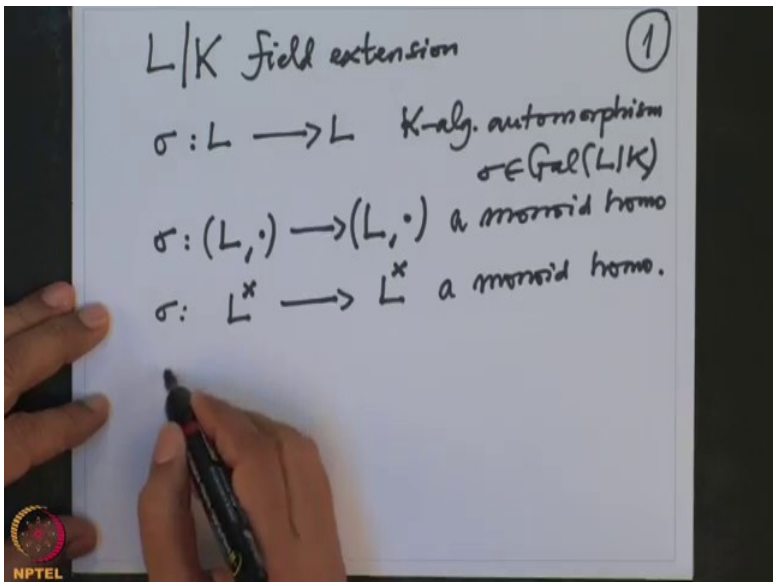
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics,
Indian Institute of Science, Bangalore.
Lecture No. 25
Dedekind-Artin Theorem

So in the last lecture, I stated Dedekind Artins theorem, will said that the order of the Galois group is bonded by the degree of the field extension, so to prove this, a Dedekind proved in a classical case and Artin proved it in little bit more journal setup, so I will first recall Artins remarks and then we will tie-up and at the end we will prove the Dedekind Artin Theorem, so I am now preparing for Artins little bit more general proof.

(Refer Slide Time: 1:13)

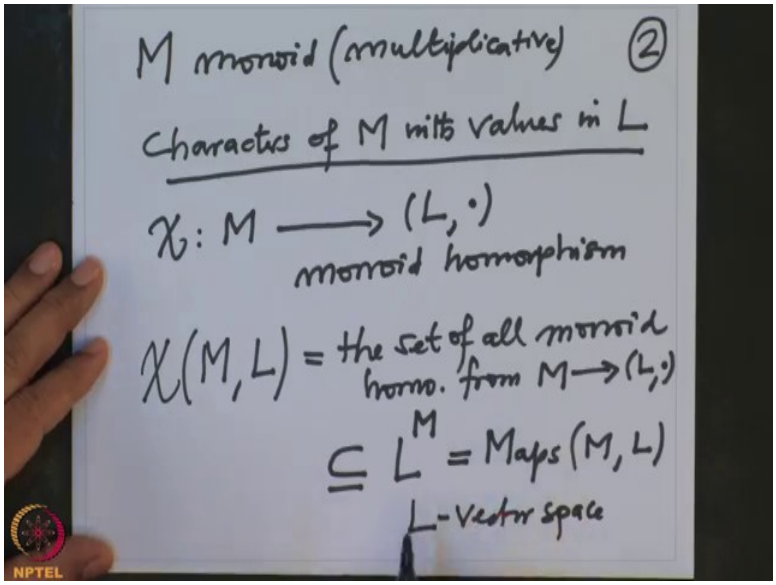


So as usual notation is L over K field extension and assume finite, when I need really than I will write down it is finite, but right now I do not need, so if I take an automorphism σ from L to L, K algebra automorphism that means an element of the Galois group of L over K that is σ belongs to $Gal(L|K)$, then, that means if I just look at the multiplication that means σ $(L,.)\rightarrow(L,.)$, this is a monoid homomorphism, because it respect the multiplication and obviously zero goes to zero because σ is linear here, so zero goes to zero.

