7

Canonical Forms

As we learned in Chapter 5, the advantage of a diagonalizable linear operator lies in the simplicity of its description. Such an operator has a diagonal matrix representation, or, equivalently, there is an ordered basis for the underlying vector space consisting of eigenvectors of the operator. However, not every linear operator is diagonalizable, even if its characteristic polynomial splits. Example 3 of Section 5.2 describes such an operator.

It is the purpose of this chapter to consider alternative matrix representations for nondiagonalizable operators. These representations are called *canonical forms*. There are different kinds of canonical forms, and their advantages and disadvantages depend on how they are applied. The choice of a canonical form is determined by the appropriate choice of an ordered basis. Naturally, the canonical forms of a linear operator are not diagonal matrices if the linear operator is not diagonalizable.

In this chapter, we treat two common canonical forms. The first of these, the *Jordan canonical form*, requires that the characteristic polynomial of the operator splits. This form is always available if the underlying field is algebraically closed, that is, if every polynomial with coefficients from the field splits. For example, the field of complex numbers is algebraically closed by the fundamental theorem of algebra (see Appendix D). The first two sections deal with this form. The *rational canonical form*, treated in Section 7.4, does not require such a factorization.

7.1 THE JORDAN CANONICAL FORM I

Let T be a linear operator on a finite-dimensional vector space V, and suppose that the characteristic polynomial of T splits. Recall from Section 5.2 that the diagonalizability of T depends on whether the union of ordered bases for the distinct eigenspaces of T is an ordered basis for V. So a lack of diagonalizability means that at least one eigenspace of T is too "small."

In this section, we extend the definition of eigenspace to *generalized eigenspace*. From these subspaces, we select ordered bases whose union is an ordered basis β for V such that

$$[\mathsf{T}]_\beta = \begin{pmatrix} A_1 & O & \cdots & O \\ O & A_2 & \cdots & O \\ \vdots & \vdots & & \vdots \\ O & O & \cdots & A_k \end{pmatrix},$$

where each O is a zero matrix, and each A_i is a square matrix of the form (λ) or

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}$$

for some eigenvalue λ of T. Such a matrix A_i is called a **Jordan block** corresponding to λ, and the matrix $[\mathsf{T}]_\beta$ is called a **Jordan canonical form** of T. We also say that the ordered basis β is a **Jordan canonical basis** for T. Observe that each Jordan block A_i is "almost" a diagonal matrix—in fact, $[\mathsf{T}]_\beta$ is a diagonal matrix if and only if each A_i is of the form (λ).

Example 1

Suppose that T is a linear operator on C^8, and $\beta = \{v_1, v_2, \ldots, v_8\}$ is an ordered basis for C^8 such that

$$J = [\mathsf{T}]_\beta = \left(\begin{array}{ccc|ccccc} 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

is a Jordan canonical form of T. Notice that the characteristic polynomial of T is $\det(J - tI) = (t-2)^4(t-3)^2t^2$, and hence the multiplicity of each eigenvalue is the number of times that the eigenvalue appears on the diagonal of J. Also observe that v_1, v_4, v_5, and v_7 are the only vectors in β that are eigenvectors of T. These are the vectors corresponding to the columns of J with no 1 above the diagonal entry. ◆

In Sections 7.1 and 7.2, we prove that every linear operator whose characteristic polynomial splits has a Jordan canonical form that is unique up to the order of the Jordan blocks. Nevertheless, it is not the case that the Jordan canonical form is completely determined by the characteristic polynomial of the operator. For example, let T' be the linear operator on C^8 such that $[T']_\beta = J'$, where β is the ordered basis in Example 1 and

$$J' = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then the characteristic polynomial of T' is also $(t-2)^4(t-3)^2t^2$. But the operator T' has the Jordan canonical form J', which is different from J, the Jordan canonical form of the linear operator T of Example 1.

Consider again the matrix J and the ordered basis β of Example 1. Notice that $T(v_2) = v_1 + 2v_2$ and therefore, $(T-2I)(v_2) = v_1$. Similarly, $(T-2I)(v_3) = v_2$. Since v_1 and v_4 are eigenvectors of T corresponding to $\lambda = 2$, it follows that $(T-2I)^3(v_i) = 0$ for $i = 1, 2, 3$, and 4. Similarly $(T-3I)^2(v_i) = 0$ for $i = 5, 6$, and $(T-0I)^2(v_i) = 0$ for $i = 7, 8$.

Because of the structure of each Jordan block in a Jordan canonical form, we can generalize these observations: *If v lies in a Jordan canonical basis for a linear operator T and is associated with a Jordan block with diagonal entry λ, then $(T-\lambda I)^p(v) = 0$ for sufficiently large p.* Eigenvectors satisfy this condition for $p = 1$.

Definition. *Let T be a linear operator on a vector space V, and let λ be a scalar. A nonzero vector x in V is called a* **generalized eigenvector of T corresponding to λ** *if $(T-\lambda I)^p(x) = 0$ for some positive integer p.*

Notice that if x is a generalized eigenvector of T corresponding to λ, and p is the smallest positive integer for which $(T-\lambda I)^p(x) = 0$, then $(T-\lambda I)^{p-1}(x)$ is an eigenvector of T corresponding to λ. Therefore λ is an eigenvalue of T.

In the context of Example 1, each vector in β is a generalized eigenvector of T. In fact, v_1, v_2, v_3 and v_4 correspond to the scalar 2, v_5 and v_6 correspond to the scalar 3, and v_7 and v_8 correspond to the scalar 0.

Just as eigenvectors lie in eigenspaces, generalized eigenvectors lie in "generalized eigenspaces."

Definition. *Let T be a linear operator on a vector space V, and let λ be an eigenvalue of T. The* **generalized eigenspace of T corresponding to**

λ, *denoted* K_λ, *is the subset of* V *defined by*

$$\mathsf{K}_\lambda = \{x \in \mathsf{V} : (\mathsf{T} - \lambda\mathsf{I})^p(x) = 0 \text{ for some positive integer } p\}.$$

Note that K_λ consists of the zero vector and all generalized eigenvectors corresponding to λ.

Recall that a subspace W of V is T-invariant for a linear operator T if $\mathsf{T}(\mathsf{W}) \subseteq \mathsf{W}$. In the development that follows, we assume the results of Exercises 3 and 4 of Section 5.4. In particular, for any polynomial $g(x)$, if W is T-invariant, then it is also $g(\mathsf{T})$-invariant. Furthermore, the range of a linear operator T is T-invariant.

Theorem 7.1. *Let* T *be a linear operator on a vector space* V, *and let* λ *be an eigenvalue of* T. *Then*

(a) K_λ *is a* T*-invariant subspace of* V *containing* E_λ *(the eigenspace of* T *corresponding to* λ*).*

(b) *For any scalar* $\mu \neq \lambda$, *the restriction of* $\mathsf{T} - \mu\mathsf{I}$ *to* K_λ *is one-to-one.*

Proof. (a) Clearly, $0 \in \mathsf{K}_\lambda$. Suppose that x and y are in K_λ. Then there exist positive integers p and q such that

$$(\mathsf{T} - \lambda\mathsf{I})^p(x) = (\mathsf{T} - \lambda\mathsf{I})^q(y) = 0.$$

Therefore

$$\begin{aligned}(\mathsf{T} - \lambda\mathsf{I})^{p+q}(x+y) &= (\mathsf{T} - \lambda\mathsf{I})^{p+q}(x) + (\mathsf{T} - \lambda\mathsf{I})^{p+q}(y)\\ &= (\mathsf{T} - \lambda\mathsf{I})^q(0) + (\mathsf{T} - \lambda\mathsf{I})^p(0)\\ &= 0,\end{aligned}$$

and hence $x+y \in \mathsf{K}_\lambda$. The proof that K_λ is closed under scalar multiplication is straightforward.

To show that K_λ is T-invariant, consider any $x \in \mathsf{K}_\lambda$. Choose a positive integer p such that $(\mathsf{T} - \lambda\mathsf{I})^p(x) = 0$. Then

$$(\mathsf{T} - \lambda\mathsf{I})^p\mathsf{T}(x) = \mathsf{T}(\mathsf{T} - \lambda\mathsf{I})^p(x) = \mathsf{T}(0) = 0.$$

Therefore $\mathsf{T}(x) \in \mathsf{K}_\lambda$.

Finally, it is a simple observation that E_λ is contained in K_λ.

(b) Let $x \in \mathsf{K}_\lambda$ and $(\mathsf{T} - \mu\mathsf{I})(x) = 0$. By way of contradiction, suppose that $x \neq 0$. Let p be the smallest integer for which $(\mathsf{T} - \lambda\mathsf{I})^p(x) = 0$, and let $y = (\mathsf{T} - \lambda\mathsf{I})^{p-1}(x)$. Then

$$(\mathsf{T} - \lambda\mathsf{I})(y) = (\mathsf{T} - \lambda\mathsf{I})^p(x) = 0,$$

and hence $y \in \mathsf{E}_\lambda$. Furthermore,

$$(\mathsf{T} - \mu\mathsf{I})(y) = (\mathsf{T} - \mu\mathsf{I})(\mathsf{T} - \lambda\mathsf{I})^{p-1}(x) = (\mathsf{T} - \lambda\mathsf{I})^{p-1}(\mathsf{T} - \mu\mathsf{I})(x) = 0,$$

so that $y \in \mathsf{E}_\mu$. But $\mathsf{E}_\lambda \cap \mathsf{E}_\mu = \{0\}$, and thus $y = 0$, contrary to the hypothesis. So $x = 0$, and the restriction of $\mathsf{T} - \mu\mathsf{I}$ to K_λ is one-to-one. ∎

Theorem 7.2. *Let T be a linear operator on a finite-dimensional vector space V such that the characteristic polynomial of T splits. Suppose that λ is an eigenvalue of T with multiplicity m. Then*

(a) $\dim(\mathsf{K}_\lambda) \leq m$.

(b) $\mathsf{K}_\lambda = \mathsf{N}((\mathsf{T} - \lambda\mathsf{I})^m)$.

Proof. (a) Let $\mathsf{W} = \mathsf{K}_\lambda$, and let $h(t)$ be the characteristic polynomial of T_W. By Theorem 5.21 (p. 314), $h(t)$ divides the characteristic polynomial of T, and by Theorem 7.1(b), λ is the only eigenvalue of T_W. Hence $h(t) = (-1)^d(t-\lambda)^d$, where $d = \dim(\mathsf{W})$, and $d \leq m$.

(b) Clearly $\mathsf{N}((\mathsf{T} - \lambda\mathsf{I})^m) \subseteq \mathsf{K}_\lambda$. Now let W and $h(t)$ be as in (a). Then $h(\mathsf{T}_\mathsf{W})$ is identically zero by the Cayley–Hamilton theorem (p. 317); therefore $(\mathsf{T} - \lambda\mathsf{I})^d(x) = 0$ for all $x \in \mathsf{W}$. Since $d \leq m$, we have $\mathsf{K}_\lambda \subseteq \mathsf{N}((\mathsf{T} - \lambda\mathsf{I})^m)$. ∎

Theorem 7.3. *Let T be a linear operator on a finite-dimensional vector space V such that the characteristic polynomial of T splits, and let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of T. Then, for every $x \in \mathsf{V}$, there exist vectors $v_i \in \mathsf{K}_{\lambda_i}$, $1 \leq i \leq k$, such that*

$$x = v_1 + v_2 + \cdots + v_k.$$

Proof. The proof is by mathematical induction on the number k of distinct eigenvalues of T. First suppose that $k = 1$, and let m be the multiplicity of λ_1. Then $(\lambda_1 - t)^m$ is the characteristic polynomial of T, and hence $(\lambda_1\mathsf{I} - \mathsf{T})^m = \mathsf{T}_0$ by the Cayley–Hamilton theorem (p. 317). Thus $\mathsf{V} = \mathsf{K}_{\lambda_1}$, and the result follows.

Now suppose that for some integer $k > 1$, the result is established whenever T has fewer than k distinct eigenvalues, and suppose that T has k distinct eigenvalues. Let m be the multiplicity of λ_k, and let $f(t)$ be the characteristic polynomial of T. Then $f(t) = (t - \lambda_k)^m g(t)$ for some polynomial $g(t)$ not divisible by $(t - \lambda_k)$. Let $\mathsf{W} = \mathsf{R}((\mathsf{T} - \lambda_k\mathsf{I})^m)$. Clearly W is T-invariant. Observe that $(\mathsf{T} - \lambda_k\mathsf{I})^m$ maps K_{λ_i} onto itself for $i < k$. For suppose that $i < k$. Since $(\mathsf{T} - \lambda_k\mathsf{I})^m$ maps K_{λ_i} into itself and $\lambda_k \neq \lambda_i$, the restriction of $\mathsf{T} - \lambda_k\mathsf{I}$ to K_{λ_i} is one-to-one (by Theorem 7.1(b)) and hence is onto. One consequence of this is that for $i < k$, K_{λ_i} is contained in W, and hence λ_i is an eigenvalue of T_W with corresponding generalized eigenspace K_{λ_i}.

Next, observe that λ_k is not an eigenvalue of T_W. For suppose that $\mathsf{T}(v) = \lambda_k v$ for some $v \in \mathsf{W}$. Then $v = (\mathsf{T} - \lambda_k\mathsf{I})^m(y)$ for some $y \in \mathsf{V}$, and it follows that

$$0 = (\mathsf{T} - \lambda_k\mathsf{I})(v) = (\mathsf{T} - \lambda_k\mathsf{I})^{m+1}(y).$$

Therefore $y \in \mathsf{K}_{\lambda_k}$. So by Theorem 7.2, $v = (\mathsf{T} - \lambda_k\mathsf{I})^m(y) = 0$.

Since every eigenvalue of T_W is an eigenvalue of T, the distinct eigenvalues of T_W are $\lambda_1, \lambda_2, \ldots, \lambda_{k-1}$.

Now let $x \in V$. Then $(T - \lambda_k I)^m(x) \in W$. Since T_W has the $k-1$ distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_{k-1}$, the induction hypothesis applies. The corresponding generalized eigenspace of T_W for each λ_i is K_{λ_i}, and hence there are vectors $w_i \in K_{\lambda_i}$, $1 \le i \le k-1$, such that

$$(T - \lambda_k I)^m(x) = w_1 + w_2 + \cdots + w_{k-1}.$$

Since $(T - \lambda_k I)^m$ maps K_{λ_i} onto itself for $i < k$, there exist vectors $v_i \in K_{\lambda_i}$ such that $(T - \lambda_k I)^m(v_i) = w_i$ for $i < k$. Thus

$$(T - \lambda_k I)^m(x) = (T - \lambda_k I)^m(v_1) + (T - \lambda_k I)^m(v_2) + \cdots + (T - \lambda_k I)^m(v_{k-1}),$$

and it follows that $x - (v_1 + v_2 + \cdots + v_{k-1}) \in K_{\lambda_k}$. Therefore there exists a vector $v_k \in K_{\lambda_k}$ such that

$$x = v_1 + v_2 + \cdots + v_k. \qquad \blacksquare$$

The next result extends Theorem 5.9(b) (p. 268) to all linear operators whose characteristic polynomials split. In this case, the eigenspaces are replaced by generalized eigenspaces.

Theorem 7.4. *Let T be a linear operator on a finite-dimensional vector space V such that the characteristic polynomial of T splits, and let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of T with corresponding multiplicities $m_1, m_2, \ldots, m_k$. For $1 \le i \le k$, let β_i be an ordered basis for K_{λ_i}. Then the following statements are true.*

(a) $\beta_i \cap \beta_j = \varnothing$ *for* $i \ne j$.
(b) $\beta = \beta_1 \cup \beta_2 \cup \cdots \cup \beta_k$ *is an ordered basis for* V.
(c) $\dim(K_{\lambda_i}) = m_i$ *for all* i.

Proof. (a) Suppose that $x \in \beta_i \cap \beta_j \subseteq K_{\lambda_i} \cap K_{\lambda_j}$, where $i \ne j$. By Theorem 7.1(b), $T - \lambda_i I$ is one-to-one on K_{λ_j}, and therefore $(T - \lambda_i I)^p(x) \ne 0$ for any positive integer p. But this contradicts the fact that $x \in K_{\lambda_i}$, and the result follows.

(b) Let $x \in V$. By Theorem 7.3, for $1 \le i \le k$, there exist vectors $v_i \in K_{\lambda_i}$ such that $x = v_1 + v_2 + \cdots + v_k$. Since each v_i is a linear combination of the vectors of β_i, it follows that x is a linear combination of the vectors of β. Therefore β spans V. Let q be the number of vectors in β. Then $\dim(V) \le q$. For each i, let $d_i = \dim(K_{\lambda_i})$. Then, by Theorem 7.2(a),

$$q = \sum_{i=1}^{k} d_i \le \sum_{i=1}^{k} m_i = \dim(V).$$

Hence $q = \dim(V)$. Consequently β is a basis for V by Corollary 2 to the replacement theorem (p. 47).

(c) Using the notation and result of (b), we see that $\sum_{i=1}^{k} d_i = \sum_{i=1}^{k} m_i$. But $d_i \leq m_i$ by Theorem 7.2(a), and therefore $d_i = m_i$ for all i. ∎

Corollary. *Let T be a linear operator on a finite-dimensional vector space V such that the characteristic polynomial of T splits. Then T is diagonalizable if and only if $\mathsf{E}_\lambda = \mathsf{K}_\lambda$ for every eigenvalue λ of T.*

Proof. Combining Theorems 7.4 and 5.9(a) (p. 268), we see that T is diagonalizable if and only if $\dim(\mathsf{E}_\lambda) = \dim(\mathsf{K}_\lambda)$ for each eigenvalue λ of T. But $\mathsf{E}_\lambda \subseteq \mathsf{K}_\lambda$, and hence these subspaces have the same dimension if and only if they are equal. ∎

We now focus our attention on the problem of selecting suitable bases for the generalized eigenspaces of a linear operator so that we may use Theorem 7.4 to obtain a Jordan canonical basis for the operator. For this purpose, we consider again the basis β of Example 1. We have seen that the first four vectors of β lie in the generalized eigenspace K_2. Observe that the vectors in β that determine the first Jordan block of J are of the form

$$\{v_1, v_2, v_3\} = \{(\mathsf{T} - 2\mathsf{I})^2(v_3), (\mathsf{T} - 2\mathsf{I})(v_3), v_3\}.$$

Furthermore, observe that $(\mathsf{T} - 2\mathsf{I})^3(v_3) = 0$. The relation between these vectors is the key to finding Jordan canonical bases. This leads to the following definitions.

Definitions. *Let T be a linear operator on a vector space V, and let x be a generalized eigenvector of T corresponding to the eigenvalue λ. Suppose that p is the smallest positive integer for which $(\mathsf{T} - \lambda\mathsf{I})^p(x) = 0$. Then the ordered set*

$$\{(\mathsf{T} - \lambda\mathsf{I})^{p-1}(x), (\mathsf{T} - \lambda\mathsf{I})^{p-2}(x), \ldots, (\mathsf{T} - \lambda\mathsf{I})(x), x\}$$

is called a ***cycle of generalized eigenvectors*** *of T corresponding to λ. The vectors $(\mathsf{T} - \lambda\mathsf{I})^{p-1}(x)$ and x are called the* ***initial vector*** *and the* ***end vector*** *of the cycle, respectively. We say that the* ***length*** *of the cycle is p.*

Notice that the initial vector of a cycle of generalized eigenvectors of a linear operator T is the only eigenvector of T in the cycle. Also observe that if x is an eigenvector of T corresponding to the eigenvalue λ, then the set $\{x\}$ is a cycle of generalized eigenvectors of T corresponding to λ of length 1.

In Example 1, the subsets $\beta_1 = \{v_1, v_2, v_3\}$, $\beta_2 = \{v_4\}$, $\beta_3 = \{v_5, v_6\}$, and $\beta_4 = \{v_7, v_8\}$ are the cycles of generalized eigenvectors of T that occur in β. Notice that β is a disjoint union of these cycles. Furthermore, setting $\mathsf{W}_i = \operatorname{span}(\beta_i)$ for $1 \leq i \leq 4$, we see that β_i is a basis for W_i and $[\mathsf{T}_{\mathsf{W}_i}]_{\beta_i}$ is the ith Jordan block of the Jordan canonical form of T. This is precisely the condition that is required for a Jordan canonical basis.

Theorem 7.5. *Let T be a linear operator on a finite-dimensional vector space V whose characteristic polynomial splits, and suppose that β is a basis for V such that β is a disjoint union of cycles of generalized eigenvectors of T. Then the following statements are true.*

(a) *For each cycle γ of generalized eigenvectors contained in β, $\mathsf{W} = \operatorname{span}(\gamma)$ is T-invariant, and $[\mathsf{T}_\mathsf{W}]_\gamma$ is a Jordan block.*

(b) *β is a Jordan canonical basis for V.*

Proof. (a) Suppose that γ corresponds to λ, γ has length p, and x is the end vector of γ. Then $\gamma = \{v_1, v_2, \ldots, v_p\}$, where

$$v_i = (\mathsf{T} - \lambda\mathsf{I})^{p-i}(x) \text{ for } i < p \quad \text{and} \quad v_p = x.$$

So

$$(\mathsf{T} - \lambda\mathsf{I})(v_1) = (\mathsf{T} - \lambda\mathsf{I})^p(x) = 0,$$

and hence $\mathsf{T}(v_1) = \lambda v_1$. For $i > 1$,

$$(\mathsf{T} - \lambda\mathsf{I})(v_i) = (\mathsf{T} - \lambda\mathsf{I})^{p-(i-1)}(x) = v_{i-1}.$$

Therefore T maps W into itself, and, by the preceding equations, we see that $[\mathsf{T}_\mathsf{W}]_\gamma$ is a Jordan block.

For (b), simply repeat the arguments of (a) for each cycle in β in order to obtain $[\mathsf{T}]_\beta$. We leave the details as an exercise. ∎

In view of this result, we must show that, under appropriate conditions, there exist bases that are disjoint unions of cycles of generalized eigenvectors. Since the characteristic polynomial of a Jordan canonical form splits, this is a necessary condition. We will soon see that it is also sufficient. The next result moves us toward the desired existence theorem.

Theorem 7.6. *Let T be a linear operator on a vector space V, and let λ be an eigenvalue of T. Suppose that $\gamma_1, \gamma_2, \ldots, \gamma_q$ are cycles of generalized eigenvectors of T corresponding to λ such that the initial vectors of the γ_i's are distinct and form a linearly independent set. Then the γ_i's are disjoint, and their union $\gamma = \bigcup_{i=1}^{q} \gamma_i$ is linearly independent.*

Proof. Exercise 5 shows that the γ_i's are disjoint.

The proof that γ is linearly independent is by mathematical induction on the number of vectors in γ. If this number is less than 2, then the result is clear. So assume that, for some integer $n > 1$, the result is valid whenever γ has fewer than n vectors, and suppose that γ has exactly n vectors. Let W be the subspace of V generated by γ. Clearly W is $(\mathsf{T} - \lambda\mathsf{I})$-invariant, and $\dim(\mathsf{W}) \leq n$. Let U denote the restriction of $\mathsf{T} - \lambda\mathsf{I}$ to W.

For each i, let γ_i' denote the cycle obtained from γ_i by deleting the end vector. Note that if γ_i has length one, then $\gamma_i' = \varnothing$. In the case that $\gamma_i' \neq \varnothing$, each vector of γ_i' is the image under U of a vector in γ_i, and conversely, every nonzero image under U of a vector of γ_i is contained in γ_i'. Let $\gamma' = \bigcup_i \gamma_i'$. Then by the last statement, γ' generates $\mathsf{R}(\mathsf{U})$. Furthermore, γ' consists of $n - q$ vectors, and the initial vectors of the γ_i''s are also initial vectors of the γ_i's. Thus we may apply the induction hypothesis to conclude that γ' is linearly independent. Therefore γ' is a basis for $\mathsf{R}(\mathsf{U})$. Hence $\dim(\mathsf{R}(\mathsf{U})) = n - q$. Since the q initial vectors of the γ_i's form a linearly independent set and lie in $\mathsf{N}(\mathsf{U})$, we have $\dim(\mathsf{N}(\mathsf{U})) \geq q$. From these inequalities and the dimension theorem, we obtain

$$\begin{aligned} n &\geq \dim(\mathsf{W}) \\ &= \dim(\mathsf{R}(\mathsf{U})) + \dim(\mathsf{N}(\mathsf{U})) \\ &\geq (n-q) + q \\ &= n. \end{aligned}$$

We conclude that $\dim(\mathsf{W}) = n$. Since γ generates W and consists of n vectors, it must be a basis for W. Hence γ is linearly independent. ∎

Corollary. *Every cycle of generalized eigenvectors of a linear operator is linearly independent.*

Theorem 7.7. *Let T be a linear operator on a finite-dimensional vector space V, and let λ be an eigenvalue of T. Then K_λ has an ordered basis consisting of a union of disjoint cycles of generalized eigenvectors corresponding to λ.*

Proof. The proof is by mathematical induction on $n = \dim(\mathsf{K}_\lambda)$. The result is clear for $n = 1$. So suppose that for some integer $n > 1$ the result is valid whenever $\dim(\mathsf{K}_\lambda) < n$, and assume that $\dim(\mathsf{K}_\lambda) = n$. Let U denote the restriction of $\mathsf{T} - \lambda\mathsf{I}$ to K_λ. Then $\mathsf{R}(\mathsf{U})$ is a subspace of K_λ of lesser dimension, and $\mathsf{R}(\mathsf{U})$ is the space of generalized eigenvectors corresponding to λ for the restriction of T to $\mathsf{R}(\mathsf{U})$. Therefore, by the induction hypothesis, there exist disjoint cycles $\gamma_1, \gamma_2, \ldots, \gamma_q$ of generalized eigenvectors of this restriction, and hence of T itself, corresponding to λ for which $\gamma = \bigcup_{i=1}^{q} \gamma_i$ is a basis for $\mathsf{R}(\mathsf{U})$. For $1 \leq i \leq q$, the end vector of γ_i is the image under U of a vector $v_i \in \mathsf{K}_\lambda$, and so we can extend each γ_i to a larger cycle $\tilde{\gamma}_i = \gamma_i \cup \{v_i\}$ of generalized eigenvectors of T corresponding to λ. For $1 \leq i \leq q$, let w_i be the initial vector of $\tilde{\gamma}_i$ (and hence of γ_i). Since $\{w_1, w_2, \ldots, w_q\}$ is a linearly independent subset of E_λ, this set can be extended to a basis $\{w_1, w_2, \ldots, w_q, u_1, u_2, \ldots, u_s\}$

for E_λ. Then $\tilde{\gamma}_1, \tilde{\gamma}_2, \ldots, \tilde{\gamma}_q, \{u_1\}, \{u_2\}, \ldots, \{u_s\}$ are disjoint cycles of generalized eigenvectors of T corresponding to λ such that the initial vectors of these cycles are linearly independent. Therefore their union $\tilde{\gamma}$ is a linearly independent subset of K_λ by Theorem 7.6.

