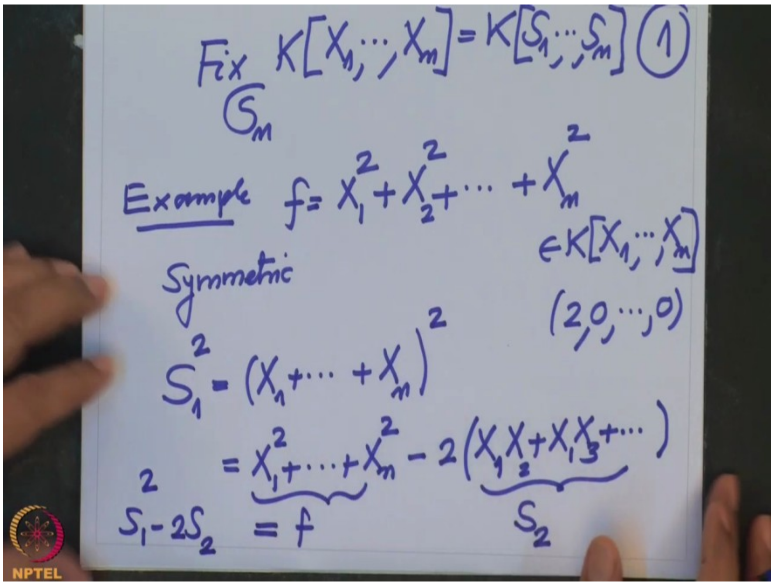
Galois Theory

Professor Dilip Patil
Department of mathematics
IISc Bangalore

Lecture 46

Gal (K[X1, X2,...,Xn] /KS1,S2...,Sn])

(Refer Slide Time: 0:34)



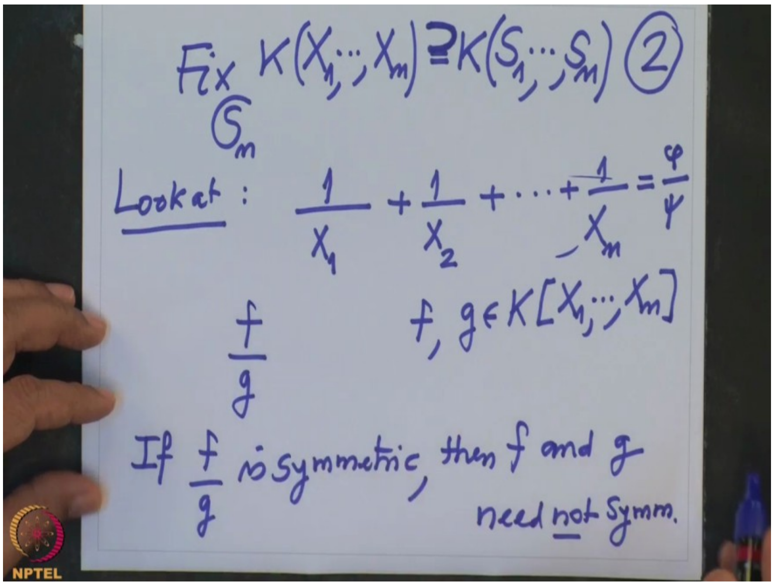
So last time you finish the proof of the fundament theorem on symmetric polynomials, so we have proved that the fixed fields with respect to Sn of the polynomial ring is precisely the polynomials in S_1 to S_n with coefficients in K I just want to illustrate these by one example, our process. So for example you get the polynomial $X_1^2+X_2^2+...+X_n^2$ this polynomial is obviously symmetric polynomial.

This is symmetric polynomial in $K[X_1,\ldots,X_n]$, so what is our process to write it as a polynomial in S_1 to S_n, what? So what is the multi-degree turn is, this one. X_1^2 is the multi-degree of, so 20 0 0 0 this is a multi-degree of this polynomial f and we know what to cancel this term and so on. But directly also you can see this is very simple, if you take S_1 and square it which is $(X_1+...+X_n)^2$, so this is symmetric and we subtract from this given polynomial f and then this term will get cancelled and keep doing it but in this case observation is very clear.

This is $X_1^2+X_2^2+...+X_n^2$ minus the cross terms, so that is 2 times $X_1X_2+X_1X_3$ and so on. So for 2 at a time, so this is nothing but S_2, so this is therefore the given polynomial f, this was f and I shift these 2 S_1 to the other side, so this f will be equal to $S_1^2-2S_2$ which is the other side is clearly symmetric. And this one this is the process, so this is actually our proof is very algorithmic.

Alright, see this is one another remark I want to make is little bit more serious because, see we have proved that now I want to know about the rational functions.

(Refer Slide Time: 3:20)



So I want to say the fixed field of Sn of the rational function field X_1 to X_n this is equal to rational functions in S_1 to S_n this I want to check. So obviously this is obvious because if you do the rational function in S_1 to S_n then all these Sis are fixed under every permutation therefore the polynomial will be fixed under every permutation and this is a polynomial divided by polynomial. So therefore they will be fixed therefore rational function is fixed, so this proof is clear.

