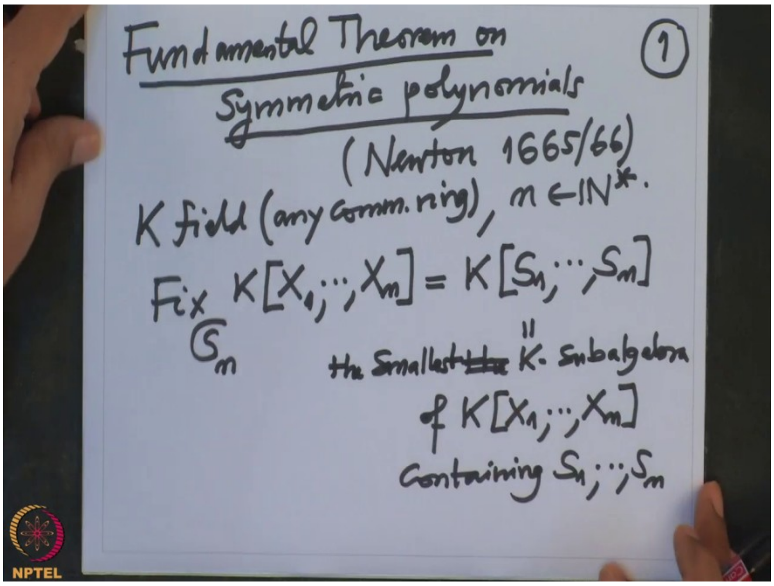
Galois Theory
Professor Dilip Patil
Department of mathematics
IISc Bangalore
Lecture 45
Fundamental theorem on symmetric polynomials

In the last lecture I have stated a fundamental theorem on symmetric polynomials and we will prove it today just now. So let us recall what it is, so this was a fundamental theorem.

(Refer Slide Time: 0:42)

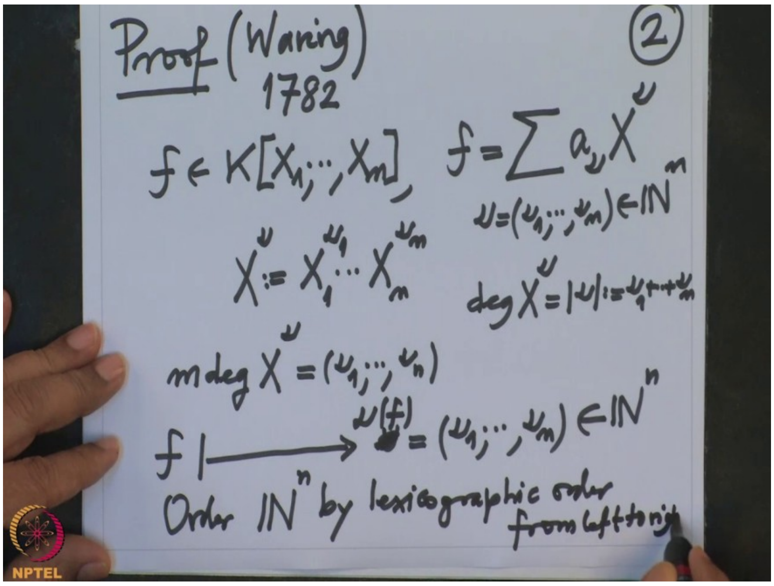


Fundamental theorem on symmetric polynomials this is, some old books also will say it as Newton's theorem and 1665/66, okay. K field marginally it can be ring also, any ring, any commentative ring where we can add and multiply elements and so on and n is nonzero natural number then we are describing the fix field of fix S_nK polynomial bringing n variables or k, this polynomial algebra is precisely the sub algebra generated by elementary symmetric polynomials.

Remember this notation is the K sub algebra of $K[X_1,\ldots,X_n]$ containing $S_1,\ldots,S_n$, smallest, smallest, the smallest K sub algebra of the polynomial containing $S_1,\ldots,S_n$, this is what we want to prove.

So let us start proving it, so for the proof, group is very simple. So proof, this proof is due to varying.

