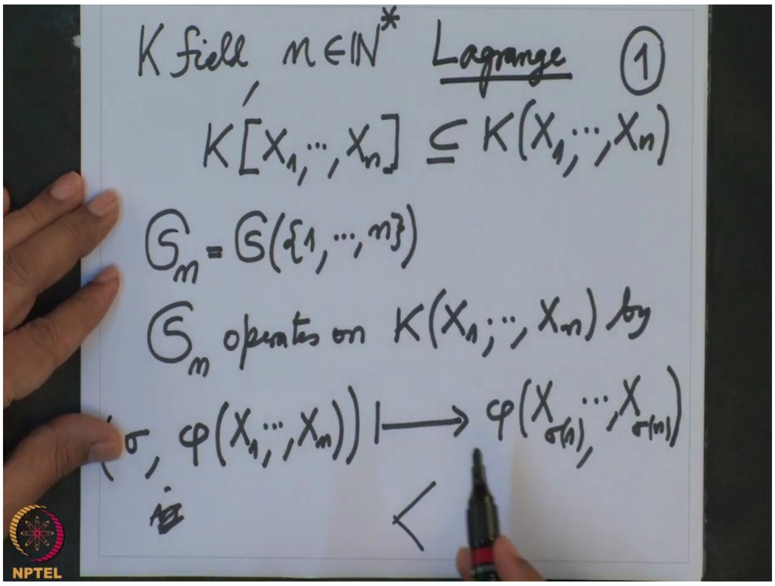
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture 44
Elementary Symmetric Polynomials

Now we are starting a new investigation namely, remember that this course main aim is to study the 0 is of a polynomial over a field in one variable. And we want to gather information about these zeros from the knowledge of the Galois group for example. And when you want to know when these zeros have the formulas, so in order to understand zeros of a polynomial without computing that is the main task because remember computing a 0 all zeros of a polynomial is a very big task and we want to avoid that big one and just looking at the Cauchys we want to extract the information that is the main aim and to know whether there are formulas or not.

So first of all there are so many terms way here what I have talked, when you say polynomials where are the zeros and so on and so on. So I am going to start a polynomial over many-many variables and when I specialize it to the zeros I will also get my coefficients specialized at the zeros, so in general I call, so soon things will become clear when I have a precise notation.

(Refer Slide Time: 2:22)



K field, $n \in \mathbb{N}^*$ Lagrange (1)

$K[X_1,\cdots,X_n] \subseteq K(X_1,\cdots,X_n)$

$\mathfrak{S}_n = \mathfrak{S}(\{1,\cdots,n\})$

$\mathfrak{S}_n$ operates on $K(X_1,\cdots,X_n)$ by

$(\sigma, \varphi(X_1,\cdots,X_n)) \longmapsto \varphi(X_{\sigma(1)},\cdots,X_{\sigma(n)})$

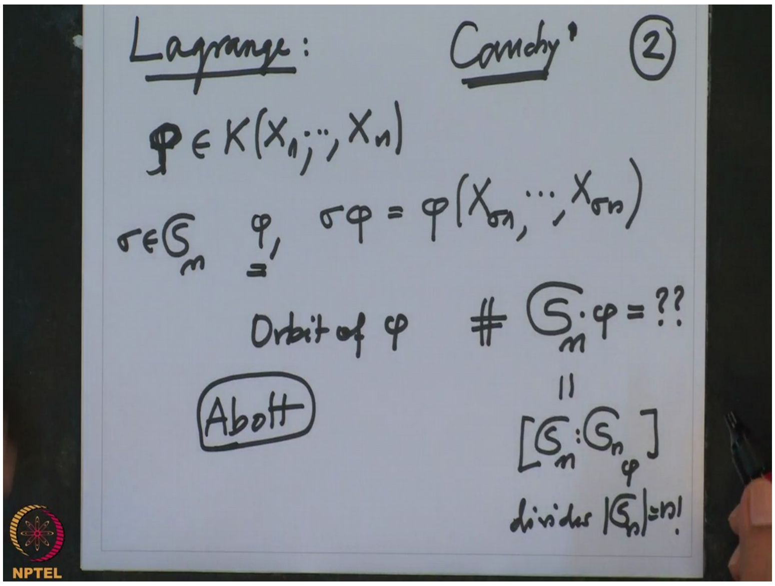
So I consider so suppose K is a field given this is given and an integer natural number n is also given. And I consider a polynomial over this field in n variables so I consider this $K\left[X_1,\ldots,X_n\right]$, this is the polynomial bringing in several variables over this. We know the

