# 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, tensor products, exterior algebra, fields, rings, modules, principal ideal domains, groups, quaternions, Clifford algebra, octonions, Noetherian rings

# 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 a treatment of this subject in sufficient depth to 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 $\lambda_j$ 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 $\lambda_j$ 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.

Chapter 5 deals with multilinear maps and related constructions, including tensor products in §5.2 and exterior algebra in §5.3, which we approach as a further development of the theory of determinants, initiated in §1.5. Results of this chapter are particularly useful in the development of differential geometry and manifold theory, involving studies of tensor fields and differential forms.

In Chapter 6 we extend the scope of our study of vector spaces, adding to $\mathbb{R}$ and $\mathbb{C}$ more general fields $\mathbb{F}$. We define the notion of a field, give a number of additional examples, and describe how results of Chapters 1, 2, 4, and 5 extend to vector spaces over a general field $\mathbb{F}$. Specific fields considered include both finite fields, such as $\mathbb{Z}/(p)$, and fields of algebraic numbers. In §6.2 we show that the set $\mathcal{A}$ of algebraic numbers, which are roots of polynomials with rational coefficients, are precisely the eigenvalues of square matrices with rational entries. We use this, together with some results of §5.2, to obtain a proof that $\mathcal{A}$ is a field, different from that given in §6.1. This line is carried forward in the next chapter, where we identify the ring of algebraic integers with the set of eigenvalues of square matrices with integer entries.

In Chapter 7 we extend the scope of linear algebra further, from vector spaces over fields to modules over rings. Specific rings considered include the ring $\mathbb{Z}$ of integers, rings of polynomials, and matrix rings. We discuss $\mathcal{R}$-linear maps between two $\mathcal{R}$-modules, for various rings $\mathcal{R}$, with an emphasis on commutative rings with unit. We pay particular interest, in §7.2, to modules over principal ideal domains (PIDs). Examples of PIDs include both $\mathbb{Z}$ and polynomial rings $\mathbb{F}[t]$. In §7.3 we revisit results obtained in §2.2 and §2.4 on generalized eigenspaces and the Jordan canonical form for $A \in \mathcal{L}(V)$, and show how they follow from results on the structure of $\mathcal{R}$-modules in §7.2, when $\mathcal{R} = \mathbb{F}[t]$.

Section 7.5 introduces the class of Noetherian rings and the associated class of Noetherian modules. This class of rings, defined by a certain finiteness condition, contains the class of PIDs. It also contains other important classes of rings, in particular polynomial rings in several variables, thanks to a fundamental result known as the Hilbert basis theorem. Section 7.6 treats unique factorization domains (UFDs), and shows that this class of rings shares with the class of Noetherian rings the property of being preserved under passing from $\mathcal{R}$ to $\mathcal{R}[x]$.

In Chapter 8 we encounter a sample of special structures in linear algebra. Section 8.1 deals with quaternions, objects of the form $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{R}$, which form a noncommutative ring $\mathbb{H}$, with a number of interesting properties. In particular, the quaternion product captures both the dot product and the cross product of vectors in $\mathbb{R}^3$. We also discuss matrices with entries in $\mathbb{H}$, with special attention to a family of groups $Sp(n) \subset M(n, \mathbb{H})$.

Section 8.2 discusses the general concept of an algebra, an object that is simultaneously a vector space over a field $\mathbb{F}$ and a ring, such that the product is $\mathbb{F}$-bilinear. Many of the rings introduced earlier, such as $\mathcal{L}(V)$ and $\mathbb{H}$, are algebras, but some, such as $\mathbb{Z}$ and $\mathbb{Z}[t]$, are not. We introduce some new ones, such as the tensor algebra $\otimes^* V$ associated to a vector space, and the tensor product $\mathcal{A} \otimes \mathcal{B}$ of two algebras. Properly speaking, these algebras are *associative algebras*. We briefly mention a class of nonassociative algebras known as Lie algebras, and another class, known as Jordan algebras.

Section 8.3 treats an important class of algebras called Clifford algebras. These are intimately related to the construction of a class of differential operators known as Dirac operators. Section 8.4 treats an intriguing nonassociative algebra called the algebra of octonions (or Cayley numbers). We discuss similarities and differences with the algebra of quaternions, and also examine its particularly intriguing group of automorphisms.

We end with some appendices, treating some background material as well as complementary topics. Appendix A.1 gives a proof of the Fundamental Theorem of Algebra, that every nonconstant polynomial with complex coefficients has complex roots. This result has several applications in §2.1 and §2.2. Appendix A.2 takes up the notion of averaging a set of rotations. We produce the "average" as a solution to a minimization problem.

Appendix A.3 brings up another algebraic structure, that of a group. It describes how various groups have arisen in the text, and presents some general results on these objects, with emphasis on two classes of groups: infinite matrix groups like $G\ell(n, \mathbb{R})$ on the one hand, and groups like the permutation groups $S_n$, which are finite groups, on the other. We cap our treatment of basic results on groups with a discussion of an application to a popular encryption scheme, based on a choice of two large prime numbers.

Appendix A.4 produces new fields $\widetilde{\mathbb{F}}$ from old fields, constructed so that a polynomial $P \in \mathbb{F}[x]$ without roots in $\mathbb{F}$ will have roots in $\widetilde{\mathbb{F}}$. In particular, we obtain all finite fields in this fashion, proceeding from the fields $\mathbb{Z}/(p)$. Material in this appendix provides a further arsenal of fields to which the results of Chapter 6 apply, and also puts the reader in a position to tackle treatments of Galois theory.

The material presented in this text could serve for a two semester course in linear algebra. For a one semester course, I recommend a straight shot through Chapters 1–4, with attention to Appendices A.1 and A.3. Material in Chapters 5–7 and a selection from Chapter 8 and the appendices could work well in a second semester course. To be sure, there is considerable flexibility in the presentation of this material. For example, one might move the treatment of vector spaces over general fields way up, to follow Chapter 2 directly. In any case, I encourage the student/reader to sample all the sections, as an encounter with the wonderful mathematical subject that is linear algebra.

We point out some distinctive features of this treatment of linear algebra.

1) Basics first. We start with vector spaces over the set $\mathbb{R}$ of real numbers or the set $\mathbb{C}$ of complex numbers, and linear transformations between such vector spaces. Thus the reader who has seen multivariable calculus should be comfortable with the setting of the early chapters. We treat the two cases simultaneously, and use the label $\mathbb{F}$ to apply either to $\mathbb{R}$ or to $\mathbb{C}$, as the occasion warrents. This is a forward-looking strategy, since we will later on consider vector spaces over general *fields*, denoted $\mathbb{F}$, and the reader can appreciate the early material on this more general level with minimal effort.

2) Development of determinants. The determinant is a fundamental tool in linear algebra. Many treatments of this topic start with a complicated formula, involving a sum of products of matrix entries, as a proposed definition of the determinant, and this is rightly seen as off-putting. However, there is a better way. Section 1.5 establishes that there is a unique function $\vartheta : M(n, \mathbb{F}) \to \mathbb{F}$, satisfying three simple rules, and this defines the determinant. A straightforward application of these rules leads to the formula mentioned above, but one does not have to remember this formula, just the 3 simple rules. They lead directly to essential results, such as multiplicativity, $\det AB = (\det A)(\det B)$, and also invariance of the determinant under certain column operations. That nasty formula does have one simple, useful consequence, namely $\det A = \det A^t$, which also allows one to bring in row operations.

3) Contact with geometry and analysis. We get into metric properties of linear spaces in Chapter 3, and associate norms both to elements of a vector space and to linear transformations. We draw parallels between metric properties of inner product spaces and $n$-dimensional Euclidean geometry.

One use of norms is to be able to treat infinite series of linear transformations, in particular the matrix exponential, which ties in with systems of differential equations.

4) Going beyond basics. After Chapter 4 we start to extend the scope of linear algebra beyond the study of linear transformations between a pair of real or complex vector spaces.

We look at *multilinear algebra*, the study of multilinear maps on an $n$-tuple of vector spaces, i.e., maps that are linear in each of the $n$ arguments. Actually such an object arose in §1.5, the determinant, which, acting on an $n \times n$ matrix, was analyzed as acting on an $n$-tuple of column vectors. In Chapter 5 we take this further, and tie in theories of multilinear maps with tensor products and exterior algebras, the latter topic directly extending the theory of the determinant.

Next, we look at vector spaces over general fields, a concept defined in Chapter 6. The way we set up the earlier chapters, once we define the concept of a field, $\mathbb{F}$, most of the material of Chapters 1, 2, 4, and 5 extends in a straightforward fashion to this more general setting.

The next step extends the theory of vector spaces over a field to that of modules over a ring, taken up in Chapter 7. Substantially new phenomena arise in this expanded setting. Some of the constructions here feed back to material of Chapter 6, in that the theory of rings provides further material on the theory of fields.

**Acknowledgments.** Thanks to Robert Bryant for useful conversations related to various topics treated here, particularly regarding octonions.

During the preparation of this book, my research has been supported by a number of NSF grants, most recently DMS-1500817.

# 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 $\geq 0$.

$\mathbb{N}$ is the set of integers $\geq 1$ (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,

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

## 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 $\mathbb{R}^2$.

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

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

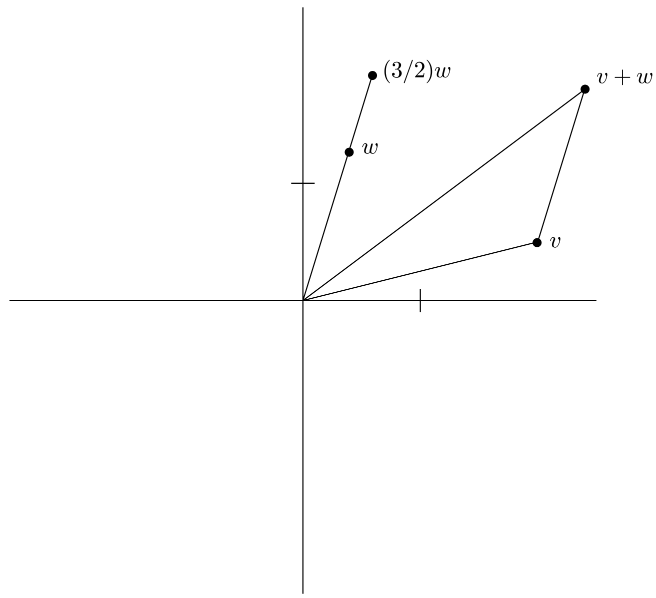


**Figure 1.1.1.** Vector operations on $\mathbb{R}^2$

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 $\le n$. 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

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

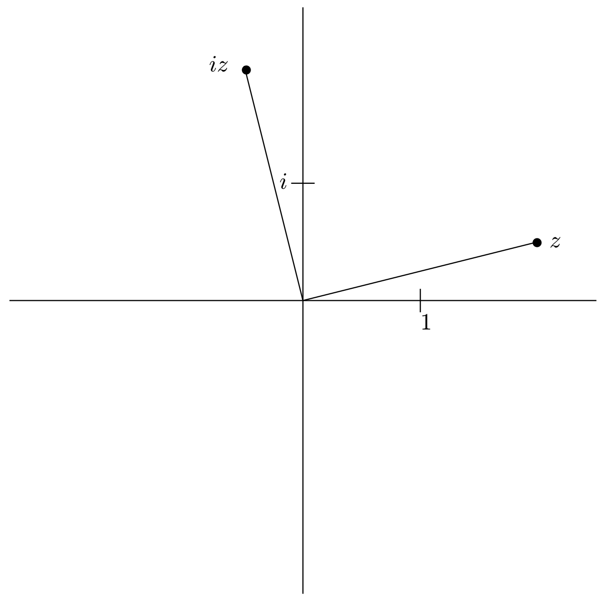


**Figure 1.1.2.** Multiplication by $i$ in $\mathbb{C}$

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:

(1.1.10) Commutative law : $u + v = v + u,$

(1.1.11) Associative law : $(u + v) + w = u + (v + w),$

(1.1.12) Zero vector : $\exists\ 0 \in V,\ v + 0 = v,$

(1.1.13) Negative : $\exists - v,\ v + (-v) = 0.$

Next there are laws for multiplication by scalars:

(1.1.14) Associative law : $a(bv) = (ab)v,$

(1.1.15) Unit : $1 \cdot v = v.$

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

$$w_j \in W,\ a_j \in \mathbb{F} \Longrightarrow a_1w_1+a_2w_2 \in W. \tag{1.1.19}$$

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

$$T(a_1 v_1 + a_2 v_2) = a_1 T v_1 + a_2 T v_2, \quad \forall \ a_j \in \mathbb{F}, \ v_j \in V. \tag{1.2.2}$$

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:

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

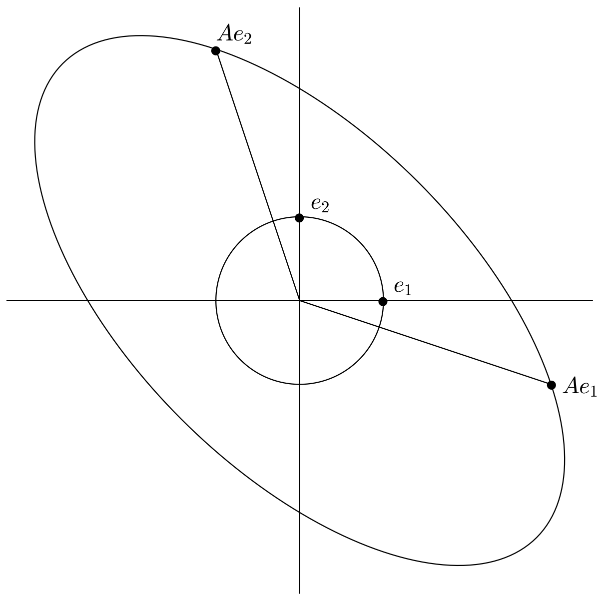


**Figure 1.2.1.** Action of the linear transformation $A$ in (1.2.6)

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 $\leq k$.

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

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

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 $j$th 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 $j$th 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 $j$th 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 $\le n$ (with coefficients in $\mathbb{F}$). Pick distinct points $a_j \in \mathbb{F}$, $1 \le j \le n+1$, 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 $S = \{a_1, \dots, a_{n+1}\}$. Here is our surjectivity result.

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

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

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

Then

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

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

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

In other words,

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

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

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

## Exercises

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

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

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 $A^t B^t$ and $B^t A^t$.

11. Let $A, B, C$ be matrices satisfying $C = AB$. Denote by $b_k$ the $k$th column of $B$, cf. (1.2.22), and similarly let $a_k$ and $c_k$ denote the $k$th 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 $k$th column of $C$:

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

Note that the second identity represents the $k$th column of $C$ as a linear combination of the columns of $A$, with coefficients coming from the $k$th 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

$$a_1 w_1 + \cdots + a_k w_k = 0,$$

so we have

$$a_1 v_1 + \cdots + a_k v_k = (a_1 v_{k1} + \cdots + a_k v_{kk}) v_{k+1},$$

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

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 $\ell \le k$. $\square$

**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 $W$. $\square$

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 $L = \operatorname{Span}\{u_1, \dots, u_m\}$, and consider

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

Clearly $w \in \mathcal{R}(A) \Rightarrow w = A(a_1 w_1 + \cdots + a_\ell w_\ell + b_1 u_1 + \cdots + b_m u_m) = A_0(b_1 u_1 + \cdots + b_m u_m)$, 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 $M_x : \mathcal{P} \to \mathcal{P}$ $(M_x f(x) = xf(x))$ 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*

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

*and*

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

**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

$$B(a_1 w_1 + \cdots + a_\ell w_\ell) = a_1 v_1 + \cdots + a_\ell v_\ell. \tag{1.3.14}$$

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

$$C(a_1 w_1 + \cdots + a_k w_k + b_1 u_1 + \cdots + b_m u_m) = a_1 v_1 + \cdots + a_k v_k. \tag{1.3.15}$$

This works in (1.3.13). $\square$

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,

$$A\Big(\sum_{j=1}^{n} c_j e_j\Big) = 0 \Longleftrightarrow \sum_{j=1}^{n} c_j a_j = 0, \tag{1.3.20}$$

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 $\le 10$. Specify a basis of $V$ and compute $\dim V$.

3. Let $V$ be the space of polynomials in $x$ of degree $\le 5$, 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

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

8. Show that

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

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 $\{w_j, iw_j : 1 \le j \le n\}$ 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 $j$th 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 $\Sigma$, 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 (3.2)–(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

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

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 $2 \times 2$ 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 $j$th 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)* $\vartheta$ *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 $j$th 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 $\ell$ are distinct, that is, unless $(j, k, \ell)$ 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 $(e_j, e_k, e_\ell)$ 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 $3 \times 3$ determinants. Given $A \in M(3, \mathbb{F})$, form a $3 \times 5$ 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 $2 \times 2$ 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 $\sigma$, 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 $\sigma$ and $\tau$ 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 $\sigma$ 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 $\tau$ 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 $j$th column of $A^t$ has the same entries as the $j$th 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 $j$th column $b_j$, then

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

Clearly rule (a) holds for $\vartheta_1$. 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 $\vartheta_1$. Finally, rule (c′) holds for $\vartheta_1$, with $r = \det A$, and (1.5.38) follows. $\square$

**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 $\det A \neq 0$. $\square$

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 $ca_\ell$ 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 $a_\ell$. Hence $A^b$ has two identical columns, so $\det A^b = 0$, and (1.5.41) holds. $\square$

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 $k$th 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 $3 \times 3$ 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 $\sigma$ 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 $\det(e_j, a_2, \dots, a_n) = (-1)^{j-1} \det A_{1j}$ where $A_{kj}$ is formed by deleting the $k$th column and the $j$th 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 $k$th column.

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

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

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 $a_\ell$ in the $k$th column as well as in the $\ell$th 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 $A_\nu$ 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 $n$th 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

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

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

$$\begin{gathered} P_\sigma \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = \begin{pmatrix} v_{\sigma(1)} \\ \vdots \\ v_{\sigma(m)} \end{pmatrix} \quad M_c \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = \begin{pmatrix} c_1 v_1 \\ \vdots \\ c_m v_m \end{pmatrix}, \\ E_{jk\gamma} \begin{pmatrix} v_1 \\ \vdots \\ v_j \\ \vdots \\ v_m \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_j - \gamma v_k \\ \vdots \\ v_m \end{pmatrix}, \end{gathered} \tag{1.6.12}$$

with $v = (v_1, \dots, v_m)^t \in \mathbb{F}^m$. To illustrate what these matrices are when $m = 2$ and $\sigma, c$, and $(j, k, \gamma)$ 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 $P_\sigma, M_c$, 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

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

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 $j$th 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 $2 \times 2$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ 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 $\Omega$ into a countable collection of "cells," i.e., rectangular solids of the form $R = I_1 \times \cdots \times I_n$, a product

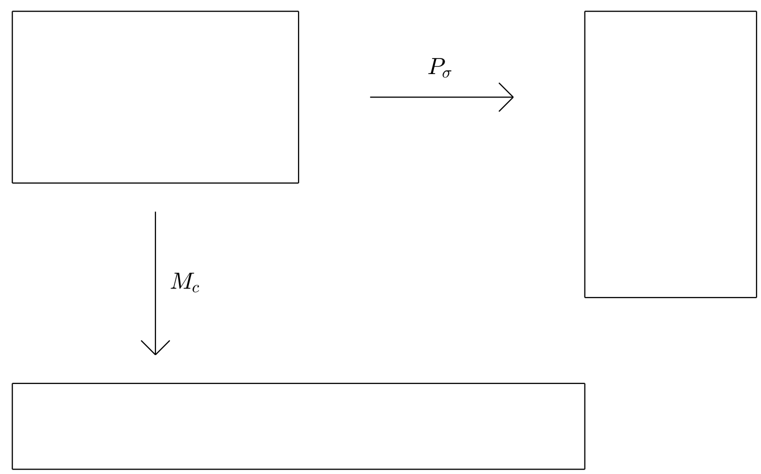


**Figure 1.6.1.** Actions of $P_\sigma$ and $M_c$ on a cell

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 $I_\nu$. Then we set $\mathrm{Vol}(\Omega)$ to be the countable sum of the volumes of the cells in such a partition. One faces the task of showing that $\mathrm{Vol}(\Omega)$ 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 $\sigma$ 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 $\Omega$ be open sets in $\mathbb{R}^n$, and let $F : \mathcal{O} \to \Omega$ be a bijective map. Assume $F$ and

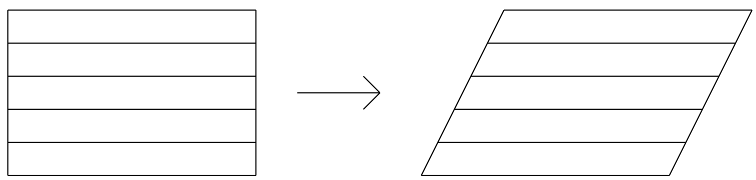

**Figure 1.6.2.** Action of $E_{12\gamma}$ on a cell

its inverse $F^{-1} : \Omega \to \mathcal{O}$ are both continuously differentiable. Let $DF(x)$ denote the $n \times n$ matrix

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

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

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

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 [**24**], and more generally for all Lebesgue integrable $u : \Omega \to \mathbb{R}$ in Chapter 7 of [**29**].

**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 *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 $2 \le j \le m$, 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 $j$th 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 $j \ne 2$, 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 $j$th 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 $j$th 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 $\mu$ 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 $\mu$. It follows that the column rank of $\widetilde{A}$ is also $\mu$, so $\mathcal{R}(\widetilde{A})$ has dimension $\mu$. 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 $P_\sigma$ 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

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

**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 $S_\nu$ has the form (1.6.51). As seen in (1.6.14), $E_{jk\gamma}^{-1} = E_{jk,-\gamma}$ so each matrix $S_\nu^{-1}$ 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.,*

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

*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 $P_\sigma$). 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. $\square$

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

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

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,

$$A = L_1 U_1 = L_2 U_2 \tag{1.6.59}$$

implies

$$L_2^{-1} L_1 = U_2 U_1^{-1}. \tag{1.6.60}$$

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):

$$A = L_0 D U_0, \tag{1.6.61}$$

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 $L = L_0 D_\ell$ and $U = D_r U_0$, 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 $A = A^t = U_0^t D L_0^t$, which is another factorization of the form (1.6.61). Uniqueness implies $L_0 = U_0^t$, so

$$A = A^t = L_0 D L_0^t. \tag{1.6.62}$$

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

$$A = A^* = L_0 D L_0^*, \quad D \ \text{ real.} \tag{1.6.63}$$

## 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 $\lambda$. 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 A.1) 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 $\lambda$, 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 $\lambda_j$ 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 $\mathrm{Spec}(T)$. Clearly $\lambda_j \in \mathrm{Spec}(T)$ if and only if $T - \lambda_j I$ is not injective, so, if $V$ is finite dimensional,

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

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 A.1 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 $\lambda_j$, then there is a real $\lambda_j$-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

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

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 $v_j \in \mathcal{E}(T, \lambda_j)$, $1 \le j \le k$. 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

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

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. $\square$

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

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

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

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

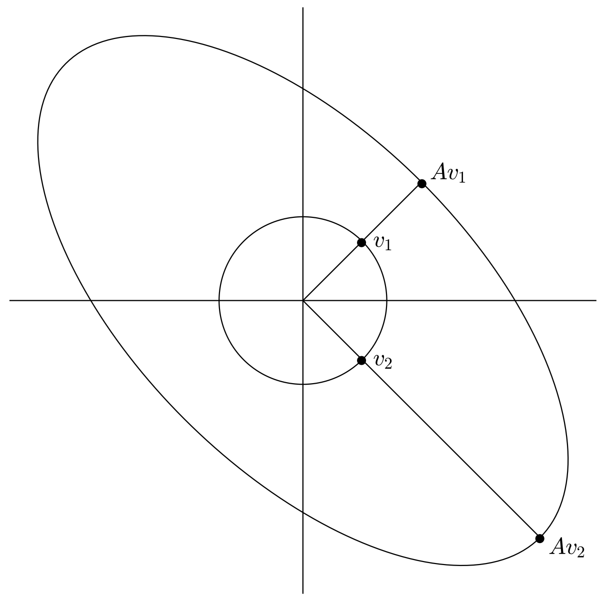


**Figure 2.1.1.** Behavior of the linear transformation $A$ in (2.1.8), with two distinct real eigenvalues

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 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.

