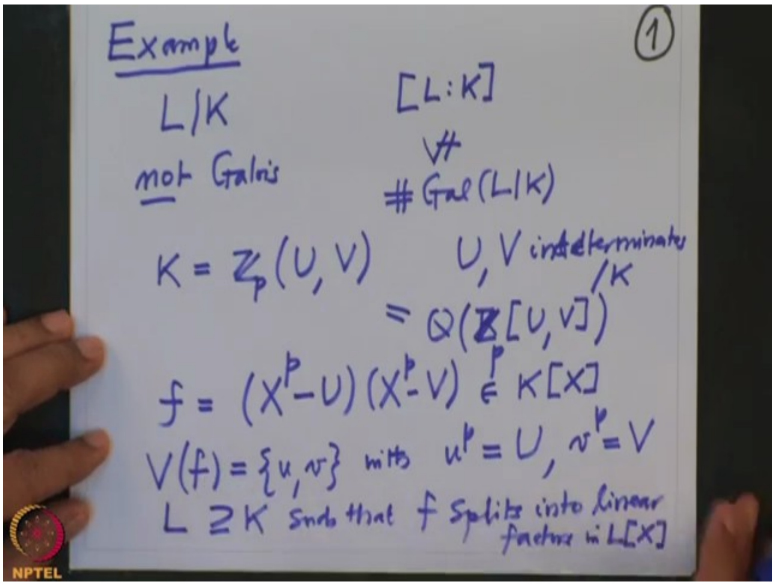
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 29
Digression on Linear Algebra

In the last time we saw one example of a simple extension where minimal polynomial does not split into linear factor in the field L, so it is not Galois. Now I want to show an example of a field extension which is which the 2nd condition can also fail so that is I want the field extension L over K.

(Refer Slide Time: 0:58)



Example ①

$L|K$ $\qquad$ $[L:K]$

not Galois $\qquad$ $\vee\!\!\!\#$ $\#\,\mathrm{Gal}(L|K)$

$K = \mathbb{Z}_p(U,V)$ $\qquad$ U, V indeterminates $/K$

$= Q(\mathbb{Z}_p[U,V])$

$f = (X^p - U)(X^p - V) \in K[X]$

$V(f) = \{u, v\}$ with $u^p = U$, $v^p = V$

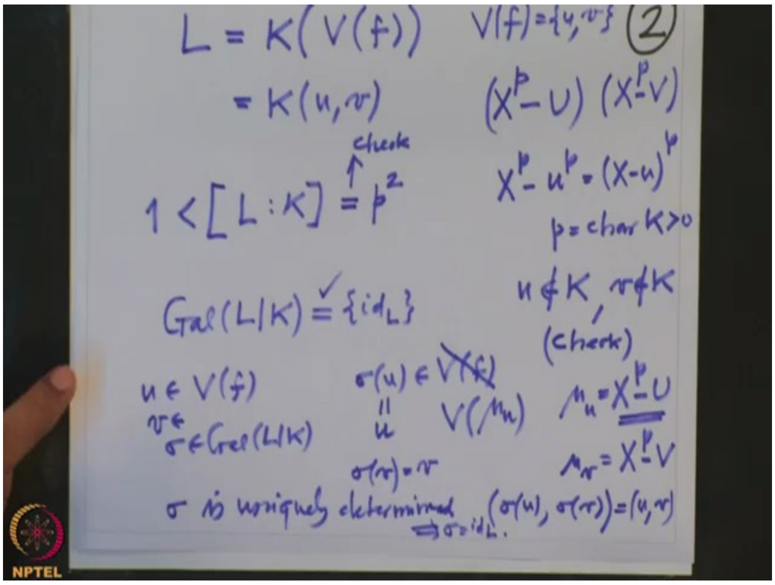
$L \supseteq K$ such that f splits into linear factors in $L[X]$

So example L over K I want and such that the degree is more than this degree should be strictly bigger than the cardinality of the Galois group, I am writing such an example, so therefore L over K cannot be Galois. Alright, so it will not be… because it is not Galois it will not be simple extension because we are going to prove soon the Galois extensions are simple extensions, so and how do I give such example of course one easy way out is I want an example of a field extension where degree is more than one but the Galois group was trivial, so in other words I want to rigid field extension.