Cauchy field is precisely the field of rational function $X_1,\ldots,X_n$. And we have a group S_n, this is the permutation group on n letters 1 to n, this is a group and I want the natural action of this group on this polynomial. So then I want to say that S_n operates on the field rational function field in n variables over K by what? So I should tell when what happens to the rational function.

So taking a rational function $\phi,\phi\left(X_1,\ldots,X_n\right)$, remember this is a rational function so this means it is a polynomial divided by polynomial. In this I want to interchange I want to permute the variables according to the permutation, the given permutation in S_n. So given any element here and any element in the group σ this goes to $\phi\left(X_{\sigma(1)},\ldots,X_{\sigma(n)}\right)$, so this is clearly an operation of group so this this that means S_n operates on this field by this operation. So that is very easy to check that this is an operation, remember we will have to check two things if σ is identity then you do not... This is also same as ϕ and if I have two permutations then whether I apply individually and then I apply the composition that is the same operation so this is clearly a group operation.

Now, whenever we have a group operation one has to understand the fix elements and one has to understand orbits and one has to understand the stabilizers, this is always and then we have the information from this. Let me just mention here, Lagrange was the one who started this but Lagrange did not have this language that time of operation or a group or an isotropy, he did not have this operation he did not have this language but he was thinking along the same lines and his problem was, what was his problem? I will just mention it before we go into the precise, so Lagrange was looking for what? Lagrange, he was looking for the following.

(Refer Slide Time: 6:12)



Lagrange: Cauchy' ②

$\varphi \in K(X_1, \dots, X_n)$

$\sigma \in \mathfrak{S}_n$ $\underline{\underline{\varphi}}$, $\sigma\varphi = \varphi(X_{\sigma 1}, \dots, X_{\sigma n})$

Orbit of φ $\# \, \mathfrak{S}_n \cdot \varphi = ??$

$\|$

$[\mathfrak{S}_n : \mathfrak{S}_{n_\varphi}]$

Abott

divides $|\mathfrak{S}_n| = n!$

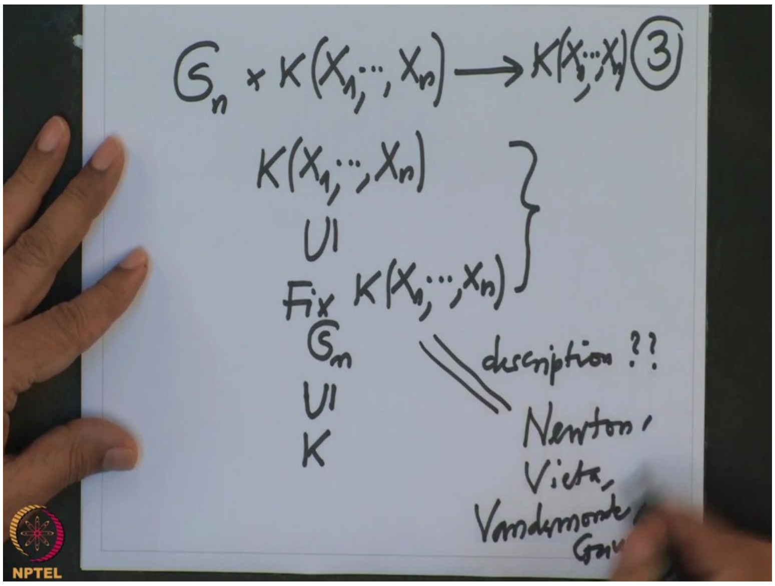
He started with the given f, he started with f rational function ϕ rational function in n variables and he took he took elements from S_n, those are the per quotations, that time there was not even in knowledge that they are permutations. Later on when people developed when people thought about what an odd, people developed language of permutations and more about permutations like transpositions, cycles, what are their orders, what are their decompositions, what are their signatures and so on. And the 1^{st} systematic study started by Cauchy, this is study of permutation and study of groups also, finite groups specially therefore you could prove the theorem if P is divisor of the order of the group then there is element of order P etc, etc.

