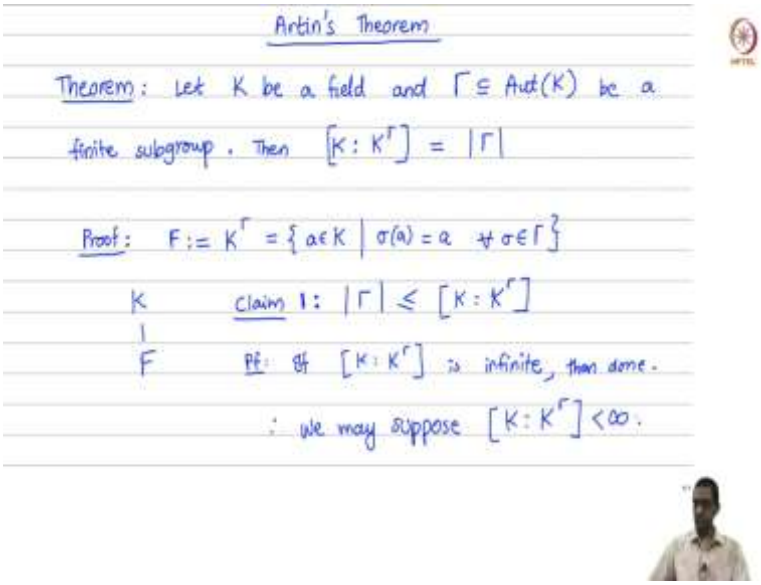
Algebra - II
Professor S Viswanath
Department of Mathematics
The Institute of Mathematical Science
Lecture 33
Artin's Theorem – Part I

(Refer Slide Time: 00:14)



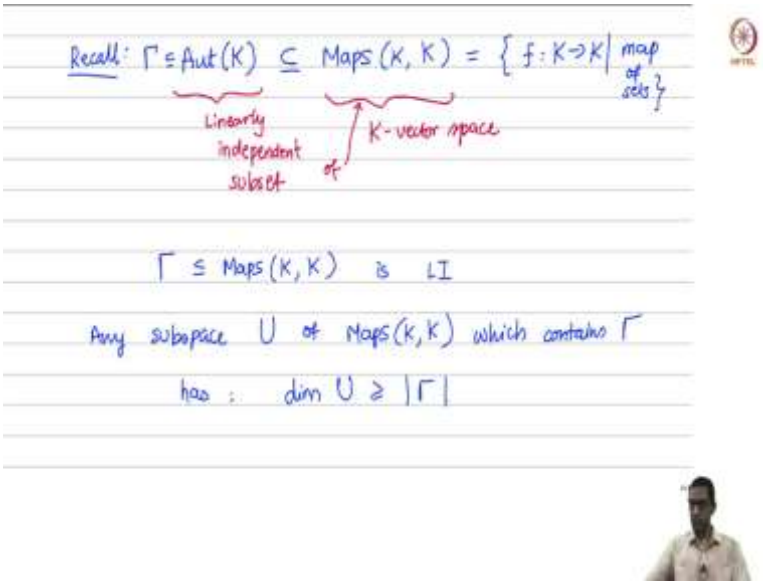
Today we will prove the following important theorem due to Emil Artin. So, statement is the following: Let K be any field, K be a field and gamma be a finite subgroup of the group of automorphisms of the field, be a finite subgroup, of the group of automorphisms. Then recall we talked about the fixed field of K, just a set of all elements of K which are fixed by every element of gamma, then K colon K comma that is the degree of this extension is finite and in fact, it is equal to the cardinality of this subgroup gamma.

So, recall the finiteness of this extension is also part of the theorem and you know this, this theorem is rather important, it will play an important role in the further development of Galois theory as we go along. Let us prove this theorem; we already established one important ingredient of the proof, which is the linear independence of characters. So that is what is going to be used here. So let us prove, let us set up some notation first.