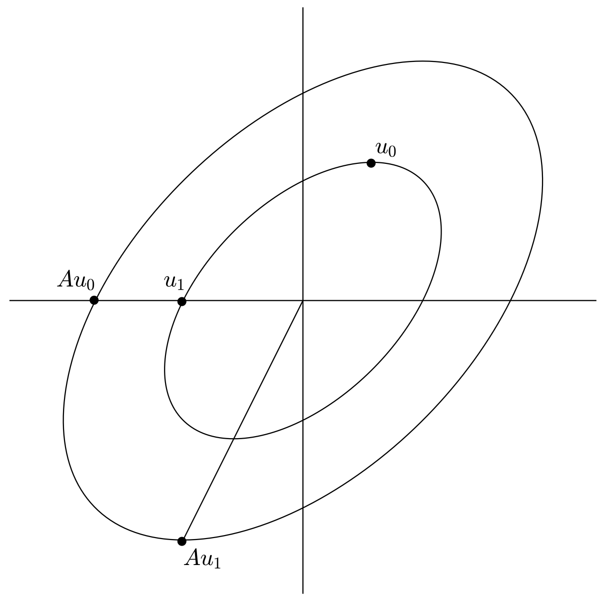


**Figure 2.1.2.** Action of the linear transformation (2.1.10) on $\mathbb{R}^2$, with purely imaginary eigenvalues, and eigenvectors $v_\pm = u_0 \mp iu_1$

## 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?

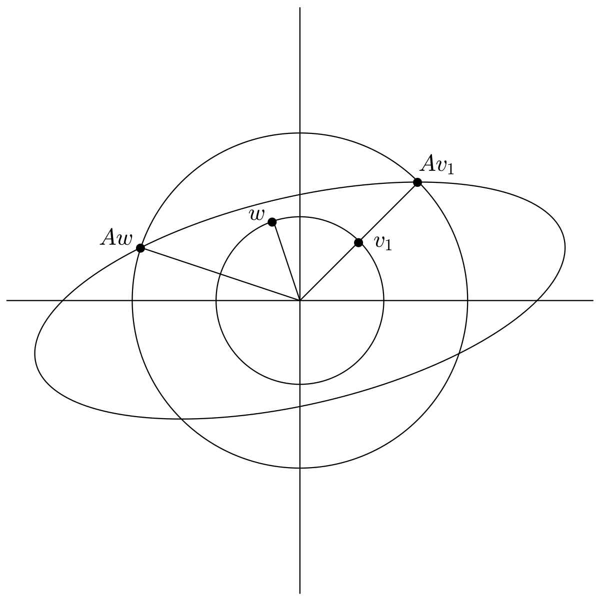


**Figure 2.1.3.** Action of the transformation (2.1.15) on $\mathbb{R}^2$, with a double eigenvalue and one-dimensional eigenspace

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 $0 \in \mathrm{Spec}(A)$. 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 $\sigma_k$ 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 $\lambda_j$-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 $\mathcal{GE}(T, \lambda_j) \neq 0$,*

$$T - \mu I : \mathcal{GE}(T, \lambda_j) \longrightarrow \mathcal{GE}(T, \lambda_j) \quad \textit{is an isomorphism}, \ \forall\, \mu \neq \lambda_j. \tag{2.2.5}$$

**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 $\lambda_j$. In particular, the set of $\lambda_j$ for which $\mathcal{GE}(T, \lambda_j)$ is nonzero coincides with $\mathrm{Spec}(T)$, 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 $\lambda$.

**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:

$$\begin{gathered} p, q \in \mathcal{I} \Longrightarrow p + q \in \mathcal{I}, \\ p \in \mathcal{I},\ q \in \mathcal{P} \Longrightarrow pq \in \mathcal{I}. \end{gathered} \tag{2.2.9}$$

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. $\square$

Remark. We hence see that each $\lambda_j$ 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 7.3 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 $\lambda$ 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 $\mathcal{GE}(T, \lambda_\ell)$, $1 \le \ell \le K$, denote the generalized eigenspaces of $T$ (with $\lambda_\ell$ 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 $w_\ell$ 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 $c_j \ne 0$ for each $j \in \{1, \dots, m\}$. As seen in Lemma 2.2.1,

$$T - \mu I : \mathcal{GE}(T, \lambda_\ell) \longrightarrow \mathcal{GE}(T, \lambda_\ell) \ \text{ is an isomorphism}, \ \forall\, \mu \ne \lambda_\ell. \tag{2.2.27}$$

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 $\lambda_j$-eigenvectors $v_j$, $1 \le j \le 3$, span $\mathbb{C}^3$.

(II) $A$ has 2 distinct eigenvalues, say $\lambda_1$ (single) and $\lambda_2$ (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, $\lambda_1$. Then $\operatorname{Spec}(A-\lambda_1 I) = \{0\}$, 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

$$\begin{aligned} \mathcal{GE}(L_A, \lambda_j) &= \operatorname{Span}\{vw^t : v \in \mathcal{GE}(A, \lambda_j), w \in \mathbb{C}^n\}, \\ \mathcal{GE}(R_B, \mu_k) &= \operatorname{Span}\{vw^t : v \in \mathbb{C}^n, w \in \mathcal{GE}(B^t, \mu_k)\}. \end{aligned}$$

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:*

$$N \ \textit{ is nilpotent}, \tag{2.3.2}$$

$$\mathrm{Spec}(N) = \{0\}, \tag{2.3.3}$$

(2.3.4) *There is a basis of $V$ for which $N$ is strictly upper triangular*,

(2.3.5) *There is a basis of $V$ for which $N$ is strictly lower triangular.*

**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 $\lambda^n$ (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

$$(N - \mu I)^{-1} = -\frac{1}{\mu}\Bigl(I - \frac{1}{\mu}N\Bigr)^{-1} = -\frac{1}{\mu}\sum_{\ell=0}^{k-1} \frac{1}{\mu^\ell} N^\ell, \tag{2.3.6}$$

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. $\square$

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 $\operatorname{Spec}(T) = \{\lambda_\ell : 1 \leq \ell \leq K\}$ 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 $S_\ell$ of $V_\ell$ with respect to which $T_\ell - \lambda_\ell I$ is strictly upper triangular, hence in which $T_\ell$ 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 $A_\ell$, 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 $\nu$, $AB_\nu$ 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.

$$\begin{aligned} &A = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ &\qquad \Longrightarrow AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad BA = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. \end{aligned} \tag{2.3.18}$$

## 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 $a_0, \dots, a_{n-1}$ 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 $\le k$ 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 $\lambda_j$ 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 $N^m v_0 = 0$; $m \le n$. 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 $V \le 1$.

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:

$$\{v_j, Nv_j, \dots, N^{\ell_j} v_j\}, \quad 1 \le j \le d. \tag{2.4.2}$$

Furthermore, each $v_j$ has the form $v_j = Nw_j$ for some $w_j \in V$. Hence we have the following strings in $V$:

$$\{w_j, v_j = Nw_j, Nv_j, \dots, N^{\ell_j} v_j\}, \quad 1 \le j \le d. \tag{2.4.3}$$

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

$$b_j = 0, \quad a_{j\ell} = 0, \quad \forall\, j \in \{1, \dots, d\},\ \ell \le \ell_j - 1. \tag{2.4.6}$$

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

$$\{N^{\ell_j} v_j : 1 \le j \le d\} \tag{2.4.9}$$

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

$$c_i = 0, \quad \forall\, i \in \{1, \dots, \nu\}, \quad a_{j,\ell_j} = 0, \quad \forall\, j \in \{1, \dots, d\}, \tag{2.4.13}$$

since (2.4.9)–(2.4.10) form a basis of $\mathcal{N}(N)$. We have the asserted linear independence of

$$\{w_j, v_j, \dots, N^{\ell_j} v_j\},\ 1 \le j \le d, \quad \{\xi_1, \dots, \xi_\nu\}. \tag{2.4.14}$$

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. $\square$

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

$$\mathcal{R}(N) = \operatorname{Span}\{e_1, e_3\}, \tag{2.4.24}$$

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

$$\mathcal{N}(N) = \operatorname{Span}\{e_1, e_2 - e_3\}. \tag{2.4.27}$$

Consequently, a string basis of $\mathbb{C}^4$ consists of two strings:

$$\{e_4 - e_3, e_3, e_1\} \ \text{ and } \ \{e_2 - e_3\}. \tag{2.4.28}$$

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).

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 $2 \times 2$ 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 $\lambda$-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 $v_j = x_j + i y_j$, with $x_j, y_j \in \mathbb{R}$, we have $\overline{v}_j = x_j - i y_j$, 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:

$$(a_1 v_1 + a_2 v_2, w) = a_1 (v_1, w) + a_2 (v_2, w), \tag{3.1.5}$$

$$(v, w) = \overline{(w, v)}, \tag{3.1.6}$$

$$(v, v) > 0, \quad \text{unless} \quad v = 0. \tag{3.1.7}$$

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

$$\|av\| = |a| \cdot \|v\|, \quad \forall a \in \mathbb{F},\ v \in V, \tag{3.1.12}$$

$$\|v\| > 0, \quad \text{unless} \quad v = 0, \tag{3.1.13}$$

$$\|v + w\| \leq \|v\| + \|w\|. \tag{3.1.14}$$

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),

$$|(v, w)| \leq \|v\|\,\|w\|, \quad \forall\ v, w \in V. \tag{3.1.17}$$

**Proof.** We start with

$$0 \leq \|v - w\|^2 = \|v\|^2 - 2\,\mathrm{Re}\,(v, w) + \|w\|^2, \tag{3.1.18}$$

which implies

$$2\,\mathrm{Re}\,(v, w) \leq \|v\|^2 + \|w\|^2, \quad \forall\ v, w \in V. \tag{3.1.19}$$

Replacing $v$ by $\alpha v$ for arbitrary $\alpha \in \mathbb{F}$ of absolute value 1 yields $2\,\mathrm{Re}\,\alpha(v, w) \leq \|v\|^2 + \|w\|^2$. This implies

$$2|(v, w)| \leq \|v\|^2 + \|w\|^2, \quad \forall\ v, w \in V. \tag{3.1.20}$$

Replacing $v$ by $tv$ and $w$ by $t^{-1}w$ for arbitrary $t \in (0, \infty)$, we have

$$2|(v, w)| \leq t^2\|v\|^2 + t^{-2}\|w\|^2, \quad \forall\ v, w \in V,\ t \in (0, \infty). \tag{3.1.21}$$

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

$$\begin{aligned} v = a_1 u_1 + \cdots + a_n u_n, \quad & w = b_1 u_1 + \cdots + b_n u_n \\ & \Rightarrow (v, w) = a_1 \overline{b}_1 + \cdots + a_n \overline{b}_n. \end{aligned} \tag{3.1.25}$$

It is often useful to construct orthonormal bases. The construction we now describe is called the Gramm-Schmidt construction.

**Proposition 3.1.2.** *Let $\{v_1, \dots, v_n\}$ be a basis of $V$, an inner product space. Then there is an orthonormal basis $\{u_1, \dots, u_n\}$ 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 $P_1 v = (v, u_1) u_1$ and set

$$\tilde{v}_2 = v_2 - P_1 v_2 = v_2 - (v_2, u_1) u_1. \tag{3.1.28}$$

We see that $(\tilde{v}_2, u_1) = (v_2, u_1) - (v_2, u_1) = 0$. Also $\tilde{v}_2 \ne 0$ 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 $\{u_1, \dots, u_m\}$ 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 $\mathrm{Span}(u_1, \dots, u_m)$) by

$$P_m v = (v, u_1) u_1 + \cdots + (v, u_m) u_m, \tag{3.1.30}$$

and set

$$\begin{aligned} \tilde{v}_{m+1} &= v_{m+1} - P_m v_{m+1} \\ &= v_{m+1} - (v_{m+1}, u_1) u_1 - \cdots - (v_{m+1}, u_m) u_m. \end{aligned} \tag{3.1.31}$$

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 $v_{m+1} \notin \operatorname{Span}\{v_1, \dots, v_m\} = \operatorname{Span}\{u_1, \dots, u_m\}$, 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

$$u_1(x) = \frac{1}{\sqrt{2}}. \tag{3.1.35}$$

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.

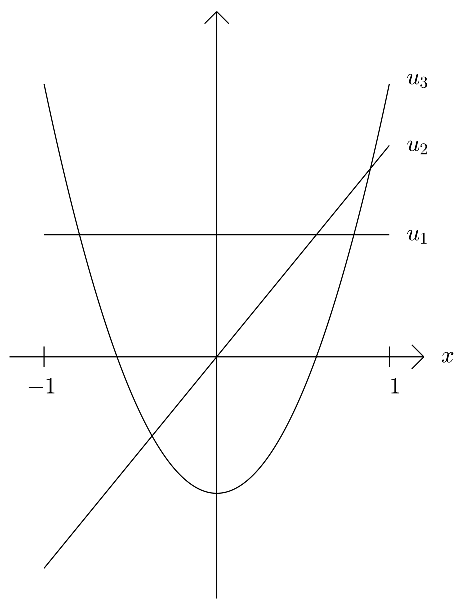


**Figure 3.1.1.** Orthogonal polynomials

## 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

$$W^\perp = \mathrm{Span}\{u_1, \dots, u_\ell\}, \tag{3.1.41}$$

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 $\mathrm{Span}\{a_1, \dots, a_j\} = \mathrm{Span}\{q_1, \dots, q_j\}$ for $1 \le j \le n$. 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 $n = 2$.

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

$$b = \sqrt{2a}. \tag{3.1.48}$$

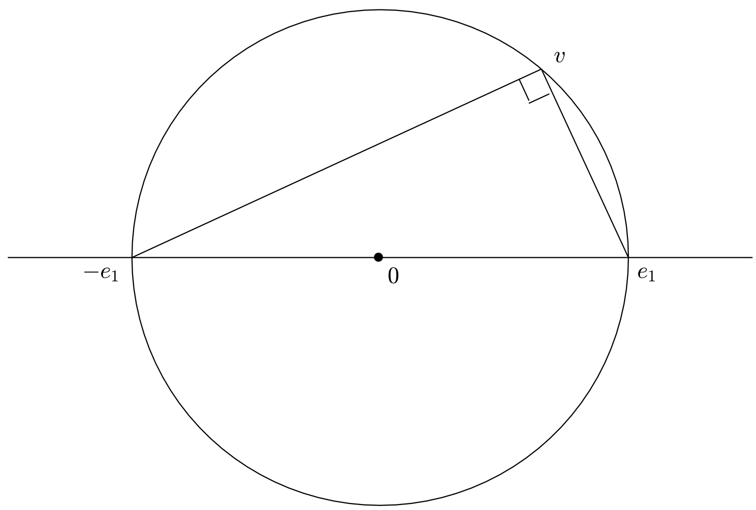


**Figure 3.1.2.** Right triangle in a circle

*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 $(\ ,\ )$ with respect to which $\mathcal{B}$ is an orthonormal basis of $V$. Denote the associated norm by $| \cdot |$, so

$$|v|^2 = (v, v).$$

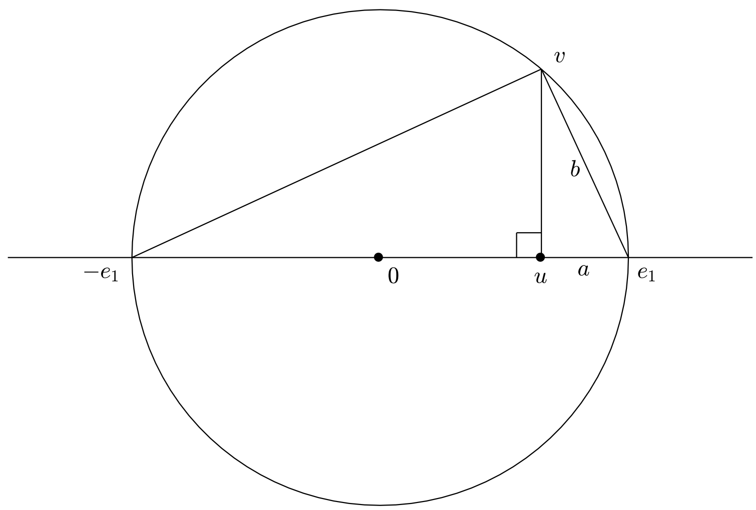


**Figure 3.1.3.** Geometric construction of $b = \sqrt{2a}$

14. Set $M = \max\{\|u_1\|, \dots, \|u_n\|\}$. Show that

$$\|v\| \le nM\,|v|.$$

*Hint.* Start with $v = c_1 u_1 + \cdots + c_n u_n,\ c_j = (v, u_j)$, and apply the triangle inequality to the resulting formula for $\|v\|$. Note that

$$|c_j| \le |v|.$$

15. This exercise treats the reverse inequality. It uses concepts developed in Chapters 2–3 of [**23**]. 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 $\varphi$ is continuous.

(c) By (a) and (b), $\varphi$ 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

$$\|T\| = \sup\{\|Tv\| : \|v\| \le 1\}. \tag{3.2.1}$$

Equivalently, $\|T\|$ is the smallest quantity $K$ such that

$$\|Tv\| \le K\|v\|, \quad \forall\, v \in V. \tag{3.2.2}$$

To see the equivalence, note that (10.2) holds if and only if $\|Tv\| \le K$ 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

$$\|STv\| \le \|S\|\,\|Tv\| \le \|S\|\,\|T\|\,\|v\|, \quad \forall\, v \in V, \tag{3.2.3}$$

and hence

$$\|ST\| \le \|S\|\,\|T\|. \tag{3.2.4}$$

In particular, we have by induction that

$$T : V \to V \Longrightarrow \|T^n\| \le \|T\|^n. \tag{3.2.5}$$

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

$$T \text{ injective} \iff T^* \text{ surjective}.$$

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

$$\|S + T\| \le \|S\| + \|T\|.$$

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

$$\lambda \in \operatorname{Spec}(A) \Longrightarrow |\lambda| \le \|A\|.$$

8. Show that, for any real $\theta$, 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 $T \in \mathcal{L}(V)$,

$$\|T\| = \sup\{|(Tu, v)| : \|u\|, \|v\| \le 1\}.$$

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
$$\begin{aligned}\frac{d}{dt} \det(A + tB)\Big|_{t=0} = \det(b_1, a_2, \dots, a_n) + \cdots + \det(a_1, \dots, b_k, \dots, a_n) \\ + \cdots + \det(a_1, \dots, a_{n-1}, b_n).\end{aligned}$$
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 $k$th column and the $j$th 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 $\lambda_j$ is an eigenvalue of a self-adjoint $T \in \mathcal{L}(V)$, then $\lambda_j$ 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

$$\lambda_j(v_j, v_k) = (Tv_j, v_k) = (v_j, Tv_k) = \lambda_k(v_j, v_k).$$

$\square$

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

$$\text{Span}\{u, v\} \subset V \tag{3.3.14}$$

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*

$$A \textit{ is positive definite } \Longleftrightarrow \det A_\ell > 0, \quad \forall\, \ell \in \{1, \dots, n\}. \tag{3.3.27}$$

**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 $A_\ell$ must be positive definite, hence have positive determinant, so we have $\Rightarrow$.

The implication $\Leftarrow$ is easy enough for $2 \times 2$ 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 $\leq 0$, so all of the eigenvaules of $A$ must be positive. Thus Proposition 3.3.6 is proven once we have the following. $\square$

**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 $v_1, \dots, v_n$ 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 $\lambda_1, \lambda_2$, are $\leq 0$. Let $W = \operatorname{Span}(v_1, v_2)$, 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. $\square$

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 $A_\ell$ 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:

$$\begin{aligned} Q(a_1u_1 + a_2u_2, v_1) &= a_1Q(u_1, v_1) + a_2Q(u_2, v_1), \\ Q(u_1, b_1v_1 + b_2v_2) &= b_1Q(u_1, v_1) + b_2Q(u_1, v_2), \end{aligned} \tag{3.3.33}$$

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

$$Ae_j = \sum_\ell a_{j\ell}e_\ell, \quad \text{so} \ \ (Ae_j, e_k) = Q(e_j, e_k). \tag{3.3.36}$$

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 $\lambda_j$ 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 $\varepsilon_j$ 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*

$$\dim \widetilde{V}_0 \le p \quad \text{and} \quad \dim \widetilde{V}_1 \le q. \tag{3.3.45}$$

**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

$$Q(u,u) > 0 \quad \text{and} \quad Q(u,u) < 0, \tag{3.3.46}$$

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 $T \in \mathrm{Skew}(V)$ if and only if $T^* = -T$. (Compare (3.3.7).) Show that

$$S, T \in \mathrm{Skew}(V) \Longrightarrow [S, T] \in \mathrm{Skew}(V),$$

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 $f : \mathrm{Spec}(T) \to \mathbb{C}$, 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 $T = T^* \in \mathcal{L}(V)$, $\mathrm{Spec}\, T = \{\lambda_j\}, E_j = \mathcal{E}(T, \lambda_j)$, 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

$$Au_j = \lambda_j J u_j, \quad 1 \le j \le k,\ \lambda_j \in \mathbb{R}.$$

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

$$(Ju_j, u_\ell) = 0, \quad \text{for} \ \ j \ne \ell.$$

Show that

$$\langle u_j, u_\ell\rangle = \langle u_j, Ju_\ell\rangle = \langle Ju_j, Ju_\ell\rangle = 0, \quad \text{for} \ \ j \ne \ell.$$

Then show that

$$\{u_j, Ju_j : 1 \le j \le k\} \ \text{ is an orthonormal basis of } V,$$

with respect to $\langle\ ,\ \rangle$. With respect to this basis,

$$Au_j = \lambda_j J u_j, \quad AJu_j = -\lambda_j u_j.$$

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 $\lambda_j$ 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. $\square$

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 $\overline{\lambda}_k^{-1} = \lambda_k$. $\square$

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

$$\|u\| = \|v\| \quad \text{and} \quad u \perp v. \tag{3.4.15}$$

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 $\theta$, uniquely determined up to an additive multiple of $2\pi$, 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 $\theta$.

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 $A = I$. $\square$

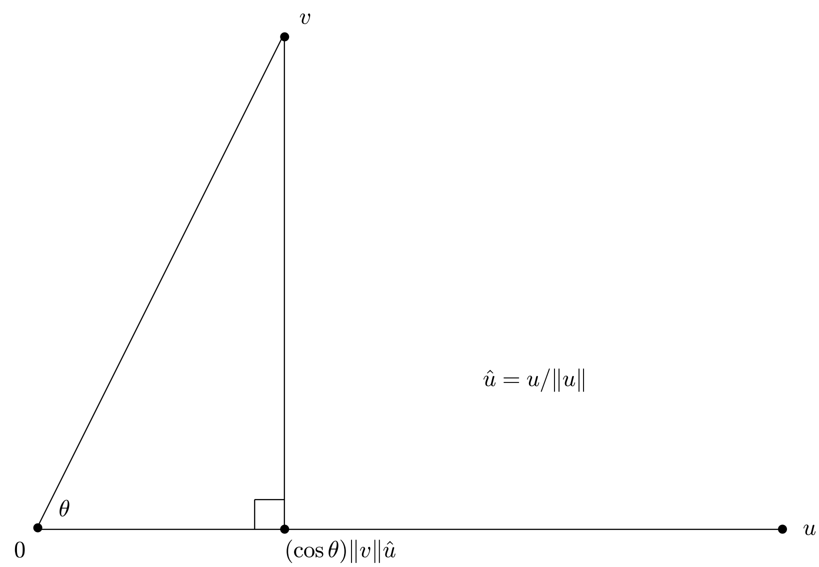


**Figure 3.4.1.** The cosine of an angle

## Exercises

1. Let $V$ be a real inner product space. Consider nonzero vectors $u, v \in V$. Show that the *angle* $\theta$ between these vectors is uniquely defined by the formula

$$(u, v) = \|u\| \cdot \|v\| \cos\theta, \quad 0 \le \theta \le \pi.$$

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 $\theta$ between $u$ and $v$ is given by

$$\begin{aligned} \theta = \varphi \qquad & \text{if } \ 0 \le \varphi \le \pi, \\ 2\pi - \varphi \quad & \text{if } \ \pi \le \varphi < 2\pi. \end{aligned}$$

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 $\mathbb{R}^3$. One might reconsider these when reading Section 8.1.

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 $\Pi$ is bilinear is to say $\Pi(u, v)$ is linear in both $u$ and $v$.

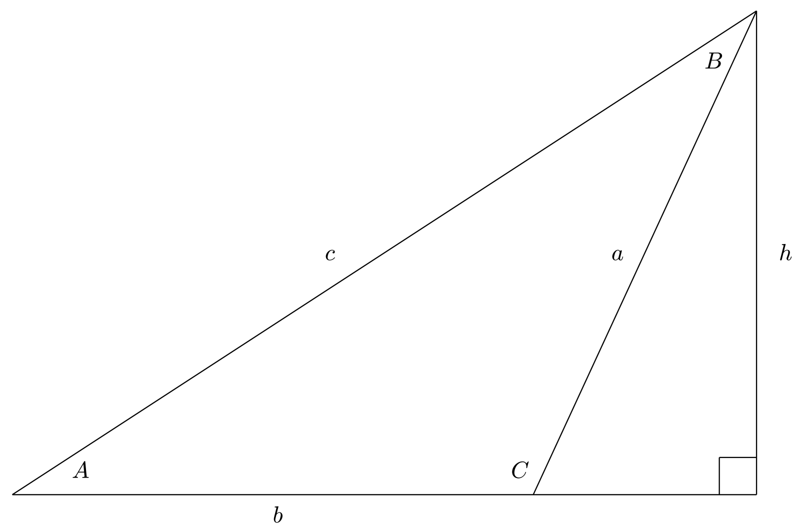


**Figure 3.4.2.** Law of Sines

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

$$u \times v = \det \begin{pmatrix} i & u_1 & v_1 \\ j & u_2 & v_2 \\ k & u_3 & v_3 \end{pmatrix} = \begin{pmatrix} u_2v_3 - u_3v_2 \\ u_3v_1 - u_1v_3 \\ u_1v_2 - u_2v_1 \end{pmatrix}. \tag{3.4.33}$$

6. Recall that $T \in SO(3)$ provided that $T$ is a real $3 \times 3$ 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 $3 \times 3$ matrix in (3.4.32) on the left by $T$.

