Linear Algebra

Kenneth Hoffman

Ray Kunze

Professor of Mathematics, Massachusetts Institute of Technology

Professor of Mathematics, University of California, Irvine

Contents

CHAPTER 1

Linear Equations

CHAPTER 2

Vector Spaces

CHAPTER 3

Linear Transformations

CHAPTER 4

Polynomials

CHAPTER 5

Determinants

5.1. Commutative Rings

In this chapter we shall prove the essential facts about determinants of square matrices. We shall do this not only for matrices over a field, but also for matrices with entries which are 'scalars' of a more general type. There are two reasons for this generality. First, at certain points in the next chapter, we shall find it necessary to deal with determinants of matrices with polynomial entries. Second, in the treatment of determinants which we present, one of the axioms for a field plays no role, namely, the axiom which guarantees a multiplicative inverse for each non-zero element. For these reasons, it is appropriate to develop the theory of determinants for matrices, the entries of which are elements from a commutative ring with identity.

Definition 5.1. A **ring** is a set K, together with two operations $(x, y) \to x + y$ and $(x, y) \to xy$ satisfying

(1) K is a commutative group under the operation $(x, y) \to x + y$ (K is a commutative group under addition);
(2) $(xy)\, z = x\, (yz)$ (multiplication is associative);
(3) $x\, (y + z) = xy + xz$; $(y + z)\, x = yx + zx$ (the two distributive laws hold).

If $xy = yx$ for all x and y in K, we say that the ring K is **commutative**. If there is an element 1 in K such that $1x = x1 = x$ for each x, K is said to be a **ring with identity**, and 1 is called the **identity** for K.

We are interested here in commutative rings with identity. Such a ring can be described briefly as a set K, together with two operations which satisfy all the axioms for a field given in Chapter 1, except possibly for axiom **??** and the condition $1 \neq 0$. Thus, a field is a commutative ring with non-zero identity such that to each non-zero x there corresponds an element x^{-1} with $xx^{-1} = 1$. The set of integers, with the usual operations, is a commutative ring with identity which is not a field. Another commutative ring with identity is the set of all polynomials over a field, together with the addition and multiplication which we have defined for polynomials.

If K is a commutative ring with identity, we define an $m \times n$ matrix over K to be a function A from the set of pairs (i, j) of integers, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, into K. As usual we represent such a matrix by a rectangular array having m rows and n columns. The sum and product of matrices over K are defined as for matrices over a field

$$(A + B)_{ij} = A_{ij} + B_{ij},$$
$$(AB)_{ij} = \sum_k A_{ik} B_{kj},$$

the sum being defined when A and B have the same number of rows and the same number of columns, the product being defined when the number of columns of A is equal to the number of rows of B. The basic algebraic properties of these operations are again valid. For example,

$$A\,(B+C)=AB+AC, \qquad (AB)\,C=A\,(BC)\,, \qquad \text{etc.}$$

As in the case of fields, we shall refer to the elements of K as scalars. We may then define linear combinations of the rows or columns of a matrix as we did earlier. Roughly speaking, all that we previously did for matrices over a field is valid for matrices over K, excluding those results which depended upon the ability to 'divide' in K.

5.2. Determinant Functions

Let K be a commutative ring with identity. We wish to assign to each $n \times n$ (square) matrix over K a scalar (element of K) to be known as the determinant of the matrix. It is possible to define the determinant of a square matrix A by simply writing down a formula for this determinant in terms of the entries of A. One can then deduce the various properties of determinants from this formula. However, such a formula is rather complicated, and to gain some technical advantage we shall proceed as follows. We shall define a 'determinant function' on $K^{n\times n}$ as a function which assigns to each $n \times n$ matrix over K a scalar, the function having these special properties. It is linear as a function of each of the rows of the matrix; its value is 0 on any matrix having two equal rows; and its value on the $n \times n$ identity matrix is 1. We shall prove that such a function exists, and then that it is unique, i.e., that there is precisely one such function. As we prove the uniqueness, an explicit formula for the determinant will be obtained, along with many of its useful properties.

This section will be devoted to the definition of 'determinant function' and to the proof that at least one such function exists.

Definition 5.2. Let K be a commutative ring with identity, n a positive integer, and let D be a function which assigns to each $n \times n$ matrix A over K a scalar $D\,(A)$ in K. We say that D is **n-linear** if for each i, $1 \leqslant i \leqslant n$, D is a linear function of the ith row when the other $(n-1)$ rows are held fixed.

This definition requires some clarification. If D is a function from $K^{n\times n}$ into K, and if α_1, ..., α_n are the rows of the matrix A, let us also write

$$D\,(A)=D\,(\alpha_1,\,\dots,\,\alpha_n)$$

that is, let us also think of D as the function of the rows of A. The statement that D is n-linear then means

$$\begin{aligned}(5.1)\quad D\,(\alpha_1,\,\dots,\,c\alpha_i+\alpha_i',\,\dots,\,\alpha_n)=cD\,(\alpha_1,\,\dots,\,\alpha_i,\,\dots,\,\alpha_n)&\\ +\,D\,(\alpha_1,\,\dots,\,\alpha_i',\,\dots,\,\alpha_n)\,.&\end{aligned}$$

If we fix all rows except row i and regard D as a function of the ith row, it is often convenient to write $D\,(\alpha_i)$ for $D\,(A)$. Thus, we may abbreviate (5.1) to

$$D\,(c\alpha_i+\alpha_i')=cD\,(\alpha_i)+D\,(\alpha_i')$$

so long as it is clear what the meaning is.

Example 5.1. Let k_1, ..., k_n be positive integers, $1 \leqslant k_i \leqslant n$, and let a be an element of K. For each $n \times n$ matrix A over K, define

$$D\,(A)=aA\,(1,\,k_1)\cdots A\,(n,\,k_n)\,. \tag{5.2}$$

Then the function D defined by (5.2) is n-linear. For, if we regard D as a function of the ith row of A, the others being fixed, we may write

$$D\,(\alpha_i)=A\,(i,\,k_i)\,b$$

where b is some fixed element of K. Let $\alpha'_i = (A'_{i1}, \ldots, A'_{in})$. Then we have

$$D(c\alpha_i + \alpha'_i) = [cA(i, k_i) + A'(i, k_i)]\, b = cD(\alpha_i) + D(\alpha'_i).$$

Thus D is a linear function of each of the rows of A.

A particular n-linear function of this type is

$$D(A) = A_{11}A_{22} \cdots A_{nn}.$$

In other words, the 'product of the diagonal entries' is an n-linear function on $K^{n\times n}$.

