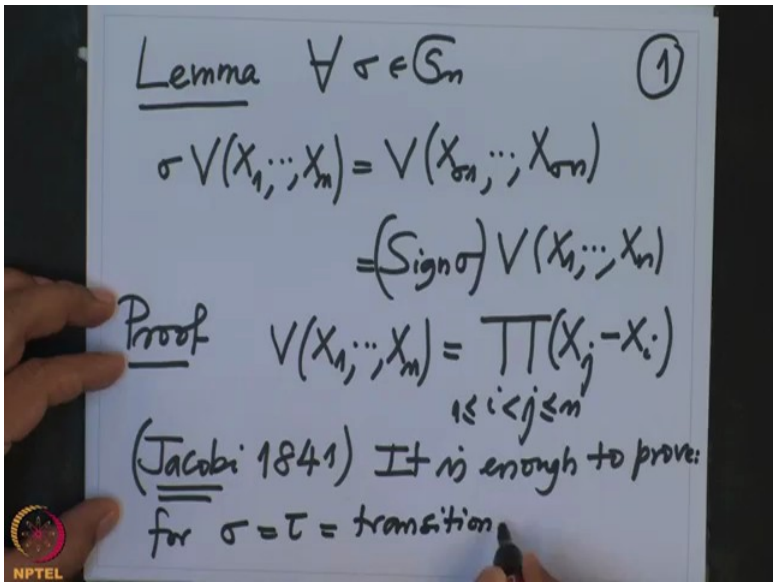
**Galois' Theory**
**Professor Dilip P. Patil**
**Department of Mathematics**
**Indian Institute of Science, Bangalore**
**Lecture 48**
**Discriminant of a polynomial**

(Refer Slide Time: 00:36)




Alright now we after a digression on the signature of a permutation etc. now we come to the proof of the lemma I stated, so the lemma we wanted to prove was so this was the lemma that for every permutation $\sigma \in S_n$, if I permute the Vandermonde determinant variables that is if I write $V(X_{\sigma 1}, \ldots, X_{\sigma n})$, what I get is sign of $\sigma$ times the Vandermonde determinant.

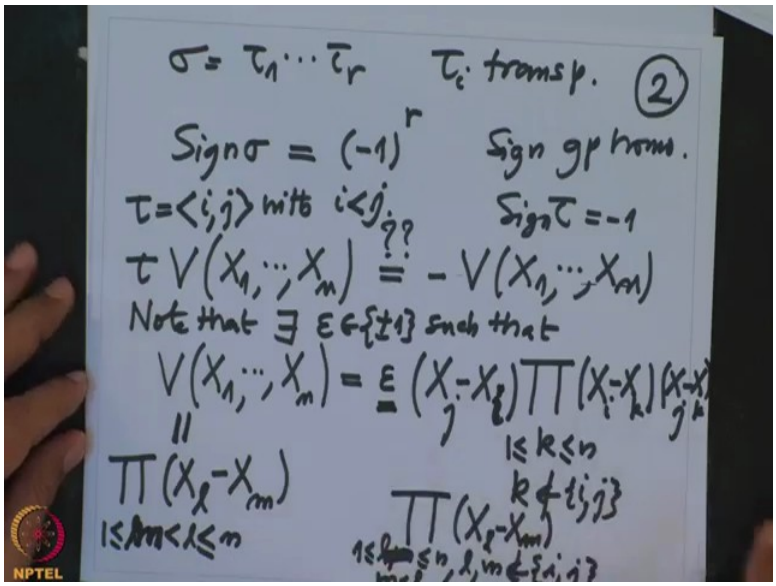
So this Vandermonde determinant is not a invariant under all permutations but it is invariant under only at the permutations where sign is 1 that is advantage, so proof, so what was the Vandermonde determinant was by definition was this, $V(X_1, \ldots, X_n)$, this is the product, product is running over this and this is $i \leqslant j$, $X_j - X_i$ and I wanted to apply $\sigma$ to this variables, I want to permute the variables according to the $\sigma$ and so the proof I am going to give, this is a proof due to Jacobi that was in 1841.

Because Jacobi studied what happens to the Vandermonde when you permute the transpositions, when you permute, when you apply a transposition to the variables what happens to the Vandermonde determinant, Jacobi study that, so that means so it is enough to prove that, to prove this formula for transpositions because every we saw in digression that

every permutation is a product of disjoints cycles and every cycle is a product of transpositions.

I am not saying disjoint transpositions but transpositions so all together every permutation is a product of transpositions and the sign is a homomorphism so sign commutes whether I compose the transpositions, apply the sign or take the signature and multiply that so therefore it is enough to prove for $\sigma$ equal to $\tau$ where $\tau$ is a transposition.

(Refer Slide Time: 03:30)




Because remember if $\sigma$ is a product of r transpositions, $\sigma = \tau_1 \ldots \tau_r$ , these are, tau i's are transpositions then sign of $\sigma$ will be $(-1)^r$ because here I am using sign as a group homomorphism and sign of a transposition is -1 this therefore enough to prove that I have to prove this $V(X_1, \ldots, X_n)$ and if I apply $\tau$ to this I get $-V(X_1, \ldots, X_n)$ , this is what we have to prove, this is enough to prove alright.