We show that $\tilde{\gamma}$ is a basis for K_λ. Suppose that γ consists of $r = \text{rank}(\mathsf{U})$ vectors. Then $\tilde{\gamma}$ consists of $r + q + s$ vectors. Furthermore, since $\{w_1, w_2, \ldots, w_q, u_1, u_2, \ldots, u_s\}$ is a basis for $\mathsf{E}_\lambda = \mathsf{N}(\mathsf{U})$, it follows that $\text{nullity}(\mathsf{U}) = q + s$. Therefore

$$\dim(\mathsf{K}_\lambda) = \text{rank}(\mathsf{U}) + \text{nullity}(\mathsf{U}) = r + q + s.$$

So $\tilde{\gamma}$ is a linearly independent subset of K_λ containing $\dim(\mathsf{K}_\lambda)$ vectors. It follows that $\tilde{\gamma}$ is a basis for K_λ. ∎

The following corollary is immediate.

Corollary 1. *Let T be a linear operator on a finite-dimensional vector space V whose characteristic polynomial splits. Then T has a Jordan canonical form.*

Proof. Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of T. By Theorem 7.7, for each i there is an ordered basis β_i consisting of a disjoint union of cycles of generalized eigenvectors corresponding to λ_i. Let $\beta = \beta_1 \cup \beta_2 \cup \cdots \cup \beta_k$. Then, by Theorem 7.4(b), β is an ordered basis for V. ∎

The Jordan canonical form also can be studied from the viewpoint of matrices.

Definition. *Let $A \in \mathsf{M}_{n\times n}(F)$ be such that the characteristic polynomial of A (and hence of L_A) splits. Then the* **Jordan canonical form** *of A is defined to be the Jordan canonical form of the linear operator L_A on F^n.*

The next result is an immediate consequence of this definition and Corollary 1.

Corollary 2. *Let A be an $n \times n$ matrix whose characteristic polynomial splits. Then A has a Jordan canonical form J, and A is similar to J.*

Proof. Exercise. ∎

We can now compute the Jordan canonical forms of matrices and linear operators in some simple cases, as is illustrated in the next two examples. The tools necessary for computing the Jordan canonical forms in general are developed in the next section.

Example 2

Let

$$A = \begin{pmatrix} 3 & 1 & -2 \\ -1 & 0 & 5 \\ -1 & -1 & 4 \end{pmatrix} \in \mathsf{M}_{3\times 3}(R).$$

To find the Jordan canonical form for A, we need to find a Jordan canonical basis for $\mathsf{T} = \mathsf{L}_A$.

The characteristic polynomial of A is

$$f(t) = \det(A - tI) = -(t-3)(t-2)^2.$$

Hence $\lambda_1 = 3$ and $\lambda_2 = 2$ are the eigenvalues of A with multiplicities 1 and 2, respectively. By Theorem 7.4, $\dim(\mathsf{K}_{\lambda_1}) = 1$, and $\dim(\mathsf{K}_{\lambda_2}) = 2$. By Theorem 7.2, $\mathsf{K}_{\lambda_1} = \mathsf{N}(\mathsf{T}-3\mathsf{I})$, and $\mathsf{K}_{\lambda_2} = \mathsf{N}((\mathsf{T}-2\mathsf{I})^2)$. Since $\mathsf{E}_{\lambda_1} = \mathsf{N}(\mathsf{T}-3\mathsf{I})$, we have that $\mathsf{E}_{\lambda_1} = \mathsf{K}_{\lambda_1}$. Observe that $(-1,2,1)$ is an eigenvector of T corresponding to $\lambda_1 = 3$; therefore

$$\beta_1 = \left\{ \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix} \right\}$$

is a basis for K_{λ_1}.

Since $\dim(\mathsf{K}_{\lambda_2}) = 2$ and a generalized eigenspace has a basis consisting of a union of cycles, this basis is either a union of two cycles of length 1 or a single cycle of length 2. The former case is impossible because the vectors in the basis would be eigenvectors—contradicting the fact that $\dim(\mathsf{E}_{\lambda_2}) = 1$. Therefore the desired basis is a single cycle of length 2. A vector v is the end vector of such a cycle if and only if $(A-2I)v \neq 0$, but $(A-2I)^2 v = 0$. It can easily be shown that

$$\left\{ \begin{pmatrix} 1 \\ -3 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix} \right\}$$

is a basis for the solution space of the homogeneous system $(A-2I)^2 x = 0$. Now choose a vector v in this set so that $(A-2I)v \neq 0$. The vector $v = (-1,2,0)$ is an acceptable candidate for v. Since $(A-2I)v = (1,-3,-1)$, we obtain the cycle of generalized eigenvectors

$$\beta_2 = \{(A-2I)v, v\} = \left\{ \begin{pmatrix} 1 \\ -3 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix} \right\}$$

as a basis for K_{λ_2}. Finally, we take the union of these two bases to obtain

$$\beta = \beta_1 \cup \beta_2 = \left\{ \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -3 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix} \right\},$$

which is a Jordan canonical basis for A. Therefore,

$$J = [\mathsf{T}]_\beta = \left(\begin{array}{c|cc} 3 & 0 & 0 \\ \hline 0 & 2 & 1 \\ 0 & 0 & 2 \end{array}\right)$$

is a Jordan canonical form for A. Notice that A is similar to J. In fact, $J = Q^{-1}AQ$, where Q is the matrix whose columns are the vectors in β. ♦

Example 3

Let T be the linear operator on $\mathsf{P}_2(R)$ defined by $\mathsf{T}(g(x)) = -g(x) - g'(x)$. We find a Jordan canonical form of T and a Jordan canonical basis for T.

Let β be the standard ordered basis for $\mathsf{P}_2(R)$. Then

$$[\mathsf{T}]_\beta = \begin{pmatrix} -1 & -1 & 0 \\ 0 & -1 & -2 \\ 0 & 0 & -1 \end{pmatrix},$$

which has the characteristic polynomial $f(t) = -(t+1)^3$. Thus $\lambda = -1$ is the only eigenvalue of T, and hence $\mathsf{K}_\lambda = \mathsf{P}_2(R)$ by Theorem 7.4. So β is a basis for K_λ. Now

$$\dim(\mathsf{E}_\lambda) = 3 - \operatorname{rank}(A + I) = 3 - \operatorname{rank} \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -2 \\ 0 & 0 & 0 \end{pmatrix} = 3 - 2 = 1.$$

Therefore a basis for K_λ cannot be a union of two or three cycles because the initial vector of each cycle is an eigenvector, and there do not exist two or more linearly independent eigenvectors. So the desired basis must consist of a single cycle of length 3. If γ is such a cycle, then γ determines a single Jordan block

$$[\mathsf{T}]_\gamma = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix},$$

which is a Jordan canonical form of T.

The end vector $h(x)$ of such a cycle must satisfy $(\mathsf{T} + \mathsf{I})^2(h(x)) \neq 0$. In any basis for K_λ, there must be a vector that satisfies this condition, or else

no vector in K_λ satisfies this condition, contrary to our reasoning. Testing the vectors in β, we see that $h(x) = x^2$ is acceptable. Therefore

$$\gamma = \{(\mathsf{T}+\mathsf{I})^2(x^2), (\mathsf{T}+\mathsf{I})(x^2), x^2\} = \{2, -2x, x^2\}$$

is a Jordan canonical basis for T. ♦

In the next section, we develop a computational approach for finding a Jordan canonical form and a Jordan canonical basis. In the process, we prove that Jordan canonical forms are unique up to the order of the Jordan blocks.

Let T be a linear operator on a finite-dimensional vector space V, and suppose that the characteristic polynomial of T splits. By Theorem 5.11 (p. 278), T is diagonalizable if and only if V is the direct sum of the eigenspaces of T. If T is diagonalizable, then the eigenspaces and the generalized eigenspaces coincide. The next result, which is optional, extends Theorem 5.11 to the nondiagonalizable case.

Theorem 7.8. *Let T be a linear operator on a finite-dimensional vector space V whose characteristic polynomial splits. Then V is the direct sum of the generalized eigenspaces of T.*

Proof. Exercise. ∎

EXERCISES

1. Label the following statements as true or false.
   (a) Eigenvectors of a linear operator T are also generalized eigenvectors of T.
   (b) It is possible for a generalized eigenvector of a linear operator T to correspond to a scalar that is not an eigenvalue of T.
   (c) Any linear operator on a finite-dimensional vector space has a Jordan canonical form.
   (d) A cycle of generalized eigenvectors is linearly independent.
   (e) There is exactly one cycle of generalized eigenvectors corresponding to each eigenvalue of a linear operator on a finite-dimensional vector space.
   (f) Let T be a linear operator on a finite-dimensional vector space whose characteristic polynomial splits, and let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of T. If, for each i, β_i is a basis for K_{λ_i}, then $\beta_1 \cup \beta_2 \cup \cdots \cup \beta_k$ is a Jordan canonical basis for T.
   (g) For any Jordan block J, the operator L_J has Jordan canonical form J.
   (h) Let T be a linear operator on an n-dimensional vector space whose characteristic polynomial splits. Then, for any eigenvalue λ of T, $\mathsf{K}_\lambda = \mathsf{N}((\mathsf{T} - \lambda\mathsf{I})^n)$.

2. For each matrix A, find a basis for each generalized eigenspace of L_A consisting of a union of disjoint cycles of generalized eigenvectors. Then find a Jordan canonical form J of A.

(a) $A = \begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}$ (b) $A = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$

(c) $A = \begin{pmatrix} 11 & -4 & -5 \\ 21 & -8 & -11 \\ 3 & -1 & 0 \end{pmatrix}$ (d) $A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 1 & -1 & 3 \end{pmatrix}$

3. For each linear operator T, find a basis for each generalized eigenspace of T consisting of a union of disjoint cycles of generalized eigenvectors. Then find a Jordan canonical form J of T.

(a) T is the linear operator on $\mathsf{P}_2(R)$ defined by $\mathsf{T}(f(x)) = 2f(x) - f'(x)$

(b) V is the real vector space of functions spanned by the set of real valued functions $\{1, t, t^2, e^t, te^t\}$, and T is the linear operator on V defined by $\mathsf{T}(f) = f'$.

(c) T is the linear operator on $\mathsf{M}_{2\times 2}(R)$ defined by $\mathsf{T}(A) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot A$ for all $A \in \mathsf{M}_{2\times 2}(R)$.

(d) $\mathsf{T}(A) = 2A + A^t$ for all $A \in \mathsf{M}_{2\times 2}(R)$.

4.† Let T be a linear operator on a vector space V, and let γ be a cycle of generalized eigenvectors that corresponds to the eigenvalue λ. Prove that $\text{span}(\gamma)$ is a T-invariant subspace of V.

5. Let $\gamma_1, \gamma_2, \ldots, \gamma_p$ be cycles of generalized eigenvectors of a linear operator T corresponding to an eigenvalue λ. Prove that if the initial eigenvectors are distinct, then the cycles are disjoint.

6. Let $\mathsf{T}: \mathsf{V} \to \mathsf{W}$ be a linear transformation. Prove the following results.

(a) $\mathsf{N}(\mathsf{T}) = \mathsf{N}(-\mathsf{T})$.

(b) $\mathsf{N}(\mathsf{T}^k) = \mathsf{N}((-\mathsf{T})^k)$.

(c) If $\mathsf{V} = \mathsf{W}$ (so that T is a linear operator on V) and λ is an eigenvalue of T, then for any positive integer k

$$\mathsf{N}((\mathsf{T} - \lambda \mathsf{I}_\mathsf{V})^k) = \mathsf{N}((\lambda \mathsf{I}_\mathsf{V} - \mathsf{T})^k).$$

7. Let U be a linear operator on a finite-dimensional vector space V. Prove the following results.

(a) $\mathsf{N}(\mathsf{U}) \subseteq \mathsf{N}(\mathsf{U}^2) \subseteq \cdots \subseteq \mathsf{N}(\mathsf{U}^k) \subseteq \mathsf{N}(\mathsf{U}^{k+1}) \subseteq \cdots$.

(b) If $\text{rank}(\mathsf{U}^m) = \text{rank}(\mathsf{U}^{m+1})$ for some positive integer m, then $\text{rank}(\mathsf{U}^m) = \text{rank}(\mathsf{U}^k)$ for any positive integer $k \geq m$.

(c) If $\text{rank}(\mathsf{U}^m) = \text{rank}(\mathsf{U}^{m+1})$ for some positive integer m, then $\mathsf{N}(\mathsf{U}^m) = \mathsf{N}(\mathsf{U}^k)$ for any positive integer $k \geq m$.

(d) Let T be a linear operator on V, and let λ be an eigenvalue of T. Prove that if $\text{rank}((\mathsf{T}-\lambda\mathsf{I})^m) = \text{rank}((\mathsf{T}-\lambda\mathsf{I})^{m+1})$ for some integer m, then $\mathsf{K}_\lambda = \mathsf{N}((\mathsf{T}-\lambda\mathsf{I})^m)$.

(e) *Second Test for Diagonalizability.* Let T be a linear operator on V whose characteristic polynomial splits, and let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of T. Then T is diagonalizable if and only if $\text{rank}(\mathsf{T}-\lambda_i\mathsf{I}) = \text{rank}((\mathsf{T}-\lambda_i\mathsf{I})^2)$ for $1 \leq i \leq k$.

(f) Use (e) to obtain a simpler proof of Exercise 24 of Section 5.4: If T is a diagonalizable linear operator on a finite-dimensional vector space V and W is a T-invariant subspace of V, then T_W is diagonalizable.

8. Use Theorem 7.4 to prove that the vectors $v_1, v_2, \ldots, v_k$ in the statement of Theorem 7.3 are unique.

9. Let T be a linear operator on a finite-dimensional vector space V whose characteristic polynomial splits.

(a) Prove Theorem 7.5(b).

(b) Suppose that β is a Jordan canonical basis for T, and let λ be an eigenvalue of T. Let $\beta' = \beta \cap \mathsf{K}_\lambda$. Prove that β' is a basis for K_λ.

10. Let T be a linear operator on a finite-dimensional vector space whose characteristic polynomial splits, and let λ be an eigenvalue of T.

(a) Suppose that γ is a basis for K_λ consisting of the union of q disjoint cycles of generalized eigenvectors. Prove that $q \leq \dim(\mathsf{E}_\lambda)$.

(b) Let β be a Jordan canonical basis for T, and suppose that $J = [\mathsf{T}]_\beta$ has q Jordan blocks with λ in the diagonal positions. Prove that $q \leq \dim(\mathsf{E}_\lambda)$.

11. Prove Corollary 2 to Theorem 7.7.

Exercises 12 and 13 are concerned with direct sums of matrices, defined in Section 5.4 on page 320.

12. Prove Theorem 7.8.

13. Let T be a linear operator on a finite-dimensional vector space V such that the characteristic polynomial of T splits, and let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of T. For each i, let J_i be the Jordan canonical form of the restriction of T to K_{λ_i}. Prove that

$$J = J_1 \oplus J_2 \oplus \cdots \oplus J_k$$

is the Jordan canonical form of J.

7.2 THE JORDAN CANONICAL FORM II

For the purposes of this section, we fix a linear operator T on an n-dimensional vector space V such that the characteristic polynomial of T splits. Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of T.

By Theorem 7.7 (p. 490), each generalized eigenspace K_{λ_i} contains an ordered basis β_i consisting of a union of disjoint cycles of generalized eigenvectors corresponding to λ_i. So by Theorems 7.4(b) (p. 487) and 7.5 (p. 489), the union $\beta = \bigcup_{i=1}^{k} \beta_i$ is a Jordan canonical basis for T. For each i, let T_i be the restriction of T to K_{λ_i}, and let $A_i = [\mathsf{T}_i]_{\beta_i}$. Then A_i is the Jordan canonical form of T_i, and

$$J = [\mathsf{T}]_\beta = \begin{pmatrix} A_1 & O & \cdots & O \\ O & A_2 & \cdots & O \\ \vdots & \vdots & & \vdots \\ O & O & \cdots & A_k \end{pmatrix}$$

is the Jordan canonical form of T. In this matrix, each O is a zero matrix of appropriate size.

In this section, we compute the matrices A_i and the bases β_i, thereby computing J and β as well. While developing a method for finding J, it becomes evident that in some sense the matrices A_i are unique.

To aid in formulating the uniqueness theorem for J, we adopt the following convention: The basis β_i for K_{λ_i} will henceforth be ordered in such a way that the cycles appear in order of decreasing length. That is, if β_i is a disjoint union of cycles $\gamma_1, \gamma_2, \ldots, \gamma_{n_i}$ and if the length of the cycle γ_j is p_j, we index the cycles so that $p_1 \geq p_2 \geq \cdots \geq p_{n_i}$. This ordering of the cycles limits the possible orderings of vectors in β_i, which in turn determines the matrix A_i. It is in this sense that A_i is unique. It then follows that the Jordan canonical form for T is unique up to an ordering of the eigenvalues of T. As we will see, there is no uniqueness theorem for the bases β_i or for β. Specifically, we show that for each i, the number n_i of cycles that form β_i, and the length p_j $(j = 1, 2, \ldots, n_i)$ of each cycle, is completely determined by T.

Example 1

To illustrate the discussion above, suppose that, for some i, the ordered basis β_i for K_{λ_i} is the union of four cycles $\beta_i = \gamma_1 \cup \gamma_2 \cup \gamma_3 \cup \gamma_4$ with respective

lengths $p_1 = 3$, $p_2 = 3$, $p_3 = 2$, and $p_4 = 1$. Then

$$A_i = \left(\begin{array}{ccc|ccc|cc|c} \lambda_i & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_i & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_i & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \lambda_i & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda_i & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_i & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & \lambda_i & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_i & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_i \end{array}\right). \quad \blacklozenge$$

To help us visualize each of the matrices A_i and ordered bases β_i, we use an array of dots called a **dot diagram** of T_i, where T_i is the restriction of T to K_{λ_i}. Suppose that β_i is a disjoint union of cycles of generalized eigenvectors $\gamma_1, \gamma_2, \ldots, \gamma_{n_i}$ with lengths $p_1 \geq p_2 \geq \cdots \geq p_{n_i}$, respectively. The dot diagram of T_i contains one dot for each vector in β_i, and the dots are configured according to the following rules.

1. The array consists of n_i columns (one column for each cycle).
2. Counting from left to right, the jth column consists of the p_j dots that correspond to the vectors of γ_j starting with the initial vector at the top and continuing down to the end vector.

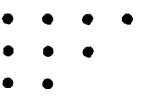
Denote the end vectors of the cycles by $v_1, v_2, \ldots, v_{n_i}$. In the following dot diagram of T_i, each dot is labeled with the name of the vector in β_i to which it corresponds.

$$\begin{array}{llll} \bullet\,(\mathsf{T} - \lambda_i \mathsf{I})^{p_1 - 1}(v_1) & \bullet\,(\mathsf{T} - \lambda_i \mathsf{I})^{p_2 - 1}(v_2) & \cdots & \bullet\,(\mathsf{T} - \lambda_i \mathsf{I})^{p_{n_i} - 1}(v_{n_i}) \\ \bullet\,(\mathsf{T} - \lambda_i \mathsf{I})^{p_1 - 2}(v_1) & \bullet\,(\mathsf{T} - \lambda_i \mathsf{I})^{p_2 - 2}(v_2) & \cdots & \bullet\,(\mathsf{T} - \lambda_i \mathsf{I})^{p_{n_i} - 2}(v_{n_i}) \\ \vdots & \vdots & & \vdots \\ & & & \bullet\,(\mathsf{T} - \lambda_i \mathsf{I})(v_{n_i}) \\ & & & \bullet\, v_{n_i} \\ & \bullet\,(\mathsf{T} - \lambda_i \mathsf{I})(v_2) & & \\ & \bullet\, v_2 & & \\ \bullet\,(\mathsf{T} - \lambda_i \mathsf{I})(v_1) & & & \\ \bullet\, v_1 & & & \end{array}$$

Notice that the dot diagram of T_i has n_i columns (one for each cycle) and p_1 rows. Since $p_1 \geq p_2 \geq \cdots \geq p_{n_i}$, the columns of the dot diagram become shorter (or at least not longer) as we move from left to right.

Now let r_j denote the number of dots in the jth row of the dot diagram. Observe that $r_1 \geq r_2 \geq \cdots \geq r_{p_1}$. Furthermore, the diagram can be reconstructed from the values of the r_i's. The proofs of these facts, which are combinatorial in nature, are treated in Exercise 9.

In Example 1, with $n_i = 4$, $p_1 = p_2 = 3$, $p_3 = 2$, and $p_4 = 1$, the dot diagram of T_i is as follows:



Here $r_1 = 4$, $r_2 = 3$, and $r_3 = 2$.

We now devise a method for computing the dot diagram of T_i using the ranks of linear operators determined by T and λ_i. Hence the dot diagram is completely determined by T, from which it follows that it is unique. On the other hand, β_i is not unique. For example, see Exercise 8. (It is for this reason that we associate the dot diagram with T_i rather than with β_i.)

To determine the dot diagram of T_i, we devise a method for computing each r_j, the number of dots in the jth row of the dot diagram, using only T and λ_i. The next three results give us the required method. To facilitate our arguments, we fix a basis β_i for K_{λ_i} so that β_i is a disjoint union of n_i cycles of generalized eigenvectors with lengths $p_1 \geq p_2 \geq \cdots \geq p_{n_i}$.

Theorem 7.9. *For any positive integer r, the vectors in β_i that are associated with the dots in the first r rows of the dot diagram of T_i constitute a basis for $\mathsf{N}((\mathsf{T} - \lambda_i\mathsf{I})^r)$. Hence the number of dots in the first r rows of the dot diagram equals* $\text{nullity}((\mathsf{T} - \lambda_i\mathsf{I})^r)$.

Proof. Clearly, $\mathsf{N}((\mathsf{T} - \lambda_i\mathsf{I})^r) \subseteq \mathsf{K}_{\lambda_i}$, and K_{λ_i} is invariant under $(\mathsf{T} - \lambda_i\mathsf{I})^r$. Let U denote the restriction of $(\mathsf{T} - \lambda_i\mathsf{I})^r$ to K_{λ_i}. By the preceding remarks, $\mathsf{N}((\mathsf{T} - \lambda_i\mathsf{I})^r) = \mathsf{N}(\mathsf{U})$, and hence it suffices to establish the theorem for U. Now define

$$S_1 = \{x \in \beta_i : \mathsf{U}(x) = 0\} \quad \text{and} \quad S_2 = \{x \in \beta_i : \mathsf{U}(x) \neq 0\}.$$

Let a and b denote the number of vectors in S_1 and S_2, respectively, and let $m_i = \dim(\mathsf{K}_{\lambda_i})$. Then $a + b = m_i$. For any $x \in \beta_i$, $x \in S_1$ if and only if x is one of the first r vectors of a cycle, and this is true if and only if x corresponds to a dot in the first r rows of the dot diagram. Hence a is the number of dots in the first r rows of the dot diagram. For any $x \in S_2$, the effect of applying U to x is to move the dot corresponding to x exactly r places up its column to another dot. It follows that U maps S_2 in a one-to-one fashion into β_i. Thus $\{\mathsf{U}(x) : x \in S_2\}$ is a basis for $\mathsf{R}(\mathsf{U})$ consisting of b vectors. Hence $\text{rank}(\mathsf{U}) = b$, and so $\text{nullity}(\mathsf{U}) = m_i - b = a$. But S_1 is a linearly independent subset of $\mathsf{N}(\mathsf{U})$ consisting of a vectors; therefore S_1 is a basis for $\mathsf{N}(\mathsf{U})$. ∎

In the case that $r = 1$, Theorem 7.9 yields the following corollary.

Corollary. *The dimension of E_{λ_i} is n_i. Hence in a Jordan canonical form of T, the number of Jordan blocks corresponding to λ_i equals the dimension of E_{λ_i}.*

Proof. Exercise. ∎

We are now able to devise a method for describing the dot diagram in terms of the ranks of operators.

Theorem 7.10. *Let r_j denote the number of dots in the jth row of the dot diagram of T_i, the restriction of T to K_{λ_i}. Then the following statements are true.*

(a) $r_1 = \dim(\mathsf{V}) - \operatorname{rank}(\mathsf{T} - \lambda_i \mathsf{I})$.

(b) $r_j = \operatorname{rank}((\mathsf{T} - \lambda_i \mathsf{I})^{j-1}) - \operatorname{rank}((\mathsf{T} - \lambda_i \mathsf{I})^j)$ *if* $j > 1$.

Proof. By Theorem 7.9, for $1 \le j \le p_1$, we have

$$\begin{aligned} r_1 + r_2 + \cdots + r_j &= \operatorname{nullity}((\mathsf{T} - \lambda_i \mathsf{I})^j) \\ &= \dim(\mathsf{V}) - \operatorname{rank}((\mathsf{T} - \lambda_i \mathsf{I})^j). \end{aligned}$$

Hence

$$r_1 = \dim(\mathsf{V}) - \operatorname{rank}(\mathsf{T} - \lambda_i \mathsf{I}),$$

and for $j > 1$,

$$\begin{aligned} r_j &= (r_1 + r_2 + \cdots + r_j) - (r_1 + r_2 + \cdots + r_{j-1}) \\ &= [\dim(\mathsf{V}) - \operatorname{rank}((\mathsf{T} - \lambda_i \mathsf{I})^j)] - [\dim(\mathsf{V}) - \operatorname{rank}((\mathsf{T} - \lambda_i \mathsf{I})^{j-1})] \\ &= \operatorname{rank}((\mathsf{T} - \lambda_i \mathsf{I})^{j-1}) - \operatorname{rank}((\mathsf{T} - \lambda_i \mathsf{I})^j). \end{aligned}$$

∎

Theorem 7.10 shows that the dot diagram of T_i is completely determined by T and λ_i. Hence we have proved the following result.

Corollary. *For any eigenvalue λ_i of T, the dot diagram of T_i is unique. Thus, subject to the convention that the cycles of generalized eigenvectors for the bases of each generalized eigenspace are listed in order of decreasing length, the Jordan canonical form of a linear operator or a matrix is unique up to the ordering of the eigenvalues.*

We apply these results to find the Jordan canonical forms of two matrices and a linear operator.

Example 2

Let

$$A = \begin{pmatrix} 2 & -1 & 0 & 1 \\ 0 & 3 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & 3 \end{pmatrix}.$$

We find the Jordan canonical form of A and a Jordan canonical basis for the linear operator $\mathsf{T} = \mathsf{L}_A$. The characteristic polynomial of A is

$$\det(A - tI) = (t-2)^3(t-3).$$

Thus A has two distinct eigenvalues, $\lambda_1 = 2$ and $\lambda_2 = 3$, with multiplicities 3 and 1, respectively. Let T_1 and T_2 be the restrictions of L_A to the generalized eigenspaces K_{λ_1} and K_{λ_2}, respectively.

Suppose that β_1 is a Jordan canonical basis for T_1. Since λ_1 has multiplicity 3, it follows that $\dim(\mathsf{K}_{\lambda_1}) = 3$ by Theorem 7.4(c) (p. 487); hence the dot diagram of T_1 has three dots. As we did earlier, let r_j denote the number of dots in the jth row of this dot diagram. Then, by Theorem 7.10,

$$r_1 = 4 - \operatorname{rank}(A - 2I) = 4 - \operatorname{rank}\begin{pmatrix} 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix} = 4 - 2 = 2,$$

and

$$r_2 = \operatorname{rank}(A - 2I) - \operatorname{rank}((A - 2I)^2) = 2 - 1 = 1.$$

(Actually, the computation of r_2 is unnecessary in this case because $r_1 = 2$ and the dot diagram only contains three dots.) Hence the dot diagram associated with β_1 is

$$\begin{array}{ll} \bullet & \bullet \\ \bullet & \end{array}$$

So

$$A_1 = [\mathsf{T}_1]_{\beta_1} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Since $\lambda_2 = 3$ has multiplicity 1, it follows that $\dim(\mathsf{K}_{\lambda_2}) = 1$, and consequently any basis β_2 for K_{λ_2} consists of a single eigenvector corresponding to $\lambda_2 = 3$. Therefore

$$A_2 = [\mathsf{T}_2]_{\beta_2} = (3).$$

Setting $\beta = \beta_1 \cup \beta_2$, we have

$$J = [\mathsf{L}_A]_\beta = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix},$$

and so J is the Jordan canonical form of A.

