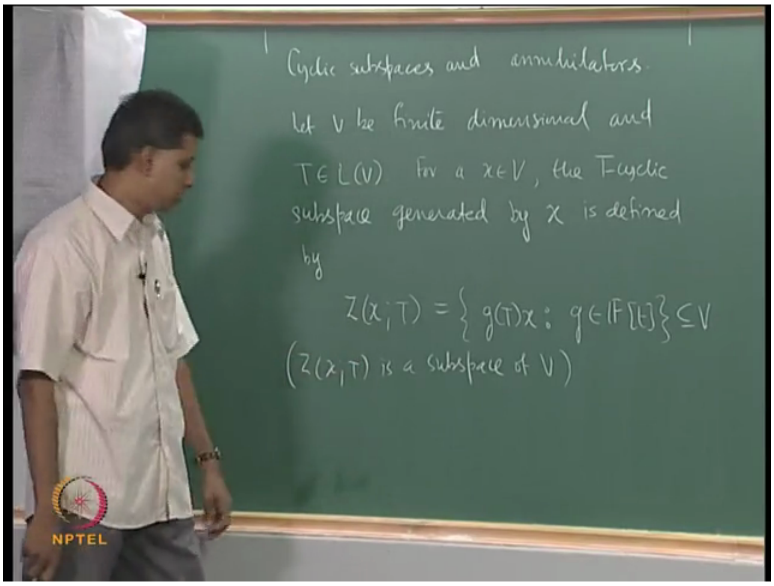
Linear Algebra
Professor K.C Sivakumar
Department of Mathematics
Indian Institute of Technology, Madras
Module 10 Primary and Cyclic Decomposition Theorems
Lecture 36
Cyclic Subspaces and Annihilators

(Refer Slide Time: 0:35)

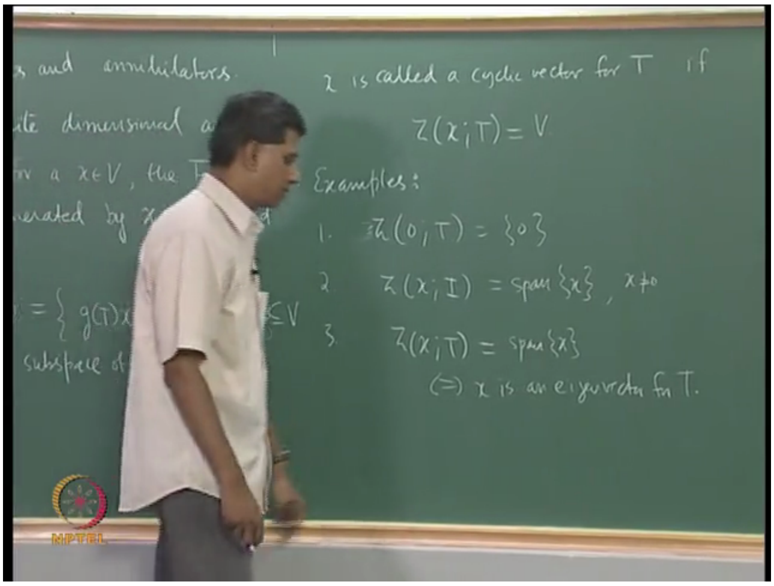


Okay, so cyclic decomposition theorem is the next important result I will first start with the notion of cyclic subspaces, cyclic subspaces and annihilators. Annihilators we have seen before cyclic subspaces let me define that first, okay. So what is the cyclic subspace? What is the cyclic vector? For defining a cyclic vector I will look at the following subspace. So V is finite dimensional and T is a linear operator on V for a fixed vector x in V, the T cyclic subspace generated by x.

So T is the operator that we start with for any fixed x I want to define this T cyclic subspace generated by x is defined by the notation is Z x; T Z x; T is the T cyclic subspace generated by x this is the set of all g capital T x such that g belongs to F F of t, okay observe how this is constructed take any polynomial arbitrary take any polynomial any degree look at g capital T T is fixed g capital T and then operate on x that will be some vector in the vector space V put that in this Z x, T do this for all polynomials do this for all such polynomials so this is obviously an infinite set and it is also obvious that this is a subspace, observe that this is a subspace of V this is contained in V to begin with it is a subspace of V this is a subspace I am just emphasizing I have already given the name T cyclic subspace but I want to emphasize that this is a subspace this is called the T cyclic subspace generated by x.

If this is a subspace of V there are times when this subspace is equal to W is equal to V that is special occasion happens for some vector x that will be called a cyclic vector.

(Refer Slide Time: 3:39)

