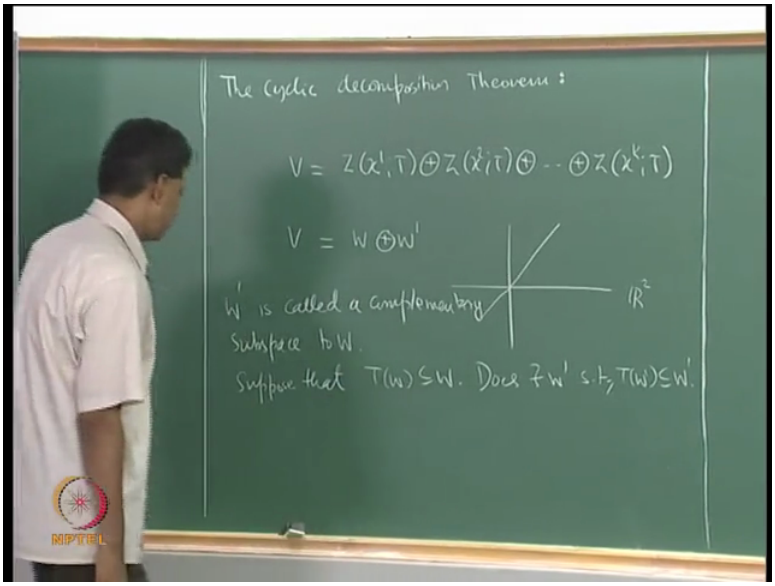
Linear Algebra
Professor K.C Sivakumar
Department of Mathematics
Indian Institute of Technology, Madras
Module 10 Primary and Cyclic Decomposition Theorems
Lecture 37
The Cyclic Decomposition Theorem 1

(Refer Slide Time: 0:20)



Okay, so I will state and proof the cyclic decomposition theorem okay I have mentioned this before what the statement is I will make the precise statement a little later but I need to tell u what is the problem, the question is can we write a finite dimensional vector space V as follows Z x 1; T direct sum Z x 2; T etc Z x k; T that is can I decompose a finite dimensional vector space V such that into a sum of into a direct sum of subspaces such that each subspace is cyclic cyclic with respect to the operator T. So can I find vectors x 1, x 2, etc x k such that this decomposition is possible, okay.

The answer is yes it is related to the following problem this is related to the following problem. See this is the reason why one must look for such a decomposition is that dealing with dealing with operators over cyclic subspaces is easier than dealing with operators over the general space. So one would like to look at the restriction operators the restriction of the operator T on the cyclic subspace then we have already derived some consequences.

For example if u look at the matrix of the restriction of T over the subspace that is a companion matrix, etc, okay. I have not mentioned that is a restriction operator but it is

essentially that so there are some simplifications possible when you study an operator T by restricting the operator to certain subspaces in this instance the cyclic subspaces. This problem is related to another problem which is the following.

Given a finite dimensional vector space V there are subspaces W and W prime such that V is the direct sum of these two subspaces for a finite dimensional vector space this is true even though we will not prove it in this course this is true now what is possible is that given a subspace W of V which is not the whole of V in the finite dimensional case there are infinitely many choices for W prime given a subspace W there are examples where given a subspace W there are infinitely many choices of W prime, okay.

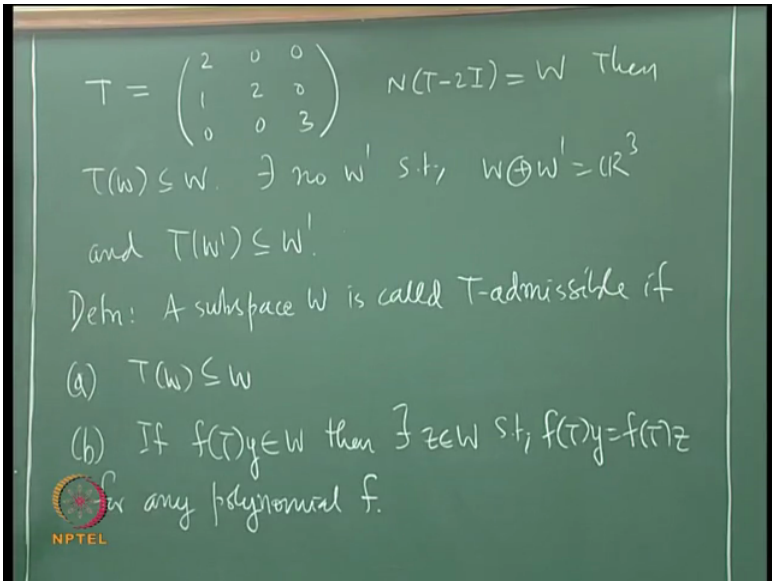
I can give a simple example motivated by the geometry geometry of R 2 this is gives a decomposition the horizontal axis, the vertical axis this gives a decomposition take the horizontal axis and look at the subspace generated subspace of all points lying on this line passing through the origin horizontal space and this slanted space this this subspace has the property that the sum is a direct sum decomposition of R 2 you can verify this easily, unit vector is 1 0 you can take this is the line y equals x so unit vector is 1 by root 2 comma 1 by root 2 then any these two vectors are independent so these two vectors form a direct sum decomposition of R 2.