7. Show that, if $\theta$ 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 $u, v, w, x \in \mathbb{R}^3$,

$$(3.4.36)\qquad \begin{aligned}(u \times v) \cdot (w \times x) &= (u \cdot w)(v \cdot x) - (u \cdot x)(v \cdot w) \\ &= \det \begin{pmatrix} u \cdot w & u \cdot x \\ v \cdot w & v \cdot x \end{pmatrix}.\end{aligned}$$

*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 $3 \times 3$ matrices, given by

$$(3.4.37)\qquad \kappa(y) = \begin{pmatrix} 0 & -y_3 & y_2 \\ y_3 & 0 & -y_1 \\ -y_2 & y_1 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix},$$

satisfies

$$(3.4.38)\qquad \kappa(y)x = y \times x.$$

Show that, with $[A, B] = AB - BA$,

$$(3.4.39)\qquad \begin{aligned}\kappa(x \times y) &= \big[\kappa(x), \kappa(y)\big], \\ \mathrm{Tr}\,\big(\kappa(x)\kappa(y)^t\big) &= 2x \cdot y.\end{aligned}$$

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 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

$$\mathcal{C} : \mathrm{Skew}(V) \longrightarrow \{A \in U(V) : -1 \notin \operatorname{Spec} A\}, \tag{3.4.42}$$

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

$$\mathcal{C} : \mathrm{Skew}(n) \longrightarrow \{A \in SO(n) : -1 \notin \operatorname{Spec} A\},$$

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 $1 \le j \le n$. 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

$$\mathcal{E}(T^*, 0) = \operatorname{Span}\left\{ \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \right\}. \tag{3.5.6}$$

Thus, in the notation of the proof of Lemma 3.5.3, we have $v_1 = (1, -2, 1)^t$. Hence

$$V_2 = (v_1)^\perp = \operatorname{Span}\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \right\}. \tag{3.5.7}$$

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*

$$
\sum_{j=1}^{n} |\lambda_j|^2 \le \|T\|_{\mathrm{HS}}^2. \tag{3.5.15}
$$

**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

$$\begin{aligned} \sum_{j=1}^{n} |\lambda_j|^2 &= \sum_{j=1}^{n} |a_{jj}|^2 \\ &\le \sum_{j,k} |a_{jk}|^2 \\ &= \|A\|_{\mathrm{HS}}^2 = \|T\|_{\mathrm{HS}}^2. \end{aligned} \tag{3.5.16}$$

□

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* $\{\lambda_1, \dots, \lambda_n\}$ *are the roots of the polynomial* $p(\lambda)$ *in* (3.5.17)*, then*

$$\sum_{k=1}^{n} |\lambda_k|^2 \le n - 1 + \sum_{j=0}^{n-1} |a_j|^2. \tag{3.5.20}$$

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 $\Phi$ 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 $\lambda_j$ 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*

$$A = KP, \quad K \in O(n), \quad P = P^*, \quad \textit{positive definite.} \tag{3.6.8}$$

**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

$$\|Pv\|^2 = (P^2 v, v) = (A^* A v, v) = \|Av\|^2, \tag{3.6.9}$$

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

$$V_0 = \mathcal{R}(P) = \operatorname{Span}\{v_j : \lambda_j > 0\}, \quad V_1 = \mathcal{N}(P) = \mathcal{N}(A), \tag{3.6.10}$$

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

$$K_0 P v = Av, \quad \forall\, v \in V_0, \tag{3.6.12}$$

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. $\square$

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

$$\begin{aligned} A^*A &= \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix} = P^2, \quad \text{with} \\ P &= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}. \end{aligned} \tag{3.6.17}$$

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

$$\begin{aligned} A^*A &= \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} = P^2, \quad \text{with} \\ P &= \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}. \end{aligned} \tag{3.6.20}$$

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

$$K_0 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2} A \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{3.6.23}$$

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

$$\begin{aligned}K\begin{pmatrix}1\\0\end{pmatrix}&=\tfrac{1}{2}K_0\begin{pmatrix}1\\1\end{pmatrix}+\tfrac{1}{2}K_1\begin{pmatrix}1\\-1\end{pmatrix},\\ K\begin{pmatrix}0\\1\end{pmatrix}&=\tfrac{1}{2}K_0\begin{pmatrix}1\\1\end{pmatrix}-\tfrac{1}{2}K_1\begin{pmatrix}1\\-1\end{pmatrix}.\end{aligned} \tag{3.6.26}$$

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*

$$A=UDV^*,\quad U,V\in U(n),\quad D\in M(n,\mathbb{C})\ \ \textit{diagonal}, \tag{3.6.28}$$

*in fact,*

$$D=\begin{pmatrix}d_1&&\\&\ddots&\\&&d_n\end{pmatrix},\quad d_j\ge 0. \tag{3.6.29}$$

*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

$$\begin{gathered} \mathcal{E}(AA^*, 3) = \operatorname{Span} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \mathcal{E}(AA^*, 2) = \operatorname{Span} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \\ \mathcal{E}(AA^*, 0) = \operatorname{Span} \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}. \end{gathered} \tag{3.6.46}$$

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*

$$j > J \Longrightarrow d_j \le \delta. \tag{3.6.49}$$

*Define* $A_J : \mathbb{C}^n \to \mathbb{C}^m$ *by*

$$A_J w = \sum_{j \le J} d_j (w, v_j) u_j. \tag{3.6.50}$$

*Then*

$$\|A - A_J\| \le \delta. \tag{3.6.51}$$

**Proof.** We have

$$\begin{aligned} \|(A - A_J)w\|^2 &= \sum_{j>J} d_j^2 |(w, v_j)|^2 \\ &\le \delta^2 \|w\|^2. \end{aligned} \tag{3.6.52}$$

□

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 $2000 \times 2000$ 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 $d_j \ge 0$, arranged in decreasing order, $d_j \searrow$. For a discussion of how this can be done, see [**6**].

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 [**22**].

## 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 $\leq 2$, 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 [**23**]). 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,

$$x_0 = v, \quad x_1 = Av, \quad x_2 = \frac{1}{2} A^2 v, \ \dots, \quad x_k = \frac{1}{k!} A^k v, \dots, \tag{3.7.6}$$

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

$$\frac{d}{dt}\bigl(B(t)X(t)\bigr) = B'(t)X(t) + B(t)X'(t) \tag{3.7.12}$$

to $B(t) = e^{-tA}$ and $X(t)$ as in (3.7.11). Thus, via (3.7.10), with $A$ replaced by $-A$,

$$\frac{d}{dt}\bigl(e^{-tA}X(t)\bigr) = -e^{-tA}AX(t) + e^{-tA}AX(t) = 0, \tag{3.7.13}$$

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

$$\frac{d}{dt}\bigl(e^{(s+t)A}e^{-tA}\bigr) = e^{(s+t)A}Ae^{-tA} - e^{(s+t)A}Ae^{-tA} = 0, \tag{3.7.17}$$

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,

$$\begin{aligned} \frac{d}{dt}\big(e^{t(A+B)} e^{-tB} e^{-tA}\big) = e^{t(A+B)}&(A+B) e^{-tB} e^{-tA} \\ &- e^{t(A+B)} B e^{-tB} e^{-tA} \\ &- e^{t(A+B)} e^{-tB} A e^{-tA}. \end{aligned} \tag{3.7.22}$$

Next, we note that, for $s \in \mathbb{R}$,

$$e^{sB} A = \sum_{k=0}^{\infty} \frac{s^k}{k!} B^k A = \sum_{k=0}^{\infty} \frac{s^k}{k!} A B^k, \tag{3.7.23}$$

provided $A$ and $B$ commute, so

$$AB = BA \Longrightarrow e^{sB} A = A e^{sB},\ \forall\, s \in \mathbb{R}. \tag{3.7.24}$$

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). $\square$

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 $\lambda$, 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,

$$A = C^{-1} B C \Rightarrow A^k = C^{-1} B^k C \Rightarrow e^{tA} = C^{-1} e^{tB} C. \tag{3.7.27}$$

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 $\lambda I$ 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 $\le \ell$, 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 $v = c_1 v_1 + \cdots + c_n v_n$. Then

$$e^{tA}v = c_1 e^{tA} v_1 + \cdots + c_n e^{tA} v_n. \tag{3.7.35}$$

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 $j$th column of $e^{tA}$ is $e^{tA}e_j$, where $e_j$ is the $j$th 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
(3.7.39)

$$\mathcal{E}(A, 0) = \operatorname{Span} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad \mathcal{E}(A, 1) = \operatorname{Span} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \mathcal{E}(A, 2) = \operatorname{Span} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Hence
(3.7.40)

$$e^{tA} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad e^{tA} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = e^t \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad e^{tA} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = e^{2t} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

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 Spec $A=\{0,1\}$, and 0 is a double root of the characteristic polynomial of $A$. We have

$$\mathcal{E}(A,1)=\text{Span}\begin{pmatrix}0\\1\\0\end{pmatrix},\quad \mathcal{E}(A,0)=\text{Span}\begin{pmatrix}1\\0\\-1\end{pmatrix}, \tag{3.7.45}$$

and, noting that

$$A^2=\begin{pmatrix}0 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{pmatrix}, \tag{3.7.46}$$

we have

$$\mathcal{GE}(A,0)=\text{Span}\Big\{\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\end{pmatrix}\Big\}. \tag{3.7.47}$$

Hence

$$\begin{aligned} v\in\mathcal{GE}(A,0)\Rightarrow e^{tA}v&=(I+tA)v\\ &=\begin{pmatrix}1+t & 0 & t\\ 0 & 1+t & 0\\ -t & 0 & 1-t\end{pmatrix}v. \end{aligned} \tag{3.7.48}$$

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 $\lambda$s. 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 $\le m$ 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 $\le m$. (If $\alpha = 0$, one also gets* (3.7.56)*, with $q(t)$ of degree $\le m+1$.)*

**Proof.** The map $p = Tq$ defined by

$$\frac{d}{dt}\bigl(q(t)e^{\alpha t}\bigr) = p(t)e^{\alpha t} \tag{3.7.57}$$

is a linear map on the $(m+1)$-dimensional vector space $\mathcal{P}_m$ of polynomials of degree $\le m$. 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 $\lambda_j$s 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 $\lambda_j$ 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 $G_{\lambda_j}$ is invariant under $A$, and*

$$A_j = A\big|_{G_{\lambda_j}} \quad \text{has exactly one eigenvalue}, \lambda_j. \tag{3.7.62}$$

**Proof.** The decomposition (3.7.61) follows directly from Proposition 3.7.2. The invariance of $G_{\lambda_j}$ 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*

$$N^m = 0 \text{ for some } m \le k. \tag{3.7.65}$$

**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

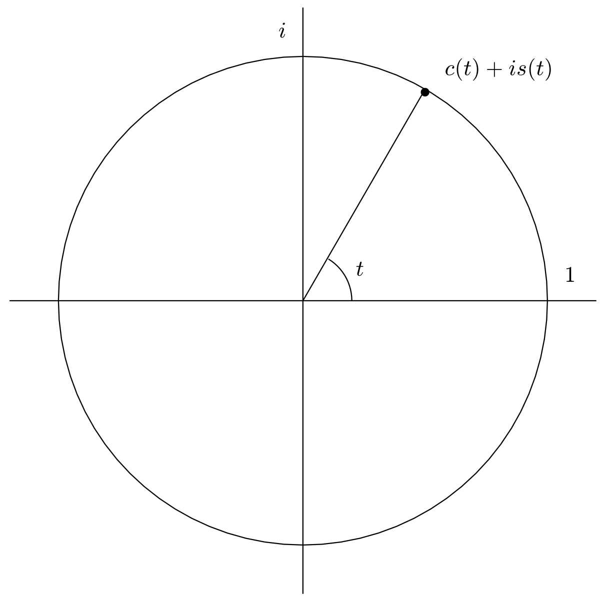


**Figure 3.7.1.** The circle $e^{it} = c(t) + is(t)$

between the two rays described above, and if we write $\gamma(t)$ in terms of its real and imaginary parts as $\gamma(t) = c(t) + is(t)$, 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.

## 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 $n$th 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 $n$th 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 $\lambda_j$ is a root of $p(\lambda)$ of multiplicity $k_j$, show that the $n$th 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 $A, B \in M(n, \mathbb{C})$,*

$$e^{t(A+B)} = e^{tA} e^{tB} \quad \forall\, t \in \mathbb{R} \Longrightarrow AB = BA.$$

*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

$$Z(s) = e^{sB} A e^{-sB}.$$

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 $\omega^j$-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 $\omega^m \ne 1$ implies this sum vanishes, hence if $j \ne \ell$ 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

$$\|f * g\| \le \Bigl(\max_j |\hat{f}(j)|\Bigr) \|g\|. \tag{3.8.31}$$

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 [**26**] 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

$$\begin{aligned} a * b &= \mathcal{F}^{-1}\bigl((\mathcal{F}a)(\mathcal{F}b)\bigr) \\ &= n\mathcal{F}^*\bigl((\mathcal{F}a)(\mathcal{F}b)\bigr). \end{aligned} \tag{3.8.36}$$

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 $\omega^{-m}$ 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

$$\begin{aligned} f_0(\ell) &= f(\ell) + f(\ell + n/2), \qquad (3.8.50)\\ f_1(\ell) &= \omega^{-\ell}[f(\ell) - f(\ell + n/2)], \quad \omega = e^{2\pi i/n}. \qquad (3.8.51) \end{aligned}$$

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 $\ell$ 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 $\omega$ replaced by $\omega^2$. 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 $\omega_m$ 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:*

$$e_0 \equiv 1, \quad \sqrt{2}c_j, \ \sqrt{2}s_j, \ \ 1 \leq j < \frac{n}{2}, \tag{3.8.78}$$

*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,

$$
\hat{f}_c\Bigl(\frac{n}{2}\Bigr) = (f, e_{n/2}) = \frac{1}{n} \sum_{k\in\mathbb{Z}/(n)} (-1)^k f(k). \tag{3.8.91}
$$

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

$$
\|f\|^2 = |\hat{f}_c(0)|^2 + 2 \sum_{1\le j<n/2} \Bigl\{ |\hat{f}_c(j)|^2 + \hat{f}_s(j)|^2 \Bigr\}, \tag{3.8.93}
$$

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

$$\begin{aligned} \delta_j(k) = 1&, \quad \text{if } j = k \text{ in } \mathbb{Z}/(n), \\ 0&, \quad \text{otherwise.} \end{aligned}$$

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

$$\begin{aligned} \mathcal{F}_c(f * g)(j) &= \hat{f}_c(j)\hat{g}_c(j) - \hat{f}_s(j)\hat{g}_s(j), \\ \mathcal{F}_s(f * g)(j) &= \hat{f}_c(j)\hat{g}_s(j) + \hat{f}_s(j)\hat{g}_c(j). \end{aligned}$$

*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
$$\mathcal{F}\partial_+ = M_{e_1 - 1}\mathcal{F}, \quad \mathcal{F}\partial_- = M_{1-\bar{e}_1}\mathcal{F}.$$

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 $\Phi$ 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 $\Phi$, 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 $\geq 0$, 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:

$$\langle a_1 e_1 + \cdots + a_n e_n, w \rangle = \sum a_j w_j, \quad w_j = \langle e_j, w \rangle. \tag{4.1.4}$$

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,

$$\begin{gathered} \operatorname{Spec} A^t = \operatorname{Spec} A, \quad \dim \mathcal{E}(A^t, \lambda) = \dim \mathcal{E}(A, \lambda), \\ \text{and} \quad \dim \mathcal{GE}(A^t, \lambda) = \dim \mathcal{GE}(A, \lambda). \end{gathered}$$

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 $\le n$. 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 $\{\delta_k : 0 \le k \le n\}$ 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 $\{q_k(x) = x^k : 0 \le k \le n\}$ of $\mathcal{P}_n$, express the dual basis $\{\varepsilon_k : 0 \le k \le n\}$ 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 $\iota$ coincides with

$$\iota^t : V \longrightarrow V',$$

where we identify $V''$ with $V$ as in (4.1.9), and the property that

$$0 \ne u \in V \Longrightarrow \langle u, \iota(u) \rangle > 0.$$

## 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 [**23**]. As for the uniqueness, if $p \notin K$ and $q, q' \in K$ satisfy

$$|q - p| = |q' - p|, \tag{4.2.3}$$

and if $q \ne q'$, 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*

$$\begin{aligned} &\alpha(p) > \alpha_0, \quad \alpha(x) \le \alpha_0, \ \forall\, x \in K, \ \textit{and} \\ &\alpha(q) = \alpha_0 \ \textit{for some } q \in K. \end{aligned} \tag{4.2.6}$$

**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 $\alpha_0 = (q, p - q)$. $\square$

**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

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*

$$\sum a_j x_j, \quad x_j \in E, \quad a_j \ge 0, \quad \sum a_j = 1. \tag{4.2.9}$$

*Then $F = K$.*

We first need to show that $E \neq \emptyset$. The following will be a convenient tool.

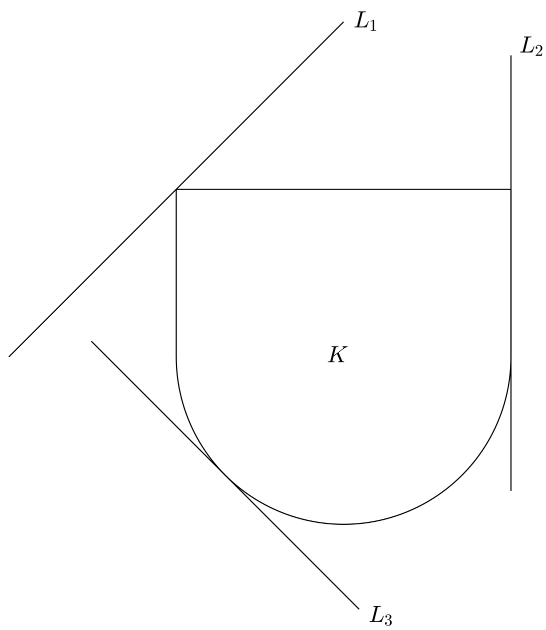


**Figure 4.2.1.** Convex set $K$ and three supporting hyperplanes

**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 $K$. □

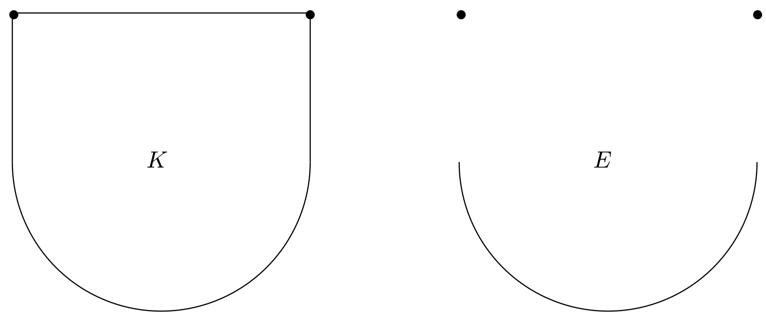


**Figure 4.2.2.** Convex set $K$, and its extreme points, $E$

**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

$$\alpha(p) > \alpha_0, \quad \alpha(x) \le \alpha_0, \ \forall\, x \in F. \tag{4.2.10}$$

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. $\square$

## 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 $\Sigma$. 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 $\gamma$ 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 $\|A\| \le 1$. 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 $\le 1$. 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 $\dim W = m \le n$ (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 $\Pi$:

$$\Pi : V \longrightarrow V/W, \quad \Pi v = [v]. \tag{4.3.8}$$

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 $\gamma$ 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 $\gamma$ in (4.3.17) is also surjective. To summarize,

**Proposition 4.3.4.** *The map $\gamma$ 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 $\Sigma$ 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 $\Phi$ 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 $\Phi$ 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 [**24**]. 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*

$$w \in \overset{\circ}{C}{}_+^n \quad \textit{and} \quad \mu > 0 \quad \textit{such that} \quad A^t w = \mu w. \tag{4.4.14}$$

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 $\mu = \lambda$. $\square$

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 $\Sigma$ 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 $\le 1$.

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

$$v \in \mathbb{R}^n, \quad v \notin \operatorname{Span} \mathbf{1} \Longrightarrow \|Av\|_\infty < \|v\|_\infty. \tag{4.4.28}$$

$\square$

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 $\lambda$-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, $\lambda$ 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 $\lambda$ 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. $\square$

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 $v \in \mathbb{R}^n$,*

$$A^k v \longrightarrow \mathcal{P}v, \quad \text{as} \ \ k \to \infty. \tag{4.4.31}$$

**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

$$\|A^\ell B_V^j (I-\mathcal{P})v\|_\infty \le \beta^j \|(I-\mathcal{P})v\|_\infty. \tag{4.4.34}$$

This completes the proof. $\square$

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

$$\|(A^\ell B_V^j (I-\mathcal{P}))^t\|_1 = \|A^\ell B_V^j(I-\mathcal{P})\|_\infty \le \beta^j \|I-\mathcal{P}\|_\infty. \tag{4.4.37}$$

Note also that $\mathcal{P}^t$ is the projection of $\mathbb{R}^n$ onto 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

$$\frac{d}{dt} Z_\varepsilon(t) = X Z_\varepsilon(t) + \varepsilon Y Z_\varepsilon(t), \quad Z_\varepsilon(0) = I, \tag{4.4.47}$$

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 [**19**].

## 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 $\Sigma$ 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

$$T w_n = w_n + \frac{1}{n}(v_n - v_0).$$

Since $\Sigma \subset \mathbb{R}^n$ is closed and bounded, $\{w_n\}$ has a convergent subsequence, $w_{n_j} \to w \in \Sigma$. (See [**23**], Chapter 2, for a proof.) Show that

$$Tw = w.$$

Compare this with the production of $\mathbf{p}$ in (4.4.19).

Chapter 5

# Multilinear algebra

Depending on perspective, one can say that multilinear algebra is an extension of linear algebra or that it is part of linear algebra. It is our goal to develop both perspectives here.

Section 5.1 treats multilinear maps, bringing in

$$\mathcal{M}(V_1, \dots, V_\ell; W), \tag{5.0.1}$$

the space of maps $\beta : V_1 \times \cdots \times V_\ell \to W$ that are linear in each variable. The first example of such a map arose in §1.5,

$$\det : \mathbb{F}^n \times \cdots \times \mathbb{F}^n \longrightarrow \mathbb{F}, \tag{5.0.2}$$

with $\ell = n,\ V_j = \mathbb{F}^n$. In this case, $V_1 = \cdots = V_\ell = V$ (which equals $\mathbb{F}^n$), and the resulting special case of (5.0.1) is denoted

$$\mathcal{M}^\ell(V, W). \tag{5.0.3}$$

The determinant det provides an element of

$$\mathrm{Alt}^\ell(V, W), \tag{5.0.4}$$

with $\ell = n, V = \mathbb{F}^n, W = \mathbb{F}$, where an element of (5.0.4) is a multilinear map $\beta(v_1, \dots, v_\ell)$ that changes sign when two elements, e.g., $v_j$ and $v_k$ with $j \neq k$, are interchanged.

In §5.2 we treat tensor products. If $V_j$ are finite-dimensional vector spaces, of dimension $d_j$, then $V_1 \otimes \cdots \otimes V_\ell$ is a vector space, of dimension $d_1 \cdots d_\ell$, for which we have a natural isomorphism

$$\mathcal{M}(V_1, \dots, V_\ell; W) \xrightarrow{\approx} \mathcal{L}(V_1 \otimes \cdots \otimes V_\ell, W), \tag{5.0.5}$$

for each vector space $W$. This tensor product construction ties together linear algebra and multilinear algebra.

Section 5.3 treats exterior algebra, which provides a natural algebraic extension of the theory of the determinant described in §1.5. If $V$ is a finite-dimensional vector space over $\mathbb{F}$, we set $\Lambda^0 V' = \mathbb{F}$, $\Lambda^1 V' = V'$, and, generally,

$$\Lambda^k V' = \mathrm{Alt}^k(V, \mathbb{F}). \tag{5.0.6}$$

This sequence of vector spaces carries a wedge product,

$$\alpha \in \Lambda^k V', \ \beta \in \Lambda^\ell V' \Longrightarrow \alpha \wedge \beta \in \Lambda^{k+\ell} V'. \tag{5.0.7}$$

Topics treated in §5.2 include an approach to Cramer's formula, first established in §1.5, given here in terms of the structure of the exterior algebra. In the exercises we also treat an extension of Cramer's formula, due to Jacobi, using exterior algebra.

Results from exterior algebra are important in the development of the theory of differential forms, as a tool in multivariable calculus. Such a development is given in Chapters 4–6 of [**24**].

