Introduction to Linear Algebra

Michael Taylor

Math. Dept., UNC
E-mail address: met@math.unc.edu

2010 *Mathematics Subject Classification.* 15-00, 15-01

Key words and phrases. vector spaces, linear transformations, matrices, determinants, eigenvectors, eigenvalues, generalized eigenvectors, inner products, norms, trace, adjoint, unitary, orthogonal transformations, Jordan canonical form, polar decomposition, singular value decomposition

Contents

Preface

Linear algebra is an important gateway connecting elementary mathematics to more advanced subjects, such as multivariable calculus, systems of differential equations, differential geometry, and group representations. The purpose of this work is to provide an introduction to this subject that will prepare the reader to tackle such further material.

In Chapter 1 we define the class of vector spaces (real or complex) and discuss some basic examples, including $\mathbb{R}^n$ and $\mathbb{C}^n$, or, as we denote them, $\mathbb{F}^n$, with $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. We then consider linear transformations between such spaces. In particular, we look at an $m \times n$ matrix A as defining a linear transformation $A : \mathbb{F}^n \to \mathbb{F}^m$. We define the range $\mathcal{R}(T)$ and null space $\mathcal{N}(T)$ of a linear transformation $T : V \to W$. In §1.3 we define the notion of basis of a vector space. Vector spaces with finite bases are called finite dimensional. We establish the crucial property that any two bases of such a vector space V have the same number of elements (denoted $\dim V$). We apply this to other results on bases of vector spaces, culminating in the "fundamental theorem of linear algebra," that if $T : V \to W$ is linear and V is finite dimensional, then $\dim \mathcal{N}(T) + \dim \mathcal{R}(T) = \dim V$, and discuss some of its important consequences.

A linear transformation $T : V \to V$ is said to be invertible provided it is one-to-one and onto, i.e., provided $\mathcal{N}(T) = 0$ and $\mathcal{R}(T) = V$. In §1.5 we define the determinant of such T, $\det T$ (when V is finite dimensional), and show that T is invertible if and only if $\det T \neq 0$. One useful tool in the study of determinants consists of row operations and column operations. In §1.6 we pursue these operations further, and show how applying row reduction to an $m \times n$ matrix A works to display a basis of its null space, while applying column reduction to A works to display a basis of its range.

In Chapter 2 we study eigenvalues λ_j and eigenvectors v_j of a linear transformation $T : V \to V$, satisfying $Tv_j = \lambda_j v_j$. Results of §1.5 imply that λ_j is a root of the "characteristic polynomial" $\det(\lambda I - T)$. Section 2.2 extends the scope of this study to a treatment of generalized eigenvectors of T, which are shown to always

form a basis of V, when V is a finite-dimensional complex vector space. This ties in with a treatment of properties of nilpotent matrices and triangular matrices, in §2.3. Combining the results on generalized eigenvectors with a closer look at the structure of nilpotent matrices leads to the presentation of the Jordan canonical form for an $n \times n$ complex matrix, in §2.4.

In Chapter 3 we introduce inner products on vector spaces and endow them with a Euclidean geometry, in particular with a distance and a norm. In §3.2 we discuss two types of norms on linear transformations, the "operator norm" and the "Hilbert-Schmidt norm." Then, in §§3.3–3.4, we discuss some special classes on linear transformations on inner product spaces: self-adjoint, skew-adjoint, unitary, and orthogonal transformations. In §3.5 we establish a theorem of Schur that for each $n \times n$ matrix A, there is an orthonormal basis of $\mathbb{C}^n$ with respect to which A takes an upper triangular form. Section 3.6 establishes a polar decomposition result, that each $n \times n$ complex matrix can be written as KP, with K unitary and P positive semidefinite, and a related result known as the singular value decomposition of a complex matrix (square or rectangular).

In §3.7 we define the matrix exponential e^{tA}, for $A \in M(n, \mathbb{C})$, so that $x(t) = e^{tA}v$ solves the differential equation $dx/dt = Ax,\ x(0) = v$. We produce a power series for e^{tA} and establish some basic properties. The matrix exponential is fundamental to applications of linear algebra to ODE. Here, we use this connection to produce another proof that if A is an $n \times n$ complex matrix, then $\mathbb{C}^n$ has a basis consisting of generalized eigenvectors of A. The proof given here is completely different from that of §2.2.

Section 3.8 takes up the discrete Fourier transform (DFT), acting on functions $f : \mathbb{Z} \to \mathbb{C}$ that are periodic, of period n. This transform diagonalizes an important class of operators known as convolution operators. This section also treats a fast implementation of the DFT, known as the Fast Fourier Transform (FFT).

Chapter 4 introduces some further basic concepts in the study of linear algebra on real and complex vector spaces. In §4.1 we define the dual space V' to a vector space. We associate to a linear map $A : V \to W$ its transpose $A^t : W' \to V'$ and establish a natural isomorphism $V \approx (V')'$ when $\dim V < \infty$. Section 4.2 looks at convex subsets of a finite-dimensional vector space. Section 4.3 deals with quotient spaces V/W when W is a linear subspace of V.

In §4.4 we study positive matrices, including the important class of stochastic matrices. We establish the Perron-Frobenius theorem, which states that, under a further hypothesis called irreducibility, a positive matrix has a positive eigenvector, unique up to scalar multiple, and draw useful corollaries for the behavior of irreducible stochastic matrices.

Some basic notation

$\mathbb{R}$ is the set of real numbers.

$\mathbb{C}$ is the set of complex numbers.

$\mathbb{Z}$ is the set of integers.

$\mathbb{Z}^+$ is the set of integers ≥ 0.

$\mathbb{N}$ is the set of integers ≥ 1 (the "natural numbers").

$\mathbb{Q}$ is the set of rational numbers.

$x \in \mathbb{R}$ means x is an element of $\mathbb{R}$, i.e., x is a real number.

(a, b) denotes the set of $x \in \mathbb{R}$ such that $a < x < b$.

$[a, b]$ denotes the set of $x \in \mathbb{R}$ such that $a \leq x \leq b$.

$\{x \in \mathbb{R} : a \leq x \leq b\}$ denotes the set of x in $\mathbb{R}$ such that $a \leq x \leq b$.

$[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$ and $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$.

$\overline{z} = x - iy$ if $z = x + iy \in \mathbb{C},\ x, y \in \mathbb{R}$.

$f : A \to B$ denotes that the function f takes points in the set A to points in B. One also says f maps A to B.

$x \to x_0$ means the variable x tends to the limit x_0.

Chapter 1

Vector spaces, linear transformations, and matrices

This chapter introduces the principal objects of linear algebra and develops some basic properties. These objects are linear transformations, acting on vector spaces. A vector space V possesses the operations of vector addition and multiplication by a scalar (a number, real or complex); that is, one has

$$u, v \in V,\ a \in \mathbb{F} \Longrightarrow u + v,\ av \in V.$$

Here, $\mathbb{F}$ stands for either $\mathbb{R}$ (the set of real numbers) or $\mathbb{C}$ (the set of complex numbers). In Chapter 6 we will bring in more general classes of scalars. A linear transformation is a map $T : V \to W$ between two vector spaces that preserves these vector operations.

Basic cases of vector spaces are the familiar Euclidean spaces $\mathbb{R}^n$ and their complex counterparts. In these cases a vector is uniquely specified by its components. More generally, vector spaces have bases, in terms of which one can uniquely expand a vector. We show in §1.3 that any two bases of a vector space V have the same number of elements. This number is called the dimension of V, and denoted $\dim V$.

Two basic objects associated to a linear transformation $T : V \to W$ are its null space,

$$\mathcal{N}(T) = \{v \in V : Tv = 0\},$$

and its range,

$$\mathcal{R}(T) = \{Tv : v \in V\}.$$

These subspaces of V and W, respectively, are also vector spaces. The "fundamental theorem of linear algebra" is an identity connecting $\dim \mathcal{N}(T)$, $\dim \mathcal{R}(T)$, and $\dim V$.

Matrices provide a convenient representation of linear transformations. A matrix is a rectangular array of numbers,

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}.$$

We say A is an $m \times n$ matrix and write $A \in M(m \times n, \mathbb{F})$, if the entries a_{jk} of A are elements of $\mathbb{F}$. In case $m = n$, we say $A \in M(n, \mathbb{F})$. Horizontal arrays in A are called rows, and vertical arrays are called columns. The composition of linear transformations can be expressed in terms of matrix products.

One fundamental question is how to determine whether an $n \times n$ matrix is invertible. In §1.5 we introduce the determinant, and show that $A \in M(n, \mathbb{F})$ is invertible if and only if $\det A \neq 0$. We introduce the determinant by three simple rules. We show that these rules uniquely specify the determinant, and lead to a formula for $\det A$ as a sum of products of the entries a_{jk} of A. An important ingredient in our development of the determinant is an investigation of how $\det A$ transforms when we apply to A a class of operations called row operations and column operations.

Use of these operations is explored further in §1.6. One application is to a computation of the inverse A^{-1}, via a sequence of row operations. This is called the method of Gaussian elimination. Going further, for $A \in M(m \times n, \mathbb{F})$, we show that the null space $\mathcal{N}(A)$ is invariant under row operations and the range $\mathcal{R}(A)$ is invariant under column operations. This can be used to construct bases of $\mathcal{N}(A)$ and of $\mathcal{R}(A)$.

The process of applying a sequence of row operations to an invertible $n \times n$ matrix A to compute its inverse has the effect of representing A as a product of matrices of certain particularly simple forms (cf. (1.6.12)). We also make use of this in §1.6 to derive the following geometrical interpretation of the determinant of an invertible matrix $A \in M(n, \mathbb{R})$. Namely, if $\Omega \subset \mathbb{R}^n$ is a bounded open set,

$$\mathrm{Vol}(A(\Omega)) = |\det A| \, \mathrm{Vol}(\Omega).$$

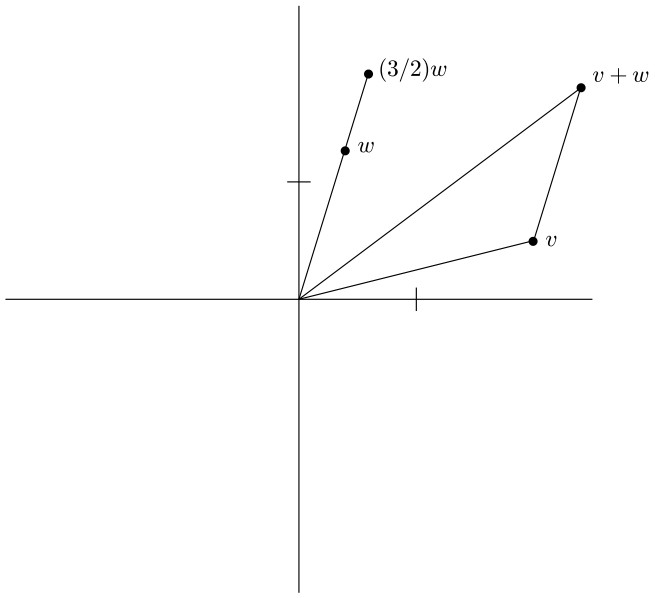

Figure 1.1.1. Vector operations on $\mathbb{R}^2$

1.1. Vector spaces

Vector spaces arise as a natural setting in which to make a mathematical study of multidimensional phenomena. The first case is the Euclidean plane, which, in the Cartesian system, consists of points that are specified by pairs of real numbers,

$$v = (v_1, v_2). \tag{1.1.1}$$

We denote the Cartesian plane by $\mathbb{R}^2$. Similarly, the three-dimensional space of common experience can be identified with $\mathbb{R}^3$, the set of triples $v = (v_1, v_2, v_3)$ of real numbers.

More generally we have n-space $\mathbb{R}^n$, whose elements consist of n-tuples of real numbers:

$$v = (v_1, \dots, v_n). \tag{1.1.2}$$

There is vector addition; if also $w = (w_1, \dots, w_n) \in \mathbb{R}^n$,

$$v + w = (v_1 + w_1, \dots, v_n + w_n). \tag{1.1.3}$$

There is also multiplication by scalars; if a is a real number (a *scalar*),

$$av = (av_1, \dots, av_n). \tag{1.1.4}$$

Figure 1.1.1 illustrates these vector operations on the Euclidean plane $\mathbb{R}^2$.

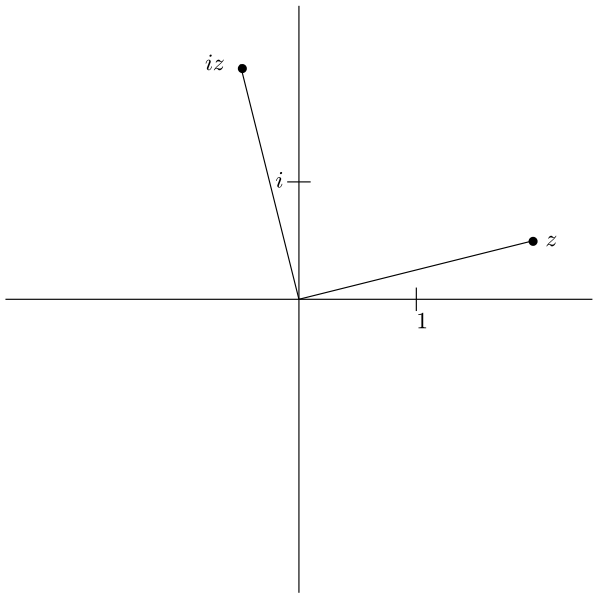

Figure 1.1.2. Multiplication by i in $\mathbb{C}$

We could also use complex numbers, replacing $\mathbb{R}^n$ by $\mathbb{C}^n$, and allowing $a \in \mathbb{C}$ in (1.1.4). Recall that a complex number $z \in \mathbb{C}$ has the form $z = x + iy,\ x, y \in \mathbb{R}$. If also $w = u + iv$, we have

$$z + w = (x + u) + i(y + v), \tag{1.1.5}$$

similar to vector addition on $\mathbb{R}^2$. In addition, there is complex multiplication,

$$\begin{aligned} zw &= (x + iy)(u + iv) \\ &= (xu - yv) + i(xv + yu), \end{aligned} \tag{1.1.6}$$

governed by the rule

$$i^2 = -1. \tag{1.1.7}$$

See Figure 1.1.2 for an illustration of the operation $z \mapsto iz$ in the complex plane $\mathbb{C}$.

We will use $\mathbb{F}$ to denote $\mathbb{R}$ or $\mathbb{C}$.

Above we represented elements of $\mathbb{F}^n$ as *row vectors*. Often we represent elements of $\mathbb{F}^n$ as *column vectors*. We write

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \quad av + w = \begin{pmatrix} av_1 + w_1 \\ \vdots \\ av_n + w_n \end{pmatrix}. \tag{1.1.8}$$

There are other mathematical objects that have natural analogues of the vector operations (1.1.3)–(1.1.4). For example, let $I = [a, b]$ denote an interval in $\mathbb{R}$ and let $C(I)$ denote the set of functions $f : I \to \mathbb{F}$ that are continuous. We can define addition and multiplication by a scalar on $C(I)$ by

$$(f + g)(x) = f(x) + g(x), \quad (af)(x) = af(x). \tag{1.1.9}$$

Similarly, if k is a positive integer, let $C^k(I)$ denote the set of functions $f : I \to \mathbb{F}$ whose derivatives up ot order k exist and are continuous on I. Again we have the "vector operations" (1.1.9). Other examples include $\mathcal{P}$, the set of polynomials in x, and $\mathcal{P}_n$, the set of polynomials in x of degree $\leq n$. These sets also have vector operations given by (1.1.9). In the case of polynomials in $\mathcal{P}_n$,

$$\begin{aligned} f(x) &= a_n x^n + \cdots + a_1 x + a_0, \\ g(x) &= b_n x^n + \cdots + b_1 x + b_0, \end{aligned}$$

the formulas (1.1.9) also yield

$$\begin{aligned} (f + g)(x) &= (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0), \\ (cf)(x) &= ca_n x^n + \cdots + ca_1 x + ca_0, \end{aligned}$$

closely parallel to (1.1.3)–(1.1.4).

The spaces just described are all examples of vector spaces.

We define this general notion now. A *vector space* over $\mathbb{F}$ is a set V, endowed with two operations, that of vector addition and multiplication by scalars. That is, given $v, w \in V$ and $a \in \mathbb{F}$, then $v + w$ and av are defined in V. Furthermore, the following properties are to hold, for all $u, v, w \in V,\ a, b \in \mathbb{F}$. First there are laws for vector addition:

$$\text{Commutative law} \ : \quad u + v = v + u, \tag{1.1.10}$$

$$\text{Associative law} \ : \quad (u + v) + w = u + (v + w), \tag{1.1.11}$$

$$\text{Zero vector} \ : \quad \exists\ 0 \in V,\ v + 0 = v, \tag{1.1.12}$$

$$\text{Negative} \ : \quad \exists - v,\ v + (-v) = 0. \tag{1.1.13}$$

Next there are laws for multiplication by scalars:

$$\text{Associative law} \ : \quad a(bv) = (ab)v, \tag{1.1.14}$$

$$\text{Unit} \ : \quad 1 \cdot v = v. \tag{1.1.15}$$

Finally there are two distributive laws:

$$a(u + v) = au + av, \tag{1.1.16}$$

$$(a + b)u = au + bu. \tag{1.1.17}$$

The eight rules just set down are rules that, first of all, apply to the cases $V = \mathbb{R}$ and $V = \mathbb{C}$, and as such are familiar rules of algebra in that setting. One can readily verify these rules also for $\mathbb{R}^n$ and $\mathbb{C}^n$, and for the various function spaces such as $C^k(I)$ and $\mathcal{P}_n$, with vector operations defined by (1.1.9),

A number of other simple identities are automatic consequences of the rules given above. Here are some, which the reader is invited to verify:

$$\begin{aligned} &v + w = v \Rightarrow w = 0, \\ &v + 0 \cdot v = (1 + 0)v = v, \\ &0 \cdot v = 0, \\ &v + w = 0 \Rightarrow w = -v, \\ &v + (-1)v = 0 \cdot v = 0, \\ &(-1)v = -v. \end{aligned} \tag{1.1.18}$$

We mention some other ways to produce vector spaces. For one, we say a subset W of a vector space V is a linear subspace provided

$$w_j \in W,\ a_j \in \mathbb{F} \Longrightarrow a_1 w_1 + a_2 w_2 \in W. \tag{1.1.19}$$

Then W inherits the structure of a vector space. For example, $C^k(I)$ is a linear subspace of $C^\ell(I)$ if $k > \ell$, and $\mathcal{P}_n$ is a linear subspace of $\mathcal{P}_m$ if $n < m$. Further examples of linear subspaces will arise in subsequent sections. This notion will be seen to be a fundamental part of linear algebra.

A further class of vector spaces arises as follows, extending the construction of $\mathbb{F}^n$ as n-tuples of elements of $\mathbb{F}$. To begin, let $V_1, \dots, V_n$ be vector spaces (over $\mathbb{F}$). Then we define the *direct sum*

$$V_1 \oplus \cdots \oplus V_n \tag{1.1.20}$$

to consist of n-tuples

$$v = (v_1, \dots, v_n), \quad v_j \in V_j. \tag{1.1.21}$$

If also $w = (w_1, \dots, w_n)$ with $w_j \in V_j$, we define vector addition as in (1.1.3) and multiplication by $a \in \mathbb{F}$ as in (1.1.4). The reader can verify that the direct sum V so defined satisfies the conditions for being a vector space.

Exercises

1. Show that the results in (1.1.18) follow from the basic rules (1.1.10)–(1.1.17).
Hint. To start, add $-v$ to both sides of the identity $v + w = v$, and take account first of the associative law (1.1.11), and then of the rest of (1.1.10)–(1.1.13). For the second line of (1.1.18), use the rules (1.1.15) and (1.1.17). Then use the first two lines of (1.1.18) to justify the third line...

2. Demonstrate that the following results hold for every vector space V. Take $a \in \mathbb{F},\ v \in V$.

$$a \cdot 0 = 0 \in V,$$
$$a(-v) = -av.$$

Hint. Feel free to use the results of (1.1.18).

Let V be a vector space (over $\mathbb{F}$) and $W, X \subset V$ linear subspaces. We say

$$V = W + X \tag{1.1.22}$$

provided each $v \in V$ can be written

$$v = w + x, \quad w \in W,\ x \in X. \tag{1.1.23}$$

We say

$$V = W \oplus X \tag{1.1.24}$$

provided each $v \in V$ has a unique representation (1.1.23).

3. Show that

$$V = W \oplus X \Longleftrightarrow V = W + X \ \text{ and } \ W \cap X = 0.$$

4. Take $V = \mathbb{R}^3$. Specify in each case below whether $V = W + X$ and whether $V = W \oplus X$.

$$W = \{(x, y, z) : z = 0\}, \quad X = \{(x, y, z) : x = 0\},$$
$$W = \{(x, y, z) : z = 0\}, \quad X = \{(x, y, z) : x = y = 0\},$$
$$W = \{(x, y, z) : z = 0\}, \quad X = \{(x, y, z) : y = z = 0\}.$$

5. If $V_1, \dots, V_n$ are linear subspaces of V, extend (1.1.22) to the notion

$$V = V_1 + \cdots + V_n, \tag{1.1.25}$$

and extend (1.1.24) to the notion that

$$V = V_1 \oplus \cdots \oplus V_n. \tag{1.1.26}$$

6. Compare the notion of $V_1 \oplus \cdots \oplus V_n$ in Exercise 5 with that in (1.1.20)–(1.1.21).

1.2. Linear transformations and matrices

If V and W are vector spaces over $\mathbb{F}$ ($\mathbb{R}$ or $\mathbb{C}$), a map

$$T : V \longrightarrow W \tag{1.2.1}$$

is said to be a *linear transformation* provided

$$T(a_1v_1 + a_2v_2) = a_1Tv_1 + a_2Tv_2, \quad \forall\ a_j \in \mathbb{F},\ v_j \in V. \tag{1.2.2}$$

We also write $T \in \mathcal{L}(V, W)$. In case $V = W$, we also use the notation $\mathcal{L}(V) = \mathcal{L}(V, V)$.

Linear transformations arise in a number of ways. For example, an $m \times n$ matrix, i.e., a rectangular array

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}, \tag{1.2.3}$$

with entries in $\mathbb{F}$, defines a linear transformation

$$A : \mathbb{F}^n \longrightarrow \mathbb{F}^m, \tag{1.2.4}$$

by

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} \Sigma a_{1\ell} b_\ell \\ \vdots \\ \Sigma a_{m\ell} b_\ell \end{pmatrix}. \tag{1.2.5}$$

We say $A \in M(m \times n, \mathbb{F})$ when A is given by (1.2.3). If $m = n$, we say $A \in M(n, \mathbb{F})$.

See Figure 1.2.1 for an illustration of the action of the transformation

$$A : \mathbb{R}^2 \longrightarrow \mathbb{R}^2, \quad A = \begin{pmatrix} 3 & -1 \\ -1 & 3 \end{pmatrix}, \tag{1.2.6}$$

showing the distinguished vectors $e_1 = (1, 0)^t$ and $e_2 = (0, 1)^t$, and their images $Ae_1,\ Ae_2$. We also display the circle $x^2 + y^2 = 1$ and its image under A. A further examination of the structure of linear transformations in Chapter 2 will lead to Figure 2.1.1, displaying additional information on the behavior of this transformation.

We also have linear transformations on function spaces, such as multiplication operators

$$M_f : C^k(I) \longrightarrow C^k(I), \quad M_f g(x) = f(x)g(x), \tag{1.2.7}$$

given $f \in C^k(I),\ I = [a, b]$, and the operation of differentiation:

$$D : C^{k+1}(I) \longrightarrow C^k(I), \quad Df(x) = f'(x). \tag{1.2.8}$$

We also have integration:

$$\mathcal{I} : C^k(I) \longrightarrow C^{k+1}(I), \quad \mathcal{I}f(x) = \int_a^x f(y)\, dy. \tag{1.2.9}$$

Note also that

$$D : \mathcal{P}_{k+1} \longrightarrow \mathcal{P}_k, \quad \mathcal{I} : \mathcal{P}_k \longrightarrow \mathcal{P}_{k+1}, \tag{1.2.10}$$

where $\mathcal{P}_k$ denotes the space of polynomials in x of degree $\leq k$.

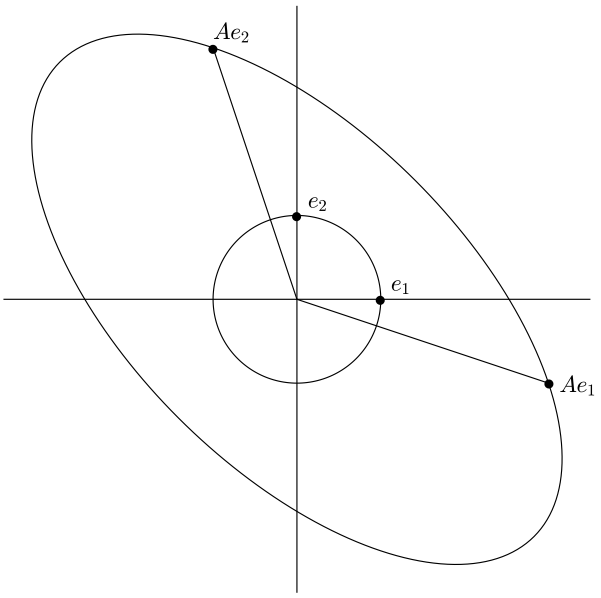

Figure 1.2.1. Action of the linear transformation A in (1.2.6)

Two linear transformations $T_j \in \mathcal{L}(V, W)$ can be added:

$$T_1 + T_2 : V \longrightarrow W, \quad (T_1 + T_2)v = T_1 v + T_2 v. \tag{1.2.11}$$

Also $T \in \mathcal{L}(V, W)$ can be multiplied by a scalar:

$$aT : V \longrightarrow W, \quad (aT)v = a(Tv). \tag{1.2.12}$$

This makes $\mathcal{L}(V, W)$ a vector space.

We can also compose linear transformations $S \in \mathcal{L}(W, X),\ T \in \mathcal{L}(V, W)$:

$$ST : V \longrightarrow X, \quad (ST)v = S(Tv). \tag{1.2.13}$$

For example, we have

$$M_f D : C^{k+1}(I) \longrightarrow C^k(I), \quad M_f Dg(x) = f(x)g'(x), \tag{1.2.14}$$

given $f \in C^k(I)$. When two transformations

$$A : \mathbb{F}^n \longrightarrow \mathbb{F}^m, \quad B : \mathbb{F}^k \longrightarrow \mathbb{F}^n \tag{1.2.15}$$

are represented by matrices, e.g., A as in (1.2.3)–(1.2.5) and

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1k} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nk} \end{pmatrix}, \tag{1.2.16}$$

then

$$AB : \mathbb{F}^k \longrightarrow \mathbb{F}^m \tag{1.2.17}$$

is given by matrix multiplication:

$$AB = \begin{pmatrix} \Sigma a_{1\ell} b_{\ell 1} & \cdots & \Sigma a_{1\ell} b_{\ell k} \\ \vdots & & \vdots \\ \Sigma a_{m\ell} b_{\ell 1} & \cdots & \Sigma a_{m\ell} b_{\ell k} \end{pmatrix}. \tag{1.2.18}$$

For example,

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}. \tag{1.2.19}$$

Another way of writing (1.2.18) is to represent A and B as

$$A = (a_{ij}), \quad B = (b_{ij}), \tag{1.2.20}$$

and then we have

$$AB = (d_{ij}), \quad d_{ij} = \sum_{\ell=1}^{n} a_{i\ell} b_{\ell j}. \tag{1.2.21}$$

To establish the identity (1.2.18), we note that it suffices to show the two sides have the same effect on each $e_j \in \mathbb{F}^k$, $1 \le j \le k$, where e_j is the column vector in $\mathbb{F}^k$ whose jth entry is 1 and whose other entries are 0. First note that

$$Be_j = \begin{pmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix}, \tag{1.2.22}$$

which is the jth column in B, as one can see via (1.2.5). Similarly, if D denotes the right side of (1.2.18), De_j is the jth column of this matrix, i.e.,

$$De_j = \begin{pmatrix} \Sigma a_{1\ell} b_{\ell j} \\ \vdots \\ \Sigma a_{m\ell} b_{\ell j} \end{pmatrix}. \tag{1.2.23}$$

On the other hand, applying A to (1.2.22), via (1.2.5), gives the same result, so (1.2.18) holds.

Associated with a linear transformation as in (1.2.1) there are two special linear spaces, the *null space* of T and the *range* of T. The null space of T is

$$\mathcal{N}(T) = \{v \in V : Tv = 0\}, \tag{1.2.24}$$

and the range of T is

$$\mathcal{R}(T) = \{Tv : v \in V\}. \tag{1.2.25}$$

Note that $\mathcal{N}(T)$ is a linear subspace of V and $\mathcal{R}(T)$ is a linear subspace of W. If $\mathcal{N}(T) = 0$ we say T is injective; if $\mathcal{R}(T) = W$ we say T is surjective. Note that T is injective if and only if T is one-to-one, i.e.,

$$Tv_1 = Tv_2 \Longrightarrow v_1 = v_2. \tag{1.2.26}$$

If T is surjective, we also say T is *onto*. If T is one-to-one and onto, we say it is an *isomorphism*. In such a case the *inverse*

$$T^{-1} : W \longrightarrow V \tag{1.2.27}$$

is well defined, and it is a linear transformation. We also say T is invertible, in such a case.

We illustrate the notions of surjectivity and injectivity with the following example. Take $\mathcal{P}_n$, the space of polynomials of degree $\leq n$ (with coefficients in $\mathbb{F}$). Pick distinct points $a_j \in \mathbb{F},\ 1 \leq j \leq n+1$, and define

$$E_S : \mathcal{P}_n \longrightarrow \mathbb{F}^{n+1}, \quad E_S p = \begin{pmatrix} p(a_1) \\ \vdots \\ p(a_{n+1}) \end{pmatrix}. \tag{1.2.28}$$

Here $S = \{a_1, \ldots, a_{n+1}\}$. Here is our surjectivity result.

Proposition 1.2.1. *The map E_S in* (1.2.28) *is surjective.*

Proof. For $j \in \{1, \ldots, n+1\}$, define $q_j \in \mathcal{P}_n$ by

$$q_j(t) = \prod_{\ell \neq j} (t - a_\ell). \tag{1.2.29}$$

Then

$$q_j(a_k) = 0 \Longleftrightarrow k \neq j. \tag{1.2.30}$$

We can define

$$F_S : \mathbb{F}^{n+1} \longrightarrow \mathcal{P}_n \tag{1.2.31}$$

by

$$F_S \begin{pmatrix} b_1 \\ \vdots \\ b_{n+1} \end{pmatrix} = \sum_{j=1}^{n+1} \frac{b_j}{q_j(a_j)} q_j, \tag{1.2.32}$$

and see from (1.2.30) that

$$p = F_S \begin{pmatrix} b_1 \\ \vdots \\ b_{n+1} \end{pmatrix} \Longrightarrow p(a_k) = b_k,\ \forall\, k \in \{1, \ldots, n+1\}. \tag{1.2.33}$$

In other words,

$$E_S F_S = I \ \text{ on } \ \mathbb{F}^{n+1}. \tag{1.2.34}$$

This establishes surjectivity. □

The formula (1.2.32) for F_S, satisfying (1.2.33), is called the Lagrange interpolation formula.

As a companion to Proposition 1.2.1, we have

Proposition 1.2.2. *The map E_S in* (1.2.28) *is injective.*

Proof. A polynomial $p \in \mathcal{P}_n$ belongs to $\mathcal{N}(E_S)$ if and only if

$$p(a_j) = 0, \quad \forall\, j \in \{1, \dots, n+1\}. \tag{1.2.35}$$

Now we can divide $t - a_1$ into $p(t)$, obtaining $p_1 \in \mathcal{P}_{n-1}$ and $r_1 \in \mathcal{P}_0$ such that

$$p(t) = (t - a_1)p_1(t) + r_1, \tag{1.2.36}$$

and plugging in $t = a_1$ yields $r_1 = 0$, so in fact

$$p(t) = (t - a_1)p_1(t), \quad p_1 \in \mathcal{P}_{n-1}. \tag{1.2.37}$$

Proceeding inductively, we have

$$p(t) = (t - a_1) \cdots (t - a_n)p_n, \quad p_n \in \mathcal{P}_0, \tag{1.2.38}$$

so

$$p(a_{n+1}) = 0 \Rightarrow p_n = 0 \Rightarrow p = 0, \tag{1.2.39}$$

and we have injectivity. □

Remark. In §1.3 we will see that $\mathcal{P}_n$ and $\mathbb{F}^{n+1}$ both have dimension $n + 1$, and hence, as a consequence of the fundamental theorem of linear algebra, injectivity of E_S and surjectivity of E_S are equivalent. At present, we have from Propositions 1.2.1–1.2.2 that $E_S^{-1} = F_S$, hence

$$F_S E_S = I \ \text{ on } \ \mathcal{P}_n. \tag{1.2.40}$$

Exercises

1. Using the definitions given in this section, show that the linear system of equations

$$ax + by = u,$$
$$cx + dy = v$$

is equivalent to the matrix equation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}.$$

2. Consider $A, B : \mathbb{R}^3 \to \mathbb{R}^3$, given by

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Compute AB and BA.

3. In the context of Exercise 2, specify

$$\mathcal{N}(A), \quad \mathcal{N}(B), \quad \mathcal{R}(A), \quad \mathcal{R}(B).$$

4. We say two $n \times n$ matrices A and B *commute* provided $AB = BA$. Note that $AB \neq BA$ in Exercise 2. Pick out the pair of commuting matrices from this list:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

5. Let $A \in M(n, \mathbb{F})$. Define A^k for $k \in \mathbb{Z}^+$ by

$$A^0 = I, \quad A^1 = A, \quad A^{k+1} = AA^k.$$

Show that A commutes with A^k for each k. (*Hint.* Use associativity.)

6. Show that (1.2.5) is a special case of matrix multiplication, as defined by the right side of (1.2.18).

7. Show, without using the formula (1.2.18) identifying compositions of linear transformations and matrix multiplication, that matrix multiplication is associative, i.e.,

$$A(BC) = (AB)C, \tag{1.2.41}$$

where $C : \mathbb{F}^\ell \to \mathbb{F}^k$ is given by a $k \times \ell$ matrix and the products in (1.2.41) are defined as matrix products, as in (1.2.21).

8. Show that the asserted identity (1.2.18) identifying compositions of linear transformations with matrix products follows from the result of Exercise 7.
Hint. (1.2.5), defining the action of A on $\mathbb{F}^n$, is a matrix product.

9. Define the transpose of an $m \times n$ matrix $A = (a_{jk})$ to be the $n \times m$ matrix $A^t = (a_{kj})$. Thus, if A is as in (1.2.3)–(1.2.5),

$$A^t = \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{mn} \end{pmatrix}. \tag{1.2.42}$$

For example,

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \Longrightarrow A^t = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}.$$

Suppose also B is an $n \times k$ matrix, as in (1.2.16), so AB is defined, as in (1.2.17). Show that

$$(AB)^t = B^t A^t. \tag{1.2.43}$$

10. Let

$$A = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 2 \\ 0 \\ 2 \end{pmatrix}.$$

Compute AB and BA. Then compute A^tB^t and B^tA^t.

11. Let A, B, C be matrices satisfying $C = AB$. Denote by b_k the kth column of B, cf. (1.2.22), and similarly let a_k and c_k denote the kth columns of A and C, respectively. Using the identity $c_{jk} = \sum_\ell a_{j\ell} b_{\ell k}$, verify the following formulas for the kth column of C:

$$c_k = Ab_k, \quad c_k = \sum_\ell b_{\ell k} a_\ell. \tag{1.2.44}$$

Note that the second identity represents the kth column of C as a linear combination of the columns of A, with coefficients coming from the kth column of B.

12. With D and $\mathcal{I}$ given by (1.2.8)–(1.2.9), compute $D\mathcal{I}$ and $\mathcal{I}D$. Specify

$$\mathcal{N}(D), \quad \mathcal{N}(\mathcal{I}), \quad \mathcal{R}(D), \quad \mathcal{R}(\mathcal{I}).$$

NOTE. Calculations of $D\mathcal{I}$ and $\mathcal{I}D$ bring in the fundamental theorem of calculus.

13. As a variant of Exercise 12, define

$$T : C(I) \oplus C^1(I) \longrightarrow C(I) \oplus C^1(I), \quad T(g, f) = (Df, \mathcal{I}g).$$

Here the direct sum $C(I) \oplus C^1(I)$ is defined as in (1.1.20)–(1.1.21). Compute T^2. Also, specify

$$\mathcal{N}(T), \quad \mathcal{N}(T^2), \quad \mathcal{R}(T), \quad \mathcal{R}(T^2).$$

14. For another variant, define

$$E : C^1(I) \longrightarrow C(I) \oplus \mathbb{F}, \quad Ef = (f', f(a)),$$
$$\mathcal{J} : C(I) \oplus \mathbb{F} \longrightarrow C^1(I), \quad \mathcal{J}(g, c)(t) = c + \int_a^t g(s)\, ds.$$

(Here $I = [a, b]$.) Compute $\mathcal{J}E$ and $E\mathcal{J}$.

15. As an illustration of Propositions 1.2.1–1.2.2, specify the unique polynomial $p \in \mathcal{P}_4$ such that

$$p(j) = \frac{j}{j^2 + 1}, \quad j \in \{-2, -1, 0, 1, 2\}.$$

1.3. Basis and dimension

Given a finite set $S = \{v_1, \dots, v_k\}$ in a vector space V, the *span* of S, denoted $\operatorname{Span} S$, is the set of vectors in V of the form

$$c_1 v_1 + \cdots + c_k v_k, \tag{1.3.1}$$

with c_j arbitrary scalars, ranging over $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. This set, denoted $\operatorname{Span}(S)$ is a linear subspace of V. The set S is said to be *linearly dependent* if and only if there exist scalars $c_1, \dots, c_k$, not all zero, such that (1.3.1) vanishes. Otherwise we say S is *linearly independent*.

If $\{v_1, \dots, v_k\}$ is linearly independent, we say S is a *basis* of $\operatorname{Span}(S)$, and that k is the *dimension* of $\operatorname{Span}(S)$. In particular, if this holds and $\operatorname{Span}(S) = V$, we say $k = \dim V$. We also say V has a finite basis, and that V is finite dimensional.

By convention, if V has only one element, the zero element, we say $V = 0$ and $\dim V = 0$.

It is easy to see that any finite set $S = \{v_1, \dots, v_k\} \subset V$ has a maximal subset that is linearly independent, and such a subset has the same span as S, so $\operatorname{Span}(S)$ has a basis. To take a complementary perspective, S will have a minimal subset S_0 with the same span, and any such minimal subset will be a basis of $\operatorname{Span}(S)$. Soon we will show that any two bases of a finite-dimensional vector space V have the same number of elements (so $\dim V$ is well defined). First, let us relate V to $\mathbb{F}^k$.

So say V has a basis $S = \{v_1, \dots, v_k\}$. We define a linear transformation

$$\mathcal{J}_S : \mathbb{F}^k \longrightarrow V, \qquad \text{by}$$

$$\mathcal{J}_S \begin{pmatrix} c_1 \\ \vdots \\ c_k \end{pmatrix} = c_1 v_1 + \cdots + c_k v_k. \tag{1.3.2}$$

Equivalently,

$$\mathcal{J}_S(c_1 e_1 + \cdots + c_k e_k) = c_1 v_1 + \cdots + c_k v_k, \tag{1.3.3}$$

where

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots\dots, e_k = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \tag{1.3.4}$$

We say $\{e_1, \dots, e_k\}$ is the standard basis of $\mathbb{F}^k$. The linear independence of S is equivalent to the injectivity of $\mathcal{J}_S$ and the statement that S spans V is equivalent to the surjectivity of $\mathcal{J}_S$. Hence the statement that S is a basis of V is equivalent to the statement that $\mathcal{J}_S$ is an isomorphism, with inverse uniquely specified by

$$\mathcal{J}_S^{-1}(c_1 v_1 + \cdots + c_k v_k) = c_1 e_1 + \cdots + c_k e_k. \tag{1.3.5}$$

We begin our demonstration that $\dim V$ is well defined, with the following concrete result.

Lemma 1.3.1. *If $v_1, \dots, v_{k+1}$ are vectors in $\mathbb{F}^k$, then they are linearly dependent.*

Proof. We use induction on k. The result is obvious if $k = 1$. We can suppose the last component of some v_j is nonzero, since otherwise we can regard these vectors as elements of $\mathbb{F}^{k-1}$ and use the inductive hypothesis. Reordering these vectors, we can assume the last component of v_{k+1} is nonzero, and it can be assumed to be 1. Form

$$w_j = v_j - v_{kj}v_{k+1}, \quad 1 \le j \le k,$$

where $v_j = (v_{1j}, \dots, v_{kj})^t$. Then the last component of each of the vectors $w_1, \dots, w_k$ is 0, so we can regard these as k vectors in $\mathbb{F}^{k-1}$. By induction, there exist scalars $a_1, \dots, a_k$, not all zero, such that

$$a_1w_1 + \cdots + a_kw_k = 0,$$

so we have

$$a_1v_1 + \cdots + a_kv_k = (a_1v_{k1} + \cdots + a_kv_{kk})v_{k+1},$$

the desired linear dependence relation on $\{v_1, \dots, v_{k+1}\}$. □

With this result in hand, we proceed.

Proposition 1.3.2. *If V has a basis $\{v_1, \dots, v_k\}$ with k elements and if the set $\{w_1, \dots, w_\ell\} \subset V$ is linearly independent, then $\ell \le k$.*

Proof. Take the isomorphism $\mathcal{J}_S : \mathbb{F}^k \to V$ described in (3.2)–(3.3). The hypotheses imply that $\{\mathcal{J}_S^{-1}w_1, \dots, \mathcal{J}_S^{-1}w_\ell\}$ is linearly independent in $\mathbb{F}^k$, so Lemma 1.3.1 implies $\ell \le k$. □

Corollary 1.3.3. *If V is finite-dimensional, any two bases of V have the same number of elements. If V is isomorphic to W, these spaces have the same dimension.*

Proof. If S (with $\#S$ elements) and T are bases of V, we have $\#S \le \#T$ and $\#T \le \#S$, hence $\#S = \#T$. For the latter part, an isomorphism of V onto W takes a basis of V to a basis of W. □

The following is an easy but useful consequence.

Proposition 1.3.4. *If V is finite dimensional and $W \subset V$ a linear subspace, then W has a finite basis, and* $\dim W \le \dim V$.

Proof. Suppose $\{w_1, \dots, w_\ell\}$ is a linearly independent subset of W. Proposition 3.2 implies $\ell \le \dim V$. If this set spans W, we are done. If not, there is an element $w_{\ell+1} \in W$ not in this span, and $\{w_1, \dots, w_{\ell+1}\}$ is a linearly independent subset of W. Again $\ell + 1 \le \dim V$. Continuing this process a finite number of times must produce a basis of W. □

A similar argument establishes:

Proposition 1.3.5. *Suppose V is finite dimensional, $W \subset V$ a linear subspace, and $\{w_1, \dots, w_\ell\}$ a basis of W. Then V has a basis of the form $\{w_1, \dots, w_\ell, u_1, \dots, u_m\}$, and $\ell + m = \dim V$.*

Having this, we can establish the following result, sometimes called the fundamental theorem of linear algebra.

Proposition 1.3.6. *Assume V and W are vector spaces, V finite dimensional, and*

$$A : V \longrightarrow W \tag{1.3.6}$$

a linear map. Then

$$\dim \mathcal{N}(A) + \dim \mathcal{R}(A) = \dim V. \tag{1.3.7}$$

Proof. Let $\{w_1, \dots, w_\ell\}$ be a basis of $\mathcal{N}(A) \subset V$, and complete it to a basis

$$\{w_1, \dots, w_\ell, u_1, \dots, u_m\}$$

of V. Set $L = \text{Span}\{u_1, \dots, u_m\}$, and consider

$$A_0 : L \longrightarrow W, \quad A_0 = A\big|_L. \tag{1.3.8}$$

Clearly $w \in \mathcal{R}(A) \Rightarrow w = A(a_1w_1 + \cdots + a_\ell w_\ell + b_1u_1 + \cdots + b_mu_m) = A_0(b_1u_1 + \cdots + b_mu_m)$, so

$$\mathcal{R}(A_0) = \mathcal{R}(A). \tag{1.3.9}$$

Furthermore,

$$\mathcal{N}(A_0) = \mathcal{N}(A) \cap L = 0. \tag{1.3.10}$$

Hence $A_0 : L \to \mathcal{R}(A_0)$ is an isomorphism. Thus $\dim \mathcal{R}(A) = \dim \mathcal{R}(A_0) = \dim L = m$, and we have (1.3.7). □

The following is a significant special case.

Corollary 1.3.7. *Let V be finite dimensional, and let $A : V \to V$ be linear. Then*

$$A \text{ injective} \Longleftrightarrow A \text{ surjective} \Longleftrightarrow A \text{ isomorphism}. \tag{1.3.11}$$

We mention that these equivalences can fail for infinite dimensional spaces. For example, if $\mathcal{P}$ denotes the space of polynomials in x, then $M_x : \mathcal{P} \to \mathcal{P}$ $(M_xf(x) = xf(x))$ is injective but not surjective, while $D : \mathcal{P} \to \mathcal{P}$ $(Df(x) = f'(x))$ is surjective but not injective.

Next we have the following important characterization of injectivity and surjectivity.

Proposition 1.3.8. *Assume V and W are finite dimensional and $A : V \to W$ is linear. Then*

$$A \text{ surjective} \Longleftrightarrow AB = I_W, \text{ for some } B \in \mathcal{L}(W, V), \tag{1.3.12}$$

and

$$A \text{ injective} \Longleftrightarrow CA = I_V, \text{ for some } C \in \mathcal{L}(W, V). \tag{1.3.13}$$

Proof. Clearly $AB = I \Rightarrow A$ surjective and $CA = I \Rightarrow A$ injective. We establish the converses.

First assume $A : V \to W$ is surjective. Let $\{w_1, \dots, w_\ell\}$ be a basis of W. Pick $v_j \in V$ such that $Av_j = w_j$. Set

$$B(a_1w_1 + \cdots + a_\ell w_\ell) = a_1v_1 + \cdots + a_\ell v_\ell. \tag{1.3.14}$$

This works in (1.3.12).

Next assume $A : V \to W$ is injective. Let $\{v_1, \dots, v_k\}$ be a basis of V. Set $w_j = Av_j$. Then $\{w_1, \dots, w_k\}$ is linearly independent, hence a basis of $\mathcal{R}(A)$, and we then can produce a basis $\{w_1, \dots, w_k, u_1, \dots, u_m\}$ of W. Set

$$C(a_1w_1 + \cdots + a_kw_k + b_1u_1 + \cdots + b_mu_m) = a_1v_1 + \cdots + a_kv_k. \tag{1.3.15}$$

This works in (1.3.13). □

An $m \times n$ matrix A defines a linear transformation $A : \mathbb{F}^n \to \mathbb{F}^m$, as in (1.2.3)–(1.2.5). The columns of A are

$$a_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}. \tag{1.3.16}$$

As seen in §1.2,

$$Ae_j = a_j, \tag{1.3.17}$$

where $e_1, \dots, e_n$ is the standard basis of $\mathbb{F}^n$. Hence

$$\mathcal{R}(A) = \text{ linear span of the columns of } A, \tag{1.3.18}$$

so

$$\mathcal{R}(A) = \mathbb{F}^m \Longleftrightarrow a_1, \dots, a_n \text{ span } \mathbb{F}^m. \tag{1.3.19}$$

Furthermore,

$$A\Big(\sum_{j=1}^{n} c_je_j\Big) = 0 \Longleftrightarrow \sum_{j=1}^{n} c_ja_j = 0, \tag{1.3.20}$$

so

$$\mathcal{N}(A) = 0 \Longleftrightarrow \{a_1, \dots, a_n\} \text{ is linearly independent.} \tag{1.3.21}$$

We have the following conclusion, in case $m = n$.

Proposition 1.3.9. *Let A be an $n \times n$ matrix, defining $A : \mathbb{F}^n \to \mathbb{F}^n$. Then the following are equivalent:*

$$\begin{aligned} &A \text{ is invertible}, \\ &\text{The columns of } A \text{ are linearly independent}, \\ &\text{The columns of } A \text{ span } \mathbb{F}^n. \end{aligned} \tag{1.3.22}$$

If (1.3.22) holds, then we denote the inverse of A by A^{-1}. Compare (1.2.27).

Exercises

1. Suppose $\{v_1, \dots, v_k\}$ is a basis of V. Show that

$$w_1 = v_1, \quad w_2 = v_1 + v_2, \ \dots \ , w_j = v_1 + \cdots + v_j, \ \dots \ , w_k = v_1 + \cdots + v_k$$

is also a basis of V.

2. Let V be the space of polynomials in x and y of degree ≤ 10. Specify a basis of V and compute $\dim V$.

3. Let V be the space of polynomials in x of degree ≤ 5, satisfying $p(-1) = p(0) = p(1) = 0$. Find a basis of V and give its dimension.

4. Using Euler's formula

$$e^{it} = \cos t + i \sin t, \tag{1.3.23}$$

show that $\{e^{it}, e^{-it}\}$ and $\{\cos t, \sin t\}$ are both bases for the same vector space over $\mathbb{C}$. (See the end of §3.7 for a proof of Euler's formula.)

5. Denote the space of $m \times n$ matrices with entries in $\mathbb{F}$ (as in (1.2.5)) by

$$M(m \times n, \mathbb{F}). \tag{1.3.24}$$

If $m = n$, denote it by

$$M(n, \mathbb{F}). \tag{1.3.25}$$

Show that

$$\dim M(m \times n, \mathbb{F}) = mn,$$

especially

$$\dim M(n, \mathbb{F}) = n^2.$$

6. If V and W are finite dimensional vector spaces, $n = \dim V$, $m = \dim W$, what is $\dim \mathcal{L}(V, W)$?

Let V be a finite dimensional vector space, with linear subspaces W and X. Recall the conditions under which $V = W + X$ or $V = W \oplus X$, from §1.1. Let $\{w_1, \dots, w_k\}$ be a basis of W and $\{x_1, \dots, x_\ell\}$ a basis of X.

7. Show that

$$V = W + X \Longleftrightarrow \{w_1, \dots, w_k, x_1, \dots, x_\ell\} \text{ spans } V$$
$$V = W \oplus X \Longleftrightarrow \{w_1, \dots, w_k, x_1, \dots, x_\ell\} \text{ is a basis of } V.$$

8. Show that

$$V = W + X \Longrightarrow \dim W + \dim X \geq \dim V,$$
$$V = W \oplus X \Longleftrightarrow W \cap X = 0 \quad \text{and} \quad \dim W + \dim X = \dim V.$$

9. Produce variants of Exercises 7–8 involving $V = V_1 + \cdots + V_n$ and $V = V_1 \oplus \cdots \oplus V_n$, as in (1.1.25)–(1.1.26).