So in fact any line so take the horizontal and take any slanted line set of all points lying on that line that will be a subspace these two together will give rise to a direct sum decomposition of R 2 this can be done in R n also. So given given a subspace it is possible that there are infinitely many subspaces W prime that satisfy this condition we call W prime as a subspace complementary to W, W prime is called a complementary subspace is called a complementary subspace complementary to W complement to W is called a complementary subspace complement to W.

The question is if you have an operator T can I also look for T invariant subspaces? Can we extend this to a problem where suppose I have suppose the T of W is contained in W that is W is invariant under T can I get a W prime such that W prime is also invariant under T, does there exist W prime a subspace such that W prime is also invariant under T, okay this is rather too much to expect the answer is in general no, okay but we will give a condition onto which this holds, we will we can impose okay the general answer to this question is no, general answer to this question is yes given a subspace W in a finite dimensional vector space given a subspace W can I find a complementary subspace W prime this is always possible.

Given a subspace W such that given a subspace W that is invariant under T, can I find a subspace W prime which is also invariant under T, answer is no. I will give an example so that you will be convinced to get an affirmative answer you need to impose something more on W that is what I will discuss next but I will give an example to show that the answer in general is no.

(Refer Slide Time: 6:38)

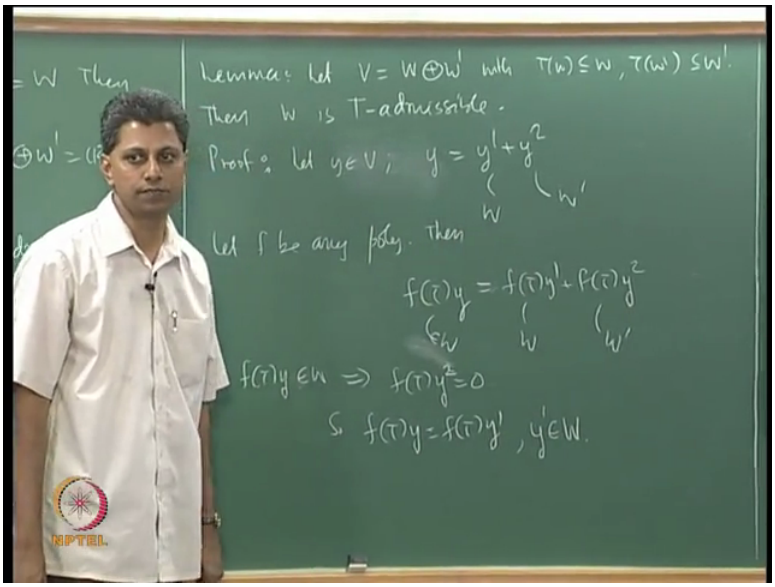


Look at look at the following operator T the matrix of T I will write okay I will write T straight away. Let us look at this diagonal matrix 1 2 0 0 0 3 you look at the space which is null 2 to 3 are the eigenvalues look at null space of 2 minus T I call that W, I am not going to show but I am going to leave this as an exercise show that this see this W is an eigenspace so T W is contained in W this is invariant under T, that is not a problem, okay but there exist no W prime such that W plus W prime is R 3 together with the condition the T W prime contained in W prime, okay.

So if you are seeking an invariant subspace if you are given an invariant subspace W for seeking an invariant subspace W prime the answer in general is no, you need some more conditions on W so that this will be satisfied, what is that condition? That condition is called T-admissibility that condition is called T-admissibility. So let me give this definition condition on a subspace being T admissible, so this is a framework V is a finite dimensional vector space, T is an operator on V, W is a subspace this subspace W is called T admissible if the following two conditions are satisfied.

First condition is that it must be invariant under T, the second condition is that if f T of y belongs to W where f is any polynomial if f T y belongs to W then there exist Z in W such that f T y equals f T z for any polynomial f this is T-admissibility, okay where does this come from? For one thing that the question is how it is related to the notion that we discussed just now? How is this related to seeking a subspace W prime which is also invariant under T given that there is a subspace W which is invariant under T with the assumption that W plus W prime is the whole space W, comma W prime gives a direct sum decomposition where does it come from?

(Refer Slide Time: 9:55)