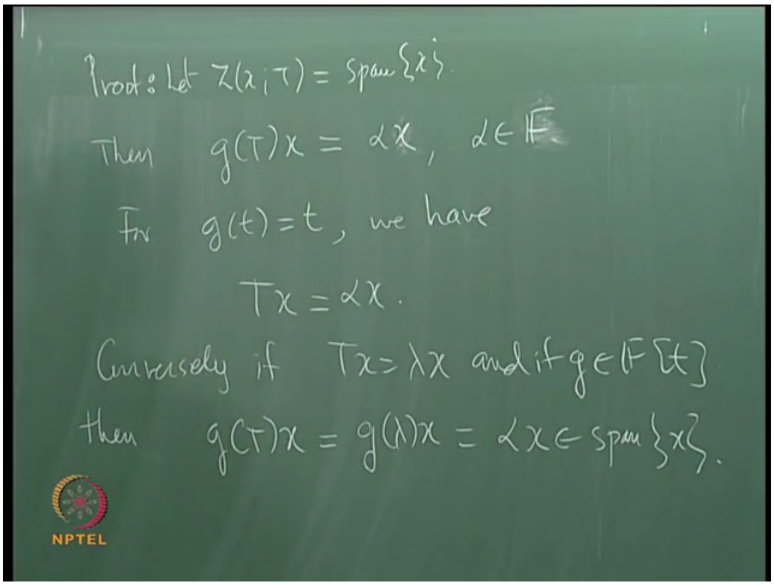


X is called a cyclic vector by the way the name why it is cyclic will be clear when we get a basis for this subspace. So right now we will just keep it as it is x is called a cyclic vector for T x is called a cyclic vector for T if this vector x satisfies the condition that this subspace is the whole of V x is a cyclic vector of a T if the subspace the whole of V, okay. To consolidate let us get some examples.

Take the case when x is 0, what is this cyclic subspace generated by 0? Take all polynomials then g T 0, if capital T is a polynomial, g of capital T is also, if capital T is linear g of capital T is also linear so this is just single term 0, okay what about any vector x identity operator? What is this subspace? It is not difficult to see that is span of x, it of course assume x not 0, x 0 has been taken care of, x 0 has been taken care of earlier so this is span of x.

A little more general in the third example Z is equal to span of x if and only if x is an eigenvector for T again x is assumed to be non-zero I will not emphasize in this this is more general, this subspace is generated by the vector x if and only if the vector x is an eigenvector for T, a quick proof of this.

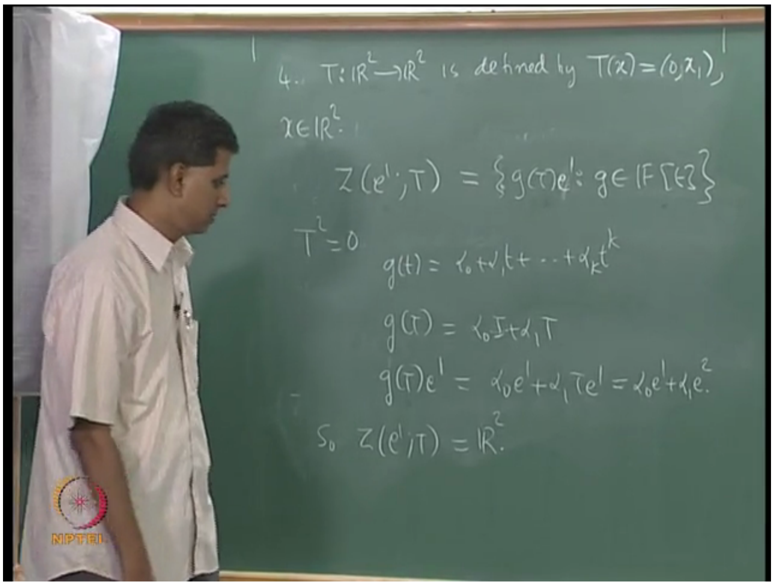
(Refer Slide Time: 6:14)



Suppose that this is equal to span of x then g T x this is the general term in this subspace this is a multiple of x for any polynomial in the field for any polynomial g g T of x is in Z x, T that is the definition, if it is a span of a single vector it is a multiple of that. I want to show from this that x is an eigenvector this is true for all polynomials g in particular g of t equals t. For g of t equals t we have Tx we have Tx equals alpha x, x is not 0 so this is an eigenvector, okay.

Conversely something that we have seen before okay let me go to this quickly it is easy still. Conversely if Tx equals lambda x and if g is any polynomial then what happens to g T x is what I want to see I want to show that this is a multiple of x so it will follow that any anything in Z is a multiple of x, g T x we know is what Tx equals lambda x so it is g lambda this is just g lambda x that is a number alpha times x alpha is g lambda so what we have shown g T x is a multiple of x so this belongs to span of x, okay so that is the third example generalizing the second this is for the subspace, for a cyclic vector is there an example?

(Refer Slide Time: 8:47)



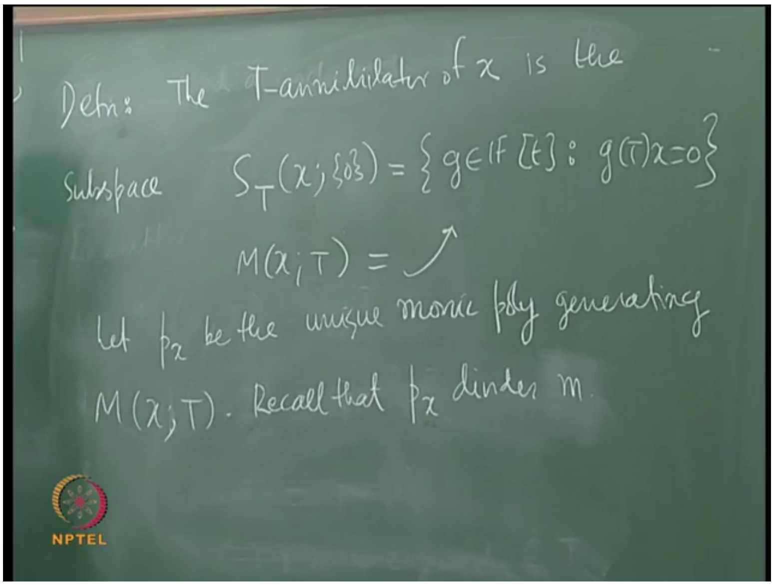
Let us define T on R 2 0, comma x 1 x is in R 2 first coordinate is 0, second coordinate is the first coordinate of x that is T, what is this subspace? e 1 is a first standard basis vector 10 I want to determine this subspace I want to show that this is equal to R 2, okay okay. Let us observe that this T has a property that T square equal to 0 nilpotent T square equal to 0, Z is what by definition this is the set of all g T x such that g is F in F t.