Example 5.2. Let us find all 2-linear functions on 2×2 matrices over K. Let D be such a function. If we denote the rows of the 2×2 identity matrix by ϵ_1, ϵ_2, we have

$$D(A) = D(A_{11}\epsilon_1 + A_{12}\epsilon_2,\ A_{21}\epsilon_1 + A_{22}\epsilon_2).$$

Using the fact that D is 2-linear, (5.1), we have

$$\begin{aligned} D(A) &= A_{11}D(\epsilon_1,\ A_{21}\epsilon_1 + A_{22}\epsilon_2) + A_{12}D(\epsilon_2,\ A_{21}\epsilon_1 + A_{22}\epsilon_2) \\ &= A_{11}A_{21}D(\epsilon_1, \epsilon_1) + A_{11}A_{22}D(\epsilon_1, \epsilon_2) \\ &\qquad + A_{12}A_{21}D(\epsilon_2, \epsilon_1) + A_{12}A_{22}D(\epsilon_2, \epsilon_2). \end{aligned}$$

Thus D is completely determined by the four scalars

$$D(\epsilon_1, \epsilon_1), \qquad D(\epsilon_1, \epsilon_2), \qquad D(\epsilon_2, \epsilon_1), \qquad \text{and} \qquad D(\epsilon_2, \epsilon_2).$$

The reader should find it easy to verify the following. If a, b, c, d are any four scalars in K and if we define

$$D(A) = A_{11}A_{21}a + A_{11}A_{22}b + A_{12}A_{21}c + A_{12}A_{22}d$$

then D is a 2-linear function on 2×2 matrices over K and

$$\begin{aligned} D(\epsilon_1, \epsilon_1) &= a, \qquad & D(\epsilon_1, \epsilon_2) &= b, \\ D(\epsilon_2, \epsilon_1) &= c, \qquad & D(\epsilon_2, \epsilon_2) &= d. \end{aligned}$$

Lemma 5.1. *A linear combination of n-linear functions is n-linear.*

Proof. It suffices to prove that a linear combination of two n-linear functions is n-linear. Let D and E be n-linear functions. If a and b belong to K, the linear combination $aD + bE$ is of course defined by

$$(aD + bE)(A) = aD(A) + bE(A).$$

Hence, if we fix all rows except row i

$$\begin{aligned} (aD + bE)(c\alpha_i + \alpha'_i) &= aD(c\alpha_i + \alpha'_i) + bE(c\alpha_i + \alpha'_i) \\ &= acD(\alpha_i) + aD(\alpha'_i) + bcE(\alpha_i) + bE(\alpha'_i) \\ &= c(aD + bE)(\alpha_i) + (aD + bE)(\alpha'_i). \end{aligned}$$ □

If K is a field and V is the set of $n \times n$ matrices over K, the above lemma says the following. The set of n-linear functions on V is a subspace of the space of all functions from V into K.

Example 5.3. Let D be the function defined on 2×2 matrices over K by

$$D(A) = A_{11}A_{22} - A_{12}A_{21}. \tag{5.3}$$

Now D is the sum of two functions of the type described in Example 5.1:

$$\begin{aligned} D &= D_1 + D_2, \\ D_1(A) &= A_{11}A_{22}, \\ D_2(A) &= -A_{12}A_{21}. \end{aligned}$$

By the above lemma, D is a 2-linear function. The reader who has had any experience with determinants will not find this surprising, since he will recognize (5.3) as the usual definition of the determinant of a 2×2 matrix. Of course the function D we have just defined is not a typical 2-linear function. It has many special properties. Let us note some of these properties. First, if I is the 2×2 identity matrix, then $D(I) = 1$, i.e., $D(\epsilon_1, \epsilon_2) = 1$. Second, if the two rows of A are equal, then

$$D(A) = A_{11}A_{12} - A_{12}A_{11} = 0.$$

Third, if A' is the matrix obtained from a 2×2 matrix A by interchanging its rows, then $D(A') = -D(A)$; for

$$\begin{aligned} D(A') &= A'_{11}A'_{22} - A'_{12}A'_{21} \\ &= A_{21}A_{12} - A_{22}A_{11} \\ &= -D(A). \end{aligned}$$

Definition 5.3. Let D be an n-linear function. We say D is **alternating** (or **alternate**) if the following two conditions are satisfied:

(1) $D(A) = 0$ whenever two rows of A are equal.
(2) If A' is a matrix obtained from A by interchanging two rows of A, then $D(A') = -D(A)$.

We shall prove below that any n-linear function D which satisfies (1) automatically satisfies (2). We have put both properties in the definition of alternating n-linear function as a matter of convenience. The reader will probably also note that if D satisfies (2) and A is a matrix with two equal rows, then $D(A) = -D(A)$. It is tempting to conclude that D satisfies condition (1) as well. This is true, for example, if K is a field in which $1 + 1 \neq 0$, but in general (1) is not a consequence of (1).

Definition 5.4. Let K be a commutative ring with identity, and let n be a: positive integer. Suppose D is a function from $n \times n$ matrices over K into K. We say that D is a **determinant function** if D is n-linear, alternating, and $D(I) = 1$.

As we stated earlier, we shall ultimately show that there is exactly one determinant function on $n \times n$ matrices over K. This is easily seen for 1×1 matrices $A = [a]$ over K. The function D given by $D(A) = a$ is a determinant function, and clearly this is the only determinant function on 1×1 matrices. We are also in a position to dispose of the case $n = 2$. The function

$$D(A) = A_{11}A_{22} - A_{12}A_{21} \tag{5.4}$$

was shown in Example 5.3 to be a determinant function. Furthermore, the formula exhibited in Example 5.2 shows that D is the only determinant function on 2×2 matrices. For we showed that for any 2-linear function D

$$\begin{aligned} D(A) = A_{11}A_{21}D(\epsilon_1, \epsilon_1) &+ A_{11}A_{22}D(\epsilon_1, \epsilon_2) \\ &+ A_{12}A_{21}D(\epsilon_2, \epsilon_1) + A_{12}A_{22}D(\epsilon_2, \epsilon_2). \end{aligned}$$

If D is alternating, then

$$D(\epsilon_1, \epsilon_1) = D(\epsilon_2, \epsilon_2) = 0$$

and

$$D(\epsilon_2, \epsilon_1) = -D(\epsilon_1, \epsilon_2) = -D(I).$$

If D also satisfies $D(I) = 1$, then

$$D(A) = A_{11}A_{22} - A_{12}A_{21}.$$

EXAMPLE 5.4. Let F be a field and let D be any alternating 3-linear function on 3×3 matrices over the polynomial ring $F[x]$.