We now find a Jordan canonical basis for $\mathsf{T} = \mathsf{L}_A$. We begin by determining a Jordan canonical basis β_1 for T_1. Since the dot diagram of T_1 has two columns, each corresponding to a cycle of generalized eigenvectors, there are two such cycles. Let v_1 and v_2 denote the end vectors of the first and second cycles, respectively. We reprint below the dot diagram with the dots labeled with the names of the vectors to which they correspond.

$$\begin{matrix} \bullet\,(\mathsf{T}-2\mathsf{I})(v_1) & \bullet\, v_2 \\ \bullet\, v_1 & \end{matrix}$$

From this diagram we see that $v_1 \in \mathsf{N}((\mathsf{T}-2\mathsf{I})^2)$ but $v_1 \notin \mathsf{N}(\mathsf{T}-2\mathsf{I})$. Now

$$A-2I = \begin{pmatrix} 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix} \quad \text{and} \quad (A-2I)^2 = \begin{pmatrix} 0 & -2 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & 1 \end{pmatrix}.$$

It is easily seen that

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 2 \end{pmatrix} \right\}$$

is a basis for $\mathsf{N}((\mathsf{T}-2\mathsf{I})^2) = \mathsf{K}_{\lambda_1}$. Of these three basis vectors, the last two do not belong to $\mathsf{N}(\mathsf{T}-2\mathsf{I})$, and hence we select one of these for v_1. Suppose that we choose

$$v_1 = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix}.$$

Then

$$(\mathsf{T}-2\mathsf{I})(v_1) = (A-2I)(v_1) = \begin{pmatrix} 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \end{pmatrix}.$$

Now simply choose v_2 to be a vector in E_{λ_1} that is linearly independent of $(\mathsf{T}-2\mathsf{I})(v_1)$; for example, select

$$v_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Thus we have associated the Jordan canonical basis

$$\beta_1 = \left\{ \begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

with the dot diagram in the following manner.

$$\bullet \begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \end{pmatrix} \quad \bullet \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\bullet \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix}$$

By Theorem 7.6 (p. 489), the linear independence of β_1 is guaranteed since v_2 was chosen to be linearly independent of $(\mathsf{T} - 2\mathsf{I})(v_1)$.

Since $\lambda_2 = 3$ has multiplicity 1, $\dim(\mathsf{K}_{\lambda_2}) = \dim(\mathsf{E}_{\lambda_2}) = 1$. Hence any eigenvector of L_A corresponding to $\lambda_2 = 3$ constitutes an appropriate basis β_2. For example,

$$\beta_2 = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

Thus

$$\beta = \beta_1 \cup \beta_2 = \left\{ \begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

is a Jordan canonical basis for L_A.

Notice that if

$$Q = \begin{pmatrix} -1 & 0 & 1 & 1 \\ -1 & 1 & 0 & 0 \\ -1 & 2 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix},$$

then $J = Q^{-1}AQ$. ♦

Example 3

Let

$$A = \begin{pmatrix} 2 & -4 & 2 & 2 \\ -2 & 0 & 1 & 3 \\ -2 & -2 & 3 & 3 \\ -2 & -6 & 3 & 7 \end{pmatrix}.$$

We find the Jordan canonical form J of A, a Jordan canonical basis for L_A, and a matrix Q such that $J = Q^{-1}AQ$.

The characteristic polynomial of A is $\det(A - tI) = (t-2)^2(t-4)^2$. Let $\mathsf{T} = \mathsf{L}_A$, $\lambda_1 = 2$, and $\lambda_2 = 4$, and let T_i be the restriction of L_A to K_{λ_i} for $i = 1, 2$.

We begin by computing the dot diagram of T_1. Let r_1 denote the number of dots in the first row of this diagram. Then

$$r_1 = 4 - \operatorname{rank}(A - 2I) = 4 - 2 = 2;$$

hence the dot diagram of T_1 is as follows.

• •

Therefore

$$A_1 = [\mathsf{T}_1]_{\beta_1} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},$$

where β_1 is any basis corresponding to the dots. In this case, β_1 is an arbitrary basis for $\mathsf{E}_{\lambda_1} = \mathsf{N}(\mathsf{T} - 2\mathsf{I})$, for example,

$$\beta_1 = \left\{ \begin{pmatrix} 2 \\ 1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix} \right\}.$$

Next we compute the dot diagram of T_2. Since $\operatorname{rank}(A - 4I) = 3$, there is only $4 - 3 = 1$ dot in the first row of the diagram. Since $\lambda_2 = 4$ has multiplicity 2, we have $\dim(\mathsf{K}_{\lambda_2}) = 2$, and hence this dot diagram has the following form:

•
•

Thus

$$A_2 = [\mathsf{T}_2]_{\beta_2} = \begin{pmatrix} 4 & 1 \\ 0 & 4 \end{pmatrix},$$

where β_2 is any basis for K_{λ_2} corresponding to the dots. In this case, β_2 is a cycle of length 2. The end vector of this cycle is a vector $v \in \mathsf{K}_{\lambda_2} = \mathsf{N}((\mathsf{T} - 4\mathsf{I})^2)$ such that $v \notin \mathsf{N}(\mathsf{T} - 4\mathsf{I})$. One way of finding such a vector was used to select the vector v_1 in Example 2. In this example, we illustrate another method. A simple calculation shows that a basis for the null space of $\mathsf{L}_A - 4\mathsf{I}$ is

$$\left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right\}.$$

Choose v to be any solution to the system of linear equations

$$(A - 4I)x = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix},$$

for example,

$$v = \begin{pmatrix} 1 \\ -1 \\ -1 \\ 0 \end{pmatrix}.$$

Thus

$$\beta_2 = \{(\mathsf{L}_A - 4\mathsf{I})(v), v\} = \left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \\ 0 \end{pmatrix} \right\}.$$

Therefore

$$\beta = \beta_1 \cup \beta_2 = \left\{ \begin{pmatrix} 2 \\ 1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \\ 0 \end{pmatrix} \right\}$$

is a Jordan canonical basis for L_A. The corresponding Jordan canonical form is given by

$$J = [\mathsf{L}_A]_\beta = \begin{pmatrix} A_1 & O \\ O & A_2 \end{pmatrix} = \left(\begin{array}{cc|cc} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 4 \end{array} \right).$$

Finally, we define Q to be the matrix whose columns are the vectors of β listed in the same order, namely,

$$Q = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 1 & 1 & 1 & -1 \\ 0 & 2 & 1 & -1 \\ 2 & 0 & 1 & 0 \end{pmatrix}.$$

Then $J = Q^{-1}AQ$. ♦

Example 4

Let V be the vector space of polynomial functions in two real variables x and y of degree at most 2. Then V is a vector space over R and $\alpha = \{1, x, y, x^2, y^2, xy\}$ is an ordered basis for V. Let T be the linear operator on V defined by

$$\mathsf{T}(f(x,y)) = \frac{\partial}{\partial x} f(x,y).$$

For example, if $f(x,y) = x + 2x^2 - 3xy + y$, then

$$\mathsf{T}(f(x,y)) = \frac{\partial}{\partial x}(x + 2x^2 - 3xy + y) = 1 + 4x - 3y.$$

We find the Jordan canonical form and a Jordan canonical basis for T.

Let $A = [\mathsf{T}]_\alpha$. Then

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

and hence the characteristic polynomial of T is

$$\det(A - tI) = \det \begin{pmatrix} -t & 1 & 0 & 0 & 0 & 0 \\ 0 & -t & 0 & 2 & 0 & 0 \\ 0 & 0 & -t & 0 & 0 & 1 \\ 0 & 0 & 0 & -t & 0 & 0 \\ 0 & 0 & 0 & 0 & -t & 0 \\ 0 & 0 & 0 & 0 & 0 & -t \end{pmatrix} = t^6.$$

Thus $\lambda = 0$ is the only eigenvalue of T, and $\mathsf{K}_\lambda = \mathsf{V}$. For each j, let r_j denote the number of dots in the jth row of the dot diagram of T. By Theorem 7.10,

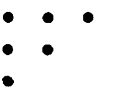
$$r_1 = 6 - \operatorname{rank}(A) = 6 - 3 = 3,$$

and since

$$A^2 = \begin{pmatrix} 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$r_2 = \text{rank}(A) - \text{rank}(A^2) = 3 - 1 = 2$.

Because there are a total of six dots in the dot diagram and $r_1 = 3$ and $r_2 = 2$, it follows that $r_3 = 1$. So the dot diagram of T is



We conclude that the Jordan canonical form of T is

$$J = \left(\begin{array}{ccc|ccc} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

We now find a Jordan canonical basis for T. Since the first column of the dot diagram of T consists of three dots, we must find a polynomial $f_1(x, y)$ such that $\frac{\partial^2}{\partial x^2} f_1(x, y) \neq 0$. Examining the basis $\alpha = \{1, x, y, x^2, y^2, xy\}$ for $\mathsf{K}_\lambda = \mathsf{V}$, we see that x^2 is a suitable candidate. Setting $f_1(x, y) = x^2$, we see that

$$(\mathsf{T} - \lambda \mathsf{I})(f_1(x, y)) = \mathsf{T}(f_1(x, y)) = \frac{\partial}{\partial x}(x^2) = 2x$$

and

$$(\mathsf{T} - \lambda \mathsf{I})^2(f_1(x, y)) = \mathsf{T}^2(f_1(x, y)) = \frac{\partial^2}{\partial x^2}(x^2) = 2.$$

Likewise, since the second column of the dot diagram consists of two dots, we must find a polynomial $f_2(x, y)$ such that

$$\frac{\partial}{\partial x}(f_2(x, y)) \neq 0, \quad \text{but} \quad \frac{\partial^2}{\partial x^2}(f_2(x, y)) = 0.$$

Since our choice must be linearly independent of the polynomials already chosen for the first cycle, the only choice in α that satisfies these constraints is xy. So we set $f_2(x, y) = xy$. Thus

$$(\mathsf{T} - \lambda \mathsf{I})(f_2(x, y)) = \mathsf{T}(f_2(x, y)) = \frac{\partial}{\partial x}(xy) = y.$$

Finally, the third column of the dot diagram consists of a single polynomial that lies in the null space of T. The only remaining polynomial in α is y^2, and it is suitable here. So set $f_3(x, y) = y^2$. Therefore we have identified polynomials with the dots in the dot diagram as follows.

$$\begin{array}{lll} \bullet\, 2 & \bullet\, y & \bullet\, y^2 \\ \bullet\, 2x & \bullet\, xy & \\ \bullet\, x^2 & & \end{array}$$

Thus $\beta = \{2, 2x, x^2, y, xy, y^2\}$ is a Jordan canonical basis for T. ♦

In the three preceding examples, we relied on our ingenuity and the context of the problem to find Jordan canonical bases. The reader can do the same in the exercises. We are successful in these cases because the dimensions of the generalized eigenspaces under consideration are small. We do not attempt, however, to develop a general algorithm for computing Jordan canonical bases, although one could be devised by following the steps in the proof of the existence of such a basis (Theorem 7.7 p. 490).

The following result may be thought of as a corollary to Theorem 7.10.

Theorem 7.11. *Let A and B be $n \times n$ matrices, each having Jordan canonical forms computed according to the conventions of this section. Then A and B are similar if and only if they have (up to an ordering of their eigenvalues) the same Jordan canonical form.*

Proof. If A and B have the same Jordan canonical form J, then A and B are each similar to J and hence are similar to each other.

Conversely, suppose that A and B are similar. Then A and B have the same eigenvalues. Let J_A and J_B denote the Jordan canonical forms of A and B, respectively, with the same ordering of their eigenvalues. Then A is similar to both J_A and J_B, and therefore, by the corollary to Theorem 2.23 (p. 115), J_A and J_B are matrix representations of L_A. Hence J_A and J_B are Jordan canonical forms of L_A. Thus $J_A = J_B$ by the corollary to Theorem 7.10. ∎

Example 5

We determine which of the matrices

$$A = \begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 & -1 \\ -4 & 4 & -2 \\ -2 & 1 & 1 \end{pmatrix},$$

$$C = \begin{pmatrix} 0 & -1 & -1 \\ -3 & -1 & -2 \\ 7 & 5 & 6 \end{pmatrix}, \quad \text{and} \quad D = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

are similar. Observe that A, B, and C have the same characteristic polynomial $-(t-1)(t-2)^2$, whereas D has $-t(t-1)(t-2)$ as its characteristic polynomial. Because similar matrices have the same characteristic polynomials, D cannot be similar to A, B, or C. Let J_A, J_B, and J_C be the Jordan canonical forms of A, B, and C, respectively, using the ordering 1, 2 for their common eigenvalues. Then (see Exercise 4)

$$J_A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}, \quad J_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad \text{and} \quad J_C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Since $J_A = J_C$, A is similar to C. Since J_B is different from J_A and J_C, B is similar to neither A nor C. ◆

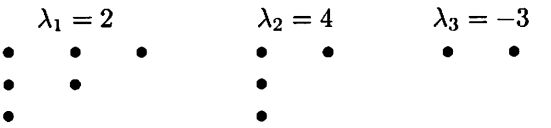
The reader should observe that any diagonal matrix is a Jordan canonical form. Thus a linear operator T on a finite-dimensional vector space V *is diagonalizable if and only if its Jordan canonical form is a diagonal matrix. Hence* T *is diagonalizable if and only if the Jordan canonical basis for* T *consists of eigenvectors of* T. Similar statements can be made about matrices. Thus, of the matrices A, B, and C in Example 5, A and C are not diagonalizable because their Jordan canonical forms are not diagonal matrices.

EXERCISES

1. Label the following statements as true or false. Assume that the characteristic polynomial of the matrix or linear operator splits.

- **(a)** The Jordan canonical form of a diagonal matrix is the matrix itself.
- **(b)** Let T be a linear operator on a finite-dimensional vector space V that has a Jordan canonical form J. If β is any basis for V, then the Jordan canonical form of $[\mathsf{T}]_\beta$ is J.
- **(c)** Linear operators having the same characteristic polynomial are similar.
- **(d)** Matrices having the same Jordan canonical form are similar.
- **(e)** Every matrix is similar to its Jordan canonical form.
- **(f)** Every linear operator with the characteristic polynomial $(-1)^n(t-\lambda)^n$ has the same Jordan canonical form.
- **(g)** Every linear operator on a finite-dimensional vector space has a unique Jordan canonical basis.
- **(h)** The dot diagrams of a linear operator on a finite-dimensional vector space are unique.

2. Let T be a linear operator on a finite-dimensional vector space V such that the characteristic polynomial of T splits. Suppose that $\lambda_1 = 2$, $\lambda_2 = 4$, and $\lambda_3 = -3$ are the distinct eigenvalues of T and that the dot diagrams for the restriction of T to K_{λ_i} $(i = 1, 2, 3)$ are as follows:



Find the Jordan canonical form J of T.

3. Let T be a linear operator on a finite-dimensional vector space V with Jordan canonical form

$$\left(\begin{array}{ccc|cc|cc} 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{array}\right).$$

(a) Find the characteristic polynomial of T.
(b) Find the dot diagram corresponding to each eigenvalue of T.
(c) For which eigenvalues λ_i, if any, does $\mathsf{E}_{\lambda_i} = \mathsf{K}_{\lambda_i}$?
(d) For each eigenvalue λ_i, find the smallest positive integer p_i for which $\mathsf{K}_{\lambda_i} = \mathsf{N}((\mathsf{T} - \lambda_i \mathsf{I})^{p_i})$.
(e) Compute the following numbers for each i, where U_i denotes the restriction of $\mathsf{T} - \lambda_i \mathsf{I}$ to K_{λ_i}.
(i) $\text{rank}(\mathsf{U}_i)$
(ii) $\text{rank}(\mathsf{U}_i^2)$
(iii) $\text{nullity}(\mathsf{U}_i)$
(iv) $\text{nullity}(\mathsf{U}_i^2)$

4. For each of the matrices A that follow, find a Jordan canonical form J and an invertible matrix Q such that $J = Q^{-1}AQ$. Notice that the matrices in (a), (b), and (c) are those used in Example 5.

(a) $A = \begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix}$ **(b)** $A = \begin{pmatrix} 0 & 1 & -1 \\ -4 & 4 & -2 \\ -2 & 1 & 1 \end{pmatrix}$

(c) $A = \begin{pmatrix} 0 & -1 & -1 \\ -3 & -1 & -2 \\ 7 & 5 & 6 \end{pmatrix}$ **(d)** $A = \begin{pmatrix} 0 & -3 & 1 & 2 \\ -2 & 1 & -1 & 2 \\ -2 & 1 & -1 & 2 \\ -2 & -3 & 1 & 4 \end{pmatrix}$

5. For each linear operator T, find a Jordan canonical form J of T and a Jordan canonical basis β for T.

   (a) V is the real vector space of functions spanned by the set of real-valued functions $\{e^t, te^t, t^2e^t, e^{2t}\}$, and T is the linear operator on V defined by $T(f) = f'$.

   (b) T is the linear operator on $P_3(R)$ defined by $T(f(x)) = xf''(x)$.

   (c) T is the linear operator on $P_3(R)$ defined by $T(f(x)) = f''(x) + 2f(x)$.

   (d) T is the linear operator on $M_{2\times 2}(R)$ defined by

$$T(A) = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix} \cdot A - A^t.$$

   (e) T is the linear operator on $M_{2\times 2}(R)$ defined by

$$T(A) = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix} \cdot (A - A^t).$$

   (f) V is the vector space of polynomial functions in two real variables x and y of degree at most 2, as defined in Example 4, and T is the linear operator on V defined by

$$T(f(x,y)) = \frac{\partial}{\partial x} f(x,y) + \frac{\partial}{\partial y} f(x,y).$$

6. Let A be an $n \times n$ matrix whose characteristic polynomial splits. Prove that A and A^t have the same Jordan canonical form, and conclude that A and A^t are similar. *Hint:* For any eigenvalue λ of A and A^t and any positive integer r, show that $\operatorname{rank}((A - \lambda I)^r) = \operatorname{rank}((A^t - \lambda I)^r)$.

7. Let A be an $n \times n$ matrix whose characteristic polynomial splits, γ be a cycle of generalized eigenvectors corresponding to an eigenvalue λ, and W be the subspace spanned by γ. Define γ' to be the ordered set obtained from γ by reversing the order of the vectors in γ.

   (a) Prove that $[T_W]_{\gamma'} = ([T_W]_\gamma)^t$.

   (b) Let J be the Jordan canonical form of A. Use (a) to prove that J and J^t are similar.

   (c) Use (b) to prove that A and A^t are similar.

8. Let T be a linear operator on a finite-dimensional vector space, and suppose that the characteristic polynomial of T splits. Let β be a Jordan canonical basis for T.

   (a) Prove that for any nonzero scalar c, $\{cx : x \in \beta\}$ is a Jordan canonical basis for T.

(b) Suppose that γ is one of the cycles of generalized eigenvectors that forms β, and suppose that γ corresponds to the eigenvalue λ and has length greater than 1. Let x be the end vector of γ, and let y be a nonzero vector in E_λ. Let γ' be the ordered set obtained from γ by replacing x by $x + y$. Prove that γ' is a cycle of generalized eigenvectors corresponding to λ, and that if γ' replaces γ in the union that defines β, then the new union is also a Jordan canonical basis for T.

(c) Apply (b) to obtain a Jordan canonical basis for L_A, where A is the matrix given in Example 2, that is different from the basis given in the example.

9. Suppose that a dot diagram has k columns and m rows with p_j dots in column j and r_i dots in row i. Prove the following results.

(a) $m = p_1$ and $k = r_1$.

(b) $p_j = \max\{i: r_i \geq j\}$ for $1 \leq j \leq k$ and $r_i = \max\{j: p_j \geq i\}$ for $1 \leq i \leq m$. *Hint:* Use mathematical induction on m.

(c) $r_1 \geq r_2 \geq \cdots \geq r_m$.

(d) Deduce that the number of dots in each column of a dot diagram is completely determined by the number of dots in the rows.

10. Let T be a linear operator whose characteristic polynomial splits, and let λ be an eigenvalue of T.

(a) Prove that $\dim(\mathsf{K}_\lambda)$ is the sum of the lengths of all the blocks corresponding to λ in the Jordan canonical form of T.

(b) Deduce that $\mathsf{E}_\lambda = \mathsf{K}_\lambda$ if and only if all the Jordan blocks corresponding to λ are 1×1 matrices.

The following definitions are used in Exercises 11–19.

Definitions. *A linear operator T on a vector space V is called* **nilpotent** *if $\mathsf{T}^p = \mathsf{T}_0$ for some positive integer p. An $n \times n$ matrix A is called* **nilpotent** *if $A^p = O$ for some positive integer p.*

11. Let T be a linear operator on a finite-dimensional vector space V, and let β be an ordered basis for V. Prove that T is nilpotent if and only if $[\mathsf{T}]_\beta$ is nilpotent.

12. Prove that any square upper triangular matrix with each diagonal entry equal to zero is nilpotent.

13. Let T be a nilpotent operator on an n-dimensional vector space V, and suppose that p is the smallest positive integer for which $\mathsf{T}^p = \mathsf{T}_0$. Prove the following results.

(a) $\mathsf{N}(\mathsf{T}^i) \subseteq \mathsf{N}(\mathsf{T}^{i+1})$ for every positive integer i.

(b) There is a sequence of ordered bases $\beta_1, \beta_2, \ldots, \beta_p$ such that β_i is a basis for $\mathsf{N}(\mathsf{T}^i)$ and β_{i+1} contains β_i for $1 \leq i \leq p-1$.
(c) Let $\beta = \beta_p$ be the ordered basis for $\mathsf{N}(\mathsf{T}^p) = \mathsf{V}$ in (b). Then $[\mathsf{T}]_\beta$ is an upper triangular matrix with each diagonal entry equal to zero.
(d) The characteristic polynomial of T is $(-1)^n t^n$. Hence the characteristic polynomial of T splits, and 0 is the only eigenvalue of T.

14. Prove the converse of Exercise 13(d): If T is a linear operator on an n-dimensional vector space V and $(-1)^n t^n$ is the characteristic polynomial of T, then T is nilpotent.

15. Give an example of a linear operator T on a finite-dimensional vector space such that T is not nilpotent, but zero is the only eigenvalue of T. Characterize all such operators.

16. Let T be a nilpotent linear operator on a finite-dimensional vector space V. Recall from Exercise 13 that $\lambda = 0$ is the only eigenvalue of T, and hence $\mathsf{V} = \mathsf{K}_\lambda$. Let β be a Jordan canonical basis for T. Prove that for any positive integer i, if we delete from β the vectors corresponding to the last i dots in each column of a dot diagram of β, the resulting set is a basis for $\mathsf{R}(\mathsf{T}^i)$. (If a column of the dot diagram contains fewer than i dots, all the vectors associated with that column are removed from β.)

17. Let T be a linear operator on a finite-dimensional vector space V such that the characteristic polynomial of T splits, and let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of T. Let $\mathsf{S}: \mathsf{V} \to \mathsf{V}$ be the mapping defined by

$$\mathsf{S}(x) = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k,$$

where, for each i, v_i is the unique vector in K_{λ_i} such that $x = v_1 + v_2 + \cdots + v_k$. (This unique representation is guaranteed by Theorem 7.3 (p. 486) and Exercise 8 of Section 7.1.)

(a) Prove that S is a diagonalizable linear operator on V.
(b) Let $\mathsf{U} = \mathsf{T} - \mathsf{S}$. Prove that U is nilpotent and commutes with S, that is, $\mathsf{SU} = \mathsf{US}$.

18. Let T be a linear operator on a finite-dimensional vector space V, and let J be the Jordan canonical form of T. Let D be the diagonal matrix whose diagonal entries are the diagonal entries of J, and let $M = J - D$. Prove the following results.

(a) M is nilpotent.
(b) $MD = DM$.

(c) If p is the smallest positive integer for which $M^p = O$, then, for any positive integer $r < p$,

$$J^r = D^r + rD^{r-1}M + \frac{r(r-1)}{2!}D^{r-2}M^2 + \cdots + rDM^{r-1} + M^r,$$

and, for any positive integer $r \geq p$,

$$J^r = D^r + rD^{r-1}M + \frac{r(r-1)}{2!}D^{r-2}M^2 + \cdots + \frac{r!}{(r-p+1)!(p-1)!}D^{r-p+1}M^{p-1}.$$

19. Let

$$J = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}$$

be the $m \times m$ Jordan block corresponding to λ, and let $N = J - \lambda I_m$. Prove the following results:

(a) $N^m = O$, and for $1 \leq r < m$,

$$N_{ij}^r = \begin{cases} 1 & \text{if } j = i + r \\ 0 & \text{otherwise.} \end{cases}$$

(b) For any integer $r \geq m$,

$$J^r = \begin{pmatrix} \lambda^r & r\lambda^{r-1} & \frac{r(r-1)}{2!}\lambda^{r-2} & \cdots & \frac{r(r-1)\cdots(r-m+2)}{(m-1)!}\lambda^{r-m+1} \\ 0 & \lambda^r & r\lambda^{r-1} & \cdots & \frac{r(r-1)\cdots(r-m+3)}{(m-2)!}\lambda^{r-m+2} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda^r \end{pmatrix}.$$

(c) $\lim_{r\to\infty} J^r$ exists if and only if one of the following holds:

(i) $|\lambda| < 1$.

(ii) $\lambda = 1$ and $m = 1$.

(Note that $\lim_{r\to\infty} \lambda^r$ exists under these conditions. See the discussion preceding Theorem 5.13 on page 285.) Furthermore, $\lim_{r\to\infty} J^r$ is the zero matrix if condition (i) holds and is the 1×1 matrix (1) if condition (ii) holds.

(d) Prove Theorem 5.13 on page 285.

The following definition is used in Exercises 20 and 21.

Definition. *For any $A \in \mathsf{M}_{n\times n}(C)$, define the norm of A by*

$$\|A\| = \max\{|A_{ij}| : 1 \le i, j \le n\}.$$

20. Let $A, B \in \mathsf{M}_{n\times n}(C)$. Prove the following results.

(a) $\|A\| \ge 0$ and $\|A\| = 0$ if and only if $A = O$.

(b) $\|cA\| = |c| \cdot \|A\|$ for any scalar c.

(c) $\|A + B\| \le \|A\| + \|B\|$.

(d) $\|AB\| \le n\|A\|\|B\|$.

21. Let $A \in \mathsf{M}_{n\times n}(C)$ be a transition matrix. (See Section 5.3.) Since C is an algebraically closed field, A has a Jordan canonical form J to which A is similar. Let P be an invertible matrix such that $P^{-1}AP = J$. Prove the following results.

(a) $\|A^m\| \le 1$ for every positive integer m.

(b) There exists a positive number c such that $\|J^m\| \le c$ for every positive integer m.

(c) Each Jordan block of J corresponding to the eigenvalue $\lambda = 1$ is a 1×1 matrix.