Take g to be any polynomial let us say g of t is alpha not plus alpha 1 t, etc alpha k to the t k, if you look at g T it will simply be alpha not identity plus alpha 1 T because T square T cube etc are 0 so g of T is this, I want to calculate g T x g T e 1 sorry this is g T e 1 please correct this this is g T e 1 I am looking at the cyclic subspace generated by e 1 in this example.

So g T e 1 is alpha not e 1 plus alpha 1 T e 1, I am applying this to e 1 but T e 1 is e 2 this is alpha not e 1 plus alpha 1 e 2, g T e 1 is alpha not e 1 plus alpha 1 e 2, g is arbitrary, can I get all vectors in R 2 from this combination that is g is essentially the first two alpha not and if I vary alpha not alpha g varies so is it clear that this then is this subspace generates all vectors in R 2.

So it is clear that cyclic subspace generated by e 1 is the whole of R 2, I leave it as an exercise for you to show that e 2 is not a cyclic vector because T e 2 is 0 T e 2 is 0 so you cannot so can you see already what cyclicity here means e 1 T e 1 that is what we have done here e 1 T e 1 in general e 1 T e 1 T e T square e 1 etc in general a vector x, Tx, T square x, etc that will be a basis for a cyclic subspace that is what we will proof next in fact, okay so I have given an example of a cyclic vector in R 2 for a particular linear transformation, okay.

(Refer Slide Time: 12:28)



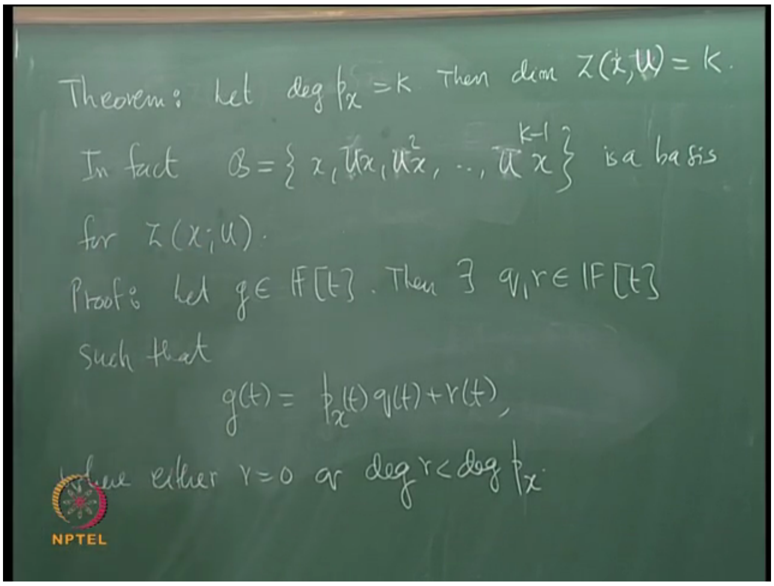
So I want to proof this theorem now which makes it clear why this is called a cyclic subspace but before that I need a definition. So let me give that definition this definition is something that we have seen before I want to recall this the T-annihilator of a vector x the T-annihilator of a vector x is it is the subspace I remember having used S T x; V no T-annihilator of x will just be S T of x. I define S T x W for a subspace W earlier I am looking at a particular case when W is single term 0 this was mentioned even that time this is the set of all polynomials now such that g T x is 0 set of all annihilating polynomials that annihilate x in particular (()) (14:10) not all annihilating polynomials ya all polynomials that annihilate T belong to this but it is it has more general polynomials.

In this in this situation this will be renamed as just M x; T just call it capital M x; T I have given this notation because we have seen this before I will call it M x; T so for me M x; T is this subspace of F t this is an ideal this is an ideal this is an ideal and principle ideal domain there is a unique monic polynomial which generates this ideal that monic polynomial will also be called the T-annihilator of x, okay.

Let p x be the unique monic polynomial generating M x; T, I started with a fixed x, I am fixing T p x will be for me monic generator of this ideal in F t we have seen this fact before that the minimal polynomial is a member of this and so p x divides the minimal polynomial. All this is to recall that m divides p x the minimal polynomial of capital T divides p x of T, I am sorry p x divides that the degree of p x could be smaller p x divides m belongs to small m belongs to capital M small m belongs to capital M, this could have a lesser degree than the minimal polynomial so p x divides m, okay.

Now these notions are related cyclic vector and this p x are related that is the next theorem let me state and proof this, okay so is it clear I will refer to the polynomial the unique monic polynomial that generates this ideal also as the T-annihilator of x the notation is p x. In general p x could have a lesser degree than the minimal polynomial of T, okay.