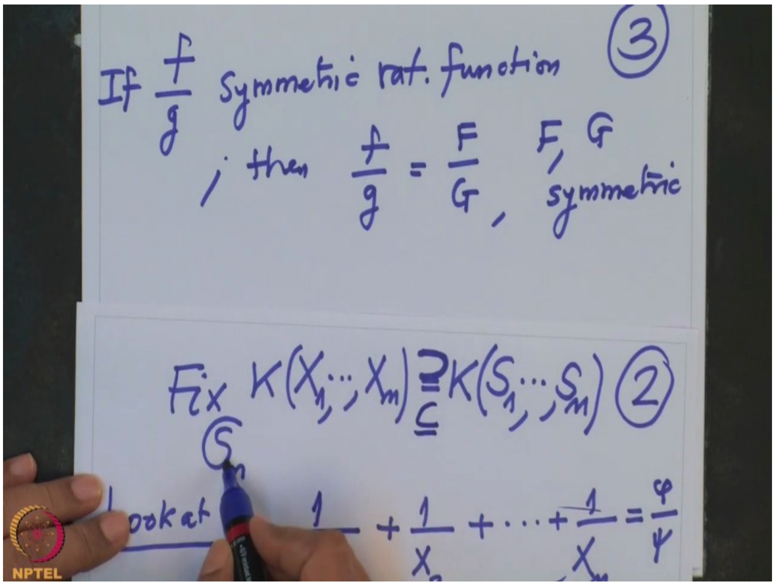
But to the other proof it is little bit more serious because look at example, look at the following example 1 over X_1, this is a rational function 1 over X_2 this is also rational function plus so on and so on plus 1 over X_n this is a rational function and what is it? if I want to write it then but how do you write this as a quotient we want to write this as some polynomial what do I call it? Some polynomial ϕ by some polynomial ψ where this ψ is the polynomial in S_1 to S_n and ψ is a polynomial in S_1 to S_n.

So we need little bit more work, so therefore we cannot say that if we have a rational function f by g suppose f and g are 2 polynomials and I consider this rational function f, g in

$K[X_1,\ldots,X_n]$ and if I call this as this is my rational function, this is symmetric if f by g is symmetric then f and g need not be symmetric. There is very easy because here is an above example.

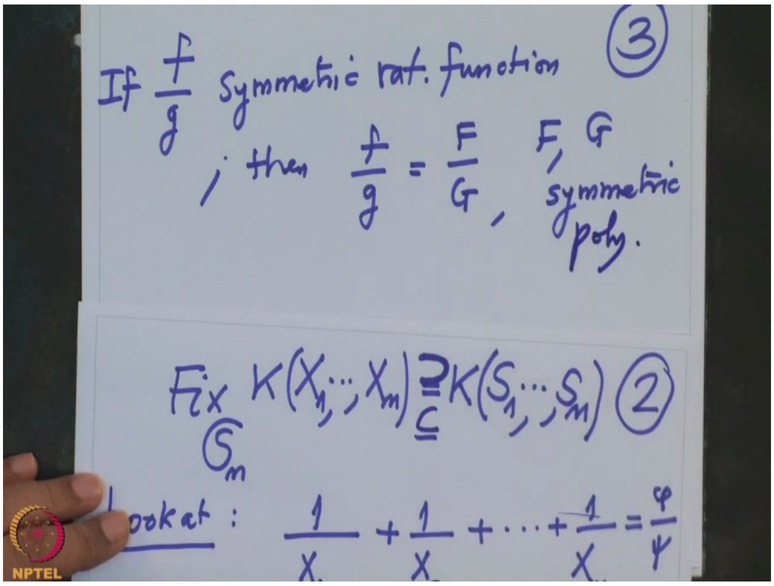
You see if I write it what you see inside this case? ψ will be obviously X_1 to X_n and ϕ will be what? That will be I have to multiply this by X_2 to X_n and so on. And that will be the sum, so therefore if a rational function is symmetric than the individually f and g may not be symmetric polynomial but you know writing this is not a unique way of writing the rational functions.

(Refer Slide Time: 6:28)



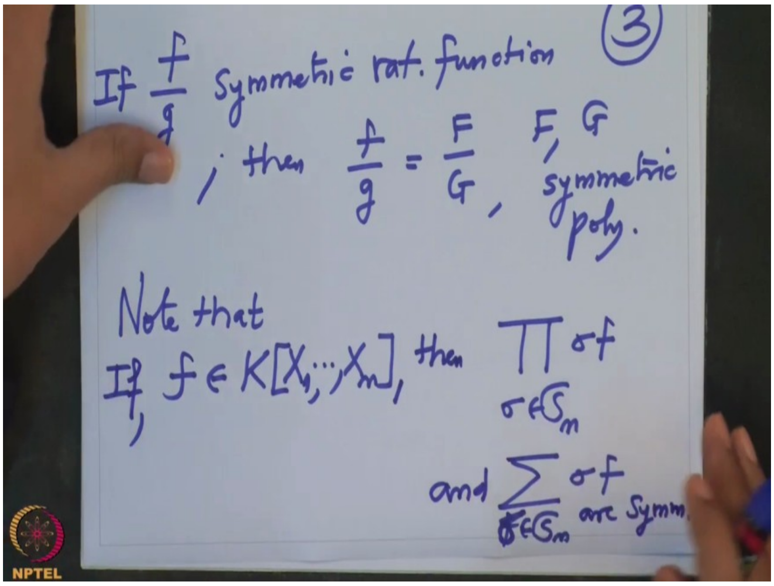
So how do you make it more clearer? Alright, so I will take suppose f by g is symmetric assume that. If f by g is symmetric rational function then I want to write I want to write f by g by capital F by G, so that F and G are no symmetric then that will prove the other inclusion.