So the Galois group is minimal that is only the trivial group identity element and field extension has more degree. Alright, so in the base field and K to be $\mathbb{Z}_p$ and then a rational function field in 2 variables $K[U,V]$, U and V are indeterminate over K and this is precisely the coefficient field of the polynomial ring in 2 variables over $\mathbb{Z}_p$. This is my base field and I am looking at the polynomial f, f is a polynomial in this field which has 2 factors $(X^p - U)(X^p - V)$ these are the 2 factors and I am going to write what are the roots of, what other zeros of f, zeros of f are precisely there are only 2 zeros u and v with $u^p = U$ and $v^p = V$ that is very easy to check 1st of all if u is a 0 of this polynomial.

Let us take an element u in the…so this polynomial is a polynomial with coefficient in K, so I definitely know there is a field L which is field extension of K such that f splits into linear factors in $L[X]$. This we know such a field exist because remember Kronecker's Theorem which says that given any polynomial f we can enlarge a field so that all zeros of this f lies in this field and I only take the field L which is obtained from K which is obtained from K by attaching all zeros of f.

(Refer Slide Time: 5:13)



$L = K(V(f))$ $V(f) = \{u, v\}$ 2

$= K(u, v)$ $(X^p - U)(X^p - V)$

$1 < [L:K] \overset{\overset{\text{check}}{\uparrow}}{=} p^2$ $X^p - u^p = (X-u)^p$

$p = \text{char } K > 0$

$\mathrm{Gal}(L|K) \overset{\checkmark}{=} \{id_L\}$ $u \notin K, v \notin K$ (check)

$u \in V(f)$ $\sigma(u) \in V(\cancel{f})$ $V(\mu_u)$ $\mu_u = X^p - U$

$v \in$ $\sigma \in \mathrm{Gal}(L|K)$ $\sigma(u) = u$

$\sigma(v) = v$ $\mu_v = X^p - V$

σ is uniquely determined $(\sigma(u), \sigma(v)) = (u, v)$ $\Rightarrow \sigma = id_L$.

So in the notation also one will write this L is K attach with all zeros of the polynomial f and I know all the zeros they are precisely u and v there cannot be any other 0 because if u is 1 zero that means u power v will be equal to u and once u power p equal to 1 that means they are the zeros of... U is the zero of this phenomenal and once u is the 0 then $X^p - U$ is u^p and this polynomial is nothing but $(X-u)^p$ because p is the characteristics of the base field which is positive therefore once I know 1 zero of this polynomial I know all the zeros of this polynomial.

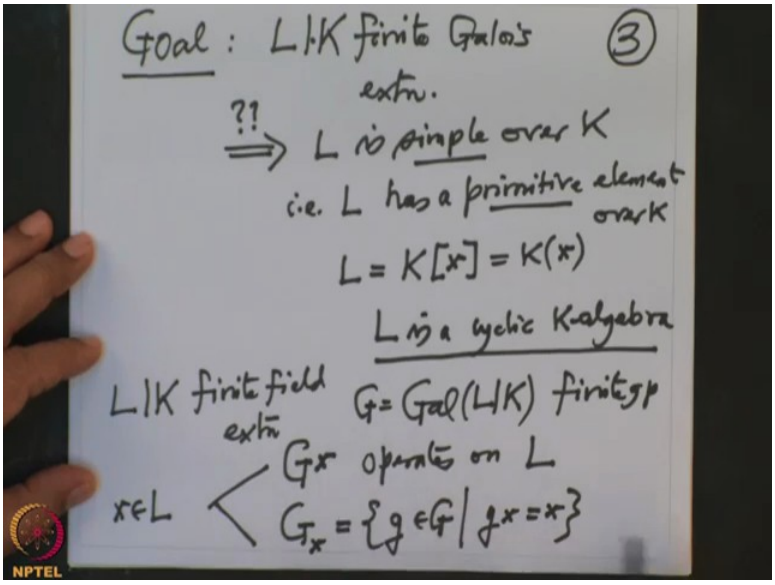
Similarly once I know 1 zero of this polynomial then I know all the zeros of this polynomial and they are precisely u and v, so therefore there are only 2 zeros v_p what it shows is V of f equals to u, v so there are 2 zeros. Alright so what is their degree? 1st of all the degree of the field extension is definitely more than one that is because u cannot belong to K and v also cannot belong to K for the same reason, u cannot belong to K is very simple because that is easy to check, so I will just write here check, so therefore degrees is definitely more than 1.