So let me call this fixed field as F. So let me, let F denote the fixed field K gamma, which is the set of all elements of K, such that sigma a is a, for all sigma (())(2:02). Recall it is a subfield. So let us look at the extension K over F and we will establish the theorem in two parts. We will establish inequalities in both directions, for the dimension. So let us say first claim is going to be that the cardinality of gamma is at most the degree of extinction.

So this is the first claim and then claim two will be the reverse inequality that the degree of the extinction is at most the cardinality of gamma. So we will prove this using the linear independence of characters. So first observe if the degree of extraction is infinite, then of course, this is trivially true is nothing to it, is infinite. Then we are done because cardinality gammas finite the areas. It is infinite; there is really no content there. So let us assume so therefore, we may assume, we mean suppose that the degree of his extension is finite. So it is a finite extension. So we make that assumption.

(Refer Slide Time: 03:24)



Now, recall the following that the space of automorphisms, the group of automorphisms is a subset of what we call maps k, k set of all, this is just all set maps just functions from k to k. This map of sets, no further structure and we said that this is of course a vector space this is a vector space over k and the corollary to proof of linear independence of characters, we said that the space or k is actually are linearly independent subset.

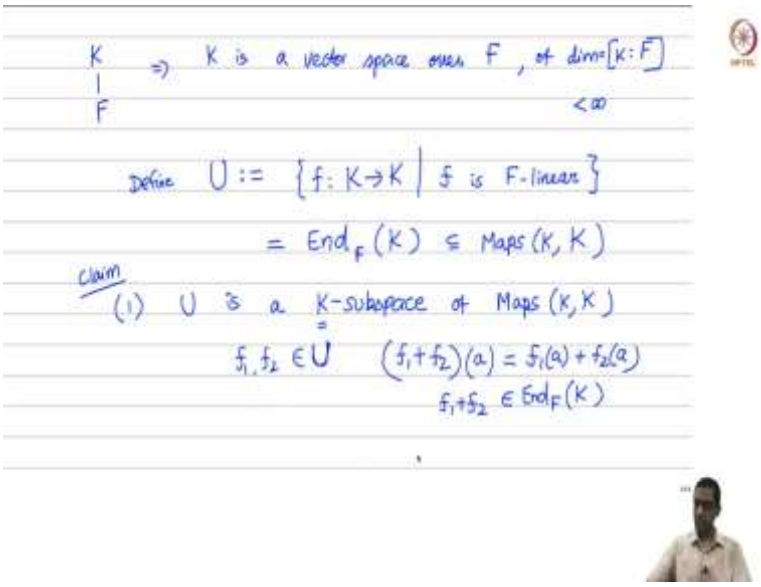
So, this is a linearly independent subset of this k vector space, maps k, k. Now, so what does that mean? When I have a vector space and they have linearly independent subset inside this vector space then, let us look at gamma because that is what we are interested in. Let us look at gamma. It is a sample of a linearly independent set.

So gamma is also linearly independent. So, clearly the elements; the automorphisms in the gamma subset of maps k k is also linearly dependent. And in particular, this implies that if I take a subset of available, take a subspace. So any subspace it is called U of maps k k, which contains gamma has dimension at least, so satisfies the following property that the dimension

of U must be at least the cardinality of gamma because gamma is a linearly independent subset and use a subspace which contains it.

So the dimension of U is definitely more than the dimension of gamma. So, that is going to be our approach, we are going to try and prove this inequality by producing a subspace U inside maps k k, which has dimension equal to the degree of the extension. So the right hand side will be realized as the dimension of some subspace of the space of maps.

(Refer Slide Time: 06:10)



So that is the idea and in this case, it is not too hard to construct this subspace. So recall K, so what are we thinking of K as: K is an extension field of F. But that in particular, of course means that K is a vector space over F and we also know its dimension. It is called degree dimensioning into K over F and recall to start with, we assume that this is finite.

So therefore, this is in fact, a finite dimensional vector; K is a finite dimensional vector space over F and therefore the subspace, let us look at the following subspace. For the moment, a subset, let us define U to be the set of all maps, think of it as the set of all maps f from K to K, set functions which satisfy an additional property that f is a linear transformation of K thought of as a f vector space. So f is F linear.

