CHAPTER 8

Canonical Forms

Recall that at the beginning of Section 7.5 we stated that a canonical form for $T \in L(V)$ is simply a representation in which the matrix takes on an especially simple form. For example, if there exists a basis of eigenvectors of T, then the matrix representation will be diagonal. In this case, it is then quite trivial to assess the various properties of T such as its rank, determinant and eigenvalues. Unfortunately, while this is generally the most desirable form for a matrix representation, it is also generally impossible to achieve.

We now wish to determine certain properties of T that will allow us to learn as much as we can about the possible forms its matrix representation can take. There are three major canonical forms that we will consider in this chapter : triangular, rational and Jordan. (This does not count the Smith form, which is really a tool, used to find the rational and Jordan forms.) As we have done before, our approach will be to study each of these forms in more than one way. By so doing, we shall gain much insight into their meaning, as well as learning additional techniques that are of great use in various branches of mathematics.

8.1 ELEMENTARY CANONICAL FORMS

In order to ease into the subject, this section presents a simple and direct method of treating two important results: the triangular form for complex matrices and the diagonalization of normal matrices. To begin with, suppose

that we have a matrix $A \in M_n(\mathbb{C})$. We define the **adjoint** (or **Hermitian adjoint**) of A to be the matrix $A^\dagger = A^{*T}$. In other words, the adjoint of A is its complex conjugate transpose. From Theorem 3.18(d), it is easy to see that

$$(AB)^\dagger = B^\dagger A^\dagger \ .$$

If it so happens that $A^\dagger = A$, then A is said to be a **Hermitian** matrix.

If a matrix $U \in M_n(\mathbb{C})$ has the property that $U^\dagger = U^{-1}$, then we say that U is **unitary**. Thus a matrix U is unitary if $UU^\dagger = U^\dagger U = I$. (Note that by Theorem 3.21, it is only necessary to require either $UU^\dagger = I$ or $U^\dagger U = I$.) We also see that the product of two unitary matrices U and V is unitary since $(UV)^\dagger UV = V^\dagger U^\dagger UV = V^\dagger IV = V^\dagger V = I$. If a matrix $N \in M_n(\mathbb{C})$ has the property that it commutes with its adjoint, i.e., $NN^\dagger = N^\dagger N$, then N is said to be a **normal** matrix. Note that Hermitian and unitary matrices are automatically normal.

Example 8.1 Consider the matrix $A \in M_2(\mathbb{C})$ given by

$$A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ i & i \end{pmatrix} \ .$$

Then the adjoint of A is given by

$$A^\dagger = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -1 & -i \end{pmatrix}$$

and we leave it to the reader to verify that $AA^\dagger = A^\dagger A = 1$, and hence show that A is unitary. //

We will devote considerable time in Chapter 10 to the study of these matrices. However, for our present purposes, we wish to point out one important property of unitary matrices. Note that since $U \in M_n(\mathbb{C})$, the rows U_i and columns U^i of U are just vectors in $\mathbb{C}^n$. This means that we can take their inner product relative to the standard inner product on $\mathbb{C}^n$ (see Example 2.9). Writing out the relation $UU^\dagger = I$ in terms of components, we have

$$(UU^\dagger)_{ij} = \sum_{k=1}^{n} u_{ik} u^\dagger{}_{kj} = \sum_{k=1}^{n} u_{ik} u_{jk}^* = \sum_{k=1}^{n} u_{jk}^* u_{ik} = \langle U_j, U_i \rangle = \delta_{ij}$$

and from $U^\dagger U = I$ we see that

$$(U^\dagger U)_{ij} = \sum_{k=1}^{n} u^\dagger{}_{ik} u_{kj} = \sum_{k=1}^{n} u_{ki}^* u_{kj} = \langle U^i, U^j \rangle = \delta_{ij} \ .$$

In other words, a matrix is unitary if and only if its rows (or columns) each form an orthonormal set. Note we have shown that if the rows (columns) of $U \in M_n(\mathbb{C})$ form an orthonormal set, then so do the columns (rows), and either of these is a sufficient condition for U to be unitary. For example, the reader can easily verify that the matrix A in Example 8.1 satisfies these conditions.

It is also worth pointing out that Hermitian and unitary matrices have important analogues over the real number system. If $A \in M_n(\mathbb{R})$ is Hermitian, then $A = A^\dagger = A^T$, and we say that A is **symmetric**. If $U \in M_n(\mathbb{R})$ is unitary, then $U^{-1} = U^\dagger = U^T$, and we say that U is **orthogonal**. Repeating the above calculations over $\mathbb{R}$, it is easy to see that a real matrix is orthogonal if and only if its rows (or columns) form an orthonormal set.

It will also be useful to recall from Section 3.6 that if A and B are two matrices for which the product AB is defined, then the i*th* row of AB is given by $(AB)_i = A_iB$ and the i*th* column of AB is given by $(AB)^i = AB^i$. We now prove yet another version of the triangular form theorem.

Theorem 8.1 (**Schur Canonical Form**) If $A \in M_n(\mathbb{C})$, then there exists a unitary matrix $U \in M_n(\mathbb{C})$ such that $U^\dagger AU$ is upper-triangular. Furthermore, the diagonal entries of $U^\dagger AU$ are just the eigenvalues of A.

Proof If n = 1 there is nothing to prove, so we assume that the theorem holds for any square matrix of size $n - 1 \geq 1$, and suppose A is of size n. Since we are dealing with the algebraically closed field $\mathbb{C}$, we know that A has n (not necessarily distinct) eigenvalues (see Section 7.3). Let λ be one of these eigenvalues, and denote the corresponding eigenvector by $\tilde{U}^1$. By Theorem 2.10 we extend $\tilde{U}^1$ to a basis for $\mathbb{C}^n$, and by the Gram-Schmidt process (Theorem 2.21) we assume that this basis is orthonormal. From our discussion above, we see that this basis may be used as the columns of a unitary matrix $\tilde{U}$ with $\tilde{U}^1$ as its first column. We then see that

$$\begin{aligned}(\tilde{U}^\dagger A\tilde{U})^1 &= \tilde{U}^\dagger(A\tilde{U})^1 = \tilde{U}^\dagger(A\tilde{U}^1) = \tilde{U}^\dagger(\lambda\tilde{U}^1) = \lambda(\tilde{U}^\dagger\tilde{U}^1) \\ &= \lambda(\tilde{U}^\dagger\tilde{U})^1 = \lambda I^1\end{aligned}$$

and hence $\tilde{U}^\dagger A\tilde{U}$ has the form

$$\tilde{U}^\dagger A\tilde{U} = \begin{pmatrix} \lambda & * & \cdots & * \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$$

where $B \in M_{n-1}(\mathbb{C})$ and the *'s are (in general) nonzero scalars. By our induction hypothesis, we may choose a unitary matrix $W \in M_{n-1}(\mathbb{C})$ such that $W^\dagger BW$ is upper-triangular. Let $V \in M_n(\mathbb{C})$ be a unitary matrix of the form

$$V = \begin{pmatrix} 1 & 0 \cdots 0 \\ 0 & \\ \vdots & \boxed{W} \\ 0 & \end{pmatrix}$$

and define the unitary matrix $U = \tilde{U}V \in M_n(\mathbb{C})$. Then

$$U^\dagger AU = (\tilde{U}V)^\dagger A(\tilde{U}V) = V^\dagger(\tilde{U}^\dagger A\tilde{U})V$$

is upper-triangular since (in an obvious shorthand notation)

$$V^\dagger(\tilde{U}^\dagger A\tilde{U})V = \begin{pmatrix} 1 & 0 \\ 0 & W^\dagger \end{pmatrix}\begin{pmatrix} \lambda & * \\ 0 & B \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & W \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & W^\dagger \end{pmatrix}\begin{pmatrix} \lambda & * \\ 0 & BW \end{pmatrix}$$
$$= \begin{pmatrix} \lambda & * \\ 0 & W^\dagger BW \end{pmatrix}$$

and $W^\dagger BW$ is upper-triangular by the induction hypothesis.

Noting that $\lambda I - U^\dagger AU$ is upper-triangular, it is easy to see (using Theorem 4.5) that the roots of $\det(\lambda I - U^\dagger AU)$ are just the diagonal entries of $U^\dagger AU$. But

$$\det(\lambda I - U^\dagger AU) = \det[U^\dagger(\lambda I - A)U] = \det(\lambda I - A)$$

so that A and $U^\dagger AU$ have the same eigenvalues. ∎

Corollary If $A \in M_n(\mathbb{R})$ has all its eigenvalues in $\mathbb{R}$, then the matrix U defined in Theorem 8.1 may be chosen to have all real entries.

Proof If $\lambda \in \mathbb{R}$ is an eigenvalue of A, then $A - \lambda I$ is a real matrix with determinant $\det(A - \lambda I) = 0$, and therefore the homogeneous system of equations $(A - \lambda I)X = 0$ has a real solution. Defining $\tilde{U}^1 = X$, we may now proceed as in Theorem 8.1. The details are left to the reader (see Exercise 8.8.1). ∎

We say that two matrices $A, B \in M_n(\mathbb{C})$ are **unitarily similar** (written $A \sim B$) if there exists a unitary matrix U such that $B = U^\dagger AU = U^{-1}AU$. Since this

defines an equivalence relation on the set of all matrices in $M_n(\mathbb{C})$, many authors say that A and B are **unitarily equivalent**. However, we will be using the term "equivalent" in a somewhat more general context later in this chapter, and the word "similar" is in accord with our earlier terminology.

We leave it to the reader to show that if A and B are unitarily similar and A is normal, then B is also normal (see Exercise 8.8.2). In particular, suppose that U is unitary and N is such that $U^\dagger NU = D$ is diagonal. Since any diagonal matrix is automatically normal, it follows that N must be normal also. We now show that the converse is also true, i.e., that any normal matrix is unitarily similar to a diagonal matrix.

To see this, suppose N is normal, and let $U^\dagger NU = D$ be the Schur canonical form of N. Then D is both upper-triangular and normal (since it is unitarily similar to a normal matrix). We claim that the only such matrices are diagonal. For, consider the (1, 1) elements of $DD^\dagger$ and $D^\dagger D$. From what we showed above, we have

$$(DD^\dagger)_{11} = \langle D_1, D_1 \rangle = |d_{11}|^2 + |d_{12}|^2 + \cdots + |d_{1n}|^2$$

and

$$(D^\dagger D)_{11} = \langle D^1, D^1 \rangle = |d_{11}|^2 + |d_{21}|^2 + \cdots + |d_{n1}|^2 \ .$$

But D is upper-triangular so that $d_{21} = \cdots = d_{n1} = 0$. By normality we must have $(DD^\dagger)_{11} = (D^\dagger D)_{11}$, and therefore $d_{12} = \cdots = d_{1n} = 0$ also. In other words, with the possible exception of the (1, 1) entry, all entries in the first row and column of D must be zero. In the same manner, we see that

$$(DD^\dagger)_{22} = \langle D_2, D_2 \rangle = |d_{21}|^2 + |d_{22}|^2 + \cdots + |d_{2n}|^2$$

and

$$(D^\dagger D)_{22} = \langle D^2, D^2 \rangle = |d_{12}|^2 + |d_{22}|^2 + \cdots + |d_{n2}| \ .$$

Since the fact that D is upper-triangular means $d_{32} = \cdots = d_{n2} = 0$ and we just showed that $d_{21} = d_{12} = 0$, it again follows by normality that $d_{23} = \cdots = d_{2n} = 0$. Thus all entries in the second row and column with the possible exception of the (2, 2) entry must be zero.

Continuing this procedure, it is clear that D must be diagonal as claimed. In other words, *an upper-triangular normal matrix is necessarily diagonal*. This discussion proves the following very important theorem.

Theorem 8.2 A matrix $N \in M_n(\mathbb{C})$ is normal if and only if there exists a unitary matrix U such that $U^\dagger NU$ is diagonal.

Corollary If $A = (a_{ij}) \in M_n(\mathbb{R})$ is symmetric, then there exists an orthogonal matrix S such that $S^T AS$ is diagonal.

Proof If we can show that a real symmetric matrix has all real eigenvalues, then this corollary will follow from the corollary to Theorem 8.1 and the real analogue of the proof of Theorem 8.2. Now suppose $A = A^T$ so that $a_{ij} = a_{ji}$. If λ is an eigenvalue of A, then there exists a (nonzero and not necessarily real) vector $x \in \mathbb{C}^n$ such that $Ax = \lambda x$ or

$$\sum_{j=1}^{n} a_{ij}x_j = \lambda x_i \quad . \tag{1}$$

Multiplying (1) by x_i^*, summing over i and using the standard inner product on $\mathbb{C}^n$ we obtain

$$\sum_{i,j=1}^{n} x_i^* a_{ij} x_j = \lambda \|x\|^2 \quad . \tag{2}$$

On the other hand, we may take the complex conjugate of (1), then multiply by x_i and sum over i to obtain (since each a_{ij} is real)

$$\sum_{i,j=1}^{n} x_i a_{ij} x_j^* = \lambda^* \|x\|^2 \quad . \tag{3}$$

But $a_{ij} = a_{ji}$ and therefore the left hand side of (3) becomes

$$\sum_{i,j=1}^{n} x_i a_{ij} x_j^* = \sum_{i,j=1}^{n} x_j^* a_{ji} x_i = \sum_{i,j=1}^{n} x_i^* a_{ij} x_j$$

where in the last step we relabelled the index i by j and the index j by i. Since this shows that the left hand sides of (2) and (3) are equal, it follows that $\lambda = \lambda^*$ as claimed. ∎

We will return to this theorem in Chapter 10 where it will be proved in an entirely different manner.

Exercises

1. Finish the proof of the corollary to Theorem 8.1.

2. Show that if $A, B \in M_n(\mathbb{C})$ are unitarily similar and A is normal, then B is also normal.

3. Suppose $A, B \in M_n(\mathbb{C})$ commute (i.e., $AB = BA$).
   (a) Prove there exists a unitary matrix U such that $U^\dagger AU$ and $U^\dagger BU$ are both upper-triangular. [*Hint*: Let $V_\lambda \subset \mathbb{C}^n$ be the eigenspace of B corresponding to the eigenvalue λ. Show that V_λ is invariant under A, and

hence show that A and B have a common eigenvector $\tilde{U}^1$. Now proceed as in the proof of Theorem 8.1.]
(b) Show that if A and B are also normal, then there exists a unitary matrix U such that $U^\dagger AU$ and $U^\dagger BU$ are diagonal.

4. Can every matrix $A \in M_n(\mathbb{C})$ be written as a product of two unitary matrices? Explain.

5. (a) Prove that if H is Hermitian, then det H is real.
(b) Is it the case that every square matrix A can be written as the product of finitely many Hermitian matrices? Explain.

6. A matrix M is **skew-Hermitian** if $M^\dagger = -M$.
(a) Show that skew-Hermitian matrices are normal.
(b) Show that any square matrix A can be written as a sum of a skew-Hermitian matrix and a Hermitian matrix.

7. Describe all diagonal unitary matrices. Prove that any n x n diagonal matrix can be written as a finite sum of unitary diagonal matrices. [*Hint*: Do the cases n = 1 and n = 2 to get the idea.]

8. Using the previous exercise, show that any n x n normal matrix can be written as the sum of finitely many unitary matrices.

9. If A is unitary, does this imply that $\det A^k = 1$ for some integer k? What if A is a real unitary matrix (i.e., orthogonal)?

10. (a) Is an n x n matrix A that is similar (but not necessarily *unitarily* similar) to a Hermitian matrix necessarily Hermitian?
(b) If A is similar to a normal matrix, is A necessarily normal?

11. If N is normal and $Nx = \lambda x$, prove that $N^\dagger x = \lambda^* x$. [*Hint*: First treat the case where N is diagonal.]

12. Does the fact that A is similar to a diagonal matrix imply that A is normal?

13. Discuss the following conjecture: If N_1 and N_2 are normal, then $N_1 + N_2$ is normal if and only if $N_1N_2^\dagger = N_2^\dagger N_1$.

14. (a) If $A \in M_n(\mathbb{R})$ is nonzero and skew-symmetric, show that A can not have any real eigenvalues.
    (b) What can you say about the eigenvalues of such a matrix?
    (c) What can you say about the rank of A?

15. Let $\sigma \in S_n$ be a permutation, and let f: {1, . . . , n} → {+1, −1}. Define the **signed permutation matrix** P_σ^f by

$$P_\sigma^f(i, j) = \begin{cases} f(j) & \text{if } \sigma(j) = i \\ 0 & \text{otherwise} \end{cases}.$$

    Show that signed permutation matrices are orthogonal.

16. (a) Prove that a real n x n matrix A that commutes with all n-square real orthogonal matrices is a multiple of I_n. [*Hint*: Show that the matrices E_{ij} of Section 3.6 can be represented as sums of signed permutation matrices.]
    (b) What is true for a complex matrix that commutes with all unitary matrices?

8.2 MATRICES OVER THE RING OF POLYNOMIALS

For the remainder of this chapter we will be discussing matrices with polynomial entries. Unfortunately, this requires some care since the ring of polynomials $\mathcal{F}[x]$ does not form a field (see Theorem 6.2, Corollary 3). However, the reader should recall that it is possible to embed $\mathcal{F}[x]$ (or any integral domain for that matter) in a field of quotients as we saw in Section 6.5 (see Theorem 6.16). This simply means that quotients (i.e., rational functions) such as f(x)/g(x) are defined (if g ≠ 0), along with their inverses g(x)/f(x) (if f ≠ 0).

First of all, we will generally restrict ourselves to only the real and complex number fields. In other words, $\mathcal{F}$ will be taken to mean either $\mathbb{R}$ or $\mathbb{C}$ unless otherwise stated. Next, we introduce some additional simplifying notation. We denote $\mathcal{F}[x]$ (the ring of polynomials) by $\mathcal{P}$, and the associated field of quotients by $\mathcal{R}$ (think of $\mathcal{P}$ as meaning polynomial and $\mathcal{R}$ as meaning ratio). Thus, an m x n matrix with polynomial entries is an element of $M_{mxn}(\mathcal{P})$, and an m x n matrix over the field of quotients is an element of $M_{m\ x\ n}(\mathcal{R})$. Note that $M_{mxn}(\mathcal{P})$ is actually a subset of $M_{mxn}(\mathcal{R})$ since any polynomial p(x) may be written as p(x)/1.