(Refer Slide Time: 7:06)



Then this will prove this will prove this inclusion because as to how do they do rational function which is symmetric and I have written it as F by G where F and G are symmetric polynomials, so I have to prove this.

(Refer Slide Time: 7:17)

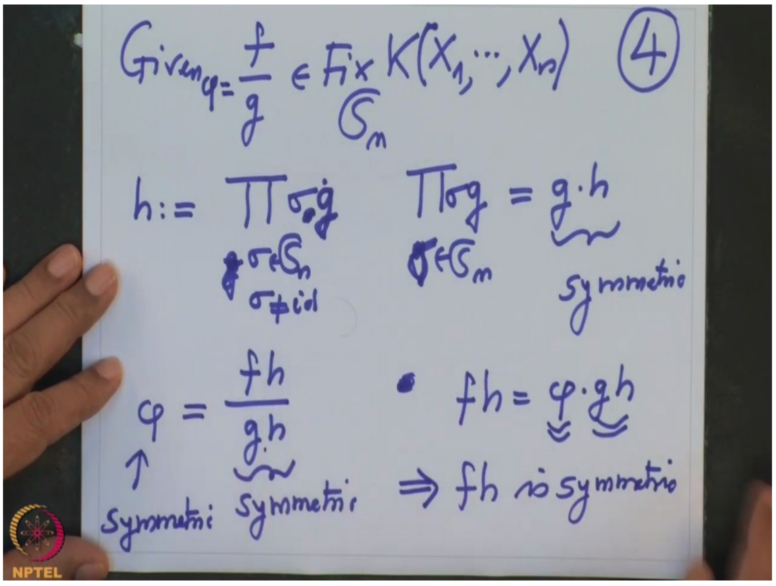


And this means I have to I'm allowed to multiply up and down by the same polynomial then this action doesn't change that is ideal. So what will I multiply by? So obviously note that how do I make a given polynomial, if I have even arbitrary polynomial f, arbitrary. How do I make it symmetric? So to make f symmetric what I have to do is?

I have to take the product, product is varying over σ in S_n, σ of f, σ f these are obviously symmetric because when I take any permutation, apply permutation to this product. Permutation is a k algebra homomorphism, no. So therefore this will be product and therefore this is clearly symmetric because if I apply σ that is applying σ here but then because this is a group this product will not change, so it is symmetric.

Either this or also another one is sum, take the sum σ f f, σ varies in S_n both these are symmetric polynomials. If note that if f is arbitrary polynomial then this and this are symmetric this is what I will use it, okay. Now obviously f is a factor here because σ is identity, so it is a factor, f is a factor there.

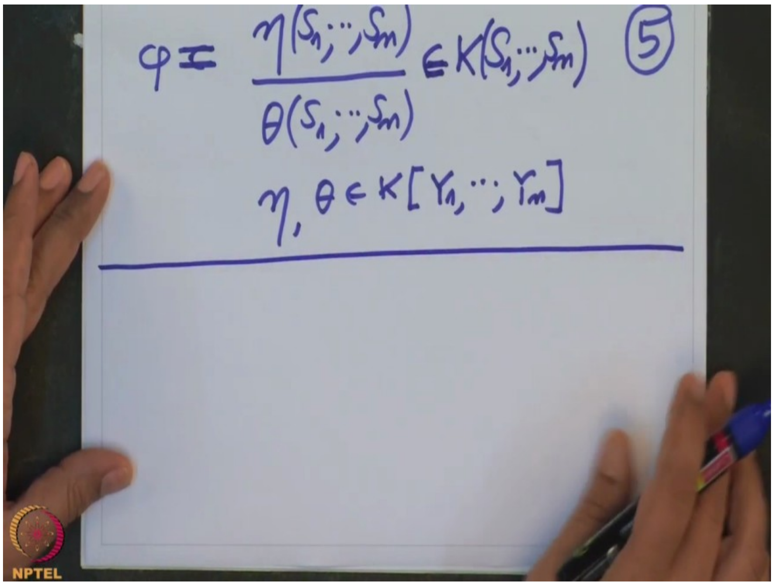
(Refer Slide Time: 9:24)



So now given f by g in the fixed Sn $K[X_1, \ldots, X_n]$ symmetric rational function then I am going to multiply up and down by h. So h equal to product σ g as σ varies in Sn but σ is not identity to get this product. So obviously what I said was the g is if I take product σ in S_n σ g, this is g times h and this g times h is symmetric.