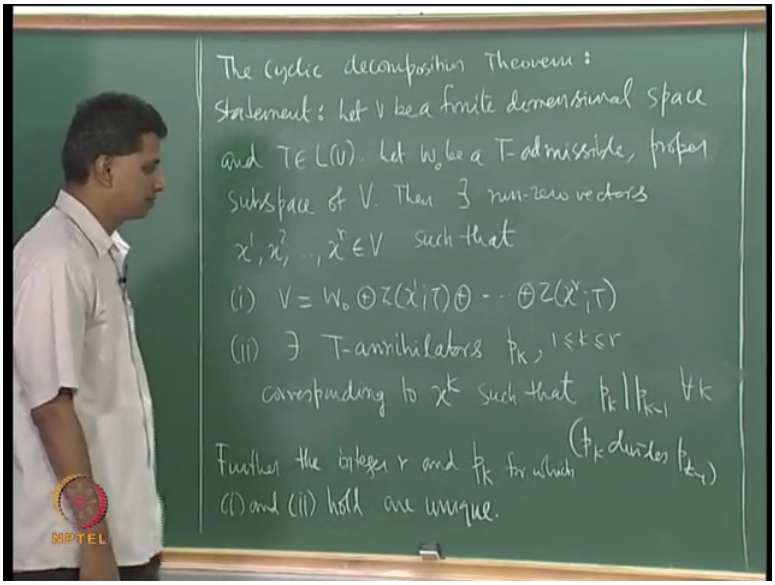
If I have a subspace W given a invariant subspace W so let me make this statement this is easy to see little lemma may be let V be W direct sum W prime with the following T W is contained in W, T W prime is contained in W prime then W is T admissible then W is T admissible this is very easy to see the converse is not at all easy the converse is non-trivial the converse is non-trivial consequence of the cyclic decomposition theorem.

What is the what is the converse is the question that I asked you to begin with, okay how does this follow this is very easy let me proof this quickly I want to show that this condition is satisfied by W, okay see this this I want to show that W is T admissible, okay this condition do not involve W prime, okay I want to show W is T admissible. So let me start with f T y in okay let I will start like this this is a take an arbitrary vector in the vector space then I can write this as y 1 plus y 2, y 1 is in W, y 2 is in W prime in a unique way because of the direct sum decomposition, V is a direct sum decomposition so this representation is unique.

For any polynomial f I look at f T y, f T is linear so f T is f T y 1 plus f T y 2 both these subspaces are T invariant so this belongs to W, this belongs to W prime because both these are invariant subspaces. If this belongs to W if this belongs to W then what is the consequence? This has to be 0, so f T y belongs to W this statement will imply that f T y 2 is 0 this is in W, f T y 2 is 0, if f T y 2 is 0 it means f T is f T y 1 that is f T y equals f T y 1 with the extra provision for us that y 1 belongs to W this is the condition 2 this is second condition.

If f T y belongs to W then there must be existence Z such that f T y equals f T Z in this case Z is y 1, okay so this is simple consequence of the fact that both W and W prime forming a direct sum decomposition of V are invariant under T, okay the converse is not that easy it is a consequence of the cyclic decomposition theorem. So this is a notion that is relevant to the statement of the decomposition theorem T-admissibility of a subspace.

(Refer Slide Time: 13:38)



So let me write down the statement T is a linear operator on a finite dimensional vector space V. Let W be a T admissible, proper subspace of V, W is a T admissible, proper subspace of V so W is not the whole of V but W could be single term 0, T admissible proper subspace of V. Then what we want to show is that there exist non-zero vectors I will call them x 1, x 2, etc x r non-zero vectors in V such that the following conditions hold.

Condition 1 is that V is the direct sum of I will start with W not, W 0 is the invariant subspace T admissible subspace that I start with then V can be shown to be the direct sum of W not and the subspaces Z x 1; T, x 2; T, etc (x) Z x r ; T. I also have another condition there exist T-

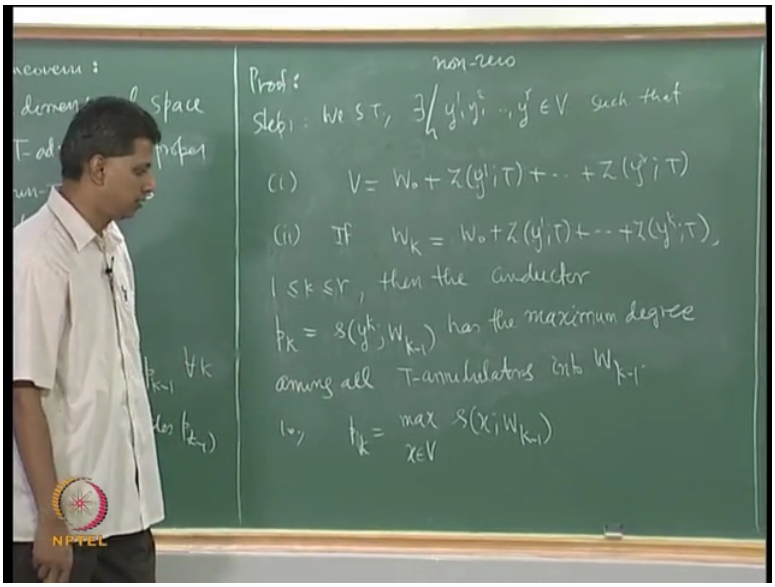
annihilators there exist T-annihilators I will call them p k 1 less than or equal to k less than or equal to r T-annihilators of what of the x case.

T-annihilators p k corresponding to the vector x k that is p k is the T-annihilator of x k, etc for 1 upto r, k running from 1 upto r such that I have this condition p k divides p k minus 1 for all k, k running from 2 to r this time this is p k divides p k minus 1, okay may be I will just write p k divides p k minus 1 for k equal to 2, 3, etc r. The last part says that the last part I will write here itself.