It is important to realize that since $\mathcal{R}$ is a field, all of our previous results apply to $M_{mxn}(\mathcal{R})$ just as they do to $M_{mxn}(\mathcal{F})$. However, we need to reformulate some of our definitions in order to handle $M_{mxn}(\mathcal{P})$. In other words, as

long as we allow all operations in $\mathcal{R}$ there is no problem. Where we must be careful is when we restrict ourselves to multiplication by polynomials only (rather than by rational functions). To begin with, we must modify the definition of elementary row and column operations that we gave in Section 3.2. In particular, we now define the **$\mathcal{P}$-elementary** row (column) operations as follows. The type α operation remains the same, the type β operation is multiplication by $c \in \mathcal{F}$, and the type γ operation is now taken to be the addition of a polynomial multiple of one row (column) to another. In other words, if A_i is the i*th* row of $A \in M_{m \times n}(\mathcal{P})$, then the $\mathcal{P}$-elementary operations are:

(α) Interchange A_i and A_j.
(β) $A_i \rightarrow cA_i$ where $c \in \mathcal{F}$.
(γ) $A_i \rightarrow A_i + pA_j$ where $p \in \mathcal{P}$.

With these modifications, it is easy to see that all of our discussion on the techniques of reduction to row-echelon form remains valid, although now the distinguished elements of the matrix (i.e., the first nonzero entry in each row) will in general be polynomials (which we will assume to be monic). In other words, the row-echelon form of a matrix $A \in M_n(\mathcal{P})$ will in general be an upper-triangular matrix in $M_n(\mathcal{P})$ (which may, however, have zeros on the main diagonal). However, if $A \in M_n(\mathcal{P})$ is nonsingular, then $r(A) = n$, and the row-echelon form of A will be upper-triangular with nonzero monic polynomials down the main diagonal. (This is true since $M_n(\mathcal{P}) \subset M_n(\mathcal{R})$, and hence all of our results dealing with the rank remain valid for elements of $M_n(\mathcal{P})$). In other words, the row-echelon form of $A \in M_n(\mathcal{P})$ will be

$$\begin{pmatrix} p_{11} & p_{12} & p_{13} & \cdots & p_{1n} \\ 0 & p_{22} & p_{23} & \cdots & p_{2n} \\ 0 & 0 & p_{33} & \cdots & p_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & p_{nn} \end{pmatrix}$$

where each $p_{ij} \in \mathcal{P}$.

Example 8.2 Let us illustrate the basic approach in applying $\mathcal{P}$-elementary operations. For notational simplicity we will consider only the first column of a matrix $A \in M_3(\mathcal{P})$. Thus, suppose we have

$$\begin{pmatrix} x^2 - 2x + 1 \\ x - 1 \\ x^2 + 2 \end{pmatrix}.$$

Multiplying the second row by −x and adding to the third yields

$$\begin{pmatrix} x^2 - 2x + 1 \\ x - 1 \\ x + 2 \end{pmatrix}.$$

Adding −1 times the second row to the third and then multiplying the third by 1/3 now yields

$$\begin{pmatrix} x^2 - 2x + 1 \\ x - 1 \\ 1 \end{pmatrix}.$$

Adding −(x − 1) times the third row to the second, and $-(x^2 - 2x + 1)$ times the third to the first gives us

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

Finally, interchanging rows 1 and 3 will put this into row-echelon form. Note that while we came up with a field element in this last form, we could have ended up with some other nonconstant polynomial.

We now repeat this procedure on column 2, but only on rows 2 and 3 since only these rows have zeros in the first column. This results in a matrix that will in general have nonzero elements in row 1 of column 1, in rows 1 and 2 of column 2, and in all three rows of column 3. It should now be clear that when applied to any $A \in M_n(\mathcal{P})$, this procedure will result in an upper-triangular matrix. //

A moments thought should convince the reader that it will not be possible in general to transform a matrix in $M_n(\mathcal{P})$ to reduced row-echelon form if we allow only $\mathcal{P}$-elementary operations. For example, if the row-echelon form of $A \in M_2(\mathcal{P})$ is

$$\begin{pmatrix} x^2 + 1 & 2x - 3 \\ 0 & x^2 \end{pmatrix}$$

then it is impossible to add any polynomial multiple of the second row to the first to eliminate the $2x - 3$ term. This is exactly the type of difference that occurs between operations in the ring $\mathcal{P}$ and those in the field $\mathcal{R}$.

It should also be clear that we can define $\mathcal{P}$-elementary matrices in the obvious way, and that each $\mathcal{P}$-elementary matrix is also in $M_n(\mathcal{P})$. Moreover, each $\mathcal{P}$-elementary matrix has an inverse which is also in $M_n(\mathcal{P})$, as is its transpose (see Theorem 3.23). In addition, Theorem 4.5 remains valid for matrices over $\mathcal{P}$, as does Theorem 4.4 since replacing row A_i by $A_i + pA_j$ where p is a polynomial also has no effect on det A. This shows that if we reduce a matrix $A \in M_n(\mathcal{P})$ to its row-echelon form $\tilde{A}$, then the fact that $\tilde{A}$ is upper-triangular means that

$$\det \tilde{A} = k \det A$$

where k is a unit in $\mathcal{P}$ (recall from Example 6.4 that the units of the ring $\mathcal{P} = \mathcal{F}[x]$ are just the elements of $\mathcal{F}$, i.e., the nonzero constant polynomials). We will refer to units of $\mathcal{P}$ as (nonzero) **scalars**.

We say that a matrix $A \in M_n(\mathcal{P})$ is a **unit matrix** if A^{-1} exists and is also an element of $M_n(\mathcal{P})$. (Do not confuse a unit matrix with the identity matrix.) Note this is more restrictive than to say that $A \in M_n(\mathcal{P})$ is merely invertible, because we now also require that A^{-1} have entries only in $\mathcal{P}$, whereas in general it could have entries in $\mathcal{R}$. From our discussion above, we see that $\mathcal{P}$-elementary matrices are also unit matrices. The main properties of unit matrices that we shall need are summarized in the following theorem.

Theorem 8.3 If $A \in M_n(\mathcal{P})$ and $\tilde{A} \in M_n(\mathcal{P})$ is the row-echelon form of A, then

(a) A is a unit matrix if and only if A can be row-reduced to $\tilde{A} = I$.
(b) A is a unit matrix if and only if det A is a nonzero scalar.
(c) A is a unit matrix if and only if A is a product of $\mathcal{P}$-elementary matrices.

Proof (a) If A is a unit matrix, then A^{-1} exists so that $r(A) = n$ (Theorem 3.21). This means that the row-echelon form of A is an upper-triangular matrix $\tilde{A} = (p_{ij}) \in M_n(\mathcal{P})$ with n nonzero diagonal entries. Since $AA^{-1} = I$, it follows that $(\det A)(\det A^{-1}) = 1$ (Theorem 4.8 is also still valid) and hence $\det A \neq 0$. Furthermore, since both det A and $\det A^{-1}$ are in $\mathcal{P}$, Theorem 6.2(b) shows us that $\deg(\det A) = \deg(\det A^{-1}) = 0$ and thus det A is a scalar. Our discussion above showed that

$$k \det A = \det \tilde{A} = \prod_{i=1}^{n} p_{ii}$$

where k is a scalar, and therefore each polynomial p_{ii} must also be of degree zero (i.e., a scalar). In this case we can apply $\mathcal{P}$-elementary row operations to further reduce $\tilde{A}$ to the identity matrix I.

Conversely, if A is row-equivalent to $\tilde{A} = I$, then we may write

$$E_1 \cdots E_r A = I$$

where each $E_i \in M_n(\mathcal{P})$ is an elementary matrix. It follows that A^{-1} exists and is given by $A^{-1} = E_1 \cdots E_r \in M_n(\mathcal{P})$. Thus A is a unit matrix.

(b) If A is a unit matrix, then the proof of part (a) showed that det A is a nonzero scalar. On the other hand, if det A is a nonzero scalar, then the proof of part (a) showed that $\tilde{A} = E_1 \cdots E_r A = I$, and hence $A^{-1} = E_1 \cdots E_r \in M_n(\mathcal{P})$ so that A is a unit matrix.

(c) If A is a unit matrix, then the proof of part (a) showed that A may be written as a product of $\mathcal{P}$-elementary matrices. Conversely, if A is the product of $\mathcal{P}$-elementary matrices, then we may write $A = E_r^{-1} \cdots E_1^{-1} \in M_n(\mathcal{P})$. Therefore $A^{-1} = E_1 \cdots E_r \in M_n(\mathcal{P})$ also and hence A is a unit matrix. ∎

Recall from Section 5.4 that two matrices A, $B \in M_n(\mathcal{F})$ are said to be similar if there exists a nonsingular matrix $S \in M_n(\mathcal{F})$ such that $A = S^{-1}BS$. In order to generalize this, we say that two matrices A, $B \in M_{m\times n}(\mathcal{P})$ are equivalent over $\mathcal{P}$ if there exist unit matrices $P \in M_m(\mathcal{P})$ and $Q \in M_n(\mathcal{P})$ such that A = PBQ. The reader should have no trouble showing that this defines an equivalence relation on the set of all m x n matrices over $\mathcal{P}$.

Note that since P and Q are unit matrices, they may be written as a product of $\mathcal{P}$-elementary matrices (Theorem 8.3). Now recall from our discussion at the end of Section 3.8 that multiplying B from the right by an elementary matrix E has the same effect on the columns of B as multiplying from the left by E^T does on the rows. We thus conclude that if A and B are equivalent over $\mathcal{P}$, then A is obtainable from B by a sequence of $\mathcal{P}$-elementary row and column operations. Conversely, if A is obtainable from B by a sequence of $\mathcal{P}$-elementary row and column operations, the fact that each $E_i \in M_n(\mathcal{P})$ is a unit matrix means that A and B are $\mathcal{P}$-equivalent.

Theorem 8.4 (a) Two matrices A, $B \in M_{m\times n}(\mathcal{P})$ are equivalent over $\mathcal{P}$ if and only if A can be obtained from B by a sequence of $\mathcal{P}$-elementary row and column operations.

(b) $\mathcal{P}$-equivalent matrices have the same rank.

Proof (a) This was proved in the preceding discussion.

(b) Suppose A, B $\in M_{m\times n}(\mathcal{P})$ and A = PBQ where P $\in M_m(\mathcal{P})$ and Q $\in M_n(\mathcal{P})$ are unit matrices and hence nonsingular. Then, applying the corollary to Theorem 3.20, we have

$$\begin{aligned} r(A) = r(PBQ) &\le \min\{r(P), r(BQ)\} = \min\{m, r(BQ)\} = r(BQ) \\ &\le \min\{r(B), r(Q)\} = r(B) \ . \end{aligned}$$

Similarly, we see that $r(B) = r(P^{-1}AQ^{-1}) \le r(A)$ and hence r(A) = r(B). ∎

Another point that should be clarified is the following computational technicality that we will need to apply several times in the remainder of this chapter. Referring to Section 6.1, we know that the product of two polynomials $p(x) = \sum_{i=0}^{m} a_i x^i$ and $q(x) = \sum_{j=0}^{n} b_j x^j$ is given by

$$p(x)q(x) = \sum_{k=0}^{m+n} \sum_{t=0}^{k} a_t x^t b_{k-t} x^{k-t}$$

where we have been careful to write everything in its original order. In the special case that x, a_i, $b_j \in \mathcal{F}$, this may be written in the more common and simpler form

$$p(x)q(x) = \sum_{k=0}^{m+n} c_k x^k$$

where $c_k = \sum_{t=0}^{k} a_t b_{k-t}$. However, we will need to evaluate the product of two polynomials when the coefficients as well as the indeterminate x are matrices. In this case, none of the terms in the general form for pq can be assumed to commute with each other, and we shall have to be very careful in evaluating such products. We do though, have the following useful special case.

Theorem 8.5 Let $p(x) = \sum_{i=0}^{m} a_i x^i$ and $q(x) = \sum_{j=0}^{n} b_j x^j$ be polynomials with (matrix) coefficients a_i, $b_j \in M_s(\mathcal{F})$, and let $r(x) = \sum_{k=0}^{m+n} c_k x^k$ where $c_k = \sum_{t=0}^{k} a_t b_{k-t}$. Then if A $\in M_s(\mathcal{F})$ commutes with all of the $b_j \in M_s(\mathcal{F})$, we have p(A)q(A) = r(A).

Proof We simply compute using $Ab_j = b_jA$:

$$\begin{aligned} p(A)q(A) &= \sum_{k=0}^{m+n} \sum_{t=0}^{k} a_t A^t b_{k-t} A^{k-t} = \sum_{k=0}^{m+n} \sum_{t=0}^{k} a_t b_{k-t} A^k \\ &= \sum_{k=0}^{m+n} c_k A^k = r(A) \ . \ ∎ \end{aligned}$$

What this theorem has shown us is that if A commutes with all of the b_j, then we may use the simpler form for the product of two polynomials. As an interesting application of this result, we now give yet another (very simple) proof of the **Cayley-Hamilton theorem**. Suppose $A \in M_n(\mathcal{F})$, and consider its characteristic matrix $xI - A$ along with the characteristic polynomial $\Delta_A(x) = \det(xI - A)$. Writing equation (1b) of Section 4.3 in matrix notation we obtain

$$[\text{adj}(xI - A)](xI - A) = \Delta_A(x)I \ .$$

Now notice that any matrix with polynomial entries may be written as a polynomial with (constant) matrix coefficients (see the proof of Theorem 7.10). Then $\text{adj}(xI - A)$ is just a polynomial in x of degree $n - 1$ with (constant) matrix coefficients, and $xI - A$ is similarly a polynomial in x of degree 1. Since A obviously commutes with I and A, we can apply Theorem 8.5 with $p(x) = \text{adj}(xI - A)$ and $q(x) = xI - A$ to obtain $p(A)q(A) = \Delta_A(A)$. But $q(A) = 0$, and hence we find that $\Delta_A(A) = 0$.

The last technical point that we wish to address is the possibility of dividing two polynomials with matrix coefficients. The reason that this is a problem is that all of our work in Chapter 6 was based on the assumption that we were dealing with polynomials over a field, and the set of all square matrices of any fixed size certainly does not in general form a field. Referring back to the proof of the division algorithm (Theorem 6.3), we see that the process of dividing $f(x) = a_m x^m + \cdots + a_1 x + a_0$ by $g(x) = b_n x^n + \cdots + b_1 x + b_0$ depends on the existence of b_n^{-1}. This then allows us to show that $x - c$ is a factor of f(x) if and only if c is a root of f(x) (Corollary to Theorem 6.4).

We would like to apply Theorem 6.4 to a special case of polynomials with matrix coefficients. Thus, consider the polynomials $f(x) = B_n x + \cdots + B_1 x + B_0$ and $g(x) = xI - A$ where $A, B_i \in M_n(\mathcal{F})$. In this case, I is obviously invertible and we may divide g(x) into f(x) in the usual manner. The first two terms of the quotient q(x) are then given by

$$\begin{array}{r} B_n x^{n-1} + (B_{n-1} + B_n A)x^{n-2} \\ \hline xI - A \,\big)\, B_n x^n + B_{n-1}x^{n-1} + \cdots + B_1 x + B_0 \\ \underline{B_n x^n - B_n A x^{n-1}} \\ (B_{n-1} + B_n A)x^{n-1} \end{array}$$

It should now be clear (using Theorem 8.5) that Theorem 6.4 applies in this special case, and if $f(A) = 0$, then we may write $f(x) = q(x)(xI - A)$. In other words, if A is a root of f(x), then $xI - A$ is a factor of f(x). Note that in order

to divide $f(x) = B_n x^n + \cdots + B_0$ by $g(x) = A_m x^m + \cdots + A_0$, only the leading coefficient A_m of $g(x)$ need be invertible.

Let us also point out that because matrix multiplication is not generally commutative, the order in which we multiply the divisor and quotient is important when dealing with matrix coefficients. We will adhere to the convention used in the above example.

Another point that we should take note of is the following. Two polynomials $p(x) = \sum_{k=0}^{m} A_k x^k$ and $q(x) = \sum_{k=0}^{m} B_k x^k$ with coefficients in $M_n(\mathcal{F})$ are defined to be equal if $A_k = B_k$ for every $k = 1, \ldots, m$. For example, recalling that x is just an indeterminate, we consider the polynomial $p(x) = A_0 + A_1 x = A_0 + xA_1$. If $C \in M_n(\mathcal{F})$ does not commute with A_1 (i.e., $CA_1 \neq A_1 C$), then $A_0 + A_1 C \neq A_0 + CA_1$. This means that going from an equality such as $p(x) = q(x)$ to $p(C) = q(C)$ must be done with care in that the same convention for placing the indeterminate be applied to both $p(x)$ and $q(x)$.

Exercise

Determine whether or not each of the following matrices is a unit matrix by verifying each of the properties listed in Theorem 8.3:

$$(a)\ \begin{pmatrix} x+2 & 1 & -3x^3-6x^2 \\ 2x+6 & 2 & -6x^3-18x^2 \\ x^2+2x & x^2+x+1 & -3x^4-6x^3-3 \end{pmatrix}$$

$$(b)\ \begin{pmatrix} x+1 & x^2 & -2 \\ x^2-1 & x^3-x^2 & x+7 \\ 3x^2+3x & 3 & 0 \end{pmatrix}$$

$$(c)\ \begin{pmatrix} x^2+3x+2 & 0 & x & x^3-3x^2 \\ 2x^2+4x & x^2 & 0 & x-3 \\ x+2 & -x^2 & 1 & x^2-3x \\ 3x+6 & -6x^2 & 3 & 3x^2-9x \end{pmatrix}$$

8.3 THE SMITH CANONICAL FORM

If the reader has not studied (or does not remember) the Cauchy-Binet theorem (Section 4.6), now is the time to go back and read it. We will need this result several times in what follows, as well as the notation defined in that section.

We know that the norm of any integer is just its absolute value, and the greatest common divisor of a set of nonzero integers is just the largest *positive* integer that divides them all. Similarly, we define the **norm** of any polynomial to be its degree, and the **greatest common divisor** (frequently denoted by gcd) of a set of nonzero polynomials is the polynomial of highest degree that divides all of them. By convention, we will assume that the gcd is monic (i.e., the leading coefficient is 1).

Suppose $A \in M_{mxn}(\mathcal{P})$, and assume that $1 \le k \le \min\{m, n\}$. If A has at least one nonzero k-square subdeterminant, then we define f_k to be the greatest common divisor of all k*th* order subdeterminants of A. In other words,

$$f_k = \gcd\{\det A[\alpha|\beta]: \alpha \in INC(k, m), \beta \in INC(k, n)\} .$$

If there is no nonzero k*th* order subdeterminant, then we define $f_k = 0$. Furthermore, for notational convenience we define $f_0 = 1$. The numbers f_k are called the **determinantal divisors** of A. We will sometimes write $f_k(A)$ if there is more than one matrix under consideration.