Let

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

If we denote the rows of the 3×3 identity matrix by ϵ_1, ϵ_2, ϵ_3, then

$$D(A) = D\left(x\epsilon_1 - x^2\epsilon_3,\, \epsilon_2,\, \epsilon_1 + x^3\epsilon_3\right).$$

Since D is linear as a function of each row,

$$\begin{aligned} D(A) &= xD(\epsilon_1,\, \epsilon_2,\, \epsilon_1 + x^3\epsilon_3) - x^2 D(\epsilon_3,\, \epsilon_2,\, \epsilon_1 + x^3\epsilon_3) \\ &= xD(\epsilon_1,\, \epsilon_2,\, \epsilon_1) + x^4 D(\epsilon_1,\, \epsilon_2,\, \epsilon_3) - x^2 D(\epsilon_3,\, \epsilon_2,\, \epsilon_1) - x^5 D(\epsilon_3,\, \epsilon_2,\, \epsilon_3). \end{aligned}$$

Because D is alternating it follows that

$$D(A) = \left(x^4 + x^2\right) D(\epsilon_1,\, \epsilon_2,\, \epsilon_3).$$

LEMMA 5.2. *Let D be a 2-linear function with the property that $D(A) = 0$ for all 2×2 matrices A over K having equal rows. Then D is alternating.*

PROOF. What we must show is that if A is a 2×2 matrix and A' is obtained by interchanging the rows of A, then $D(A') = -D(A)$. lf the rows of A are α and β, this means we must show that $D(\beta,\, \alpha) = -D(\alpha,\, \beta)$. Since D is 2-linear,

$$D(\alpha + \beta,\, \alpha + \beta) = D(\alpha,\, \alpha) + D(\alpha,\, \beta) + D(\beta,\, \alpha) + D(\beta,\, \beta).$$

By our hypothesis $D(\alpha + \beta,\, \alpha + \beta) = D(\alpha,\, \alpha) = D(\beta,\, \beta) = 0$. So

$$0 = D(\alpha,\, \beta) + D(\beta,\, \alpha).$$ □

LEMMA 5.3. *Let D be an n-linear function on $n \times n$ matrices over K. Suppose D has the property that $D(A) = 0$ whenever two adjacent rows of A are equal. Then D is alternating.*

PROOF. □

CHAPTER 6

Elementary Canonical Forms

6.1. Introduction

We have mentioned earlier that our principal aim is to study linear transformations on finite-dimensional vector spaces. By this time, we have seen many specific examples of linear transformations, and we have proved a few theorems about the general linear transformation. In the finite-dimensional case we have utilized ordered bases to represent such transformations by matrices, and this representation adds to our insight into their behavior. We have explored the vector space $L(V, W)$, consisting of the linear transformations from one space into another, and we have explored the linear algebra $L(V, V)$, consisting of the linear transformations of a space into itself.

In the next two chapters, we shall be preoccupied with linear operators. Our program is to select a single linear operator T on a finite-dimensional vector space V and to 'take it apart to see what makes it tick.' At this early stage, it is easiest to express our goal in matrix language: Given the linear operator T, find an ordered basis for V in which the matrix of T assumes an especially simple form.

Here is an illustration of what we have in mind. Perhaps the simplest matrices to work with, beyond the scalar multiples of the identity, are the diagonal matrices:

$$D = \begin{bmatrix} c_1 & 0 & 0 & \cdots & 0 \\ 0 & c_2 & 0 & \cdots & 0 \\ 0 & 0 & c_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & c_n \end{bmatrix}. \tag{6.1}$$

Let T be a linear operator on an n-dimensional space V. If we could find an ordered basis $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ for V in which T were represented by a diagonal matrix D (6.1), we would gain considerable information about T. For instance, simple numbers associated with T, such as the rank of T or the determinant of T, could be determined with little more than a glance at the matrix D. We could describe explicitly the range and the null space of T. Since $[T]_{\mathcal{B}} = D$ if and only if

$$T_{\alpha_k} = c_k \alpha_k, \qquad k = 1, \dots, n, \tag{6.2}$$

the range would be the subspace spanned by those α_k's for which $c_k \neq 0$ and the null space would be spanned by the remaining α_k's. Indeed, it seems fair to say that, if we knew a basis $\mathcal{B}$ and a diagonal matrix D such that $[T]_{\mathcal{B}} = D$, we could answer readily any question about T which might arise.

Can each linear operator T be represented by a diagonal matrix in some ordered basis? If not, for which operators T does such a basis exist? How can we find such a basis if there is one? If no such basis exists, what is the simplest type of matrix by which we can represent T? These are some of the questions which we shall attack in this (and the next) chapter. The form of our questions will become more sophisticated as we learn what some of the difficulties are.

6.2. Characteristic Values

The introductory remarks of the previous section provide us with a starting point for our attempt to analyze the general linear operator T. We take our cue from (6.2), which suggests that we should study vectors which are sent by T into scalar multiples of themselves.

Definition 6.1. Let V be a vector space over the field F and let T be a linear operator on V. A **characteristic value** of T is a scalar c in F such that there is a non-zero vector α in V with $T\alpha = c\alpha$. If c is a characteristic value of T, then

(1) any α such that $T\alpha = c\alpha$ is called a **characteristic vector** of T associated with the characteristic value c;
(2) the collection of all α such that $T\alpha = c\alpha$ is called the **characteristic space** associated with c.

Characteristic values are often called characteristic roots, latent roots, eigenvalues, proper values, or spectral values. In this book we shall use only the name 'characteristic values.'

If T is any linear operator and c is any scalar, the set of vectors α such that $T\alpha = c\alpha$ is a subspace of V. It is the null space of the linear transformation $(T - cI)$. We call c a characteristic value of T if this subspace is different from the zero subspace, i.e., if $(T - cI)$ fails to be 1:1. If the underlying space V is finite-dimensional, $(T - cI)$ fails to be 1:1 precisely when its determinant is different from 0. Let us summarize.

Theorem 6.1. *Let T be a linear operator on a finite-dimensional space V and let c he a scalar. The following are equivalent.*

(1) c is a characteristic value of T.
(2) The operator $(T - cI)$ is singular (not invertible).
(3) $\det(T - cI) = 0$.

The determinant criterion (3) is very important because it tells us where to look for the characteristic values of T. Since $\det(T - cI)$ is a polynomial of degree n in the variable c, we will find the characteristic values as the roots of that polynomial. Let us explain carefully.

If $\mathcal{B}$ is any ordered basis for V and $A = [T]_{\mathcal{B}}$, then $(T - cI)$ is invertible if and only if the matrix $(A - cI)$ is invertible. Accordingly, we make the following definition.

Definition 6.2. If A is an $n \times n$ matrix over the field F, a **characteristic value of A in F** is a scalar c in F such that the matrix $(A - cI)$ is singular (not invertible).