Further the integer r that is what is the number of vectors x 1, etc x r that integer r and p k the integer r and p k for which 1 and 2 hold for which 1 and 2 hold are unique, okay that is the complete statement as I mentioned before this has four steps the last step is the uniqueness I am going to skip the last step uniqueness is not very important so I will skip the last step I will take the other three steps and proof this theorem, okay.

You could ask this question how does this answer how does this decomposition answer the one that we started with Z x 1; T, etc Z x r; T, I mentioned that you could start with W not to be single term 0 so this will not be there so V is a direct sum of this this is called the cyclic decomposition of the vector space V. We also have extra things about the annihilators and how they are related, okay okay.

(Refer Slide Time: 18:35)



There are three steps here as I mentioned the proof has three steps, first step is to show the following. Step 1 we show that there exist vectors y 1, y 2, etc y r in V there exist non-zero vectors there exist non-zero vectors such that such that V is not the direct sum it is just the

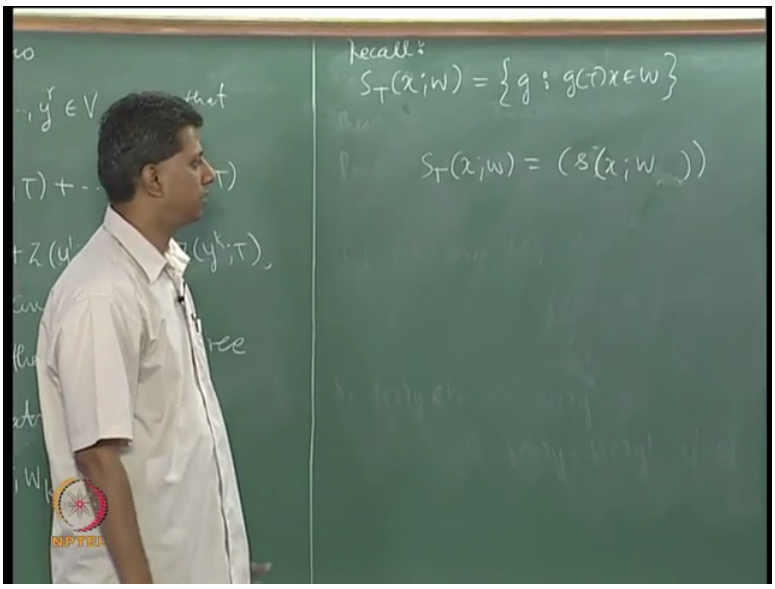
sum W not plus Z y 1; T, etc Z y r; T, okay not that this is not the direct sum just the sum this is the first condition.

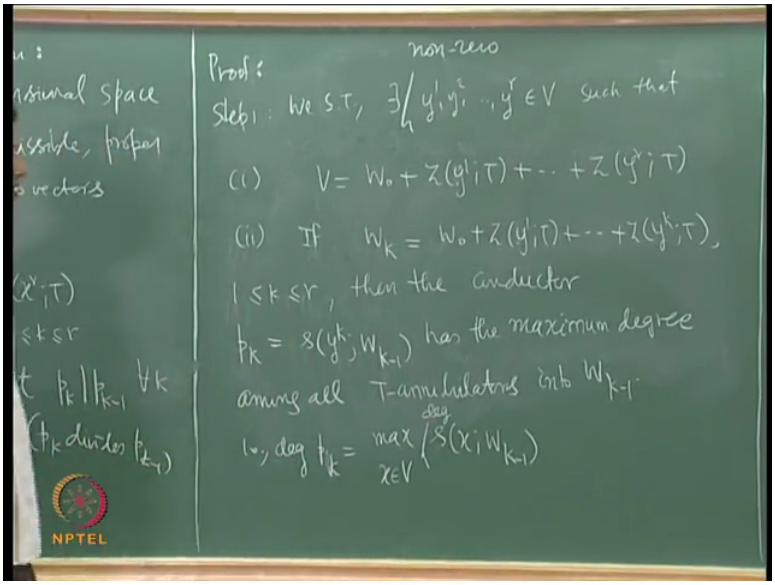
Second condition if W k is is W not plus Z y 1; T etc Z y k; T, W k is the subspace I get by adding these k subspaces to W not that is W k. If W k is this for 1 less than or equal to k less than or equal to r then the conductor then the conductor p k, I will use s y k; W k minus 1, this is the notation I have got explained this notation, okay I will do it a little later, p k is a polynomial it is a conductor this conductor has following property has the maximum degree.

See I must tell you that the statement is complicated but the proof this is easy first step as a maximum degree among among all T-annihilators into W k minus 1, what is the meaning of this? See W k is this subspace I look at a particular polynomial this polynomial is denoted by p k this p k has the property that among all the T-annihilators into W k minus 1 this one has a maximum degree.

So let me write down the formulation p k is p k is maximum p k is maximum over all maximum x element of V, s of x; comma W k minus 1 I have still not defined what this little s is we will do this now and then proof this first step. Once I define s the second part should be clear.

