Chapter 4
Linear Transformations of a Vector Space to Itself

4.1 Eigenvectors and Invariant Subspaces

In the previous chapter we introduced the notion of a linear transformation of a vector space L into a vector space M. In this and the following chapters, we shall consider the important special case in which M coincides with L, which in this book will always be assumed to be finite-dimensional. Then a linear transformation $\mathcal{A}: \mathsf{L} \to \mathsf{L}$ will be called a linear transformation of the space *L to itself*, or simply a linear transformation of the space L. This case is of great importance, since it is encountered frequently in various fields of mathematics, mechanics, and physics. We now recall some previously introduced facts regarding this case. First of all, as before, we shall understand the term *number* or *scalar* in the broadest possible sense, namely as a real or complex number or indeed as an element of any field $\mathbb{K}$ (of the reader's choosing).

As established in the preceding chapter, to represent a transformation $\mathcal{A}$ by a matrix, one has to choose a basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ of the space L and then to write the coordinates of the vectors $\mathcal{A}(\boldsymbol{e}_1), \dots, \mathcal{A}(\boldsymbol{e}_n)$ in terms of that basis as the columns of a matrix. The result will be a square matrix A of order n. If the transformation $\mathcal{A}$ of the space L is nonsingular, then the vectors $\mathcal{A}(\boldsymbol{e}_1), \dots, \mathcal{A}(\boldsymbol{e}_n)$ themselves form a basis of the space L, and we may interpret A as a transition matrix from the basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ to the basis $\mathcal{A}(\boldsymbol{e}_1), \dots, \mathcal{A}(\boldsymbol{e}_n)$. A nonsingular transformation $\mathcal{A}$ obviously has an inverse, $\mathcal{A}^{-1}$, with matrix A^{-1}.

Example 4.1 Let us write down the matrix of the linear transformation $\mathcal{A}$ that acts by rotating the plane in the counterclockwise direction about the origin through the angle α. To do so, we first choose a basis consisting of two mutually perpendicular vectors $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$ of unit length in the plane, where the vector $\boldsymbol{e}_2$ is obtained from $\boldsymbol{e}_1$ by a counterclockwise rotation through a right angle (see Fig. 4.1).

Then it is easy to see that we obtain the relationship

$$\mathcal{A}(\boldsymbol{e}_1) = \cos\alpha\,\boldsymbol{e}_1 + \sin\alpha\,\boldsymbol{e}_2, \qquad \mathcal{A}(\boldsymbol{e}_2) = -\sin\alpha\,\boldsymbol{e}_1 + \cos\alpha\,\boldsymbol{e}_2,$$

I.R. Shafarevich, A.O. Remizov, *Linear Algebra and Geometry*,
DOI 10.1007/978-3-642-30994-6_4, © Springer-Verlag Berlin Heidelberg 2013

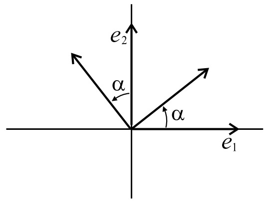

Fig. 4.1 Rotation through the angle α

and it follows from the definition that the matrix of the transformation $\mathcal{A}$ in the given basis is equal to

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}. \tag{4.1}$$

Example 4.2 Consider the linear transformation $\mathcal{A}$ of the complex plane that consists in multiplying each number $z \in \mathbb{C}$ by a given fixed complex number $p + iq$ (here i is the imaginary unit).

If we consider the complex plane as a vector space L over the field $\mathbb{C}$, then it is clear that in an arbitrary basis of the space L, such a transformation $\mathcal{A}$ has a matrix of order 1, consisting of a unique element, namely the given complex number $p + iq$. Thus in this case, we have $\dim \mathsf{L} = 1$, and we need to choose in L a basis consisting of an arbitrary nonzero vector in L, that is, an arbitrary complex number $z \neq 0$. Thus we obtain $\mathcal{A}(z) = (p + iq)z$.

Now let us consider the complex plane as a vector space L over the field $\mathbb{R}$. In this case, $\dim \mathsf{L} = 2$, since every complex number $z = x + iy$ is represented by a pair of real numbers x and y. Let us choose in L the same basis as in Example 4.1. Now we choose the vector $\boldsymbol{e}_1$ lying on the real axis, and the vector $\boldsymbol{e}_2$ on the imaginary axis. From the equation

$$(x + iy)(p + iq) = (px - qy) + i(py + qx)$$

it follows that

$$\mathcal{A}(\boldsymbol{e}_1) = p\boldsymbol{e}_1 + q\boldsymbol{e}_2, \qquad \mathcal{A}(\boldsymbol{e}_2) = -q\boldsymbol{e}_1 + p\boldsymbol{e}_2,$$

from which it follows by definition that the matrix of the transformation $\mathcal{A}$ in the given basis takes the form

$$A = \begin{pmatrix} p & -q \\ q & p \end{pmatrix}. \tag{4.2}$$

In the case $|p + iq| = 1$, we may put $p = \cos\alpha$ and $q = \sin\alpha$ for a certain number $0 \leq \alpha < 2\pi$ (such an α is called the *argument* of the complex number $p + iq$). Then the matrix (4.2) coincides with (4.1); that is, multiplication by a complex number with modulus 1 and argument α is equivalent to the counterclockwise rotation about the origin of the complex plane through the angle α. We note that every complex number $p + iq$ can be expressed as the product of a real number r and a complex number of modulus 1; that is, $p + iq = r(p' + iq')$, where $|p' + iq'| = 1$ and $r = |p + iq|$. From this it is clear that multiplication by $p + iq$ is the product of two linear transformations of the complex plane: a rotation through the angle α and a dilation (or contraction) by the factor r.

In Sect. 3.4, we established that in the transition from a basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ of the space L to some other basis $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$, the matrix of the transformation is changed according to the formula

$$A' = C^{-1} A C, \tag{4.3}$$

where C is the transition matrix from the second basis to the first.

Definition 4.3 Two square matrices A and A' related by (4.3), where C is any nonsingular matrix, are said to be *similar*.

It is not difficult to see that in the set of square matrices of a given order, the similarity relation thus defined is an equivalence relation (see the definition on p. xii).

It follows from formula (4.3) that in changing bases, the determinant of the transformation matrix does not change, and therefore it is possible to speak not simply about the determinant of the transformation matrix, but about the determinant of the *linear transformation* $\mathcal{A}$ itself, which will be denoted by $|\mathcal{A}|$. A linear transformation $\mathcal{A} : \mathsf{L} \to \mathsf{L}$ is nonsingular if and only if $|\mathcal{A}| \neq 0$. If L is a real space, then this number $|\mathcal{A}| \neq 0$ is also real and can be either positive or negative.

Definition 4.4 A nonsingular linear transformation $\mathcal{A} : \mathsf{L} \to \mathsf{L}$ of the real space L is called *proper* if $|\mathcal{A}| > 0$, and *improper* if $|\mathcal{A}| < 0$.

One of the basic tasks in the theory of linear transformations, one with which we shall be occupied in the sequel, is to find, given a linear transformation of a vector space into itself, a basis for which the matrix of the transformation takes the simplest possible form. An equivalent formulation of this task is for a given square matrix to find the simplest matrix that is similar to it. Having such a basis (or similar matrix) gives us the possibility of surveying a number of important properties of the initial linear transformation (or matrix). In its most general form, this problem will be solved in Chap. 5, but at present, we shall examine it for a particular type of linear transformation that is most frequently encountered.

Definition 4.5 A subspace L' of a vector space L is called *invariant* with respect to the linear transformation $\mathcal{A} : \mathsf{L} \to \mathsf{L}$ if for every vector $\boldsymbol{x} \in \mathsf{L}'$, we have $\mathcal{A}(\boldsymbol{x}) \in \mathsf{L}'$.

It is clear that according to this definition, the zero subspace $(\mathbf{0})$ and the entire space L are invariant with respect to any linear transformation $\mathcal{A} : \mathsf{L} \to \mathsf{L}$. Thus whenever we enumerate the invariant subspaces of a space L, we shall always mean the subspaces $\mathsf{L}' \subset \mathsf{L}$ other than $(\mathbf{0})$ and L.

Example 4.6 Let L be the three-dimensional space studied in courses in analytic geometry consisting of vectors originating at a given fixed point O, and consider the transformation $\mathcal{A}$ that reflects each vector with respect to a given plane L' passing through the point O. It is then easy to see that $\mathcal{A}$ has two invariant subspaces: the plane L' itself and the straight line L'' passing through O and perpendicular to L'.

Example 4.7 Let L be the same space as in the previous example, and now let the transformation $\mathcal{A}$ be a rotation through the angle α, $0 < \alpha < \pi$, about a given axis L' passing through O. Then $\mathcal{A}$ has two invariant subspaces: the line L' itself and the plane L'' perpendicular to L' and passing through O.

Example 4.8 Let L be the same as in the previous example, and let $\mathcal{A}$ be a homothety, that is, $\mathcal{A}$ acts by multiplying each vector by a fixed number $\alpha \neq 0$. Then it is easy to see that every line and every plane passing through O is an invariant subspace with respect to the transformation $\mathcal{A}$. Moreover, it is not difficult to observe that if $\mathcal{A}$ is a homothety on an arbitrary vector space L, then every subspace of L is invariant.

Example 4.9 Let L be the plane consisting of all vectors originating at some point O, and let $\mathcal{A}$ be the transformation that rotates a vector about O through the angle α, $0 < \alpha < \pi$. Then $\mathcal{A}$ has no invariant subspace.

It is evident that the restriction of a linear transformation $\mathcal{A}$ to an invariant subspace $\mathsf{L}' \subset \mathsf{L}$ is a linear transformation of L' into itself. We shall denote this transformation by $\mathcal{A}'$, that is, $\mathcal{A}' : \mathsf{L}' \to \mathsf{L}'$ and $\mathcal{A}'(\boldsymbol{x}) = \mathcal{A}(\boldsymbol{x})$ for all $\boldsymbol{x} \in \mathsf{L}'$.

Let $\boldsymbol{e}_1, \dots, \boldsymbol{e}_m$ be a basis of the subspace L'. Then since it consists of linearly independent vectors, it is possible to extend it to a basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ of the entire space L. Let us examine how the matrix of the linear transformation $\mathcal{A}$ appears in this basis. The vectors $\mathcal{A}(\boldsymbol{e}_1), \dots, \mathcal{A}(\boldsymbol{e}_m)$ are expressed as a linear combination of $\boldsymbol{e}_1, \dots, \boldsymbol{e}_m$; this is equivalent to saying that $\boldsymbol{e}_1, \dots, \boldsymbol{e}_m$ is the basis of a subspace that is invariant with respect to the transformation $\mathcal{A}$. We therefore obtain the system of equations

$$\begin{cases} \mathcal{A}(\boldsymbol{e}_1) = a_{11}\boldsymbol{e}_1 + a_{21}\boldsymbol{e}_2 + \dots + a_{m1}\boldsymbol{e}_m, \\ \mathcal{A}(\boldsymbol{e}_2) = a_{12}\boldsymbol{e}_1 + a_{22}\boldsymbol{e}_2 + \dots + a_{m2}\boldsymbol{e}_m, \\ \vdots \\ \mathcal{A}(\boldsymbol{e}_m) = a_{1m}\boldsymbol{e}_1 + a_{2m}\boldsymbol{e}_2 + \dots + a_{mm}\boldsymbol{e}_m. \end{cases}$$

It is clear that the matrix

$$A' = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} \tag{4.4}$$

is the matrix of the linear transformation $\mathcal{A}' : \mathsf{L}' \to \mathsf{L}'$ in the basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_m$. In general, we can say nothing about the vectors $\mathcal{A}(\boldsymbol{e}_i)$ for $i > m$ except that they are linear combinations of vectors from the basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ of the entire space L. However, we shall represent this by separating out terms that are multiples of $\boldsymbol{e}_1, \dots, \boldsymbol{e}_m$ (we shall write the associated coefficients as b_{ij}) and those that are multiples of the vectors $\boldsymbol{e}_{m+1}, \dots, \boldsymbol{e}_n$ (here we shall write the associated coefficients as c_{ij}). As a result we obtain the matrix

$$A = \begin{pmatrix} A' & B' \\ 0 & C' \end{pmatrix}, \tag{4.5}$$

where B' is a matrix of type $(m, n-m)$, C' is a square matrix of order $n-m$, and 0 is a matrix of type $(n-m, m)$ all of whose elements are equal to zero.

