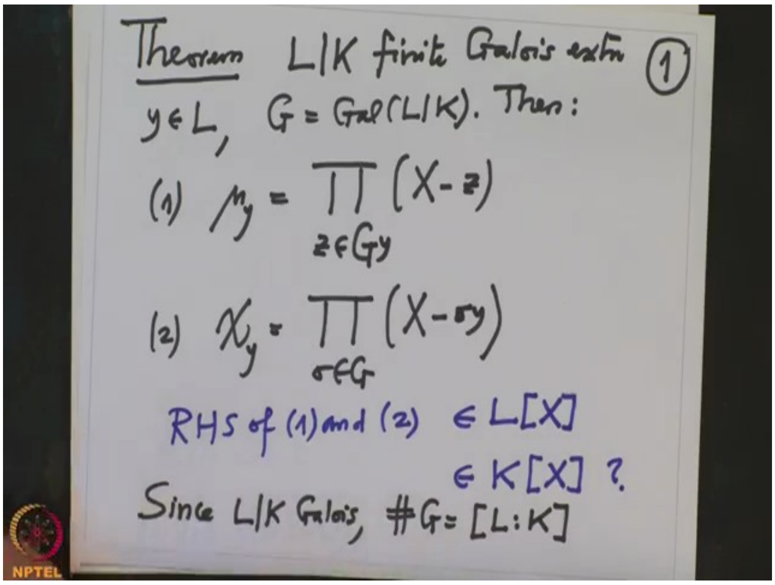
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 30
Minimal and Characteristic Polynomials, Norms, Trace of elements

We are on our way to prove that finite field extension if it is Galois then it is simple. This is what we want to prove and for this we are preparing and we use the action of the Galois group of L over K on L and we want to decide how do you compute minimal polynomial and characteristic polynomial of the arbitrary element of the field L, so we are left with proving 2 equalities and they are the following, so let me just recall that part.

(Refer Slide Time: 1:11)



Theorem L|K finite Galois extn 1

$y \in L$, $G = \mathrm{Gal}(L|K)$. Then:

(1) $\mu_y = \prod_{z \in Gy} (X - z)$

(2) $\chi_y = \prod_{\sigma \in G} (X - \sigma y)$

RHS of (1) and (2) $\in L[X]$

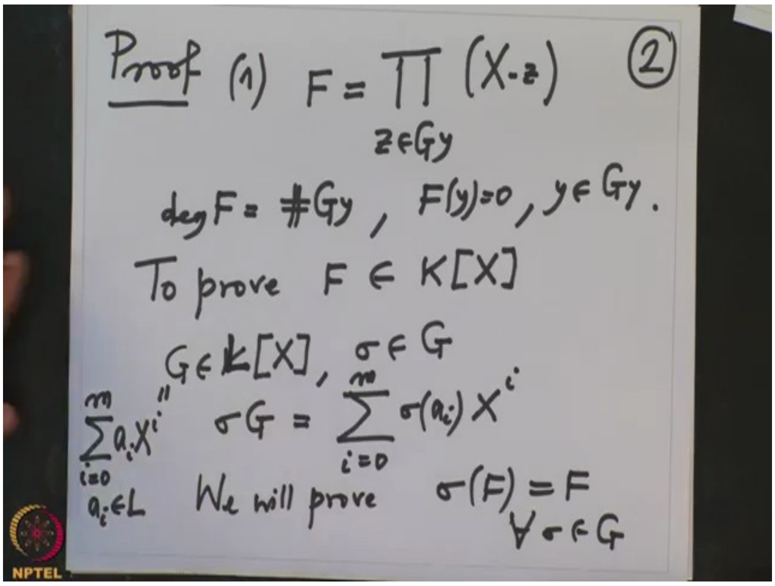
$\in K[X]$?

Since L|K Galois, $\# G = [L:K]$

So theorem what we want to prove, if L over K is finite Galois extension and y is an element in L and G we are denoting the Galois group of L over K. Then we want to prove one minimal polynomial of y is the product $X-z$ where z varies in the orbit of y this was one and 2nd was characteristic polynomial of y is the product σ in G $X-\sigma(y)$, so we want to prove this and as I said last time also it is more important to prove that the polynomial on the right hand side, there are priory polynomials in $L[X]$, so this RHX, RHS of 1 and 2 are polynomials in $L[X]$ but we want to prove they are actually in $K[X]$ this is what is very important because by definition the left-hand sides are polynomial is in $K[X]$.