(Refer Slide Time: 22:28)





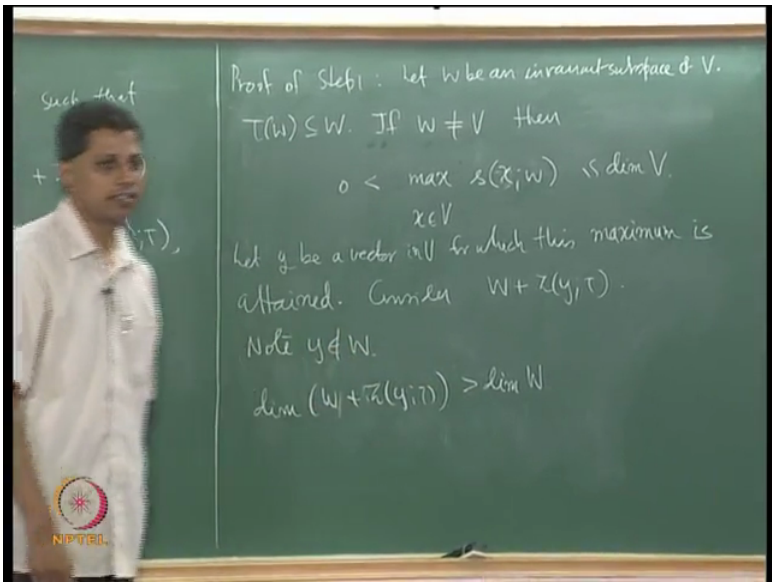
So what is this s? You recall this subspace S T x; W for a subspace so this is really to recall this notion this is the T conductor of x into W that is the set of all polynomials g such that g T x belongs to W this is the T conductor of x into W this is S T. We know that this is an ideal this is an ideal in the principle domain (f D) f T so this is generated by a unique monic polynomial that monic polynomial I will denote it by little s okay to be specific this s for me will be x; comma W k minus 1 this is the this is generated by the polynomial s that unique monic generator s to denote that it depends on x and the subspace W sorry and the subspace W I will denote it like this s x; W so little s always denotes the unique monic generator of a particular ideal of polynomials in this instance it is x; W S T x; W so it is determined by x and W, okay. So now go back and check this go back and see what this definition is.

Look at all see look at s x; W k minus 1 I told you what this is you look at that ideal S T x; comma W k minus 1 fix an x and then your little s x; W k minus 1 is a unique monic generator of that ideal you vary x in V and take the maximum of the degree of all those, okay. Then just mention degree p k degree p k if p k see this is this is an infinite set okay x belongs to V, I look at the maximum of that degrees of you must also write maximum degree here.

So please make this correction also maximum of that degrees of these polynomials the polynomial is s I look at the degrees of those and I will maximize that degree. What I am saying is that maximum degree will be equal to degree of p k where what is p k p k is this particular polynomial p k is this particular T annihilator that is you look at the unique monic generator of the ideal capital S y k; W k minus 1 that is this little s if that is denoted by p k then p k has this maximum property, okay.

So I look at this ideal take the unique monic generator I am calling that as p k, what is the property that p k has with W k minus 1? What is the property that p k has with W k minus 1? In relation to W k minus 1 this is that property among all those vectors x which which are taken for that for that ideal I compute those unique monic polynomials take the maximum of those degrees that degree that number will be equal to degree of this polynomial, okay only those numbers coincide.

(Refer Slide Time: 26:06)



So proof of step 1. Let see I want to start with the invariant subspace W not I want to start with the invariant subspace W not and then construct this V, I would rather start with an invariant subspace W and then apply W not for that. Let W be an invariant subspace of V that is T of W is W contained in W, I take an arbitrary vector y in V. If W is a proper invariant subspace of V then we have the following inequalities two inequalities I look at maximum s x; comma W x in V, if W is not V there exist y in V such that y is not in W.

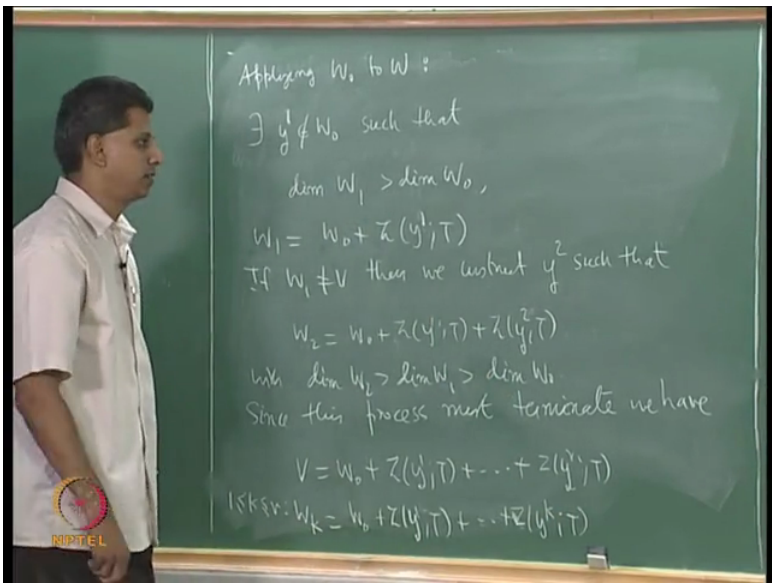
So I want to show what I want to say is if W is not equal to V then I have the following look at if W is not equal to V then maximum of s x; comma W x in V can can this be 0? Can see this is the degree of a polynomial see this s x; W is the unique monic generator of S T x; W can this be 0? If the maximum is 0, can you see that W has to be the whole of V? So this cannot be 0 for one thing it is strictly positive and for the other it cannot exceed the dimension of V, no it can be equal to V dimension can be equal to V the degree can be equal to the dimension of V that is possible because this maximum could happen could happen for the characteristic polynomial this maximum could happen for the characteristic polynomial in which case it could be equal to dimension of V but it is strictly greater than 0 it is strictly