(Refer Slide Time: 17:08)



So now we are in a position to proof that this theorem. Let degree of p x be equal to k the framework is already there V is a finite dimensional vector space, T is a linear operator on V, p is the unique p is the T-annihilator of x. Let degree of p x equal to k than dimension of this cyclic subspace generated by x is also k these are related. In fact we have the following in fact if script B is x, comma Tx, T square x, etc T to the k minus 1 x this has k elements this is a basis for this is a basis for I am going to change the notation because I am I am actually looking at subspaces, okay.

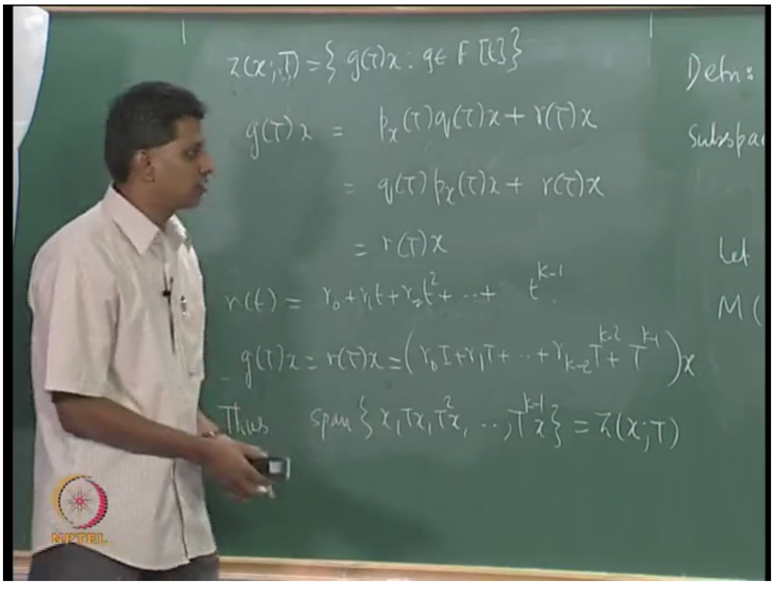
So degree of p x is k, dimension Z instead of T I will take an operator u that is equal to k than this will be x, ux, u square x, u to the k minus 1 x this is a basis for Z x; u, okay this is the theorem now it should be clear why this is called a cyclic subspace you have something like a single vector x all the other basis vectors can be obtained by action of u okay so it is a cyclic subspace, okay.

Proof of this so u is a linear operator, degree of p x is k. Let g be any polynomial let g be any polynomial see I want to show that this is a subspace of this I will study Z x; u closely and then show that this is a basis. Take g in F t then I have two polynomials one is g, the other one is p x I will apply the division algorithm F t is a principle ideal domain it is an euclidean domain so I can apply euclidean algorithm, what is euclidean algorithm? It is a generalization of this that if A and B are two integers positive integers then I can write A as B times C plus R where either R is 0 or R is less than B I started with A and B ya R is less than B.

Same thing happens for a euclidean domain for this euclidean domain F t I am going to look at g and p x, okay. I will say that there exist q and r which are polynomials q is the quotient, r is the remainder that is the suggestion such that such that this polynomial g of t can be written as the polynomial p x t the annihilating polynomial for x into q the quotient plus the remainder r where q and r satisfy where either r is equal to 0, or ya not q and r where r and p degree of r is less than degree of p between any two polynomials this can be done between any two polynomials let us say p and g this can be done.

If the degree of g is less than p, q can be taken to 0 and r is equal to g, if the degree of g is greater than p then you can actually divide p by I am sorry ya you can divide g by p there is a quotient under remainder the quotient is a polynomial q, remainder is this the remainders has this property that the degree is less, okay we are looking at Z x; u so I need to look at g t x really what happens to g t x?

(Refer Slide Time: 22:12)



So I am just writing Z x; u this is the collection of all g T x so now I am I have a formula for g. So look at g T x g T x is p x T q T x plus r T x where either r is 0 or degree of r is then degree of p these are polynomials in T so they commute so I can write this as q T p x T x plus r T x but p x T x must be 0 because T x is the unique p x is the annihilator of x p x to begin with must be a member of this subspace so this is 0, so this is just r T x, okay whatever be the degree of the polynomial g if you look at the action of g on T then the powers of T beyond k do not matter because r the degree of r is less than degree of p x, right.

Look at r of T the degree of r is less than degree of p, p x has degree k. So I have r as r not plus r 1 t etc I am just coming degree of r is less than degree of p x, p x has degree k so this will be r k minus 1 t to the k minus 1 ya what is your question?

Student is asking: p x T x is 2 to 0.

P x T comes from this I collect all the polynomials g that satisfy the property that g T x is 0 this subspace is an ideal that is generated by the unique monic polynomial p x in the first place p x is the member of this so p x capital T x is 0 p x capital T x is 0 it is an annihilating polynomial. I have gone back to T, I wanted u does not matter by force of habit I have gone back to T let us keep it as T, okay.