So, it will also induce $L^x \rightarrow L^x$ monoid homomorphism, more generally, I could consider, more generally, see ultimately we want to prove that there are as many elements as at most the number of elements in the Galois group are the degree of the field extension, so somehow I have to relate linear independence and elements of the Galois group, so elements of the

Galois group, there are monoid homomorphism, so more generally, I will consider, so consider little bit more generally situation.

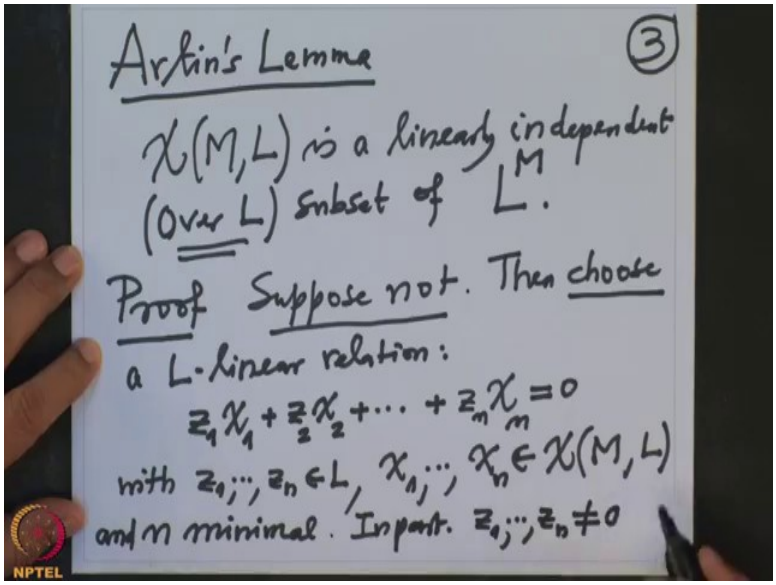
(Refer Slide Time: 3:27)



So M, I take a monoid and I will denote monoid multiplicative the notation will be multiplicative and so-called characters of M, with values in a field, with values in L that means what, that means a monoid homomorphism, χ from M to $(L,.)$ monoid homomorphism, such monoid homomorphism are called characters of M with L is in L and the set of all monoid homomorphism from M to L, I am denote by $\chi(M,L)$, this is the set of all monoid homomorphisms from M to $(L,.)$ or characters, from M to with values in L and think of also this is a subset, so they are mapped for M to L, so think of this as a subset of L^M , so L^M is not so good notation, so this is the set of all maps from M to L.

So this all characters is a subset of maps from M to L and this set has a structure, this is a vectors space, this is a L vectors space, component wise, scalar multiplication and component wise addition is a vector space structure on this set, that means you added point wise and scalar multiply will also point wise, so therefore these set is a subset of these vectors space, I want to prove that this set is linear independent over L that is what Artin's Lemma.

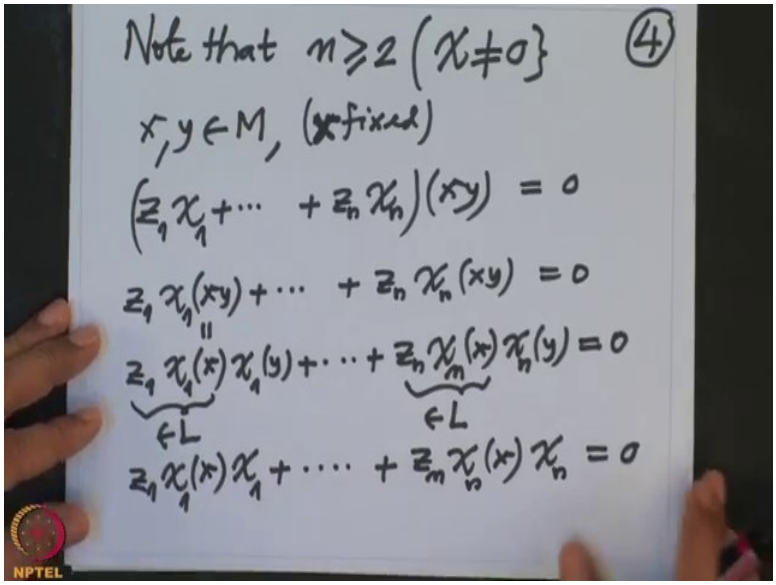
(Refer Slide Time: 6:04)



So this Artin's Lemma says that $\chi(M,L)$, is a linearly independent over L, a subset of these vectors space L^M , now when do you say subset is linearly independent, when there is no linear relation, a linear relation is also a finite, so that means no finality many elements of this set satisfy a linear relation with coefficients in L, that is where over L, so let us prove this first, this is very simple, so proof.