In §5.4 we establish an isomorphism

$$\mathrm{Skew}(n) \approx \Lambda^2 \mathbb{R}^n, \tag{5.0.8}$$

and use this, when $n = 2k$ is even, to produce a map called the *Pfaffian*

$$\mathrm{Pf} : \mathrm{Skew}(2k) \longrightarrow \mathbb{R}, \tag{5.0.9}$$

satisfying the remarkable identities

$$\begin{aligned} \mathrm{Pf}(A)^2 &= \det A, \\ \mathrm{Pf}(B^t A B) &= (\det B)\, \mathrm{Pf}(A), \end{aligned} \tag{5.0.10}$$

for $A \in \mathrm{Skew}(2k)$, $B \in \mathcal{L}(\mathbb{R}^{2k})$. One notable consequence of the latter identity is that the Pfaffian is invariant under conjugation by elements of $SO(2k)$, but not invariant under conjugation by other elements of $O(2k)$.

## 5.1. Multilinear mappings

If $V_1, \dots, V_\ell$ and $W$ are vector spaces over $\mathbb{F}$, we set

$$\begin{aligned} \mathcal{M}(V_1, \dots, V_\ell; W) = \text{set of mappings } \ \beta : V_1 \times \cdots \times V_\ell \to W \\ \text{that are linear in each variable.} \end{aligned} \tag{5.1.1}$$

That is, for each $j \in \{1, \dots, \ell\}$,

$$\begin{aligned} &v_j, w_j \in V_j, \ a, b \in \mathbb{F} \Longrightarrow \\ &\qquad \beta(u_1, \dots, av_j + bw_j, \dots, u_\ell) \\ &\qquad = a\beta(u_1, \dots, v_j, \dots, u_\ell) + b\beta(u_1, \dots, w_j, \dots, u_\ell). \end{aligned} \tag{5.1.2}$$

This has the natural structure of a vector space, and one readily computes that

$$\dim \mathcal{M}(V_1, \dots, V_\ell; W) = (\dim V_1) \cdots (\dim V_\ell)(\dim W). \tag{5.1.3}$$

If $\{e_{j,1}, \dots, e_{j,d_j}\}$ is a basis of $V_j$ (of dimension $d_j$), then $\beta$ is uniquely determined by the elements

$$\begin{aligned} &b_j \in W, \quad b_j = \beta(e_{1,j_1}, \dots, e_{\ell,j_\ell}\}, \\ &j = (j_1, \dots, j_\ell), \quad 1 \le j_\nu \le d_\nu. \end{aligned} \tag{5.1.4}$$

In many cases of interest, all the $V_j$ are the same. Then we set

$$\mathcal{M}^\ell(V, W) = \mathcal{M}(V_1, \dots, V_\ell; W), \quad V_1 = \cdots = V_\ell = V. \tag{5.1.5}$$

This is the space of $\ell$-linear maps from $V$ to $W$. It has two distinguished subspaces,

$$\mathrm{Sym}^\ell(V, W), \quad \mathrm{Alt}^\ell(V, W), \tag{5.1.6}$$

where, given $\beta \in \mathcal{M}^\ell(V, W)$,

$$\begin{aligned} &\beta \in \mathrm{Sym}^\ell(V, W) \Longleftrightarrow \\ &\beta(v_1, \dots, v_j, \dots, v_k, \dots, v_\ell) = \beta(v_1, \dots, v_k, \dots, v_j, \dots, v_\ell), \\ &\beta \in \mathrm{Alt}^\ell(V, W) \Longleftrightarrow \\ &\beta(v_1, \dots, v_j, \dots, v_k, \dots, v_\ell) = -\beta(v_1, \dots, v_k, \dots, v_j, \dots, v_\ell), \end{aligned} \tag{5.1.7}$$

whenever $1 \le j < k \le \ell$.

We mention some examples of multilinear maps that have arisen earlier in this text. In §1.5 we saw $\vartheta = \det : M(n, \mathbb{F}) \to \mathbb{F}$ as an element

$$\vartheta \in \mathrm{Alt}^n(\mathbb{F}^n, \mathbb{F}), \tag{5.1.8}$$

in Proposition 1.5.1. As put there, for $A \in M(n, \mathbb{F})$, $\det A$ is linear in each column of $A$ and changes sign upon switching any two columns. In §3.4 we came across the cross product

$$\kappa \in \mathrm{Alt}^2(\mathbb{R}^3, \mathbb{R}^3), \quad \kappa(u, v) = u \times v, \tag{5.1.9}$$

defined by (3.4.32). Other examples of multilinear maps include the matrix product

$$\Pi \in \mathcal{M}^2(M(n,\mathbb{F}), M(n,\mathbb{F})), \quad \Pi(A,B) = AB, \tag{5.1.10}$$

and the matrix commutator,

$$\mathcal{C} \in \mathrm{Alt}^2(M(n,\mathbb{F}), M(n,\mathbb{F})), \quad \mathcal{C}(A,B) = AB - BA, \tag{5.1.11}$$

and anticommutator,

$$\mathcal{A} \in \mathrm{Sym}^2(M(n,\mathbb{F}), M(n,\mathbb{F})), \quad \mathcal{A}(A,B) = AB + BA. \tag{5.1.12}$$

Considerations of multilinear maps lead naturally to material treated in the next two sections, namely tensor products and exterior algebra. In §5.2 we define the tensor product $V_1 \otimes \cdots \otimes V_\ell$ of finite-dimensional vector spaces and describe a natural isomorphism

$$\mathcal{M}(V_1, \dots, V_\ell; W) \approx \mathcal{L}(V_1 \otimes \cdots \otimes V_\ell, W). \tag{5.1.13}$$

In §5.3 we discuss spaces $\Lambda^k V$ and describe a natural isomorphism

$$\mathrm{Alt}^k(V, W) \approx \mathcal{L}(\Lambda^k V, W). \tag{5.1.14}$$

## Exercises

1. If $V$ and $W$ are finite dimensional vector spaces over $\mathbb{F}$, produce a natural isomorphism

$$\mathcal{M}(V, W; \mathbb{F}) \approx \mathcal{L}(V, W').$$

2. More generally, if $V_j$ and $W$ are finite dimensional, produce a natural isomorphism

$$\mathcal{M}(V_1, \dots, V_k, W; \mathbb{F}) \approx \mathcal{M}(V_1, \dots, V_k; W').$$

3. Take $V_1 = V_2 = W = \mathbb{R}^3$ and draw a connection between the cross product (5.1.9) and Exercise 2.

4. Let $\mathcal{H}_{n,k}$ denote the space of polynomials in $(x_1, \dots, x_n)$ (with coefficients in $\mathbb{F}$) that are homogeneous of degree $k$. Produce an isomorphism

$$\mathcal{H}_{n,k} \approx \mathrm{Sym}^k(\mathbb{F}^n, \mathbb{F}).$$

5. If $\dim V = n$, specify the dimensions of
$$\mathcal{M}^k(V, \mathbb{F}), \quad \mathrm{Sym}^k(V, \mathbb{F}), \quad \mathrm{Alt}^k(V, \mathbb{F}).$$

6. Show that
$$\mathcal{M}^2(V, \mathbb{F}) = \mathrm{Sym}^2(V, \mathbb{F}) \oplus \mathrm{Alt}^2(V, \mathbb{F}).$$

7. What can you say about
$$\mathcal{M}^3(V, \mathbb{F}) / (\mathrm{Sym}^3(V, \mathbb{F}) \oplus \mathrm{Alt}^3(V, \mathbb{F}))?$$

## 5.2. Tensor products

Here all vector spaces will be finite-dimensional vector spaces over $\mathbb{F}$ ($\mathbb{R}$ or $\mathbb{C}$).

**Definition.** Given vector spaces $V_1, \dots, V_\ell$, the tensor product $V_1 \otimes \cdots \otimes V_\ell$ is the space of $\ell$-linear maps

$$\beta : V_1' \times \cdots \times V_\ell' \longrightarrow \mathbb{F}. \tag{5.2.1}$$

Given $v_j \in V_j$, we define $v_1 \otimes \cdots \otimes v_\ell \in V_1 \otimes \cdots \otimes V_\ell$ by

$$(v_1 \otimes \cdots \otimes v_\ell)(w_1, \dots, w_\ell) = \langle v_1, w_1 \rangle \cdots \langle v_\ell, w_\ell \rangle, \quad w_j \in V_j'. \tag{5.2.2}$$

If $\{e_{j,1}, \dots, e_{j,d_j}\}$ is a basis of $V_j$ (of dimension $d_j$), with dual basis $\{\varepsilon_{j,1}, \dots, \varepsilon_{j,d_j}\}$ for $V_j'$, then $\beta$ in (5.2.1) is uniquely determined by the numbers

$$b_j = \beta(\varepsilon_{1,j_1}, \dots, \varepsilon_{\ell,j_\ell}\}, \quad j = (j_1, \dots, j_\ell),\ 1 \le j_\nu \le d_\nu. \tag{5.2.3}$$

It follows that

$$\dim V_1 \otimes \cdots \otimes V_\ell = d_1 \cdots d_\ell, \tag{5.2.4}$$

and a basis of $V_1 \otimes \cdots \otimes V_\ell$ is given by

$$e_{1,j_1} \otimes \cdots \otimes e_{\ell,j_\ell}, \quad 1 \le j_\nu \le d_\nu. \tag{5.2.5}$$

The following is a universal property for the tensor product.

**Proposition 5.2.1.** *Given vector spaces $V_j$ and $W$, there is a natural isomorphism*

$$\Phi : \mathcal{M}(V_1, \dots, V_\ell; W) \xrightarrow{\approx} \mathcal{L}(V_1 \otimes \cdots \otimes V_\ell, W). \tag{5.2.6}$$

**Proof.** Given an $\ell$-linear map

$$\alpha : V_1 \times \cdots \times V_\ell \longrightarrow W, \tag{5.2.7}$$

the map $\Phi\alpha : V_1 \otimes \cdots \otimes V_\ell \to W$ should satisfy

$$\Phi\alpha(v_1 \otimes \cdots \otimes v_\ell) = \alpha(v_1, \dots, v_\ell), \quad v_j \in V_j. \tag{5.2.8}$$

In fact, in terms of the basis (5.2.5) of $V_1 \otimes \cdots \otimes V_\ell$, we can specify that

$$\Phi\alpha(e_{1,j_1} \otimes \cdots \otimes e_{\ell,j_\ell}) = \alpha(e_{1,j_1}, \dots, e_{\ell,j_\ell}), \quad 1 \le j_\nu \le d_\nu, \tag{5.2.9}$$

and then extend $\Phi\alpha$ by linearity. Such an extension uniquely defines $\Phi\alpha \in \mathcal{L}(V_1 \otimes \cdots \otimes V_\ell, W)$, and it satisfies (5.2.8). In light of this, it follows that the construction of $\Phi\alpha$ is independent of the choice of bases of $V_1, \dots, V_\ell$. We see that $\Phi$ is then injective. In fact, if $\Phi\alpha = 0$, then (5.2.9) is identically 0, so $\alpha = 0$. Since $\mathcal{M}(V_1, \dots, V_\ell; W)$ and $\mathcal{L}(V_1 \otimes \cdots \otimes V_\ell, W)$ both have dimension $d_1 \cdots d_\ell(\dim W)$, the isomorphism property of $\Phi$ follows. □

We next note that linear maps $A_j : V_j \to W_j$ naturally induce a linear map

$$A_1 \otimes \cdots \otimes A_\ell : V_1 \otimes \cdots \otimes V_\ell \longrightarrow W_1 \otimes \cdots \otimes W_\ell, \tag{5.2.10}$$

as follows. If $\omega_j \in W_j'$, and $\beta : V_1' \times \cdots \times V_\ell' \to \mathbb{F}$ defines $\beta \in V_1 \otimes \cdots \otimes V_\ell$, then

$$(A_1 \otimes \cdots \otimes A_\ell)\beta(\omega_1, \dots, \omega_\ell) = \beta(A_1^t \omega_1, \dots, A_\ell^t \omega_\ell), \tag{5.2.11}$$

with $A_j^t \omega_j \in V_j'$. One sees readily that, for $v_j \in V_j$,

$$(A_1 \otimes \cdots \otimes A_\ell)(v_1 \otimes \cdots \otimes v_\ell) = (A_1 v_1) \otimes \cdots \otimes (A_\ell v_\ell). \tag{5.2.12}$$

For notational simplicity, we now restrict attention to the case $\ell = 2$, i.e., to tensor products of two vector spaces. The following is straightforward. Compare Exercises 9–11 of §2.2.

**Proposition 5.2.2.** *Given $A \in \mathcal{L}(V)$, $B \in \mathcal{L}(W)$, inducing $A \otimes B \in \mathcal{L}(V \otimes W)$, suppose* $\operatorname{Spec} A = \{\lambda_j\}$ *and* $\operatorname{Spec} B = \{\mu_k\}$. *Then*

$$\operatorname{Spec} A \otimes B = \{\lambda_j \mu_k\}. \tag{5.2.13}$$

*Also,*

$$\begin{aligned} \mathcal{E}(A \otimes B, \sigma) = \operatorname{Span}\{v \otimes w : v \in \mathcal{E}(A, \lambda_j),& \\ w \in \mathcal{E}(B, \mu_k),\ \sigma = \lambda_j \mu_k\},& \end{aligned} \tag{5.2.14}$$

*and*

$$\begin{aligned} \mathcal{GE}(A \otimes B, \sigma) = \operatorname{Span}\{v \otimes w : v \in \mathcal{GE}(A, \lambda_j),& \\ w \in \mathcal{GE}(B, \mu_k),\ \sigma = \lambda_j \mu_k\}.& \end{aligned} \tag{5.2.15}$$

*Furthermore,*

$$\operatorname{Spec}(A \otimes I + I \otimes B) = \{\lambda_j + \mu_k\}, \tag{5.2.16}$$

*and we have*

$$\begin{aligned} \mathcal{E}(A \otimes I + I \otimes B, \tau) = \operatorname{Span}\{v \otimes w : v \in \mathcal{E}(A, \lambda_j),& \\ w \in \mathcal{E}(B, \mu_k),\ \tau = \lambda_j + \mu_k\},& \end{aligned} \tag{5.2.17}$$

*and*

$$\begin{aligned} \mathcal{GE}(A \otimes I + I \otimes B, \tau) = \operatorname{Span}\{v \otimes w : v \in \mathcal{GE}(A, \lambda_j),& \\ w \in \mathcal{GE}(B, \mu_k),\ \tau = \lambda_j + \mu_k\}.& \end{aligned} \tag{5.2.18}$$

## Exercises

1. If $V$ and $W$ are finite dimensional vector spaces, produce a natural isomorphism
$$\mathcal{L}(V, W) \approx V' \otimes W.$$

2. Prove Proposition 5.2.2.

3. With $A$ and $B$ as in Proposition 5.2.2, show that
$$\operatorname{Tr}(A \otimes B) = (\operatorname{Tr} A)(\operatorname{Tr} B),$$
$$\det(A \otimes B) = (\det A)^{d_W} (\det B)^{d_V},$$
where $d_V = \dim V,\ d_W = \dim W$.

4. Taking $W = \mathbb{F}$ in (5.2.6), show that there is a natural isomorphism
$$(V_1 \otimes \cdots \otimes V_\ell)' \approx V_1' \otimes \cdots \otimes V_\ell'.$$

5. Show that there exists a natural isomorphism
$$(V_1 \otimes \cdots \otimes V_k) \otimes (W_1 \otimes \cdots \otimes W_\ell) \approx V_1 \otimes \cdots \otimes V_k \otimes W_1 \otimes \cdots \otimes W_\ell.$$

6. Produce a natural isomorphism
$$V_1 \otimes (V_2 \otimes V_3) \approx (V_1 \otimes V_2) \otimes V_3.$$

7. Produce a natural isomorphism
$$\mathcal{L}(V_1 \otimes V_2, W_1 \otimes W_2) \approx \mathcal{L}(V_1, W_1) \otimes \mathcal{L}(V_2, W_2).$$

8. Determine various vector spaces that are naturally isomorphic to
$$\mathcal{L}(V_1 \otimes \cdots \otimes V_k, W_1 \otimes \cdots \otimes W_\ell).$$

9. Show that there exists a natural isomorphism
$$M : \mathcal{L}(V) \otimes \mathcal{L}(W) \xrightarrow{\approx} \mathcal{L}(\mathcal{L}(V, W)), \quad M(B \otimes A)T = ATB.$$

## 5.3. Exterior algebra

Let $V$ be a finite dimensional vector space over $\mathbb{F}$ ($\mathbb{R}$ or $\mathbb{C}$), with dual $V'$. We define the spaces $\Lambda^k V'$ as follows:

$$\Lambda^0 V' = \mathbb{F}, \quad \Lambda^1 V' = V', \tag{5.3.1}$$

and, for $k \geq 2$,

$$\begin{aligned} \Lambda^k V' = \text{set of } &k\text{-linear maps } \alpha : V \times \cdots \times V \to \mathbb{F} \\ &\text{that are anti-symmetric,} \end{aligned} \tag{5.3.2}$$

i.e.,

$$\alpha(v_1, \dots, v_j, \dots, v_\ell, \dots, v_k) = -\alpha(v_1, \dots, v_\ell, \dots, v_j, \dots, v_k), \tag{5.3.3}$$

for $v_1, \dots, v_k \in V$, $1 \leq j < \ell \leq k$. Another way to picture such $\alpha$ is as a map

$$\alpha : M(k \times n, \mathbb{F}) \longrightarrow \mathbb{F} \tag{5.3.4}$$

that is linear in each column $v_1, \dots, v_k$ of $A = (v_1, \dots, v_k) \in M(k \times n, \mathbb{F})$, and satisfies the anti-symmetry condition (5.3.3), if

$$n = \dim V, \quad \text{so} \quad V \approx \mathbb{F}^n. \tag{5.3.5}$$

In case $k = n$, Proposition 1.5.1 applies, to show that any such $\alpha : M(n \times n, \mathbb{F}) \to \mathbb{F}$ must be a multiple of the determinant. We have

**Proposition 5.3.1.** *Given* (5.3.5)*,*

$$\dim \Lambda^n V' = 1. \tag{5.3.6}$$

Before examining $\dim \Lambda^k V'$ for other values of $k$, let us look into the following. Pick a basis $\{e_1, \dots, e_n\}$ of $V$, and let $\{\varepsilon_1, \dots, \varepsilon_n\}$ denote the dual basis of $V'$. Clearly an element $\alpha \in \Lambda^k V'$ is uniquely determined by its values

$$a_j = \alpha(e_{j_1}, \dots, e_{j_k}), \quad j = (j_1, \dots, j_k), \tag{5.3.7}$$

as $j$ runs over the set of $k$-tuples $(j_1, \dots, j_k)$, with $1 \leq j_\nu \leq n$. Now, $\alpha$ satisfies the anti-symmetry condition (5.3.3) if and only if

$$a_{j_1 \cdots j_k} = (\operatorname{sgn} \sigma) a_{j_{\sigma(1)} \cdots j_{\sigma(k)}}, \tag{5.3.8}$$

for each $\sigma \in S_k$, i.e., for each permutation $\sigma$ of $\{1, \dots, k\}$, with $\operatorname{sgn} \sigma$ defined as in §1.5. In particular,

$$j_\mu = j_\nu \text{ for some } \mu \neq \nu \Longrightarrow \alpha(e_{j_1}, \dots, e_{j_k}) = 0. \tag{5.3.9}$$

Applying this observation to $k > n$ yields the following:

**Proposition 5.3.2.** *In the setting of Proposition 5.3.1,*

$$k > n \Longrightarrow \Lambda^k V' = 0. \tag{5.3.10}$$

Meanwhile, if $1 \le k \le n$, an element $\alpha$ of $\Lambda^k V'$ is uniquely determined by its values

$$a_j = \alpha(e_{j_1}, \dots, e_{j_k}), \quad 1 \le j_1 < \cdots < j_k \le n. \tag{5.3.11}$$

There are $\binom{n}{k}$ such multi-indices, so we have the following (which contains Proposition 5.3.1).

**Proposition 5.3.3.** *In the setting of Proposition 5.3.1,*

$$1 \le k \le n \Longrightarrow \dim \Lambda^k V' = \binom{n}{k}. \tag{5.3.12}$$

Here is some useful notation. Given the dual basis $\{\varepsilon_1, \dots, \varepsilon_n\}$, we define

$$\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k} \in \Lambda^k V', \tag{5.3.13}$$

for $j_\nu \in \{1, \dots, n\}$, all distinct, by

$$\begin{aligned} &(\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k})(e_{j_1}, \dots, e_{j_k}) = 1, \\ &(\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k})(e_{\ell_1}, \dots, e_{\ell_k}) = 0, \ \text{ if } \ \{\ell_1, \dots, \ell_k\} \ne \{j_1, \dots, j_k\}. \end{aligned} \tag{5.3.14}$$

The anti-symmetry condition then specifies

$$(\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k})(e_{j_{\sigma(1)}}, \dots, e_{j_{\sigma(k)}}) = \operatorname{sgn} \sigma, \quad \text{for} \ \ \sigma \in S_k. \tag{5.3.15}$$

Note that

$$\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k} = (\operatorname{sgn} \sigma)\, \varepsilon_{j_{\sigma(1)}} \wedge \cdots \wedge \varepsilon_{j_{\sigma(k)}}, \tag{5.3.16}$$

if $\sigma \in S_k$. In light of this, if not all $\{j_1, \dots, j_k\}$ are distinct, i.e., if $j_\mu = j_\nu$ for some $\mu \ne \nu$, we say (5.3.16) vanishes, i.e.,

$$\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k} = 0 \ \text{ if } \ j_\mu = j_\nu \text{ for some } \mu \ne \nu. \tag{5.3.17}$$

Then, for arbitrary $\alpha \in \Lambda^k V'$, we can write

$$\alpha = \frac{1}{k!} \sum_j a_j\, \varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k}, \tag{5.3.18}$$

as $j$ runs over all $k$-tuples, and $a_j$ is as in (5.3.7). Alternatively, we can write

$$\alpha = \sum_{1 \le j_1 < \cdots < j_k \le n} a_j\, \varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k}, \tag{5.3.19}$$

with $a_j$ as in (5.3.7). Proposition 5.3.3 has the following more explicit form.

**Proposition 5.3.4.** *In the setting of Proposition 5.3.3, if* $1 \le k \le n$*,*

$$\{\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k} : 1 \le j_1 < \cdots < j_k \le n\} \ \ \textit{is a basis of} \ \ \Lambda^k V'. \tag{5.3.20}$$

The products arising in (5.3.13)–(5.3.20) are called *wedge products*. As these formulas suggest, it is useful to define wedge products as bilinear maps

$$w : \Lambda^k V' \times \Lambda^\ell V' \longrightarrow \Lambda^{k+\ell} V', \quad w(\alpha, \beta) = \alpha \wedge \beta, \tag{5.3.21}$$

such that

$$(\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k}) \wedge (\varepsilon_{m_1} \wedge \cdots \wedge \varepsilon_{m_\ell}) = \varepsilon_{j_1} \wedge \cdots \varepsilon_{j_k} \wedge \varepsilon_{m_1} \wedge \cdots \wedge \varepsilon_{m_\ell}, \tag{5.3.22}$$

with equivalencies as in (5.3.16)–(5.3.17). We also want to define (5.3.21) in a fashion that does not depend on the choice of basis of $V$ (and associated dual basis of $V'$). The following result gives a clue as to how to do this.

**Proposition 5.3.5.** *If* $\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k} \in \Lambda^k V'$ *is specified by* (5.3.14)–(5.3.17), *then, for* $v_1, \dots, v_k \in V$,

$$(\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k})(v_1, \dots, v_k) = \sum_{\sigma \in S_k} (\operatorname{sgn} \sigma) \varepsilon_{j_{\sigma(1)}}(v_1) \cdots \varepsilon_{j_{\sigma(k)}}(v_k). \tag{5.3.23}$$

**Proof.** The argument is parallel to the proof of Proposition 1.5.1. We set

$$v_\ell = \sum_{j=1}^n a_{j\ell} e_j, \quad a_{j\ell} = \varepsilon_j(v_\ell), \tag{5.3.24}$$

and substitute into the left side of (5.3.23), obtaining

$$\sum_{\ell_1, \dots, \ell_k = 1}^n \varepsilon_{\ell_1}(v_1) \cdots \varepsilon_{\ell_k}(v_k) (\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k})(e_{\ell_1}, \dots, e_{\ell_k}), \tag{5.3.25}$$

and (5.3.14)–(5.3.17) gives

$$(\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k})(e_{\ell_1}, \dots, e_{\ell_k}) = 0, \tag{5.3.26}$$

unless $\{j_1, \dots, j_k\} = \{\ell_1, \dots, \ell_k\}$, and the $k$ numbers are all distinct, in which case $\ell_\nu = j_{\sigma(\nu)}$ for some $\sigma \in S_k$, and we get $\operatorname{sgn} \sigma$ in (5.3.26). Thus (5.3.25) is converted to the right side of (5.3.23). (Both sides of (5.3.23) vanish if the numbers $j_1, \dots, j_k$ are not all distinct.) $\square$

Remark. In case $n = k$, we obtain precisely Proposition 1.5.1. Note also that the right side of (5.3.23) is equal to

$$\sum_{\sigma \in S_k} (\operatorname{sgn} \sigma) \varepsilon_{j_1}(v_{\sigma(1)}) \cdots \varepsilon_{j_k}(v_{\sigma(k)}). \tag{5.3.27}$$

Compare (1.5.36).