So, it is a linear transformation from k to k, when you view k as an F vector space and this is the canonical standard notation for this. This is just the end f k, the space of all f linear and endomorphisms of the vector space K. So I am going to define U as this. Clearly use a subset

of maps k k and let us check the following properties of U. Firstly, U is in fact a, so maps k k is a K vector space. So claim is that U is actually a subspace.

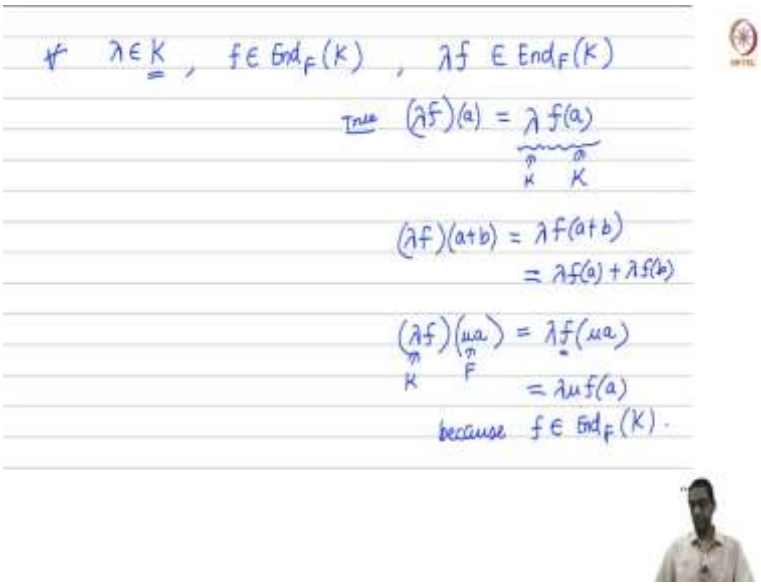
So just to emphasize that, now we are talking, every vector spaces are over K now, rather than over F. So recall, right now, we sort of have both things are vector spaces over K which we are looking at. There are also, K itself is thought of as a vector space over F. So let us just make things clear by, I just put a K there to say that I am thinking of U as a subspace of the K vector space maps k, k.

So I claim firstly. So here are some properties claim, use in fact, a K subspace of the vector space maps k, k. So that is in fact rather easy because what is, what do elements of U look like? So if I have f1 and f2, two elements of U. So I need to, to ensure that they are closed under addition, and it is closed under scalar multiplication by K.

So what should I do? First, let me check if it is closed under addition. I take f1 plus f2 and I ask how does it work? What is the value at a it is just a f1 a plus f2 a and of course, we know that sum of two linear transformations is automatically a linear transformation. So that is the definition and this is anyone can easily check that f1 plus f2 is F linear.

It is again a linear operate. So this is the easy part. The part that is somehow not immediately obvious is, if I take an element F in U and I take a scalar lambda from K, not lambda from F, but lambda from K. So you already know that if you take a linear transformation, linear operator on a vector space, if I multiply it by the scalar from the base field, then of course, what I get again is a linear operator.

(Refer Slide Time: 10:19)



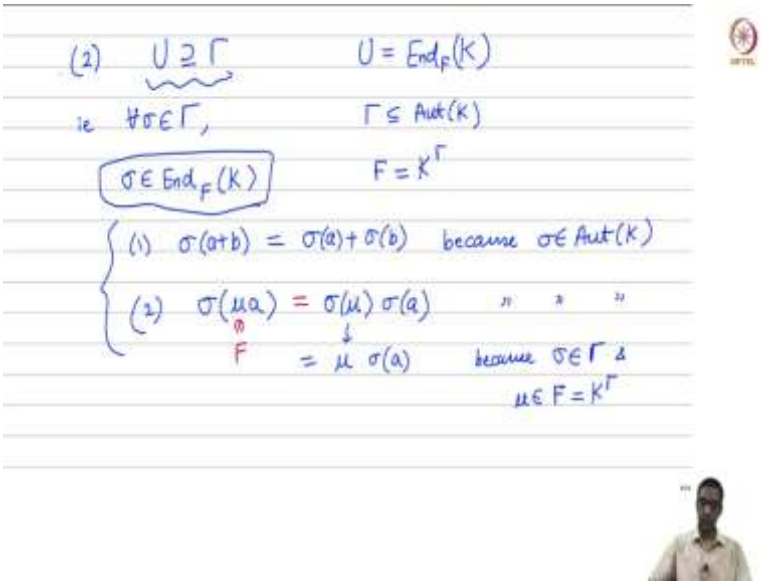
If lambda comes from F, lambda times from the base field F, then lambda times f, small f here, lambda f could of course automatically be a linear transformation. But I want to claim that if I take lambda in K and f in U; let us do it in the next page. So we need to actually check this to ensure things are okay, we take any element of K and for all lambda in K and for all elements linear operators F on K, we need to check that this lambda f is again, f linear operator.