10. Let V_j be finite-dimensional vector spaces over $\mathbb{F}$, and define $V_1 \oplus \cdots \oplus V_n$ as in (1.1.20)–(1.1.21). Show that

$$\dim V_1 \oplus \cdots \oplus V_n = \dim V_1 + \cdots + \dim V_n.$$

11. Let V be a vector space , W and X linear subspaces. Assume

$$n = \dim V, \quad k = \dim W, \quad \ell = \dim X.$$

Show that

$$\dim W \cap X \geq (k + \ell) - n.$$

Hint. Define $T : W \oplus X \to V$ by $T(w, x) = w - x$. Show that $W \cap X \approx \mathcal{N}(T)$. Then apply the fundamental theorem of linear algebra.

12. Let $\mathcal{W}$ be a vector space over $\mathbb{C}$, with basis $\{w_j : 1 \leq j \leq n\}$. Denote by W the set $\mathcal{W}$, with vector addition unchanged, but with multiplication by a scalar a restricted to $a \in \mathbb{R}$, so W is a vector space over $\mathbb{R}$. Show that $\{w_j, iw_j : 1 \leq j \leq n\}$ is a basis of W. We write

$$\dim_{\mathbb{C}} \mathcal{W} = n, \quad \dim_{\mathbb{R}} W = 2n.$$

13. Let V be a finite-dimensional vector space over $\mathbb{R}$. Assume we have $J \in \mathcal{L}(V)$ such that

$$J^2 = -I.$$

Define the action of $a + ib \in \mathbb{C}$ (with $a, b \in \mathbb{R}$) on V by

$$(a + ib) \cdot v = av + bJv, \quad v \in V.$$

Show that this yields a vector space over $\mathbb{C}$. Call this complex vector space $\mathcal{V}$. Show that

$$\dim_{\mathbb{C}} \mathcal{V} = k \Longrightarrow \dim_{\mathbb{R}} V = 2k.$$

REMARK. We say that J endows V with a *complex structure*.

14. Let V be a real vector space. We define $V_{\mathbb{C}}$ to be $V \oplus V$, consisting of ordered pairs (u, v), with $u, v \in V$, and with multiplication by a complex scalar $a + ib \in \mathbb{C}$ given by

$$(a + ib) \cdot (u, v) = (au - bv, bu + av).$$

Show that $V_{\mathbb{C}}$ is a vector space over $\mathbb{C}$. If we identify $V \hookrightarrow V_{\mathbb{C}}$ by $u \mapsto (u, 0)$, we can write

$$(u, v) = u + iv,$$

and the action of multiplication by $a + ib$ as

$$(a + ib) \cdot (u + iv) = (au - bv) + i(bu + av).$$

Show that

$$\dim_{\mathbb{R}} V = n \Longrightarrow \dim_{\mathbb{C}} V_{\mathbb{C}} = n.$$

Finally, show that $J \in \mathcal{L}(V \oplus V)$, given by

$$J(u, v) = (v, -u),$$

produces the same conplex structure on $V_{\mathbb{C}}$ as defined above.

REMARK. We call $V_{\mathbb{C}}$ the *complexification* of V.

1.4. Matrix representation of a linear transformation

We show how a linear transformation

$$T : V \longrightarrow W \tag{1.4.1}$$

has a representation as an $m \times n$ matrix, with respect to a basis $S = \{v_1, \dots, v_n\}$ of V and a basis $\Sigma = \{w_1, \dots, w_m\}$ of W. Namely, define a_{ij} by

$$Tv_j = \sum_{i=1}^{m} a_{ij} w_i, \quad 1 \le j \le n. \tag{1.4.2}$$

The matrix representation of T with respect to these bases is then

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}. \tag{1.4.3}$$

Note that the jth column of A consists of the coefficients of Tv_j, when this is written as a linear combination of $w_1, \dots, w_m$. Compare (1.2.22).

If we want to record the dependence on the bases S and Σ, we can write

$$A = \mathcal{M}_S^{\Sigma}(T). \tag{1.4.4}$$

Equivalently given the isomorphism $\mathcal{J}_S : \mathbb{F}^n \to V$ as in (1.3.2)–(1.3.3) (with n instead of k) and its counterpart $\mathcal{J}_\Sigma : \mathbb{F}^m \to W$, we have

$$A = \mathcal{M}_S^{\Sigma}(T) = \mathcal{J}_\Sigma^{-1} T \mathcal{J}_S : \mathbb{F}^n \to \mathbb{F}^m, \tag{1.4.5}$$

naturally identified with the matrix A as in (1.2.3)–(1.2.5).

The definition of matrix multiplication is set up precisely so that, if X is a vector space with basis $\Gamma = \{x_1, \dots x_k\}$ and $U : X \to V$ is linear, then $TU : X \to W$ has matrix representation

$$\mathcal{M}_\Gamma^{\Sigma}(TU) = AB, \quad B = \mathcal{M}_\Gamma^{S}(U). \tag{1.4.6}$$

Indeed, if we complement (1.4.5) with

$$B = \mathcal{J}_S^{-1} U \mathcal{J}_\Gamma = \mathcal{M}_\Gamma^{S}(U), \tag{1.4.7}$$

we have

$$AB = (\mathcal{J}_\Sigma^{-1} T \mathcal{J}_S)(\mathcal{J}_S^{-1} U \mathcal{J}_\Gamma) = \mathcal{J}_\Sigma^{-1}(TU)\mathcal{J}_\Gamma. \tag{1.4.8}$$

As for the representation of AB as a matrix product, see the discussion around (1.2.17)–(1.2.23).

For example, if

$$T : V \longrightarrow V, \tag{1.4.9}$$

and we use the basis S of V as above, we have an $n \times n$ matrix $\mathcal{M}_S^S(T)$. If we pick another basis $\widetilde{S} = \{\tilde{v}_1, \dots, \tilde{v}_n\}$ of V, it follows from (1.4.6) that

$$\mathcal{M}_{\widetilde{S}}^{\widetilde{S}}(T) = \mathcal{M}_S^{\widetilde{S}}(I)\mathcal{M}_S^S(T)\mathcal{M}_{\widetilde{S}}^S(I). \tag{1.4.10}$$

Here

$$\mathcal{M}_{\widetilde{S}}^S(I) = \mathcal{J}_S^{-1}\mathcal{J}_{\widetilde{S}} = C = (c_{ij}), \tag{1.4.11}$$

where

$$\tilde{v}_j = \sum_{i=1}^{n} c_{ij} v_i, \quad 1 \le j \le n, \tag{1.4.12}$$

and we see (via (1.4.6)) that

$$\mathcal{M}_S^{\widetilde{S}}(I) = \mathcal{J}_{\widetilde{S}}^{-1} \mathcal{J}_S = C^{-1}. \tag{1.4.13}$$

To rewrite (1.4.10), we can say that if A is the matrix representation of T with respect to the basis S and $\widetilde{A}$ the matrix representation of T with respect to the basis $\widetilde{S}$, then

$$\widetilde{A} = C^{-1} A C. \tag{1.4.14}$$

REMARK. We say that $n \times n$ matrices A and $\widetilde{A}$, related as in (1.4.14), are *similar*.

EXAMPLE. Consider the linear transformation

$$D : \mathcal{P}_2 \longrightarrow \mathcal{P}_2, \quad Df(x) = f'(x). \tag{1.4.15}$$

With respect to the basis

$$v_1 = 1, \quad v_2 = x, \quad v_3 = x^2, \tag{1.4.16}$$

D has the matrix representation

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}, \tag{1.4.17}$$

since $Dv_1 = 0,\ Dv_2 = v_1$, and $Dv_3 = 2v_2$. With respect to the basis

$$\tilde{v}_1 = 1, \quad \tilde{v}_2 = 1 + x, \quad \tilde{v}_3 = 1 + x + x^2, \tag{1.4.18}$$

D has the matrix representation

$$\widetilde{A} = \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}, \tag{1.4.19}$$

since $D\tilde{v}_1 = 0,\ D\tilde{v}_2 = \tilde{v}_1$, and $D\tilde{v}_3 = 1 + 2x = 2\tilde{v}_2 - \tilde{v}_1$. The reader is invited to verify (1.4.14) for this example.

Exercises

1. Consider $\mathcal{T} : \mathcal{P}_2 \to \mathcal{P}_2$, given by $\mathcal{T}p(x) = x^{-1}\int_0^x p(y)\,dy$. Compute the matrix representation B of $\mathcal{T}$ with respect to the basis (1.4.16). Compute AB and BA, with A given by (1.4.17).

2. In the setting of Exercise 1, compute $D\mathcal{T}$ and $\mathcal{T}D$ on $\mathcal{P}_2$ and compare their matrix representations, with respect to the basis (1.4.16), with AB and BA.

3. In the setting of Exercise 1, take $a \in \mathbb{R}$ and define

$$\mathcal{T}_a p(x) = \frac{1}{x-a}\int_a^x p(y)\,dy, \quad \mathcal{T}_a : \mathcal{P}_2 \longrightarrow \mathcal{P}_2. \tag{1.4.20}$$

Compute the matrix representation of $\mathcal{T}_a$ with respect to the basis (1.4.16).

4. Compute the matrix representation of $\mathcal{T}_a$, given by (1.4.20), with respect to the basis of $\mathcal{P}_2$ given in (1.4.18).

5. Let $A : \mathbb{C}^2 \to \mathbb{C}^2$ be given by

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

(with respect to the standard basis). Find a basis of $\mathbb{C}^2$ with respect to which the matrix representation of A is

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

6. Let $V = \{a\cos t + b\sin t : a, b \in \mathbb{C}\}$, and consider

$$D = \frac{d}{dt} : V \longrightarrow V.$$

Compute the matrix representation of D with respect to the basis $\{\cos t, \sin t\}$.

7. In the setting of Exercise 6, compute the matrix representation of D with respect to the basis $\{e^{it}, e^{-it}\}$. (See Exercise 4 of §1.3.)

1.5. Determinants and invertibility

Determinants arise in the study of inverting a matrix. To take the 2×2 case, solving for x and y the system

$$\begin{aligned} ax + by &= u, \\ cx + dy &= v \end{aligned} \tag{1.5.1}$$

can be done by multiplying these equations by d and b, respectively, and subtracting, and by multiplying them by c and a, respectively, and subtracting, yielding

$$\begin{aligned} (ad - bc)x &= du - bv, \\ (ad - bc)y &= av - cu. \end{aligned} \tag{1.5.2}$$

The factor on the left is

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc, \tag{1.5.3}$$

and solving (1.5.2) for x and y leads to

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Longrightarrow A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \tag{1.5.4}$$

provided $\det A \neq 0$.

We now consider determinants of $n \times n$ matrices. Let $M(n, \mathbb{F})$ denote the set of $n \times n$ matrices with entries in $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. We write

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} = (a_1, \dots, a_n), \tag{1.5.5}$$

where

$$a_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} \tag{1.5.6}$$

is the jth column of A. The determinant is defined as follows.

Proposition 1.5.1. *There is a unique function*

$$\vartheta : M(n, \mathbb{F}) \longrightarrow \mathbb{F}, \tag{1.5.7}$$

satisfying the following three properties:

(a) ϑ is linear in each column a_j of A,
(b) $\vartheta(\widetilde{A}) = -\vartheta(A)$ if $\widetilde{A}$ is obtained from A by interchanging two columns,
(c) $\vartheta(I) = 1$.

This defines the determinant:

$$\vartheta(A) = \det A. \tag{1.5.8}$$

If (c) is replaced by

(c′) $\vartheta(I) = r$,

then

$$\vartheta(A) = r \det A. \tag{1.5.9}$$

The proof will involve constructing an explicit formula for $\det A$ by following the rules (a)–(c). We start with the case $n = 3$. We have

$$\det A = \sum_{j=1}^{3} a_{j1} \det(e_j, a_2, a_3), \tag{1.5.10}$$

by applying (a) to the first column of A, $a_1 = \sum_j a_{j1} e_j$. Here and below, $\{e_j : 1 \le j \le n\}$ denotes the standard basis of $\mathbb{F}^n$, so e_j has a 1 in the jth slot and 0s elsewhere. Applying (a) to the second and third columns gives

$$\begin{aligned} \det A &= \sum_{j,k=1}^{3} a_{j1} a_{k2} \det(e_j, e_k, a_3) \\ &= \sum_{j,k,\ell=1}^{3} a_{j1} a_{k2} a_{\ell 3} \det(e_j, e_k, e_\ell). \end{aligned} \tag{1.5.11}$$

This is a sum of 27 terms, but most of them are 0. Note that rule (b) implies

$$\det B = 0 \quad \text{whenever} \quad B \quad \text{has two identical columns.} \tag{1.5.12}$$

Hence $\det(e_j, e_k, e_\ell) = 0$ unless j, k, and ℓ are distinct, that is, unless (j, k, ℓ) is a *permutation* of $(1, 2, 3)$. Now rule (c) says

$$\det(e_1, e_2, e_3) = 1, \tag{1.5.13}$$

and we see from rule (b) that $\det(e_j, e_k, e_\ell) = 1$ if one can convert (e_j, e_k, e_ℓ) to (e_1, e_2, e_3) by an even number of column interchanges, and $\det(e_j, e_k, e_\ell) = -1$ if it takes an odd number of interchanges. Explicitly,

$$\begin{aligned} &\det(e_1, e_2, e_3) = 1, \quad \det(e_1, e_3, e_2) = -1, \\ &\det(e_2, e_3, e_1) = 1, \quad \det(e_2, e_1, e_3) = -1, \\ &\det(e_3, e_1, e_2) = 1, \quad \det(e_3, e_2, e_1) = -1. \end{aligned} \tag{1.5.14}$$

Consequently (1.5.11) yields

$$\begin{aligned} \det A = {} & a_{11}a_{22}a_{33} - a_{11}a_{32}a_{23} \\ & + a_{21}a_{32}a_{13} - a_{21}a_{12}a_{33} \\ & + a_{31}a_{12}a_{23} - a_{31}a_{22}a_{13}. \end{aligned} \tag{1.5.15}$$

Note that the second indices occur in $(1, 2, 3)$ order in each product. We can rearrange these products so that the *first* indices occur in $(1, 2, 3)$ order:

$$\begin{aligned} \det A = {} & a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} \\ & + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} \\ & + a_{12}a_{23}a_{31} - a_{13}a_{22}a_{31}. \end{aligned} \tag{1.5.16}$$

In connection with (1.5.16), we mention one convenient method to compute 3×3 determinants. Given $A \in M(3, \mathbb{F})$, form a 3×5 rectangular matrix by copying the first two columns of A on the right. The products in (1.5.16) with plus signs

are the products of each of the three downward sloping diagonals marked in bold below:

$$\begin{pmatrix} \mathbf{a_{11}} & \mathbf{a_{12}} & \mathbf{a_{13}} & a_{11} & a_{12} \\ a_{21} & \mathbf{a_{22}} & \mathbf{a_{23}} & \mathbf{a_{21}} & a_{22} \\ a_{31} & a_{32} & \mathbf{a_{33}} & \mathbf{a_{31}} & \mathbf{a_{32}} \end{pmatrix}. \tag{1.5.17}$$

The products in (1.5.16) with a minus sign are the products of each of the three upward sloping diagonals marked in bold below:

$$\begin{pmatrix} a_{11} & a_{12} & \mathbf{a_{13}} & \mathbf{a_{11}} & \mathbf{a_{12}} \\ a_{21} & \mathbf{a_{22}} & \mathbf{a_{23}} & \mathbf{a_{21}} & a_{22} \\ \mathbf{a_{31}} & \mathbf{a_{32}} & \mathbf{a_{33}} & a_{31} & a_{32} \end{pmatrix}. \tag{1.5.18}$$

This method can be regarded as an analogue of the method of computing 2×2 determinants given in (1.5.3). However, there is not a straightforward extension of this method to larger determinants.

We now tackle the case of general n. Parallel to (1.5.10)–(1.5.11), we have

$$\begin{aligned} \det A &= \sum_j a_{j1} \det(e_j, a_2, \dots, a_n) = \cdots \\ &= \sum_{j_1,\dots,j_n} a_{j_1 1} \cdots a_{j_n n} \det(e_{j_1}, \dots e_{j_n}), \end{aligned} \tag{1.5.19}$$

by applying rule (a) to each of the n columns of A. As before, (1.5.12) implies $\det(e_{j_1}, \dots, e_{j_n}) = 0$ unless $(j_1, \dots, j_n)$ are all distinct, that is, unless $(j_1, \dots, j_n)$ is a permutation of the set $(1, 2, \dots, n)$. We set

$$S_n = \text{ set of permutations of } (1, 2, \dots, n). \tag{1.5.20}$$

That is, S_n consists of elements σ, mapping the set $\{1, \dots, n\}$ to itself,

$$\sigma : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}, \tag{1.5.21}$$

that are one-to-one and onto. We can compose two such permutations, obtaining the product $\sigma\tau \in S_n$, given σ and τ in S_n. A permutation that interchanges just two elements of $\{1, \dots, n\}$, say j and k ($j \neq k$), is called a *transposition*, and labeled (jk). It is easy to see that each permutation of $\{1, \dots, n\}$ can be achieved by successively transposing pairs of elements of this set. That is, each element $\sigma \in S_n$ is a product of transpositions. We claim that

$$\det(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = (\operatorname{sgn}\sigma) \det(e_1, \dots, e_n) = \operatorname{sgn}\sigma, \tag{1.5.22}$$

where

$$\begin{aligned} \operatorname{sgn}\sigma = \ & 1 \quad \text{if } \sigma \text{ is a product of an even number of transpositions,} \\ & -1 \quad \text{if } \sigma \text{ is a product of an odd number of transpositions.} \end{aligned} \tag{1.5.23}$$

In fact, the first identity in (1.5.22) follows from rule (b) and the second identity from rule (c).

There is one point to be checked here. Namely, we claim that a given $\sigma \in S_n$ cannot simultaneously be written as a product of an even number of transpositions and an odd number of transpositions. If σ could be so written, $\operatorname{sgn}\sigma$ would not be well defined, and it would be impossible to satisfy condition (b), so Proposition

1.5.1 would fail. One neat way to see that $\operatorname{sgn}\sigma$ is well defined is the following. Let $\sigma \in S_n$ act on functions of n variables by

$$(\sigma f)(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)}). \tag{1.5.24}$$

It is readily verified that if also $\tau \in S_n$,

$$g = \sigma f \Longrightarrow \tau g = (\tau\sigma) f. \tag{1.5.25}$$

Now, let P be the polynomial

$$P(x_1, \dots, x_n) = \prod_{1 \le j < k \le n} (x_j - x_k). \tag{1.5.26}$$

One readily has

$$(\sigma P)(x) = -P(x), \quad \text{whenever} \quad \sigma \quad \text{is a transposition}, \tag{1.5.27}$$

and hence, by (1.5.25),

$$(\sigma P)(x) = (\operatorname{sgn}\sigma) P(x), \quad \forall\, \sigma \in S_n, \tag{1.5.28}$$

and $\operatorname{sgn}\sigma$ is well defined.

The proof of (1.5.22) is complete, and substitution into (1.5.19) yields the formula

$$\det A = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n}. \tag{1.5.29}$$

It is routine to check that this satisfies the properties (a)–(c). Regarding (b), note that if $\vartheta(A)$ denotes the right side of (1.5.29) and $\widetilde{A}$ is obtained from A by applying a permutation τ to the columns of A, so $\widetilde{A} = (a_{\tau(1)}, \dots, a_{\tau(n)})$, then

$$\begin{aligned} \vartheta(\widetilde{A}) &= \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma) a_{\sigma(1)\tau(1)} \cdots a_{\sigma(n)\tau(n)} \\ &= \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma) a_{\sigma\tau^{-1}(1)1} \cdots a_{\sigma\tau^{-1}(n)n} \\ &= \sum_{\omega \in S_n} (\operatorname{sgn}\omega\tau) a_{\omega(1)1} \cdots a_{\omega(n)n} \\ &= (\operatorname{sgn}\tau)\vartheta(A), \end{aligned} \tag{1.5.30}$$

the last identity because

$$\operatorname{sgn}\omega\tau = (\operatorname{sgn}\omega)(\operatorname{sgn}\tau), \quad \forall\, \omega, \tau \in S_n. \tag{1.5.31}$$

As for the final part of Proposition 1.5.1, if (c) is replaced by (c′), then (1.5.22) is replaced by

$$\vartheta(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = r(\operatorname{sgn}\sigma), \tag{1.5.32}$$

and (1.5.9) follows.

Remark. Some authors take (1.5.29) as a definition of the determinant. Our perspective is that, while (1.5.29) is a useful *formula* for the determinant, it is a bad *definition*, indeed one that has perhaps led to a bit of fear and loathing among math students.

REMARK. Here is another formula for $\operatorname{sgn}\sigma$, which the reader is invited to verify. If $\sigma \in S_n$,

$$\operatorname{sgn}\sigma = (-1)^{\kappa(\sigma)}, \tag{1.5.33}$$

where

$$\begin{aligned}\kappa(\sigma) = {} & \text{number of pairs } (j,k) \text{ such that } 1 \le j < k \le n, \\ & \text{but } \sigma(j) > \sigma(k).\end{aligned} \tag{1.5.34}$$

Note that

$$a_{\sigma(1)1} \cdots a_{\sigma(n)n} = a_{1\tau(1)} \cdots a_{n\tau(n)}, \quad \text{with } \tau = \sigma^{-1}, \tag{1.5.35}$$

and $\operatorname{sgn}\sigma = \operatorname{sgn}\sigma^{-1}$, so, parallel to (1.5.16), we also have

$$\det A = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}. \tag{1.5.36}$$

Comparison with (1.5.29) gives

$$\det A = \det A^t, \tag{1.5.37}$$

where $A = (a_{jk}) \Rightarrow A^t = (a_{kj})$. Note that the jth column of A^t has the same entries as the jth row of A. In light of this, we have:

Corollary 1.5.2. *In Proposition 1.5.1, one can replace "columns" by "rows."*

The following is a key property of the determinant.

Proposition 1.5.3. *Given A and B in $M(n,\mathbb{F})$,*

$$\det(AB) = (\det A)(\det B). \tag{1.5.38}$$

Proof. For fixed A, apply Proposition 1.5.1 to

$$\vartheta_1(B) = \det(AB). \tag{1.5.39}$$

If $B = (b_1, \dots, b_n)$, with jth column b_j, then

$$AB = (Ab_1, \dots, Ab_n). \tag{1.5.40}$$

Clearly rule (a) holds for ϑ_1. Also, if $\widetilde{B} = (b_{\sigma(1)}, \dots, b_{\sigma(n)})$ is obtained from B by permuting its columns, then $A\widetilde{B}$ has columns $(Ab_{\sigma(1)}, \dots, Ab_{\sigma(n)})$, obtained by permuting the columns of AB in the same fashion. Hence rule (b) holds for ϑ_1. Finally, rule (c′) holds for ϑ_1, with $r = \det A$, and (1.5.38) follows. □

Corollary 1.5.4. *If $A \in M(n,\mathbb{F})$ is invertible, then $\det A \neq 0$.*

Proof. If A is invertible, there exists $B \in M(n,\mathbb{F})$ such that $AB = I$. Then, by (1.5.38), $(\det A)(\det B) = 1$, so $\det A \neq 0$. □

The converse of Corollary 1.5.4 also holds. Before proving it, it is convenient to show that the determinant is invariant under a certain class of column operations, given as follows.

Proposition 1.5.5. *If $\widetilde{A}$ is obtained from $A = (a_1, \dots, a_n) \in M(n, \mathbb{F})$ by adding ca_ℓ to a_k for some $c \in \mathbb{F}$, $\ell \neq k$, then*

$$\det \widetilde{A} = \det A. \tag{1.5.41}$$

Proof. By rule (a), $\det \widetilde{A} = \det A + c \det A^b$, where A^b is obtained from A by replacing the column a_k by a_ℓ. Hence A^b has two identical columns, so $\det A^b = 0$, and (1.5.41) holds. □

We now extend Corollary 1.5.4.

Proposition 1.5.6. *If $A \in M(n, \mathbb{F})$, then A is invertible if and only if $\det A \neq 0$.*

Proof. We have half of this from Corollary 1.5.4. To finish, assume A is not invertible. As seen in §1.3, this implies the columns $a_1, \dots, a_n$ of A are linearly dependent. Hence, for some k,

$$a_k + \sum_{\ell \neq k} c_\ell a_\ell = 0, \tag{1.5.42}$$

with $c_\ell \in \mathbb{F}$. Now we can apply Proposition 1.5.5 to obtain $\det A = \det \widetilde{A}$, where $\widetilde{A}$ is obtained by adding $\sum c_\ell a_\ell$ to a_k. But then the kth column of $\widetilde{A}$ is 0, so $\det A = \det \widetilde{A} = 0$. This finishes the proof of Proposition 1.5.6. □

Having seen the usefulness of the operation we called a column operation in Proposition 1.5.5, let us pursue this, and list the following:

Column operations. For $A \in M(n, \mathbb{F})$, these include

$$\begin{aligned} &\text{interchanging two columns of } A, \\ &\text{factoring a scalar } c \text{ out of a column of } A, \\ &\text{adding } c \text{ times the } \ell\text{th column of } A \\ &\qquad \text{to the } k\text{th column of } A \ (\ell \neq k). \end{aligned} \tag{1.5.43}$$

Of these operations, the first changes the sign of the determinant, by property (b) of Proposition 1.5.1, the second factors a c out of the determinant, by property (a) of Proposition 1.5.1, and the third leaves the determinant unchanged, by Proposition 1.5.5. In light of Corollary 1.5.2, the same can be said about the following:

Row operations. For $A \in M(n, \mathbb{F})$, these include

$$\begin{aligned} &\text{interchanging two rows of } A, \\ &\text{factoring a scalar } c \text{ out of a row of } A, \\ &\text{adding } c \text{ times the } \ell\text{th row of } A \text{ to the } k\text{th row of } A \ (\ell \neq k). \end{aligned} \tag{1.5.44}$$

We illustrate the application of row operations to the following 3×3 determinant:

$$\begin{aligned}\det \begin{pmatrix} 0 & 3 & 5 \\ 2 & 4 & 6 \\ 3 & 5 & 8 \end{pmatrix} &= -\det \begin{pmatrix} 2 & 4 & 6 \\ 0 & 3 & 5 \\ 3 & 5 & 8 \end{pmatrix} \\ &= -2 \det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 3 & 5 \\ 3 & 5 & 8 \end{pmatrix} \\ &= -2 \det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 3 & 5 \\ 0 & -1 & -1 \end{pmatrix}. \end{aligned} \tag{1.5.45}$$

From here, one can multiply the bottom row by 3 and add it to the middle row, to get

$$-2 \det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 2 \\ 0 & -1 & -1 \end{pmatrix} = -2 \det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}, \tag{1.5.46}$$

where for the last identity we have interchanged the last two rows and multiplied one by -1. The last matrix is an upper triangular matrix, and its determinant is equal to the product of its diagonal elements, thanks to the following result.

Proposition 1.5.7. *Assume $A \in M(n, \mathbb{F})$ is upper triangular, i.e., A has the form* (1.5.5) *with*

$$a_{jk} = 0 \quad \text{for} \quad j > k. \tag{1.5.47}$$

Then $\det A$ *is the product of the diagonal entries, i.e.,*

$$\det A = a_{11} a_{22} \cdots a_{nn}. \tag{1.5.48}$$

Proof. This follows from the formula (1.5.29) for $\det A$, involving a sum over $\sigma \in S_n$. The key observation is that if σ is a permutation of $\{1, \dots, n\}$, then

$$\text{either } \sigma(j) = j \text{ for all } j, \text{ or } \sigma(j) > j \text{ for some } j. \tag{1.5.49}$$

Hence, if (1.5.47) holds, every term in the sum (1.5.29) vanishes except the term yielding the right side of (1.5.48). □

Remark. A second proof of Proposition 1.5.7 is indicated in Exercise 11 below.

Row operations and column operations have further applications, including constructing the inverse of an invertible $n \times n$ matrix, constructing a basis of the range $\mathcal{R}(A)$, via column operations, and constructing a basis of the null space $\mathcal{N}(A)$, via row operations, given $A \in M(m \times n, \mathbb{F})$. Material on this appears in §1.6.

Further useful facts about determinants arise in the following exercises.

Exercises

1. Compute the determinants of the following matrices.

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ -1 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}, \quad C = \begin{pmatrix} 2 & 1 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 3 \end{pmatrix}.$$

2. Given the matrices A, B, and C in Exercise 1, compute

$$AB, \quad AC, \quad \det(AB), \quad \det(AC).$$

Compare these determinant calculations with the identities

$$\det(AB) = (\det A)(\det B), \quad \det(AC) = (\det A)(\det C),$$

using Proposition 1.5.3.

3. Which matrices in Exercise 1 are invertible?

4. Use row operations to compute the determinant of

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

5. Use column operations to compute the determinant of M in Exercise 4.

6. Use a combination of row and column operations to compute $\det M$.

7. Show that

$$\det \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \det \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \det A_{11} \tag{1.5.50}$$

where $A_{11} = (a_{jk})_{2 \le j,k \le n}$.

Hint. Do the first identity using Proposition 1.5.5. Then exploit uniqueness for $\det$ on $M(n-1, \mathbb{F})$.

8. Deduce that $\det(e_j, a_2, \ldots, a_n) = (-1)^{j-1} \det A_{1j}$ where A_{kj} is formed by deleting the kth column and the jth row from A.

9. Deduce from the first sum in (1.5.19) that

$$\det A = \sum_{j=1}^{n} (-1)^{j-1} a_{j1} \det A_{1j}. \tag{1.5.51}$$

More generally, for any $k \in \{1, \dots, n\}$,

$$\det A = \sum_{j=1}^{n} (-1)^{j-k} a_{jk} \det A_{kj}. \tag{1.5.52}$$

This is called an expansion of $\det A$ by minors, down the kth column.

10. Let $c_{kj} = (-1)^{j-k} \det A_{kj}$. Show that

$$\sum_{j=1}^{n} a_{j\ell} c_{kj} = 0, \quad \text{if } \ \ell \neq k. \tag{1.5.53}$$

Deduce from this and (1.5.52) that $C = (c_{jk})$ satisfies

$$CA = (\det A)I. \tag{1.5.54}$$

Hint. Reason as in Exercises 7–9 that the left side of (1.5.53) is equal to

$$\det (a_1, \dots, a_\ell, \dots, a_\ell, \dots, a_n),$$

with a_ℓ in the kth column as well as in the ℓth column. The identity (1.5.54) is known as Cramer's formula. Note how this generalizes (1.5.4).

11. Give a second proof of Proposition 1.5.7, i.e.,

$$\det \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & a_{22} & \cdots & a_{2n} \\ & & \ddots & \vdots \\ & & & a_{nn} \end{pmatrix} = a_{11} a_{22} \cdots a_{nn}, \tag{1.5.55}$$

using (1.5.50) and induction.

The next two exercises deal with the determinant of a linear transformation. Let V be an n-dimensional vector space, and

$$T : V \longrightarrow V \tag{1.5.56}$$

a linear transformation. We would like to define

$$\det T = \det A, \tag{1.5.57}$$

where $A = \mathcal{M}_S^S(T)$ for some basis $S = \{v_1, \dots, v_n\}$ of V.

12. Suppose $\widetilde{S} = \{\tilde{v}_1, \dots, \tilde{v}_n\}$ is another basis of V. Show that

$$\det A = \det \widetilde{A}, \tag{1.5.58}$$

where $\widetilde{A} = \mathcal{M}_{\widetilde{S}}^{\widetilde{S}}(T)$. Hence (1.5.57) defines $\det T$, independently of the choice of basis of V.
Hint. Use (1.4.14) and (1.5.38).

13. If also $U \in \mathcal{L}(V)$, show that

$$\det(UT) = (\det U)(\det T).$$

Denseness of $G\ell(n,\mathbb{F})$ in $M(n,\mathbb{F})$

Given $A \in M(n,\mathbb{F})$, we say A belongs to $G\ell(n,\mathbb{F})$ provided A is invertible. By Proposition 1.5.6, this invertibility holds if and only if $\det A \neq 0$.

We say a sequence A_ν of matrices in $M(n,\mathbb{F})$ converges to A ($A_\nu \to A$) if and only if convergence holds for each entry: $(a_\nu)_{jk} \to a_{jk}$, for all $j,k \in \{1,\dots,n\}$. The following is a useful result.

Proposition 1.5.8. *For each n, $G\ell(n,\mathbb{F})$ is dense in $M(n,\mathbb{F})$. That is, given $A \in M(n,\mathbb{F})$, there exist $A_\nu \in G\ell(n,\mathbb{F})$ such that $A_\nu \to A$.*

The following steps justify this.

14. Show that $\det : M(n,\mathbb{F}) \to \mathbb{F}$ is continuous, i.e., $A_\nu \to A$ implies that $\det(A_\nu) \to \det A$.
Hint. $\det A$ is a polynomial in the entries of A.

15. Show that if $A \in M(n,\mathbb{F})$, $\delta > 0$, and B is not invertible for all $B \in M(n,\mathbb{F})$ such that $|b_{jk} - a_{jk}| < \delta$, for all j and k, then $\det : M(n,\mathbb{F}) \to \mathbb{F}$ vanishes for all such B.

16. Let $p : \mathbb{F}^k \to \mathbb{F}$ be a polynomial. Suppose there exists $w \in \mathbb{F}$ and $\delta > 0$ such that

$$z \in \mathbb{F}^k,\ |w_j - z_j| < \delta\ \forall\, j \in \{1,\dots,k\} \Longrightarrow p(z) = 0.$$

Show that $p(z)$ is identically zero, for all $z \in \mathbb{F}^k$.
Hint. Take $q(z) = p(w+z)$, so $q(z) = 0$ provided $|z_j| < \delta$ for all j. Show that this implies all the coefficients of q vanish.

17. Using the results of Exercises 14–16, prove Proposition 1.5.8.

The Vandermonde determinant

For $n \geq 2$, the Vandermonde determinant is defined by

$$V_n(x_1, \dots, x_n) = \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{pmatrix}. \tag{1.5.59}$$

We claim that

$$V_n(x_1, \dots, x_n) = \prod_{1 \leq j < k \leq n} (x_k - x_j), \tag{1.5.60}$$

which, up to a sign, coincides with (1.5.26). We can prove this by induction on n, starting at $n = 2$, where $V_2(x_1, x_2) = x_2 - x_1$ is clear. To do the induction step, it is convenient to change notation, and consider

$$P(z) = V_n(a_1, \dots, a_{n-1}, z) = \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & z \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & z^{n-1} \end{pmatrix}, \tag{1.5.61}$$

which is a polynomial in z of degree $n - 1$. Clearly $P(a_j) = 0$ for each j, so

$$P(z) = A_{n-1} \prod_{1 \leq j < n} (z - a_j), \tag{1.5.62}$$

where A_{n-1} is the coefficient of z^{n-1} in $P(z)$. Expansion of the determinant in (1.5.61) by minors, down the nth column (cf. Exercise 9) yields

$$A_{n-1} = V_{n-1}(a_1, \dots, a_{n-1}). \tag{1.5.63}$$

Reversion to the notation of (1.5.59) then gives

$$V_n(x_1, \dots, x_n) = V_{n-1}(x_1, \dots, x_{n-1}) \prod_{1 \leq j < n} (x_n - x_j), \tag{1.5.64}$$

which readily yields the inductive proof of (1.5.60).

Exercise

1. Use the Lagrange interpolation formula, discussed in Proposition 1.2.1, to derive a formula for the inverse of the Vandermonde matrix, whose determinant is defined in (1.5.59), or equivalently of

$$A = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{pmatrix}, \tag{1.5.65}$$

given $x_1, \dots, x_n$ distinct.
Hint. The columns of A have the form

$$\begin{pmatrix} p_\ell(x_1) \\ \vdots \\ p_\ell(x_n) \end{pmatrix}, \quad p_\ell(x) = x^\ell. \tag{1.5.66}$$

Relate this to the transformation E_S, given by (1.2.28), with n replaced by $n-1$ and with $S = \{x_1, \dots, x_n\}$. The column in (1.5.66) is $E_S p_\ell$.

1.6. Applications of row reduction and column reduction

In §1.5 we introduced row operations and column operations on an $n \times n$ matrix, and examined their effect on determinants. Here we explore their use in providing further important information on matrices. We also expand the scope of these operations, to $m \times n$ matrices.

Let $A \in M(m \times n, \mathbb{F})$ be as in (1.2.5),

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}, \quad A : \mathbb{F}^n \to \mathbb{F}^m. \tag{1.6.1}$$

It will be useful to supplement the representation of A as an array of columns,

$$A = (a_1, \dots, a_n), \quad a_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}, \tag{1.6.2}$$

by a representation as an array of rows,

$$A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}, \quad \alpha_j = (a_{j1}, \dots, a_{jn}). \tag{1.6.3}$$

Taking a cue from (1.5.44), we define the following row operations,

$$\rho_\sigma, \mu_c, \varepsilon_{jk\gamma} : M(m \times n, \mathbb{F}) \longrightarrow M(m \times n, \mathbb{F}). \tag{1.6.4}$$

First,

$$\rho_\sigma \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = \begin{pmatrix} \alpha_{\sigma(1)} \\ \vdots \\ \alpha_{\sigma(m)} \end{pmatrix}, \quad \sigma \in S_m. \tag{1.6.5}$$

Next,

$$\mu_c \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = \begin{pmatrix} c_1\alpha_1 \\ \vdots \\ c_m\alpha_m \end{pmatrix}, \quad c = (c_1, \dots, c_m), \text{ each } c_j \neq 0. \tag{1.6.6}$$

Finally,

$$\varepsilon_{jk\gamma} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_j \\ \vdots \\ \alpha_m \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_j - \gamma\alpha_k \\ \vdots \\ \alpha_m \end{pmatrix}, \quad j \neq k, \ \gamma \in \mathbb{F}. \tag{1.6.7}$$

We note that all these transformations are invertible, with inverses

$$\rho_\sigma^{-1} = \rho_{\sigma^{-1}}, \quad \mu_c^{-1} = \mu_{c^{-1}}, \quad \varepsilon_{jk\gamma}^{-1} = \varepsilon_{jk,-\gamma}, \tag{1.6.8}$$

where $c^{-1} = (c_1^{-1}, \dots, c_m^{-1})$.

To illustrate the operations introduced in (1.6.4)–(1.6.7), we take

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad \sigma(1) = 2,\ \sigma(2) = 1, \quad c = (2, -1), \quad jk\gamma = 121, \tag{1.6.9}$$

obtaining

$$\rho_\sigma(A) = \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}, \quad \mu_c(A) = \begin{pmatrix} 2 & 4 \\ -3 & -4 \end{pmatrix}, \quad \varepsilon_{121}(A) = \begin{pmatrix} 4 & 6 \\ 3 & 4 \end{pmatrix}. \tag{1.6.10}$$

An important observation is that these row can be presented as left multiplication by $m \times m$ matrices,

$$\rho_\sigma(A) = P_\sigma A, \quad \mu_c(A) = M_c A, \quad \varepsilon_{jk\gamma}(A) = E_{jk\gamma} A, \tag{1.6.11}$$

where $P_\sigma, M_c, E_{jk\gamma} \in M(m, \mathbb{F})$ are defined by

$$P_\sigma \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = \begin{pmatrix} v_{\sigma(1)} \\ \vdots \\ v_{\sigma(m)} \end{pmatrix} \quad M_c \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = \begin{pmatrix} c_1 v_1 \\ \vdots \\ c_m v_m \end{pmatrix},$$

$$E_{jk\gamma} \begin{pmatrix} v_1 \\ \vdots \\ v_j \\ \vdots \\ v_m \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_j - \gamma v_k \\ \vdots \\ v_m \end{pmatrix}, \tag{1.6.12}$$

with $v = (v_1, \dots, v_m)^t \in \mathbb{F}^m$. To illustrate what these matrices are when $m = 2$ and σ, c, and (j, k, γ) are as in (1.6.9), we then have

$$P_\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad M_c = \begin{pmatrix} 2 & \\ & -1 \end{pmatrix}, \quad E_{121} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}. \tag{1.6.13}$$

Returning to generalities, parallel to (1.6.8), we have

$$P_\sigma^{-1} = P_{\sigma^{-1}}, \quad M_c^{-1} = M_{c^{-1}}, \quad E_{jk\gamma}^{-1} = E_{jk,-\gamma}. \tag{1.6.14}$$

If $\widetilde{A} \in M(m \times n, \mathbb{F})$ is obtained from $A \in M(m \times n, \mathbb{F})$ by a sequence of operations of the form (1.6.4), we say that $\widetilde{A}$ is obtained from A by a sequence of row operations. Since the $m \times m$ matrices P_σ, M_c, and $E_{jk\gamma}$ in (1.6.11)–(1.6.12) are all invertible, it follows that all the matrices $\rho_\sigma(A)$, $\mu_c(A)$, and $\varepsilon_{jk\gamma}(A)$ have the same null space, $\mathcal{N}(A)$. This leads to the following.

Proposition 1.6.1. *Applying a sequence of row operations to an $m \times n$ matrix does not alter its null space.*

We have a parallel set of column operations,

$$\tilde{\rho}_\sigma, \tilde{\mu}_c, \tilde{\varepsilon}_{jk\gamma} : M(m \times n, \mathbb{F}) \longrightarrow M(m \times n, \mathbb{F}), \tag{1.6.15}$$

given by

$$\begin{aligned} &\tilde{\rho}_\sigma(A) = (a_{\sigma(1)}, \dots, a_{\sigma(m)}), \quad \sigma \in S_n, \\ &\tilde{\mu}_c(A) = (c_1 a_1, \dots, c_n a_n), \quad c = (c_1, \dots, c_n), \text{ all } c_j \neq 0, \\ &\tilde{\varepsilon}_{jk\gamma}(a_1, \dots, a_j, \dots, a_n) = (a_1, \dots, a_j - \gamma a_k, \dots, a_n), \quad j \neq k. \end{aligned} \tag{1.6.16}$$

Note that

$$\tilde{\rho}_\sigma(A) = \rho_\sigma(A^t)^t, \quad \tilde{\mu}_c(A) = \mu_c(A^t)^t, \quad \tilde{\varepsilon}_{jk\gamma}(A) = \varepsilon_{jk\gamma}(A^t)^t. \tag{1.6.17}$$

Consequently,

$$\tilde{\rho}_\sigma(A) = AP_\sigma^t, \quad \tilde{\mu}_c(A) = AM_c^t, \quad \tilde{\varepsilon}_{jk\gamma}(A) = AE_{jk\gamma}^t, \tag{1.6.18}$$

with $P_\sigma^t, M_c^t, E_{jk\gamma}^t \in M(n, \mathbb{F})$, all invertible. It follows that all the matrices in (1.6.18) have the same range, $\mathcal{R}(A)$, so we have the following counterpart to Proposition 1.6.1.

Proposition 1.6.2. *Applying a sequence of column operations to an $m \times n$ matrix does not alter its range.*

To utilize Propositions 1.6.1–1.6.2, we want to apply a sequence of row operations (respectively, a sequence of column operations) that transform a given matrix A into one that has a simpler form. When this is done, we say that we are applying *row reduction* (respectively, *column reduction*) to A. Here is one basic class of matrices amenable to such reductions.

Proposition 1.6.3. *Let $A \in M(n, \mathbb{F})$ be invertible. Then one can apply a sequence of row operations to A that yield the $n \times n$ identity matrix I. Similarly, one can apply a sequence of column operations to A that yield I.*

Proof. Since A and A^t are simultaneously invertible, it suffices to deal with column operations. As seen in §1.3, A is invertible if and only if its columns $a_1, \dots, a_n$ form a basis of $\mathbb{F}^n$. Thus we can write the first standard basis element e_1 of $\mathbb{F}^n$ as a linear combination,

$$e_1 = c_{11}a_1 + \cdots + c_{1n}a_n.$$

If $c_{11} \neq 0$, we can apply a sequence of column operations of the form $\tilde{\varepsilon}_{1k\gamma}$ to turn the first column into be_1, for some $b \neq 0$, and then apply a column operation to change b to 1. If $c_{11} = 0$ but $c_{1k} \neq 0$, one can apply a column operation of the form $\tilde{\rho}_\sigma$ to interchange a_1 and a_k and proceed as before. Repeating such steps next leads to putting e_2 in the second column, and ultimately leads to I.

The corresponding passage from A to I via row operations is done similarly. □

A little later we describe a more "algorithmic" approach to applying row reductions, in the more general setting of $m \times n$ matrices.

Gaussian elimination

The following is an important application of row reduction to the computation of matrix inverses.

Proposition 1.6.4. *Let $A \in M(n, \mathbb{F})$ be invertible, and apply a sequence of row operations to A to obtain the identity matrix I. Then applying the same sequence of row operations to I yields A^{-1}.*

Proof. Say you apply k row operations to A to get I. Applying the jth such row operation amounts to applying a left multiplication by one of the matrices given in (1.6.12) (here $m = n$); call it S_j. In other words,

$$I = S_k \cdots S_1 A. \tag{1.6.19}$$

Consequently,

$$S_k \cdots S_1 = A^{-1}, \tag{1.6.20}$$

and we have the proposition. □

EXAMPLE. We take a 2×2 matrix A, write A and I side by side, and perform the same sequence of row operations on each of these two matrices, obtaining finally I and A^{-1} side by side.

$$\begin{aligned} A = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \qquad & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad & \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad & \begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix} = A^{-1}. \end{aligned} \tag{1.6.21}$$

REMARK. This method of constructing A^{-1} is called the method of *Gaussian elimination*. The method of Gaussian elimination is much more efficient than the use of Cramer's formula (1.5.54) as a tool for computing matrix inverses, though Cramer's formula is a useful tool for understanding the nature of the matrix inverse.

A related issue is that, for computing determinants of $n \times n$ matrices, for $n \geq 4$, it is computationally advantageous to utilize a sequence of row and/or column operations, rather than using the formula (1.5.29), which contains $n!$ terms.

Determinants and volumes

Here we will use Proposition 1.6.3 and its corollary (1.6.19) to derive the following identity relating determinants and volumes.

Proposition 1.6.5. *Let $\Omega \subset \mathbb{R}^n$ be a bounded open set, and let $A \in M(n, \mathbb{R})$ be invertible. Then*

$$\operatorname{Vol}(A(\Omega)) = |\det A| \operatorname{Vol}(\Omega). \tag{1.6.22}$$

To say Ω is open is to say that, if $x_0 \in \Omega$, there exists $\varepsilon > 0$ such that $|x - x_0| < \varepsilon \Rightarrow x \in \Omega$. The set $A(\Omega) = \{Ax : x \in \Omega\}$ is the image of Ω under the map $A : \mathbb{R}^n \to \mathbb{R}^n$. It is also an open subset of $\mathbb{R}^n$.

To derive this result, we use (1.6.19) to write

$$A = T_1 \cdots T_k, \quad T_j = S_j^{-1}. \tag{1.6.23}$$

Each $T_j \in M(n, \mathbb{R})$ is a matrix of the form listed in (1.6.12), with $m = n$, i.e.,

$$\begin{aligned} P_\sigma(x_1, \dots, x_n)^t &= (x_{\sigma(1)}, \dots, x_{\sigma(n)})^t, \\ M_c(x_1, \dots, x_n)^t &= (c_1 x_1, \dots, c_n x_n)^t, \\ E_{jk\gamma}(x_1, \dots, x_n)^t &= (x_1, \dots, x_j - \gamma x_k, \dots, x_n), \end{aligned} \tag{1.6.24}$$

with $x = (x_1, \dots, x_n)^t \in \mathbb{R}^n$, $\sigma \in S_n$, and $c_j \in \mathbb{R} \setminus 0$. We have

$$\det P_\sigma = \operatorname{sgn}(\sigma) = \pm 1, \quad \det M_c = c_1 \cdots c_n, \quad \det E_{jk\gamma} = 1. \tag{1.6.25}$$

By comparison, each transformation in (1.6.24) maps bounded open sets to bounded open sets, and, if Ω is such a set, we have

$$\begin{aligned} \operatorname{Vol}(P_\sigma(\Omega)) &= \operatorname{Vol}(\Omega), \\ \operatorname{Vol}(M_c(\Omega)) &= |c_1 \cdots c_n| \operatorname{Vol}(\Omega), \\ \operatorname{Vol}(E_{jk\gamma}(\Omega)) &= \operatorname{Vol}(\Omega). \end{aligned} \tag{1.6.26}$$

Comparing (1.6.25) and (1.6.26), and using the fact that

$$\det A = (\det T_1) \cdots (\det T_k), \tag{1.6.27}$$

we have (1.6.22).

We have called the argument above a "derivation" of (1.6.22), rather than a proof. We have not given a definition of $\operatorname{Vol}(\Omega)$, and indeed such a task is rightly part of a treatment of multivariable calculus. An approach to such a definition would be to partition Ω into a countable collection of "cells," i.e., rectangular solids of the form $R = I_1 \times \cdots \times I_n$, a product of bounded intervals $I_\nu \subset \mathbb{R}$, such that two such cells would intersect only along faces. We take the volume of R to be the product of the lengths of the intervals I_ν. Then we set $\operatorname{Vol}(\Omega)$ to be the countable sum of the volumes of the cells in such a partition. One faces the task of showing that $\operatorname{Vol}(\Omega)$ is then well defined, independently of the choice of such a partition.

Of the transformations listed in (1.6.24), the first two preserve the class of rectangular solids, leading to the first two identities in (1.6.26). Such actions (with $n = 2$) are illustrated in Figure 1.6.1, with σ interchanging 1 and 2, and with $c = (2, 1/2)$.

On the other hand, the transformations $E_{jk\gamma}$ map rectangular solids to more general sorts of parallelepipeds, so some further argument is needed to show these maps preserve volume. In such a case, one can partition a cell R into smaller cells, on each of which $E_{jk\gamma}$ is approximately a translation, and then make a limiting argument. See Figure 1.6.2 for an illustration of the action of $E_{12\gamma}$.