Note that by definition of these Vandermonde I will rearrange this product and when I rearrange I will have to multiply by $\pm 1$ so note that there exist $\epsilon$ belonging to $\pm 1$ such that this $\epsilon$ times $X_j - X_i$ okay and now I am assuming, I want to prove this formula for $\tau$ so $\tau$ is the transposition i j with i strictly less than j and then I want to prove this equality.

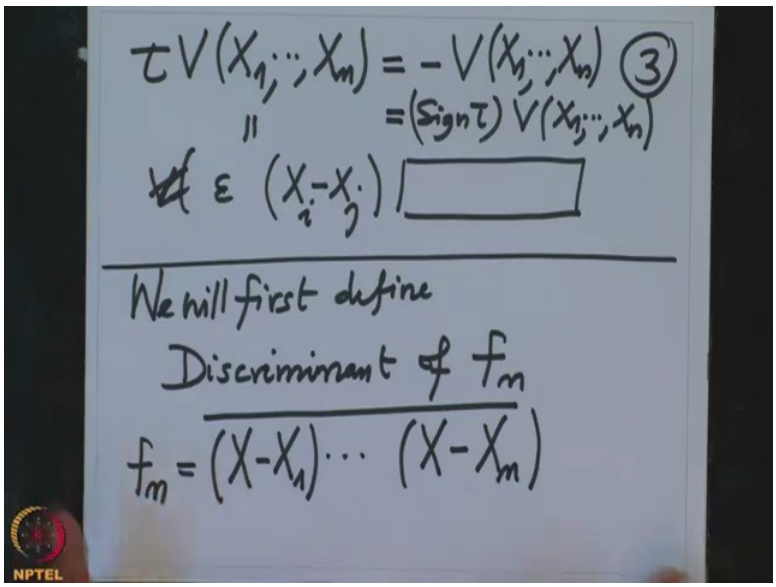
So find $\epsilon$ which belongs to $\pm 1$ , this times product, product is running over k, k is in between 1 and n and k is not in the set i j, this is $(X_i - X_k)(X_j - X_k)$ and still I have to, no place here but product now this product is running over l and m in between 1 and m and l m

both are not in i j and this product is $X_l - X_m$ , so here I should have written m is strictly less than l, m and l in between but strictly less than this and l and m not in i and j.

So I have rearranged these product, see originally this was a product X, now I will write $X_l - X_m$ , 1 less equal to l less equal to m less than l less equal to m, this was the definition because i and j are fixed here so I do not want to use that running index and this I want to rearrange this, first of all if l and m they are different, they are not in i and j because none of them is i and j then I have kept that as it is.

The remaining factors will have the property that l and m is i j or they are different form so that is and then while rearranging this I might have to apply by some either -1 or 1 so this is very easy now I have to apply $\tau$ to this, when I apply $\tau$ to this what happens.

(Refer Slide Time: 07:49)



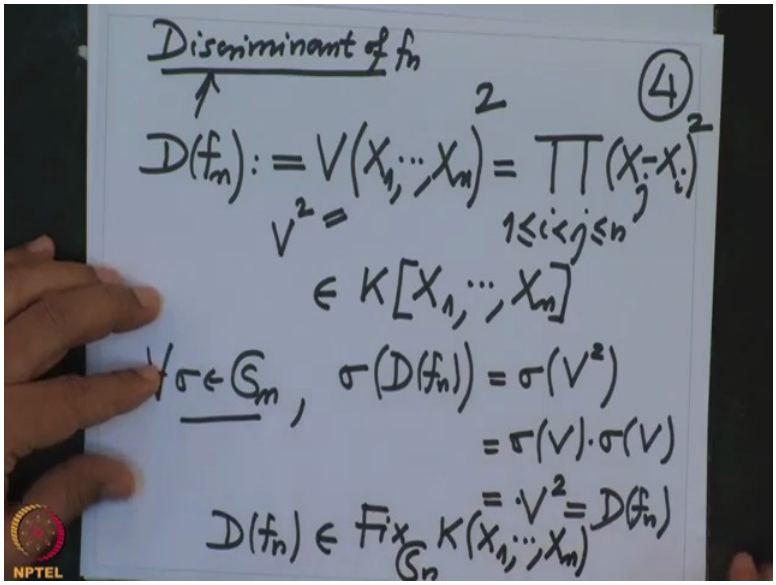

So therefore $\tau$ of $V(X_1, \ldots, X_n)$ , this is what we want to compute, this is V of so I am applying $\tau$ to this side so that I push the $\tau$ inside then what will happen to this, this $\epsilon$ remains as it is and this i and j get change, i and j this becomes $X_i - X_j$ and this factor does not change now because this will go to this and this will go this, so this factor does not change because this one go to this and this one go to this.

So the factor does not change and this one do not change at all therefore only one change happens namely this change, this has become this, so therefore it is obvious that this is equal to, so remaining it is same as earlier and therefore this $\epsilon$ also remains same so therefore

the $\tau$ of this V is nothing but minus $V(X_1,\ldots,X_n)$ which is equal to sign of $\tau$ times $V(X_1,\ldots,X_n)$ .