So this is what one has to prove and then proving one we need to prove that μ … this right inside is minimal monic polynomial of y, so y is the 0 of this that is clear because y is in the orbit of y, so we need to prove that this polynomial is the minimal one that means it is the polynomial of minimal degree, so that y is the 0 of that polynomial this is what we want to prove. It is clear that in 2 both polynomials have the same degree because the extension is Galois, so since L over K is Galois, cardinality of G equal to degree of the extension and it is clear from this side that the cardinality of this product is running over all σ so cardinality is G which is the dimensional this, so at least the degrees are equal in this case.

(Refer Slide Time: 4:33)



Proof (1) $F = \prod_{z \in Gy} (X - z)$ ②

$\deg F = \# Gy$, $F(y) = 0$, $y \in Gy$.

To prove $F \in K[X]$

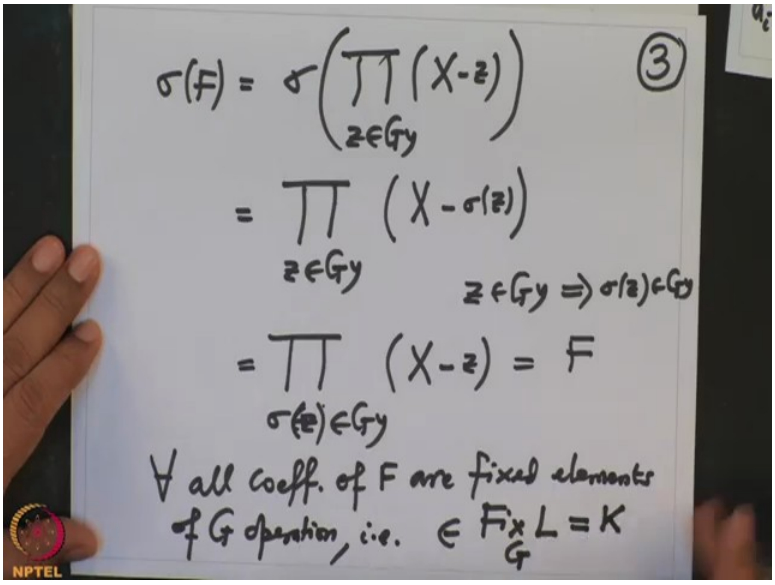
$G \in K[X]$, $\sigma \in G$

$\sum_{i=0}^{m} a_i X^i$ " $\sigma G = \sum_{i=0}^{m} \sigma(a_i) X^i$

$a_i \in L$ We will prove $\sigma(F) = F$ $\forall \sigma \in G$

Okay, so let us prove 1, so proof 1 so let me call F to be the polynomial on the right side, this is product z in G y orbit of y $X - z$, so what is clear? It is clear that the degree of F is cardinality of the orbit and F of y is 0 because y is in the orbit of y. Okay so I want to 1^{st} prove that the polynomial F is in… So to prove F has coefficients in K, so what do you have to prove? So I will prove that, so for arbitrary polynomial G in $K[X]$ or $L[X]$ and σ element in the Galois group G I want to define what is σG ? σG by definition you apply σ to the coefficient of G, so if G is summation $a_i X^i$, i is from 0 to some m. These a i are elements in L then the σG by definition summation i is from 0 to m σ of $a_i X^i$ it is applying to the coefficients and to prove that F belongs to K enough to prove, so to prove this we will prove σ of F equal to F for every σ in G us if I prove this, let us prove this first, so to prove this have to apply σ and see what it is can mark.