The identity (1.6.22) is the first step in an important change of variable formula for multidimensional integrals, which goes as follows. Let $\mathcal{O}$ and Ω be open sets in $\mathbb{R}^n$, and let $F : \mathcal{O} \to \Omega$ be a bijective map. Assume F and its inverse $F^{-1} : \Omega \to \mathcal{O}$ are both continuously differentiable. Let $DF(x)$ denote the $n \times n$ matrix

$$DF(x) = \left(\frac{\partial f_j}{\partial x_k} \right), \tag{1.6.28}$$

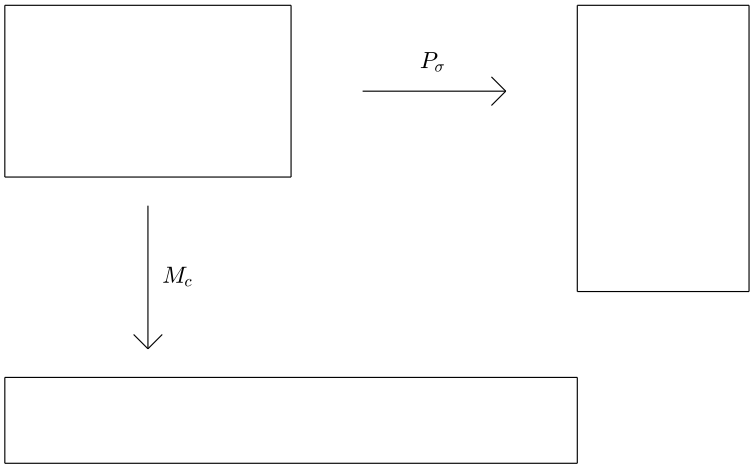

Figure 1.6.1. Actions of P_σ and M_c on a cell

where $F = (f_1, \dots, f_n)$. The formula is

$$\int_\Omega u(x)\,dx = \int_{\mathcal{O}} u(F(x))|\det DF(x)|\,dx. \tag{1.6.29}$$

Such an identity is established first for u continuous and supported on a closed, bounded set $K \subset \Omega$, then for Riemann integrable u supported on such K in Chapter 3 of [**11**], and more generally for all Lebesgue integrable $u : \Omega \to \mathbb{R}$ in Chapter 7 of [**14**].

Row echelon forms and column echelon forms

We now describe more systematically how to apply a sequence of row reductions to an $m \times n$ matrix $A \in M(m \times n, \mathbb{F})$, producing what is called a reduced row echelon form of A.

To start, given such A, we aim to apply row operations to it to obtain a matrix with 1 in the $(1, 1)$ slot and zeros in the rest of the first column, if possible (but only if possibie). This can be done if and only if some row of A has a nonzero first entry, or equivalently if and only if the first column is not identically zero. (If the first column is zero, skip along to the next step.) Say row j has a nonzero first entry. If this does not hold for $j = 1$, switch row 1 and row j. (This is called a

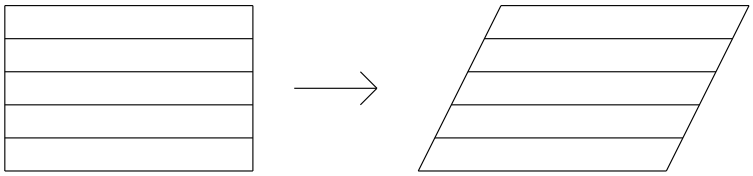

Figure 1.6.2. Action of $E_{12\gamma}$ on a cell

pivot.) Now divide (what is now) row 1 by its first entry, so now the first entry of row 1 is 1. Re-notate, so that, at this stage,

$$\widetilde{A} = \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}. \tag{1.6.30}$$

Now, for $2 \leq j \leq m$, replace row j by this row minus a_{j1} times row 1. Again re-notate, so at this stage we have

$$\widetilde{A} = \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ 0 & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \tag{1.6.31}$$

unless the first column is 0. Note that the a_{22} in (1.6.31) is typically different from the a_{22} in (1.6.30).

To proceed, look at rows 2 through m. The first entry of each of these rows is now zero. If the second entry of each such row is 0, skip to the next step. On the other hand, if the second entry of the jth row is nonzero, (and j is the smallest such index) proceed as follows. If $j > 2$, switch row 2 and row j (this is also called a pivot). Now the second entry of row 2 is nonzero. Divide row 2 by this quantity,

so now the second entry of row 2 is 1. Then, for each $j \neq 2$, replace row j, i.e., $(a_{j1}, \dots, a_{jn})$, by that row minus a_{j2} times row 2. At this stage, we have

$$\widetilde{A} = \begin{pmatrix} 1 & 0 & \cdots & a_{1n} \\ 0 & 1 & \cdots & a_{2n} \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & a_{mn} \end{pmatrix}. \tag{1.6.32}$$

This assumes that the first column of the original A was not 0 and the second column of the matrix $\widetilde{A}$ in (1.6.31) (below the first entry) was not zero. Otherwise, make the obvious adjustments. For example, if we achieve (1.6.31) but the second entry of the jth column in (1.6.31) is 0 for each $j \geq 2$, then, instead of (1.6.32), we have

$$\widetilde{A} = \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & 0 & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{mn} \end{pmatrix}. \tag{1.6.33}$$

Continue in this fashion. When done, the matrix $\widetilde{A}$, obtained from the original A in (1.6.1), is said to be in reduced row echelon form. The jth row of the final matrix $\widetilde{A}$ has a 1 as its first nonzero entry (if the row is not identically zero), and the position of the initial 1 moves to the right as j increases. Also, each such initial 1 occurs in a column with no other nonzero entries.

Here is an example of a sequence of row reductions.

$$\begin{gathered} A = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 2 & 4 & 2 & 4 \\ 1 & 2 & 1 & 2 \end{pmatrix}, \quad \widetilde{A}_1 = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \\ \widetilde{A}_2 = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \end{gathered} \tag{1.6.34}$$

For this example, $A : \mathbb{R}^4 \to \mathbb{R}^3$. It is a special case of Proposition 1.6.2 that the three matrices in (1.6.34) all have the same null space. Clearly $(x, y, z, w)^t$ belongs to $\mathcal{N}(\widetilde{A}_2)$ if and only if

$$x = -2y - w \quad \text{and} \quad z = -w.$$

Thus we can pick y and w arbitrarily and determine x and z uniquely. It follows that $\dim \mathcal{N}(\widetilde{A}_2) = 2$. Picking, respectively, $y = 1, w = 0$ and $y = 0, w = 1$ gives

$$\begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} -1 \\ 0 \\ -1 \\ 1 \end{pmatrix} \tag{1.6.35}$$

as a basis of $\mathcal{N}(A)$, for A in (1.6.34).

More generally, suppose A is an $m \times n$ matrix, as in (1.6.1), and suppose it has a reduced row echelon form $\widetilde{A}$. Of the m rows of $\widetilde{A}$, assume that μ of them are nonzero, with 1 as the leading nonzero element, and assume that $m - \mu$ of the rows

of $\widetilde{A}$ are zero. Hence the row rank of $\widetilde{A}$ is μ. It follows that the column rank of $\widetilde{A}$ is also μ, so $\mathcal{R}(\widetilde{A})$ has dimension μ. Consequently

$$\dim \mathcal{N}(\widetilde{A}) = n - \mu, \tag{1.6.36}$$

so of course $\dim \mathcal{N}(A) = n - \mu$. To determine $\mathcal{N}(\widetilde{A})$ explicitly, it is convenient to make the following construction. Permute the *columns* of $\widetilde{A}$ to obtain

$$\widetilde{B} = \tilde{\rho}_\sigma(\widetilde{A}) = \begin{pmatrix} I & Y \\ 0 & 0 \end{pmatrix}, \tag{1.6.37}$$

where I is the $\mu \times \mu$ identity matrix and Y is a $\mu \times (n - \mu)$ matrix,

$$Y = \begin{pmatrix} y_{1,\mu+1} & \cdots & y_{1,n} \\ \vdots & & \vdots \\ y_{\mu,\mu+1} & \cdots & y_{\mu,n} \end{pmatrix}. \tag{1.6.38}$$

Since

$$\begin{pmatrix} I & Y \\ 0 & 0 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} u + Yv \\ 0 \end{pmatrix}, \tag{1.6.39}$$

we see that an isomorphism of $\mathbb{F}^{n-\mu}$ with $\mathcal{N}(\widetilde{B})$ is given by

$$Z : \mathbb{F}^{n-\mu} \xrightarrow{\approx} \mathcal{N}(\widetilde{B}) \subset \mathbb{F}^n, \quad Zv = \begin{pmatrix} -Yv \\ v \end{pmatrix}. \tag{1.6.40}$$

Now, by (1.6.32),

$$\tilde{\rho}_\sigma(\widetilde{A}) = \widetilde{A} P_\sigma^t, \tag{1.6.41}$$

so

$$\mathcal{N}(A) = \mathcal{N}(\widetilde{A}) = (P_\sigma^t)^{-1} \mathcal{N}(\widetilde{B}) = (P_\sigma^t)^{-1} Z(\mathbb{F}^{n-\mu}). \tag{1.6.42}$$

Note that each P_σ is an orthogonal matrix, so

$$(P_\sigma^t)^{-1} = P_\sigma, \tag{1.6.43}$$

and we conclude that

$$P_\sigma Z : \mathbb{F}^{n-\mu} \xrightarrow{\approx} \mathcal{N}(A). \tag{1.6.44}$$

Note that, in the setting of (1.6.34), the construction in (1.6.37) becomes

$$\widetilde{B} = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \text{so} \quad Y = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}. \tag{1.6.45}$$

The reader can check the essential equivalence of (1.6.44) and (1.6.35) in this case.

The systematic approach to row reduction described above is readily adapted to column reduction. Indeed, column reduction of a matrix B can be achieved by taking $A = B^t$, row reducing A, and then taking the transpose of the result. In particular, taking the transpose of the reduced row echelon form of A yields the *reduced column echelon form* of B. Of course, one need not actually take transposes; simply use column operations instead of row operations. From the reduced column echelon form of B one can read off a basis of $\mathcal{R}(B)$.

Here is an example, related to (1.6.34) by taking transposes:

$$B = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \\ 1 & 4 & 2 \end{pmatrix}, \quad \widetilde{B}_1 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 2 & 1 \\ 1 & 2 & 1 \end{pmatrix}, \quad \widetilde{B}_2 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}. \tag{1.6.46}$$

Here, $\widetilde{B}_2$ is a reduced column echelon form of B. We read off from $\widetilde{B}_2$ that

$$\mathcal{R}(B) = \mathrm{Span}\Big\{ \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \Big\}. \tag{1.6.47}$$

LU-factorization

We turn to the application of row reduction to the problem of taking a matrix $A \in M(n, \mathbb{F})$ and writing it as

$$A = LU, \tag{1.6.48}$$

where $L \in M(n, \mathbb{F})$ is lower triangular and $U \in M(n, \mathbb{F})$ is upper triangular. When this can be done, it is called an LU-factorization of A. Here is a condition that guarantees the existence of such a factorization.

Proposition 1.6.6. *Take $A \in M(n, \mathbb{F})$. Assume that A can be transformed to an upper triangular matrix U via a sequence of row operations of the form*

$$\varepsilon_{jk\gamma}, \quad j > k, \ \gamma \in \mathbb{F}. \tag{1.6.49}$$

Then A has a factorization of the form (1.6.48)*, with L lower triangular.*

Proof. As we have seen, for $B \in M(n, \mathbb{F})$,

$$\varepsilon_{jk\gamma}(B) = E_{jk\gamma} B, \tag{1.6.50}$$

with $E_{jk\gamma}$ as in (1.6.12) (with $m = n$). An examination of this matrix shows that

$$E_{jk\gamma} \text{ is lower triangular, if } j > k. \tag{1.6.51}$$

We deduce that, under the hypothesis of Proposition 1.6.6,

$$U = S_\ell \cdots S_1 A, \tag{1.6.52}$$

where each S_ν has the form (1.6.51). As seen in (1.6.14), $E_{jk\gamma}^{-1} = E_{jk,-\gamma}$ so each matrix S_ν^{-1} is also lower triangular. We thus have (1.6.48), with

$$L = S_1^{-1} \cdots S_\ell^{-1}. \tag{1.6.53}$$

□

Here is a specific class of matrices to which Proposition 1.6.6 applies.

Proposition 1.6.7. *Take $A \in M(n, \mathbb{F})$ and for $\ell \in \{1, \dots, n\}$ let $A^{(\ell)}$ denote the $\ell \times \ell$ matrix forming the upper left corner of A, i.e.,*

$$A^{(1)} = (a_{11}), \quad A^{(2)} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \dots, A^{(n)} = A. \tag{1.6.54}$$

Assume each $A^{(\ell)}$ is invertible, i.e.,

$$\det A^{(\ell)} \neq 0 \quad \textit{for} \quad 1 \leq \ell \leq n. \tag{1.6.55}$$

Then Proposition 1.6.6 applies, so A has an LU-factorization (1.6.48).

Proof. We start with the hypothesis that $a_{11} \neq 0$. Then we apply a sequence of row operations of the form

$$\varepsilon_{j1\gamma}, \quad j > 1, \quad \gamma = a_{11}^{-1} a_{j1},$$

to clear out all the elements of the first column of A below a_{11}. This yields a sequence of row operations of the form (1.6.49) that take A to A_1, and the first column of A_1 has a_{11} as its only nonzero element.

Before proceeding, we make the following useful observation.

Lemma. If $A \in M(n, \mathbb{F})$, then applying a row operation of the form (1.6.49) leaves each quantity $\det A^{(\ell)}$ invariant.
Proof. Exercise.

To proceed, the hypothesis $\det A^{(\ell)} \neq 0$, together with the lemma, implies that the 22-entry of A_1 is nonzero. Thus we can apply a sequence of row operations of the form $\varepsilon_{j2\gamma}$, with $j > 2$ and $\gamma = a_{22}^{-1} a_{j2}$, to clear out all the entries of the second column below the second one. Thus we have a further sequence of row operations of the form (1.6.49), taking A_1 to A_2, and the first two columns of A_2 are zero below the diagonal. Also all the upper-left blocks of A_2 have the same determinant as do those of A. In particular, if $n \geq 3$ and $\det A^{(3)} \neq 0$, the 33-entry of A_2 is nonzero.

Continuing, we see that Proposition 1.6.6 is applicable, under the hypotheses of Proposition 1.6.7, so we have the LU-factorization (1.6.48). □

Sometimes when the condition given in Proposition 1.6.7 fails for A, it can be restored by permuting the rows of A. Then the condition holds for PA, where P is a permutation matrix (i.e., of the form P_σ). Then we have

$$PA = LU. \tag{1.6.56}$$

Obtaining this is called LU-factorization with *partial pivoting*. We have the following result.

Proposition 1.6.8. *If $A \in M(n, \mathbb{F})$ is invertible, then one can permute its rows to obtain a matrix to which Proposition 1.6.7 applies.*

Proof. It suffices to show that a permutation of the rows of A produces a matrix B for which $B^{(n-1)}$ is invertible, since then an inductive argument finishes the proof.

Now invertibility of A implies its rows $\alpha_1, \dots, \alpha_n$ are linearly independent n-vectors. With $\alpha_j = (a_{j1}, \dots, a_{jn})$, set

$$\alpha'_j = (a_{j1}, \dots, a_{j,n-1}),$$

so $\alpha_j = (\alpha'_j, a_{jn})$. Then $\{\alpha'_1, \dots, \alpha'_n\}$ spans $\mathbb{F}^{n-1}$, so some subset forms a basis; this subset must have $n-1$ elements. A permutation that makes the first $n-1$

elements a basis then induces a permutation of the rows of A, yielding B with the desired property. □

We have discussed how row operations applied to $A \in M(n, \mathbb{F})$ allow for convenient calculations of $\det A$ and of A^{-1} (when A is invertible). The LU factorization (1.6.48), or more generally (1.6.56), also lead to relatively efficient calculations of these objects. For one, $\det L$ and $\det U$ are simply the products of the diagonal entries of these matrices. Furthermore, computing L^{-1} amounts to solving

$$\begin{pmatrix} L_{11} & & \\ \vdots & \ddots & \\ L_{n1} & \cdots & L_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}, \tag{1.6.57}$$

i.e., to solving

$$\begin{aligned} L_{11}v_1 &= w_1, \\ L_{21}v_1 + L_{22}v_2 &= w_2, \\ &\vdots \\ L_{n1}v_1 + \cdots + L_{nn}v_n &= w_n. \end{aligned} \tag{1.6.58}$$

One takes $v_1 = w_1/L_{11}$, plugs this into the second equation and solves for v_2, and proceeds iteratively. Inversion of U is done similarly.

Suppose $A \in M(n, \mathbb{F})$ is invertible and has an LU-factorization, as in (1.6.48). We consider the extent to which such a factorization is unique. In fact,

$$A = L_1U_1 = L_2U_2 \tag{1.6.59}$$

implies

$$L_2^{-1}L_1 = U_2U_1^{-1}. \tag{1.6.60}$$

Now the left side of (1.6.60) is lower triangular and the right side is upper triangular. Hence both sides are diagonal. This leads to the following variant of (1.6.48):

$$A = L_0DU_0, \tag{1.6.61}$$

where D is diagonal, L_0 is lower triangular, U_0 is upper triangular, and both L_0 and U_0 have only 1s on the diagonal. If A is invertible and has the form (1.6.48), one easily writes $L = L_0D_\ell$ and $U = D_rU_0$, and achieves (1.6.61) with $D = D_\ell D_r$. Then an argument parallel to (1.6.59)–(1.6.60) shows that the factorization (1.6.61) is unique.

This uniqueness has further useful consequences. Suppose $A = (a_{jk}) \in M(n, \mathbb{F})$ is invertible and symmetric, i.e. $A = A^t$, or equivalently $a_{jk} = a_{kj}$, and A has the form (1.6.61). Applying the transpose gives $A = A^t = U_0^tDL_0^t$, which is another factorization of the form (1.6.61). Uniqueness implies $L_0 = U_0^t$, so

$$A = A^t = L_0DL_0^t. \tag{1.6.62}$$

Similarly, suppose A is invertible and self-adjoint, i.e., $A = A^*$, or $a_{jk} = \overline{a_{kj}}$ (see §3.2), and A has the form (1.6.61). Taking the adjoint of (1.6.61) yields $A = A^* = U_0^*D^*L_0^*$, and now uniqueness implies $L_0 = U_0^*$ and $D = D^*$ (i.e., D is real), so

$$A = A^* = L_0DL_0^*, \quad D \text{ real}. \tag{1.6.63}$$

Exercises

1. Use Gaussian elimination to compute the inverse of the following matrix.

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

2. Construct a reduced row echelon form for each of the following matrices.

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 0 \\ 3 & 2 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}.$$

3. Construct a basis of the null space of each of the matrices in Exercise 2.

4. Construct a reduced column echelon form for each of the matrices in Exercise 2.

5. Construct a basis of the range of each of the matrices in Exercise 2.

6. Construct an LU-factorization of the matrix X in Exercise 1. Construct the inverse of each factor, and use this to obtain another calculation of X^{-1}.

7. Apply the method of Gaussian elimination to compute A^{-1}, for

$$A = \begin{pmatrix} c & -s \\ s & c \end{pmatrix}, \quad c, s \in (-1, 1), \quad c, s \neq 0, \quad c^2 + s^2 = 1.$$

Use this calculation to derive the identity

$$\begin{pmatrix} c & s \\ -s & c \end{pmatrix} = M_{(1/c,1)} E_{12,-s} M_{(1/s,1)} E_{211} M_{(s,c)}.$$

Explain the relevance of this identity to the issue of how the transformation A affects areas of planar domains.

8. Let $A, B \in M(n, \mathbb{F})$ and assume A is invertible. Show that if you apply a sequence of row reductions to A, taking it to I, and then apply the same sequence of row operations to B, it takes

$$B \text{ to } A^{-1}B.$$

Chapter 2

Eigenvalues, eigenvectors, and generalized eigenvectors

Eigenvalues and eigenvectors provide a powerful tool with which to understand the structure of a linear transformation on a finite-dimensional vector space. Give $A \in \mathcal{L}(V)$, if $v \in V$ is nonzero and $Av = \lambda v$, we say v is an eigenvector of A, with eigenvalue λ. This concept motivates us to bring in the eigenspace

$$\mathcal{E}(A, \lambda) = \{v \in V : (A - \lambda I)v = 0\}. \tag{2.0.1}$$

This is nonzero if and only if $A - \lambda I$ is not invertible, i.e., if and only if

$$K_A(\lambda) = \det(\lambda I - A) = 0. \tag{2.0.2}$$

The polynomial $K_A(\lambda)$ is called the characteristic polynomial of A. A key result called the Fundamental Theorem of Algebra (presented in Appendix 2.A) implies it has complex roots.

One application of results on eigenvalues and eigenvectors arises in the study of first-order systems of differential equations of the form

$$\frac{dx}{dt} = Ax, \tag{2.0.3}$$

for $x(t) \in V,\ A \in \mathcal{L}(V)$. A fruitful attack involves seeking solutions of the form

$$x(t) = e^{\lambda t}v, \tag{2.0.4}$$

with $v \in V,\ \lambda \in \mathbb{C}$. Applying d/dt to both sides yields the equation

$$e^{\lambda t}Av = \lambda e^{\lambda t}v, \tag{2.0.5}$$

and dividing by $e^{\lambda t}$ shows that we have a solution of (2.0.3) if and only if $v \in \mathcal{E}(A, \lambda)$. We can hence obtain solutions to (2.0.3), in the form of linear combinations of solutions of the type (2.0.4), with arbitrary initial data, if and only if each vector in V can be written as a linear combination of eigenvectors of A.

This illustrates a natural problem: given $A \in \mathcal{L}(V)$, when does V have a basis of eigenvectors of A? Consider the following three examples:

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{pmatrix}. \tag{2.0.6}$$

Methods developed in §2.1 will show that $\mathbb{C}^3$ has a basis of eigenvectors for A, and it has a basis of eigenvectors for B, but it does not have a basis of eigenvectors for C.

To delve further into the structure of a linear transformation $A \in \mathcal{L}(V)$, we look at generalized eigenvectors of A, associated to the eigenvalue λ, i.e., to nonzero elements of the generalized eigenspace

$$\mathcal{GE}(A, \lambda) = \{v \in V : (A - \lambda I)^k v = 0, \text{ for some } k \in \mathbb{N}\}. \tag{2.0.7}$$

In §2.2 we show that if V is a finite-dimensional complex vector space and $A \in \mathcal{L}(V)$, then V has a basis consisting of generalized eigenvectors of A.

One can also use generalized eigenvectors of A to obtain solutions to (2.0.3), of a form a little more complicated than (2.0.4). We take this up in §3.7.

The restriction N of $A - \lambda I$ to $W = \mathcal{GE}(A, \lambda)$ yields $N \in \mathcal{L}(W)$ satisfying

$$N^k = 0. \tag{2.0.8}$$

We say N is nilpotent. In §2.3 we analyze nilpotent transformations as precisely those linear transformations that can be put in strictly upper triangular form, with respect to an appropriate choice of basis. This, combined with results of §2.2, implies that each $A \in \mathcal{L}(V)$ can be put in upper triangular form (with the eigenvalues on the diagonal), with respect to a basis of generalized eigenvectors, whenever V is a finite-dimensional complex vector space.

In §2.4 we show that if $N \in \mathcal{L}(W)$ is nilpotent and $\dim W < \infty$, then W has a basis with respect to which the matrix form of N consists of blocks, each block being a matrix of all 0s, except for a string of 1s right above the diagonal, e.g., such as

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ & 0 & 1 & 0 \\ & & 0 & 1 \\ & & & 0 \end{pmatrix}. \tag{2.0.9}$$

In concert with results of §2.3, this establishes a *Jordan canonical form* for each $A \in \mathcal{L}(V)$, whenever V is a finite-dimensional complex vector space.

2.1. Eigenvalues and eigenvectors

Let $T : V \to V$ be linear. If there is a nonzero $v \in V$ such that

$$Tv = \lambda_j v, \tag{2.1.1}$$

for some $\lambda_j \in \mathbb{F}$, we say λ_j is an eigenvalue of T, and v is an eigenvector. Let $\mathcal{E}(T, \lambda_j)$ denote the set of vectors $v \in V$ such that (2.1.1) holds. It is clear that $\mathcal{E}(T, \lambda_j)$ is a linear subspace of V and

$$T : \mathcal{E}(T, \lambda_j) \longrightarrow \mathcal{E}(T, \lambda_j). \tag{2.1.2}$$

The set of $\lambda_j \in \mathbb{F}$ such that $\mathcal{E}(T, \lambda_j) \neq 0$ is denoted $\operatorname{Spec}(T)$. Clearly $\lambda_j \in \operatorname{Spec}(T)$ if and only if $T - \lambda_j I$ is not injective, so, if V is finite dimensional,

$$\lambda_j \in \operatorname{Spec}(T) \Longleftrightarrow \det(\lambda_j I - T) = 0. \tag{2.1.3}$$

We call $K_T(\lambda) = \det(\lambda I - T)$ the *characteristic polynomial* of T.

If $\mathbb{F} = \mathbb{C}$, we can use the *fundamental theorem of algebra*, which says every non-constant polynomial with complex coefficients has at least one complex root. (See Appendix 2.A for a proof of this result.) This proves the following.

Proposition 2.1.1. *If V is a finite-dimensional complex vector space and $T \in \mathcal{L}(V)$, then T has at least one eigenvector in V.*

REMARK. If V is real and $K_T(\lambda)$ does have a real root λ_j, then there is a real λ_j-eigenvector.

Sometimes a linear transformation has only one eigenvector, up to a scalar multiple. Consider the transformation $A : \mathbb{C}^3 \to \mathbb{C}^3$ given by

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}. \tag{2.1.4}$$

We see that $\det(\lambda I - A) = (\lambda - 2)^3$, so $\lambda = 2$ is a triple root. It is clear that

$$\mathcal{E}(A, 2) = \operatorname{Span}\{e_1\}, \tag{2.1.5}$$

where $e_1 = (1, 0, 0)^t$ is the first standard basis vector of $\mathbb{C}^3$.

If one is given $T \in \mathcal{L}(V)$, it is of interest to know whether V has a basis of eigenvectors of T. The following result is useful.

Proposition 2.1.2. *Assume that the characteristic polynomial of $T \in \mathcal{L}(V)$ has k distinct roots, $\lambda_1, \dots, \lambda_k$, with eigenvectors $v_j \in \mathcal{E}(T, \lambda_j)$, $1 \leq j \leq k$. Then $\{v_1, \dots, v_k\}$ is linearly independent. In particular, if $k = \dim V$, these vectors form a basis of V.*

Proof. We argue by contradiction. If $\{v_1, \dots, v_k\}$ is linearly dependent, take a minimal subset that is linearly dependent and (reordering if necessary) say this set is $\{v_1, \dots, v_m\}$, with $Tv_j = \lambda_j v_j$, and

$$c_1 v_1 + \cdots + c_m v_m = 0, \tag{2.1.6}$$

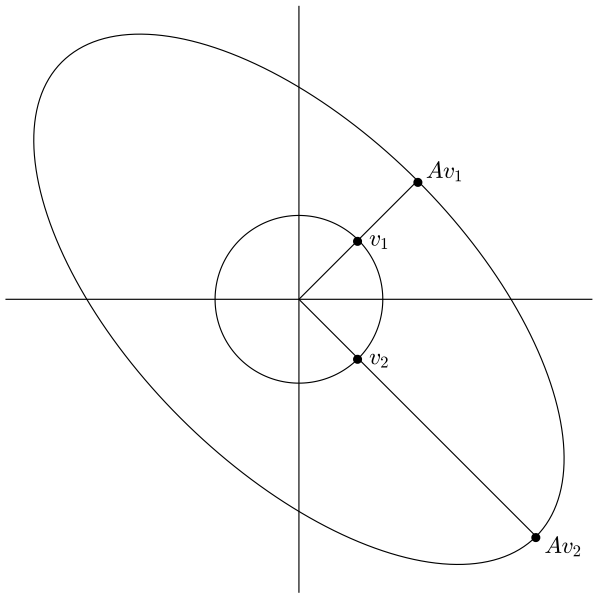

Figure 2.1.1. Behavior of the linear transformation A in (2.1.8), with two distinct real eigenvalues

with $c_j \neq 0$ for each $j \in \{1, \dots, m\}$. Applying $T - \lambda_m I$ to (6.6) gives

$$c_1(\lambda_1 - \lambda_m)v_1 + \cdots + c_{m-1}(\lambda_{m-1} - \lambda_m)v_{m-1} = 0, \tag{2.1.7}$$

a linear dependence relation on the smaller set $\{v_1, \dots, v_{m-1}\}$. This contradiction proves the proposition. □

See Figure 2.1.1 for an illustration of the action of the transformation

$$A : \mathbb{R}^2 \longrightarrow \mathbb{R}^2, \quad A = \begin{pmatrix} 3 & -1 \\ -1 & 3 \end{pmatrix}, \tag{2.1.8}$$

with two distinct eigenvalues, and associated eigenvectors

$$\lambda_1 = 2, \ \lambda_2 = 4, \quad v_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \ v_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{2.1.9}$$

We also display the circle $x^2 + y^2 = 1$, and its image under A. Compare Figure 1.2.1.

For contrast, we consider the linear transformation

$$A : \mathbb{R}^2 \longrightarrow \mathbb{R}^2, \quad A = \begin{pmatrix} 1 & -2 \\ 2 & -1 \end{pmatrix}, \tag{2.1.10}$$

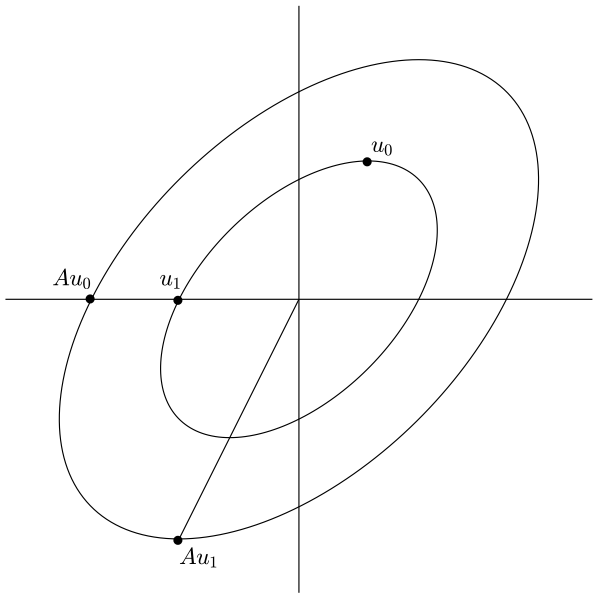

Figure 2.1.2. Action of the linear transformation (2.1.10) on $\mathbb{R}^2$, with purely imaginary eigenvalues, and eigenvectors $v_\pm = u_0 \mp iu_1$

whose eigenvalues $\lambda_\pm$ are purely imaginary and whose eigenvectors $v_\pm$ are not real:

$$\lambda_\pm = \pm i\sqrt{3}, \quad v_\pm = \frac{1}{2\sqrt{2}}\begin{pmatrix} 1 \pm i\sqrt{3} \\ 2 \end{pmatrix}. \tag{2.1.11}$$

We can write

$$v_- = u_0 + iu_1, \quad u_0 = \frac{1}{2\sqrt{2}}\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad u_1 = \frac{1}{2\sqrt{2}}\begin{pmatrix} -\sqrt{3} \\ 0 \end{pmatrix}, \tag{2.1.12}$$

and capture the behavior of A as

$$Au_0 = \sqrt{3}u_1, \quad Au_1 = -\sqrt{3}u_0. \tag{2.1.13}$$

See Figure 2.1.2 for an illustration. This figure also displays the ellipse

$$\gamma(t) = (\cos t)u_0 + (\sin t)u_1, \quad 0 \le t \le 2\pi, \tag{2.1.14}$$

and its image under A.

For another contrast, we look at the transformation

$$A : \mathbb{R}^2 \longrightarrow \mathbb{R}^2, \quad A = \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}, \tag{2.1.15}$$

for which $\lambda = 2$ is a double eigenvalue. We have

$$A - 2I = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}, \quad \mathcal{E}(A, 2) = \operatorname{Span}\{v_1\}, \quad v_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}. \tag{2.1.16}$$

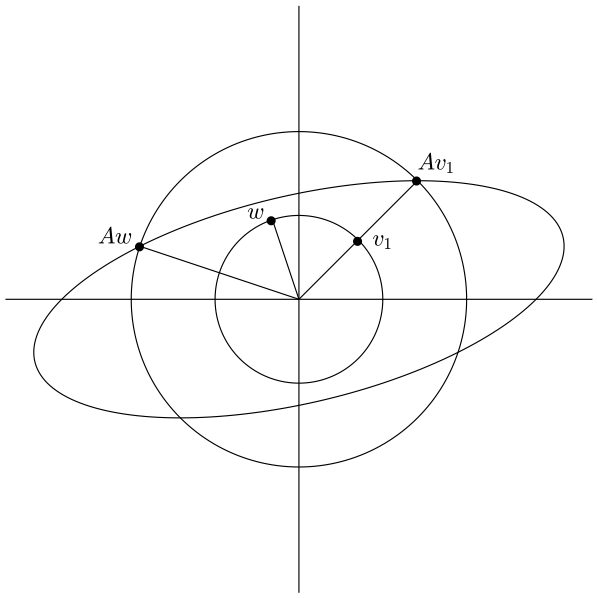

Figure 2.1.3. Action of the transformation (2.1.15) on $\mathbb{R}^2$, with a double eigenvalue and one-dimensional eigenspace

Figure 2.1.3 illustrates the action of this transformation on $\mathbb{R}^2$. It displays the unit circle $x^2 + y^2 = 1$, containing v_1, and the image of this circle under the map A (the ellipse) and under the map $2I$ (the larger circle). These two image curves intersect at 4 points, $\pm Av_1$ and $\pm Aw$, where

$$w = \sqrt{\frac{9}{10}} \begin{pmatrix} -1/3 \\ 1 \end{pmatrix}. \tag{2.1.17}$$

Thus this figure illustrates that there is not an eigenvector of A that is linearly independent of v_1.

Further information on when $T \in \mathcal{L}(V)$ yields a basis of eigenvectors, and on what one can say when it does not, will be given in the following sections.

Exercises

1. Compute the eigenvalues and eigenvectors of each of the following matrices.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \quad \begin{pmatrix} i & i \\ 0 & 1 \end{pmatrix}.$$

In which cases does $\mathbb{C}^2$ have a basis of eigenvectors?

2. Compute the eigenvalues and eigenvectors of each of the following matrices.

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

3. Let $A \in M(n, \mathbb{C})$. We say A is diagonalizable if and only if there exists an invertible $B \in M(n, \mathbb{C})$ such that $B^{-1}AB$ is diagonal:

$$B^{-1}AB = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}.$$

Show that A is diagonalizable if and only if $\mathbb{C}^n$ has a basis of eigenvectors of A. Recall from (1.4.14) that the matrices A and $B^{-1}AB$ are said to be similar.

4. More generally, if V is an n-dimensional complex vector space, we say $T \in \mathcal{L}(V)$ is diagonalisable if and only if there exists invertible $B : \mathbb{C}^n \to V$ such that $B^{-1}TB$ is diagonal, with respect to the standard basis of $\mathbb{C}^n$. Formulate and establish the natural analogue of Exercise 3.

5. In the setting of (2.1.1)–(2.1.2), given $S \in \mathcal{L}(V, V)$, show that

$$ST = TS \Longrightarrow S : \mathcal{E}(T, \lambda_j) \to \mathcal{E}(T, \lambda_j).$$

6. Let $A \in M(n, \mathbb{C})$, and assume A is not invertible, so $0 \in \operatorname{Spec}(A)$. Show that there exists $\delta > 0$ such that if $\lambda \neq 0$ but $|\lambda| < \delta$, then $A - \lambda I$ is invertible. Use this to deduce that $G\ell(n, \mathbb{C})$ is dense in $M(n, \mathbb{C})$. Similarly deduce that $G\ell(n, \mathbb{R})$ is dense in $M(n, \mathbb{R})$. Compare the proof of Proposition 1.5.8 indicated in §1.5.

7. Given $A \in M(n, \mathbb{C})$, let the roots of the characteristic polynomial of A be

$\{\lambda_1, \dots, \lambda_n\}$, repeated according to multiplicity, so

$$\det(\lambda I - A) = \prod_{k=1}^{n} (\lambda - \lambda_k).$$

Show that this is also given by

$$\det(\lambda I - A) = \sum_{k=0}^{n} (-1)^k \sigma_k(\lambda_1, \dots, \lambda_n) \lambda^{n-k},$$

where $\sigma_0(\lambda_1, \dots, \lambda_n) = 1$, and, for $1 \le k \le n$,

$$\sigma_k(\lambda_1, \dots, \lambda_n) = \sum_{1 \le j_1 < \cdots < j_k \le n} \lambda_{j_1} \cdots \lambda_{j_k}.$$

The polynomials σ_k are called the elementary symmetric polynomials.

8. If $A, B \in M(n, \mathbb{C})$, B invertible, and $D = B^{-1}AB$, show that, for all $k \in \mathbb{N}$,

$$D^k = B^{-1} A^k B.$$

9. Let A denote the first matrix in Exercise 2. Diagonalize A and use this to compute

$$A^{100}.$$

10. Let $M \in M(m+n, \mathbb{C})$ have the form

$$M = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}, \quad A \in M(n, \mathbb{C}), \quad B \in M(m, \mathbb{C}).$$

Show that

$$\det M = (\det A)(\det B),$$

and, more generally, for $\lambda \in \mathbb{C}$,

$$\det(M - \lambda I) = \det(A - \lambda I) \cdot \det(B - \lambda I).$$

11. Find the eigenvalues and eigenvectors of

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

2.2. Generalized eigenvectors and the minimal polynomial

As we have seen, the matrix

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \tag{2.2.1}$$

has only one eigenvalue, 2, and, up to a scalar multiple, just one eigenvector, e_1. However, we have

$$(A - 2I)^2 e_2 = 0, \quad (A - 2I)^3 e_3 = 0. \tag{2.2.2}$$

Generally, if $T \in \mathcal{L}(V)$, we say a nonzero $v \in V$ is a generalized λ_j-eigenvector if there exists $k \in \mathbb{N}$ such that

$$(T - \lambda_j I)^k v = 0. \tag{2.2.3}$$

We denote by $\mathcal{GE}(T, \lambda_j)$ the set of vectors $v \in V$ such that (2.2.3) holds, for some k, and call it the generalized eigenspace. It is clear that $\mathcal{GE}(T, \lambda_j)$ is a linear subspace of V and

$$T : \mathcal{GE}(T, \lambda_j) \longrightarrow \mathcal{GE}(T, \lambda_j). \tag{2.2.4}$$

The following is a useful comment.

Lemma 2.2.1. *For each $\lambda_j \in \mathbb{F}$ such that $\mathcal{GE}(T, \lambda_j) \neq 0$,*

$$T - \mu I : \mathcal{GE}(T, \lambda_j) \longrightarrow \mathcal{GE}(T, \lambda_j) \quad \text{is an isomorphism, } \forall\, \mu \neq \lambda_j. \tag{2.2.5}$$

Proof. If $T - \mu I$ is not an isomorphism in (2.2.5), then $Tv = \mu v$ for some nonzero $v \in \mathcal{GE}(T, \lambda_j)$. But then $(T - \lambda_j I)^k v = (\mu - \lambda_j)^k v$ for all $k \in \mathbb{N}$, and hence this cannot ever be zero, unless $\mu = \lambda_j$. □

Note that if V is a finite-dimensional complex vector space, then each nonzero space appearing in (2.2.4) contains an eigenvector, by Proposition 2.1.1. Clearly the corresponding eigenvalue must be λ_j. In particular, the set of λ_j for which $\mathcal{GE}(T, \lambda_j)$ is nonzero coincides with $\operatorname{Spec}(T)$, as given in (2.1.3).

We intend to show that if V is a finite-dimensional complex vector space and $T \in \mathcal{L}(V)$, then V is spanned by generalized eigenvectors of T. One tool in this demonstration will be the construction of polynomials $p(\lambda)$ such that $p(T) = 0$. Here, if

$$p(\lambda) = a_n \lambda^n + a_{n-1} \lambda^{n-1} + \cdots + a_1 \lambda + a_0, \tag{2.2.6}$$

then

$$p(T) = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0 I. \tag{2.2.7}$$

Let us denote by $\mathcal{P}$ the space of polynomials in λ.

Lemma 2.2.2. *If V is finite dimensional and $T \in \mathcal{L}(V)$, then there exists a nonzero $p \in \mathcal{P}$ such that $p(T) = 0$.*

Proof. If $\dim V = n$, then $\dim \mathcal{L}(V) = n^2$, so $\{I, T, \dots, T^{n^2}\}$ is linearly dependent. □

Let us set

$$\mathcal{I}_T = \{p \in \mathcal{P} : p(T) = 0\}. \tag{2.2.8}$$

We see that $\mathcal{I} = \mathcal{I}_T$ has the following properties:

$$\begin{aligned} p, q \in \mathcal{I} &\Longrightarrow p + q \in \mathcal{I}, \\ p \in \mathcal{I},\ q \in \mathcal{P} &\Longrightarrow pq \in \mathcal{I}. \end{aligned} \tag{2.2.9}$$

A set $\mathcal{I} \subset \mathcal{P}$ satisfying (2.2.9) is called an *ideal*. Here is another construction of a class of ideals in $\mathcal{P}$. Given $\{p_1, \dots, p_k\} \subset \mathcal{P}$, set

$$\mathcal{I}(p_1, \dots, p_k) = \{p_1 q_1 + \cdots + p_k q_k : q_j \in \mathcal{P}\}. \tag{2.2.10}$$

We will find it very useful to know that all nonzero ideals in $\mathcal{P}$, including $\mathcal{I}_T$, have the following property.

Lemma 2.2.3. *Let $\mathcal{I} \subset \mathcal{P}$ be a nonzero ideal, and let $p_1 \in \mathcal{I}$ have minimal degree amongst all nonzero elements of $\mathcal{I}$. Then*

$$\mathcal{I} = \mathcal{I}(p_1). \tag{2.2.11}$$

Proof. Take any $p \in \mathcal{I}$. We divide $p_1(\lambda)$ into $p(\lambda)$ and take the remainder, obtaining

$$p(\lambda) = q(\lambda)p_1(\lambda) + r(\lambda). \tag{2.2.12}$$

Here $q, r \in \mathcal{P}$, hence $r \in \mathcal{I}$. Also $r(\lambda)$ has degree less than the degree of $p_1(\lambda)$, so by minimality we have $r \equiv 0$. This shows $p \in \mathcal{I}(p_1)$, and we have (2.2.11). □

Applying this to $\mathcal{I}_T$, we denote by $m_T(\lambda)$ the polynomial of smallest degree in $\mathcal{I}_T$ (having leading coefficient 1), and say

$$m_T(\lambda) \text{ is the minimal polynomial of } T. \tag{2.2.13}$$

Thus every $p \in \mathcal{P}$ such that $p(T) = 0$ is a multiple of $m_T(\lambda)$.

Assuming V is a *complex* vector space of dimension n, we can apply the fundamental theorem of algebra to write

$$m_T(\lambda) = \prod_{j=1}^{K} (\lambda - \lambda_j)^{k_j}, \tag{2.2.14}$$

with distinct roots $\lambda_1, \dots, \lambda_K$. The following polynomials will also play a role in our study of the generalized eigenspaces of T. For each $\ell \in \{1, \dots, K\}$, set

$$p_\ell(\lambda) = \prod_{j \neq \ell} (\lambda - \lambda_j)^{k_j} = \frac{m_T(\lambda)}{(\lambda - \lambda_\ell)^{k_\ell}}. \tag{2.2.15}$$

We have the following useful result.

Proposition 2.2.4. *If V is an n-dimensional complex vector space and $T \in \mathcal{L}(V)$, then, for each $\ell \in \{1, \dots, K\}$,*

$$\mathcal{GE}(T, \lambda_\ell) = \mathcal{R}(p_\ell(T)). \tag{2.2.16}$$

Proof. Given $v \in V$,

$$(T - \lambda_\ell)^{k_\ell} p_\ell(T)v = m_T(T)v = 0, \tag{2.2.17}$$

so $p_\ell(T) : V \to \mathcal{GE}(T, \lambda_\ell)$. Furthermore, each factor

$$(T - \lambda_j)^{k_j} : \mathcal{GE}(T, \lambda_\ell) \longrightarrow \mathcal{GE}(T, \lambda_\ell), \quad j \neq \ell, \tag{2.2.18}$$

in $p_\ell(T)$ is an isomorphism, by Lemma 2.2.1, so $p_\ell(T) : \mathcal{GE}(T, \lambda_\ell) \to \mathcal{GE}(T, \lambda_\ell)$ is an isomorphism. □

REMARK. We hence see that each λ_j appearing in (2.2.14) is an element of $\operatorname{Spec} T$.

We now establish the following spanning property.

Proposition 2.2.5. *If V is an n-dimensional complex vector space and $T \in \mathcal{L}(V)$, then*

$$V = \mathcal{GE}(T, \lambda_1) + \cdots + \mathcal{GE}(T, \lambda_K). \tag{2.2.19}$$

That is, each $v \in V$ can be written as $v = v_1 + \cdots + v_K$, with $v_j \in \mathcal{GE}(T, \lambda_j)$.

Proof. Let $m_T(\lambda)$ be the minimal polynomial of T, with the factorization (2.2.14), and define $p_\ell(\lambda)$ as in (2.2.15), for $\ell = 1, \dots, K$. We claim that

$$\mathcal{I}(p_1, \dots, p_K) = \mathcal{P}. \tag{2.2.20}$$

In fact we know from Lemma 2.2.3 that $\mathcal{I}(p_1, \dots, p_K) = \mathcal{I}(p_0)$ for some $p_0 \in \mathcal{P}$. Then any root of $p_0(\lambda)$ must be a root of each $p_\ell(\lambda)$, $1 \leq \ell \leq K$. But these polynomials are constructed so that no $\mu \in \mathbb{C}$ is a root of all K of them. Hence $p_0(\lambda)$ has no root so (again by the fundamental theorem of algebra) it must be constant, i.e., $1 \in \mathcal{I}(p_1, \dots, p_K)$, which gives (2.2.20), and in particular we have that there exist $q_\ell \in \mathcal{P}$ such that

$$p_1(\lambda)q_1(\lambda) + \cdots + p_K(\lambda)q_K(\lambda) = 1. \tag{2.2.21}$$

We use this as follows to write an arbitrary $v \in V$ as a linear combination of generalized eigenvectors. Replacing λ by T in (2.2.21) gives

$$p_1(T)q_1(T) + \cdots + p_K(T)q_K(T) = I. \tag{2.2.22}$$

Hence, for any given $v \in V$,

$$v = p_1(T)q_1(T)v + \cdots + p_K(T)q_K(T)v = v_1 + \cdots + v_K, \tag{2.2.23}$$

with $v_\ell = p_\ell(T)q_\ell(T)v \in \mathcal{GE}(T, \lambda_\ell)$, by Proposition 2.2.4. □

We next produce a basis consisting of generalized eigenvectors.

Proposition 2.2.6. *Under the hypotheses of Proposition 2.2.5, let $\mathcal{GE}(T, \lambda_\ell)$, $1 \leq \ell \leq K$, denote the generalized eigenspaces of T (with λ_ℓ mutually distinct), and let*

$$S_\ell = \{v_{\ell 1}, \dots, v_{\ell, d_\ell}\}, \quad d_\ell = \dim \mathcal{GE}(T, \lambda_\ell), \tag{2.2.24}$$

be a basis of $\mathcal{GE}(T, \lambda_\ell)$. Then

$$S = S_1 \cup \cdots \cup S_K \tag{2.2.25}$$

is a basis of V.

Proof. It follows from Proposition 2.2.5 that S spans V. We need to show that S is linearly independent. To show this it suffices to show that if w_ℓ are nonzero elements of $\mathcal{GE}(T, \lambda_\ell)$, then no nontrivial linear combination can vanish. The demonstration of this is just slightly more elaborate than the corresponding argument in Proposition 2.1.2. If there exist such linearly dependent sets, take one with a minimal number of elements, and rearrange $\{\lambda_\ell\}$, to write it as $\{w_1, \dots, w_m\}$, so we have

$$c_1 w_1 + \cdots + c_m w_m = 0, \tag{2.2.26}$$

and $c_j \neq 0$ for each $j \in \{1, \dots, m\}$. As seen in Lemma 2.2.1,

$$T - \mu I : \mathcal{GE}(T, \lambda_\ell) \longrightarrow \mathcal{GE}(T, \lambda_\ell) \text{ is an isomorphism, } \forall\ \mu \neq \lambda_\ell. \tag{2.2.27}$$

Take $k \in \mathbb{N}$ so large that $(T - \lambda_m I)^k$ annihilates each element of the basis S_m of $\mathcal{GE}(T, \lambda_m)$, and apply $(T - \lambda_m I)^k$ to (2.2.26). Given (2.2.27), we will obtain a non-trivial linear dependence relation involving $m - 1$ terms, a contradiction, so the purported linear dependence relation cannot exist. This proves Proposition 2.2.6. □

Example. Let us consider $A : \mathbb{C}^3 \to \mathbb{C}^3$, given by

$$A = \begin{pmatrix} 2 & 3 & 3 \\ 0 & 2 & 3 \\ 0 & 0 & 1 \end{pmatrix}. \tag{2.2.28}$$

Then $\operatorname{Spec}(A) = \{2, 1\}$, so $m_A(\lambda) = (\lambda - 2)^a(\lambda - 1)^b$ for some positive integers a and b. Computations give

$$(A - 2I)(A - I) = \begin{pmatrix} 0 & 3 & 9 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad (A - 2I)^2(A - I) = 0, \tag{2.2.29}$$

hence $m_A(\lambda) = (\lambda - 2)^2(\lambda - 1)$. Thus we have

$$p_1(\lambda) = \lambda - 1, \quad p_2(\lambda) = (\lambda - 2)^2, \tag{2.2.30}$$

using the ordering $\lambda_1 = 2,\ \lambda_2 = 1$. As for $q_\ell(\lambda)$ such that (2.2.21) holds, a little trial and error gives $q_1(\lambda) = -(\lambda - 3),\ q_2(\lambda) = 1$, i.e.,

$$-(\lambda - 1)(\lambda - 3) + (\lambda - 2)^2 = 1. \tag{2.2.31}$$

Note that

$$A - I = \begin{pmatrix} 1 & 3 & 3 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \end{pmatrix}, \quad (A - 2I)^2 = \begin{pmatrix} 0 & 0 & 6 \\ 0 & 0 & -3 \\ 0 & 0 & 1 \end{pmatrix}. \tag{2.2.32}$$

Hence, by (2.2.16),

$$\mathcal{GE}(A, 2) = \operatorname{Span}\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}, \quad \mathcal{GE}(A, 1) = \operatorname{Span}\left\{ \begin{pmatrix} 6 \\ -3 \\ 1 \end{pmatrix} \right\}. \tag{2.2.33}$$

Alternatively, in place of (2.2.16), we can use

$$\mathcal{GE}(A, 2) = \mathcal{N}((A - 2I)^2), \quad \mathcal{GE}(A, 1) = \mathcal{N}(A - I), \tag{2.2.34}$$

together with the calculations of $A-I$ and $(A-2I)^2$ in (2.2.32) to recover (2.2.33). See Exercise 8 below for a more general result.

REMARK. In general, for $A \in M(3,\mathbb{C})$, there are the following three possibilities.

(I) A has 3 distinct eigenvalues, $\lambda_1, \lambda_2, \lambda_3$. Then λ_j-eigenvectors v_j, $1 \le j \le 3$, span $\mathbb{C}^3$.

