution and that solution is in the base field. Now that is how I will, through examples I will also develop a language. So K field and we have a polynomial f in K[X]. Now solutions of, solution set of f(x) = 0, where, so first of all I will say V_K, this is by definition all those elements $x \in K$ so that x is a solution of f. f(x) = 0.

Remember this is a subset of K. So f were a linear, degree f = 1, then I know this precisely. V_K (f) is precisely only one element, namely $\frac{-a_0}{a_1}$. This is only one solution, exactly one. So where remember f we have written like this: $a_0 + a_1 X + \ldots + a_n X^n$. n is equal to degree of f. So that means a n is non-zero. Now even for degree 2 let us see.

If you take, for example if you take a polynomial like this, $X^2 - 2$, think of this as a polynomial with rational coefficients, and what are the solutions? V Q of this, this already you learned in the school. That means X is $\pm\sqrt{2}$. So this means, what is this? Then we have learned in the school that $\sqrt{2}$ is not rational. That means there is nobody in this. So this is empty set. This is empty set. So again, that means this polynomial does not have rational solution.

(Refer Slide Time: 21:46)



$$V_{\mathbb{R}}(X^2-2) = \{\pm\sqrt{2}\} = V_{\mathbb{C}}(X^2-2)$$

$f = X^2 + bX + c$ deg f = 2

$$V_{\mathbb{C}}(f) = \left\{\frac{-b \pm \sqrt{b^2-4c}}{2}\right\}$$

$$V_{\mathbb{R}}(f) \neq \phi \Leftrightarrow \underbrace{b^2-4c}_{\text{Discriminant of } f} \geq 0$$

But then we, where do the solutions are there? So obviously, they are all real solutions. $V_{\mathbb{R}}(X^2 - 2) = \pm\sqrt{2}$. They are real solution, and therefore they are complex solution also. This is also same as $V_{\mathbb{C}}(X^2 - 2)$, the complex solution. So therefore it is very very important where are we looking for solutions. And mainly, most, many times we do not have solutions in the base field. So we try to enlarge the field to the bigger field and so on. So this is what we will do.

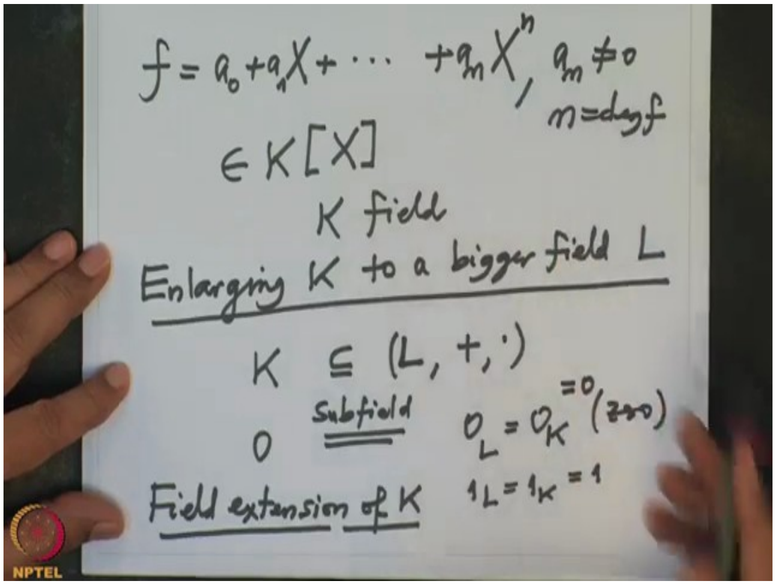
Now in this case, solutions are this $\sqrt{2}$. So that means, and where do this root 2 came from? It came from this 2. More generally, if you take equation like this, quadratic equation like this, $X^2 + bX + c$, this is f, this is degree 2, so that means the f is quadratic. And we have studied in the school that $V_{\mathbb{C}}(f) = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$. This may be real or maybe complex.

But definitely they are complex solutions. So one learns, and then one can also write when will $V_{\mathbb{R}}(f)$ will be non-empty, that if and only if the quantity here under the square root, it should be positive. So b^2-4c should be positive, non-negative. This is called the discriminant of f. And as you see there is nothing special about defining discriminant of a degree to polynomial. I will soon define discriminant of an arbitrary polynomial.