(Refer Slide Time: 7:00)



③

$$\sigma(F) = \sigma\left(\prod_{z\in Gy}(X-z)\right)$$

$$= \prod_{z\in Gy}(X-\sigma(z))$$

$z\in Gy \Rightarrow \sigma(z)\in Gy$

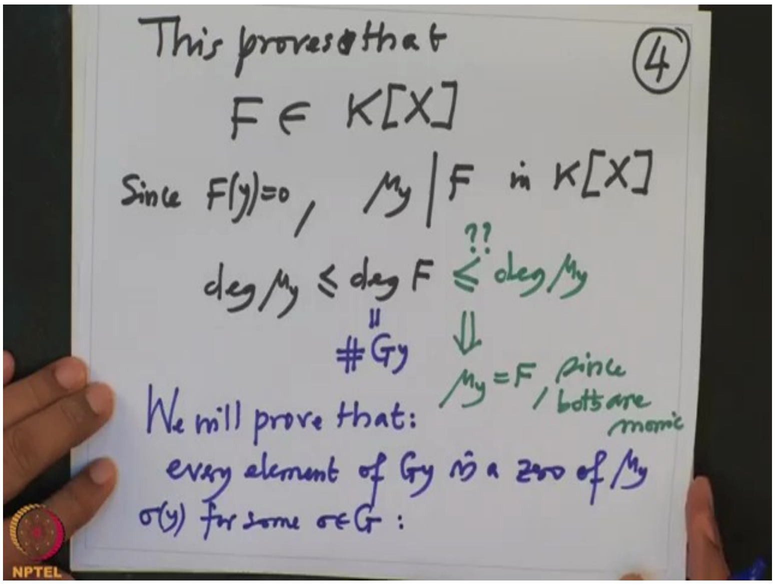
$$= \prod_{\sigma(z)\in Gy}(X-z) = F$$

∀ all coeff. of F are fixed elements of G operation, i.e. $\in \mathrm{Fix}_G L = K$

So what is σ of F? So F we know so σ of F is applying σ to the coefficients but F is the product $X-z$ as z varies in the orbit and then I have to apply σ to this but that means this is for product $z\in Gy$ because σ respect the multiplication, so this is same as the product will come out and X nothing to do with σ, so $X-\sigma(z)$ but remember if s is in the orbit $\sigma(z)$ is also in the orbit. Not only that, therefore this…I could have just replace σ …

So this is same as this product is running over orbit of y, so I could have simply written this as $\sigma(z)$ in Gy $X-z$. So this is same as F because you apply again apply… Okay there is nothing much to say, so therefore $\sigma(F)$ is F, alright so therefore all the coefficients of F are invariant under all the elements of G, so therefore all coefficients of F are fix elements of the G operation that is they belong where? They belong to the fix field of G but this is K because we have proved that if L over K is Galois then the fixed field is this.

(Refer Slide Time: 9:37)



This proves that

$F \in K[X]$

Since $F(y)=0$, $\mu_y \mid F$ in $K[X]$

$$\deg \mu_y \leq \underset{\#Gy}{\underset{\shortparallel}{\deg F}} \overset{??}{\leq} \deg \mu_y$$

$$\Downarrow$$

$\mu_y = F$, since both are monic

4

We will prove that:

every element of Gy is a zero of μ_y

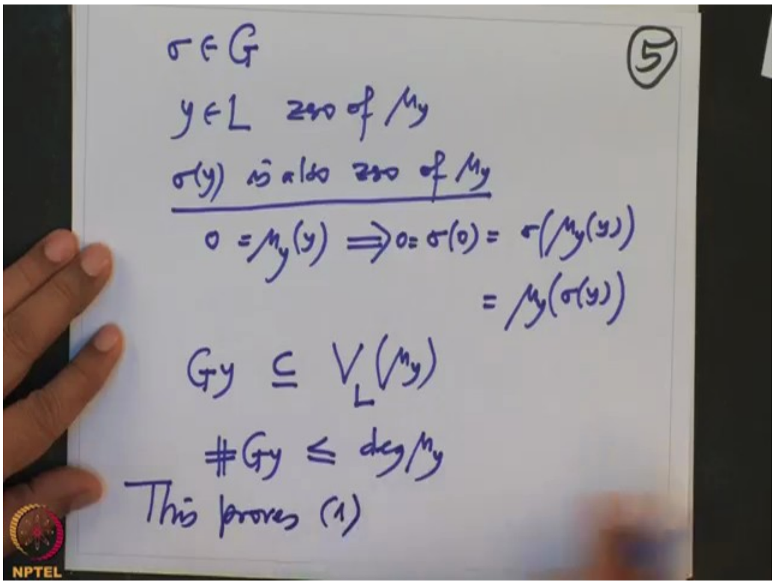
$\sigma(y)$ for some $\sigma \in G$:

So this proves that the polynomial F actually indeed polynomial in $K[X]$. Now we have noted that $F(y)$ is 0 since $F(y)$ is 0 μ_y must divide F were in $K[X]$ because μ_y is a minimal polynomial of y and this F is arbitrary polynomial of y, so arbitrary polynomial where not arbitrary one polynomial why is 0, so therefore this F is in the kernel of this substitution map and kernel of this substitution map is generated by μ_y, so μ_y has to divide F. Alright but now let us compare the degrees, so therefore degree of μ_y is smaller equal to degree of F. Remember both are monic F is also monic by definition of F.

So both are monic polynomial 1 degree is smaller equal to this but now I want to prove that degree of F is smaller equal to degree of μ, I want to prove this. Once I prove this the degrees will be equal and both are monic polynomial one divides the other, so that will imply μ equal to X, so once I prove this, this will imply μ_y equal to F since both are monic. So I want to prove this alright, so remember again our very important observation from Galois theory that I want to prove therefore what? I want the degree of F I know what is the degree of F, degree of F is cardinality of the orbit because F is the product of the linear factors which arise from each element of the orbit, so these degrees I know and if I want to prove this I should prove that this μ_y has so many zeros.

If there are so many zeros then the degree of that polynomial will be at least that, so I have to prove that, so we will prove that every element of the orbit G y is a 0 of μ_y, so therefore μ_y will have at least the cardinality of orbit number of zeros, so the degree will be at least cardinality of orbit and that will prove what we wanted to prove. So take any element of the orbit, so any element of the orbit will look like $\sigma(y)$ for some σ in G and now what was our observation? I want to use my observation namely if I have an element and element of this Galois group.

(Refer Slide Time: 13:35)



5

$\sigma \in G$

$y \in L$ zero of μ_y

$\sigma(y)$ is also zero of μ_y

$$0 = \mu_y(y) \Rightarrow 0 = \sigma(0) = \sigma(\mu_y(y))$$
$$= \mu_y(\sigma(y))$$

$$Gy \subseteq V_L(\mu_y)$$

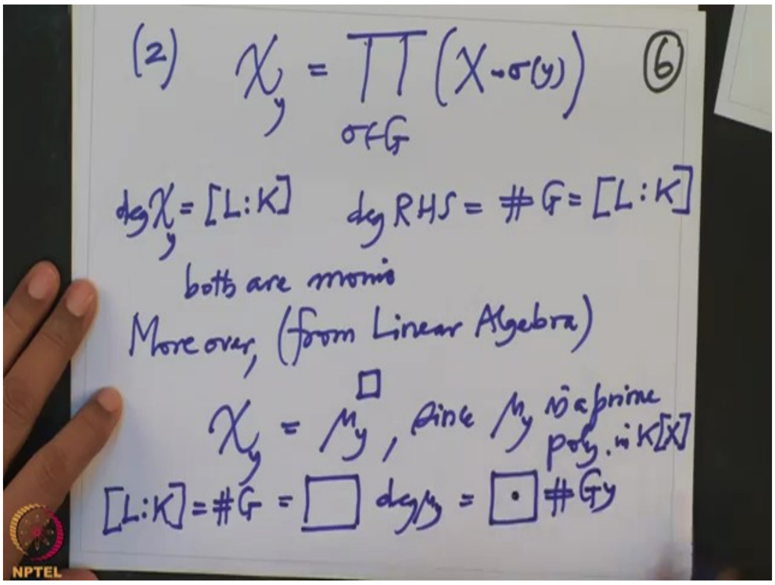
$$\# Gy \leq \deg \mu_y$$

This proves (1)

So what is the observation? σ is in element in G and y was an element in L and y is a 0 of μ_y then if I apply σ to y $\sigma(y)$ is also 0 of μ_y, so that is simple because $\mu_y(y)$ is 0 and apply σ to this equation and I apply σ to this equation, $\sigma(0)$ which is 0 that is σ of μ_y but σ is an algebra homomorphism with respect to the scalar multiplication with respect the sum and with respect to the powers of y also, so this is same as μ_y of $\sigma(y)$, so therefore $\sigma(y)$ is also 0, so that shows this.