(II) A has 2 distinct eigenvalues, say λ_1 (single) and λ_2 (double). Then

$$m_A(\lambda) = (\lambda - \lambda_1)(\lambda - \lambda_2)^k, \quad k = 1 \text{ or } 2. \tag{2.2.35}$$

Whatever the value of k, $p_2(\lambda) = \lambda - \lambda_1$, and hence

$$\mathcal{GE}(A, \lambda_2) = \mathcal{R}(A - \lambda_1 I), \tag{2.2.36}$$

which in turn is the span of the columns of $A - \lambda_1 I$. We have

$$\mathcal{GE}(A, \lambda_2) = \mathcal{E}(A, \lambda_2) \Longleftrightarrow k = 1. \tag{2.2.37}$$

In any case, $\mathbb{C}^3 = \mathcal{E}(A, \lambda_1) \oplus \mathcal{GE}(A, \lambda_2)$.

(III) A has a triple eigenvalue, λ_1. Then $\mathrm{Spec}(A - \lambda_1 I) = \{0\}$, and

$$\mathcal{GE}(A, \lambda_1) = \mathbb{C}^3. \tag{2.2.38}$$

Compare results of the next section.

Exercises

1. Consider the matrices

$$A_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ -1 & 0 & -1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 1 & 3 \\ 0 & -2 & 1 \end{pmatrix}.$$

Compute the eigenvalues and eigenvectors of each A_j.

2. Find the minimal polynomial of A_j and find a basis of generalized eigenvectors of A_j.

3. Consider the transformation $D : \mathcal{P}_2 \to \mathcal{P}_2$ given by (1.4.15). Find the eigenvalues and eigenvectors of D. Find the minimal polynomial of D and find a basis of $\mathcal{P}_2$ consisting of generalized eigenvectors of D.

4. Suppose V is a finite dimensional complex vector space and $T : V \to V$. Show that V has a basis of eigenvectors of T if and only if all the roots of the minimal polynomial $m_T(\lambda)$ are simple.

5. In the setting of (2.2.3)–(2.2.4), given $S \in \mathcal{L}(V)$, show that

$$ST = TS \Longrightarrow S : \mathcal{GE}(T, \lambda_j) \to \mathcal{GE}(T, \lambda_j).$$

6. Show that if V is an n-dimensional complex vector space, $S, T \in \mathcal{L}(V)$, and $ST = TS$, then V has a basis consisting of vectors that are simultaneously generalized eigenvectors of T and of S.
Hint. Apply Proposition 2.2.6 to $S : \mathcal{GE}(T, \lambda_j) \to \mathcal{GE}(T, \lambda_j)$.

7. Let V be a complex n-dimensional vector space, and take $T \in \mathcal{L}(V)$, with minimal polynomial $m_T(\lambda)$, as in (2.2.13). For $\ell \in \{1, \dots, K\}$, set

$$P_\ell(\lambda) = \frac{m_T(\lambda)}{\lambda - \lambda_\ell}.$$

Show that, for each $\ell \in \{1, \dots, K\}$, there exists $w_\ell \in V$ such that $v_\ell = P_\ell(T)w_\ell \neq 0$. Then show that $(T - \lambda_\ell I)v_\ell = 0$, so one has a proof of Proposition 2.1.1 that does not use determinants.

8. In the setting of Exercise 7, show that the exponent k_j in (2.2.14) is the smallest integer such that

$$(T - \lambda_j I)^{k_j} \text{ annihilates } \mathcal{GE}(T, \lambda_j).$$

Hint. Review the proof of Proposition 2.2.4.

9. Show that Proposition 2.2.6 refines Proposition 2.2.5 to

$$V = \mathcal{GE}(T, \lambda_1) \oplus \cdots \oplus \mathcal{GE}(T, \lambda_K).$$

10. Given $A, B \in M(n, \mathbb{C})$, define $L_A, R_B : M(n, \mathbb{C}) \to M(n, \mathbb{C})$ by

$$L_A X = AX, \quad R_B X = XB.$$

Show that if $\operatorname{Spec} A = \{\lambda_j\}$, $\operatorname{Spec} B = \{\mu_k\}$ $(= \operatorname{Spec} B^t)$, then

$$\mathcal{GE}(L_A, \lambda_j) = \operatorname{Span}\{vw^t : v \in \mathcal{GE}(A, \lambda_j), w \in \mathbb{C}^n\},$$
$$\mathcal{GE}(R_B, \mu_k) = \operatorname{Span}\{vw^t : v \in \mathbb{C}^n, w \in \mathcal{GE}(B^t, \mu_k)\}.$$

Show that

$$\mathcal{GE}(L_A - R_B, \sigma) = \operatorname{Span}\{vw^t : v \in \mathcal{GE}(A, \lambda_j), w \in \mathcal{GE}(B^t, \mu_k), \sigma = \lambda_j - \mu_k\}.$$

11. In the setting of Exercise 10, show that if A is diagonalizable, then $\mathcal{GE}(L_A, \lambda_j) = \mathcal{E}(L_A, \lambda_j)$. Draw analogous conclusions if also B is diagonalizable.

12. In the setting of Exercise 10, show that if $\operatorname{Spec} A = \{\lambda_j\}$ and $\operatorname{Spec} B = \{\mu_k\}$, then

$$\operatorname{Spec}(L_A - R_B) = \{\lambda_j - \mu_k\}.$$

Deduce that if $C_A : M(n, \mathbb{C}) \to M(n, \mathbb{C})$ is defined by

$$C_A X = AX - XA,$$

then

$$\operatorname{Spec} C_A = \{\lambda_j - \lambda_k\}.$$

2.3. Triangular matrices and upper triangularization

We say an $n \times n$ matrix $A = (a_{jk})$ is upper triangular if $a_{jk} = 0$ for $j > k$, and strictly upper triangular if $a_{jk} = 0$ for $j \geq k$. Similarly we have the notion of lower triangular and strictly lower triangular matrices. Here are two examples:

$$A = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}; \tag{2.3.1}$$

A is upper triangular and B is strictly upper triangular; A^t is lower triangular and B^t strictly lower triangular. Note that $B^3 = 0$.

We say $T \in \mathcal{L}(V)$ is *nilpotent* provided $T^k = 0$ for some $k \in \mathbb{N}$. The following is a useful characterization of nilpotent transformations.

Proposition 2.3.1. *Let V be a finite-dimensional complex vector space, $N \in \mathcal{L}(V)$. The following are equivalent:*

$$N \text{ is nilpotent}, \tag{2.3.2}$$

$$\mathrm{Spec}(N) = \{0\}, \tag{2.3.3}$$

$$\text{There is a basis of } V \text{ for which } N \text{ is strictly upper triangular}, \tag{2.3.4}$$

$$\text{There is a basis of } V \text{ for which } N \text{ is strictly lower triangular}. \tag{2.3.5}$$

Proof. The implications (2.3.4) $\Rightarrow$ (2.3.2) and (2.3.5) $\Rightarrow$ (2.3.2) are easy. Also (2.3.4) implies the characteristic polynomial of N is λ^n (if $n = \dim V$), which is equivalent to (2.3.3), and similarly (2.3.5) $\Rightarrow$ (2.3.3). We need to establish a couple more implications.

To see that (2.3.2) $\Rightarrow$ (2.3.3), note that if $N^k = 0$ we can write

$$(N - \mu I)^{-1} = -\frac{1}{\mu}\Big(I - \frac{1}{\mu}N\Big)^{-1} = -\frac{1}{\mu}\sum_{\ell=0}^{k-1}\frac{1}{\mu^\ell}N^\ell, \tag{2.3.6}$$

whenever $\mu \neq 0$.

Next, given (2.3.3), $N : V \to V$ is not an isomorphism, so $V_1 = N(V)$ has dimension $\leq n - 1$. Now $N_1 = N|_{V_1} \in \mathcal{L}(V_1)$ also has only 0 as an eigenvalue, so $N_1(V_1) = V_2$ has dimension $\leq n - 2$, and so on. Thus $N^k = 0$ for sufficiently large k. We have (2.3.3) $\Rightarrow$ (2.3.2). Now list these spaces as $V = V_0 \supset V_1 \supset \cdots \supset V_{k-1}$, with $V_{k-1} \neq 0$ but $N(V_{k-1}) = 0$. Pick a basis for V_{k-1}, augment it as in Proposition 1.3.5 to produce a basis for V_{k-2}, and continue, obtaining in this fashion a basis of V, with respect to which N is strictly upper triangular. Thus (2.3.3) $\Rightarrow$ (2.3.4). On the other hand, if we reverse the order of this basis we have a basis with respect to which N is strictly lower triangular, so also (2.3.3) $\Rightarrow$ (2.3.5). The proof of Proposition 2.3.1 is complete. □

Remark. Having proven Proposition 2.3.1, we see another condition equivalent to (2.3.2)–(2.3.5):

$$N^k = 0, \quad \forall\ k \geq \dim V. \tag{2.3.7}$$

EXAMPLE. Consider

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

We have

$$N^2 = \begin{pmatrix} 6 & 0 & 6 \\ 0 & 0 & 0 \\ -6 & 0 & -6 \end{pmatrix}, \quad N^3 = 0.$$

Hence we have a chain $V = V_0 \supset V_1 \supset V_2$ as in the proof of Proposition 2.3.1, with

$$\begin{aligned} V_2 &= \operatorname{Span} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad V_1 = \operatorname{Span} \left\{ \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}, \\ V_0 &= \operatorname{Span} \left\{ \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\} = \operatorname{Span}\{v_1, v_2, v_3\}, \end{aligned} \tag{2.3.8}$$

and we have

$$Nv_1 = 0, \quad Nv_2 = -v_1, \quad Nv_3 = 3v_2,$$

so the matrix representation of N with respect to the basis $\{v_1, v_2, v_3\}$ is

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

Generally, if A is an upper triangular $n \times n$ matrix with diagonal entries $d_1, \dots, d_n$, the characteristic polynomial of A is

$$\det(\lambda I - A) = (\lambda - d_1) \cdots (\lambda - d_n), \tag{2.3.9}$$

by Proposition 1.5.7, so $\operatorname{Spec}(A) = \{d_j\}$. If $d_1, \dots, d_n$ are all distinct it follows that $\mathbb{F}^n$ has a basis of eigenvectors of A.

We can show that whenever V is a finite-dimensional complex vector space and $T \in \mathcal{L}(V)$, then V has a basis with respect to which T is upper triangular. In fact, we can say a bit more. Recall what was established in Proposition 2.2.6. If $\operatorname{Spec}(T) = \{\lambda_\ell : 1 \le \ell \le K\}$ and $S_\ell = \{v_{\ell 1}, \dots, v_{\ell, d_\ell}\}$ is a basis of $\mathcal{GE}(T, \lambda_\ell)$, then $S = S_1 \cup \cdots \cup S_K$ is a basis of V. Now look more closely at

$$T_\ell : V_\ell \longrightarrow V_\ell, \quad V_\ell = \mathcal{GE}(T, \lambda_\ell),\ T_\ell = T\big|_{V_\ell}. \tag{2.3.10}$$

The result (2.2.5) says $\operatorname{Spec}(T_\ell) = \{\lambda_\ell\}$, i.e., $\operatorname{Spec}(T_\ell - \lambda_\ell I) = \{0\}$, so we can apply Proposition 2.3.1. Thus we can pick a basis S_ℓ of V_ℓ with respect to which $T_\ell - \lambda_\ell I$ is strictly upper triangular, hence in which T_ℓ takes the form

$$A_\ell = \begin{pmatrix} \lambda_\ell & & * \\ & \ddots & \\ 0 & & \lambda_\ell \end{pmatrix}. \tag{2.3.11}$$

Then, with respect to the basis $S = S_1 \cup \cdots \cup S_K$, T has a matrix representation A consisting of blocks A_ℓ, given by (2.3.11). It follows that

$$K_T(\lambda) = \det(\lambda I - T) = \prod_{\ell=1}^{K} (\lambda - \lambda_\ell)^{d_\ell}, \quad d_\ell = \dim V_\ell. \tag{2.3.12}$$

This matrix representation also makes it clear that $K_T(T)|_{V_\ell} = 0$ for each $\ell \in \{1, \dots, K\}$ (cf. (2.3.7)). This establishes the following result, known as the *Cayley-Hamilton theorem*.

Proposition 2.3.2. *If $T \in \mathcal{L}(V)$, $\dim V < \infty$, and $K_T(\lambda)$ is its characteristic polynomial, then*

$$K_T(T) = 0 \quad \text{on} \quad V. \tag{2.3.13}$$

Consequently,

$$K_T(\lambda) \quad \text{is a polynomial multiple of} \quad m_T(\lambda). \tag{2.3.14}$$

Recall that $m_T(\lambda)$, the minimal polynomial of T, introduced in (2.2.14), has the property that $\mathcal{I}(m_T)$ consists of all polynomials $p(\lambda)$ such that $p(T) = 0$.

We next use the upper triangularization process described above to prove the following.

Proposition 2.3.3. *If $A, B \in M(n, \mathbb{C})$, then AB and BA have the same eigenvalues, with the same multiplicity. Consequently,*

$$\dim \mathcal{GE}(AB, \lambda_j) = \dim \mathcal{GE}(BA, \lambda_j).$$

Proof. An equivalent conclusion is

$$\det(AB - \lambda I) = \det(BA - \lambda I), \quad \forall\, \lambda \in \mathbb{C}, \tag{2.3.15}$$

in light of (2.3.12). Now if B is invertible, we have $AB = B^{-1}(BA)B$, so AB and BA are similar, and (2.3.15) follows. However, if neither A nor B is invertible, an additional argument is needed. We proceed as follows. By Proposition 1.5.8, we can find invertible $B_\nu \in M(n, \mathbb{C})$ such that $B_\nu \to B$ as $\nu \to \infty$. Then

$$\det(AB - \lambda I) = \lim_{\nu \to \infty} \det(AB_\nu - \lambda I). \tag{2.3.16}$$

But for each ν, AB_ν and $B_\nu A$ are similar, so (2.3.16) is equal to

$$\lim_{\nu \to \infty} \det(B_\nu A - \lambda I) = \det(BA - \lambda I), \tag{2.3.17}$$

so we have Proposition 2.3.3. □

Remark. From the hypotheses of Proposition 2.3.3 we *cannot* deduce that AB and BA are similar. Here is a counterexample.

$$\begin{aligned} A = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ \Longrightarrow AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad BA = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. \end{aligned} \tag{2.3.18}$$

Companion matrices

Given a polynomial $p(\lambda)$ of degree n,

$$p(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0, \quad a_j \in \mathbb{C}, \tag{2.3.19}$$

one associates the following $n \times n$ matrix,

$$A = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}, \tag{2.3.20}$$

with 1s above the diagonal and the negatives of the coefficients $a_0, \ldots, a_{n-1}$ of $p(\lambda)$ along the bottom row. This is called the companion matrix of $p(\lambda)$. It has the following significant property.

Proposition 2.3.4. *If $p(\lambda)$ is a polynomial of the form* (2.3.19)*, with companion matrix A, given by* (2.3.20)*, then*

$$p(\lambda) = \det(\lambda I - A). \tag{2.3.21}$$

Proof. We look at

$$\lambda I - A = \begin{pmatrix} \lambda & -1 & \cdots & 0 & 0 \\ 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & & \lambda & -1 \\ a_0 & a_1 & \cdots & a_{n-2} & \lambda + a_{n-1} \end{pmatrix}, \tag{2.3.22}$$

and compute its determinant by expanding by minors down the first column. We see that

$$\det(\lambda I - A) = \lambda \det(\lambda I - \widetilde{A}) + (-1)^{n-1} a_0 \det B, \tag{2.3.23}$$

where

$$\begin{aligned} &\widetilde{A} \text{ is the companion matrix of } \lambda^{n-1} + a_{n-1}\lambda^{n-2} + \cdots + a_1, \\ &B \text{ is lower triangular, with } -1\text{s on the diagonal.} \end{aligned} \tag{2.3.24}$$

By induction on n, we have $\det(\lambda I - \widetilde{A}) = \lambda^{n-1} + a_{n-1}\lambda^{n-2} + \cdots + a_1$, while the transpose of (1.5.55) implies $\det B = (-1)^{n-1}$. Substituting this into (2.3.23) gives (2.3.21). □

Exercises

1. Consider

$$A_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \\ 3 & 2 & 1 \end{pmatrix}.$$

Compute the characteristic polynomial of each A_j and verify that these matrices satisfy the Caley-Hamilton theorem, (2.3.13).

2. Let $\mathcal{P}_k$ denote the space of polynomials of degree $\leq k$ in x, and consider

$$D : \mathcal{P}_k \longrightarrow \mathcal{P}_k, \quad Dp(x) = p'(x).$$

Show that $D^{k+1} = 0$ on $\mathcal{P}_k$ and that $\{1, x, \dots, x^k\}$ is a basis of $\mathcal{P}_k$ with respect to which D is strictly upper triangular.

3. Use the identity

$$(I - D)^{-1} = \sum_{\ell=0}^{k+1} D^\ell, \quad \text{on} \ \ \mathcal{P}_k,$$

to obtain a solution $u \in \mathcal{P}_k$ to

$$u' - u = x^k. \tag{2.3.25}$$

4. Use the equivalence of (2.3.25) with

$$\frac{d}{dx}(e^{-x}u) = x^k e^{-x}$$

to obtain a formula for

$$\int x^k e^{-x}\, dx.$$

5. The proof of Proposition 2.3.1 given above includes the chain of implications

$$(2.3.4) \Rightarrow (2.3.2) \Leftrightarrow (2.3.3) \Rightarrow (2.3.4).$$

Use Proposition 2.2.4 to give another proof that

$$(2.3.3) \Rightarrow (2.3.2).$$

6. Establish the following variant of Proposition 2.2.4. Let $K_T(\lambda)$ be the characteristic polynomial of T, as in (2.3.12), and set

$$P_\ell(\lambda) = \prod_{j \neq \ell} (\lambda - \lambda_j)^{d_j} = \frac{K_T(\lambda)}{(\lambda - \lambda_\ell)^{d_\ell}}.$$

Show that

$$\mathcal{GE}(T, \lambda_\ell) = \mathcal{R}(P_\ell(T)).$$

7. Show that, if λ_j is a root of $\det(\lambda I - A) = 0$ of multiplicity d_j, then

$$\dim \mathcal{GE}(A, \lambda_j) = d_j, \quad \text{and} \quad \mathcal{GE}(A, \lambda_j) = \mathcal{N}((A - \lambda_j I)^{d_j}).$$

For a refinement of the latter identity, see Exercise 4 in the sext section.

2.4. The Jordan canonical form

Let V be an n-dimensional complex vector space, and suppose $T : V \to V$. The following result gives the Jordan canonical form for T.

Proposition 2.4.1. *There is a basis of V with respect to which T is represented as a direct sum of blocks of the form*

$$\begin{pmatrix} \lambda_j & 1 & & \\ & \lambda_j & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_j \end{pmatrix}. \tag{2.4.1}$$

These blocks are known as Jordan blocks. In light of Proposition 2.2.6 on generalized eigenspaces, together with Proposition 2.3.1 characterizing nilpotent operators and the discussion around (2.3.10), to prove Proposition 2.4.1 it suffices to establish such a Jordan canonical form for a nilpotent transformation $N : V \to V$. (Then $\lambda_j = 0$.) We turn to this task.

Given $v_0 \in V$, let m be the smallest integer such that $N^m v_0 = 0$; $m \leq n$. If $m = n$, then $\{v_0, Nv_0, \dots, N^{m-1}v_0\}$ gives a basis of V putting N in Jordan canonical form, with one block of the form (2.4.1) (with $\lambda_j = 0$). In any case, we call $\{v_0, \dots, N^{m-1}v_0\}$ a *Jordan string* (or *string*, for short). To obtain a Jordan canonical form for N, it will suffice to find a basis of V consisting of a family of strings. We will establish that this can be done by induction on $\dim V$. This result is clear for $\dim V \leq 1$.

So, given a nilpotent $N : V \to V$, we can assume inductively that $V_1 = N(V)$ has a basis that is a union of strings:

$$\{v_j, Nv_j, \dots, N^{\ell_j}v_j\}, \quad 1 \leq j \leq d. \tag{2.4.2}$$

Furthermore, each v_j has the form $v_j = Nw_j$ for some $w_j \in V$. Hence we have the following strings in V:

$$\{w_j, v_j = Nw_j, Nv_j, \dots, N^{\ell_j}v_j\}, \quad 1 \leq j \leq d. \tag{2.4.3}$$

We claim that the vectors in (2.4.3) are linearly independent. To see this, we apply N to a linear combination and invoke the independence of the vectors in (2.4.2).

In more detail, suppose there is a linear dependence relation,

$$\sum_{j=1}^{d} b_j w_j + \sum_{j=1}^{d} \sum_{\ell=0}^{\ell_j} a_{j\ell} N^\ell v_j = 0. \tag{2.4.4}$$

Applying N yields

$$\sum_{j=1}^{d} b_j v_j + \sum_{j=1}^{d} \sum_{\ell=0}^{\ell_j - 1} a_{j\ell} N^{\ell+1} v_j = 0. \tag{2.4.5}$$

This is a linear dependence relation among the vectors listed in (2.4.2), so

$$b_j = 0, \quad a_{j\ell} = 0, \quad \forall\, j \in \{1, \dots, d\},\ \ell \leq \ell_j - 1. \tag{2.4.6}$$

Hence (2.4.4) yields

$$\sum_{j=1}^{d} a_{j,\ell_j} v_j = 0, \tag{2.4.7}$$

again a linear dependence relation among vectors listed in (2.4.2), so

$$a_{j,\ell_j} = 0, \quad \forall\, j \in \{1, \dots, d\}, \tag{2.4.8}$$

and we have linear independence of all the vectors listed in (2.4.3).

To proceed, note that the vectors in

$$\{N^{\ell_j} v_j : 1 \leq j \leq d\} \tag{2.4.9}$$

all belong to $\mathcal{N}(N)$ and are linearly independent. If this set does not span $\mathcal{N}(N)$, complete it to a basis of $\mathcal{N}(N)$, by adding

$$\{\xi_1, \dots, \xi_\nu\}. \tag{2.4.10}$$

We now claim that the vectors listed in (2.4.3) *and* (2.4.10) are linearly independent. Indeed, suppose there is a linear dependence relation

$$\sum_{i=1}^{\nu} c_i \xi_i + \sum_{j=1}^{d} b_j w_j + \sum_{j=1}^{d} \sum_{\ell=0}^{\ell_j} a_{j\ell} N^\ell v_j = 0. \tag{2.4.11}$$

Applying N yields an identity of the form (2.4.5), which in turn yields identities of the form (2.4.6). Hence (2.4.11) yields

$$\sum_{i=1}^{\nu} c_i \xi_i + \sum_{j=1}^{d} a_{j,\ell_j} N^{\ell_j} v_j = 0, \tag{2.4.12}$$

thus yielding

$$c_i = 0, \ \ \forall\, i \in \{1, \dots, \nu\}, \quad a_{j,\ell_j} = 0, \ \ \forall\, j \in \{1, \dots, d\}, \tag{2.4.13}$$

since (2.4.9)–(2.4.10) form a basis of $\mathcal{N}(N)$. We have the asserted linear independence of

$$\{w_j, v_j, \dots, N^{\ell_j} v_j\}, \ 1 \leq j \leq d, \quad \{\xi_1, \dots, \xi_\nu\}. \tag{2.4.14}$$

Finally, we claim this is a *basis* of V.

To see this, note that the number of vectors in (2.4.3) is $\dim \mathcal{R}(N) + d$, while $\dim \mathcal{N}(N) = d + \nu$. Hence the number of vectors in (2.4.14) is

$$\begin{aligned} \dim \mathcal{R}(N) + d + \nu &= \dim \mathcal{R}(N) + \dim \mathcal{N}(N) \\ &= \dim V. \end{aligned} \tag{2.4.15}$$

Thus (2.4.14) yields a basis of V, and hence the strings (2.4.3) together with $\{\xi_1\}, \dots, \{\xi_\nu\}$ form a string basis of V. This proves Proposition 2.4.1. □

There is some choice in producing bases putting $T \in \mathcal{L}(V)$ in block form. So we ask, in what sense is the Jordan form canonical? The answer is that the sizes of the various blocks is independent of the choices made. To show this, again it

suffices to consider the case of a nilpotent $N : V \to V$. Let $\beta(k)$ denote the number of blocks of size $k \times k$ in a Jordan decomposition of N. Equivalently,

$$\beta(k) = \text{number of Jordan strings of length } k, \tag{2.4.16}$$

in such a Jordan decomposition of N. Then

$$\beta = \sum_k \beta(k) \tag{2.4.17}$$

is the total number of Jordan blocks, and clearly

$$\beta = \dim \mathcal{N}(N). \tag{2.4.18}$$

On the other hand, a direct inspection of the Jordan canonical form yields the following.

Proposition 2.4.2. *Let $N \in \mathcal{L}(V)$ be nilpotent, $\dim V < \infty$, and take a string basis of V. If*

$$\gamma(k) = \textit{number of Jordan strings of length} > k, \tag{2.4.19}$$

then

$$\gamma(k) = \dim \mathcal{N}(N^{k+1}) - \dim \mathcal{N}(N^k). \tag{2.4.20}$$

To connect $\gamma(k)$ with $\beta(k)$, note that

$$\gamma(k) = \sum_{\ell > k} \beta(\ell), \tag{2.4.21}$$

so

$$\beta(k) = \gamma(k-1) - \gamma(k). \tag{2.4.22}$$

To illustrate the steps taken in the proof of Proposition 2.4.1, to treat nilpotent $N \in \mathcal{L}(V)$, we work through the following example. Take

$$N = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{2.4.23}$$

This matrix is strictly upper triangular, hence clearly nilpotent, but not in Jordan canonical form. We seek a string basis. To start, we have

$$\mathcal{R}(N) = \text{Span}\{e_1, e_3\}, \tag{2.4.24}$$

where $\{e_1, \dots, e_4\}$ denotes the standard basis of $\mathbb{C}^4$. Note that

$$N(e_3) = e_1, \quad N(e_1) = 0, \tag{2.4.25}$$

so $\{e_3, e_1\}$ forms a string basis of $\mathcal{R}(N)$. Furthermore, $e_3 = N(e_4 - e_3)$, so

$$\{e_4 - e_3, e_3, e_1\} \tag{2.4.26}$$

is a longer string in $V = \mathbb{C}^4$, as in (2.4.3). As noted above, $e_1 \in \mathcal{N}(N)$. Since $\mathcal{R}(N)$ is two-dimensional, so is $\mathcal{N}(N)$, and we can check that

$$\mathcal{N}(N) = \text{Span}\{e_1, e_2 - e_3\}. \tag{2.4.27}$$

Consequently, a string basis of $\mathbb{C}^4$ consists of two strings:

$$\{e_4 - e_3, e_3, e_1\} \quad \text{and} \quad \{e_2 - e_3\}. \tag{2.4.28}$$

If we set

$$v_4 = e_2 - e_3, \quad v_3 = e_4 - e_3, \quad v_2 = e_3, \quad v_1 = e_1, \tag{2.4.29}$$

then the matrix representation of N with respect to the basis $\{v_1, v_2, v_3, v_4\}$ is

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ & 0 & 1 & 0 \\ & & 0 & 0 \\ & & & 0 \end{pmatrix}. \tag{2.4.30}$$

This is the Jordan canonical form for (2.4.23). There are two Jordan blocks:

$$\begin{pmatrix} 0 & 1 & 0 \\ & 0 & 1 \\ & & 0 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 \end{pmatrix}. \tag{2.4.31}$$

Finally, one can calculate $\dim \mathcal{N}(N^k)$ and check the formula (2.4.19)–(2.4.20) against the size of the strings in (2.4.31).

Exercises

1. Produce Jordan canonical forms for each of the following matrices.

$$\begin{pmatrix} 2 & 3 & 3 \\ 0 & 2 & 3 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ -1 & 0 & -1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 0 \\ 3 & 1 & 3 \\ 0 & -2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}.$$

2. Produce the Jordan canonical form for the companion matrix associated with the polynomial $p(\lambda) = \lambda(\lambda - 1)^2$.

3. In the setting of Exercise 2, take $p(\lambda) = (\lambda - 1)^3$.

4. Assume $A \in M(n, \mathbb{C})$ and, for each $\lambda_j \in \operatorname{Spec} A$, the largest Jordan block of A, of the form (2.4.1), has size $k_j \times k_j$. Show that the minimal polynomial $m_A(\lambda)$ of A is

$$m_A(\lambda) = \prod_j (\lambda - \lambda_j)^{k_j},$$

and that

$$\mathcal{GE}(A, \lambda_j) = \mathcal{N}\big((A - \lambda_j I)^{k_j}\big).$$

Show that $m_A(\lambda) = K_A(\lambda)$ (the characteristic polynomial) if and only if each $\lambda_j \in \operatorname{Spec} A$ appears in only *one* Jordan block.

5. Guided by Exercises 2–3, formulate a conjecture about the minimal polynomial and the Jordan normal form of a companion matrix. See if you can prove it. Relate this to Exercise 11 in §3.7 (when you get to that).

2.A. The fundamental theorem of algebra

The following result is known as the fundamental theorem of algebra. It played a crucial role in §2.1, to guarantee the existence of eigenvalues of a complex $n \times n$ matrix.

Theorem 2.A.1. *If $p(z)$ is a nonconstant polynomial (with complex coefficients), then $p(z)$ must have a complex root.*

Proof. We have, for some $n \geq 1,\ a_n \neq 0$,

$$\begin{aligned} p(z) &= a_n z^n + \cdots + a_1 z + a_0 \\ &= a_n z^n \Big(1 + R(z)\Big), \quad |z| \to \infty, \end{aligned} \tag{2.A.1}$$

where

$$|R(z)| \leq \frac{C}{|z|}, \quad \text{for } |z| \text{ large.}$$

This implies

$$\lim_{|z|\to\infty} |p(z)| = \infty. \tag{2.A.2}$$

Picking $R \in (0, \infty)$ such that

$$\inf_{|z|\geq R} |p(z)| > |p(0)|, \tag{2.A.3}$$

we deduce that

$$\inf_{|z|\leq R} |p(z)| = \inf_{z\in\mathbb{C}} |p(z)|. \tag{2.A.4}$$

Since $D_R = \{z : |z| \leq R\}$ is closed and bounded and p is continuous, there exists $z_0 \in D_R$ such that

$$|p(z_0)| = \inf_{z\in\mathbb{C}} |p(z)|. \tag{2.A.5}$$

(For further discussion of this point, see Proposition 1.10.6 of [**10**].) The proof is hence completed by the following lemma. □

Lemma 2.A.2. *If $p(z)$ is a nonconstant polynonial and* (2.A.5) *holds, then $p(z_0) = 0$.*

Proof. Suppose to the contrary that

$$p(z_0) = a \neq 0. \tag{2.A.6}$$

We can write

$$p(z_0 + \zeta) = a + q(\zeta), \tag{2.A.7}$$

where $q(\zeta)$ is a nonconstant polynomial in ζ, satisfying $q(0) = 0$. Hence, for some $k \geq 1$ and $b \neq 0$, we have $q(\zeta) = b\zeta^k + \cdots + b_n\zeta^n$, i.e.,

$$q(\zeta) = b\zeta^k + \zeta^{k+1} r(\zeta), \quad |r(\zeta)| \leq C, \tag{2.A.8}$$

for $|\zeta| \leq 1$, so, with $\zeta = \varepsilon\omega,\ \omega \in S^1 = \{\omega : |\omega| = 1\}$,

$$p(z_0 + \varepsilon\omega) = a + b\omega^k\varepsilon^k + (\varepsilon\omega)^{k+1} r(\varepsilon\omega), \quad \varepsilon \searrow 0. \tag{2.A.9}$$

Pick $\omega \in S^1$ such that

$$\frac{b}{|b|}\omega^k = -\frac{a}{|a|}, \tag{2.A.10}$$

which is possible since $a \neq 0$ and $b \neq 0$. Then

$$p(z_0 + \varepsilon\omega) = a\Big(1 - \Big|\frac{b}{a}\Big|\varepsilon^k\Big) + (\varepsilon\omega)^{k+1} r(\varepsilon\omega), \tag{2.A.11}$$

with $r(\zeta)$ as in (2.A.8), which contradicts (2.A.5) for $\varepsilon > 0$ small enough. Thus (2.A.6) is impossible. This proves Lemma 2.A.2, hence Theorem 2.A.1. □

Now that we have shown that $p(z)$ in (2.A.1) must have one root, we can show it has n roots (counting multiplicity).

Proposition 2.A.3. *For a polynomial $p(z)$ of degree n, as in* (2.A.1)*, there exist $r_1, \dots, r_n \in \mathbb{C}$ such that*

$$p(z) = a_n(z - r_1) \cdots (z - r_n). \tag{2.A.12}$$

Proof. We have shown that $p(z)$ has one root; call it r_1. Dividing $p(z)$ by $z - r_1$, we have

$$p(z) = (z - r_1)\tilde{p}(z) + q, \tag{2.A.13}$$

where $\tilde{p}(z) = a_n z^{n-1} + \cdots + \tilde{a}_0$ and q is a polynomial of degree < 1, i.e., a constant. Setting $z = r_1$ in (2.A.13) yields $q = 0$, i.e.,

$$p(z) = (z - r_1)\tilde{p}(z). \tag{2.A.14}$$

Since $\tilde{p}(z)$ is a polynomial of degree $n - 1$, the result (2.A.12) follows by induction on n. □

Remark 1. The numbers r_j, $1 \leq j \leq n$, in (2.A.12) are the roots of $p(z)$. If k of them coincide (say with r_ℓ), we say r_ℓ is a root of multiplicity k. If r_ℓ is distinct from r_j for all $j \neq \ell$, we say r_ℓ is a simple root.

Remark 2. In complex analysis texts, like [**15**], one can find proofs of the fundamental theorem of algebra that are even shorter than that given above, but that use more advanced techniques.

Chapter 3

Linear algebra on inner product spaces

Many important problems in linear algebra arise in the setting of vector spaces equipped with an additional structure, an inner product, which gives them metric properties familiar in Euclidean geometry. The first examples are Euclidean spaces $\mathbb{R}^n$, with the dot product, defined for vectors $v = (v_1, \dots, v_n)$ and $w = (w_1, \dots, w_n)$ by

$$v \cdot w = v_1 w_1 + \cdots + v_n w_n. \tag{3.0.1}$$

On $\mathbb{C}^n$ one has a Hermitian inner product,

$$(v, w) = v_1 \overline{w}_1 + \cdots + v_n \overline{w}_n. \tag{3.0.2}$$

More general inner products on finite-dimensional real or complex vector spaces are introduced in §3.1. A *norm* is defined by

$$\|v\|^2 = (v, v). \tag{3.0.3}$$

This in turn defines the distance between vectors v and w, as $\|v - w\|$. Results on the inner product lead to the triangle inequality,

$$\|v + w\| \le \|v\| + \|w\|. \tag{3.0.4}$$

We show that if V is an n-dimensional inner product space, it has an orthonormal basis $\{v_1, \dots, v_n\}$, i.e., a basis satisfying

$$(v_j, v_k) = \delta_{jk}. \tag{3.0.5}$$

Such a basis gives rise to an isomorphism of V with $\mathbb{R}^n$ or $\mathbb{C}^n$ (depending on whether V is a real or a complex vector space), taking the inner product on V to that on $\mathbb{F}^n$ given above.

Inner products and norms on vector spaces give rise to norms on linear transformations, both the *operator norm* $\|A\|$ and the *Hilbert-Schmidt norm* $\|A\|_{\mathrm{HS}}$. These

norms satisfy triangle inequalities. As for compositions, we have

$$\|AB\| \le \|A\| \cdot \|B\|, \quad \|AB\|_{\mathrm{HS}} \le \|A\| \cdot \|B\|_{\mathrm{HS}} \le \|A\|_{\mathrm{HS}} \|B\|_{\mathrm{HS}}, \tag{3.0.6}$$

as seen in §3.2. Also associated to a linear map $A : V \to W$ between inner product spaces is the adjoint, $A^* : W \to V$, satisfying

$$(Av, w) = (v, A^*w), \quad \forall\, v \in V,\ w \in W. \tag{3.0.7}$$

There are several special classes of linear transformations on an inner product space V, defined by the relation between such an operator A and its adjoint A^*. We say A is self adjoint if $A^* = A$, skew adjoint if $A^* = -A$. If $A^* = A^{-1}$, we say A is orthogonal if V is a real vector space, and unitary if V is a complex vector space. We study these classes in §§3.3–3.4. We show that in all these cases, V has an orthonormal basis of eigenvectors of A, is V is complex. If V is a real vector space, it has an orthonormal basis of eigenvectors of A when A is self adjoint, and special orthonormal bases of a different sort (involving 2×2 blocks) if A is skew adjoint or orthogonal.

In §3.5 we establish a result of Schur: if V is a complex inner product space of dimension n and $A \in \mathcal{L}(V)$, then V has an orthonormal basis with respect to which A is in upper triangular form. This has some of the flavor of the upper triangularization result of §2.3, but there are also significant differences, and the proofs are completely different. There follows in §3.6 a result on polar decomposition: if $A \in \mathcal{L}(V)$ is invertible, it can be factored as

$$A = KP, \tag{3.0.8}$$

with K unitary and P positive definite. This factorization is then extended to a "singular value decomposition."

In §3.7 we take up the matrix exponential. This arises to solve $n \times n$ systems of differential equations,

$$\frac{dx}{dt} = Ax, \quad x(0) = v, \tag{3.0.9}$$

with $A \in M(n, \mathbb{C})$, $v \in \mathbb{C}^n$. We construct a solution to (3.0.9) as a power series, yielding

$$x(t) = e^{tA}v, \quad e^{tA} = \sum_{k=0}^{\infty} \frac{t^k}{k!} A^k. \tag{3.0.10}$$

Convergence of such a power series follows from operator norm estimates established in §3.2, including (3.0.6). In Chapter 2 we noted that (3.0.9) is solved by $x(t) = e^{t\lambda}v$ provided v is a λ-eigenvector of A, i.e., $v \in \mathcal{E}(A, \lambda)$, and we advertised an extension to more general $v \in \mathcal{GE}(A, \lambda)$ here. The use of the matrix exponential provides a very natural approach to such a formula.

Going in the opposite direction, we use the matrix exponential as a tool to obtain a second proof that, if $A \in M(n, \mathbb{C})$, then $\mathbb{C}^n$ has a basis of generalized eigenvectors of A, a proof that is completely different from that given in Chapter 2.

Section 3.8 deals with the discrete Fourier transform (DFT), which acts on functions $f : \mathbb{Z} \to \mathbb{C}$ that are periodic of period n, or equivalently functions on $\mathbb{Z}/(n)$,

which consists of equivalence classes of integers "mod n." The translation operator $Tf(k) = f(k+1)$ is a unitary operator on this space, and the DFT represents f in terms of an orthonormal basis of eigenvectors of T. The DFT diagonalizes an important class of operators known as convolution operators. We describe the Fast Fourier Transform (FFT), which in turn allows for a fast evaluation of convolution operators.

3.1. Inner products and norms

Vectors in $\mathbb{R}^n$ have a dot product, given by

$$v \cdot w = v_1 w_1 + \cdots + v_n w_n, \tag{3.1.1}$$

where $v = (v_1, \dots, v_n)$, $w = (w_1, \dots, w_n)$. Then the norm of v, denoted $\|v\|$, is given by

$$\|v\|^2 = v \cdot v = v_1^2 + \cdots + v_n^2. \tag{3.1.2}$$

The geometrical significance of $\|v\|$ as the distance of v from the origin is a version of the Pythagorean theorem. If $v, w \in \mathbb{C}^n$, we use

$$(v, w) = v \cdot \overline{w} = v_1 \overline{w}_1 + \cdots + v_n \overline{w}_n, \tag{3.1.3}$$

and then

$$\|v\|^2 = (v, v) = |v_1|^2 + \cdots + |v_n|^2; \tag{3.1.4}$$

here, if $v_j = x_j + iy_j$, with $x_j, y_j \in \mathbb{R}$, we have $\overline{v}_j = x_j - iy_j$, and $|v_j|^2 = x_j^2 + y_j^2$.

The objects (3.1.1) and (3.1.3) are special cases of *inner products*. Generally, an inner product on a vector space (over $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$) assigns to vectors $v, w \in V$ the quantity $(v, w) \in \mathbb{F}$, in a fashion that obeys the following three rules:

$$(a_1 v_1 + a_2 v_2, w) = a_1(v_1, w) + a_2(v_2, w), \tag{3.1.5}$$

$$(v, w) = \overline{(w, v)}, \tag{3.1.6}$$

$$(v, v) > 0, \quad \text{unless } v = 0. \tag{3.1.7}$$

If $\mathbb{F} = \mathbb{R}$, then (3.1.6) just means $(v, w) = (w, v)$. Note that (3.1.5)–(3.1.6) together imply

$$(v, b_1 w_1 + b_2 w_2) = \overline{b}_1 (v, w_1) + \overline{b}_2 (v, w_2). \tag{3.1.8}$$

A vector space equipped with an inner product is called an inner product space. Inner products arise naturally in various contexts. For example,

$$(f, g) = \int_a^b f(x) \overline{g(x)}\, dx \tag{3.1.9}$$

defines an inner product on $C([a, b])$. It also defines an inner product on $\mathcal{P}$, the space of polynomials in x. Different choices of a and b yield different inner products on $\mathcal{P}$. More generally, one considers inner products of the form

$$(f, g) = \int_a^b f(x) \overline{g(x)}\, w(x)\, dx, \tag{3.1.10}$$

on various function spaces, where w is a positive, integrable "weight" function.

Given an inner product on V, one says the object $\|v\|$ defined by

$$\|v\| = \sqrt{(v, v)} \tag{3.1.11}$$

is the *norm* on V associated with the inner product. Generally, a norm on V is a function $v \mapsto \|v\|$ satisfying

$$\|av\| = |a| \cdot \|v\|, \quad \forall a \in \mathbb{F},\ v \in V, \tag{3.1.12}$$

$$\|v\| > 0, \quad \text{unless } v = 0, \tag{3.1.13}$$

$$\|v + w\| \leq \|v\| + \|w\|. \tag{3.1.14}$$

Here $|a|$ denotes the absolute value of $a \in \mathbb{F}$. The property (3.1.14) is called the *triangle inequality*. A vector space equipped with a norm is called a normed vector space.

If $\|v\|$ is given by (3.1.11), from an inner product satisfying (3.1.5)–(3.1.7), it is clear that (3.1.12)–(3.1.13) hold, but (3.1.14) requires a demonstration. Note that

$$\begin{aligned} \|v+w\|^2 &= (v+w, v+w) \\ &= \|v\|^2 + (v,w) + (w,v) + \|w\|^2 \\ &= \|v\|^2 + 2\,\mathrm{Re}\,(v,w) + \|w\|^2, \end{aligned} \tag{3.1.15}$$

while

$$(\|v\| + \|w\|)^2 = \|v\|^2 + 2\|v\| \cdot \|w\| + \|w\|^2. \tag{3.1.16}$$

Thus to establish (3.1.14) it suffices to prove the following, known as Cauchy's inequality:

Proposition 3.1.1. *For any inner product on a vector space V, with $\|v\|$ defined by* (3.1.11)*,*

$$|(v,w)| \le \|v\|\,\|w\|, \quad \forall\ v, w \in V. \tag{3.1.17}$$

Proof. We start with

$$0 \le \|v-w\|^2 = \|v\|^2 - 2\,\mathrm{Re}\,(v,w) + \|w\|^2, \tag{3.1.18}$$

which implies

$$2\,\mathrm{Re}\,(v,w) \le \|v\|^2 + \|w\|^2, \quad \forall\ v, w \in V. \tag{3.1.19}$$

Replacing v by αv for arbitrary $\alpha \in \mathbb{F}$ of absolute value 1 yields $2\,\mathrm{Re}\,\alpha(v,w) \le \|v\|^2 + \|w\|^2$. This implies

$$2|(v,w)| \le \|v\|^2 + \|w\|^2, \quad \forall\ v, w \in V. \tag{3.1.20}$$

Replacing v by tv and w by $t^{-1}w$ for arbitrary $t \in (0,\infty)$, we have

$$2|(v,w)| \le t^2\|v\|^2 + t^{-2}\|w\|^2, \quad \forall\ v, w \in V,\ t \in (0,\infty). \tag{3.1.21}$$

If we take $t^2 = \|w\|/\|v\|$, we obtain the desired inequality (3.1.17). (This assumes v and w are both nonzero, but (3.1.17) is trivial if v or w is 0.) □

There are other norms on vector spaces besides those that are associated with inner products. For example, on $\mathbb{F}^n$, we have

$$\|v\|_1 = |v_1| + \cdots + |v_n|, \quad \|v\|_\infty = \max_{1 \le k \le n} |v_k|, \tag{3.1.22}$$

and many others, but we will not dwell on this here.

If V is a finite-dimensional inner product space, a basis $\{u_1, \dots, u_n\}$ of V is called an *orthonormal basis* of V provided

$$(u_j, u_k) = \delta_{jk}, \quad 1 \le j, k \le n, \tag{3.1.23}$$

i.e.,

$$\|u_j\| = 1, \quad j \ne k \Rightarrow (u_j, u_k) = 0. \tag{3.1.24}$$

(When $(u_j, , u_k) = 0$, we say u_j and u_k are *orthogonal*.) When (3.1.23) holds, we have

$$\begin{aligned} v = a_1u_1 + \cdots + a_nu_n, \quad w = b_1u_1 + \cdots + b_nu_n \\ \Rightarrow (v, w) = a_1\overline{b}_1 + \cdots + a_n\overline{b}_n. \end{aligned} \tag{3.1.25}$$

It is often useful to construct orthonormal bases. The construction we now describe is called the Gramm-Schmidt construction.

Proposition 3.1.2. *Let $\{v_1, \ldots, v_n\}$ be a basis of V, an inner product space. Then there is an orthonormal basis $\{u_1, \ldots, u_n\}$ of V such that*

$$\mathrm{Span}\{u_j : j \le \ell\} = \mathrm{Span}\{v_j : j \le \ell\}, \quad 1 \le \ell \le n. \tag{3.1.26}$$

Proof. To begin, take

$$u_1 = \frac{1}{\|v_1\|}v_1. \tag{3.1.27}$$

Now define the linear transformation $P_1 : V \to V$ by $P_1v = (v, u_1)u_1$ and set

$$\tilde{v}_2 = v_2 - P_1v_2 = v_2 - (v_2, u_1)u_1. \tag{3.1.28}$$

We see that $(\tilde{v}_2, u_1) = (v_2, u_1) - (v_2, u_1) = 0$. Also $\tilde{v}_2 \neq 0$ since u_1 and v_2 are linearly independent. Hence we set

$$u_2 = \frac{1}{\|\tilde{v}_2\|}\tilde{v}_2. \tag{3.1.29}$$

Inductively, suppose we have an orthonormal set $\{u_1, \ldots, u_m\}$ with $m < n$ and (3.1.26) holding for $1 \le \ell \le m$. Then define $P_m : V \to V$ (the orthogonal projection of V onto $\mathrm{Span}(u_1, \ldots, u_m)$) by

$$P_mv = (v, u_1)u_1 + \cdots + (v, u_m)u_m, \tag{3.1.30}$$

and set

$$\begin{aligned} \tilde{v}_{m+1} &= v_{m+1} - P_mv_{m+1} \\ &= v_{m+1} - (v_{m+1}, u_1)u_1 - \cdots - (v_{m+1}, u_m)u_m. \end{aligned} \tag{3.1.31}$$

We see that

$$j \le m \Rightarrow (\tilde{v}_{m+1}, u_j) = (v_{m+1}, u_j) - (v_{m+1}, u_j) = 0. \tag{3.1.32}$$

Also, since $v_{m+1} \notin \mathrm{Span}\{v_1, \ldots, v_m\} = \mathrm{Span}\{u_1, \ldots, u_m\}$, it follows that $\tilde{v}_{m+1} \neq 0$. Hence we set

$$u_{m+1} = \frac{1}{\|\tilde{v}_{m+1}\|}\tilde{v}_{m+1}. \tag{3.1.33}$$

This completes the construction. □

EXAMPLE. Take $V = \mathcal{P}_2$, with basis $\{1, x, x^2\}$, and inner product given by

$$(p, q) = \int_{-1}^{1} p(x)\overline{q(x)}\, dx. \tag{3.1.34}$$

The Gramm-Schmidt construction gives first

$$u_1(x) = \frac{1}{\sqrt{2}}. \tag{3.1.35}$$

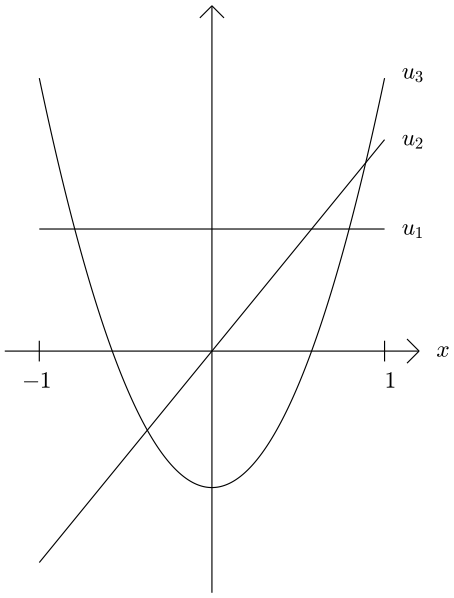

Figure 3.1.1. Orthogonal polynomials

Then

$$\tilde{v}_2(x) = x, \tag{3.1.36}$$

since by symmetry $(x, u_1) = 0$. Now $\int_{-1}^{1} x^2\,dx = 2/3$, so we take

$$u_2(x) = \sqrt{\frac{3}{2}}x. \tag{3.1.37}$$

Next

$$\tilde{v}_3(x) = x^2 - (x^2, u_1)u_1 = x^2 - \frac{1}{3}, \tag{3.1.38}$$

since by symmetry $(x^2, u_2) = 0$. Now $\int_{-1}^{1}(x^2 - 1/3)^2\,dx = 8/45$, so we take

$$u_3(x) = \sqrt{\frac{45}{8}}\Big(x^2 - \frac{1}{3}\Big). \tag{3.1.39}$$

See Figure 3.1.1 for graphs of these polynomials.

Exercises

1. Let V be a finite dimensional inner product space, and let W be a linear subspace of V. Show that any orthonormal basis $\{w_1, \dots, w_k\}$ of W can be enlarged to an orthonormal basis $\{w_1, \dots, w_k, u_1, \dots, u_\ell\}$ of V, with $k + \ell = \dim V$.
Hint. First enlarge the basis of W to a basis of V. Then apply Gramm-Schmidt.

