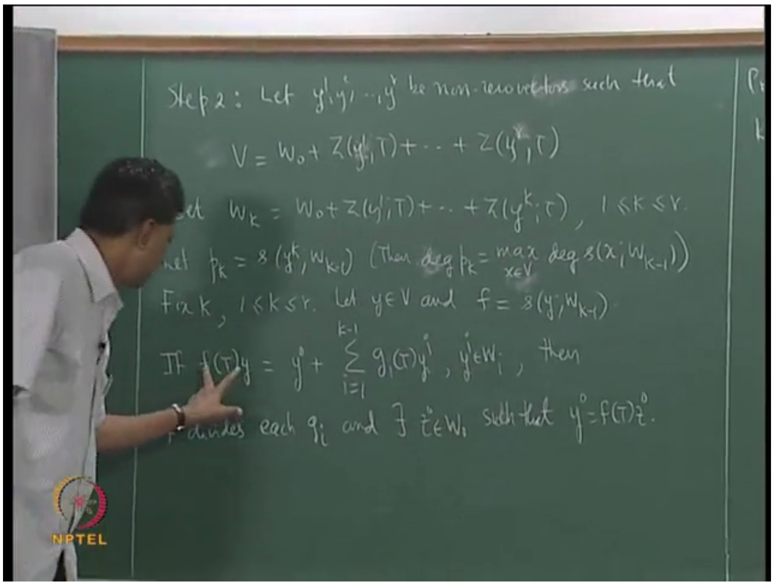
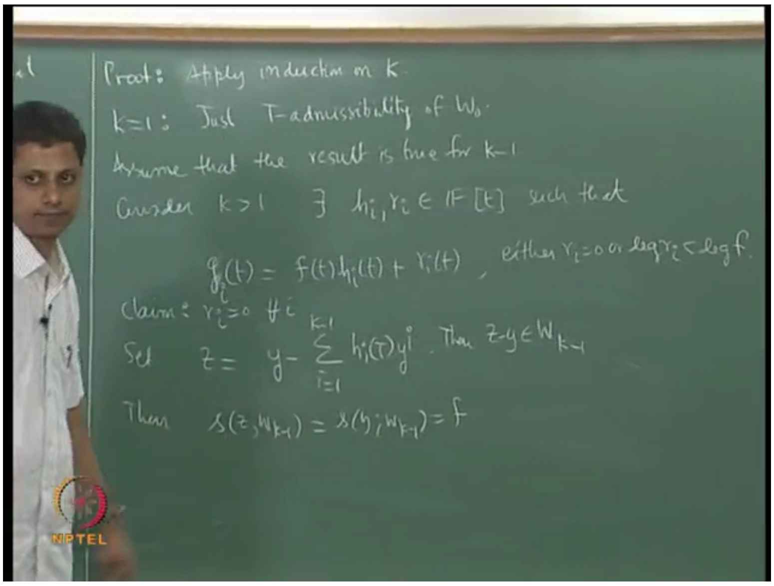
Linear Algebra
Professor K.C Sivakumar
Department of Mathematics
Indian Institute of Technology, Madras
Module 10 Primary and Cyclic Decomposition Theorems
Lecture 38
The Cyclic Decomposition Theorem 2. The Rational Form

(Refer Slide Time: 0:21)





Okay we are proving step 2, okay step 2 the statement I have written down once again, essentially what we have is this representation we have this representation for f T y, y has y is an arbitrary vector, f is this polynomial so f T y must belong to W k minus 1 I am looking at a general representation of f T y then when whenever I have a representation like this it always holds this is what we must show it always holds that this f divides each of this polynomials g 1, g 2, etc g k minus 1 and this y not has this property that it can be written as f T Z not for Z not in W not. I mentioned that this is T admissibility T admissibility of W not W not is a T admissible subspace of V, okay.

The proof is by induction on k and k equal to 1 is just T admissibility of W for k equal to 1 there are no terms here for k equal to 1 f T y is y not then y not it f T Z not okay that is that comes so for k equal to 1 I need to only verify this part because there are no polynomials here the polynomials g i's are not present. So k equal to 1 is just T admissibility of a subspace W not.

We will assume that the result is true for k minus 1 assume that the result is true for k minus 1, we will prove it for k we will prove it for k so consider k greater than 1. I look at these polynomials g and I look at the polynomials g i and f apply division algorithm, I will just say that there exist polynomials h i and r i such that such that I can write f as say f T is I am sorry I am looking at g g i of t is f of t h i of t plus r i of t for every i where r i's are polynomials that satisfy where either r i is equal to 0 or degree r i strictly less than degree f this is by the division algorithm.

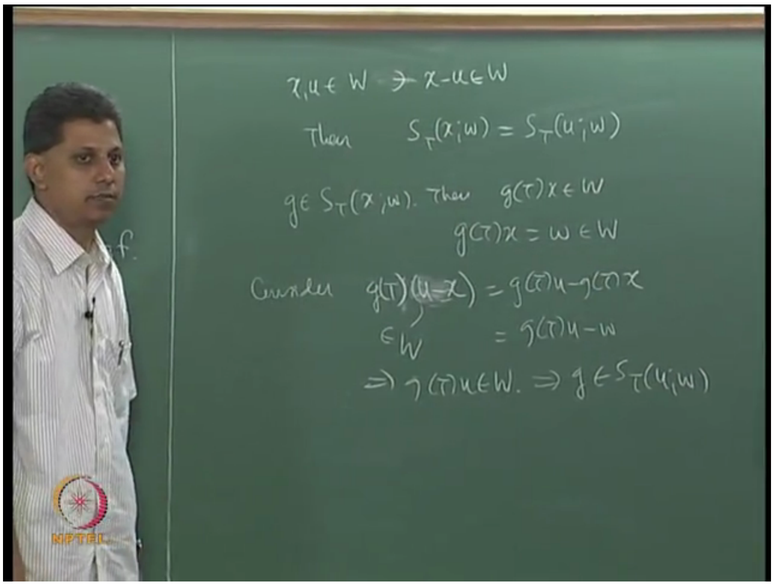
The claim is that r i equals 0 for all i claim is r i is remainder is 0 for all i, if let us say we have proved this claim it would then follow that f divides g i that is what we want to show the second part follows from admissibility, okay. You want to show that f divides g i so we will show that r i is 0, proof will be by contradiction. Suppose some r i is not 0 we will get a contradiction contradiction to the hypotheses that it is true whenever the index is k minus 1, okay.