So suppose not, that means what that means they are finitely many elements in chi M L and there is a linear relation among them with coefficients in L, but among all such relations, I am going to choose a relation which has a minimal length, so this means choose, then choose a linear relation $z_1\chi_1+z_2\chi_2+\ldots+z_m\chi_m$ and suppose this is zero where with z_1 to z_n , are elements in L, coefficients are in L and χ_1 to χ_n they are characters they are elements of $\chi(M,L)$ that characters from on L, with values in L and I want to choose n minimal choose relation with and n minimal. So therefore all this is z are nonzero, so in particular z_1 to z_n are nonzero all are nonzero.

(Refer Slide Time: 9:09)



Also note that n has to be at least 2 because no character is, so characters are always nonzero, because it is a monoid homomorphism, so identity of the monoid is going to, go to the identity of the monoid $(L,.)$ but identity of the monoid $(L,.)$ is 1, so characters are always nonzero and one character is nonzero, any nonzero element times character is also nonzero, so if at all it is a linear relation it has to have at least linked two and we have chosen the minimal one.

Alright, so now this linear relation means what? That means, evaluated at every point of M, it is zero, so therefore keep, let us take two elements, x and y in the monoid M and let us remember that y I want to fix it, y is fixed, element in M and x I am going to vary, so when I evaluate this $z_1\chi_1 + \ldots + z_n\chi_n$ this evaluated at x, y, x times y, x, y are elements in M, M is a monoid, so productive is also there and this has to be 0 because we are assuming this linear relation is 0, so evaluated at any element it is 0.

But this is now, what is this? When? How is it defined the linear relation? It goes inside, so this is $z_1\chi_1(x)\chi_1(y) + \ldots + z_n\chi_n(x)\chi_n(y)$ this is 0, but this one is because it is a monoid homomorphism, so this one is $z_1\chi_1(x)\chi_1(y)$ because it is a monoid homomorphism, and so on, so the last one is $z_n\chi_n(x)\chi_n(y)$, this is 0.

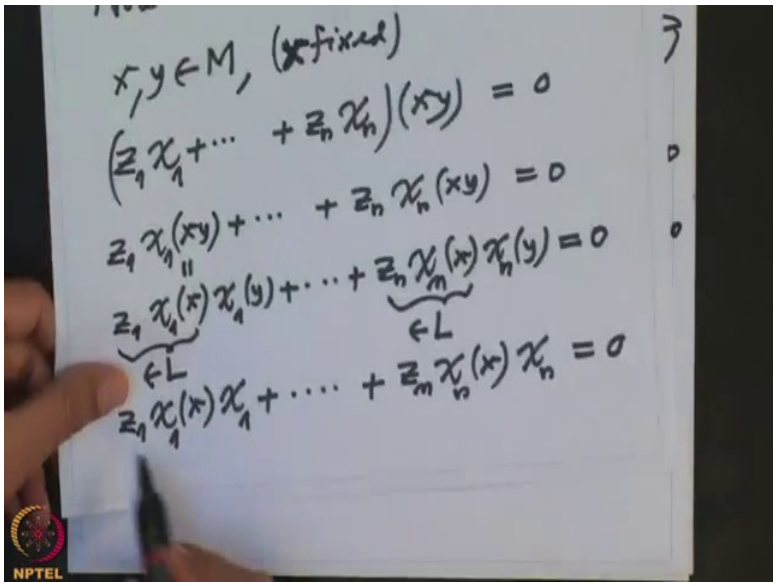
Now this is in L, this is also in L and this is zero for all, y is varying but, so this is, y is varying and this is zero for all y, so therefore we get. I should have said x, keep x fixed and y