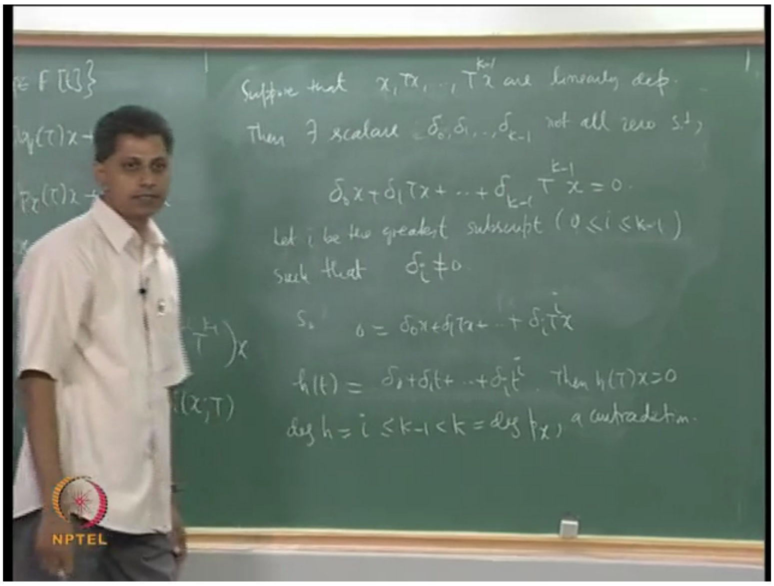
Is this clear? The degree of r is less than degree of p x so I can write this but it is a monic polynomial so this r k minus 1 is 1 so I can remove it, okay it is a unique monic polynomial the degree of the highest power of t the coefficient of highest power of t must be 1, okay that is my r so g T x is r T x which is r not I plus r 1 T plus etc plus r k minus 2 T k minus 2 plus r k minus 1 is 1 T k minus 1 this acts on x that is g T x. I have written the complete action of any polynomial in T on the vector x so I know Z I know Z x T I have written the action of any polynomial I started with g as any polynomial I have written the action of g T on any I have written the action of g for g being any polynomial on x that is what I have here for one thing, okay what is that I have written it here see I have written u and a T here so I need to stick to some notation we call it T go back to this.

So this g T x must belong to this this Z is a set of all such g T x so for one thing it must be clear that span of these vectors span of which vectors x T x etc T square x etc T to the k minus 1 x span of these vectors must be equal to the subspace there x; T this is a spanning set I want to show this is a basis in fact this is a spanning set I must show that they are linearly independent also, is it clear the calculations that we have done?

I have started with a general polynomial g, I want to look at Z x; T so I must know the action of g T x to know the action of g T x I have applied euclidean algorithm and I observe that this is the same as the action of a polynomial of degree k minus 1 whose the coefficient of the highest degree is 1. So I have written so this this type is clear that the span of these vectors is

Z x; T I must show that these are linearly independent if they are not you will get a contradiction.

(Refer Slide Time: 27:42)

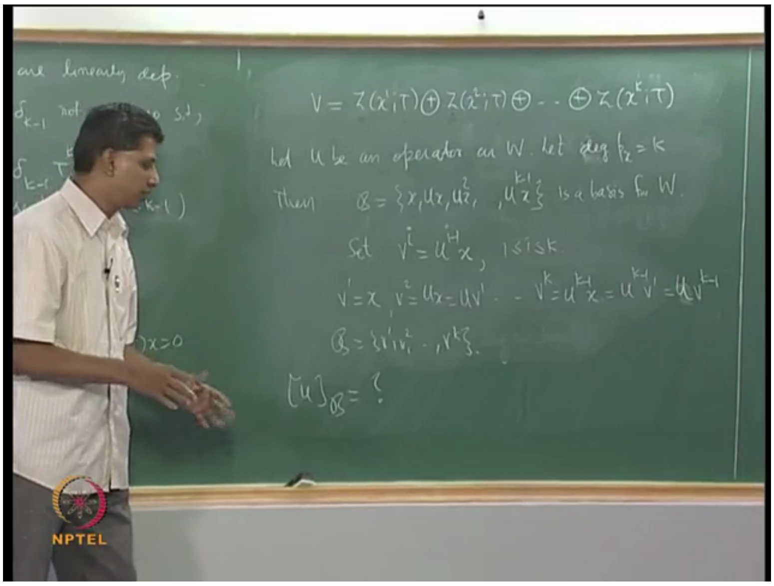


So suppose that they are linearly independent suppose that x, Tx, etc T to the k minus 1 x are dependent then their exist scalars their exist scalars let us call them delta not delta 1, etc delta k minus 1 not all 0 such that delta not x plus delta 1 Tx plus etc delta k minus 1 T k minus 1 x is 0 suppose these vectors are linearly dependent we will get a contradiction.

Let i be the greatest subscript 1 less than or equal to sorry 0 less than or equal to i less than or equal to k minus 1 let i be the greatest subscript such that delta i is not 0 there is at least one because at least one of them is not 0 they are linearly dependent this is the greatest all the terms from that term onwards will be 0, so I get 0 as delta not x plus delta 1 Tx etc plus delta i is not equal to 0 so delta i T to the i x that is 0 all the other terms are not there all the other terms will have the coefficient 0 this is the greatest subscript.

What we must do next is clear I define a polynomial h of t using these numbers delta not plus delta 1 t etc plus delta i t to the i this polynomial has the property that h of capital T x is 0. So this is a kind of polynomial argument we have seen before this polynomial has this property h t x is 0 because of this degree of h is i that cannot exceed k minus 1 which cannot exceed k a contradiction because p x is the annihilating polynomial the degree is k it cannot be less than k this is the contradiction and so these vectors are also linearly independent and so this subspace Z x; T is generated by these vectors x, Tx, etc T to the k minus 1 generated by this is a basis is what I want to say this is a basis for the cyclic subspace Z x; T, okay okay.