(d) $\lim_{m\to\infty} A^m$ exists if and only if 1 is the only eigenvalue of A with absolute value 1.

(e) Theorem 5.20(a) using (c) and Theorem 5.19.

The next exercise requires knowledge of absolutely convergent series as well as the definition of e^A for a matrix A. (See page 312.)

22. Use Exercise 20(d) to prove that e^A exists for every $A \in \mathsf{M}_{n\times n}(C)$.

23. Let $x' = Ax$ be a system of n linear differential equations, where x is an n-tuple of differentiable functions $x_1(t), x_2(t), \ldots, x_n(t)$ of the real variable t, and A is an $n \times n$ coefficient matrix as in Exercise 15 of Section 5.2. In contrast to that exercise, however, do not assume that A is diagonalizable, but assume that the characteristic polynomial of A splits. Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of A.

(a) Prove that if u is the end vector of a cycle of generalized eigenvectors of L_A of length p and u corresponds to the eigenvalue λ_i, then for any polynomial $f(t)$ of degree less than p, the function

$$e^{\lambda_i t}[f(t)(A-\lambda_i \mathsf{I})^{p-1} + f'(t)(A-\lambda_i \mathsf{I})^{p-2} + \cdots + f^{(p-1)}(t)]u$$

is a solution to the system $x' = Ax$.

(b) Prove that the general solution to $x' = Ax$ is a sum of the functions of the form given in (a), where the vectors u are the end vectors of the distinct cycles that constitute a fixed Jordan canonical basis for L_A.

24. Use Exercise 23 to find the general solution to each of the following systems of linear equations, where x, y, and z are real-valued differentiable functions of the real variable t.

(a)
$$\begin{aligned} x' &= 2x + y \\ y' &= 2y - z \\ z' &= 3z \end{aligned}$$

(b)
$$\begin{aligned} x' &= 2x + y \\ y' &= 2y + z \\ z' &= 2z \end{aligned}$$

7.3 THE MINIMAL POLYNOMIAL

The Cayley-Hamilton theorem (Theorem 5.23 p. 317) tells us that for any linear operator T on an n-dimensional vector space, there is a polynomial $f(t)$ of degree n such that $f(\mathsf{T}) = \mathsf{T}_0$, namely, the characteristic polynomial of T. Hence there is a polynomial of least degree with this property, and this degree is at most n. If $g(t)$ is such a polynomial, we can divide $g(t)$ by its leading coefficient to obtain another polynomial $p(t)$ of the same degree with leading coefficient 1, that is, $p(t)$ is a *monic* polynomial. (See Appendix E.)

Definition. *Let T be a linear operator on a finite-dimensional vector space. A polynomial $p(t)$ is called a* ***minimal polynomial*** *of T if $p(t)$ is a monic polynomial of least positive degree for which $p(\mathsf{T}) = \mathsf{T}_0$.*

The preceding discussion shows that every linear operator on a finite-dimensional vector space has a minimal polynomial. The next result shows that it is unique.

Theorem 7.12. *Let $p(t)$ be a minimal polynomial of a linear operator T on a finite-dimensional vector space V.*

(a) *For any polynomial $g(t)$, if $g(\mathsf{T}) = \mathsf{T}_0$, then $p(t)$ divides $g(t)$. In particular, $p(t)$ divides the characteristic polynomial of T.*

(b) *The minimal polynomial of T is unique.*

Proof. (a) Let $g(t)$ be a polynomial for which $g(\mathsf{T}) = \mathsf{T}_0$. By the division algorithm for polynomials (Theorem E.1 of Appendix E, p. 562), there exist polynomials $q(t)$ and $r(t)$ such that

$$g(t) = q(t)p(t) + r(t), \tag{1}$$

where $r(t)$ has degree less than the degree of $p(t)$. Substituting T into (1) and using that $g(\mathsf{T}) = p(\mathsf{T}) = \mathsf{T}_0$, we have $r(\mathsf{T}) = \mathsf{T}_0$. Since $r(t)$ has degree less than $p(t)$ and $p(t)$ is the minimal polynomial of T, $r(t)$ must be the zero polynomial. Thus (1) simplifies to $g(t) = q(t)p(t)$, proving (a).

(b) Suppose that $p_1(t)$ and $p_2(t)$ are each minimal polynomials of T. Then $p_1(t)$ divides $p_2(t)$ by (a). Since $p_1(t)$ and $p_2(t)$ have the same degree, we have that $p_2(t) = cp_1(t)$ for some nonzero scalar c. Because $p_1(t)$ and $p_2(t)$ are monic, $c = 1$; hence $p_1(t) = p_2(t)$. ∎

The minimal polynomial of a linear operator has an obvious analog for a matrix.

Definition. *Let $A \in \mathsf{M}_{n\times n}(F)$. The* **minimal polynomial** *$p(t)$ of A is the monic polynomial of least positive degree for which $p(A) = O$.*

The following results are now immediate.

Theorem 7.13. *Let T be a linear operator on a finite-dimensional vector space V, and let β be an ordered basis for V. Then the minimal polynomial of T is the same as the minimal polynomial of $[\mathsf{T}]_\beta$.*

Proof. Exercise.. ∎

Corollary. *For any $A \in \mathsf{M}_{n\times n}(F)$, the minimal polynomial of A is the same as the minimal polynomial of L_A.*

Proof. Exercise. ∎

In view of the preceding theorem and corollary, Theorem 7.12 and all subsequent theorems in this section that are stated for operators are also valid for matrices.

For the remainder of this section, we study primarily minimal polynomials of operators (and hence matrices) whose characteristic polynomials split. A more general treatment of minimal polynomials is given in Section 7.4.

Theorem 7.14. *Let T be a linear operator on a finite-dimensional vector space V, and let $p(t)$ be the minimal polynomial of T. A scalar λ is an eigenvalue of T if and only if $p(\lambda) = 0$. Hence the characteristic polynomial and the minimal polynomial of T have the same zeros.*

Proof. Let $f(t)$ be the characteristic polynomial of T. Since $p(t)$ divides $f(t)$, there exists a polynomial $q(t)$ such that $f(t) = q(t)p(t)$. If λ is a zero of $p(t)$, then

$$f(\lambda) = q(\lambda)p(\lambda) = q(\lambda)\cdot 0 = 0.$$

So λ is a zero of $f(t)$; that is, λ is an eigenvalue of T.

Conversely, suppose that λ is an eigenvalue of T, and let $x \in \mathsf{V}$ be an eigenvector corresponding to λ. By Exercise 22 of Section 5.1, we have

$$0 = \mathsf{T}_0(x) = p(\mathsf{T})(x) = p(\lambda)x.$$

Since $x \neq 0$, it follows that $p(\lambda) = 0$, and so λ is a zero of $p(t)$. ∎

The following corollary is immediate.

Corollary. *Let T be a linear operator on a finite-dimensional vector space V with minimal polynomial $p(t)$ and characteristic polynomial $f(t)$. Suppose that $f(t)$ factors as*

$$f(t) = (\lambda_1 - t)^{n_1}(\lambda_2 - t)^{n_2} \cdots (\lambda_k - t)^{n_k},$$

where $\lambda_1, \lambda_2, \ldots, \lambda_k$ are the distinct eigenvalues of T. Then there exist integers $m_1, m_2, \ldots, m_k$ such that $1 \leq m_i \leq n_i$ for all i and

$$p(t) = (t - \lambda_1)^{m_1}(t - \lambda_2)^{m_2} \cdots (t - \lambda_k)^{m_k}.$$

Example 1

We compute the minimal polynomial of the matrix

$$A = \begin{pmatrix} 3 & -1 & 0 \\ 0 & 2 & 0 \\ 1 & -1 & 2 \end{pmatrix}.$$

Since A has the characteristic polynomial

$$f(t) = \det \begin{pmatrix} 3-t & -1 & 0 \\ 0 & 2-t & 0 \\ 1 & -1 & 2-t \end{pmatrix} = -(t-2)^2(t-3),$$

the minimal polynomial of A must be either $(t-2)(t-3)$ or $(t-2)^2(t-3)$ by the corollary to Theorem 7.14. Substituting A into $p(t) = (t-2)(t-3)$, we find that $p(A) = O$; hence $p(t)$ is the minimal polynomial of A. ◆

Example 2

Let T be the linear operator on R^2 defined by

$$\mathsf{T}(a, b) = (2a + 5b, 6a + b)$$

and β be the standard ordered basis for R^2. Then

$$[\mathsf{T}]_\beta = \begin{pmatrix} 2 & 5 \\ 6 & 1 \end{pmatrix},$$

and hence the characteristic polynomial of T is

$$f(t) = \det \begin{pmatrix} 2-t & 5 \\ 6 & 1-t \end{pmatrix} = (t-7)(t+4).$$

Thus the minimal polynomial of T is also $(t-7)(t+4)$. ◆

Example 3

Let D be the linear operator on $\mathsf{P}_2(R)$ defined by $\mathsf{D}(g(x)) = g'(x)$, the derivative of $g(x)$. We compute the minimal polynomial of T. Let β be the standard ordered basis for $\mathsf{P}_2(R)$. Then

$$[\mathsf{D}]_\beta = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix},$$

and it follows that the characteristic polynomial of D is $-t^3$. So by the corollary to Theorem 7.14, the minimal polynomial of D is t, t^2, or t^3. Since $\mathsf{D}^2(x^2) = 2 \neq 0$, it follows that $\mathsf{D}^2 \neq \mathsf{T}_0$; hence the minimal polynomial of D must be t^3. ♦

In Example 3, it is easily verified that $\mathsf{P}_2(R)$ is a D-cyclic subspace (of itself). Here the minimal and characteristic polynomials are of the same degree. This is no coincidence.

Theorem 7.15. *Let T be a linear operator on an n-dimensional vector space V such that V is a T-cyclic subspace of itself. Then the characteristic polynomial $f(t)$ and the minimal polynomial $p(t)$ have the same degree, and hence $f(t) = (-1)^n p(t)$.*

Proof. Since V is a T-cyclic space, there exists an $x \in \mathsf{V}$ such that

$$\beta = \{x, \mathsf{T}(x), \ldots, \mathsf{T}^{n-1}(x)\}$$

is a basis for V (Theorem 5.22 p. 315). Let

$$g(t) = a_0 + a_1 t + \cdots + a_k t^k,$$

be a polynomial of degree $k < n$. Then $a_k \neq 0$ and

$$g(\mathsf{T})(x) = a_0 x + a_1 \mathsf{T}(x) + \cdots + a_k \mathsf{T}^k(x),$$

and so $g(\mathsf{T})(x)$ is a linear combination of the vectors of β having at least one nonzero coefficient, namely, a_k. Since β is linearly independent, it follows that $g(\mathsf{T})(x) \neq 0$; hence $g(\mathsf{T}) \neq \mathsf{T}_0$. Therefore the minimal polynomial of T has degree n, which is also the degree of the characteristic polynomial of T. ∎

Theorem 7.15 gives a condition under which the degree of the minimal polynomial of an operator is as large as possible. We now investigate the other extreme. By Theorem 7.14, the degree of the minimal polynomial of an operator must be greater than or equal to the number of distinct eigenvalues of the operator. The next result shows that the operators for which the degree of the minimal polynomial is as small as possible are precisely the diagonalizable operators.

Theorem 7.16. *Let* T *be a linear operator on a finite-dimensional vector space* V. *Then* T *is diagonalizable if and only if the minimal polynomial of* T *is of the form*

$$p(t) = (t - \lambda_1)(t - \lambda_2) \cdots (t - \lambda_k),$$

where $\lambda_1, \lambda_2, \ldots, \lambda_k$ *are the distinct eigenvalues of* T.

Proof. Suppose that T is diagonalizable. Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of T, and define

$$p(t) = (t - \lambda_1)(t - \lambda_2) \cdots (t - \lambda_k).$$

By Theorem 7.14, $p(t)$ divides the minimal polynomial of T. Let $\beta = \{v_1, v_2, \ldots, v_n\}$ be a basis for V consisting of eigenvectors of T, and consider any $v_i \in \beta$. Then $(\mathsf{T} - \lambda_j \mathsf{I})(v_i) = 0$ for some eigenvalue λ_j. Since $t - \lambda_j$ divides $p(t)$, there is a polynomial $q_j(t)$ such that $p(t) = q_j(t)(t - \lambda_j)$. Hence

$$p(\mathsf{T})(v_i) = q_j(\mathsf{T})(\mathsf{T} - \lambda_j \mathsf{I})(v_i) = 0.$$

It follows that $p(\mathsf{T}) = \mathsf{T}_0$, since $p(\mathsf{T})$ takes each vector in a basis for V into 0. Therefore $p(t)$ is the minimal polynomial of T.

Conversely, suppose that there are distinct scalars $\lambda_1, \lambda_2, \ldots, \lambda_k$ such that the minimal polynomial $p(t)$ of T factors as

$$p(t) = (t - \lambda_1)(t - \lambda_2) \cdots (t - \lambda_k).$$

By Theorem 7.14, the λ_i's are eigenvalues of T. We apply mathematical induction on $n = \dim(\mathsf{V})$. Clearly T is diagonalizable for $n = 1$. Now assume that T is diagonalizable whenever $\dim(\mathsf{V}) < n$ for some $n > 1$, and let $\dim(\mathsf{V}) = n$ and $\mathsf{W} = \mathsf{R}(\mathsf{T} - \lambda_k \mathsf{I})$. Obviously $\mathsf{W} \neq \mathsf{V}$, because λ_k is an eigenvalue of T. If $\mathsf{W} = \{0\}$, then $\mathsf{T} = \lambda_k \mathsf{I}$, which is clearly diagonalizable. So suppose that $0 < \dim(\mathsf{W}) < n$. Then W is T-invariant, and for any $x \in \mathsf{W}$,

$$(\mathsf{T} - \lambda_1 \mathsf{I})(\mathsf{T} - \lambda_2 \mathsf{I}) \cdots (\mathsf{T} - \lambda_{k-1} \mathsf{I})(x) = 0.$$

It follows that the minimal polynomial of T_W divides the polynomial $(t - \lambda_1)(t - \lambda_2) \cdots (t - \lambda_{k-1})$. Hence by the induction hypothesis, T_W is diagonalizable. Furthermore, λ_k is not an eigenvalue of T_W by Theorem 7.14. Therefore $\mathsf{W} \cap \mathsf{N}(\mathsf{T} - \lambda_k \mathsf{I}) = \{0\}$. Now let $\beta_1 = \{v_1, v_2, \ldots, v_m\}$ be a basis for W consisting of eigenvectors of T_W (and hence of T), and let $\beta_2 = \{w_1, w_2, \ldots, w_p\}$ be a basis for $\mathsf{N}(\mathsf{T} - \lambda_k \mathsf{I})$, the eigenspace of T corresponding to λ_k. Then β_1 and β_2 are disjoint by the previous comment. Moreover, $m + p = n$ by the dimension theorem applied to $\mathsf{T} - \lambda_k \mathsf{I}$. We show that $\beta = \beta_1 \cup \beta_2$ is linearly independent. Consider scalars $a_1, a_2, \ldots, a_m$ and $b_1, b_2, \ldots, b_p$ such that

$$a_1 v_1 + a_2 v_2 + \cdots + a_m v_m + b_1 w_1 + b_2 w_2 + \cdots + b_p w_p = 0.$$

Let

$$x = \sum_{i=1}^{m} a_i v_i \qquad \text{and} \qquad y = \sum_{i=1}^{p} b_i w_i.$$

Then $x \in \mathsf{W}$, $y \in \mathsf{N}(\mathsf{T} - \lambda_k \mathsf{I})$, and $x + y = 0$. It follows that $x = -y \in \mathsf{W} \cap \mathsf{N}(\mathsf{T} - \lambda_k \mathsf{I})$, and therefore $x = 0$. Since β_1 is linearly independent, we have that $a_1 = a_2 = \cdots = a_m = 0$. Similarly, $b_1 = b_2 = \cdots = b_p = 0$, and we conclude that β is a linearly independent subset of V consisting of n eigenvectors. It follows that β is a basis for V consisting of eigenvectors of T, and consequently T is diagonalizable. ∎

In addition to diagonalizable operators, there are methods for determining the minimal polynomial of any linear operator on a finite-dimensional vector space. In the case that the characteristic polynomial of the operator splits, the minimal polynomial can be described using the Jordan canonical form of the operator. (See Exercise 13.) In the case that the characteristic polynomial does not split, the minimal polynomial can be described using the *rational canonical form*, which we study in the next section. (See Exercise 7 of Section 7.4.)

Example 4

We determine all matrices $A \in \mathsf{M}_{2\times 2}(R)$ for which $A^2 - 3A + 2I = O$. Let $g(t) = t^2 - 3t + 2 = (t-1)(t-2)$. Since $g(A) = O$, the minimal polynomial $p(t)$ of A divides $g(t)$. Hence the only possible candidates for $p(t)$ are $t-1$, $t-2$, and $(t-1)(t-2)$. If $p(t) = t-1$ or $p(t) = t-2$, then $A = I$ or $A = 2I$, respectively. If $p(t) = (t-1)(t-2)$, then A is diagonalizable with eigenvalues 1 and 2, and hence A is similar to

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}. \quad \blacklozenge$$

Example 5

Let $A \in \mathsf{M}_{n\times n}(R)$ satisfy $A^3 = A$. We show that A is diagonalizable. Let $g(t) = t^3 - t = t(t+1)(t-1)$. Then $g(A) = O$, and hence the minimal polynomial $p(t)$ of A divides $g(t)$. Since $g(t)$ has no repeated factors, neither does $p(t)$. Thus A is diagonalizable by Theorem 7.16. ◆

Example 6

In Example 3, we saw that the minimal polynomial of the differential operator D on $\mathsf{P}_2(R)$ is t^3. Hence, by Theorem 7.16, D is not diagonalizable. ◆

EXERCISES

1. Label the following statements as true or false. Assume that all vector spaces are finite-dimensional.
   (a) Every linear operator T has a polynomial $p(t)$ of largest degree for which $p(\mathsf{T}) = \mathsf{T}_0$.
   (b) Every linear operator has a unique minimal polynomial.
   (c) The characteristic polynomial of a linear operator divides the minimal polynomial of that operator.
   (d) The minimal and the characteristic polynomials of any diagonalizable operator are equal.
   (e) Let T be a linear operator on an n-dimensional vector space V, $p(t)$ be the minimal polynomial of T, and $f(t)$ be the characteristic polynomial of T. Suppose that $f(t)$ splits. Then $f(t)$ divides $[p(t)]^n$.
   (f) The minimal polynomial of a linear operator always has the same degree as the characteristic polynomial of the operator.
   (g) A linear operator is diagonalizable if its minimal polynomial splits.
   (h) Let T be a linear operator on a vector space V such that V is a T-cyclic subspace of itself. Then the degree of the minimal polynomial of T equals $\dim(\mathsf{V})$.
   (i) Let T be a linear operator on a vector space V such that T has n distinct eigenvalues, where $n = \dim(\mathsf{V})$. Then the degree of the minimal polynomial of T equals n.

2. Find the minimal polynomial of each of the following matrices.

   (a) $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

   (c) $\begin{pmatrix} 4 & -14 & 5 \\ 1 & -4 & 2 \\ 1 & -6 & 4 \end{pmatrix}$ (d) $\begin{pmatrix} 3 & 0 & 1 \\ 2 & 2 & 2 \\ -1 & 0 & 1 \end{pmatrix}$

3. For each linear operator T on V, find the minimal polynomial of T.
   (a) $\mathsf{V} = \mathsf{R}^2$ and $\mathsf{T}(a, b) = (a + b, a - b)$
   (b) $\mathsf{V} = \mathsf{P}_2(R)$ and $\mathsf{T}(g(x)) = g'(x) + 2g(x)$
   (c) $\mathsf{V} = \mathsf{P}_2(R)$ and $\mathsf{T}(f(x)) = -xf''(x) + f'(x) + 2f(x)$
   (d) $\mathsf{V} = \mathsf{M}_{n\times n}(R)$ and $\mathsf{T}(A) = A^t$. *Hint:* Note that $\mathsf{T}^2 = \mathsf{I}$.

4. Determine which of the matrices and operators in Exercises 2 and 3 are diagonalizable.

5. Describe all linear operators T on R^2 such that T is diagonalizable and $\mathsf{T}^3 - 2\mathsf{T}^2 + \mathsf{T} = \mathsf{T}_0$.

6. Prove Theorem 7.13 and its corollary.

7. Prove the corollary to Theorem 7.14.

8. Let T be a linear operator on a finite-dimensional vector space, and let $p(t)$ be the minimal polynomial of T. Prove the following results.
   (a) T is invertible if and only if $p(0) \neq 0$.
   (b) If T is invertible and $p(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$, then

$$\mathsf{T}^{-1} = -\frac{1}{a_0}\left(\mathsf{T}^{n-1} + a_{n-1}\mathsf{T}^{n-2} + \cdots + a_2\mathsf{T} + a_1\mathsf{I}\right).$$

9. Let T be a diagonalizable linear operator on a finite-dimensional vector space V. Prove that V is a T-cyclic subspace if and only if each of the eigenspaces of T is one-dimensional.

10. Let T be a linear operator on a finite-dimensional vector space V, and suppose that W is a T-invariant subspace of V. Prove that the minimal polynomial of T_W divides the minimal polynomial of T.

11. Let $g(t)$ be the auxiliary polynomial associated with a homogeneous linear differential equation with constant coefficients (as defined in Section 2.7), and let V denote the solution space of this differential equation. Prove the following results.
   (a) V is a D-invariant subspace, where D is the differentiation operator on C^∞.
   (b) The minimal polynomial of D_V (the restriction of D to V) is $g(t)$.
   (c) If the degree of $g(t)$ is n, then the characteristic polynomial of D_V is $(-1)^n g(t)$.

   Hint: Use Theorem 2.32 (p. 135) for (b) and (c).

12. Let D be the differentiation operator on $\mathsf{P}(R)$, the space of polynomials over R. Prove that there exists no polynomial $g(t)$ for which $g(\mathsf{D}) = \mathsf{T}_0$. Hence D has no minimal polynomial.

13. Let T be a linear operator on a finite-dimensional vector space, and suppose that the characteristic polynomial of T splits. Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of T, and for each i let p_i be the order of the largest Jordan block corresponding to λ_i in a Jordan canonical form of T. Prove that the minimal polynomial of T is

$$(t-\lambda_1)^{p_1}(t-\lambda_2)^{p_2}\cdots(t-\lambda_k)^{p_k}.$$

The following exercise requires knowledge of direct sums (see Section 5.2).

14. Let T be linear operator on a finite-dimensional vector space V, and let W_1 and W_2 be T-invariant subspaces of V such that $V = W_1 \oplus W_2$. Suppose that $p_1(t)$ and $p_2(t)$ are the minimal polynomials of T_{W_1} and T_{W_2}, respectively. Prove or disprove that $p_1(t)p_2(t)$ is the minimal polynomial of T.

Exercise 15 uses the following definition.

Definition. *Let T be a linear operator on a finite-dimensional vector space V, and let x be a nonzero vector in V. The polynomial $p(t)$ is called a* **T-annihilator** *of x if $p(t)$ is a monic polynomial of least degree for which $p(T)(x) = 0$.*

15.† Let T be a linear operator on a finite-dimensional vector space V, and let x be a nonzero vector in V. Prove the following results.

- **(a)** The vector x has a unique T-annihilator.
- **(b)** The T-annihilator of x divides any polynomial $g(t)$ for which $g(T) = T_0$.
- **(c)** If $p(t)$ is the T-annihilator of x and W is the T-cyclic subspace generated by x, then $p(t)$ is the minimal polynomial of T_W, and $\dim(W)$ equals the degree of $p(t)$.
- **(d)** The degree of the T-annihilator of x is 1 if and only if x is an eigenvector of T.

16. T be a linear operator on a finite-dimensional vector space V, and let W_1 be a T-invariant subspace of V. Let $x \in V$ such that $x \notin W_1$. Prove the following results.

- **(a)** There exists a unique monic polynomial $g_1(t)$ of least positive degree such that $g_1(T)(x) \in W_1$.
- **(b)** If $h(t)$ is a polynomial for which $h(T)(x) \in W_1$, then $g_1(t)$ divides $h(t)$.
- **(c)** $g_1(t)$ divides the minimal and the characteristic polynomials of T.
- **(d)** Let W_2 be a T-invariant subspace of V such that $W_2 \subseteq W_1$, and let $g_2(t)$ be the unique monic polynomial of least degree such that $g_2(T)(x) \in W_2$. Then $g_1(t)$ divides $g_2(t)$.

7.4* THE RATIONAL CANONICAL FORM

Until now we have used eigenvalues, eigenvectors, and generalized eigenvectors in our analysis of linear operators with characteristic polynomials that split. In general, characteristic polynomials need not split, and indeed, operators need not have eigenvalues! However, the unique factorization theorem for polynomials (see Appendix E) guarantees that the characteristic polynomial $f(t)$ of any linear operator T on an n-dimensional vector space factors

uniquely as

$$f(t) = (-1)^n(\phi_1(t))^{n_1}(\phi_2(t))^{n_2}\cdots(\phi_k(t))^{n_k},$$

where the $\phi_i(t)$'s $(1 \le i \le k)$ are distinct irreducible monic polynomials and the n_i's are positive integers. In the case that $f(t)$ splits, each irreducible monic polynomial factor is of the form $\phi_i(t) = t - \lambda_i$, where λ_i is an eigenvalue of T, and there is a one-to-one correspondence between eigenvalues of T and the irreducible monic factors of the characteristic polynomial. In general, eigenvalues need not exist, but the irreducible monic factors always exist. In this section, we establish structure theorems based on the irreducible monic factors of the characteristic polynomial instead of eigenvalues.

In this context, the following definition is the appropriate replacement for eigenspace and generalized eigenspace.

Definition. *Let T be a linear operator on a finite-dimensional vector space V with characteristic polynomial*

$$f(t) = (-1)^n(\phi_1(t))^{n_1}(\phi_2(t))^{n_2}\cdots(\phi_k(t))^{n_k},$$

where the $\phi_i(t)$'s $(1 \le i \le k)$ are distinct irreducible monic polynomials and the n_i's are positive integers. For $1 \le i \le k$, we define the subset K_{ϕ_i} of V by

$$\mathsf{K}_{\phi_i} = \{x \in \mathsf{V}\colon (\phi_i(\mathsf{T}))^p(x) = 0 \text{ for some positive integer } p\}.$$

We show that each K_{ϕ_i} is a nonzero T-invariant subspace of V. Note that if $\phi_i(t) = t - \lambda$ is of degree one, then K_{ϕ_i} is the generalized eigenspace of T corresponding to the eigenvalue λ.

Having obtained suitable generalizations of the related concepts of eigenvalue and eigenspace, our next task is to describe a canonical form of a linear operator suitable to this context. The one that we study is called the *rational canonical form*. Since a canonical form is a description of a matrix representation of a linear operator, it can be defined by specifying the form of the ordered bases allowed for these representations.

Here the bases of interest naturally arise from the generators of certain cyclic subspaces. For this reason, the reader should recall the definition of a T-cyclic subspace generated by a vector and Theorem 5.22 (p. 315). We briefly review this concept and introduce some new notation and terminology.