Actually it is not too difficult to prove that the degree is actually p^2 , so I will also say here check degree is p square and on the other hand what is the Galois group? Galois group I want to compute and I want to show that Galois group of L over K is nothing but only the identity map of L, so that is because remember the most important observation of the Galois theory which says that if u is a 0 of a polynomial then and any σ is any automorphism of L over K then σ of that is also 0 of the same polynomial.

So therefore I want to apply that to this f, so u is a 0 of f and see if σ is any automorphism then $\sigma(u)$ is also 0 of f but $\sigma(u)$ is actually more than that, $\sigma(u)$ is a 0 of the minimal polynomial of not only this but v of minimal polynomial of u but minimal polynomial of u is nothing but $X^p - U$, this is minimal polynomial and f is not the minimal polynomial, this is a minimal polynomial of u over K, so therefore and the only 0 is u, so therefore we have no choice but $\sigma(u)$ has to this u. Similarly v is a 0 of this polynomial f and minimal polynomial of v is $X^p - V$, so therefore that forces Sigma v is also equal to v that means every automorphism of the field extension L over K maps u and v to themselves but remember the σ is uniquely determined by its values on u and v.

So $\sigma(u)$ is uniquely determine by this pair which is u, v so therefore you have no choice $\sigma(u)$ has to be identity, so this proves that the Galois group is only identity, so that in place σ has to be identity on L, so that proves our assertions, so these extension cannot be Galois extension. In this case what fails is the fact that there are no automorphism at all of the nontrivial field extension, so this can also happen but this happens in characteristics p. We will come back to this in a retail way once we have enough vocabulary connected to the Galois group and field extension.

(Refer Slide Time: 10:03)