So therefore we have proved our lemma that, so this proves the lemma. Alright now remember our problem was to define discriminant of a polynomial so I am going to define first, so we will first define discriminant of $f_n$ , this is a general polynomial of degree n, so I have these polynomial $f_n=(X-X_1)...(X-X_n)$ , this is a polynomial that the advantage here is, I have the variables only so I can play around with the polynomial, so I want to define the discriminant of this.

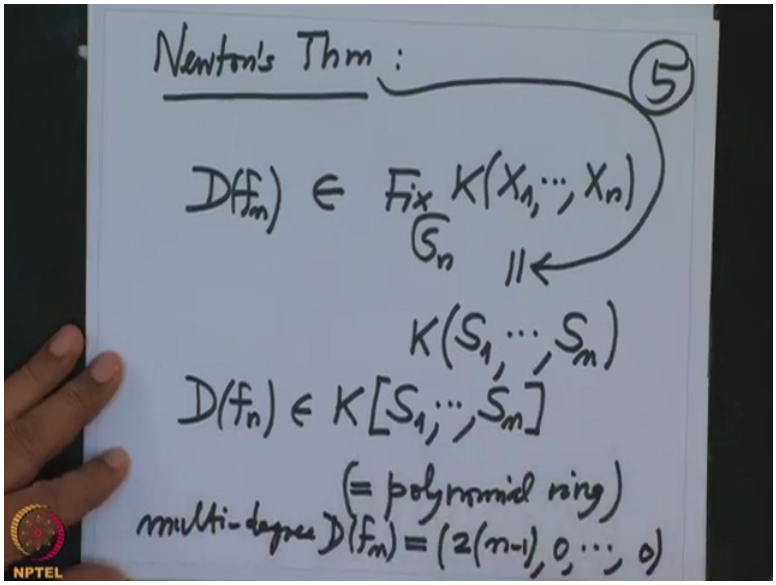
(Refer Slide Time: 10:26)




Alright so you take the Vandermonde of $X_1,\ldots,X_n$ and take its square so what is this? Before taking the square it is a product 1 less equal to i strictly less than j less equal to n and $X_j-X_i$ and I take the square so I take the square inside this, this is by definition discriminant of $f_n$ , this is called a discriminant of $f_n$ . Now where is this, note that this is clearly a polynomial in n variables over k and also note that see I have taken the square therefore it is very clear that for every $\sigma\in S_n$ , $\sigma(D(f_n))$ is, I will just abbreviate this by V.

So this is $V^2$ , this is $\sigma(V^2)$ which is $\sigma(V)\sigma(V)$ but this is -V and this is -V so it is $V^2$ which is $D(f_n)$ , so what does that mean? That mean this $\sigma$ , this discriminant is fixed under every $\sigma$ so that means this discriminant $f_n$ belongs to the fixed field of $S_n$ of the rational functional field in n variables but we know it by Newton's Theorem.

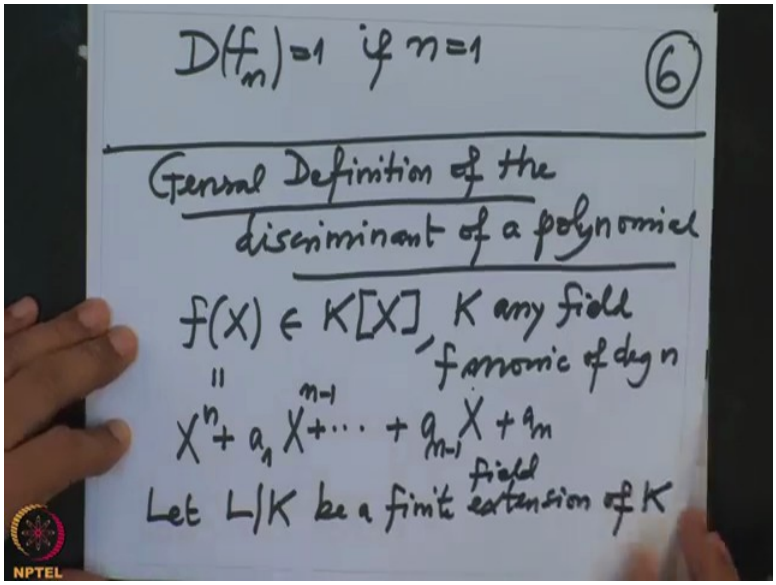
(Refer Slide Time: 12:37)




We know Newton Theorem, we know that this fixed field is precisely the quotient field of, it is a function field in elementary symmetric polynomials $S_1,\ldots,S_n$ , this is a Newton's Theorem is equality and we have proved that $D(f_n)$ is an element here so therefore $D(f_n)$ is actually you know it is a polynomial therefore $D(f_n)$ is actually belongs to the polynomial ring generated by $S_1,\ldots,S_n$ over k, this is the polynomial ring we have check last time, this is a polynomial ring generated by $S_1,\ldots,S_n$ over K, this is the polynomial ring we have checked last time, this is a polynomial ring.