If it turns out to be possible to find an invariant subspace L'' related to the invariant subspace L' by $\mathsf{L} = \mathsf{L}' \oplus \mathsf{L}''$, then by joining the bases of L' and L'', we obtain a basis for the space L in which the matrix of our linear transformation $\mathcal{A}$ can be written in the form

$$A = \begin{pmatrix} A' & 0 \\ 0 & C' \end{pmatrix},$$

where A' is the matrix (4.4) and C' is the matrix of the linear transformation obtained by restricting the transformation $\mathcal{A}$ to the subspace L''. Analogously, if

$$\mathsf{L} = \mathsf{L}_1 \oplus \mathsf{L}_2 \oplus \cdots \oplus \mathsf{L}_k,$$

where all the L_i are invariant subspaces with respect to the transformation $\mathcal{A}$, then the matrix of the transformation $\mathcal{A}$ can be written in the form

$$A = \begin{pmatrix} A'_1 & 0 & \cdots & 0 \\ 0 & A'_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A'_k \end{pmatrix}, \tag{4.6}$$

where A'_i is the matrix of the linear transformation obtained by restricting $\mathcal{A}$ to the invariant subspace L_i. Matrices of the form (4.6) are called *block-diagonal*.

The simplest case is that of an invariant subspace of dimension 1. This subspace has a basis consisting of a single vector $\boldsymbol{e} \neq \mathbf{0}$, and its invariance is expressed by the relationship

$$\mathcal{A}(\boldsymbol{e}) = \lambda \boldsymbol{e} \tag{4.7}$$

for some number λ.

Definition 4.10 If the relationship (4.7) is satisfied for a vector $\boldsymbol{e} \neq \mathbf{0}$, then $\boldsymbol{e}$ is called an *eigenvector*, and the number λ is called an *eigenvalue* of the transformation $\mathcal{A}$.

Given an eigenvalue λ, it is easy to verify that the set of all vectors $\boldsymbol{e} \in \mathsf{L}$ satisfying the relationship (4.7), including here also the zero vector, forms an invariant subspace of L. It is called the *eigensubspace* for the eigenvalue λ and is denoted by L_λ.

Example 4.11 In Example 4.6, the eigenvectors of the transformation $\mathcal{A}$ are, first of all, all the vectors in the plane L' (in this case the eigenvalue is $\lambda = 1$), and secondly, every vector on the line L'' (the eigenvalue is $\lambda = -1$). In Example 4.7, the eigenvectors are all vectors lying on the line L', and to them correspond the eigenvalue $\lambda = 1$. In Example 4.8, every vector in the space is an eigenvector with eigenvalue $\lambda = \alpha$. Of course all the vectors that we are speaking about are nonzero vectors.

Example 4.12 Let L be the space consisting of all infinitely differentiable functions, and let the transformation $\mathcal{A}$ be differentiation, that is, it maps every function $x(t)$ in L to its derivative $x'(t)$. Then the eigenvectors of $\mathcal{A}$ are the functions $x(t)$, not identically zero, that are solutions of the differential equation $x'(t) = \lambda x(t)$. One easily verifies that such solutions are the functions $x(t) = ce^{\lambda t}$, where c is an arbitrary constant. It follows that to every number λ there corresponds a one-dimensional invariant subspace of the transformation $\mathcal{A}$ consisting of all vectors $x(t) = ce^{\lambda t}$, and for $c \neq 0$ these are eigenvectors.

There is a convenient method for finding eigenvalues of a transformation $\mathcal{A}$ and the associated subspaces. We must first choose an arbitrary basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ of the space L and then search for vectors $\boldsymbol{e}$ that satisfy relation (4.7), in the form of the linear combination

$$\boldsymbol{e} = x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 + \cdots + x_n\boldsymbol{e}_n. \tag{4.8}$$

Let the matrix of the linear transformation $\mathcal{A}$ in the basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ be $A = (a_{ij})$. Then the coordinates of the vector $\mathcal{A}(\boldsymbol{e})$ in the same basis can be expressed by the equations

$$\begin{cases} y_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n, \\ y_2 = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n, \\ \vdots \\ y_n = a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n. \end{cases}$$

Now we can write down relation (4.7) in the form

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = \lambda x_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = \lambda x_2, \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = \lambda x_n, \end{cases}$$

or equivalently,

$$\begin{cases} (a_{11}-\lambda)x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0, \\ a_{21}x_1 + (a_{22}-\lambda)x_2 + \cdots + a_{2n}x_n = 0, \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + (a_{nn}-\lambda)x_n = 0. \end{cases} \tag{4.9}$$

For the coordinates $x_1, x_2, \ldots, x_n$ of the vector (4.8), we obtain a system of n homogeneous linear equations. By Corollary 2.13, this system will have a nonzero solution if and only if the determinant of its matrix is equal to zero. We may write this condition in the form

$$|A - \lambda E| = 0.$$

Using the formula for the expansion of the determinant, we see that the determinant $|A - tE|$ is a polynomial in t of degree n. It is called the *characteristic polynomial* of the transformation $\mathcal{A}$. The eigenvalues of $\mathcal{A}$ are precisely the zeros of this polynomial.

Let us prove that the characteristic polynomial is independent of the basis in which we write down the matrix of the transformation. It is only after we have accomplished this that we shall have the right to speak of the characteristic polynomial of the transformation itself and not merely of its matrix in a particular basis.

Indeed, as we have seen (formula (4.3)), in another basis we obtain the matrix $A' = C^{-1}AC$, where $|C| \neq 0$. For this matrix, the characteristic polynomial is

$$\left|A' - tE\right| = \left|C^{-1}AC - tE\right| = \left|C^{-1}(A - tE)C\right|.$$

Using the formula for the multiplication of determinants and the formula for the determinant of an inverse matrix, we obtain

$$\left|C^{-1}(A - tE)C\right| = \left|C^{-1}\right| \cdot |A - tE| \cdot |C| = |A - tE|.$$

If a space has a basis $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ consisting of eigenvectors, then in this basis, we have $\mathcal{A}(\boldsymbol{e}_i) = \lambda_i \boldsymbol{e}_i$. From this, it follows that the matrix of a transformation $\mathcal{A}$ in this basis has the *diagonal form*

$$\begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}.$$

This is a special case of (4.6) in which the invariant subspaces L_i are one-dimensional, that is, $\mathsf{L}_i = \langle \boldsymbol{e}_i \rangle$. Such linear transformations are called *diagonalizable*.

As the following example shows, not all transformations are diagonalizable.

Example 4.13 Let $\mathcal{A}$ be a linear transformation of the (real or complex) plane that in some basis $\boldsymbol{e}_1, \boldsymbol{e}_2$ has the matrix

$$A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, \quad b \neq 0.$$

The characteristic polynomial $|A - tE| = (t - a)^2$ of this transformation has a unique zero $t = a$, of multiplicity 2, to which corresponds the one-dimensional eigensubspace $\langle \boldsymbol{e}_1 \rangle$. From this it follows that the transformation $\mathcal{A}$ is nondiagonalizable.

This can be proved by another method, using the concept of similar matrices. If the transformation $\mathcal{A}$ were diagonalizable, then there would exist a nonsingular matrix C of order 2 that would satisfy the relation $C^{-1}AC = aE$, or equivalently, the equation $AC = aC$. With respect to the unknown elements of the matrix $C = (c_{ij})$, the previous equality gives us two equations, $bc_{21} = 0$ and $bc_{22} = 0$, whence by virtue of $b \neq 0$, it follows that $c_{21} = c_{22} = 0$, and the matrix C is thus seen to be singular.

We have seen that the number of eigenvalues of a linear transformation is finite, and it cannot exceed the number n (the dimension of the space L), since they are the zeros of the characteristic polynomial, whose degree is n.

Theorem 4.14 *The dimension of the eigensubspace $\mathsf{L}_\lambda \subset \mathsf{L}$ associated with the eigenvalue λ is at most the multiplicity of the value λ as a zero of the characteristic polynomial.*

Proof Suppose the dimension of the eigensubspace L_λ is m. Let us choose a basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_m$ of this subspace and extend it to a basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ of the entire space L, in which the matrix of the transformation $\mathcal{A}$ has the form (4.5). Since by the definition of an eigensubspace, $\mathcal{A}(\boldsymbol{e}_i) = \lambda \boldsymbol{e}_i$ for all $i = 1, \dots, m$, it follows that in (4.5), the matrix A' is equal to λE_m, where E_m is the identity matrix of order m. Then

$$A - tE = \begin{pmatrix} A' - tE_m & B' \\ 0 & C' - tE_{n-m} \end{pmatrix} = \begin{pmatrix} (\lambda - t)E_m & B' \\ 0 & C' - tE_{n-m} \end{pmatrix},$$

where E_{n-m} is the identity matrix of order $n - m$. Therefore,

$$|A - tE| = (\lambda - t)^m \left| C' - tE_{n-m} \right|.$$

On the other hand, if $\mathsf{L} = \mathsf{L}_\lambda \oplus \mathsf{L}''$, then $\mathsf{L}_\lambda \cap \mathsf{L}'' = (\mathbf{0})$, which means that the restriction of the transformation $\mathcal{A}$ to L'' has no eigenvectors with eigenvalue λ. This means that $|C' - \lambda E_{n-m}| \neq 0$, that is, the number λ is not a zero of the polynomial $|C' - tE_{n-m}|$, which is what we had to show. □

In the previous chapter we were introduced to the operations of addition and multiplication (composition) of linear transformations, which are clearly defined for the special case of a transformation of a space L into itself. Therefore, for any integer $n > 0$ we may define the nth *power* of a linear transformation. By definition, $\mathcal{A}^n$ for $n > 0$ is the result of multiplying $\mathcal{A}$ by itself n times, and for $n = 0$, $\mathcal{A}^0$ is the identity transformation $\mathcal{E}$. This enables us to introduce the concept of a *polynomial in a linear transformation*, which will play an important role in what follows.

Let $\mathcal{A}$ be a linear transformation of the vector space L (real, complex, or over an arbitrary field $\mathbb{K}$) and define

$$f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_k x^k,$$

a polynomial with scalar coefficients (respectively real, complex, or from the field $\mathbb{K}$).