As a further preparation for defining $\alpha \wedge \beta$ in (5.3.21), note that

$$\alpha \in \Lambda^k V' \Rightarrow \alpha(v_1, \dots, v_k) = \frac{1}{k!} \sum_{\sigma \in S_k} (\operatorname{sgn} \sigma) \alpha(v_{\sigma(1)}, \dots, v_{\sigma(k)}). \tag{5.3.28}$$

We now define the wedge product:

**Definition.** If $\alpha \in \Lambda^k V'$ and $\beta \in \Lambda^\ell V'$, then $\alpha \wedge \beta \in \Lambda^{k+\ell} V'$ is given by

$$\begin{aligned}&(\alpha \wedge \beta)(v_1, \dots, v_{k+\ell}) \\ &= \frac{1}{k!\ell!} \sum_{\sigma \in S_{k+\ell}} (\operatorname{sgn} \sigma) \alpha(v_{\sigma(1)}, \dots, v_{\sigma(k)}) \cdot \beta(v_{\sigma(k+1)}, \dots, v_{\sigma(k+\ell)}).\end{aligned} \tag{5.3.29}$$

Our first task is to check the fundamental identity (5.3.22).

**Proposition 5.3.6.** *With $\alpha \wedge \beta$ defined as in* (5.3.29)*, the identity* (5.3.22) *holds.*

**Proof.** With $\alpha = \varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k}$ and $\beta = \varepsilon_{m_1} \wedge \cdots \wedge \varepsilon_{m_\ell}$, we have

$$\begin{aligned}&(\alpha \wedge \beta)(v_1, \dots, v_{k+\ell}) \\ &\quad = \frac{1}{k!\ell!} \sum_{\sigma \in S_{k+\ell}} (\operatorname{sgn} \sigma)(\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k})(v_{\sigma(1)}, \dots, v_{\sigma(k)}) \\ &\qquad\qquad \cdot (\varepsilon_{m_1} \wedge \cdots \wedge \varepsilon_{m_\ell})(v_{\sigma(k+1)}, \dots, v_{\sigma(k+\ell)}),\end{aligned} \tag{5.3.30}$$

which expands out to

$$\begin{aligned}&\frac{1}{k!\ell!} \sum_{\sigma \in S_{k+\ell}} \sum_{\tau \in S_k} \sum_{\rho \in S_\ell} (\operatorname{sgn} \sigma)(\operatorname{sgn} \tau)(\operatorname{sgn} \rho) \\ &\qquad \cdot \varepsilon_{j_1}(v_{\sigma\tau(1)}) \cdots \varepsilon_{j_k}(v_{\sigma\tau(k)}) \cdot \varepsilon_{m_1}(v_{\sigma\rho(k+1)}) \cdots \varepsilon_{m_\ell}(v_{\sigma\rho(k+\ell)}).\end{aligned} \tag{5.3.31}$$

Here, $\sigma$ permutes $\{1, \dots, k+\ell\}$, $\tau$ permutes $\{1, \dots, k\}$, and $\rho$ permutes $\{k+1, \dots, k+\ell\}$. Note that such $\sigma, \tau, \rho$ yield $\gamma(\sigma, \tau, \rho) \in S_{k+\ell}$, with

$$\begin{aligned}\gamma(\sigma, \tau, \rho)(\nu) &= \sigma\tau(\nu) \quad \text{for} \quad 1 \le \nu \le k, \\ &\quad\ \sigma\rho(\nu) \quad \text{for} \quad k+1 \le \nu \le k+\ell,\end{aligned} \tag{5.3.32}$$

and $\operatorname{sgn} \gamma(\sigma, \tau, \rho) = (\operatorname{sgn} \sigma)(\operatorname{sgn} \tau)(\operatorname{sgn} \rho)$. Also, for each fixed $\tau \in S_k,\ \rho \in S_\ell$ $\gamma(\sigma, \tau, \rho)$ runs over $S_{k+\ell}$ once as $\sigma$ runs over $S_{k+\ell}$. Hence, if we fix $\tau$ and $\rho$ in (5.3.31) and just sum over $\sigma$, we get

$$\begin{aligned}&\sum_{\sigma \in S_{k+\ell}} (\operatorname{sgn} \gamma(\sigma, \tau, \rho)) \varepsilon_{j_1}(v_{\gamma(\sigma,\tau,\rho)(1)}) \cdots \varepsilon_{j_k}(v_{\gamma(\sigma,\tau,\rho)(k)}) \\ &\qquad\qquad \cdot \varepsilon_{m_1}(v_{\gamma(\sigma,\tau,\rho)(k+1)}) \cdots \varepsilon_{m_\ell}(v_{\gamma(\sigma,\tau,\rho)(k+\ell)}),\end{aligned} \tag{5.3.33}$$

and each such sum is equal to

$$(\varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k} \wedge \varepsilon_{m_1} \wedge \cdots \wedge \varepsilon_{m_\ell})(v_1, \dots, v_k, v_{k+1}, \dots, v_{k+\ell}). \tag{5.3.34}$$

Then summing over $\tau \in S_k$ and $\rho \in S_\ell$ and dividing by $k!\ell!$ also yields (5.3.34), as desired. $\square$

From here, the following is straightforward.

**Proposition 5.3.7.** *The wedge product $\alpha \wedge \beta$, defined by* (5.3.29)*, produces a well defined bilinear map $\Lambda^k V' \times \Lambda^\ell V' \to \Lambda^{k+\ell} V'$. Furthermore, given $\alpha \in \Lambda^k V'$ and $\beta \in \Lambda^\ell V'$,*

$$\alpha \wedge \beta = (-1)^{k\ell} \beta \wedge \alpha, \tag{5.3.35}$$

*and, if also $\gamma \in \Lambda^m V'$,*

$$(\alpha \wedge \beta) \wedge \gamma = \alpha \wedge (\beta \wedge \gamma). \tag{5.3.36}$$

The wedge product gives us an algebra. We define the *exterior algebra* $\Lambda^* V'$ to be

$$\Lambda^* V' = \bigoplus_{k \geq 0} \Lambda^k V', \tag{5.3.37}$$

keeping in mind that the summands on the right are nonvanishing only for $k \leq n = \dim V$. Proposition 5.3.7 says this is an algebra. The element $1 \in \mathbb{F} = \Lambda^0 V' \subset \Lambda^* V'$ acts as the unit in this algebra. The identity (5.3.36) is the associative law for the wedge product. By (5.3.35), this is not a commutative algebra (if $n > 1$).

We next consider the action a linear map on $V$ induces on $\Lambda^* V'$. A linear map $A : V \to V$ induces a linear map

$$\Lambda^k A^t : \Lambda^k V' \longrightarrow \Lambda^k V', \tag{5.3.38}$$

via

$$(\Lambda^k A^t)\alpha(v_1, \dots, v_k) = \alpha(Av_1, \dots, Av_k). \tag{5.3.39}$$

In particular, $\Lambda^1 A^t = A^t : V' \to V'$. A straightforward calculation from (5.3.29) yields

$$\begin{aligned} \alpha \in & \Lambda^k V', \ \beta \in \Lambda^\ell V', \ A \in \mathcal{L}(V) \\ & \Longrightarrow (\Lambda^{k+\ell} A^t)(\alpha \wedge \beta) = (\Lambda^k A^t)\alpha \wedge (\Lambda^\ell A^t)\beta. \end{aligned} \tag{5.3.40}$$

Here is a natural extension of the identity $(AB)^t = B^t A^t$.

**Proposition 5.3.8.** *If $A, B \in \mathcal{L}(V)$, then*

$$\Lambda^k (AB)^t = (\Lambda^k B^t)\,(\Lambda^k A^t). \tag{5.3.41}$$

**Proof.** We have

$$\begin{aligned} \Lambda^k (AB)^t \alpha(v_1, \dots, v_k) &= \alpha(ABv_1, \dots, ABv_k) \\ &= (\Lambda^k A^t)\alpha(Bv_1, \dots, Bv_k) \\ &= (\Lambda^k B^t)(\Lambda^k A^t)\alpha(v_1, \dots, v_k). \end{aligned} \tag{5.3.42}$$

$\square$

We now return to determinants.

**Proposition 5.3.9.** *If $A \in \mathcal{L}(V)$ and $n = \dim V$, then, for $\omega \in \Lambda^n V'$,*

$$(\Lambda^n A^t)\omega = (\det A)\omega. \tag{5.3.43}$$

**Proof.** We may as well take $\omega = \varepsilon_1 \wedge \cdots \wedge \varepsilon_n$. Then an iteration of (5.3.40) gives

$$(\Lambda^n A^t)\omega = (A^t\varepsilon_1) \wedge \cdots \wedge (A^t\varepsilon_n). \tag{5.3.44}$$

If $A = (a_{jk})$ with respect to the basis $\{e_j\}$, then $A^t\varepsilon_j = \sum_k a_{jk}\varepsilon_k$, so

$$\begin{aligned}(\Lambda^n A^t)\omega &= \sum_{1\le k_\nu \le n} a_{1k_1}\cdots a_{nk_n}\, \varepsilon_{k_1} \wedge \cdots \wedge \varepsilon_{k_n} \\ &= \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma) a_{1\sigma(1)}\cdots a_{n\sigma(n)}\, \varepsilon_1 \wedge \cdots \wedge \varepsilon_n \\ &= (\det A)\, \varepsilon_1 \wedge \cdots \wedge \varepsilon_n,\end{aligned} \tag{5.3.45}$$

the last identity by (1.5.36). $\square$

Combining Propositions 5.3.8 and 5.3.9 yields the following alternative proof of Proposition 1.5.3.

**Corollary 5.3.10.** *If $A, B \in \mathcal{L}(V)$, then*

$$\det(AB) = (\det A)(\det B). \tag{5.3.46}$$

## Interior products

We next define the interior product

$$\iota_v : \Lambda^k V' \longrightarrow \Lambda^{k-1} V', \quad \text{for } \ v \in V, \tag{5.3.47}$$

$k \ge 1$, as follows. If $\alpha \in \Lambda^k V'$, then $\iota_v\alpha \in \Lambda^{k-1}V'$ is defined by

$$(\iota_v\alpha)(v_1, \dots, v_{k-1}) = \alpha(v, v_1, \dots, v_{k-1}). \tag{5.3.48}$$

From this we can compute that, if $\{e_1, \dots, e_n\}$ is a basis of $V$, with dual basis $\{\varepsilon_1, \dots, \varepsilon_n\}$ for $V'$, then, if $j_1, \dots, j_k$ are distinct,

$$\alpha = \varepsilon_{j_1} \wedge \cdots \wedge \varepsilon_{j_k} \Rightarrow \iota_{e_{j_\ell}}\alpha = (-1)^{\ell-1}\varepsilon_{j_1} \wedge \cdots \wedge \widehat{\varepsilon}_{j_\ell} \wedge \cdots \wedge \varepsilon_{j_k}, \tag{5.3.49}$$

where $\widehat{\varepsilon}_{j_\ell}$ denotes removing the factor $\varepsilon_{j_\ell}$. Furthermore, for such $\alpha$,

$$m \notin \{j_1, \dots, j_k\} \Longrightarrow \iota_{e_m}\alpha = 0. \tag{5.3.50}$$

By convention, $\iota_v\alpha = 0$ if $\alpha \in \Lambda^0 V'$.

We make use of the operators $\wedge_k$ and $\iota_k$ on $\Lambda^* V'$:

$$\wedge_k \alpha = \varepsilon_k \wedge \alpha, \quad \iota_k \alpha = \iota_{e_k} \alpha. \tag{5.3.51}$$

There is the following useful anticommutation relation:

**Proposition 5.3.11.** *With the notation (21.51),*

$$\wedge_k \iota_\ell + \iota_\ell \wedge_k = \delta_{k\ell}, \tag{5.3.52}$$

*where* $\delta_{k\ell} = 1$ *if* $k = \ell$, $0$ *otherwise.*

The proof is an exercise. We also have

$$\wedge_j \wedge_k + \wedge_k \wedge_j = 0, \quad \iota_j \iota_k + \iota_k \iota_j = 0. \tag{5.3.53}$$

We mention that (5.3.52) implies the following.

$$(\wedge_w \iota_v + \iota_v \wedge_w)\alpha = \langle v, w \rangle \alpha, \tag{5.3.54}$$

given $\alpha \in \Lambda^k V',\ w \in V',\ v \in V$, with the notation

$$\wedge_w \alpha = w \wedge \alpha. \tag{5.3.55}$$

## Cramer's formula

Cramer's formula, given in (1.5.54), computes a matrix inverse $A^{-1}$ in terms of $\det A$ and the $(n-1) \times (n-1)$ minors of $A$ (or better, of $A^t$). We present an alternative derivation of such a formula here, using exterior algebra.

Let $V$ be $n$-dimensional, with dual $V'$. Let $A \in \mathcal{L}(V)$, with transpose $A^t \in \mathcal{L}(V')$. We bring in the isomorphism

$$\kappa : V \otimes \Lambda^n V' \xrightarrow{\approx} \Lambda^{n-1} V', \tag{5.3.56}$$

given by

$$\kappa(u \otimes \omega)(v_1, \dots, v_{n-1}) = \omega(u, v_1, \dots, v_{n-1}). \tag{5.3.57}$$

We aim to prove the following version of Cramer's formula.

**Proposition 5.3.12.** *If* $A \in \mathcal{L}(V)$ *is invertible, then*

$$(\det A)\, A^{-1} \otimes I = \kappa^{-1} \circ \Lambda^{n-1} A^t \circ \kappa, \tag{5.3.58}$$

*in* $\mathcal{L}(V \otimes \Lambda^n V')$.

**Proof.** Since $\Lambda^n A^t = (\det A) I$ in $\mathcal{L}(\Lambda^n V')$, the desired identity (5.3.58) is equivalent to

$$(\Lambda^{n-1} A^t) \circ \kappa = \kappa \circ (A^{-1} \otimes \Lambda^n A^t), \tag{5.3.59}$$

in $\mathcal{L}(V\otimes\Lambda^n V', \Lambda^{n-1}V')$. Recall that $\Lambda^{n-1}A^t\in\mathcal{L}(\Lambda^{n-1}V')$ is defined by

$$(\Lambda^{n-1}A^t)\beta(v_1,\dots,v_{n-1})=\beta(Av_1,\dots,Av_{n-1}). \tag{5.3.60}$$

Hence if we take $u\otimes\omega\in V\otimes\Lambda^n V'$, we get

$$\begin{aligned}(\Lambda^{n-1}A^t)\circ\kappa(u\otimes\omega)(v_1,\dots,v_{n-1})&=\kappa(u\otimes\omega)(Av_1,\dots,Av_{n-1})\\&=\omega(u,Av_1,\dots,Av_{n-1}).\end{aligned} \tag{5.3.61}$$

On the other hand, since

$$(A^{-1}\otimes\Lambda^n A^t)(u\otimes\omega)=A^{-1}u\otimes\Lambda^n A^t\omega, \tag{5.3.62}$$

we have

$$\begin{aligned}\kappa\circ(A^{-1}&\otimes\Lambda^n A^t)(u\otimes\omega)(v_1,\dots,v_{n-1})\\&=\kappa(A^{-1}u\otimes\Lambda^n A^t\omega)(v_1,\dots,v_{n-1})\\&=(\Lambda^n A^t\omega)(A^{-1}u,v_1,\dots,v_{n-1})\\&=\omega(u,Av_1,\dots,Av_{n-1}),\end{aligned} \tag{5.3.63}$$

which agrees with the right side of (5.3.61). This completes the proof. □

**The exterior algebra $\Lambda^*V$**

If $V$ is an $n$-dimensional space, we define $\Lambda^k V$ in a fashion to the definition of $\Lambda^k V'$, simply by switching $V$ and $V'$, using the natural isomorphism $V\approx(V')'$. Thus we set $\Lambda^0 V=\mathbb{F}$, $\Lambda^1 V=V$, and, for $k\ge 2$,

$$\begin{aligned}\Lambda^k V=\ &\text{set of } k\text{-linear maps } \beta: V'\times\cdots\times V'\to\mathbb{F}\\&\text{that are anti-symmetric.}\end{aligned} \tag{5.3.64}$$

All the results from the early part of this section go through, with the roles of $V$ and $V'$, and also of the bases $\{e_1,\dots,e_n\}$ and $\{\varepsilon_1,\dots,\varepsilon_n\}$, interchanged. For example, for $1\le k\le n$,

$$\{e_{j_1}\wedge\cdots\wedge e_{j_k}:1\le j_1<\cdots<j_k\le n\}\ \text{ is a basis of }\ \Lambda^k V. \tag{5.3.65}$$

With these facts in mind, we can pass from $A\in\mathcal{L}(V)$ to $A^t\in\mathcal{L}(V')$ to

$$\Lambda^k A:\Lambda^k V\longrightarrow\Lambda^k V, \tag{5.3.66}$$

and, parallel to (5.3.40),

$$\begin{aligned}\alpha\in&\Lambda^k V,\ \beta\in\Lambda^\ell V,\ A\in\mathcal{L}(V)\\&\Longrightarrow(\Lambda^{k+\ell}A)(\alpha\wedge\beta)=(\Lambda^k A)\alpha\wedge(\Lambda^\ell A)\beta.\end{aligned} \tag{5.3.67}$$

Consequently,

$$(\Lambda^k A)(e_{j_1}\wedge\cdots\wedge e_{j_k})=Ae_{j_1}\wedge\cdots\wedge Ae_{j_k}. \tag{5.3.68}$$

We now mention a "universal property" possessed by $\Lambda^k V$. Let $W$ be another finite-dimensional vector space over $\mathbb{F}$, and set

$$\begin{aligned}\operatorname{Alt}^k(V,W) = \text{set of } k\text{-linear maps } V \times \cdots \times V \to W \\ \text{that are anti-symmetric.}\end{aligned} \tag{5.3.69}$$

This has the structure of a finite-dimensional vector space.

**Proposition 5.3.13.** *There is a natural linear isomorphism*

$$\Phi : \operatorname{Alt}^k(V,W) \xrightarrow{\approx} \mathcal{L}(\Lambda^k V, W). \tag{5.3.70}$$

One way to describe $\Phi$ is with the aid of a basis $\{e_1, \dots, e_n\}$ of $V$, leading, as mentioned, to the basis (5.3.65) of $\Lambda^k V$. Given $\alpha \in \operatorname{Alt}^k(V,W)$, hence

$$\alpha : V \times \cdots \times V \longrightarrow W, \tag{5.3.71}$$

we can define $\Phi\alpha : \Lambda^k V \to W$ by

$$(\Phi\alpha)(e_{j_1} \wedge \cdots \wedge e_{j_k}) = \alpha(e_{j_1}, \dots, e_{j_k}). \tag{5.3.72}$$

It is clear that this defines a linear map $\Phi : \operatorname{Alt}^k(V,W) \to \mathcal{L}(\Lambda^k V, W)$. One needs to show that this is an isomorphism and that it is independent of the choice of basis $\{e_j\}$ of $V$. We leave these tasks to the enthusiastic reader.

Now that, in case $W = \mathbb{F}$, we have

$$\operatorname{Alt}^k(V,\mathbb{F}) = \Lambda^k V', \quad \mathcal{L}(\Lambda^k V, \mathbb{F}) = (\Lambda^k V)', \tag{5.3.73}$$

and Proposition 5.3.13 implies that there is a natural isomorphism

$$\Lambda^k V' \approx (\Lambda^k V)'. \tag{5.3.74}$$

## Exercises

1. Let $A \in M(n,\mathbb{C})$ have eigenvalues $\{\lambda_1, \dots, \lambda_n\}$, repeated according to multiplicity. Show that, for $1 \le k \le n$,

$$\begin{aligned}\operatorname{Tr} \Lambda^k A &= \sigma_k(\lambda_1, \dots, \lambda_n) \\ &= \sum_{1 \le j_1 < \cdots < j_k \le n} \lambda_{j_1} \cdots \lambda_{j_k}.\end{aligned}$$

Here $\sigma_k$ are the elementary symmetric polynomials, introduced in Exercise 7 of §2.1.

2. Deduce from Exercise 1 above, plus Exercise 7 of §2.1, that

$$\det(\lambda I - A) = \sum_{k=0}^{n} (-1)^k (\operatorname{Tr} \Lambda^k A) \lambda^{n-k}.$$

3. Let $V$ be an $n$-dimensional vector space over $\mathbb{F}$, with dual $V'$. Show that there is a natural isomorphism

$$\kappa : \Lambda^k V \otimes \Lambda^n V' \longrightarrow \Lambda^{n-k} V',$$

satisfying

$$\kappa(v_1, \wedge \cdots \wedge v_k \otimes \alpha)(w_1, \dots, w_{n-k}) = \alpha(v_1, \dots, v_k, w_1, \dots, w_{n-k}).$$

4. In the setting of Exercise 3, establish the following generalization of Proposition 5.3.12 (due, in other language, to Jacobi).

**Proposition 5.3.14.** *If $A \in \mathcal{L}(V)$ is invertible, then*

$$(\det A)\, \Lambda^k A^{-1} \otimes I = \kappa^{-1} \circ \Lambda^{n-k} A^t \circ \kappa,$$

*in $\mathcal{L}(\Lambda^k V \otimes \Lambda^n V')$.*

*Hint.* Adapt the proof of Proposition 5.3.12.

5. Establish the following variant of Proposition 5.3.8. If $A, B \in \mathcal{L}(V)$, then

$$\Lambda^k (AB) = (\Lambda^k A)(\Lambda^k B).$$

If $\{e_1, \dots, e_n\}$ is the standard basis of $\mathbb{R}^n$, define an inner product on $\Lambda^k \mathbb{R}^n$ be declaring an orthonormal basis to be

$$\{e_{j_1} \wedge \cdots \wedge e_{j_k} : 1 \le j_1 < \cdots \wedge j_k \le n\}.$$

If $A : \Lambda^k \mathbb{R}^n \to \Lambda^k \mathbb{R}^n$, define $A^* : \Lambda^k \mathbb{R}^n \to \Lambda^k \mathbb{R}^n$ by

$$\langle A\alpha, \beta \rangle = \langle \alpha, A^* \beta \rangle, \quad \alpha, \beta \in \Lambda^k \mathbb{R}^n,$$

where $\langle\ ,\ \rangle$ is the inner product on $\Lambda^k \mathbb{R}^n$ defined above.

6. Show that, if $T : \mathbb{R}^n \to \mathbb{R}^n$ is linear, with adjoint $T^*$, then

$$(\Lambda^k T)^* = \Lambda^k (T^*).$$

*Hint.* Check the identity $\langle (\Lambda^k T)\alpha, \beta \rangle = \langle \alpha, (\Lambda^k T^*)\beta \rangle$ when $\alpha$ and $\beta$ run over the orthonormal basis described above. That is, show that if $\alpha = e_{j_1} \wedge \cdots \wedge e_{j_k}$ and $\beta = e_{i_1} \wedge \cdots \wedge e_{i_k}$, then

$$\langle T e_{j_1} \wedge \cdots \wedge T e_{j_k}, e_{i_1} \wedge \cdots \wedge e_{i_k} \rangle = \langle e_{j_1} \wedge \cdots \wedge e_{j_k}, T^* e_{i_1} \wedge \cdots \wedge T^* e_{i_k} \rangle.$$

*Hint.* Say $T = (t_{ij})$. In the spirit of (5.3.45), expand $Te_{j_1} \wedge \cdots \wedge Te_{j_k}$, and show that the left side of the asserted identity above is

$$\sum_{\sigma \in S_k} (\operatorname{sgn} \sigma) t_{i_{\sigma(1)} j_1} \cdots t_{i_{\sigma(k)} j_k}.$$

Similarly, show that the right side is equal to

$$\sum_{\tau \in S_k} (\operatorname{sgn} \tau) t_{i_1 j_{\tau(1)}} \cdots t_{i_k j_{\tau(k)}}.$$

To compare these two formulas, see the derivation of (1.5.36).

7. Show that if $\{u_1, \dots u_n\}$ is any orthonormal basis of $\mathbb{R}^n$, then the set

$$\{u_{j_1} \wedge \cdots \wedge u_{j_k} : 1 \le j_1 < \cdots < j_k \le n\}$$

is an orthonormal basis of $\Lambda^k \mathbb{R}^n$.
*Hint.* Use Exercises 5 and 6 to show that if $T : \mathbb{R}^n \to \mathbb{R}^n$ is an orthogonal transformation on $\mathbb{R}^n$ (i.e., preserves the inner product) then $\Lambda^k T$ is an orthogonal transformation on $\Lambda^k \mathbb{R}^n$.

8. Let $v_j, w_j \in \mathbb{R}^n$, $1 \le j \le k$ $(k < n)$. Form the matrices $V$, whose $k$ columns are the column vectors $v_1, \dots, v_k$, and $W$, whose $k$ columns are the column vectors $w_1, \dots, w_k$. Show that

$$\begin{aligned} \langle v_1 \wedge \cdots \wedge v_k, w_1 \wedge \cdots \wedge w_k \rangle &= \det W^t V \\ &= \det V^t W. \end{aligned}$$

*Hint.* Show that both sides are linear in each $v_j$ and in each $w_j$. (To treat the right side, use material in §5.) Use this to reduce the problem to verifying the asserted identity when each $v_j$ and each $w_j$ is chosen from among the set of basis vectors $\{e_1, \dots, e_n\}$. Use anti-symmetries to reduce the problem further.