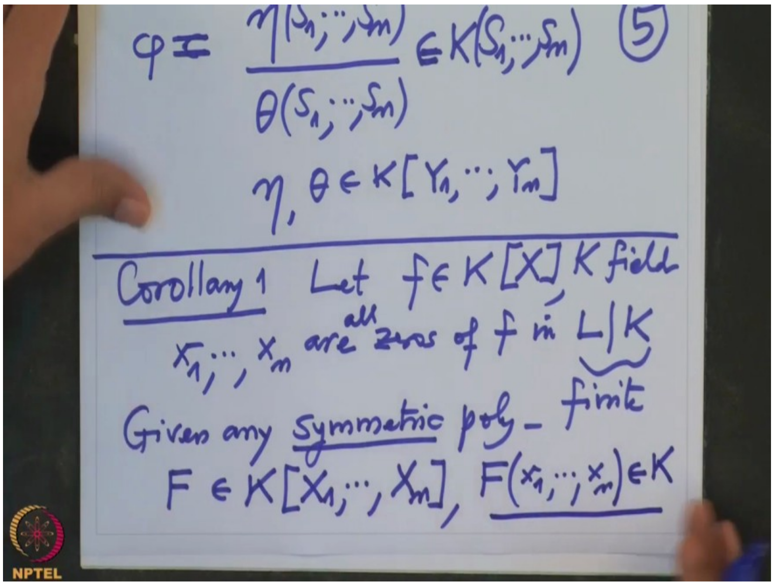
And now I'm going to multiply up and down by h, so f h and gh now this becomes symmetric and this is my ϕ, let's call this as ϕ, ϕ or symmetric. So I have symmetric and this is symmetric therefore fh which is ϕ times gh but now because ϕ is symmetric gh is symmetric therefore fh is symmetric. So therefore both are symmetric.

(Refer Slide Time: 11:43)



So therefore the ϕ we have written it as some polynomial above because it is a symmetric polynomial. It is a polynomial some η of S_1 to S_n divided by θ of S_1 to S_n. Where η and θ are polynomials in n variables or K and this is therefore an element in K S_1 to S_n, so that proves our theorem for rational function field also and we are interested in more in that.

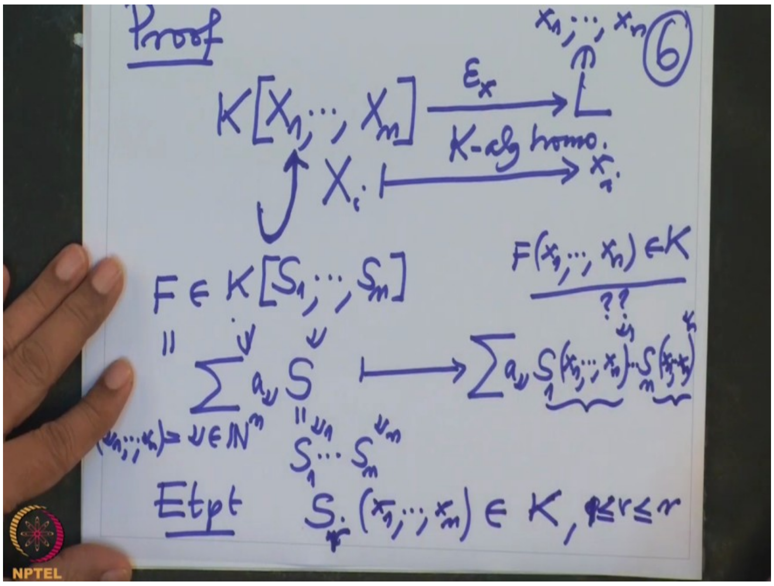
(Refer Slide Time: 12:36)



So now I'm going to deduce couple of corollaries from this theorem, so for example Corollary 1, okay. So suppose I have any polynomial f in 1 variable, now you see I'm going deduce consequences for polynomials variable, so suppose let I have f is polynomial in 1 variable over f a filed K, k Field. And suppose X_1 to X_n are zeros of f in L over K. So I'm taking all zeros, we know that there exist a finite field extension L over K such that all the routes of f lie there.

This was precisely Kronicker's theorem, so I have a field extension where all the roots are there, okay. Then what? What am I saying? Then given any symmetric polynomial capital F symmetric is very important in n variables K, I will call them $K[X_1, \ldots, X_n]$, given any symmetric polynomial in n variable capital F, if I evaluate this F at X_1 to X_n then this is an element in K, that's what I want to check.

(Refer Slide Time: 14:30)



So that means what, so proof? Proof, what we are doing is a falling? We have a polynomial being here $K[X_1, \ldots, X_n]$ and we have that field L where all these routes X_1toX_n they all belong to this capital L and we have the substitution homomorphism here ϵ_X. What is it? These variables capitals X_i go into small x_is this is the key algebra homomorphism. And what I'm saying now?

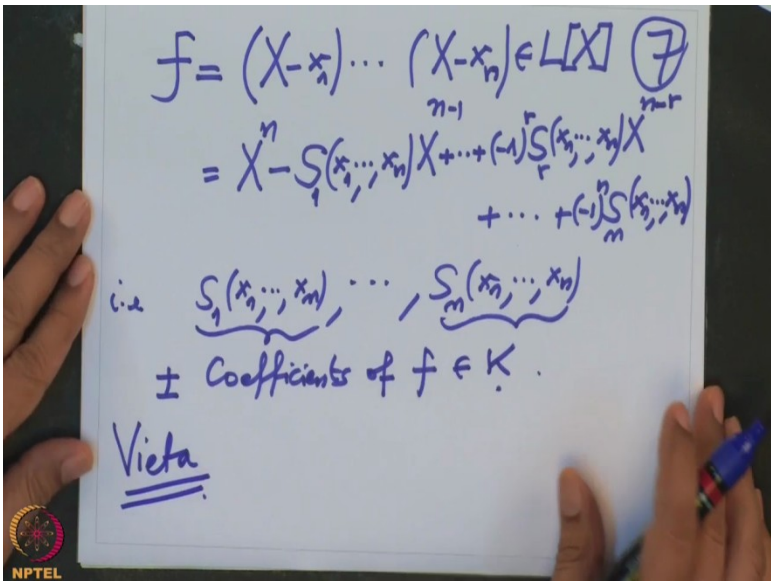
A polynomial capital F symmetric means what? That is a polynomial in capital S_1 to S_n or take an arbitrary polynomial F and this is contained here, all this is contained here. In fact this is the fixed ring of this under the action of Sn, F is here and take its image here appropriately it lies in L but I'm saying it actually lies in K, so F of$X_1$to$X_n$this is the image of F under this, this actually lies in K that is what we want to prove, this is what we want to prove.