Let T be a linear operator on a finite-dimensional vector space V, and let x be a nonzero vector in V. We use the notation C_x for the T-cyclic subspace generated by x. Recall (Theorem 5.22) that if $\dim(\mathsf{C}_x) = k$, then the set

$$\{x, \mathsf{T}(x), \mathsf{T}^2(x), \ldots, \mathsf{T}^{k-1}(x)\}$$

is an ordered basis for C_x. To distinguish this basis from all other ordered bases for C_x, we call it the **T-cyclic basis generated by x** and denote it by

β_x. Let A be the matrix representation of the restriction of T to C_x relative to the ordered basis β_x. Recall from the proof of Theorem 5.22 that

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{k-1} \end{pmatrix},$$

where

$$a_0 x + a_1 \mathsf{T}(x) + \cdots + a_{k-1}\mathsf{T}^{k-1}(x) + \mathsf{T}^k(x) = 0.$$

Furthermore, the characteristic polynomial of A is given by

$$\det(A - tI) = (-1)^k(a_0 + a_1 t + \cdots + a_{k-1}t^{k-1} + t^k).$$

The matrix A is called the **companion matrix** of the monic polynomial $h(t) = a_0 + a_1 t + \cdots + a_{k-1}t^{k-1} + t^k$. Every monic polynomial has a companion matrix, and the characteristic polynomial of the companion matrix of a monic polynomial $g(t)$ of degree k is equal to $(-1)^k g(t)$. (See Exercise 19 of Section 5.4.) By Theorem 7.15 (p. 519), the monic polynomial $h(t)$ is also the minimal polynomial of A. Since A is the matrix representation of the restriction of T to C_x, $h(t)$ is also the minimal polynomial of this restriction. By Exercise 15 of Section 7.3, $h(t)$ is also the T-annihilator of x.

It is the object of this section to prove that for every linear operator T on a finite-dimensional vector space V, there exists an ordered basis β for V such that the matrix representation $[\mathsf{T}]_\beta$ is of the form

$$\begin{pmatrix} C_1 & O & \cdots & O \\ O & C_2 & \cdots & O \\ \vdots & \vdots & & \vdots \\ O & O & \cdots & C_r \end{pmatrix},$$

where each C_i is the companion matrix of a polynomial $(\phi(t))^m$ such that $\phi(t)$ is a monic irreducible divisor of the characteristic polynomial of T and m is a positive integer. A matrix representation of this kind is called a **rational canonical form** of T. We call the accompanying basis a **rational canonical basis** for T.

The next theorem is a simple consequence of the following lemma, which relies on the concept of T-annihilator, introduced in the Exercises of Section 7.3.

Lemma. *Let T be a linear operator on a finite-dimensional vector space V, let x be a nonzero vector in V, and suppose that the T-annihilator of x is of the form $(\phi(t))^p$ for some irreducible monic polynomial $\phi(t)$. Then $\phi(t)$ divides the minimal polynomial of T, and $x \in \mathsf{K}_\phi$.*

Proof. By Exercise 15(b) of Section 7.3, $(\phi(t))^p$ divides the minimal polynomial of T. Therefore $\phi(t)$ divides the minimal polynomial of T. Furthermore, $x \in \mathsf{K}_\phi$ by the definition of K_ϕ. ∎

Theorem 7.17. *Let* T *be a linear operator on a finite-dimensional vector space* V, *and let* β *be an ordered basis for* V. *Then* β *is a rational canonical basis for* T *if and only if* β *is the disjoint union of* T*-cyclic bases* β_{v_i}, *where each* v_i *lies in* K_ϕ *for some irreducible monic divisor* $\phi(t)$ *of the characteristic polynomial of* T.

Proof. Exercise. ∎

Example 1

Suppose that T is a linear operator on R^8 and

$$\beta = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$$

is a rational canonical basis for T such that

$$C = [\mathsf{T}]_\beta = \left(\begin{array}{cc|cccc|cc} 0 & -3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

is a rational canonical form of T. In this case, the submatrices C_1, C_2, and C_3 are the companion matrices of the polynomials $\phi_1(t)$, $(\phi_2(t))^2$, and $\phi_2(t)$, respectively, where

$$\phi_1(t) = t^2 - t + 3 \quad \text{and} \quad \phi_2(t) = t^2 + 1.$$

In the context of Theorem 7.17, β is the disjoint union of the T-cyclic bases; that is,

$$\begin{aligned} \beta &= \beta_{v_1} \cup \beta_{v_3} \cup \beta_{v_7} \\ &= \{v_1, v_2\} \cup \{v_3, v_4, v_5, v_6\} \cup \{v_7, v_8\}. \end{aligned}$$

By Exercise 40 of Section 5.4, the characteristic polynomial $f(t)$ of T is the product of the characteristic polynomials of the companion matrices:

$$f(t) = \phi_1(t)(\phi_2(t))^2\phi_2(t) = \phi_1(t)(\phi_2(t))^3. \quad \blacklozenge$$

The rational canonical form C of the operator T in Example 1 is constructed from matrices of the form C_i, each of which is the companion matrix of some power of a monic irreducible divisor of the characteristic polynomial of T. Furthermore, each such divisor is used in this way at least once.

In the course of showing that every linear operator T on a finite dimensional vector space has a rational canonical form C, we show that the companion matrices C_i that constitute C are always constructed from powers of the monic irreducible divisors of the characteristic polynomial of T. A key role in our analysis is played by the subspaces K_ϕ, where $\phi(t)$ is an irreducible monic divisor of the minimal polynomial of T. Since the minimal polynomial of an operator divides the characteristic polynomial of the operator, every irreducible divisor of the former is also an irreducible divisor of the latter. We eventually show that the converse is also true; that is, the minimal polynomial and the characteristic polynomial have the same irreducible divisors.

We begin with a result that lists several properties of irreducible divisors of the minimal polynomial. The reader is advised to review the definition of T-annihilator and the accompanying Exercise 15 of Section 7.3.

Theorem 7.18. *Let* T *be a linear operator on a finite-dimensional vector space* V, *and suppose that*

$$p(t) = (\phi_1(t))^{m_1}(\phi_2(t))^{m_2}\cdots(\phi_k(t))^{m_k}$$

is the minimal polynomial of T, *where the* $\phi_i(t)$*'s* $(1 \le i \le k)$ *are the distinct irreducible monic factors of* $p(t)$ *and the* m_i*'s are positive integers. Then the following statements are true.*

(a) K_{ϕ_i} *is a nonzero* T*-invariant subspace of* V *for each* i.
(b) *If* x *is a nonzero vector in some* K_{ϕ_i}, *then the* T*-annihilator of* x *is of the form* $(\phi_i(t))^p$ *for some integer* p.
(c) $\mathsf{K}_{\phi_i} \cap \mathsf{K}_{\phi_j} = \{0\}$ *for* $i \neq j$. .
(d) K_{ϕ_i} *is invariant under* $\phi_j(\mathsf{T})$ *for* $i \neq j$, *and the restriction of* $\phi_j(\mathsf{T})$ *to* K_{ϕ_i} *is one-to-one and onto.*
(e) $\mathsf{K}_{\phi_i} = \mathsf{N}((\phi_i(\mathsf{T}))^{m_i})$ *for each* i.

Proof. If $k = 1$, then (a), (b), and (c) are obvious, while (c) and (d) are vacuously true. Now suppose that $k > 1$.

(a) The proof that K_{ϕ_i} is a T-invariant subspace of V is left as an exercise. Let $f_i(t)$ be the polynomial obtained from $p(t)$ by omitting the factor $(\phi_i(t))^{m_i}$. To prove that K_{ϕ_i} is nonzero, first observe that $f_i(t)$ is a proper divisor of $p(t)$; therefore there exists a vector $z \in \mathsf{V}$ such that $x = f_i(\mathsf{T})(z) \neq 0$. Then $x \in \mathsf{K}_{\phi_i}$ because

$$(\phi_i(\mathsf{T}))^{m_i}(x) = (\phi_i(\mathsf{T}))^{m_i} f_i(\mathsf{T})(z) = p(\mathsf{T})(z) = 0.$$

(b) Assume the hypothesis. Then $(\phi_i(\mathsf{T}))^q(x) = 0$ for some positive integer q. Hence the T-annihilator of x divides $(\phi_i(t))^q$ by Exercise 15(b) of Section 7.3, and the result follows.

(c) Assume $i \neq j$. Let $x \in \mathsf{K}_{\phi_i} \cap \mathsf{K}_{\phi_j}$, and suppose that $x \neq 0$. By (b), the T-annihilator of x is a power of both $\phi_i(t)$ and $\phi_j(t)$. But this is impossible because $\phi_i(t)$ and $\phi_j(t)$ are relatively prime (see Appendix E). We conclude that $x = 0$.

(d) Assume $i \neq j$. Since K_{ϕ_i} is T-invariant, it is also $\phi_j(\mathsf{T})$-invariant. Suppose that $\phi_j(\mathsf{T})(x) = 0$ for some $x \in \mathsf{K}_{\phi_i}$. Then $x \in \mathsf{K}_{\phi_i} \cap \mathsf{K}_{\phi_j} = \{0\}$ by (c). Therefore the restriction of $\phi_j(\mathsf{T})$ to K_{ϕ_i} is one-to-one. Since V is finite-dimensional, this restriction is also onto.

(e) Suppose that $1 \leq i \leq k$. Clearly, $\mathsf{N}((\phi_i(\mathsf{T}))^{m_i}) \subseteq \mathsf{K}_{\phi_i}$. Let $f_i(t)$ be the polynomial defined in (a). Since $f_i(t)$ is a product of polynomials of the form $\phi_j(t)$ for $j \neq i$, we have by (d) that the restriction of $f_i(\mathsf{T})$ to K_{ϕ_i} is onto. Let $x \in \mathsf{K}_{\phi_i}$. Then there exists $y \in \mathsf{K}_{\phi_i}$ such that $f_i(\mathsf{T})(y) = x$. Therefore

$$((\phi_i(\mathsf{T}))^{m_i})(x) = ((\phi_i(\mathsf{T}))^{m_i} f_i(\mathsf{T})(y) = p(\mathsf{T})(y) = 0,$$

and hence $x \in \mathsf{N}((\phi_i(\mathsf{T}))^{m_i})$. Thus $\mathsf{K}_{\phi_i} = \mathsf{N}((\phi_i(\mathsf{T}))^{m_i})$. ∎

Since a rational canonical basis for an operator T is obtained from a union of T-cyclic bases, we need to know when such a union is linearly independent. The next major result, Theorem 7.19, reduces this problem to the study of T-cyclic bases within K_ϕ, where $\phi(t)$ is an irreducible monic divisor of the minimal polynomial of T. We begin with the following lemma.

Lemma. *Let* T *be a linear operator on a finite-dimensional vector space* V, *and suppose that*

$$p(t) = (\phi_1(t))^{m_1}(\phi_2(t))^{m_2} \cdots (\phi_k(t))^{m_k}$$

is the minimal polynomial of T, *where the* ϕ_i*'s* $(1 \leq i \leq k)$ *are the distinct irreducible monic factors of* $p(t)$ *and the* m_i*'s are positive integers. For* $1 \leq i \leq k$, *let* $v_i \in \mathsf{K}_{\phi_i}$ *be such that*

$$v_1 + v_2 + \cdots + v_k = 0. \tag{2}$$

Then $v_i = 0$ *for all* i.

Proof. The result is trivial if $k = 1$, so suppose that $k > 1$. Consider any i. Let $f_i(t)$ be the polynomial obtained from $p(t)$ by omitting the factor $(\phi_i(t))^{m_i}$. As a consequence of Theorem 7.18, $f_i(\mathsf{T})$ is one-to-one on K_{ϕ_i}, and $f_i(\mathsf{T})(v_j) = 0$ for $i \neq j$. Thus, applying $f_i(\mathsf{T})$ to (2), we obtain $f_i(\mathsf{T})(v_i) = 0$, from which it follows that $v_i = 0$. ∎

Theorem 7.19. *Let* T *be a linear operator on a finite-dimensional vector* space V, *and suppose that*

$$p(t) = (\phi_1(t))^{m_1}(\phi_2(t))^{m_2} \cdots (\phi_k(t))^{m_k}$$

is the minimal polynomial of T, *where the* ϕ_i*'s* $(1 \le i \le k)$ *are the distinct irreducible monic factors of* $p(t)$ *and the* m_i*'s are positive integers. For* $1 \le i \le k$, *let* S_i *be a linearly independent subset of* K_{ϕ_i}. *Then*

(a) $S_i \cap S_j = \varnothing$ *for* $i \neq j$

(b) $S_1 \cup S_2 \cup \cdots \cup S_k$ *is linearly independent.*

Proof. If $k = 1$, then (a) is vacuously true and (b) is obvious. Now suppose that $k > 1$. Then (a) follows immediately from Theorem 7.18(c). Furthermore, the proof of (b) is identical to the proof of Theorem 5.8 (p. 267) with the eigenspaces replaced by the subspaces K_{ϕ_i}. ∎

In view of Theorem 7.19, we can focus on bases of individual spaces of the form $\mathsf{K}_{\phi}(t)$, where $\phi(t)$ is an irreducible monic divisor of the minimal polynomial of T. The next several results give us ways to construct bases for these spaces that are unions of T-cyclic bases. These results serve the dual purposes of leading to the existence theorem for the rational canonical form and of providing methods for constructing rational canonical bases.

For Theorems 7.20 and 7.21 and the latter's corollary, we fix a linear operator T on a finite-dimensional vector space V and an irreducible monic divisor $\phi(t)$ of the minimal polynomial of T.

Theorem 7.20. *Let* $v_1, v_2, \ldots, v_k$ *be distinct vectors in* K_{ϕ} *such that*

$$S_1 = \beta_{v_1} \cup \beta_{v_2} \cup \cdots \cup \beta_{v_k}$$

is linearly independent. For each i, *choose* $w_i \in \mathsf{V}$ *such that* $\phi(\mathsf{T})(w_i) = v_i$. *Then*

$$S_2 = \beta_{w_1} \cup \beta_{w_2} \cup \cdots \cup \beta_{w_k}$$

is also linearly independent.

Proof. Consider any linear combination of vectors in S_2 that sums to zero, say,

$$\sum_{i=1}^{k} \sum_{j=0}^{n_i} a_{ij} \mathsf{T}^j(w_i) = 0. \tag{3}$$

For each i, let $f_i(t)$ be the polynomial defined by

$$f_i(t) = \sum_{j=0}^{n_i} a_{ij} t^j.$$

Then (3) can be rewritten as

$$\sum_{i=1}^{k} f_i(\mathsf{T})(w_i) = 0. \tag{4}$$

Apply $\phi(\mathsf{T})$ to both sides of (4) to obtain

$$\sum_{i=1}^{k} \phi(\mathsf{T}) f_i(\mathsf{T})(w_i) = \sum_{i=1}^{k} f_i(\mathsf{T})\phi(\mathsf{T})(w_i) = \sum_{i=1}^{k} f_i(\mathsf{T})(v_i) = 0.$$

This last sum can be rewritten as a linear combination of the vectors in S_1 so that each $f_i(\mathsf{T})(v_i)$ is a linear combination of the vectors in β_{v_i}. Since S_1 is linearly independent, it follows that

$$f_i(\mathsf{T})(v_i) = 0 \quad \text{for all } i.$$

Therefore the T-annihilator of v_i divides $f_i(t)$ for all i. (See Exercise 15 of Section 7.3.) By Theorem 7.18(b), $\phi(t)$ divides the T-annihilator of v_i, and hence $\phi(t)$ divides $f_i(t)$ for all i. Thus, for each i, there exists a polynomial $g_i(t)$ such that $f_i(t) = g_i(t)\phi(t)$. So (4) becomes

$$\sum_{i=1}^{k} g_i(\mathsf{T})\phi(\mathsf{T})(w_i) = \sum_{i=1}^{k} g_i(\mathsf{T})(v_i) = 0.$$

Again, linear independence of S_1 requires that

$$f_i(\mathsf{T})(w_i) = g_i(\mathsf{T})(v_i) = 0 \quad \text{for all } i.$$

But $f_i(\mathsf{T})(w_i)$ is the result of grouping the terms of the linear combination in (3) that arise from the linearly independent set β_{w_i}. We conclude that for each i, $a_{ij} = 0$ for all j. Therefore S_2 is linearly independent. ∎

We now show that K_ϕ has a basis consisting of a union of T-cycles.

Lemma. *Let* W *be a* T*-invariant subspace of* K_ϕ*, and let* β *be a basis for* W*. Then the following statements are true.*

(a) *Suppose that* $x \in \mathsf{N}(\phi(\mathsf{T}))$*, but* $x \notin \mathsf{W}$*. Then* $\beta \cup \beta_x$ *is linearly independent.*

(b) *For some* $w_1, w_2, \ldots, w_s$ *in* $\mathsf{N}(\phi(\mathsf{T}))$*,* β *can be extended to the linearly independent set*

$$\beta' = \beta \cup \beta_{w_1} \cup \beta_{w_2} \cup \cdots \cup \beta_{w_s},$$

whose span contains $\mathsf{N}(\phi(\mathsf{T}))$*.*

Proof. (a) Let $\beta = \{v_1, v_2, \ldots, v_k\}$, and suppose that

$$\sum_{i=1}^{k} a_i v_i + z = 0 \qquad \text{and} \qquad z = \sum_{j=0}^{d-1} b_j \mathsf{T}^j(x),$$

where d is the degree of $\phi(t)$. Then $z \in \mathsf{C}_x \cap \mathsf{W}$, and hence $\mathsf{C}_z \subseteq \mathsf{C}_x \cap \mathsf{W}$. Suppose that $z \neq 0$. Then z has $\phi(t)$ as its T-annihilator, and therefore

$$d = \dim(\mathsf{C}_z) \leq \dim(\mathsf{C}_x \cap \mathsf{W}) \leq \dim(\mathsf{C}_x) = d.$$

It follows that $\mathsf{C}_x \cap \mathsf{W} = \mathsf{C}_x$, and consequently $x \in \mathsf{W}$, contrary to hypothesis. Therefore $z = 0$, from which it follows that $b_j = 0$ for all j. Since β is linearly independent, it follows that $a_i = 0$ for all i. Thus $\beta \cup \beta_x$ is linearly independent.

(b) Suppose that W does not contain $\mathsf{N}(\phi(\mathsf{T}))$. Choose a vector $w_1 \in \mathsf{N}(\phi(t))$ that is not in W. By (a), $\beta_1 = \beta \cup \beta_{w_1}$ is linearly independent. Let $\mathsf{W}_1 = \text{span}(\beta_1)$. If W_1 does not contain $\mathsf{N}(\phi(t))$, choose a vector w_2 in $\mathsf{N}(\phi(t))$, but not in W_1, so that $\beta_2 = \beta_1 \cup \beta_{w_2} = \beta \cup \beta_{w_1} \cup \beta_{w_2}$ is linearly independent. Continuing this process, we eventually obtain vectors $w_1, w_2, \ldots, w_s$ in $\mathsf{N}(\phi(\mathsf{T}))$ such that the union

$$\beta' = \beta \cup \beta_{w_1} \cup \beta_{w_2} \cup \cdots \cup \beta_{w_s}$$

is a linearly independent set whose span contains $\mathsf{N}(\phi(\mathsf{T}))$. ∎

Theorem 7.21. *If the minimal polynomial of* T *is of the form* $p(t) = (\phi(t))^m$, *then there exists a rational canonical basis for* T.

Proof. The proof is by mathematical induction on m. Suppose that $m = 1$. Apply (b) of the lemma to $\mathsf{W} = \{0\}$ to obtain a linearly independent subset of V of the form $\beta_{v_1} \cup \beta_{v_2} \cup \cdots \cup \beta_{v_k}$, whose span contains $\mathsf{N}(\phi(\mathsf{T}))$. Since $\mathsf{V} = \mathsf{N}(\phi(\mathsf{T}))$, this set is a rational canonical basis for V.

Now suppose that, for some integer $m > 1$, the result is valid whenever the minimal polynomial of T is of the form $(\phi(\mathsf{T}))^k$, where $k < m$, and assume that the minimal polynomial of T is $p(t) = (\phi(t))^m$. Let $r = \text{rank}(\phi(\mathsf{T}))$. Then $\mathsf{R}(\phi(\mathsf{T}))$ is a T-invariant subspace of V, and the restriction of T to this subspace has $(\phi(t))^{m-1}$ as its minimal polynomial. Therefore we may apply the induction hypothesis to obtain a rational canonical basis for the restriction of T to $\mathsf{R}(\mathsf{T})$. Suppose that $v_1, v_2, \ldots, v_k$ are the generating vectors of the T-cyclic bases that constitute this rational canonical basis. For each i, choose w_i in V such that $v_i = \phi(\mathsf{T})(w_i)$. By Theorem 7.20, the union β of the sets β_{w_i} is linearly independent. Let $\mathsf{W} = \text{span}(\beta)$. Then W contains $\mathsf{R}(\phi(\mathsf{T}))$. Apply (b) of the lemma and adjoin additional T-cyclic bases $\beta_{w_{k+1}}, \beta_{w_{k+2}}, \ldots, \beta_{w_s}$ to β, if necessary, where w_i is in $\mathsf{N}(\phi(\mathsf{T}))$ for $i \geq k$, to obtain a linearly independent set

$$\beta' = \beta_{w_1} \cup \beta_{w_2} \cup \cdots \cup \beta_{w_k} \cup \cdots \cup \beta_{w_s}$$

whose span W′ contains both W and $\mathsf{N}(\phi(\mathsf{T}))$.

We show that $W' = V$. Let U denote the restriction of $\phi(T)$ to W', which is $\phi(T)$-invariant. By the way in which W' was obtained from $R(\phi(T))$, it follows that $R(U) = R(\phi(T))$ and $N(U) = N(\phi(T))$. Therefore

$$\begin{aligned}\dim(W') &= \operatorname{rank}(U) + \operatorname{nullity}(U)\\ &= \operatorname{rank}(\phi(T)) + \operatorname{nullity}(\phi(T))\\ &= \dim(V).\end{aligned}$$

Thus $W' = V$, and β' is a rational canonical basis for T. ∎

Corollary. *K_ϕ has a basis consisting of the union of T-cyclic bases.*

Proof. Apply Theorem 7.21 to the restriction of T to K_ϕ. ∎

We are now ready to study the general case.

Theorem 7.22. *Every linear operator on a finite-dimensional vector space has a rational canonical basis and, hence, a rational canonical form.*

Proof. Let T be a linear operator on a finite-dimensional vector space V, and let $p(t) = (\phi_1(t))^{m_1}(\phi_2(t))^{m_2}\cdots(\phi_k(t))^{m_k}$ be the minimal polynomial of T, where the $\phi_i(t)$'s are the distinct irreducible monic factors of $p(t)$ and $m_i > 0$ for all i. The proof is by mathematical induction on k. The case $k = 1$ is proved in Theorem 7.21.

Suppose that the result is valid whenever the minimal polynomial contains fewer than k distinct irreducible factors for some $k > 1$, and suppose that $p(t)$ contains k distinct factors. Let U be the restriction of T to the T-invariant subspace $W = R((\phi_k(T)^{m_k})$, and let $q(t)$ be the minimal polynomial of U. Then $q(t)$ divides $p(t)$ by Exercise 10 of Section 7.3. Furthermore, $\phi_k(t)$ does not divide $q(t)$. For otherwise, there would exist a nonzero vector $x \in W$ such that $\phi_k(U)(x) = 0$ and a vector $y \in V$ such that $x = (\phi_k(T))^{m_k}(y)$. It follows that $(\phi_k(T))^{m_k+1}(y) = 0$, and hence $y \in K_{\phi_k}$ and $x = (\phi_k(T))^{m_k}(y) = 0$ by Theorem 7.18(e), a contradiction. Thus $q(t)$ contains fewer than k distinct irreducible divisors. So by the induction hypothesis, U has a rational canonical basis β_1 consisting of a union of U-cyclic bases (and hence T-cyclic bases) of vectors from some of the subspaces K_{ϕ_i}, $1 \le i \le k-1$. By the corollary to Theorem 7.21, K_{ϕ_k} has a basis β_2 consisting of a union of T-cyclic bases. By Theorem 7.19, β_1 and β_2 are disjoint, and $\beta = \beta_1 \cup \beta_2$ is linearly independent. Let s denote the number of vectors in β. Then

$$\begin{aligned}s &= \dim(R((\phi_k(T))^{m_k})) + \dim(K_{\phi_k})\\ &= \operatorname{rank}((\phi_k(T))^{m_k}) + \operatorname{nullity}((\phi_k(T))^{m_k})\\ &= n.\end{aligned}$$

We conclude that β is a basis for V. Therefore β is a rational canonical basis, and T has a rational canonical form. ∎

In our study of the rational canonical form, we relied on the minimal polynomial. We are now able to relate the rational canonical form to the characteristic polynomial.

Theorem 7.23. *Let T be a linear operator on an n-dimensional vector space V with characteristic polynomial*

$$f(t) = (-1)^n(\phi_1(t))^{n_1}(\phi_2(t))^{n_2}\cdots(\phi_k(t))^{n_k},$$

where the $\phi_i(t)$'s $(1 \le i \le k)$ are distinct irreducible monic polynomials and the n_i's are positive integers. Then the following statements are true.

(a) *$\phi_1(t), \phi_2(t), \ldots, \phi_k(t)$ are the irreducible monic factors of the minimal polynomial.*

(b) *For each i, $\dim(\mathsf{K}_{\phi_i}) = d_i n_i$, where d_i is the degree of $\phi_i(t)$.*

(c) *If β is a rational canonical basis for T, then $\beta_i = \beta \cap \mathsf{K}_{\phi_i}$ is a basis for K_{ϕ_i} for each i.*

(d) *If γ_i is a basis for K_{ϕ_i} for each i, then $\gamma = \gamma_1 \cup \gamma_2 \cup \cdots \cup \gamma_k$ is a basis for V. In particular, if each γ_i is a disjoint union of T-cyclic bases, then γ is a rational canonical basis for T.*

Proof. (a) By Theorem 7.22, T has a rational canonical form C. By Exercise 40 of Section 5.4, the characteristic polynomial of C, and hence of T, is the product of the characteristic polynomials of the companion matrices that compose C. Therefore each irreducible monic divisor $\phi_i(t)$ of $f(t)$ divides the characteristic polynomial of at least one of the companion matrices, and hence for some integer p, $(\phi_i(t))^p$ is the T-annihilator of a nonzero vector of V. We conclude that $(\phi_i(t))^p$, and so $\phi_i(t)$, divides the minimal polynomial of T. Conversely, if $\phi(t)$ is an irreducible monic polynomial that divides the minimal polynomial of T, then $\phi(t)$ divides the characteristic polynomial of T because the minimal polynomial divides the characteristic polynomial.

(b), (c), and (d) Let $C = [\mathsf{T}]_\beta$, which is a rational canonical form of T. Consider any i, $(1 \le i \le k)$. Since $f(t)$ is the product of the characteristic polynomials of the companion matrices that compose C, we may multiply those characteristic polynomials that arise from the T-cyclic bases in β_i to obtain the factor $(\phi_i(t))^{n_i}$ of $f(t)$. Since this polynomial has degree $n_i d_i$, and the union of these bases is a linearly independent subset β_i of K_{ϕ_i}, we have

$$n_i d_i \le \dim(\mathsf{K}_{\phi_i}).$$

Furthermore, $n = \sum_{i=1}^{k} d_i n_i$, because this sum is equal to the degree of $f(t)$. Now let s denote the number of vectors in γ. By Theorem 7.19, γ is linearly independent, and therefore

$$n = \sum_{i=1}^{k} d_i n_i \le \sum_{i=1}^{k} \dim(\mathsf{K}_{\phi_i}) = s \le n.$$

Hence $n = s$, and $d_i n_i = \dim(\mathsf{K}_{\phi_i})$ for all i. It follows that γ is a basis for V and β_i is a basis for K_{ϕ_i} for each i. ∎

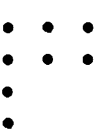
Uniqueness of the Rational Canonical Form

Having shown that a rational canonical form exists, we are now in a position to ask about the extent to which it is unique. Certainly, the rational canonical form of a linear operator T can be modified by permuting the T-cyclic bases that constitute the corresponding rational canonical basis. This has the effect of permuting the companion matrices that make up the rational canonical form. As in the case of the Jordan canonical form, we show that except for these permutations, the rational canonical form is unique, although the rational canonical bases are not.

