Find the T-annihilator of the vector $(1, 0, 0)$. Find the T-annihilator of $(1, 0, i)$.

4. Prove that if T^2 has a cyclic vector, then T has a cyclic vector. Is the converse true?

5. Let V be an n-dimensional vector space over the field F, and let N be a nilpotent linear operator on V. Suppose $N^{n-1} \neq 0$, and let α be any vector in V such that $N^{n-1}\alpha \neq 0$. Prove that α is a cyclic vector for N. What exactly is the matrix of N in the ordered basis $\{\alpha, N\alpha, \ldots, N^{n-1}\alpha\}$?

6. Give a direct proof that if A is the companion matrix of the monic polynomial p, then p is the characteristic polynomial for A.

7. Let V be an n-dimensional vector space, and let T be a linear operator on V. Suppose that T is *diagonalizable.*

(a) If T has a cyclic vector, show that T has n distinct characteristic values.

(b) If T has n distinct characteristic values, and if $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of characteristic vectors for T, show that $\alpha = \alpha_1 + \cdots + \alpha_n$ is a cyclic vector for T.

8. Let T be a linear operator on the finite-dimensional vector space V. Suppose T has a cyclic vector. Prove that if U is any linear operator which commutes with T, then U is a polynomial in T.

7.2. Cyclic Decompositions and the Rational Form

The primary purpose of this section is to prove that if T is any linear operator on a finite-dimensional space V, then there exist vectors $\alpha_1, \ldots, \alpha_r$ in V such that

$$V = Z(\alpha_1; T) \oplus \cdots \oplus Z(\alpha_r; T).$$

In other words, we wish to prove that V is a direct sum of T-cyclic subspaces. This will show that T is the direct sum of a finite number of linear operators, each of which has a cyclic vector. The effect of this will be to reduce many questions about the general linear operator to similar questions about an operator which has a cyclic vector. The theorem which we prove (Theorem 3) is one of the deepest results in linear algebra and has many interesting corollaries.

The cyclic decomposition theorem is closely related to the following question. Which T-invariant subspaces W have the property that there exists a T-invariant subspace W' such that $V = W \oplus W'$? If W is any subspace of a finite-dimensional space V, then there exists a subspace W' such that $V = W \oplus W'$. Usually there are many such subspaces W' and each of these is called **complementary** to W. We are asking when a T-invariant subspace has a complementary subspace which is also invariant under T.

Let us suppose that $V = W \oplus W'$ where both W and W' are invariant under T and then see what we can discover about the subspace W. Each vector β in V is of the form $\beta = \gamma + \gamma'$ where γ is in W and γ' is in W'. If f is any polynomial over the scalar field, then

$$f(T)\beta = f(T)\gamma + f(T)\gamma'.$$

Since W and W' are invariant under T, the vector $f(T)\gamma$ is in W and $f(T)\gamma'$ is in W'. Therefore $f(T)\beta$ is in W if and only if $f(T)\gamma' = 0$. What interests us is the seemingly innocent fact that, if $f(T)\beta$ is in W, then $f(T)\beta = f(T)\gamma$.

Definition. *Let* T *be a linear operator on a vector space* V *and let* W *be a subspace of* V. *We say that* W *is* **T-admissible** *if*

(i) W *is invariant under* T;
(ii) *if* f(T)β *is in* W, *there exists a vector* γ *in* W *such that* f(T)β = f(T)γ.

As we just showed, if W is invariant and has a complementary invariant subspace, then W is admissible. One of the consequences of Theorem 3 will be the converse, so that admissibility characterizes those invariant subspaces which have complementary invariant subspaces.

Let us indicate how the admissibility property is involved in the attempt to obtain a decomposition

$$V = Z(\alpha_1; T) \oplus \cdots \oplus Z(\alpha_r; T).$$

Our basic method for arriving at such a decomposition will be to inductively select the vectors $\alpha_1, \ldots, \alpha_r$. Suppose that by some process or another we have selected $\alpha_1, \ldots, \alpha_j$ and the subspace

$$W_j = Z(\alpha_1; T) + \cdots + Z(\alpha_j; T)$$

is proper. We would like to find a non-zero vector α_{j+1} such that

$$W_j \cap Z(\alpha_{j+1}; T) = \{0\}$$

because the subspace $W_{j+1} = W_j \oplus Z(\alpha_{j+1}; T)$ would then come at least one dimension nearer to exhausting V. But, why should any such α_{j+1} exist? If $\alpha_1, \ldots, \alpha_j$ have been chosen so that W_j is a T-admissible subspace, then it is rather easy to see that we can find a suitable α_{j+1}. This is what will make our proof of Theorem 3 work, even if that is not how we phrase the argument.