Example 8.3 Suppose

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

Then the sets of nonzero 1-, 2- and 3-square subdeterminants are, respectively,

$$\{x, 2x^2, 1, x^3, x + 2, x^2, x + 2, x - 1\}$$

$$\{-x(2x^4 - x - 2), 2x^4 - x - 2, x^4 - x^3 - x^2 - 4x - 4, -x^2(x + 2), -x^2(x - 1), -x(2x^2 + 3x + 1), -(x + 2), -(x - 1)\}$$

$$\{2x^5 + 4x^4 - x^2 - 4x - 4\}$$

and hence $f_1 = 1$, $f_2 = 1$ and $f_3 = x^5 + 2x^4 - (1/2)x^2 - 2x - 2$. //

Our next result contains two very simple but important properties of determinantal divisors. Recall that the notation p|q means p divides q.

Theorem 8.6 (a) If $f_k = 0$, then $f_{k+1} = 0$.
(b) If $f_k \neq 0$, then $f_k | f_{k+1}$.

Proof Using Theorem 6.6, it is easy to see that these are both immediate consequences of Theorem 4.10 since a $(k + 1)$*th* order subdeterminant may be written as a linear combination of k*th* order subdeterminants. ∎

If $A \in M_{mxn}(\mathcal{P})$ has rank r, then Theorem 4.12 tells us that $f_r \neq 0$ while $f_{r+1} = 0$. Hence, according to Theorem 8.6(b), we may define the quotients q_k by

$$f_k = q_k f_{k-1}$$

for each $k = 1, \ldots, r$. The polynomials q_k are called the **invariant factors** of A. Note that $f_0 = 1$ implies $f_1 = q_1$, and hence

$$f_k = q_k f_{k-1} = q_k q_{k-1} f_{k-2} = \cdots = q_k q_{k-1} \cdots q_1 .$$

Because each f_k is defined to be monic, it follows that each q_k is also monic. Moreover, the unique factorization theorem (Theorem 6.6) shows that each q_k $(k = 1, \ldots, r)$ can be factored uniquely (except for order) into products of powers of prime (i.e., irreducible) polynomials as

$$q_k = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$$

where $p_1, \ldots, p_s$ are *all* the distinct prime factors of the invariant factors, and each e_i is a nonnegative integer. Of course, since every q_k will not necessarily contain all of the p_i's as factors, some of the e_i's may be zero.

Each of the factors $p_i^{e_i}$ for which $e_i > 0$ is called an **elementary divisor** of A. We count an elementary divisor once for each time that it appears as a factor of an invariant factor. This is because a given elementary divisor can appear as a factor in more than one invariant factor. Note also that the elementary divisors clearly depend on the field under consideration (see Example 6.7). However, the elementary divisors of a matrix over $\mathbb{C}[x]$ are always powers of linear polynomials (Theorem 6.13). As we shall see following Theorem 8.8 below, the list of elementary divisors determines the list of invariant factors, and hence the determinantal divisors.

Example 8.4 Let A_1 be the 3 x 3 matrix

$$A_1 = \begin{pmatrix} x & -1 & 0 \\ 0 & x & -1 \\ -1 & 1 & x-1 \end{pmatrix}$$

and note that $\det A_1 = (x - 1)(x^2 + 1)$. Now consider the block diagonal matrix

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_1 \end{pmatrix} .$$

Using Theorem 4.14, we immediately find

$$f_6 = \det A = (x - 1)^2(x^2 + 1)^2 .$$

We now observe that every 5 x 5 submatrix of A is either block triangular with a 3 x 3 matrix on its diagonal that contains one zero row (so the determinant is zero), or else is block diagonal with A_1 as one of the blocks (you should try to write out some of these and see this for yourself). Therefore

$$f_5 = (x - 1)(x^2 + 1)$$

and hence

$$q_6 = f_6/f_5 = (x - 1)(x^2 + 1) .$$

As to f_4, we see that some of the 4 x 4 subdeterminants contain $\det A_1$ while others (such as the one obtained by deleting both rows and columns 3 and 4) do not contain any factors in common with this. Thus $f_4 = 1$ and we must have $q_5 = f_5$. Since $f_6 = q_1q_2 \cdots q_6$, it follows that $q_4 = q_3 = q_2 = q_1 = 1$.

If we regard A as a matrix over $\mathbb{R}[x]$, then the elementary divisors of A are $x - 1$, $x^2 + 1$, $x - 1$, $x^2 + 1$. However, if we regard A as a matrix over $\mathbb{C}[x]$, then its elementary divisors are $x - 1$, $x + i$, $x - i$, $x - 1$, $x + i$, $x - i$. //

Theorem 8.7 Equivalent matrices have the same determinantal divisors.

Proof Suppose that A = PBQ. Applying the Cauchy-Binet theorem (the corollary to Theorem 4.15), we see that any k*th* order subdeterminant of A is just a sum of multiples of k*th* order subdeterminants of B. But then the gcd of all k*th* order subdeterminants of B must divide all the k*th* order subdeterminants of A. In other words, $f_k(B)|f_k(A)$. Conversely, writing $B = P^{-1}AQ^{-1}$ we see that $f_k(A)|f_k(B)$, and therefore $f_k(A) = f_k(B)$. ∎

From Example 8.4 (which was based on a relatively simple block diagonal matrix), it should be obvious that a brute force approach to finding invariant factors leaves much to be desired. The proof of our next theorem is actually nothing more than an algorithm for finding the invariant factors of any matrix A. The matrix B defined in the theorem is called the **Smith canonical** (or **normal**) **form** of A. After the proof, we give an example that should clarify the various steps outlined in the algorithm.

Theorem 8.8 (**Smith Canonical Form**) Suppose $A \in M_{m \times n}(\mathcal{P})$ has rank r. Then A has precisely r + 1 nonzero determinantal divisors $f_0, f_1, \ldots, f_r$, and A is equivalent over $\mathcal{P}$ to a unique diagonal matrix $B = (b_{ij}) \in M_{m \times n}(\mathcal{P})$ with $b_{ii} = q_i = f_i/f_{i-1}$ for $i = 1, \ldots, r$ and $b_{ij} = 0$ otherwise. Moreover $q_i | q_{i+1}$ for each $i = 1, \ldots, r - 1$.

Proof While we have already seen that A has precisely r + 1 nonzero determinantal divisors, this will also fall out of the proof below. Furthermore, the uniqueness of B follows from the fact that equivalence classes are disjoint, along with Theorem 8.7 (because determinantal divisors are defined to be monic). As to existence, we assume that $A \neq 0$ or it is already in Smith form. Note in the following that all we will do is perform a sequence of $\mathcal{P}$-elementary row and column operations on A. Recall that if E is an elementary matrix, then EA represents the same elementary row operation applied to A, and AE^T is the same operation applied to the columns of A. Therefore, what we will finally arrive at is a matrix of the form B = PAQ where $P = E_{i_1} \cdots E_{i_r}$ and $Q = E_{j_1}{}^T \cdots E_{j_s}{}^T$. Recall also that the norm of a polynomial is defined to be its degree.

Step 1. Search A for a nonzero entry of least norm and bring it to the (1, 1) position by row and column interchanges. By subtracting the appropriate multiples of row 1 from rows 2, . . . , m, we obtain a matrix in which every element of column 1 below the (1, 1) entry is either 0 or of smaller norm than the (1, 1) entry. Now perform the appropriate column operations to make every element of row 1 to the right of the (1, 1) entry either 0 or of smaller norm than the (1, 1) entry. Denote this new matrix by $\tilde{A}$.

Step 2. Search the first row and column of $\tilde{A}$ for a nonzero entry of least norm and bring it to the (1, 1) position. Now repeat the procedure of Step 1 to decrease the norm of every element of the first row and column outside the (1, 1) position by at least 1. Repeating this step a finite number of times, we must eventually arrive at a matrix A_1 equivalent to A which is 0 everywhere in the first row and column outside the (1, 1) position. Let us denote the (1, 1) entry of A_1 by a.

Step 3. Suppose b is the (i, j) element of A_1 (where $i, j > 1$) and $a \nmid b$. If no such b exists, then go on to Step 4. Put b in the (1, j) position by adding row i

to row 1. Since $a \nmid b$, we may write $b = aq + r$ where $r \neq 0$ and $\deg r < \deg a$ (Theorem 6.3). We place r in the (1, j) position by subtracting q times column 1 from column j. This results in a matrix with an entry of smaller norm than that of a. Now repeat Steps 1 and 2 with this matrix to obtain a new matrix A_2 equivalent to A which is 0 everywhere in the first row and column outside the (1, 1) position.

This process is repeated with A_2 to obtain A_3 and so forth. We thus obtain a sequence $A_1, A_2, \ldots, A_s$ of matrices in which the norms of the (1, 1) entries are strictly decreasing, and in which all elements of row 1 and column 1 are 0 outside the (1, 1) position. Furthermore, we go on from A_p to obtain A_{p+1} only as long as there is an element of $A_p(1|1)$ that is not divisible by the (1, 1) element of A_p. Since the norms of the (1, 1) entries are strictly decreasing, this process must terminate with a matrix $C = (c_{ij}) \in M_{m\times n}(\mathcal{P})$ equivalent to A and having the following properties:

(i) $c_{11} | c_{ij}$ for every $i, j > 1$;
(ii) $c_{1j} = 0$ for every $j = 2, \ldots, n$;
(iii) $c_{i1} = 0$ for every $i = 2, \ldots, m$.

Step 4. Now repeat the entire procedure on the matrix C, except that this time apply the $\mathcal{P}$-elementary row and column operations to rows $2, \ldots, m$ and columns $2, \ldots, n$. This will result in a matrix $D = (d_{ij})$ that has all 0 entries in the first two rows and columns except for the (1, 1) and (2, 2) entries. Since $c_{11} | c_{ij}$ (for $i, j > 1$), it follows that $c_{11} | d_{ij}$ for all i, j. (This true because every element of D is just a linear combination of elements of C.) Thus the form of D is

$$D = \begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ 0 & d & \cdots & 0 \\ \vdots & \vdots & G & \\ 0 & 0 & & \end{pmatrix}$$

where $G = (g_{ij}) \in M_{(m-2)\times(n-2)}(\mathcal{P})$, $c_{11} | d$ and $c_{11} | g_{ij}$ for $i = 1, \ldots, m-2$ and $j = 1, \ldots, n-2$. It is clear that we can continue this process until we eventually obtain a diagonal matrix $H = (h_{ij}) \in M_{m\times n}(\mathcal{P})$ with the property that $h_{ii} | h_{i+1\, i+1}$ and $h_{i+1\, i+1} \neq 0$ for $i = 1, \ldots, p-1$ (where $p = \operatorname{rank} H$). But H is equivalent to A so that H and A have the same determinantal divisors (Theorem 8.7) and $p = r(H) = r(A) = r$ (Theorem 8.4(b)).

For each k with $1 \leq k \leq r$, we observe that the only nonzero k-square subdeterminants of H are of the form $\prod_{s=1}^{k} h_{i_s i_s}$, and the gcd of all such products is

$$f_k = \prod_{i=1}^{k} h_{ii}$$

(since $h_{ii}|h_{i+1\ i+1}$ for i = 1, . . . , r − 1). But then applying the definition of invariant factors, we see that

$$\prod_{i=1}^{k} h_{ii} = f_k = \prod_{i=1}^{k} q_i \quad .$$

In particular, this shows us that

$$\begin{aligned} h_{11} &= q_1 \\ h_{11}h_{22} &= q_1q_2 \\ &\vdots \\ h_{11}\cdots h_{rr} &= q_1\cdots q_r \end{aligned}$$

and hence $h_{22} = q_2, \ldots, h_{rr} = q_r$ also. In other words, H is precisely the desired matrix B. Finally, note that $h_{ii}|h_{i+1\ i+1}$ is just the statement that $q_i|q_{i+1}$. ∎

Suppose $A \in M_{mxn}(\mathcal{P})$ has rank r, and suppose that we are given a list of all the elementary divisors of A. From Theorem 8.8, we know that $q_i|q_{i+1}$ for i = 1, . . . , r − 1. Therefore, to compute the invariant factors of A, we first multiply together the highest powers of all the *distinct* primes that appear in the list of elementary divisors. This gives us q_r. Next, we multiply together the highest powers of the remaining distinct primes to obtain q_{r-1} . Continuing this process until the list of elementary divisors is exhausted, suppose that q_k is the last invariant factor so obtained. If k > 1, we then set $q_1 = \cdots = q_{k-1} = 1$. The reader should try this on the list of elementary divisors given at the end of Example 8.4.

Corollary If $A, B \in M_{mxn}(\mathcal{P})$, then A is $\mathcal{P}$-equivalent to B if and only if A and B have the same invariant factors (or determinantal divisors or elementary divisors).

Proof Let A_S and B_S be the Smith forms for A and B. If A and B have the same invariant factors then they have the same Smith form. If we denote $\mathcal{P}$-equivalence by ≈ , then $A \approx A_S = B_S \approx B$ so that A ≈ B. Conversely, if A ≈ B then $A \approx B \approx B_S$ implies that $A \approx B_S$, and hence the uniqueness of A_S implies that $A_S = B_S$, and thus A and B have the same invariant factors.

If we recall Theorem 6.6, then the statement for elementary divisors follows immediately. Now note that $f_0 = 1$ so that $f_1 = q_1$, and in general we then have $f_k = q_kf_{k-1}$. This takes care of the statement for determinantal divisors. ∎

Example 8.5 Consider the matrix A given in Example 7.3. We shall compute the invariant factors of the associated characteristic matrix xI − A. The reason for using the characteristic matrix will become clear in a later section. According to Step 1, we obtain the following sequence of equivalent matrices. Start with

$$xI - A = \begin{pmatrix} x-2 & -1 & 0 & 0 \\ 0 & x-2 & 0 & 0 \\ 0 & 0 & x-2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

Put −1 in the (1, 1) position:

$$\begin{pmatrix} -1 & x-2 & 0 & 0 \\ x-2 & 0 & 0 & 0 \\ 0 & 0 & x-2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

Add x − 2 times row 1 to row 2, and x − 2 times column 1 to column 2:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & (x-2)^2 & 0 & 0 \\ 0 & 0 & x-2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

Since all entries in row 1 and column 1 are 0 except for the (1, 1) entry, this last matrix is A_1 and we have also finished Step 2. Furthermore, there is no element $b \in A_1$ that is not divisible by −1, so we go on to Step 4 applied to the 3 x 3 matrix in the lower right hand corner. In this case, we first apply Step 1 and then follow Step 3. We thus obtain the following sequence of matrices. Put x − 2 in the (2, 2) position:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & x-2 & 0 & 0 \\ 0 & 0 & (x-2)^2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

$(x-2) \nmid (x-5)$ so add row 4 to row 2:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & x-2 & 0 & x-5 \\ 0 & 0 & (x-2)^2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

Note $x - 5 = 1(x - 2) + (-3)$, so subtract 1 times column 2 from column 4:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & x-2 & 0 & -3 \\ 0 & 0 & (x-2)^2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

Now put -3 in the (2, 2) position:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -3 & 0 & x-2 \\ 0 & 0 & (x-2)^2 & 0 \\ 0 & x-5 & 0 & 0 \end{pmatrix}.$$

Add $(x - 5)/3$ times row 2 to row 4, and then add $(x - 2)/3$ times column 2 to column 4 to obtain

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & (x-2)^2 & 0 \\ 0 & 0 & 0 & (x-2)(x-5)/3 \end{pmatrix}.$$

Elementary long division (see Example 6.2) shows that $(x - 2)(x - 5)/3$ divided by $(x - 2)^2$ equals $1/3$ with a remainder of $-x + 2$. Following Step 3, we add row 4 to row 3 and then subtract 1/3 times column 3 from column 4 to obtain

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & (x-2)^2 & -x+2 \\ 0 & 0 & 0 & (x-2)(x-5)/3 \end{pmatrix}.$$

Going back to Step 1, we first put $-x + 2 = -(x - 2)$ in the (3, 3) position. We then add $(x - 5)/3$ times row 3 to row 4 and $(x - 2)$ times column 3 to column 4 resulting in

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & -(x-2) & 0 \\ 0 & 0 & 0 & (x-2)^2(x-5)/3 \end{pmatrix}.$$

Lastly, multiplying each row by a suitable nonzero scalar we obtain the final (unique) Smith form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x-2 & 0 \\ 0 & 0 & 0 & (x-2)^2(x-5) \end{pmatrix}. \; /\!/$$

Exercises

1. Find the invariant factors of the matrix A given in Example 8.4 by using the list of elementary divisors also given in that example.

2. For each of the following matrices A, find the invariant factors of the characteristic matrix xI – A:

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

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

8.4 SIMILARITY INVARIANTS

Recall that A, B $\in M_n(\mathcal{F})$ are similar over $\mathcal{F}$ if there exists a nonsingular matrix S $\in M_n(\mathcal{F})$ such that $A = S^{-1}BS$. Note that similar matrices are therefore also equivalent, although the converse is certainly not true (since in general $P \neq Q^{-1}$ in our definition of equivalent matrices). For our present purposes however, the following theorem is quite useful.

Theorem 8.9 Two matrices A, B $\in M_n(\mathcal{F})$ are similar over $\mathcal{F}$ if and only if their characteristic matrices xI − A and xI − B are equivalent over $\mathcal{P} = \mathcal{F}[x]$. In particular, if xI − A = P(xI − B)Q where $Q^{-1} = R_m x^m + \cdots + R_1 x + R_0$, then $A = S^{-1}BS$ where $S^{-1} = R_m B^m + \cdots + R_1 B + R_0$.

Proof If A and B are similar, then there exists a nonsingular matrix S $\in M_n(\mathcal{F})$ for which $A = S^{-1}BS$, and hence

$$xI - A = xI - S^{-1}BS = S^{-1}(xI - B)S \ .$$

But S is a unit matrix in $M_n(\mathcal{P})$, and therefore xI − A and xI − B are $\mathcal{P}$-equivalent.

On the other hand, if xI − A and xI − B are $\mathcal{P}$-equivalent, then there exist unit matrices P, Q $\in M_n(\mathcal{P})$ such that

$$xI - A = P(xI - B)Q \ .$$

We wish to find a matrix S $\in M_n(\mathcal{F})$ for which $A = S^{-1}BS$. Since Q $\in M_n(\mathcal{P})$ is a unit matrix, we may apply Theorem 4.11 to find its inverse R $\in M_n(\mathcal{P})$ which is also a unit matrix and hence will also have polynomial entries. In fact, we may write (as in the proof of Theorem 7.10)

$$R = R_m x^m + R_{m-1} x^{m-1} + \cdots + R_1 x + R_0 \qquad (1)$$

where m is the highest degree of any polynomial entry of R and each $R_i \in M_n(\mathcal{F})$.