(Refer Slide Time: 3:02)



And this was in the year 1782; the idea is very simple, so what do we want to prove? We want to prove that every symmetric polynomial is a polynomial in $S_1, \ldots, S_n$ with co-efficiency in K, all right. So for each I will introduce some notation which we will be using in the proof, for each polynomial f in $K\left[X_1, \ldots, X_n\right]$ a polynomial in $K\left[X_1, \ldots, X_n\right]$ I can always write uniquely as sum of monomials.

Monomials in $X_1, \ldots, X_n$ and some coefficients, so $a_v X^v$ where this v is a tuple $v_1, \ldots, v_n$ which is as natural coefficients, so this is an element in $\mathbb{N}^m$ and we are using here calculus notation, what is X^v? X^v is by definition $X_1^{v_1} \ldots X_n^{v_m}$ that is the definition of this and when we say degree of this monomial X^v.

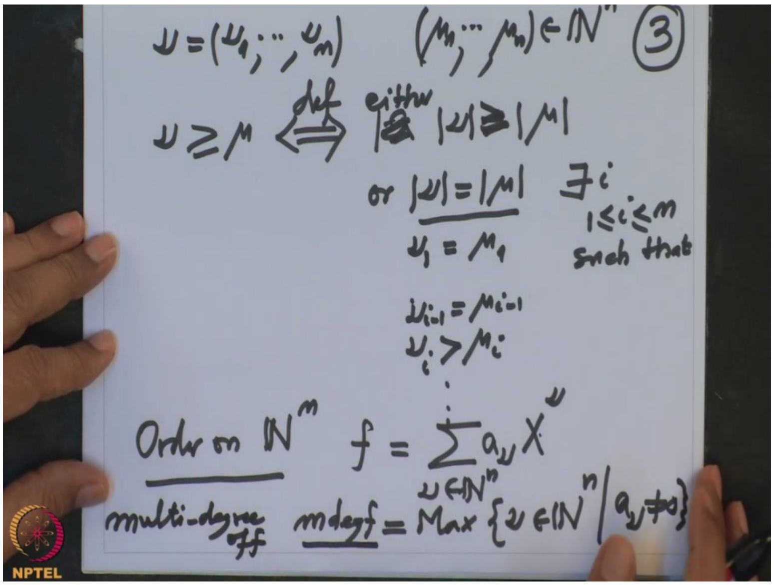
These degrees precisely mod v which is by definition v_1 plus sum of all vs that is called a degree. This is the usual this degree, total degree. So usual degree as a polynomial is the one where mod v is maximum. So this is the finite sum and mod v is maximum then that will be the degree monomial and the remaining monomials will have smaller degree but I am not, I am not going to consider usual degree.

I'm going to consider what is called multi-degree, so I will call it m deg, m deg of a monomial there is only one term, so I don't have to define what is m deg of a monomial that is by definition $v_1, \ldots, v_n$. So first of all let me remind you multi-degree of a polynomial is not an integer, it is a tuple. So to each polynomial f I'm going to attach and element v.

This v is an element $v_1,\dots,v_n$ in N power m this is multi-degree and because it will depend on your I will call it v f and what is it? So that means I have to order the set N^n, so order N^n by lexicographic order, order from left to right what does that mean?

So let me scale out what is this order, its order on the set and how do I compare two elements in that, I have to tell you.

(Refer Slide Time: 6:37)