Definition 4.15 A *polynomial f in the linear transformation* $\mathcal{A}$ is a linear mapping

$$f(\mathcal{A}) = \alpha_0 \mathcal{E} + \alpha_1 \mathcal{A} + \cdots + \alpha_k \mathcal{A}^k, \tag{4.10}$$

where $\mathcal{E}$ is the identity linear transformation.

We observe that this definition does not make use of coordinates, that is, the choice of a specific basis in the space L. If such a basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ is chosen, then to the linear transformation $\mathcal{A}$ there corresponds a unique square matrix A. In Sect. 2.9 we introduced the notion of a polynomial in a square matrix, which allows us to give another definition: $f(\mathcal{A})$ is the linear transformation with matrix

$$f(A) = \alpha_0 E + \alpha_1 A + \cdots + \alpha_k A^k \tag{4.11}$$

in the basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$.

It is not difficult to be convinced of the equivalence of these definitions if we recall that the actions of linear transformations are expressed through the actions of their matrices (see Sect. 3.3). It is thus necessary to show that in a change of basis from $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$, the matrix $f(A)$ also changes according to formula (4.3) with transition matrix C the same as for matrix A. Indeed, let us consider a change of coordinates (that is, switching to another basis of the space L) with matrix C. Then in the new basis, the matrix of the transformation $\mathcal{A}$ is given by $A' = C^{-1}AC$. By the associativity of matrix multiplication, we also obtain a relationship $A'^n = C^{-1}A^nC$ for every integer $n \geq 0$. If we substitute A' for A in formula (4.11), then considering what we have said, we obtain

$$\begin{aligned} f\bigl(A'\bigr) &= \alpha_0 E + \alpha_1 A' + \cdots + \alpha_k A'^k \\ &= C^{-1}\bigl(\alpha_0 E + \alpha_1 A + \cdots + \alpha_k A^k\bigr)C = C^{-1} f(A) C, \end{aligned}$$

which proves our assertion.

It should be clear that the statements that we proved in Sect. 2.9 for polynomials in a matrix (p. 69) also apply to polynomials in a linear transformation.

Lemma 4.16 *If* $f(x) + g(x) = u(x)$ *and* $f(x)g(x) = v(x)$, *then for an arbitrary linear transformation* $\mathcal{A}$, *we have*

$$f(\mathcal{A}) + g(\mathcal{A}) = u(\mathcal{A}), \tag{4.12}$$

$$f(\mathcal{A})g(\mathcal{A}) = v(\mathcal{A}). \tag{4.13}$$

Corollary 4.17 *Polynomials* $f(\mathcal{A})$ *and* $g(\mathcal{A})$ *in the same linear transformation* $\mathcal{A}$ *commute*: $f(\mathcal{A})g(\mathcal{A}) = g(\mathcal{A})f(\mathcal{A})$.

4.2 Complex and Real Vector Spaces

We shall now investigate in greater detail the concepts introduced in the previous section applied to transformations of complex and real vector spaces (that is, we shall assume that the field $\mathbb{K}$ is respectively $\mathbb{C}$ or $\mathbb{R}$). Our fundamental result applies specifically to complex spaces.

Theorem 4.18 *Every linear transformation of a complex vector space has an eigenvector.*

This follows immediately from the fact that the characteristic polynomial of a linear transformation, and in general an arbitrary polynomial of positive degree, has a complex root. Nevertheless, as Example 4.13 of the previous section shows, even in a complex space, not every linear transformation is diagonalizable.

Let us consider the question of diagonalizability in greater detail, always assuming that we are working with complex spaces. We shall prove the diagonalizability of a commonly occurring type of transformation. To this end, we require the following lemma.

Lemma 4.19 *Eigenvectors associated with distinct eigenvalues are linearly independent.*

Proof Suppose the eigenvectors $\boldsymbol{e}_1, \dots, \boldsymbol{e}_m$ are associated with distinct eigenvalues $\lambda_1, \dots, \lambda_m$,

$$\mathcal{A}(\boldsymbol{e}_i) = \lambda_i \boldsymbol{e}_i, \quad i = 1, \dots, m.$$

We shall prove the lemma by induction on the number m of vectors. For the case $m = 1$, the result follows from the definition of an eigenvector, namely that $\boldsymbol{e}_1 \neq \boldsymbol{0}$.

Let us assume that there exists a linear dependence

$$\alpha_1 \boldsymbol{e}_1 + \alpha_2 \boldsymbol{e}_2 + \cdots + \alpha_m \boldsymbol{e}_m = \boldsymbol{0}. \tag{4.14}$$

Applying the transformation $\mathcal{A}$ to both sides of the equation, we obtain

$$\lambda_1 \alpha_1 \boldsymbol{e}_1 + \lambda_2 \alpha_2 \boldsymbol{e}_2 + \cdots + \lambda_m \alpha_m \boldsymbol{e}_m = \boldsymbol{0}. \tag{4.15}$$

Subtracting (4.14) multiplied by λ_m from (4.15), we obtain

$$\alpha_1(\lambda_1 - \lambda_m)\boldsymbol{e}_1 + \alpha_2(\lambda_2 - \lambda_m)\boldsymbol{e}_2 + \cdots + \alpha_{m-1}(\lambda_{m-1} - \lambda_m)\boldsymbol{e}_{m-1} = \mathbf{0}.$$

By our induction hypothesis, we may consider that the lemma has been proved for $m-1$ vectors $\boldsymbol{e}_1, \dots, \boldsymbol{e}_{m-1}$. Thus we obtain that $\alpha_1(\lambda_1 - \lambda_m) = 0, \dots, \alpha_{m-1}(\lambda_{m-1} - \lambda_m) = 0$, and since by the condition in the lemma, $\lambda_1 \neq \lambda_m, \dots, \lambda_{m-1} \neq \lambda_m$, it follows that $\alpha_1 = \cdots = \alpha_{m-1} = 0$. Substituting this into (4.14), we arrive at the relationship $\alpha_m \boldsymbol{e}_m = \mathbf{0}$, that is (by the definition of an eigenvector), $\alpha_m = 0$. Therefore, in (4.14), all the α_i are equal to zero, which demonstrates the linear independence of $\boldsymbol{e}_1, \dots, \boldsymbol{e}_m$. □

By Lemma 4.19, we have the following result.

Theorem 4.20 *A linear transformation on a complex vector space is diagonalizable if its characteristic polynomial has no multiple roots.*

As is well known, in this case, the characteristic polynomial has n distinct roots (we recall once again that we are speaking about polynomials over the field of complex numbers).

Proof of Theorem 4.20 Let $\lambda_1, \dots, \lambda_n$ be the distinct roots of the characteristic polynomial of the transformation $\mathcal{A}$ and let $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ be the corresponding eigenvectors. It suffices to show that these vectors form a basis of the entire space. Since their number is equal to the dimension of the space, this is equivalent to showing their linear independence, which follows from Lemma 4.19. □

If A is the matrix of the transformation $\mathcal{A}$ in some basis, then the condition of Theorem 4.20 is satisfied if and only if the so-called *discriminant* of the characteristic polynomial is nonzero.[1] For example, if the order of a matrix A is 2, and

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then

$$|A - tE| = \begin{vmatrix} a-t & b \\ c & d-t \end{vmatrix} = (a-t)(d-t) - bc = t^2 - (a+d)t + ad - bc.$$

The condition that this quadratic trinomial have two distinct roots is that $(a+d)^2 - 4(ad - bc) \neq 0$. This can be rewritten in the form

$$(a-d)^2 + 4bc \neq 0. \tag{4.16}$$

[1]For the general notion of the discriminant of a polynomial, see, for instance, *Polynomials*, by Victor V. Prasolov, Springer 2004.

Similarly, for complex vector spaces of arbitrary dimension, linear transformations not satisfying the conditions of Theorem 4.20 have a matrix that regardless of the basis, has elements that satisfy a special algebraic relationship. In this sense, only exceptional transformations do not meet the conditions of Theorem 4.20.

Analogous considerations give necessary and sufficient conditions for a linear transformation to be diagonalizable.

Theorem 4.21 *A linear transformation of a complex vector space is diagonalizable if and only if for each of its eigenvalues λ, the dimension of the corresponding eigenspace L_λ is equal to the multiplicity of λ as a root of the characteristic polynomial.*

In other words, the bound on the dimension of the subspace L_λ obtained in Theorem 4.14 is attained.

Proof of Theorem 4.21 Let the transformation $\mathcal{A}$ be diagonalizable, that is, in some basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ it has the matrix

$$A = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}.$$

It is possible to arrange the eigenvalues $\lambda_1, \dots, \lambda_n$ so that those that are equal are next to each other, so that altogether, they have the form

$$\underbrace{\lambda_1, \dots, \lambda_1}_{m_1 \text{ times}}, \underbrace{\lambda_2, \dots, \lambda_2}_{m_2 \text{ times}}, \dots\dots\dots, \underbrace{\lambda_k, \dots, \lambda_k}_{m_k \text{ times}},$$

where all the numbers $\lambda_1, \dots, \lambda_k$ are distinct. In other words, we can write the matrix A in the block-diagonal form

$$A = \begin{pmatrix} \lambda_1 E_{m_1} & 0 & \cdots & 0 \\ 0 & \lambda_2 E_{m_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_k E_{m_k} \end{pmatrix}, \tag{4.17}$$

where E_{m_i} is the identity matrix of order m_i. Then

$$|A - tE| = (\lambda_1 - t)^{m_1} (\lambda_2 - t)^{m_2} \cdots (\lambda_k - t)^{m_k},$$

that is, the number λ_i is a root of multiplicity m_i of the characteristic equation. On the other hand, the equality $\mathcal{A}(\boldsymbol{x}) = \lambda_i \boldsymbol{x}$ for vectors $\boldsymbol{x} = \alpha_1 \boldsymbol{e}_1 + \cdots + \alpha_n \boldsymbol{e}_n$ gives the relationship $\lambda_s \alpha_j = \lambda_i \alpha_j$ for all $j = 1, \dots, n$ and $s = 1, \dots, k$, that is, either $\alpha_j = 0$ or $\lambda_s = \lambda_i$. In other words, the vector $\boldsymbol{x}$ is a linear combination only of those eigenvectors $\boldsymbol{e}_j$ that correspond to the eigenvalue λ_i. This means that the subspace L_{λ_i} consists of all linear combinations of such vectors, and consequently, $\dim \mathsf{L}_{\lambda_i} = m_i$.