Because we have checked that $S_1,\ldots,S_n$ are algebraically independent and this is therefore discriminant is a polynomial in $S_1,\ldots,S_n$ alright. Also you can check this I will not use but it is interesting to mention, this is a polynomial in $S_1,\ldots,S_n$ and the multi-degree of this polynomial $D(f_n)$ is 2 times n minus 1, 0, 0, 0, 0, this is the degree of the highest polynomial which appear in these polynomial.

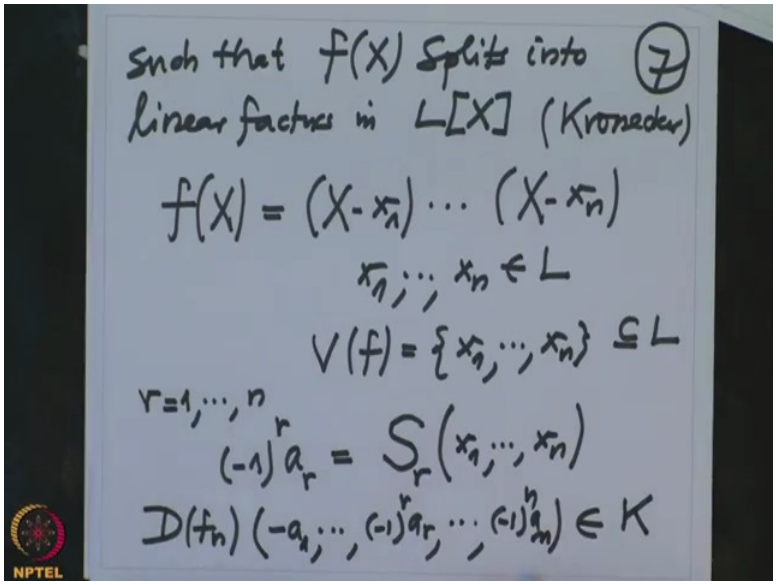
(Refer Slide Time: 14:31)




Note that when n is 1, $D(f_n)$ is 1, if n is equal to 1 because in this case the matrix is identity matrix therefore the determinant will be 1, anyway so that was, so we have proved that the discriminant is the symmetric polynomial and therefore it is a polynomial in elementary symmetric functions, now you can do a general definition, so general definition of the discriminant of a polynomial and this will actually we do not need over field, we can do it over arbitrary commutative ring but this course I will stick to the field.

So start with any polynomial $f(X)$ over any field in one variable, K any field and write it as and I can assume it is monic so f is monic, f monic of degree n, so f looks like $X^n + a_1 X^{n-1} + ... + a_{n-1} X + a_n$ , any polynomial of degree n monic look like this where these ai's are the co-efficients, they are in the base field k, alright then we know that what is the relation between $a_i$ 's and the roots of these polynomial. Now remember we have to enlarge our field so let L over K be a finite extension, finite field extension of K.

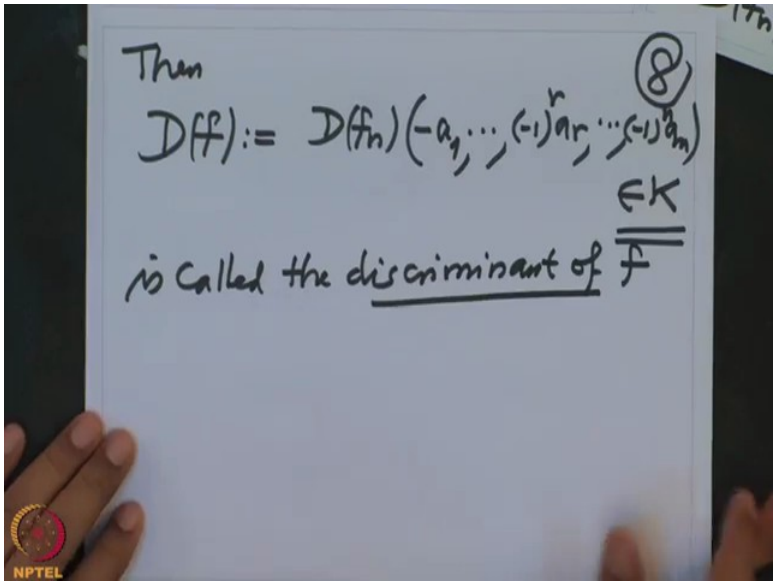
(Refer Slide Time: 17:00)




Such that $f(X)$ splits into linear factors in $L[X]$, this was what we proved this theorem long back due to Kronecker, that means what, in symbols $f(X)$ we can split this into linear factors because f is monic, all factors are linear so it is like this, where $x_1,\ldots,x_n$ they are precisely all zeroes of f and they all lie in L, they could be repetition. So V of f is therefore $x_1,\ldots,x_n$ and they all lie in L and what is the relation between these exercise and the co-efficients that we studied last time, in fact what we know is in general for any r from 1 to n, $(-1)^r a_r$, this is nothing but the elementary symmetric function $S_r$ and then evaluate this at the, this zeroes.