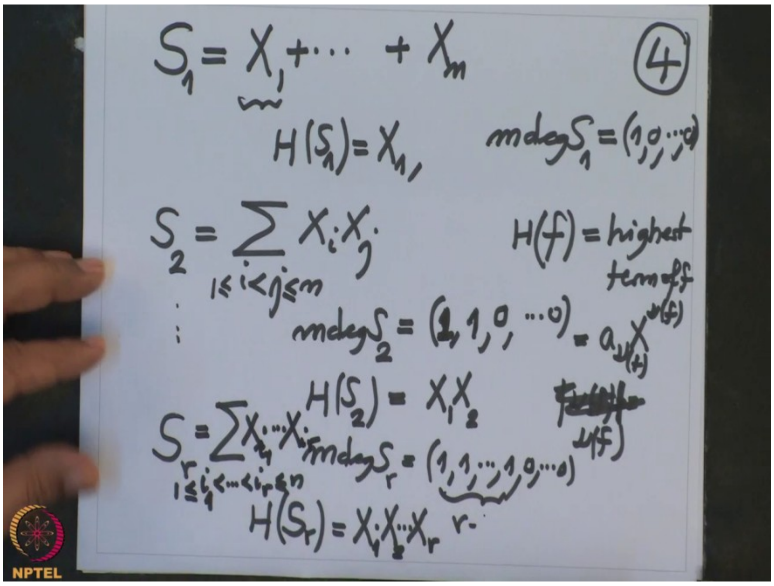
So suppose I have two tuples one is $v_1,\dots,v_n$ and other is $v_1,\dots,v_n$ both are in N power n then I will say v is bigger equal to v if and only this is the definition first I compare their compare their mods. If mod is bigger equal to then I will say v is bigger equal to v but this is a total degree either this or it can be equal and then I look at, I start comparing v_1 v, if it is equal also fine.

So but there should be a stage where v_i should be strictly bigger than v_i and then afterwards I don’t care what happens. So up to here they are equal and there is, so that means there exists in this case, there exists i in between 1 and n such that up to i minus they are equal ieth stage they are more than, the v is bigger that is what it means by lexicographic found left to right.

You start comparing this; if it is equal go to the next one and so on and so on. So this is clearly, this defines order on v^m and what we will, what even in polynomial f which is, the sum is like this finite sum v where is in v^n, so they are finitely many monomial in all therefore they are finitely many n tuples involved, so I can always decide the biggest one, finite subset will have maximum because this is partial order and the is there.

So therefore I will call multi-degree of f to be the maximum of v in N^m such that v should occur here that means a v is not, so that is called multi-degree of f, multi-degree of f that is days m deg, m deg f.

(Refer Slide Time: 9:27)



Now let us give some examples to understand, so for example if I take as one, this is the first element is meeting function, this is $X_1+...+X_n$, what is mdeg of S_1? This is, see what is this monomial? This is X_1 that means 10000 that is a degree of this monomial then next one? 010000 the X_n is 0000 last coordinated then, so obviously this one gives the maximum, so multi-degree is 1000.

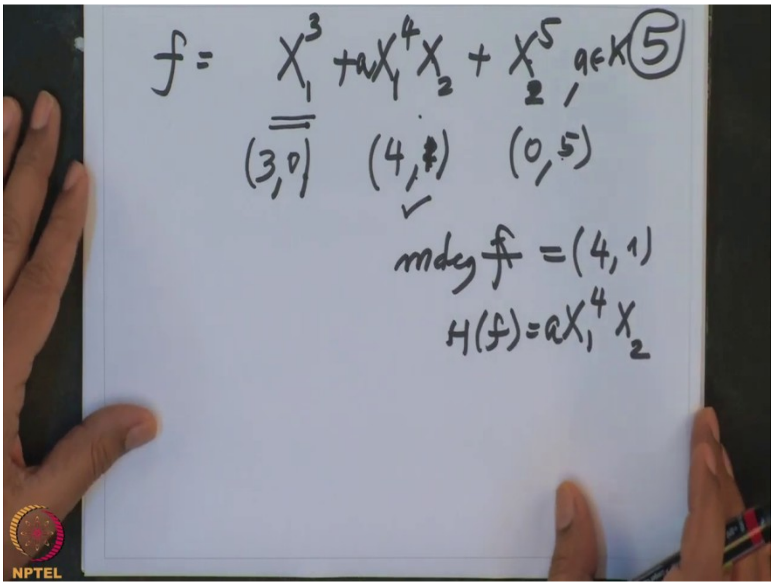
And what is the highest degree monomial? That is, so let me write that in general for a polynomial f we have a multi-degree and there is highest monomial, so that will be called highest, this is the highest term of, term of f and this will be, this will consist of only one monomial that it's a v X^v f, this also I call it mdeg, this v f use the maximum degree.

v f mod v f is, not mod v f, v f is the degree giving term of f, okay. So what is the highest of S_1? Highest term of S_1 is precisely X_1, all other terms will have smaller degree than this, smaller multi-degree, always multi-degree. What about S_2? S_2 is sum of 2 at a time. So obviously the multi-degree of S_2 is 1, 1 because I am taking i not equal to j in this.