From xI − A = P(xI − B)Q and the fact that P and Q are unit matrices we have

$$P^{-1}(xI - A) = (xI - B)Q = Qx - BQ \ . \qquad (2)$$

Now recall Theorem 8.5 and the discussion following its proof. If we write both P^{-1} and Q $\in M_n(\mathcal{P})$ in the same form as we did in (1) for R, then we may replace x by A in the resulting polynomial expression for Q to obtain a matrix

$W \in M_n(\mathcal{F})$. Since A commutes with I and A, and $B \in M_n(\mathcal{F})$, we may apply Theorem 8.5 and replace x by A on both sides of (2), resulting in

$$0 = WA - BW \ .$$

Since R is the inverse of Q and $Qx^i = x^iQ$, we have RQ = I or (from (1))

$$R_mQx^m + R_{m-1}Qx^{m-1} + \cdots + R_1Qx + R_0Q = I \ .$$

Replacing x by A in this expression yields

$$\sum_{i=0}^{m} R_i W A^i = I \ . \tag{3}$$

But WA = BW so that $WA^2 = BWA = B^2W$ and, by induction, it follows that $WA^i = B^iW$. Using this in (3) we have

$$\left(\sum_{i=0}^{m} R_i B^i\right) W = I$$

so defining

$$S^{-1} = \sum_{i=0}^{m} R_i B^i \in M_n(\mathcal{F}) \tag{4}$$

we see that $S^{-1} = W^{-1}$ and hence W = S. Finally, noting that WA = BW implies $A = W^{-1}BW$, we arrive at $A = S^{-1}BS$ as desired. ∎

Corollary 1 Two matrices $A, B \in M_n(\mathcal{F})$ are similar if and only if their characteristic matrices have the same invariant factors (or elementary divisors).

Proof This follows directly from Theorem 8.9 and the corollary to Theorem 8.8. ∎

Corollary 2 If A and B are in $M_n(\mathbb{R})$, then A and B are similar over $\mathbb{C}$ if and only if they are similar over $\mathbb{R}$.

Proof Clearly, if A and B are similar over $\mathbb{R}$ then they are also similar over $\mathbb{C}$. On the other hand, suppose that A and B are similar over $\mathbb{C}$. We claim that the algorithm in the proof of Theorem 8.9 yields a real S if A and B are real. From the definition of S in the proof of Theorem 8.9 (equation (4)), we see that S will be real if all of the R_i are real (since each B^i is real by hypothesis), and this in turn requires that Q be real (since $R = Q^{-1}$). That P and Q can indeed be chosen to be real is left as an exercise for the reader (see Exercise 8.4.1). ∎

The invariant factors of the characteristic matrix of A are called the **similarity invariants** of A. We will soon show that the similarity invariant of highest degree is just the minimal polynomial for A.

Example 8.6 Let us show that the matrices

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$$

are similar over $\mathbb{R}$. We have the characteristic matrices

$$xI - A = \begin{pmatrix} x-1 & -1 \\ -1 & x-1 \end{pmatrix} \qquad \text{and} \qquad xI - B = \begin{pmatrix} x & 0 \\ 0 & x-2 \end{pmatrix}$$

and hence the determinantal divisors are easily seen to be $f_1(A) = 1$, $f_2(A) = x(x-2)$, $f_1(B) = 1$, $f_2(B) = x(x-2)$. Thus $f_1(A) = f_1(B)$ and $f_2(A) = f_2(B)$ so that A and B must be similar by the corollary to Theorem 8.9.

For the sake of illustration, we will show how to compute the matrix S^{-1} following the method used in the proof of Theorem 8.9 (see equation (4)). While there is no general method for finding the matrices P and Q, the reader can easily verify that if we choose

$$P = \begin{pmatrix} 1 & x^2 - x + 1 \\ -1 & -x^2 + x + 1 \end{pmatrix} \qquad Q = \frac{1}{2}\begin{pmatrix} -x^2 + 3x - 1 & -x^2 + 3x - 1 \\ 1 & 1 \end{pmatrix}$$

then $xI - A = P(xI - B)Q$. It is then easy to show that

$$\begin{aligned} R = Q^{-1} &= \begin{pmatrix} 1 & x^2 - 3x + 3 \\ -1 & -x^2 + 3x - 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}x^2 + \begin{pmatrix} 0 & -3 \\ 0 & -3 \end{pmatrix}x + \begin{pmatrix} 1 & 3 \\ -1 & -1 \end{pmatrix} \end{aligned}$$

and hence (from (4)) we have

$$S^{-1} = \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}^2 + \begin{pmatrix} 0 & -3 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 3 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} . \ \text{//}$$

Now recall the definition of minimal polynomial given in Section 7.3 (see the discussion following the proof of Theorem 7.10). We also recall that the minimal polynomial m(x) for $A \in M_n(\mathcal{F})$ divides the characteristic polynomial $\Delta_A(x)$. In the particular case that $m(x) = \Delta_A(x)$, the matrix A is called **nonderogatory**, and if $m(x) \neq \Delta_A(x)$, then (as you might have guessed) A is said to be **derogatory**. Our next theorem is of fundamental importance.

Theorem 8.10 The minimal polynomial m(x) for $A \in M_n(\mathcal{F})$ is equal to its similarity invariant of highest degree.

Proof Since $\Delta_A(x) = \det(xI - A)$ is just a (monic) polynomial of degree n in x, it is clearly nonzero, and hence $q_n(x)$, the similarity invariant of highest degree, is also nonzero. Now define the matrix $Q(x) = \text{adj}(xI - A)$, and note that the entries of Q(x) are precisely all the (n − 1)-square subdeterminants of xI − A. This means $f_{n-1}(x)$ (i.e., the $(n-1)$*th* determinantal divisor of xI − A) is just the monic gcd of all the entries of Q(x), and therefore we may write

$$Q(x) = f_{n-1}(x)D(x)$$

where the matrix D(x) has entries that are relatively prime. Noting that by definition we have $\Delta_A(x) = f_n(x) = q_n(x)f_{n-1}(x)$, it follows that

$$f_{n-1}(x)D(x)(xI - A) = Q(x)(xI - A) = \Delta_A(x)I = q_n(x)f_{n-1}(x)I \tag{1}$$

where we used equation (1b) of Section 4.3. Since $f_{n-1}(x) \neq 0$ (by Theorem 8.6(a) and the fact that $f_n(x) \neq 0$), we must have

$$D(x)(xI - A) = q_n(x)I \tag{2}$$

(this follows by equating the polynomial entries of the matrices on each side of (1) and then using Corollary 2(b) of Theorem 6.2).

By writing both sides of (2) as polynomials with matrix coefficients and then applying Theorem 8.5, it follows that $q_n(A) = 0$ and hence $m(x)|q_n(x)$ (Theorem 7.4). We may now define the polynomial p(x) by writing

$$q_n(x) = m)x)p(x) \ . \tag{3}$$

By definition, A is a root of m(x), and therefore our discussion at the end of Section 8.2 tells us that we may apply Theorem 6.4 to write

$$m(x)I = C(x)(xI - A)$$

where C(x) is a polynomial with matrix coefficients. Using this in (2) we have

$$D(x)(xI - A) = q_n(x)I = p(x)m(x)I = p(x)C(x)(xI - A) \tag{4}$$

where we used the fact that m(x) and p(x) are just polynomials with scalar coefficients so that m(x)p(x) = p(x)m(x).

Since $\det(xI - A) \neq 0$, we know that $(xI - A)^{-1}$ exists over $M_n(\mathcal{R})$, and thus (4) implies that

$$D(x) = p(x)C(x) \ .$$

Now regarding both D(x) and C(x) as matrices with polynomial entries, this equation shows that p(x) divides each of the entries of D(x). But the entries of D(x) are relatively prime, and hence p(x) must be a unit (i.e., a nonzero scalar). Since both m(x) and $q_n(x)$ are monic by convention, (3) implies that p(x) = 1, and therefore $q_n(x) = m(x)$. ∎

Corollary A matrix $A \in M_n(\mathcal{F})$ is nonderogatory if and only if its first n − 1 similarity invariants are equal to 1.

Proof Let A have characteristic polynomial $\Delta_A(x)$ and minimal polynomial m(x). Using the definition of invariant factors and Theorem 8.10 we have

$$\begin{aligned}\Delta_A(x) = \det(xI - A) = f_n(x) &= q_n(x)q_{n-1}(x)\cdots q_1(x) \\ &= m(x)q_{n-1}(x)\cdots q_1(x) \ .\end{aligned}$$

Clearly, if $q_{n-1}(x) = \cdots = q_1(x) = 1$ then $\Delta_A(x) = m(x)$. On the other hand, if $\Delta_A(x) = m(x)$, then $q_{n-1}(x) \cdots q_1(x) = 1$ (Theorem 6.2, Corollary 2(b)) and hence each $q_i(x)$ (i = 1, . . . , n − 1) is a nonzero scalar (Theorem 6.2, Corollary 3). Since each $q_k(x)$ is defined to be monic, it follows that $q_{n-1}(x) = \cdots = q_1(x) = 1$. ∎

Example 8.7 Comparison of Examples 7.3 and 8.8 shows that the minimal polynomial of the matrix A is indeed the same as its similarity invariant of highest degree. //

Exercises

1. Finish the proof of Corollary 2 to Theorem 8.9.

2. Show that the minimal polynomial for $A \in M_n(\mathcal{F})$ is the least common multiple of the elementary divisors of $xI - A$.

3. If $(x^2 - 4)^4$ is the minimal polynomial of an n-square matrix A, can $A^6 - A^4 + A^2 - I_n$ ever be zero? If $(x^2 - 4)^3$ is the minimal polynomial, can $A^8 - A^4 + A^2 - I_n = 0$? Explain.

4. Is the matrix
$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$
derogatory or nonderogatory? Explain.

5. Suppose A is an n-square matrix and p is a polynomial with complex coefficients. If $p(A) = 0$, show that $p(SAS^{-1}) = 0$ for any nonsingular n-square S. Is this true if p is a polynomial with n-square matrices as coefficients?

6. Prove or disprove:
(a) The elementary divisors of A are all linear if and only if the characteristic polynomial of A is a product of distinct linear factors.
(b) The elementary divisors of A are all linear if and only if the minimal polynomial of A is a product of distinct linear factors.

7. Prove or disprove:
(a) There exists a real nonsingular matrix S such that $SAS^{-1} = B$ where
$$A = \begin{pmatrix} 3 & 0 \\ -1 & 2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 4 & 2 \\ -1 & 1 \end{pmatrix}.$$
(b) There exists a complex nonsingular matrix S such that $SAS^{-1} = B$ where
$$A = \begin{pmatrix} 3 & 0 \\ -1 & 2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 4 & 2i \\ i & 1 \end{pmatrix}.$$

8.5 THE RATIONAL CANONICAL FORM

Given any monic polynomial $p(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0 \in \mathcal{F}[x]$, the matrix $C(p(x)) \in M_n(\mathcal{F})$ defined by

$$C(p(x)) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{n-1} \end{pmatrix}$$

is called the **companion matrix** of the polynomial p(x). If there is no possible ambiguity, we will denote the companion matrix simply by C. The companion matrix has several interesting properties that we will soon discover. We will also make use of the associated characteristic matrix $xI - C \in M_n(\mathcal{R})$ given by

$$xI - C = \begin{pmatrix} x & 0 & \cdots & 0 & 0 & -a_0 \\ -1 & x & \cdots & 0 & 0 & -a_1 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & x & -a_{n-2} \\ 0 & 0 & \cdots & 0 & -1 & x - a_{n-1} \end{pmatrix}.$$

Our next theorem is quite useful.

Theorem 8.11 Let $p(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0 \in \mathcal{F}[x]$ have companion matrix C. Then $\det(xI - C) = p(x)$.

Proof We proceed by induction on the degree of p(x). If n = 1, then $p(x) = x - a_0$, $C = (a_0)$ and $xI - C = (x - a_0)$ so that

$$\det(xI - C) = x - a_0 = p(x) .$$

Now assume that the theorem is true for all polynomials of degree less than n, and suppose deg p(x) = n > 1. If we expand det(xI – C) by minors of the first row, we obtain (see Theorem 4.10)

$$\det(xI - C) = x \det C_{11} + (-a_0)(-1)^{n+1} \det C_{1n}$$

where the minor matrices C_{11} and C_{1n} are given by

$$C_{11} = \begin{pmatrix} x & 0 & \cdots & 0 & 0 & -a_1 \\ -1 & x & \cdots & 0 & 0 & -a_2 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & x & -a_{n-2} \\ 0 & 0 & \cdots & 0 & -1 & x - a_{n-1} \end{pmatrix}$$

$$C_{1n} = \begin{pmatrix} -1 & x & 0 & \cdots & 0 & 0 \\ 0 & -1 & x & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & x \\ 0 & 0 & 0 & \cdots & 0 & -1 \end{pmatrix} .$$

Defining the polynomial $p'(x) = x^{n-1} - a_{n-1}x^{n-2} - \cdots - a_2x - a_1$ along with its companion matrix C', we see that $C_{11} = xI - C'$. By our induction hypothesis, it then follows that

$$\det C_{11} = \det(xI - C') = p'(x) .$$

Next we note that C_{1n} is an upper-triangular matrix, and hence (by Theorem 4.5) $\det C_{1n} = (-1)^{n-1}$. Putting all of this together we find that

$$\det(xI - C) = xp'(x) - a_0 = p(x) . \blacksquare$$

Recall that two matrix representations are similar if and only if they represent the same underlying operator in two different bases (see Theorem 5.18).

Theorem 8.12 (a) The companion matrix $C = C(p(x))$ of any monic polynomial $p(x) \in \mathcal{F}[x]$ has $p(x)$ as its minimal polynomial $m(x)$.

(b) If $\dim V = n$ and $T \in L(V)$ has minimal polynomial $m(x)$ of degree n, then $C(m(x))$ represents T relative to some basis for V.

Proof (a) From the preceding proof, we see that deleting the first row and n*th* column of $xI - C$ and taking the determinant yields $\det C_{1n} = (-1)^{n-1}$. Therefore $f_{n-1}(x) = 1$ so that $q_1(x) = q_2(x) = \cdots = q_{n-1}(x) = 1$. Hence C is nonderogatory (corollary to Theorem 8.10), so that by Theorem 8.11 we have $m(x) = q_n(x) = \det(xI - C) = p(x)$.

(b) Note $\dim V = \deg \Delta_T(x) = n = \deg m(x)$ so that any $[T]$ has similarity invariants $q_1(x) = \cdots = q_{n-1}(x) = 1$ and $q_n(x) = m(x)$ (see Theorem 8.10 and its corollary). Since the proof of part (a) showed that $C = C(m(x))$ has the

same similarity invariants as [T], it follows from Corollary 1 of Theorem 8.9 that C and [T] are similar. ∎

Note that Theorems 8.11 and 8.12(a) together show that the companion matrix is nonderogatory.

Given any $A \in M_n(\mathcal{F})$, we can interpret A as the matrix representation of a linear transformation T on an n-dimensional vector space V. If A has minimal polynomial m(x) with deg m(x) = n, then so does T (by Theorem 7.1). Hence the companion matrix C of m(x) represents T relative to some basis for V (Theorem 8.12(b)). This means that A is similar to C (Theorem 5.18), and therefore $C = P^{-1}AP$ for some nonsingular transition matrix $P \in M_n(\mathcal{F})$. But then

$$xI - C = xI - P^{-1}AP = P^{-1}(xI - A)P$$

and hence det(xI − C) = det(xI − A) by Theorem 4.8 and its corollary. Using Theorem 8.11, we then have the following result.

Theorem 8.13 Let $A \in M_n(\mathcal{F})$ have minimal polynomial m(x) of degree n. Then m(x) = det(xI − A).

Our next theorem is a useful restatement of what we have done so far in this section.

Theorem 8.14 Let $p(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0 \in \mathcal{F}[x]$. Then the companion matrix C(p(x)) is nonderogatory, and its characteristic polynomial $\Delta_C(x)$ and minimal polynomial m(x) both equal p(x). Moreover, xI − C is equivalent over $\mathcal{P}$ to the n x n matrix (the Smith canonical form of xI − C)

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & p(x) \end{pmatrix}.$$

For notational convenience, we sometimes write a diagonal matrix by listing its diagonal entries. For example, the matrix shown in the above theorem would be written as diag(1, . . . , 1, p(x)).

Theorem 8.15 If $A \in M_n(\mathcal{F})$, then A is similar over $\mathcal{F}$ to the direct sum of the companion matrices of its nonunit similarity invariants.

Proof The proof is an application of Theorem 8.9. Assume that $A \neq cI$ (where $c \in \mathcal{F}$) or there is nothing to prove. Hence $f_1(x)$, the first determinantal divisor of $xI - A$, must be 1. But $f_0(x) = 1$ by definition, and hence we have $f_1(x) = q_1(x)f_0(x) = q_1(x) = 1$. Since at least $q_1(x) = 1$, we now assume that in fact the first k similarity invariants of A are equal to 1. In other words, we assume that $q_1(x) = \cdots = q_k(x) = 1$, and then $\deg q_i(x) = d_i \geq 1$ for $i = k + 1, \ldots, n$.

Since $f_n(x) = q_1(x) \cdots q_n(x)$, Theorem 6.2(b) tells us that $\deg f_n(x) = \sum_{j=1}^{n} \deg q_j(x)$ and hence (using $\deg q_j = 0$ for $j = 1, \ldots, k$)

$$n = \deg \Delta_A(x) = \deg f_n(x) = \sum_{j=k+1}^{n} \deg q_j(x) = \sum_{j=k+1}^{n} d_j \quad .$$

Let $Q_i = C(q_i(x)) \in M_{d_i}(\mathcal{P})$ for $i = k + 1, \ldots, n$. We want to show that $xI - A$ is equivalent over $\mathcal{P}$ to

$$xI - (Q_{k+1} \oplus \cdots \oplus Q_n) = (xI - Q_{k+1}) \oplus \cdots \oplus (xI - Q_n) \quad .$$

(Note that each of the identity matrices in this equation may be of a different size.)

It should be clear that the Smith form of $xI - A$ is the diagonal $n \times n$ matrix

$$(xI - A)_S = \operatorname{diag}(q_1(x), \ldots, q_n(x)) = \operatorname{diag}(1, \ldots, 1, q_{k+1}(x), \ldots, q_n(x)) \quad .$$

From Theorem 8.14, we know that $(xI - Q_i)_S = \operatorname{diag}(1, \ldots, 1, q_i(x)) \in M_{d_i}(\mathcal{P})$. Since $\sum_{i=k+1}^{n} d_i = n$, we now see that by suitable row and column interchanges we have

$$xI - A \approx (xI - A)_S \approx (xI - Q_{k+1})_S \oplus \cdots \oplus (xI - Q_n)_S \qquad (*)$$

where $\approx$ denotes equivalence over $\mathcal{P}$.