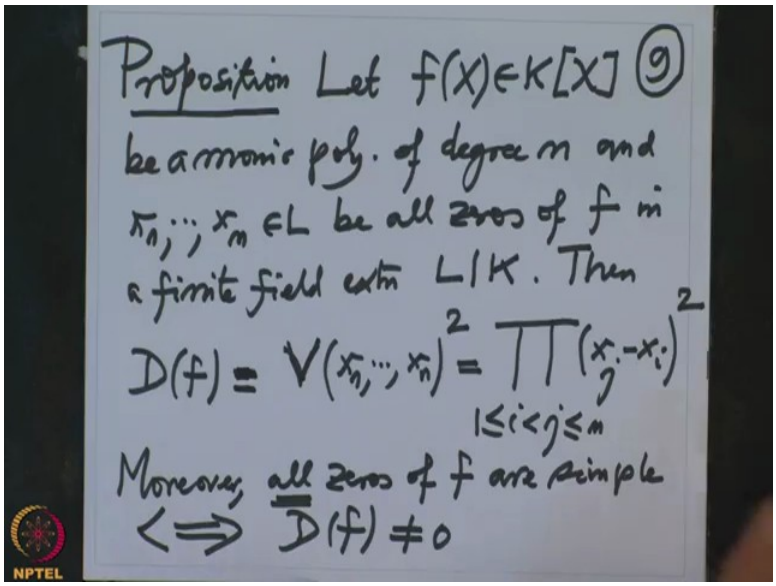
So $S_1$ is the $a_1$ that is the first co-efficient and so on, first means co-efficient of $X^n-1$, so therefore we know that $D(f_n)$, this is a polynomial in this guys therefore when I evaluate this symmetric polynomial at these points that is $-a_1$ etc. $(-1)^r a_r$ etc. $(-1)^n a_n$, this is actually indeed an element in K, this is also what we proved last time, therefore this make sense and this is called the discriminant of f.

(Refer Slide Time: 19:18)




So we say that then $D(f)$ is by definition take $D(f_n)$ and evaluate this $D(f_n)$ at these points, this is an element in K because I evaluated this was a polynomial in n variable over K and I evaluated at the points in K therefore this is indeed an element in K, this is called the discriminant of f.

(Refer Slide Time: 20:14)



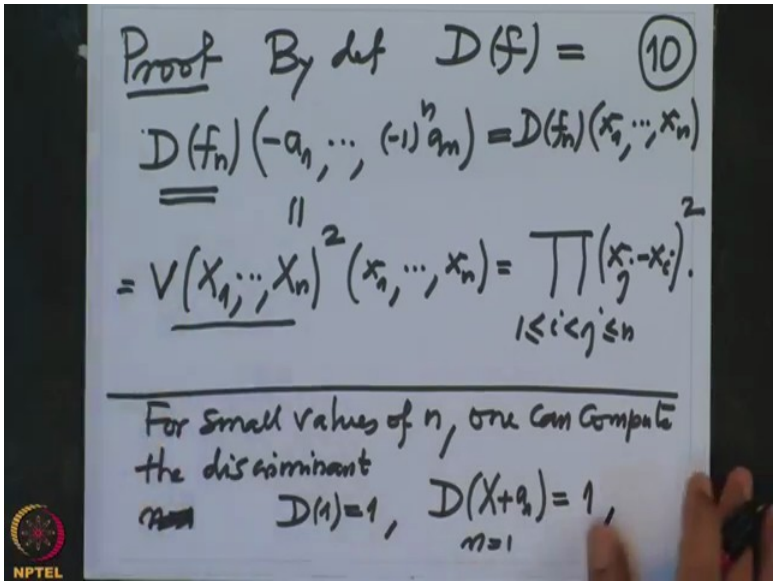

So let me write in a proposition, so formally what we did the following proposition, let $f(X) \in K[X]$ be a monic polynomial of degree n and $x_1, \ldots, x_n$ are in L be all zeroes of f in a finite field extension L over K then $D(f)$ is by definition the discriminant of $f_n$ you evaluated at those thing but that is same as $V(x_1, \ldots, x_n)^2$ which is same thing as

product 1 less equal to i less than j less equal to n, $(x_j - x_i)^2$ , this V is the Vandermonde, not the zero set.

So slightly one has to be careful while reading the notation V but this V will not come so often so $D(f)$ is this, so moreover all zeroes of f are simple if and only if $D(f)$ is non-zero, all. So discriminant is a constant which measures the non-zeroness of the discriminant measures whether the polynomial all routes are simple or not, so it is visible here, the last statement is very clear from this formula because if the two roots are repeated this product will be 0 and therefore $D(f)$ is 0.

Conversely if $D(f)$ is 0, this is in a field K therefore K and this product is individually you think of it as an element in field L and this product is 0 then at least one component will be 0 and therefore at least one 0 will be repeated, so this is a good measure for the and what is the proof so let me write the proof formally.