9. Deduce from Exercise 8 that if $v_j, w_j \in \mathbb{R}^n$, then

$$\langle v_1 \wedge \cdots \wedge v_k, w_1 \wedge \cdots \wedge w_k \rangle = \sum_{\pi \in S_k} (\operatorname{sgn} \pi) \langle v_1, w_{\pi(1)} \rangle \cdots \langle v_k, w_{\pi(k)} \rangle.$$

10. Show that the conclusion of Exercise 7 also follows from Exercise 9.

11. Let $A, B : \mathbb{R}^k \to \mathbb{R}^n$ be linear maps and set $\omega = e_1 \wedge \cdots \wedge e_k \in \Lambda^k \mathbb{R}^k$. We have $\Lambda^k A\omega$, $\Lambda^k B\omega \in \Lambda^k \mathbb{R}^n$. Deduce from Exercise 8 that

$$\langle \Lambda^k A\omega, \Lambda^k B\omega \rangle = \det B^t A.$$

Given $A : \mathbb{R}^n \to \mathbb{R}^n$, an $\ell \times \ell$ minor of $A$ is the determinant of an $\ell \times \ell$ matrix of the form

$$\begin{pmatrix} a_{j(1)k(1)} & \cdots & a_{j(1)k(\ell)} \\ \vdots & & \vdots \\ a_{j(\ell)k(1)} & \cdots & a_{j(\ell)k(\ell)} \end{pmatrix},$$

where $1 \le j(1) < \cdots < j(\ell) \le n,\ 1 \le k(1) < \cdots < k(\ell) \le n$, and $A = (a_{jk})$. The $(n-1) \times (n-1)$ minors were introduced in Exercises 3–4 of §1.5 and played a role in Cramer's formula.

12. Relate the $\ell \times \ell$ minors of $A$ to the matrix entries of $\Lambda^\ell A$, with respect to the basis of $\Lambda^\ell \mathbb{R}^n$ given by (21.65) (with $k = \ell$).

13. Say also $B : \mathbb{R}^n \to \mathbb{R}^n$. Restate the identity $\Lambda^\ell(AB) = (\Lambda^\ell A)(\Lambda^\ell B)$ (cf. Exercise 5) in terms of an identity for the product of the matrices of $\ell \times \ell$ minors of $A$ and of $B$, respectively. The result is a version of the Cauchy-Binet formula.

14. Assume $A : \mathbb{R}^n \to \mathbb{R}^n$ is invertible. Using the result of Exercise 12, with $\ell = k$ and $\ell = n - k$, respectively, derive from Exercise 4 a formula relating the $k \times k$ minors of $A^{-1}$ to the $(n-k) \times (n-k)$ minors of $A^t$. This yields the classical version of Jacobi's generalization of Cramer's formula.

## 5.4. Isomorphism Skew($V$) $\approx \Lambda^2 V$ and the Pfaffian

Let $V$ be an $n$-dimensional real inner product space. Recall from §3.3 that, given $X \in \mathcal{L}(V)$, we say $X \in \mathrm{Skew}(V)$ if and only if $X^* = -X$. The inner product produces an isomorphism

$$\eta : \mathrm{Skew}(V) \xrightarrow{\approx} \mathrm{Alt}^2(V, \mathbb{R}), \quad \eta(X)(u, v) = (Xu, v). \tag{5.4.1}$$

It also produces an isomorphism $V \approx V'$, hence $\mathrm{Alt}^2(V, \mathbb{R}) \approx \mathrm{Alt}^2(V', \mathbb{R}) = \Lambda^2 V$. Composition with (5.4.1) yields an isomorphism

$$\xi : \mathrm{Skew}(V) \xrightarrow{\approx} \Lambda^2 V. \tag{5.4.2}$$

If $\{e_1, \dots, e_n\}$ is an orthonormal basis of $V$ and $X \in \mathrm{Skew}(V)$ has the matrix representation $(X_{jk})$ with respect to this basis, then

$$\xi(X) = \frac{1}{2} \sum_{j,k} X_{jk}\, e_j \wedge e_k. \tag{5.4.3}$$

Compare (5.3.18).

Note that if $X \in \mathrm{Skew}(V)$ and $T \in \mathcal{L}(V)$, then also $TXT^* \in \mathrm{Skew}(V)$. We have

$$\eta(TXT^*)(u, v) = (TXT^* u, v) = \eta(X)(T^* u, T^* v), \tag{5.4.4}$$

hence

$$\xi(TXT^*) = (\Lambda^2 T)\xi(X). \tag{5.4.5}$$

By (5.4.3) and (5.3.68),

$$(\Lambda^2 T)\xi(X) = \frac{1}{2} \sum_{j,k} X_{jk}\, (Te_j) \wedge (Te_k), \tag{5.4.6}$$

which can also be seen to yield the left side of (5.4.5) directly.

We now add the assumption that $\dim V = n = 2k$, and define a function called the *Pfaffian*,

$$\mathrm{Pf} : \mathrm{Skew}(V) \longrightarrow \mathbb{R}, \tag{5.4.7}$$

as follows. Recalling the orthonormal basis $\{e_j\}$ of $V$, we set

$$\omega = e_1 \wedge \cdots \wedge e_n \in \Lambda^n V. \tag{5.4.8}$$

Previous results from this section imply that $\omega$ is independent of the choice of orthonormal basis of $V$, up to sign. In fact, each $\Lambda^k V$ gets an inner product, and $\omega$ is the unique element of $\Lambda^n V$ of norm 1, up to sign. The choice of such an element is called an *orientation* of $V$, so we are set to define (5.4.7) when $V$ is an oriented, real inner product space, of dimension $n = 2k$. The defining equation, for $X \in \mathrm{Skew}(V)$, is

$$\mathrm{Pf}(X)\omega = \frac{1}{k!}\, \xi(X) \wedge \cdots \wedge \xi(X) \quad (k \text{ factors}). \tag{5.4.9}$$

Here is an important transformation property. Take $T \in \mathcal{L}(V)$. It follows from (5.4.5) that

$$\operatorname{Pf}(TXT^*)\omega = (\Lambda^{2k}T)\operatorname{Pf}(X)\omega, \tag{5.4.10}$$

hence, by (5.3.43),

$$\operatorname{Pf}(TXT^*) = (\det T)\ \operatorname{Pf}(X), \quad \forall\, X \in \operatorname{Skew}(V), T \in \mathcal{L}(V). \tag{5.4.11}$$

With this, we can relate $\operatorname{Pf}(X)$ to the determinant.

**Proposition 5.4.1.** *If $V$ is an even-dimensional, oriented, real inner product space and $X \in \operatorname{Skew}(V)$, then*

$$\operatorname{Pf}(X)^2 = \det X. \tag{5.4.12}$$

**Proof.** There is no loss of generality in taking $V = \mathbb{R}^n$, with its standard orthonormal basis. It follows from results of §3.3 that, given $X \in \operatorname{Skew}(V)$, we can write $X = TYT^*$, where $T \in SO(n)$ and $Y$ is a sum of $2 \times 2$ skew-symmetric blocks, of the form

$$Y_\nu = \begin{pmatrix} 0 & \lambda_\nu \\ -\lambda_\nu & 0 \end{pmatrix}, \quad \lambda_\nu \in \mathbb{R}. \tag{5.4.13}$$

Then

$$\xi(Y) = \lambda_1\, e_1 \wedge e_2 + \cdots + \lambda_k\, e_{2k-1} \wedge e_{2k}, \tag{5.4.14}$$

so (5.4.9) yields

$$\operatorname{Pf}(Y) = \lambda_1 \cdots \lambda_k. \tag{5.4.15}$$

Now $\det Y = (\lambda_1 \cdots \lambda_k)^2$, so (5.4.12) follows from this and (5.4.11). ∎

Chapter 6

# Linear algebra over more general fields

We extend the class of vector spaces we work with in the following way. Instead of taking $\mathbb{F}$ to be $\mathbb{R}$ or $\mathbb{C}$, we allow $\mathbb{F}$ to be an arbitrary *field*. A field is a set endowed with operations of addition and multiplication, and these operations satisfy the same set of commutative, associative, and distributive laws as do $\mathbb{R}$ and $\mathbb{C}$. A set with this structure is called a commutative ring. In addition, we assume $\mathbb{F}$ has a multiplicative identity, 1, and that every nonzero element $a \in \mathbb{F}$ has associated an element $a^{-1}$ such that $aa^{-1} = 1$. See the beginning of §6.1 for more details.

In §6.1 we review topics from previous chapters and discuss how many of them extend from $\mathbb{R}$ and $\mathbb{C}$ to more general fields. We also produce various examples of fields. Examples include

$$\mathbb{Z}/(p), \tag{6.0.1}$$

when $p \in \mathbb{N}$ is a prime, and

$$\mathbb{F}(t), \tag{6.0.2}$$

the set of quotients $p(t)/q(t)$ (with $q \neq 0$) of polynomials in $t$ with coefficients in a field $\mathbb{F}$. These polynomials form a ring, denoted $\mathbb{F}[t]$, and (6.0.2) is an example of the *quotient field* of a ring $\mathcal{R}$, which is defined when $\mathcal{R}$ has the property that if $a, b \in \mathcal{R}$ and $ab = 0$, then $a = 0$ or $b = 0$ (we then say $\mathcal{R}$ is an *integral domain*). Applying this construction to the ring $\mathbb{Z}$ of integers gives the field $\mathbb{Q}$ of rational numbers.

Other examples discussed in §6.1 involve algebraic numbers, i.e., roots of a polynomial with coefficients in $\mathbb{Q}$. For example, we can take $a_1, \dots, a_k$

to be algebraic numbers (we say they are elements of $\mathcal{A}$) and form

$$\mathbb{Q}[a_1, \dots, a_k], \tag{6.0.3}$$

the set of numbers in $\mathbb{C}$ that are polynomials in $a_1, \dots, a_k$ with coefficients in $\mathbb{Q}$, or equivalently the ring generated by $\mathbb{Q}$ and $\{a_1, \dots, a_k\}$. The fact that (6.0.3) is actually a field is a special case of the following result established in §6.1. Assume $\mathcal{R}$ is a ring satisfying

$$\mathbb{Q} \subset \mathcal{R} \subset \mathbb{C}. \tag{6.0.4}$$

It follows that $\mathcal{R}$ is a vector space over $\mathbb{Q}$. Then

$$\dim_{\mathbb{Q}} \mathcal{R} < \infty \Longrightarrow \mathcal{R} \text{ is a field.} \tag{6.0.5}$$

The proof is a simple application of the fundamental theorem of linear algebra (which extends readily to the setting of vector spaces over a general field). Taking off from here, it is shown in §6.1 that $\mathcal{A}$ is a field. Furthermore, $\mathcal{A}$ is shown to be algebraically closed, i.e., each polynomial $p \in \mathcal{A}[t]$ has roots in $\mathcal{A}$. One consequence is that if $T \in M(n, \mathcal{A})$, then $T$ can be conjugated to its Jordan canonical form via an element of $M(n, \mathcal{A})$.

In §6.2 we show that the set $\mathcal{A}$ of algebraic numbers coincides with the set of numbers that are eigenvalues of square matrices with entries in $\mathbb{Q}$. We use this together with some matrix constructions to obtain another proof that $\mathcal{A}$ is a field.

See Appendix A.4 for further results on construction of fields, including general finite fields, of which the fields $\mathbb{Z}/(p)$ are the first examples. This appendix pushes beyond algebraic extensions of $\mathbb{Q}$ (which give rise to elements of $\mathcal{A}$), to algebraic extensions of general fields.

## 6.1. Vector spaces over more general fields

So far we have considered vector spaces over $\mathbb{F}$, when $\mathbb{F}$ is either the set $\mathbb{R}$ of real numbers or the set $\mathbb{C}$ of complex numbers. We now introduce a more general class of candidates for $\mathbb{F}$, called *fields*. By definition, a field is a set $\mathbb{F}$, endowed with two operations, addition and multiplication. That is, given $a, b \in \mathbb{F}$, then $a + b$ and $ab$ are defined in $\mathbb{F}$. Furthermore, the following properties are to hold, for all $a, b, c \in \mathbb{F}$. First, there are laws for addition:

$$\text{Commutative law} \ : \ a + b = b + a, \tag{6.1.1}$$

$$\text{Associative law} \ : \ (a + b) + c = a + (b + c), \tag{6.1.2}$$

$$\text{Zero} \ : \ \exists\, 0 \in \mathbb{F}, \ a + 0 = a, \tag{6.1.3}$$

$$\text{Negative} \ : \ \exists - a, \ a + (-a) = 0. \tag{6.1.4}$$

If only these conditions hold, we say $\mathbb{F}$ is a commutative, additive group. Next, there are laws for multiplication:

$$\text{Commutative law} \ : \ ab = ba, \tag{6.1.5}$$

$$\text{Associative law} \ : \ a(bc) = (ab)c, \tag{6.1.6}$$

$$\text{Unit} \ : \ \exists\, 1 \in \mathbb{F}, \ 1 \cdot a = a, \tag{6.1.7}$$

and a distributive law, connecting addition and multiplication:

$$a(b + c) = ab + ac. \tag{6.1.8}$$

Compare the conditions (1.1.10)–(1.1.17). If (6.1.1)–(6.1.8) hold, one says $\mathbb{F}$ is a commutative ring with unit. If (6.1.7) is omitted, one says $\mathbb{F}$ is a commutative ring. If (6.1.5) is also omitted, one says $\mathbb{F}$ is a ring, provided that (6.1.8) is supplemented by

$$(b + c)a = ba + ca. \tag{6.1.9}$$

We say $\mathbb{F}$ is a field provided (6.1.1)–(6.1.8) hold and also the following holds:

$$\text{Inverse} : \ \forall\, a \neq 0, \ \exists\, a^{-1} \in \mathbb{F} \text{ such that } aa^{-1} = 1, \quad 1 \neq 0. \tag{6.1.10}$$

The reader should be familiar with the fact that $\mathbb{R}$ and $\mathbb{C}$ satisfy (6.1.1)–(6.1.10). (Proofs can be found in Chapter 1 of [**23**].) Another field is $\mathbb{Q}$, the set of rational numbers. The set $\mathbb{Z}$ of integers satisfies (6.1.1)–(6.1.8), but not (6.1.10), so $\mathbb{Z}$ is a commutative ring with unit, but not a field. The sets $M(n, \mathbb{R})$ and $M(n, \mathbb{C})$ of matrices satisfy (6.1.1)–(6.1.9), with the exception of (6.1.5) (if $n > 1$), so they are rings (with unit), but not commutative rings. More generally, $M(n, \mathbb{F})$ is a ring for each field $\mathbb{F}$, and, even more generally, for each ring $\mathbb{F}$.

Another important class of rings comes from modular arithmetic. Given an integer $n \geq 2$, we define $\mathbb{Z}/(n)$ to consist of equivalence classes of integers, where, given $a, a' \in \mathbb{Z}$,

$$a \sim a' \Longleftrightarrow n \text{ divides } a - a'. \tag{6.1.11}$$

(Another notation is $a = a' \bmod n$. We also say $a = a'$ in $\mathbb{Z}/(n)$.) It is easy to verify that

$$a \sim a',\ b \sim b' \Longrightarrow a + b \sim a' + b' \text{ and } ab \sim a'b', \tag{6.1.12}$$

so addition and multiplication are naturally well defined on $\mathbb{Z}/(n)$. One also readily verifies (6.1.1)–(6.1.8), so $\mathbb{Z}/(n)$ is a commutative ring with unit, for each such $n$.

If $n$ is not a prime, say $n = jk$ with integers $j$ and $k$, both $\geq 2$, then

$$j, k \neq 0 \quad \text{in} \quad \mathbb{Z}/(n) \quad \text{but} \quad jk = 0 \quad \text{in} \quad \mathbb{Z}/(n), \tag{6.1.13}$$

which is impossible if $j$ has a multiplicative inverse as in (6.1.10). Thus $\mathbb{Z}/(n)$ is not a field if $n$ is not a prime. Conversely, we have the following.

**Proposition 6.1.1.** *If $p \in \mathbb{N}$ is a prime, then $\mathbb{Z}/(p)$ is a field.*

**Proof.** Pick $a \in \mathbb{Z}$ such that $a \neq 0$ in $\mathbb{Z}/(p)$, i.e., $a$ is not a multiple of $p$. Let

$$\mathcal{I} = \{aj + pk : j, k \in \mathbb{Z}\}. \tag{6.1.14}$$

The set $\mathcal{I} \subset \mathbb{Z}$ has the following properties:

$$\alpha, \beta \in \mathcal{I} \Rightarrow \alpha + \beta \in \mathcal{I}, \quad \alpha \in \mathcal{I},\ \beta \in \mathbb{Z} \Rightarrow \alpha\beta \in \mathcal{I}. \tag{6.1.15}$$

(One says $\mathcal{I}$ is an ideal.) Let $\ell$ be the smallest positive element of $\mathcal{I}$. It follows from (6.1.15) that

$$\mathcal{J} = \{\ell k : k \in \mathbb{Z}\} \Longrightarrow \mathcal{J} \subset \mathcal{I}. \tag{6.1.16}$$

If $\mathcal{J} \neq \mathcal{I}$, then there exists $k \in \mathbb{N}$ and $\mu \in \mathcal{I}$ such that

$$k\ell < \mu < (k+1)\ell. \tag{6.1.17}$$

But then we get

$$0 < \mu - k\ell < \ell, \text{ and } \mu - k\ell \in \mathcal{I}, \tag{6.1.18}$$

contradicting the fact that $\ell$ is the smallest positive element of $\mathcal{I}$. Hence it is impossible that $\mathcal{J} \neq \mathcal{I}$, so

$$\mathcal{J} = \mathcal{I}. \tag{6.1.19}$$

Looking at (6.1.14), we see that

$$\text{both } a \text{ and } p \text{ must be multiples of } \ell.$$

Now if the prime $p$ is a multiple of $\ell$, then either $\ell = 1$ or $\ell = p$. Our hypothesis on $a$ does not allow $\ell = p$, so $\ell = 1$. Hence $\mathcal{J} = \mathbb{Z}$, so $\mathcal{I} = \mathbb{Z}$. Thus there exist $j, k \in \mathbb{Z}$ such that

$$aj + pk = 1. \tag{6.1.20}$$

Then the equivalence class of $j$ in $\mathbb{Z}/(p)$ is the desired inverse $a^{-1}$. This proves Proposition 6.1.1. $\square$

We recall that the notion of an ideal arose in §2.2, in the production of the minimal polynomial. Compare (2.2.9). In that setting, we were dealing with the set $\mathcal{P}$ of polynomials, of the form

$$p(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0, \tag{6.1.21}$$

with $a_j \in \mathbb{C}$. Now addition and multiplication of polynomials is well defined, and one readily verifies that $\mathcal{P}$ satisfies (6.1.1)–(6.1.8), so $\mathcal{P}$ is a commutative ring with unit. We can then construct the space $\mathcal{R}$ of rational functions, consisting of quotients

$$\frac{p}{q}, \quad p, q \in \mathcal{P}, \quad q \neq 0. \tag{6.1.22}$$

We say

$$\frac{p}{q} \sim \frac{\tilde{p}}{\tilde{q}} \Longleftrightarrow p\tilde{q} = \tilde{p}q. \tag{6.1.23}$$

It is readily verified that (6.1.1)–(6.1.8) hold for $\mathcal{R}$. Also (6.1.10) holds:

$$\Bigl(\frac{p}{q}\Bigr)^{-1} = \frac{q}{p}, \quad \text{if} \ \ p \neq 0. \tag{6.1.24}$$

Hence $\mathcal{R}$ is a field.

More generally, instead of requiring the coefficients $a_j$ in (6.1.21) to belong to $\mathbb{C}$, we can take any field $\mathbb{F}$ and consider all objects of the form (6.1.21) with $a_j \in \mathbb{F}$. We obtain a commutative ring with unit, typically denoted $\mathbb{F}[\lambda]$. Then one can pass to the set of quotients as in (6.1.22) and obtain a field, denoted $\mathbb{F}(\lambda)$. It is useful to make a comment about the nonvanishing condition. Namely, given $p \in \mathbb{F}[\lambda]$, as in (6.1.21), with $a_j \in \mathbb{F}$, we say

$$p = 0 \Longleftrightarrow a_0 = \cdots = a_n = 0. \tag{6.1.25}$$

Now, such a polynomial also defines a function

$$\Phi(p) : \mathbb{F} \longrightarrow \mathbb{F},$$

whose value at $a \in \mathbb{F}$ is $p(a)$. When $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, we make no notational distinction between $p$ and $\Phi(p)$, because

$$\text{if } \mathbb{F} = \mathbb{R} \text{ or } \mathbb{C}, \text{ then } p(a) = 0 \ \forall\, a \in \mathbb{F} \Rightarrow p = 0 \text{ in } \mathbb{F}[\lambda]. \tag{6.1.26}$$

However, for some fields this can fail. For example, if $r$ is a prime,

$$\mathbb{F} = \mathbb{Z}/(r), \; p(\lambda) = \lambda^r - \lambda \Rightarrow p(a) = 0, \; \forall\, a \in \mathbb{F}. \tag{6.1.27}$$

In such a case, one must carefully distinguish between $p \in \mathbb{F}[\lambda]$ and the associated function $\Phi(p)$ on $\mathbb{F}$.

Having defined the notion of a field and given several examples, we turn to the notion of a vector space over a field. Actually, this is formally just like that introduced in §1.1. If $\mathbb{F}$ is a field, then a vector space over $\mathbb{F}$ is a set $V$, endowed with two operations, vector addition and multiplication by scalars (elements of $\mathbb{F}$), satisfying the conditions (1.1.10)–(1.1.17).

One standard example of such a vector space is $\mathbb{F}^n$, defined exactly as in (1.1.8). An $n \times n$ matrix $A$ with entries in $\mathbb{F}$ produces a map $A : \mathbb{F}^n \to \mathbb{F}^n$ just as in (1.2.3)–(1.2.5). This map is linear, where the concept of a linear map $T : V \to W$ from one vector space over $\mathbb{F}$ to another is defined just as in (1.2.1)–(1.2.2). Then $\mathcal{L}(V, W)$, the space of linear transformations from $V$ to $W$, has the structure of a vector space over $\mathbb{F}$, just as in (1.2.11)–(1.2.12). Composition of such operators is given by matrix multiplication, as in (1.2.15)–(1.2.18). Given such $T \in \mathcal{L}(V, W)$, the spaces $\mathcal{N}(T)$ and $\mathcal{R}(T)$ are defined just as in (1.2.24)–(1.2.25), and they are vector spaces over $\mathbb{F}$.

The results on linear independence, bases, and dimension developed in §1.3 extend to this more general setting, as does the fundamental theorem of linear algebra, Proposition 1.3.6, and its corollaries, which finish up §1.3.

Material on determinants and invertibility developed in §1.5 extends to $n \times n$ matrices with coefficients in a general field $\mathbb{F}$, though one wrinkle is encountered. The argument in Proposition 1.5.1 needs to be modified for those fields $\mathbb{F}$ (such as $\mathbb{Z}/(2)$) for which $1 = -1$. Details are given at the end of this section; see Proposition 6.1.9. For the special case $\mathbb{F} = \mathbb{Z}/(2)$, see Exercise 4 below. For another approach, valid for matrices over commutative rings, see material in §7.1, involving (7.1.19)–(7.1.25). One result of §1.5 that is special to the fields $\mathbb{F} = \mathbb{R}$ and $\mathbb{C}$ is Proposition 1.5.8 on denseness of $G\ell(n, \mathbb{F})$ in $M(n, \mathbb{F})$. This does not extend to general fields.

Material in §2.1 on eigenvalues and eigenvectors extend to general fields $\mathbb{F}$, except for results that invoke the fundamental theorem of algebra, such as Proposition 2.1.1. For Proposition 2.1.1 to work when $V$ is a vector space over a field $\mathbb{F}$, one needs to know that, whenever $p(\lambda)$ is a polynomial of the form (6.1.21), with $a_j \in \mathbb{F}$, $n \geq 1$, and $a_n \neq 0$, then $p(\lambda_k) = 0$ for some $\lambda_k \in \mathbb{F}$. When a field $\mathbb{F}$ has this property, we say $\mathbb{F}$ is *algebraically closed*. The content of the fundamental theorem of algebra (established in Appendix A.1) is that $\mathbb{C}$ is algebraically closed. On the other hand, $\mathbb{R}$ is not algebraically closed, since $\lambda^2 + 1$ has no root in $\mathbb{R}$. It is significant that

$\mathbb{R}$ is contained in the algebraically closed field $\mathbb{C}$. Generally, we have the following.

**Proposition 6.1.2.** *Each field $\mathbb{F}$ is a subfield of some algebraically closed field $\widetilde{\mathbb{F}}$.*

A proof of this would take us too far afield (so to speak), and we refer to [**11**], Chapter 7, §2.