So Lagrange was doing the following, I started the rational function then some permutation and then applied let me write σ $\phi$by definition ϕ of permute the variables, this is new rational function. Now if this was different from ϕ keep it, if it is equal throw it then take another permutation and do the same thing and he wanted to go on like this and question is how long you can go on and what is the least number he has to stop. So in our language now it is very easy that means he had taken ϕ and he had taken the orbit of ϕ under this action. So in our notation remember it is S_n multiples of ϕ and his question was what is the cardinality? That was what Lagrange wanted.

And you could guess clearly that this is the device of n factorial but you could not prove this and that is what led in general to the orbit stabilizer theorem, now it is very clear that this is the device of because this cardinality of this orbit is same thing as index of the stabilizer in this group so this is again the notation S_n suffix ϕ, this is the stabilizer of ϕ that is the cardinality of the orbit and this is clearly a divisor of the order of this divides order of S_n which is we know it is n factorial.

So this was Lagrange, we started by Lagrange, Lagrange did not prove this precisely and his student Abott proved it finally and later on standard textbooks on finite group theory you will find now the Lagrange's theorem which says that order of a subgroup finite group divides the order of that group, this is what it came into the existence okay. So now what do you want to do?

(Refer Slide Time: 10:02)



$S_n \times K(X_1,\ldots,X_n) \longrightarrow K(X_1,\ldots,X_n)$ ③

$$\left.\begin{array}{c} K(X_1,\ldots,X_n) \\ \cup\!\!| \\ \mathrm{Fix}_{S_n} K(X_1,\ldots,X_n) \end{array}\right\}$$

$\cup\!\!|$

K

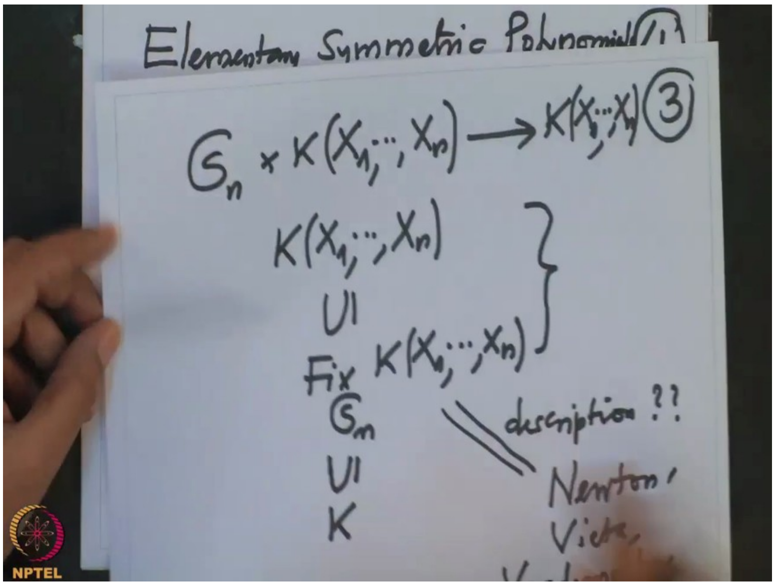
description ??

Newton, Vieta, Vandermonde, Gau

We know that S_n operates on this field rational function field so we write like this, this to $K\left[X_1,\ldots,X_n\right]$ there is this operation map. And whenever a group operating on the set, it is most important to find the fixed element so what is, now I have a field. This is the field $K\left[X_1,\ldots,X_n\right]$, this is an extension of K, this is a very big field and this group is operating there so I want to find, what are the fix S_n $K\left[X_1,\ldots,X_n\right]$ and this is contained here that is obvious and this. And now there are so many questions for example, we can ask about this bill extension namely is infinite, if it is finite what is its degree? Is it Galois? What is this Galois group and so on? All these questions are cropping up.