(Refer Slide Time: 31:24)



What we are going to do is to look at okay let me tell you the general scheme why are these cyclic subspaces important okay I will just write down this general scheme this is really the cyclic decomposition theorem which we will proof in the next couple of lectures. So the objective is to write V as a direct sum of cyclic vectors x 1 cyclic vector of this subspace cyclic vector of this subspace etc okay.

We have already seen a decomposition of this type for the subspace is W 1 etc W k where W i is the null space of p i t of r i p i t to the r i coming from the primary decomposition theorem, okay we have seen a direct sum decomposition of a finite dimensional vector space in this manner where the subspace is W 1 etc W k come from the primary decomposition theorem right away you have a connection between eigenvalues and those subspaces here the connection is not very clear but that will be made clear in due course where does eigenvalue come where does eigenvalue come in this, okay but this is what we want to proof this is cyclic decomposition theorem that is the reason why these subspaces are important that is why (())(32:36) cyclic subspaces of an operator T, okay.

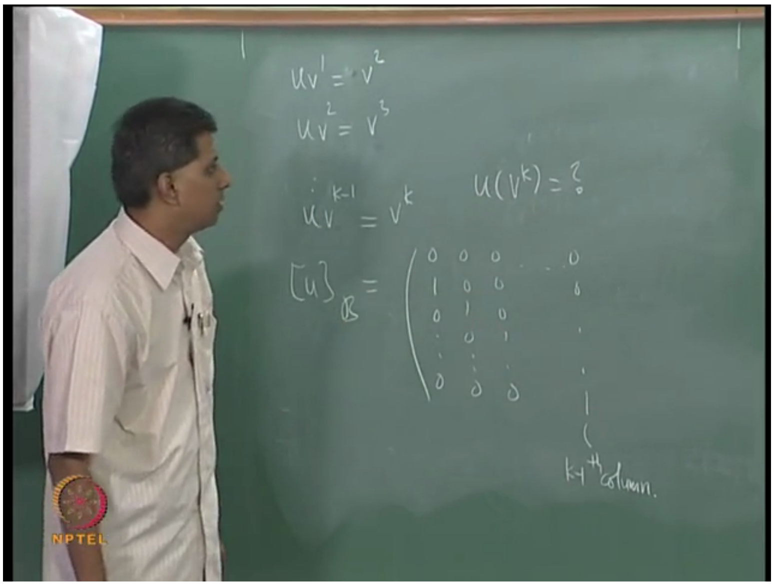
So we really need to look at the matrix of the operator T corresponding to this that will be a block the next block will be the matrix of the operator T corresponding to a basis of this etc I will write down the matrix of T relative to the cyclic basis that I have for this subspace then this subspace cyclic basis for this subspace, etc cyclic basis for this subspace I will collect those cyclic basis, take the union write down the matrix of T relative to this this will essentially be the Jordan form Jordan Canonical form, okay that is what we will proof that is the last result of this course.

So we need to actually look at the action of we need to look at the matrix of T relative to the basis cyclic basis that we constructed for this so we will look at each subspace look at the matrix of T corresponding to that particular cyclic basis, okay. Let us now look at the operator u not the operator T so let us say I have this framework let u be an operator on really a subspace W. Suppose the degree of p x is k then what we have shown just now is that the vectors x, u x, u square x, etc u to the k minus 1 x these vectors form a basis and this is a basis for W this is what we have seen just now I have only changed V to W, T to u. I want to write down the matrix relative to this basis what is that matrix what is the information that we have from that matrix.

To write down that we will need another notation let me define really renaming let me call V i as u to the i minus 1 x, for 1 less than or equal to i less than or equal to k I am calling this as V 1, V 2, etc V k V 1 for instance is just x the first vector i is 1, V 2 is u x that is u V 1, etc I can go upto the last but one look at okay V k is also u to the k minus 1 x which is u to the k minus 1 V 1 but you can proceed by induction V is V 2 is u V 1, V 3 is u V 2 really it will be u V 2 you can proceed to show that this is equal to u V k minus so capital U V k minus 1 this can be shown by induction ya so this have been relabelled as V 1, etc V k.

So I have V as V 1, V 2, etc V k I want the matrix of u relative to this basis that is the question. What is the matrix of u relative of this basis? So I must by definition how do I get this matrix? I look at the image of u V 1 I must write it as a linear combination of V 1, V 2, etc V k that will be the first column, u V 2 the linear combination of V 1, etc V k that is the second column etc.