So when the discriminant is non-negative, it has a real solution and in fact both are real solutions. So in fact, in this case also there are two solutions in general. One may be repeated. Now you see all kinds of questions are cropping up. For example, given a polynomial of degree n, how many solutions are there even when you enlarge the field and how many distinct? So all these things in next few minutes I will try to summarize.

So first of all, note that all our efforts in this course will be very very down to the earth and mainly they will involve polynomials. And sometimes we make the abstract definition but ultimately we will have to come back to the concrete examples.

(Refer Slide Time: 25:09)



$f = a_0 + a_1 X + \cdots + a_n X^n$, $a_n \neq 0$
$n = \deg f$

$\in K[X]$

K field

Enlarging K to a bigger field L

$K \subseteq (L, +, \cdot)$

0 Subfield $0_L = 0_K \overset{=0}{} \text{(zero)}$

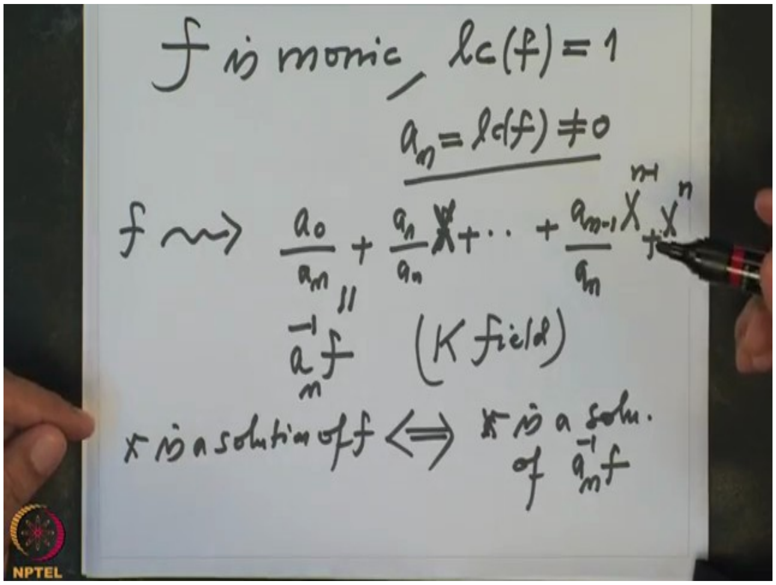
Field extension of K $1_L = 1_K = 1$

So if you have a polynomial $f = a_0 + a_1 X + ... + a_n X^n$, this is an arbitrary polynomial of degree n. And as we have seen also as the degree grows, finding the solutions as well as their analysis, how many are there and some may be repeated like in case of the earlier example, they may be repeated when the discriminant is 0 and so on, so all this analysis is very very important for our study. So as far as, so this is a polynomial over a field K.

So when we say enlarge, enlarging, so K is a field, enlarging K to a bigger field which I will denote usually by L, what does that mean? This means we have this given field K, you look at the bigger field L, so that this K is a subfield. See the subfield means that the same operations which are here of plus and dot, same operations are inherited to K. So in particular 0, which is a neutral element for 0, addition, is also the same 0 here. So that means we can write $0_L = 0_K$. Here is 0. Similarly $1_L = 1_K$, this is usually denoted by 1.

So therefore we will not have confusion. And such a thing is called a field extension of K. So K is a field and field extension of K. And then we are given a polynomial f, we are looking for its solutions in this L. Or even, so the biggest possible so that f has a solution. Now to do this, first of all I want to reduce the problem that we can always assume this polynomial is monic. So what are, for doing this what are all we assume?

(Refer Slide Time: 28:01)



f is monic, $lc(f) = 1$

$a_n = lc(f) \neq 0$

$$f \rightsquigarrow \frac{a_0}{a_n} + \frac{a_1}{a_n} X + \cdots + \frac{a_{n-1}}{a_n} X^{n-1} + X^n$$