So the first question I want to understand, I want to concentrate is what is the fix field? So I want to describe this fix field, the description of this fix field that is what I want to do. And not only Lagrange that were many people involved in this and the main people involved in this right from the Newton, Viete or Vandermorkm Gauss, all these people were involved in this to understand this. And the theorem which I will write that theorem in those days it was never written up precisely but it was sort of known that everybody knows it. The 1st written proof we can find only in a Gauss' writings so that is it so for that I want to now I want to give some examples of fix points of these fix elements in a rational function field so that at least to start with, so those are precisely called Elementary symmetric polynomials.

(Refer Slide Time: 13:04)



Elementary Symmetric Polynomials

$\mathfrak{S}_n \times K(X_1,\cdots,X_n) \longrightarrow K(X_1,\cdots,X_n)$ ③

$$\left.\begin{array}{c} K(X_1,\cdots,X_n) \\ \cup\!\mid \\ \operatorname{Fix}_{\mathfrak{S}_n} K(X_1,\cdots,X_n) \end{array}\right\}$$

$\cup\!\mid$

K

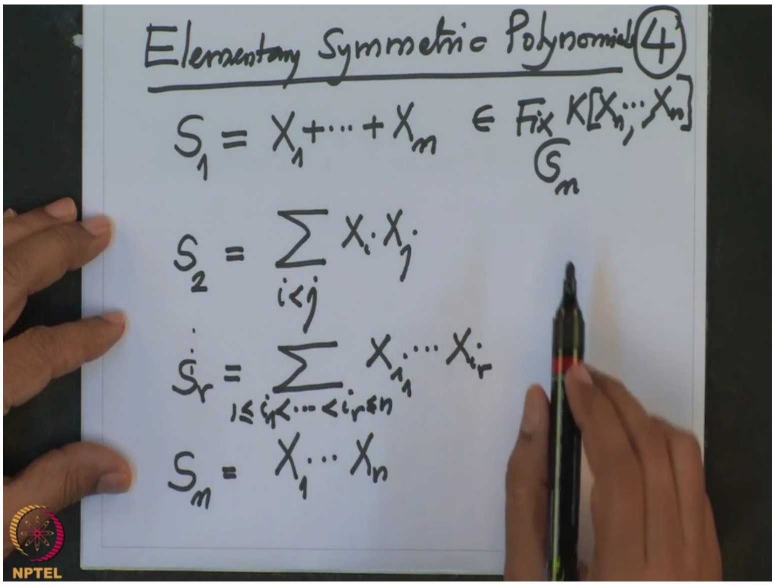
description ??

Newton,

Viete,

What are they? So note that this action of S_n on the rational function field, it is also if I restrict it to the polynomials it also go to polynomials so S_n also operates not only on the rational function , it operates on the polynomials also.

(Refer Slide Time: 13:20)



Elementary Symmetric Polynomials ④

$s_1 = X_1 + \cdots + X_n \in \operatorname{Fix}_{\mathfrak{S}_n} K[X_1,\cdots,X_n]$