If we write $(xI - Q_i)_S = E_i(xI - Q_i)F_i$ where E_i and F_i are unit matrices, then (by multiplying out the block diagonal matrices) it is easy to see that

$$\begin{aligned} &E_{k+1}(xI - Q_{k+1})F_{k+1} \oplus \cdots \oplus E_n(xI - Q_n)F_n \\ &\quad = [E_{k+1} \oplus \cdots \oplus E_n][(xI - Q_{k+1}) \oplus \cdots \oplus (xI - Q_n)][F_{k+1} \oplus \cdots \oplus F_n] \quad . \end{aligned}$$

Since the direct sum of unit matrices is clearly a unit matrix (so that both $E_{k+1} \oplus \cdots \oplus E_n$ and $F_{k+1} \oplus \cdots \oplus F_n$ are unit matrices), this shows that the right hand side of (*) is equivalent to $(xI - Q_{k+1}) \oplus \cdots \oplus (xI - Q_n)$. (Note we have shown that if $\{S_i\}$ and $\{T_i\}$ are finite collections of matrices such that $S_i \approx T_i$, then it follows that $S_1 \oplus \cdots \oplus S_n \approx T_1 \oplus \cdots \oplus T_n$.) Therefore $xI - A$

is equivalent to $xI - (Q_{k+1} \oplus \cdots \oplus Q_n)$ which is what we wanted to show. The theorem now follows directly from Theorem 8.9. ∎

We are now in a position to prove the **rational canonical form** theorem. Note that the name is derived from the fact that the rational form of a matrix is obtained by the application of a finite number of rational operations (which essentially constitute the Smith algorithm).

Theorem 8.16 (**Rational Canonical Form**) A matrix $A \in M_n(\mathcal{F})$ is similar over $\mathcal{F}$ to the direct sum of the companion matrices of the elementary divisors of $xI - A$.

Proof As in the proof of Theorem 8.15, we assume that the first k similarity invariants of A are $q_1(x) = \cdots = q_k(x) = 1$ and that $\deg q_i(x) = d_i \geq 1$ for $i = k + 1, \ldots, n$. Changing notation slightly from our first definition, we write each nonunit invariant factor as a product of powers of prime polynomials (i.e., as a product of elementary divisors): $q_i(x) = e_{i1}(x) \cdots e_{im_i}(x)$ for each $i = k + 1, \ldots, n$. From Theorem 8.14, we know that $xI - Q_i = xI - C(q_i(x))$ is $\mathcal{P}$-equivalent to the $d_i \times d_i$ matrix

$$B_i = \operatorname{diag}(1, \ldots, 1, q_i(x)) \ .$$

Similarly, if $c_{ij} = \deg e_{ij}(x)$, each $xI - C(e_{ij}(x))$ $(j = 1, \ldots, m_i)$ is $\mathcal{P}$-equivalent to a $c_{ij} \times c_{ij}$ matrix

$$D_{ij} = \operatorname{diag}(1, \ldots, 1, e_{ij}(x)) \ .$$

Since $\deg q_i(x) = \sum_j \deg e_{ij}(x)$, it follows that the block diagonal matrix

$$\begin{aligned} D_i &= D_{i1} \oplus \cdots \oplus D_{im_i} \\ &= \operatorname{diag}(1, \ldots, 1, e_{i1}(x)) \oplus \operatorname{diag}(1, \ldots, 1, e_{i2}(x)) \\ &\qquad \oplus \cdots \oplus \operatorname{diag}(1, \ldots, 1, e_{im_i}(x)) \end{aligned}$$

is also a $d_i \times d_i$ matrix. We first show that B_i (and hence also $xI - Q_i$) is $\mathcal{P}$-equivalent to D_i.

Consider the collection of all $(d_i - 1) \times (d_i - 1)$ subdeterminants of D_i. For each $r = 1, \ldots, m_i$, this collection will contain that subdeterminant obtained by deleting the row and column containing e_{ir}. In particular, this subdeterminant will be $\prod_{j \neq r} e_{ij}$. But the gcd of all such subdeterminants taken over r (for a fixed i of course) is just 1. (To see this, consider the product abcd. If we look at the collection of products obtained by deleting one of a, b, c or d we obtain {bcd, acd, abd, abc}. Since there is no factor in common with all four of these

products, it follows that the gcd of this collection is 1.) Therefore the $(d_i - 1)$*th* determinantal divisor $f_{d_i-1}(x)$ of D_i is 1, and hence the fact that $f_{k-1}(x)$ divides $f_k(x)$ means $f_1(x) = \cdots = f_{d_i-1}(x) = 1$ and $f_{d_i}(x) = \prod_j e_{ij}(x) = q_i(x)$. From the definition of determinantal divisor (or the definition of invariant factor along with the fact that B_i is in its Smith canonical form), it is clear that B_i has precisely these same determinantal divisors, and hence (by the corollary to Theorem 8.8) B_i must be $\mathcal{P}$-equivalent to D_i.

All that remains is to put this all together and apply Theorem 8.9 again. We now take the direct sum of each side of the equivalence relation $xI - Q_i \approx B_i \approx D_{i1} \oplus \cdots \oplus D_{im_i} = D_i$ using the fact that (as we saw in the proof of Theorem 8.15) $(xI - Q_{k+1}) \oplus \cdots \oplus (xI - Q_n) \approx D_{k+1} \oplus \cdots \oplus D_n$. It will be convenient to denote direct sums by $\Sigma\oplus$. For example, we have already seen it is true in general that

$$\sum_{i=k+1}^{n} \oplus (xI - Q_i) = xI - \sum_{i=k+1}^{n} \oplus Q_i$$

(where we again remark that the identity matrices in this equation may be of different dimensions). Therefore, we have shown that

$$\begin{aligned} xI - \sum_{i=k+1}^{n} \oplus Q_i &= \sum_{i=k+1}^{n} \oplus (xI - Q_i) \approx \sum_{i=k+1}^{n} \oplus (D_{i1} \oplus \cdots \oplus D_{im_i}) \\ &= \sum_{i=k+1}^{n} \oplus \left(\sum_{j=1}^{m_i} \oplus D_{ij} \right) \approx \sum_{i=k+1}^{n} \oplus \left(\sum_{j=1}^{m_i} \oplus [xI - C(e_{ij}(x))] \right) \\ &= xI - \sum_{i=k+1}^{n} \oplus \left(\sum_{j=1}^{m_i} \oplus C(e_{ij}(x)) \right) \end{aligned}$$

and hence $\Sigma_{i=k+1}^{n}\oplus Q_i$ is similar over $\mathcal{F}$ to $\Sigma_{i=k+1}^{n} \oplus [\Sigma_{j=1}^{m_i} \oplus C(e_{ij}(x))]$. But Theorem 8.15 tells us that A is similar over $\mathcal{F}$ to $\Sigma_{i=k+1}^{n}\oplus Q_i$, and therefore we have shown that A is similar over $\mathcal{F}$ to

$$\sum_{i=k+1}^{n} \oplus \left(\sum_{j=1}^{m_i} \oplus C(e_{ij}(x)) \right) . \quad \blacksquare$$

Example 8.8 Consider the polynomial

$$p(x) = (x - 1)^2(x^2 + 1)^2 = x^6 - 2x^5 + 3x^4 - 4x^3 + 3x^2 - 2x + 1 .$$

Its companion matrix is

$$C = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & -3 \\ 0 & 0 & 1 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & -3 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix} \in \mathrm{M}_6(\mathbb{R}) \ .$$

According to Theorem 8.14, C is nonderogatory and its minimal polynomial is p(x). Then by Theorem 8.10 and its corollary, the only nonunit similarity invariant of C is also p(x). This means that C is already in the form given by Theorem 8.15.

The elementary divisors (in $\mathbb{R}[x]$) of xI – C are

$$e_1(x) = (x - 1)^2 = x^2 - 2x + 1$$

and

$$e_2(x) = (x^2 + 1)^2 = x^4 + 2x^2 + 1 \ .$$

These have the companion matrices

$$C(e_1(x)) = \begin{pmatrix} 0 & -1 \\ 0 & 2 \end{pmatrix}$$

$$C(e_2(x)) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

and hence Theorem 8.16 tells us that C is similar over $\mathbb{R}$ to the direct sum $C(e_1(x)) \oplus C(e_2(x))$. We leave it to the reader to find the rational canonical form of C if we regard it as a matrix over $\mathbb{C}[x]$. //

Exercises

1. Prove Corollary 1 of Theorem 7.24 using the rational canonical form.

2. (a) Let V be a real 6-dimensional vector space, and suppose $T \in L(V)$ has minimal polynomial $m(x) = (x^2 - x + 3)(x - 2)^2$. Write down all possible rational canonical forms for T (except for the order of the blocks).
   (b) Let V be a real 7-dimensional vector space, and suppose $T \in L(V)$ has minimal polynomial $m(x) = (x^2 + 2)(x + 3)^3$. Write down all possible rational canonical forms for T (except for the order of the blocks).

3. Let A be a 4 x 4 matrix with minimal polynomial $m(x) = (x^2 + 1)(x^2 - 3)$. Find the rational canonical form if A is a matrix over:
   (a) The rational field $\mathbb{Q}$.
   (b) The real field $\mathbb{R}$.
   (c) The complex field $\mathbb{C}$.

4. Find the rational canonical form for the Jordan block

$$\begin{pmatrix} a & 1 & 0 & 0 \\ 0 & a & 1 & 0 \\ 0 & 0 & a & 1 \\ 0 & 0 & 0 & a \end{pmatrix}.$$

5. Find a 3 x 3 matrix A with integral entries such that $A^3 + 3A^2 + 2A + 2 = 0$. Prove that your matrix satisfies this identity.

6. Discuss the validity of each of the following assertions:
   (a) Two square matrices are similar if and only if they have the same eigenvalues (including multiplicities).
   (b) Two square matrices are similar if and only if they have the same minimal polynomial.
   (c) Two square matrices are similar if and only if they have the same elementary divisors.
   (d) Two square matrices are similar if and only if they have the same determinantal divisors.

7. Suppose $A = B \oplus C$ where B and C are square matrices. Is the list of elementary divisors of A equal to the list of elementary divisors of B concatenated with (i.e., "added on to") the list of elementary divisors of C? What if "elementary divisors" is replaced by "invariant factors" or "determinantal divisors" in this statement?

8.6 THE JORDAN CANONICAL FORM

We have defined a canonical form as that matrix representation A of a linear transformation $T \in L(V)$ that is of a particularly simple form in some basis for V. If all the eigenvalues of T lie in the base field $\mathcal{F}$, then the minimal polynomial m(x) for T will factor into a product of linear terms. In addition, if the eigenvalues are all distinct, then T will be diagonalizable (Theorem 7.24). But in the general case of repeated roots, we must (so far) fall back to the triangular form described in Chapter 7 and in Section 8.1. However, in this more general case there is another very important form that follows easily from what we have already done. If $A \in M_n(\mathbb{C})$, then (by Theorem 6.13) all the elementary divisors of $xI - A$ will be of the simple form $(x - a)^k$. We shall now investigate the "simplest" form that such an A can take.

To begin with, given a polynomial $p(x) = (x - a_0)^n \in \mathcal{F}[x]$, we define the **hypercompanion matrix** $H(p(x)) \in M_n(\mathcal{F})$ to be the upper-triangular matrix

$$\begin{pmatrix} a_0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & a_0 \end{pmatrix}.$$

A matrix of this form is also referred to as a **basic Jordan block** belonging to a_0. Now consider the characteristic matrix $xI - H(p(x))$. Note that if we delete the n*th* row and first column of this characteristic matrix, we obtain a lower-triangular matrix with all diagonal entries equal to -1, and hence its determinant is equal to $(-1)^{n-1}$. Thus the corresponding determinantal divisor $f_{n-1}(x)$ is equal to 1, and therefore $f_1(x) = \cdots = f_{n-1}(x) = 1$ (because $f_{k-1}(x) | f_k(x)$). Using $f_k(x) = q_k(x) f_{k-1}(x)$, it follows that $q_1(x) = \cdots = q_{n-1}(x) = 1$, and thus H is nonderogatory (corollary to Theorem 8.10). Since it is obvious that $\Delta_H(x) = (x - a_0)^n = p(x)$, we conclude that $\Delta_H(x) = m(x) = p(x)$. (Alternatively, by Theorem 8.10, we see that the minimal polynomial for H is $q_n(x) = f_n(x) = (x - a)^n$ which is also just the characteristic polynomial of H.) Along with the definition of the Smith canonical form, this proves the following result analogous to Theorem 8.14.

Theorem 8.17 The hypercompanion matrix $H(p(x))$ of the polynomial $p(x) = (x - a)^n \in \mathcal{F}[x]$ is nonderogatory, and its characteristic and minimal polynomials both equal p(x). Furthermore, the Smith form of $xI - H(p(x))$ is

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & p(x) \end{pmatrix}.$$

Theorems 8.14 and 8.17 show that given the polynomial $p(x) = (x - a)^n \in \mathbb{C}[x]$, both $C = C(p(x))$ and $H = H(p(x))$ have precisely the same similarity invariants. Using Theorem 8.16, we then see that C and H are similar over $\mathbb{C}$. Now, if $A \in M_n(\mathbb{C})$, we know that the elementary divisors of $xI - A$ will be of the form $(x - a)^k$. Furthermore, Theorem 8.16 shows us that A is similar over $\mathbb{C}$ to the direct sum of the companion matrices of these elementary divisors. But each companion matrix is similar over $\mathbb{C}$ to the corresponding hypercompanion matrix, and hence A is similar over $\mathbb{C}$ to the direct sum of the hypercompanion matrices of the elementary divisors of $xI - A$.

It may be worth briefly showing that the notions of similarity and direct sums may be treated in the manner just claimed. In other words, denoting similarity over $\mathbb{C}$ by $\sim$, we suppose that $A \sim C_1 \oplus C_2 = S^{-1}AS$ for some nonsingular matrix $S \in M_n(\mathbb{C})$. We now also assume that $C_i \sim H_i = T_i^{-1}C_iT_i$ for each $i = 1, 2$. Then we see that

$$\begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix} = \begin{pmatrix} T_1^{-1}C_1T_1 & 0 \\ 0 & T_2^{-1}C_2T_2 \end{pmatrix}$$

$$= \begin{pmatrix} T_1^{-1} & 0 \\ 0 & T_2^{-1} \end{pmatrix} \begin{pmatrix} C_1 & 0 \\ 0 & C_2 \end{pmatrix} \begin{pmatrix} T_1 & 0 \\ 0 & T_2 \end{pmatrix}$$

which (in an obvious shorthand notation) may be written in the form $H = T^{-1}CT$ if we note that

$$\begin{pmatrix} T_1^{-1} & 0 \\ 0 & T_2^{-1} \end{pmatrix} = \begin{pmatrix} T_1 & 0 \\ 0 & T_2 \end{pmatrix}^{-1}.$$

We therefore have $H = T^{-1}CT = T^{-1}S^{-1}AST = (ST)^{-1}A(ST)$ which shows that A is indeed similar to the direct sum of the hypercompanion matrices. In any case, we have proved the difficult part of the next very important theorem (see also Theorem 7.42).

Theorem 8.18 (**Jordan Canonical Form**) If $A \in M_n(\mathbb{C})$, then A is similar over $\mathbb{C}$ to the direct sum of the hypercompanion matrices of all the elementary divisors of $xI - A$, and this direct sum is unique except for the order of the blocks. Moreover, the numbers appearing on the main diagonal of the Jordan form are precisely the eigenvalues of A. (Note that the field $\mathbb{C}$ can be replaced by an arbitrary field $\mathcal{F}$ if all the eigenvalues of A lie in $\mathcal{F}$.)

Proof Existence was proved in the above discussion, so we now consider uniqueness. According to our general prescription, given a matrix $A \in M_n(\mathbb{C})$, we would go through the following procedure to find its Jordan form. First we reduce the characteristic matrix $xI - A$ to its *unique* Smith form, thus obtaining the similarity invariants of A. These similarity invariants are then factored (over $\mathbb{C}$) to obtain the elementary divisors of $xI - A$. Finally, the corresponding hypercompanion matrices are written down, and the Jordan form of A is just their direct sum.

All that remains is to prove the statement about the eigenvalues of A. To see this, recall that the eigenvalues of A are the roots of the characteristic polynomial $\det(xI - A)$. Suppose that $J = S^{-1}AS$ is the Jordan form of A. Then the eigenvalues of J are the roots of

$$\det(xI - J) = \det(xI - S^{-1}AS) = \det[S^{-1}(xI - A)S] = \det(xI - A)$$

so that A and J have the same eigenvalues. But J is an upper-triangular matrix, and hence the roots of $\det(xI - J)$ are precisely the diagonal entries of J. ∎

Example 8.9 Referring to Example 8.8, we regard C as a matrix over $M_6(\mathbb{C})$. Then its elementary divisors are $e_1(x) = (x - 1)^2$, $e_2(x) = (x + i)^2$ and $e_3(x) = (x - i)^2$. The corresponding hypercompanion matrices are

$$H_1 = H(e_1(x)) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$H_2 = H(e_2(x)) = \begin{pmatrix} -i & 1 \\ 0 & -i \end{pmatrix}$$

$$H_3 = H(e_3(x)) = \begin{pmatrix} i & 1 \\ 0 & i \end{pmatrix}$$

and therefore A is similar over $\mathbb{C}$ to its Jordan form $H_1 \oplus H_2 \oplus H_3$. //

Our next theorem is really a corollary to Theorem 8.18, but it is a sufficiently important result that we single it out by itself.

Theorem 8.19 The geometric multiplicity of an eigenvalue λ_i (i.e., $\dim V_{\lambda_i}$) belonging to a matrix $A \in M_n(\mathbb{C})$ is the number of elementary divisors of the characteristic matrix $xI - A$ that correspond to λ_i. In other words, the number of basic Jordan blocks (i.e., hypercompanion matrices) belonging to λ_i in the Jordan canonical form of A is the same as the geometric multiplicity of λ_i.