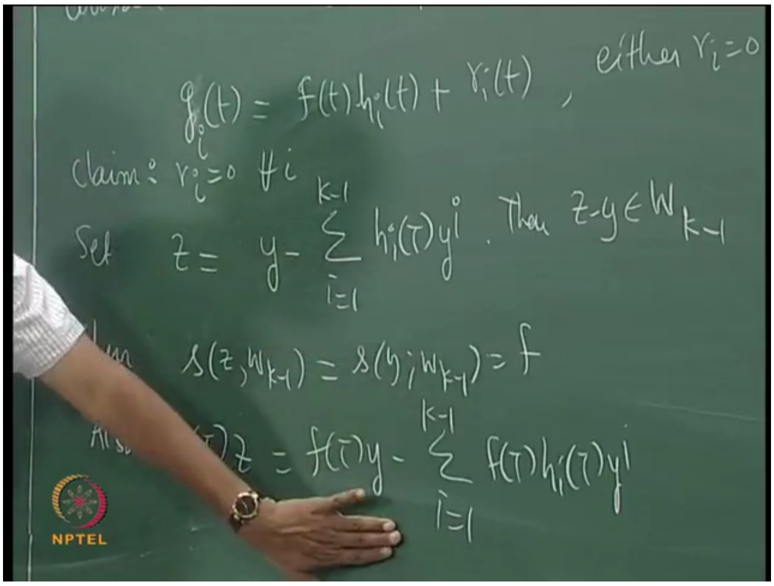
So we want to show r i is 0 for all i, let us now define remember that I have been given a vector y so I will use this vector y and define a vector Z as y minus summation i equals 1 o k minus 1 h i of T y i, I know the polynomials h 1, etc h k minus 1 coming from the previous term these polynomials are known I define a vector Z in this manner, okay W not is T admissible each W i is also T admissible each W i is T invariant each W i is T invariant, W k is this each of this cyclic subspaces is invariant under T, W not is invariant under T so at every step you are adding a subspace which is invariant under T so W k is invariant under T so this look at y i they are taken from i equal to 1 to k minus 1.

Can you see that this belongs to this whole thing belongs to (W j) W k minus 1 because W k has this property that W k minus 1, W k minus 2, etc they are all contained in W k it is a kind of a nested sequence of subspaces, okay W 1 contained in W 2 contained in W 3, etc. So each of each of these terms will belong to W k minus 1 the last one and so if you look at the difference Z minus y that belongs to W k minus 1 the difference Z minus y belongs to W k minus 1.

Now if this happens then we should quickly make this observation then look at s Z of W k minus 1 I am claiming that it is a same as s y W k minus 1 s y W k minus 1 I have already denoted that by f so all I need to do is to show that these two polynomials are the same. In other words I want to show that if x y belongs to a subspace W then little s y; comma W is equal to little s x; comma W this is what I want to show. The difference Z minus y belongs to the subspace W k minus 1 but that comes from the definition, okay the fact that these two are the same comes from the definition of the of those sets S T.

(Refer Slide Time: 6:40)



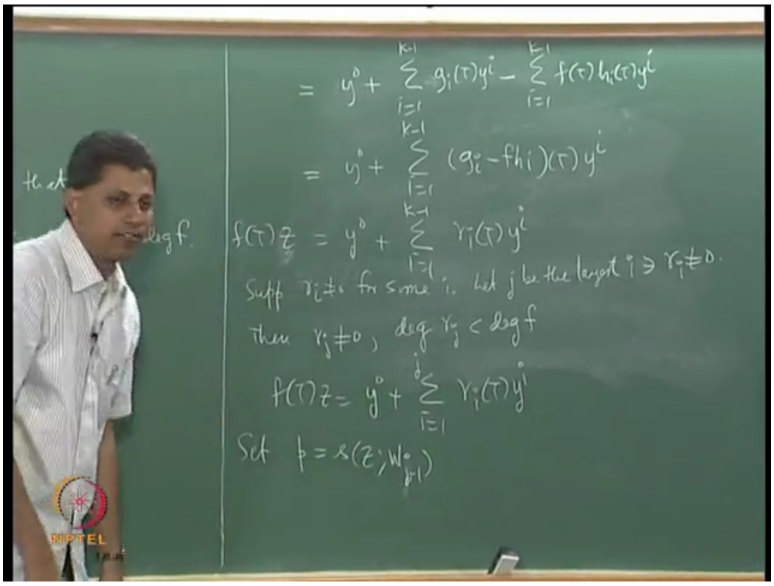


So maybe I will just quickly highlight that let us say I have x, comma u in a subspace W such that x minus u belongs to W then I want to show that this s T x; W I want to show that this is in fact the same as S T u; comma W okay if these two subspace are the same then their generators will also be the same these are the generators, okay. Let us S T x; W let us say that g belongs to S T x; W then by definition g T x belongs to W that is g T x equals W. Now look at look at g T of (y) u g T u can be written as okay I consider g T x minus u u minus x consider g T u minus x this is g T u minus g T x what I know is that this belongs to W this belongs to W, okay because u minus x belongs to W so this belongs to W.

So this is g T u minus g T x g T u minus W that belongs to W g T u minus W that belongs to W, W is in W capital W is a subspace so g T u is also in W the whole process can be reversed. So what I have shown is that okay this means g belongs to S T u; W this is really straight forward and I am just explaining it quickly g belongs to S T x; W implies g belongs to S T u; W the whole process can be reversed, okay.