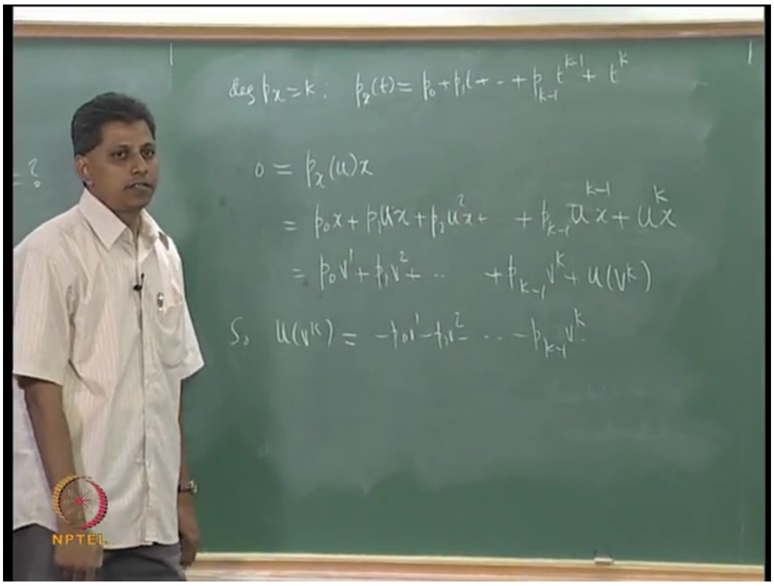
(Refer Slide Time: 37:17)

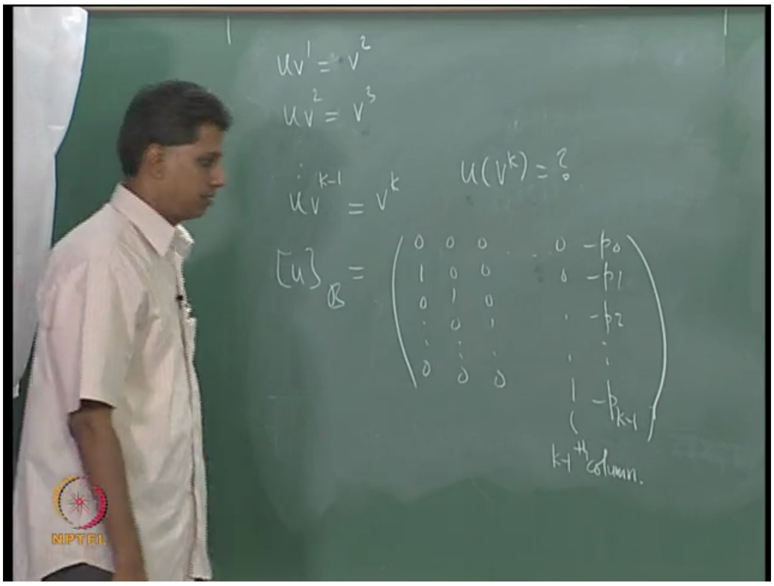


u V 1 u V 1 is V 2, okay then u V 2 is V 3, etc I can go upto u V k minus 1 u V k minus 1 I have written it that is V k which means I have the first k minus 1 columns of u V 2 there is no V 1 first term 0, second term 1 all others are 0 that is the first column, V 3 0 0 1 all others are 0, 0 0 0 1 all others are 0, the k minus 1th column will be 0 0 etc the last entry is 1 this is the k minus 1th column remember there are just k minus 1 equations here.

The last column will be filled if I know what is u V k? What is action of u on V k now that comes from the minimal that comes from the annihilating polynomial p x I need to fill up the last column. So I need to know what is u V k? What is u V k then I know I take u V k write it as a linear combination of V 1, etc V k then I know the last column, okay what is that? So I will come back to this and fill it up let us do the calculation, what is u V k?

(Refer Slide Time: 38:50)



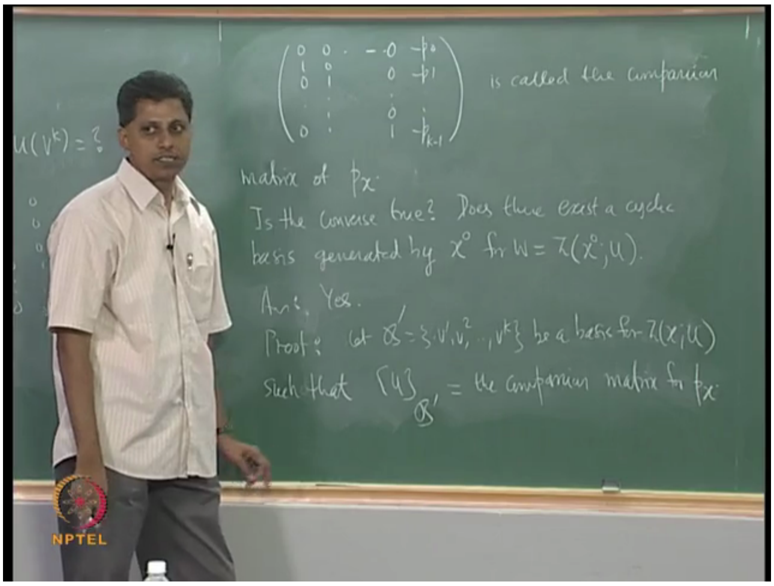


I know is that degree p x is k let me take p x to be of this form, okay shall I use p not p not plus p 1 t etc p k minus 1 t k minus 1 plus the coefficient here is 1 t k I have written the polynomial the annihilating polynomial p x like this using the fact that this is an annihilating polynomial I will be able to compute u V k, what I know is that 0 is p x u x which is p not x plus p 1 Tx sorry p 1 ux plus p 2 u square x plus etc plus p k minus 1 T to the k sorry u to the k minus 1 x plus u to the k x that is p x u x that is 0 this is the operator U capital U.