Proof Suppose that there are n_i elementary divisors belonging to λ_i, and let $\{H_{i1}, \ldots, H_{in_i}\}$ be the corresponding hypercompanion matrices. By suitably numbering the eigenvalues, we may write the Jordan form of A as

$$A = H_{11} \oplus \cdots \oplus H_{1n_1} \oplus \cdots \oplus H_{r1} \oplus \cdots \oplus H_{rn_r}$$

where we assume that there are r distinct eigenvalues of A. For definiteness, let us arbitrarily consider the eigenvalue λ_1 and look at the matrix $\lambda_1 I - A$. Since $\lambda_1 - \lambda_i \neq 0$ for $i \neq 1$, this matrix takes the form

$$\lambda_1 I - A = B_{11} \oplus \cdots \oplus B_{1n_1} \oplus J_{21} \oplus \cdots \oplus J_{2n_2} \oplus \cdots \oplus J_{r1} \oplus \cdots \oplus J_{rn_r}$$

where each B_{ij} is of the form

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

and each J_{ij} looks like

$$\begin{pmatrix} \lambda_1 - \lambda_i & -1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_1 - \lambda_i & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_1 - \lambda_i & -1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_1 - \lambda_i \end{pmatrix}.$$

It should be clear that each J_{ij} is nonsingular (since they are all equivalent to the identity matrix of the appropriate size), and that each B_{ij} has rank equal to one less than its size. Since A is of size n, this means that the rank of $\lambda_1 I - A$

is $n - n_1$ (just look at the number of linearly independent rows in $\lambda_1 I - A$). But from Theorem 5.6 we have

$$\dim V_{\lambda_1} = \dim \mathrm{Ker}(\lambda_1 I - A) = \mathrm{nul}(\lambda_1 I - A) = n - r(\lambda_1 I - A) = n_1 .$$

In other words, the geometric multiplicity of λ_1 is equal to the number of hypercompanion matrices corresponding to λ_1 in the Jordan form of A. Since λ_1 could have been any of the eigenvalues, we are finished. ∎

Example 8.10 Suppose $A \in M_6(\mathbb{C})$ has characteristic polynomial

$$\Delta_A(x) = (x - 2)^4(x - 3)^2$$

and minimal polynomial

$$m(x) = (x - 2)^2(x - 3)^2 .$$

Then A has eigenvalue $\lambda_1 = 2$ with multiplicity 4, and $\lambda_2 = 3$ with multiplicity 2, and these must lie along the diagonal of the Jordan canonical form. We know that (see the proof of the corollary to Theorem 8.10)

$$\Delta_A(x) = m(x)q_{n-1}(x) \cdots q_1(x)$$

where $q_n(x) = m(x), \ldots, q_1(x)$ are the similarity invariants of A, and that the elementary divisors of $xI - A$ are the powers of the prime factors of the $q_i(x)$. What we do not know however, is whether the set of elementary divisors of $xI - A$ is $\{(x - 2)^2, (x - 3)^2, (x - 2)^2\}$ or $\{(x - 2)^2, (x - 3)^2, x - 2, x - 2\}$.

Using Theorem 8.18, we then see that the only possible Jordan canonical forms are (up to the order of the blocks)

$$\begin{pmatrix} \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & & \\ & \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & \\ & & \boxed{\begin{matrix} 3 & 1 \\ & 3 \end{matrix}} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & & & \\ & \boxed{2} & & \\ & & \boxed{2} & \\ & & & \boxed{\begin{matrix} 3 & 1 \\ & 3 \end{matrix}} \end{pmatrix}$$

Note that in the first case, the geometric multiplicity of $\lambda_1 = 2$ is two, while in the second case, the geometric multiplicity of $\lambda_1 = 2$ is three. In both cases, the eigenspace corresponding to $\lambda_2 = 3$ is of dimension 1. //

Example 8.11 Let us determine all possible Jordan canonical forms for the matrix $A \in \mathbb{C}(3)$ given by

$$\begin{pmatrix} 2 & a & b \\ 0 & 2 & c \\ 0 & 0 & -1 \end{pmatrix}.$$

The characteristic polynomial for A is easily seen to be

$$\Delta_A(x) = (x - 2)^2(x + 1)$$

and hence (by Theorem 7.12) the minimal polynomial is either the same as $\Delta_A(x)$, or is just $(x - 2)(x + 1)$. If $m(x) = \Delta(x)$, then (using Theorem 8.18 again) the Jordan form must be

$$\begin{pmatrix} \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & & \\ & & \\ & & \boxed{-1} \end{pmatrix}$$

while in the second case, it must be

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

If A is to be diagonalizable, then (either by Theorem 7.26 or the fact that the Jordan form in the second case is already diagonal) we must have the second case, and hence

$$0 = m(A) = (A - 2I)(A + I) = \begin{pmatrix} 0 & 3a & ac \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

so that A will be diagonalizable if and only if $a = 0$. //

As another application of Theorem 8.16 we have the following useful result. Note that here the field $\mathcal{F}$ can be either $\mathbb{R}$ or $\mathbb{C}$, and need not be algebraically closed in general.

Theorem 8.20 Suppose $B_i \in M_{n_i}(\mathcal{F})$ for $i = 1, \ldots, r$ and let $A = B_1 \oplus \cdots \oplus B_r \in M_n(\mathcal{F})$ (so that $n = \sum_{i=1}^{r} n_i$). Then the set of elementary divisors of $xI - A$ is the totality of elementary divisors of all the $xI - B_i$ taken together.

Proof We prove the theorem for the special case of $A = B_1 \oplus B_2$. The general case follows by an obvious induction argument. Let $S = \{e_1(x), \ldots, e_m(x)\}$ denote the totality of elementary divisors of $xI - B_1$ and $xI - B_2$ taken together. Thus, the elements of S are powers of prime polynomials. Following the method discussed at the end of Theorem 8.8, we multiply together the highest powers of all the distinct primes that appear in S to obtain a polynomial which we denote by $q_n(x)$. Deleting from S those $e_i(x)$ that we just used, we now multiply together the highest powers of all the remaining distinct primes to obtain $q_{n-1}(x)$. We continue this procedure until all the elements of S are exhausted, thereby obtaining the polynomials $q_{k+1}(x), \ldots, q_n(x)$. Note that our construction guarantees that $q_j(x) | q_{j+1}(x)$ for $j = k + 1, \ldots, n - 1$. Since $f_n(x) = q_1(x) \cdots q_n(x)$, it should also be clear that

$$\sum_{i=k+1}^{n} \deg q_j(x) = n_1 + n_2 = n \quad .$$

Denote the companion matrix $C(q_j(x))$ by simply C_j, and define the matrix

$$Q = C_{k+1} \oplus \cdots \oplus C_n \in M_n(\mathcal{F}) \quad .$$

Then

$$xI - Q = (xI - C_{k+1}) \oplus \cdots \oplus (xI - C_n) \quad .$$

But according to Theorem 8.14, $xI - C_j \approx \operatorname{diag}(1, \ldots, 1, q_j(x))$, and hence

$$xI - Q \approx \operatorname{diag}(1, \ldots, 1, q_{k+1}(x)) \oplus \cdots \oplus \operatorname{diag}(1, \ldots, 1, q_n(x)) \quad .$$

Then (since the Smith form is unique) the nonunit similarity invariants of Q are just the $q_j(x)$ (for $j = k + 1, \ldots, n$), and hence (by definition of elementary divisor) the elementary divisors of $xI - Q$ are exactly the polynomials in S. Then by Theorem 8.16, Q is similar to the direct sum of the companion matrices of all the polynomials in S.

On the other hand, Theorem 8.16 also tells us that B_1 and B_2 are each similar to the direct sum of the companion matrices of the elementary divisors of $xI - B_1$ and $xI - B_2$ respectively. Therefore $B_1 \oplus B_2 = A$ is similar to the direct sum of the companion matrices of all the polynomials in S. We now see that A is similar to Q, and hence (by Theorem 8.9, Corollary 1) $xI - A$ and $xI - Q$ have the same elementary divisors. Since the elementary divisors of $xI - Q$ are just the polynomials in S, and S was defined to be the totality of elementary divisors of $xI - B_1$ and $xI - B_2$, the proof is complete. ∎

The notion of "uniqueness" in Theorem 8.18 is an assertion that the Jordan form is "uniquely defined" or "well-defined." Suppose $A \in M_n(\mathbb{C})$ has Jordan form $H_1 \oplus \cdots \oplus H_p$ where each H_i is a basic Jordan block, and suppose that $G_1 \oplus \cdots \oplus G_q$ is any other matrix similar to A which is a direct sum of basic Jordan blocks. Then it follows from Theorem 8.20 that the G_i must, except for order, be exactly the same as the H_i (see Exercise 8.6.4). We state this in the following corollary to Theorem 8.20.

Corollary (**Uniqueness of the Jordan form**) Suppose $A \in M_n(\mathbb{C})$, and let both $G = G_1 \oplus \cdots \oplus G_p$ and $H = H_1 \oplus \cdots \oplus H_q$ be similar to A, where each G_i and H_i is a basic Jordan block. Then $p = q$ and, except for order, the G_i are the same as the H_i.

We saw in Section 7.5 that if a vector space V is the direct sum of T-invariant subspaces W_i (where $T \in L(V)$), then the matrix representation A of T is the direct sum of the matrix representations of $T_i = T|W_i$ (Theorem 7.20). Another common way of describing this decomposition of A is the following. We say that a matrix is **reducible** over $\mathcal{F}$ if it is similar to a block diagonal matrix with more than one block. In other words, $A \in M_n(\mathcal{F})$ is reducible if there exists a nonsingular matrix $S \in M_n(\mathcal{F})$ and matrices $B \in M_p(\mathcal{F})$ and $C \in M_q(\mathcal{F})$ with $p + q = n$ such that $S^{-1}AS = B \oplus C$. If A is not reducible, then we say that A is **irreducible**. A fundamental result is the following.

Theorem 8.21 A matrix $A \in M_n(\mathcal{F})$ is irreducible over $\mathcal{F}$ if and only if A is nonderogatory and the characteristic polynomial $\Delta_A(x)$ is a power of a prime polynomial. Alternatively, A is irreducible if and only if $xI - A$ has only one elementary divisor.

Proof If A is irreducible, then $xI - A$ can have only one elementary divisor (which is then necessarily a prime to some power) because (by Theorem 8.16) A is similar to the direct sum of the companion matrices of all the elementary divisors of $xI - A$. But these elementary divisors are the factors of the similarity invariants $q_k(x)$ where $q_k(x)|q_{k+1}(x)$, and therefore it follows that

$$q_1(x) = \cdots = q_{n-1}(x) = 1 \ .$$

Hence A is nonderogatory (corollary to Theorem 8.10).

Now assume that A is nonderogatory and that $\Delta_A(x)$ is a power of a prime polynomial. From Theorem 8.10 and its corollary we know that $q_1(x) = \cdots = q_{n-1}(x) = 1$, and hence $q_n(x) = m(x) = \Delta_A(x)$ is now the only elementary divisor of $xI - A$. If A were reducible, then (in the above notation) it would be similar over $\mathbb{F}$ to a matrix of the form $B \oplus C = S^{-1}AS$, and by Corollary 1 of Theorem 8.9, it would then follow that $xI - A$ has the same elementary divisors as $xI - (B \oplus C) = (xI - B) \oplus (xI - C)$. Note that by the corollary to Theorem 8.8, $xI - A$ and $S^{-1}(xI - A)S = xI - S^{-1}AS$ have the same elementary divisors. But $xI - B$ and $xI - C$ necessarily have at least one elementary divisor each (since their characteristic polynomials are nonzero), and (by Theorem 8.20) the elementary divisors of $xI - S^{-1}AS$ are the totality of the elementary divisors of $xI - B$ plus those of $xI - C$. This contradicts the fact that $xI - A$ has only one elementary divisor, and therefore A must be irreducible. ∎

For example, we see from Theorem 8.17 that the hypercompanion matrix $H((x - a)^k)$ is always irreducible. One consequence of this is that the Jordan canonical form of a matrix is the "simplest" in the sense that there is no similarity transformation that will further reduce any of the blocks on the diagonal. Similarly, since any elementary divisor is a power of a prime polynomial, we see from Theorem 8.14 that the companion matrix of an elementary divisor is always irreducible. Thus the rational canonical form can not be further reduced either. Note that the rational canonical form of a matrix $A \in M_n(\mathbb{C})$ will have the same "shape" as the Jordan form of A. In other words, both forms will consist of the same number of blocks of the same size on the diagonal.

In Sections 7.2 and 7.7 we proved several theorems that showed some of the relationships between eigenvalues and diagonalizability. Let us now relate what we have covered in this chapter to the question of diagonalizability. It is easiest to do this in the form of two simple theorems. The reader should note that the companion matrix of a linear polynomial $x - a_0$ is just the 1 x 1 matrix (a_0).

Theorem 8.22 A matrix $A \in M_n(\mathcal{F})$ is similar over $\mathcal{F}$ to a diagonal matrix $D \in M_n(\mathcal{F})$ if and only if all the elementary divisors of $xI - A$ are linear.

Proof If the elementary divisors of $xI - A$ are linear, then each of the corresponding companion matrices consists of a single scalar, and hence the rational canonical form of A will be diagonal (Theorem 8.16). Conversely, if A is similar to a diagonal matrix D, then $xI - A$ and $xI - D$ will have the same elementary divisors (Theorem 8.9, Corollary 1). Writing $D = D_1 \oplus \cdots \oplus D_n$ where $D_i = (d_i)$ is just a 1 x 1 matrix, we see from Theorem 8.20 that the ele-

mentary divisors of $xI - D$ are the linear polynomials $\{x - d_1, \ldots, x - d_n\}$ (since the elementary divisor of $xI - D_i = (x - d_i)$ is just $x - d_i$). ∎

Theorem 8.23 A matrix $A \in M_n(\mathcal{F})$ is similar over $\mathcal{F}$ to a diagonal matrix $D \in M_n(\mathcal{F})$ if and only if the minimal polynomial for A has distinct linear factors in $\mathcal{P} = \mathcal{F}[x]$.

Proof Recall that the elementary divisors of a matrix in $M_n(\mathcal{P})$ are the powers of prime polynomials that factor the invariant factors $q_k(x)$, and furthermore, that $q_k(x) | q_{k+1}(x)$. Then all the elementary divisors of such a matrix will be linear if and only if its invariant factor of highest degree has distinct linear factors in $\mathcal{P}$. But by Theorem 8.10, the minimal polynomial for $A \in M_n(\mathcal{F})$ is just its similarity invariant of highest degree (i.e., the invariant factor of highest degree of $xI - A \in M_n(\mathcal{P})$). Then applying Theorem 8.22, we see that A will be diagonalizable if and only if the minimal polynomial for A has distinct linear factors in $\mathcal{P}$. ∎

While it is certainly not true that any $A \in M_n(\mathbb{C})$ is similar to a diagonal matrix, it is an interesting fact that A is similar to a matrix in which the off-diagonal entries are arbitrarily small. To see this, we first put A into its Jordan canonical form J. In other words, we have

$$J = S^{-1}AS = \begin{pmatrix} j_{11} & j_{12} & 0 & 0 & \cdots & 0 & 0 \\ 0 & j_{22} & j_{23} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & j_{n-1\,n-1} & j_{n-1\,n} \\ 0 & 0 & 0 & 0 & \cdots & 0 & j_{nn} \end{pmatrix}.$$

If we now define the matrix $T = \text{diag}(1, \delta, \delta^2, \ldots, \delta^{n-1})$, then we leave it to the reader to show that

$$T^{-1}JT = (ST)^{-1}A(ST)$$
$$= \begin{pmatrix} j_{11} & \delta j_{12} & 0 & 0 & \cdots & 0 & 0 \\ 0 & j_{22} & \delta j_{23} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & j_{n-1\,n-1} & \delta j_{n-1\,n} \\ 0 & 0 & 0 & 0 & \cdots & 0 & j_{nn} \end{pmatrix}.$$

By choosing δ as small as desired, we obtain the form claimed.

Exercises

1. If all the eigenvalues of $A \in M_n(\mathcal{F})$ lie in $\mathcal{F}$, show that the Jordan canonical form of A has the same "block structure" as its rational canonical form.

2. Prove Theorem 7.25 using the Jordan canonical form (Theorem 8.18).

3. Prove Theorem 7.26 using the Jordan canonical form.

4. Finish proving the corollary to Theorem 8.20.

5. State and prove a corollary to Theorem 8.16 that is the analogue of the corollary to Theorem 8.20.

6. (a) Suppose a matrix A has characteristic polynomial

$$\Delta_A(x) = (x-2)^4(x-3)^3$$

and minimal polynomial

$$m(x) = (x-2)^2(x-3)^2 \ .$$

What are the possible Jordan forms for A?
(b) Suppose A has characteristic polynomial $\Delta_A(x) = (x-2)^3(x-5)^2$. What are the possible Jordan forms?

7. Find all possible Jordan forms for those matrices with characteristic and minimal polynomials given by:
(a) $\Delta(x) = (x-2)^4(x-3)^2$ and $m(x) = (x-2)^2(x-3)^2$.
(b) $\Delta(x) = (x-7)^5$ and $m(x) = (x-7)^2$.
(c) $\Delta(x) = (x-2)^7$ and $m(x) = (x-2)^3$.
(d) $\Delta(x) = (x-3)^4(x-5)^4$ and $m(x) = (x-3)^2(x-5)^2$.

8. Show that every complex matrix is similar to its transpose.

9. Is it true that all complex matrices $A \in M_n(\mathbb{C})$ with the property that $A^n = I$ but $A^k \neq I$ for $k < n$ are similar? Explain.

10. (a) Is it true that an eigenvalue λ of a matrix $A \in M_n(\mathbb{C})$ has multiplicity 1 if and only if $\lambda I - A$ has rank $n - 1$?
(b) Suppose an eigenvalue λ of $A \in M_n(\mathbb{C})$ is such that $r(\lambda I - A) = n - 1$. Prove that either λ has multiplicity 1, or else $r(\lambda I - A)^2 = n - 2$.

11. Suppose $A \in M_n(\mathbb{C})$ is idempotent, i.e., $A^2 = A$. What is the Jordan form of A?

12. Suppose $A \in M_n(\mathbb{C})$ is such that $p(A) = 0$ where

$$p(x) = (x - 2)(x - 3)(x - 4) .$$

Prove or disprove the following statements:
(a) The minimal polynomial for A must be of degree 3.
(b) A must be of size $n \leq 3$.
(c) If $n > 3$, then the characteristic polynomial of A must have multiple roots.
(d) A is nonsingular.
(e) A must have 2, 3 and 4 as eigenvalues.
(f) If $n = 3$, then the minimal and characteristic polynomials of A must be the same.
(g) If $n = 3$ then, up to similarity, there are exactly 10 different choices for A.