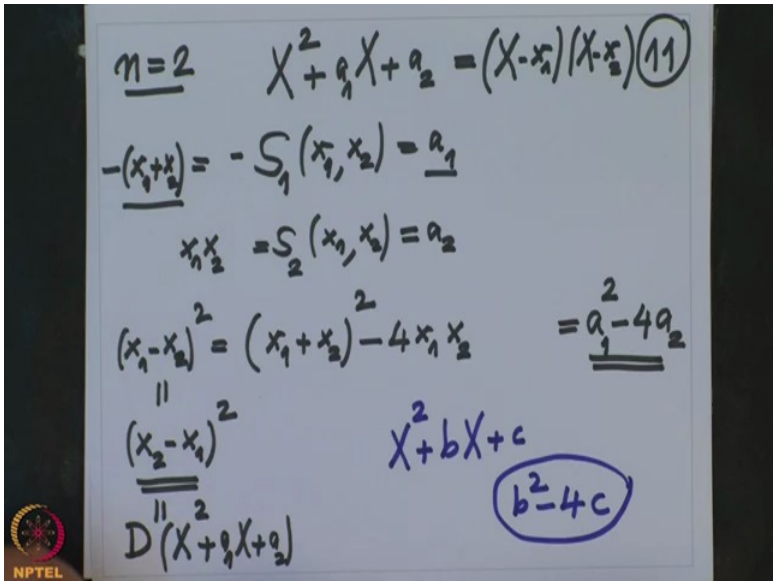
(Refer Slide Time: 23:09)




So proof, so what is by definition, $D(f)$ , I want to prove $D(f)$ equal to somebody and so $D(f)$ is by definition $D(f_n)$ evaluated at $-a_1$ etc. etc. $(-1)^n a_n$ but $D(f_n)$ is by definition $V(X_1, \ldots, X_n)$ , capital $X_1, \ldots, X_n$ whole square and that this one was same thing as $D(f_n)$ evaluated at $X_1, \ldots, X_n$ and this is same as this evaluated at $X_1, \ldots, X_n$ but this is same thing as product, this is the definition of this, 1 less equal to i less than j less equal to n, small xj minus small xi whole square, that is it.

So the proof is very simple, now some small values you can calculate by hand, so for small values of n, one can compute the discriminant for example when n equal to 1, D of 1 is by definition 1, what will be D of $X+X_1$ , this is n equal to, no this is n equal to 1 case, n equal to 1 what is the discriminant now, yes so what do you have to do, degree 1 so there is the what is V? It is only 1 root and therefore it is 1.

(Refer Slide Time: 25:46)

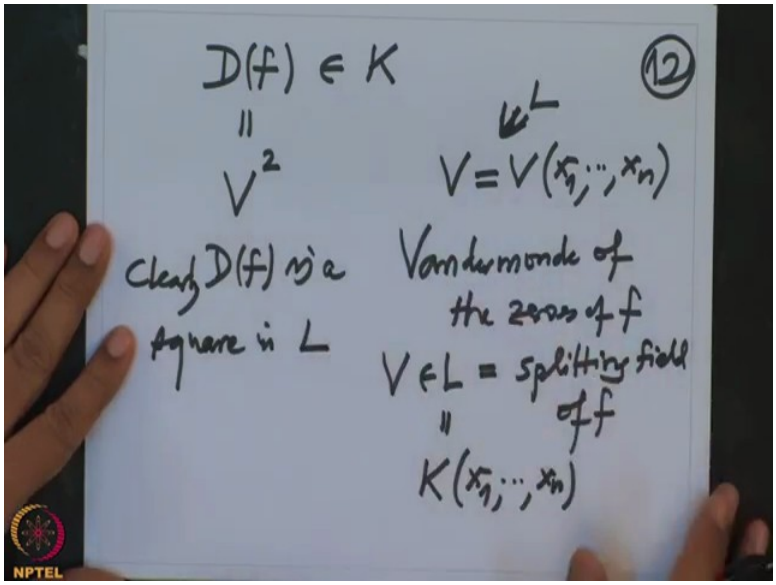



Okay what about, now degree 2 is interesting, n equal to 2, this is what we did in the school days right, I have the quadratic polynomial, it is written like this in our notation and therefore we know if you would have written so if you would know this polynomial as $(X-x_1)(X-x_2)$ , they are at most 2, exactly 2 roots, if you count with multiplicity also, it is written like this and therefore what we get is $S_1$ evaluated at $x_1, x_2$ , this is $-a_1$ , , but this one is $-(x_1+x_2)$ .

And $S_2(x_1, x_2)$ is, this is the product $x_1x_2$ and this is equal to $a_2$ and therefore we want to get rid of this $x_1x_2$ and write in terms of $a_1, a_2$ , so the famous formula is $(x_1-x_2)^2$ , this is the square of this which is $a_1^2$ and then how do I get rid of the middle term here, that is $-4x_1x_2$ which is $-4a_2$ , this is same thing as $(x_1-x_2)^2$ or I have written the same thing as $(x_1-x_2)^2$ , this is Vandermonde square and that is this, so this is our discriminant of X, $D(X^2+a_1X+a_2)$ , so this is the discriminant.