Conversely, for distinct eigenvalues $\lambda_1, \dots, \lambda_k$, let the dimension of the eigensubspace L_{λ_i} be equal to the multiplicity m_i of the number λ_i as a root of the characteristic polynomial. Then from known properties of polynomials, it follows that $m_1 + \cdots + m_k = n$, which means that

$$\dim \mathsf{L}_{\lambda_1} + \cdots + \dim \mathsf{L}_{\lambda_k} = \dim \mathsf{L}. \tag{4.18}$$

We shall show that the sum $\mathsf{L}_{\lambda_1} + \cdots + \mathsf{L}_{\lambda_k}$ is a direct sum of its eigensubspaces L_{λ_i}. To do so, it suffices to show that for all vectors $\boldsymbol{x}_1 \in \mathsf{L}_{\lambda_1}, \dots, \boldsymbol{x}_k \in \mathsf{L}_{\lambda_k}$, the equality $\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_k = \boldsymbol{0}$ is possible only in the case that $\boldsymbol{x}_1 = \cdots = \boldsymbol{x}_k = \boldsymbol{0}$. But since $\boldsymbol{x}_1, \dots, \boldsymbol{x}_k$ are eigenvectors of the transformation $\mathcal{A}$ corresponding to distinct eigenvalues $\lambda_1, \dots, \lambda_k$, the required assertion follows by Lemma 4.19. Therefore, by equality (4.18), we have the decomposition

$$\mathsf{L} = \mathsf{L}_{\lambda_1} \oplus \cdots \oplus \mathsf{L}_{\lambda_k}.$$

Having chosen from each eigensubspace L_{λ_i}, $i = 1, \dots, k$, a basis (consisting of m_i vectors), and having ordered them in such a way that the vectors entering into a particular subspace L_{λ_i} are adjacent, we obtain a basis of the space L in which the matrix A of the transformation $\mathcal{A}$ has the form (4.17). This means that the transformation $\mathcal{A}$ is diagonalizable. □

The case of real vector spaces is more frequently encountered in applications. Their study proceeds in almost the same way as with complex vector spaces, except that the results are somewhat more complicated. We shall introduce here a proof of the real analogue of Theorem 4.18.

Theorem 4.22 *Every linear transformation of a real vector space of dimension $n > 2$ has either a one-dimensional or two-dimensional invariant subspace.*

Proof Let $\mathcal{A}$ be a linear transformation of a real vector space L of dimension $n > 2$, and let $\boldsymbol{x} \in \mathsf{L}$ be some nonnull vector. Since the collection $\boldsymbol{x}, \mathcal{A}(\boldsymbol{x}), \mathcal{A}^2(\boldsymbol{x}), \dots, \mathcal{A}^n(\boldsymbol{x})$ consists of $n + 1 > \dim \mathsf{L}$ vectors, then by the definition of the dimension of a vector space, these vectors must be linearly dependent. This means that there exist real numbers $\alpha_0, \alpha_1, \dots, \alpha_n$, not all zero, such that

$$\alpha_0 \boldsymbol{x} + \alpha_1 FF(\boldsymbol{x}) + \alpha_2 \mathcal{A}^2(\boldsymbol{x}) + \cdots + \alpha_n \mathcal{A}^n(\boldsymbol{x}) = \boldsymbol{0}. \tag{4.19}$$

Consider the polynomial $P(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_n t^n$ and substitute for the variable t, the transformation $\mathcal{A}$, as was done in Sect. 4.1 (formula (4.10)). Then the equality (4.19) can be written in the form

$$P(\mathcal{A})(\boldsymbol{x}) = \boldsymbol{0}. \tag{4.20}$$

A polynomial $P(t)$ satisfying equality (4.20) is called an *annihilator polynomial* of the vector $\boldsymbol{x}$ (where it is implied that it is relative to the given transformation $\mathcal{A}$).

Let us assume that the annihilator polynomial $P(t)$ of some vector $\boldsymbol{x} \neq \mathbf{0}$ is the product of two polynomials of lower degree: $P(t) = Q_1(t)Q_2(t)$. Then by definition (4.20) and formula (4.13) from the previous section, we have $Q_1(\mathcal{A})Q_2(\mathcal{A})(\boldsymbol{x}) = \mathbf{0}$. Then either $Q_2(\mathcal{A})(\boldsymbol{x}) = \mathbf{0}$, and hence the vector $\boldsymbol{x}$ is annihilated by an annihilator polynomial $Q_2(t)$ of lower degree, or else $Q_2(\mathcal{A})(\boldsymbol{x}) \neq \mathbf{0}$. If we assume $\boldsymbol{y} = Q_2(\mathcal{A})(\boldsymbol{x})$, we obtain the equality $Q_1(\mathcal{A})(\boldsymbol{y}) = \mathbf{0}$, which means that the nonnull vector $\boldsymbol{y}$ is annihilated by the annihilator polynomial $Q_1(t)$ of lower degree. As is well known, an arbitrary polynomial with real coefficients is a product of polynomials of first and second degree. Applying to $P(t)$ as many times as necessary the process described above, we finally arrive at a polynomial $Q(t)$ of first or second degree and a nonnull vector $\boldsymbol{z}$ such that $Q(\mathcal{A})(\boldsymbol{z}) = \mathbf{0}$. This is the real analogue of Theorem 4.18.

Factoring out the coefficient of the high-order term of $Q(t)$, we may assume that this coefficient is equal to 1. If the degree of $Q(t)$ is equal to 1, then $Q(t) = t - \lambda$ for some λ, and the equality $Q(\mathcal{A})(\boldsymbol{z}) = \mathbf{0}$ yields $(\mathcal{A} - \lambda\mathcal{E})(\boldsymbol{z}) = \mathbf{0}$. This means that λ is an eigenvalue of $\boldsymbol{z}$, which is an eigenvector of the transformation $\mathcal{A}$, and therefore, $\langle \boldsymbol{z} \rangle$ is a one-dimensional invariant subspace of the transformation $\mathcal{A}$.

If the degree of $Q(t)$ is equal to 2, then $Q(t) = t^2 + pt + q$ and $(\mathcal{A}^2 + p\mathcal{A} + q\mathcal{E})(\boldsymbol{z}) = \mathbf{0}$. In this case, the subspace $\mathsf{L}' = \langle \boldsymbol{z}, \mathcal{A}(\boldsymbol{z}) \rangle$ is two-dimensional and is invariant with respect to $\mathcal{A}$. Indeed, the vectors $\boldsymbol{z}$ and $\mathcal{A}(\boldsymbol{z})$ are linearly independent, since otherwise, we would have the case of an eigenvector $\boldsymbol{z}$ considered above. This means that $\dim \mathsf{L}' = 2$. We shall show that L' is an invariant subspace of the transformation $\mathcal{A}$. Let $\boldsymbol{x} = \alpha\boldsymbol{z} + \beta\mathcal{A}(\boldsymbol{z})$. To show that $\mathcal{A}(\boldsymbol{x}) \in \mathsf{L}'$, it suffices to verify that vectors $\mathcal{A}(\boldsymbol{z})$ and $\mathcal{A}(\mathcal{A}(\boldsymbol{z}))$ belong to L'. This holds for the former by the definition of L'. It holds for the latter by the fact that $\mathcal{A}(\mathcal{A}(\boldsymbol{z})) = \mathcal{A}^2(\boldsymbol{z})$ and by the condition of the theorem, $\mathcal{A}^2(\boldsymbol{z}) + p\mathcal{A}(\boldsymbol{z}) + q\boldsymbol{z} = \mathbf{0}$, that is, $\mathcal{A}^2(\boldsymbol{z}) = -q\boldsymbol{z} - p\mathcal{A}(\boldsymbol{z})$. □

Let us discuss the concept of the annihilator polynomial that we encountered in the proof of Theorem 4.22. An annihilator polynomial of a vector $\boldsymbol{x} \neq \mathbf{0}$ having minimal degree is called a *minimal polynomial* of the vector $\boldsymbol{x}$.

Theorem 4.23 *Every annihilator polynomial is divisible by a minimal polynomial.*

Proof Let $P(t)$ be an annihilator polynomial of the vector $\boldsymbol{x} \neq \mathbf{0}$, and $Q(t)$ a minimal polynomial. Let us suppose that P is not divisible by Q. We divide P by Q with remainder. This gives the equality $P = UQ + R$, where U and R are polynomials in t, and moreover, R is not identically zero, and the degree of R is less than that of Q. If we substitute into this equality the transformation $\mathcal{A}$ for the variable t, then by formulas (4.12) and (4.13), we obtain that

$$P(\mathcal{A})(\boldsymbol{x}) = U(\mathcal{A})Q(\mathcal{A})(\boldsymbol{x}) + R(\mathcal{A})(\boldsymbol{x}), \tag{4.21}$$

and since P and Q are annihilator polynomials of the vector $\boldsymbol{x}$, it follows that $R(\mathcal{A})(\boldsymbol{x}) = \mathbf{0}$. Since the degree of R is less than that of Q, this contradicts the minimality of the polynomial Q. □

Corollary 4.24 *The minimal polynomial of a vector $\boldsymbol{x} \neq \mathbf{0}$ is uniquely defined up to a constant factor.*

Let us note that for the annihilator polynomial, Theorem 4.23 and its converse hold: any multiple of any annihilator polynomial is also an annihilator polynomial (of course, of the same vector $\boldsymbol{x}$). This follows from the fact that in this case, in equality (4.21), we have $R = 0$. From this follows the assertion that there exists a single polynomial that is an annihilator for all vectors of the space L. Indeed, let $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ be some basis of the space L, and let $P_1, \dots, P_n$ be annihilator polynomials for these vectors. Let us denote by Q the least common multiple of these polynomials. Then from what we have said above, it follows that Q is an annihilator polynomial for each of the vectors $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$; that is, $Q(\mathcal{A})(\boldsymbol{e}_i) = \mathbf{0}$ for all $i = 1, \dots, n$. We shall prove that Q is an annihilator polynomial for every vector $\boldsymbol{x} \in \mathsf{L}$. By definition, $\boldsymbol{x}$ is a linear combination of vectors of a basis, that is, $\boldsymbol{x} = \alpha_1 \boldsymbol{e}_1 + \alpha_2 \boldsymbol{e}_2 + \cdots + \alpha_n \boldsymbol{e}_n$. Then

$$\begin{aligned} Q(\mathcal{A})(\boldsymbol{x}) &= Q(\mathcal{A})(\alpha_1 \boldsymbol{e}_1 + \cdots + \alpha_n \boldsymbol{e}_n) \\ &= \alpha_1 Q(\mathcal{A})(\boldsymbol{e}_1) + \cdots + \alpha_n Q(\mathcal{A})(\boldsymbol{e}_n) \\ &= \mathbf{0}. \end{aligned}$$

Definition 4.25 A polynomial the annihilates every vector of a space L is called an *annihilator polynomial* of this space (keeping in mind that we mean for the given linear transformation $\mathcal{A} : \mathsf{L} \to \mathsf{L}$).

In conclusion, let us compare the arguments used in the proofs of Theorems 4.18 and 4.22. In the first case, we relied on the existence of a root (that is, a factor of degree 1) of the *characteristic* polynomial, while in the latter case, we required the existence of a simplest factor (of degree 1 or 2) for the *annihilator* polynomial. The connection between these polynomials relies on a result that is important in and of itself. It is called the *Cayley–Hamilton theorem.*

Theorem 4.26 *The characteristic polynomial is an annihilator polynomial for its associated vector space.*

The proof of this theorem is based on arguments analogous to those used in the proof of Lemma 4.19, but relating to a much more general situation. We shall now consider polynomials in the variable t whose coefficients are not numbers, but linear transformations of the vector space L into itself or (which is the same thing if some fixed basis has been chosen in L) square matrices P_i:

$$P(t) = P_0 + P_1 t + \cdots + P_k t^k.$$

One can work with these as with ordinary polynomials if one assumes that the variable t commutes with the coefficients. It is also possible to substitute for t the matrix A of a linear transformation. We shall denote the result of this substitution by $P(A)$, that is,

$$P(A) = P_0 + P_1 A + \cdots + P_k A^k.$$

It is important here that t and A are written to the right of the coefficients P_i. Further, we shall consider the situation in which P_i and A are square matrices of one and the same order. In view of what we have said above, all assertions will be true as well for the case that in the last formula, instead of the matrices P_i and A we have the linear transformations $\mathcal{P}_i$ and $\mathcal{A}$ of some vector space L into itself:

$$\mathcal{P}(\mathcal{A}) = \mathcal{P}_0 + \mathcal{P}_1 \mathcal{A} + \cdots + \mathcal{P}_k \mathcal{A}^k.$$

However, in this case, the analogue of formula (4.13) from Sect. 4.1 does not hold, that is, if the polynomial $R(t)$ is equal to $P(t)Q(t)$ and A is the matrix of an arbitrary linear transformation of the vector space L. Then generally speaking, $R(A) \neq P(A)Q(A)$. For example, if we have polynomials $P = P_1 t$ and $Q = Q_0$, then $P_1 t Q_0 = P_1 Q_0 t$, but it is not true that $P_1 A Q_0 = P_1 Q_0 A$ for an arbitrary matrix A, since matrices A and Q_0 do not necessarily commute. However, there is one important special case in which formula (4.13) holds.