2. As in Exercise 1, let V be a finite dimensional inner product space, and let W be a linear subspace of V. Define the orthogonal complement

$$W^\perp = \{v \in V : (v, w) = 0, \, \forall \, w \in W\}. \tag{3.1.40}$$

Show that

$$W^\perp = \operatorname{Span}\{u_1, \dots, u_\ell\}, \tag{3.1.41}$$

in the context of Exercise 1. Deduce that

$$(W^\perp)^\perp = W. \tag{3.1.42}$$

3. In the context of Exercise 2, show that

$$\dim V = n, \ \dim W = k \Longrightarrow \dim W^\perp = n - k.$$

4. Take V and W as in Exercise 1, and let $\{w_1, \dots, w_k\}$ be an orthonormal basis of W. Define $P \in \mathcal{L}(V)$ by

$$Pv = \sum_{j=1}^{k} (v, w_j) w_j. \tag{3.1.43}$$

Show that

$$P : V \to W, \quad P^2 = P, \quad I - P : V \to W^\perp. \tag{3.1.44}$$

Show that the properties in (3.1.44) uniquely determine P, i.e., if $Q \in \mathcal{L}(V)$ has these properties, then $Q = P$. In particular, P is independent of the choice of orthonormal basis of W.
Hint. Write $v = Pv + (I - P)v = Qv + (I - Q)v$ as

$$Pv - Qv = (I - Q)v - (I - P)v.$$

The left side is an element of W.
We call P the *orthogonal projection* of V onto W.

5. Construct an orthonormal basis of the $(n-1)$-dimensional vector space

$$V = \left\{ \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{R}^n : v_1 + \cdots + v_n = 0 \right\}.$$

6. Take $V = \mathcal{P}_2$, with basis $\{1, x, x^2\}$, and inner product

$$(p, q) = \int_0^1 p(x)\overline{q(x)}\, dx,$$

in contrast to (3.1.34). Construct an orthonormal basis of this inner product space.

7. Take V, with basis $\{1, \cos x, \sin x\}$, and inner product

$$(f, g) = \int_0^\pi f(x)\overline{g(x)}\, dx.$$

Construct an orthonormal basis of this inner product space.

8. Let $A \in G\ell(n, \mathbb{R})$ have columns $a_1, \dots, a_n \in \mathbb{R}^n$. Use the Gramm-Schmidt construction to produce the orthonormal basis $\{q_1, \dots, q_n\}$ of $\mathbb{R}^n$ such that $\text{Span}\{a_1, \dots, a_j\} = \text{Span}\{q_1, \dots, q_j\}$ for $1 \leq j \leq n$. Denote by Q the matrix with columns $q_1, \dots, q_n$. Show that

$$A = QR, \tag{3.1.45}$$

where R is the upper triangular matrix

$$R = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{n1} \\ & \alpha_{22} & \cdots & \alpha_{n2} \\ & & & \vdots \\ & & & \alpha_{nn} \end{pmatrix}, \quad \alpha_{jk} = (a_j, q_k). \tag{3.1.46}$$

This factorization is known as the QR factorization. See §3.4 for more. (We will see that $Q \in O(n)$.)
Hint. Show that

$$\begin{aligned} a_1 &= \alpha_{11} q_1 \\ a_2 &= \alpha_{21} q_1 + \alpha_{22} q_2 \\ &\vdots \\ a_n &= \alpha_{n1} q_1 + \cdots + \alpha_{nn} q_n. \end{aligned} \tag{3.1.47}$$

Exercises 9–12 make contact with topics in classical Euclidean geometry.

9. Recall that two vectors $x, y \in \mathbb{R}^n$ are orthogonal (we write $x \perp y$) if and only if $x \cdot y = 0$. Show that, for $x, y \in \mathbb{R}^n$,

$$x \perp y \Longleftrightarrow \|x + y\|^2 = \|x\|^2 + \|y\|^2.$$

10. Let $e_1, v \in \mathbb{R}^n$ and assume $\|e_1\| = \|v\| = 1$. Show that

$$e_1 - v \perp e_1 + v.$$

Hint. Expand $(e_1 - v) \cdot (e_1 + v)$.
See Figure 3.1.2 for the geometrical significance of this, when $n = 2$.

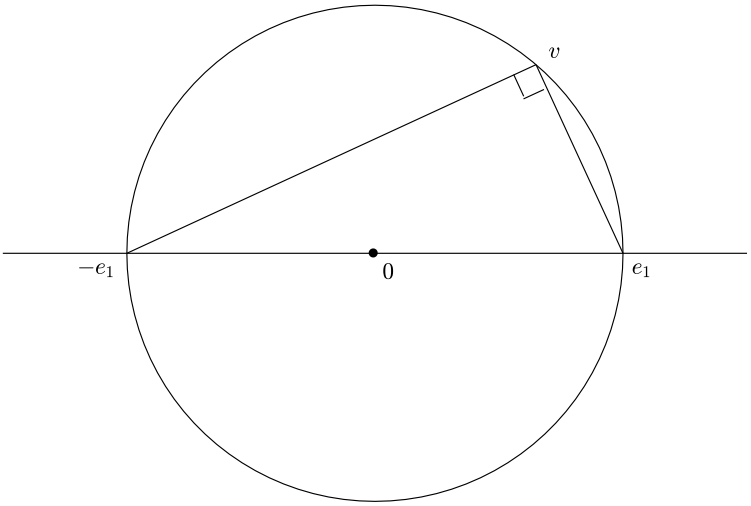

Figure 3.1.2. Right triangle in a circle

11. Let $S^1 = \{x \in \mathbb{R}^2 : \|x\| = 1\}$ denote the unit circle in $\mathbb{R}^2$, and set $e_1 = (1, 0) \in S^1$. Pick $a \in \mathbb{R}$ such that $0 < a < 1$, and set $u = (1 - a)e_1$. See Figure 3.1.3. Then pick

$$v \in S^1 \text{ such that } v - u \perp e_1, \text{ and set } b = \|v - e_1\|.$$

Show that

$$b = \sqrt{2a}. \tag{3.1.48}$$

Hint. Note that $1 - a = u \cdot e_1 = v \cdot e_1$, hence $a = 1 - v \cdot e_1$.
Now expand $b^2 = (v - e_1) \cdot (v - e_1)$.

12. Recall the approach to (3.1.48) in classical Euclidean geometry, using similarity of triangles, leading to

$$\frac{a}{b} = \frac{b}{2}.$$

What is the relevance of Exercise 10 to this?

Exercises 13–15 compare two different norms on a finite-dimensional vector space. Let V be an n-dimensional vector space, with a norm $\| \cdot \|$.

13. Take a basis $\mathcal{B} = \{u_1, \dots, u_n\}$ of V. Show that V has a unique inner product

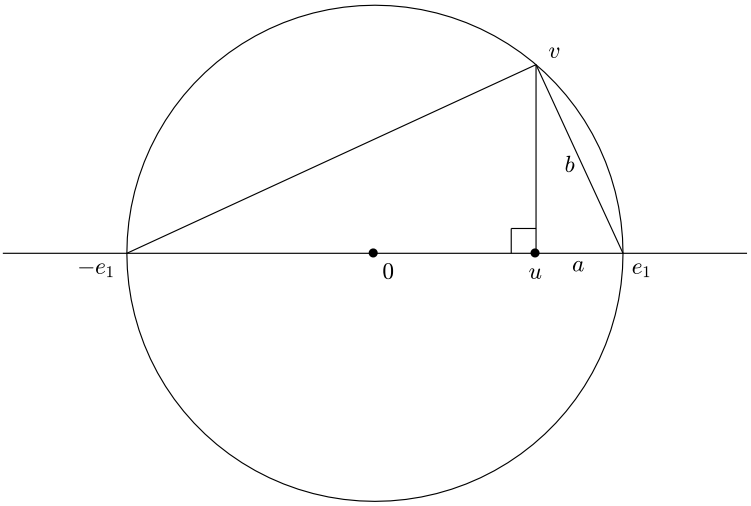

Figure 3.1.3. Geometric construction of $b = \sqrt{2a}$

(,) with respect to which $\mathcal{B}$ is an orthonormal basis of V. Denote the associated norm by $|\cdot|$, so

$$|v|^2 = (v, v).$$

14. Set $M = \max\{\|u_1\|, \dots, \|u_n\|\}$. Show that

$$\|v\| \leq nM\,|v|.$$

Hint. Start with $v = c_1u_1 + \cdots + c_nu_n$, $c_j = (v, u_j)$, and apply the triangle inequality to the resulting formula for $\|v\|$. Note that

$$|c_j| \leq |v|.$$

15. This exercise treats the reverse inequality. It uses concepts developed in Chapters 2–3 of [**10**]. The reader who has access to this text can fill in the details of the following argument.

(a) Consider $S = \{x \in V : |x| = 1\}$. This is a *compact* subset of V.

(b) Consider

$$\varphi : S \longrightarrow \mathbb{R}, \quad \varphi(v) = \|v\|.$$

It follows from Exercise 14 that φ is continuous.

(c) By (a) and (b), φ assumes a minimum on S. Hence there exists $w_0 \in V$ such that

$$|w_0| = 1, \quad \text{and} \quad \|w_0\| = \min\{\|v\| : |v| = 1\}.$$

(d) Since $\|\cdot\|$ is a norm, $\|w_0\| = \alpha > 0$. We deduce that, for all $v \in V$,

$$|v| \leq \frac{1}{\alpha}\|v\|.$$

3.2. Norm, trace, and adjoint of a linear transformation

If V and W are normed linear spaces and $T \in \mathcal{L}(V, W)$, we define

$$\|T\| = \sup\{\|Tv\| : \|v\| \leq 1\}. \tag{3.2.1}$$

Equivalently, $\|T\|$ is the smallest quantity K such that

$$\|Tv\| \leq K\|v\|, \quad \forall\ v \in V. \tag{3.2.2}$$

To see the equivalence, note that (3.2.2) holds if and only if $\|Tv\| \leq K$ for all v such that $\|v\| = 1$. We call $\|T\|$ the *operator norm* of T. If V and W are finite dimensional, this norm is finite for all $T \in \mathcal{L}(V, W)$. We will make some specific estimates below when V and W are inner product spaces.

Note that if also $S : W \to X$, another normed vector space, then

$$\|STv\| \leq \|S\|\,\|Tv\| \leq \|S\|\,\|T\|\,\|v\|, \quad \forall\ v \in V, \tag{3.2.3}$$

and hence

$$\|ST\| \leq \|S\|\,\|T\|. \tag{3.2.4}$$

In particular, we have by induction that

$$T : V \to V \Longrightarrow \|T^n\| \leq \|T\|^n. \tag{3.2.5}$$

This will be useful when we discuss the exponential of a linear transformation, in §3.7.

We turn to the notion of the *trace* of a transformation $T \in \mathcal{L}(V)$, given $\dim V < \infty$. We start with the trace of an $n \times n$ matrix, which is simply the sum of the diagonal elements:

$$A = (a_{jk}) \in M(n, \mathbb{F}) \Longrightarrow \operatorname{Tr} A = \sum_{j=1}^{n} a_{jj}. \tag{3.2.6}$$

Note that if also $B = (b_{jk}) \in M(n, \mathbb{F})$, then

$$\begin{aligned} AB = C = (c_{jk}), \quad c_{jk} &= \sum_{\ell} a_{j\ell} b_{\ell k}, \\ BA = D = (d_{jk}), \quad d_{jk} &= \sum_{\ell} b_{j\ell} a_{\ell k}, \end{aligned} \tag{3.2.7}$$

and hence

$$\operatorname{Tr} AB = \sum_{j,\ell} a_{j\ell} b_{\ell j} = \operatorname{Tr} BA. \tag{3.2.8}$$

Hence, if B is invertible,

$$\operatorname{Tr} B^{-1}AB = \operatorname{Tr} ABB^{-1} = \operatorname{Tr} A. \tag{3.2.9}$$

Thus if $T \in \mathcal{L}(V)$, we can choose a basis $S = \{v_1, \dots, v_n\}$ of V, if $\dim V = n$, and define

$$\operatorname{Tr} T = \operatorname{Tr} A, \quad A = \mathcal{M}_S^S(T), \tag{3.2.10}$$

and (3.2.9) implies this is independent of the choice of basis.

Next we define the *adjoint* of $T \in \mathcal{L}(V, W)$, when V and W are finite-dimensional inner product spaces, as the transformation $T^* \in \mathcal{L}(W, V)$ with the property

$$(Tv, w) = (v, T^*w), \quad \forall\ v \in V,\ w \in W. \tag{3.2.11}$$

If $\{v_1, \dots, v_n\}$ is an orthonormal basis of V and $\{w_1, \dots, w_m\}$ an orthonormal basis of W, then

$$A = (a_{ij}), \quad a_{ij} = (Tv_j, w_i), \tag{3.2.12}$$

is the matrix representation of T, as in (1.4.2), and the matrix representation of T^* is

$$A^* = (\overline{a}_{ji}). \tag{3.2.13}$$

Now we define the Hilbert-Schmidt norm of $T \in \mathcal{L}(V, W)$ when V and W are finite-dimensional inner product spaces. Namely, we set

$$\|T\|_{HS}^2 = \operatorname{Tr} T^*T. \tag{3.2.14}$$

In terms of the matrix representation (3.2.12) of T, we have

$$T^*T = (b_{jk}), \quad b_{jk} = \sum_\ell \overline{a}_{\ell j} a_{\ell k}, \tag{3.2.15}$$

hence

$$\|T\|_{HS}^2 = \sum_j b_{jj} = \sum_{j,k} |a_{jk}|^2. \tag{3.2.16}$$

Equivalently, using an arbitrary orthonormal basis $\{v_1, \dots, v_n\}$ of V, we have

$$\|T\|_{HS}^2 = \sum_{j=1}^n \|Tv_j\|^2. \tag{3.2.17}$$

If also $\{w_1, \dots, w_m\}$ is an orthonormal basis of W, then

$$\begin{aligned} \|T\|_{HS}^2 &= \sum_{j,k} |(Tv_j, w_k)|^2 = \sum_{j,k} |(v_j, T^*w_k)|^2 \\ &= \sum_K \|T^*w_k\|_{HS}^2. \end{aligned} \tag{3.2.18}$$

This gives $\|T\|_{HS} = \|T^*\|_{HS}$. Also, the right side of (3.2.18) is clearly independent of the choice of the orthonormal basis $\{v_1, \dots, v_n\}$ of V. Of course, we already know that the right side of (3.2.14) is independent of such a choice of basis.

Using (3.2.17), we can show that the operator norm of T is dominated by the Hilbert-Schmidt norm:

$$\|T\| \le \|T\|_{HS}. \tag{3.2.19}$$

In fact, pick a unit $v_1 \in V$ such that $\|Tv_1\|$ is maximized on $\{v : \|v\| \le 1\}$, extend this to an orthonormal basis $\{v_1, \dots, v_n\}$, and use

$$\|T\|^2 = \|Tv_1\|^2 \le \sum_{j=1}^n \|Tv_j\|^2 = \|T\|_{HS}^2. \tag{3.2.20}$$

Also we can dominate each term on the right side of (3.2.17) by $\|T\|^2$, so

$$\|T\|_{HS} \le \sqrt{n}\|T\|, \quad n = \dim V. \tag{3.2.21}$$

Another consequence of (3.2.17)–(3.2.19) is

$$\|ST\|_{HS} \le \|S\|\,\|T\|_{HS} \le \|S\|_{HS}\|T\|_{HS}, \tag{3.2.22}$$

for S as in (3.2.3). In particular, parallel to (3.2.5), we have

$$T : V \to V \Longrightarrow \|T^n\|_{HS} \le \|T\|_{HS}^n. \tag{3.2.23}$$

Exercises

1. Suppose V and W are finite dimensional inner product spaces and $T \in \mathcal{L}(V, W)$. Show that

$$T^{**} = T.$$

2. In the context of Exercise 1, show that

$$T \text{ injective } \Longleftrightarrow T^* \text{ surjective.}$$

More generally, show that

$$\mathcal{N}(T) = \mathcal{R}(T^*)^\perp.$$

(See Exercise 2 of §3.1 for a discussion of the orthogonal complement $W^\perp$.)

3. Say A is a $k \times n$ real matrix and the k columns are linearly independent. Show that A has k linearly independent rows. (Similarly treat complex matrices.)
Hint. The hypothesis is equivalent to $A : \mathbb{R}^k \to \mathbb{R}^n$ being injective. What does that say about $A^* : \mathbb{R}^n \to \mathbb{R}^k$?

4. If A is a $k \times n$ real (or complex) matrix, we define the *column rank* of A to be the dimension of the span of the columns of A. We similarly define the *row rank* of A. Show that the row rank of A is equal to its column rank.
Hint. Reduce this to showing $\dim \mathcal{R}(A) = \dim \mathcal{R}(A^*)$. Apply Exercise 2 (and Exercise 3 of §3.1).

5. If V and W are normed linear spaces and $S, T \in \mathcal{L}(V, W)$, show that

$$\|S + T\| \leq \|S\| + \|T\|.$$

6. Suppose A is an $n \times n$ matrix and $\|A\| < 1$. Show that

$$(I - A)^{-1} = I + A + A^2 + \cdots + A^k + \cdots,$$

a convergent infinite series.

7. If A is an $n \times n$ complex matrix, show that

$$\lambda \in \operatorname{Spec}(A) \Longrightarrow |\lambda| \leq \|A\|.$$

8. Show that, for any real θ, the matrix

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

has operator norm 1. Compute its Hilbert-Schmidt norm.

9. Given $a > b > 0$, show that the matrix

$$B = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

has operator norm a. Compute its Hilbert-Schmidt norm.

10. Show that if V is an n-dimensional complex inner product space, then, for $T \in \mathcal{L}(V)$,

$$\det T^* = \overline{\det T}.$$

11. If V is an n-dimensional inner product space, show that, for $T \in \mathcal{L}(V)$,

$$\|T\| = \sup\{|(Tu, v)| : \|u\|, \|v\| \leq 1\}.$$

Show that

$$\|T^*\| = \|T\|, \quad \text{and} \quad \|T^*T\| = \|T\|^2.$$

12. Show that if $B \in M(n, \mathbb{F})$,

$$\frac{d}{dt} \det(I + tB) = \operatorname{Tr} B.$$

13. Writing

$$\det(A + tB) = \det(a_1 + tb_1, \dots, a_n + tb_n),$$

with notation as in (1.5.5), and using linearity in each column, show that

$$\frac{d}{dt} \det(A + tB)\big|_{t=0} = \det(b_1, a_2, \dots, a_n) + \cdots + \det(a_1, \dots, b_k, \dots, a_n) + \cdots + \det(a_1, \dots, a_{n-1}, b_n).$$

Use an appropriate version of (1.5.52) to deduce that

$$\frac{d}{dt} \det(A + tB)\big|_{t=0} = \sum_{j,k} (-1)^{j-k} b_{jk} \det A_{kj},$$

with A_{kj} as in Exercise 8 of §1.5, i.e., A_{kj} is obtained by deleting the kth column and the jth row from A. In other words,

$$\frac{d}{dt} \det(A + tB)\big|_{t=0} = \sum_{j,k} b_{jk} c_{kj} = \operatorname{Tr} BC,$$

with $C = (c_{jk})$ as in Exercise 10 of §1.5, i.e., $c_{jk} = (-1)^{k-j} \det A_{jk}$.

14. If A is invertible, show that for each $B \in M(n, \mathbb{F})$,

$$\frac{d}{dt} \det(A + tB)\big|_{t=0} = (\det A) \frac{d}{dt} (I + tA^{-1}B)\big|_{t=0} = (\det A) \operatorname{Tr}(A^{-1}B).$$

Use Exercise 13 to conclude that

$$(\det A) A^{-1} = C.$$

Compare the derivation of Cramer's formula in Exercises 9–10 of §1.5.

3.3. Self-adjoint and skew-adjoint transformations

If V is a finite-dimensional inner product space, $T \in \mathcal{L}(V)$ is said to be self-adjoint if $T = T^*$ and skew-adjoint if $T = -T^*$. If $\{u_1, \dots, u_n\}$ is an orthonormal basis of V and A the matrix representation of T with respect to this basis, given by

$$A = (a_{ij}), \quad a_{ij} = (Tu_j, u_i), \tag{3.3.1}$$

then T^* is represented by $A^* = (\overline{a}_{ji})$, so T is self-adjoint if and only if $a_{ij} = \overline{a}_{ji}$ and T is skew-adjoint if and only if $a_{ij} = -\overline{a}_{ji}$.

The eigenvalues and eigenvectors of these two classes of operators have special properties, as we proceed to show.

Lemma 3.3.1. *If λ_j is an eigenvalue of a self-adjoint $T \in \mathcal{L}(V)$, then λ_j is real.*

Proof. Say $Tv_j = \lambda_j v_j,\ v_j \neq 0$. Then

$$\lambda_j \|v_j\|^2 = (Tv_j, v_j) = (v_j, Tv_j) = \overline{\lambda}_j \|v_j\|^2, \tag{3.3.2}$$

so $\lambda_j = \overline{\lambda}_j$. □

This allows us to prove the following result for both real and complex vector spaces.

Proposition 3.3.2. *If V is a finite-dimensional inner product space and $T \in \mathcal{L}(V)$ is self-adjoint, then V has an orthonormal basis of eigenvectors of T.*

Proof. Proposition 2.1.1 (and the comment following it in case $\mathbb{F} = \mathbb{R}$) implies there is a unit $v_1 \in V$ such that $Tv_1 = \lambda_1 v_1$, and we know $\lambda_1 \in \mathbb{R}$. Say $\dim V = n$. Let

$$W = \{w \in V : (v_1, w) = 0\}. \tag{3.3.3}$$

Then $\dim W = n - 1$, as we can see by completing $\{v_1\}$ to an orthonormal basis of V. We claim

$$T = T^* \Longrightarrow T : W \to W. \tag{3.3.4}$$

Indeed,

$$w \in W \Rightarrow (v_1, Tw) = (Tv_1, w) = \lambda_1 (v_1, w) = 0 \Rightarrow Tw \in W. \tag{3.3.5}$$

An inductive argument gives an orthonormal basis of W consisting of eigenvalues of T, so Proposition 3.3.2 is proven. □

The following could be deduced from Proposition 3.3.2, but we prove it directly.

Proposition 3.3.3. *Assume $T \in \mathcal{L}(V)$ is self-adjoint. If $Tv_j = \lambda_j v_j$, $Tv_k = \lambda_k v_k$, and $\lambda_j \neq \lambda_k$, then $(v_j, v_k) = 0$.*

Proof. Then we have

$$\lambda_j (v_j, v_k) = (Tv_j, v_k) = (v_j, Tv_k) = \lambda_k (v_j, v_k).$$

□

If $\mathbb{F} = \mathbb{C}$, we have

$$T \text{ skew-adjoint } \iff iT \text{ self-adjoint}, \tag{3.3.6}$$

so Proposition 3.3.2 has an extension to skew-adjoint transformations if $\mathbb{F} = \mathbb{C}$. The case $\mathbb{F} = \mathbb{R}$ requires further study.

If V is a real n-dimensional inner product space and $T \in \mathcal{L}(V)$ is skew adjoint, then V does not have an orthonormal basis of eigenvectors of T, unless $T = 0$. However, V does have an orthonormal basis with respect to which T has a special structure, as we proceed to show. To get it, we consider the complexification of V,

$$V_{\mathbb{C}} = \{u + iv : u, v, \in V\}, \tag{3.3.7}$$

which has the natural structure of a complex n-dimensional vector space, with a Hermitian inner product. A transformation $T \in \mathcal{L}(V)$ has a unique $\mathbb{C}$-linear extension to a transformation on $V_{\mathbb{C}}$, which we continue to denote by T, and this extended transformation is skew adjoint on $V_{\mathbb{C}}$. Hence $V_{\mathbb{C}}$ has an orthonormal basis of eigenvectors of T. Say $u + iv \in V_{\mathbb{C}}$ is such an eigenvector,

$$T(u + iv) = i\lambda(u + iv), \quad \lambda \in \mathbb{R} \setminus 0. \tag{3.3.8}$$

We have

$$\begin{aligned} Tu &= -\lambda v \\ Tv &= \lambda u. \end{aligned} \tag{3.3.9}$$

In such a case, applying complex conjugation to (3.3.8) yields

$$T(u - iv) = -i\lambda(u - iv), \tag{3.3.10}$$

and $i\lambda \neq -i\lambda$, so Proposition 3.3.3 (applied to iT) yields

$$u + iv \perp u - iv, \tag{3.3.11}$$

hence

$$\begin{aligned} 0 &= (u + iv, u - iv) \\ &= (u, u) - (v, v) + i(v, u) + i(u, v) \\ &= \|u\|^2 - \|v\|^2 + 2i(u, v), \end{aligned} \tag{3.3.12}$$

or equivalently

$$\|u\| = \|v\|, \quad \text{and} \quad u \perp v. \tag{3.3.13}$$

Now

$$\operatorname{Span}\{u, v\} \subset V \tag{3.3.14}$$

has an $(n-2)$-dimensional orthogonal complement, W, and, parallel to (3.3.4), we have

$$T = -T^* \Longrightarrow T : W \to W. \tag{3.3.15}$$

We are reduced to examining the skew-adjoint transformation on a lower dimensional inner product space. An inductive argument then gives the following.

Proposition 3.3.4. *If V is an n-dimensional real inner product space and $T \in \mathcal{L}(V)$ is skew adjoint, then V has an orthonormal basis in which the matrix representation of T consists of blocks*

$$\begin{pmatrix} 0 & \lambda_j \\ -\lambda_j & 0 \end{pmatrix}, \tag{3.3.16}$$

plus perhaps a zero matrix, when $\mathcal{N}(T) \neq 0$.

EXAMPLE. Take $V = \mathbb{R}^3$ and

$$T = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{3.3.17}$$

Then $\det(T - \lambda I) = -\lambda(\lambda^2 + 2)$, so the eigenvalues of T are

$$\lambda_0 = 0, \quad i\lambda_\pm = \pm\sqrt{2}i. \tag{3.3.18}$$

One readily obtains eigenvectors in $V_{\mathbb{C}} = \mathbb{C}^3$,

$$v_0 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad v_\pm = \begin{pmatrix} 1 \\ \mp\sqrt{2}i \\ -1 \end{pmatrix}, \tag{3.3.19}$$

readily seen to be mutually orthogonal vectors in $\mathbb{C}^3$. We can write

$$v_+ = u + iv, \quad u = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad v = \begin{pmatrix} 0 \\ -\sqrt{2} \\ 0 \end{pmatrix}, \tag{3.3.20}$$

and note that u and $v \in \mathbb{R}^3$ are orthogonal and each have norm $\sqrt{2}$. Furthermore, a calculation gives

$$Tu = -\sqrt{2}v, \quad Tv = \sqrt{2}u. \tag{3.3.21}$$

Hence

$$u_1 = \frac{1}{\sqrt{2}}u, \quad u_2 = \frac{1}{\sqrt{2}}v, \quad u_3 = \frac{1}{\sqrt{2}}v_0 \tag{3.3.22}$$

gives an orthonormal basis of $\mathbb{R}^3$ with respect to which the matrix representation of T is

$$A = \begin{pmatrix} 0 & \sqrt{2} & \\ -\sqrt{2} & 0 & \\ & & 0 \end{pmatrix}. \tag{3.3.23}$$

Let us return to the setting of self-adjoint transformations. If V is a finite dimensional inner product space, we say $T \in \mathcal{L}(V)$ is positive definite if and only if $T = T^*$ and

$$(Tv, v) > 0 \ \text{ for all nonzero } \ v \in V. \tag{3.3.24}$$

We say T is positive semidefinite if and only if $T = T^*$ and

$$(Tv, v) \geq 0, \quad \forall\, v \in V. \tag{3.3.25}$$

The following is a basic characterization of these classes of transformations.

Proposition 3.3.5. *Given $T = T^* \in \mathcal{L}(V)$, with eigenvalues $\{\lambda_j\}$,*
(i) T is positive definite if and only if each $\lambda_j > 0$.
(ii) T is positive semidefinite if and only if each $\lambda_j \geq 0$.

Proof. This follows by writing $v = \sum a_j v_j$, where $\{v_j\}$ is the orthonormal basis of V consisting of eigenvectors of T given by Proposition 3.3.2, satisfying $Tv_j = \lambda_j v_j$, and observing that

$$(Tv, v) = \sum_j |a_j|^2 \lambda_j. \tag{3.3.26}$$

□

The following is a useful test for positive definiteness.

Proposition 3.3.6. *Let $A = (a_{jk}) \in M(n, \mathbb{C})$ be self adjoint. For $1 \leq \ell \leq n$, form the $\ell \times \ell$ matrix $A_\ell = (a_{jk})_{1 \leq j,k \leq \ell}$. Then*

$$A \text{ is positive definite } \iff \det A_\ell > 0, \quad \forall\, \ell \in \{1, \ldots, n\}. \tag{3.3.27}$$

Proof. Regarding the implication $\Rightarrow$, note that if A is positive definite, then $\det A = \det A_n$ is the product of its eigenvalues, all > 0, hence is > 0. Also, in this case, it follows from the hypothesis of (3.3.27) that each A_ℓ must be positive definite, hence have positive determinant, so we have $\Rightarrow$.

The implication $\Leftarrow$ is easy enough for 2×2 matrices. If $A = A^*$ and $\det A > 0$, then either both its eigenvalues are positive (so A is positive definite) or both are negative (so A is negative definite). In the latter case, $A_1 = (a_{11})$ must be negative. Thus we have $\Leftarrow$ for $n = 2$.

We prove $\Leftarrow$ for $n \geq 3$, using induction. The inductive hypothesis implies that if $\det A_\ell > 0$ for each $\ell \leq n$, then A_{n-1} is positive definite. The next lemma then guarantees that $A = A_n$ has at least $n - 1$ positive eigenvalues. The hypothesis that $\det A > 0$ does not allow that the remaining eigenvalue be ≤ 0, so all of the eigenvaules of A must be positive. Thus Proposition 3.3.6 is proven once we have the following. □

Lemma 3.3.7. *In the setting of Proposition 3.3.6, if A_{n-1} is positive definite, then $A = A_n$ has at least $n - 1$ positive eigenvalues.*

Proof. Since $A = A^*$, $\mathbb{C}^n$ has an orthonormal basis $v_1, \ldots, v_n$ of eigenvectors of A, satisfying $Av_j = \lambda_j v_j$. If the conclusion of the lemma is false, at least two of the eigenvalues, say λ_1, λ_2, are ≤ 0. Let $W = \mathrm{Span}(v_1, v_2)$, so

$$w \in W \Longrightarrow (Aw, w) \leq 0.$$

Since W has dimension 2, $\mathbb{C}^{n-1} \subset \mathbb{C}^n$ satisfies $\mathbb{C}^{n-1} \cap W \neq 0$, so there exists a nonzero $w \in C^{n-1} \cap W$, and then

$$(A_{n-1}w, w) = (Aw, w) \leq 0,$$

contradicting the hypothesis that A_{n-1} is positive definite. □

We next apply results on LU-factorization, discussed in §1.6, to $A \in M(n, \mathbb{C})$ when A is positive definite. This factorization has the form

$$A = LU, \tag{3.3.28}$$

where $L, U \in M(n, \mathbb{C})$ are lower triangular and upper triangular, respectively; see (1.6.48). As shown in §1.6, this factorization is always possible when the upper left submatrices A_ℓ described above are all invertible. Hence this factorization always works when A is positive definite. Moreover, as shown in (1.6.63), in such a case it can be rewritten as

$$A = L_0 D L_0^*, \tag{3.3.29}$$

where L_0 is lower triangular with all 1s on the diagonal, and D is diagonal, with real entries. Moreover, this factorization is unique. Since

$$(Av, v) = (DL_0^* v, L_0^* v), \tag{3.3.30}$$

we see that if A is positive definite, then all the diagonal entries d_j of D must be positive. Thus we can write

$$D = E^2, \tag{3.3.31}$$

where E is diagonal with diagonal entries $\sqrt{d_j}$. Thus, whenever $A \in M(n, \mathbb{C})$ is positive definite, we can write

$$A = LL^*, \quad L = L_0 E, \text{ lower triangular.} \tag{3.3.32}$$

This is called the *Cholesky decomposition*.

Symmetric bilinear forms

Let V be an n-dimensional real vector space. A bilinear form Q on V is a map $Q : V \times V \to \mathbb{R}$ that satisfies the following bilinerity conditions:

$$\begin{aligned} Q(a_1 u_1 + a_2 u_2, v_1) &= a_1 Q(u_1, v_1) + a_2 Q(u_2, v_1), \\ Q(u_1, b_1 v_1 + b_2 v_2) &= b_1 Q(u_1, v_1) + b_2 Q(u_1, v_2), \end{aligned} \tag{3.3.33}$$

for all $u_j, v_j \in V$, $a_j, b_j \in \mathbb{R}$. We say Q is a symmetric bilinear form if, in addition,

$$Q(u, v) = Q(v, u), \quad \forall\, u, v \in V. \tag{3.3.34}$$

To relate the structure of such Q to previous material in this section, we pick a basis $\{e_1, \dots, e_n\}$ of V and put on V an inner product $(\ ,\ )$ such that this basis is orthonormal. Then we set

$$a_{jk} = Q(e_j, e_k), \tag{3.3.35}$$

and define $A : V \to V$ by

$$Ae_j = \sum_\ell a_{j\ell} e_\ell, \quad \text{so} \quad (Ae_j, e_k) = Q(e_j, e_k). \tag{3.3.36}$$

It follows that

$$Q(u, v) = (Au, v), \quad \forall\, u, v \in V. \tag{3.3.37}$$

The symmetry condition (3.3.34) implies $a_{jk} = a_{kj}$, hence $A^* = A$. By Proposition 3.3.2, V has an orthonormal basis $\{f_1, \dots, f_n\}$ such that

$$Af_j = \lambda_j f_j, \quad \lambda_j \in \mathbb{R}. \tag{3.3.38}$$

Hence

$$Q(f_j, f_k) = (Af_j, f_k) = \lambda_j \delta_{jk}. \tag{3.3.39}$$

If Q is a symmetric bilinear form on V, we say it is *nondegenerate* provided that for each nonzero $u \in V$, there exists $v \in V$ such that $Q(u, v) \neq 0$. Given (3.3.37), it is clear that Q is nondegenerate if and only if A is invertible, hence if and only if each λ_j in (3.3.38) is nonzero. If Q is nondegenerate, we have the basis $\{g_1, \dots, g_n\}$ of V, given by

$$g_j = |\lambda_j|^{-1/2} f_j. \tag{3.3.40}$$

then

$$Q(g_j, g_k) = |\lambda_j \lambda_k|^{-1/2} (Af_j, f_k) = \varepsilon_j \delta_{jk}, \tag{3.3.41}$$

where

$$\varepsilon_j = \frac{\lambda_j}{|\lambda_j|} \in \{\pm 1\}. \tag{3.3.42}$$

If p of the numbers ε_j in (3.3.42) are $+1$ and q of them are -1 (so $p + q = n$), we say the nondegenerate symmetric bilinear form Q has signature (p, q).

The construction (3.3.41)–(3.3.42) involved some arbitrary choices, so we need to show that, given such Q, the pair (p, q) is uniquely defined. To see this, let V_0 denote the linear span of the g_j in (3.3.41) such that $\varepsilon_j = +1$ and let V_1 denote the linear span of the g_j in (3.3.41) such that $\varepsilon_j = -1$. Hence

$$V = V_0 \oplus V_1 \tag{3.3.43}$$

is an orthogonal direct sum, and we have Q positive definite on $V_0 \times V_0$, and negative definite on $V_1 \times V_1$. That the signature of Q is well defined is a consequence of the following.

Proposition 3.3.8. *Let $\widetilde{V}_0$ and $\widetilde{V}_1$ be linear subspaces of V such that*

$$Q \text{ is positive definite on } \widetilde{V}_0 \times \widetilde{V}_0, \text{ negative definite on } \widetilde{V}_1 \times \widetilde{V}_1. \tag{3.3.44}$$

Then

$$\dim \widetilde{V}_0 \leq p \quad \text{and} \quad \dim \widetilde{V}_1 \leq q. \tag{3.3.45}$$

Proof. If the first assertion of (3.3.45) is false, then $\dim \widetilde{V}_0 > p$, so $\dim \widetilde{V}_0 + \dim V_1 > n = \dim V$. Hence there exists a nonzero $u \in \widetilde{V}_0 \cap V_1$. This would imply that

$$Q(u, u) > 0 \ \text{ and } \ Q(u, u) < 0, \tag{3.3.46}$$

which is impossible. The proof of the second assertion in (3.3.45) is parallel. □

Exercises

1. Verify Proposition 3.3.2 for $V = \mathbb{R}^3$ and

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

2. Verify Proposition 3.3.4 for

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

3. In the setting of Proposition 3.3.2, suppose $S, T \in \mathcal{L}(V)$ are both self-adjoint and suppose they *commute*, i.e., $ST = TS$. Show that V has an orthonormal basis of vectors that are simultaneously eigenvectors of S and of T.

4. Let V be a finite-dimensional inner product space, $W \subset V$ a linear subspace. The orthogonal projection P of V onto W was introduced in Exercise 4 of §3.1. Show that this orthogonal projection is also uniquely characterized as the element $P \in \mathcal{L}(V)$ satisfying

$$P^2 = 0, \quad P^* = P, \quad \mathcal{R}(P) = W.$$

5. If $T \in \mathcal{L}(V)$ is positive semidefinite, show that

$$\|T\| = \max\{\lambda : \lambda \in \operatorname{Spec} T\}.$$

6. If $S \in \mathcal{L}(V)$, show that S^*S is positive semidefinite, and

$$\|S\|^2 = \|S^*S\|.$$

Show that

$$\|S\| = \max\{\lambda^{1/2} : \lambda \in \operatorname{Spec} S^*S\}.$$

7. Let $A \in M(n, \mathbb{C})$ be positive definite, with Cholesky decomposition $A = L_1 L_1^*$, as in (3.3.32). Show that A has another Cholesky decomposition $A = L_2 L_2^*$ if and only if

$$L_1 = L_2 D,$$

with D diagonal and all diagonal entries d_j satisfying $|d_j| = 1$.
Hint. To start, we must have

$$L_2^{-1} L_1 = L_2^* (L_1^*)^{-1},$$

both lower triangular and upper triangular, hence diagonal; call it D.

8. If V is an n-dimensional real inner product space, and $T \in \mathcal{L}(V)$, we say $T \in \text{Skew}(V)$ if and only if $T^* = -T$. (Compare (3.3.7).) Show that

$$S, T \in \text{Skew}(V) \Longrightarrow [S, T] \in \text{Skew}(V),$$

where

$$[S, T] = ST - TS.$$

9. Given $T = T^* \in \mathcal{L}(V)$ and an orthonormal basis $\{v_j\}$ of V such that $Tv_j = \lambda_j v_j$, and given $f : \text{Spec}(T) \to \mathbb{C}$, define $f(T) \in \mathcal{L}(V)$ by

$$f(T)v_j = f(\lambda_j)v_j.$$

Show that

$$f(t) = t^k,\ k \in \mathbb{Z}^+ \Longrightarrow f(T) = T^k,$$

that

$$h(t) = f(t)g(t) \Longrightarrow h(T) = f(T)g(T),$$

and that

$$\overline{f}(T) = f(T)^*.$$

10. Let $T = T^* \in \mathcal{L}(V)$, $\text{Spec}\, T = \{\lambda_j\}$, $E_j = \mathcal{E}(T, \lambda_j)$, and let P_j be the orthogonal projection of V onto E_j. With $f(T)$ defined as in Exercise 9, show that

$$f(T) = \sum_j f(\lambda_j)P_j.$$

11. If $A \in M(n, \mathbb{C})$ is invertible, its *condition number* $c(A)$ is defined to be

$$c(A) = \|A\| \cdot \|A^{-1}\|.$$

Take the positive definite matrix $P = (A^*A)^{1/2}$ (see Exercises 6 and 9). Show that

$$c(A) = c(P) = \frac{\lambda_{\max}(P)}{\lambda_{\min}(P)}.$$

12. Let V be a finite-dimensional inner product space, $W \subset V$ a linear subspace, $T \in \mathcal{L}(V)$. Show that

$$T : W \to W \Longrightarrow T^* : W^\perp \to W^\perp.$$

13. Let V be a finite-dimensional, real inner product space, with inner product denoted $\langle\ ,\ \rangle$. Assume we have $J \in \mathcal{L}(V)$, satisfying

$$J^2 = -I, \quad J^* = -J.$$

We can make V into a complex vector space (denoted $\mathcal{V}$), with the action of $a + ib \in \mathbb{C}$ on V given by

$$(a + ib) \cdot v = av + bJv.$$

Then

$$\dim_{\mathbb{C}} \mathcal{V} = k \Longrightarrow \dim_{\mathbb{R}} V = 2k.$$

(See Exercise 13 in §1.3.) Now set

$$(u, v) = \langle u, v\rangle + i\langle u, Jv\rangle, \quad u, v \in V = \mathcal{V}.$$

Show that this is a Hermitian inner product on the complex vector space $\mathcal{V}$, especially

$$(v, u) = \overline{(u, v)}, \quad (u, Jv) = -i(u, v).$$

14. In this exercise, let V be a finite-dimensional real inner product space, with inner product $\langle\ ,\ \rangle$. Let $A \in \mathcal{L}(V)$, and assume

$$A^* = -A, \quad \mathcal{N}(A) = 0.$$

(a) Show that $\dim_{\mathbb{R}} V$ must be even.

(b) Set

$$P = A^*A = -A^2,$$

which is self adjoint and positive definite, and take

$$Q = P^{1/2}.$$

Show that Q and A commute.
Hint. Show that there is a polynomial $p(\lambda)$ such that $p(\mu_j) = \mu_j^{1/2}$ for each $\mu_j \in \operatorname{Spec} P$, hence $Q = p(P)$.

(c) Set

$$J = AQ^{-1}.$$

Show that $J = Q^{-1}A$ and

$$J^2 = -I, \quad J^* = -J.$$

In particular, J puts a complex structure on V. Denote the associated complex vector space by $\mathcal{V}$, so

$$\dim_{\mathbb{C}} \mathcal{V} = \frac{1}{2} \dim_{\mathbb{R}} V.$$

(d) Show that

$$AJ = JA,$$

so $A : \mathcal{V} \to \mathcal{V}$ is $\mathbb{C}$-linear.

(e) As in Exercise 13, for the Hermitian inner product on $\mathcal{V}$,

$$(u, v) = \langle u, v\rangle + i\langle u, Jv\rangle.$$

Show that

$$(Au, v) = -(u, Av).$$

Thus A defines a skew-adjoint transformation on the complex inner product space $\mathcal{V}$.

(f) Say $\dim_{\mathbb{R}} V = 2k$. By Proposition 3.3.2 and (3.3.6), $\mathcal{V}$ has an orthonormal basis $\{u_j : 1 \le j \le k\}$ (with respect to $(\ ,\ )$), consisting of eigenvectors of $A \in \mathcal{L}(\mathcal{V})$, with eigenvalues $i\lambda_j$, so

$$Au_j = \lambda_j Ju_j, \quad 1 \le j \le k,\ \lambda_j \in \mathbb{R}.$$

Deduce from part (c) that

$$Qu_j = \lambda_j u_j, \quad \text{hence each} \ \ \lambda_j > 0.$$

(g) Note that $Ju_j \in \mathrm{Span}_{\mathbb{C}}\{u_j\}$, and hence

$$(Ju_j, u_\ell) = 0, \quad \text{for} \ \ j \neq \ell.$$

Show that

$$\langle u_j, u_\ell \rangle = \langle u_j, Ju_\ell \rangle = \langle Ju_j, Ju_\ell \rangle = 0, \quad \text{for} \ \ j \neq \ell.$$

Then show that

$$\{u_j, Ju_j : 1 \leq j \leq k\} \ \ \text{is an orthonormal basis of } V,$$

with respect to $\langle \ , \ \rangle$. With respect to this basis,

$$Au_j = \lambda_j Ju_j, \quad AJu_j = -\lambda_j u_j.$$

Compare this with the conclusion of Proposition 3.3.4.

3.4. Unitary and orthogonal transformations

Let V be a finite-dimensional inner product space (over $\mathbb{F}$) and $T \in \mathcal{L}(V)$. Suppose

$$T^{-1} = T^*. \tag{3.4.1}$$

If $\mathbb{F} = \mathbb{C}$ we say T is *unitary*, and if $\mathbb{F} = \mathbb{R}$ we say T is *orthogonal*. We denote by $U(n)$ the set of unitary transformations on $\mathbb{C}^n$ and by $O(n)$ the set of orthogonal transformations on $\mathbb{R}^n$. More generally, we use the notations $U(V)$ and $O(V)$. Note that (3.4.1) implies

$$|\det T|^2 = (\det T)(\det T^*) = 1, \tag{3.4.2}$$

i.e., $\det T \in \mathbb{F}$ has absolute value 1. In particular,

$$T \in O(n) \Longrightarrow \det T = \pm 1. \tag{3.4.3}$$

We set

$$\begin{aligned} SO(n) &= \{T \in O(n) : \det T = 1\}, \\ SU(n) &= \{T \in U(n) : \det T = 1\}. \end{aligned} \tag{3.4.4}$$

As with self-adjoint and skew-adjoint transformations, the eigenvalues and eigenvectors of unitary transformations have special properties, as we now demonstrate.

Lemma 3.4.1. *If λ_j is an eigenvalue of a unitary $T \in \mathcal{L}(V)$, then $|\lambda_j| = 1$.*

Proof. Say $Tv_j = \lambda_j v_j,\ v_j \neq 0$. Then

$$\|v_j\|^2 = (T^*Tv_j, v_j) = (Tv_j, Tv_j) = |\lambda_j|^2 \|v_j\|^2. \tag{3.4.5}$$

□

Next, parallel to Proposition 3.3.2, we show unitary transformations have eigenvectors forming a basis.

Proposition 3.4.2. *If V is a finite-dimensional complex inner product space and $T \in \mathcal{L}(V)$ is unitary, then V has an orthonormal basis of eigenvectors of T.*

Proof. Proposition 2.1.1 implies there is a unit $v_1 \in V$ such that $Tv_1 = \lambda_1 v_1$. Say $\dim V = n$. Let

$$W = \{w \in V : (v_1, w) = 0\}. \tag{3.4.6}$$

As in the analysis of (3.3.3) we have $\dim W = n - 1$. We claim

$$T \text{ unitary} \Longrightarrow T : W \to W. \tag{3.4.7}$$

Indeed,

$$w \in W \Rightarrow (v_1, Tw) = (T^{-1}v_1, w) = \lambda_1^{-1}(v_1, w) = 0 \Rightarrow Tw \in W. \tag{3.4.8}$$

Now, as in Proposition 3.3.2, an inductive argument gives an orthonormal basis of W consisting of eigenvectors of T, so Proposition 3.4.2 is proven. □

Next we have a result parallel to Proposition 3.3.3:

Proposition 3.4.3. *Assume $T \in \mathcal{L}(V)$ is unitary. If $Tv_j = \lambda_j v_j$ and $Tv_k = \lambda_k v_k$, and $\lambda_j \neq \lambda_k$, then $(v_j, v_k) = 0$.*

Proof. Then we have

$$\lambda_j(v_j, v_k) = (Tv_j, v_k) = (v_j, T^{-1}v_k) = \lambda_k(v_j, v_k),$$

since $\overline{\lambda}_k^{-1} = \lambda_k$. □

If V is a real, n-dimensional, inner product space and $T \in \mathcal{L}(V)$ satisfies (3.4.1), we say T is an orthogonal transformation and write $T \in O(V)$. In such a case, V typically does not have an orthonormal basis of eigenvectors of T. However, V does have an orthonormal basis with respect to which such an orthogonal transformation has a special structure, as we proceed to show. To get it, we construct the complexification of V,

$$V_{\mathbb{C}} = \{u + iv : u, v \in V\}, \tag{3.4.9}$$

which has a natural structure of a complex n-dimensional vector space, with a Hermitian inner product. A transformation $T \in O(V)$ has a unique $\mathbb{C}$-linear extension to a transformation on $V_{\mathbb{C}}$, which we continue to denote by T, and this extended transformation is unitary on $V_{\mathbb{C}}$. Hence $V_{\mathbb{C}}$ has an orthonormal basis of eigenvectors of T. Say $u + iv \in V_{\mathbb{C}}$ is such an eigenvector,

$$T(u + iv) = e^{-i\theta}(u + iv), \quad e^{i\theta} \notin \{1, -1\}. \tag{3.4.10}$$

(Peek ahead to (3.7.77) for the use of the notation $e^{i\theta}$.) Writing $e^{i\theta} = c + is$, $c, s \in \mathbb{R}$, we have

$$\begin{aligned} Tu + iTv &= (c - is)(u + iv) \\ &= cu + sv + i(-su + cv), \end{aligned} \tag{3.4.11}$$

hence

$$\begin{aligned} Tu &= cu + sv, \\ Tv &= -su + cv. \end{aligned} \tag{3.4.12}$$

In such a case, applying complex conjugation to (3.4.10) yields

$$T(u - iv) = e^{i\theta}(u - iv),$$

and $e^{i\theta} \neq e^{-i\theta}$ if $e^{i\theta} \notin \{1, -1\}$, so Proposition 3.4.3 yields

$$u + iv \perp u - iv, \tag{3.4.13}$$

hence

$$\begin{aligned} 0 &= (u + iv, u - iv) \\ &= (u, u) - (v, v) + i(v, u) + i(u, v) \\ &= \|u\|^2 - \|v\|^2 + 2i(u, v), \end{aligned} \tag{3.4.14}$$

or equivalently

$$\|u\| = \|v\| \ \text{ and } \ u \perp v. \tag{3.4.15}$$

Now

$$\operatorname{Span}\{u, v\} \subset V$$

has an $(n-2)$-dimensional orthogonal complement, on which T acts, and an inductive argument gives the following.

Proposition 3.4.4. *Let V be an n-dimensional real inner product space, $T : V \to V$ an orthogonal transformation. Then V has an orthonormal basis in which the matrix representation of T consists of blocks*

$$\begin{pmatrix} c_j & -s_j \\ s_j & c_j \end{pmatrix}, \quad c_j^2 + s_j^2 = 1, \tag{3.4.16}$$

plus perhaps an identity matrix block if $1 \in \operatorname{Spec} T$, and a block that is $-I$ if $-1 \in \operatorname{Spec} T$.

EXAMPLE 1. Picking $c, s \in \mathbb{R}$ such that $c^2 + s^2 = 1$, we see that

$$B = \begin{pmatrix} c & s \\ s & -c \end{pmatrix}$$

is orthogonal, with $\det B = -1$. Note that $\operatorname{Spec}(B) = \{1, -1\}$. Thus there is an orthonormal basis of $\mathbb{R}^2$ in which the matrix representation of B is

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

If $A : \mathbb{R}^3 \to \mathbb{R}^3$ is orthogonal, it has either 1 or 3 real eigenvalues. Furthermore, there is an orthonormal basis $\{u_1, u_2, u_3\}$ of $\mathbb{R}^3$ in which

$$A = \begin{pmatrix} c & -s & \\ s & c & \\ & & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} c & -s & \\ s & c & \\ & & -1 \end{pmatrix}, \tag{3.4.17}$$

depending on whether $\det A = 1$ or $\det A = -1$. Since $c^2 + s^2 = 1$, it follows that there is an angle θ, uniquely determined up to an additive multiple of 2π, such that

$$c = \cos\theta, \quad s = \sin\theta. \tag{3.4.18}$$

If $\det A = 1$ in (3.4.17) we say A is a rotation about the axis u_3, through an angle θ.