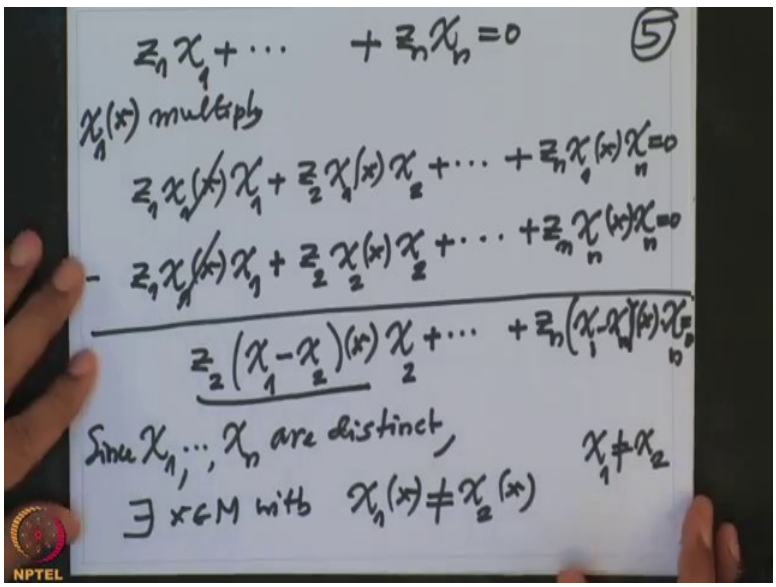
vary, so y is varying, so therefore from here you conclude that $z_1\chi_1(x)\chi_1+\ldots+z_n\chi_n(x)\chi_n$ this is zero, because this evaluated at y is precisely the earlier one and that is zero for all y.

Therefore this linear relation we get with coefficients in L and now I am going to produce a linear relation with a smaller length. So, now this one is 1 and the original one is this one, $z_1\chi_1$ etc, etc, I want to cancel one term, so I am going to multiply this equation by $\chi_1(x)$ and let see what happens.

So, that means I want to consider, I want to multiply this original relation, so I have to write on the next page.

(Refer Slide Time: 13:06)



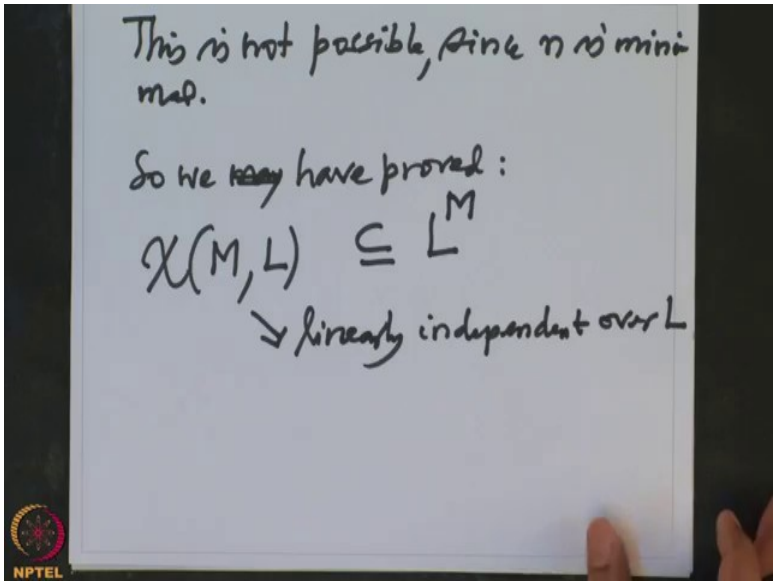


So this, original relation was this and I want to multiply this relation throughout by $\chi_1(x)$, multiply, then we will get $z_1\chi_1(x)\chi_1+...+z_n\chi_n(x)\chi_n$, this is still zero because we have multiply this equation by $\chi_1(x)$ and the new equation which I got, I will rewrite below this that is $z_1\chi_1(x)\chi_1+...+z_n\chi_n(x)\chi_n$, this is zero, this is how we got the this equation, this one and now I want to cancel, so I subtract, if I subtract this from this, what do I get, the first one, get cancel, that is how I multiplied this get cancel with this and here what we get, (we get z_1), z_2 and what is the term $(\chi_1-\chi_2)(x)\chi_2+...+(\chi_1-\chi_n)(x)\chi_n$ and this is zero.