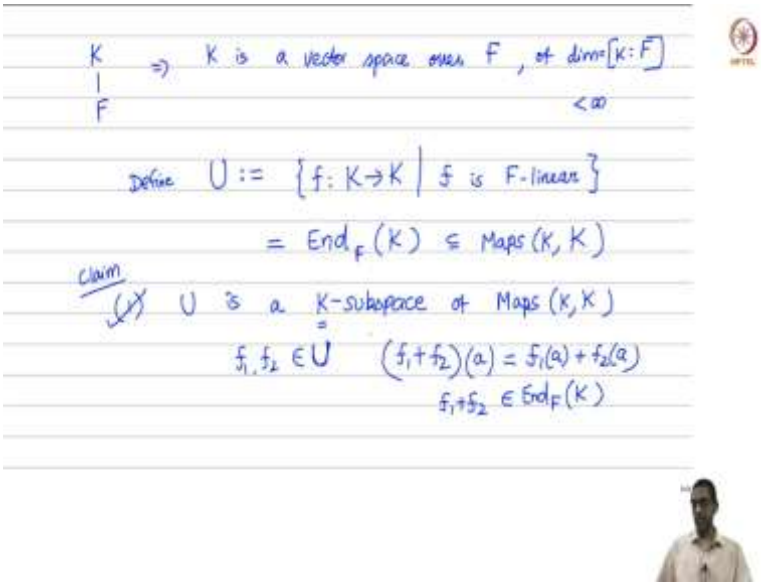
And why is this true? Because just from the definition this is true because just see what lambda f does to a. You first evaluate f on a, that is now an element of K because f was a map from k to k in a. And now you multiply that element of K by this other element of K, which is lambda. So it is just multiplication. And now this new definition is lambda f.

Why is this f linear? Well, you have to check that if I put a plus b, then I will get a plus b on the other side, but it is more or less, I just had to multiply by lambda anyway, afterwards and f was, f was linear, f was linear over the base v. And similarly, if I take lambda f, and I need to check the linearity of the base field, if I multiply by some element mu from the base field, so mu is from the base field f, lambda is from the bigger field K.

I need to check whether I can pull the mu out, first by definition, this is lambda f of mu a and the map f is a linear transformation, which is f linear over the base field. So I can pull the mu out. So this is a lambda mu f of a, because f is actually in end F K.

(Refer Slide Time: 12:29)





So I can pull out scalars from F. So what this says so like I said, it required a little checking but it is a, it is still a very simple fact that you multiply by lambda coming from k, what you get is still a f linear transformation. So that checks the first claim that the subspace U is actually a K of space.

Property 2; let us check that U actually contains gamma, so recall that that is how we are going to prove that I mentioned bound, as U contain gamma, what is U and what is gamma? So recall U is just set of all F, linear operators of K, gamma is some subgroup of a group and the key definition here F is actually this, the set of fixed points of gamma.