EXAMPLE 2. Take $V = \mathbb{R}^3$ and

$$T = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \tag{3.4.19}$$

Then $\det(T - \lambda I) = -(\lambda^3 - 1) = -(\lambda - 1)(\lambda^2 + \lambda + 1)$, with roots

$$\lambda_0 = 1, \quad \lambda_\pm = e^{\pm 2\pi i/3} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i. \tag{3.4.20}$$

We obtain eigenvectors in $V_{\mathbb{C}} = \mathbb{C}^3$,

$$v_0 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad v_\pm = \begin{pmatrix} -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i \\ 1 \\ -\frac{1}{2} \mp \frac{\sqrt{3}}{2} i \end{pmatrix} = \begin{pmatrix} e^{\pm 2\pi i/2} \\ 1 \\ e^{\mp 2\pi i/3} \end{pmatrix}, \tag{3.4.21}$$

readily seen to be mutually orthogonal in $\mathbb{C}^3$. We can write

$$v_+ = u + iv, \tag{3.4.22}$$

with

$$u = \begin{pmatrix} -\frac{1}{2} \\ 1 \\ -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} \cos\frac{2\pi}{3} \\ 1 \\ \cos\frac{2\pi}{3} \end{pmatrix}, \quad v = \frac{\sqrt{3}}{2}\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} \sin\frac{2\pi}{3} \\ 0 \\ -\sin\frac{2\pi}{3} \end{pmatrix}, \tag{3.4.23}$$

and note that u and $v \in \mathbb{R}^3$ are orthogonal (to each other and to v_0), and each has norm $\sqrt{3/2}$. One can then apply T in (3.4.19) to u and v in (3.4.23) and verify directly that

$$Tu = cu + sv, \quad Tv = -su + cv, \tag{3.4.24}$$

with

$$c = -\frac{1}{2} = \cos\frac{2\pi}{3}, \quad s = -\frac{\sqrt{3}}{2} = -\sin\frac{2\pi}{3}, \tag{3.4.25}$$

consistent with (3.4.10)–(3.4.12), with $\lambda_+ = e^{-i\theta}$.

Collecting these calculations, we see that, with v_0 as in (3.4.21) and u, v as in (3.4.23),

$$u_1 = \sqrt{\frac{2}{3}}u, \quad u_2 = \sqrt{\frac{2}{3}}v, \quad u_3 = \sqrt{\frac{1}{3}}v_0 \tag{3.4.26}$$

form an orthonormal basis of $\mathbb{R}^3$ with respect to which the matrix form of T in (3.4.19) becomes

$$A = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} & \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} & \\ & & 1 \end{pmatrix}. \tag{3.4.27}$$

Returning to the basic definitions, we record the following useful complementary characterization of unitary transformations.

Proposition 3.4.5. *Let V be a finite-dimensional inner product space, $T \in \mathcal{L}(V)$. Then T is unitary if and only if it is an isometry on V, i.e., if and only if*

$$\|Tu\| = \|u\|, \quad \forall\, u \in V. \tag{3.4.28}$$

Proof. First,

$$\|Tu\|^2 = (Tu, Tu) = (T^*Tu, u), \tag{3.4.29}$$

so $T^*T = I \Rightarrow T$ is an isometry. For the converse, we see that if T is an isometry, then $A = T^*T$ is a self-adjoint transformation satisfying

$$(Au, u) = (u, u), \quad \forall\, u \in V. \tag{3.4.30}$$

In particular, if $u = u_j$ is an eigenvector of A, satisfying $Au_j = \mu_j u_j$, then

$$\mu_j \|u_j\|^2 = (Au_j, u_j) = \|u_j\|^2, \tag{3.4.31}$$

so all eigenvalues of A are 1, hence $A = I$. □

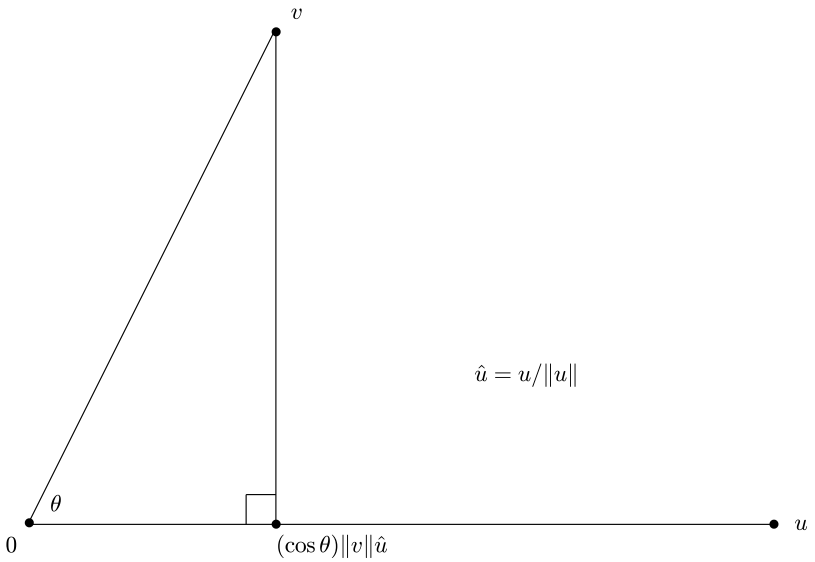

Figure 3.4.1. The cosine of an angle

Exercises

1. Let V be a real inner product space. Consider nonzero vectors $u, v \in V$. Show that the *angle* θ between these vectors is uniquely defined by the formula

$$(u, v) = \|u\| \cdot \|v\| \cos\theta, \quad 0 \leq \theta \leq \pi.$$

See Figure 3.4.1. Show that $0 < \theta < \pi$ if and only if u and v are linearly independent. Show that

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2 + 2\|u\| \cdot \|v\| \cos\theta.$$

This identity is known as the Law of Cosines.
If u and v are linearly independent, produce a linear isomorphism from $\mathrm{Span}\{u, v\}$ to $\mathbb{R}^2$ that preserves inner products and takes u to $\|u\|i$. Peek ahead at §3.7, and make contact with the characterization of cos and sin in (3.7.76).

For V as above, $u, v, w \in V$, we define the angle between the line segment from w to u and the line segment from w to v to be the angle between $u - w$ and $v - w$. (We assume $w \neq u$ and $w \neq v$.)

2. Take $V = \mathbb{R}^2$, with its standard orthonormal basis $i = (1, 0),\ j = (0, 1)$. Let

$$u = (1, 0), \quad v = (\cos\varphi, \sin\varphi), \quad 0 \le \varphi < 2\pi.$$

Show that, according to the definition of Exercise 1, the angle θ between u and v is given by

$$\begin{aligned} \theta &= \varphi \qquad\quad \text{if } \ 0 \le \varphi \le \pi, \\ &\quad 2\pi - \varphi \quad \text{if } \ \pi \le \varphi < 2\pi. \end{aligned}$$

3. Let V be a real inner product space and let $R \in \mathcal{L}(V)$ be orthogonal. Show that if $u, v \in V$ are nonzero and $\tilde{u} = Ru,\ \tilde{v} = Rv$, then the angle between u and v is equal to the angle between $\tilde{u}$ and $\tilde{v}$. Show that if $\{e_j\}$ is an orthonormal basis of V, there exists an orthogonal transformation R on V such that $Ru = \|u\|e_1$ and Rv is in the linear span of e_1 and e_2.

4. Consider a triangle as in Fig. 3.4.2. Show that

$$h = c \sin A,$$

and also

$$h = a \sin C.$$

Use these calculations to show that

$$\frac{\sin A}{a} = \frac{\sin C}{c} = \frac{\sin B}{b}.$$

This identity is known as the Law of Sines.

Exercises 5–11 deal with cross products of vectors in $\mathbb{R}^3$.

5. If $u, v \in \mathbb{R}^3$, we define the cross product $u \times v = \Pi(u, v)$ to be the unique bilinear map $\Pi : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ satisfying

$$\begin{gathered} u \times v = -v \times u, \quad \text{and} \\ i \times j = k, \quad j \times k = i, \quad k \times i = j, \end{gathered}$$

where $\{i, j, k\}$ is the standard basis of $\mathbb{R}^3$.
Note. To say Π is bilinear is to say $\Pi(u, v)$ is linear in both u and v.
Show that, for all $u, v, w \in \mathbb{R}^3$,

$$w \cdot (u \times v) = \det \begin{pmatrix} w_1 & u_1 & v_1 \\ w_2 & u_2 & v_2 \\ w_3 & u_3 & v_3 \end{pmatrix}, \tag{3.4.32}$$

and show that this property uniquely specifies $u \times v$. Explain how (3.4.32) can be rewritten as

$$u \times v = \det \begin{pmatrix} i & u_1 & v_1 \\ j & u_2 & v_2 \\ k & u_3 & v_3 \end{pmatrix} = \begin{pmatrix} u_2 v_3 - u_3 v_2 \\ u_3 v_1 - u_1 v_3 \\ u_1 v_2 - u_2 v_1 \end{pmatrix}. \tag{3.4.33}$$

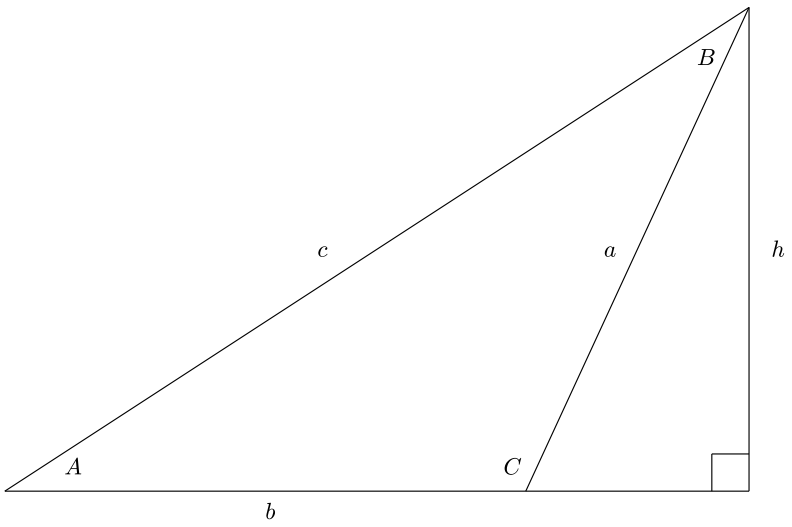

Figure 3.4.2. Law of Sines

6. Recall that $T \in SO(3)$ provided that T is a real 3×3 matrix satisfying $T^tT = I$ and $\det T > 0$, (hence $\det T = 1$). Show that

$$T \in SO(3) \Longrightarrow Tu \times Tv = T(u \times v). \tag{3.4.34}$$

Hint. Multiply the 3×3 matrix in (3.4.32) on the left by T.

7. Show that, if θ is the angle between u and v in $\mathbb{R}^3$, then

$$\|u \times v\| = \|u\| \cdot \|v\| \cdot |\sin\theta|. \tag{3.4.35}$$

More generally, show that for all $u, v, w, x \in \mathbb{R}^3$,

$$\begin{aligned}(u \times v) \cdot (w \times x) &= (u \cdot w)(v \cdot x) - (u \cdot x)(v \cdot w) \\ &= \det \begin{pmatrix} u \cdot w & u \cdot x \\ v \cdot w & v \cdot x \end{pmatrix}.\end{aligned} \tag{3.4.36}$$

Hint. Check these identities for $u = i,\ v = ai + bj$, in which case $u \times v = bk$, and use Exercise 6 to show that this suffices.
Note that the left side of (3.4.36) is then

$$bk \cdot (w \times x) = \det \begin{pmatrix} 0 & w \cdot i & x \cdot i \\ 0 & w \cdot j & x \cdot j \\ b & w \cdot k & x \cdot k \end{pmatrix}.$$

Show that this equals the right side of (3.4.36).

8. Show that $\kappa : \mathbb{R}^3 \to$ Skew(3), the set of antisymmetric real 3×3 matrices, given by

$$\kappa(y) = \begin{pmatrix} 0 & -y_3 & y_2 \\ y_3 & 0 & -y_1 \\ -y_2 & y_1 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}, \tag{3.4.37}$$

satisfies

$$\kappa(y)x = y \times x. \tag{3.4.38}$$

Show that, with $[A, B] = AB - BA$,

$$\begin{aligned} \kappa(x \times y) &= \big[\kappa(x), \kappa(y)\big], \\ \operatorname{Tr}\big(\kappa(x)\kappa(y)^t\big) &= 2x \cdot y. \end{aligned} \tag{3.4.39}$$

9. Show that if $u, v, w \in \mathbb{R}^3$, then the first part of (3.4.39) implies

$$(u \times v) \times w = u \times (v \times w) - v \times (u \times w).$$

Relate this to the identity

$$[[A, B], C] = [A, [B, C]] - [B, [A, C]],$$

for $A, B, C \in M(n, \mathbb{R})$ (with $n = 3$).

10. Show that, if $u, v, w, \in \mathbb{R}^3$,

$$v \times (u \times w) = (v \cdot w)u - (v \cdot u)w.$$

Hint. Start with the observation that $v \times (u \times w)$ is in $\operatorname{Span}\{u, w\}$ and is orthogonal to v. *Alternative.* Use Exercise 6 to reduce the calculation to the case $u = i,\ w = ai + bj$.

11. Deduce from (3.4.32) that, for $u, v, w \in \mathbb{R}^3$,

$$u \cdot (v \times w) = (u \times v) \cdot w.$$

12. Demonstrate the following result, which contains both Proposition 3.3.2 and Proposition 3.4.2. Let V be a finite dimensional inner product space. We say $T : V \to V$ is *normal* provided T and T^* commute, i.e.,

$$TT^* = T^*T. \tag{3.4.40}$$

Proposition 3.4.6. *If V is a finite dimensional complex inner product space and $T \in \mathcal{L}(V)$ is normal, then V has an orthonormal basis of eigenvectors of T.*

Hint. Write $T = A + iB,\ A$ and B self adjoint. Then (3.4.40) $\Rightarrow AB = BA$. Apply Exercise 3 of §3.3.

13. Show that if $A \in O(n)$ and $\det A = -1$, then -1 is an eigenvalue of A, with odd multiplicity.

Recall from §3.3 that if V is an inner product space, $T \in \mathcal{L}(V)$ belongs to $\mathrm{Skew}(V)$ if and only if $T^* = -T$. For such T, all eigenvalues are purely imaginary.

14. Show that

$$\mathcal{C}(T) = (I - T)^{-1}(I + T) \tag{3.4.41}$$

defines a map

$$\mathcal{C} : \mathrm{Skew}(V) \longrightarrow \{A \in U(V) : -1 \notin \mathrm{Spec}\, A\}, \tag{3.4.42}$$

with inverse

$$\mathcal{C}^{-1}(A) = -(I + A)^{-1}(I - A). \tag{3.4.43}$$

We call $\mathcal{C}$ the *Cayley transform*.
Hint. If $A = \mathcal{C}(T)$, start by showing

$$A^* = (I + T)^*\big((I - T)^{-1}\big)^* = (I - T)(I + T)^{-1}.$$

15. Specializing Exercise 14 to $V = \mathbb{R}^n$, show that (3.4.42) becomes

$$\mathcal{C} : \mathrm{Skew}(n) \longrightarrow \{A \in SO(n) : -1 \notin \mathrm{Spec}\, A\},$$

one-to-one and onto.

16. Extend the scope of Exercise 8 in §3.1, on QR factorization, as follows. Let $A \in G\ell(n, \mathbb{C})$ have columns $a_1, \dots, a_n \in \mathbb{C}^n$. Use the Gramm-Schmidt construction to produce an orthonormal basis $\{q_1, \dots, q_n\}$ of $\mathbb{C}^n$ such that $\mathrm{Span}\{a_1, \dots, a_j\} = \mathrm{Span}\{q_1, \dots, q_j\}$ for $1 \leq j \leq n$. Denote by $Q \in U(n)$ the matrix with columns $q_1, \dots, q_n$. Show that

$$A = QR,$$

where R is the same sort of upper triangular matrix as described in that Exercise 8.

17. Let $A \in M(n, \mathbb{C})$ be positive definite. Apply to $A^{1/2}$ the QR factorization described in Exercise 16:

$$A^{1/2} = QR, \quad Q \in U(n), \quad R \text{ upper triangular.}$$

Deduce that

$$A = LL^*, \quad L = R^* \text{ lower triangular.}$$

This is a Cholesky decomposition. Use Exercise 7 of §3.3 to compare this with (3.3.32).

3.5. Schur's upper triangular representation

Let V be an n-dimensional complex vector space, equipped with an inner product, and let $T \in \mathcal{L}(V)$. The following is an important alternative to Proposition 2.4.1.

Proposition 3.5.1. *There is an orthonormal basis of V with respect to which T has an upper triangular form.*

Note that an upper triangular form with respect to some basis was achieved in (2.3.11), but there the basis was not guaranteed to be orthonormal. We will obtain Proposition 3.5.1 as a consequence of

Proposition 3.5.2. *There is a sequence of vector spaces V_j of dimension j such that*

$$V = V_n \supset V_{n-1} \supset \cdots \supset V_1 \tag{3.5.1}$$

and

$$T : V_j \to V_j. \tag{3.5.2}$$

We show how Proposition 3.5.2 implies Proposition 3.5.1. In fact, given (3.5.1)–(3.5.2), pick $u_n \perp V_{n-1}$, a unit vector, then pick a unit $u_{n-1} \in V_{n-1}$ such that $u_{n-1} \perp V_{n-2}$, and so forth, to achieve the conclusion of Proposition 3.5.1. Otherwise said, $\{u_j : 1 \le j \le n\}$ is constructed to be an orthonormal basis of V satisfying $u_j \in V_j$ for each j. We see that, for each j, Tu_j is a linear combination of $\{u_\ell : \ell \le j\}$, and this yields the desired upper triangular form. □

Meanwhile, Proposition 3.5.2 is a simple inductive consequence of the following result.

Lemma 3.5.3. *Given $T \in \mathcal{L}(V)$ as above, there is a linear subspace V_{n-1}, of dimension $n-1$, such that $T : V_{n-1} \to V_{n-1}$.*

Proof. We apply Proposition 2.1.1 to T^* to obtain a nonzero $v_1 \in V$ such that $T^* v_1 = \lambda v_1$, for some $\lambda \in \mathbb{C}$. Then the conclusion of Lemma 3.5.3 holds with $V_{n-1} = (v_1)^\perp$. □

We illustrate the steps described above to achieve a "Schur normal form" with the following example: $V = \mathbb{C}^3$ and

$$T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 2 \end{pmatrix}. \tag{3.5.3}$$

Note that

$$\det(\lambda I - A) = \lambda^3 - 2\lambda^2 + \lambda = \lambda(\lambda - 1)^2. \tag{3.5.4}$$

We have

$$T^* = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}, \tag{3.5.5}$$

and

$$\mathcal{E}(T^*, 0) = \mathrm{Span}\Big\{ \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \Big\}. \tag{3.5.6}$$

Thus, in the notation of the proof of Lemma 3.5.3, we have $v_1 = (1, -2, 1)^t$. Hence

$$V_2 = (v_1)^\perp = \mathrm{Span}\Big\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \Big\}. \tag{3.5.7}$$

The unit vector $u_3 \perp V_2$ might as well be

$$u_3 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}. \tag{3.5.8}$$

We next need a one-dimensional subspace $V_1 \subset V_2$, invariant under T. In fact,

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \tag{3.5.9}$$

so we can take V_1 to be the span of this vector. Thus V_1 is spanned by the unit vector

$$u_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \tag{3.5.10}$$

and this, together with

$$u_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \tag{3.5.11}$$

forms an orthonormal basis of V_2. We have

$$\begin{aligned} Tu_1 &= u_1, \\ Tu_2 &= \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ -1 \\ -2 \end{pmatrix} = -\sqrt{\frac{3}{2}} u_1 + u_2, \\ Tu_3 &= \frac{1}{\sqrt{6}} \begin{pmatrix} -2 \\ 1 \\ 4 \end{pmatrix} = \frac{1}{\sqrt{2}} u_1 - \sqrt{3} u_2. \end{aligned} \tag{3.5.12}$$

Thus, with respect to the orthonormal basis $\{u_1, u_2, u_3\}$, the matrix representation of T is

$$M = \begin{pmatrix} 1 & -\sqrt{3/2} & \sqrt{1/2} \\ 0 & 1 & -\sqrt{3} \\ 0 & 0 & 0 \end{pmatrix}, \tag{3.5.13}$$

and this is a Schur normal form of T.

Recall from §3.2 that the Hilbert-Schmidt norm of a linear transformation is independent of the choice of orthonormal basis. In this case, we readily verify that

$$\begin{aligned} \|T\|_{\mathrm{HS}}^2 &= 1+1+1+4 = 7, \\ \|M\|_{\mathrm{HS}}^2 &= 1+1+\tfrac{3}{2}+\tfrac{1}{2}+3 = 7. \end{aligned} \tag{3.5.14}$$

Proposition 3.5.1 has uses that do not depend on knowing a specific Schur normal form for T. Here is an example of such an application, known as *Schur's inequality*. It involves the Hilbert-Schmidt norm, introduced in §3.2 and mentioned above.

Proposition 3.5.4. *Let $T \in \mathcal{L}(V)$, where V is a complex inner product space of dimension n. Assume the eigenvlues of T are $\lambda_1, \dots, \lambda_n$ (repeated according to multiplicity). Then*

$$\sum_{j=1}^{n} |\lambda_j|^2 \leq \|T\|_{\mathrm{HS}}^2. \tag{3.5.15}$$

Proof. Let $A = (a_{jk})$ denote the matrix representation of T described in Proposition 3.5.1. Since A is upper triangular, the eigenvalues of A are precisely the diagonal entries, a_{jj}. Hence

$$\begin{aligned} \sum_{j=1}^{n} |\lambda_j|^2 &= \sum_{j=1}^{n} |a_{jj}|^2 \\ &\leq \sum_{j,k} |a_{jk}|^2 \\ &= \|A\|_{\mathrm{HS}}^2 = \|T\|_{\mathrm{HS}}^2. \end{aligned} \tag{3.5.16}$$

□

There is an interesting application of Proposition 3.5.4 to roots of a polynomial. Take a polynomial of degree n,

$$p(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0, \tag{3.5.17}$$

with $a_j \in \mathbb{C}$. As shown in Proposition 2.3.4, we can form the companion matrix

$$A = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}, \tag{3.5.18}$$

and

$$\det(\lambda I - A) = p(\lambda). \tag{3.5.19}$$

Thus the eigenvalues of A coincide with the roots $\lambda_1, \dots, \lambda_n$ of $p(\lambda)$, repeated according to multiplicity. Applying (3.5.15), we have the following.

Corollary 3.5.5. *If* $\{\lambda_1, \ldots, \lambda_n\}$ *are the roots of the polynomial* $p(\lambda)$ *in* (3.5.17), *then*

$$\sum_{k=1}^{n} |\lambda_k|^2 \leq n - 1 + \sum_{j=0}^{n-1} |a_j|^2. \tag{3.5.20}$$

REMARK. The matrix (3.5.3) is the companion matrix of the polynomial $\lambda(\lambda-1)^2$, arising in (3.5.4).

Exercises

1. Put the following matrices in Schur upper triangular form.

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ -1 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 2 & 0 \\ 3 & 0 & 3 \\ 0 & -2 & 0 \end{pmatrix}.$$

2. Let $\mathcal{D}(n) \subset M(n, \mathbb{C})$ denote the set of matrices all of whose eigenvalues are distinct. Show that $\mathcal{D}(n)$ is dense in $M(n, \mathbb{C})$, i.e., given $A \in M(n, \mathbb{C})$, there exist $A_k \in \mathcal{D}(n)$ such that $A_k \to A$.
Hint. Pick an orthonormal basis to put A in upper triangular form and tweak the diagonal entries.

3. Fill in the details in the following proposed demonstration of the Cayley-Hamilton theorem, i.e.,

$$K_A(\lambda) = \det(\lambda I - A) \Longrightarrow K_A(A) = 0, \quad \forall\, A \in M(n, \mathbb{C}).$$

First, demonstrate this for A diagonal, then for A diagonalizable, hence for $A \in \mathcal{D}(n)$. Show that $\Phi(A) = K_A(A)$ defines a continuous map Φ on $M(n, \mathbb{C})$. Then use Exercise 2.

4. In the setting of Proposition 3.5.1, let $S, T \in \mathcal{L}(V)$ commute, i.e., $ST = TS$. Show that V has an orthonormal basis with respect to which S and T are simultaneously in upper triangular form.
Hint. Start by extending Lemma 3.5.3.

5. Let $A \in \mathcal{L}(\mathbb{R}^n)$. Show that there is an orthonormal basis of $\mathbb{R}^n$ with respect to which A has an upper triangular form if and only if all the eigenvalues of A are real.

6. In the setting of Proposition 3.5.4, show that the inequality (3.5.15) is an *equality* if and only if T is normal. (Recall Exercise 12 of §3.4.)

3.6. Polar decomposition and singular value decomposition

For complex numbers, polar decomposition is the representation

$$z = re^{i\theta}, \tag{3.6.1}$$

for a given $z \in \mathbb{C}$, with $r \geq 0$ and $\theta \in \mathbb{R}$. In fact, $r = |z| = (z\overline{z})^{1/2}$. If $z \neq 0$, then $r > 0$ and $e^{i\theta}$ is uniquely determined. The following is a first version of polar decomposition for square matrices.

Proposition 3.6.1. *If $A \in M(n, \mathbb{C})$ is invertible, then it has a unique factorization*

$$A = KP, \quad K \in U(n), \quad P = P^*, \quad \textit{positive definite.} \tag{3.6.2}$$

Proof. If A has such a factorization, then

$$A^*A = P^2. \tag{3.6.3}$$

Conversely, if A is invertible, then A^*A is self adjoint and positive definite, and, as seen in §3.3, all its eigenvalues λ_j are > 0, and there exists an orthonormal basis $\{v_j\}$ of $\mathbb{C}^n$ consisting of associated eigenvectors. Thus, we obtain (3.6.3) with

$$Pv_j = \lambda_j^{1/2} v_j. \tag{3.6.4}$$

In such a case, we have $A = KP$ if we set

$$K = AP^{-1}. \tag{3.6.5}$$

We want to show that $K \in U(n)$. It suffices to show that

$$\|Ku\| = \|u\| \tag{3.6.6}$$

for all $u \in \mathbb{C}^n$. To see this, note that, for $v \in \mathbb{C}^n$,

$$\|KPv\|^2 = \|Av\|^2 = (Av, Av) = (A^*Av, v) = (P^2v, v) = \|Pv\|^2. \tag{3.6.7}$$

This gives (3.6.6) whenever $u = Pv$, but P is invertible, so we do have (3.6.6) for all $u \in \mathbb{C}^n$. This establishes the existence of the factorization (3.6.2). The formulas (3.6.4)–(3.6.5) for P and K establish uniqueness. □

Here is the real case.

Proposition 3.6.2. *If $A \in M(n, \mathbb{R})$ is invertible, then it has a unique factorization*

$$A = KP, \quad K \in O(n), \quad P = P^*, \ \textit{positive definite.} \tag{3.6.8}$$

Proof. In the proof of Proposition 3.6.1, adapted to the current setting, $\mathbb{R}^n$ has an orthonormal basis $\{v_j\}$ of eigenvectors of A^*A, so (3.6.4) defines a positive definite $P \in M(n, \mathbb{R})$. Then $K = AP^{-1}$ is unitary and belongs to $M(n, \mathbb{R})$, so it belongs to $O(n)$. □

We extend Proposition 3.6.1 to non-invertible matrices.

Proposition 3.6.3. *If $A \in M(n, \mathbb{C})$, then it has a factorization of the form* (3.6.2)*, with P positive semidefinite.*

Proof. We no longer assert uniqueness of K in (3.6.2). However, P is still uniquely defined by (3.6.3)–(3.6.4). This time we have only $\lambda_j \geq 0$, so P need not be invertible, and we cannot bring in (3.6.5). Instead, we proceed as follows. First, somewhat parallel to (3.6.7), we have

$$\|Pv\|^2 = (P^2v, v) = (A^*Av, v) = \|Av\|^2, \tag{3.6.9}$$

for all $v \in \mathbb{C}^n$. Hence $\mathcal{N}(P) = \mathcal{N}(A)$, and we have the following orthogonal, direct sum decomposition,

$$\mathbb{C}^n = V_0 \oplus V_1,$$

where

$$V_0 = \mathcal{R}(P) = \mathrm{Span}\{v_j : \lambda_j > 0\}, \quad V_1 = \mathcal{N}(P) = \mathcal{N}(A), \tag{3.6.10}$$

with v_j as in (3.6.4). We set

$$\begin{aligned} &Q : V_0 \longrightarrow V_0, \quad Qv_j = \lambda_j^{-1/2} v_j, \\ &K_0 : V_0 \longrightarrow \mathbb{C}^n, \quad K_0 v = AQv. \end{aligned} \tag{3.6.11}$$

It follows that

$$K_0 Pv = Av, \quad \forall\, v \in V_0, \tag{3.6.12}$$

and that (3.6.7) holds for all $v \in V_0$, so $K_0 : V_0 \to \mathbb{C}^n$ is an injective isometry. Now we can define

$$K_1 : V_1 \longrightarrow \mathcal{R}(K_0)^\perp = \mathcal{R}(A)^\perp \tag{3.6.13}$$

to be any isometric isomorphism between V_1 and $\mathcal{R}(K_0)^\perp$, which have the same dimension. Then we set

$$K = K_0 \oplus K_1 : V_0 \oplus V_1 \longrightarrow \mathbb{C}^n, \tag{3.6.14}$$

which is an isometric isomorphism, hence an element of $U(n)$. We have

$$KPv = Av, \tag{3.6.15}$$

both for $v \in V_0$, by (3.6.12), and for $v \in V_1 = \mathcal{N}(P) = \mathcal{N}(A)$, thus proving Proposition 3.6.3. □

Parallel to Proposition 3.6.2, there is the following analogue of Proposition 3.6.3 for real matrices.

Proposition 3.6.4. *If $A \in M(n, \mathbb{R})$, then it has a factorization of the form* (3.6.8)*, with P positive semidefinite.*

We give some examples to illustrate polar decomposition.

Example 1. Take

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \tag{3.6.16}$$

which is invertible. We have

$$A^*A = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix} = P^2, \quad \text{with} \\ P = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}. \tag{3.6.17}$$

Then $A = KP$, with

$$K = AP^{-1} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{3.6.18}$$

Example 2. Take

$$A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \tag{3.6.19}$$

which is not invertible. We have

$$A^*A = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} = P^2, \quad \text{with} \\ P = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}. \tag{3.6.20}$$

Following the treatment of Proposition 3.6.3, we have $\mathbb{R}^2 = V_0 \oplus V_1$, with

$$V_0 = \mathcal{R}(P) = \operatorname{Span} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad V_1 = \mathcal{N}(P) = \mathcal{N}(A) = \operatorname{Span} \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{3.6.21}$$

As in (3.6.11), we take

$$K_0 : V_0 \to \mathbb{R}^2, \quad K_0 v = AQv. \tag{3.6.22}$$

where Q inverts P on V_0. Since $P|_{V_0}$ has the single eigenvalue 2, K_0 is specified by

$$K_0 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \tfrac{1}{2} A \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{3.6.23}$$

Next, we take

$$K_1 : V_1 \to \mathcal{R}(K_0)^\perp = \mathcal{R}(A)^\perp = \operatorname{Span} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{3.6.24}$$

to be any isometric isomorphism. Since these vector spaces are 1-dimensional, there are two choices:

$$K_1 \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \text{or} \quad K_1 \begin{pmatrix} 1 \\ -1 \end{pmatrix} = -\begin{pmatrix} 1 \\ 1 \end{pmatrix}. \tag{3.6.25}$$

We can now specify $K = K_0 \oplus K_1$ in the polar decomposition $A = KP$, via

$$K \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \tfrac{1}{2} K_0 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \tfrac{1}{2} K_1 \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \\ K \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \tfrac{1}{2} K_0 \begin{pmatrix} 1 \\ 1 \end{pmatrix} - \tfrac{1}{2} K_1 \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{3.6.26}$$

Hence, in the two respective cases given in (3.6.25),

$$K = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \text{or} \quad K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{3.6.27}$$

In cases where $\dim V_1 > 1$ (i.e., where $\dim \mathcal{N}(A) > 1$, or $\mathbb{F} = \mathbb{C}$), one would have an infinite number of possibilities for K in the polar decomposition of A.

Having treated polar decomposition, we now apply Propositions 3.6.3–3.6.4 to the following factorization.

Proposition 3.6.5. *If $A \in M(n, \mathbb{C})$, then we can write*

$$A = UDV^*, \quad U, V \in U(n), \quad D \in M(n, \mathbb{C}) \ \text{ diagonal}, \tag{3.6.28}$$

in fact,

$$D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}, \quad d_j \geq 0. \tag{3.6.29}$$

If $A \in M(n, \mathbb{R})$, we have (3.6.28) *with $U, V \in O(n)$.*

Proof. By Proposition 3.6.3 we have $A = KP$, with $K \in U(n)$, P positive semidefinite. By results of §3.3, we have $P = VDV^*$, for some $V \in U(n)$, D as in (3.6.29). Hence (3.6.28) holds with $U = KV$. If $A \in M(n, \mathbb{R})$, a similar use of Proposition 3.6.4 applies. □

A factorization of the form (3.6.28)–(3.6.29) is called a singular value decomposition (or SVD) of A. The elements d_j in (3.6.29) that are > 0 are called the singular values of A.

Finally, we extend the singular value decomposition to rectangular matrices.

Proposition 3.6.6. *If $A \in M(m \times n, \mathbb{C})$, so $A : \mathbb{C}^n \to \mathbb{C}^m$, then we can write*

$$A = UDV^*, \quad U \in U(m), \ V \in U(n), \tag{3.6.30}$$

and

$$D \in M(m \times n, \mathbb{C}) \ \text{ diagonal, with diagonal entries } d_j \geq 0. \tag{3.6.31}$$

Proof. We treat the case

$$A : \mathbb{C}^n \longrightarrow \mathbb{C}^m, \quad m = n + k > n. \tag{3.6.32}$$

If $m < n$, one can apply the argument that follows to A^*.

When (3.6.32) holds, there exists

$$K \in U(m), \quad K : \mathcal{R}(A) \longrightarrow \mathbb{C}^n \subset \mathbb{C}^m, \tag{3.6.33}$$

so that

$$KA = \begin{pmatrix} B \\ 0 \end{pmatrix}, \quad B \in M(n, \mathbb{C}), \ 0 \in M(k \times n, \mathbb{C}). \tag{3.6.34}$$

By Proposition 3.6.5, we can write

$$B = WD_0V^*, \quad W, V \in U(n), \ D_0 \ \text{ diagonal}, \tag{3.6.35}$$

so

$$KA = \begin{pmatrix} WD_0V^* \\ 0 \end{pmatrix} = \begin{pmatrix} W & \\ & I \end{pmatrix} \begin{pmatrix} D_0 \\ 0 \end{pmatrix} V^*, \tag{3.6.36}$$

and hence (3.6.30) holds with

$$U = K^{-1}\begin{pmatrix} W & \\ & I \end{pmatrix}, \quad D = \begin{pmatrix} D_0 \\ 0 \end{pmatrix}. \tag{3.6.37}$$

□

There is a similar result for real rectangular matrices.

Proposition 3.6.7. *If $A \in M(m \times n, \mathbb{R})$, then we can write*

$$A = UDV^*, \quad U \in O(m),\ V \in O(n), \tag{3.6.38}$$

and D as in (3.6.31).

Remark. As in the setting of Proposition 3.6.5, the nonzero quantities d_j in (3.6.31) are called the singular values of A.

Having Propositions 3.6.6 and 3.6.7, we record some additional useful identities associated to the decomposition (3.6.30), namely

$$A^*A = V(D^*D)V^*, \quad AA^* = U(DD^*)U^*, \tag{3.6.39}$$

and

$$D^*D = D_0^2, \quad DD^* = \begin{pmatrix} D_0^* & 0 \\ 0 & 0 \end{pmatrix}. \tag{3.6.40}$$

Example. Take

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}. \tag{3.6.41}$$

We have

$$A^*A = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}, \quad AA^* = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}. \tag{3.6.42}$$

Hence we have the first identity in (3.6.39) with

$$V = I, \quad D^*D = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}, \tag{3.6.43}$$

which yields

$$D_0 = \begin{pmatrix} \sqrt{3} & \\ & \sqrt{2} \end{pmatrix}, \quad D = \begin{pmatrix} \sqrt{3} & 0 \\ 0 & \sqrt{2} \\ 0 & 0 \end{pmatrix}, \quad DD^* = \begin{pmatrix} 3 & & \\ & 2 & \\ & & 0 \end{pmatrix}. \tag{3.6.44}$$

To proceed, we have

$$\operatorname{Spec} AA^* = \{3, 2, 0\}, \tag{3.6.45}$$

and

$$\mathcal{E}(AA^*, 3) = \operatorname{Span}\begin{pmatrix}1\\1\\1\end{pmatrix}, \quad \mathcal{E}(AA^*, 2) = \operatorname{Span}\begin{pmatrix}1\\0\\-1\end{pmatrix}, \tag{3.6.46}$$
$$\mathcal{E}(AA^*, 0) = \operatorname{Span}\begin{pmatrix}1\\-2\\1\end{pmatrix}.$$

The norms of these three vectors are $\sqrt{3}, \sqrt{2}$, and $\sqrt{6}$, respectively. If we take

$$U = \begin{pmatrix}1/\sqrt{3} & -1/\sqrt{2} & 1/\sqrt{6}\\ 1/\sqrt{3} & 0 & -2/\sqrt{6}\\ 1/\sqrt{3} & 1/\sqrt{2} & 1/\sqrt{6}\end{pmatrix}, \tag{3.6.47}$$

we verify that $AA^* = U(DD^*)U^*$, and that the singular value decomposition (3.6.30) holds, with V, D, and U given in (3.6.43), (3.6.44), and (3.6.47).

Returning to generalities, we record the following straightforward consequence of (3.6.30).

Corollary 3.6.8. *Assume $A \in M(m \times n, \mathbb{C})$ has the SVD form (3.6.30)–(3.6.31). Let $\{u_j\}$ denote the columns of U and $\{v_j\}$ the columns of V. Then, for $w \in \mathbb{C}^n$,*

$$Aw = \sum_j d_j(w, v_j)u_j. \tag{3.6.48}$$

This result in turn readily leads to the following.

Proposition 3.6.9. *In the setting of Corollary 3.6.8, assume*

$$j > J \Longrightarrow d_j \leq \delta. \tag{3.6.49}$$

Define $A_J : \mathbb{C}^n \to \mathbb{C}^m$ by

$$A_J w = \sum_{j \leq J} d_j(w, v_j)u_j. \tag{3.6.50}$$

Then

$$\|A - A_J\| \leq \delta. \tag{3.6.51}$$

Proof. We have

$$\begin{aligned}\|(A - A_J)w\|^2 &= \sum_{j>J} d_j^2 |(w, v_j)|^2\\ &\leq \delta^2 \|w\|^2.\end{aligned} \tag{3.6.52}$$

□

Proposition 3.6.9 is exploited in an approach to *image compression*, which we can illustrate as follows. Suppose one has a picture of a scene, made up of 2000×2000 pixels. The data can be regarded as encoded in a matrix $A \in M(n, \mathbb{R})$, $n = 2000$. The entries could represent either a grey scale or a color scale. Take the singular value decomposition of A, as in (3.6.30). Doing this is way beyond hand

calculation, but various numerical software packages allow one to do this on a computer, using a command with syntax like

$$[U, D, V] = \mathrm{SVD}(A). \tag{3.6.53}$$

In the current case, D is a diagonal matrix with 2000 diagonal entries $d_j \geq 0$, arranged in decreasing order, $d_j \searrow$. For a discussion of how this can be done, see [**3**].

Now it has been observed that, for many such matrices arising from pictures of typical scenes, the entries d_j get quite small fairly quickly, so that A_J, given by (3.6.50), is a useful approximation to A for $J = 100$, or maybe even smaller. The task of storing the information needed to produce A_J for such a value of J involves much less memory than is needed to store the original matrix A. This would allow for the storage of many more pictures on a device with a given amount of memory. For more on this, see pp. 332–333 of [**9**].

Exercises

1. Produce polar decompositions for the following matrices.

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

2. Produce singular value decompositions for the following matrices.

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

3. Extend the results on polar decomposition given in this section from $A \in M(n, \mathbb{F})$ to the setting of $A \in \mathcal{L}(V)$, where V is a finite-dimensional inner product space (over $\mathbb{R}$ or $\mathbb{C}$).

4. Extend the results on SVDs given in this section from $A \in M(m \times n, \mathbb{F})$ to the setting of $A \in \mathcal{L}(V, W)$, where V and W are finite-dimensional inner product spaces (over $\mathbb{R}$ or $\mathbb{C}$).

5. Let $\mathcal{P}_2$ be the space of polynomials in x of degree ≤ 2, with inner product

$$(f, g) = \frac{1}{2} \int_{-1}^{1} f(x)\overline{g(x)}\, dx,$$

and let $A : \mathcal{P}_2 \to \mathcal{P}_2$ be given by

$$Af(x) = f'(x) + f(x).$$

Give the polar decomposition of A.

6. In the setting of Exercise 5, give the singular value decomposition of A.

3.7. The matrix exponential

Take $A \in M(n, \mathbb{F})$, with $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. The matrix exponential arises to represent solutions to the differential equation

$$\frac{dx}{dt} = Ax, \quad x(0) = v, \tag{3.7.1}$$

for a function $x : \mathbb{R} \to \mathbb{F}^n$, given $v \in \mathbb{F}^n$. One way to approach (3.7.1) is to construct the solution as a power series,

$$x(t) = \sum_{k=0}^{\infty} x_k t^k, \tag{3.7.2}$$

with coefficients $x_k \in \mathbb{F}^n$. As shown in calculus courses, if (3.7.2) is absolutely convergent on an interval $|t| < T$, then $x(t)$ is differentiable on this interval, and its derivative is obtained by differentiating the series term by term (cf. Chapter 4 of [**10**]). Anticipating that this will work, we write

$$x'(t) = \sum_{k=1}^{\infty} k x_k t^{k-1} = \sum_{\ell=0}^{\infty} (\ell + 1) x_{\ell+1} t^{\ell}. \tag{3.7.3}$$

Meanwhile,

$$Ax(t) = \sum_{\ell=0}^{\infty} A x_\ell t^{\ell}. \tag{3.7.4}$$

Comparing (3.7.3) and (3.7.4), we require

$$x_{\ell+1} = \frac{1}{\ell + 1} A x_\ell, \quad \ell \geq 0. \tag{3.7.5}$$

Meanwhile, the initial condition $x(0) = v$ forces $x_0 = v$. Thus, inductively,

$$x_0 = v, \quad x_1 = Av, \quad x_2 = \frac{1}{2} A^2 v, \ \ldots, \quad x_k = \frac{1}{k!} A^k v, \ldots, \tag{3.7.6}$$

and we have the power series

$$x(t) = \sum_{k=0}^{\infty} \frac{t^k}{k!} A^k v. \tag{3.7.7}$$

This power series is absolutely convergent for all $t \in \mathbb{R}$. To see this, we use (3.2.4) and the triangle inequality (3.1.14) to obtain the estimate

$$\Big\| \sum_{k=M}^{M+N} \frac{t^k}{k!} A^k v \Big\| \leq \sum_{k=M}^{M+N} \frac{|t|^k}{k!} \|A\|^k \|v\|, \tag{3.7.8}$$

which together with the ratio test guarantees absolute convergence for all $t \in \mathbb{R}$. Thus the term by term differentiation of (3.7.7) is valid, and we have a solution to (3.7.1). We write this solution as $x(t) = e^{tA} v$, where we set

$$e^{tA} = \sum_{k=0}^{\infty} \frac{t^k}{k!} A^k. \tag{3.7.9}$$

This is the matrix exponential. Calculations parallel to (3.7.3) give

$$\frac{d}{dt}e^{tA} = Ae^{tA} = e^{tA}A. \tag{3.7.10}$$

In fact, $e^{tA}v$ is the unique solution to (3.7.1). An essentially equivalent result is that e^{tA} is the unique solution to the matrix ODE

$$X'(t) = AX(t), \quad X(0) = I. \tag{3.7.11}$$

To see this, we apply the product rule

$$\frac{d}{dt}\big(B(t)X(t)\big) = B'(t)X(t) + B(t)X'(t) \tag{3.7.12}$$

to $B(t) = e^{-tA}$ and $X(t)$ as in (3.7.11). Thus, via (3.7.10), with A replaced by $-A$,

$$\frac{d}{dt}\big(e^{-tA}X(t)\big) = -e^{-tA}AX(t) + e^{-tA}AX(t) = 0, \tag{3.7.13}$$

so $e^{-tA}X(t)$ is independent of t. Evaluation at $t = 0$ gives

$$e^{-tA}X(t) = I, \quad \forall\, t \in \mathbb{R}, \tag{3.7.14}$$

whenever $X(t)$ solves (3.7.11). Since e^{tA} solves (3.7.11), we get

$$e^{-tA}e^{tA} = I, \quad \forall\, t \in \mathbb{R}, \tag{3.7.15}$$

i.e., e^{-tA} is the matrix inverse to e^{tA}. Multiplying (3.7.14) on the left by e^{tA} then gives

$$X(t) = e^{tA}, \tag{3.7.16}$$

which is the asserted uniqueness.

A useful computation related to (3.7.13) arises by applying d/dt to the product $e^{(s+t)A}e^{-tA}$. We have

$$\frac{d}{dt}\big(e^{(s+t)A}e^{-tA}\big) = e^{(s+t)A}Ae^{-tA} - e^{(s+t)A}Ae^{-tA} = 0, \tag{3.7.17}$$

so $e^{(s+t)A}e^{-tA}$ is independent of t. Evaluation at $t = 0$ gives

$$e^{(s+t)A}e^{-tA} = e^{sA}, \quad \forall\, s, t \in \mathbb{R}. \tag{3.7.18}$$

Multiplying on the right by e^{tA} and using (3.7.15) (with t replaced by $-t$) gives

$$e^{(s+t)A} = e^{sA}e^{tA}, \quad \forall\, s, t \in \mathbb{R}. \tag{3.7.19}$$

The following result generalizes (3.7.19).

Proposition 3.7.1. *Given $A, B \in M(n, \mathbb{F})$, we have*

$$e^{t(A+B)} = e^{tA}e^{tB}, \quad \forall\, t \in \mathbb{R}, \tag{3.7.20}$$

provided A and B commute, i.e.,

$$AB = BA. \tag{3.7.21}$$

Proof. This time we differentiate a triple product,

$$\begin{aligned}\frac{d}{dt}\big(e^{t(A+B)}e^{-tB}e^{-tA}\big) &= e^{t(A+B)}(A+B)e^{-tB}e^{-tA}\\ &\quad - e^{t(A+B)}Be^{-tB}e^{-tA}\\ &\quad - e^{t(A+B)}e^{-tB}Ae^{-tA}.\end{aligned} \tag{3.7.22}$$

Next, we note that, for $s \in \mathbb{R}$,

$$e^{sB}A = \sum_{k=0}^{\infty} \frac{s^k}{k!} B^k A = \sum_{k=0}^{\infty} \frac{s^k}{k!} AB^k, \tag{3.7.23}$$

provided A and B commute, so

$$AB = BA \Longrightarrow e^{sB}A = Ae^{sB}, \ \forall\, s \in \mathbb{R}. \tag{3.7.24}$$

Taking $s = -t$ allows us to push A to the left in the third term on the right side of (3.7.22), yielding 0. Hence the triple product is independent of t. Evaluating at $t = 0$ gives

$$e^{t(A+B)}e^{-tB}e^{-tA} = I, \quad \forall\, t \in \mathbb{R}. \tag{3.7.25}$$

provided (3.7.21) holds. Multiplying on the right first by e^{tA}, then by e^{tB}, using again (3.7.15), we obtain (3.7.20). □

Returning to (3.7.1), we have seen that solving this equation is equivalent to evaluating e^{tA}. Typically, one does not want to do this by computing the infinite series (3.7.9). We want to relate the evaluation of $e^{tA}v$ to results in linear algebra.

For example, if v is an eigenvector of A, with eigenvalue λ, then

$$\begin{aligned}Av = \lambda v &\Longrightarrow A^k v = \lambda^k v\\ &\Longrightarrow e^{tA}v = \sum_{k=0}^{\infty} \frac{t^k}{k!}\lambda^k v = e^{t\lambda}v.\end{aligned} \tag{3.7.26}$$

A related identity is that, if $C \in M(n, \mathbb{F})$ is invertible,

$$A = C^{-1}BC \Rightarrow A^k = C^{-1}B^kC \Rightarrow e^{tA} = C^{-1}e^{tB}C. \tag{3.7.27}$$

If B is diagonal,

$$\begin{aligned}B = \begin{pmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{pmatrix} &\Rightarrow B^k = \begin{pmatrix}\lambda_1^k & & \\ & \ddots & \\ & & \lambda_n^k\end{pmatrix}\\ &\Rightarrow e^{tB} = \begin{pmatrix}e^{t\lambda_1} & & \\ & \ddots & \\ & & e^{t\lambda_n}\end{pmatrix},\end{aligned} \tag{3.7.28}$$

which in conjunction with (3.7.27) gives

$$e^{tA} = C^{-1}\begin{pmatrix}e^{t\lambda_1} & & \\ & \ddots & \\ & & e^{t\lambda_n}\end{pmatrix}C, \tag{3.7.29}$$

if $A = C^{-1}BC$ with B as in (3.7.28), i.e., if A is diagonalizable.

As we know, not all matrices are diagonalizable. As discussed in §2.2, a vector $v \in \mathbb{C}^n$ is a generalized eigenvector of A, associated to $\lambda \in \mathbb{C}$, provided

$$(A - \lambda I)^\ell v = 0, \quad \text{for some } \ell \in \mathbb{N}, \tag{3.7.30}$$

the case $\ell = 1$ making v an eigenvector. When (3.7.30) holds, we can compute $e^{tA}v$ as follows. First

$$\begin{aligned} e^{tA}v &= e^{t(A-\lambda I)+t\lambda I}v \\ &= e^{t\lambda}e^{t(A-\lambda I)}v, \end{aligned} \tag{3.7.31}$$

the second identity via (3.7.20), with $A - \lambda I$ in place of A and λI in place of B, noting that the identity matrix $I \in M(n, \mathbb{C})$ commutes with every element of $M(n, \mathbb{C})$. Now the infinite series

$$e^{t(A-\lambda I)}v = \sum_{k=0}^{\infty} \frac{t^k}{k!}(A - \lambda I)^k v \tag{3.7.32}$$

terminates at $k = \ell - 1$, by (3.7.30), so we get

$$e^{tA}v = e^{t\lambda} \sum_{k=0}^{\ell-1} \frac{t^k}{k!}(A - \lambda I)^k v, \tag{3.7.33}$$

which has the form $e^{t\lambda}w(t)$, where $w(t)$ is a polynomial, of degree $\leq \ell$, with coefficients in $\mathbb{C}^n$. As shown in §2.2,

$$\begin{aligned} &\text{Given } A \in M(n, \mathbb{C}), \ \mathbb{C}^n \text{ has a basis} \\ &\text{consisting of generalized eigenvectors of } A. \end{aligned} \tag{3.7.34}$$

Let us summarize our analysis on how to evaluate a matrix exponential.