This is p not into x x is V 1 plus p 1 into u x u x is V 2 plus etc plus p k minus 1 U k minus 1 x U k minus 1 x is V k plus U k x U k x you can show is V k U k x equal to you can show it is U of V k U k x is U of V k which is what we need to determine so push this to the left hand side I get the unique representation for U of V k in terms of these vectors is minus p not V 1 minus p 1 V 2, etc minus p k minus 1 V k remember that p is a polynomial of degree k so there are k plus 1 terms here this side I have k terms p 0 upto p k minus 1 there are k coefficients those k coefficients fill up the last column, okay.

So I go back and write complete this matrix of U relative to this basis B. See this entry is 1 the last column entry minus p not minus p 1 minus p 2 etc minus p k minus 1 this is the k by k matrix this has a special structure the matrix of U relative to the cyclic basis the matrix of U relative to the cyclic basis has this form this matrix is called the companion matrix for the polynomial p x, okay.

(Refer Slide Time: 41:58)



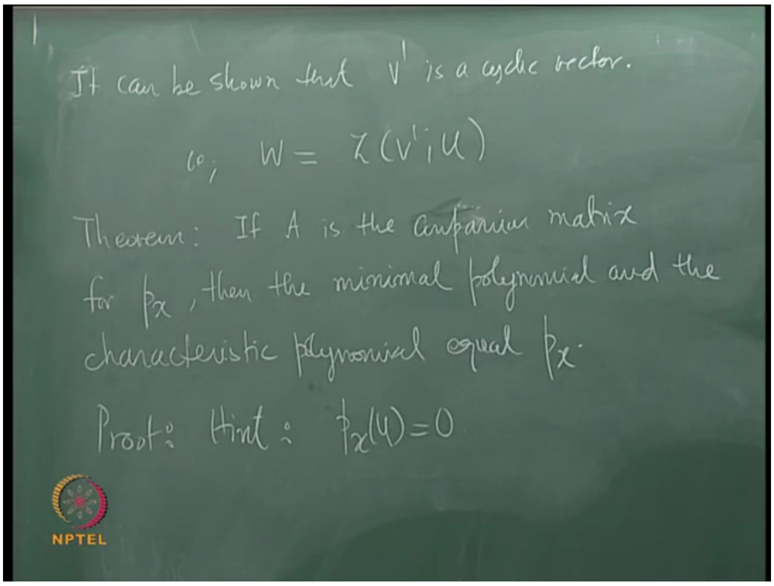
0 1 etc 0 0 1 etc 0 0 etc 0 1 minus p not minus p 1 etc minus p k minus 1 these are the coefficients that determine the polynomial p x, okay this is called the companion matrix the companion matrix of p x the matrix that accompanies this polynomial p x. What we have shown is that the matrix of the operator U relative to the cyclic basis is the companion matrix is the converse true? Is the converse true? What is the converse? What is the converse? The matrix of U relative to the cyclic basis is the companion matrix, can I get a basis which is a cyclic basis from this can I get a basis the question is this.

I know p x, I know the companion matrix, so what is the converse? Does there exist a basis a cyclic basis really cyclic basis by which I mean there is a vector x then the next is u x, u square x etc does there exist a cyclic basis for W such that can I say cyclic basis generated by x for W which is this subspace what I know is that the matrix of U relative to a basis is the companion matrix I have the operator U with respect to some basis the matrix of U is the companion matrix does it follow from this that there is a cyclic basis for U that is a converse, okay given the operator U there is a basis such that the basis has the property that the matrix of U relative to that basis is the companion matrix of the polynomial p x, can I find a vector x? So I should not probably call this x cyclic basis generated by some x not cyclic basis generated by some vector x not.

The answer is yes so the proof of this is as follows the answer is yes first let me write down the answer the answer is yes. The proof is really one line what is that one line proof let B be V 1, V 2, etc V k be a basis for this subspace such that should I call it B prime I will reserve this script B for the cyclic basis so B prime is this basis be a basis for this such that the matrix of U relative to B prime equals the companion matrix equals the companion matrix that goes with p x companion matrix for p x.

The question is can I get a basis which probably I could call it B can I get a basis B which is a cyclic basis for this subspace for this subspace Z x; U, how do I construct? I am not going to proof this I will simply tell u what u must do show that V 1 is a cyclic vector that is all so I am really leaving this as an exercise.

(Refer Slide Time: 47:24)



It can be shown that V 1 is a cyclic vector that is the subspace W is Z V 1; U so what I call is x not I am saying V 1 is a candidate for x not this is just one candidate in fact there are k candidates at least k candidates for this for this cyclic basis, okay. the final result I will again state not prove it, okay so remember what we have done is we have looked at a notion of a cyclic subspace generated by a vector, we looked at a basis for that and then we wrote down the matrix of U relative to that basis okay that is the companion matrix.

The final result is the following if A is if A is the companion matrix if A is the companion matrix for p x if A is the companion matrix for the annihilating the T-annihilator of x then the minimal polynomial and the characteristic polynomial both the minimal polynomial and the characteristic polynomial equal the polynomial p x both the minimal polynomial and the characteristic polynomial equal the polynomial p x.

The proof is really by verifying that this annihilating T-annihilator of x is an annihilating polynomial for for U or T. Proof the only hint is that show that p x u equals 0 show that p x equals 0 it then follows that it is a characteristic polynomial as well as a minimal polynomial, okay so let me stop here.