Why that? That is very simple because what do we know this is a polynomial in S_1 to S_n and therefore if I write this as as summation $a_v S^v$ this is running over v finite subset and a vs are elements in the field K and this is the standard notation what we are using it $S_1^{v_1} \ldots S_n^{v_n}$ where this v is v_1 to v_n then where is the image?

This goes to the same here, this is natural inclusion map and then I have to evaluate, so where does it go? so this polynomial F goes to summation a miu because a mius are constant so they go to the same and this one will go to S_1 evaluated at X_1 to $X_n^{v_1}$ and so on. Sn evaluated at X_1 to $X_n^{v_n}$ this is where it goes. So I only have to check, so enough to prove.

Enough to prove that if I take any elementary symmetric polynomial S_i or S_r and evaluate it at X_1 to X_n that should belong to K this is what enough to check for all r from 1 to r where all these guys individually they are in k therefore their powers are in K therefore the sum is in K and then you finish.

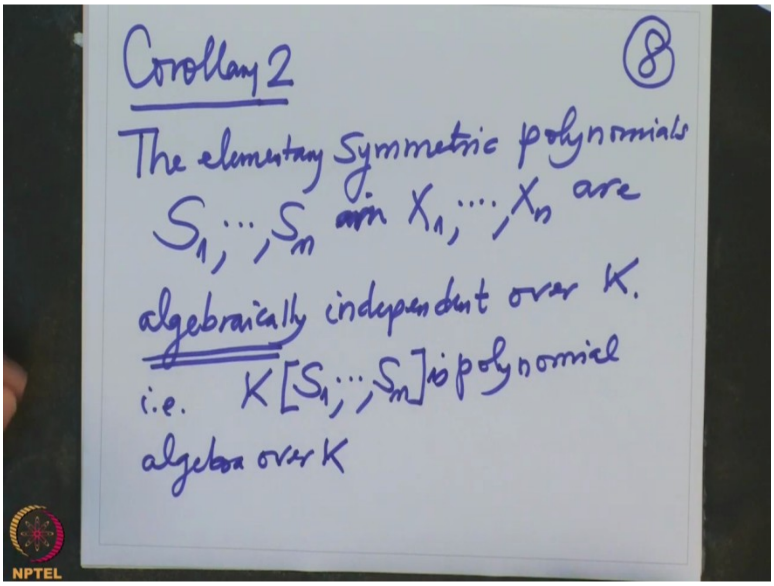
(Refer Slide Time: 17:58)



But what do you know about this? What is the relation between F roots and the symmetric function? So remember f is splits into linear factors that is this, this is in $L[X]$ under there and when I expand it what do I? I get $X^n - S_1(X_1, \ldots, X_n, X_{n-1})$ and so on. Middle term (-$(-1)^r$ X Power S_r evaluated at X_1 to X_n times X^{n-r} and so on.

The last term is $(-1)^n S_n(X_1, \ldots, X_n)$ this is what when we expand it and collect the terms together. And these are where then, these are precisely therefore that is $S_r(X_1, \ldots, X_n)$ so on, S_n evaluated at X_1 to X_n these are coefficients of f and they belong to therefore K and plus minus sign. So therefore all these terms they belong to K therefore the f evaluated atX_1 to X_n will belong to K, so that finishes the proof. So this was Vieta, okay so that was corollary 1.

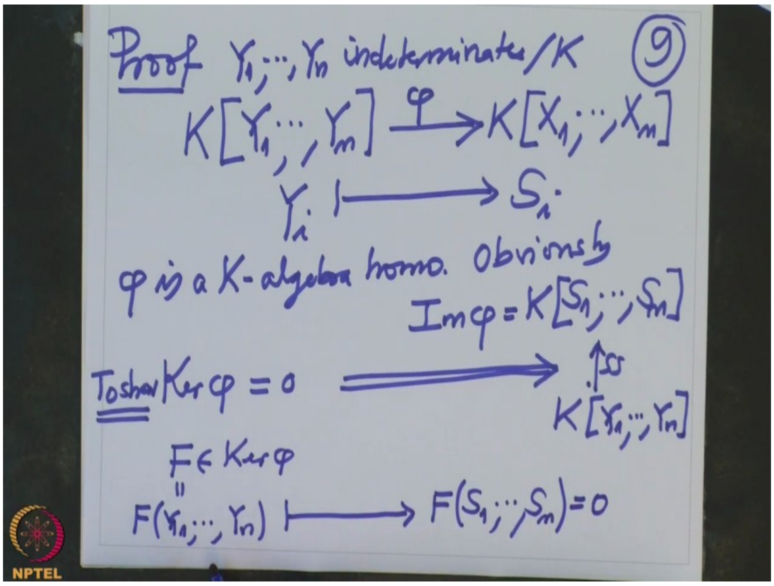
(Refer Slide Time: 19:52)



Now corollary 2, okay now I want to say that the elementary symmetric functions symmetric polynomials I sometimes interchange the word polynomials and functions but they are same at least for us in this context. Elementary symmetric polynomials S_1 to S_n are in X_1 to X_n are algebraically independent over K that means they don't satisfy any relation among themselves, any polynomial relation among them not only linear they are algebraically independent, no relation.