Goal : $L|K$ finite Galois extn. ③

?? $\Longrightarrow$ L is simple over K

i.e. L has a primitive element over K

$L = K[x] = K(x)$

L is a cyclic K-algebra

$L|K$ finite field extn $G = \mathrm{Gal}(L|K)$ finite gp

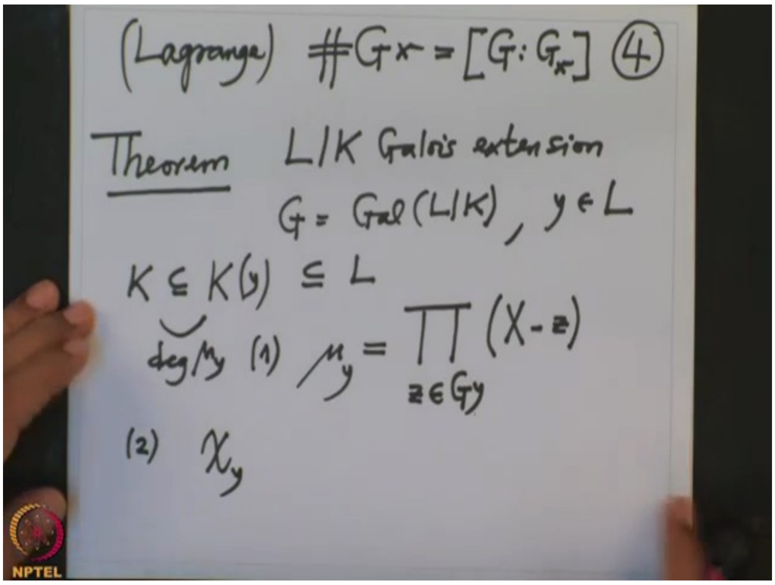
$x \in L$ $<$ Gx operates on L

$G_x = \{g \in G \,|\, gx = x\}$

So now the next goal is to prove that the Galois extensions are simple, so I will write a goal here so L over K finite extension, finite Galois extension then I want to prove, this is our goal L is simple over K or that means that is L has a primitive element over K that means L is generated as K algebra by one element this is also around bracket because we are algebraic extension, so I will also keep saying L is cycling K algebra that means as an algebra over K it is generated by one element that is what we want to prove. Alright and what will be our missionary?

Remember whenever you have a field extension L over K finite field extension then we have a group attached to that namely the Galois group and this is the finite group and this group obviously acts in a natural way and this operates on L, so and it operates on L means given any element x in L I have 2 things attach that namely the orbit of x those are the G multiple of x and the isotropy G_x this is a subgroup of g, $g \in G$ let us call this group as G, $g \in G$ such that g of x is x. I would prefer to denote elements of G as σ, τ et cetera, so that means this is precisely all those fixed points of… x is a fixed point of everybody that means $\sigma(x)$ is x for all σ. These are the 2 objects attached to that and we know the relation between them also the cardinality of the orbit that is very important.

(Refer Slide Time: 12:54)



(Lagrange) $\#Gx = [G : G_x]$ (4)

Theorem L/K Galois extension

$G = \mathrm{Gal}(L/K)$, $y \in L$

$\underbrace{K \subseteq K(y)}_{\deg \mu_y} \subseteq L$

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

(2) χ_y

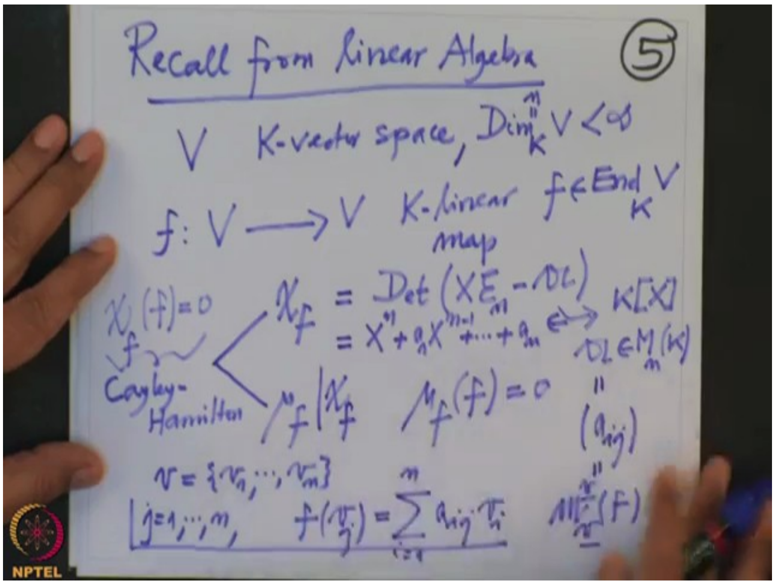
So I will just write that because we will soon use it we know this was Lagrange, it says cardinality of the orbit equal to the index of the stabiliser, index of the stabiliser is precisely the number of left cosets of Gx in G or number of right cosets of Gx in G both these numbers are same for arbitraries of group of an arbitrary group, so this is what I want to use it, so let me state a theorem now, so theorem this is what we will prove and as a consequence we will prove that the Galois extensions are simple, so L over K Galois extension and G is the Galois group. Okay let us take y arbitrary element of L we want to prove at least one y there so that L is generated as a K algebra by that y.