Since c is a characteristic value of A if and only if $\det(A - cI) = 0$, or equivalently if and only if $\det(cI - A) = 0$, we form the matrix $(xI - A)$ with polynomial entries, and consider the polynomial $f = \det(xI - A)$. Clearly the characteristic values of A in F are just the scalars c in F such that $f(c) = 0$. For this reason f is called the **characteristic polynomial** of A. It is important to note that f is a monic polynomial which has degree exactly n. This is easily seen from the formula for the determinant of a matrix in terms of its entries.

Lemma 6.1. *Similar matrices have the same characteristic polynomial.*

Proof. It $B = P^{-1}AP$, then

$$\begin{aligned}\det(xI - B) &= \det(xI - P^{-1}AP)\\ &= \det\left(P^{-1}(xI - A)\,P\right)\end{aligned}$$

$$
\begin{aligned}
&= \det P^{-1} \cdot \det (xI - A) \cdot \det P \\
&= \det (xI - A) . \qquad \square
\end{aligned}
$$

This lemma enables us to define sensibly the characteristic polynomial of the operator T as the characteristic polynomial of any $n \times n$ matrix which represents T in some ordered basis for V. Just as for matrices, the characteristic values of T will be the roots of the characteristic polynomial for T. In particular, this shows us that T cannot have more than n distinct characteristic values. It is important to point out that T may not have any characteristic values.

EXAMPLE 6.1. Let T be the linear operator on R^2 which is represented in the standard ordered basis by the matrix

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

The characteristic polynomial for T (or for A) is

$$\det (xI - A) = \begin{vmatrix} x & 1 \\ -1 & x \end{vmatrix} = x^2 + 1.$$

Since this polynomial has no real roots, T has no characteristic values. If U is the linear operator on C^2 which is represented by A in the standard ordered basis, then U has two characteristic values, i and $-$i. Here we see a subtle point. In discussing the characteristic values of a matrix A, we must be careful to stipulate the field involved. The matrix A above has no characteristic values in R, but has the two characteristic values i and $-$i in C.

EXAMPLE 6.2. Let A be the (real) 3×3 matrix

$$\begin{bmatrix} 3 & 1 & -1 \\ 2 & 2 & -1 \\ 2 & 2 & 0 \end{bmatrix}.$$

Then the characteristic polynomial for A is

$$\begin{vmatrix} x-3 & -1 & 1 \\ -2 & x-2 & 1 \\ -2 & -2 & x \end{vmatrix} = x^3 - 5x^2 + 8x - 4 = (x-1)(x-2)^2 .$$

Thus the characteristic values of A are 1 and 2.

Suppose that T is the linear operator on R^3 which is represented by A in the standard basis. Let us find the characteristic vectors of T associated with the characteristic values, 1 and 2. Now

$$A - I = \begin{bmatrix} 2 & 1 & -1 \\ 2 & 1 & -1 \\ 2 & 2 & -1 \end{bmatrix}.$$

It is obvious at a glance that $A - I$ has rank equal to 2 (and hence $T - I$ has nullity equal to 1). So the space of characteristic vectors associated with the characteristic value 1 is one-dimensional. The vector $\alpha_1 = (1, 0, 2)$ spans the null space of $T - I$. Thus $T\alpha = \alpha$ if and only if α is a scalar multiple of α_1. Now consider

$$A - 2I = \begin{bmatrix} 1 & 1 & -1 \\ 2 & 0 & -1 \\ 2 & 2 & -2 \end{bmatrix}.$$

Evidently $A-2I$ also has rank 2, so that the space of characteristic vectors associated with the characteristic value 2 has dimension 1. Evidently $T\alpha = 2\alpha$ if and only if α is a scalar multiple of $\alpha_2 = (1, 1, 2)$.

DEFINITION 6.3. Let T be a linear operator on the finite-dimensional space V. We say that T is **diagonalizable** if there is a basis for V each vector of which is a characteristic vector of T.

The reason for the name should be apparent; for, if there is an ordered basis $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ for V in which each α_i is a characteristic vector of T, then the matrix of T in the ordered basis $\mathcal{B}$ is diagonal. If $T_{\alpha_i} = c_i\alpha_i$, then

$$[T]_{\mathcal{B}} = \begin{bmatrix} c_1 & 0 & \cdots & 0 \\ 0 & c_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & c_n \end{bmatrix}.$$

We certainly do not require that the scalars $c_1, \dots, c_n$ be distinct; indeed, they may all be the same scalar (when T is a scalar multiple of the identity operator).

One could also define T to be diagonalizable when the characteristic vectors of T span V. This is only superficially different from our definition, since we can select a basis out of any spanning set of vectors.

For Examples 6.1 and 6.2 we purposely chose linear operators T on R^n which are not diagonalizable. In Example 6.1, we have a linear operator on R^2 which is not diagonalizable, because it has no characteristic values. In Example 6.2, the operator T has characteristic values; in fact, the characteristic polynomial for T factors completely over the real number field: $f = (x-1)(x-2)^2$. Nevertheless T fails to be diagonalizable. There is only a one-dimensional space of characteristic vectors associated with each of the two characteristic values of T. Hence, we cannot possibly form a basis for R^3 which consists of characteristic vectors of T.

Suppose that T is a diagonalizable linear operator. Let $c_1, \dots, c_k$ be the *distinct* characteristic values of T. Then there is an ordered basis $\mathcal{B}$ in which T is represented by a diagonal matrix which has for its diagonal entries the scalars c_i, each repeated a certain number of times. If c_i is repeated d_i times, then (we may arrange that) the matrix has the block form

$$[T]_{\mathcal{B}} = \begin{bmatrix} c_1I_1 & 0 & \cdots & 0 \\ 0 & c_2I_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & c_kI_k \end{bmatrix} \tag{6.3}$$

where I_j is the $d_j \times d_j$ identity matrix. From that matrix we see two things. First, the characteristic polynomial for T is the product of (possibly repeated) linear factors:

$$f = (x-c_1)^{d_1} \cdots (x-c_k)^{d_k}$$

If the scalar field F is algebraically closed, e.g., the field of complex numbers, every polynomial over F can be so factored (see Section ??); however, if F is not algebraically closed, we are citing a special property of T when we say that its characteristic polynomial has such a factorization. The second thing we see from (6.3) is that d_i, the number of times which c_i is repeated as root of f, is equal to the dimension of the space of characteristic vectors associated with the characteristic value c_i. That is because the nullity of a diagonal matrix is equal to the number of zeros which it has on its main diagonal, and the matrix $[T - c_iI]_{\mathcal{B}}$ has d_i zeros on its main diagonal. This relation between the dimension of the characteristic space and the multiplicity of the characteristic value as a root of f does not seem exciting at first; however, it will provide us with a simpler way of determining whether a given operator is diagonalizable.