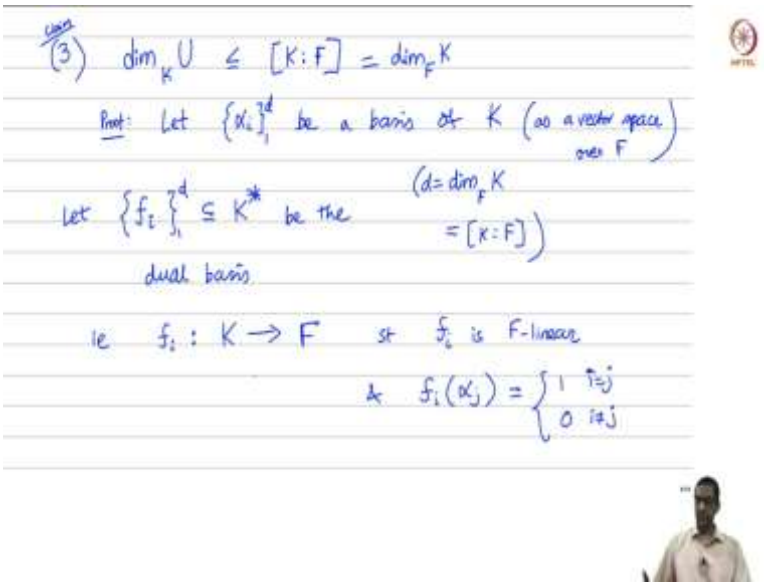
So, why does U contain gamma? We just have to check that. So, to check this I need to check IE. So, what is the statement say? IE will take any element sigma and gamma. Sigma is actually a linear transformation from, I can think of, sigma is actually a field automorphism. But sigma is actually also a linear transformation from k to k with, linearity over the base field F.

So, is this true? Let us check the properties. So, sigma of a plus b has to be sigma a plus sigma b, but that is true because sigma is a field automorphism. Because sigma, it is in gamma. So in particular, it is a field automorphism. Property 2; if I take sigma and I multiply a by an element mu, mu is a scalar from F, then I should be able to pull out the mu.

That is what linearity means. But now, this is the same as sigma mu sigma a, again for the same reason, sigma is a field automorphism but now sigma of mu is actually mu again. And why is this? This is because sigma is actually in gamma and mu is in F, which is the fixed field of gamma. So that means that sigma certainly fixes mu.

Sigma mu must be mu because mu is coming from K gamma. So, that is the key thing to check that. So, that means the mu can be pulled out. It really came out as a sigma mu but sigma turns out to be a mu in this case. So, we have actually checked both properties and sigma is required to satisfy in order to be a linear transformation.

(Refer Slide Time: 15:28)



So we have also done this. So we have sort of done what we set out to do. We have constructed a subspace U which contains gamma and the subspace is the obvious one here,

the set of all F linear automorphisms of K viewed as a vector space. But then finally, here is the thing, U is actually finite dimensional. U is actually; recall we said U is a K vector space. But in fact, its dimension, over K is finite and is actually equal to the degree of the extension, the dimension, is the dimension of K over F.

It is actually equal. But we do not need the full force of that. So I am not going to bother proving it. I am just going to show you that the dimension of U is at most, the dimension of K over F. And I will sort of leave the proving of the universe inequality as an exercise. We will not need for the proof itself.

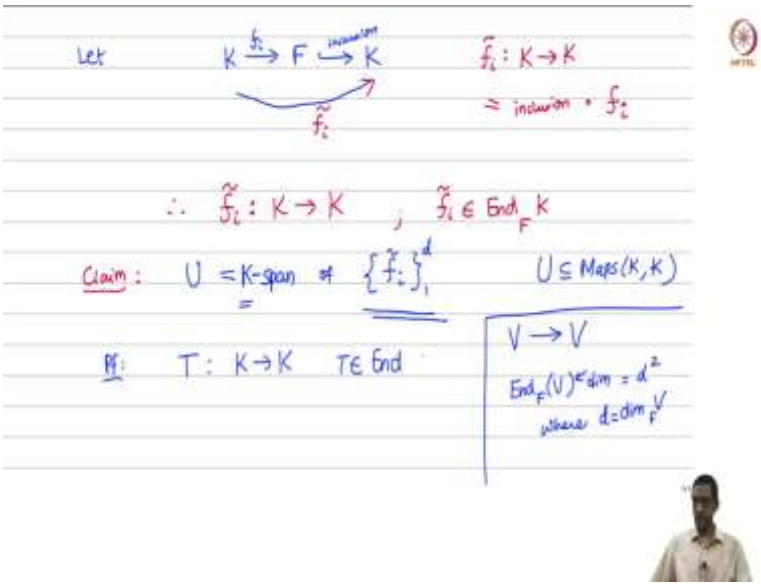
So this is the third and important claim that the dimension of this space U is at most the dimension of K over F. Now, this requires a little prove. So let us prove this. So, what was U? U was the space of endomorphisms and let me try and construct for you a spanning set of U which has cardinality equal to the dimension of K over F. So how are they going to this?