Let W be a proper T-invariant subspace. Let us try to find a non-zero vector α such that

$$W \cap Z(\alpha; T) = \{0\}. \tag{7-3}$$

We can choose some vector β which is not in W. Consider the *T-conductor* $S(\beta; W)$, which consists of all polynomials g such that $g(T)\beta$ is in W. Recall that the monic polynomial $f = s(\beta; W)$ which generates the ideal $S(\beta; W)$ is also called the *T-conductor of* β *into* W. The vector $f(T)\beta$ is in W. Now, if W is T-admissible, there is a γ in W with $f(T)\beta = f(T)\gamma$. Let $\alpha = \beta - \gamma$ and let g be any polynomial. Since $\beta - \alpha$ is in W, $g(T)\beta$ will be in W if and only if $g(T)\alpha$ is in W; in other words, $S(\alpha; W) = S(\beta; W)$. Thus the polynomial f is also the T-conductor of α into W. But $f(T)\alpha = 0$. That tells us that $g(T)\alpha$ is in W if and only if $g(T)\alpha = 0$, i.e., the subspaces $Z(\alpha; T)$ and W are independent (7-3) and f is the T-annihilator of α.

Theorem 3 (Cyclic Decomposition Theorem). *Let* T *be a linear operator on a finite-dimensional vector space* V *and let* W_0 *be a proper* T-*admissible subspace of* V. *There exist non-zero vectors* $\alpha_1, \ldots, \alpha_r$ *in* V *with respective* T-*annihilators* $p_1, \ldots, p_r$ *such that*

(i) $V = W_0 \oplus Z(\alpha_1; T) \oplus \cdots \oplus Z(\alpha_r; T)$;
(ii) p_k *divides* p_{k-1}, $k = 2, \ldots, r$.

Furthermore, the integer r *and the annihilators* $p_1, \ldots, p_r$ *are uniquely determined by* (i), (ii), *and the fact that no* α_k *is* 0.

Proof. The proof is rather long; hence, we shall divide it into four steps. For the first reading it may seem easier to take $W_0 = \{0\}$, although it does not produce any substantial simplification. Throughout the proof, we shall abbreviate $f(T)\beta$ to $f\beta$.

Step 1. There exist non-zero vectors $\beta_1, \ldots, \beta_r$ *in* V *such that*

(a) $V = W_0 + Z(\beta_1; T) + \cdots + Z(\beta_r; T)$;
(b) *if* $1 \le k \le r$ *and*

$$W_k = W_0 + Z(\beta_1; T) + \cdots + Z(\beta_k; T)$$

then the conductor $p_k = s(\beta_k; W_{k-1})$ *has maximum degree among all* T-*conductors into the subspace* W_{k-1}, i.e., *for every* k

$$\deg p_k = \max_{\alpha \text{ in } V} \deg s(\alpha; W_{k-1}).$$

This step depends only upon the fact that W_0 is an invariant subspace. If W is a proper T-invariant subspace, then

$$0 < \max_{\alpha} \deg s(\alpha; W) \le \dim V$$

and we can choose a vector β so that $\deg s(\beta; W)$ attains that maximum. The subspace $W + Z(\beta; T)$ is then T-invariant and has dimension larger than $\dim W$. Apply this process to $W = W_0$ to obtain β_1. If $W_1 = W_0 + Z(\beta_1; T)$ is still proper, then apply the process to W_1 to obtain β_2. Continue in that manner. Since $\dim W_k > \dim W_{k-1}$, we must reach $W_r = V$ in not more than $\dim V$ steps.

Step 2. Let $\beta_1, \ldots, \beta_r$ *be non-zero vectors which satisfy conditions (a) and (b) of Step 1. Fix* k, $1 \le k \le r$. *Let* β *be any vector in* V *and let* $f = s(\beta; W_{k-1})$. *If*

$$f\beta = \beta_0 + \sum_{1 \le i < k} g_i\beta_i, \qquad \beta_i \textit{ in } W_i$$

then f *divides each polynomial* g_i *and* $\beta_0 = f\gamma_0$, *where* γ_0 *is in* W_0.

If $k = 1$, this is just the statement that W_0 is T-admissible. In order to prove the assertion for $k > 1$, apply the division algorithm:

$$g_i = fh_i + r_i, \qquad r_i = 0 \quad \text{or} \quad \deg r_i < \deg f. \tag{7-4}$$

We wish to show that $r_i = 0$ for each i. Let

$$\gamma = \beta - \sum_{1}^{k-1} h_i\beta_i. \tag{7-5}$$

Since $\gamma - \beta$ is in W_{k-1},

$$s(\gamma; W_{k-1}) = s(\beta; W_{k-1}) = f.$$

Furthermore

$$f\gamma = \beta_0 + \sum_{1}^{k-1} r_i\beta_i. \tag{7-6}$$

Suppose that some r_i is different from 0. We shall deduce a contradiction. Let j be the largest index i for which $r_i \neq 0$. Then

$$f\gamma = \beta_0 + \sum_{1}^{j} r_i\beta_i, \qquad r_j \neq 0 \quad \text{and} \quad \deg r_j < \deg f. \tag{7-7}$$

Let $p = s(\gamma; W_{j-1})$. Since W_{k-1} contains W_{j-1}, the conductor $f = s(\gamma; W_{k-1})$ must divide p:

$$p = fg.$$

Apply $g(T)$ to both sides of (7-7):

$$p\gamma = gf\gamma = gr_j\beta_j + g\beta_0 + \sum_{1 \leq i < j} gr_i\beta_i. \tag{7-8}$$