So please check the details and then verify that since those ideals are the same the monic generators will also be the same so I get this the notation for this polynomial is f that is what we have here we have assumed this is the notation so I have this also look at f T Z f T Z is f T y minus summation i equals 1 to k minus 1 f T h i of T y i, I have applied f T to this vector f T Z is f T y minus summation f T h i T y i that is this this is f T y there is an expression from the theorem or from this representation f T y there is a expression.

(Refer Slide Time: 9:40)

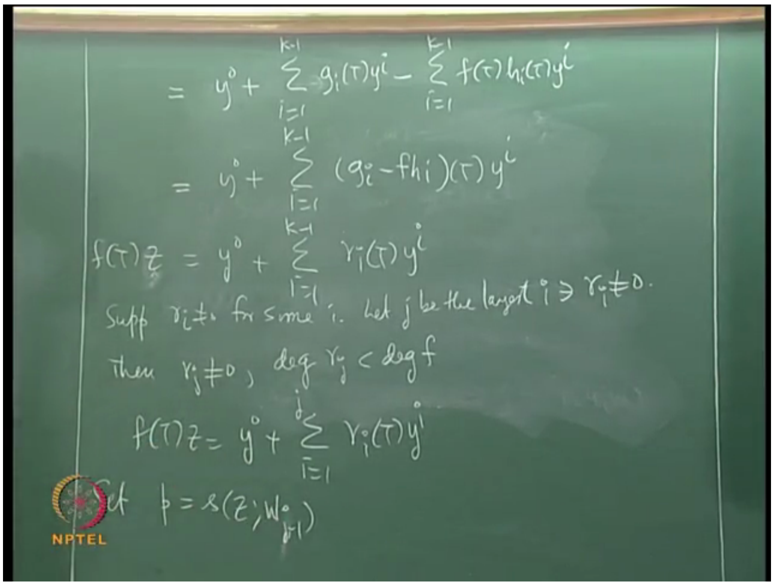


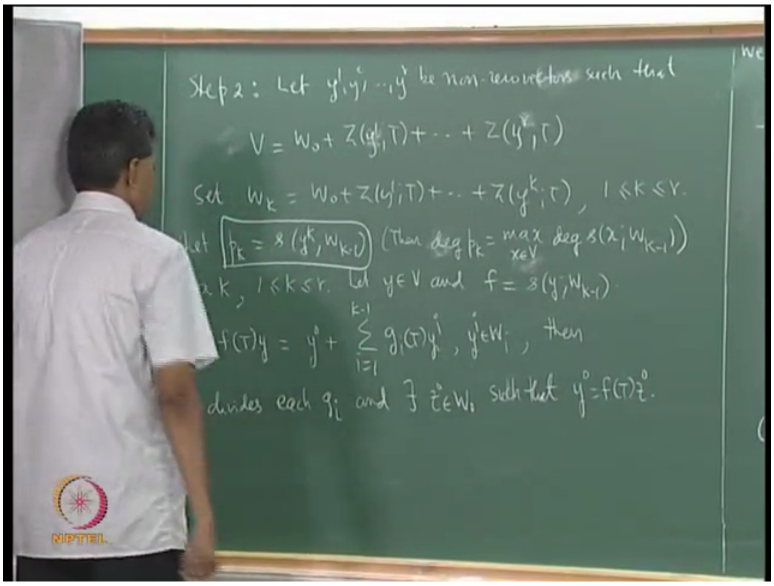
So I write this as y not plus summation i equals 1 to k minus 1 g i of T y i minus summation i equals 1 to k minus 1 f T h i of T y i this is y not plus summation i equals 1 to k minus 1 g i minus f h i y i g i minus f h i g i minus f h i is r i so this expression is so let me write I am looking at f T f T Z expression for f T Z is y not plus summation i equals 1 to k minus 1 r i of T y i r i is the remainder, okay.

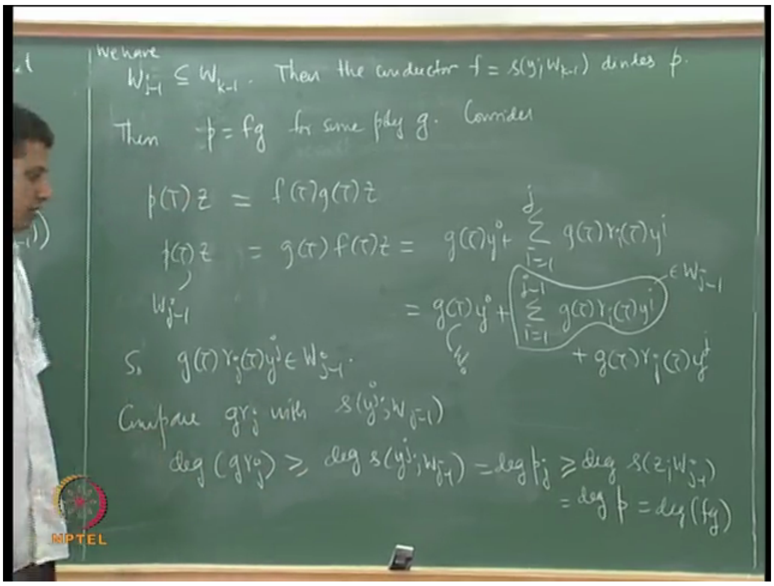
I want to show that each r i is 0 suppose some r i is not 0 suppose r i is not 0 for some i among all those non-zero r i's I will take the one with a largest subscript. Let j be the largest i such that r i is not 0 let j be the largest subscript such that r i is not 0 then r j is 0 sorry r j is not 0 and I also know coming from the condition for each r i the degree r j is strictly less than the degree of the polynomial f and I go back to this representation for f T Z rewrite it by making use of this j.

I can write f T Z as y not plus summation i equal 1 to j this time only upto j that is a largest after those the other r i's are 0 so the summation is only upto j, i equal to 1 to j r i of T y i let me now use a short notation for this polynomial Z W j minus 1 I have defined Z here I look at all those polynomials say some g g T Z such that g T Z belongs to W j minus 1 that is generated by is unique polynomial little s I am calling that as p, p is the monic generator of that ideal the set of all polynomials g such that g T Z belongs to W j minus 1, okay.