Lemma 4.27 *Let*

$$P(t) = P_0 + P_1 t + \cdots + P_k t^k, \qquad Q(t) = Q_0 + Q_1 t + \cdots + Q_l t^l,$$

and suppose that the polynomial $R(t)$ equals $P(t)Q(t)$. Then $R(A) = P(A)Q(A)$ if the matrix A commutes with every coefficient of the polynomial $Q(t)$, that is, $AQ_i = Q_i A$ for all $i = 1, \ldots, l$.

Proof It is not difficult to see that the polynomial $R(t) = P(t)Q(t)$ can be represented in the form $R(t) = R_0 + R_1 t + \cdots + R_{k+l} t^{k+l}$ with coefficients $R_s = \sum_{i=0}^{s} P_i Q_{s-i}$, where $P_i = 0$ if $i > k$, and $Q_i = 0$ if $i > l$. Similarly, the polynomial $R(A) = P(A)Q(A)$ can be expressed in the form

$$R(A) = \sum_{s=0}^{k+l} \left(\sum_{i=0}^{s} P_i A^i Q_{s-i} A^{s-i} \right)$$

with the same conditions: $P_i = 0$ if $i > k$, and $Q_i = 0$ if $i > l$. By the condition of the lemma, $AQ_j = Q_j A$, whence by induction, we easily obtain that $A^i Q_j = Q_j A^i$ for every choice of i and j. Thus our expression takes the form

$$R(A) = \sum_{s=0}^{k+l} \left(\sum_{i=0}^{s} P_i Q_{s-i} A^s \right) = P(A)Q(A).$$

□

Of course, the analogous assertion holds for all polynomials for which the variable t stands to the left of the coefficients (then the matrix A must commute with every coefficient of the polynomial P, and not Q).

Using Lemma 4.27, we can prove the Cayley–Hamilton theorem.

Proof of Theorem 4.26 Let us consider the matrix $tE - A$ and denote its determinant by $\varphi(t) = |tE - A|$. The coefficients of the polynomial $\varphi(t)$ are numbers, and as is easily seen, it is equal to the characteristic polynomial matrix A multiplied by $(-1)^n$ (in order to make the coefficient of t^n equal to 1). Let us denote by $B(t)$ the adjugate matrix to $tE - A$ (see the definition on p. 73). It is clear that $B(t)$ will contain as its elements certain polynomials in t of degree at most $n-1$, and consequently, we may write it in the form $B(t) = B_0 + B_1 t + \cdots + B_{n-1} t^{n-1}$, where the B_i are certain matrices. Formula (2.70) for the adjugate matrix yields

$$B(t)(tE - A) = \varphi(t)E. \tag{4.22}$$

Let us substitute into formula (4.22) in place of the variable t the matrix A of the linear transformation $\mathcal{A}$ with respect to some basis of the vector space L. Since the matrix A commutes with the identity matrix E and with itself, then by Lemma 4.27, we obtain the matrix equality $B(A)(AE - A) = \varphi(A)E$, the left-hand side of which is equal to the null matrix. It is clear that in an arbitrary basis, the null matrix is the matrix of the null transformation $\mathcal{O} : \mathsf{L} \to \mathsf{L}$, and consequently, $\varphi(\mathcal{A}) = \mathcal{O}$. And this is the assertion of Theorem 4.26. □

In particular, it is now clear that by the proof of Theorem 4.22, we may take as the annihilator polynomial the characteristic polynomial of the transformation $\mathcal{A}$.

4.3 Complexification

In view of the fact that real vector spaces are encountered especially frequently in applications, we present here another method of determining the properties of linear transformations of such spaces, proceeding from already proved properties of linear transformations of complex spaces.

Let L be a finite-dimensional real vector space. In order to apply our previously worked-out arguments, it will be necessary to *embed* it in some complex space $\mathsf{L}^{\mathbb{C}}$. For this, we shall use the fact that, as we saw in Sect. 3.5, L is isomorphic to the space of rows of length n (where $n = \dim \mathsf{L}$), which we denote by $\mathbb{R}^n$.

In view of the usual set inclusion $\mathbb{R} \subset \mathbb{C}$, we may consider $\mathbb{R}^n$ a subset of $\mathbb{C}^n$. In this case, it is not, of course, a subspace of $\mathbb{C}^n$ as a vector space over the field $\mathbb{C}$. For example, multiplication by the complex scalar i does not take $\mathbb{R}^n$ into itself. On the contrary, as is easily seen, we have the decomposition

$$\mathbb{C}^n = \mathbb{R}^n \oplus i\mathbb{R}^n$$

(let us recall that in $\mathbb{C}^n$, multiplication by i is defined for all vectors, and in particular for vectors in the subset $\mathbb{R}^n$). We shall now denote $\mathbb{R}^n$ by L, while $\mathbb{C}^n$ will be denoted by $\mathsf{L}^{\mathbb{C}}$. The previous relationship is now written thus:

$$\mathsf{L}^{\mathbb{C}} = \mathsf{L} \oplus i\mathsf{L}. \tag{4.23}$$

An arbitrary linear transformation $\mathcal{A}$ on a vector space L (as a space over the field $\mathbb{R}$) can then be extended to all of $\mathsf{L}^{\mathbb{C}}$ (as a space over the field $\mathbb{C}$). Namely, as follows from the decomposition (4.23), every vector $\boldsymbol{x} \in \mathsf{L}^{\mathbb{C}}$ can be uniquely represented in the form $\boldsymbol{x} = \boldsymbol{u} + i\boldsymbol{v}$, where $\boldsymbol{u}, \boldsymbol{v} \in \mathsf{L}$, and we set

$$\mathcal{A}^{\mathbb{C}}(\boldsymbol{x}) = \mathcal{A}(\boldsymbol{u}) + i\mathcal{A}(\boldsymbol{v}). \tag{4.24}$$

We omit the obvious verification that the mapping $\mathcal{A}^{\mathbb{C}}$ defined by the relationship (4.24) is a linear transformation of the space $\mathsf{L}^{\mathbb{C}}$ (over the field $\mathbb{C}$). Moreover, it is not difficult to prove that $\mathcal{A}^{\mathbb{C}}$ is the only linear transformation of the space $\mathsf{L}^{\mathbb{C}}$ whose restriction to L coincides with $\mathcal{A}$, that is, for which the equality $\mathcal{A}^{\mathbb{C}}(\boldsymbol{x}) = \mathcal{A}(\boldsymbol{x})$ is satisfied for all $\boldsymbol{x}$ in L.

The construction presented here may seem somewhat inelegant, since it uses an isomorphism of the spaces L and $\mathbb{R}^n$, for whose construction it is necessary to choose some basis of L. Although in the majority of applications such a basis exists, we shall give a construction that does not depend on the choice of basis. For this, we recall that the space L can be reconstructed from its dual space L^* via the isomorphism $\mathsf{L} \simeq \mathsf{L}^{**}$, which we constructed in Sect. 3.7. In other words, $\mathsf{L} \simeq \mathfrak{L}(\mathsf{L}^*, \mathbb{R})$, where as before, $\mathfrak{L}(\mathsf{L}, \mathsf{M})$ denotes the space of linear mappings $\mathsf{L} \to \mathsf{M}$ (here either all spaces are considered complex or else they are all considered real).

We now consider $\mathbb{C}$ as a two-dimensional vector space over the field $\mathbb{R}$ and set

$$\mathsf{L}^{\mathbb{C}} = \mathfrak{L}\big(\mathsf{L}^*, \mathbb{C}\big), \tag{4.25}$$

where in $\mathfrak{L}(\mathsf{L}^*, \mathbb{C})$, both spaces L^* and $\mathbb{C}$ are considered real. Thus the relationship (4.25) carries $\mathsf{L}^{\mathbb{C}}$ into a vector space over the field $\mathbb{R}$. But we can convert it into a space over the field $\mathbb{C}$ after defining multiplication of vectors in $\mathsf{L}^{\mathbb{C}}$ by complex scalars. Namely, if $\boldsymbol{\varphi} \in \mathfrak{L}(\mathsf{L}^*, \mathbb{C})$ and $z \in \mathbb{C}$, then we set $z\boldsymbol{\varphi} = \boldsymbol{\psi}$, where $\boldsymbol{\psi} \in \mathfrak{L}(\mathsf{L}^*, \mathbb{C})$ is defined by the condition

$$\boldsymbol{\psi}(\boldsymbol{f}) = z \cdot \boldsymbol{\varphi}(\boldsymbol{f}) \quad \text{for all } \boldsymbol{f} \in \mathsf{L}^*.$$

It is easily verified that $\mathsf{L}^{\mathbb{C}}$ thus defined is a vector space over the field $\mathbb{C}$, and passage from L to $\mathsf{L}^{\mathbb{C}}$ will be the same as described above, for an arbitrary choice of basis L (that is, choice of the isomorphism $\mathsf{L} \simeq \mathbb{R}^n$).

If $\mathcal{A}$ is a linear transformation of the space L, then we shall define a corresponding linear transformation $\mathcal{A}^{\mathbb{C}}$ of the space $\mathsf{L}^{\mathbb{C}}$, after assigning to each vector $\boldsymbol{\psi} \in \mathsf{L}^{\mathbb{C}}$ the value $\mathcal{A}^{\mathbb{C}}(\boldsymbol{\psi}) \in \mathsf{L}^{\mathbb{C}}$ using the relation

$$\big(\mathcal{A}^{\mathbb{C}}(\boldsymbol{\psi})\big)(\boldsymbol{f}) = \boldsymbol{\psi}\big(\mathcal{A}^*(\boldsymbol{f})\big) \quad \text{for all } \boldsymbol{f} \in \mathsf{L}^*,$$

where $\mathcal{A}^* : \mathsf{L}^* \to \mathsf{L}^*$ is the dual transformation to $\mathcal{A}$ (see p. 125). It is clear that $\mathcal{A}^{\mathbb{C}}$ is indeed a linear transformation of the space $\mathsf{L}^{\mathbb{C}}$, and its restriction to L coincides with the transformation $\mathcal{A}$, that is, for every $\boldsymbol{\psi} \in \mathsf{L}$, $\mathcal{A}^{\mathbb{C}}(\boldsymbol{\psi})(\boldsymbol{f}) = \mathcal{A}(\boldsymbol{\psi})(\boldsymbol{f})$ is satisfied for all $\boldsymbol{f} \in \mathsf{L}^*$.