So I want to write down what is the degree of $K(y)$ over K and when will it be equal to the degree of L over K in that case they will be equal, so note that $K(y)$ is contained in L and it contains K and we are hoping that we can choose y so that equality holds here that is our aim and that can happen only when the degree of L over K equal to degree of this over this, this degree I know, the degree of this extension we know it is degree of the minimal polynomial of y, so I want to choose y so that the degree of L over K equal to degree of μ_y this is what our aim is?

So I am interested in finding out what is the minimal polynomial in terms of, of course the group okay, so what do I say? So I will write down formulas so μ_y minimal polynomial of y is nothing but look at the product $X - z$, where z belongs to the orbit of y. Now I want to prove this, this is not obvious because this side is where, where is this polynomial? Apriori this polynomial is in L, the coefficients are in L because z are where? z are in the orbit of y, so they are apparently in $L[X]$.

So this polynomial is in $L[X]$ but to show that this equality I have to show that this polynomial equal to μ_y to show this I have to show first that the coefficients are in K and not only that this is minimal polynomial also I have to say. This polynomial is of the least degree polynomial and y is zero that is obvious because y is an element of the orbit, every element belongs to its orbit, so 0 is obvious. Now I have to show that 2 important things the degree the coefficients are in K and it is a minimal polynomial that means it is a minimal of the smallest degree polynomial, these 2 things I have to show. So this is an assertion 1, 2 now $\chi(y)$ so let me remind you, so this is remembering from linear algebra.

(Refer Slide Time: 17:04)



Recall from linear Algebra ⑤

V K-vector space, $\mathrm{Dim}_K V \overset{m}{=} < \infty$

$f : V \longrightarrow V$ K-linear map $f \in \mathrm{End}_K V$

$\chi_f(f) = 0$ Cayley-Hamilton

$\chi_f = \mathrm{Det}(XE_m - \mathfrak{A}) = X^m + a_1 X^{m-1} + \cdots + a_m \in K[X]$

$\mu_f \mid \chi_f$ $\mu_f(f) = 0$

$\mathfrak{A} \in M_m(K) = (a_{ij}) = M^{v}_{v}(f)$

$v = \{v_1, \ldots, v_m\}$

$j = 1, \ldots, m,$ $f(v_j) = \sum_{i=1}^{m} a_{ij} v_i$

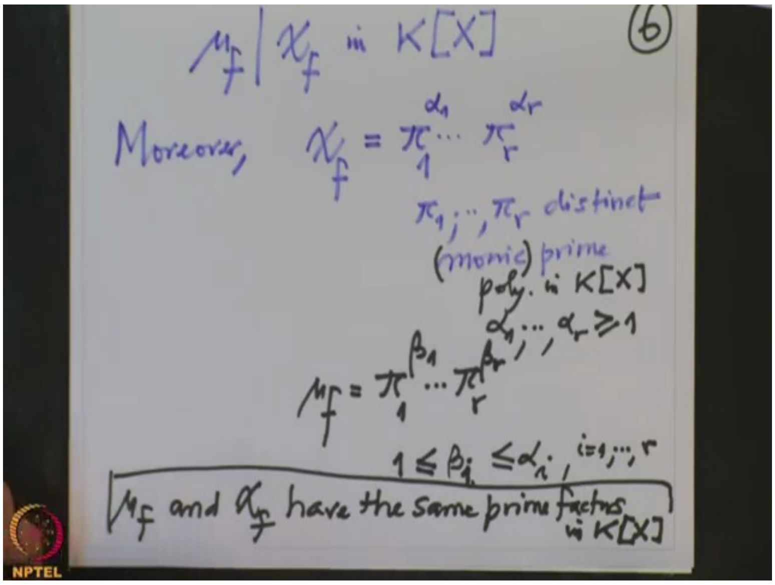
So I will write it record from linear algebra, what do I want to recall? So whenever I have a vector space V, V is a K vector space and linear operator on V, $f : V \to V$, K linear operator, K linear map, so it is an element f belongs to $End_K V$ that means it is an endomorphism as K, not K algebra, K algebra does not make sense, it is a K linear map that is this and now with this we have attached to polynomials one is the characteristics polynomial of f and the other is minimal polynomial of f, minimal polynomial of f is the monic polynomial of the smallest degree so that μ_f when I substitute X equal to f it is 0 operator.