(Refer Slide Time: 12:53)







With this notation observe before that W j minus 1 is contained in W k minus 1 see j is this fixed index such that j is the largest index such that r i is not 0. So W j minus 1 contained in W k minus 1 from this can you see that this is always true from this can we see that tell me if this is correct f is already defined as s y; W k minus 1 then this conductor divides p, p is the polynomial that I defined just now, W j minus 1 contained in W k minus 1 which only means that if you take a polynomial g if you take a polynomial g if it has the property that g T if it has the property that g T Z belongs to W j minus 1 it will be such that g T Z belongs to W k minus 1, okay any polynomial that is present in W any polynomial that is present any polynomial g which has the property that g T of Z that belongs to W j minus 1 will also be present in this, okay from this it follows that this conductor divides p.

The degree of the polynomial coming from this will divide the degree of polynomial coming from this the polynomial the degree of this will be less than the degree of this the degree of the conductor corresponding to this will be less than the degree of the conductor corresponding to this in fact the polynomial f will divide p, okay this can be verified quickly once you have this you have the following.

If f divides p then I can write f divides p then I can write p as f times g for some polynomial g. I look at p T Z p T Z by definition is f T g T Z this is g T f T Z these two commute and g T f T Z I will write it is g T y not plus summation i equals 1 to j g T r i of T y i see I am using the expression for f T Z here these two polynomials commute so it is g of f of Z so I have p T Z to be this.

Now what is p? p is p is defined here p is defined here p of capital T of Z must be in W j minus 1 that is the definition p of capital T Z that must belongs to W j minus 1 so this polynomial let me write once again this this vector belongs to W j minus 1, okay look at what we have on the right on the right I will rewrite it as g T y not plus summation i equals 1 to j minus 1 and then j, g T r i of T y i plus g T r j of T y j that is the last term, I am just splitting this term upto j minus 1 and then the last term we have observed that left hand side this vector belongs to W j minus 1.

Look at this vector that belongs to W j minus 1 because this is a sum that happening the first term comes from y 1 the first term has y 1, second term has y 2, etc we have just now observed that all these are contained in the last one that is W j minus 1. So this belongs to W j minus 1, this belongs to W not but W not is also contained in W j minus 1, W not is contained in each W k so these two terms belongs to W j minus 1, this belongs to W j minus 1, so this must also belong to W j minus 1 that is g of T r j of T y j this must belong to W j minus 1. Which means I will now compare I will now compare the polynomial I will now compare the polynomial g r j with with s y j W j minus 1, I compare this polynomial g r j with this polynomial this is a unique monic generator of that ideal of all polynomials let us say some L L of T L of capital T y j belongs to W j minus 1 this is another polynomial that is a one with a least degree.

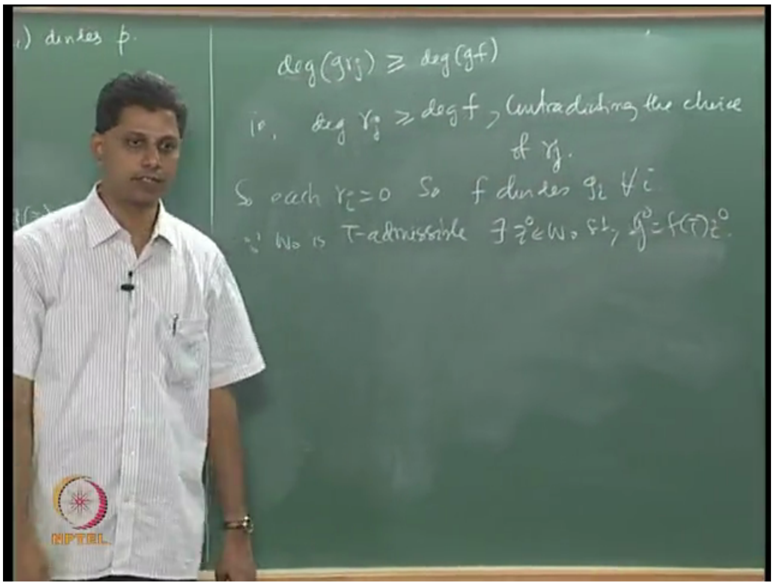
So degree g r j for one thing must be greater than or equal to degree s y j W j minus 1, agreed? g r j is a polynomial that belongs to that ideal g r j is a polynomial that belongs to the ideal of all polynomials L of T such that L of capital T y j belongs to W j minus 1 but that that ideal has this little s as the generator so that is the polynomial with the least degree with that property.

So I have this now s y j W j minus 1 come back to this that is p j so this is the same as degree p j the polynomials are the same for each j p j is y j s y j W j minus 1 but p j has this maximum property that among all the polynomials among all the polynomials tell me if you agree with this among all those see p j has the property that among all those polynomials let us say again L with a property that L T Z belongs to W j minus 1 p j is the one with the maximum degree.

So this is one such polynomial see this means little s of capital T of Z belongs to W j minus 1 but p j is the one with the maximum degree among all those polynomials. So I have this but this is equal to degree p by our notation p is s Z W j minus 1 this is the most crucial step in this proof, step 2 is the most crucial most crucial is these inequalities degree p we are at the last step the sequence of inequalities.

But what is p? p is fg so this is degree fg let me just write down the final inequality that we want ya by the way you cannot do not assume that you can understand the proof of the theorem right here in the class and then it is done with you have to you have to work with many of these steps here some of the steps I am not giving details, some of the steps I am giving details here but you cannot be able to understand here, okay but you got to go back home work it out and then verify that these are all correct statements.

(Refer Slide Time: 21:36)



Finally as I said I want only this inequality degree g r j is greater than or equal to degree fg that is degree gf product of polynomials this means degree of g sorry g I will cancel degree r j is greater than or equal to degree f a contradiction because the remainders have been chosen in such a way that the degrees must be less than degree f, I have that here but remember that this contradicts contradicting the choice of r i in particular r j degree of r j cannot exceed the degree of f contradiction is because of the fact that we have assumed r i is not 0, okay so each r i must be 0, okay.