LEMMA 6.2. *Suppose that $T\alpha = c\alpha$. If f is any polynomial, then $f(T)\alpha = f(c)\alpha$.*

PROOF. Exercise. □

LEMMA 6.3. *Let T be a linear operator on the finite-dimensional space V. Let c_1, ..., c_k be the distinct characteristic values of T and let W_i be the space of characteristic vectors associated with the characteristic value c_i. If $W = W_1 + \cdots + W_k$, then*

$$\dim W = \dim W_1 + \cdots + \dim W_k.$$

In fact, if $\mathcal{B}_i$ is an ordered basis for W_i, then $\mathcal{B} = (\mathcal{B}_1, \ldots, \mathcal{B}_k)$ is an ordered basis for W.

PROOF. The space $W = W_1 + \cdots + W_k$ is the subspace spanned by all of the characteristic vectors of T. Usually when one forms the sum W of subspaces W_i, one expects that $\dim W < \dim W_1 + \cdots + \dim W_k$ because of linear relations which may exist between vectors in the various spaces. This lemma states that the characteristic spaces associated with different characteristic values are independent of one another.

Suppose that (for each i) we have a vector β_i in W_i, and assume that $\beta_1 + \cdots + \beta_k = 0$. We shall show that $\beta_i = 0$ for each i. Let f be any polynomial. Since $T\beta_i = c_i\beta_i$, the preceding lemma tells us that

$$\begin{aligned} 0 = f(T)\,0 &= f(T)\,\beta_1 + \cdots + f(T)\,\beta_k \\ &= f(c_1)\,\beta_1 + \cdots + f(c_k)\,\beta_k. \end{aligned}$$

Choose polynomials f_1, ..., f_k such that

$$f_i(c_j) = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

Then

$$\begin{aligned} 0 = f_i(T)\,0 &= \sum_j \delta_{ij}\beta_j \\ &= \beta_i. \end{aligned}$$

Now, let $\mathcal{B}_i$ be an ordered basis for W_i, and let $\mathcal{B}$ be the sequence $\mathcal{B} = (\mathcal{B}_1, \ldots, \mathcal{B}_k)$. Then $\mathcal{B}$ spans the subspace $W = W_i + \cdots + W_k$. Also, $\mathcal{B}$ is a linearly independent sequence of vectors, for the following reason. Any linear relation between the vectors in $\mathcal{B}$ will have the form $\beta_1 + \cdots + \beta_k = 0$, where β_i is some linear combination of the vectors in $\mathcal{B}_i$. From what we just did, we know that $\beta_i = 0$ for each i. Since each $\mathcal{B}_i$ is linearly independent, we see that we have only the trivial linear relation between the vectors in $\mathcal{B}$. □

THEOREM 6.2. *Let T be a linear operator on a finite-dimensional space V. Let c_1, ..., c_k be the distinct characteristic values of T and let W_i be the null space of $(T - c_iI)$. The following are equivalent.*

(1) T is diagonalizable.
(2) The characteristic polynomial for T is

$$f = (X - c_1)^{d_1} \cdots (X - c_k)^{d_k}$$

and $\dim W_i = d_i$, $i = 1, \ldots, k$.
(3) $\dim W_1 + \cdots + \dim W_k = \dim V$.

PROOF. We have observed that (1) implies (2). If the characteristic polynomial f is the product of linear factors, as in (2), then $d_1 + \cdots + d_k = \dim V$. For, the sum of the d_i's is the degree of the characteristic polynomial, and that degree is $\dim V$. Therefore (2) implies (3). Suppose (3) holds. By the lemma, we must have $V = W_1 + \cdots + W_k$, i.e., the characteristic vectors of T span V. □

The matrix analogue of Theorem 6.2 may be formulated as follows. Let A be an $n \times n$ matrix with entries in a field F, and let c_1, ..., c_k be the distinct characteristic values of A in F. For each i, let W_i be the space of column matrices X (with entries in F) such that

$$(A - c_i I)\, X = 0,$$

and let $\mathcal{B}_i$ be an ordered basis for W_i. The bases $\mathcal{B}_1$, ..., $\mathcal{B}_k$ collectively string together to form the sequence of columns of a matrix P:

$$P = [P_1, P_2, ...] = (\mathcal{B}_1, \ldots, \mathcal{B}_k).$$

The matrix A is similar over F to a diagonal matrix if and only if P is a square matrix. When P is square, P is invertible and $P^{-1}AP$ is diagonal.

EXAMPLE 6.3. Let T be the linear operator on R^3 which is represented in the standard ordered basis by the matrix

$$A = \begin{bmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}.$$

Let us indicate how one might compute the characteristic polynomial, using various row and column operations:

$$\begin{aligned} \begin{vmatrix} x-5 & 6 & 6 \\ 1 & x-4 & -2 \\ -3 & 6 & x+4 \end{vmatrix} &= \begin{vmatrix} x-5 & 0 & 6 \\ 1 & x-2 & -2 \\ -3 & 2-x & x+4 \end{vmatrix} \\ &= (x-2) \begin{vmatrix} x-5 & 0 & 6 \\ 1 & 1 & -2 \\ -3 & -1 & x+4 \end{vmatrix} \\ &= (x-2) \begin{vmatrix} x-5 & 6 \\ -2 & x+2 \end{vmatrix} \\ &= (x-2)\,(x^2 - 3x + 2) \\ &= (x-2)^2\,(x-1). \end{aligned}$$

What are the dimensions of the spaces of characteristic vectors associated with the two characteristic values? We have

$$A - I = \begin{bmatrix} 4 & -6 & -6 \\ -1 & 3 & 2 \\ 3 & -6 & -5 \end{bmatrix}$$

$$A - 2I = \begin{bmatrix} 3 & -6 & -6 \\ -1 & 2 & 2 \\ 3 & -6 & -6 \end{bmatrix}.$$

We know that $A - I$ is singular and obviously $\operatorname{rank}(A - I) \geqslant 2$. Therefore, $\operatorname{rank}(A - I) = 2$. It is evident that $\operatorname{rank}(A - 2I) = 1$.

Let W_1, W_2 be the spaces of characteristic vectors associated with the characteristic values 1, 2. We know that $\dim W_1 = 1$ and $\dim W_2 = 2$. By Theorem 6.2, T is diagonalizable. It is easy to exhibit a basis for R^3 in which T is represented by a diagonal matrix. The null space of $(T - I)$ is spanned by the vector $\alpha_1 = (3, -1, 3)$ and so α_1 is a basis for W_1. The null space of $T - 2I$ (i.e., the space W_2) consists of the vectors (x_1, x_2, x_3) with $x_1 = 2x_2 + 2x_3$. Thus, one example of a basis for W_2 is

$$\begin{aligned} \alpha_2 &= (2, 1, 0) \\ \alpha_3 &= (2, 0, 1). \end{aligned}$$

If $\mathcal{B} = \{\alpha_1, \alpha_2, \alpha_3\}$, then $[T]_{\mathcal{B}}$ is the diagonal matrix

$$D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

The fact that T is diagonalisable means that the original matrix A is similar (over R) to the diagonal matrix D. The matrix P which enables us to change coordinates from the basis $\mathcal{B}$ to the standard basis is (of course) the matrix which has the transposes of α_1, α_2, α_3 as its column vectors:

$$P = \begin{bmatrix} 3 & 2 & 2 \\ -1 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix}.$$

Furthermore, $AP = PD$, so that

$$P^{-1}AP = D.$$

Exercises.