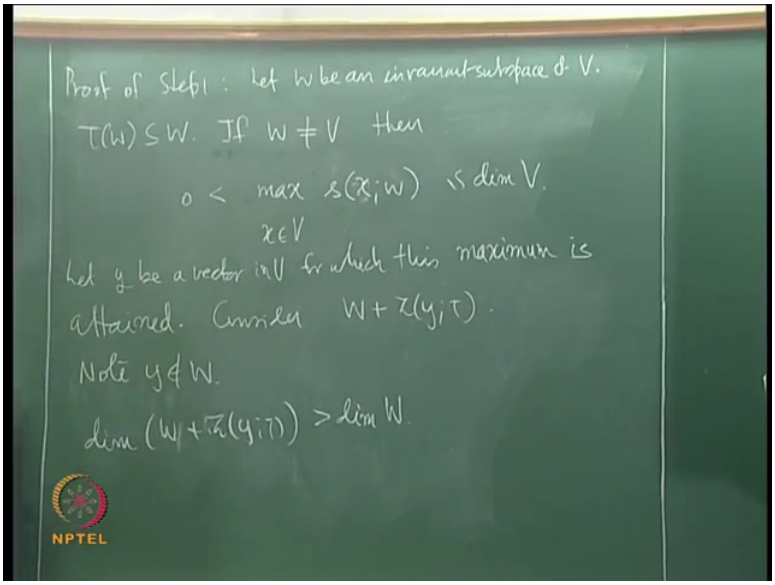
greater than 0 otherwise this W will be the whole of V, I will take a particular vector y which attends this maximum.

Let y be a vector in V for which this maximum is attained in principle this y can be found out there is a y there is a there is a y that attains this maximum. All that I will do is consider a new subspace W plus Z y of T by the way this y cannot be in W, I have not mentioned that this y cannot be in W. Note if y is in W then that degree is 0 y is in W that degree is 0. See I am looking at maximum of all this is y; W, y cannot be in W the degree will otherwise be 0 but strictly positive.

So consider this subspace now since y does not belong to W remember that we could write down a cyclic basis for this subspace Z y; T we could write down a cyclic basis for this subspace so okay now that cyclic if if y belongs to W then this subspace will be contained in W but y is not in W. So the dimension of this subspace the dimension of this subspace will be strictly greater than the dimension of W dimension of this subspace W that we started with there is at least this is at least one dimensional and that the vector in any basis the vector in particular the cyclic basis is independent with sorry not W 1 just W the vector in Z y; T in that cyclic basis will be independent with W because it does not belong to W. So this dimension is strictly greater than dimension of the subspace W that we started with.

(Refer Slide Time: 32:14)





So what I do now is this is true for any invariant subspace W in particular W not I am given an invariant subspace so I will remove this statement we approving applying W not to W, what we have is that there exist a vector instead of y I call it y not there exist y not which does not belong to W not such that such that dimension of W 1 is strictly greater than dimension of W not where for me W 1 will be the subspace W not plus Z y not; comma T, I call it y 1 so that in consistent with my notation.

If there are k subspaces here that will be W k there is only one subspace, okay what is ya W 1 is given here what I do now is look at W 1 W 1 for one thing W not is invariant under T, this is invariant under T cyclic subspace this is invariant under T so the sum will also be invariant under T so W 1 is invariant under T. If W 1 is the whole of the space we are done otherwise I can apply this step to W 1.

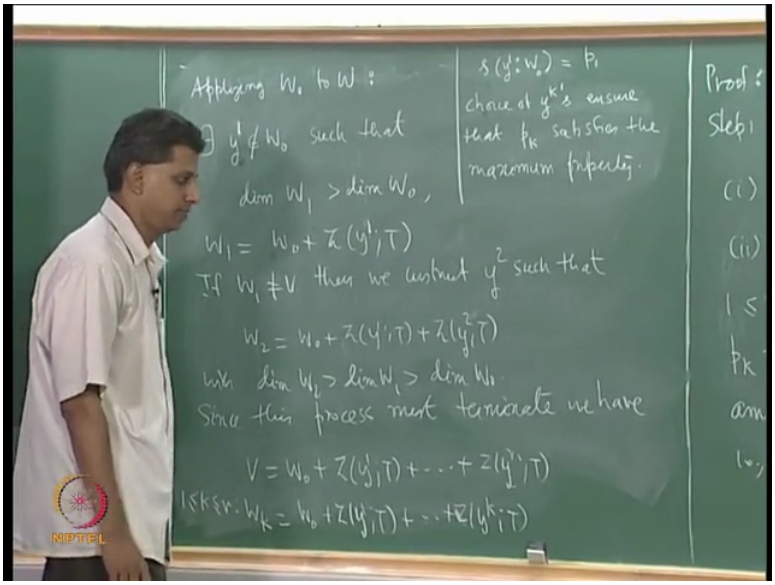
If W 1 is not equal to V then we construct y 2 such that that is we apply the previous that little result to W 1, y 2 such that W 2 equals W not plus Z y 1; T plus Z y 2; T where the dimension of W 2 is strictly greater than the dimension of W 1 strictly greater than dimension of W not every step the dimension increases by at least one, V is finite dimension so this procedure has to terminate, okay this procedure terminates at some point because V is finite dimensional and every time we are increasing the dimension by at least one this procedure has to terminate.