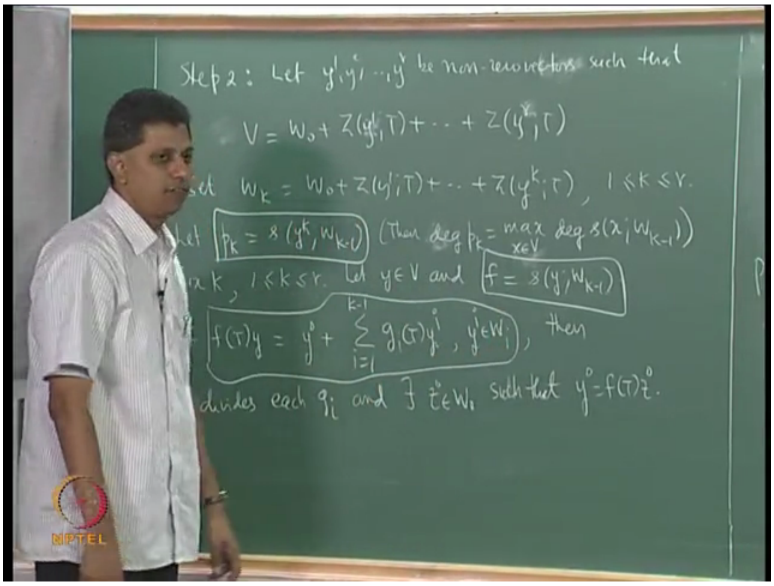
So each r i is 0 that is f divides g i for all i we have taken k polynomials this time we have taken k polynomials this time it will also ponder over where we have used induction hypotheses I have not mentioned this could not have come without the induction hypotheses that the result is true for k minus 1 upto k minus 1 we are proving it for k, okay ponder over that but I am saying that the second step is over here f divides g i this is what we wanted to show we want to show that f divides each g i and there exists Z not's with this property but then as I told you this y not is a vector that comes from W not, W not is T admissible so that part is easy, okay.

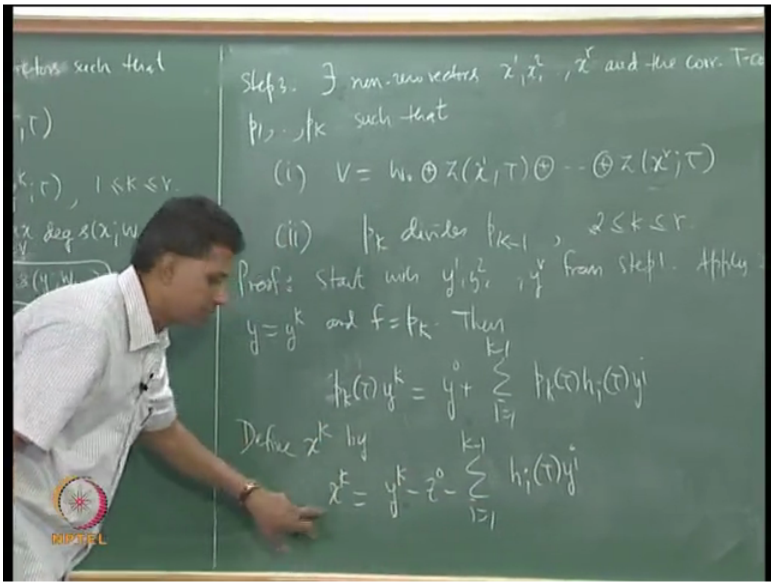
Since W not is T admissible there exist Z not in W not such that (f T) sorry y not is f T Z so second part is there (())(23:58) that is the proof of step 2.

Let me write down step 3, I will write step 3 here and prove it quickly, okay what what is left really what is left in the cyclic decomposition theorem the cyclic decomposition theorem you have got to show that V is a direct sum of these subspaces and that the T annihilators of x k that is those p k's have the property that p k divides p k minus 1 for k equal to 2 to r. So what is left is the sum is direct sum we have already got the sum step 2 gives me the sum I want to show this is a direct sum it is not enough with these y 1, etc y r I will define new vectors which will give rise to a direct sum.

So I need to prove really independence of these subspaces I need to prove independence of these subspaces and then the fact that p k divides p k minus 1 then the proof is over except the last part where there is some uniqueness uniqueness I will not proof, okay.

(Refer Slide Time: 25:05)





What is step 3? There exists non-zero vectors this time x 1, x 2, etc x r and the corresponding T-annihilators we call them p 1, p 2, etc p k such that V is the direct sum W not direct sum Z this time x 1 not y 1 y 2 etc p k divides p k minus 1 this is what I need to prove that step 3. So I will just look at the construction how look at how to construct these vectors x 1, etc.

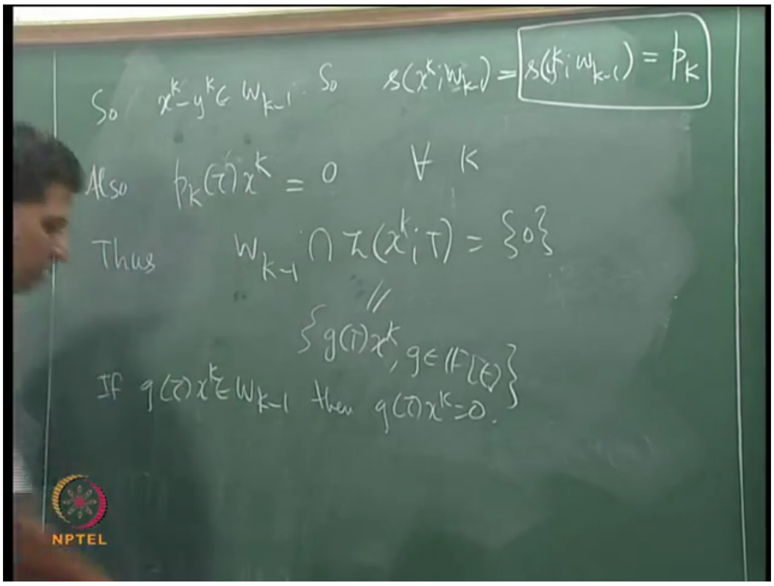
Proof of step 3 start with vectors y 1, y 2, etc y r these are coming from step 1 step 1 gives me these vectors. Apply step 2 apply step 2 to this vector y equal to y k and so f is p k, okay that is the reason why I have retained step 2 here. Step 2 I told you essentially is some inference about this representation if I have this representation then each of these polynomials g i must be divisible by f and this y not has a property.