To simplify this task, we adopt the convention of ordering every rational canonical basis so that all the T-cyclic bases associated with the same irreducible monic divisor of the characteristic polynomial are grouped together. Furthermore, within each such grouping, we arrange the T-cyclic bases in decreasing order of size. Our task is to show that, subject to this order, the rational canonical form of a linear operator is unique up to the arrangement of the irreducible monic divisors.

As in the case of the Jordan canonical form, we introduce arrays of dots from which we can reconstruct the rational canonical form. For the Jordan canonical form, we devised a dot diagram for each eigenvalue of the given operator. In the case of the rational canonical form, we define a dot diagram for each irreducible monic divisor of the characteristic polynomial of the given operator. A proof that the resulting dot diagrams are completely determined by the operator is also a proof that the rational canonical form is unique.

In what follows, T is a linear operator on a finite-dimensional vector space with rational canonical basis β; $\phi(t)$ is an irreducible monic divisor of the characteristic polynomial of T; $\beta_{v_1}, \beta_{v_2}, \ldots, \beta_{v_k}$ are the T-cyclic bases of β that are contained in K_{ϕ}; and d is the degree of $\phi(t)$. For each j, let $(\phi(t))^{p_j}$ be the annihilator of v_j. This polynomial has degree dp_j; therefore, by Exercise 15 of Section 7.3, β_{v_j} contains dp_j vectors. Furthermore, $p_1 \geq p_2 \geq \cdots \geq p_k$ since the T-cyclic bases are arranged in decreasing order of size. We define the **dot diagram** of $\phi(t)$ to be the array consisting of k columns of dots with p_j dots in the jth column, arranged so that the jth column begins at the top and terminates after p_j dots. For example, if $k = 3$, $p_1 = 4$, $p_2 = 2$, and $p_3 = 2$, then the dot diagram is



Although each column of a dot diagram corresponds to a T-cyclic basis

β_{v_i} in K_ϕ, there are fewer dots in the column than there are vectors in the basis.

Example 2

Recall the linear operator T of Example 1 with the rational canonical basis β and the rational canonical form $C = [\mathsf{T}]_\beta$. Since there are two irreducible monic divisors of the characteristic polynomial of T, $\phi_1(t) = t^2 - t + 3$ and $\phi_2(t) = t^2 + 1$, there are two dot diagrams to consider. Because $\phi_1(t)$ is the T-annihilator of v_1 and β_{v_1} is a basis for K_{ϕ_1}, the dot diagram for $\phi_1(t)$ consists of a single dot. The other two T cyclic bases, β_{v_3} and β_{v_7}, lie in K_{ϕ_2}. Since v_3 has T-annihilator $(\phi_2(t))^2$ and v_7 has T-annihilator $\phi_2(t)$, in the dot diagram of $\phi_2(t)$ we have $p_1 = 2$ and $p_2 = 1$. These diagrams are as follows:

Dot diagram for $\phi_1(t)$ Dot diagram for $\phi_2(t)$ ♦

In practice, we obtain the rational canonical form of a linear operator from the information provided by dot diagrams. This is illustrated in the next example.

Example 3

Let T be a linear operator on a finite-dimensional vector space over R, and suppose that the irreducible monic divisors of the characteristic polynomial of T are

$$\phi_1(t) = t - 1, \quad \phi_2(t) = t^2 + 2, \quad \text{and} \quad \phi_3(t) = t^2 + t + 1.$$

Suppose, furthermore, that the dot diagrams associated with these divisors are as follows:

Diagram for $\phi_1(t)$ Diagram for $\phi_2(t)$ Diagram for $\phi_3(t)$

Since the dot diagram for $\phi_1(t)$ has two columns, it contributes two companion matrices to the rational canonical form. The first column has two dots, and therefore corresponds to the 2×2 companion matrix of $(\phi_1(t))^2 = (t-1)^2$. The second column, with only one dot, corresponds to the 1×1 companion matrix of $\phi_1(t) = t - 1$. These two companion matrices are given by

$$C_1 = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} \quad \text{and} \quad C_2 = \begin{pmatrix} 1 \end{pmatrix}.$$

The dot diagram for $\phi_2(t) = t^2 + 2$ consists of two columns. each containing a single dot; hence this diagram contributes two copies of the 2×2 companion

matrix for $\phi_2(t)$, namely,

$$C_3 = C_4 = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}.$$

The dot diagram for $\phi_3(t) = t^2 + t + 1$ consists of a single column with a single dot contributing the single 2×2 companion matrix

$$C_5 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Therefore the rational canonical form of T is the 9×9 matrix

$$C = \begin{pmatrix} C_1 & O & O & O & O \\ O & C_2 & O & O & O \\ O & O & C_3 & O & O \\ O & O & O & C_4 & O \\ O & O & O & O & C_5 \end{pmatrix}$$

$$= \left(\begin{array}{cc|ccccccc} 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{array}\right). \quad \blacklozenge$$

We return to the general problem of finding dot diagrams. As we did before, we fix a linear operator T on a finite-dimensional vector space and an irreducible monic divisor $\phi(t)$ of the characteristic polynomial of T. Let U denote the restriction of the linear operator $\phi(\mathsf{T})$ to K_ϕ. By Theorem 7.18(d), $\mathsf{U}^q = \mathsf{T}_0$ for some positive integer q. Consequently, by Exercise 12 of Section 7.2, the characteristic polynomial of U is $(-1)^m t^m$, where $m = \dim(\mathsf{K}_\phi)$. Therefore K_ϕ is the generalized eigenspace of U corresponding to $\lambda = 0$, and U has a Jordan canonical form. The dot diagram associated with the Jordan canonical form of U gives us a key to understanding the dot diagram of T that is associated with $\phi(t)$. We now relate the two diagrams.

Let β be a rational canonical basis for T, and $\beta_{v_1}, \beta_{v_2}, \ldots, \beta_{v_k}$ be the T-cyclic bases of β that are contained in K_ϕ. Consider one of these T-cyclic bases β_{v_j}, and suppose again that the T-annihilator of v_j is $(\phi(t))^{p_j}$. Then β_{v_j} consists of dp_j vectors in β. For $0 \le i < d$, let γ_i be the cycle of generalized eigenvectors of U corresponding to $\lambda = 0$ with end vector $\mathsf{T}^i(v_j)$,

where $\mathsf{T}^0(v_j) = b_j$. Then

$$\gamma_i = \{(\phi(\mathsf{T}))^{p_j-1}\mathsf{T}^i(v_j), (\phi(\mathsf{T}))^{p_j-2}\mathsf{T}^i(v_j), \ldots, (\phi(\mathsf{T}))\mathsf{T}^i(v_j), \mathsf{T}^i(v_j)\}.$$

By Theorem 7.1 (p. 485), γ_i is a linearly independent subset of C_{v_i}. Now let

$$\alpha_j = \gamma_0 \cup \gamma_1 \cup \cdots \cup \gamma_{d-1}.$$

Notice that α_j contains $p_j d$ vectors.

Lemma 1. *α_j is an ordered basis for C_{v_j}.*

Proof. The key to this proof is Theorem 7.4 (p. 487). Since α_j is the union of cycles of generalized eigenvectors of U corresponding to $\lambda = 0$, it suffices to show that the set of initial vectors of these cycles

$$\{(\phi(\mathsf{T}))^{p_j-1}(v_j), (\phi(\mathsf{T}))^{p_j-1}\mathsf{T}(v_j), \ldots, (\phi(\mathsf{T}))^{p_j-1}\mathsf{T}^{d-1}(v_j)\}$$

is linearly independent. Consider any linear combination of these vectors

$$a_0(\phi(\mathsf{T}))^{p_j-1}(v_j) + a_1(\phi(\mathsf{T}))^{p_j-1}\mathsf{T}(v_j) + \cdots + a_{d-1}(\phi(\mathsf{T}))^{p_j-1}\mathsf{T}^{d-1}(v_j),$$

where not all of the coefficients are zero. Let $g(t)$ be the polynomial defined by $g(t) = a_0 + a_1 t + \cdots + a_{d-1}t^{d-1}$. Then $g(t)$ is a nonzero polynomial of degree less than d, and hence $(\phi(t))^{p_j-1}g(t)$ is a nonzero polynomial with degree less than $p_j d$. Since $(\phi(t))^{p_j}$ is the T-annihilator of v_j, it follows that $(\phi(\mathsf{T}))^{p_j-1}g(\mathsf{T})(v_j) \neq 0$. Therefore the set of initial vectors is linearly independent. So by Theorem 7.4, α_j is linearly independent, and the γ_i's are disjoint. Consequently, α_j consists of $p_j d$ linearly independent vectors in C_{v_j}, which has dimension $p_j d$. We conclude that α_j is a basis for C_{v_j}. ∎

Thus we may replace β_{v_j} by α_j as a basis for C_{v_j}. We do this for each j to obtain a subset $\alpha = \alpha_1 \cup \alpha_2 \cdots \cup \alpha_k$ of K_ϕ.

Lemma 2. *α is a Jordan canonical basis for K_ϕ.*

Proof. Since $\beta_{v_1} \cup \beta_{v_2} \cup \cdots \cup \beta_{v_k}$ is a basis for K_ϕ, and since $\text{span}(\alpha_i) = \text{span}(\beta_{v_i}) = \mathsf{C}_{v_i}$, Exercise 9 implies that α is a basis for K_ϕ. Because α is a union of cycles of generalized eigenvectors of U, we conclude that α is a Jordan canonical basis. ∎

We are now in a position to relate the dot diagram of T corresponding to $\phi(t)$ to the dot diagram of U, bearing in mind that in the first case we are considering a rational canonical form and in the second case we are considering a Jordan canonical form. For convenience, we designate the first diagram D_1, and the second diagram D_2. For each j, the presence of the T-cyclic basis β_{x_j} results in a column of p_j dots in D_1. By Lemma 1, this basis is

replaced by the union α_j of d cycles of generalized eigenvectors of U, each of length p_j, which becomes part of the Jordan canonical basis for U. In effect, α_j determines d columns each containing p_j dots in D_2. So each column in D_1 determines d columns in D_2 of the same length, and all columns in D_2 are obtained in this way. Alternatively, each row in D_2 has d times as many dots as the corresponding row in D_1. Since Theorem 7.10 (p. 500) gives us the number of dots in any row of D_2, we may divide the appropriate expression in this theorem by d to obtain the number of dots in the corresponding row of D_1. Thus we have the following result.

Theorem 7.24. *Let* T *be a linear operator on a finite-dimensional vector space* V, *let* $\phi(t)$ *be an irreducible monic divisor of the characteristic polynomial of* T *of degree* d, *and let* r_i *denote the number of dots in the* i*th row of the dot diagram for* $\phi(t)$ *with respect to a rational canonical basis for* T. *Then*

(a) $r_1 = \frac{1}{d}[\dim(\mathsf{V}) - \operatorname{rank}(\phi(\mathsf{T}))]$

(b) $r_i = \frac{1}{d}[\operatorname{rank}((\phi(\mathsf{T}))^{i-1}) - \operatorname{rank}((\phi(\mathsf{T}))^i)]$ *for* $i > 1$.

Thus the dot diagrams associated with a rational canonical form of an operator are completely determined by the operator. Since the rational canonical form is completely determined by its dot diagrams, we have the following uniqueness condition.

Corollary. *Under the conventions described earlier, the rational canonical form of a linear operator is unique up to the arrangement of the irreducible monic divisors of the characteristic polynomial.*

Since the rational canonical form of a linear operator is unique, the polynomials corresponding to the companion matrices that determine this form are also unique. These polynomials, which are powers of the irreducible monic divisors, are called the **elementary divisors** of the linear operator. Since a companion matrix may occur more than once in a rational canonical form, the same is true for the elementary divisors. We call the number of such occurrences the **multiplicity** of the elementary divisor.

Conversely, the elementary divisors and their multiplicities determine the companion matrices and, therefore, the rational canonical form of a linear operator.

Example 4

Let

$$\beta = \{e^x \cos 2x, e^x \sin 2x, xe^x \cos 2x, xe^x \sin 2x\}$$

be viewed as a subset of $\mathcal{F}(R, R)$, the space of all real-valued functions defined on R, and let $\mathsf{V} = \text{span}(\beta)$. Then V is a four-dimensional subspace of $\mathcal{F}(R, R)$, and β is an ordered basis for V. Let D be the linear operator on V defined by $\mathsf{D}(y) = y'$, the derivative of y, and let $A = [\mathsf{D}]_\beta$. Then

$$A = \begin{pmatrix} 1 & 2 & 1 & 0 \\ -2 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & -2 & 1 \end{pmatrix},$$

and the characteristic polynomial of D, and hence of A, is

$$f(t) = (t^2 - 2t + 5)^2.$$

Thus $\phi(t) = t^2 - 2t + 5$ is the only irreducible monic divisor of $f(t)$. Since $\phi(t)$ has degree 2 and V is four-dimensional, the dot diagram for $\phi(t)$ contains only two dots. Therefore the dot diagram is determined by r_1, the number of dots in the first row. Because ranks are preserved under matrix representations, we can use A in place of D in the formula given in Theorem 7.24. Now

$$\phi(A) = \begin{pmatrix} 0 & 0 & 0 & 4 \\ 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and so

$$r_1 = \tfrac{1}{2}[4 - \text{rank}(\phi(A))] = \tfrac{1}{2}[4 - 2] = 1.$$

It follows that the second dot lies in the second row, and the dot diagram is as follows:

Hence V is a D-cyclic space generated by a single function with D-annihilator $(\phi(t))^2$. Furthermore, its rational canonical form is given by the companion matrix of $(\phi(t))^2 = t^4 - 4t^3 + 14t^2 - 20t + 25$, which is

$$\begin{pmatrix} 0 & 0 & 0 & -25 \\ 1 & 0 & 0 & 20 \\ 0 & 1 & 0 & -14 \\ 0 & 0 & 1 & 4 \end{pmatrix}.$$

Thus $(\phi(t))^2$ is the only elementary divisor of D, and it has multiplicity 1. For the cyclic generator, it suffices to find a function g in V for which $\phi(\mathsf{D})(g) \neq 0$.

Since $\phi(A)(e_3) \neq 0$, it follows that $\phi(\mathsf{D})(xe^x \cos 2x) \neq 0$; therefore $g(x) = xe^x \cos 2x$ can be chosen as the cyclic generator. Hence

$$\beta_g = \{xe^x \cos 2x, \mathsf{D}(xe^x \cos 2x), \mathsf{D}^2(xe^x \cos 2x), \mathsf{D}^3(xe^x \cos 2x)\}$$

is a rational canonical basis for D. Notice that the function h defined by $h(x) = xe^x \sin 2x$ can be chosen in place of g. This shows that the rational canonical basis is not unique. ♦

It is convenient to refer to the rational canonical form and elementary divisors of a matrix, which are defined in the obvious way.

Definitions. *Let $A \in \mathsf{M}_{n\times n}(F)$. The* ***rational canonical form*** *of A is defined to be the rational canonical form of L_A. Likewise, for A, the* ***elementary divisors*** *and their* ***multiplicities*** *are the same as those of L_A.*

Let A be an $n \times n$ matrix, let C be a rational canonical form of A, and let β be the appropriate rational canonical basis for L_A. Then $C = [\mathsf{L}_A]_\beta$, and therefore A is similar to C. In fact, if Q is the matrix whose columns are the vectors of β in the same order, then $Q^{-1}AQ = C$.

Example 5

For the following real matrix A, we find the rational canonical form C of A and a matrix Q such that $Q^{-1}AQ = C$.

$$A = \begin{pmatrix} 0 & 2 & 0 & -6 & 2 \\ 1 & -2 & 0 & 0 & 2 \\ 1 & 0 & 1 & -3 & 2 \\ 1 & -2 & 1 & -1 & 2 \\ 1 & -4 & 3 & -3 & 4 \end{pmatrix}$$

The characteristic polynomial of A is $f(t) = -(t^2 + 2)^2(t - 2)$; therefore $\phi_1(t) = t^2 + 2$ and $\phi_2(t) = t - 2$ are the distinct irreducible monic divisors of $f(t)$. By Theorem 7.23, $\dim(\mathsf{K}_{\phi_1}) = 4$ and $\dim(\mathsf{K}_{\phi_2}) = 1$. Since the degree of $\phi_1(t)$ is 2, the total number of dots in the dot diagram of $\phi_1(t)$ is $4/2 = 2$, and the number of dots r_1 in the first row is given by

$$\begin{aligned} r_1 &= \tfrac{1}{2}[\dim(\mathsf{R}^5) - \operatorname{rank}(\phi_1(A))] \\ &= \tfrac{1}{2}[5 - \operatorname{rank}(A^2 + 2I)] \\ &= \tfrac{1}{2}[5 - 1] = 2. \end{aligned}$$

Thus the dot diagram of $\phi_1(t)$ is

• •

and each column contributes the companion matrix

$$\begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}$$

for $\phi_1(t) = t^2 + 2$ to the rational canonical form C. Consequently $\phi_1(t)$ is an elementary divisor with multiplicity 2. Since $\dim(\mathsf{K}_{\phi_2}) = 1$, the dot diagram of $\phi_2(t) = t - 2$ consists of a single dot, which contributes the 1×1 matrix $\begin{pmatrix} 2 \end{pmatrix}$. Hence $\phi_2(t)$ is an elementary divisor with multiplicity 1. Therefore the rational canonical form C is

$$C = \left(\begin{array}{cc|ccc} 0 & -2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 2 \end{array}\right).$$

We can infer from the dot diagram of $\phi_1(t)$ that if β is a rational canonical basis for L_A, then $\beta \cap \mathsf{K}_{\phi_1}$ is the union of two cyclic bases β_{v_1} and β_{v_2}, where v_1 and v_2 each have annihilator $\phi_1(t)$. It follows that both v_1 and v_2 lie in $\mathsf{N}(\phi_1(\mathsf{L}_A))$. It can be shown that

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0 \\ 1 \end{pmatrix} \right\}$$

is a basis for $\mathsf{N}(\phi_1(\mathsf{L}_A))$. Setting $v_1 = e_1$, we see that

$$Av_1 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Next choose v_2 in $\mathsf{K}_{\phi_1} = \mathsf{N}(\phi(\mathsf{L}_A))$, but not in the span of $\beta_{v_1} = \{v_1, Av_1\}$. For example, $v_2 = e_2$. Then it can be seen that

$$Av_2 = \begin{pmatrix} 2 \\ -2 \\ 0 \\ -2 \\ -4 \end{pmatrix},$$

and $\beta_{v_1} \cup \beta_{v_2}$ is a basis for K_{ϕ_1}.

Since the dot diagram of $\phi_2(t) = t-2$ consists of a single dot, any nonzero vector in K_{ϕ_2} is an eigenvector of A corresponding to the eigenvalue $\lambda = 2$. For example, choose

$$v_3 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 2 \end{pmatrix}.$$

By Theorem 7.23, $\beta = \{v_1, Av_1, v_2, Av_2, v_3\}$ is a rational canonical basis for L_A. So setting

$$Q = \begin{pmatrix} 1 & 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & -2 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -2 & 1 \\ 0 & 1 & 0 & -4 & 2 \end{pmatrix},$$

we have $Q^{-1}AQ = C$. ♦

Example 6

For the following matrix A, we find the rational canonical form C and a matrix Q such that $Q^{-1}AQ = C$:

$$A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Since the characteristic polynomial of A is $f(t) = (t-2)^4$, the only irreducible monic divisor of $f(t)$ is $\phi(t) = t - 2$, and so $\mathsf{K}_\phi = \mathsf{R}^4$. In this case, $\phi(t)$ has degree 1; hence in applying Theorem 7.24 to compute the dot diagram for $\phi(t)$, we obtain

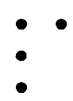
$$r_1 = 4 - \operatorname{rank}(\phi(A)) = 4 - 2 = 2,$$
$$r_2 = \operatorname{rank}(\phi(A)) - \operatorname{rank}((\phi(A))^2) = 2 - 1 = 1,$$

and

$$r_3 = \operatorname{rank}((\phi(A))^2) - \operatorname{rank}((\phi(A))^3) = 1 - 0 = 1,$$

where r_i is the number of dots in the ith row of the dot diagram. Since there are $\dim(\mathsf{R}^4) = 4$ dots in the diagram, we may terminate these computations

with r_3. Thus the dot diagram for A is



Since $(t-2)^3$ has the companion matrix

$$\begin{pmatrix} 0 & 0 & 8 \\ 1 & 0 & -12 \\ 0 & 1 & 6 \end{pmatrix}$$

and $(t-2)$ has the companion matrix (2), the rational canonical form of A is given by

$$C = \left(\begin{array}{ccc|c} 0 & 0 & 8 & 0 \\ 1 & 0 & -12 & 0 \\ 0 & 1 & 6 & 0 \\ \hline 0 & 0 & 0 & 2 \end{array}\right).$$

Next we find a rational canonical basis for L_A. The preceding dot diagram indicates that there are two vectors v_1 and v_2 in R^4 with annihilators $(\phi(t))^3$ and $\phi(t)$, respectively, and such that

$$\beta = \{\beta_{v_1} \cup \beta_{v_2}\} = \{v_1, Av_1, A^2v_1, v_2\}$$

is a rational canonical basis for L_A. Furthermore, $v_1 \notin \mathsf{N}((\mathsf{L}_A - 2\mathsf{I})^2)$, and $v_2 \in \mathsf{N}(\mathsf{L}_A - 2\mathsf{I})$. It can easily be shown that

$$\mathsf{N}(\mathsf{L}_A - 2\mathsf{I}) = \operatorname{span}(\{e_1, e_4\})$$

and

$$\mathsf{N}((\mathsf{L}_A - 2\mathsf{I})^2) = \operatorname{span}(\{e_1, e_2, e_4\}).$$

The standard vector e_3 meets the criteria for v_1; so we set $v_1 = e_3$. It follows that

$$Av_1 = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix} \quad \text{and} \quad A^2v_1 = \begin{pmatrix} 1 \\ 4 \\ 4 \\ 0 \end{pmatrix}.$$

Next we choose a vector $v_2 \in \mathsf{N}(\mathsf{L}_A - 2\mathsf{I})$ that is not in the span of β_{v_1}. Clearly, $v_2 = e_4$ satisfies this condition. Thus

$$\left\{ \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

is a rational canonical basis for L_A.

Finally, let Q be the matrix whose columns are the vectors of β in the same order:

$$Q = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 4 & 0 \\ 1 & 2 & 4 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $C = Q^{-1}AQ$. ♦

Direct Sums*

The next theorem is a simple consequence of Theorem 7.23.

Theorem 7.25 (Primary Decomposition Theorem). *Let T be a linear operator on an n-dimensional vector space V with characteristic polynomial*

$$f(t) = (-1)^n(\phi_1(t))^{n_1}(\phi_2(t))^{n_2}\cdots(\phi_k(t))^{n_k},$$

where the $\phi_i(t)$'s $(1 \le i \le k)$ are distinct irreducible monic polynomials and the n_i's are positive integers. Then the following statements are true.

(a) $\mathsf{V} = \mathsf{K}_{\phi_1} \oplus \mathsf{K}_{\phi_2} \oplus \cdots \oplus \mathsf{K}_{\phi_k}$.

(b) *If T_i $(1 \le i \le k)$ is the restriction of T to K_{ϕ_i} and C_i is the rational canonical form of T_i, then $C_1 \oplus C_2 \oplus \cdots \oplus C_k$ is the rational canonical form of T.*

Proof. Exercise. ∎

The next theorem is a simple consequence of Theorem 7.17.

Theorem 7.26. *Let T be a linear operator on a finite-dimensional vector space V. Then V is a direct sum of T-cyclic subspaces C_{v_i}, where each v_i lies in K_ϕ for some irreducible monic divisor $\phi(t)$ of the characteristic polynomial of T.*

Proof. Exercise. ∎

EXERCISES

1. Label the following statements as true or false.

   (a) Every rational canonical basis for a linear operator T is the union of T-cyclic bases.

(b) If a basis is the union of T-cyclic bases for a linear operator T, then it is a rational canonical basis for T.
(c) There exist square matrices having no rational canonical form.
(d) A square matrix is similar to its rational canonical form.
(e) For any linear operator T on a finite-dimensional vector space, any irreducible factor of the characteristic polynomial of T divides the minimal polynomial of T.
(f) Let $\phi(t)$ be an irreducible monic divisor of the characteristic polynomial of a linear operator T. The dots in the diagram used to compute the rational canonical form of the restriction of T to K_ϕ are in one-to-one correspondence with the vectors in a basis for K_ϕ.
(g) If a matrix has a Jordan canonical form, then its Jordan canonical form and rational canonical form are similar.

2. For each of the following matrices $A \in \mathsf{M}_{n\times n}(F)$, find the rational canonical form C of A and a matrix $Q \in \mathsf{M}_{n\times n}(F)$ such that $Q^{-1}AQ = C$.

(a) $A = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}$ $F = R$

(b) $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ $F = R$

(c) $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ $F = C$

(d) $A = \begin{pmatrix} 0 & -7 & 14 & -6 \\ 1 & -4 & 6 & -3 \\ 0 & -4 & 9 & -4 \\ 0 & -4 & 11 & -5 \end{pmatrix}$ $F = R$

(e) $A = \begin{pmatrix} 0 & -4 & 12 & -7 \\ 1 & -1 & 3 & -3 \\ 0 & -1 & 6 & -4 \\ 0 & -1 & 8 & -5 \end{pmatrix}$ $F = R$

3. For each of the following linear operators T, find the elementary divisors, the rational canonical form C, and a rational canonical basis β.

(a) T is the linear operator on $\mathsf{P}_3(R)$ defined by

$$\mathsf{T}(f(x)) = f(0)x - f'(1).$$

(b) Let $S = \{\sin x, \cos x, x\sin x, x\cos x\}$, a subset of $\mathcal{F}(R, R)$, and let $\mathsf{V} = \text{span}(S)$. Define T to be the linear operator on V such that

$$\mathsf{T}(f) = f'.$$

(c) T is the linear operator on $\mathsf{M}_{2\times 2}(R)$ defined by

$$\mathsf{T}(A) = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \cdot A.$$

(d) Let $S = \{\sin x \sin y, \sin x \cos y, \cos x \sin y, \cos x \cos y\}$, a subset of $\mathcal{F}(R \times R, R)$, and let $\mathsf{V} = \text{span}(S)$. Define T to be the linear operator on V such that

$$\mathsf{T}(f)(x, y) = \frac{\partial f(x, y)}{\partial x} + \frac{\partial f(x, y)}{\partial y}.$$

4. Let T be a linear operator on a finite-dimensional vector space V with minimal polynomial $(\phi(t))^m$ for some positive integer m.

(a) Prove that $\mathsf{R}(\phi(\mathsf{T})) \subseteq \mathsf{N}((\phi(\mathsf{T}))^{m-1})$.