$s_2 = \sum_{i<j} X_i \cdot X_j$

$\vdots$

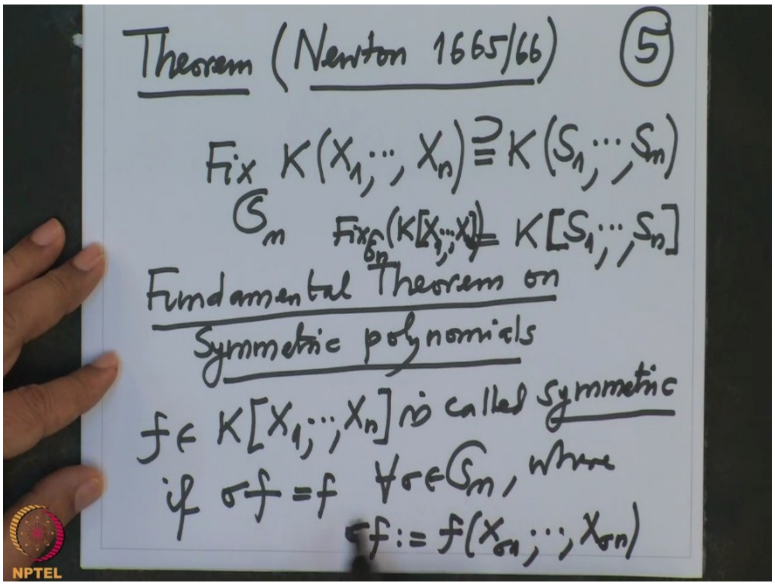
$s_r = \sum_{1 \le i_1 < \cdots < i_r \le n} X_{i_1} \cdots X_{i_r}$

$s_n = X_1 \cdots X_n$

So the first one S_1, look at the sum of these variables, it is obvious that if I permute the variables this S_1 will not change so therefore it is clear that this one belongs to the fix points of S_n and the polynomials. And another thing I want to note here, even this field is not playing any role you could take orbit ring and this group is operating on this polynomial ring over orbit ring K and this polynomial is the sum of the variables. It is clearly fix because when I permute the variables, this polynomial is not going to change. Now S_2, now you take product two at a time so that means the sum $X_i X_j$ and this is running over all the indices i less than j so product 2 at a time and I could have chosen sort of this.

This is clearly fix because if you interchange the variables this product will go to some other product which is also a part and so on. Similarly, I can go on till S_n this is the product of all $X_1, \ldots, X_n$. If I have to write r in between S_r is what? r at a time so that one should write it as submission running over the tuples $i_1, \ldots, i_r$, so this is running over i_1 less than less than less than i_r. I can always order them according to the increasing order and write in that fashion. All these polynomials they are fixed under the action of S_n and they are called elementary symmetric polynomials.

(Refer Slide Time: 15:46)



Theorem (**Newton 1665/66**) ⑤

$\operatorname{Fix}_{\mathfrak{S}_n} K(X_1, \cdots, X_n) \overset{\supseteq}{=} K(S_1, \cdots, S_n)$

$\operatorname{Fix}_{\mathfrak{S}_n}(K[X_1, \cdots, X_n]) = K[S_1, \cdots, S_n]$

Fundamental Theorem on Symmetric polynomials

$f \in K[X_1, \cdots, X_n]$ is called **symmetric** if $\sigma f = f \;\; \forall \sigma \in \mathfrak{S}_n$, where

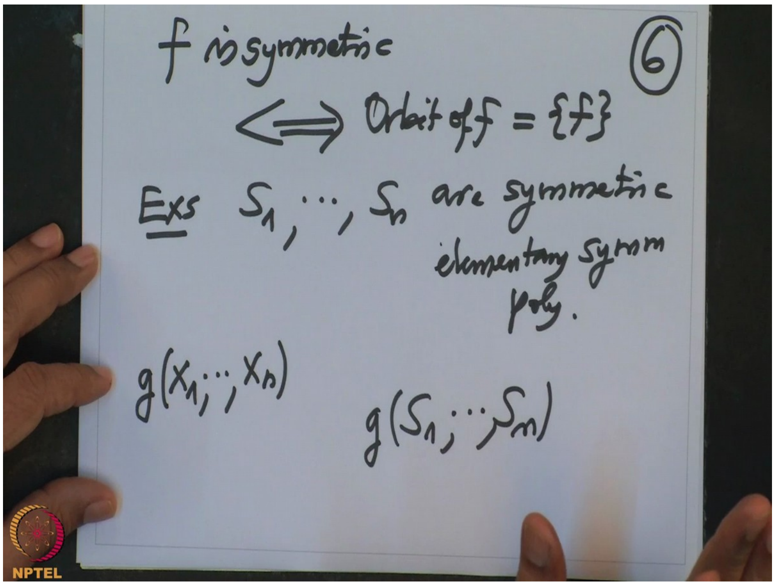
$\sigma f := f(X_{\sigma 1}, \cdots, X_{\sigma n})$

Now the theorem says, so this is the theorem. This if you see the writings of Newton, you already feel that you knew this and this is Newton and it must be around 1665-66, what does it say? That the fix field of the operation of S_n on the rational function field in n variables this is nothing but a field generated over K by this elementary symmetric polynomials, this is what the theorem is, we will soon prove it. So this is also known as fundamental theorem on symmetric polynomials. This is very-very important and later on I will use this theorem to prove that the field of complex numbers is algebraically closed.