If $\mathbb{F}$ is a subfield of $\widetilde{\mathbb{F}}$ and $V$ is an $n$-dimensional vector space over $\mathbb{F}$, we can pass to a vector space $\widetilde{V}$ over $\widetilde{\mathbb{F}}$ by taking a basis $\{e_1, \dots, e_n\}$ of $V$ and letting the coefficients $a_j$ in $a_1e_1 + \cdots + a_ne_n$ run over $\widetilde{\mathbb{F}}$. For example, $V = \mathbb{F}^n$ gives rise to $\widetilde{V} = \widetilde{\mathbb{F}}^n$. An element $T \in \mathcal{L}(V)$ with matrix representation $(a_{jk})$, $a_{jk} \in \mathbb{F}$, naturally acts also on $\widetilde{V}$.

If $V$ is an $n$-dimensional vector space over $\mathbb{F}$ and $\mathbb{F}$ is algebraically closed, then Proposition 2.1.1 works, and the results of §2.2 on generalized eigenvectors also work. Going further, the results of §2.3 on triangular matrices and nilpotent matrices extend to the setting where $V$ is a vector space over an algebraically closed field $\mathbb{F}$ (including the Cayley-Hamilton theorem), and so do the results of §2.4, on the Jordan canonical form.

On the other hand, results of Chapter 3 are special to vector spaces over $\mathbb{R}$ and $\mathbb{C}$.

Back to generalities, results of §§4.1 and 4.3, and §§5.1–5.3 extend readily to vector spaces over a general field $\mathbb{F}$, except for wrinkles in exterior algebra when $1 = -1$ in $\mathbb{F}$.

The reader can have fun verifying these claims, none of which are hard (though they require a vigorous re-examination of these previous sections).

We return to the issue of describing examples of fields, and discuss some subsets of $\mathbb{R}$ and $\mathbb{C}$ that can be shown to be fields. To start, we take the irrational number $\sqrt{2}$ and consider

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}. \tag{6.1.28}$$

It is readily verified that $\mathbb{Q}[\sqrt{2}]$ is a subset of $\mathbb{R}$ that is closed under addition and multiplication, so it is a commutative ring with unit. As for (6.1.10), note that if $a, b \in \mathbb{Q}$,

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in \mathbb{Q}[\sqrt{2}], \tag{6.1.29}$$

if either $a \neq 0$ or $b \neq 0$. Indeed, in such a case, the fact that $\sqrt{2}$ is irrational implies that the denominator $a^2 - 2b^2$ on the right side of (6.1.29) is nonzero. Thus $\mathbb{Q}[\sqrt{2}]$ is a field. A similar analysis applies to

$$\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}, \tag{6.1.30}$$

where $i = \sqrt{-1}$, and to many other cases, such as $\mathbb{Q}[\sqrt{3}]$ and $\mathbb{Q}[\sqrt{-5}]$. Note that these are vector spaces over $\mathbb{Q}$ of dimension 2.

We next look at $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, the ring generated by $\mathbb{Q}$, $\sqrt{2}$, and $\sqrt{3}$, i.e.,

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}. \tag{6.1.31}$$

This is a vector space over $\mathbb{Q}$ of dimension 4. It is in fact a field, but the demonstration is perhaps not as straightforward as that for $\mathbb{Q}[\sqrt{2}]$ in (6.1.29). That it is a field is, however, a special case of the following.

**Proposition 6.1.3.** *Let $\mathcal{R}$ be a ring such that $\mathbb{Q} \subset \mathcal{R} \subset \mathbb{C}$. Assume $\mathcal{R}$ is a finite-dimensional vector space over $\mathbb{Q}$. Then $\mathcal{R}$ is a field.*

**Proof.** Given a nonzero $a \in \mathcal{R}$, consider

$$M_a : \mathcal{R} \longrightarrow \mathcal{R}, \quad M_a b = ab, \tag{6.1.32}$$

which is linear over $\mathbb{Q}$. As long as $a \neq 0$, $M_a$ is clearly injective. The finite dimensionality of $\mathcal{R}$ then implies $M_a$ is surjective (cf. Corollary 1.3.7), so there exists $b \in \mathcal{R}$ such that $ab = 1$. □

Let $\mathcal{R}$ be as in Proposition 6.1.3. Say its dimension, as a vector space over $\mathbb{Q}$, is $n$. We write

$$\dim_{\mathbb{Q}} \mathcal{R} = n. \tag{6.1.33}$$

Take $\xi \in \mathcal{R}$. Then $\{1, \xi, \dots, \xi^n\}$ is a subset of $\mathcal{R}$ with $n + 1$ elements, so it is linearly dependent. Thus there exist $a_j \in \mathbb{Q}$, not all 0, such that

$$a_n \xi^n + \cdots + a_0 = 0. \tag{6.1.34}$$

We say $\xi$ is an algebraic number (of degree $\leq n$) if it satisfies an equation of the form (6.1.34). We have established the following.

**Proposition 6.1.4.** *If $\mathcal{R} \supset \mathbb{Q}$ is a ring satisfying* (6.1.33)*, then each $\xi \in \mathcal{R}$ is an algebraic number of degree $\leq n$.*

This has an easy converse.

**Proposition 6.1.5.** *If $\xi \in \mathbb{C}$ is an algebraic number of degree $n$, then the ring $\mathbb{Q}[\xi]$ has dimension $\leq n$.*

**Proof.** If $\xi$ satisfies (6.1.34) with $a_j \in \mathbb{Q}$, not all 0, then the set $\{1, \xi, \dots, \xi^{n-1}\}$ spans $\mathbb{Q}[\xi]$. □

Suppose we have two algebraic numbers, $\xi$, satisfying (6.1.34), and $\eta$, satisfying

$$b_m \eta^m + \cdots + b_0 = 0, \tag{6.1.35}$$

with $b_j \in \mathbb{Q}$, not all 0. Consider the ring $\mathbb{Q}[\xi, \eta] \subset \mathbb{C}$. Elements of this ring have the form

$$\sum_{j,k=0}^{N} a_{jk} \xi^j \eta^k, \quad a_{jk} \in \mathbb{Q},\ N \in \mathbb{N}. \tag{6.1.36}$$

The equations (6.1.34) and (6.1.35) guarantee that

$$\{\xi^j \eta^k : 0 \le j \le n-1, 0 \le k \le m-1\} \text{ spans } \mathbb{Q}[\xi, \eta],$$

as a vector space over $\mathbb{Q}$. Thus

$$\dim_{\mathbb{Q}} \mathbb{Q}[\xi, \eta] \le mn, \tag{6.1.37}$$

and Propositions 6.1.3–6.1.4 apply. Thus $\mathbb{Q}[\xi, \eta]$ is a field, and both $\xi + \eta$ and $\xi\eta$ belong to it, as does $\xi^{-1}$, if $\xi \neq 0$. Since, by Proposition 6.1.4, each element of $\mathbb{Q}[\xi, \eta]$ is an algebraic number, we have the following.

**Proposition 6.1.6.** *The set $\mathcal{A}$ of algebraic numbers in $\mathbb{C}$ is a field.*

A different proof of this result is given in section 6.2.

We can extend the argument leading to (6.1.37). If $a_j \in \mathbb{C}$ are algebraic numbers, of degree $\le m_j$, for $1 \le j \le \mu$, and if $\mathbb{Q}[a_1, \dots, a_\mu]$ is the ring generated by them, whose elements have the form

$$\sum_{j_1, \dots, j_\mu = 0}^{N} b_{j_1 \cdots j_\mu} a_1^{j_1} \cdots a_\mu^{j_\mu}, \quad b_{j_1 \cdots j_\mu} \in \mathbb{Q},\ N \in \mathbb{N}, \tag{6.1.38}$$

then

$$\dim_{\mathbb{Q}} \mathbb{Q}[a_1, \dots, a_\mu] \le m_1 \cdots m_\mu. \tag{6.1.39}$$

Suppose now that $\xi \in \mathbb{C}$ satisfies

$$a_\mu \xi^\mu + \cdots + a_1 \xi + a_0 = 0, \tag{6.1.40}$$

with $a_j \in \mathcal{A}$ as above, $a_\mu \neq 0$. Consider the ring

$$\mathbb{Q}[a_1, \dots, a_\mu, \xi] = \mathbb{F}[\xi], \tag{6.1.41}$$

where $\mathbb{F}$ is the field (thanks to (6.1.39) and Proposition 6.1.3)

$$\mathbb{F} = \mathbb{Q}[a_1, \dots, a_\mu]. \tag{6.1.42}$$

The equation (6.1.40) implies

$$\dim_{\mathbb{F}} \mathbb{F}[\xi] \le \mu, \tag{6.1.43}$$

This together with (6.1.39) gives

$$\dim_{\mathbb{Q}} \mathbb{Q}[a_1, \dots, a_\mu, \xi] \le \mu m_1 \cdots m_\mu. \tag{6.1.44}$$

Thus $\mathbb{Q}[a_1, \dots, a_\mu, \xi]$ is a field, consisting of algebraic numbers, and in particular we conclude that $\xi \in \mathcal{A}$. This proves the following.

**Proposition 6.1.7.** *The field $\mathcal{A}$ of algebraic numbers is algebraically closed.*

REMARK. The proof of Proposition 6.1.7 given above started with a root $\xi \in \mathbb{C}$ of (6.1.40), and hence made use of the fundamental theorem of algebra (established in Appendix A.1).

In light of Proposition 6.1.7, results of §§2.1–2.2 on eigenvectors and generalized eigenvectors apply, as do results of §13 on the Jordan canonical form. We record the latter.

**Proposition 6.1.8.** *Let $\mathcal{A} \subset \mathbb{C}$ denote the field of algebraic numbers. Given $A \in M(n, \mathcal{A})$, each eigenvalue of $A$ is an element of $\mathcal{A}$, and there exists an invertible $B \in M(n, \mathcal{A})$ such that $B^{-1}AB$ is in Jordan normal form.*

### More on determinants

Earlier in this section we noted that material in §1.5 extends to $n \times n$ matrices with coefficients in a general field $\mathbb{F}$, except that a modification is needed for fields in which $1 = -1$. (One says $\mathbb{F}$ has characteristic 2.) Here we provide a development of the determinant that works uniformly for all fields, including those of characteristic 2. The key is to establish the following variant of Proposition 1.5.1.

**Proposition 6.1.9.** *Let $\mathbb{F}$ be a field. There is a unique function*

$$\vartheta : M(n, \mathbb{F}) \longrightarrow \mathbb{F} \tag{6.1.45}$$

*satisfying the following three properties:*

*(a)* $\vartheta$ *is linear in each column of* $A$,
*(b′)* $\vartheta(A) = 0$ *if* $A$ *has two columns that are identical,*
*(c)* $\vartheta(I) = 1$.

*We denote this function by* det.

The way this differs from Proposition 1.5.1 (aside from involving more general fields) is that here the hypothesis (b′) replaces

(b) $\vartheta(\widetilde{A}) = -\vartheta(A)$ if $\widetilde{A}$ is obtained from $A$ by interchanging two columns.

From (b) it follows that $\vartheta(A) = -\vartheta(A)$ if two columns of $A$ are identical, and this implies $\vartheta(A) = 0$ unless $\mathbb{F}$ has characteristic 2. On the other hand, we claim that, for every field $\mathbb{F}$,

$$\text{(a) and (b}') \Rightarrow \text{(b)}. \tag{6.1.46}$$

To see this, let $\widetilde{A}$ be obtained from $A$ by switching columns $j$ and $k$; say $j < k$, so $A = (a_1, \dots, a_j, \dots, a_k, \dots, a_n)$. Then (a) and (b$'$) imply

$$\begin{aligned} \vartheta(A) &= \vartheta(a_1, \dots, a_j + a_k, \dots, a_k, \dots, a_n) \\ &= \vartheta(a_1, \dots, a_j + a_k, \dots, -a_j, \dots, a_n) \\ &= \vartheta(a_1, \dots, a_k, \dots, -a_j, \dots, a_n) \\ &= -\vartheta(\widetilde{A}), \end{aligned} \tag{6.1.47}$$

as desired.

**Proof of Proposition 6.1.9.** In light of (6.1.46), calculations made in the proof of Proposition 1.5.1 apply here to show that if $\vartheta$ satisfies (a), (b$'$) and (c) (and hence also (b)), then the following identity must hold:

$$\vartheta(A) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{\sigma(1)1} \cdots a_{\sigma(j)j} \cdots a_{\sigma(k)k} \cdots a_{\sigma(n)n}. \tag{6.1.48}$$

It remains to show that $\vartheta$, given by (6.1.48), satisfies (a), (b$'$), and (c). Arguments given in §1.5 show that $\vartheta$ satisfies (a), (b), and (c). It remains to show that $\vartheta$ satisfies (b$'$).

For this, let us set

$$S_n = S_n^+ \cup S_n^-, \quad S_n^\pm = \{\sigma \in S_n : \operatorname{sgn} \sigma = \pm 1\}, \tag{6.1.49}$$

so

$$\begin{aligned} \vartheta(A) &= \delta^+(A) - \delta^-(A), \\ \delta^\pm(A) &= \sum_{\sigma \in S_n^\pm} a_{\sigma(1)1} \cdots a_{\sigma(j)j} \cdots a_{\sigma(k)k} \cdots a_{\sigma(n)n}. \end{aligned} \tag{6.1.50}$$

Now suppose $\widetilde{A}$ is obtained from $A$ by switching columns $j$ and $k$ (say $j < k$). Then

$$\begin{aligned} \delta^+(\widetilde{A}) &= \sum_{\sigma \in S_n^+} a_{\sigma(1)1} \cdots a_{\sigma(j)k} \cdots a_{\sigma(k)j} \cdots a_{\sigma(n)n} \\ &= \sum_{\sigma \in S_n^+} a_{\sigma_{jk}(1)1} \cdots a_{\sigma_{jk}(j)j} \cdots a_{\sigma_{jk}(k)k} \cdots a_{\sigma_{jk}(n)n}, \end{aligned} \tag{6.1.51}$$

where

$$\sigma_{jk} = \sigma \circ \gamma_{jk}, \quad \gamma_{jk} \in S_n \ \text{ switches } j \text{ and } k. \tag{6.1.52}$$

For each such $j$ and $k$, $\{\sigma \circ \gamma_{jk} : \sigma \in S_n^+\} = S_n^-$, so (6.1.51) yields

$$\begin{aligned} \delta^+(A) &= \sum_{\sigma \in S_n^-} a_{\sigma(1)1} \cdots a_{\sigma(j)j} \cdots a_{\sigma(k)k} \cdots a_{\sigma(n)n} \\ &= \delta^-(A). \end{aligned} \tag{6.1.53}$$

In particular,

$$A = \widetilde{A} \Longrightarrow \delta^+(A) = \delta^-(A) \Longrightarrow \vartheta(A) = 0, \tag{6.1.54}$$

and we have (b′). This proves Proposition 6.1.9. □

## Exercises

1. Let $\mathbb{F}$ be a field. Show that, if $a, b \in \mathbb{F}$,

$$\begin{aligned} &a + b = a \Rightarrow b = 0, \\ &a + 0 \cdot a = (1 + 0)a = a, \\ &0 \cdot a = 0, \\ &a + b = 0 \Rightarrow b = -a, \\ &a + (-1)a = 0 \cdot a = 0, \\ &(-1)a = -a. \end{aligned}$$

*Hint.* See Exercise 2 of §1.1.

2. Let $V$ be a vector space over $\mathbb{F}$. Take $a \in \mathbb{F}$, $v, w \in V$. Show that the results (1.1.18) hold. Show also that

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

*Hint.* See Exercises 2–3 of §1.1.

3. Check (6.1.27) explicitly for $r = 2, 3$, and $5$.
Try to prove it for all primes $r$. *Hint.* See Appendix A.3.

4. Given $A = (a_{jk}) \in M(n, \mathbb{Z}/(2))$, pick

$$\widetilde{A} = (\tilde{a}_{jk}) \in M(n, \mathbb{Z}) \subset M(n, \mathbb{R}), \quad a_{jk} = \tilde{a}_{jk} \text{ mod } 2.$$

Show that $\det \widetilde{A}$ mod 2 is independent of the choice of such $\widetilde{A}$. Show that taking

$$\det : M(n, \mathbb{Z}/(2)) \longrightarrow \mathbb{Z}/(2), \quad \det A = \det \widetilde{A} \text{ mod } 2,$$

gives a good determinant on $M(n, \mathbb{Z}/(2))$.

5. For which primes $p$ does $-1$ have a square root in $\mathbb{Z}/(p)$?

6. Set $\mathbb{F} = \mathbb{Z}/(3)$ and consider the ring $\mathcal{R} = \mathbb{F}[\sqrt{-1}]$. Show that $\mathcal{R}$ is a field. What is $\dim_{\mathbb{F}} \mathcal{R}$?

In Exercises 7–8, we take

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in M(2, \mathbb{F}).$$

7. Find the eigenvalues and eigenvectors of $A$ when

$$\mathbb{F} = \mathbb{Z}/(2),$$
$$\mathbb{F} = \mathbb{Z}/(5).$$

8. Find the eigenvalues and eigenvectors of $A$ when

$$\mathbb{F} = \mathbb{Z}/(3)[\sqrt{-1}].$$

*Hint.* One task is to figure out what this object is and why it is a field. This was set up in Exercise 6. One might also peek ahead at Exercises 17–18 of §7.1. For still more, see Appendix A.4.

Exercises 9–12 expand on arguments used to prove Proposition 6.1.1.

9. Recall that an ideal in $\mathbb{Z}$ is a nonempty subset $\mathcal{I} \subset \mathbb{Z}$ satisfying (6.1.15). Show that, if $\mathcal{I} \subset \mathbb{Z}$ is a nonzero ideal and $\ell$ is the smallest positive element of $\mathcal{I}$, then

$$\mathcal{I} = (\ell) = \{\ell k : k \in \mathbb{Z}\}.$$

*Hint.* Review the proof of Proposition 6.1.1.

10. Generally, if $\ell_1, \dots, \ell_\mu \in \mathbb{Z}$, we set

$$(\ell_1, \dots, \ell_\mu) = \{\ell_1 k_1 + \cdots + \ell_\mu k_\mu : k_j \in \mathbb{Z}\}.$$

Show that this is an ideal. This is called the ideal in $\mathbb{Z}$ generated by the set $\{\ell_1, \dots, \ell_\mu\}$.

11. Given $m, n \in \mathbb{Z}$, both nonzero, apply Exercises 9–10 to the ideal $(m, n)$ to conclude that there exists $\ell \in \mathbb{N}$ such that $(m, n) = (\ell)$. Explain why $\ell$ is called the *greatest common divisor* of $m$ and $n$. We write

$$\ell = \gcd(m, n).$$

12. Given $m, n \in \mathbb{Z}$, both nonzero, we say they are relatively prime if they have no common prime factors. Show that this holds if and only if $\gcd(m, n) = 1$, and hence if and only if there exist $j, k \in \mathbb{Z}$ such that

$$mj + nk = 1.$$

13. Given $m, n \in \mathbb{N}$, we denote by $\operatorname{lcm}(m, n)$ the least common multiple of $m$ and $n$, i.e., the smallest element of $\mathbb{N}$ that is an integral multiple of both $m$ and $n$. Show that

$$\operatorname{lcm}(m, n) \cdot \gcd(m, n) = mn.$$

14. Take $m_1$ and $m_2$ in $\mathbb{N}$, say $m_2 < m_1$. This exercise sketches a method to compute $\gcd(m_1, m_2)$, known as the *Euclidean algorithm.* To start, divide $m_2$ into $m_1$, computing quotient and remainder, to write

$$m_1 = q_2 m_2 + m_3, \quad q_2 \in \mathbb{N},\ 0 \le m_3 < m_2.$$

If $m_3 = 0$, then $\gcd(m_1, m_2) = m_2$. Otherwise, show that

$$\gcd(m_1, m_2) = \gcd(m_2, m_3).$$

To proceed, write

$$m_2 = q_3 m_3 + m_4, \quad q_3 \in \mathbb{N},\ 0 \le m_4 < m_3,$$

and continue. Show that this process terminates in a finite number of steps, with

$$m_\nu = q_{\nu+1} m_{\nu+1},$$

hence $m_{\nu+1} = \gcd(m_1, m_2)$.

15. Show that the set $\mathcal{A}$ of algebraic numbers is countable.
*Hint.* The set of polynomials with rational coefficients is countable.

## 6.2. Rational matrices and algebraic numbers

Algebraic numbers are numbers that are roots of polynomials with rational coefficients. In other words, given $a \in \mathbb{C}$, $a$ is an algebraic number if and only if there exists a polynomial

$$p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0, \quad a_j \in \mathbb{Q}, \tag{6.2.1}$$

such that

$$p(a) = 0. \tag{6.2.2}$$

Clearly numbers like $2^{1/2}$ and $3^{1/3}$ are algebraic numbers. It might not be so clear that $2^{1/2} + 3^{1/3}$ and $(2^{1/2} + 3^{1/3})(5^{1/2} + 7^{1/3})$ are. Such results are special cases of the following (which was proved in Proposition 6.1.6, by a different method).

**Theorem 6.2.1.** *If $a, b \in \mathbb{C}$ are algebraic numbers, so are $a + b$ and $ab$. If also $a \neq 0$, then $1/a$ is an algebraic number. Hence the set of algebraic numbers is a field.*

Here we present another proof of this, using some linear algebra. The following result is the first key.

**Proposition 6.2.2.** *Given $a \in \mathbb{C}$, $a$ is an algebraic number if and only if there exists $A \in M(n, \mathbb{Q})$ such that $a$ is an eigenvalue of $A$.*

**Proof.** This proposition has two parts. For the first part, assume $A \in M(n, \mathbb{Q})$. The eigenvalues of $A$ are roots of the characteristic polynomial

$$p(z) = \det(zI - A). \tag{6.2.3}$$

It is clear that such $p(z)$ has the form (6.2.1), so by definition such roots are algebraic numbers.

For the converse, given that $a \in \mathbb{C}$ is a root of $p(z)$, as in (6.2.1), we can form the companion matrix,

$$A = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}, \tag{6.2.4}$$

as in (2.3.20), with 1s above the diagonal and the negatives of the coefficients $a_0, \dots, a_{n-1}$ along the bottom row. As shown in Proposition 2.3.4, if $A$ is given by (6.2.4), and $p(z)$ by (6.2.1), then (6.2.3) holds. Consequently, if $a \in \mathbb{C}$ is a root of $p(z)$, in (6.2.1), then $a$ is an eigenvalue of the matrix $A$ in (6.2.4), and such $A$ belongs to $M(n, \mathbb{Q})$. $\square$

Returning to Theorem 6.2.1, given algebraic numbers $a$ and $b$, pick $A \in M(n,\mathbb{Q})$ such that $a$ is an eigenvalue of $A$ and $B \in M(m,\mathbb{Q})$ such that $b$ is an eigenvalue of $B$. Consider

$$A \otimes I_m + I_n \otimes B : \mathbb{C}^{mn} \longrightarrow \mathbb{C}^{mn}. \tag{6.2.5}$$

It follows from Proposition 5.2.2 that

$$\operatorname{Spec}(A \otimes I_m + I_n \otimes B) = \{\alpha + \beta : \alpha \in \operatorname{Spec} A,\ \beta \in \operatorname{Spec} B\}. \tag{6.2.6}$$

Thus

$$a + b \text{ is an eigenvalue of } A \otimes I_m + I_n \otimes B \in M(mn,\mathbb{Q}), \tag{6.2.7}$$

so $a+b$ is an algebraic number.

Next, consider

$$A \otimes B : \mathbb{C}^{mn} \longrightarrow \mathbb{C}^{mn}. \tag{6.2.8}$$

Proposition 5.2.2 also gives

$$\operatorname{Spec}(A \otimes B) = \{\alpha\beta : \alpha \in \operatorname{Spec} A,\ \beta \in \operatorname{Spec} B\}. \tag{6.2.9}$$

Thus

$$ab \text{ is an eigenvalue of } A \otimes B \in M(mn,\mathbb{Q}), \tag{6.2.10}$$

so $ab$ is an algebraic number.

Finally, let $a \neq 0$ be an algebraic number. Then $a$ is a root of a polynomial of the form (6.2.1), and since $a \neq 0$, we can assume $a_0 \neq 0$ in (6.2.1). (Otherwise, factor out an appropriate power of $z$.) Now the identity (6.2.3) for the companion matrix $A$ in (6.2.4) implies

$$\det A = (-1)^n p(0) = (-1)^n a_0 \neq 0, \tag{6.2.11}$$

so $A \in M(n,\mathbb{Q})$ in (6.2.4) is invertible. Formulas for $A^{-1}$ from §1.5 yield

$$A^{-1} \in M(n,\mathbb{Q}), \tag{6.2.12}$$

and $1/a$ is an eigenvalue of $A^{-1}$. Hence $1/a$ is an algebraic number, as asserted. This finishes the proof of Theorem 6.2.1.