(b) Give an example to show that the subspaces in (a) need not be equal.

(c) Prove that the minimal polynomial of the restriction of T to $\mathsf{R}(\phi(\mathsf{T}))$ equals $(\phi(t))^{m-1}$.

5. Let T be a linear operator on a finite-dimensional vector space. Prove that the rational canonical form of T is a diagonal matrix if and only if T is diagonalizable.

6. Let T be a linear operator on a finite-dimensional vector space V with characteristic polynomial $f(t) = (-1)^n \phi_1(t)\phi_2(t)$, where $\phi_1(t)$ and $\phi_2(t)$ are distinct irreducible monic polynomials and $n = \dim(\mathsf{V})$.

(a) Prove that there exist $v_1, v_2 \in \mathsf{V}$ such that v_1 has T-annihilator $\phi_1(t)$, v_2 has T-annihilator $\phi_2(t)$, and $\beta_{v_1} \cup \beta_{v_2}$ is a basis for V.

(b) Prove that there is a vector $v_3 \in \mathsf{V}$ with T-annihilator $\phi_1(t)\phi_2(t)$ such that β_{v_3} is a basis for V.

(c) Describe the difference between the matrix representation of T with respect to $\beta_{v_1} \cup \beta_{v_2}$ and the matrix representation of T with respect to β_{v_3}.

Thus, to assure the uniqueness of the rational canonical form, we require that the generators of the T-cyclic bases that constitute a rational canonical basis have T-annihilators equal to powers of irreducible monic factors of the characteristic polynomial of T.

7. Let T be a linear operator on a finite-dimensional vector space with minimal polynomial

$$f(t) = (\phi_1(t))^{m_1}(\phi_2(t))^{m_2} \cdots (\phi_k(t))^{m_k},$$

where the $\phi_i(t)$'s are distinct irreducible monic factors of $f(t)$. Prove that for each i, m_i is the number of entries in the first column of the dot diagram for $\phi_i(t)$.

8. Let T be a linear operator on a finite-dimensional vector space V. Prove that for any irreducible polynomial $\phi(t)$, if $\phi(\mathsf{T})$ is not one-to-one, then $\phi(t)$ divides the characteristic polynomial of T. *Hint:* Apply Exercise 15 of Section 7.3.

9. Let V be a vector space and $\beta_1, \beta_2, \ldots, \beta_k$ be disjoint subsets of V whose union is a basis for V. Now suppose that $\gamma_1, \gamma_2, \ldots, \gamma_k$ are linearly independent subsets of V such that $\text{span}(\gamma_i) = \text{span}(\beta_i)$ for all i. Prove that $\gamma_1 \cup \gamma_2 \cup \cdots \cup \gamma_k$ is also a basis for V.

10. Let T be a linear operator on a finite-dimensional vector space, and suppose that $\phi(t)$ is an irreducible monic factor of the characteristic polynomial of T. Prove that if $\phi(t)$ is the T-annihilator of vectors x and y, then $x \in \mathsf{C}_y$ if and only if $\mathsf{C}_x = \mathsf{C}_y$.

Exercises 11 and 12 are concerned with direct sums.

11. Prove Theorem 7.25.

12. Prove Theorem 7.26.

INDEX OF DEFINITIONS FOR CHAPTER 7

Appendices

APPENDIX A SETS

A **set** is a collection of objects, called **elements** of the set. If x is an element of the set A, then we write $x \in A$; otherwise, we write $x \notin A$. For example, if Z is the set of integers, then $3 \in Z$ and $\frac{1}{2} \notin Z$.

One set that appears frequently is the set of real numbers, which we denote by R throughout this text.

Two sets A and B are called **equal**, written $A = B$, if they contain exactly the same elements. Sets may be described in one of two ways:

1. By listing the elements of the set between set braces { }.
2. By describing the elements of the set in terms of some characteristic property.

For example, the set consisting of the elements 1, 2, 3, and 4 can be written as $\{1, 2, 3, 4\}$ or as

$$\{x: x \text{ is a positive integer less than } 5\}.$$

Note that the order in which the elements of a set are listed is immaterial; hence

$$\{1, 2, 3, 4\} = \{3, 1, 2, 4\} = \{1, 3, 1, 4, 2\}.$$

Example 1

Let A denote the set of real numbers between 1 and 2. Then A may be written as

$$A = \{x \in R: 1 < x < 2\}. \quad \blacklozenge$$

A set B is called a **subset** of a set A, written $B \subseteq A$ or $A \supseteq B$, if every element of B is an element of A. For example, $\{1, 2, 6\} \subseteq \{2, 8, 7, 6, 1\}$. If $B \subseteq A$, and $B \neq A$, then B is called a **proper subset** of A. Observe that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$, a fact that is often used to prove that two sets are equal.

The **empty set**, denoted by $\varnothing$, is the set containing no elements. The empty set is a subset of every set.

Sets may be combined to form other sets in two basic ways. The **union** of two sets A and B, denoted $A \cup B$, is the set of elements that are in A, or B, or both; that is,

$$A \cup B = \{x: x \in A \text{ or } x \in B\}.$$

The **intersection** of two sets A and B, denoted $A \cap B$, is the set of elements that are in both A and B; that is,

$$A \cap B = \{x: x \in A \text{ and } x \in B\}.$$

Two sets are called **disjoint** if their intersection equals the empty set.

Example 2

Let $A = \{1, 3, 5\}$ and $B = \{1, 5, 7, 8\}$. Then

$$A \cup B = \{1, 3, 5, 7, 8\} \quad \text{and} \quad A \cap B = \{1, 5\}.$$

Likewise, if $X = \{1, 2, 8\}$ and $Y = \{3, 4, 5\}$, then

$$X \cup Y = \{1, 2, 3, 4, 5, 8\} \quad \text{and} \quad X \cap Y = \varnothing.$$

Thus X and Y are disjoint sets. ♦

The union and intersection of more than two sets can be defined analogously. Specifically, if $A_1, A_2, \ldots, A_n$ are sets, then the union and intersections of these sets are defined, respectively, by

$$\bigcup_{i=1}^{n} A_i = \{x: x \in A_i \text{ for some } i = 1, 2, \ldots, n\}$$

and

$$\bigcap_{i=1}^{n} A_i = \{x: x \in A_i \text{ for all } i = 1, 2, \ldots, n\}.$$

Similarly, if Λ is an index set and $\{A_\alpha: \alpha \in \Lambda\}$ is a collection of sets, the union and intersection of these sets are defined, respectively, by

$$\bigcup_{\alpha \in \Lambda} A_\alpha = \{x: x \in A_\alpha \text{ for some } \alpha \in \Lambda\}$$

and

$$\bigcap_{\alpha \in \Lambda} A_\alpha = \{x: x \in A_\alpha \text{ for all } \alpha \in \Lambda\}.$$

Example 3

Let $\Lambda = \{\alpha \in R: \alpha > 1\}$, and let

$$A_\alpha = \left\{x \in R: \frac{-1}{\alpha} \leq x \leq 1 + \alpha\right\}$$

for each $\alpha \in \Lambda$. Then

$$\bigcup_{\alpha \in \Lambda} A_\alpha = \{x \in R: x > -1\} \quad \text{and} \quad \bigcap_{\alpha \in \Lambda} A_\alpha = \{x \in R: 0 \leq x \leq 2\}. \quad ♦$$

By a relation on a set A, we mean a rule for determining whether or not, for any elements x and y in A, x stands in a given relationship to y. More precisely, a **relation** on A is a set S of ordered pairs of elements of A such that $(x, y) \in S$ if and only if x stands in the given relationship to y. On the set of real numbers, for instance, "is equal to," "is less than," and "is greater than or equal to" are familiar relations. If S is a relation on a set A, we often write $x \sim y$ in place of $(x, y) \in S$.

A relation S on a set A is called an **equivalence relation** on A if the following three conditions hold:

1. For each $x \in A$, $x \sim x$ *(reflexivity).*
2. If $x \sim y$, then $y \sim x$ *(symmetry).*
3. If $x \sim y$ and $y \sim z$, then $x \sim z$ *(transitivity).*

For example, if we define $x \sim y$ to mean that $x - y$ is divisible by a fixed integer n, then $\sim$ is an equivalence relation on the set of integers.

APPENDIX B FUNCTIONS

If A and B are sets, then a **function** f from A to B, written $f: A \to B$, is a rule that associates to each element x in A a unique element denoted $f(x)$ in B. The element $f(x)$ is called the **image** of x (under f), and x is called a **preimage** of $f(x)$ (under f). If $f: A \to B$, then A is called the **domain** of f, B is called the **codomain** of f, and the set $\{f(x): x \in A\}$ is called the **range** of f. Note that the range of f is a subset of B. If $S \subseteq A$, we denote by $f(S)$ the set $\{f(x): x \in S\}$ of all images of elements of S. Likewise, if $T \subseteq B$, we denote by $f^{-1}(T)$ the set $\{x \in A: f(x) \in T\}$ of all preimages of elements in T. Finally, two functions $f: A \to B$ and $g: A \to B$ are **equal**, written $f = g$, if $f(x) = g(x)$ for all $x \in A$.

Example 1

Suppose that $A = [-10, 10]$. Let $f: A \to R$ be the function that assigns to each element x in A the element $x^2 + 1$ in R; that is, f is defined by $f(x) = x^2 + 1$. Then A is the domain of f, R is the codomain of f, and $[1, 101]$ is the range of f. Since $f(2) = 5$, the image of 2 is 5, and 2 is a preimage of 5. Notice that -2 is another preimage of 5. Moreover, if $S = [1, 2]$ and $T = [82, 101]$, then $f(S) = [2, 5]$ and $f^{-1}(T) = [-10, -9] \cup [9, 10]$. ♦

As Example 1 shows, the preimage of an element in the range need not be unique. Functions such that each element of the range has a unique preimage are called **one-to-one**; that is $f: A \to B$ is one-to-one if $f(x) = f(y)$ implies $x = y$ or, equivalently, if $x \neq y$ implies $f(x) \neq f(y)$.

If $f: A \to B$ is a function with range B, that is, if $f(A) = B$, then f is called **onto**. So f is onto if and only if the range of f equals the codomain of f.

Let $f: A \to B$ be a function and $S \subseteq A$. Then a function $f_S: S \to B$, called the **restriction** of f to S, can be formed by defining $f_S(x) = f(x)$ for each $x \in S$.

The next example illustrates these concepts.

Example 2

Let $f: [-1, 1] \to [0, 1]$ be defined by $f(x) = x^2$. This function is onto, but not one-to-one since $f(-1) = f(1) = 1$. Note that if $S = [0, 1]$, then f_S is both onto and one-to-one. Finally, if $T = [\frac{1}{2}, 1]$, then f_T is one-to-one, but not onto. ◆

Let A, B, and C be sets and $f: A \to B$ and $g: B \to C$ be functions. By following f with g, we obtain a function $g \circ f: A \to C$ called the **composite** of g and f. Thus $(g \circ f)(x) = g(f(x))$ for all $x \in A$. For example, let $A = B = C = R$, $f(x) = \sin x$, and $g(x) = x^2 + 3$. Then $(g \circ f)(x) = (g(f(x)) = \sin^2 x + 3$, whereas $(f \circ g)(x) = f(g(x)) = \sin(x^2 + 3)$. Hence, $g \circ f \neq f \circ g$. Functional composition is associative, however; that is, if $h: C \to D$ is another function, then $h \circ (g \circ f) = (h \circ g) \circ f$.

A function $f: A \to B$ is said to be **invertible** if there exists a function $g: B \to A$ such that $(f \circ g)(y) = y$ for all $y \in B$ and $(g \circ f)(x) = x$ for all $x \in A$. If such a function g exists, then it is unique and is called the **inverse** of f. We denote the inverse of f (when it exists) by f^{-1}. It can be shown that f is invertible if and only if f is both one-to-one and onto.

Example 3

The function $f: R \to R$ defined by $f(x) = 3x + 1$ is one-to-one and onto; hence f is invertible. The inverse of f is the function $f^{-1}: R \to R$ defined by $f^{-1}(x) = (x - 1)/3$. ◆

The following facts about invertible functions are easily proved.

1. If $f: A \to B$ is invertible, then f^{-1} is invertible, and $(f^{-1})^{-1} = f$.
2. If $f: A \to B$ and $g: B \to C$ are invertible, then $g \circ f$ is invertible, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

APPENDIX C FIELDS

The set of real numbers is an example of an algebraic structure called a *field*. Basically, a field is a set in which four operations (called addition, multiplication, subtraction, and division) can be defined so that, with the exception of division by zero, the sum, product, difference, and quotient of any two elements in the set is an element of the set. More precisely, a field is defined as follows.

Definitions. *A field F is a set on which two operations $+$ and $\cdot$ (called* **addition** *and* **multiplication**, *respectively) are defined so that, for each pair of elements x, y in F, there are unique elements $x+y$ and $x \cdot y$ in F for which the following conditions hold for all elements a, b, c in F.*

(F 1) $a+b=b+a$ and $a \cdot b=b \cdot a$
(commutativity of addition and multiplication)

(F 2) $(a+b)+c=a+(b+c)$ and $(a \cdot b) \cdot c=a \cdot(b \cdot c)$
(associativity of addition and multiplication)

(F 3) *There exist distinct elements* 0 *and* 1 *in F such that*

$$0+a=a \quad \text{and} \quad 1 \cdot a=a$$

(existence of identity elements for addition and multiplication)

(F 4) For each element a in F and each nonzero element b in F, there exist elements c and d in F such that

$$a+c=0 \quad \text{and} \quad b \cdot d=1$$

(existence of inverses for addition and multiplication)

(F 5) $a \cdot(b+c)=a \cdot b+a \cdot c$
(distributivity of multiplication over addition)

The elements $x+y$ and $x \cdot y$ are called the **sum** *and* **product**, *respectively, of x and y. The elements* 0 *(read "***zero***")* and 1 *(read "***one***") mentioned in* (F 3) *are called* **identity elements** *for addition and multiplication, respectively, and the elements c and d referred to in* (F 4) *are called an* **additive inverse** *for a and a* **multiplicative inverse** *for b, respectively.*

Example 1

The set of real numbers R with the usual definitions of addition and multiplication is a field. ♦

Example 2

The set of rational numbers with the usual definitions of addition and multiplication is a field. ♦

Example 3

The set of all real numbers of the form $a+b\sqrt{2}$, where a and b are rational numbers, with addition and multiplication as in R is a field. ♦

Example 4

The field Z_2 consists of two elements 0 and 1 with the operations of addition and multiplication defined by the equations

$$0+0=0, \quad 0+1=1+0=1, \quad 1+1=0,$$
$$0 \cdot 0=0, \quad 0 \cdot 1=1 \cdot 0=0, \quad \text{and} \quad 1 \cdot 1=1. \quad ♦$$

Example 5

Neither the set of positive integers nor the set of integers with the usual definitions of addition and multiplication is a field, for in either case (F 4) does not hold. ♦

The identity and inverse elements guaranteed by (F 3) and (F 4) are unique; this is a consequence of the following theorem.

Theorem C.1 (Cancellation Laws). *For arbitrary elements a, b, and c in a field, the following statements are true.*

(a) *If $a + b = c + b$, then $a = c$.*

(b) *If $a \cdot b = c \cdot b$ and $b \neq 0$, then $a = c$.*

Proof. (a) The proof of (a) is left as an exercise.

(b) If $b \neq 0$, then (F 4) guarantees the existence of an element d in the field such that $b \cdot d = 1$. Multiply both sides of the equality $a \cdot b = c \cdot b$ by d to obtain $(a \cdot b) \cdot d = (c \cdot b) \cdot d$. Consider the left side of this equality: By (F 2) and (F 3), we have

$$(a \cdot b) \cdot d = a \cdot (b \cdot d) = a \cdot 1 = a.$$

Similarly, the right side of the equality reduces to c. Thus $a = c$. ∎

Corollary. *The elements 0 and 1 mentioned in* (F 3), *and the elements c and d mentioned in* (F 4), *are unique.*

Proof. Suppose that $0' \in F$ satisfies $0' + a = a$ for each $a \in F$. Since $0 + a = a$ for each $a \in F$, we have $0' + a = 0 + a$ for each $a \in F$. Thus $0' = 0$ by Theorem C.1.

The proofs of the remaining parts are similar. ∎

Thus each element b in a field has a unique additive inverse and, if $b \neq 0$, a unique multiplicative inverse. (It is shown in the corollary to Theorem C.2 that 0 has no multiplicative inverse.) The additive inverse and the multiplicative inverse of b are denoted by $-b$ and b^{-1}, respectively. Note that $-(-b) = b$ and $(b^{-1})^{-1} = b$.

Subtraction and *division* can be defined in terms of addition and multiplication by using the additive and multiplicative inverses. Specifically, subtraction of b is defined to be addition of $-b$ and division by $b \neq 0$ is defined to be multiplication by b^{-1}; that is,

$$a - b = a + (-b) \quad \text{and} \quad \frac{a}{b} = a \cdot b^{-1}.$$

In particular, the symbol $\frac{1}{b}$ denotes b^{-1}. Division by zero is undefined, but, with this exception, the sum, product, difference, and quotient of any two elements of a field are defined.

Many of the familiar properties of multiplication of real numbers are true in any field, as the next theorem shows.

Theorem C.2. *Let a and b be arbitrary elements of a field. Then each of the following statements are true.*

(a) $a \cdot 0 = 0$.
(b) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.
(c) $(-a) \cdot (-b) = a \cdot b$.

Proof. (a) Since $0 + 0 = 0$, (F 5) shows that

$$0 + a \cdot 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Thus $0 = a \cdot 0$ by Theorem C.1.

(b) By definition, $-(a \cdot b)$ is the unique element of F with the property $a \cdot b + [-(a \cdot b)] = 0$. So in order to prove that $(-a) \cdot b = -(a \cdot b)$, it suffices to show that $a \cdot b + (-a) \cdot b = 0$. But $-a$ is the element of F such that $a + (-a) = 0$; so

$$a \cdot b + (-a) \cdot b = [a + (-a)] \cdot b = 0 \cdot b = b \cdot 0 = 0$$

by (F 5) and (a). Thus $(-a) \cdot b = -(a \cdot b)$. The proof that $a \cdot (-b) = -(a \cdot b)$ is similar.

(c) By applying (b) twice, we find that

$$(-a) \cdot (-b) = -[a \cdot (-b)] = -[-(a \cdot b)] = a \cdot b. \qquad \blacksquare$$

Corollary. *The additive identity of a field has no multiplicative inverse.*

In an arbitrary field F, it may happen that a sum $1 + 1 + \cdots + 1$ (p summands) equals 0 for some positive integer p. For example, in the field Z_2 (defined in Example 4), $1 + 1 = 0$. In this case, the smallest positive integer p for which a sum of p 1's equals 0 is called the **characteristic** of F; if no such positive integer exists, then F is said to have **characteristic zero**. Thus Z_2 has characteristic two, and R has characteristic zero. Observe that if F is a field of characteristic $p \neq 0$, then $x + x + \cdots + x$ (p summands) equals 0 for all $x \in F$. In a field having nonzero characteristic (especially characteristic two), many unnatural problems arise. For this reason, some of the results about vector spaces stated in this book require that the field over which the vector space is defined be of characteristic zero (or, at least, of some characteristic other than two).

Finally, note that in other sections of this book, the product of two elements a and b in a field is usually denoted ab rather than $a \cdot b$.

APPENDIX D COMPLEX NUMBERS

For the purposes of algebra, the field of real numbers is not sufficient, for there are polynomials of nonzero degree with real coefficients that have no zeros in the field of real numbers (for example, $x^2 + 1$). It is often desirable to have a field in which any polynomial of nonzero degree with coefficients from that field has a zero in that field. It is possible to "enlarge" the field of real numbers to obtain such a field.

Definitions. *A* ***complex number*** *is an expression of the form $z = a+bi$, where a and b are real numbers called the* ***real part*** *and the* ***imaginary part*** *of z, respectively.*

The ***sum*** *and* ***product*** *of two complex numbers $z = a+bi$ and $w = c+di$ (where a, b, c, and d are real numbers) are defined, respectively, as follows:*

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i$$

and

$$zw = (a + bi)(c + di) = (ac - bd) + (bc + ad)i.$$

Example 1

The sum and product of $z = 3 - 5i$ and $w = 9 + 7i$ are, respectively,

$$z + w = (3 - 5i) + (9 + 7i) = (3 + 9) + [(-5) + 7]i = 12 + 2i$$

and

$$zw = (3 - 5i)(9 + 7i) = [3 \cdot 9 - (-5) \cdot 7] + [(-5) \cdot 9 + 3 \cdot 7]i = 62 - 24i. \quad \blacklozenge$$

Any real number c may be regarded as a complex number by identifying c with the complex number $c + 0i$. Observe that this correspondence preserves sums and products; that is,

$$(c + 0i) + (d + 0i) = (c + d) + 0i \quad \text{and} \quad (c + 0i)(d + 0i) = cd + 0i.$$

Any complex number of the form $bi = 0 + bi$, where b is a nonzero real number, is called **imaginary**. The product of two imaginary numbers is real since

$$(bi)(di) = (0 + bi)(0 + di) = (0 - bd) + (b \cdot 0 + 0 \cdot d)i = -bd.$$

In particular, for $i = 0 + 1i$, we have $i \cdot i = -1$.

The observation that $i^2 = i \cdot i = -1$ provides an easy way to remember the definition of multiplication of complex numbers: simply multiply two complex numbers as you would any two algebraic expressions, and replace i^2 by -1. Example 2 illustrates this technique.

Example 2

The product of $-5+2i$ and $1-3i$ is

$$\begin{aligned}(-5+2i)(1-3i) &= -5(1-3i)+2i(1-3i)\\ &= -5+15i+2i-6i^2\\ &= -5+15i+2i-6(-1)\\ &= 1+17i. \quad \blacklozenge\end{aligned}$$

The real number 0, regarded as a complex number, is an additive identity element for the complex numbers since

$$(a+bi)+0=(a+bi)+(0+0i)=(a+0)+(b+0)i=a+bi.$$

Likewise the real number 1, regarded as a complex number, is a multiplicative identity element for the set of complex numbers since

$$(a+bi)\cdot 1=(a+bi)(1+0i)=(a\cdot 1-b\cdot 0)+(b\cdot 1+a\cdot 0)i=a+bi.$$

Every complex number $a+bi$ has an additive inverse, namely $(-a)+(-b)i$. But also each complex number except 0 has a multiplicative inverse. In fact,

$$(a+bi)^{-1}=\left(\frac{a}{a^2+b^2}\right)-\left(\frac{b}{a^2+b^2}\right)i.$$

In view of the preceding statements, the following result is not surprising.

Theorem D.1. *The set of complex numbers with the operations of addition and multiplication previously defined is a field.*

Proof. Exercise. ∎

Definition. *The* ***(complex) conjugate*** *of a complex number $a+bi$ is the complex number $a-bi$. We denote the conjugate of the complex number z by $\overline{z}$.*

Example 3

The conjugates of $-3+2i$, $4-7i$, and 6 are, respectively,

$$\overline{-3+2i}=-3-2i, \quad \overline{4-7i}=4+7i, \quad \text{and} \quad \overline{6}=\overline{6+0i}=6-0i=6. \quad \blacklozenge$$

The next theorem contains some important properties of the conjugate of a complex number.

Theorem D.2. *Let z and w be complex numbers. Then the following statements are true.*

(a) $\overline{\overline{z}} = z$.
(b) $\overline{(z+w)} = \overline{z} + \overline{w}$.
(c) $\overline{zw} = \overline{z} \cdot \overline{w}$.
(d) $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$ *if* $w \neq 0$.
(e) z *is a real number if and only if* $\overline{z} = z$.

Proof. We leave the proofs of (a), (d), and (e) to the reader.
(b) Let $z = a + bi$ and $w = c + di$, where $a, b, c, d \in R$. Then

$$\begin{aligned}\overline{(z+w)} &= \overline{(a+c)+(b+d)i} = (a+c) - (b+d)i \\ &= (a-bi) + (c-di) = \overline{z} + \overline{w}.\end{aligned}$$

(c) For z and w, we have

$$\begin{aligned}\overline{zw} &= \overline{(a+bi)(c+di)} = \overline{(ac-bd)+(ad+bc)i} \\ &= (ac-bd) - (ad+bc)i = (a-bi)(c-di) = \overline{z} \cdot \overline{w}.\end{aligned}$$

For any complex number $z = a + bi$, $z\overline{z}$ is real and nonnegative, for

$$z\overline{z} = (a+bi)(a-bi) = a^2 + b^2.$$

This fact can be used to define the absolute value of a complex number.

Definition. *Let* $z = a + bi$, *where* $a, b \in R$. *The* ***absolute value*** *(or* ***modulus****) of* z *is the real number* $\sqrt{a^2 + b^2}$. *We denote the absolute value of* z *by* $|z|$.

Observe that $z\overline{z} = |z|^2$. The fact that the product of a complex number and its conjugate is real provides an easy method for determining the quotient of two complex numbers; for if $c + di \neq 0$, then

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i.$$

Example 4

To illustrate this procedure, we compute the quotient $(1 + 4i)/(3 - 2i)$:

$$\frac{1+4i}{3-2i} = \frac{1+4i}{3-2i} \cdot \frac{3+2i}{3+2i} = \frac{-5+14i}{9+4} = -\frac{5}{13} + \frac{14}{13}i. \quad \blacklozenge$$

The absolute value of a complex number has the familiar properties of the absolute value of a real number, as the following result shows.

Theorem D.3. *Let* z *and* w *denote any two complex numbers. Then the following statements are true.*

(a) $|zw| = |z| \cdot |w|$.
(b) $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$ *if* $w \neq 0$.
(c) $|z + w| \leq |z| + |w|$.
(d) $|z| - |w| \leq |z + w|$.

Proof. (a) By Theorem D.2, we have

$$|zw|^2 = (zw)\overline{(zw)} = (zw)(\overline{z} \cdot \overline{w}) = (z\overline{z})(w\overline{w}) = |z|^2|w|^2,$$

proving (a).

(b) For the proof of (b), apply (a) to the product $\left(\frac{z}{w}\right) w$.

(c) For any complex number $x = a + bi$, where $a, b \in R$, observe that

$$x + \overline{x} = (a + bi) + (a - bi) = 2a \leq 2\sqrt{a^2 + b^2} = 2|x|.$$

Thus $x + \overline{x}$ is real and satisfies the inequality $x + \overline{x} \leq 2|x|$. Taking $x = w\overline{z}$, we have, by Theorem D.2 and (a),

$$w\overline{z} + \overline{w}z \leq 2|w\overline{z}| = 2|w||\overline{z}| = 2|z||w|.$$

Using Theorem D.2 again gives

$$\begin{aligned} |z + w|^2 = (z + w)\overline{(z + w)} &= (z + w)(\overline{z} + \overline{w}) = z\overline{z} + w\overline{z} + z\overline{w} + w\overline{w} \\ &\leq |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2. \end{aligned}$$

By taking square roots, we obtain (c).

(d) From (a) and (c), it follows that

$$|z| = |(z + w) - w| \leq |z + w| + |-w| = |z + w| + |w|.$$

So

$$|z| - |w| \leq |z + w|,$$

proving (d). ∎

It is interesting as well as useful that complex numbers have both a geometric and an algebraic representation. Suppose that $z = a + bi$, where a and b are real numbers. We may represent z as a vector in the complex plane (see Figure D.1(a)). Notice that, as in R^2, there are two axes, the **real axis** and the **imaginary axis**. The real and imaginary parts of z are the first and second coordinates, and the absolute value of z gives the length of the vector z. It is clear that addition of complex numbers may be represented as in R^2 using the parallelogram law.