Definition 4.28 The complex vector space $\mathsf{L}^{\mathbb{C}}$ is called the *complexification* of the real vector space L, while the transformation $\mathcal{A}^{\mathbb{C}} : \mathsf{L}^{\mathbb{C}} \to \mathsf{L}^{\mathbb{C}}$ is the *complexification* of the transformation $\mathcal{A} : \mathsf{L} \to \mathsf{L}$.

Remark 4.29 The construction presented above is applicable as well to a more general situation: using it, it is possible to assign to any vector space L over an arbitrary field $\mathbb{K}$ the space $\mathsf{L}^{\mathbb{K}'}$ over the bigger field $\mathbb{K}' \supset \mathbb{K}$, and to the linear transformation $\mathcal{A}$ of the field L, the linear transformation $\mathcal{A}^{\mathbb{K}'}$ of the field $\mathsf{L}^{\mathbb{K}'}$.

In the space $\mathsf{L}^{\mathbb{C}}$ that we constructed, it will be useful to introduce the operation of complex conjugation, which assigns to a vector $\boldsymbol{x} \in \mathsf{L}^{\mathbb{C}}$ the vector $\overline{\boldsymbol{x}} \in \mathsf{L}^{\mathbb{C}}$, or interpreting $\mathsf{L}^{\mathbb{C}}$ as $\mathbb{C}^n$ (with which we began this section), taking the complex conjugate for each number in the row $\boldsymbol{x}$, or (equivalently) using (4.23), setting $\overline{\boldsymbol{x}} = \boldsymbol{u} - i\boldsymbol{v}$ for $\boldsymbol{x} = \boldsymbol{u} + i\boldsymbol{v}$. It is clear that

$$\overline{\boldsymbol{x} + \boldsymbol{y}} = \overline{\boldsymbol{x}} + \overline{\boldsymbol{y}}, \qquad \overline{(\alpha \boldsymbol{x})} = \overline{\alpha}\overline{\boldsymbol{x}}$$

hold for all vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathsf{L}^{\mathbb{C}}$ and arbitrary complex scalar α.

The transformation $\mathcal{A}^{\mathbb{C}}$ obtained according to the rule (4.24) from a certain transformation $\mathcal{A}$ of a real vector space L will be called *real*. For a real transformation $\mathcal{A}^{\mathbb{C}}$, we have the relationship

$$\overline{\mathcal{A}^{\mathbb{C}}(\boldsymbol{x})} = \mathcal{A}^{\mathbb{C}}(\overline{\boldsymbol{x}}), \tag{4.26}$$

which follows from the definition (4.24) of a transformation $\mathcal{A}^{\mathbb{C}}$. Indeed, if we have $\boldsymbol{x} = \boldsymbol{u} + i\boldsymbol{v}$, then

$$\mathcal{A}^{\mathbb{C}}(\boldsymbol{x}) = \mathcal{A}(\boldsymbol{u}) + i\mathcal{A}(\boldsymbol{v}), \qquad \overline{\mathcal{A}^{\mathbb{C}}(\boldsymbol{x})} = \mathcal{A}(\boldsymbol{u}) - i\mathcal{A}(\boldsymbol{v}).$$

On the other hand, $\overline{\boldsymbol{x}} = \boldsymbol{u} - i\boldsymbol{v}$, from which follows $\mathcal{A}^{\mathbb{C}}(\overline{\boldsymbol{x}}) = \mathcal{A}(\boldsymbol{u}) - i\mathcal{A}(\boldsymbol{v})$ and therefore (4.26).

Consider the linear transformation $\mathcal{A}$ of the real vector space L. To it there corresponds, as shown above, the linear transformation $\mathcal{A}^{\mathbb{C}}$ of the complex vector space $\mathsf{L}^{\mathbb{C}}$. By Theorem 4.18, the transformation $\mathcal{A}^{\mathbb{C}}$ has an eigenvector $\boldsymbol{x} \in \mathsf{L}^{\mathbb{C}}$ for which, therefore, one has the equality

$$\mathcal{A}^{\mathbb{C}}(\boldsymbol{x}) = \lambda \boldsymbol{x}, \tag{4.27}$$

where λ is a root of the characteristic polynomial of the transformation $\mathcal{A}$ and, generally speaking, is a certain complex number. We must distinguish two cases: λ real and λ complex.

Case 1: λ is a real number. In this case, the characteristic polynomial of the transformation $\mathcal{A}$ has a real root, and therefore $\mathcal{A}$ has an eigenvector in the field L; that is, L has a one-dimensional invariant subspace.

Case 2: λ is a complex number. Let $\lambda = a + ib$, where a and b are real numbers, $b \neq 0$. The eigenvector $\boldsymbol{x}$ can also be written in the form $\boldsymbol{x} = \boldsymbol{u} + i\boldsymbol{v}$, where the vectors $\boldsymbol{u}, \boldsymbol{v}$ are in L. By assumption, $\mathcal{A}^{\mathbb{C}}(\boldsymbol{x}) = \mathcal{A}(\boldsymbol{u}) + i\mathcal{A}(\boldsymbol{v})$, and then relationship (4.27), in view of the decomposition (4.23), gives

$$\mathcal{A}(\boldsymbol{v}) = a\boldsymbol{v} + b\boldsymbol{u}, \qquad \mathcal{A}(\boldsymbol{u}) = -b\boldsymbol{v} + a\boldsymbol{u}. \tag{4.28}$$

This means that the subspace $\mathsf{L}' = \langle \boldsymbol{v}, \boldsymbol{u} \rangle$ of the space L is invariant with respect to the transformation $\mathcal{A}$. The dimension of the subspace L' is equal to 2, and vectors $\boldsymbol{v}, \boldsymbol{u}$ form a basis of it. Indeed, it suffices to verify their linear independence. The linear dependence of $\boldsymbol{v}$ and $\boldsymbol{u}$ would imply that $\boldsymbol{v} = \xi\boldsymbol{u}$ (or else that $\boldsymbol{u} = \xi\boldsymbol{v}$) for some real ξ. But by $\boldsymbol{v} = \xi\boldsymbol{u}$, the second equality of (4.28) would yield the relationship $\mathcal{A}(\boldsymbol{u}) = (a - b\xi)\boldsymbol{u}$, and that would imply that $\boldsymbol{u}$ is a real eigenvector of the transformation $\mathcal{A}$, with the real eigenvalue $a - b\xi$; that is, we are dealing with case 1. The case $\boldsymbol{u} = \xi\boldsymbol{v}$ is similar.

Uniting cases 1 and 2, we obtain another proof of Theorem 4.22. We observe that in fact, we have now proved even more than what is asserted in that theorem. Namely, we have shown that in the two-dimensional invariant subspace L' there exists a basis $\boldsymbol{v}, \boldsymbol{u}$ in which the transformation $\mathcal{A}$ gives the formula (4.28), that is, it has a matrix of the form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad b \neq 0.$$

Definition 4.30 A linear transformation $\mathcal{A}$ of a real vector space L is said to be *block-diagonalizable* if in some basis, its matrix has the form

$$A = \begin{pmatrix} \alpha_1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \alpha_r & 0 & \ddots & \vdots \\ \vdots & \ddots & 0 & B_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & B_s \end{pmatrix}, \tag{4.29}$$

where $\alpha_1, \dots, \alpha_r$ are real matrices of order 1 (that is, real numbers), and $B_1, \dots, B_s$ are real matrices of order 2 of the form

$$B_j = \begin{pmatrix} a_j & -b_j \\ b_j & a_j \end{pmatrix}, \quad b_j \neq 0. \tag{4.30}$$

Block-diagonalizable linear transformations are the real analogue of diagonalizable transformations of complex vector spaces. The connection between these two concepts is established in the following theorem.

Theorem 4.31 *A linear transformation $\mathcal{A}$ of a vector space L is block-diagonalizable if and only if its complexification $\mathcal{A}^{\mathbb{C}}$ is a diagonalizable transformation of the space $\mathsf{L}^{\mathbb{C}}$.*

Proof Suppose the linear transformation $\mathcal{A}:\mathsf{L}\to\mathsf{L}$ is block-diagonalizable. This means that in some basis of the space L, its matrix has the form (4.29), which is equivalent to the decomposition

$$\mathsf{L}=\mathsf{L}_1\oplus\cdots\oplus\mathsf{L}_r\oplus\mathsf{M}_1\oplus\cdots\oplus\mathsf{M}_s, \tag{4.31}$$

where L_i and M_j are subspaces that are invariant with respect to the transformation $\mathcal{A}$. In our case, $\dim\mathsf{L}_i=1$, so that $\mathsf{L}_i=\langle \boldsymbol{e}_i\rangle$ and $\mathcal{A}(\boldsymbol{e}_i)=\alpha_i\boldsymbol{e}_i$, and $\dim\mathsf{M}_j=2$, where in some basis of the subspace M_j, the restriction of the transformation $\mathcal{A}$ to M_j has matrix of the form (4.30). Using formula (4.30), one is easily convinced that the restriction $\mathcal{A}^{\mathbb{C}}$ to the two-dimensional subspace M_j has two distinct complex-conjugate eigenvalues: λ_j and $\overline{\lambda}_j$. If $\boldsymbol{f}_j$ and $\boldsymbol{f}'_j$ are the corresponding eigenvectors, then in $\mathsf{L}^{\mathbb{C}}$ there is a basis $\boldsymbol{e}_1,\dots,\boldsymbol{e}_r,\boldsymbol{f}_1,\boldsymbol{f}'_1,\dots,\boldsymbol{f}_s,\boldsymbol{f}'_s$, in which the matrix of the transformation $\mathcal{A}^{\mathbb{C}}$ assumes the form

$$\begin{pmatrix}
\alpha_1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 & 0\\
0 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0\\
\vdots & \ddots & \alpha_r & 0 & \ddots & \ddots & \ddots & \vdots\\
\vdots & \ddots & 0 & \lambda_1 & \ddots & \ddots & \ddots & \vdots\\
\vdots & \ddots & \ddots & \ddots & \overline{\lambda}_1 & \ddots & \ddots & \vdots\\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots\\
0 & \ddots & \ddots & \ddots & \ddots & \ddots & \lambda_s & 0\\
0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 & \overline{\lambda}_s
\end{pmatrix}. \tag{4.32}$$

This means that the transformation $\mathcal{A}^{\mathbb{C}}$ is diagonalizable.