How to compute $e^{tA}v$.

1. Find a basis $\{v_1, \dots, v_n\}$ of $\mathbb{C}^n$, consisting of generalized eigenvectors of A.

2. Find $c_1, \dots, c_n \in \mathbb{C}$ such that $v = c_1v_1 + \cdots + c_nv_n$. Then

$$e^{tA}v = c_1e^{tA}v_1 + \cdots + c_ne^{tA}v_n. \tag{3.7.35}$$

3. Here is how to compute $e^{tA}v_j$.
A. If v_j is an eigenvector, say $Av_j = \lambda_j v_j$, then

$$e^{tA}v_j = e^{t\lambda_j}v_j. \tag{3.7.36}$$

B. If v_j is a generalized eigenvector, satisfying $(A - \lambda_j I)^\ell v_j = 0$, then

$$e^{tA}v_j = e^{t\lambda_j} \sum_{k=0}^{\ell-1} \frac{t^k}{k!}(A - \lambda_j I)^k v_j. \tag{3.7.37}$$

How to compute the $n \times n$ matrix e^{tA}.

The jth column of e^{tA} is $e^{tA}e_j$, where e_j is the jth standard basis vector of $\mathbb{C}^n$.

We work out a couple of examples.

Example 1. Take

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}. \tag{3.7.38}$$

Then $\operatorname{Spec} A = \{0, 1, 2\}$, and

$$\mathcal{E}(A, 0) = \operatorname{Span} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad \mathcal{E}(A, 1) = \operatorname{Span} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \mathcal{E}(A, 2) = \operatorname{Span} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}. \tag{3.7.39}$$

Hence

$$e^{tA} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad e^{tA} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = e^{t} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad e^{tA} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = e^{2t} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}. \tag{3.7.40}$$

Meanwhile,

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \tag{3.7.41}$$

hence

$$e^{tA} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + \frac{e^{2t}}{2} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad e^{tA} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \frac{e^{2t}}{2} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}. \tag{3.7.42}$$

From this and the second identity in (3.7.40), we have

$$e^{tA} = \begin{pmatrix} \frac{1}{2}(e^{2t} + 1) & 0 & \frac{1}{2}(e^{2t} - 1) \\ 0 & e^{t} & 0 \\ \frac{1}{2}(e^{2t} - 1) & 0 & \frac{1}{2}(e^{2t} + 1) \end{pmatrix}. \tag{3.7.43}$$

Example 2. Take

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & -1 \end{pmatrix}. \tag{3.7.44}$$

Then $\operatorname{Spec} A = \{0, 1\}$, and 0 is a double root of the characteristic polynomial of A. We have

$$\mathcal{E}(A, 1) = \operatorname{Span} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \mathcal{E}(A, 0) = \operatorname{Span} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \tag{3.7.45}$$

and, noting that

$$A^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \tag{3.7.46}$$

we have

$$\mathcal{GE}(A, 0) = \operatorname{Span}\Big\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \Big\}. \tag{3.7.47}$$

Hence

$$v \in \mathcal{GE}(A,0) \Rightarrow e^{tA}v = (I+tA)v = \begin{pmatrix} 1+t & 0 & t \\ 0 & 1+t & 0 \\ -t & 0 & 1-t \end{pmatrix} v. \tag{3.7.48}$$

It follows that

$$e^{tA} = \begin{pmatrix} 1+t & 0 & t \\ 0 & e^t & 0 \\ -t & 0 & 1-t \end{pmatrix}. \tag{3.7.49}$$

Returning to generalities, let us note from (3.7.34) that, for each $v \in \mathbb{C}^n$, $e^{tA}v$ is a linear combination of terms of the form (3.7.33), with different λs. We have the following.

Proposition 3.7.2. *Given $A \in M(n,\mathbb{C})$, $v \in \mathbb{C}^n$,*

$$e^{tA}v = \sum_j e^{\lambda_j t} v_j(t), \tag{3.7.50}$$

where $\{\lambda_j\}$ is the set of eigenvalues of A and $v_j(t)$ are $\mathbb{C}^n$-valued polynomials.

It is now our goal to turn this reasoning around. We intend to give a proof of Proposition 3.7.2 that does not depend on (3.7.34), and then use this result to provide a new proof of (3.7.34), via an argument very different from that used in §2.2.

Second proof of Proposition 3.7.2. To start, by (3.7.27) it suffices to show that e^{tB} has such a structure for some $B \in M(n,\mathbb{C})$ similar to A, i.e., satisfying $A = C^{-1}BC$ for some invertible $C \in M(n,\mathbb{C})$. We now bring in Schur's result, Proposition 3.5.1, which implies that A is similar to an upper triangular matrix. We recall that the proof of Proposition 3.5.1 is *very short*, and makes no use of concepts involving generalized eigenvectors. In view of this, we are reduced to proving Proposition 3.7.2 when A has the form

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & a_{22} & \cdots & a_{2n} \\ & & \ddots & \\ & & & a_{nn} \end{pmatrix}, \tag{3.7.51}$$

with all zeros below the diagonal. It follows from (1.5.55), with A replaced by $A - \lambda I$, that the eigenvalues of A are precisely the diagonal entries a_{jj}.

To proceed, set $x(t) = e^{tA}v$, solving

$$\frac{dx}{dt} = \begin{pmatrix} a_{11} & * & * \\ & \ddots & * \\ & & a_{nn} \end{pmatrix} x, \tag{3.7.52}$$

with $x(t) = (x_1(t), \dots, x_n(t))^t$. We can solve the last ODE for x_n, as it is just

$$\frac{dx_n}{dt} = a_{nn}x_n, \quad \text{so} \quad x_n(t) = Ce^{a_{nn}t}. \tag{3.7.53}$$

We can obtain $x_j(t)$ for $j < n$ inductively by solving inhomogeneous scalar differential equations

$$\frac{dx_j}{dt} = a_{jj}x_j + b_j(t), \tag{3.7.54}$$

where $b_j(t)$ is a linear combination of $x_{j+1}(t), \dots, x_n(t)$.

The equation (3.7.54) is a particularly easy sort, with solution given by

$$x_j(t) = e^{ta_{jj}}x_j(0) + e^{ta_{jj}} \int_0^t e^{-sa_{jj}} b_j(s)\, ds. \tag{3.7.55}$$

See Exercise 1 below. Given $x_n(t)$ in (3.7.53), $b_{n-1}(t)$ is a multiple of $e^{a_{nn}t}$. If $a_{n-1,n-1} \neq a_{nn}$, then $x_{n-1}(t)$ will be a linear combination of $e^{a_{nn}t}$ and $e^{a_{n-1,n-1}t}$, but if $a_{n-1,n-1} = a_{nn}$, $x_{n-1}(t)$ may be a linear combination of $e^{a_{nn}t}$ and $te^{a_{nn}t}$. Further integration will involve $\int p(t)e^{\alpha t}\, dt$, where $p(t)$ is a polynomial. That no other sort of function will arise is guaranteed by the following result.

Lemma 3.7.3. *If $p(t)$ is a polynomial of degree $\leq m$ and $\alpha \neq 0$, then*

$$\int p(t)e^{\alpha t}\, dt = q(t)e^{\alpha t} + C, \tag{3.7.56}$$

for some polynomial $q(t)$ of degree $\leq m$. (If $\alpha = 0$, one also gets (3.7.56)*, with $q(t)$ of degree $\leq m + 1$.)*

Proof. The map $p = Tq$ defined by

$$\frac{d}{dt}(q(t)e^{\alpha t}) = p(t)e^{\alpha t} \tag{3.7.57}$$

is a linear map on the $(m+1)$-dimensional vector space $\mathcal{P}_m$ of polynomials of degree $\leq m$. In fact, we have

$$Tq(t) = \alpha q(t) + q'(t). \tag{3.7.58}$$

It suffices to show that $T : \mathcal{P}_m \to \mathcal{P}_m$ is invertible, when $\alpha \neq 0$. But $D = d/dt$ is nilpotent on $\mathcal{P}_m$; $D^{m+1} = 0$. Hence

$$T^{-1} = \alpha^{-1}(I + \alpha^{-1}D)^{-1} = \alpha^{-1}(I - \alpha^{-1}D + \cdots + \alpha^{-m}(-D)^m). \tag{3.7.59}$$

This proves the lemma, and hence completes the proof of Proposition 3.7.2. □

Having Proposition 3.7.2, we proceed as follows. Given $\lambda \in \mathbb{C}$, let $\mathcal{V}_\lambda$ denote the space of $\mathbb{C}^n$-valued functions of the form $e^{\lambda t}v(t)$, where $v(t)$ is a $\mathbb{C}^n$-valued polynomial in t. Then $\mathcal{V}_\lambda$ is invariant under the action of both d/dt and A, hence of $d/dt - A$. Hence, if a sum $V_1(t) + \cdots + V_k(t)$, $V_j \in \mathcal{V}_{\lambda_j}$ (with λ_js distinct) is annihilated by $d/dt - A$, so is each term in this sum. (See Exercise 3 below.)

Therefore, if (3.7.5) is a sum over the distinct eigenvalues λ_j of A, it follows that each term $e^{\lambda_j t}v_j(t)$ is annihilated by $d/dt - A$, or, equivalently, is of the form $e^{tA}w_j$, where $w_j = v_j(0)$. This leads to the following conclusion.

Proposition 3.7.4. *Given $A \in M(n, \mathbb{C})$, $\lambda \in \mathbb{C}$, set*

$$G_\lambda = \{v \in \mathbb{C}^n : e^{tA}v = e^{t\lambda}v(t),\ v(t) \text{ polynomial}\}. \tag{3.7.60}$$

Then $\mathbb{C}^n$ has a direct sum decomposition

$$\mathbb{C}^n = G_{\lambda_1} \oplus \cdots \oplus G_{\lambda_k}, \tag{3.7.61}$$

where $\lambda_1, \dots, \lambda_k$ are the distinct eigenvalues of A. Furthermore, each G_{λ_j} is invariant under A, and

$$A_j = A\big|_{G_{\lambda_j}} \text{ has exactly one eigenvalue, } \lambda_j. \tag{3.7.62}$$

Proof. The decomposition (3.7.61) follows directly from Proposition 3.7.2. The invariance of G_{λ_j} under A is clear from the definition (3.7.60). It remains only to establish (3.7.62), and this holds because $e^{tA}v$ involves only the exponential $e^{\lambda_j t}$ when $v \in G_{\lambda_j}$. □

Having Proposition 3.7.4, we next claim that

$$\begin{aligned} G_{\lambda_j} &= \mathcal{GE}(A, \lambda_j) \\ &= \{v \in \mathbb{C}^n : (A - \lambda_j I)^k v = 0 \text{ for some } k \in \mathbb{N}\}, \end{aligned} \tag{3.7.63}$$

the latter identity defining the generalized eigenspace $\mathcal{GE}(A, \lambda_j)$, as in (2.2.3). The fact that

$$\mathcal{GE}(A, \lambda_j) \subset G_{\lambda_j} \tag{3.7.64}$$

follows from (3.7.33). Since $N_j = A_j - \lambda_j I \in \mathcal{L}(G_{\lambda_j})$ has only 0 as an eigenvalue, we are led to the following result.

Lemma 3.7.5. *Let W be a k-dimensional vector space over $\mathbb{C}$ and suppose $N : W \to W$ has only 0 as an eigenvalue. Then N is nilpotent, in fact*

$$N^m = 0 \text{ for some } m \leq k. \tag{3.7.65}$$

Proof. The assertion is equivalent to the implication (2.3.3) ⇒ (2.3.4), given in §2.3. We recall the argument. Let $W_j = N^j(W)$. Then $W \supset W_1 \supset W_2 \supset \cdots$ is a sequence of finite dimensional vector spaces, each invariant under N. This sequence must stabilize, so for some m, $N : W_m \to W_m$ bijectively. If $W_m \neq 0$, N has a nonzero eigenvalue. □

Lemma 3.7.5 provides the reverse inclusion to (3.7.64), and hence we have (3.7.63). Thus (3.7.61) yields the desired decomposition

$$\mathbb{C}^n = \mathcal{GE}(A, \lambda_1) \oplus \cdots \oplus \mathcal{GE}(A, \lambda_k) \tag{3.7.66}$$

of $\mathbb{C}^n$ as a direct sum of generalized eigenspaces of A. This provides another proof of Proposition 2.2.6.

Exponential and trigonometric functions

When material developed above on the exponential of an $n \times n$ matrix is specialized to $n = 1$, we have the exponential of a complex number,

$$e^z = \sum_{k=0}^{\infty} \frac{1}{k!} z^k, \quad z \in \mathbb{C}. \tag{3.7.67}$$

Then (3.7.10) specializes to

$$\frac{d}{dt} e^{at} = a e^{at}, \quad \forall\, t \in \mathbb{R}, a \in \mathbb{C}. \tag{3.7.68}$$

Here we want to study

$$\gamma(t) = e^{it}, \quad t \in \mathbb{R}, \tag{3.7.69}$$

which is a curve in the complex plane. We claim $\gamma(t)$ lies on the unit circle, i.e., $|\gamma(t)| \equiv 1$, where, for $z = x + iy,\ x, y \in \mathbb{R}$,

$$|z|^2 = x^2 + y^2 = z\,\overline{z}, \quad \text{with } \overline{z} = x - iy. \tag{3.7.70}$$

It follows from (3.7.67) that

$$e^{\overline{z}} = \overline{e^z}, \quad \forall\, z \in \mathbb{C}, \tag{3.7.71}$$

so, for $t \in \mathbb{R}$,

$$\overline{e^{it}} = e^{-it}, \quad \text{hence } |\gamma(t)|^2 = e^{it} e^{-it} \equiv 1. \tag{3.7.72}$$

Next, we consider the velocity

$$\gamma'(t) = i e^{it}. \tag{3.7.73}$$

From (3.7.70) it follows that, if also $w \in \mathbb{C}$, then $|zw|^2 = |z|^2 |w|^2$, so (3.7.73) yields

$$|\gamma'(t)|^2 = 1. \tag{3.7.74}$$

Thus $\gamma(t)$ is a unit speed curve on the unit circle, starting at $\gamma(0) = 1$, in the upward vertical direction $\gamma'(0) = i$. Thus the path from $t_0 = 0$ to t travels a distance

$$\ell(t) = \int_0^t |\gamma'(s)|\, ds = t, \tag{3.7.75}$$

for $t > 0$. Now the ray from the origin $0 \in \mathbb{C}$ to 1 meets the ray from 0 to $\gamma(t)$ at an angle which, measured in radians, is $\ell(t) = t$. See Figure 3.7.1

Having this geometrical information on the curve $\gamma(t)$, we bring in the basic trigonometric functions sine and cosine. By definition, if t is the angle between the two rays described above, and if we write $\gamma(t)$ in terms of its real and imaginary parts as $\gamma(t) = c(t) + i s(t)$, then

$$\cos t = c(t), \quad \sin t = s(t). \tag{3.7.76}$$

We have arrived at the important conclusion that

$$e^{it} = \cos t + i \sin t, \tag{3.7.77}$$

which is known as Euler's formula.

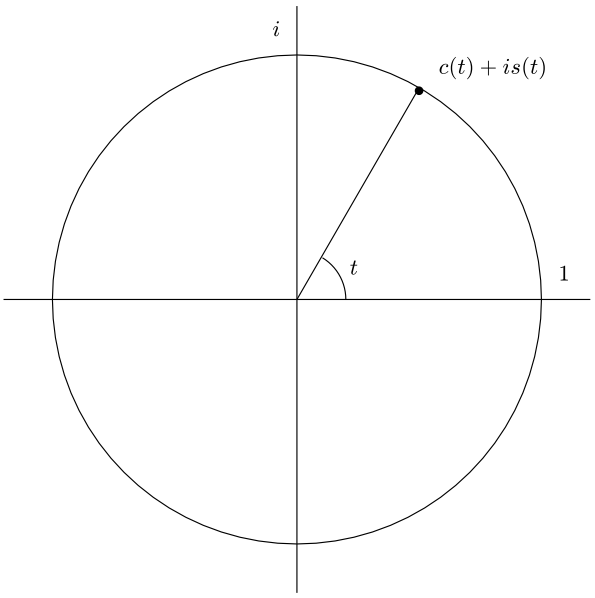

Figure 3.7.1. The circle $e^{it} = c(t) + is(t)$

Exercises

1. Given $A \in \mathbb{C},\ b : \mathbb{R} \to \mathbb{C}$ continuous, show that the solution to

$$\frac{dy}{dt} = Ay + b(t), \quad y(0) = y_0,$$

is given by the following, called Duhamel's formula:

$$y(t) = e^{At}y_0 + e^{At}\int_0^t e^{-As}b(s)\,ds.$$

Hint. Show that an equivalent differential equation for $z(t) = e^{-At}y(t)$ is

$$\frac{dz}{dt} = e^{-At}b(t), \quad z(0) = y_0.$$

2. Show that the result of Exercise 1 continues to hold in the setting

$$A \in M(n, \mathbb{C}), \quad y_0 \in \mathbb{C}^n, \quad b : \mathbb{R} \to \mathbb{C}^n,$$

and one solves for $y : \mathbb{R} \to \mathbb{C}^n$.

3. Suppose $v_j(t)$ are $\mathbb{C}^n$-valued polynomials, $\lambda_1, \dots, \lambda_k \in \mathbb{C}$ are distinct, and

$$e^{\lambda_1 t} v_1(t) + \cdots + e^{\lambda_k t} v_k(t) \equiv 0.$$

Show that $v_j(t) \equiv 0$ for each $j \in \{1, \dots, k\}$.

4. Examining the proof of Proposition 3.7.2, show that if $A \in M(n, \mathbb{C})$ is the upper triangular matrix (3.7.51), then

$$e^{tA} = \begin{pmatrix} e_{11}(t) & \cdots & e_{1n}(t) \\ & \ddots & \vdots \\ & & e_{nn}(t) \end{pmatrix}, \quad e_{jj}(t) = e^{t a_{jj}}.$$

4A. Here is another approach to the conclusion of Exercise 4. Suppose A and $B \in M(n, \mathbb{C})$ are upper triangular, with A as in (3.7.51) and B of a similar form, with a_{jk} replaced by b_{jk}. Show that $C = AB$ is upper triangular, with diagonal entries

$$c_{jj} = a_{jj} b_{jj}.$$

Deduce that, for $n \in \mathbb{N}$, A^n is upper triangular, with diagonal entries a_{jj}^n. Shoe that the conclusion of Exercise 4 follows from this.

5. Show that if $A \in M(n, \mathbb{C})$, then

$$\det e^{tA} = e^{t \operatorname{Tr} A}.$$

Hint. Show that this follows from Exercise 4 (or 4A) if A is upper triangular. Then show that it holds when A is similar to an upper triangular matrix.

6. Show that the identities

$$\frac{d}{dt} \cos t = -\sin t, \quad \frac{d}{dt} \sin t = \cos t$$

follow from (3.7.77) and (3.7.73).

7. Show that

$$J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \Longrightarrow e^{tJ} = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}.$$

Equivalently,

$$e^{tJ} = (\cos t) I + (\sin t) J.$$

Relate this to Euler's formula.

8. Show that

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Longrightarrow e^{tA} = \begin{pmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{pmatrix}.$$

9. Show that, for $A \in M(n, \mathbb{C})$,

$$e^{tA^*} = (e^{tA})^*, \quad \forall\, t \in \mathbb{R}.$$

Note that this generalizes (3.7.71).

10. Show that

$$A \in M(n,\mathbb{R}),\ A^* = -A \Longrightarrow e^{tA} \in SO(n),\ \forall\, t \in \mathbb{R},$$

and

$$A \in M(n,\mathbb{C}),\ A^* = -A \Longrightarrow e^{tA} \in U(n),\ \forall\, t \in \mathbb{R}.$$

Note that this generalizes (3.7.72).

11. Let $x : \mathbb{R} \to \mathbb{C}$ solve the nth order ODE

$$x^{(n)}(t) + a_{n-1}x^{(n-1)}(t) + \cdots + a_1 x'(t) + a_0 x(t) = 0.$$

Convert this to a first order $n \times n$ system for $y : \mathbb{R} \to \mathbb{C}^n$, with

$$y(t) = (y_0(t), \dots, y_{n-1}(t))^t, \quad y_j(t) = x^{(j)}(t).$$

Show that $y(t)$ solves

$$\frac{dy}{dt} = Ay,$$

where

$$A = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & & & & \\ 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix},$$

the *companion matrix* for the polynomial $p(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0$, introduced in (2.3.20).

REMARK. $x(t) = e^{\lambda t}$ solves the nth order ODE above if and only if $p(\lambda) = 0$, which, by Proposition 2.3.4, is equivalent to $\det(\lambda I - A) = 0$.

12. Let $B = \lambda_j I + N$ be a "Jordan block," as in (2.4.1). Assume $B \in M(k,\mathbb{C})$. Show that

$$e^{tB} = e^{\lambda_j t} \sum_{\ell=0}^{k-1} \frac{t^\ell}{\ell!} N^\ell.$$

13. If $p(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0$, and if λ_j is a root of $p(\lambda)$ of multiplicity k_j, show that the nth order ODE introduced in Exercise 11 has solutions

$$t^\ell e^{\lambda_j t}, \quad 0 \le \ell \le k_j - 1.$$

Deduce that the Jordan normal form for the companion matrix A to $p(\lambda)$, described in Exercise 11, has just one Jordan block of the form (2.4.1), and it is a $k_j \times k_j$ matrix.

14. Establish the following converse to Proposition 3.7.1.

Proposition 3.7.6. *Given $A, B \in M(n,\mathbb{C})$,*

$$e^{t(A+B)} = e^{tA}e^{tB} \ \ \forall\, t \in \mathbb{R} \Longrightarrow AB = BA.$$

Hint. Apply d/dt to both sides and deduce that the hypothesis implies

$$(A+B)e^{t(A+B)} = Ae^{tA}e^{tB} + e^{tA}Be^{tB}, \quad \forall\, t \in \mathbb{R}.$$

Replacing $e^{t(A+B)}$ by $e^{tA}e^{tB}$ on the left, deduce that

$$Be^{tA} = e^{tA}B, \quad \forall\, t \in \mathbb{R}.$$

Apply d/dt again, and set $t = 0$.

15. Take the following route to proving (3.7.24). Set

$$Z(s) = e^{sB}Ae^{-sB}.$$

Show that

$$\begin{aligned} AB = BA &\Longrightarrow Z'(s) \equiv 0 \\ &\Longrightarrow Z(s) \equiv A. \end{aligned}$$

Deduce (3.7.24) from this (avoiding (3.7.23)).

16. Compute e^{tA}, e^{tB}, and e^{tC} in the following cases.

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 2 \end{pmatrix}.$$

3.8. The discrete Fourier transform

Here we look at a number of important linear transformations that arise on the space of functions $f : \mathbb{Z} \to \mathbb{C}$ that are periodic, say of period n. It is convenient to re-cast this function space as follows. We form

$$\mathbb{Z}/(n), \tag{3.8.1}$$

the set of equivalence classes of integers, "mod n," where the equivalence relation is

$$j \sim j' \Longleftrightarrow \frac{j - j'}{n} \in \mathbb{Z}. \tag{3.8.2}$$

Note that each integer $j \in \mathbb{Z}$ is equivalent to exactly one element of the set $\{0, 1, \dots, n-1\}$. We then form the vector space

$$\ell^2(\mathbb{Z}/(n)) = \text{ set of functions } f : \mathbb{Z}/(n) \to \mathbb{C}, \tag{3.8.3}$$

which we endow with the inner product

$$\begin{aligned}(f, g) &= \frac{1}{n} \sum_{k \in \mathbb{Z}/(n)} f(k)\overline{g(k)} \\ &= \frac{1}{n} \sum_{k=0}^{n-1} f(k)\overline{g(k)}.\end{aligned} \tag{3.8.4}$$

This is a complex inner product space. We will also be interested in the real vector space,

$$\ell^2_{\mathbb{R}}(\mathbb{Z}/(n)) = \text{ set of functions } f : \mathbb{Z}/(n) \to \mathbb{R}, \tag{3.8.5}$$

with the same sort of inner product.

Special operators on these spaces arise from the fact that addition is well defined on $\mathbb{Z}/(n)$:

$$j, k \in \mathbb{Z}/(n) \Longrightarrow j + k \in \mathbb{Z}/(n), \tag{3.8.6}$$

which follows from the observation that

$$j \sim j',\ k \sim k' \Longrightarrow j + k \sim j' + k'. \tag{3.8.7}$$

In particular, we have the *translation operator*

$$Tf(k) = f(k + 1), \tag{3.8.8}$$

acting as a unitary operator on $\ell^2(\mathbb{Z}/(n))$, and as an orthogonal operator on $\ell^2_{\mathbb{R}}(z/(n))$. Thus $\ell^2(\mathbb{Z}/(n))$ has an orthonormal basis of eigenvectors for T, which we proceed to find.

Note that

$$T^n = I, \tag{3.8.9}$$

so each eigenvalue of T is an element of

$$\{\omega^j : 0 \le j \le n-1\}, \quad \text{where } \omega = e^{2\pi i/n}. \tag{3.8.10}$$

Note that an element $e_j \in \ell^2(\mathbb{Z}/(n))$ is an ω^j-eigenvector if and only if

$$e_j(k) = T^k e_j(0) = \omega^{jk} e_j(0), \tag{3.8.11}$$

so setting $e_j(0) = 1$ gives

$$e_j(k) = \omega^{jk}. \tag{3.8.12}$$

We have

$$e_j \in \mathcal{E}(T, \omega^j), \quad \|e_j\|^2 = \frac{1}{n}\sum_{k=0}^{n-1} |\omega^{jk}|^2 = 1, \tag{3.8.13}$$

so our desired orthonormal basis of eigenvectors of T is

$$\{e_j : 0 \le j \le n-1\}. \tag{3.8.14}$$

Note that

$$j \sim j' \Longrightarrow \omega^j = \omega^{j'}, \tag{3.8.15}$$

so we can also write this set as

$$\{e_j : j \in \mathbb{Z}/(n)\}. \tag{3.8.16}$$

As a direct check on orthogonality, note that

$$(e_j, e_\ell) = \frac{1}{n}\sum_{k\in\mathbb{Z}/(n)} \omega^{(j-\ell)k}, \tag{3.8.17}$$

and

$$\begin{aligned} \omega^m \sum_{k\in\mathbb{Z}/(n)} \omega^{mk} &= \sum_{k\in\mathbb{Z}/(n)} \omega^{m(k+1)} \\ &= \sum_{k\in\mathbb{Z}/(n)} \omega^{mk}, \end{aligned} \tag{3.8.18}$$

since $k+1$ runs once over $\mathbb{Z}/(n)$ when k does. We see that $\omega^m \neq 1$ implies this sum vanishes, hence if $j \neq \ell$ in $\mathbb{Z}/(n)$, then the inner product (3.8.17) vanishes.

Using the orthonormal basis (3.8.16), we can write each $f \in \ell^2(\mathbb{Z}/(n))$ as

$$f = \sum_{j\in\mathbb{Z}/(n)} \hat{f}(j) e_j, \tag{3.8.19}$$

where

$$\hat{f}(j) = (f, e_j) = \frac{1}{n}\sum_{\ell\in\mathbb{Z}/(n)} f(\ell)\omega^{-j\ell}. \tag{3.8.20}$$

Thus, for $k \in \mathbb{Z}/(n)$,

$$f(k) = \sum_{\ell\in\mathbb{Z}/(n)} \hat{f}(j)\omega^{jk}. \tag{3.8.21}$$

This yields the *discrete Fourier transform* (or DFT)

$$\mathcal{F} : \ell^2(\mathbb{Z}/(n)) \longrightarrow \ell^2(\mathbb{Z}/(n)), \tag{3.8.22}$$

as

$$\mathcal{F}f(k) = \hat{f}(k). \tag{3.8.23}$$

By orthonormality of the basis $\{e_j\}$, we have

$$\|f\|^2 = \sum_{j\in\mathbb{Z}/(n)} |\hat{f}(j)|^2, \tag{3.8.24}$$

hence

$$\|\mathcal{F}f\|^2 = \frac{1}{n}\|f\|^2, \tag{3.8.25}$$

i.e., $n^{1/2}\mathcal{F}$ is a unitary operator on $\ell^2(\mathbb{Z}/(n))$. The identity (3.8.21), which we call the discrete Fourier inversion formula, is equivalent to

$$\mathcal{F}^{-1} = n\mathcal{F}^*. \tag{3.8.26}$$

Another important operation on functions on $\mathbb{Z}/(n)$ is the *convolution*, defined by

$$f * g(k) = \frac{1}{n}\sum_{\ell\in\mathbb{Z}/(n)} f(\ell)g(k-\ell). \tag{3.8.27}$$

We can compute the Fourier transform of $f * g$ as follows:

$$\begin{aligned}\widehat{f * g}(j) &= \frac{1}{n}\sum_k (f * g)(k)\omega^{-jk} \\ &= \frac{1}{n^2}\sum_{k,\ell} f(\ell)g(k-\ell)\omega^{-jk} \\ &= \frac{1}{n^2}\sum_{k,\ell} f(\ell)\omega^{-j\ell}g(k-\ell)\omega^{-j(k-\ell)},\end{aligned} \tag{3.8.28}$$

and deduce that

$$\widehat{f * g}(j) = \hat{f}(j)\hat{g}(j). \tag{3.8.29}$$

One consequence is that

$$\begin{aligned}\|f * g\|^2 &= \sum_j |\widehat{f * g}(j)|^2 \\ &= \sum_j |\hat{f}(j)\hat{g}(j)|^2,\end{aligned} \tag{3.8.30}$$

which implies

$$\|f * g\| \leq \Big(\max_j |\hat{f}(j)|\Big)\|g\|. \tag{3.8.31}$$

The convolution product on functions on $\mathbb{Z}/(n)$ has many applications to problems in differential equations, in concert with the process of discretization. We refer to Chapter 3 of [**12**] for a discussion of this. Here we look as another application, involving multiplying polynomials. Say you have two polynomials of degree $m-1$,

$$p(z) = \sum_{j=0}^{m-1} a_j z^j, \quad q(z) = \sum_{j=0}^{m-1} b_j z^j. \tag{3.8.32}$$

Then

$$\begin{aligned} p(z)q(z) &= \sum_{j,\ell=0}^{m-1} a_j b_\ell z^{j+\ell} \\ &= \sum_{k=0}^{2m-2} \sum_{j=0}^{m-1} a_j b_{k-j} z^k. \end{aligned} \tag{3.8.33}$$

Here we take $n = 2m$ and regard $a(j) = a_j$ and $b(j) = b_j$ as functions on $\mathbb{Z}/(n)$ that vanish outside $\{0, \dots, m-1\}$. Then

$$p(z)q(z) = n \sum_{k=0}^{n-2} (a * b)(k)\, z^k, \tag{3.8.34}$$

where $a * b$ is the convolution of two functions on $\mathbb{Z}/(n)$. Since $\mathcal{F} : \ell^2(\mathbb{Z}/(n)) \to \ell^2(\mathbb{Z}/(n))$ gives

$$\mathcal{F}(a * b) = (\mathcal{F}a)(\mathcal{F}b), \tag{3.8.35}$$

we have

$$\begin{aligned} a * b &= \mathcal{F}^{-1}\big((\mathcal{F}a)(\mathcal{F}b)\big) \\ &= n\mathcal{F}^*\big((\mathcal{F}a)(\mathcal{F}b)\big). \end{aligned} \tag{3.8.36}$$

A straightforward calculation of $a * b$ involves approximately m^2 multiplications and a comparable number of additions. If $m = 1000$, this adds up. If one has in hand $\mathcal{F}a$ and $\mathcal{F}b$, forming the product $(\mathcal{F}a)(\mathcal{F}b)$ as a function on $\mathbb{Z}/(n)$ takes just n multiplications. This leaves one with the problem of how many operations it takes to compute $\mathcal{F}f$, for $f \in \ell^2(\mathbb{Z}/(n))$. There is a "fast" way of doing this, which we take up shortly.

First we mention an application of (3.8.34)–(3.8.26) to the "fast multiplication" of large integers. Suppose p and q are 1024-digit integers:

$$p = \sum_{j=0}^{m-1} a_j 10^j, \quad q = \sum_{j=0}^{m-1} b_j 10^j, \quad m = 2^{10}, \quad 0 \le a_j, b_j \le 9. \tag{3.8.37}$$

Then (3.8.34) gives

$$pq = n \sum_{k=0}^{2046} (a * b)(k)\, 10^k, \quad n = 2^{11}, \tag{3.8.38}$$

with $a * b$ given by convolution on $\mathbb{Z}/(n)$, $n = 2^{11}$, satisfying (3.8.36). The FFT described below leads to an efficient evaluation of $a * b$ on $\mathbb{Z}/(2^{11})$. This does not quite give the decimal representation of pq as a 2048-digit integer, since we only know that

$$0 \le n(a * b)(k) < 100 \cdot 2^{11}. \tag{3.8.39}$$

However, a straightforward process of "carrying" yields from (3.8.38) a representation

$$pq = \sum_{k=0}^{n-1} c_k 10^k, \quad 0 \le c_k \le 9, \quad n = 2^{11}. \tag{3.8.40}$$

The Fast Fourier Transform

We turn to the issue of providing an efficient evaluation of the Fourier transform of a function f on $\mathbb{Z}/(n)$, which, recall, is given by

$$\hat{f}(j) = \frac{1}{n} \sum_{\ell \in \mathbb{Z}/(n)} f(\ell)\omega^{-j\ell}, \quad \omega = e^{2\pi i/n}. \tag{3.8.41}$$

For each fixed j, computing the right side of (3.8.41) involves $n-1$ additions and n multiplications of complex numbers, plus n integer products $j\ell = m$ and loooking up ω^{-m} and $f(\ell)$. If the computations for varying j are done independently, the total effort to compute $\mathcal{F}f$ involves n^2 multiplications and $n(n-1)$ additions of complex numbers, plus some further operations. The *Fast Fourier Transform* (or FFT) is a method for computing $\mathcal{F}f$ in $Cn(\log n)$ steps, when n is a power of 2.

The possibility of doing this arises from observing redundancies in the calculation of the Fourier coefficients $\hat{f}(j)$. To illustrate this in the case of functions on $\mathbb{Z}/(4)$, we write

$$\begin{aligned} 4\hat{f}(0) &= [f(0) + f(2)] + [f(1) + f(3)], \\ 4\hat{f}(2) &= [f(0) + f(2)] - [f(1) + f(2)], \end{aligned} \tag{3.8.42}$$

and

$$\begin{aligned} 4\hat{f}(1) &= [f(0) - f(2)] - i[f(1) - f(3)], \\ 4\hat{f}(3) &= [f(0) - f(2)] + i[f(1) - f(3)]. \end{aligned} \tag{3.8.43}$$

Note that each term in square brackets appears twice. Furthermore, (3.8.42) gives the Fourier coefficients of a function on $\mathbb{Z}/(2)$. In fact, if

$$f_0(0) = f(0) + f(1), \quad f_0(1) = f(1) + f(3), \tag{3.8.44}$$

then

$$2\hat{f}(2j) = \hat{f}_0(j), \quad \text{for } \ j = 0 \text{ or } 1. \tag{3.8.45}$$

Similarly, if we set

$$f_1(0) = f(0) - f(2), \quad f_1(1) = -i[f(1) - f(3)], \tag{3.8.46}$$

then

$$2\hat{f}(2j+1) = \hat{f}_1(j), \quad \text{for } \ j = 0 \text{ or } 1. \tag{3.8.47}$$

This phenomenon is a special case of a more general result, which leads to a fast inductive procedure for evaluating $\mathcal{F}f$.

To proceed, assume $n = 2^k$, and set

$$G_k = \mathbb{Z}/(n), \quad n = 2^k. \tag{3.8.48}$$

Given $f : G_k \to \mathbb{C}$, define the functions

$$f_0, f_1 : G_{k-1} \longrightarrow \mathbb{C} \tag{3.8.49}$$

by

$$f_0(\ell) = f(\ell) + f(\ell + n/2), \tag{3.8.50}$$

$$f_1(\ell) = \omega^{-\ell}[f(\ell) - f(\ell + n/2)], \quad \omega = e^{2\pi i/n}. \tag{3.8.51}$$

Note that the factor $\omega^{-\ell}$ in (3.8.51) makes $f_1(\ell)$ well defined for $\ell \in G_{k-1}$, i.e., the right side of (3.8.51) is unchanged if ℓ is replaced by $\ell + n/2$. In other words,

$$f \in \ell^2(G_k) \text{ yields } f_0, f_1 \in \ell^2(G_{k-1}), \tag{3.8.52}$$

hence

$$\mathcal{F}f \in \ell^2(G_k), \text{ and } \mathcal{F}f_0,\ \mathcal{F}f_1 \in \ell^2(G_{k-1}). \tag{3.8.53}$$

The following result extends (3.8.42)–(3.8.43).

Proposition 3.8.1. *Given $f \in \ell^2(G_k)$, we have the following identities relating the Fourier transforms of f_0, f_1, and f:*

$$2\hat{f}(2j) = \hat{f}_0(j), \tag{3.8.54}$$

and

$$2\hat{f}(2j+1) = \hat{f}_1(j), \tag{3.8.55}$$

for $j \in \{0, 1, \dots, 2^{k-1} - 1\}$.

Proof. Note that $\hat{f}_0(j)$ and $\hat{f}_1(j)$ are given by a formula parallel to (3.8.41), with $\mathbb{Z}/(n) = G_k$ replaced by G_{k-1} and ω replaced by ω^2. Hence

$$\begin{aligned} n\hat{f}(2j) &= \sum_{\ell=0}^{2^k-1} f(\ell)\omega^{-2j\ell} \\ &= \sum_{\ell=0}^{2^{k-1}-1} [f(\ell) + f(\ell + 2^{k-1})](\omega^2)^{-j\ell}, \end{aligned} \tag{3.8.56}$$

giving (3.8.54). Next, since $\omega^{n/2} = -1$,

$$\begin{aligned} n\hat{f}(2j+1) &= \sum_{\ell=0}^{2^k-1} f(\ell)\omega^{-\ell}\omega^{-2j\ell} \\ &= \sum_{\ell=0}^{2^{k-1}-1} \omega^{-\ell}[f(\ell) - f(\ell + 2^{k-1})]\omega^{-2j\ell}, \end{aligned} \tag{3.8.57}$$

giving (3.8.55). □

Thus the problem of computing $\mathcal{F}f$, given $f \in \ell^2(G_k)$, is transformed after $n/2$ multiplications and n additions of complex numbers in (3.8.50)–(3.8.51) to the problem of computing the Fourier transforms of *two* functions on G_{k-1}. After $n/4$ new new multiplications and $n/2$ new additions for each of these functions f_0 and f_1, i.e., after an additional total of $n/2$ new multiplications and n additions, this is reduced to the problem of computing *four* Fourier transforms of functions on G_{k-2}. After k iterations, we obtain $2^k = n$ functions on $G_0 = \mathbb{Z}/(1) = \{0\}$, at which point we have the Fourier coefficients of f. Doing this takes

$$kn = (\log_2 n)n \text{ additions and } \tfrac{1}{2}kn = \tfrac{1}{2}(\log_2 n)n \text{ multiplications}$$

of complex numbers, plus a comparable number of integer operations and fetching from memory values of given or previously computed functions.

To describe explicitly this inductive procedure, it is convenient to bring in some notation. To each $j \in \mathbb{Z}/(n),\ n = 2^k$, we assign the unique k-tuple

$$J = (J_1, J_2, \dots, J_k) \tag{3.8.58}$$

of elements of $\{0, 1\}$ such that

$$J_1 + J_2 \cdot 2 + \cdots + J_k \cdot 2^{k-1} = j \bmod n, \tag{3.8.59}$$

and set

$$f^{\#}(J) = \hat{f}(j). \tag{3.8.60}$$

Then the formulas (3.8.54)–(3.8.55) state that

$$\begin{aligned} 2f^{\#}(0, J_2, \dots, J_k) &= f_0^{\#}(J_2, \dots, J_k), \\ 2f^{\#}(1, J_2, \dots, J_k) &= f_1^{\#}(J_2, \dots, J_k). \end{aligned} \tag{3.8.61}$$

The inductive procedure described above gives, from f_0 and f_1, defined on G_{k-1}, the functions

$$f_{00} = (f_0)_0, \quad f_{01} = (f_0)_1, \quad f_{10} = (f_1)_0, \quad f_{11} = (f_1)_1, \tag{3.8.62}$$

defined on G_{k-2}, and so forth. We see from (3.8.60)–(3.8.61) that

$$\hat{f}(j) = \frac{1}{n} f_J^{\#}(0) = \frac{1}{n} f_J(0). \tag{3.8.63}$$

From (3.8.50)–(3.8.51) we have an inductive formula for

$$f_{J_1 \cdots J_m J_{m+1}} : G_{k-m-1} \longrightarrow \mathbb{C}, \tag{3.8.64}$$

given by

$$\begin{aligned} f_{J_1 \cdots J_m 0}(\ell) &= f_{J_1 \cdots J_m}(\ell) + f_{J_1 \cdots J_m}(\ell + 2^{k-m-1}), \\ f_{J_1 \cdots J_m 1}(\ell) &= \omega_m^{-\ell} \big[f_{J_1 \cdots J_m}(\ell) - f_{J_1 \cdots J_m}(\ell + 2^{k-m-1}) \big], \end{aligned} \tag{3.8.65}$$

where ω_m is defined by $\omega_0 = \omega = e^{2\pi i/n}\ (n = 2^k),\ \omega_{m-1} = \omega_m^2$, i.e.,

$$\omega_m = \omega^{2^m}. \tag{3.8.66}$$

For the purpose of implementing this procedure in a computer program, it is perhaps easier to work with integers j than with m-tuples $(J_1, \dots, J_m)$. Therefore, let us set

$$F_m(j + 2^m \ell) = f_{J_1 \cdots J_m}(\ell), \tag{3.8.67}$$

where

$$j = J_1 + J_2 \cdot 2 + \cdots + J_m \cdot 2^{m-1} \in \{0, 1, \dots, 2^m - 1\}, \tag{3.8.68}$$

and

$$\ell \in \{0, 1, \dots, 2^{k-m} - 1\}. \tag{3.8.69}$$

This defines F_m on $\{0, 1, \dots, 2^k - 1\}$. For $m = 0$, we have

$$F_0(\ell) = f(\ell), \quad 0 \le \ell \le 2^k - 1. \tag{3.8.70}$$

The iterative formulas in (3.8.65) translate to

$$\begin{aligned} F_{m+1}(j+2^{m+1}\ell) &= F_m(j+2^m\ell) + F_m(j+2^m\ell+2^{k-1}),\\ F_{m+1}(j+2^m+2^{m+1}\ell) &= \omega_m^{-\ell}\big[F_m(j+2^m\ell) - F_m(j+2^m\ell+2^{k-1})\big], \end{aligned} \tag{3.8.71}$$

for

$$0 \le \ell \le 2^{k-m-1}-1, \quad 0 \le j \le 2^m - 1. \tag{3.8.72}$$

The formula (3.8.63) for $\hat{f}$ becomes

$$\hat{f}(j) = \frac{1}{n} F_k(j), \quad 0 \le j \le 2^k - 1. \tag{3.8.73}$$

Real DFT

We can construct an orthonormal basis for $\ell^2_{\mathbb{R}}(\mathbb{Z}/(n))$ by taking the real and imaginary parts of the elements $e_j \in \ell^2(\mathbb{Z}/(n))$. Let us set

$$e_j = c_j + is_j, \tag{3.8.74}$$

where

$$\begin{aligned} c_j(k) &= \operatorname{Re} e^{2\pi ijk/n} = \cos\frac{2\pi}{n}jk,\\ s_j(k) &= \operatorname{Im} e^{2\pi ijk/n} = \sin\frac{2\pi}{n}jk. \end{aligned} \tag{3.8.75}$$

Note that $s_0 \equiv 0$ and, if n is even $s_{n/2} \equiv 0$. Otherwise, since $Te_j = \omega^j e_j$ and $\omega^j \neq \omega^{-j}$, $e_j \perp e_{-j}$ in $\ell^2(\mathbb{Z}/(n))$, so

$$\begin{aligned} 0 &= (c_j + is_j, c_j - is_j)\\ &= \|c_j\|^2 - \|s_j\|^2 + 2i(c_j, s_j), \end{aligned} \tag{3.8.76}$$

and we have

$$\|c_j\|^2 = \|s_j\|^2 = \frac{1}{2}, \quad c_j \perp s_j, \quad \text{for } \ 0 < j < \frac{n}{2}. \tag{3.8.77}$$

If also $0 < k < n/2$ and $j \neq k$, we have e_j orthogonal to e_k and to e_{-k}, hence to c_k and to s_k. This yields the following.

Proposition 3.8.2. *An orthonormal basis of $\ell^2_{\mathbb{R}}(\mathbb{Z}/(n))$ is given by the following set of vectors:*

$$e_0 \equiv 1, \quad \sqrt{2}c_j,\ \sqrt{2}s_j, \quad 1 \le j < \frac{n}{2}, \tag{3.8.78}$$

together with

$$e_{n/2}, \tag{3.8.79}$$

if n is even.

Note that, if n is even

$$e_{n/2}(k) = e^{2\pi ik(n/2)/n} = e^{\pi ik} = (-1)^k. \tag{3.8.80}$$

Computations such as done in Proposition 3.4.4 exhibit the behavior of T on this basis. Let us set

$$\begin{aligned}\omega^j &= \alpha_j + \beta_j \\ &= \cos\frac{2\pi}{n}j + i\sin\frac{2\pi}{n}j.\end{aligned} \tag{3.8.81}$$

Then the identity $Te_j = \omega^j e_j$ yields

$$Tc_j + iTs_j = (\alpha_j + i\beta_j)(c_j + is_j), \tag{3.8.82}$$

hence

$$\begin{aligned}Tc_j &= \alpha_j c_j - \beta_j s_j, \\ Ts_j &= \beta_j c_j + \alpha_j s_j,\end{aligned} \tag{3.8.83}$$

a set of identities completed by

$$Te_0 = e_0, \tag{3.8.84}$$

and, if n is even,

$$Te_{n/2} = -e_{n/2}. \tag{3.8.85}$$

We now take the Fourier transform $\mathcal{F}$ on $\ell^2(\mathbb{Z}/(n))$ and produce a pair of transforms

$$\mathcal{F}_c,\, \mathcal{F}_s : \ell^2_{\mathbb{R}}(\mathbb{Z}/(n)) \longrightarrow \ell^2_{\mathbb{R}}(\mathbb{Z}/(n)), \tag{3.8.86}$$

as follows. If f is real valued, we split $\hat{f}(j)$ into its real and imaginary parts,

$$\hat{f}(j) = \hat{f}_c(j) + i\hat{f}_s(j), \tag{3.8.87}$$

where

$$\begin{aligned}\hat{f}_c(j) &= (f, c_j) = \frac{1}{n}\sum_{k\in\mathbb{Z}/(n)} f(k)\cos\frac{2\pi}{n}jk, \\ \hat{f}_s(j) &= -(f, s_j) = -\frac{1}{n}\sum_{k\in\mathbb{Z}/(n)} f(k)\sin\frac{2\pi}{n}jk.\end{aligned} \tag{3.8.88}$$

Note that

$$f \text{ real } \Longrightarrow \hat{f}(-j) = \overline{\hat{f}(j)}, \tag{3.8.89}$$

so, as in Proposition 3.8.2, we use (3.8.87)–(3.8.88) for $1 \le j < n/2$. We also have

$$\hat{f}_c(0) = (f, e_0) = \frac{1}{n}\sum_{k\in\mathbb{Z}/(n)} f(k), \tag{3.8.90}$$

and, if n is even,

$$\hat{f}_c\Big(\frac{n}{2}\Big) = (f, e_{n/2}) = \frac{1}{n}\sum_{k\in\mathbb{Z}/(n)} (-1)^k f(k). \tag{3.8.91}$$

We set $\hat{f}_s(j) = 0$ for $j = 0$ and (if n is even) for $j = n/2$. Then $\mathcal{F}_c$ and $\mathcal{F}_s$ in (3.8.86) are defined by

$$\mathcal{F}_c f(j) = \hat{f}_c(j), \quad \mathcal{F}_s f(j) = \hat{f}_s(j). \tag{3.8.92}$$

In light of Proposition 3.8.2, we have

$$\|f\|^2 = |\hat{f}_c(0)|^2 + 2 \sum_{1 \le j < n/2} \Big\{ |\hat{f}_c(j)|^2 + \hat{f}_s(j)|^2 \Big\}, \tag{3.8.93}$$

plus $|\hat{f}_c(n/2)|^2$ if n is even.

We next examine how the convolution operator C_f, given by

$$C_f g = f * g, \tag{3.8.94}$$

behaves on the basis (3.8.78)–(3.8.79), when f is real valued. This follows from the readily established identity

$$C_f e_j = \hat{f}(j) e_j, \tag{3.8.95}$$

valid for complex valued f (and essentially equivalent to (3.8.29)). Writing e_j as in (3.8.74) and $\hat{f}(j)$ as in (3.8.87), we have

$$C_f c_j + i C_f s_j = (\hat{f}_c(j) + i \hat{f}_s(j))(c_j + i s_j), \tag{3.8.96}$$

hence

$$\begin{aligned} C_f c_j &= \hat{f}_c(j) c_j - \hat{f}_s(j) s_j, \\ C_f s_j &= \hat{f}_s(j) c_j + \hat{f}_c(j) s_j. \end{aligned} \tag{3.8.97}$$

Exercises

1. Define $\delta_j \in \ell^2(\mathbb{Z}/(n))$ by

$$\delta_j(k) = 1, \quad \text{if } j = k \text{ in } \mathbb{Z}/(n),$$
$$0, \quad \text{otherwise.}$$

Show that, for all $g \in \ell^2(\mathbb{Z}/(n))$,

$$g = \sum_j g(j)\delta_j = \sum_j g(j)T^{-j}\delta_0.$$

2. Show that

$$f * g = g * f = \sum_j g(j)T^{-j}f.$$

3. Given $C_f g = f * g$, show that C_f commutes with T.

4. Assume $S : \ell^2(\mathbb{Z}/(n)) \to \ell^2(\mathbb{Z}/(n))$ commutes with T. Show that

$$Sg = C_f g, \quad \text{for} \quad f = S\delta_0.$$

5. Given $f, g \in \ell^2_{\mathbb{R}}(\mathbb{Z}/(n))$, show that

$$\mathcal{F}_c(f * g)(j) = \hat{f}_c(j)\hat{g}_c(j) - \hat{f}_s(j)\hat{g}_s(j),$$
$$\mathcal{F}_s(f * g)(j) = \hat{f}_c(j)\hat{g}_s(j) + \hat{f}_s(j)\hat{g}_c(j).$$

Hint. Use $\mathcal{F}(f * g)(j) = \hat{f}(j)\hat{g}(j)$, together with

$$\hat{f}(j) = \hat{f}_c(j) + i\hat{f}_s(j),$$

etc.