This is the very important observation which is the crux of the Galois theory and I will use it thousands of times I will uses, so what did we check? We check that $\sigma(y)$ is the 0 of μ_y that means whole orbit is containing the 0 set of μ_y and that is in L, so therefore the cardinality this polynomial, so therefore the cardinality of the orbit is smaller equal to the degree of μ_y and that proves what we wanted to prove and that finishes the prove that 1. So I will just say this proves 1.

(Refer Slide Time: 15:32)



(2) $\chi_y = \prod_{\sigma\in G} (X - \sigma(y))$ ⑥

$\deg \chi_y = [L:K]$ $\deg RHS = \# G = [L:K]$

both are monic

Moreover, (from Linear Algebra)

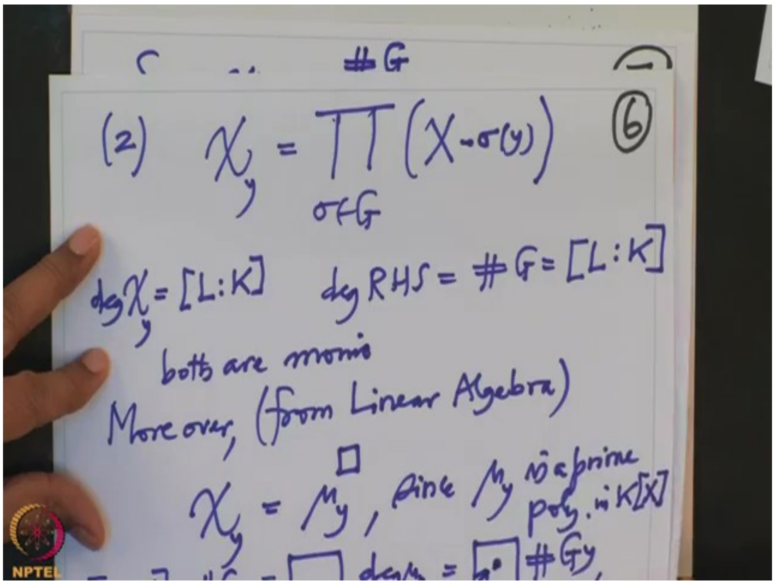
$\chi_y = \mu_y^{\square}$, since μ_y is a prime poly. in $K[X]$

$[L:K] = \# G = \square \deg \mu_y = \boxed{\cdot} \# G_y$

Now prove 2 it is about the characteristic polynomial but that is very simple because what we want to prove? I want to prove χ_y equal to product $\sigma\in G$ $X-\sigma(y)$ this is what I want to prove. First of all what is the degree of RHS? Degree of RHS equal to cardinality of the group G which is the dimensions of L over K which is the degree of the field extension and this χ_y also have degree because χ_y is a characteristics polynomial of…this is a linear operator on L and L is a K vector space of this dimension so therefore this is also LK, so both have the same degree, both are monic.

Yes so and therefore…well there is an easy way also to conclude, so both are monic, both have the same degree and what do I know about χ_y . Moreover this is from linear algebra what we observed χ_y has to be power of μ , some power of μ because since μ_y is prime polynomial in $K[X]$ because it is a field extension. Now therefore what power? Here the degree of χ_y is the degree of L over K which is cardinality of G because L over K is Galois and on this side is what? So I want to know what can I write here, which power? So that we may somebody here times degree of μ_y that is somebody, degree of μ_y I know it is the cardinality of the orbit of y, so what can I do here there is no other choice than the index.