And so I will simply say since this process must terminate we have after at most dimension V steps we have V equals W not plus there is no direct sum just the sum W not plus to begin with in step 1 W not plus Z y 1; T Z y 2; T etc Z y r; T, I am assure that these polynomials

satisfy those conditions, okay that is easy but this is the first part where we have used W k to denote for any k 1 less than or equal to k less than or equal to r W k is the subspace W not Z y 1; T etc Z y k; T.

So we apply this we apply the procedure that we started with to this subspace W k to get this formula V is just the sum of these subspaces, is it now clear that this these p k's p k's have been chosen like this is it clear that p k must divide okay that comes later I will do that later. So is it clear that is it clear that what is the condition that we have imposed on y 1 for instance, okay we will go back to go back to this step we have started with the invariant subspace W what is the condition that we have imposed on y, y is that vector for which this maximum is attained y is that vector in V for which this maximum is attained.

(Refer Slide Time: 37:25)

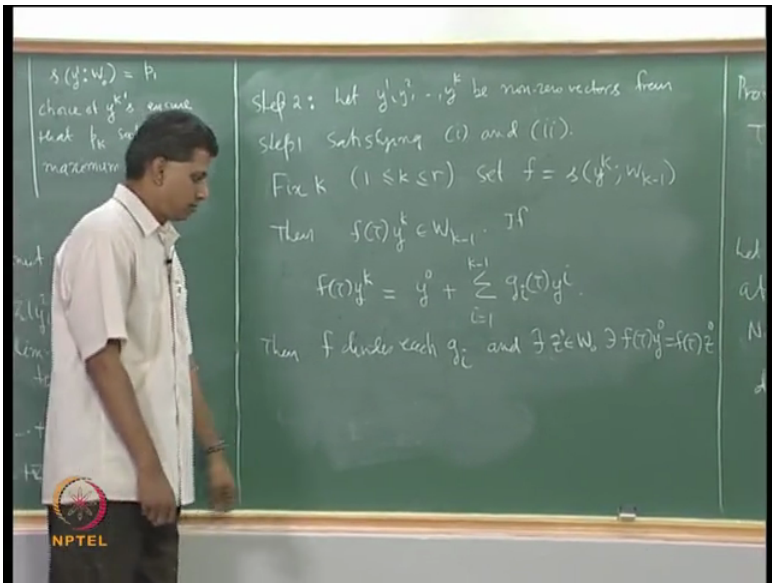


So if you go to first step go to the first step y 1 is the vector for which that maximum is attained, okay. So if you look at if you look at s I will write that here if you look at little s y 1; W k minus 1 that is this time W not y 1 W not I am calling this p 1 right. So by definition this is a maximum degree among all T-annihilators into W not is that not how I see I am applying this for W not I am applying this for W not among all those among all those among all those x so among all those x in V I look at the subspace W not I look at the polynomial that generates that S T and take the maximum.

I do that for y 1 I get p 1, p 2 similarly so this is really a consequence of how we have chosen y 1, y 2 etc okay. So I will just write here that choice of y k's ensure that p k satisfies the maximum property so as I told you this is an easy consequence of the construction of the

vectors I just illustrated for the first vector that this p k satisfies the property that it has maximum degree among all T-annihilators into W k minus 1 comes from the construction of the vectors y 1, etc y k, okay that is step 1 really, is that fine?

(Refer Slide Time: 39:32)



Let us move to step 2 I will proceed from step 1. Let y 1, y 2, etc y k be non-zero vectors the fact that these are non-zero I have not mentioned but these cannot be 0 otherwise the dimension cannot increase so I skip that, none of these vectors can be 0 because if one of them remember that the Z 0; comma T we know it is just single term 0, okay. So dimension cannot increase if this is the crucial step right if y is 0 the dimension cannot increase. So in none of these vectors can be 0, so I have not mentioned but that is easy to see.

Let y 1, etc y k be the non-zero vectors coming from step 2 non-zero vectors from step 1 satisfying just emphasizing the conditions 1 and 2 satisfying the conditions 1 and 2 for a fixed k let me set f as I fixed k I fix the k and then I am looking at I am looking at that (sub) that sub bring that ideal S T y k; comma W k minus 1 my little s is the unique monic generator of that ideal.