Let me also say that this inclusion is clear because all these are we know that all these S_1 to S_n are fix under the operation of S_n so therefore if I take any polynomial in S_1 to S_n, they are also fix under the operation of S_n and therefore, all the S_n functions are also fixed. So I also should write that $K[S]$ the ring generated algebra generated by S_1 to S_n over K, this is a polynomial this is also the fix S_n polynomial $K[X_1,\dots,X_n]$. And therefore why this theorem is so fundamental because it explains all the polynomials which are symmetric. Now, when do we say a polynomial is symmetric? You say a polynomial is symmetric if it is invariant under all permutations of the variables.

So let us recall a polynomial f over K in many variables is called symmetric if f $\sigma(f)$ equal to f or every σ in S_n. And what is the stigma of f, where $\sigma(f)$ is by definition take a look at that f and permute the variables according to that σ, so f is not changing under every σ. That means this condition means orbit of every single term so we should also write it and I am going to write in modern notation only.

(Refer Slide Time: 19:34)



f is symmetric

6

$\Longleftrightarrow$ Orbit of $f = \{f\}$

Exs $S_1, \cdots, S_n$ are symmetric
elementary symm
poly.

$g(X_1, \cdots, X_n)$

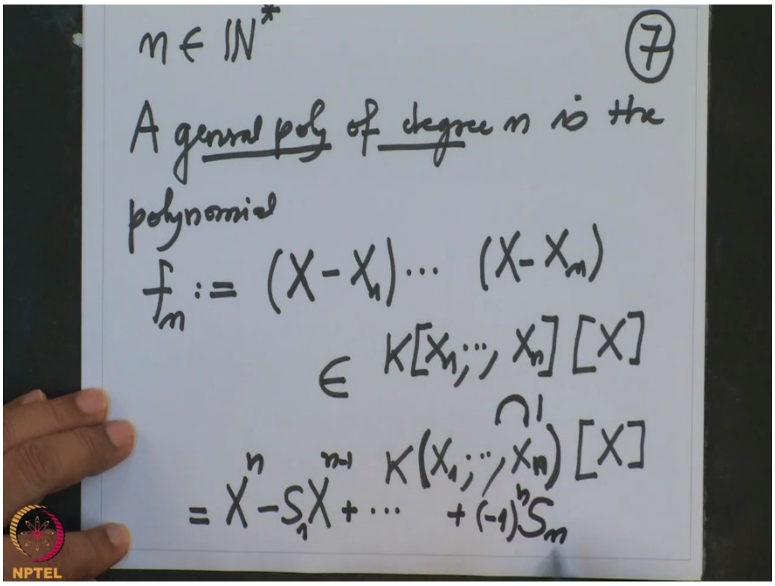
$g(S_1, \cdots, S_n)$

So f is symmetric if and only if orbit of f equals to single term f, and this theorem therefore explains. So example of symmetric polynomials are all these polynomials from S_1 to S_n are symmetric and they are called elementary because they have got the definitions of S_1 to S_n, got by very elementary way that S_1 is a sum, S_2 is you take product 2 at a time and their sum,

S_3 is product 3 at a time and their sum and so on, so they are they are called elementary symmetric polynomials. And the theorem says if you know this then you know all the symmetric polynomials, they are precisely the polynomials in this S_1 to S_n.