So, let us pick alpha i from 1 to d be a basis of K over F, basis of K as a vector space over F. So recall, we have already assumed that the K over F is a final dimension vector space. So, let d denote this the dimension of this space. So, for me here, d will be just the dimension of K as a vector space over F. Yes, I take a basis and let us construct, let us look at it is what we call the dual basis.

So, let for these alpha i corresponding to the alpha I, I have maps f i. So, what are the f is? Onto d these are elements of the dual vector space. So, let this be the dual basis. So, what does that mean? So, recall dual basis given a basis you can construct its dual basis of linear functionals.

So, i e what are the f is? The f is are linear functionals on K. In other words, they are maps from k to the base field, the field remember is F here. So, f is are maps from K to F and they satisfy the property, I mean they are linear such that f phi is linear functional. It is F linear and f i evaluated on the basis elements gives me 1 or 0. So, this is 1 (())(18:32) to j, 0 if i not equal to j, so this would be called a dual basis corresponding to a given basis alpha.

(Refer Slide Time: 18:53)



So, now what have I done? I have constructed d elements or d f is which are all maps from K to F but I will now think of these as maps from k to k. So, what should we do? Let us call a fi tilde be the following map. It is a map from k to F composed with the inclusion map from K to F. So, let us do the following packet fine. And this is just the inclusion map. The composition of these two things we will call as fi tilde.

So, what is now fi tilde? It is become a map from k to k. It is just the inclusion composed with and observes, this is a composition the inclusion map is also a linear transformation of these two f vector spaces. So think of everything here as being an f vector space. Then fi is F linear inclusion is F linear. Therefore, this composed map that we have constructed should be thought of as a map from k to k, which is F linear.

In other words, fi tilde is an endo morphism of K over F. So these are, we are almost there, we now have a bunch of maps. Our claim is that this subspace U that we are looking at, is spanned by these fields. So U is just the span of these d elements fi tilde. So U was what? U was just a full set of endo morphisms. The claim is these d endo morphisms are enough to span the whole space but now we call everything is.

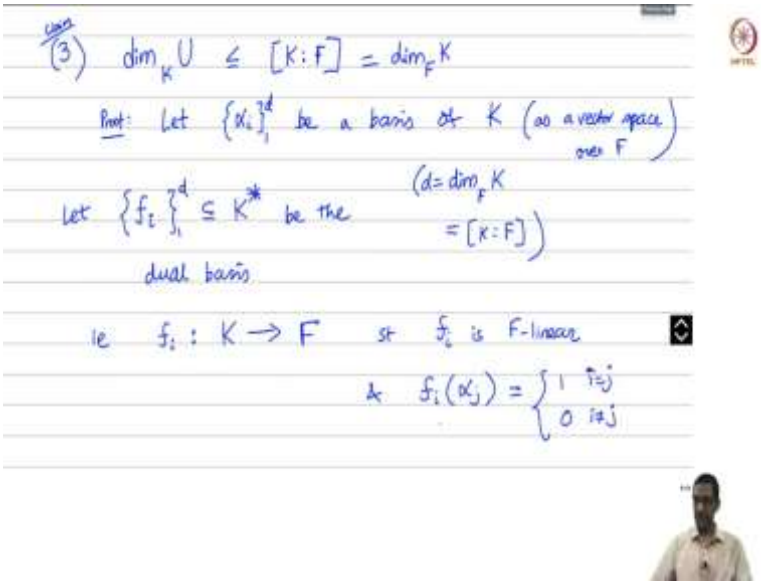
So now I have, I am again switching fields. I am thinking of U as really a subspace of the space of all maps from k to k and so these are all and we have already shown that use a vector space. So I claim that over k thought of as a k vector space, the span of a fi tilde will actually give me everything.