By definition, $p\gamma$ is in W_{j-1}, and the last two terms on the right side of (7-8) are in W_{j-1}. Therefore, $gr_j\beta_j$ is in W_{j-1}. Now we use condition (b) of Step 1:

$$\begin{aligned} \deg (gr_j) &\geq \deg s(\beta_j; W_{j-1}) \\ &= \deg p_j \\ &\geq \deg s(\gamma; W_{j-1}) \\ &= \deg p \\ &= \deg (fg). \end{aligned}$$

Thus $\deg r_j \geq \deg f$, and that contradicts the choice of j. We now know that f divides each g_i and hence that $\beta_0 = f\gamma$. Since W_0 is T-admissible, $\beta_0 = f\gamma_0$ where γ_0 is in W_0. We remark in passing that Step 2 is a strengthened form of the assertion that each of the subspaces $W_1, W_2, \ldots, W_r$ is T-admissible.

Step 3. There exist non-zero vectors $\alpha_1, \ldots, \alpha_r$ *in* V *which satisfy conditions* (i) *and* (ii) *of Theorem 3.*

Start with vectors $\beta_1, \ldots, \beta_r$ as in Step 1. Fix k, $1 \leq k \leq r$. We apply Step 2 to the vector $\beta = \beta_k$ and the T-conductor $f = p_k$. We obtain

$$p_k\beta_k = p_k\gamma_0 + \sum_{1 \leq i < k} p_kh_i\beta_i \tag{7-9}$$

where γ_0 is in W_0 and $h_1, \ldots, h_{k-1}$ are polynomials. Let

(7-10) $$\alpha_k = \beta_k - \gamma_0 - \sum_{1 \leq i < k} h_i\beta_i.$$

Since $\beta_k - \alpha_k$ is in W_{k-1},

(7-11) $$s(\alpha_k; W_{k-1}) = s(\beta_k; W_{k-1}) = p_k$$

and since $p_k\alpha_k = 0$, we have

(7-12) $$W_{k-1} \cap Z(\alpha_k; T) = \{0\}.$$

Because each α_k satisfies (7-11) and (7-12), it follows that

$$W_k = W_0 \oplus Z(\alpha_1; T) \oplus \cdots \oplus Z(\alpha_k; T)$$

and that p_k is the T-annihilator of α_k. In other words, the vectors $\alpha_1, \ldots, \alpha_r$ define the same sequence of subspaces $W_1, W_2, \ldots$ as do the vectors $\beta_1, \ldots, \beta_r$ and the T-conductors $p_k = s(\alpha_k, W_{k-1})$ have the same maximality properties (condition (b) of Step 1). The vectors $\alpha_1, \ldots, \alpha_r$ have the additional property that the subspaces W_0, $Z(\alpha_1; T)$, $Z(\alpha_2; T), \ldots$ are independent. It is therefore easy to verify condition (ii) in Theorem 3. Since $p_i\alpha_i = 0$ for each i, we have the trivial relation

$$p_k\alpha_k = 0 + p_1\alpha_1 + \cdots + p_{k-1}\alpha_{k-1}.$$

Apply Step 2 with $\beta_1, \ldots, \beta_k$ replaced by $\alpha_1, \ldots, \alpha_k$ and with $\beta = \alpha_k$. Conclusion: p_k divides each p_i with $i < k$.

Step 4. The number r *and the polynomials* $p_1, \ldots, p_r$ *are uniquely determined by the conditions of Theorem 3.*

Suppose that in addition to the vectors $\alpha_1, \ldots, \alpha_r$ in Theorem 3 we have non-zero vectors $\gamma_1, \ldots, \gamma_s$ with respective T-annihilators $g_1, \ldots, g_s$ such that

(7-13) $$\begin{aligned} &V = W_0 \oplus Z(\gamma_1; T) \oplus \cdots \oplus Z(\gamma_s; T) \\ &g_k \text{ divides } g_{k-1}, \qquad k = 2, \ldots, s. \end{aligned}$$

We shall show that $r = s$ and $p_i = g_i$ for each i.

It is very easy to see that $p_1 = g_1$. The polynomial g_1 is determined from (7-13) as the T-conductor of V into W_0. Let $S(V; W_0)$ be the collection of polynomials f such that $f\beta$ is in W_0 for every β in V, i.e., polynomials f such that the range of $f(T)$ is contained in W_0. Then $S(V; W_0)$ is a non-zero ideal in the polynomial algebra. The polynomial g_1 is the monic generator of that ideal, for this reason. Each β in V has the form

$$\beta = \beta_0 + f_1\gamma_1 + \cdots + f_s\gamma_s$$

and so

$$g_1\beta = g_1\beta_0 + \sum_1^s g_1f_i\gamma_i.$$

Since each g_i divides g_1, we have $g_1\gamma_i = 0$ for all i and $g_1\beta = g_1\beta_0$ is in W_0. Thus g_1 is in $S(V; W_0)$. Since g_1 is the monic polynomial of least degree