Now I am going to apply this representation for y equals y k, y equals y k you go back to this y is equal to y k then this s y; k W k minus 1 is p k that is a notation I used earlier this is the notation I used earlier ya that is here in front of me in fact if y is equal to y k then s y k W k minus 1 is p k so all that I will do is apply this with y equals y k and f equal to p k so I have the following.

In other words I am just rewriting this representation I am just rewriting this representation for y equals y k f equals p k. So f T f is p k so p k of T y k that is what I have on the left y not plus summation i equals 1 to k minus 1 g i T y i, okay this g i also I should change I remember that g is g i's are divisible by f so I will rewrite this g i is just f h i this is f h i but f is p k so p k T h i of T y i this is g i this whole thing is g i of T g i is divisible by f that is g i is divisible by p k and we have written down g i as f h i f is p k so I have this.

Let me now define vectors x k I will do that here itself define x k by x k equals y k minus Z not minus summation i equals 1 to k minus 1 h i of T y i this step is rather similar to step 2 I am defining a new vector x k, I define the vector Z there y k minus Z not minus this I will again look at I defined Z as y minus something look at x k minus y k x k minus y k is Z not plus this. Now this vector belongs to W k minus 1, this is in W not, it is also in W k minus 1.

(Refer Slide Time: 29:55)



So x k minus y k belongs to W k minus 1 and the argument as before if I have two vectors x and u such that x minus u belongs to W then those monic generators will be the same that is look at little s x k; (y) sorry W k minus 1 that will be the same as little s y k W k minus 1 but this is what I am calling as p k s y k W k minus 1 is p k, what happens to p k x k also p k T x k without writing the details let us see this quickly p k T x k is p k T y k minus p k T Z not minus p k h i minus p k h i plus p k h i will get cancel, p k T Z not is y not so p k T x k is 0, p k T x k is 0 please check this.

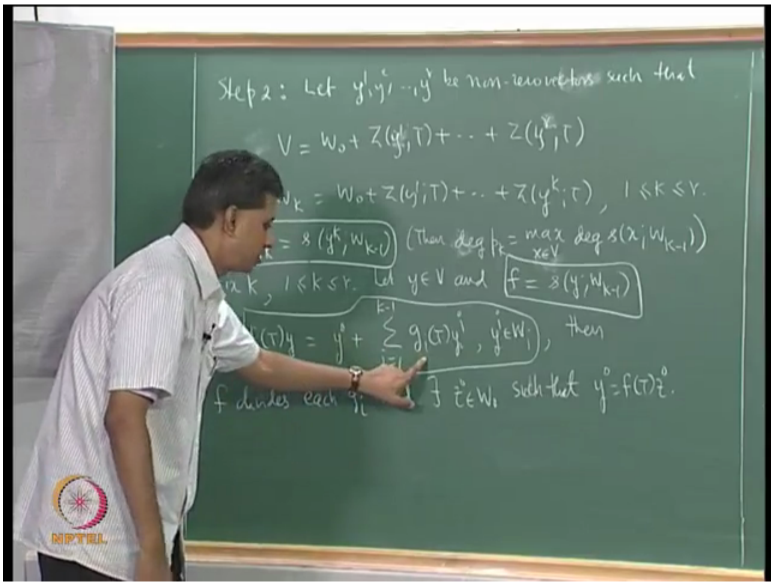
So x k the new vectors that we have defined have this property this is true for all k this is true for all k now can you see that this means W k minus 1 intersection Z x k T must be single term 0 this is the crucial step for independence that is see at each step look at the first step W not we start with W not then we are adding Z x 1 T, I want independence so I would like to know if W not intersection Z x 1 T is single term 0.

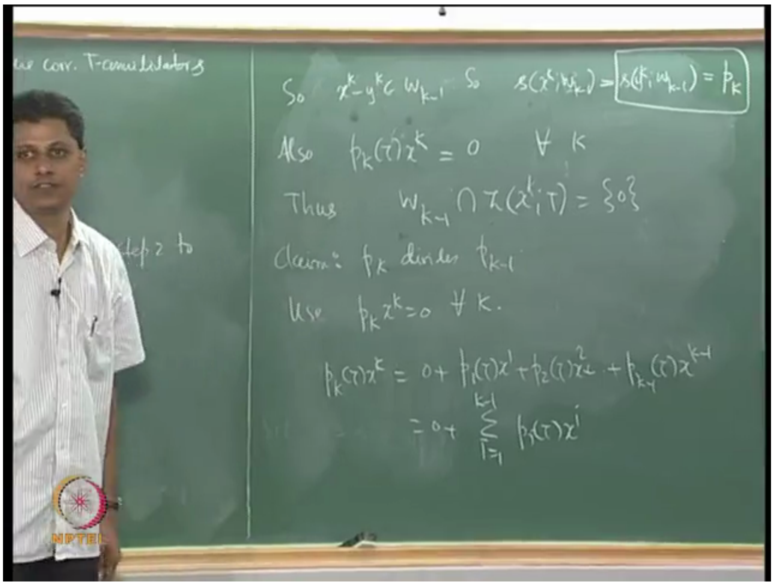
In a general step I have W k, W k is W k minus 1 plus Z x k T, I would like to know whether this Z x k T that I am adding is independent with all with the subspace W k minus 1 this this so this question is important, is the subspace Z x k T independent with W k minus 1? I am claiming that the vectors x k defined here in this manner have that property. Now why is this true? This is because see you got to go back and use this condition p k T x k is 0 means that this is single term 0, how let us do this quickly.