13. Recall that $A \in M_n(\mathbb{C})$ is said to be nilpotent of index k if k is the smallest integer such that $A^k = 0$.
(a) Describe the Jordan form of A.
Prove or disprove each of the following statements about $A \in M_n(\mathbb{C})$:
(b) A is nilpotent if and only if every eigenvalue of A is zero.
(c) If A is nilpotent, then $r(A) - r(A^2)$ is the number of elementary divisors of A.
(d) If A is nilpotent, then $r(A) - r(A^2)$ is the number of p x p Jordan blocks of A with $p > 1$.
(e) If A is nilpotent, then the nul(A) is the number of Jordan blocks of A (counting 1 x 1 blocks).
(f) If A is nilpotent, then $\text{nul}(A^{k+1}) - \text{nul}(A^k)$ is the number of Jordan blocks of size greater than k.

14. Suppose $A \in M_n(\mathbb{C})$ has eigenvalue λ of multiplicity m. Prove that the elementary divisors of A corresponding to λ are all linear if and only if $r(\lambda I - A) = r((\lambda I - A)^2)$.

15. Prove or disprove the following statements about matrices $A, B \in M_n(\mathbb{C})$:
(a) If either A or B is nonsingular, then AB and BA have the same minimal polynomial.
(b) If both A and B are singular and $AB \neq BA$, then AB and BA are not similar.

16. Suppose $A \in M_n(\mathbb{C})$, and let adj A be as in Theorem 4.11. If A is nonsingular, then $(SAS^{-1})^{-1} = SA^{-1}S^{-1}$ implies that $\text{adj}(SAS^{-1}) = S(\text{adj } A)S^{-1}$ by Theorem 4.11. By using "continuity" arguments, it is easy to show that this identity is true even if A is singular. Using this fact and the Jordan form, prove:
(a) If $\det A = 0$ but $\text{Tr}(\text{adj } A) \neq 0$, then 0 is an eigenvalue of A with multiplicity 1.
(b) If $\det A = 0$ but $\text{Tr}(\text{adj } A) \neq 0$, then $r(A) = n - 1$.

8.7 CYCLIC SUBSPACES *

It is important to realize that the Jordan form can only be found in cases where the minimal polynomial is factorable into linear polynomials (for example, if the base field is algebraically closed). On the other hand, the rational canonical form is valid over non-algebraically closed fields. In order to properly present another way of looking at the rational canonical form, we first introduce cyclic subspaces. Again, we are seeking a criterion for deciding when two matrices are similar. The clue that we now follow up on was given earlier in Theorem 7.37.

Let $V \neq 0$ be a finite-dimensional vector space over an arbitrary field $\mathbb{F}$, and suppose $T \in L(V)$. We say that a nonzero T-invariant subspace Z of V is **T-cyclic** if there exists a nonzero $v \in Z$ and a positive integer $k \geq 0$ such that Z is spanned by the set $\{v, T(v), \ldots, T^k(v)\}$. An equivalent way of defining T-cyclic subspaces is given in the following theorem.

Theorem 8.24 Let V be finite-dimensional and suppose $T \in L(V)$. A subspace $Z \subset V$ is T-cyclic if and only if there exists a nonzero $v \in Z$ such that every vector in Z can be expressed in the form $f(T)(v)$ for some $f(x) \in \mathcal{F}[x]$.

Proof If Z is T-cyclic, then by definition, any $u \in Z$ may be written in terms of the set $\{v, T(v), \ldots, T^k(v)\}$ as

$$u = a_0v + a_1T(v) + \cdots + a_kT^k(v) = (a_0 + a_1T + \cdots + a_kT^k)(v) = f(T)(v)$$

where $f(x) = a_0 + a_1x + \cdots + a_kx^k \in \mathcal{F}[x]$. On the other hand, if every $u \in Z$ is of the form $f(T)(v)$, then Z must be spanned by the set $\{v, T(v), T^2(v), \ldots\}$. But Z is finite-dimensional (since it is a subset of the finite-dimensional space V), and hence there must exist a positive integer k such that Z is spanned by the set $\{v, T(v), \ldots, T^k(v)\}$. ∎

Generalizing these definitions slightly, let $v \in V$ be nonzero. Then the set of all vectors of the form $f(T)(v)$ where $f(x)$ varies over all polynomials in $\mathcal{F}[x]$ is a T-invariant subspace called the **T-cyclic subspace of** V **generated by** v. We denote this subspace by $Z(v, T)$. We also denote the restriction of T to $Z(v, T)$ by $T_v = T|Z(v, T)$. That $Z(v, T)$ is a subspace is easily seen since for any $f, g \in \mathcal{F}[x]$ and $a, b \in \mathcal{F}$ we have

$$af(T)(v) + bg(T)(v) = [af(T) + bg(T)](v) = h(T)(v) \in Z(v, T)$$

where $h(x) = af(x) + bg(x) \in \mathcal{F}[x]$ (by Theorem 7.2). It should be clear that $Z(v, T)$ is T-invariant since any element of $Z(v, T)$ is of the form $f(T)(v)$, and hence

$$T[f(T)(v)] = [Tf(T)](v) = g(T)(v)$$

where $g(x) = x\,f(x) \in \mathcal{F}[x]$. In addition, $Z(v, T)$ is T-cyclic by Theorem 8.24. In the particular case that $Z(v, T) = V$, then v is called a **cyclic vector** for T.

Let us briefly refer to Section 7.4 where we proved the existence of a unique monic polynomial $m_v(x)$ of least degree such that $m_v(T)(v) = 0$. This polynomial was called the minimal polynomial of the vector v. The existence of $m_v(x)$ was based on the fact that V was of dimension n, and hence for any $v \in V$, the $n + 1$ vectors $\{v, T(v), \ldots, T^n(v)\}$ must be linearly dependent. This showed that $\deg m_v(x) \leq n$. Since $m_v(x)$ generates the ideal $N_T(v)$, it follows that $m_v(x)|f(x)$ for any $f(x) \in N_T(v)$, i.e., where $f(x)$ is such that $f(T)(v) = 0$. Let us now show how this approach can be reformulated in terms of T-cyclic subspaces.

Using Theorem 8.24, we see that for any nonzero $v \in V$ we may define $Z(v, T)$ as that finite-dimensional T-invariant subspace of V spanned by the linearly independent set $\{v, T(v), \ldots, T^{d-1}(v)\}$, where the integer $d \geq 1$ is defined as the smallest integer such that the set $\{v, T(v), \ldots, T^d(v)\}$ is linearly

dependent. This means that $T^d(v)$ must be a linear combination of the vectors $v, T(v), \ldots, T^{d-1}(v)$, and hence is of the form

$$T^d(v) = a_0 v + \cdots + a_{d-1}T^{d-1}(v)$$

for some set of scalars $\{a_i\}$. Defining the polynomial

$$m_v(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0$$

we see that $m_v(T)(v) = 0$, where $\deg m_v(x) = d$. All that really remains is to show that if $f(x) \in \mathcal{F}[x]$ is such that $f(T)(v) = 0$, then $m_v(x)|f(x)$. This will prove that $m_v(x)$ is the polynomial of least degree with the property that $m_v(T)(v) = 0$.

From the division algorithm, there exists $g(x) \in \mathcal{F}[x]$ such that

$$f(x) = m_v(x)g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg m_v(x)$. Substituting T and applying this to v we have (using $m_v(T)(v) = 0$)

$$0 = f(T)(v) = g(T)m_v(T)(v) + r(T)(v) = r(T)(v) \ .$$

But if $r(x) \neq 0$ with $\deg r(x) < \deg m_v(x)$, then (since $Z(v, T)$ is T-invariant) $r(T)(v)$ is a linear combination of elements in the set $\{v, T(v), \ldots, T^{d-1}(v)\}$, and hence the equation $r(T)(v) = 0$ contradicts the assumed linear independence of this set. Therefore we must have $r(x) = 0$, and hence $m_v(x)|f(x)$.

Lastly, we note that $m_v(x)$ is in fact the *unique* monic polynomial of least degree such that $m_v(T)(v) = 0$. Indeed, if $m'(x)$ is also of least degree such that $m'(T)(v) = 0$, then the fact that $\deg m'(x) = \deg m_v(x)$ together with the result of the previous paragraph tells us that $m_v(x)|m'(x)$. Thus $m'(x) = \alpha m_v(x)$ for some $\alpha \in F$, and choosing $\alpha = 1$ shows that $m_v(x)$ is the unique *monic polynomial* of least degree such that $m_v(T)(v) = 0$.

We summarize this discussion in the following theorem.

Theorem 8.25 Let $v \in V$ be nonzero and suppose $T \in L(V)$. Then there exists a unique monic polynomial $m_v(x)$ of least degree such that $m_v(T)(v) = 0$. Moreover, for any polynomial $f(x) \in \mathcal{F}[x]$ with $f(T)(v) = 0$ we have $m_v(x)|f(x)$.

Corollary If $m(x)$ is the minimal polynomial for T on V, then $m_v(x)|m(x)$ for every nonzero $v \in V$.

Proof By definition of minimal polynomial we know that $m(T) = 0$ on V, so that in particular we have $m(T)(v) = 0$. But now Theorem 8.25 shows that $m_v(x)|m(x)$. ∎

For ease of reference, we bring together Theorems 8.24 and 8.25 in the next basic result.

Theorem 8.26 Let $v \in V$ be nonzero, suppose $T \in L(V)$, and let

$$m_v(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0$$

be the minimal polynomial of v. Then $\{v, T(v), \ldots, T^{d-1}(v)\}$ is a basis for the T-cyclic subspace Z(v, T), and hence $\dim Z(v, T) = \deg m_v(x) = d$.

Proof From the way that $m_v(x)$ was constructed, the vector $T^d(v)$ is the first vector in the sequence $\{v, T(v), T^2(v), \ldots\}$ that is a linear combination of the preceding vectors. This means that the set $S = \{v, T(v), \ldots, T^{d-1}(v)\}$ is linearly independent. We must now show that $f(T)(v)$ is a linear combination of the elements of S for every $f(x) \in \mathcal{F}[x]$.

Since $m_v(T)(v) = 0$ we have $T^d(v) = \sum_{i=0}^{d-1} a_i T^i(v)$. Therefore

$$T^{d+1}(v) = \sum_{i=0}^{d-2} a_i T^{i+1}(v) + a_{d-1}T^d(v) = \sum_{i=0}^{d-2} a_i T^{i+1}(v) + a_{d-1}\sum_{i=0}^{d-2} a_i T^i(v) \quad .$$

This shows that $T^{d+1}(v)$ is a linear combination of the elements of S. We can clearly continue this process for any $T^k(v)$ with $k \geq d$, and therefore $f(T)(v)$ is a linear combination of $v, T(v), \ldots, T^{d-1}(v)$ for every $f(x) \in \mathcal{F}[x]$. Thus S is a basis for the T-cyclic subspace of V generated by v. ∎

The following example will be used in the proof of the elementary divisor theorem given in the next section.

Example 8.12 Suppose that the minimal polynomial of v is given by $m_v(x) = p(x)^n$ where p(x) is a monic prime polynomial of degree d. Defining $W = Z(v, T)$, we will show that $p(T)^s(W)$ is a T-cyclic subspace generated by $p(T)(v)$, and is of dimension $d(n - s)$ if $s < n$, and dimension 0 if $s \geq n$. It should be clear that $p(T)^s(W)$ is a T-cyclic subspace since every element of W is of the form $f(T)(v)$ for some $f(x) \in \mathcal{F}[x]$ and W is T-invariant.

Since p(x) is of degree d, we see that deg $m_v(x)$ = deg $p(x)^n$ = dn (see Theorem 6.2(b)). From Theorem 8.26, we then follows that W has the basis $\{v, T(v), \ldots, T^{dn-1}(v)\}$. This means that any $w \in W$ may be written as

$$w = a_0 v + a_1 T(v) + \cdots + a_{dn-1} T^{dn-1}(v)$$

for some set of scalars a_i. Applying $p(T)^s$ to w we have

$$p(T)^s(w) = a_0 p(T)^s(v) + \cdots + a_i [T^i p(T)^s](v) + \cdots + a_{dn-1}[T^{dn-1} p(T)^s](v) \ .$$

But $m_v(T)(v) = p(T)^n(v) = 0$ where deg $m_v(x)$ = dn, and deg $p(x)^s$ = ds. Therefore, if $s \geq n$ we automatically have $p(T)^s(w) = 0$ so that $p(T)^s(W)$ is of dimension 0. If $s < n$, then the maximum value of i in the expression for $p(T)^s(w)$ comes from the requirement that $i + ds < dn$ which is equivalent to $i < d(n - s)$. This leaves us with

$$p(T)^s(w) = a_0[p(T)^s(v)] + \cdots + a_{d(n-s)-1} T^{d(n-s)-1}[p(T)^s(v)]$$

and we now see that any element in $p(T)^s(W)$ is a linear combination of the terms $a_i T^i[p(T)^s(v)]$ for $i = 0, \ldots, d(n - s) - 1$. Therefore if $s < n$, this shows that $p(T)^s(W)$ is a T-cyclic subspace of dimension $d(n - s)$ generated by $p(T)^s(v)$. //

In Section 7.4 we showed that the minimal polynomial for T was the unique monic generator of the ideal $N_T = \cap_{v \in V} N_T(v)$. If we restrict ourselves to the subspace Z(v, T) of V then, as we now show, it is true that the minimal polynomial $m_v(x)$ of v is actually the minimal polynomial for $T_v = T|Z(v, T)$.

Theorem 8.27 Let Z(v, T) be the T-cyclic subspace of V generated by v. Then $m_v(x)$ is equal to the minimal polynomial for $T_v = T|Z(v, T)$.

Proof Since Z(v, T) is spanned by $\{v, T(v), T^2(v), \ldots, T^{d-1}(v)\}$, the fact that $m_v(T)(v) = 0$ means that $m_v(T) = 0$ on Z(v, T) (by Theorem 7.2). If p(x) is the minimal polynomial for T_v, then Theorem 7.4 tells us that $p(x)|m_v(x)$. On the other hand, from Theorem 7.17(a), we see that $p(T)(v) = p(T_v)(v) = 0$ since p(x) is the minimal polynomial for T_v. Therefore, Theorem 8.25 shows us that $m_v(x)|p(x)$. Since both $m_v(x)$ and p(x) are monic, this implies that $m_v(x) = p(x)$. ∎

Theorem 8.27 also gives us another proof of the corollary to Theorem 8.25. Thus, since $m_v(x) = p(x)$ (i.e., the minimal polynomial for T_v), Theorem 7.17(b) shows that $m_v(x)|m(x)$. Moreover, we have the next result that ties together these concepts with the structure of quotient spaces.

Theorem 8.28 Suppose $T \in L(V)$, let W be a T-invariant subspace of V and let $\bar{T} \in A(\bar{V})$ be the induced linear operator on $\bar{V} = V/W$ (see Theorem 7.35). Then the minimal polynomial $\bar{m}_v(x)$ for $\bar{v} \in V/W$ divides the minimal polynomial $m(x)$ for T.

Proof From the corollary to Theorem 8.25 we have $\bar{m}_v(x)|\bar{m}(x)$ where $\bar{m}(x)$ is the minimal polynomial for $\bar{T}$. But $\bar{m}(x)|m(x)$ by Theorem 7.35. ∎

Corollary Using the same notation as in Theorems 8.25 and 8.28, if the minimal polynomial for T is of the form $p(x)^n$ where $p(x)$ is a monic prime polynomial, then for any $v \in V$ we have $m_v(x) = p(x)^{n_1}$ and $\bar{m}_v(x) = p(x)^{n_2}$ for some $n_1, n_2 \leq n$.

Proof From the above results we know that $m_v(x)|p(x)^n$ and $\bar{m}_v(x)|p(x)^n$. The corollary then follows from this along with the unique factorization theorem (Theorem 6.6) and the fact that $p(x)$ is monic and prime. ∎

In the discussion that followed Theorem 7.16 we showed that the (unique) minimal polynomial $m(x)$ for $T \in L(V)$ is also the minimal polynomial $m_v(x)$ for some $v \in V$. (This is because each basis vector v_i for V has its own minimal polynomial $m_i(x)$, and the least common multiple of the $m_i(x)$ is both the minimal polynomial for some vector $v \in V$ and the minimal polynomial for T.) Now suppose that v also happens to be a cyclic vector for T, i.e., $Z(v, T) = V$. By Theorem 8.26 we know that

$$\dim V = \dim Z(v, T) = \deg m_v(x) = \deg m(x) .$$

However, the characteristic polynomial $\Delta_T(x)$ for T must always be of degree equal to $\dim V$, and hence the corollary to Theorem 7.42 (or Theorems 7.11 and 7.12) shows us that $m(x) = \Delta_T(x)$.

On the other hand, suppose that the characteristic polynomial $\Delta_T(x)$ of T is equal to the minimal polynomial $m(x)$ for T. Then if $v \in V$ is such that $m_v(x) = m(x)$ we have

$$\dim V = \deg \Delta_T(x) = \deg m(x) = \deg m_v(x) .$$

Applying Theorem 8.26 again, we see that dim Z(v, T) = deg $m_v(x)$ = dim V, and hence v is a cyclic vector for T. We have thus proven the following useful result.

Theorem 8.29 Let V be finite-dimensional and suppose $T \in L(V)$. Then T has a cyclic vector if and only if the characteristic and minimal polynomials for T are identical. Thus the matrix representation of T is nonderogatory.

In view of Theorem 8.12, our next result should have been expected.

Theorem 8.30 Let Z(v, T) be a T-cyclic subspace of V, let $T_v = T|Z(v, T)$ and suppose that the minimal polynomial for v is given by

$$m_v(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0 .$$

Then the matrix representation of T_v relative to the basis v, T(v), . . . , $T^{d-1}(v)$ for Z(v, T) is the companion matrix

$$C(m_v(x)) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & a_{d-2} \\ 0 & 0 & 0 & \cdots & 1 & a_{d-1} \end{pmatrix} .$$

Proof Simply look at T_v applied to each of the basis vectors of Z(v, T) and note that $m_v(T)(v) = 0$ implies that $T^d(v) = a_0v + \cdots + a_{d-1}T^{d-1}(v)$. This yields

$$\begin{aligned} T_v(v) &= 0v + T(v) \\ T_v(T(v)) &= 0v + 0T(v) + T^2(v) \\ &\vdots \\ T_v(T^{d-2}(v)) &= 0v + \cdots + T^{d-1}(v) \\ T_v(T^{d-1}(v)) &= T^d(v) = a_0v + \cdots + a_{d-1}T^{d-1}(v) \end{aligned}$$

As usual, the i*th* column of the matrix representation of T_v is just the image under T_v of the i*th* basis vector of Z(v, T) (see Theorem 5.11). ∎

Exercises

1. If $T \in L(V)$ and $v \in V$, prove that $Z(v, T)$ is the intersection of all T-invariant subspaces containing v.

2. Suppose $T \in L(V)$, and let $u, v \in V$ have relatively prime minimal polynomials $m_u(x)$ and $m_v(x)$. Show that $m_u(x)m_v(x)$ is the minimal polynomial of $u + v$.