(1) In each of the following cases, let T be the linear operator on R^2 which is represented by the matrix A in the standard ordered basis for R^2, and let U be the linear operator on C^2 represented by A in the standard ordered basis. Find the characteristic polynomial for T and that for U, find the characteristic values of each operator, and for each such characteristic value c find a basis for the corresponding space of characteristic vectors.

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad A = \begin{bmatrix} 2 & 3 \\ -1 & 1 \end{bmatrix}, \qquad A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

(2) Let V be an n-dimensional vector space over F. What is the characteristic polynomial of the identity operator on V? What is the characteristic polynomial for the zero operator?

(3) Let A be an $n \times n$ triangular matrix over the field F. Prove that the characteristic values of A are the diagonal entries of A, i.e., the scalars A_{ii}.

(4) Let T be the linear operator on R^3 which is represented in the standard ordered basis by the matrix

$$\begin{bmatrix} -9 & 4 & 4 \\ -8 & 3 & 4 \\ -16 & 8 & 7 \end{bmatrix}.$$

Prove that T is diagonalizable by exhibiting a basis for R^3, each vector of which is a characteristic vector of T.

(5) Let

$$A = \begin{bmatrix} 6 & -3 & -2 \\ 4 & -1 & -2 \\ 10 & -5 & -3 \end{bmatrix}.$$

Is A similar over the field R to a diagonal matrix? Is A similar over the field C to a diagonal matrix?

(6) Let T be the linear operator on R^4 which is represented in the standard ordered basis by the matrix

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \end{bmatrix}.$$

Under what conditions on a, b, and c is T diagonalizable?

(7) Let T be a linear operator on the n-dimensional vector space V, and suppose that T has n *distinct* characteristic values. Prove that T is diagonalizable.

(8) Let A and B be $n \times n$ matrices over the field F. Prove that if $(I - AB)$ is invertible, then $I - BA$ is invertible and

$$(I - BA)^{-1} = I + B\,(I - AB)^{-1}\,A.$$

(9) Use the result of Exercise (8) to prove that, if A and B are $n \times n$ matrices over the field F, then AB and BA have precisely the same characteristic values in F.

(10) Suppose that A is a 2×2 matrix with real entries which is symmetric ($A^{\top} = A$). Prove that A is similar over R to a diagonal matrix.

(11) Let N be a 2×2 complex matrix such that $N^2 = 0$. Prove that either $N = 0$ or N is similar over C to

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

(12) Use the result of Exercise (11) to prove the following: If A is a 2×2 matrix with complex entries, then A is similar over C to a matrix of one of the two types

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \qquad \begin{bmatrix} a & 0 \\ 1 & a \end{bmatrix}.$$

(13) Let V be the vector space of all functions from R into R which are continuous, i.e., the space of continuous real-valued functions on the real line. Let T be the linear operator on V defined by

$$(Tf)\,(x) = \int_0^x f\,(t)\,\mathrm{d}t.$$

Prove that T has no characteristic values.

(14) Let A be an $n \times n$ diagonal matrix with characteristic polynomial

$$(x - c_1)^{d_1} \cdots (x - c_k)^{d_k},$$

where c_1, ..., c_k are distinct. Let V be the space of $n \times n$ matrices B such that $AB = BA$. Prove that the dimension of V is $d_1^2 + \cdots + d_k^2$.

(15) Let V be the space of $n \times n$ matrices over F. Let A be a fixed $n \times n$ matrix over F. Let T be the linear operator 'left multiplication by A' on V. Is it true that A and T have the same characteristic values?

6.3. Annihilating Polynomials

In attempting to analyze a linear operator T, one of the most useful things to know is the class of polynomials which annihilate T. Specifically, suppose T is a linear operator on V, a vector space over the field F. If p is a polynomial over F, then $p\,(T)$ is again a linear operator on V. If q is another polynomial over F, then

$$(p + q)\,(T) = p\,(T) + q\,(T)$$
$$(pq)\,(T) = p\,(T)\,q\,(T)\,.$$

Therefore, the collection of polynomials p which annihilate T, in the sense that

$$p\,(T) = 0,$$

is an ideal in the polynomial algebra $F[x]$. It may be the zero ideal, i.e., it may be that T is not annihilated by any non-zero polynomial. But, that cannot happen if the space V is finite-dimensional.

Suppose T is a linear operator on the n-dimensional space V. Look at the first (n^2+1) powers of T:

$$I,\, T,\, T^2,\, \dots,\, T^{n^2}.$$

This is a sequence of n^2+1 operators in $L(V,\, V)$, the space of linear operators on V. The space $L(V,\, V)$ has dimension n^2. Therefore, that sequence of n^2+1 operators must be linearly dependent, i.e., we have

$$c_0 I + c_1 T + \cdots + c_{n^2} T^{n^2} = 0$$

for some scalars c_i, not all zero. So, the ideal of polynomials which annihilate T contains a non-zero polynomial of degree n^2 or less.

According to Theorem **??** of Chapter 4, every polynomial ideal consists of all multiples of some fixed monic polynomial, the generator of the ideal. Thus, there corresponds to the operator T a monic polynomial p with this property: If f is a polynomial over F, then $f(T) = 0$ if and only if $f = pg$, where g is some polynomial over F.

Definition 6.4. Let T he a linear operator on a finite-dimensional vector space V over the field F. The **minimal polynomial** for T is the (unique) monic generator of the ideal of polynomials over F which annihilate T.

The name 'minimal polynomial' stems from the fact that the generator of a polynomial ideal is characterized by being the monic polynomial of minimum degree in the ideal. That means that the minimal polynomial p for the linear operator T is uniquely determined by these three properties:

(1) p is a monic polynomial over the scalar field F.
(2) $p(T) = 0$.
(3) No polynomial over F which annihilates T has smaller degree than p has.

If A is an $n \times n$ matrix over F, we define the **minimal polynomial** for A in an analogous way, as the unique monic generator of the ideal of all polynomials over F which annihilate A. If the operator T is represented in some ordered basis by the matrix A, then T and A have the same minimal polynomial. That is because $f(T)$ is represented in the basis by the matrix $f(A)$, so that $f(T) = 0$ if and only if $f(A) = 0$.