So remember in the school notation, I just want to remind in the school notation, we were writing like this $X^2+bX+c$ and the discriminant was square of this, that is $b^2-4c$ , this was the school notation but I want to adopt this because we want to go on higher degrees, alright so we have for cubic already we will have trouble to calculate, so our strategy will be to learn more so that we can compute.

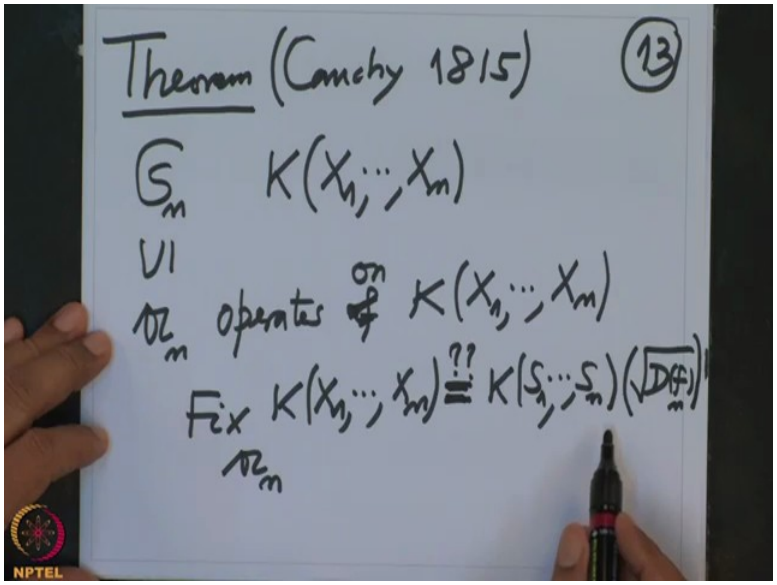
(Refer Slide Time: 28:26)




Okay so now the question is the following, so therefore we know definitely the discriminant of a polynomial which is in the constant, which is in K and this one is V square where V is the Vandermonde of the zeroes of f so this is Vandermonde of the zeroes of f and this V is not in K, this is in L, this V belongs to L and it may not be in K so V is in L where L is splitting field of f.

It is enough that we adjoin all the roots of f to that $K(x_1,\ldots,x_n)$ , therefore this $D(f)$ is a square in L. So clearly $D(f)^2$ in L, but it may not be square in K, see it is an element in K but in the bigger field it is square, but we do not know whether it is smaller field, it is this square or not, that is very important, now let me state one theorem.

(Refer Slide Time: 30:10)

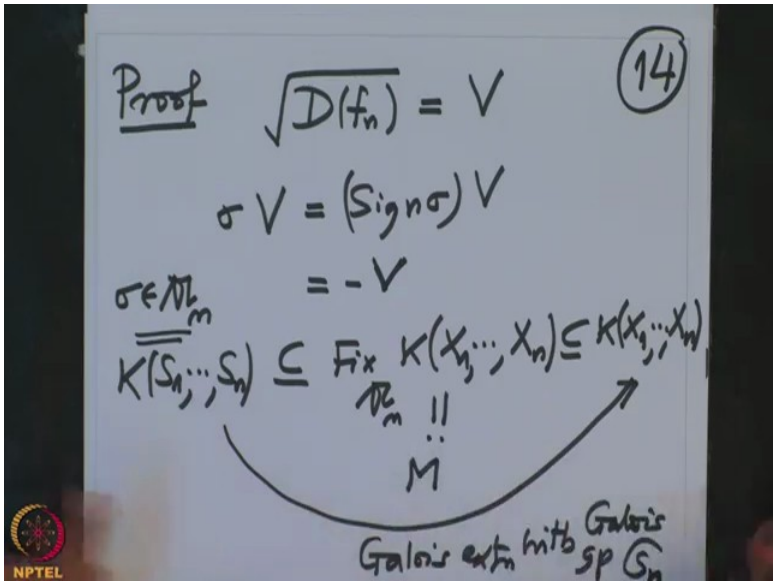



So this is very important theorem, this is due to Cauchy proved in 1815, this say that if I have, if I take the function field in n variables I know the group $S_n$ is operating on this, I know the fixed point that was the Newton's Theorem but now I take the sub group here an, this is a sub group so an operates on this, on $K[X_1,\dots,X_n]$ and I want to consider the fixed field, so the fixed an of the rational function field, what will do I get?

So this obviously it will contain this field $K[S_1,\dots,S_n]$ is contained because these guys are fixed under all permutations in particular these ones so these will smaller than this but this equality I want to write, this is nothing but adjoining the square root of $D(f_n)$ , this is what I want to check, that is the Cauchy's Theorem.

So the fixed field of the alternating group is precisely generated by a square root of the discriminant of a general polynomial over the or the rational functional field in symmetric elementary symmetric polynomials $S_1,\dots,S_n$ , that is the theorem, proof is very simple, we will finish it off.