This S_2 is sum of all terms 2 at a time product but they are different not, never repeated, so this S_2 is sum of these 2 different variables multiplied together. So therefore the multi-degrees of basically1, 00 and 0 because there is no other term, any other term will either this is 0 or if this is present this will be 0 and so on, so therefore it is very easy to see that highest degree term of, so what is H of S_2?

H of S_2 is the monomial $X_1 X_2$ and so on. So what will be the in general? What is the highest, what is the multi-degree of S_r? This is precisely 111 r times up to r stage and after that 000, these are r, r, r number of terms and what is the highest degree of, highest term of S_r? That is obviously X_1 X to up to the X_r, that is also very clear because this is sum of, this is sum running over the tuple i_1 less then less than less than i_r this is obviously less equal to n this is bigger equal to 1 and $X_{i_1}, \ldots, X_{i_r}$ very easy. So highest degree term it is very easy.

(Refer Slide Time: 13:30)

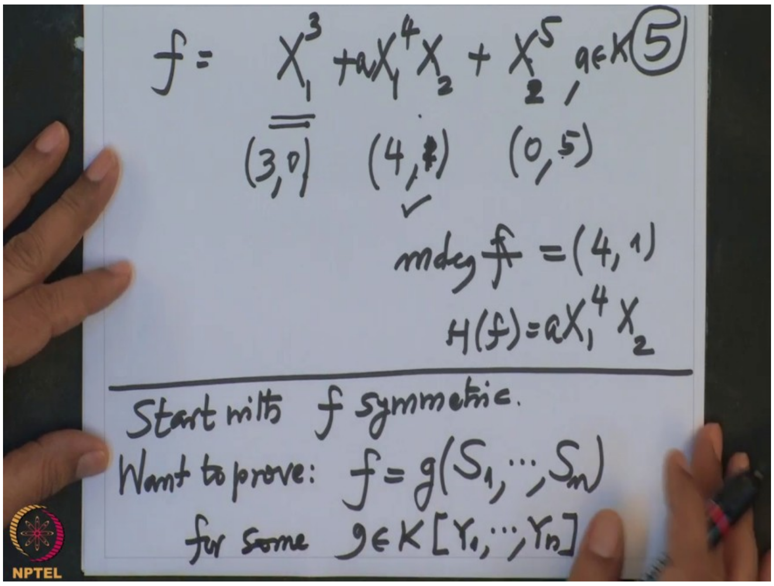


One more example which is, these are symmetric ones. One non-symmetric example one should see, what is the term? So for example if I take f equal to $X_1^3 + X_1^4 X_2 + X_2^5$ this is my polynomial in variables, so what is the, what is the degree of this monomial? It is three, 0, what is the degree here? Multi-degree I am writing, multi-degree here is 4, 2 no 4, 1 multi-degree here is 0, 5.

X_1 doesn't that means therefore 0 and X_2 on the side and therefore this, so who is highest? I should first see the, see the mod, right? This is, mod is 3, this is mod is 5; this is mod 5, so obviously this will not be the highest degree term, so I will compare these 2. And these 2 who is bigger? This is bigger, so therefore multi-degree of f in this case is, multi-degree of f equal to 4, 1.

What is the highest of f? There is this one. $X_1^4 X_2$ there could be a coefficient here, suppose it was a here then I will give you the a here and the highest degree coefficient will be a in field K that is how it was. It is more fine then the degree because you see, if it was, if you ask me what is the degree of f. The degree of f is 5 and this will be the degree term but when you say multi-degree then among them if you are comparing and this is the highest degree of f. So that is the highest degree of term.