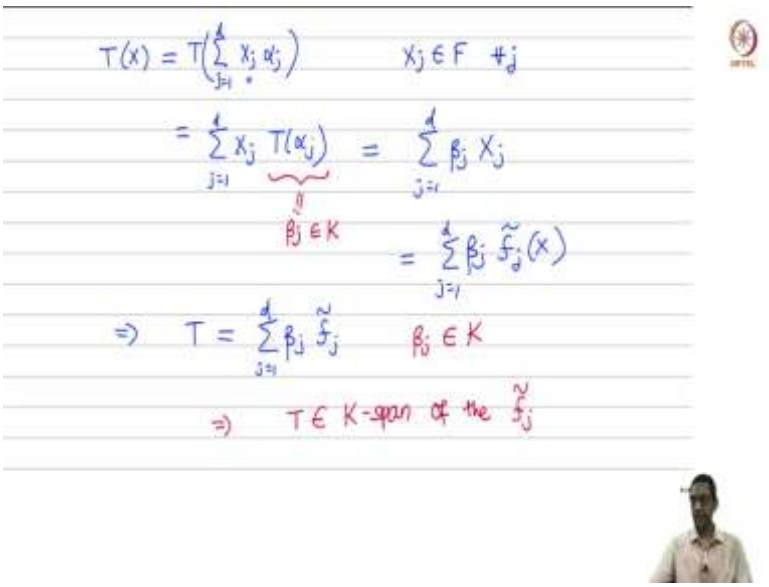
So this will not happen over F because if I have so quick aside; so suppose I have a vector space V over the field F. So I am saying, suppose I look at the space of all endo morphisms over the base field, from V to V, we know the following that this has dimension, the dimension of this space is d squared because, what is d. d is the dimension of the Ambien vector space V over F.

So, if V has dimension d, then the space of endo morphisms is like the space of all because d cross matrices. Remember linear transformations and matrices are the same thing. And so this is like the space of matrices, which has dimension d squared. So over F, this has no chance of being true. And claiming it is enough to just have d elements, these particular d elements will give me everything that is fact.

And the reason why this works is because this is actually over the bigger field K. So, we are claiming, if you take the bigger field K, then these d elements are in. So, let us prove this. So once we identify the right elements, so proof itself is easy. So let us take a linear transformation. So let us take T from K to K, T belongs to U, in other words T is K, F linear endo morphism.

(Refer Slide Time: 22:46)





I need to show T can be written as a span of these elements. So let us look at what T looks like. So T of an element x is just, so I first write the element x as a linear combination of the basis elements, alpha j. And now what are the x js? x js are all elements of the base field F and because the alpha j is former basis of K over F and now this is just summation x j, T of alpha j.

I know let us call T of alpha j as a new element of K. So T, what is T acting on alpha j? It is just going to be some other element of K. So let me call this element as beta j. This definition, beta j is this element. And that is of course, an element of K. And now know, this becomes the sum beta j x j, j equals to 1 to d and now what is x j? Because x j is just what you get.