So that means this polynomial this sub algebra is actually are polynomial algebra over K so they behave like a variable.

(Refer Slide Time: 21:24)

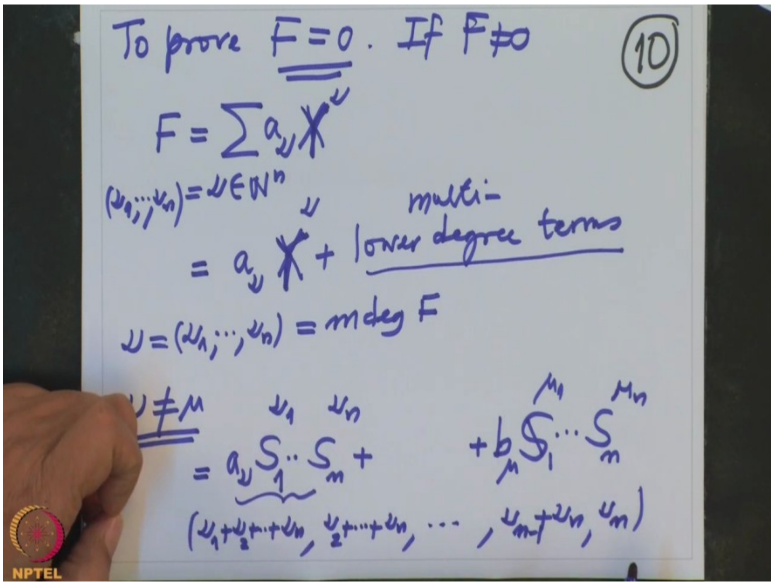


So proof, okay proof is very simple. Proof, what do we want to prove? So we want to prove that they are algebraically independent that means given any variables K n variables Y_1 to Y_n these are indeterminates, Y_1 to Y_n are indeterminates over K, so this is a polynomial algebra. And from here we are giving a map to $K[X_1,\ldots,X_n]$ this map is what if I want to give a map from one polynomial algebra to the other K algebra I just have to give its values on the variables.

So I will map Y_is to S_is and I want to check, so let us call this map as ϕ, so ϕ is a K algebra homomorphism, obviously image of ϕ is a K sub algebra generated by the images of Y_i that is S_1 to S_n and I want to now show the kernel of ϕ is 0, to show kernel of ϕ is 0, once I show this, this symmetric K sub algebra generated by the elementary symmetric polynomials, this will be isomorphic to the $K[Y_1,Y_2,\ldots,Y_n]$ mod kernel but kernel if I would have put 0 this will be isomorphic to K Y_1 to Y_0.

So that is because of this so I have to prove this, so that means what I have to prove that the kernel is 0 that means suppose F is in the kernel, suppose capital F belong to kernel of ϕ, so these F is actually polynomial in Y_1 to Y_n, so let us write it Y_1 to Y_n and it goes to 0 means when I substitute Y_i is capital S_is I get 0. And then what do I want to prove? I want to prove that F is actually a 0 polynomial.

(Refer Slide Time: 24:15)



So I want to prove, to prove capital F is 0 polynomial that means no coefficient of F is 0, alright. So suppose it has some term which is nonzero, so remember we have written in a multi-degree setup F we have written it as summation $a_\nu X^\nu$, a_ν is a tuple varying in $\mathbb{N}^n$ only finitely many terms nonzero. So suppose F were non-zero, if F is nonzero, F is nonzero that there will be a multi-degree term and there will be highest degree term, so highest multi-degree term.

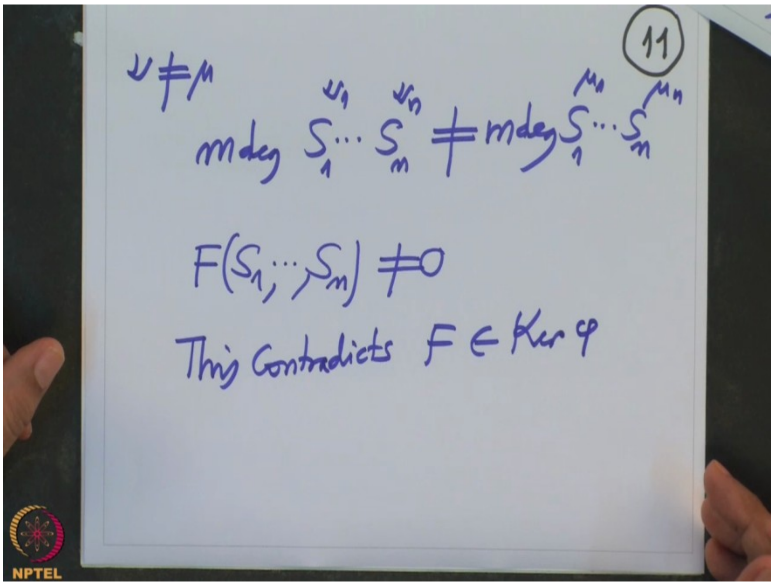
So this F will look like $a_\nu X^\nu$ plus lower multi-degree I should say But now when we write like this when we write like this, this ν which is ν_1 to $\nu_n$in our notation it is multi-degree of F and therefore this monomial will not occur anyone else in between, in this side it will not occur.