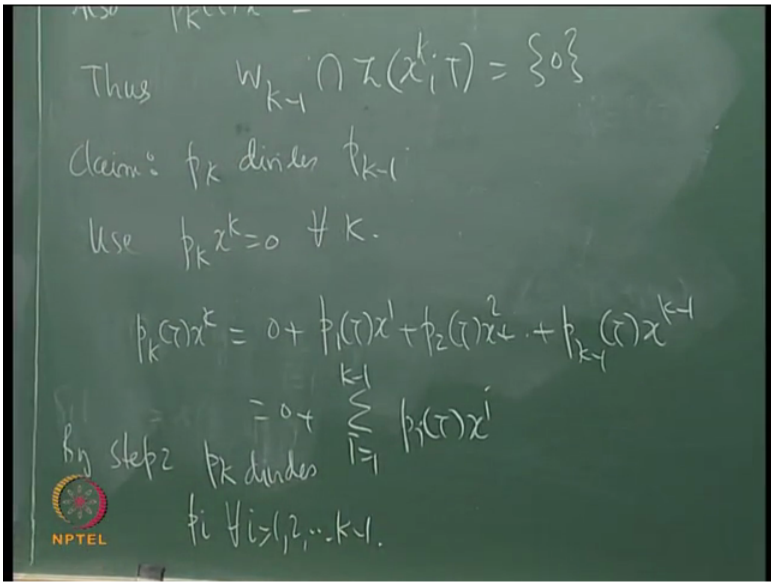
What is Z x k T? Z x k T is the set of all g T x k just the set of all g T x k such that g belongs to f T this is Z x k T, okay. What is what is p k? p k is is this in particular p k is this s x k W k minus 1 so this is the one with a least degree which means this g is a multiple of p k, is that clear? I collect all those polynomials the that satisfy the property that g T x k belongs to I have taken this from this I want to see whether I want to see what happens when g T x k belongs to W k minus 1.

If g T x k belongs to W k minus 1 then I have the following this g T must be a multiple of p k because p k is a unique monic generator anything is a multiple so this g T is a multiple of p k but p k T x k is 0 so g T x k must be 0. So if g T x k is belongs to this then g T x k is 0 please verify this not not immediately if this belongs to W k minus 1 then this must be a g must be a multiple of p k but if it is a multiple of p k then because p k T x k is 0 it follows that g T x k is also 0 and so this is independent.

(Refer Slide Time: 34:36)







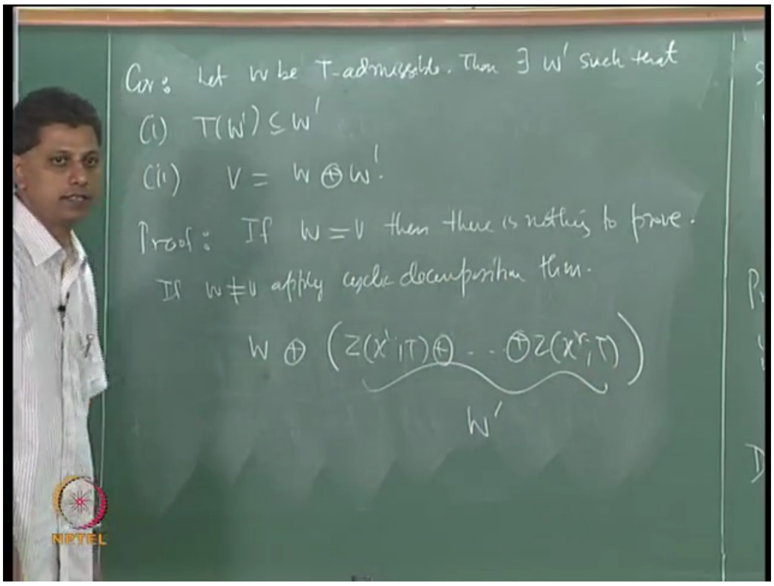
So let me remove this portion this guarantees independence this condition guarantees independence that is the first part, okay that is the first part which means what instead of y 1, etc y k I will use x 1, etc x k I get a direct sum decomposition. The last part is p k divides p k minus 1 that is the last part p k divides p k minus 1, how does this follow? What we have proved just now is that use the fact that p k x k is 0 for all k p k T x k is 0 for all k.

Now I will go back to this representation in particular I will go to this (())(35:31) I will remain here I will go back to this representation and then remember that whenever I write f T y in this manner then f must divide each of these terms instead of f I have p k instead of f I have p k that is what I have here.

So I also observe p k x k is 0 so I have p k T x k equals 0 plus p 1 T x 1 plus p 2 T x 2 plus etc plus p k minus 1 T x k minus 1 all that I have done is to write 0 as a sum of zeros. I can write this as 0 plus if you want summation i equal to 1 to k minus 1 p i of T x i just to get this similar to that representation, okay what is that that we have done? We have done p k T x k I know that belongs to W k minus 1 and this is the representation whenever I have this representation I know from step 2 that this p k must divide each of these polynomials and through step 2 consequence.

So I will just write by step 2 p k divides p i for all i running from 1 to k minus 1 the complete proof of the cyclic decomposition theorem of course the last part I have not done the part that these the positive integer r and the polynomials uniquely determine the positive integer r and the vectors non-zero vectors satisfying the conditions of the theorem uniquely determine the annihilating polynomials p 1, etc p k that I am going to skip.