From the last remark about operators and matrices it follows that similar matrices have the same minimal polynomial. That fact is also clear from the definitions because

$$f(P^{-1}AP) = P^{-1} f(A)\, P$$

for every polynomial f.

There is another basic remark which we should make about minimal polynomials of matrices. Suppose that A is an $n \times n$ matrix with entries in the field F. Suppose that F_1 is a field which contains F as a subfield. (For example, A might be a matrix with rational entries, while F_1 is the field of real numbers. Or, A might be a matrix with real entries, while F_1 is the field of complex numbers.) We may regard A either as an $n \times n$ matrix over F or as an $n \times n$ matrix over F_1. On the surface, it might appear that we obtain two different minimal polynomials for A. Fortunately that is not the case; and we must see why. What is the definition of the minimal polynomial for A, regarded as an $n \times n$ matrix over the field F? We consider all monic polynomials with coefficients in F which annihilate A, and we choose the one of least degree. If f is a monic polynomial over F:

$$f = x^k + \sum_{j=0}^{k-1} a_j x^j \tag{6.4}$$

then $f(A) = 0$ merely says that we have a linear relation between the powers of A:

$$A^k + a_{k-1}A^{k-1} + \cdots + a_1 A + a_0 I = 0. \tag{6.5}$$

The degree of the minimal polynomial is the least positive integer k such that there is a linear relation of the form (6.5) between the powers I, A, ..., A^k. Furthermore, by the uniqueness of the minimal polynomial, there is for that k one and only one relation of the form (6.5); i.e., once the minimal k is determined, there are unique scalars a_0, ..., a_{k-1} in F such that (6.5) holds. They are the coefficients of the minimal polynomial.

Now (for each k) we have in (6.5) a system of n^2 linear equations for the 'unknowns' a_0, ..., a_{k-1}. Since the entries of A lie in F, the coefficients of the system of equations (6.5) are in F. Therefore, if the system has a solution with a_0, ..., a_{k-1} in F_1 it has a solution with a_0, ..., a_{k-1} in F. (See the end of Section **??**.) It should now be clear that the two minimal polynomials are the same.

What do we know thus far about the minimal polynomial for a linear operator on an n-dimensional space? Only that its degree does not exceed n^2. That turns out to be a rather poor estimate, since the degree cannot exceed n. We shall prove shortly that the operator is annihilated by its characteristic polynomial. First, let us observe a more elementary fact.

THEOREM 6.3. *Let T he a linear operator on an n-dimensional vector space V [or, let A be an $n \times n$ matrix]. The characteristic and minimal polynomials for T [for A] have the same roots, except for multiplicities.*

PROOF. Let p be the minimal polynomial for T. Let c be a scalar. What we want to show is that $p(c) = 0$ if and only if c is a characteristic value of T.

First, suppose $p(c) = 0$. Then

$$p = (x - c)\, q$$

where q is a polynomial. Since $\deg q < \deg p$, the definition of the minimal polynomial p tells us that $q(T) \neq 0$. Choose a vector β such that $q(T)\,\beta \neq 0$. Let $\alpha = q(T)\,\beta$. Then

$$\begin{aligned} 0 &= p(T)\,\beta \\ &= (T - cI)\, q(T)\,\beta \\ &= (T - cI)\,\alpha \end{aligned}$$

and thus, c is a characteristic value of T.

Now, suppose that c is a characteristic value of T, say, $T\alpha = c\alpha$ with $\alpha \neq 0$. As we noted in a previous lemma,

$$p(T)\,\alpha = p(c)\,\alpha.$$

Since $p(T) = 0$ and $\alpha \neq 0$, we have $p(c) = 0$. □

Let T be a diagonalizable linear operator and let c_1, ..., c_k be the distinct characteristic values of T. Then it is easy to see that the minimal polynomial for T is the polynomial

$$p = (x - c_1) \cdots (x - c_k).$$

If α is a characteristic vector, then one of the operators $T - c_1 I$, ..., $T - c_k I$ sends α into 0. Therefore

$$(T - c_1 I) \cdots (T - c_k I)\,\alpha = 0$$

for every characteristic vector α. There is a basis for the underlying space which consists of characteristic vectors of T; hence

$$p(T) = (T - c_1 I) \cdots (T - c_k I) = 0.$$

What we have concluded is this. If T is a diagonalizable linear operator, then the minimal polynomial for T is a product of distinct linear factors. As we shall soon see, that property characterizes diagonalizable operators.

EXAMPLE 6.4. Let's try to find the minimal polynomials for the operators in Examples 6.1, 6.2, and 6.3. We shall discuss them in reverse order. The operator in Example 6.3 was found to be diagonalizable with characteristic polynomial

$$f = (x-1)(x-2)^2 .$$

From the preceding paragraph, we know that the minimal polynomial for T is

$$p = (x-1)(x-2) .$$

The reader might find it reassuring to verify directly that

$$(A-I)(A-2I) = 0.$$

In Example 6.2, the operator T also had the characteristic polynomial $f = (x-1)(x-2)^2$. But, this T is not diagonalizable, so we don't know that the minimal polynomial is $(x-1)(x-2)$. What do we know about the minimal polynomial in this case? From Theorem 6.3 we know that its roots are 1 and 2, with some multiplicities allowed. Thus we search for p among polynomials of the form $(x-1)^k(x-2)^l$, $k \geqslant 1$, $l \geqslant 1$. Try $(x-1)(x-2)$:

$$\begin{aligned}(A-I)(A-2I) &= \begin{bmatrix} 2 & 1 & -1 \\ 2 & 1 & -1 \\ 2 & 2 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 & -1 \\ 2 & 0 & -1 \\ 2 & 2 & -2 \end{bmatrix} \\ &= \begin{bmatrix} 2 & 0 & -1 \\ 2 & 0 & -1 \\ 4 & 0 & -2 \end{bmatrix}.\end{aligned}$$

Thus, the minimal polynomial has degree at least 3. So, next we should try either $(x-1)^2(x-2)$ or $(x-1)(x-2)^2$. The second, being the characteristic polynomial, would seem a less random choice. One can readily compute that $(A-I)(A-2I)^2 = 0$. Thus the minimal polynomial for T is its characteristic polynomial.

In Example 6.1 we discussed the linear operator T on R^2 which is represented in the standard basis by the matrix

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

The characteristic polynomial is x^2+1, which has no real roots. To determine the minimal polynomial, forget about T and concentrate on A. As a complex 2×2 matrix, A has the characteristic values i and $-$i. Both roots must appear in the minimal polynomial. Thus the minimal polynomial is divisible by x^2+1. It is trivial to verify that $A^2 + I = 0$. So the minimal polynomial is x^2+1.