So you take any polynomial g and you take any polynomial in n variables g and you take g of S_1 to S_n, this is symmetric and precisely these are symmetric that is why their theorem is very fundamental and will have lots of consequences. And one will also imagine that if you want to set polynomials in n variables, this group operation is very-very important. And why was it so important to consider this polynomial also that also I will explain before I prove the theorem. Okay so before I prove, why is this so important to consider for the study of the zeros of a given polynomial.

(Refer Slide Time: 21:45)



$n \in \mathbb{N}^*$ 7

A general poly of degree n is the polynomial

$$f_n := (X-X_1)\cdots(X-X_n)$$

$$\in K[X_1,\dots,X_n][X]$$

$$\cap|$$

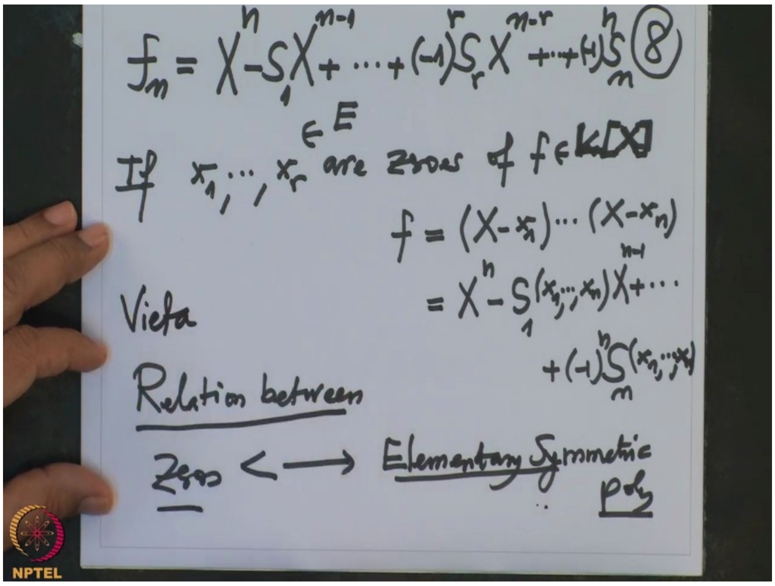
$$K(X_1,\dots,X_n)[X]$$

$$= X^n - S_1X^{n-1} + \cdots + (-1)^n S_n$$

So given any n natural number, a general polynomial of degree n is the polynomial f n, this is by definition this is a general of degree n, so what do I write? It is a monic polynomials so X is a variable, it is only in one variable $(X - X_1)\ldots(X - X_n)$ so think of this is the polynomial over f, this is the polynomial in X with coefficients in where? With coefficients in the polynomial ring in the remaining variables. But this one is containing rational function field and the polynomial over there in X, so this is the polynomial of degree n it is obvious and the coefficients I am considering this this rational function field.

And now when I expand it what do I get, when I expand it, when I multiply these products what do I get? X^n it is monic of degree n, the next coefficient is what? That is $-S_1X^{n-1}$, the last coefficient alternating, last coefficient is $(-1)^n S_n$ so let me write it on the next page.

(Refer Slide Time: 23:49)



$$f_n = X^n - S_1 X^{n-1} + \cdots + (-1)^r S_r X^{n-r} + \cdots + (-1)^n S_n \quad \boxed{8}$$

If $x_1, \ldots, x_r \in E$ are zeros of $f \in K[X]$

$$f = (X - x_1) \cdots (X - x_n)$$
$$= X^n - S_1(x_1, \ldots, x_n) X^{n-1} + \cdots$$
$$+ (-1)^n S_n(x_1, \ldots, x_n)$$