Now suppose, conversely, that $\mathcal{A}^{\mathbb{C}}$ is diagonalizable, that is, in some basis of the space $\mathsf{L}^{\mathbb{C}}$, the transformation $\mathcal{A}^{\mathbb{C}}$ has the diagonal matrix

$$\begin{pmatrix}
\lambda_1 & 0 & \cdots & 0\\
0 & \lambda_2 & \cdots & 0\\
\vdots & \vdots & \ddots & \vdots\\
0 & 0 & \cdots & \lambda_n
\end{pmatrix}. \tag{4.33}$$

Among the numbers $\lambda_1,\dots,\lambda_n$ may be found some that are real and some that are complex. All the numbers λ_i are roots of the characteristic polynomial of the transformation $\mathcal{A}^{\mathbb{C}}$. But clearly (by the definition of $\mathsf{L}^{\mathbb{C}}$), any basis of the real vector space L is a basis of the complex space $\mathsf{L}^{\mathbb{C}}$, and in such a basis, the matrices of the transformations $\mathcal{A}$ and $\mathcal{A}^{\mathbb{C}}$ coincide. That is, the matrix of the transformation $\mathcal{A}^{\mathbb{C}}$ is real in some basis. This means that its characteristic polynomial has real coefficients. It then follows from well-known properties of real polynomials that if among the numbers $\lambda_1, \dots, \lambda_n$ some are complex, then they come in conjugate pairs λ_j and $\overline{\lambda}_j$, and moreover, λ_j and $\overline{\lambda}_j$ occur the same number of times. We may assume that in the matrix of (4.33), the first r numbers are real: $\lambda_i = \alpha_i \in \mathbb{R}$ $(i \le r)$, while the remainder are complex, and moreover, λ_j and $\overline{\lambda}_j$ $(j > r)$ are adjacent to each other. In this case, the matrix of the transformation assumes the form (4.32). Along with each eigenvector $\boldsymbol{e}$ of the transformation $\mathcal{A}^{\mathbb{C}}$, the space $\mathsf{L}^{\mathbb{C}}$ contains a vector $\overline{\boldsymbol{e}}$. Moreover, if $\boldsymbol{e}$ has the eigenvalue λ, then $\overline{\boldsymbol{e}}$ has the eigenvalue $\overline{\lambda}$. This follows easily from the fact that $\mathcal{A}$ is a real transformation and from the relationship $\overline{(\mathsf{L}^{\mathbb{C}})_\lambda} = (\mathsf{L}^{\mathbb{C}})_{\overline{\lambda}}$, which can be easily verified. Therefore, we may write down the basis in which the transformation $\mathcal{A}^{\mathbb{C}}$ has the form (4.32) in the form $\boldsymbol{e}_1, \dots, \boldsymbol{e}_r, \boldsymbol{f}_1, \overline{\boldsymbol{f}_1}, \dots, \boldsymbol{f}_s, \overline{\boldsymbol{f}_s}$, where all $\boldsymbol{e}_i$ are in L.

Let us set $\boldsymbol{f}_j = \boldsymbol{u}_j + i\boldsymbol{v}_j$, where $\boldsymbol{u}_j, \boldsymbol{v}_j \in \mathsf{L}$, and let us consider the subspace $\mathsf{N}_j = \langle \boldsymbol{u}_j, \boldsymbol{v}_j \rangle$. It is clear that N_j is invariant with respect to $\mathcal{A}$, and by formula (4.28), the restriction of $\mathcal{A}$ to the subspace N_j gives a transformation that in the basis $\boldsymbol{u}_j, \boldsymbol{v}_j$ has matrix of the form (4.30). We therefore see that

$$\mathsf{L}^{\mathbb{C}} = \langle \boldsymbol{e}_1 \rangle \oplus \cdots \oplus \langle \boldsymbol{e}_r \rangle \oplus i\langle \boldsymbol{e}_1 \rangle \oplus \cdots \oplus i\langle \boldsymbol{e}_r \rangle \oplus \mathsf{N}_1 \oplus i\mathsf{N}_1 \oplus \cdots \oplus \mathsf{N}_s \oplus i\mathsf{N}_s,$$

from which follows the decomposition

$$\mathsf{L} = \langle \boldsymbol{e}_1 \rangle \oplus \cdots \oplus \langle \boldsymbol{e}_r \rangle \oplus \mathsf{N}_1 \oplus \cdots \oplus \mathsf{N}_s,$$

analogous to (4.31). This shows that the transformation $\mathcal{A} : \mathsf{L} \to \mathsf{L}$ is block-diagonalizable. □

Similarly, using the notion of complexification, it is possible to prove a real analogue of Theorems 4.14, 4.18, and 4.21.

4.4 Orientation of a Real Vector Space

The real line has two directions: to the *left* and to the *right* (from an arbitrarily chosen point, taken as the origin). Analogously, in real three-dimensional space, there are two directions for traveling around a point: *clockwise* and *counterclockwise*. We shall consider analogous concepts in an arbitrary real vector space (of finite dimension).

Let $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ and $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$ be two bases of a real vector space L. Then there exists a linear transformation $\mathcal{A} : \mathsf{L} \to \mathsf{L}$ such that

$$\mathcal{A}(\boldsymbol{e}_i) = \boldsymbol{e}'_i, \quad i = 1, \dots, n. \tag{4.34}$$

It is clear that for the given pair of bases, there exists only one such linear transformation $\mathcal{A}$, and moreover, it is not singular: ($|\mathcal{A}| \neq 0$).

Definition 4.32 Two bases $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ and $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$ are said to have the *same orientation* if the transformation $\mathcal{A}$ satisfying the condition (4.34) is proper ($|\mathcal{A}| > 0$; recall Definition 4.4), and to be *oppositely oriented* if $\mathcal{A}$ is improper ($|\mathcal{A}| < 0$).

Theorem 4.33 *The property of having the same orientation induces an equivalence relation on the set of all bases of the vector space* L.

Proof The definition of equivalence relation (on an arbitrary set) was given on page xii, and to prove the theorem, we have only to verify symmetry and transitivity, since reflexivity is completely obvious (for the mapping $\mathcal{A}$, take the identity transformation $\mathcal{E}$). Since the transformation $\mathcal{A}$ is nonsingular, it follows that relationship (4.34) can be written in the form $\mathcal{A}^{-1}(\boldsymbol{e}'_i) = \boldsymbol{e}_i$, $i = 1, \dots, n$, from which follows the symmetry property of bases having the same orientation: the transformation $\mathcal{A}$ is replaced by $\mathcal{A}^{-1}$, where here $|\mathcal{A}^{-1}| = |\mathcal{A}|^{-1}$, and the sign of the determinant remains the same.

Let bases $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ and $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$ have the same orientation, and suppose bases $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$ and $\boldsymbol{e}''_1, \dots, \boldsymbol{e}''_n$ also have the same orientation. By definition, this means that the transformations $\mathcal{A}$, from (4.34), and $\mathcal{B}$, defined by

$$\mathcal{B}\big(\boldsymbol{e}'_i\big) = \boldsymbol{e}''_i, \quad i = 1, \dots, n, \tag{4.35}$$

are proper. Replacing in (4.35) the expressions for the vectors $\boldsymbol{e}'_i$ from (4.34), we obtain

$$\mathcal{B}\mathcal{A}(\boldsymbol{e}_i) = \boldsymbol{e}''_i, \quad i = 1, \dots, n,$$

and since $|\mathcal{B}\mathcal{A}| = |\mathcal{B}| \cdot |\mathcal{A}|$, the transformation $\mathcal{B}\mathcal{A}$ is also proper, that is, the bases $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ and $\boldsymbol{e}''_1, \dots, \boldsymbol{e}''_n$ have the same orientation, which completes the proof of transitivity. □

We shall denote the set of all bases of the space L by $\mathfrak{E}$. Theorem 4.33 then tells us that the property of having the same orientation decomposes the set $\mathfrak{E}$ into two equivalence classes, that is, we have the decomposition $\mathfrak{E} = \mathfrak{E}_1 \cup \mathfrak{E}_2$, where $\mathfrak{E}_1 \cap \mathfrak{E}_2 = \varnothing$. To obtain this decomposition in practice, we may proceed as follows: Choose in L an arbitrary basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ and denote by $\mathfrak{E}_1$ the collection of all bases that have the same orientation as the chosen basis, and let $\mathfrak{E}_2$ denote the collection of bases with the opposite orientation. Theorem 4.33 tells us that this decomposition of $\mathfrak{E}$ does not depend on which basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ we choose. We can assert that any two bases appearing together in one of the two subsets $\mathfrak{E}_1$ and $\mathfrak{E}_2$ have the same orientation, and if they belong to different subsets, then they have opposite orientations.

Definition 4.34 The choice of one of the subsets $\mathfrak{E}_1$ and $\mathfrak{E}_2$ is called an *orientation* of the vector space L. Once an orientation has been chosen, the bases lying in the chosen subset are said to be *positively oriented*, while those in the other subset are called *negatively oriented*.

As can be seen from this definition, the selection of an orientation of a vector space depends on an arbitrary choice: it would have been equally possible to have called the positively oriented bases negatively oriented, and vice versa. It is no accident that in practical applications, the actual choice of orientation is frequently based on an appeal such as to the structure of the human body (left–right) or to the motion of the Sun in the heavens (clockwise or counterclockwise).

The crucial part of the theory presented in this section is that there is a connection between orientation and certain topological concepts (such as those presented in the introduction to this book; see p. xvii).

To pursue this idea, we must first of all define *convergence* for sequences of elements of the set $\mathfrak{E}$. We shall do so by introducing on the set $\mathfrak{E}$ a *metric*, that is, by converting it into a *metric space*. This means that we must define a function $r(x, y)$ for all $x, y \in \mathfrak{E}$ taking real values and satisfying properties 1–3 introduced on p. xvii. We begin by defining a metric $r(A, B)$ on the set $\mathfrak{A}$ of square matrices of a given order n with real entries.

For a matrix $A = (a_{ij})$ in $\mathfrak{A}$, we let the number $\mu(A)$ equal the maximum absolute value of its entries:

$$\mu(A) = \max_{i,j=1,\dots,n} |a_{ij}|. \tag{4.36}$$

Lemma 4.35 *The function $\mu(A)$ defined by relationship* (4.36) *exhibits the following properties*:

(a) $\mu(A) > 0$ *for* $A \neq O$ *and* $\mu(A) = 0$ *for* $A = O$.
(b) $\mu(A + B) \le \mu(A) + \mu(B)$ *for all* $A, B \in \mathfrak{A}$.
(c) $\mu(AB) \le n\mu(A)\mu(B)$ *for all* $A, B \in \mathfrak{A}$.

Proof Property (a) obviously follows from the definition (4.36), while property (b) follows from an analogous inequality for numbers: $|a_{ij} + b_{ij}| \le |a_{ij}| + |b_{ij}|$. It remains to prove property (c). Let $A = (a_{ij})$, $B = (b_{ij})$, and $C = AB = (c_{ij})$. Then $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$, and so

$$|c_{ij}| \le \sum_{k=1}^{n} |a_{ik}||b_{kj}| \le \sum_{k=1}^{n} \mu(A)\mu(B) = n\mu(A)\mu(B).$$

From this it follows that $\mu(C) \le n\mu(A)\mu(B)$. □

We can now convert the set $\mathfrak{A}$ into a metric space by setting for every pair of matrices A and B in $\mathfrak{A}$,

$$r(A, B) = \mu(A - B). \tag{4.37}$$

Properties 1–3 introduced in the definition of a metric follow from the definitions in (4.36) and (4.37) and properties (a) and (b) proved in Lemma 4.35.