(Refer Slide Time: 18:32)



⑥

(2) $\chi_y = \prod_{\sigma \in G} (X - \sigma(y))$

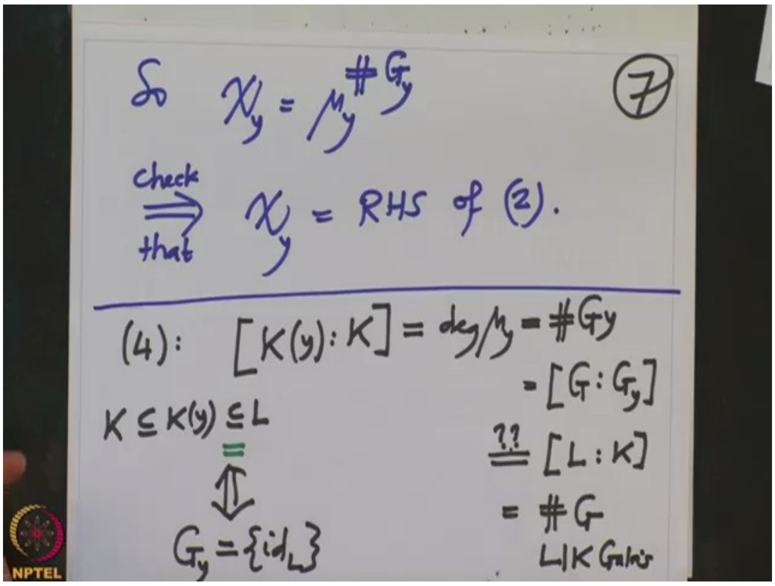
$\deg \chi_y = [L:K]$ $\deg \text{RHS} = \#G = [L:K]$

both are monic

Moreover, (from Linear Algebra)

$\chi_y = \mu_y^{\square}$, since μ_y is a prime poly. in $K[X]$

$\deg \mu_y = \boxed{\cdot}\ \#G_y$,



⑦

So $\chi_y = \mu_y^{\#G_y}$

$\overset{\text{check}}{\underset{\text{that}}{\Longrightarrow}}$ $\chi_y = \text{RHS of } (2)$.

(4): $[K(y):K] = \deg \mu_y = \#G_y$

$= [G:G_y]$

$\overset{??}{=} [L:K]$

$= \#G$

$L|K$ Galois

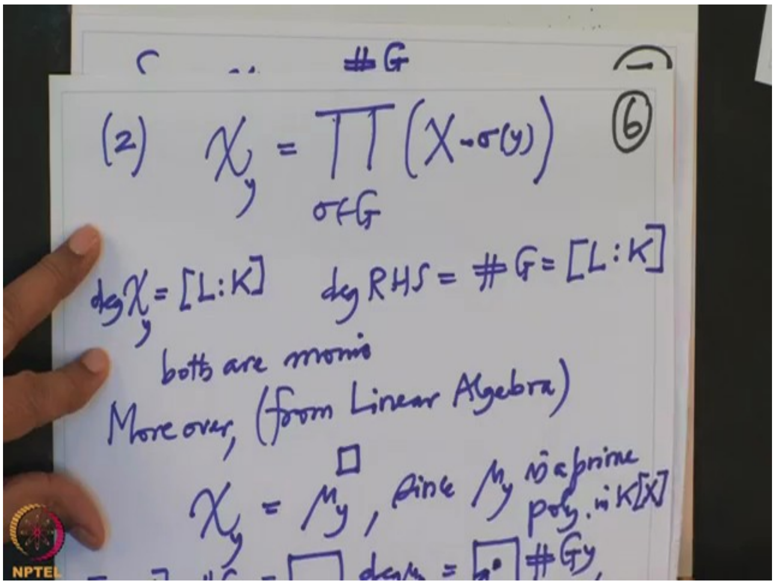
$K \subseteq K(y) \overset{=}{\subseteq} L$

$\Updownarrow$

$G_y = \{id_L\}$

So therefore what we observed is…so χ_y has to be μ_y power…no I said something wrong the power cardinality of the isotropy.

(Refer Slide Time: 18:46)



$\#G$

(2) $\chi_y = \prod_{\sigma \in G} (X - \sigma(y))$ ⑥

$\deg \chi_y = [L:K]$ $\deg RHS = \#G = [L:K]$

both are monic

Moreover, (from Linear Algebra)