Vieta

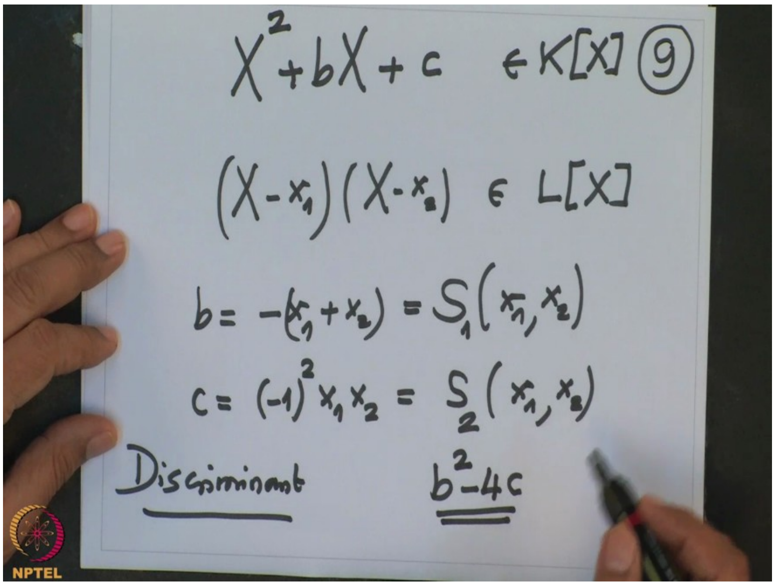
Relation between

Zeros <—> Elementary Symmetric Poly

So this polynomial is f_n is $X^n - S_1 X + ... + (-1)^r S_r$, this is n – 1, this is n – r and so on, the last term will be $(-1)^n S_n$, this is general polynomials. So if I want to study this polynomial f n, I have to study the elementary symmetric functions because now what? If I want to find if I know if we know the 0 of this polynomial then what will be the coefficient? So therefore, if $X_1, \ldots, X_r$ are zeros of a polynomial f of monic polynomial that is like this, zeros of f, f is one variable polynomial over some field I should write L from field L, this is of one variable polynomial.

And suppose I know the zeros, they may be in a bigger field, these zeros may not be in L but they may be in a bigger field say E then I know this but when I expand it what do I get? I will get X^n and the next one will be $-S$ but this S_1 we evaluate at $X_1, \ldots, X_n$ that makes sense because this is a sum and so on. Last term is $(-1)^n S_n$ we evaluated at $X_1, \ldots, X_n$. So this gives you a relation between zeros on one side, on the other side elementary symmetric polynomials, right this correspondence. If I know the zeros, I know the elementary symmetric function evaluated there and if I know those coefficients our problem is to relate them to the Zeros, this relation was already known to Vieta. So simple case let me show you and that is what we want to generalize now.

(Refer Slide Time: 26:55)



$X^2 + bX + c \in K[X]$ 9

$(X - x_1)(X - x_2) \in L[X]$

$b = -(x_1 + x_2) = S_1(x_1, x_2)$

$c = (-1)^2 x_1 x_2 = S_2(x_1, x_2)$

$\underline{\text{Discriminant}}$ $\underline{\underline{b^2 - 4c}}$

So suppose I have a quadratic $X^2 + bX + c$, so $(X - x_1)(X - x_2)$, we have written this in a bigger field, this was in a field $K[X]$ let us say then we have enlarged our field L K to L then we have written this there , and what is the relation between b and this? So obviously this $b = -(x_1 + x_2)$, this is S_1 evaluated at x_1, x_2, c is product of two with a sign so $(-1)^2 x_1 x_2$ which is S_2 evaluated at $x_1 x_2$. And then if you remember we were considering the discriminant of this, so discriminant was what? Discriminant was $b^2 - 4c$, it was a discriminant and our school formulas depended on the square root of this discriminant.

So that means we want to study the discriminant also. Now this discriminant is what we can write in terms of this s_1, s_2 and so on, so we need to go on this arbitrary degree polynomial and therefore we want to study elementary symmetric functions, we want to study symmetric polynomials, this discriminant may not be symmetric so I want to do this more general setup and to do that what is very very important is to consider the group action permutation group on n letters on the polynomials in n variables and also rational functions.

And this is what I started with, we have to prove that theorem on symmetric functions Newton's theorem that we have to prove. I will draw lots of consequences from that and I will also define a discriminant of a polynomial, more generally I will define given 2 polynomials how do you find they have a common 0 or not, to do that I will also define resultant of 2 polynomials and the relation with zeros and so on. So this is what will go on for a couple of lectures form now, so I will stop here and we will continue this in a next setup thank you.