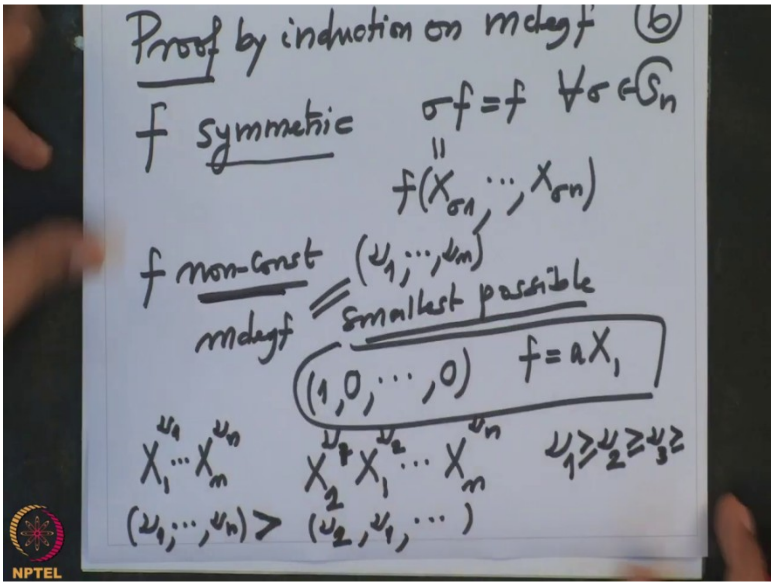
(Refer Slide Time: 15:17)



So what we want to prove, so we start with, start with a symmetric polynomial, f symmetric and we want to prove that a symmetric polynomial is a polynomial in $S_1,\ldots,S_n$ with coefficients in K that is what we want. Okay, so when I am going prove this solution, so we want to prove, what do we want to prove?

We want to prove this f equal to G of $S_1,\ldots,S_n$ where g is a polynomial in n variable K I will write for not you can get confused $Y_1,\ldots,Y_r$, we want to prove this. We want to find g, so that in g the polynomial in n variables with coefficients in K, so that when I substitute Y_1 is equal to these $S_1,\ldots,S_n$ then I get f, for some g.

(Refer Slide Time: 16:38)



And this I am going to prove this assertion by induction on multi-degree, proof by induction on m degree of f. So where do the induction starts, let us see. I will give you f is symmetric that means what? That means Sigma f equal to f for every σ permutation and this $\sigma(F)$ is by definition $f(X_{\sigma(1)},\ldots,X_{\sigma(n)})$. That means if I promote the value of f doesn't change that is what we have given.

So what is the smallest nonzero symmetric polynomial other than the constant? So if f is not constant, non-constant, what can be the smallest m degree, mdeg f smallest, smallest possible that is where the induction should start? So what is the smallest possible multi-degree that will be obviously 1 0 0, that is the smallest possible and obviously this means what?

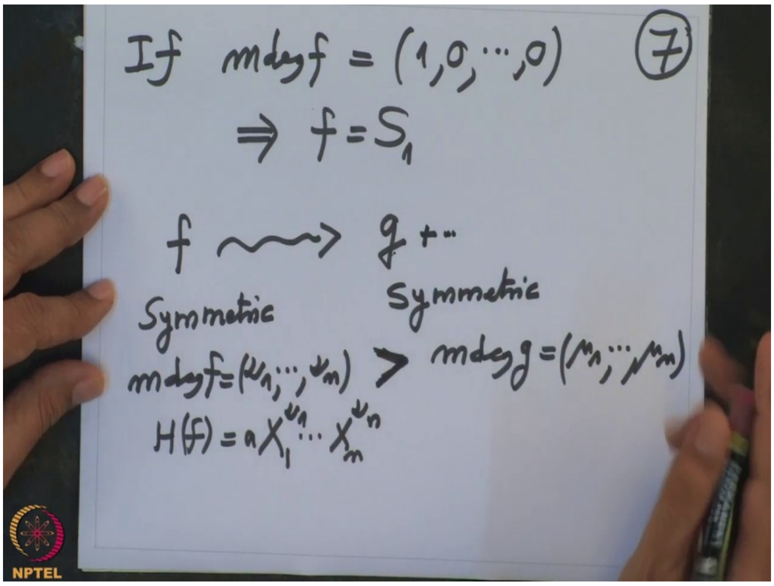
This means what? f is symmetric, so this means 1st of all this monomial X_1 appears in X_1 appears in f with coefficient, now once, okay. So I will, so let us, I want to prove that the multi-degree smallest possible is this only because suppose multi-degree of f, suppose this multi-degree of f is $v_1,\ldots,v_n$ then what do you know? So then, see I will come back to this.