Similarly, so what is the characteristics polynomial? Characteristic polynomial is defined by using the determinants and the characteristic polynomial makes sense when the vector space has finite dimensions, so we are assuming that is the finite dimensional vector space and what is the characteristic polynomial? You look at the determinant of X identity matrix minus that matrix a where this a is a matrix it is $m \times m$ matrix where m is this dimensions and entries of this matrix are precisely a ij and these entries are determined by… this is with matrix of f, matrix of f with respect to some fixed basis v.

How are they defined? Just for the sake of recall, so they are defined by using the metrics f and the basis v, v has precisely n element because the dimensional v is n, so let us take this fixed basis and a ij are determined by for every j from 1 to m, f of v_j this is m element of v, so this can be written uniquely as $a_{ij} v_i$, i is from 1 to m, so these equations gives you entries of these metrics and if I take determinant of this that means the diagonal entries x minus ai and of diagonal are the negatives of the original then this determinant does not depend on the basis and therefore this determinant is a polynomial…it is clearly it is monic polynomial of degree m with coefficient in K because this a_{ij} are elements of K.

So this polynomial χ_f looks like $X^n + a_1 X^{n-1} + ... + a_n$ where a_1 to a_n are elements in K, so that means this polynomial is in $K[X]$ and Cayley Hamilton theorem says that χ_f if I put x equal to f then χ_f , f is zero this is precisely Cayley Hamilton theorem and because this μ_f is a minimal polynomial with the property that μ_f on f is zero that shows that μ_f divides χ_f , so this divides χ_f in $K[X]$.

(Refer Slide Time: 21:28)



$\mu_f \mid \chi_f$ in $K[X]$ (6)

Moreover, $\chi_f = \pi_1^{\alpha_1} \cdots \pi_r^{\alpha_r}$

$\pi_1, \ldots, \pi_r$ distinct (monic) prime poly. in $K[X]$

$\alpha_1, \ldots, \alpha_r \geq 1$

$\mu_f = \pi_1^{\beta_1} \cdots \pi_r^{\beta_r}$

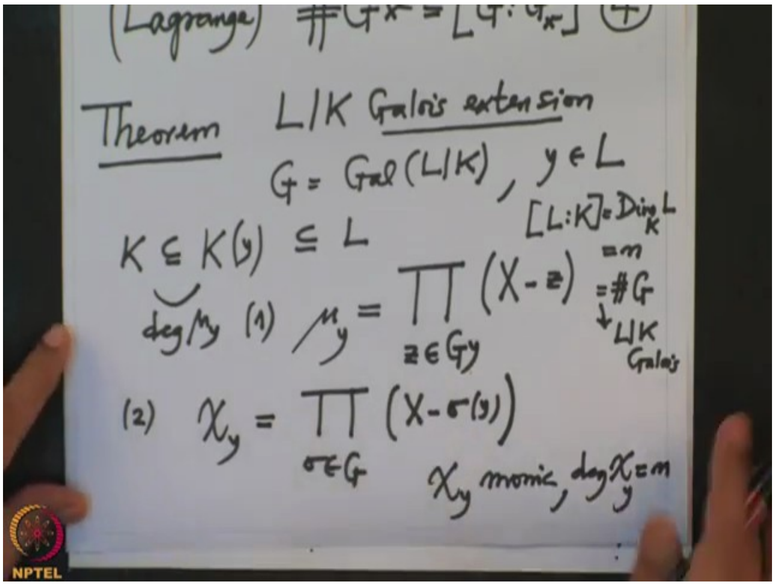
$1 \leq \beta_i \leq \alpha_i$, $i = 1, \ldots, r$