THEOREM 6.4 (Cayley–Hamilton). *Let T be a linear operator on a finite dimensional vector space V. If f is the characteristic polynomial for T, then $f(T) = 0$; in other words, the minimal polynomial divides the characteristic polynomial for T.*

PROOF. Later on we shall give two proofs of this result independent of the one to be given here. The present proof, although short, may be difficult to understand. Aside from brevity, it has the virtue of providing an illuminating and far from trivial application of the general theory of determinants developed in Chapter 5.

Let K be the commutative ring with identity consisting of all polynomials in T. Of course, K is actually a commutative algebra with identity over the scalar field. Choose an ordered basis $\{\alpha_1, \dots, \alpha_n\}$ for V, and let A be the matrix which represents T in the given basis. Then

$$T\alpha_i = \sum_{j=1}^{n} A_{ji}\alpha_j, \qquad 1 \leqslant i \leqslant n.$$

These equations may be written in the equivalent form

$$\sum_{j=1}^{n} \left(\delta_{ij}T - A_{ji}I\right)\alpha_j = 0, \qquad 1 \leqslant i \leqslant n.$$

Let B denote the element of $K^{n\times n}$ with entries

$$B_{ij} = \delta_{ij}T - A_{ji}I.$$

When $n = 2$

$$B = \begin{bmatrix} T - A_{11}I & -A_{21}I \\ -A_{12}I & T - A_{22}I \end{bmatrix}$$

and

$$\begin{aligned} \det B &= (T - A_{11}I)(T - A_{22}I) - A_{12}A_{21}I \\ &= T^2 - (A_{11} + A_{22})T + (A_{11}A_{22} - A_{12}A_{21})I \\ &= f(T) \end{aligned}$$

where f is the characteristic polynomial:

$$f = x^2 - (\operatorname{tr} A)x + \det A.$$

For the case $n > 2$, it is also clear that

$$\det B = f(T)$$

since f is the determinant of the matrix $xI - A$ whose entries are the polynomials

$$(xI - A)_{ij} = \delta_{ij}x - A_{ji}.$$

We wish to show that $f(T) = 0$. In order that $f(T)$ be the zero operator, it is necessary and sufficient that $(\det B)\alpha_k = 0$ for $k = 1, \dots, n$. By the definition of B, the vectors $\alpha_1, \dots, \alpha_n$ satisfy the equations

$$\sum_{j=1}^{n} B_{ij}\alpha_j = 0, \qquad 1 \leqslant i \leqslant n. \tag{6.6}$$

When $n = 2$, it is suggestive to write (6.6) in the form

$$\begin{bmatrix} T - A_{11}I & -A_{21}I \\ -A_{12}I & T - A_{22}I \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

In this case, the classical adjoint, $\operatorname{adj} B$ is the matrix

$$\tilde{B} = \begin{bmatrix} T - A_{22}I & A_{21}I \\ A_{12}I & T - A_{11}I \end{bmatrix}$$

and

$$\tilde{B}B = \begin{bmatrix} \det B & 0 \\ 0 & \det B \end{bmatrix}.$$

Hence, we have

$$\begin{aligned} (\det B)\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} &= \left(\tilde{B}B\right)\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} \\ &= \tilde{B}\left(B\begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix}\right) \\ &= \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \end{aligned}$$

In the general case, let $\tilde{B} = \operatorname{adj} B$. Then by (6.6)

$$\sum_{j=1}^{n} \tilde{B}_{ki} B_{ij} \alpha_j = 0$$

for each pair k, i, and summing on i, we have

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \sum_{j=1}^{n} \tilde{B}_{ki} B_{ij} \alpha_j \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \tilde{B}_{ki} B_{ij} \right) \alpha_j. \end{aligned}$$

Now $\tilde{B}B = (\det B)\, I$, so that

$$\sum_{i=1}^{n} \tilde{B}_{ki} B_{ij} = \delta_{kj} \det B.$$

Therefore

$$\begin{aligned} 0 &= \sum_{j=1}^{n} \delta_{kj} (\det B)\, \alpha_j \\ &= (\det B)\, \alpha_k, \qquad 1 \leqslant k \leqslant n. \end{aligned}$$

□

The Cayley–Hamilton theorem is useful to us at this point primarily because it narrows down the search for the minimal polynomials of various operators. If we know the matrix A which represents T in some ordered basis, then we can compute the characteristic polynomial f. We know that the minimal polynomial p divides f and that the two polynomials have the same roots. There is no method for computing precisely the roots of a polynomial (unless its degree is small); however, if f factors

$$f = (x - c_1)^{d_1} \cdots (x - c_k)^{d_k}, \qquad c_1, \ldots, c_k \text{ distinct, } d_i \geqslant 1 \tag{6.7}$$

then

$$p = (x - c_1)^{r_1} \cdots (x - c_k)^{r_k}, \qquad 1 \leqslant r_j \leqslant d_j. \tag{6.8}$$

That is all we can say in general. If f is the polynomial (6.7) and has degree n, then for every polynomial p as in (6.8) we can find an $n \times n$ matrix which has f as its characteristic polynomial and p as its minimal polynomial. We shall not prove this now. But, we want to emphasize the fact that the knowledge that the characteristic polynomial has the form (6.7) tells us that the minimal polynomial has the form (6.8), and it tells us nothing else about p.

EXAMPLE 6.5. Let A be the 4×4 (rational) matrix

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

The powers of A are easy to compute:

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

$$A^3 = \begin{bmatrix} 0 & 4 & 0 & 4 \\ 4 & 0 & 4 & 0 \\ 0 & 4 & 0 & 4 \\ 4 & 0 & 4 & 0 \end{bmatrix}.$$

Thus $A^3 = 4A$, i.e., if $p = x^3 - 4x = x(x+2)(x-2)$, then $p(A) = 0$. The minimal polynomial for A must divide p. That minimal polynomial is obviously not of degree 1, since that would mean that A was a scalar multiple of the identity. Hence, the candidates for the minimal polynomial are: p, $x(x+2)$, $x(x-2)$, $x^2 - 4$. The three quadratic polynomials can be eliminated because it is obvious at a glance that $A^2 \neq -2A$, $A^2 \neq 2A$, $A^2 \neq 4I$. Therefore p is the minimal polynomial for A. In particular 0, 2, and -2 are the characteristic values of A. One of the factors x, $x-2$, $x+2$ must be repeated twice in the characteristic polynomial. Evidently, $\operatorname{rank}(A) = 2$. Consequently there is a two-dimensional space of characteristic vectors associated with the characteristic value 0. From Theorem 6.2, it should now be clear that the characteristic polynomial is $x^2(x^2-4)$ and that A is similar over the field of rational numbers to the matrix

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & -2 \end{bmatrix}. \tag{6.9}$$

Exercises.

(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)

Index