But now all the terms if the original relation has at least two elements that means at all of them are χ_1 is not equal to χ_2 in particular because if they were equal, then I could simply add, if they were equal than I will just club it with z_1 and minimise a relation, so I can, we are assuming that all these χ_1 to χ_n are all distinct characters, so I should I mentioned it in the beginning like z_1 to z_n are nonzero, χ_1 to χ_n are distinct, since χ_1 to χ_n are distinct in particular, this $\chi_1\neq\chi_2$ and therefore at least one element they will differ. So, there exist some $x\in M$, with $\chi_1(x)\neq\chi_2(x)$ and therefore this coefficient here is nonzero because z_1 is an element in L, which is now zero, this is also is an element L, which is nonzero, by we have chosen our x.

So therefore this coefficient is definitely nonzero, so therefore I have a nontrivial relation whose length is less equal to $n-1$, so therefore it is not possible. It is a contradiction because we have chosen relation with the minimum length, so this proves the Lemma.

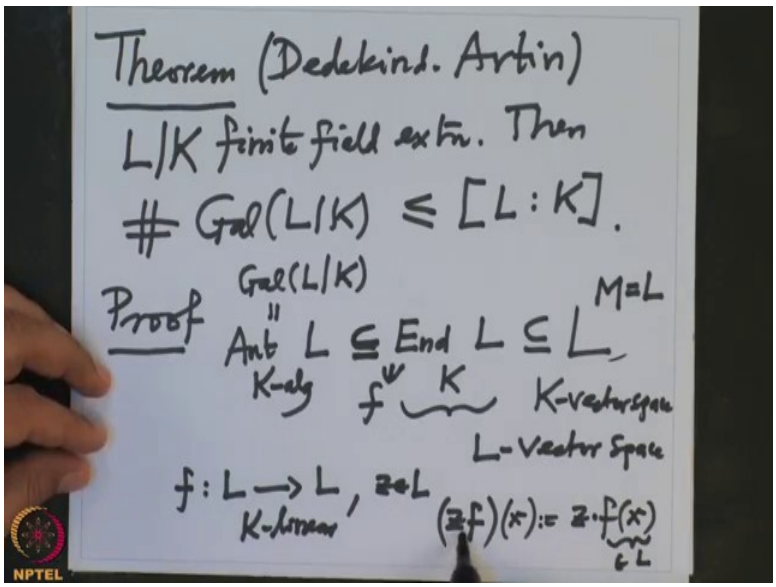
(Refer Slide Time: 16:48)



So this is not possible, since n is minimal, so that proves the assertion that chi, so we have proved that $\chi(M,L)$, this are the subset of L^M , this is linearly independent over L.

Alright, so now we will continue our proof of the, now, the proof. So let me recall what we are proving.

(Refer Slide Time: 17:52)



So the theorem we are proving is the Dedekind Artin what we are proving is L over K finite field extension, then cardinality of $Gal(L|K)$ is smaller equal to the degree of the field extension, this is what we want to proof, so proof. Alright, so let me recall, so the big vector

space, we are working here is L^M , actually M is L I am taking, $(L,.)$, M is L with a multiplication of L.

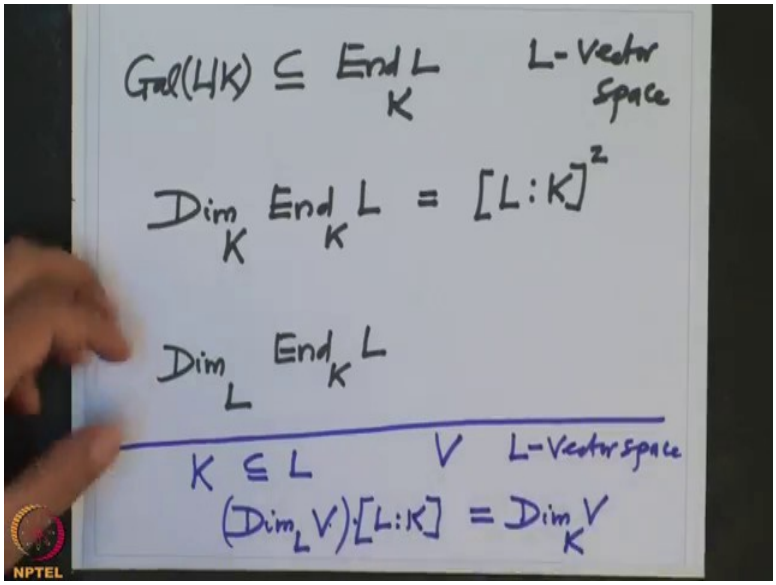
Okay, now this vector space, obviously contains their map from L to L and not arbitrary maps, but which preserves, so this are all map from L to L and if I take the endomorphisms of the vector space L over K that is a subset because this are all maps from L to L and this are maps which are K linear maps.