$\boxed{\mu_f \text{ and } \chi_f \text{ have the same prime factors in } K[X]}$

So I will write in the next page, so this is very important, so what we noted that μ_f divides χ_f in $K[X]$. This follows from 2 facts the Cayley Hamilton and the definition of the minimal polynomial but this is not good enough for our purpose, so there is a more finer…these divides is a crude observation, so I want to make it more precise. So moreover and there is very important for us, moreover look at χ_f , this may or may not be trying polynomial in $K[X]$, so this will definitely has a prime factorisation and I am going to write prime factorisation of this in $K[X]$.

So that is $\pi_1^{\alpha_1} \dots \pi_r^{\alpha_r}$ where π_1 to π_r are distinct monic prime polynomials, polynomial is in $K[X]$ and they occur with multiplicity α_1 to α_r and they are nonzero natural numbers. Actually when I say prime polynomials they are monic by definition so I need not ride monic again, so that is a prime factorisation of χ_f . If I write prime factorisation of μ_f at will also look like $\pi_1^{\beta_1} \dots \pi_r^{\beta_r}$ where the same π_r is and β_1 to β_r β_i is they are smaller equal to α_i there is no wonder because μ_f divides χ_f but what is more important is β_i are bigger equal to 1, so that means what? That means μ_f and χ_f have the same prime factors in $K[X]$. This is very important statement. In other words whatever prime factors appears in χ that should also appear in mu and convers is obvious because if a prime factors appears in μ it has to appear in χ_f but more important prime factors of μ also prime factors of χ also appears in μ definitely with a nonzero exponent.

(Refer Slide Time: 24:50)



(Lagrange) $\# Gx = [G : G_x]$ (+)

Theorem $L|K$ Galois extension

$G = Gal(L|K)$, $y \in L$

$[L:K] = \mathrm{Dim}_K L$

$K \subseteq \underbrace{K(y)}_{\deg \mu_y} \subseteq L$

$= n$

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

$\downarrow$ $L|K$ Galois

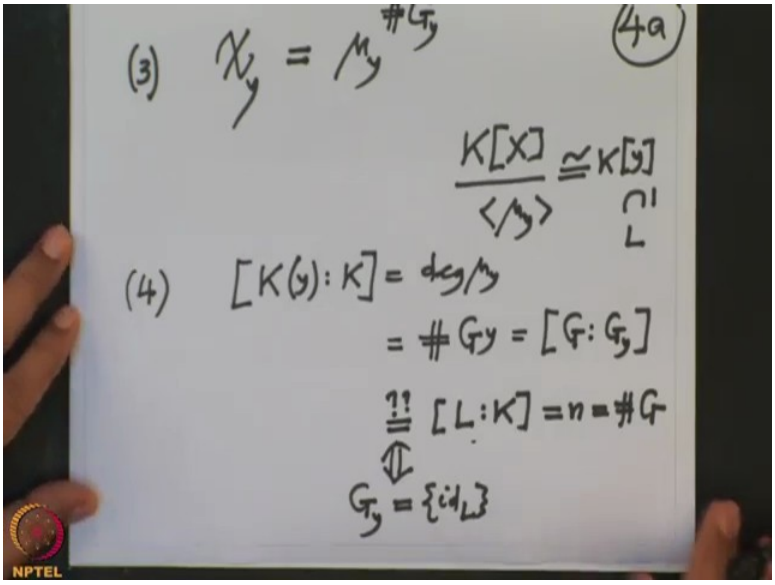
(2) $\chi_y = \prod_{\sigma \in G} (X - \sigma(y))$