A metric on $\mathfrak{A}$ enables us to introduce a metric on the set $\mathfrak{E}$ of bases of a vector space L. Let us fix a distinguished basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ and define the number $r(x, y)$ for two arbitrary bases x and y in the set $\mathfrak{E}$ as follows. Suppose the bases x and y consist of vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ and $\boldsymbol{y}_1, \dots, \boldsymbol{y}_n$, respectively. Then there exist linear transformations $\mathcal{A}$ and $\mathcal{B}$ of the space L such that

$$\mathcal{A}(\boldsymbol{e}_i) = \boldsymbol{x}_i, \qquad \mathcal{B}(\boldsymbol{e}_i) = \boldsymbol{y}_i, \quad i = 1, \dots, n. \tag{4.38}$$

The transformations $\mathcal{A}$ and $\mathcal{B}$ are nonsingular, and by condition (4.38), they are uniquely determined. Let us denote by A and B the matrices of the transformations $\mathcal{A}$ and $\mathcal{B}$ in the basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$, and set

$$r(x, y) = r(A, B), \tag{4.39}$$

where $r(A, B)$ is as defined above by relationship (4.37). Properties 1–3 in the definition of a metric hold for $r(x, y)$ from analogous properties of the metric $r(A, B)$.

However, here a difficulty arises: The definition of the metric $r(x, y)$ by relationship (4.39) depends on the choice of some basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ of the space L. Let us choose another basis $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$ and let us see how the metric $r'(x, y)$ that results differs from $r(x, y)$. To this end, we use the familiar fact that for two bases $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ and $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$ there exists a unique linear (and in addition, nonsingular) transformation $\mathcal{C} : \mathsf{L} \to \mathsf{L}$ taking the first basis into the second:

$$\boldsymbol{e}'_i = \mathcal{C}(\boldsymbol{e}_i), \quad i = 1, \dots, n. \tag{4.40}$$

Formulas (4.38) and (4.40) show that for linear transformations $\overline{\mathcal{A}} = \mathcal{A}\mathcal{C}^{-1}$ and $\overline{\mathcal{B}} = \mathcal{B}\mathcal{C}^{-1}$, one has the equality

$$\overline{\mathcal{A}}\big(\boldsymbol{e}'_i\big) = \boldsymbol{x}_i, \qquad \overline{\mathcal{B}}\big(\boldsymbol{e}'_i\big) = \boldsymbol{y}_i, \quad i = 1, \dots, n. \tag{4.41}$$

Let us denote by A' and B' the matrices of the transformations $\mathcal{A}$ and $\mathcal{B}$ in the basis $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$, and by $\overline{A}$ and $\overline{B}$, the matrices of the transformations $\overline{\mathcal{A}}$ and $\overline{\mathcal{B}}$ in this basis. Let C be the matrix of the transformation $\mathcal{C}$, that is, by (4.40), the transition matrix from the basis $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$ to the basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$. Then matrices $A', \overline{A}$ and $B', \overline{B}$ are related by $\overline{A} = A'C^{-1}$ and $\overline{B} = B'C^{-1}$. Furthermore, we observe that A and A' are matrices of the same transformation $\mathcal{A}$ in two different bases ($\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ and $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$), and similarly, B and B' are matrices of the single transformation $\mathcal{B}$. Therefore, by the formula for changing coordinates, we have $A' = C^{-1}AC$ and $B' = C^{-1}BC$, and so as a result, we obtain the relationship

$$\overline{A} = A'C^{-1} = C^{-1}A, \qquad \overline{B} = B'C^{-1} = C^{-1}B. \tag{4.42}$$

Returning to the definition (4.39) of a metric on $\mathfrak{A}$, we see that $r'(x, y) = r(\overline{A}, \overline{B})$. Substituting in the last relationship the expression (4.42) for matrices $\overline{A}$ and $\overline{B}$, and taking into account definition (4.37) and property (c) from Lemma 4.35, we obtain

$$r'(x,y) = r(\overline{A}, \overline{B}) = r\big(C^{-1}A, C^{-1}B\big)$$
$$= \mu\big(C^{-1}(A-B)\big) \le n\mu\big(C^{-1}\big)\mu(A-B) = \alpha r(x,y),$$

where the number $\alpha = n\mu(C^{-1})$ does not depend on the bases x and y, but only on $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ and $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$. Since the last two bases play a symmetric role in our construction, we may obtain analogously a second equality $r(x,y) \le \beta r'(x,y)$ with a certain positive constant β. The relationship

$$r'(x,y) \le \alpha r(x,y), \qquad r(x,y) \le \beta r'(x,y), \alpha, \quad \beta > 0, \tag{4.43}$$

shows that although the metrics $r(x,y)$ and $r'(x,y)$ defined in terms of different bases $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ and $\boldsymbol{e}'_1, \dots, \boldsymbol{e}'_n$ are different, nevertheless, on the set $\mathfrak{A}$, the notion of convergence is the same for both bases. To put this more formally, having chosen in $\mathfrak{E}$ two different bases and having with the help of these bases defined metrics $r(x,y)$ and $r'(x,y)$ on $\mathfrak{E}$, we have thereby defined two different metric spaces $\mathfrak{E}'$ and $\mathfrak{E}''$ with one and the same underlying set $\mathfrak{E}$ but with different metrics r and r' defined on it. Here the identity mapping of the space $\mathfrak{E}$ onto itself is not an isometry of $\mathfrak{E}'$ and $\mathfrak{E}''$, but by relationship (4.43), it is a homeomorphism. We may therefore speak about continuous mappings, paths in $\mathfrak{E}$, and its connected components without specifying precisely which metric we are using.

Let us move on to the question whether two bases of the set $\mathfrak{E}$ can be continuously deformed into each other (see the general definition on p. xx). This question reduces to whether there is a continuous deformation between the nonsingular matrices A and B corresponding to these bases under the selection of some auxiliary basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ (just as with other topological concepts, continuous deformability does not depend on the choice of the auxiliary basis). We wish to emphasize that the condition of nonsingularity of the matrices A and B plays here an essential role.

We shall formulate the notion of continuous deformability for matrices in a certain set $\mathfrak{A}$ (which in our case will be the set of nonsingular matrices).

Definition 4.36 A matrix A is said to be *continuously deformable* into a matrix B if there exists a family of matrices $A(t)$ in $\mathfrak{A}$ whose elements depend continuously on a parameter $t \in [0,1]$ such that $A(0) = A$ and $A(1) = B$.

It is obvious that this property of matrices being continuously deformable into each other defines an equivalence relation on the set $\mathfrak{A}$. By definition, we need to verify that the properties of reflexivity, symmetry, and transitivity are satisfied. The verification of all these properties is simple and given on p. xx.

Let us note one additional property of continuous deformability in the case that the set $\mathfrak{A}$ has another property: for two arbitrary matrices belonging to $\mathfrak{A}$, their product also belongs to $\mathfrak{A}$. It is clear that this property is satisfied if $\mathfrak{A}$ is the set of nonsingular matrices (in subsequent chapters, we shall meet other examples of such sets).

Lemma 4.37 *If a matrix A is continuously deformable into B, and $C \in \mathfrak{A}$ is an arbitrary matrix, then AC is continuously deformable into BC, and CA is continuously deformable into CB.*

Proof By the condition of the theorem, we have a family $A(t)$ of matrices in $\mathfrak{A}$, where $t \in [0, 1]$, effecting a continuous deformation of A into B. To prove the first assertion, we take the family $A(t)C$, and for the second, the family $CA(t)$. This family produces the deformations that we require. □

Theorem 4.38 *Two nonsingular square matrices of the same order with real elements are continuously deformable into each other if and only if the signs of their determinants are the same.*

Proof Let A and B be the matrices described in the statement of the theorem. The necessary condition that the determinants $|A|$ and $|B|$ be of the same sign is obvious. Indeed, in view of the formula for the expansion of the determinant (Sect. 2.7) or else by its inductive definition (Sect. 2.2), it is clear that the determinant is a polynomial in the elements of the matrix, and consequently, $|A(t)|$ is a continuous function of t. But a continuous function taking values with opposite signs at the endpoints of an interval must take the value zero at some point within the interval, while at the same time, the condition $|A(t)| \neq 0$ must be satisfied for all $t \in [0, 1]$.

Let us prove the sufficiency of the condition, at first for determinants for which $|A| > 0$. We shall show that A is continuously deformable into the identity matrix E. By Theorem 2.62, the matrix A can be represented as a product of matrices $U_{ij}(c)$, S_k, and a diagonal matrix. The matrix $U_{ij}(c)$ is continuously deformable into the identity: as the family $A(t)$, we may take the matrices $U_{ij}(ct)$. Since the S_k are themselves diagonal matrices, we see that (in view of Lemma 4.37) the matrix A is continuously deformable into the diagonal matrix D, and from the assumption $|A| > 0$ and the part of the theorem already proved, it follows that $|D| > 0$.

Let

$$D = \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_n \end{pmatrix}.$$

Every element d_i can be represented in the form $\varepsilon_i p_i$, where $\varepsilon_i = 1$ or -1, while $p_i > 0$. The matrix (p_i) of order 1 for $p_i > 0$ can be continuously deformed into (1). For this, it suffices to set $A(t) = (a(t))$, where $a(t) = t + (1-t)p_i$ for $t \in [0, 1]$. Therefore, the matrix D is continuously deformable into the matrix D', in which all $d_i = \varepsilon_i p_i$ are replaced by ε_i. As we have seen, from this it follows that $|D'| > 0$, that is, the number of -1's on the main diagonal is even. Let us combine them in pairs. If there is -1 in the ith and jth places, then we recall that the matrix

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \tag{4.44}$$

defines in the plane the central symmetry transformation with respect to the origin, that is, a rotation through the angle π. If we set

$$A(t) = \begin{pmatrix} \cos \pi t & -\sin \pi t \\ \sin \pi t & \cos \pi t \end{pmatrix}, \tag{4.45}$$

then we obtain the matrix of rotation through the angle πt, which as t changes from 0 to 1, effects a continuous deformation of the matrix (4.44) into the identity. It is clear that we thus obtain a continuous deformation of the matrix D' into E.

Denoting continuous deformability by $\sim$, we can write down three relationships: $A \sim D$, $D \sim D'$, $D' \sim E$, from which follows by transitivity that $A \sim E$. From this follows as well the assertion of Theorem 4.38 for two matrices A and B with $|A| > 0$ and $|B| > 0$.

In order to take care of matrices A with $|A| < 0$, we introduce the function $\varepsilon(A) = +1$ if $|A| > 0$ and $\varepsilon(A) = -1$ if $|A| < 0$. It is clear that $\varepsilon(AB) = \varepsilon(A)\varepsilon(B)$. If $\varepsilon(A) = \varepsilon(B) = -1$, then let us set $A^{-1}B = C$. Then $\varepsilon(C) = 1$, and by what was proved previously, $C \sim E$. By Lemma 4.37, it follows that $B \sim A$, and by symmetry, we have $A \sim B$. □

Taking into account the results of Sect. 3.4 and Lemma 4.37, from Theorem 4.38, we obtain the following result.

Theorem 4.39 *Two nonsingular linear transformations of a real vector space are continuously deformable into each other if and only if the signs of their determinants are the same.*

Theorem 4.40 *Two bases of a real vector space are continuously deformable into each other if and only if they have the same orientation.*

Recalling the topological notions introduced earlier of path-connectedness and path-connected component (p. xx), we see that the results we have obtained can be formulated as follows. The set $\mathfrak{A}$ of nonsingular matrices of a given order (or linear transformations of the space L into itself) can be represented as the union of two path-connected components corresponding to positive and negative determinants. Similarly, the set $\mathfrak{E}$ of all bases of a space L can be represented as the union of two path-connected components consisting of positively and negatively oriented bases.