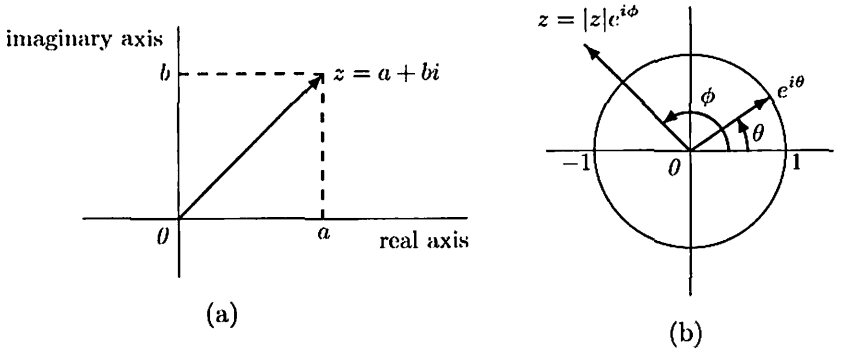


Figure D.1

In Section 2.7 (p.132), we introduce Euler's formula. The special case $e^{i\theta} = \cos\theta + i\sin\theta$ is of particular interest. Because of the geometry we have introduced, we may represent the vector $e^{i\theta}$ as in Figure D.1(b); that is, $e^{i\theta}$ is the unit vector that makes an angle θ with the positive real axis. From this figure, we see that any nonzero complex number z may be depicted as a multiple of a unit vector, namely, $z = |z|e^{i\phi}$, where ϕ is the angle that the vector z makes with the positive real axis. Thus multiplication, as well as addition, has a simple geometric interpretation: If $z = |z|e^{i\theta}$ and $w = |w|e^{i\omega}$ are two nonzero complex numbers, then from the properties established in Section 2.7 and Theorem D.3, we have

$$zw = |z|e^{i\theta} \cdot |w|e^{i\omega} = |zw|e^{i(\theta+\omega)}.$$

So zw is the vector whose length is the product of the lengths of z and w, and makes the angle $\theta + \omega$ with the positive real axis.

Our motivation for enlarging the set of real numbers to the set of complex numbers is to obtain a field such that every polynomial with nonzero degree having coefficients in that field has a zero. Our next result guarantees that the field of complex numbers has this property.

Theorem D.4 (The Fundamental Theorem of Algebra). *Suppose that* $p(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ *is a polynomial in* $\mathsf{P}(C)$ *of degree* $n \geq 1$. *Then* $p(z)$ *has a zero.*

The following proof is based on one in the book *Principles of Mathematical Analysis* 3d., by Walter Rudin (McGraw-Hill Higher Education, New York, 1976).

Proof. We want to find z_0 in C such that $p(z_0) = 0$. Let m be the greatest lower bound of $\{|p(z)|: z \in C\}$. For $|z| = s > 0$, we have

$$|p(z)| = |a_n z^n + a_{n-1}z^{n-1} + \cdots + a_0|$$

$$\begin{aligned} &\geq |a_n||z^n| - |a_{n-1}||z|^{n-1} - \cdots - |a_0| \\ &= |a_n|s^n - |a_{n-1}|s^{n-1} - \cdots - |a_0| \\ &= s^n[|a_n| - |a_{n-1}|s^{-1} - \cdots - |a_0|s^{-n}]. \end{aligned}$$

Because the last expression approaches infinity as s approaches infinity, we may choose a closed disk D about the origin such that $|p(z)| > m + 1$ if z is not in D. It follows that m is the greatest lower bound of $\{|p(z)| : z \in D\}$. Because D is closed and bounded and $p(z)$ is continuous, there exists z_0 in D such that $|p(z_0)| = m$. We want to show that $m = 0$. We argue by contradiction.

Assume that $m \neq 0$. Let $q(z) = \dfrac{p(z + z_0)}{p(z_0)}$. Then $q(z)$ is a polynomial of degree n, $q(0) = 1$, and $|q(z)| \geq 1$ for all z in C. So we may write

$$q(z) = 1 + b_k z^k + b_{k+1} z^{k+1} + \cdots + b_n z^n,$$

where $b_k \neq 0$. Because $-\dfrac{|b_k|}{b_k}$ has modulus one, we may pick a real number θ such that $e^{ik\theta} = -\dfrac{|b_k|}{b_k}$, or $e^{ik\theta} b_k = -|b_k|$. For any $r > 0$, we have

$$\begin{aligned} q(re^{i\theta}) &= 1 + b_k r^k e^{ik\theta} + b_{k+1} r^{k+1} e^{i(k+1)\theta} + \cdots + b_n r^n e^{in\theta} \\ &= 1 - |b_k| r^k + b_{k+1} r^{k+1} e^{i(k+1)\theta} + \cdots + b_n r^n e^{in\theta}. \end{aligned}$$

Choose r small enough so that $1 - |b_k| r^k > 0$. Then

$$\begin{aligned} |q(re^{i\theta})| &\leq 1 - |b_k| r^k + |b_{k+1}| r^{k+1} + \cdots + |b_n| r^n \\ &= 1 - r^k[|b_k| - |b_{k+1}| r - \cdots - |b_n| r^{n-k}]. \end{aligned}$$

Now choose r even smaller, if necessary, so that the expression within the brackets is positive. We obtain that $|q(re^{i\theta})| < 1$. But this is a contradiction. ∎

The following important corollary is a consequence of Theorem D.4 and the division algorithm for polynomials (Theorem E.1).

Corollary. *If $p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ is a polynomial of degree $n \geq 1$ with complex coefficients, then there exist complex numbers $c_1, c_2, \cdots, c_n$ (not necessarily distinct) such that*

$$p(z) = a_n(z - c_1)(z - c_2) \cdots (z - c_n).$$

Proof. Exercise. ∎

A field is called **algebraically closed** if it has the property that every polynomial of positive degree with coefficients from that field factors as a product of polynomials of degree 1. Thus the preceding corollary asserts that the field of complex numbers is algebraically closed.

APPENDIX E POLYNOMIALS

In this appendix, we discuss some useful properties of the polynomials with coefficients from a field. For the definition of a polynomial, refer to Section 1.2. Throughout this appendix, we assume that all polynomials have coefficients from a fixed field F.

Definition. *A polynomial $f(x)$ **divides** a polynomial $g(x)$ if there exists a polynomial $q(x)$ such that $g(x) = f(x)q(x)$.*

Our first result shows that the familiar long division process for polynomials with real coefficients is valid for polynomials with coefficients from an arbitrary field.

Theorem E.1 (The Division Algorithm for Polynomials). *Let $f(x)$ be a polynomial of degree n, and let $g(x)$ be a polynomial of degree $m \geq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that*

$$f(x) = q(x)g(x) + r(x), \tag{1}$$

where the degree of $r(x)$ is less than m.

Proof. We begin by establishing the existence of $q(x)$ and $r(x)$ that satisfy (1).

CASE 1. If $n < m$, take $q(x) = 0$ and $r(x) = f(x)$ to satisfy (1).

CASE 2. When $0 \leq m \leq n$, we apply mathematical induction on n. First suppose that $n = 0$. Then $m = 0$, and it follows that $f(x)$ and $g(x)$ are nonzero constants. Hence we may take $q(x) = f(x)/g(x)$ and $r(x) = 0$ to satisfy (1).

Now suppose that the result is valid for all polynomials with degree less than n for some fixed $n > 0$, and assume that $f(x)$ has degree n. Suppose that

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,$$

and let $h(x)$ be the polynomial defined by

$$h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x). \tag{2}$$

Then $h(x)$ is a polynomial of degree less than n, and therefore we may apply the induction hypothesis or CASE 1 (whichever is relevant) to obtain polynomials $q_1(x)$ and $r(x)$ such that $r(x)$ has degree less than m and

$$h(x) = q_1(x)g(x) + r(x). \tag{3}$$

Combining (2) and (3) and solving for $f(x)$ gives us $f(x) = q(x)g(x) + r(x)$ with $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$, which establishes (a) and (b) for any $n \geq 0$ by mathematical induction. This establishes the existence of $q(x)$ and $r(x)$.

We now show the uniqueness of $q(x)$ and $r(x)$. Suppose that $q_1(x)$, $q_2(x)$, $r_1(x)$, and $r_2(x)$ exist such that $r_1(x)$ and $r_2(x)$ each has degree less than m and

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x).$$

Then

$$[q_1(x) - q_2(x)]\, g(x) = r_2(x) - r_1(x). \tag{4}$$

The right side of (4) is a polynomial of degree less than m. Since $g(x)$ has degree m, it must follow that $q_1(x) - q_2(x)$ is the zero polynomial. Hence $q_1(x) = q_2(x)$; thus $r_1(x) = r_2(x)$ by (4). ∎

In the context of Theorem E.1, we call $q(x)$ and $r(x)$ the **quotient** and **remainder**, respectively, for the division of $f(x)$ by $g(x)$. For example, suppose that F is the field of complex numbers. Then the quotient and remainder for the division of

$$f(x) = (3+i)x^5 - (1-i)x^4 + 6x^3 + (-6+2i)x^2 + (2+i)x + 1$$

by

$$g(x) = (3+i)x^2 - 2ix + 4$$

are, respectively,

$$q(x) = x^3 + ix^2 - 2 \quad \text{and} \quad r(x) = (2-3i)x + 9.$$

Corollary 1. *Let $f(x)$ be a polynomial of positive degree, and let $a \in F$. Then $f(a) = 0$ if and only if $x - a$ divides $f(x)$.*

Proof. Suppose that $x - a$ divides $f(x)$. Then there exists a polynomial $q(x)$ such that $f(x) = (x-a)q(x)$. Thus $f(a) = (a-a)q(a) = 0 \cdot q(a) = 0$.

Conversely, suppose that $f(a) = 0$. By the division algorithm, there exist polynomials $q(x)$ and $r(x)$ such that $r(x)$ has degree less than one and

$$f(x) = q(x)(x-a) + r(x).$$

Substituting a for x in the equation above, we obtain $r(a) = 0$. Since $r(x)$ has degree less than 1, it must be the constant polynomial $r(x) = 0$. Thus $f(x) = q(x)(x-a)$. ∎

For any polynomial $f(x)$ with coefficients from a field F, an element $a \in F$ is called a **zero** of $f(x)$ if $f(a) = 0$. With this terminology, the preceding corollary states that a is a zero of $f(x)$ if and only if $x - a$ divides $f(x)$.

Corollary 2. *Any polynomial of degree $n \geq 1$ has at most n distinct zeros.*

Proof. The proof is by mathematical induction on n. The result is obvious if $n = 1$. Now suppose that the result is true for some positive integer n, and let $f(x)$ be a polynomial of degree $n + 1$. If $f(x)$ has no zeros, then there is nothing to prove. Otherwise, if a is a zero of $f(x)$, then by Corollary 1 we may write $f(x) = (x - a)q(x)$ for some polynomial $q(x)$. Note that $q(x)$ must be of degree n; therefore, by the induction hypothesis, $q(x)$ can have at most n distinct zeros. Since any zero of $f(x)$ distinct from a is also a zero of $q(x)$, it follows that $f(x)$ can have at most $n + 1$ distinct zeros. ∎

Polynomials having no common divisors arise naturally in the study of *canonical forms*. (See Chapter 7.)

Definition. *Two nonzero polynomials are called* **relatively prime** *if no polynomial of positive degree divides each of them.*

For example, the polynomials with real coefficients $f(x) = x^2(x - 1)$ and $h(x) = (x - 1)(x - 2)$ are not relatively prime because $x - 1$ divides each of them. On the other hand, consider $f(x)$ and $g(x) = (x - 2)(x - 3)$, which do not appear to have common factors. Could other factorizations of $f(x)$ and $g(x)$ reveal a hidden common factor? We will soon see (Theorem E.9) that the preceding factors are the only ones. Thus $f(x)$ and $g(x)$ are relatively prime because they have no common factors of positive degree.

Theorem E.2. *If $f_1(x)$ and $f_2(x)$ are relatively prime polynomials, there exist polynomials $q_1(x)$ and $q_2(x)$ such that*

$$q_1(x)f_1(x) + q_2(x)f_2(x) = 1,$$

where 1 denotes the constant polynomial with value 1.

Proof. Without loss of generality, assume that the degree of $f_1(x)$ is greater than or equal to the degree of $f_2(x)$. The proof is by mathematical induction on the degree of $f_2(x)$. If $f_2(x)$ has degree 0, then $f_2(x)$ is a nonzero constant c. In this case, we can take $q_1(x) = 0$ and $q_2(x) = 1/c$.

Now suppose that the theorem holds whenever the polynomial of lesser degree has degree less than n for some positive integer n, and suppose that $f_2(x)$ has degree n. By the division algorithm, there exist polynomials $q(x)$ and $r(x)$ such that $r(x)$ has degree less than n and

$$f_1(x) = q(x)f_2(x) + r(x). \tag{5}$$

Since $f_1(x)$ and $f_2(x)$ are relatively prime, $r(x)$ is not the zero polynomial. We claim that $f_2(x)$ and $r(x)$ are relatively prime. Suppose otherwise; then there exists a polynomial $g(x)$ of positive degree that divides both $f_2(x)$ and $r(x)$. Hence, by (5), $g(x)$ also divides $f_1(x)$, contradicting the fact that $f_1(x)$ and $f_2(x)$ are relatively prime. Since $r(x)$ has degree less than n, we may apply the induction hypothesis to $f_2(x)$ and $r(x)$. Thus there exist polynomials $g_1(x)$ and $g_2(x)$ such that

$$g_1(x)f_2(x) + g_2(x)r(x) = 1. \tag{6}$$

Combining (5) and (6), we have

$$\begin{aligned} 1 &= g_1(x)f_2(x) + g_2(x)\,[f_1(x) - q(x)f_2(x)] \\ &= g_2(x)f_1(x) + [g_1(x) - g_2(x)q(x)]\,f_2(x). \end{aligned}$$

Thus, setting $q_1(x) = g_2(x)$ and $q_2(x) = g_1(x) - g_2(x)q(x)$, we obtain the desired result. ∎

Example 1

Let $f_1(x) = x^3 - x^2 + 1$ and $f_2(x) = (x-1)^2$. As polynomials with real coefficients, $f_1(x)$ and $f_2(x)$ are relatively prime. It is easily verified that the polynomials $q_1(x) = -x + 2$ and $q_2(x) = x^2 - x - 1$ satisfy

$$q_1(x)f_1(x) + q_2(x)f_2(x) = 1,$$

and hence these polynomials satisfy the conclusion of Theorem E.2. ♦

Throughout Chapters 5, 6, and 7, we consider linear operators that are polynomials in a particular operator T and matrices that are polynomials in a particular matrix A. For these operators and matrices, the following notation is convenient.

Definitions. *Let*

$$f(x) = a_0 + a_1(x) + \cdots + a_n x^n$$

be a polynomial with coefficients from a field F. If T is a linear operator on a vector space V over F, we define

$$f(\mathsf{T}) = a_0\mathsf{I} + a_1\mathsf{T} + \cdots + a_n\mathsf{T}^n.$$

Similarly, if A is a $n \times n$ matrix with entries from F, we define

$$f(A) = a_0 I + a_1 A + \cdots + a_n A^n.$$

Example 2

Let T be the linear operator on R^2 defined by $\mathsf{T}(a,b) = (2a+b, a-b)$, and let $f(x) = x^2 + 2x - 3$. It is easily checked that $\mathsf{T}^2(a,b) = (5a+b, a+2b)$; so

$$\begin{aligned} f(\mathsf{T})(a,b) &= (\mathsf{T}^2 + 2\mathsf{T} - 3\mathsf{I})(a,b) \\ &= (5a+b, a+2b) + (4a+2b, 2a-2b) - 3(a,b) \\ &= (6a+3b, 3a-3b). \end{aligned}$$

Similarly, if

$$A = \begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix},$$

then

$$f(A) = A^2 + 2A - 3I = \begin{pmatrix} 5 & 1 \\ 1 & 2 \end{pmatrix} + 2\begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix} - 3\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 3 \\ 3 & -3 \end{pmatrix}. \quad \blacklozenge$$

The next three results use this notation.

Theorem E.3. *Let $f(x)$ be a polynomial with coefficients from a field F, and let T be a linear operator on a vector space V over F. Then the following statements are true.*

(a) *$f(\mathsf{T})$ is a linear operator on V.*

(b) *If β is a finite ordered basis for V and $A = [\mathsf{T}]_\beta$, then $[f(\mathsf{T})]_\beta = f(A)$.*

Proof. Exercise. ∎

Theorem E.4. *Let T be a linear operator on a vector space V over a field F, and let A be a square matrix with entries from F. Then, for any polynomials $f_1(x)$ and $f_2(x)$ with coefficients from F,*

(a) $f_1(\mathsf{T})f_2(\mathsf{T}) = f_2(\mathsf{T})f_1(\mathsf{T})$

(b) $f_1(A)f_2(A) = f_2(A)f_1(A)$.

Proof. Exercise. ∎

Theorem E.5. *Let T be a linear operator on a vector space V over a field F, and let A be an $n \times n$ matrix with entries from F. If $f_1(x)$ and $f_2(x)$ are relatively prime polynomials with entries from F, then there exist polynomials $q_1(x)$ and $q_2(x)$ with entries from F such that*

(a) $q_1(\mathsf{T})f_1(\mathsf{T}) + q_2(\mathsf{T})f_2(\mathsf{T}) = \mathsf{I}$

(b) $q_1(A)f_1(A) + q_2(A)f_2(A) = I$.

Proof. Exercise. ∎

In Chapters 5 and 7, we are concerned with determining when a linear operator T on a finite-dimensional vector space can be *diagonalized* and with finding a simple (canonical) representation of T. Both of these problems are affected by the factorization of a certain polynomial determined by T (the *characteristic polynomial* of T). In this setting, particular types of polynomials play an important role.

Definitions. *A polynomial $f(x)$ with coefficients from a field F is called* **monic** *if its leading coefficient is* 1. *If $f(x)$ has positive degree and cannot be expressed as a product of polynomials with coefficients from F each having positive degree, then $f(x)$ is called* **irreducible**.

Observe that whether a polynomial is irreducible depends on the field F from which its coefficients come. For example, $f(x) = x^2 + 1$ is irreducible over the field of real numbers, but it is not irreducible over the field of complex numbers since $x^2 + 1 = (x + i)(x - i)$.

Clearly any polynomial of degree 1 is irreducible. Moreover, for polynomials with coefficients from an algebraically closed field, the polynomials of degree 1 are the only irreducible polynomials.

The following facts are easily established.

Theorem E.6. *Let $\phi(x)$ and $f(x)$ be polynomials. If $\phi(x)$ is irreducible and $\phi(x)$ does not divide $f(x)$, then $\phi(x)$ and $f(x)$ are relatively prime.*

Proof. Exercise. ∎

Theorem E.7. *Any two distinct irreducible monic polynomials are relatively prime.*

Proof. Exercise. ∎

Theorem E.8. *Let $f(x)$, $g(x)$, and $\phi(x)$ be polynomials. If $\phi(x)$ is irreducible and divides the product $f(x)g(x)$, then $\phi(x)$ divides $f(x)$ or $\phi(x)$ divides $g(x)$.*

Proof. Suppose that $\phi(x)$ does not divide $f(x)$. Then $\phi(x)$ and $f(x)$ are relatively prime by Theorem E.6, and so there exist polynomials $q_1(x)$ and $q_2(x)$ such that

$$1 = q_1(x)\phi(x) + q_2(x)f(x).$$

Multiplying both sides of this equation by $g(x)$ yields

$$g(x) = q_1(x)\phi(x)g(x) + q_2(x)f(x)g(x). \tag{7}$$

Since $\phi(x)$ divides $f(x)g(x)$, there is a polynomial $h(x)$ such that $f(x)g(x) = \phi(x)h(x)$. Thus (7) becomes

$$g(x) = q_1(x)\phi(x)g(x) + q_2(x)\phi(x)h(x) = \phi(x)\left[q_1(x)g(x) + q_2(x)h(x)\right].$$

So $\phi(x)$ divides $g(x)$. ∎

Corollary. *Let $\phi(x), \phi_1(x), \phi_2(x), \ldots, \phi_n(x)$ be irreducible monic polynomials. If $\phi(x)$ divides the product $\phi_1(x)\phi_2(x)\cdots\phi_n(x)$, then $\phi(x) = \phi_i(x)$ for some i $(i = 1, 2, \ldots, n)$.*

Proof. We prove the corollary by mathematical induction on n. For $n = 1$, the result is an immediate consequence of Theorem E.7. Suppose then that for some $n > 1$, the corollary is true for any $n-1$ irreducible monic polynomials, and let $\phi_1(x), \phi_2(x), \ldots, \phi_n(x)$ be n irreducible polynomials. If $\phi(x)$ divides

$$\phi_1(x)\phi_2(x)\cdots\phi_n(x) = [\phi_1(x)\phi_2(x)\cdots\phi_{n-1}(x)]\,\phi_n(x),$$

then $\phi(x)$ divides the product $\phi_1(x)\phi_2(x)\cdots\phi_{n-1}(x)$ or $\phi(x)$ divides $\phi_n(x)$ by Theorem E.8. In the first case, $\phi(x) = \phi_i(x)$ for some i $(i = 1, 2, \ldots, n-1)$ by the induction hypothesis; in the second case, $\phi(x) = \phi_n(x)$ by Theorem E.7. ∎

We are now able to establish the unique factorization theorem, which is used throughout Chapters 5 and 7. This result states that every polynomial of positive degree is uniquely expressible as a constant times a product of irreducible monic polynomials.

Theorem E.9 (Unique Factorization Theorem for Polynomials). *For any polynomial $f(x)$ of positive degree, there exist a unique constant c; unique distinct irreducible monic polynomials $\phi_1(x), \phi_2(x), \ldots, \phi_k(x)$; and unique positive integers $n_1, n_2, \ldots, n_k$ such that*

$$f(x) = c[\phi_1(x)]^{n_1}[\phi_2(x)]^{n_2}\cdots[\phi_k(x)]^{n_k}.$$

Proof. We begin by showing the existence of such a factorization using mathematical induction on the degree of $f(x)$. If $f(x)$ is of degree 1, then $f(x) = ax + b$ for some constants a and b with $a \neq 0$. Setting $\phi(x) = x + b/a$, we have $f(x) = a\phi(x)$. Since $\phi(x)$ is an irreducible monic polynomial, the result is proved in this case. Now suppose that the conclusion is true for any polynomial with positive degree less than some integer $n > 1$, and let $f(x)$ be a polynomial of degree n. Then

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

for some constants a_i with $a_n \neq 0$. If $f(x)$ is irreducible, then

$$f(x) = a_n\left(x^n + \frac{a_{n-1}}{a_n}x^{n-1} + \cdots + \frac{a_1}{a_n} + \frac{a_0}{a_n}\right)$$

is a representation of $f(x)$ as a product of a_n and an irreducible monic polynomial. If $f(x)$ is not irreducible, then $f(x) = g(x)h(x)$ for some polynomials $g(x)$ and $h(x)$, each of positive degree less than n. The induction hypothesis

guarantees that both $g(x)$ and $h(x)$ factor as products of a constant and powers of distinct irreducible monic polynomials. Consequently $f(x) = g(x)h(x)$ also factors in this way. Thus, in either case, $f(x)$ can be factored as a product of a constant and powers of distinct irreducible monic polynomials.

It remains to establish the uniqueness of such a factorization. Suppose that

$$\begin{aligned} f(x) &= c[\phi_1(x)]^{n_1}[\phi_2(x)]^{n_2}\cdots[\phi_k(x)]^{n_k} \\ &= d[\psi_1(x)]^{m_1}[\psi_2(x)]^{m_2}\cdots[\psi_r(x)]^{m_r}, \end{aligned} \tag{8}$$

where c and d are constants, $\phi_i(x)$ and $\psi_j(x)$ are irreducible monic polynomials, and n_i and m_j are positive integers for $i = 1, 2, \ldots, k$ and $j = 1, 2, \ldots, r$. Clearly both c and d must be the leading coefficient of $f(x)$; hence $c = d$. Dividing by c, we find that (8) becomes

$$[\phi_1(x)]^{n_1}[\phi_2(x)]^{n_2}\cdots[\phi_k(x)]^{n_k} = [\psi_1(x)]^{m_1}[\psi_2(x)]^{m_2}\cdots[\psi_r(x)]^{m_r}. \tag{9}$$

So $\phi_i(x)$ divides the right side of (9) for $i = 1, 2, \ldots, k$. Consequently, by the corollary to Theorem E.8, each $\phi_i(x)$ equals some $\psi_j(x)$, and similarly, each $\psi_j(x)$ equals some $\phi_i(x)$. We conclude that $r = k$ and that, by renumbering if necessary, $\phi_i(x) = \psi_i(x)$ for $i = 1, 2, \ldots, k$. Suppose that $n_i \neq m_i$ for some i. Without loss of generality, we may suppose that $i = 1$ and $n_1 > m_1$. Then by canceling $[\phi_1(x)]^{m_1}$ from both sides of (9), we obtain

$$[\phi_1(x)]^{n_1 - m_1}[\phi_2(x)]^{n_2}\cdots[\phi_k(x)]^{n_k} = [\phi_2(x)]^{m_2}\cdots[\phi_k(x)]^{m_k}. \tag{10}$$

Since $n_1 - m_1 > 0$, $\phi_1(x)$ divides the left side of (10) and hence divides the right side also. So $\phi_1(x) = \phi_i(x)$ for some $i = 2, \ldots, k$ by the corollary to Theorem E.8. But this contradicts that $\phi_1(x), \phi_2(x), \ldots, \phi_k(x)$ are distinct. Hence the factorizations of $f(x)$ in (8) are the same. ∎

It is often useful to regard a polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with coefficients from a field F as a function $f\colon F \to F$. In this case, the value of f at $c \in F$ is $f(c) = a_n c^n + \cdots + a_1 c + a_0$. Unfortunately, for arbitrary fields there is not a one-to-one correspondence between polynomials and polynomial functions. For example, if $f(x) = x^2$ and $g(x) = x$ are two polynomials over the field Z_2 (defined in Example 4 of Appendix C), then $f(x)$ and $g(x)$ have different degrees and hence are not equal as polynomials. But $f(a) = g(a)$ for all $a \in Z_2$, so that f and g are equal polynomial functions. Our final result shows that this anomaly cannot occur over an infinite field.

Theorem E.10. *Let $f(x)$ and $g(x)$ be polynomials with coefficients from an infinite field F. If $f(a) = g(a)$ for all $a \in F$, then $f(x)$ and $g(x)$ are equal.*

Proof. Suppose that $f(a) = g(a)$ for all $a \in F$. Define $h(x) = f(x) - g(x)$, and suppose that $h(x)$ is of degree $n \geq 1$. It follows from Corollary 2 to

Theorem E.1 that $h(x)$ can have at most n zeroes. But

$$h(a) = f(a) - g(a) = 0$$

for every $a \in F$, contradicting the assumption that $h(x)$ has positive degree. Thus $h(x)$ is a constant polynomial, and since $h(a) = 0$ for each $a \in F$, it follows that $h(x)$ is the zero polynomial. Hence $f(x) = g(x)$. ∎