In exercises below, we define multiplication operators M_u on $\ell^2(\mathbb{Z}/(n))$ by

$$M_u f(k) = u(k)f(k).$$

6. Show that

$$\mathcal{F}C_f = M_{\hat{f}}\mathcal{F}, \quad \mathcal{F}T = M_{e_1}\mathcal{F},$$

where $e_1(j) = \omega^j$. These identities are called *intertwining relations.*

7. Define forward and backward difference operator on $\ell^2(\mathbb{Z}/(n))$ by

$$\partial_+ f(k) = f(k+1) - f(k), \quad \partial_- f(k) = f(k) - f(k-1).$$

Show that

$$\partial_+ = T - I, \quad \partial_- = I - T^{-1}, \quad \partial_+^* = -\partial_-,$$

and that

$$\mathcal{F}\partial_+ = M_{e_1-1}\mathcal{F}, \quad \mathcal{F}\partial_- = M_{1-\overline{e}_1}\mathcal{F}.$$

8. Set

$$\Delta = \partial_+ \partial_-.$$

Show that

$$\Delta = T - 2I + T^{-1},$$

and

$$\mathcal{F}\Delta = -M_{|\xi|^2}\mathcal{F},$$

where

$$\xi(j) = \omega^j - 1, \quad |\xi(j)|^2 = 2\Big(1 - \cos\frac{2\pi}{n}j\Big).$$

9. Define $\mathcal{J}$ on $\ell^2(\mathbb{Z}/(n))$ by

$$\mathcal{J}f(k) = f(-k).$$

Show that

$$\mathcal{F}^* = \mathcal{J}\mathcal{F} = \mathcal{F}\mathcal{J},$$

and deduce via (3.8.26) that

$$\mathcal{F}^2 = n^{-1}\mathcal{J}.$$

10. Define the *unitary* operator Φ on $\ell^2(\mathbb{Z}/(n))$ by

$$\Phi = n^{1/2}\mathcal{F}.$$

Show that the various intertwining relations in Exercises 6–8 hold with $\mathcal{F}$ replaced by Φ, and that

$$\Phi^2 = \mathcal{J}, \quad \Phi^4 = I.$$

11. Show that

$$\Delta = -\Phi^{-1}M_{|\xi|^2}\Phi.$$

12. Let

$$H = -\Delta + M_{|\xi|^2}.$$

Show that

$$\Phi H \Phi^{-1} = H.$$

Hint. Reduce this to showing that

$$\Phi^2 M_{|\xi|^2} = M_{|\xi|^2}\Phi^2,$$

i.e., $\mathcal{J}M_{|\xi|^2} = M_{|\xi|^2}\mathcal{J}$.

Chapter 4

Further basic concepts: duality, convexity, positivity

This chapter takes up four topics that are basic to linear algebra at the level we have reached so far. Two of them, duality and quotient spaces, will play an important role in the next chapter. The other two, convexity and positivity, are presented for their intrinsic interest, with pointers to further literature on their applications.

Section 4.1 deals with duality. If V is a vector space over $\mathbb{F}$, its dual, denoted V', consists of linear maps from V to $\mathbb{F}$; in other words, $V' = \mathcal{L}(V, \mathbb{F})$. We denote the dual pairing by

$$\langle v, w\rangle, \quad v \in V,\ w \in V'. \tag{4.0.1}$$

If $\dim V = n$ and $\{e_1, \dots, e_n\}$ is a basis of V, then V' has a basis $\{\varepsilon_1, \dots, \varepsilon_n\}$, called the dual basis, satisfying

$$\langle e_j, \varepsilon_k\rangle = \delta_{jk}, \quad 1 \le j, k \le n. \tag{4.0.2}$$

Also, if $A \in \mathcal{L}(V, W)$, we have the transpose $A^t \in \mathcal{L}(W', V')$, satisfying

$$\langle Av, w\rangle = \langle v, A^t w\rangle, \quad v \in V,\ w \in W'. \tag{4.0.3}$$

Section 4.2 treats convex sets. If V is a vector space, a subset $K \subset V$ is convex provided that, for each $x, y \in K$, $tx + (1-t)y \in K$ for all $t \in [0, 1]$, that is to say, the line segment from x to y is contained in K. We concentrate on convex sets that are closed and bounded, and assume $\dim V < \infty$. One result is that K is equal to the intersection of all half-spaces that contain it. Another result involves extreme points, i.e., points $p \in K$ that must be an endpoint of each line segment in K containing p. It is shown that whenever $\dim V < \infty$ and $K \subset V$ is a convex set that is closed and bounded, then each point in K is a limit of a sequence of convex combinations of extreme points of K (we say K is the closed convex hull of the set of extreme points).

Section 4.3 treats quotient spaces. If V is a vector space and W a linear subspace, the quotient V/W consists of equivalence classes of elements of V, where

we say $v \sim v' \Leftrightarrow v - v' \in W$. The quotient V/W has the structure of a vector space. When $\dim V < \infty$, we have

$$\dim V/W = \dim V - \dim W. \tag{4.0.4}$$

It is shown that if $T \in \mathcal{L}(V, X)$, then

$$\mathcal{R}(T) \approx V/\mathcal{N}(T). \tag{4.0.5}$$

Together, (4.0.4)–(4.0.5) imply the fundamental theorem of linear algebra, from §1.3. Another result established in §4.3 is the isomorphism

$$(V/W)' \approx W^{\perp}, \tag{4.0.6}$$

where, when $W \subset V$ is a linear subspace,

$$W^{\perp} = \{v \in V' : \langle w, v\rangle = 0,\ \forall\, w \in W\}. \tag{4.0.7}$$

Section 4.4 treats a class of matrices $A \in M(n, \mathbb{R})$ whose entries a_{jk} are all ≥ 0, i.e., *positive matrices*. We say A is *strictly positive* if each $a_{jk} > 0$. We say a positive matrix A is *primitive* if some power A^k is strictly positive, and we say it is *irreducible* if

$$A + \frac{1}{2}A^2 + \frac{1}{3!}A^3 + \cdots \quad \text{is strictly positive.} \tag{4.0.8}$$

A key result called the *Perron-Frobenius theorem* shows that if A is positive and irreducible, then there exist

$$\lambda > 0, \quad v \in \mathbb{R}^n \text{ strictly positive, such that } \ Av = \lambda v, \tag{4.0.9}$$

where to say $v = (v_1, \dots, v_n)^t$ is strictly positive is to say each $v_j > 0$. Under such conditions, the adjoint A^t is also positive and irreducible, and one has

$$\mu > 0, \quad w \in \mathbb{R}^n \text{ strictly positive, such that } \ A^t w = \mu w, \tag{4.0.10}$$

and in fact

$$\mu = \lambda. \tag{4.0.11}$$

Of particular interest are positive matrices A whose rows all sum to 1. These are called *stochastic matrices*, and (4.0.9) holds with $\lambda = 1$, $v = \mathbf{1} = (1, \dots, 1)^t$. If such A is irreducible, then one has (4.0.10)–(4.0.11), so

$$A^t \mathbf{p} = \mathbf{p}, \quad \mathbf{p} \in \mathbb{R}^n, \ \text{ strictly positive.} \tag{4.0.12}$$

We can normalize $\mathbf{p}$ so that its components sum to 1 (i.e., $\mathbf{p} \cdot \mathbf{1} = 1$), and regard $\mathbf{p}$ as an invariant probability distribution on the set $\{1, \dots, n\}$. A further result established in §4.4 is that if A is a primitive stochastic matrix, then

$$A^k \longrightarrow \mathcal{P}, \quad \text{as } \ k \to \infty, \tag{4.0.13}$$

where $\mathcal{P} \in M(n, \mathbb{R})$ is a projection, given by

$$\mathcal{P} = \mathbf{1}\mathbf{p}^t. \tag{4.0.14}$$

Hence also $(A^t)^k \to \mathcal{P}^t = \mathbf{p}\mathbf{1}^t$.

Another topic treated in §4.4 is the notion of a Markov semigroup, which is a set of matrices of the form

$$\{e^{tX} : t \geq 0\}, \quad X \in M(n, \mathbb{R}), \tag{4.0.15}$$

such that e^{tX} is a stochastic matrix for each $t \geq 0$. We characterize exactly which $X \in M(n, \mathbb{R})$ give rise to such a Markov semigroup.

4.1. Dual spaces

If V is an n-dimensional vector space over $\mathbb{F}$ ($\mathbb{R}$ or $\mathbb{C}$), its *dual* space V' is defined to be the space of linear transformations

$$w : V \longrightarrow \mathbb{F}. \tag{4.1.1}$$

We often use the notation

$$w(v) = \langle v, w\rangle, \quad v \in V,\ w \in V', \tag{4.1.2}$$

to denote this action. The space V' is a vector space, with vector operations

$$\langle v, w_1 + w_2\rangle = \langle v, w_1\rangle + \langle v, w_2\rangle, \quad \langle v, aw\rangle = a\langle v, w\rangle. \tag{4.1.3}$$

If $\{e_1, \dots, e_n\}$ is a basis of V, then an element $w \in V'$ is uniquely determined by its action on these basis elements:

$$\langle a_1e_1 + \cdots + a_ne_n, w\rangle = \sum a_jw_j, \quad w_j = \langle e_j, w\rangle. \tag{4.1.4}$$

Note that we can write

$$w = \sum_{j=1}^{n} w_j\varepsilon_j, \tag{4.1.5}$$

where $\varepsilon_j \in V'$ is determined by

$$\langle e_j, \varepsilon_k\rangle = \delta_{jk}, \tag{4.1.6}$$

where $\delta_{jk} = 1$ if $j = k$, 0 otherwise. It follows that each $w \in V'$ is written uniquely as a linear combination of $\{\varepsilon_1, \dots, \varepsilon_n\}$. Hence

$$\{\varepsilon_1, \dots, \varepsilon_n\} \text{ is a basis of } V'. \tag{4.1.7}$$

We say $\{\varepsilon_1, \dots, \varepsilon_n\}$ is the *dual basis* to $\{e_1, \dots, e_n\}$. It also follows that

$$\dim V = n \Longrightarrow \dim V' = n. \tag{4.1.8}$$

Note that, not only is (4.1.2) linear in $v \in V$ for each $w \in V'$, it is also linear in $w \in V'$ for each $v \in V$. This produces a natural map

$$j : V \longrightarrow (V')'. \tag{4.1.9}$$

Proposition 4.1.1. *If* $\dim V < \infty$*, the map* j *in* (4.1.9) *is an isomorphism.*

Proof. This follows readily from the material (4.1.4)–(4.1.8), as the reader can verify. □

REMARK. If $\dim V = \infty$, it still follows that j in (4.1.9) is injective, though we do not show this here. However, j is typically not surjective in such a case. In the rest of this section, we assume all vector spaces under discussion are finite dimensional.

REMARK. Given $\{\varepsilon_1, \dots, \varepsilon_n\}$ in (4.1.5)–(4.1.7) as the basis of V' dual to $\{e_1, \dots, e_n\}$, its dual basis in turn is

$$\{e_1, \dots, e_n\}, \tag{4.1.10}$$

under the identification

$$V \approx (V')' \tag{4.1.11}$$

of Proposition 4.1.1.

We turn to associating to a linear map $A : V \to W$ between two finite dimensional vector spaces the *transpose*,

$$A^t : W' \longrightarrow V', \tag{4.1.12}$$

defined by

$$\langle v, A^t\omega\rangle = \langle Av, \omega\rangle, \quad v \in V,\ \omega \in W'. \tag{4.1.13}$$

It is readily verified that, under (4.1.11) and its counterpart $(W')' \approx W$,

$$(A^t)^t = A. \tag{4.1.14}$$

If also $B : W \to X$, with transpose $B^t : X' \to W'$, then

$$(BA)^t = A^t B^t. \tag{4.1.15}$$

Exercises

1. Show that if $\dim V < \infty$ and $A \in \mathcal{L}(V)$, with transpose $A^t \in \mathcal{L}(V')$, then A and A^t have the same characteristic polynomial and the same minimal polynomial,

$$\operatorname{Spec} A^t = \operatorname{Spec} A, \quad \dim \mathcal{E}(A^t, \lambda) = \dim \mathcal{E}(A, \lambda),$$
$$\text{and} \quad \dim \mathcal{GE}(A^t, \lambda) = \dim \mathcal{GE}(A, \lambda).$$

2. Express the relation between the matrix representation of $A \in \mathcal{L}(V)$ with respect to a basis of V and the matrix representation of A^t with respect to the dual basis of V'.

3. Let $\mathcal{P}_n$ denote the space of polynomials in x of degree $\leq n$. Consider the subset $\{\psi_0, \psi_1, \dots, \psi_n\}$ of $\mathcal{P}_n'$ defined by

$$\langle p, \psi_k \rangle = p(k).$$

Show that this is a basis of $\mathcal{P}_n'$. Exhibit the dual basis (of $\mathcal{P}_n$).
Hint. See the results on the Lagrange interpolation formula, in Proposition 1.2.1.

4. Take the following basis $\{\delta_k : 0 \leq k \leq n\}$ of $\mathcal{P}_n'$,

$$\langle p, \delta_k \rangle = p^{(k)}(0).$$

Express $\{\psi_k\}$ as a linear combination of $\{\delta_k\}$, and vice-versa.
Hint. For one part, write down the power series expansion of $p(x)$ about $x = 0$, and then evaluate at $x = k \in \{0, \dots, n\}$. Show that this yields

$$\psi_k = \sum_{\ell=0}^{n} \frac{k^\ell}{\ell!} \delta_\ell.$$

Relate the task of inverting this both to the Lagrange interpolation formula and to material on the Vandermonde determinant.

5. Given the basis $\{q_k(x) = x^k : 0 \leq k \leq n\}$ of $\mathcal{P}_n$, express the dual basis $\{\varepsilon_k : 0 \leq k \leq n\}$ of $\mathcal{P}_n'$ as a linear combination of $\{\psi_k\}$, described in Exercise 3, and also as a linear combination of $\{\delta_k\}$, described in Exercise 4.

6. If $\dim V < \infty$, show that the trace yields natural isomorphisms

$$\mathcal{L}(V)' \approx \mathcal{L}(V), \quad \mathcal{L}(V)' \approx \mathcal{L}(V'),$$

via

$$\langle A, B \rangle = \operatorname{Tr} AB, \quad A, B \in \mathcal{L}(V),$$

and

$$\langle A, C \rangle = \operatorname{Tr} AC^t, \quad C \in \mathcal{L}(V').$$

7. Let V be a real vector space, of dimension n. Show that there is a natural

one-to-one correspondence (given by $(u, v) = \langle u, \iota(v)\rangle$) between
(A) inner products on V (as discussed in §3.1)
(B) isomorphisms $\iota : V \to V'$ having the property that ι coincides with

$$\iota^t : V \longrightarrow V',$$

where we identify V'' with V as in (4.1.9), and the property that

$$0 \neq u \in V \Longrightarrow \langle u, \iota(u)\rangle > 0.$$

4.2. Convex sets

Here V will be a vector space over $\mathbb{R}$, of dimension n. We assume V is an inner product space. We could just put $V = \mathbb{R}^n$, carrying the standard dot product, but it is convenient to express matters in a more general setting.

A subset $K \subset V$ is called convex if

$$x, y \in K,\ 0 \le t \le 1 \Longrightarrow tx + (1-t)y \in K. \tag{4.2.1}$$

In other words, we require that if x and y are in K, then the line segment joining x and y is also in K. We will mainly be interested in closed convex sets. A set $S \subset V$ is closed if, whenever $x_\nu \in S$ and $x_\nu \to x$ (we say x is a limit point), then $x \in S$. The closure $\overline{S}$ of a set S contains S and all its limit points. It readily follows that if $K \subset V$ is convex, so is $\overline{K}$.

Here is a useful result about convex sets.

Proposition 4.2.1. *If $K \subset V$ is a nonempty, closed, convex set and $p \in V \setminus K$, then there is a unique point $q \in K$ such that*

$$|q - p| = \inf_{x \in K} |x - p|. \tag{4.2.2}$$

Proof. The existence of such a distance minimizer follows from basic properties of closed subsets of $\mathbb{R}^n$; cf. Chapter 2 of [**10**]. As for the uniqueness, if $p \notin K$ and $q, q' \in K$ satisfy

$$|q - p| = |q' - p|, \tag{4.2.3}$$

and if $q \neq q'$, then one verifies that $\tilde{q} = (q + q')/2$ satisfies

$$|\tilde{q} - p| < |q - p|. \tag{4.2.4}$$

□

The uniqueness property actually characterizes convexity:

Proposition 4.2.2. *Let $K \subset V$ be a closed, nonempty set, with the property that, for each $p \in V \setminus K$, there is a unique $q \in K$ such that* (4.2.2) *holds. Then K is convex.*

Proof. If $x, y \in K$, $t_0 \in (0,1)$, and $t_0 x + (1-t_0)y \notin K$, one can find $t_1 \in (0,1)$ and $p = t_1 x + (1-t_1)y \notin K$ equidistant from two distinct points q and q' realizing (4.2.2). Details are left to the reader. □

Closed convex sets can be specified in terms of which half-spaces contain them. A closed half-space in V is a subset of V of the form

$$\{x \in V : \alpha(x) \le \alpha_0\} \text{ for some } \alpha_0 \in \mathbb{R}, \text{ some nonzero } \alpha \in V'. \tag{4.2.5}$$

Here is the basic result.

Proposition 4.2.3. *Let $K \subset V$ be a closed convex set, and let $p \in V \setminus K$. Then there exists a nonzero $\alpha \in V'$ and an $\alpha_0 \in \mathbb{R}$ such that*

$$\begin{aligned} &\alpha(p) > \alpha_0, \quad \alpha(x) \le \alpha_0,\ \forall\, x \in K, \text{ and} \\ &\alpha(q) = \alpha_0 \text{ for some } q \in K. \end{aligned} \tag{4.2.6}$$

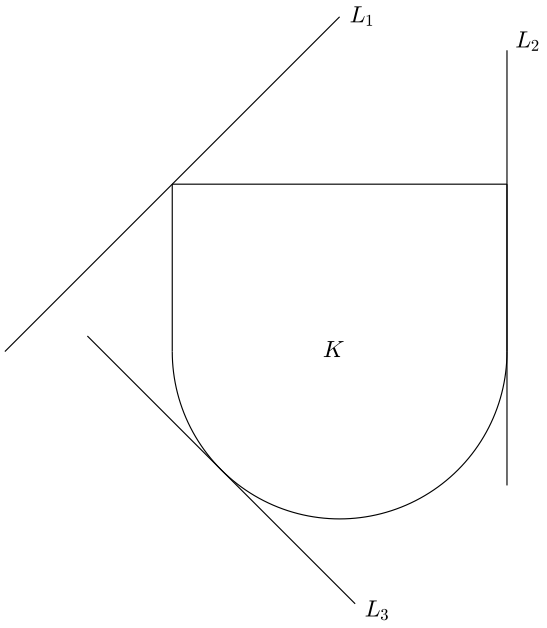

Figure 4.2.1. Convex set K and three supporting hyperplanes

Proof. Using Proposition 4.2.1, take $q \in K$ such that (4.2.2) holds. Then let $\alpha(x) = (x, p - q)$ (the inner product). Then one can verify that (4.2.6) holds, with $\alpha_0 = (q, p - q)$. □

Corollary 4.2.4. *In the setting of Proposition 4.2.3, given $p \in V \setminus K$, there exists a closed half-space H, with boundary $\partial H = L$, such that*

$$p \notin H, \quad K \subset H, \quad K \cap L \neq \emptyset. \tag{4.2.7}$$

Corollary 4.2.5. *If $K \subset V$ is a nonempty, closed, convex set, then K is the intersection of the collection of all closed half-spaces containing K.*

A set $L = \partial H$, where H is a closed half-space satisfying $K \subset H,\ K \cap L \neq \emptyset$, is called a supporting hyperplane of K. If K is a compact, convex set, one can pick any nonzero $\alpha \in V'$, and consider

$$L = \{x \in V : \alpha(x) = \alpha_0\}, \quad \alpha_0 = \sup_{x \in K} \alpha(x). \tag{4.2.8}$$

Such L is a supporting hyperplane for K. See Figure 4.2.1 for an illustration of supporting hyperplanes.

Extreme points

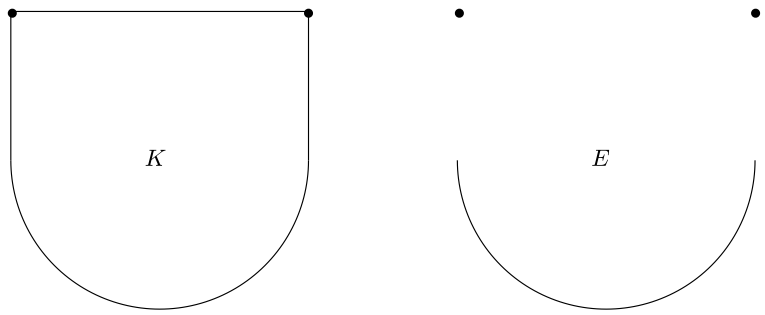

Figure 4.2.2. Convex set K, and its extreme points, E

Let $K \subset V$ be a closed, convex set. A point $x \in K$ is said to be an extreme point of K if it must be an endpoint of any line segment in K containing x. See Figure 4.2.2 for an illustration. If $K \subset V$ is a linear subspace, then K has no extreme points. Our goal is to show that if $K \subset V$ is a compact (i.e., closed and bounded) convex subset of V, then it has lots of extreme points. We aim to prove the following, a special case of a result known as the Krein-Milman theorem.

Proposition 4.2.6. *Let $K \subset V$ be a compact, convex set. Let E be the set of extreme points of K, and let F be the closed, convex hull of E, i.e., the closure of the set of points*

$$\sum a_j x_j, \quad x_j \in E, \quad a_j \geq 0, \quad \sum a_j = 1. \tag{4.2.9}$$

Then $F = K$.

We first need to show that $E \neq \emptyset$. The following will be a convenient tool.

Lemma 4.2.7. *Let $K \subset V$ be a compact, convex set, and let $L = \partial H$ be a supporting hyperplane (so $K_1 = K \cap L \neq \emptyset$). If $x_1 \in K_1$ is an extreme point of K_1, then x_1 is an extreme point of K.*

Proof. Exercise. □

Lemma 4.2.8. *In the setting of Lemma 4.2.7, each supporting hyperplane of K contains an extreme point of K.*

Proof. We proceed by induction on the dimension $n = \dim V$. The result is clear for $n = 1$, which requires K to be a compact interval (or a point). Suppose such a result is known to be true when $n < N$ ($N \geq 2$). Now assume $\dim V = N$. Let $L = \partial H$ be a supporting hyperplane of K, so $K_1 = L \cap K \neq \emptyset$. Translating, we can arrange that $0 \in L$, so L is a vector space and $\dim L = N - 1$. Arguing as in (4.2.8), there is a supporting hyperplane $L_1 = \partial H_1$ of K_1, so $K_2 = K_1 \cap L_1 \neq \emptyset$. By induction, K_1 has an extreme point in L_1. By Lemma 4.2.7, such a point must be an extreme point for K. □

Proof of Proposition 4.2.6. Under the hypotheses of Proposition 4.2.6, we know now that $E \neq \emptyset$ and F is a (nonempty) compact, convex subset of K. Suppose F is a proper subset of K, so there exists $p \in K,\ p \notin F$. By Proposition 4.2.3, with F in place of K, there exists $\alpha \in V'$ and $\alpha_0 \in \mathbb{R}$ such that

$$\alpha(p) > \alpha_0, \quad \alpha(x) \leq \alpha_0,\ \forall\, x \in F. \tag{4.2.10}$$

Now let

$$\alpha_1 = \sup_{x \in K} \alpha(x), \quad \widetilde{L} = \{x \in V : \alpha(x) = \alpha_1\}. \tag{4.2.11}$$

Then $\widetilde{L}$ is a supporting hyperplane for K, so by Lemma 4.2.8, $\widetilde{L}$ contains an extreme point of K. However, since $\alpha_1 > \alpha_0$, $\widetilde{L} \cap F = \emptyset$, so $\widetilde{L} \cap E = \emptyset$. This is a contradiction, so our hypothesis that F is a proper subset of K cannot work. This proves Proposition 4.2.6. □

Exercises

1. Let $A : V \to W$ be linear and let $K \subset V$ be a compact, convex set, $E \subset K$ its set of extreme points. Show that $A(K) \subset W$ is a compact, convex set and $A(E)$ contains the set of extreme points of $A(K)$.

2. Let $\Sigma \subset S^{n-1}$ be a proper closed subset of the unit sphere $S^{n-1} \subset \mathbb{R}^n$, and let K be the closed convex hull of Σ. Show that K must be a proper subset of the closed unit ball $\overline{B} \subset \mathbb{R}^n$.

3. Let K_1 and K_2 be compact, convex subsets of V that are disjoint ($K_1 \cap K_2 = \emptyset$). Show that there exists a hyperplane $L = \partial H$ separating K_1 and K_2, so, e.g., $K_1 \subset H$, $K_2 \subset V \setminus \overline{H}$.
Hint. Pick $p \in K_1, q \in K_2$ to minimize distance. Let L pass through the midpoint of the line segment γ from p to q and be orthogonal to this segment.

4. Let K be the subset of $\mathcal{L}(\mathbb{R}^n)$ consisting of positive-semidefinite, symmetric matrices A with operator norm $\|A\| \leq 1$. Describe the set of extreme points of K, as orthogonal projections.
Hint. Diagonalize.

5. Consider the following variant of Exercise 4. Let $A \in \mathcal{L}(\mathbb{R}^n)$ be a symmetric matrix, let $\mathcal{A} \subset \mathcal{L}(\mathbb{R}^n)$ be the linear span of I and the powers of A, and let K consist of positive semi-definite matrices in $\mathcal{A}$, of operator norm ≤ 1. Describe the set of extreme points of K.

4.3. Quotient spaces

Let V be a vector space over $\mathbb{F}$ ($\mathbb{R}$ or $\mathbb{C}$), and let $W \subset V$ be a linear subspace. The *quotient space* V/W consists of equivalence classes of elements of V, where, for $v, v' \in V$,

$$v \sim v' \Longleftrightarrow v - v' \in W. \tag{4.3.1}$$

Given $v \in V$, we denote its equivalence class in V/W by $[v]$. Then V/W has the structure of a vector space, with vector operations

$$[v_1] + [v_2] = [v_1 + v_2], \quad a[v] = [av], \tag{4.3.2}$$

given $v, v_1, v_2 \in V,\ a \in \mathbb{F}$. These operations are well defined, since

$$v_1 \sim v_1',\ v_2 \sim v_2' \Longrightarrow v_1 + v_2 \sim v_1' + v_2' \tag{4.3.3}$$

and

$$v \sim v' \Longrightarrow av \sim av'. \tag{4.3.4}$$

As seen in §1.3, if $\dim V = n < \infty$ and $W \subset V$ is a linear subspace, then $\dim W = m \leq n$ (and $m < n$ unless $W = V$). Furthermore, given any basis $\{w_1, \dots, w_m\}$ of W, there exist $v_{m+1}, \dots, v_n \in V$ such that

$$\{w_1, \dots, w_m, v_{m+1}, \dots, v_n\} \tag{4.3.5}$$

is a basis of V. It readily follows that

$$\{[v_{m+1}], \dots, [v_n]\} \text{ is a basis of } V/W, \tag{4.3.6}$$

so

$$\dim V/W = \dim V - \dim W, \tag{4.3.7}$$

if $\dim V < \infty$.

We denote the quotient map by Π:

$$\Pi : V \longrightarrow V/W, \quad \Pi v = [v]. \tag{4.3.8}$$

This is a linear map. We have $\mathcal{R}(\Pi) = V/W$ and $\mathcal{N}(\Pi) = W$.

Proposition 4.3.1. *Take $W \subset V$ as above and let X be a vector space and $T : V \to X$ be a linear map. Assume $\mathcal{N}(T) \supset W$. Then there exists a unique linear map $S : V/W \to X$ such that*

$$S \circ \Pi = T. \tag{4.3.9}$$

Proof. We need to take

$$S[v] = Tv. \tag{4.3.10}$$

Now, under our hypotheses,

$$v \sim v' \Rightarrow v - v' \in W \Rightarrow T(v - v') = 0 \Rightarrow Tv = Tv', \tag{4.3.11}$$

so (4.3.10) is well defined, and gives rise to (4.3.9). □

Proposition 4.3.2. *In the setting of Proposition 4.3.1,*

$$\mathcal{N}(S) = \mathcal{N}(T)/W. \tag{4.3.12}$$

Corollary 4.3.3. *If $T : V \to X$ is a linear map, then*

$$\mathcal{R}(T) \approx V/\mathcal{N}(T). \tag{4.3.13}$$

In case $\dim V < \infty$, we can combine (4.3.13) and (4.3.7) to recover the result that

$$\dim V - \dim \mathcal{N}(T) = \dim \mathcal{R}(T), \tag{4.3.14}$$

established in §1.3.

If $W \subset V$ is a linear subspace, we set

$$W^\perp = \{\alpha \in V' : \langle w, \alpha\rangle = 0,\ \forall\, w \in W\}. \tag{4.3.15}$$

Applying Proposition 4.3.1 with $X = \mathbb{F}$, we see that to each $\alpha \in W^\perp$ there corresponds a unique $\tilde{\alpha} : V/W \to \mathbb{F}$ (i.e., $\tilde{\alpha} \in (V/W)'$) such that

$$\tilde{\alpha} \circ \Pi = \alpha. \tag{4.3.16}$$

The correspondence $\alpha \mapsto \tilde{\alpha}$ is a linear map:

$$\gamma : W^\perp \longrightarrow (V/W)'. \tag{4.3.17}$$

Note that if $\alpha \in W^\perp$, then $\tilde{\alpha} \in (V/W)'$ is defined by

$$\langle [v], \tilde{\alpha}\rangle = \langle v, \alpha\rangle, \tag{4.3.18}$$

so $\tilde{\alpha} = 0 \Leftrightarrow \alpha = 0$. Thus γ in (4.3.17) is injective. Conversely, given $\beta : V/W \to \mathbb{F}$, we have $\beta = \gamma(\alpha)$ with $\alpha = \beta \circ \Pi$, so γ in (4.3.17) is also surjective. To summarize,

Proposition 4.3.4. *The map γ in* (4.3.17) *is an isomorphism:*

$$W^\perp \approx (V/W)'. \tag{4.3.19}$$

Exercises

1. Let $\mathcal{P}$ denote the space of all polynomials in x. Let

$$\mathcal{Q} = \{p \in \mathcal{P} : p(1) = p(-1) = 0\}.$$

Describe a basis of $\mathcal{P}/\mathcal{Q}$. What is its dimension?

2. Let $\mathcal{P}_n$ be the space of polynomials in x of degree $\leq n$. Let $\mathcal{E}_n \subset \mathcal{P}_n$ denote the set of *even* polynomials of degree $\leq n$. Describe a basis of $\mathcal{P}_n/\mathcal{E}_n$. What is its dimension?

3. Do Exercise 2 with $\mathcal{E}_n$ replaced by $\mathcal{O}_n$, the set of *odd* polynomials of degree $\leq n$.

4. Let $A \in M(n, \mathbb{C})$ be self adjoint ($A = A^*$). Let $\mathcal{A} \subset M(n, \mathbb{C})$ be the linear span of I and the powers of A. Let

$$\mathcal{B} = \{B \in M(n, \mathbb{C}) : AB = BA\}.$$

Note that $\mathcal{A} \subset \mathcal{B}$. Describe

$$\mathcal{B}/\mathcal{A}$$

in terms of the multiplicity of the eigenvalues of A.

5. Do Exercise 4, with the hypothesis that $A = A^*$ replaced by the hypothesis that A is *nilpotent*. Describe $\mathcal{B}/\mathcal{A}$ in terms of the Jordan normal form of A.

4.4. Positive matrices and stochastic matrices

Let A be a real $n \times n$ matrix, i.e.,

$$A = (a_{jk}) \in M(n, \mathbb{R}). \tag{4.4.1}$$

We say A is positive if $a_{jk} \geq 0$ for each $j, k \in \{1, \dots, n\}$. There is a circle of results about certain classes of positive matrices, known collectively as the Perron-Frobenius theorem, which we aim to treat here. We start with definitions of these various classes.

We say A is strictly positive if $a_{jk} > 0$ for each such j, k. We say A is primitive if some power A^m is strictly positive. We say A is irreducible if, for each $j, k \in \{1, \dots, n\}$, there exists $m = m(j, k)$ such that the (j, k) entry of A^m is > 0. An equivalent condition for a positive A to be irreducible is that

$$B = \sum_{k=1}^{\infty} \frac{1}{k!} A^k = e^A - I \tag{4.4.2}$$

is strictly positive. Clearly

$$A \text{ strictly positive} \Rightarrow A \text{ primitive} \Rightarrow A \text{ irreducible}. \tag{4.4.3}$$

An example of a positive matrix A that is irreducible but not primitive is

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{4.4.4}$$

We will largely work under the hypothesis that A is positive and irreducible.

Here is another perspective. With $v = (v_1, \dots, v_n)^t$ denoting an element of $\mathbb{R}^n$, let

$$C_+^n = \{v \in \mathbb{R}^n : v_j \geq 0, \ \forall\, j\}, \quad \overset{\circ}{C}{}_+^n = \{v \in \mathbb{R}^n : v_j > 0, \ \forall\, j\}. \tag{4.4.5}$$

One verifies that, for $A \in M(n, \mathbb{R})$,

$$A \text{ positive} \iff A : C_+^n \to C_+^n. \tag{4.4.6}$$

Also, given A positive

$$A \text{ irreducible} \implies A : C_+^n \setminus 0 \to C_+^n \setminus 0. \tag{4.4.7}$$

In fact,

$$B \text{ strictly positive} \implies B : C_+^n \setminus 0 \to \overset{\circ}{C}{}_+^n, \tag{4.4.8}$$

and if $B = e^A - I$, then $Av = 0 \Rightarrow Bv = 0$, so (4.4.7) follows from (4.4.8).

The first part of the Perron-Frobenius theorem is the following key result.

Proposition 4.4.1. *If $A \in M(n, \mathbb{R})$ is positive and satisfies the conclusion of (4.4.7), then there exist*

$$\lambda > 0, \quad v \in C_+^n \setminus 0, \quad \textit{such that} \quad Av = \lambda v. \tag{4.4.9}$$

Proof. With $\langle\ ,\ \rangle$ denoting the standard inner product on $\mathbb{R}^n$, let

$$\Sigma = \{v \in C_+^n : \langle \mathbf{1}, v \rangle = 1\}, \quad \mathbf{1} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}. \tag{4.4.10}$$

Thus Σ is a compact, convex subset of $\mathbb{R}^n$. We define

$$\Phi : \Sigma \longrightarrow \Sigma \tag{4.4.11}$$

by

$$\Phi(v) = \frac{1}{\langle \mathbf{1}, Av\rangle} Av. \tag{4.4.12}$$

Note that the hypotheses that $A : \Sigma \to C^n_+ \setminus 0$ implies $\langle \mathbf{1}, Av\rangle > 0$ for $v \in \Sigma$. It follows that Φ in (4.4.11) is continuous. We can invoke the following result.

Brouwer fixed point theorem. If $\Sigma \subset \mathbb{R}^n$ is a compact, convex set and $\Phi : \Sigma \to \Sigma$ is a continuous map, then Φ has a fixed point, i.e., there exists $v \in \Sigma$ such that $\Phi(v) = v$.

A proof of this result is given in Chapter 5 of [**11**]. In the setting of (4.4.11), we have a vector $v \in \Sigma$ such that

$$Av = \langle \mathbf{1}, Av\rangle v. \tag{4.4.13}$$

This proves Proposition 4.4.1. □

From here, we have:

Proposition 4.4.2. *If A is positive and irreducible, and* (4.4.9) *holds, then each component of v is > 0, so in fact $v \in \overset{\circ}{C}{}^n_+$.*

Proof. If $Av = \lambda v$, then $Bv = (e^\lambda - 1)v$. Now (4.4.8) implies $Bv \in \overset{\circ}{C}{}^n_+$, so $v \in \overset{\circ}{C}{}^n_+$. □

Clearly if A is positive and irreducible, so is its transpose, A^t, so we have the following.

Proposition 4.4.3. *If A is positive and irreducible, then there exist*

$$w \in \overset{\circ}{C}{}^n_+ \quad \text{and} \quad \mu > 0 \quad \text{such that} \quad A^t w = \mu w. \tag{4.4.14}$$

It is useful to have the following more precise result.

Proposition 4.4.4. *In the setting of Proposition 4.4.3, given* (4.4.9) *and* (4.4.14),

$$\mu = \lambda. \tag{4.4.15}$$

Proof. We have

$$\lambda\langle v, w\rangle = \langle Av, w\rangle = \langle v, A^t w\rangle = \mu\langle v, w\rangle. \tag{4.4.16}$$

Since $v, w \in \overset{\circ}{C}{}^n_+ \Rightarrow \langle v, w\rangle > 0$, this forces $\mu = \lambda$. □

To proceed, let us replace A by $\lambda^{-1}A$, which we relabel as A, so (4.4.9) holds with $\lambda = 1$, and we have

$$Av = v, \quad v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \quad v_j > 0, \ \forall\, j. \tag{4.4.17}$$

If we replace the standard basis $\{e_1, \dots, e_n\}$ of $\mathbb{R}^n$ by $\{f_1, \dots, f_n\}$, with $f_j = v_j e_j$, then, with respect to this new basis, A is a positive, irreducible matrix, and

$$A\mathbf{1} = \mathbf{1}, \tag{4.4.18}$$

with $\mathbf{1}$ as in (4.4.10). A positive matrix A satisfying (4.4.18) is called a stochastic matrix.

To continue, if A is an irreducible stochastic matrix, (4.4.14)–(4.4.15) yield a vector $\mathbf{p}$ such that

$$A^t\mathbf{p} = \mathbf{p}, \quad \mathbf{p} = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}, \quad p_j > 0, \tag{4.4.19}$$

and we can normalize this eigenvector so that

$$\sum_j p_j = 1. \tag{4.4.20}$$

In connection with this, let us note that

$$\langle \mathbf{1}, A^t w\rangle = \langle A\mathbf{1}, w\rangle = \langle \mathbf{1}, w\rangle, \tag{4.4.21}$$

so

$$A^t : \Sigma \longrightarrow \Sigma, \tag{4.4.22}$$

with Σ as in (4.4.10).

We now introduce two norms on $\mathbb{R}^n$:

$$\|v\|_\infty = \sup_j |v_j|, \quad \|v\|_1 = \sum_j |v_j|, \tag{4.4.23}$$

given $v = (v_1, \dots, v_j)^t \in \mathbb{R}^n$. We see that if A is a stochastic matrix, so (4.4.18) holds, then

$$\|A\|_\infty = 1, \quad \text{and} \quad \|A^t\|_1 = 1, \tag{4.4.24}$$

where $\|A\|_\infty$ is the operator norm of A with respect to the norm $\| \ \|_\infty$ on $\mathbb{R}^n$, and $\|A^t\|_1$ is the operator norm of A^t with respect to the norm $\| \ \|_1$ on $\mathbb{R}^n$. It follows that all the eigenvalues of A and of A^t have absolute value ≤ 1.

Before stating the next result, we set up some notation. If A is an irreducible stochastic matrix, and $\mathbf{p}$ is as in (4.4.19)–(4.4.20), let $V \subset \mathbb{R}^n$ be the orthogonal complement of $\mathbf{p}$:

$$V = \{v \in \mathbb{R}^n : \langle v, \mathbf{p}\rangle = 0\}. \tag{4.4.25}$$

It follows that

$$\mathbb{R}^n = V \oplus \operatorname{Span} \mathbf{1}, \quad A : V \to V. \tag{4.4.26}$$

Proposition 4.4.5. *Let $A \in M(n, \mathbb{R})$ be a strictly positive stochastic matrix. Then*

$$\|A|_V\|_\infty < 1. \tag{4.4.27}$$

Proof. This follows from the observation that if A is strictly positive and its row sums are all 1, then

$$v \in \mathbb{R}^n, \quad v \notin \operatorname{Span} \mathbf{1} \Longrightarrow \|Av\|_\infty < \|v\|_\infty. \tag{4.4.28}$$

□

Recalling how we modified a positive, irreducible matrix to obtain a stochastic matrix, we have the following.

Corollary 4.4.6. *Let $B \in M(n, \mathbb{R})$ be strictly positive, so B has an eigenvalue $\lambda > 0$ with associated eigenvector $v_0 \in \overset{\circ}{C}{}^n_+$, and B^t has a λ-eigenvector $w_0 \in \overset{\circ}{C}{}^n_+$. Let V be the orthogonal complement of w_0, so*

$$\mathbb{R}^n = V \oplus \operatorname{Span} v_0 \quad \text{and} \quad B : V \to V. \tag{4.4.29}$$

Then

$$\beta \in \operatorname{Spec} B|_V \Longrightarrow |\beta| < \lambda. \tag{4.4.30}$$

Corollary 4.4.7. *In the setting of Corollary 4.4.6, λ is an eigenvalue of B of algebraic multiplicity* 1.

That is to say, the generalized eigenspace $\mathcal{GE}(B, \lambda)$ of B associated to the eigenvalue λ is 1-dimensional, spanned by v_0.

Proposition 4.4.8. *Let $A \in M(n, \mathbb{R})$ be an irreducible stochastic matrix. Then* 1 *is an eigenvalue of A of algebraic multiplicity* 1.

Proof. Form $B = e^A - I$, as in (4.4.2). Then B is strictly positive, so Corollaries 4.4.6–4.4.7 apply. Note that $\mathbf{1}$ is an eigenvector of B, with eigenvalue $e - 1$. Now each vector in the generalized eigenspace $\mathcal{GE}(A, 1)$ of A is also in the generalized eigenspace $\mathcal{GE}(B, e-1)$ of B. By Corollary 4.4.7, this latter space is 1-dimensional. □

To state the next result, we bring in the following notation. Given the direct sum decomposition (4.4.26), let $\mathcal{P}$ denote the projection of $\mathbb{R}^n$ onto $\operatorname{Span} \mathbf{1}$ that annihilates V.

Proposition 4.4.9. *Let $A \in M(n, \mathbb{R})$ be a stochastic matrix, and assume A is primitive. Then, given $v \in \mathbb{R}^n$,*

$$A^k v \longrightarrow \mathcal{P}v, \quad \text{as} \quad k \to \infty. \tag{4.4.31}$$

Proof. The hypothesis implies that, for some $m \in \mathbb{N}$, $B = A^m$ is a strictly positive stochastic matrix. Proposition 4.4.5 applies, to give

$$\|B_V\|_\infty = \beta < 1, \quad B_V = B|_V. \tag{4.4.32}$$

Now, given $v \in \mathbb{R}^n,\ j \in \mathbb{N},\ \ell \in \{0, \dots, m-1\}$,

$$\begin{aligned} A^{jm+\ell} &= A^\ell A^{jm} v \\ &= A^\ell B^j v \\ &= A^\ell (\mathcal{P}v + B_V^j (I - \mathcal{P})v) \\ &= \mathcal{P}v + A^\ell B_V^j (I - \mathcal{P})v, \end{aligned} \tag{4.4.33}$$

and

$$\|A^\ell B_V^j (I - \mathcal{P})v\|_\infty \leq \beta^j \|(I - \mathcal{P})v\|_\infty. \tag{4.4.34}$$

This completes the proof. □

Note. In the setting of Proposition 4.4.9, we also have

$$(A^t)^k \longrightarrow \mathcal{P}^t, \quad \text{as} \ \ k \to \infty. \tag{4.4.35}$$

More precisely,

$$(A^t)^{jm+\ell} = \mathcal{P}^t + (A^\ell B_V^j (I - \mathcal{P}))^t, \tag{4.4.36}$$

and

$$\|(A^\ell B_V^j (I - \mathcal{P}))^t\|_1 = \|A^\ell B_V^j (I - \mathcal{P})\|_\infty \leq \beta^j \|I - \mathcal{P}\|_\infty. \tag{4.4.37}$$

Note also that $\mathcal{P}^t$ is the projection of $\mathbb{R}^n$ onto $\operatorname{Span} \mathbf{p}$ that annihilates $\{u \in \mathbb{R}^n : \langle u, \mathbf{1} \rangle = 0\}$. We also have

$$\mathcal{P} = \mathbf{1}\mathbf{p}^t, \quad \mathcal{P}^t = \mathbf{p}\mathbf{1}^t. \tag{4.4.38}$$

If A is a stochastic matrix, the set $\{A^k : k \in \mathbb{Z}^+\}$ is called a discrete-time Markov semigroup. It is also of interest to consider the following continuous time analogue.

Definition. Given $X \in M(n, \mathbb{R})$, we say

$$\{e^{tX} : t \geq 0\} \tag{4.4.39}$$

is a *Markov semigroup* provided e^{tX} is a stochastic matrix for each $t \geq 0$. In such a case, we say X generates a Markov semigroup.

The following result characterizes $n \times n$ Markov semigroups.

Proposition 4.4.10. *A matrix $X = (x_{jk}) \in M(n, \mathbb{R})$ generates a Markov semigroup if and only if*

$$X\mathbf{1} = 0, \tag{4.4.40}$$

and

$$x_{jk} \geq 0 \quad \textit{whenever} \quad j \neq k. \tag{4.4.41}$$

Proof. First, assume X generates a Markov semigroup. Since

$$\frac{d}{dt}e^{tX}\Big|_{t=0} = X, \tag{4.4.42}$$

we see that the relation $e^{tX}\mathbf{1} \equiv \mathbf{1}$ implies (4.4.40). The positivity (4.4.41) follows from (4.4.42) and the positivity

$$a_{jk}(t) \geq 0, \quad e^{tX} = A(t) = \big(a_{jk}(t)\big), \tag{4.4.43}$$

plus the fact that $a_{jk}(0) = 0$ for $j \neq k$.

For the converse, we first note that if (4.4.41) is strengthened to $x_{jk} > 0$ whenever $j \neq k$, then, via

$$e^{tX} = I + tX + O(t^2), \tag{4.4.44}$$

we have $t_0 > 0$ such that e^{tX} is positive for $0 \leq t \leq t_0$. Then positivity for all $t \geq 0$ follows from

$$e^{ntX} = \big(e^{tX}\big)^n. \tag{4.4.45}$$

To deduce positivity of e^{tX} for general $X \in M(n, \mathbb{R})$ satisfying (4.4.41), we can argue as follows. Take $Y = (y_{jk})$ with $y_{jk} \equiv 1$, and consider $X + \varepsilon Y$. Then the arguments above show that $e^{t(X+\varepsilon Y)}$ is positive for all $t \geq 0$, $\varepsilon > 0$. Now we claim that

$$\lim_{\varepsilon \searrow 0} e^{t(X+\varepsilon Y)} = e^{tX}, \tag{4.4.46}$$

which then yields positivity of e^{tX}. To see (4.4.46), note that $Z_\varepsilon(t) = e^{t(X+\varepsilon Y)}$ satisfies

$$\frac{d}{dt}Z_\varepsilon(t) = XZ_\varepsilon(t) + \varepsilon Y Z_\varepsilon(t), \quad Z_\varepsilon(0) = I, \tag{4.4.47}$$

so, by Duhamel's formula (cf. Exercise 1 of §3.7),

$$Z_\varepsilon(t) = e^{tX} + \varepsilon \int_0^t e^{(t-s)X} Y Z_\varepsilon(s)\, ds, \tag{4.4.48}$$

which leads to (4.4.46), and completes the proof of this proposition. □

The study of discrete and continuous Markov semigroups is an important area in probability theory. For more on this, see [**8**].

Exercises

1. Show that the matrix A in (4.4.4) is an irreducible stochastic matrix for which (4.4.31) fails.

2. Pick $a \in (0,1)$ and consider the stochastic matrix

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

Show that A is primitive. Compute A^{100}.

3. Let $A \in M(n,\mathbb{R})$ be a stochastic matrix, and set $T = A^t$. By (4.4.22), $T : \Sigma \to \Sigma$, with Σ as in (4.4.10). Pick $v_0 \in \Sigma$, and set

$$v_k = T^k v_0, \quad w_n = \frac{1}{n}(v_0 + v_1 + \cdots + v_{n-1}).$$

Note that $v_k, w_n \in \Sigma$. Show that

$$Tw_n = w_n + \frac{1}{n}(v_n - v_0).$$

Since $\Sigma \subset \mathbb{R}^n$ is closed and bounded, $\{w_n\}$ has a convergent subsequence, $w_{n_j} \to w \in \Sigma$. (See [**10**], Chapter 2, for a proof.) Show that

$$Tw = w.$$

Compare this with the production of $\mathbf{p}$ in (4.4.19).

Bibliography

[1] M. Artin, *Algebra*, Prentice-Hall, Englewood Cliffs, NJ, 1991.

[2] G. Birkhoff and S. MacLane, *Survey of Modern Algebra*, Macmillan, New York, 1953.

[3] G. Golub and C. van Loan, *Matrix Computations*, Johns Hopkins Univ. Press, 1996.

[4] K. Hofmann and R. Kunze, *Linear Algebra*, Prentice Hall, New Jersey, 1971.

[5] R. Horn and C. Johnson, *Matrix Analysis*, Cambridge Univ. Press, Cambridge UK, 1985.

[6] S. Lang, *Algebra*, Addison-Wesley, Reading MA, 1965.

[7] S. Lang, *Linear Algebra*, Springer, New York, 1987.

[8] E. Seneta, *Non-negative Matrices and Markov Chains*, Springer-Verlag, New York, 1981.

[9] G. Strang, *Linear Algebra and its Applications* (4th ed.), Brooks/Cole, Belmont, CA, 2006.

[10] M. Taylor, *Introduction to Analysis in One Variable*, Amer. Math. Soc., Providence RI, 2020.

[11] M. Taylor, *Introduction to Analysis in Several Variables (Advanced Calculus)*, Amer. Math. Soc., Providence RI, 2020.

[12] M. Taylor, *Partial Differential Equations*, Vols. 1–3, Springer, New York, 1996 (2nd ed., 2011).

[13] M. Taylor, *Introduction to Differential Equations*, Amer. Math. Soc., Providence RI, 2011.

[14] M. Taylor, *Measure Theory and Integration*, Amer. Math. Soc., Providence RI, 2006.

[15] M. Taylor, *Introduction to Complex Analysis*, GSM #202, Amer. Math. Soc., Providence RI, 2019.

[16] M. Taylor, *Linear Algebra*, Amer. Math. Soc., Providence RI, 2020.

[17] L. Trefethen and D. Bau, *Numerical Linear Algebra*, SIAM, 1997.

Index