Okay, and among them, this $Aut_{K-algebra}L$, this is a subset here because when I say K algebra automorphisms they are K linear automorphism and K linear automorphisms are endomorphisms, so therefore this inclusion is also clear and this is our Galois group, so we are working here and we are bothering about the cardinality, this is a big set, this is.

Okay, now this endomorphisms this one is actually what is apparently it is a K vector space, because we can add two linear maps and multiply linear maps by scalars and that becomes a vectors space over K, over K, because K linear maps, we can add point wise, we can also add, we can multiply scalar multiplications point wise, that gives you a K vector space structure, but I want more. I actually I want to say it is a L vector space, so I should tell you what is a scalar multiplication by L on that. So, if I have a linear map f from L to L, which is K linear, this means f is an element here and z is an element L, then I should tell you what is zf , this should be again a linear map K linear map from L to L, but that is you define on x is $zf(x)$.

This $f(x)$ is an element in L, z is also element in L, so this is a multiplication in the field L, so with this definition, this scalar multiplication of L on this, note that this L.

(Refer Slide Time: 21:40)



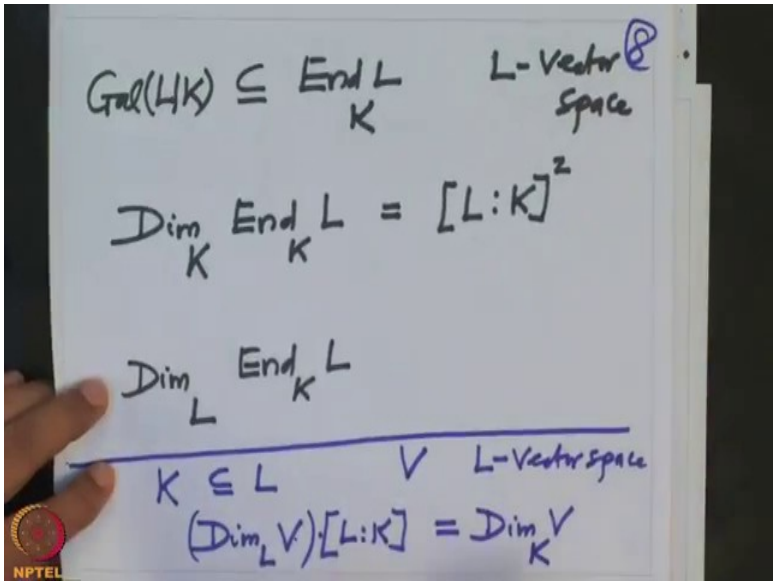
So therefore End L over K, this becomes L vector space and then there was a subset here that what we are interested in Galois group of L over K, this are all automorphisms, K algebra automorphisms of L, okay, let us remember what is the dimension, now I want to compute the dimension, so if I write dimension as a vectors space over K of End, this I know what is the dimension, the dimension is same thing as L over K square, this is because it is thing of endomorphisms will corresponds to the mattresses.

So $M_n(K)$ has dimension n^2, so by that observation dimension of this endomorphisms K precisely $[L:K]^2$. Okay, and what is the dimension of now as the vector space, now I want to compute dimensional of $End_K(L)$ as a vectors space over L, what is the relation between this to dimensional is? See this is, recall here I will write in a blue thing, so you can do the thing.