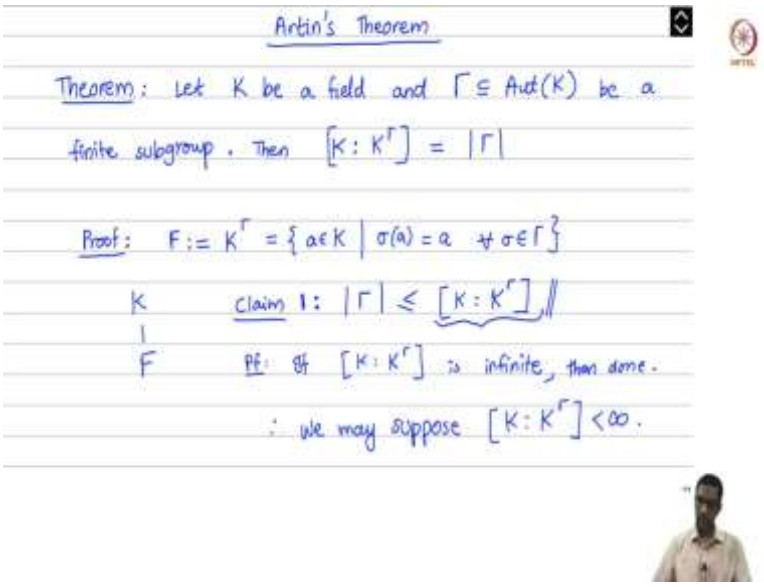
So, x j is just the coefficient of alpha j in the linear combination. This is just the value f j tilde of x. And why is that? Because of the way it was defined. So if you recall, what f, what the f is where they take value 1 on alpha j, fi takes value 1 on alpha i and 0 on everything else. fi tilde is the same thing really.

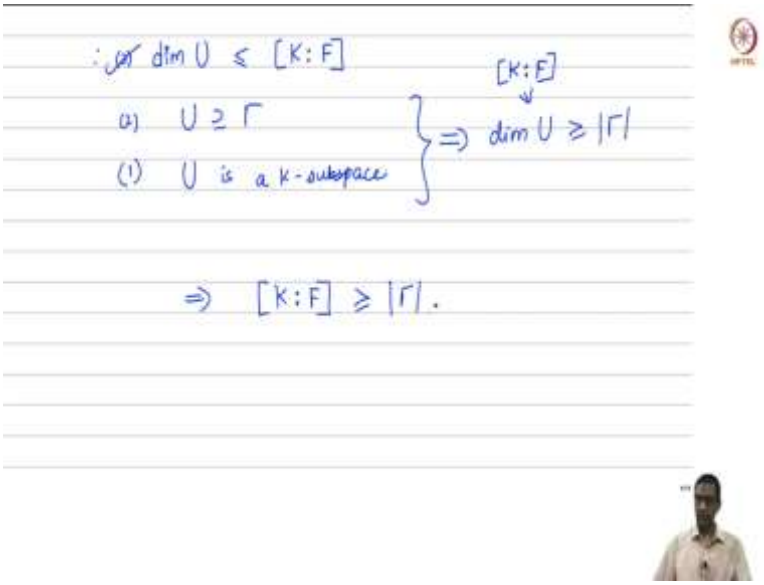
The same as a fi and then after that, you just take the inclusion into k. So, it does not do anything new. So fi tilde is just going to first map alpha i to 1 and all the other alpha j is to 0. That is what fi tilde does. And so if you ask what is f j tilde on x? You apply it to this linear combination, then it will kill all the other alpha is except for the jth one. So, there is the usual property of dual basis.

Very good. So we just look at the, what we have shown finally, this just means we have shown T is just this linear combination beta j fj tilde. And that is exactly what we set out to

prove. And the key point recall here is that beta js are now elements of K not necessarily elements of F. So that is really what makes the proof work. So this means that T belongs to the K span of the fj tilde. So, what does that give us?

(Refer Slide Time: 25:31)





It proves the following; it shows that at 4. So, let us look at all the 3 facts. So, we have shown firstly that, so let me just write this out. So this just plainly shows that dimension of this space U is at most the degree K colon F. So, having shown that this is atmost the degree, what does it, what does it give us? It says that Zion and together with the other two facts, so let us also write. This was the third fact which we have not proved. And recall facts one and two said, fact two said U contains the space gamma.

The set gamma and use a K space. So, between these two, we conclude that the dimension of this space U, whatever it is, must be at least the cardinality of sigma. And the first condition says that the dimension of U is further bounded above by K F. So finally, that proves exactly what we set out to prove that the degree of the extension is always greater than or equal to cardinality of gamma. So that is one part. Let us go back here. So the theorem, we have shown claim one of the theorem. Now, we will prove claim two in the next video.