So that means if I interchange X_1 and X_2, so this means 1st of all this monomial occurs in f but then because f is symmetric, if I permute X_1 and X_2 then what do I get here? X_1 is going to X_2 and X_2 is going to X_1 this transposition. So this X_1, X_2, X_2, X_1 will becomes X_2 this is v_2 X_1, no this is v_1 because X_1 has become X_2 and X_2 has become X_1, so this is v_2.

Now among the these 2 the remaining are same, under these 2 I know this is the biggest therefore what did the degree here is $v_1,\ldots,v_n$ and at the degree of this, multi-degree of this monomial is v_1, not v_1 v_2 I should write first that is the power of X_1. v_1, v_2 v_1 etc same and this is bigger than that we know, this is bigger because this is a multi-degree therefore we get v_1 is bigger equal to v_2.

Now if I interchange X_2 and X_3 I will get v_2 bigger equal to v_3, so therefore if a polynomial is symmetric what we noted that is multi-degree coordinates will decrease, non-decreasing. So and where will it start? Therefore this is, this is the biggest possible, right? So clearly it can be for example symmetric polynomial can't have any smaller than this degree, multi-degree and nonconstant.

(Refer Slide Time: 20:52)

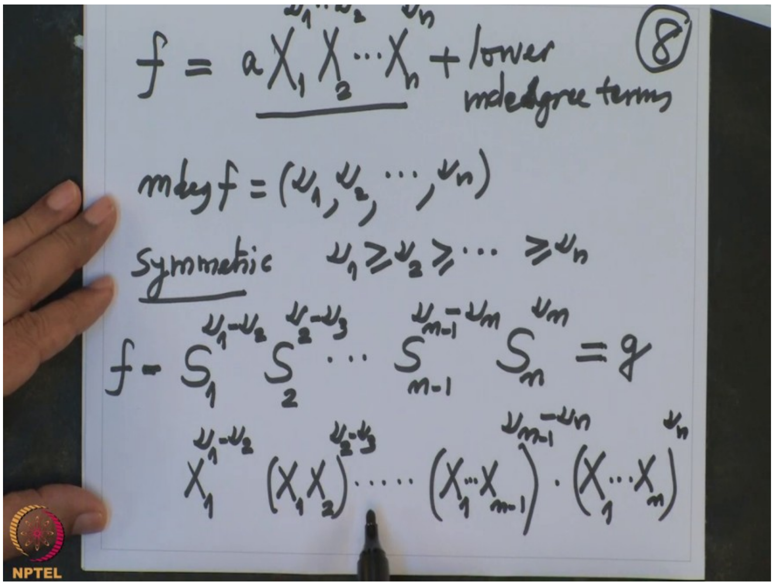


Therefore induction will start there because in this case f has to be S_1, so f if multi-degree of f is 1000 then f has to be S_1 only it can't contain any other monomial because if he does then it will not be symmetric, so it has to be S_1. Okay, now I therefore I want to, so given f I want to find g from this F I want to find g, so that g remains symmetric but the multi-degree drops and then the induction hypothesis I want to apply.

So this is symmetric multi-degree f is now let us say $v_1, \ldots, v_n$ and highest term of some constant times $X_1^{v_1} \ldots X_n^{v_n}$ from here I want to find new g, so what the property should be g should be symmetric and multi-degree of g should be $v_1, \ldots, v_n$ and this should be bigger, strictly bigger this and then I will apply induction hypothesis here because then induction hypothesis this is polynomial in $S_1, \ldots, S_n$ and then I will I will find what is the relation, yes.

So what other thing I will need? That some symmetric polynomial, so let us see what is this process? So what I'm going to do is the following, it is very simple.