So here is, we have K field, L field and vector space V, V I am considering L vector space suppose I have given this situation and then V is also L vector space by restriction and how do I compute what is relation between dimension of L over V and dimension V over K, what is the? Whose dimension is more as a vectors space over L, this dimension and will be less and as a vectors space over K, the dimension will be more and what is the? How do you compute dimension? This is L over K, multiply this by L over K and you get this, this obvious, because here the coefficients allowed are only in L and hear coefficients allowed are in K, so each coefficient in L you convert into K by a taking a basis of L over K and therefore

this dimension will be product of this two dimensions, that is obvious, because take a basis L basis of V over L and take a basis of L over K and multiply this.

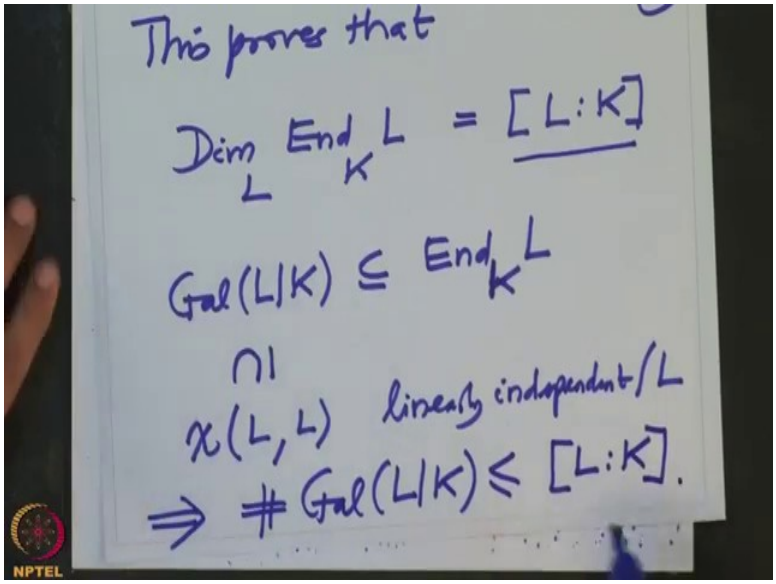
(Refer Slide Time: 25:01)



So let me right it, so this formula can be proved very easily like this, so we have, so we choose the basis of v_j , L basis of V, j is varying in some set J and take z_k , K basis of L, K is varying in some set I, then you look at this $z_k v_j$, they are kj varying in $I \times J$ then obviously check that disease a K basis of V, that means a dimension of V will be the cardinality of this which is a product and dimensional of this is the, this one.

So you get, so this formula is therefore, this is how we prove this formula, now therefore what do I say, this dimension equal to this times the degree of L over K right, so we have proved this equality, now if I want to compute this, I will just look at this extreme two things and I cancel one.

(Refer Slide Time: 26:33)



So this proves that I will write… so this proves that the dimension over L of this endomorphism of L over K, this is same thing as L over K, this is what we have proved and what do you want to prove? Dimensional is L over K and then, we want to prove about this cardinality, this is a subset of this, so therefore and we have proved the elements of this, see what are this? See this one is containing χ their elements of the Galois group are the automorphism of L over K and then you can think of their containing L, $\chi(L,L)$, these are the characters of L with values in L, just restrict them to the multiplication map, so this is a subset here, so and then we are proved this subset is linearly independent over K, over L that is, what we have proved, this subset is linearly independent over L.

So therefore the cardinality of this subset cannot be more than the dimension where it is contain, so this is… therefore, this subset cannot have more cardinality than the dimension of this as a vagal vector space, but that dimension is this, so that proves cardinality of the Galois group of L over K is smaller equal to the dimension, which is this, that is what we wanted to proof.

So we have proved that whenever we have a finite field extension, the cardinality of the Galois group cannot exceed the dimension of L over K, so this is very important step we have proved, that means whenever we consider finite field extensions, the Galois groups are always finite and as I mentioned earlier, that this already proves that the Galois group of $\mathbb{C}$ over $\mathbb{R}$ is cardinality two, Galois group of finite field extension is also exactly the equality here holds. That is what we have proved, so I will continue in the next lecture from here. Thank you.