(Refer Slide Time: 37:43)



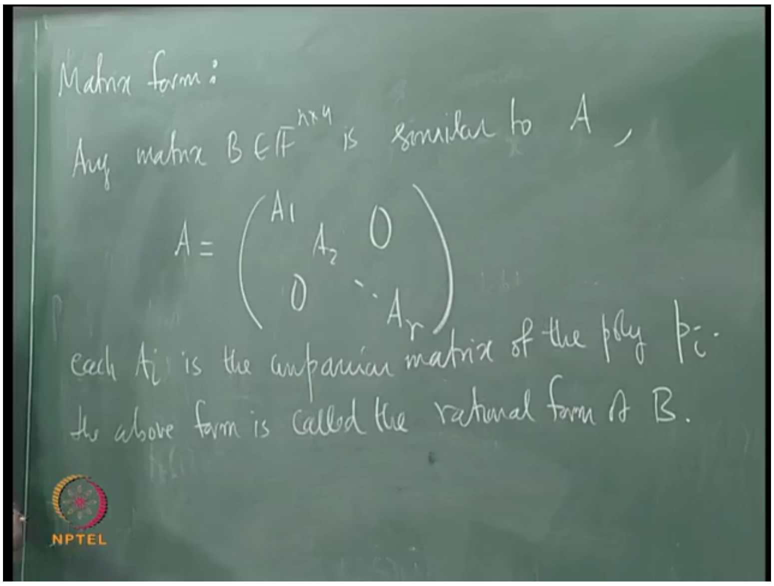
Let me look at some quick consequences of the cyclic decomposition theorem one of the results that I have been mentioning let me emphasize it once again. Suppose I have the okay let me give you this corollary first before stating this result. Remember we started with this question given subspace W which is invariant under T can I find a complementary subspace W prime which is also invariant under T the answer is the following.

Let W be invariant I want T admissibility let W be T-admissible then there exist W prime such that T of W prime is contained in W prime and the vector space V is the direct sum of these two subspaces. So if you take a general subspace just an invariant subspace in general it will not work I have given an example yesterday if you take a T admissible subspace then it works proof cyclic decomposition theorem.

Is a corollary of that start with W not whole single term is 0, W is T admissible okay can I say this if W is the whole of V then there is nothing to prove. If W is not V apply cyclic decomposition theorem I will not give the details here apply cyclic decomposition theorem that you each time you add a cyclic subspace remember that each cyclic subspace is invariant under T.

So all you are trying to do is looking at W direct sum the other ones Z x 1; T etc Z x (k) T x r T. Let us call this as W prime then I know that this W prime is the invariant subspace and V is the direct sum, okay. So answer for this question is if it is not just invariant but also T admissible then we get an invariant subspace, W prime may not be T admissible we do not know that but W prime is invariant under T this is one consequence.

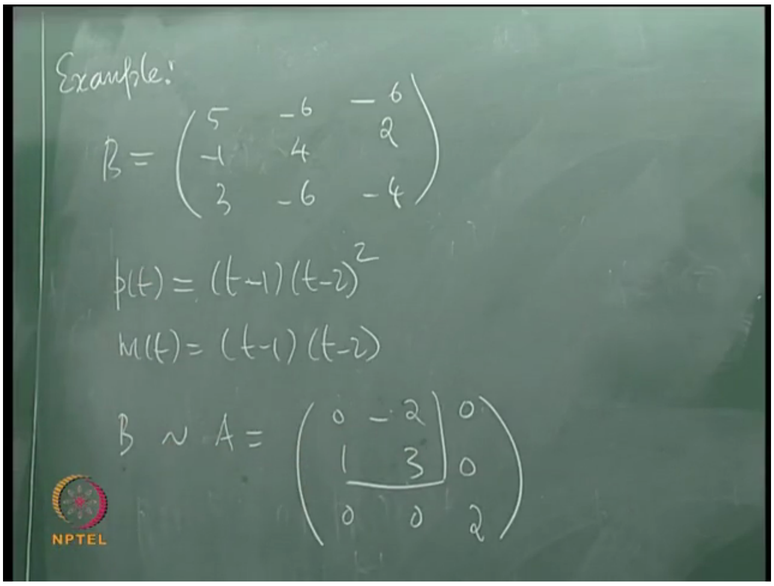
(Refer Slide Time: 40:32)



What is the matrix form? Matrix analog of the cyclic decomposition theorem is that any matrix B is similar to A, where the A is block A 1, A 2, etc A r all other entry is 0 where each A i is the companion matrix of the polynomial p i, how does the proof go? We know that the restriction operator of the operator T to a subspace W when I write down the matrix of the restriction operator with respect to the cyclic basis W is a cyclic subspace that is W equals Z x 1, T when I write down the matrix of the operator T relative to this cyclic subspace I know that the matrix is the companion matrix of the annihilating polynomial T annihilator of x T, annihilator of x 1, x i T annihilator of x i this is a basis collect all such basis put them in this block form then this is the matrix of the operator T, okay so this is the matrix form matrix analog of the cyclic decomposition theorem this is called the rational form.

The above form is called the rational form of B that is for you start with any matrix B then it can be reduced to the rational form the construction is by means of cyclic subspaces. See there is also a Jordan form but I do not have the time for that so all that I will do is I will give an example a numerical example of the rational form of a matrix, okay.

(Refer Slide Time: 43:20)



This matrix B is 5 minus 6 minus 6 minus 1 4 2 3 minus 6 minus 4 this matrix has the characteristic polynomial as t minus 1 into t minus 2 whole square the minimal polynomial is t minus 1 into t minus 2 the minimal polynomial is the product of distinct linear factors so the matrix is diagonalizable B is actually diagonalizable there is a basis of r 3 having the property that each of the basis vectors is an eigenvector, okay.

But I am I am interested in the rational form of this matrix it can be shown that this matrix B is similar to the matrix A that is you can construct a cyclic basis and the basis which corresponds to an eigenvalue I will not give the details here this A is 0 minus 2 0 1 3 0 0 0 2 see this matrix actually can be diagonalized I am just looking at another form I can show that this B is similar to A that is there is a matrix p which is invertible such that p inverse B p is equal to this matrix A, what is the structure here? The structure here comes from this first block this first block is a companion matrix corresponding to the T annihilator of the eigenvector corresponding to the eigenvalue 2.

Calculate the eigenvector corresponding to 2 call it x 1, look at x 1 T x 1 that will form a subspace the cyclic subspace compute the annihilator compute the companion matrix of this annihilator this block corresponds to that no I am sorry this does not corresponds to that t minus 2 whole square, okay in any case please verify this corresponds to a cyclic subspace companion matrix corresponding to a cyclic subspace, this corresponds to just an eigenvalue this is a rational form of the matrix V, okay. I think I will stop here.