$$\parallel$$

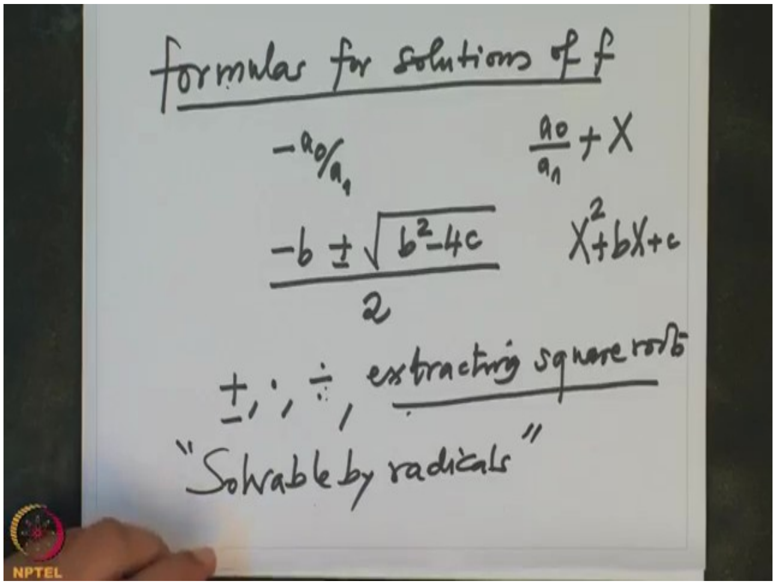
$$a_n^{-1} f \quad (K \text{ field})$$

x is a solution of f $\iff$ x is a solu. of $a_n^{-1} f$

That f is monic. That means the leading coefficient lc(f) of f is 1. And how can you achieve that? I know that a n is non-zero. n was the leading coefficient. a n, this is non-zero we know because n is a degree. And I replace f by the new polynomial $\frac{a_0}{a_n} + \frac{a_1}{a_n} X + \ldots = a_n^{-1} f(X)$. So the coefficient has become 1 now. I have divided by a power n. Simply means that I have multiplied by inverse a_n to f. And this is our new polynomial. So this is very easy because of the coefficient.

So that is where I use the fact that K is a field. So a n inverse exist because it is a non-zero element. And therefore, we can always assume for our purpose. So if x is a solution, x is a solution of f, if and only if, wherever that x is, x is a solution of a n inverse f. So we can always assume for this. But remember this we can only do it when where coefficients we are treating f as a polynomial over a field. If we are even doing over the integers, then we cannot do this because in integers the only elements which are invertible are ± 1.

(Refer Slide Time: 30:09)



formulas for solutions of f

$-a_0/a_1$ $\qquad \frac{a_0}{a_n} + X$

$\frac{-b \pm \sqrt{b^2-4c}}{2}$ $\qquad X^2+bX+c$

$\pm, \cdot, \div,$ extracting square roots

"Solvable by radicals"

So now little bit, 2-3 minutes about the problem. So now what are we looking for? We are looking for solutions. And we are looking for formulas. Formulas for solutions of f. What does that mean? So the typical example is see, linear one, we have this formula: $\frac{a_0}{a_n}$. It involve only the coefficients. In case of quadratic, remember they were $\frac{-b \pm \sqrt{b^2-4c}}{2}$.

This is a formula for the solutions of quadratic equations. This quadratic equation: X^2+bX+c .

And this was linear, so the linear also we could have done like this: $\frac{a_0}{a_n}$ + X. So just simply we send it to the other. So these formulas involve what? They involve operations addition, multiplication and division also. So these are called field operations. They are operations of the field, given field.

We can divide in non-zero element, we can divide, multiple, add, subtract. In addition to this, we have one more operation here, namely extracting square roots. That is where we need to enlarge $\mathbb{Q}$. So these are called formulas. So one now looks for formulas for polynomial equations, solutions of the polynomial equations where degrees are higher, degree 3, degree 4, degree 5 and so on.

And as I told you yesterday, there are explicit formulas are for cubic equations, bi-quadratic equations. But in general, there were no formula for degree 5 equation onward. And this theory evolved out of this that how do you decide a given polynomial of degree 5 has a solution, has a formula in terms of these operations or not. And 2000 years, this question was not satisfactorily answered till Galois came up with this theory. That, no, you cannot solve all the equations. This means you cannot write down formulas for solutions for all degree 5 and onwards equation.

But then how do you decide the given f as a solutions which can be written in these operations or not. These are called solvable by radicals. So in this course, we will develop a theory and we will apply this theory to explicit equations. And for them, there will be formulas. For the others, there will not be formulas. So this created lot of good mathematics and also lot of practical problems and so on. Thank you. We will continue next time.