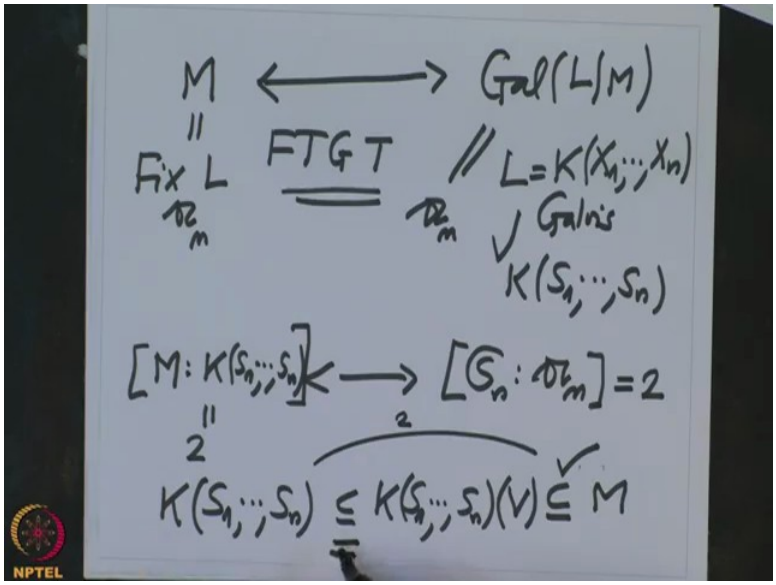
(Refer Slide Time: 32:08)




So proof, okay what did we check, so what is first of all $D(f_n)$ square root, this square root is V, this is Vandermonde because $D(f_n)$ is $V^2$ so the square root is V and what do we check in the lemma, we have checked that $\sigma$ applied on V is nothing but sign of $\sigma V$ , therefore if I take V, $\sigma \in S_n$ then this is nothing but minus V, so definitely this V is not fixed under this, therefore the fixed field, so let us call that fixed field of an of the rational function field, this fix field definitely contained in the rational function field and definitely it contains $K[S_1, \ldots, S_n]$ , so I want to call it M, let us call this as M.

This is an intermediary field between this and we have checked that this extension is a Galois extension with Galois group $S_n$ , this we know already and this is a fix field in between and what is therefore the fundament theorem of Galois theory, what does it say, it says that the fix fields will correspond to the group right.

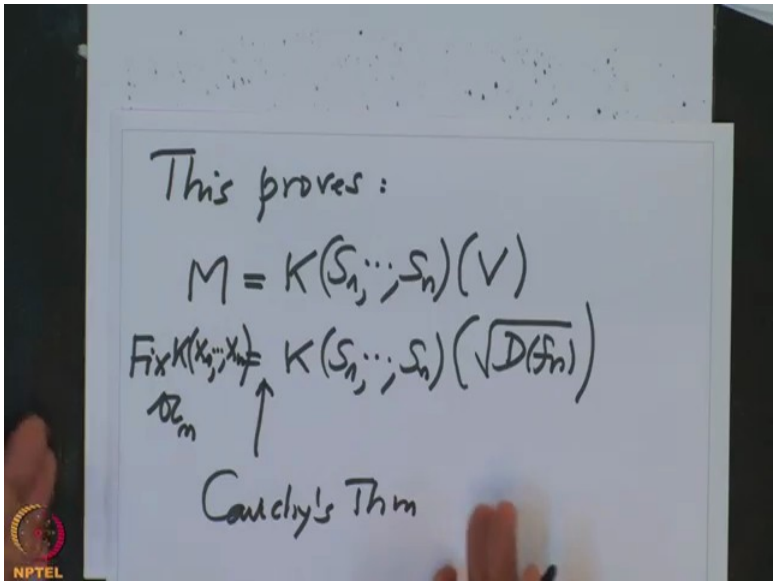
(Refer Slide Time: 34:13)




So the fixed, so this M will corresponds to this intermediary field, this will correspond to the Galois group of L over M, so L is this big field, so this is under the Galois, this is the fixed field of, this is fixed an L, so L is the rational function field and now K was not the K but this considering over $K[S_1,\ldots,S_n]$ , this is Galois, so this Galois group correspond to this fix field and we want to compute this one but what is this, this you get back an right that is precisely the fundamental theorem of Galois theory.

And this index will corresponds to the dimension that is M over K, M over this $K[S_1,\ldots,S_n]$ , this was precisely information from fundamental theorem of Galois theory but this index we know it is 2, so therefore this degree is 2 that means M is generated so but this is obvious K of $S_1,\ldots,S_n$ this M is here and M definitely contains $K[S_1,\ldots,S_n]$ adjoined with V, this definitely contained here because V is also in M because V is fixed under all elements in the alternating group so therefore this is clear and this degree is true that we know it because this index is 2 therefore we have no choice but equality here and once it is equality here that is what the assertion was.

(Refer Slide Time: 36:32)




So this proves M equal to $K[S_1, \ldots, S_n]$ adjoined with V but this is same things as $K[S_1, \ldots, S_n]$ adjoined with the square root of a discriminant but these M is nothing but the fixed field of $A_n$ of K rational function field so this was precisely Cauchy's Theorem, of course Cauchy did not prove it this way because Cauchy did not know what is fundamental theorem of Galois theory so this is a modern proof of you can say this is a modern proof of Cauchy's Theorem okay, with this I will stop and we will continue in the next lecture, thank you.