(Refer Slide Time: 22:49)



So I have f given here, f is some constant X power $v_1, \ldots, v_n$, no X power $X_1^{v_1} X_2^{v_2} \ldots$ etc X and v_n plus lower degree terms, let me write, lower multi-degree terms, multi-degree terms. And I want to find a symmetric polynomial whose highest degree term is this and cancel it, right? So what I am going to try, so first know that because this multi-degree of f equal to this $v_1, v_2, \ldots, v_n$ we observed that because if it is symmetric.

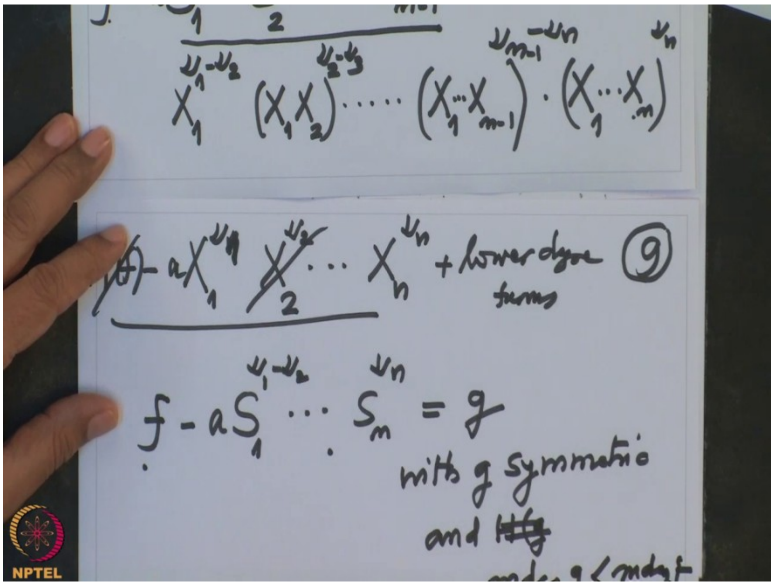
Symmetric will imply mui1 bigger equal to mui2 bigger equal to bigger equal to bigger equal to mui n this is what we have observed above because it is symmetric. This one if I permute X_1 and X_2 I get this if I permute X_3 and X_3 I get this and so on. Now I look at $S_1^{v_1 - v_2} S_2^{v_1 - v_3} \ldots S_n^{v_1 - v_n}$this is obviously symmetric polynomial.

Because with the, this is elementary symmetric functions and the powers, all these are symmetric this product is symmetric, products of symmetric polynomial is symmetric, all right. So I'm going to subtract this from f, so f minus this I'm going to do and I want to claim that whatever, this I want to call it g, this is my g. And I want to claim that the highest degree term I will cancel.

So what is the highest degree term here? That is this we know and I want to compute the highest degree terms here, right? So this should have the same multi-degrees and when I they should have the different coefficient. So what is the highest degree term here? Highest degree term of S_1 is X_1 but then power, so higher degree term of the power is power of the highest degree term, so this is $v_1 - v_2$.

What is the highest degree term here? It is $X_1 X_2$ and the power of there, which power? It is $v_2 - v_1$, and so on, so here for example here what will be X_1 to X_{n-1} and the whole thing power to v_{n-1} times X_n this is the, the last one is X_1 to X_n whole power v_n, so this is the highest degree term of this, this polynomial. So what is this? When I simply by this, what do I get?

(Refer Slide Time: 26:40)