Not only that all the monomials are different, so when mui is different this when ν not equal to ν then these terms are different, so what will happen when will this X^ν will go when I put not X it should have been Y here they are polynomials in Y. So when I put Y_i is equal to capital S_is what will I get? I will get $a_\nu S_1^{\nu_1} \ldots S_n^{\nu_n}$ and somewhere else here.

If there is some term here some b ν $S_1^{\nu_1} \ldots S_n^{\nu_n}$. Now I want to say that what is a multi-degree of this one? So we have seen multi-degree of this one is $\nu_1 + \ldots + \nu_n$, one at a time we are dropping, so at the last one will be $\nu_{n-1} + \nu_n$, ν_n this is a multi-degree term.

Because here it will be when you raise it to power mui1 that is the first one when you raise the next one is to power ν_2 that is this one and so on. When you raise this, what will be the last coordinate here? That is $X_n^{\nu_1}$ and so on.

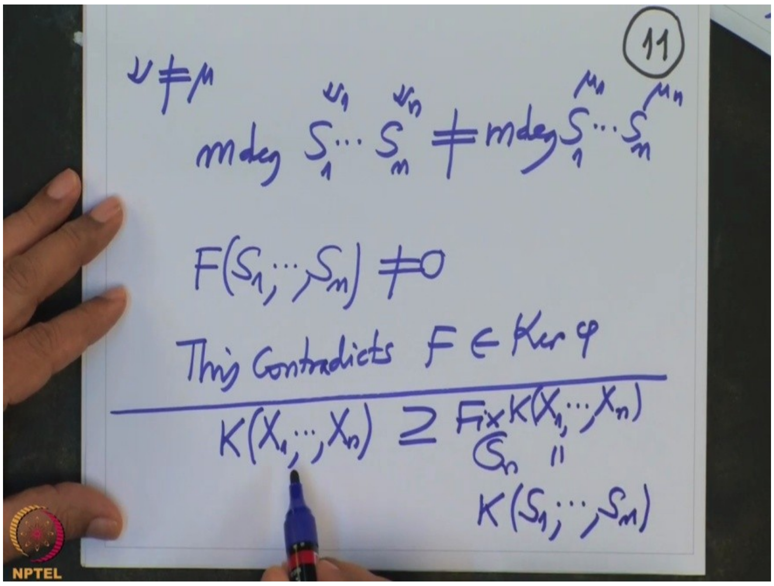
(Refer Slide Time: 27:52)



So what I want to say is the following the multi-degree terms are different, so when mui and mui are not equal multi-degree of S1 mui1 Sn mui n is different from multi-degree of S1 mui 1 Sn mui n, so how can they get cancelled? So nobody will get cancelled, so the terms are as it is they will appear in F of S_1 to S_n, so therefore F of S_1 to S_n will also be nonzero, if F is nonzero.

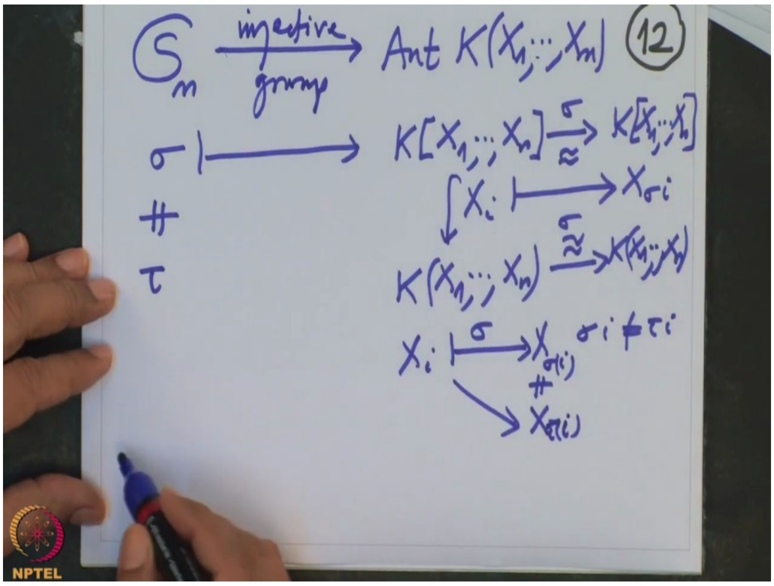
But we are assuming that therefore in the kernel, so this contradicts F belongs to the kernel of ϕ, alright. So we have proved that corollary 2 that the variables are this S_1 to S_n are algebraically independent over K.

(Refer Slide Time: 29:06)



Next time therefore we are in the following situation. We have this rational function field $K[X_1,\ldots,X_n]$ which contains the fixed field of Sn and this is what precisely the field generated over K by elementary symmetric polynomials this.