3. Prove that $Z(u, T) = Z(v, T)$ if and only if $g(T)(u) = v$ where $g(x)$ is relatively prime to $m_u(x)$.

8.8 THE ELEMENTARY DIVISOR THEREOM *

The reader should recall from Section 7.5 that if the matrix representation A of an operator $T \in L(V)$ is the direct sum of smaller matrices (in the appropriate basis for V), then V is just the direct sum of T-invariant subspaces (see Theorem 7.20). If we translate Theorem 8.16 (the rational canonical form) into the corresponding result on the underlying space V, then we obtain the elementary divisor theorem.

Theorem 8.31 (**Elementary Divisor Theorem**) Let $V \neq \{0\}$ be finite-dimensional over an arbitrary field $\mathcal{F}$, and suppose $T \in L(V)$. Then there exist vectors $v_1, \ldots, v_r$ in V such that:

(a) $V = Z(v_1, T) \oplus \cdots \oplus Z(v_r, T)$.

(b) Each v_i has minimal polynomial $p_i(x)^{n_i}$ where $p_i(x) \in \mathcal{F}[x]$ is a monic prime.

(c) The number r of terms in the decomposition of V is uniquely determined, as is the set of minimal polynomials $p_i(x)^{n_i}$.

Proof This is easy to prove from Theorem 8.16 (the rational canonical form) and what we know about companion matrices and cyclic subspaces (particularly Theorem 8.30). The details are left to the reader. ∎

From Theorem 8.26 we see that $\dim Z(v_i, T) = \deg p_i(x)^{n_i}$, and hence from the corollary to Theorem 2.15 we have

$$\dim V = \sum_{i=1}^{r} \deg p_i(x)^{n_i} \quad .$$

The polynomials $p_i(x)^{n_i}$ defined in Theorem 8.31 are just the elementary divisors of $x1 - T$. For example, suppose that $T \in L(V)$ and $x1 - T$ has the ele-

mentary divisors $x + 1$, $(x - 1)^2$, $x + 1$, $x^2 + 1$ over the field $\mathbb{R}$. This means that V is a vector space over $\mathbb{R}$ with

$$V = Z(v_1, T) \oplus Z(v_2, T) \oplus Z(v_3, T) \oplus Z(v_4, T)$$

and the minimal polynomials of v_1, v_2, v_3, v_4 are $x + 1$, $(x - 1)^2$, $x + 1$, $x^2 + 1$ respectively. Furthermore, $T = T_1 \oplus T_2 \oplus T_3 \oplus T_4$ where $T_i = T|Z(v_i, T)$ and the minimal polynomial for T_i is just the corresponding minimal polynomial of v_i (Theorem 8.27). Note that if the field were $\mathbb{C}$ instead of $\mathbb{R}$, then $x^2 + 1$ would not be prime, and hence could not be an elementary divisor of $x1 - T$.

It is important to realize that Theorem 8.31 only claims the uniqueness of the set of elementary divisors of $x1 - T$. Thus the vectors $v_1, \ldots, v_r$ and corresponding subspaces $Z(v_1, T), \ldots, Z(v_r, T)$ are themselves not uniquely determined by T. In addition, we have seen that the elementary divisors are unique only up to a rearrangement.

It is also possible to prove Theorem 8.31 without using Theorem 8.16 or any of the formalism developed in Sections 8.2 – 8.7. We now present this alternative approach as a difficult but instructive application of quotient spaces, noting that it is not needed for anything else in this book. We begin with a special case that takes care of most of the proof. Afterwards, we will show how Theorem 8.31 follows from Theorem 8.32. It should also be pointed out that Theorem 8.32 also follows from the rational canonical form (Theorem 8.16).

Theorem 8.32 Let $T \in L(V)$ have minimal polynomial $p(x)^n$ where $p(x)$ is a monic prime polynomial. Then there exist vectors $v_1, \ldots, v_r \in V$ such that

$$V = Z(v_1, T) \oplus \cdots \oplus Z(v_r, T) \ .$$

In addition, each v_i has corresponding minimal polynomial (i.e., order) given by $p(x)^{n_i}$ where $n = n_1 \geq n_2 \geq \cdots \geq n_r$. Furthermore, any other decomposition of V into the direct sum of T-cyclic subspaces has the same number r of components and the same set of minimal polynomials (i.e., orders).

Proof Throughout this (quite long) proof, we will use the term "order" rather than "minimal polynomial" for the sake of clarity. Furthermore, we will refer to the **T-order** of a vector rather than simply the order when there is a possible ambiguity with respect to the operator being referred to.

We proceed by induction on the dimension of V. First, if $\dim V = 1$, then $T(V) = V$ and hence $f(T)(V) = V$ for any $f(x) \in \mathcal{F}[x]$. Therefore V is T-cyclic

and the theorem holds in this case. Now assume dim V > 1, and suppose that the theorem holds for all vector spaces of dimension less than that of V.

Since $p(x)^n$ is the minimal polynomial for T, we know that $p(T)^n(v) = 0$ for all $v \in V$. In particular, there must exist a $v_1 \in V$ such that $p(T)^n(v_1) = 0$ but $p(T)^{n-1}(v_1) \neq 0$ (or else $p(x)^{n-1}$ would be the minimal polynomial for T). This means that $p(x)^n$ must be the T-order of v_1 (since the minimal polynomial of v_1 is unique and monic). Now let $Z_1 = Z(v_1, T)$ be the T-invariant T-cyclic subspace of V generated by v_1. We also define $\bar{V} = V/Z_1$ along with the induced operator $\bar{T} \in A(\bar{V})$. Then by Theorem 7.35 we know that the minimal polynomial for $\bar{T}$ divides the minimal polynomial $p(x)^n$ for T, and hence the minimal polynomial for $\bar{T}$ is $p(x)^{n_2}$ where $n_2 \leq n$. This means that $\bar{V}$ and $\bar{T}$ satisfy the hypotheses of the theorem, and hence by our induction hypothesis (since dim $\bar{V}$ < dim V), $\bar{V}$ must be the direct sum of T-cyclic subspaces. We thus write

$$\bar{V} = Z(\bar{v}_2, \bar{T}) \oplus \cdots \oplus Z(\bar{v}_r, \bar{T})$$

where each $\bar{v}_i$ has corresponding $\bar{T}$-order $p(x)^{n_i}$ with $n \geq n_2 \geq \cdots \geq n_r$. It is important to remember that each of these $\bar{v}_i$ is a coset of Z_1 in V, and thus may be written as $\bar{v}_i = u_i + Z_1$ for some $u_i \in V$. This means that every element of $\bar{v}_i$ is of the form $u_i + z_i$ for some $z_i \in Z_1$.

We now claim that there exists a vector v_2 in the coset $\bar{v}_2$ such that the T-order of v_2 is just the $\bar{T}$-order $p(x)^{n_2}$ of $\bar{v}_2$. To see this, let $w \in \bar{v}_2$ be arbitrary so that we may write $w = u_2 + z_2$ for some $u_2 \in V$ and $z_2 \in Z_1 \subset V$. Since $p(\bar{T})^{n_2}(\bar{v}_2) = \bar{0} = Z_1$, we have (see Theorem 7.35)

$$Z_1 = p(\bar{T})^{n_2}(\bar{v}_2) = p(\bar{T})^{n_2}(u_2 + Z_1) = p(T)^{n_2}(u_2) + Z_1$$

and hence $p(T)^{n_2}(u_2) \in Z_1$. Using the fact that Z_1 is T-invariant, we see that

$$p(T)^{n_2}(w) = p(T)^{n_2}(u_2) + p(T)^{n_2}(z_2) \in Z_1 .$$

Using the definition of Z_1 as the T-cyclic subspace generated by v_1, this last result implies that there exists a polynomial $f(x) \in \mathcal{F}[x]$ such that

$$p(T)^{n_2}(w) = f(T)(v_1) . \tag{1}$$

But $p(x)^n$ is the minimal polynomial for T, and hence (1) implies that

$$0 = p(T)^n(w) = p(T)^{n-n_2}p(T)^{n_2}(w) = p(T)^{n-n_2}f(T)(v_1) .$$

Since we showed that $p(x)^n$ is also the T-order of v_1, Theorem 8.25 tells us that $p(x)^n$ divides $p(x)^{n-n_2}f(x)$, and hence there exists a polynomial $g(x) \in \mathcal{F}[x]$ such that $p(x)^{n-n_2} f(x) = p(x)^n g(x)$. Rearranging, this may be written as $p(x)^{n-n_2}[f(x) - p(x)^{n_2}g(x)] = 0$. Since $\mathcal{F}[x]$ is an integral domain, this implies (see Theorem 6.2, Corollary 2)

$$f(x) = p(x)^{n_2}\, g(x) \quad . \tag{2}$$

We now define

$$v_2 = w - g(T)(v_1) \quad . \tag{3}$$

By definition of Z_1 we see that $w - v_2 = g(T)(v_1) \in Z_1$, and therefore (see Theorem 7.30)

$$v_2 \in w + Z_1 = u_2 + z_2 + Z_1 = u_2 + Z_1 = \bar{v}_2 \quad .$$

Since $\bar{v}_2 = u_2 + Z_1$ and $v_2 \in \bar{v}_2$, it follows that $v_2 = u_2 + z$ for some $z \in Z_1$. Now suppose that $h(x)$ is any polynomial such that $h(T)(v_2) = 0$. Then

$$0 = h(T)(v_2) = h(T)(u_2 + z) = h(T)(u_2) + h(T)(z)$$

so that $h(T)(u_2) = -h(T)(z) \in Z_1$ (since Z_1 is T-invariant). We then have

$$h(\bar{T})(\bar{v}_2) = h(\bar{T})(u_2 + Z_1) = h(T)(u_2) + Z_1 = Z_1 = \bar{0} \quad .$$

According to Theorem 8.25, this then means that the $\bar{T}$-order of $\bar{v}_2$ divides $h(x)$. In particular, choosing $h(x)$ to be the T-order of v_2, we see that the T-order of v_2 is some multiple of the $\bar{T}$-order of $\bar{v}_2$. In other words, the T-order of v_2 must equal $p(x)^{n_2}q(x)$ for some polynomial $q(x) \in \mathcal{F}[x]$. However, from (3), (1) and (2) we have

$$\begin{aligned} p(T)^{n_2}(v_2) &= p(T)^{n_2}[w - g(T)(v_1)] \\ &= p(T)^{n_2}(w) - p(T)^{n_2} g(T)(v_1) \\ &= f(T)(v_1) - f(T)(v_1) \\ &= 0 \quad . \end{aligned}$$

This shows that in fact the T-order of v_2 is equal to $p(x)^{n_2}$ as claimed.

In an exactly analogous manner, we see that there exist vectors $v_3, \ldots, v_r$ in V with $v_i \in \bar{v}_i$ and such that the T-order of v_i is equal to the $\bar{T}$-order $p(x)^{n_i}$ of $\bar{v}_i$. For each $i = 1, \ldots, r$ we then define the T-cyclic subspaces $Z_i = Z(v_i, T)$

where Z_1 was defined near the beginning of the proof. We must show that $V = Z_1 \oplus \cdots \oplus Z_r$.

Let deg $p(x) = d$ so that deg $p(x)^{n_i} = dn_i$ (see Theorem 6.2(b)). Since $p(x)^{n_i}$ is the T-order of v_i, Theorem 8.26 shows that $Z(v_i, T)$ has basis

$$\{v_i, T(v_i), \ldots, T^{dn_i-1}(v_i)\} .$$

Similarly, $p(x)^{n_i}$ is also the $\bar{T}$-order of $\bar{v}_i$ for $i = 2, \ldots, r$ and hence $Z(\bar{v}_i, \bar{T})$ has the basis

$$\{\bar{v}_i, \bar{T}(\bar{v}_i), \ldots, \bar{T}^{dn_i-1}(\bar{v}_i)\} .$$

Since $\bar{V} = Z(\bar{v}_2, \bar{T}) \oplus \cdots \oplus Z(\bar{v}_r, \bar{T})$, we see from Theorem 2.15 that $\bar{V}$ has basis

$$\{\bar{v}_2, \ldots, \bar{T}^{dn_2-1}(\bar{v}_2), \ldots, \bar{v}_r, \ldots, \bar{T}^{dn_r-1}(\bar{v}_r)\} .$$

Recall that $\bar{v}_i = u_i + Z_1$ and $v_i \in \bar{v}_i$. This means that $v_i = u_i + z_i$ for some $z_i \in Z_1$ so that

$$\bar{v}_i = v_i - z_i + Z_1 = v_i + Z_1$$

and hence (see the proof of Theorem 7.35)

$$\bar{T}^m(\bar{v}_i) = \bar{T}^m(v_i + Z_1) = \bar{T}^{\bar{m}}(v_i + Z_1) = T^m(v_i) + Z_1 .$$

Using this result in the terms for the basis of $\bar{V}$, Theorem 7.34 shows that V has the basis (where we recall that Z_1 is just $Z(v_1, T)$)

$$\{v_1, \ldots, T^{dn_1-1}(v_1), v_2, \ldots, T^{dn_2-1}(v_2), \ldots, v_r, \ldots, T^{dn_r-1}(v_r)\} .$$

Therefore, by Theorem 2.15, V must be the direct sum of the $Z_i = Z(v_i, T)$ for $i = 1, \ldots, r$. This completes the first part of the proof.

We now turn to the uniqueness of the direct sum expansion of V. Note that we have just shown that $V = Z_1 \oplus \cdots \oplus Z_r$ where each $Z_i = Z(v_i, T)$ is a T-cyclic subspace of V. In addition, the minimal polynomial (i.e., order) of v_i is $p(x)^{n_i}$ where $p(x)$ is a monic prime polynomial of degree d, and $p(x)^n$ is the minimal polynomial for T. Let us assume that we also have the decomposition $V = Z'_1 \oplus \cdots \oplus Z'_s$ where $Z'_i = Z(v'_i, T)$ is a T-cyclic subspace of V, and v'_i has minimal polynomial $p(x)^{m_i}$ with $m_1 \geq \cdots \geq m_s$. (Both v_i and v'_i have orders that are powers of the same polynomial $p(x)$ by the corollary to Theorem 8.25.) We must show that $s = r$ and that $m_i = n_i$ for $i = 1, \ldots, r$.

Suppose that $n_i \neq m_i$ for at least one i, and let k be the first integer such that $n_k \neq m_k$ while $n_j = m_j$ for $j = 1, \ldots, k - 1$. We may arbitrarily take $n_k >$

m_k. Since $V = Z'_1 \oplus \cdots \oplus Z'_s$, any $u \in V$ may be written in the form $u = u'_1 + \cdots + u'_s$ where $u'_i \in Z'_i$. Furthermore, since $p(T)^{m_i}$ is linear, we see that

$$p(T)^{m_i}(u) = p(T)^{m_i}(u'_1) + \cdots + p(T)^{m_i}(u'_s)$$

and hence we may write

$$p(T)^{m_i}(V) = p(T)^{m_i}(Z'_1) \oplus \cdots \oplus p(T)^{m_i}(Z'_s) \ .$$

Using the definition of the T-cyclic subspace Z'_k along with the fact that $p(T)^{m_k}(v'_k) = 0$, it is easy to see that $p(T)^{m_k}(Z'_k) = 0$. But the inequality $m_k \geq m_{k+1} \geq \cdots \geq m_s$ implies that $p(T)^{m_k}(Z'_i) = 0$ for $i = k, k + 1, \ldots, s$ and hence we have

$$p(T)^{m_k}(V) = p(T)^{m_k}(Z'_1) \oplus \cdots \oplus p(T)^{m_k}(Z'_{k-1}) \ .$$

From Example 8.12, we see that $p(T)^{m_i}(Z'_j)$ is of dimension $d(m_j - m_i)$ for $m_i \leq m_j$. This gives us (see the corollary to Theorem 2.15)

$$\dim p(T)^{m_k}(V) = d(m_1 - m_k) + \cdots + d(m_{k-1} - m_k) \ .$$

On the other hand, we have $V = Z_1 \oplus \cdots \oplus Z_r$, and since $k \leq r$ it follows that $Z_1 \oplus \cdots \oplus Z_k \subset V$. Therefore

$$p(T)^{m_k}(V) \supset p(T)^{m_k}(Z_1) \oplus \cdots \oplus p(T)^{m_k}(Z_k)$$

and hence, since $\dim p(T)^{m_i}(Z_j) = d(n_j - m_i)$ for $m_i \leq n_j$, we have

$$\dim p(T)^{m_k}(V) \geq d(n_1 - m_k) + \cdots + d(n_{k-1} - m_k) + d(n_k - m_k) \ .$$

However, $n_i = m_i$ for $i = 1, \ldots, k - 1$ and $n_k > m_k$. We thus have a contradiction in the value of $\dim p(T)^{m_k}(V)$, and hence $n_i = m_i$ for every $i = 1, \ldots, r$ (since if $r < s$ for example, then we would have $0 = n_s \neq m_s$ for every $s > r$). This completes the entire proof of Theorem 8.32. ∎

In order to prove Theorem 8.31 now, we must remove the requirement in Theorem 8.32 that $T \in L(V)$ have minimal polynomial $p(x)^n$. For any finite-dimensional $V \neq \{0\}$, we know that any $T \in L(V)$ has a minimal polynomial $m(x)$ (Theorem 7.4). From the unique factorization theorem (Theorem 6.6), we know that any polynomial can be factored into a product of prime polynomials. We can thus always write $m(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r}$ where each

$p_i(x)$ is prime. Hence, from the primary decomposition theorem (Theorem 7.23), we then see that V is the direct sum of T-invariant subspaces $W_i = \text{Ker } p_i(T)^{n_i}$ for $i = 1, \ldots, r$ such that minimal polynomial of $T_i = T|W_i$ is $p_i(x)^{n_i}$.

Applying Theorem 8.32 to each space W_i and operator $T_i \in L(W_i)$, we see that there exist vectors $w_{i_k} \in W_i$ for $k = 1, \ldots, r_i$ such that W_i is the direct sum of the $Z(w_{i_k}, T_i)$. Moreover, since each W_i is T-invariant, each of the T_i-cyclic subspaces $Z(w_{i_k}, T_i)$ is also T-cyclic, and the minimal polynomial of each generator w_{i_k} is a power of $p_i(x)$. This discussion completes the proof of Theorem 8.31.

Finally, we remark that it is possible to prove the rational form of a matrix from this version (i.e., proof) of the elementary divisor theorem. However, we feel that at this point it is not terribly instructive to do so, and hence the interested reader will have to find this approach in one of the books listed in the bibliography.

Exercise

Prove Theorem 8.31 using the rational canonical form.