$\chi_y = \mu_y^{\square}$, since μ_y is a prime poly. in $K[X]$

$\#G_y$,

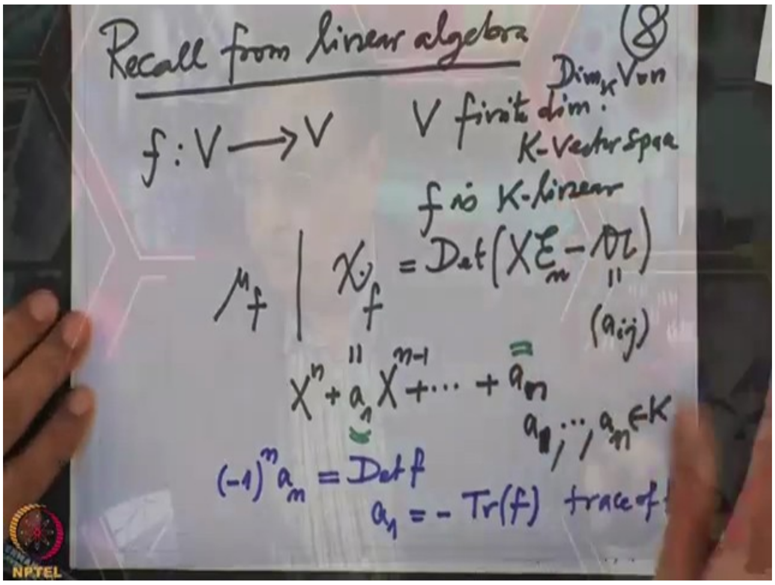
Box is I want to write somebody here but I know this is the index of the isotropy, so how can I get the order of G? I have to supply here cardinality of G y, so here you have to write cardinality of G suffix y. So we approve this formula, already we approved that μ_y is a product of this, so now if you club one and you put it 1 and then you raise it so many times.

So that is now easy to check that, so…now check I will just simply check that from this implies χ_y is RHS of 2 which is what we wanted to prove and we know that we want to …Already I have indicated in the last lecture at this proves that, so 4 was recall 4, 4 was the degree of the field extensions K y over K. Remember K is here K y is in between and this is a subfield of L and we want know when can the equality happen for which y this equality happen, so we are interested in the equality here, we are interested in the equality here, so when can that happen?

So this we have noted this is nothing but degree of the minimal polynomial of y this is the definition and this is clear and we have observed this and this is equal to cardinality of the orbit, so cardinality of the orbit is the index of the stabiliser and when can equality happen, so this equal to L over K which is we know it is cardinality G because this is L over K Galois therefore when can equality happen here? When equality will be here that means, so this is equivalent to saying this index should be one, so G y index is 1 means G y is trivial…not 1 index is the whole cardinality G that means G y is trivial. So therefore if you want to prove that there is a primitive element and you must choose, we must show that there is an element in the Galois extension who’s isotropic group is trivial, so that is what we want to prove.

Alright, so this we will prove but before we prove I want also defined important concepts which is used for the future.

(Refer Slide Time: 22:24)



Recall from linear algebra (8)

$f : V \longrightarrow V$ V finite dim. $\mathrm{Dim}_K V = n$

K-Vector Space

f is K-linear

$\mu_f \mid \chi_f = \mathrm{Det}(X E_n - \mathfrak{A})$, $\mathfrak{A} = (a_{ij})$

$\chi_f = X^n + a_1 X^{n-1} + \cdots + a_n$

$a_1, \ldots, a_n \in K$

$(-1)^n a_n = \mathrm{Det} f$

$a_1 = -\mathrm{Tr}(f)$ trace of f

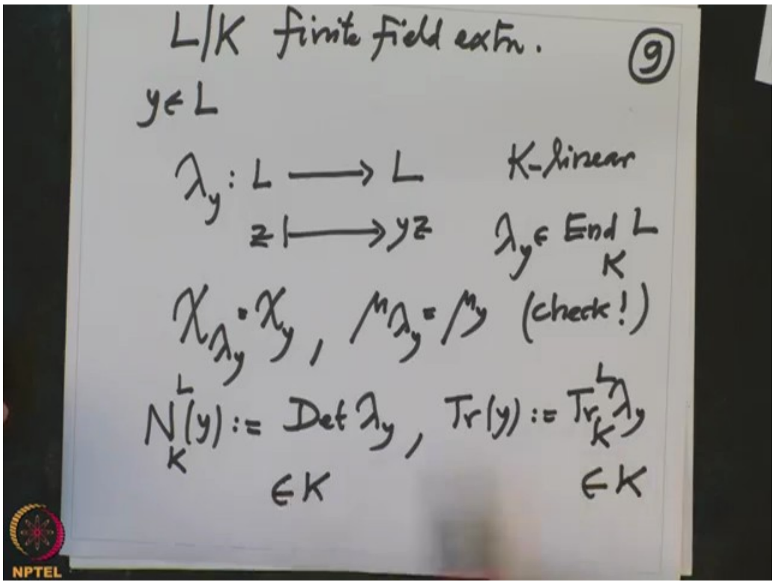
So recall, I would say recall again from linear algebra, the 2 important invariant so f is a linear operator on a finite dimensional vector space. V finite dimensional K vector space and f is K linear then I told you to this we have 2 polynomials χ_f and μ_f , the minimal polynomial χ_f is a characteristic polynomial and this χ_f divide this not only divides they are the same prime factors.