(Refer Slide Time: 29:37)



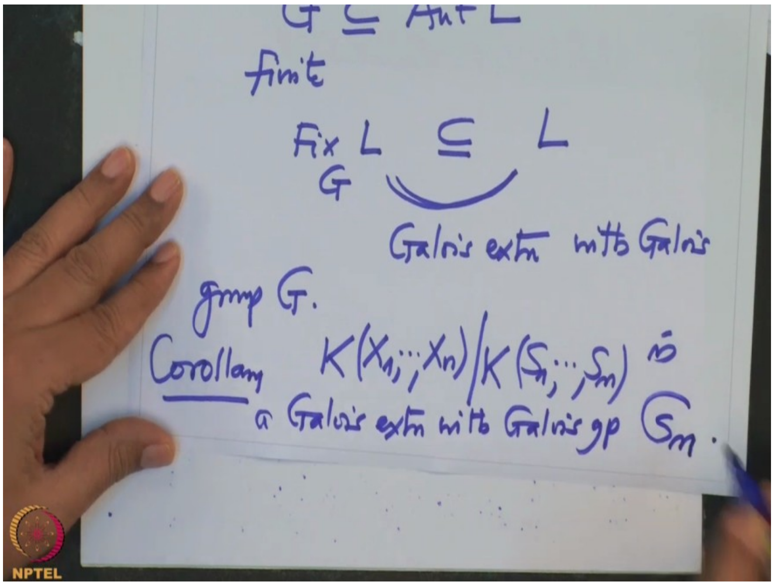
So we definitely know, so remember that this Sn and the Automorphisms of the rational function field there is a map here and σ going to, I want to define an Automorphism of this field. So it is enough to define Automorphism of the polynomial ring, so $K[X_1,\ldots,X_n]$ to $K[X_1,\ldots,X_n]$ the σ, the same σ square Xi will go to X σ i this is clearly an Automorphism of this polynomial algebra.

And therefore that will give that we can exchange that Automorphism to the rational function field that I will call it again σ only, so therefore each σ permutation on 1 to n will give you Automorphism of this field, this is a big field. And moreover this map is injective because from this Automorphism you can always recover that σ that is in fact you know that is related to the inverse of this Automorphism.

or in other words the σ and τ different, these Automorphism's are different clear because X_i and $X_{\sigma(i)}$, X_i goes to $X_{\sigma(i)}$, so if σ is not equal to τ then at least one σ i will not be $\tau(i)$ and therefore X_i under σ it will go to $X_{\sigma(i)}$ and $\tau(i)$ it will go to $X_{\tau(i)}$ but these are different therefore these are different therefore σ is not equal to τ, so it is injective group homomorphism .

So therefore this group S_n is finite, this is a subgroup of this Automorphism group.

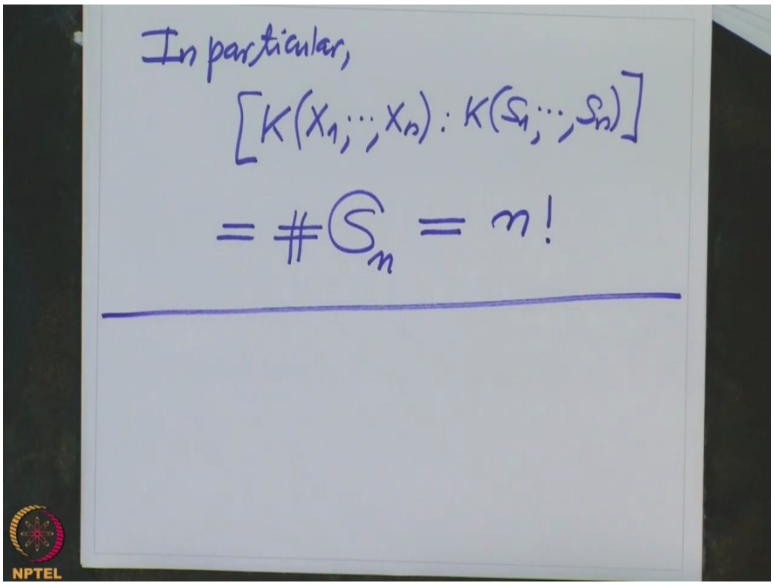
(Refer Slide Time: 31:52)



So I want to remind you that we have proved earlier that whenever we have field L, L is any field and if I take a finite subgroup G of Aut L finite then we have proved that the fixed field, this is operating on else therefore we have checked that fixed field of the G operation on L this is a subfield of L and this extension is Galois extension with Galois group G. Therefore we have proved the following corollary.

We have proved that $K\left[X_1,\ldots,X_n\right] \vee K\left[S_1,\ldots,S_n\right]$ is a Galois extension with Galois group S_n. In particle we have a Galois group S_n of this extension but remember this is not $\mathbb{Q}$, our Galois problem is finding an extension of $\mathbb{Q}$ which is Galois and Galois group is a given group, so still we are far away from that inverse Galois problem but at least this nice result is there. That this extension is Galois with Galois group Sn in particular the degree is in factorial.

(Refer Slide Time: 33:41)



So in particular degree of $K[X_1,\ldots,X_n] \vee K[S_1,\ldots,S_n]$ this degree is precisely equal to order of the Galois group which is S_n and order of the S_n is precisely $n!$, so with this I will end this lecture and we will continue studying symmetric polynomials more and then next what will come is, the discriminant and then I will also get field extension and then we will find the order of that feel extension and also we will find that Galois group of that field extension and that will be precisely the alternative group.

So thank you and we will continue in next time.