χ_y monic, $\deg \chi_y = n$

Now I am going to use in this statement, so now come back to our situation our situation was this, I have to prove the μ_i is this and I want to now write down what is χ_y , so χ_y is…no χ_y should have degree, how much? Now the vector space I am considering is L over K, vector space I am considering is L over K so that means I have to know what the dimension of L over K and dimensional of L over K is precisely the degree, so remember L over K degree is precisely the dimensional of L over K and let us call this as n, so that means this χ_y should be polynomial of degree monic polynomial of degree n but n because we are assuming it is a Galois extension this n is also equal to the order of the Galois group.

So that is order of G that we know this is because L over K is Galois that is the definition of Galois extension, so therefore χ_y should have degree equal to order of G, so this χ_y claim it is equal to product $\sigma \in G, X-\sigma(y)$. Remember $\sigma(y)$ are elements of the group… σ is an element in the group so how many elements are there? There are precisely n elements and I am looking at this linear factors and multiplying them, so therefore definitely χ_y has degree n so this is obvious, so χ_y is monic is also obvious and degree of χ_y is also n that is also obvious. What is not obvious is the coefficients are in K that is one thing, so this is our 2nd claim.

(Refer Slide Time: 26:50)



4a

(3) $\chi_y = \mu_y^{\# G_y}$

$\frac{K[X]}{\langle \mu_y \rangle} \cong K[y] \subseteq L$

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

$= \# Gy = [G:G_y]$

$\overset{!!}{=} [L:K] = n = \# G$

$\Updownarrow$

$G_y = \{id_L\}$

The 3rd one is now, the question is I know I want to use the fact that χ_y and μ_y has a same frame factors, so χ_y and μ_y , 1st of all note that μ_y is prime polynomial already, it is a monic polynomial of the field extension because what do we know? We know that $K[X]$ mod ideal generated by μ_y this is actually isomorphic to $K[y]$ and $K[y]$ is a subfield of L so therefore this residue algebra is definitely a field that means μ_y generates a nonzero time ideal therefore in particular μ_y has to be the prime element therefore μ_y is a prime element, so therefore there is no other prime factor.

So if I have to write the prime factorisation of χ_y , what will it be that? That will be χ_y and there is no other prime factor, so only which can happen is the power can occur and now I want to write down that power and that will be the observation 3, so that power is nothing but cardinality of the isotropy, this is the isotropic, this is suffix y, so that is the 3rd assumption. Once I know this then I can…the 4th now I just had to write down what is the degree of…so 4th we are interested in the degree of these extension $K[y]$ over K these extension degree is precisely degree of μ_y but degree of μ_y I will read it from 1 that degree of μ_y is nothing but cardinality of the orbit of why but cardinality of the orbit is precisely the index of the stabiliser.

So when can this degree be equal to the… See we are interested in when can this be equal to L over K because I am interested in knowing when it is L over K because if I have this then L will be equal to $K[y]$. When can this be equal to…and this I know it is n which is order of the group, so when can this order of G and when can the isotropy will be equal? When this subgroup has to be trivial? So therefore this equality holds that is the assertion 4 this equality holds if and only if the isotropy at y is the trivial support. So that means if I have to prove that the given Galois extension is simple I have to find an element y, so that the isotropic at y is the trivial isotropy group?

Okay with this I will stop and we will continue the proves of this 1, 2, 3, 4 actually 4 there is nothing 4 I have indicated how to prove 4 because this was the only nontrivial track there and the others were just trivial, so I have to prove 1, 2, 3 and 3 also I have proved because I know the prime factorisation of mu and therefore I will know prime factorisation of chi I only have to find the power and therefore that is also clear because the degree mu is the orbit, the cardinality of the orbit and therefore degree of chi will be equal to order G and I have to supply this correct power, so really I have to prove only 1 and 2 and which we will prove in the next lecture.