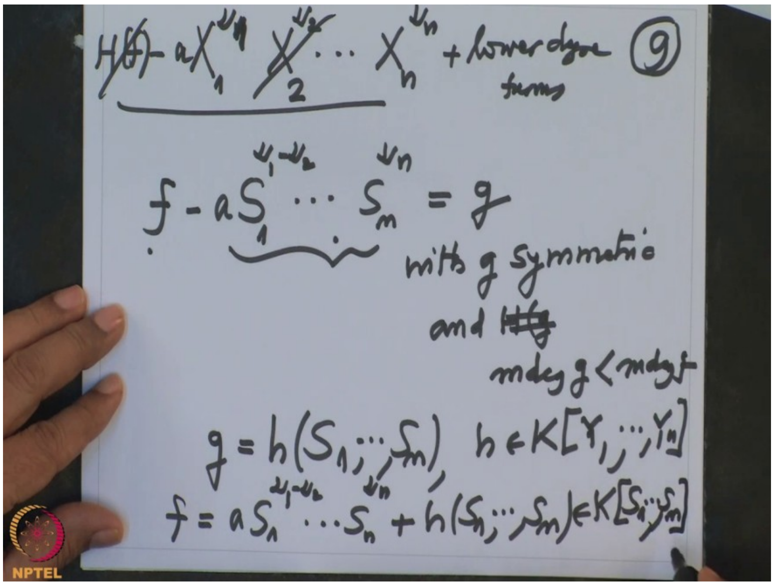


So I will collect the power of X_1, X_1 power, here it is $v_1 - v_2$, here it is $v_2 - v_3$, here it is $v_{n-1} - v_n$ and here it is v_n, so successive terms will get cancelled these v_2 will get cancelled here, v_3 will get cancelled here and so on, so what will I get? $X_1^{v_n}$ because this term is getting cancelled with this one, this will get cancelled with this one and this one will get cancelled and so on.

So only v_1 comes, v_1 remains. So what about X_2? X_2 power there is nothing here; here it is $v_2 - v_3$, so again this v_3 will get cancelled there and so on, so this will be v_2 and so on. This will be $X_n^{v_n}$ at the last because this is only one can get. So we have checked that the highest degree term of this which I have some subtracted is this and highest degree term of this is precisely, so I have to write coefficient here so that it gets cancelled.

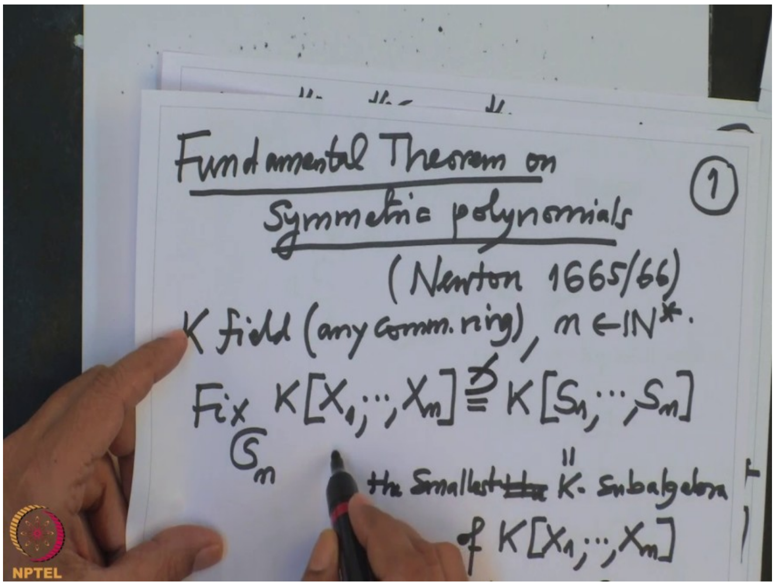
So highest degree term of f minus this, this gets cancelled and whatever remains is lower degree terms but that means what? That means I have checked that $f - aS_1^{v_1 - v_2} \ldots S_n^{v_n}$ this is equal to g and this is symmetric, this is symmetric therefore g is symmetric, so with g symmetric and higher degree term of g or multi-degree of g is strictly smaller than multi-degree of f.

(Refer Slide Time: 28:44)



So by induction the g will be equal to some polynomial h evaluated at $S_1, \dots, S_n$ where h is a polynomial in n variables with coefficients in K but then f will be equal to this one, $a\, S_1^{\nu_1-\nu_2} \dots S_n^{\nu_n} + g$ but g is this, so this belongs to the elementary symmetric this belongs to the sub algebra generated by $S_1, \dots, S_n$. So that is what we wanted to prove.

(Refer Slide Time: 29:41)



So that finishes the proof of this, I will just show you what we proved it, we proved this equality because this is obvious and we have, we have taken an element here and we proved it is here therefore this finishes the proof of the fundamental theorem on symmetric polynomials and this is very easy proof, the only idea is you define a multi-degree and next time now I will deduce consequences from here which will also be very useful for defining decrement etc.

Thank you.