This is the determinant of X identity matrix n cross in identity matrix minus the matrix a which this matrix we got it by using by choosing arbitrary bases and n dimensional, dimensional of V is m and this is a monic polynomial, so this polynomial looks like $X^n + a_1 X^{n-1} + \ldots + a_n$ and where a_1 to a_n there are elements of the field. It is monic polynomial of degree and particular interest are this coefficients as I said these polynomials does not depend on the basis chosen that is because determinant of 2 similar matters is the same and if you change the basis this a will change into the similar matrix and therefore one checks easily that this determinant does not depend upon the basis chosen.

So this is the characteristic polynomial of f and all these coefficients are therefore very important and they are good in variants and out of the 2 the last one that is the constant term of χ and coefficient of X^n are of particular importance and what are they? They are therefore so first of all this, this is up to a sign, so $(-1)^n a_n$ this is nothing but the determinant of f that is clear because I put X equal to 0. When I put X equal to 0 it is determinant of - a, so that means minus I have to get rid of minus how many times as many as rows are there so there are precisely n rows so I multiply by $(-1)^n$ and then that is the determinant and what is a_1 ? a_1 is minus the trace of f.

This is a trace of f, trace is nothing but the sum of the diagonal entries, so that again does not depend up on the basis chosen, so these are 2 very important invariants of the linear operator. Similarly the remaining coefficients also have nice meaning like this but that we do not need it here but they can also be describe in terms of this matrix and they will in fact be up to a sign. Sum of products of r at a time elements of the… They are related with the minors of a higher minors of a these are only we are taking one by one minors and here we are taking the full minor, so the definition I want to make is the following.

(Refer Slide Time: 26:49)



L/K finite field extn. ⑨

$y \in L$

$\lambda_y : L \longrightarrow L$ K-linear

$z \longmapsto yz$ $\lambda_y \in \mathrm{End}_K L$

$\chi_{\lambda_y} = \chi_y$, $\mu_{\lambda_y} = \mu_y$ (check!)

$N^L_K(y) := \mathrm{Det}\,\lambda_y$, $\mathrm{Tr}(y) := \mathrm{Tr}^L_K \lambda_y$

$\in K$ $\in K$

Now we have a field extension, finite field extension and y is an element there and we have this linear map now λ_y this is a map from L to L multiplication by L and z going to y z. This is clearly K linear it is not L linear, it is K linear it is not a K algebra homomorphism also because one does not go to one, so it is only K linear map that means this λ_y is an endomorphism of the vector space and not K algebra homomorphism, it is an endomorphism, so therefore it makes sense to talk about characteristic polynomial of λ_y minimal polynomial of λ_y but this is same thing as characteristic polynomial of y and this is same thing as minimal polynomial of y that is easy to check this equal this.

So I will strongly recommend you to check this precisely, check this equal it is. Alright once you check that it is clear what is the norm of… That is also called norm of f, so the norm of y is by definition determinant of λ_y that is the norm of y, so to be more precise in the notation norm of L over K of y and trace of y is by definition again trace of this λ_y L over K and both these are elements in K and now in the next lecture we will study more properties of these norm and trace. Here I would like to make only one comment that his concepts are defined for arbitrary finite field extension, arbitrary I am not assuming the field extension is Galois but I will use it to prove that Galois field extension is simple, so we will continue after the break, so we still have to prove that Galois extensions are simple and we are almost will almost finish the proof in the next lecture. Thank you.