For this step I am calling that polynomial as f for simplicity instead of writing this whole thing I am denoting it by f, okay. Then what do I know about this f this f has the property that this f has the property that if you look at f T y k that must belong to W k minus 1. See I have not yet written down what is it that we are going to prove in step 2, okay I have not yet written down what we are proving in step 2, I am just fixing a notation f is this polynomial

then by definition this is the polynomial coming from that S T so that is f T y k must belong to W k minus 1.

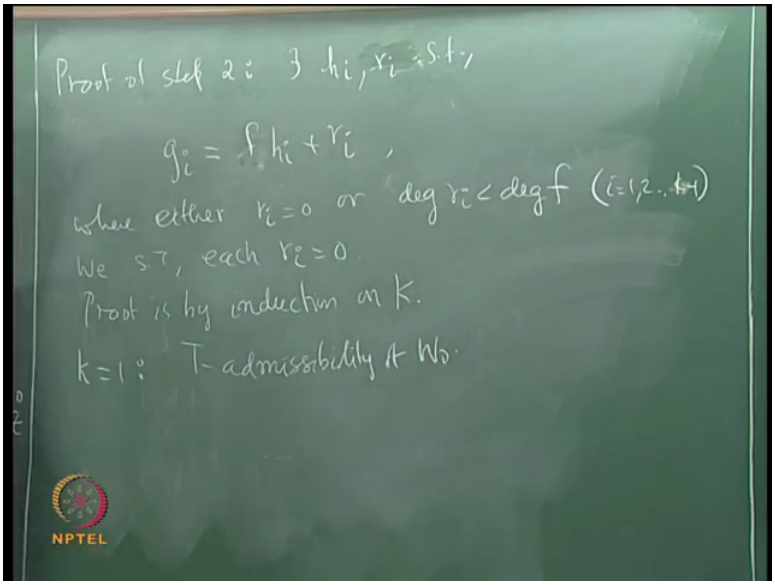
Now it is in W k minus 1 and from the previous step I know what W k is I know what W k minus 1 is. So I can write this f T y k in terms of these subspaces if okay so I have a representation. If f T y k can be written as so first one is W not I will call it y not it is in W not I am calling that y not plus f T y k belongs to W k minus 1 W k minus 1 has this plus k minus 1 terms here k minus 1 subspaces.

So I will use this notation i equals 1 to k minus 1 now I do not know what these I do not know what these vectors are but for one thing I know that these are cyclic subspaces so there is one possibility of what is the basis for instance? We know that it is y 1, T y 1, T square y 1 etc it is a polynomial in y 1. So I will write each term as a polynomial in y 1 I will call that g i I will call it g i T y i this is the most general expression for any vector in Z y k; comma T.

And remember that each of these cyclic subspaces is invariant under T so is it okay I have I have written a I have given a representation for f T y k I know that it belongs to W k minus 1 I look at the formula for W k minus 1 the first term is in W not, the rest of the terms are in those k minus 1 subspaces this is the most general formula that one could write down for those terms then what happens what is that I want to state is mentioned in step 2.

If this happens then f divides each g i, okay that is (())(44:28) f divides each g i and there exist Z not in W there exist Z not in W not such that there exist Z not in W not such that f T y not equals f T Z not this should remained you of the T-admissibility property. So this is a immediate consequence of T-admissibility of W not the rest we have to show that is quite non-trivial step 2 is probably the most non-trivial part of this proof and even in step 2 the second part is easy easy consequence of T-admissibility of W it is this part that f divides g i that is the most non-trivial (let me see).

(Refer Slide Time: 45:29)



So I want to proof step 2, proof of step 2 say I have the polynomials f and g i by euclidean algorithm there exists polynomials h i such that h i, comma r i such that I can write the polynomial g i as f i into h i plus r i by euclidean algorithm where either r i is 0 or degree of r i cannot exceed degree of f here i varies from 1, 2, etc k minus 1 k minus 1, okay I want to show that r i is 0 I want to show that r i is 0 degree of I am sorry it is not f i just f this is f into h i, f is the polynomial that I started with, g i's are the polynomials that come from the general representation of f T y k.

I want to show that each r i is 0, okay we show that each r i equal to 0, if you show that each r i is 0 then it means that f divides g i for all i, okay and second one as I mentioned is an easy consequence of T-admissibility of W not, we need to show that each r i is 0 the proof is by contradiction suppose r i is not 0 we will get a contradiction. The proof is by induction on k for proving the induction I need a basis step basis step is k equals 1 basis step is k equals 1.

For k equals 1, what do I have? What is given? What do I need to proof? For k equals 1 what I have is that f T y 1 belongs to W not the question is does f divide g 1 I am sorry just g 0 no for k equal to 1 this is (())(48:30) for k equal to 1 I have just this f T y k is y not for k equal to 1 it must be in W k minus 1 that is W not, right for k equal to 1 this is W not f T y 1 is just y not this simply does not figure f T y 1 is equal to y not.

So the only thing I need to demonstrate is whether this condition is satisfied please verify is this condition is satisfied? This is satisfied because W not is T admissible, okay this condition is satisfied because W not is T admissible. So k equal to 1 is really T-admissibility of W not I

think I have to stop here and continue tomorrow. Assume that it is true for k greater than 1 and prove it for prove it for k plus 1, okay I will stop here step 2.