Chapter 7

# Rings and modules

The concept of a ring arose in Chapter 6, on the way to defining the concept of a field. A commutative ring $\mathcal{R}$ is endowed with operations of addition and multiplication, satisfying the usual commutative, associative, and distributive laws. One can drop the commutative law of multiplication to obtain the general class of rings. However, most of our attention in this chapter will be devoted to commutative rings with unit, as we discuss the extension of linear algebra from the study of vector spaces over fields to the study of modules over such a class of rings.

The basic definitions of these two classes of objects look quite similar. A module $\mathcal{M}$ over a ring $\mathcal{R}$ is a commutative, additive group, for which there is a "scalar multiplication" $a \in \mathcal{R},\ u \in \mathcal{M} \Rightarrow au \in \mathcal{M}$, satisfying the same sorts of associative and distributive laws as one has for vector spaces (including $1 \cdot u = u$). However, passing to rings allows for a much greater variety of phenomena.

To give some flavor of the difference, consider the $n$-fold product $\mathcal{R}^n$, whose elements are $n$-tuples of elements of a ring $\mathcal{R}$; picture these as columns. We can also bring in $M(n, \mathcal{R})$, consisting of $n \times n$ matrices of elements of $\mathcal{R}$, and form

$$Au \in \mathcal{R}^n, \quad \text{for} \ \ A \in M(n, \mathcal{R}),\ u \in \mathcal{R}^n, \tag{7.0.1}$$

just as done in Chapter 1. Furthermore, the notion of determinant extends, yielding $\det A \in \mathcal{R}$, whenever $\mathcal{R}$ is a commutative ring. However, if you examine the properties

$$A \text{ is injective,} \qquad A \text{ is surjective,} \qquad \det A \neq 0, \tag{7.0.2}$$

no two of these are necessarily equivalent. Some examples of differences arise from the fact that some rings, such as $\mathbb{Z}/(k)$ when $k$ is composite, have zero-divisors, i.e., there exist $a, b \in \mathcal{R}$, both nonzero, such that $ab = 0$. A ring with no such zero-divisors is called an integral domain. Yet, even when $\mathcal{R}$ is an integral domain, one does not have equivalence in (7.0.2).

Going further, recall that if $V$ is a vector space over a field $\mathbb{F}$, and if it is spanned by a finite set of elements, then it has a basis, and it is isomorphic to $\mathbb{F}^n$ for some $n$. On the other hand, for many rings $\mathcal{R}$, a module $\mathcal{M}$ over $\mathcal{R}$ spanned by a finite number of elements (we say finitely generated) need not be isomorphic to $\mathcal{R}^n$ for any $n$. If it is, we say $\mathcal{M}$ is *free.* Lots of finitely generated modules are not free.

Section 7.1 pursues such matters on a general level. It also introduces such concepts as submodules, quotient modules, and dual modules, and discusses similarities and differences with the vector space case. In subsequent sections we look at modules over several special classes of rings.

The first special class of rings we treat is the class of principal ideal domains (PIDs). A commutative ring with unit $\mathcal{R}$ that is an integral domain is a PID provided that, if $\mathcal{I} \subset \mathcal{R}$ is an ideal, i.e.,

$$a, b \in \mathcal{I} \Longrightarrow a + b \in \mathcal{I}, \quad a \in \mathcal{I},\ b \in \mathcal{R} \Longrightarrow ab \in \mathcal{I}, \tag{7.0.3}$$

then it has a single generator, i.e.,

$$\mathcal{I} = (a_0) = \{a_0 b : b \in \mathcal{R}\}. \tag{7.0.4}$$

Such a condition (though without the name) arose in the study of generalized eigenvectors, in §2.2. In current parlance, the content of Lemma 2.2.3 is that the polynomial ring $\mathbb{C}[t]$ is a PID. The same argument shows that $\mathbb{F}[t]$ is a PID whenever $\mathbb{F}$ is a field. Another example of a PID is $\mathbb{Z}$, and numerous further examples are considered in §7.2. There is a structure theory for finitely generated modules over a PID, $\mathcal{R}$. First, if $\mathcal{E}$ is such a module, there is a submodule $\mathcal{F} \subset \mathcal{E}$ that is free, and a direct sum decomposition

$$\mathcal{E} = \mathcal{E}_\tau \oplus \mathcal{F}, \tag{7.0.5}$$

where $\mathcal{E}_\tau$ consists of torsion elements of $\mathcal{E}$, i.e., of $u \in \mathcal{E}$ such that $au = 0$ for some nonzero $a \in \mathcal{R}$. The set $\mathcal{E}_\tau$ is seen to be a submodule of $\mathcal{F}$, necessarily finitely generated. Furthermore, there is an analysis of the structure of such a finitely generated torsion module, given in Proposition 7.2.14.

In §7.3 we apply the structure theory of §7.2 to the study of a transformation $A \in \mathcal{L}(V)$ when $V$ is a finite-dimensional vector space over a field $\mathbb{F}$. The transformation $A$ gives $V$ the structure of an $\mathbb{F}[t]$-module, via

$$p \cdot v = p(A)v, \quad p \in \mathbb{F}[t], \ v \in V. \tag{7.0.6}$$

The set of $p \in \mathbb{F}[t]$ such that $p(A) = 0$ is an ideal, hence generated by a single element $m_A \in \mathbb{F}[t]$, called the minimal polynomial of $A$. Since $m_A \cdot v = 0$ for all $v$, this makes $V$ a torsion module over $\mathbb{F}[t]$, and the structure theory of Proposition 7.2.14 applies. If $\mathbb{F}$ is algebraically closed, $m_A(t)$ factors into linear factors, and (for $\mathbb{F} = \mathbb{C}$) we recover results of Chapter 2 on generalized eigenspaces and on the Jordan canonical form for $A$, now in the setting of a general algebraically closed field. The reader might compare the approach here with that taken in Chapter 2, keeping in mind how the notion of $\mathbb{C}[t]$ as a PID arose in that earlier chapter.

We mention two other significant properties of PIDs established in §7.2. One is that if $\mathcal{R}$ is a PID,

$$\begin{aligned} &\mathcal{I}_j \subset \mathcal{R} \text{ ideals}, \quad \mathcal{I}_1 \subset \mathcal{I}_2 \subset \cdots \subset \mathcal{I}_k \subset \cdots \\ &\Longrightarrow \mathcal{I}_\ell = \mathcal{I}_{\ell+1} = \cdots, \quad \text{for some } \ \ell. \end{aligned} \tag{7.0.7}$$

Another is that if $\mathcal{R}$ is a PID and $a \in \mathcal{R} \setminus 0$ is not invertible, then we can write

$$a = p_1 \cdots p_N, \quad p_j \in \mathcal{R} \ \text{ irreducible}, \tag{7.0.8}$$

i.e., $p_j = bc, \ b, c \in \mathcal{R} \Rightarrow b$ or $c$ is invertible. Furthermore, this factorization is unique, up to ordering and multiplication by invertible elements. It is of great interest that these properties hold for all PIDs, and one also seeks other classes of rings for which they hold. In connection with this, we note that the polynomial rings

$$\mathbb{Z}[t] \text{ and } \mathbb{C}[x, y] \text{ are not PIDs.} \tag{7.0.9}$$

We take this as motivation to discuss two further classes of rings, in §§7.5–7.6, after an intermezzo in §7.4, devoted to the ring of algebraic integers and its finitely generated subrings, some of which are PIDs and others of which belong to categories considered below.

Section 7.5 is devoted to *Noetherian rings*. Such a ring $\mathcal{R}$ is a commutative ring with unit, satisfying (7.0.7). Another characterization is that each ideal $\mathcal{I} \subset \mathcal{R}$ is finitely generated. The content of (7.0.7) applied to PIDs is that each PID is a Noetherian ring. It is of great interest to know that the rings in (7.0.9) are also Noetherian rings. This is a consequence of a fundamental result known as the *Hilbert basis theorem*, which states that

$$\mathcal{R} \text{ Noetherian} \Rightarrow \mathcal{R}[t] \text{ Noetherian.} \tag{7.0.10}$$

Section 7.5 also treats Noetherian modules, an important extension of the class of finitely generated modules over a PID.

Section 7.6 treats *unique factorization domains* (UFDs). Such a domain is a commutative ring with unit that is an integral domain and satisfies (7.0.8), together with the accompanying essential uniqueness statement. The content of (7.0.8) applied to PIDs is that each PID is a UFD. As it turns out, in addition the rings in (7.0.9) are UFDs. More generally, as established in §7.6,

$$\mathcal{R} \text{ is a UFD} \Rightarrow \mathcal{R}[t] \text{ is a UFD}. \tag{7.0.11}$$

This opens up a substantially larger class of rings that are seen to be UFDs.

## 7.1. Rings and modules

The notion of a ring was defined in §6.1. For the purpose of this section, a ring will always have a unit, so it satisfies the conditions (6.1.1)–(6.1.10), except for (6.1.5) (whose validity then defines the notion of a commutative ring).

Given such a ring $\mathcal{R}$, a module over $\mathcal{R}$ is a set $\mathcal{M}$ with the following structure. First, it is a commutative, additive group. Next, there is a product $\mathcal{R} \times \mathcal{M} \to \mathcal{M}$, associating to each $a \in \mathcal{R}$ and $u \in \mathcal{M}$ an element $au \in \mathcal{M}$, and the product satisfies the following conditions, for all $a, b \in \mathcal{R}$ and $u, v \in \mathcal{M}$:

$$\begin{aligned} a(u+v) &= au + av, \\ (a+b)u &= au + bu, \\ (ab)u &= a(bu), \\ 1 \cdot u &= u. \end{aligned} \tag{7.1.1}$$

Note that these conditions are close to those defining a vector space. In fact, a vector space is precisely an $\mathcal{R}$-module when $\mathcal{R}$ is a field.

Such an $\mathcal{R}$-module is also called a left $\mathcal{R}$-module. A right $\mathcal{R}$-module is a commutative additive group $\mathcal{M}$ with a product $\mathcal{M} \times \mathcal{R} \to \mathcal{M}$, assigning ot each $a \in \mathcal{R}, u \in \mathcal{M}$ an element $ua \in \mathcal{M}$, satisfying, in place of (23.1), the conditions

$$\begin{aligned} (u+v)a &= ua + va, \\ u(a+b) &= ua + ub, \\ u(ab) &= (ua)b, \\ u \cdot 1 &= u. \end{aligned} \tag{7.1.2}$$

One class of examples of modules is provided by the class of commutative additive groups. If $\mathcal{M}$ is such a group, then $\mathcal{M}$ naturally has the structure of a $\mathbb{Z}$-module, with

$$ku = u + \cdots + u \quad (k \text{ summands}), \tag{7.1.3}$$

for $k \in \mathbb{N}, u \in \mathcal{M}$, and $(-k)u = -(ku)$.

To take another class of examples, the set $\mathcal{R}^n$, consisting of columns

$$u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, \quad u_j \in \mathcal{R}, \tag{7.1.4}$$

has the structure of a left $\mathcal{R}$-module, with

$$au = \begin{pmatrix} au_1 \\ \vdots \\ au_n \end{pmatrix}, \quad a \in \mathcal{R},\ u \in \mathcal{R}^n, \tag{7.1.5}$$

and also the structure of a right $\mathcal{R}$-module, with

$$ua = \begin{pmatrix} u_1 a \\ \vdots \\ u_n a \end{pmatrix}, \quad a \in \mathcal{R},\ u \in \mathcal{R}^n. \tag{7.1.6}$$

Next, consider $M(m \times n, \mathcal{R})$, the set of $m \times n$ matrices with entries in $\mathcal{R}$, with a typical element

$$U = \begin{pmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & & \vdots \\ u_{m1} & \cdots & u_{mn} \end{pmatrix}, \quad u_{jk} \in \mathcal{R}. \tag{7.1.7}$$

Matrix operations are defined as in §1.2. We see that $M(m \times n, \mathcal{R})$ is a left $M(m, \mathcal{R})$-module, and also a right $M(n, \mathcal{R})$-module, with products

$$(A, U) \mapsto AU, \quad (U, B) \mapsto UB, \tag{7.1.8}$$

given by matrix multiplication.

Suppose $\mathcal{M}_1$ and $\mathcal{M}_2$ are both left $\mathcal{R}$-modules. A map

$$T : \mathcal{M}_1 \longrightarrow \mathcal{M}_2 \tag{7.1.9}$$

is said to be a module homomorphism (also called an $\mathcal{R}$-linear map) provided

$$T(au + bv) = aTu + bTv, \tag{7.1.10}$$

for all $a, b \in \mathcal{R}$, $u, v \in \mathcal{M}_1$. If instead $\mathcal{M}_1$ and $\mathcal{M}_2$ are right $\mathcal{R}$-modules, the condition for $T$ to be $\mathcal{R}$-linear is

$$T(ua + vb) = (Tu)a + (Tv)b, \tag{7.1.11}$$

for all such $a, b, u, v$.

For some examples of module homomorphisms, take $A \in M(m \times n, \mathcal{R})$ and consider

$$A : \mathcal{R}^n \longrightarrow \mathcal{R}^m, \tag{7.1.12}$$

with $Au$ given by matrix multiplication, as in (1.2.5). This is an $\mathcal{R}$-module homomorphism, for $\mathcal{R}^n$ and $\mathcal{R}^m$ considered as right $\mathcal{R}$-modules. Generally, it is not a homomorphism of left $\mathcal{R}$-modules, unless $\mathcal{R}$ is a commutative ring (or at least all the matrix entries $a_{jk}$ commute with each element of $\mathcal{R}$). Partly for this reason, modules over commutative rings have more in common with vector spaces than those over non-commutative rings.

Given $\mathcal{R}$-modules $\mathcal{M}_j$, we denote by $\mathcal{L}(\mathcal{M}_1, \mathcal{M}_2)$ the set of $\mathcal{R}$-linear maps from $\mathcal{M}_1$ to $\mathcal{M}_2$, if the ring $\mathcal{R}$ is understood. If we want to emphasize what $\mathcal{R}$ is, we write $\mathrm{Hom}_{\mathcal{R}}(\mathcal{M}_1, \mathcal{M}_2)$. One might see a need for notation that distinguishes between the cases of left $\mathcal{R}$-modules and right $\mathcal{R}$-modules, but we will not bring in further notational baggage.

In fact, we will have no need to. From here on, we will restrict our attention to the case where $\mathcal{R}$ is a commutative ring, with unit (and, without loss of generality, all modules will be left modules). Note that $\mathrm{Hom}_{\mathcal{R}}(\mathcal{M}_1, \mathcal{M}_2)$ gets the structure of an $\mathcal{R}$-module, such that

$$(aT)(u) = a(Tu). \tag{7.1.13}$$

In linear algebra over such a commutative ring, some results we have seen in the vector space setting extend quite cleanly, and some need moderate to substantial modification. We look at some clean extensions first, starting with determinants.

If $m = n$ in (7.1.12), the $n \times n$ matrix

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}, \quad a_{jk} \in \mathcal{R}, \tag{7.1.14}$$

represents the general $\mathcal{R}$-linear map from $\mathcal{R}^n$ to itself. We can extend Proposition 1.5.1 to produce the determinant function

$$\det : M(n, \mathcal{R}) \longrightarrow \mathcal{R}, \tag{7.1.15}$$

with essentially no change in the argument, as long as $\mathcal{R}$ has the property that

$$a \in \mathcal{R},\ a \neq 0 \Longrightarrow a \neq -a. \tag{7.1.16}$$

In such a case, we again obtain the formula (1.5.29), i.e.,

$$\det A = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n}. \tag{7.1.17}$$

Next, the proof of Proposition 1.5.3 goes through, so we have

$$\det(AB) = (\det A)(\det B), \tag{7.1.18}$$

provided $A, B \in M(n, \mathcal{R})$, where $\mathcal{R}$ is a commutative ring, with unit, satisfying (7.1.16).

There are rings that do not satisfy (7.1.16), such as $\mathbb{Z}/(2)$, which is not only a commutative ring with unit, but actually a field. What fails when $\mathcal{R}$ does not satisfy (7.1.16) is the deduction (1.5.12) from rule (b) in Proposition 1.5.1, since what rule (b) gives directly is $\det B = -\det B$, whenever $B$ has two identical columns. As we will see, we can extend the determinant to work for all commutative rings $\mathcal{R}$ with unit, even when (7.1.16) fails. We describe one approach below. For another, see Exercise 7 below.

To do this, let $\{x_\alpha : \alpha \in \mathcal{A}\}$ be a (possibly infinite) set of "variables," and form the ring

$$\widetilde{\mathcal{R}} = \mathbb{Z}[x_\alpha, \alpha \in \mathcal{A}], \tag{7.1.19}$$

i.e., the ring of polynomials in these variables, with coefficients in $\mathbb{Z}$. Certainly $\widetilde{\mathcal{R}}$ satisfies (7.1.16), so we have a determinant

$$\det_{\widetilde{\mathcal{R}}} : M(n, \widetilde{\mathcal{R}}) \longrightarrow \widetilde{\mathcal{R}}, \tag{7.1.20}$$

satisfying (7.1.17) and (7.1.18). Now let $\mathcal{R}$ be an arbitrary commutative ring with unit, perhaps not satisfying (7.1.16). Pick a set $\mathcal{A}$ and a map $x_\alpha \mapsto a_\alpha$ such that $\{a_\alpha : \alpha \in \mathcal{A}\}$ generates $\mathcal{R}$, i.e., every element of $\mathcal{R}$ is a polynomial (with integer coefficients) in these elements $a_\alpha$. (One possiblility is that $\mathcal{A} = \mathcal{R}$ and $a_\alpha = \alpha$.) This gives rise to a map

$$\varphi : \widetilde{\mathcal{R}} \longrightarrow \mathcal{R}, \tag{7.1.21}$$

taking a polynomial in $\{x_\alpha\}$ with integral coefficients to the corresponding polynomial in $\{a_\alpha\}$. This is a ring homomorphism, i.e.,

$$\varphi(p+q) = \varphi(p) + \varphi(q), \quad \varphi(pq) = \varphi(p)\varphi(q), \tag{7.1.22}$$

for all $p, q \in \widetilde{\mathcal{R}}$. Also it is surjective, i.e., given $a \in \mathcal{R}$, $a = \varphi(p)$ for some $p \in \widetilde{\mathcal{R}}$ (perhaps not unique). This gives rise to ring homomorphisms

$$\varphi_n : M(n, \widetilde{\mathcal{R}}) \longrightarrow M(n, \mathcal{R}), \tag{7.1.23}$$

taking $(x_{jk})_{1 \le j,j \le n}$ to $(\varphi(x_{jk}))$, and these maps are surjective. Thus, given $A \in M(n, \mathcal{R})$, one can pick

$$X \in M(n, \widetilde{\mathcal{R}}) \ \text{ such that } \ \varphi_n(X) = A. \tag{7.1.24}$$

We propose to define $\det : M(n, \mathcal{R}) \to \mathcal{R}$ so that

$$\det A = \varphi(\det_{\widetilde{\mathcal{R}}} X), \tag{7.1.25}$$

for $X$ as in (7.1.24). We need to show that (7.1.25) depends only on $A$, so we get the same result if $X$ in (7.1.24) is replaced by $Y \in M(n, \widetilde{\mathcal{R}})$ such that $\varphi_n(Y) = A$. Indeed, since the analogue of (7.1.17) holds for $\det_{\widetilde{\mathcal{R}}}$ in (7.1.20), it follows that, whenever (7.1.24) holds, for $A \in M(n, \mathcal{R})$, of the form (7.1.14), then $\det A$ satisfies (7.1.17), which indeed depends only on $A$. Thus $\det : M(n, \mathcal{R}) \to \mathcal{R}$ is well defined by (7.1.24)–(7.1.25). The fact that $\varphi$ is a ring homomorphism then gives (7.1.18).

With these arguments accomplished, one can extend the results of Exercises 7–9 of §1.5, on expanding determinants by minors, to matrices whose entries belong to a commutative ring $\mathcal{R}$, first in case $\mathcal{R}$ satisfies (7.1.16), hence for $\mathcal{R} = \widetilde{\mathcal{R}}$ as in (7.1.19), then for general commutative $\mathcal{R}$. One can then proceed from (1.5.52) to the Cramer formula (1.5.54), i.e.

$$CA = (\det A)I, \quad C = (c_{jk}), \quad c_{jk} = (-1)^{j-k} \det A_{kj}, \tag{7.1.26}$$

with $A_{kj} \in M(n-1, \mathcal{R})$ as in (1.5.52). If we replace $A \in M(n, \mathcal{R})$ by its transpose $A^t$, the argument yielding (1.5.37), i.e.,

$$\det A = \det A^t, \tag{7.1.27}$$

continues to hold. Then we can replace $A$ by $A^t$ in (7.1.26) and take the transpose of the resulting identity, to get

$$AC = (\det A)I. \tag{7.1.28}$$

One consequence of the identities above is the following variant of Proposition 1.5.6.

**Proposition 7.1.1.** *Let $\mathcal{R}$ be a commutative ring with unit and let $A \in M(n, \mathcal{R})$. Then $A$ is invertible if and only if*

$$\det A \textit{ has a multiplicative inverse in } \mathcal{R}. \tag{7.1.29}$$

**Proof.** If $\det A$ has an inverse $b \in \mathcal{R}$, then $bC$ is the inverse of $A$. Conversely, if $A$ has an inverse $B$ then $(\det B)(\det A) = 1$, so $\det B$ is the multiplicative inverse of $\det A$. $\square$

Invertibility of such $A$ is equivalent to the map $A : \mathcal{R}^n \to \mathcal{R}^n$ being both

$$\begin{aligned} &\text{one-to-one (injective)}, \\ \text{and}& \\ &\text{onto (surjective)}. \end{aligned} \tag{7.1.30}$$

In the case of $n$-dimensional vector spaces over a field, these two properties are equivalent, and they are also equivalent to the condition $\det A \neq 0$. Matters are different for other rings.

For example, take $n = 1, \mathcal{R} = \mathbb{Z}$, and $A \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Then $A : \mathbb{Z} \to \mathbb{Z}$ is injective but not surjective. Generally, for $n = 1$, $A$ surjective $\Rightarrow Au = 1$ for some $u \in \mathcal{R} \Rightarrow A$ invertible. The converse is clear, so

$$\text{For } n = 1,\ A \text{ is surjective} \Leftrightarrow A \text{ is invertible.} \tag{7.1.31}$$

On the other hand, if we set

$$\mathcal{Z}(\mathcal{R}) = \{a \in \mathcal{R} : ab = 0 \text{ for some nonzero } b \in \mathcal{R}\}, \tag{7.1.32}$$

then

$$\text{For } n = 1,\ A \text{ is injective} \Leftrightarrow A \in \mathcal{R} \setminus \mathcal{Z}(\mathcal{R}). \tag{7.1.33}$$

The set $\mathcal{Z}(\mathcal{R})$ is called the set of zero divisors in $\mathcal{R}$. If $\mathcal{R}$ is a commutative ring with unit and $\mathcal{Z}(\mathcal{R}) = 0$, we say $\mathcal{R}$ is an *integral domain*. Clearly $\mathbb{Z}$ is an integral domain. Every field is an integral domain, including $\mathbb{Z}/(p)$ for $p$ prime. However, if $n$ is composite, say $n = jk,\ j, k \geq 2$, then

$$n = jk \Longrightarrow j, k \in \mathcal{Z}(\mathbb{Z}/(n)). \tag{7.1.34}$$

Returning to the study of $A \in M(n, \mathcal{R})$ for general $n$, we see from (7.1.26) and (7.1.28) that

$$\begin{gathered} A \text{ and } C \text{ both injective} \Longleftrightarrow \det A \notin \mathcal{Z}(\mathcal{R}), \\ A \text{ and } C \text{ both surjective} \Longleftrightarrow \det A \text{ invertible in } \mathcal{R}. \end{gathered} \tag{7.1.35}$$

In particular, if $\mathcal{R}$ is an integral domain, then $A$ and $C$ are both injective if and only if $\det A \neq 0$. In this case, we can go further.

**Proposition 7.1.2.** *If $\mathcal{R}$ is an integral domain and $A \in M(n, \mathcal{R})$, then*

$$A \textit{ is injective } \Longleftrightarrow \det A \neq 0. \tag{7.1.36}$$

**Proof.** The "$\Leftarrow$" part follows from the first part of (7.1.35). To establish the "$\Rightarrow$" part, we bring in the following important construction. □

Given an integral domain $\mathcal{R}$, we associate a field $\mathbb{F}_{\mathcal{R}}$, called the quotient field of $\mathcal{R}$, as follows. Elements of $\mathbb{F}_{\mathcal{R}}$ consist of equivalence classes of objects

$$\frac{a}{b}, \quad a, b \in \mathcal{R}, \quad b \neq 0, \tag{7.1.37}$$

where the equivalence relation is

$$\frac{a}{b} \sim \frac{a'}{b'} \Longleftrightarrow ab' = a'b. \tag{7.1.38}$$

If also $c, d \in \mathcal{R},\ d \neq 0$, set

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{7.1.39}$$

Since $\mathcal{R}$ is an integral domain, we have $bd \neq 0$. These operations respect the equivalence relation (7.1.38) and lead to a well defined sum and product on $\mathbb{F}_{\mathcal{R}}$, which is then seen to be a field. In particular, for $a, b \in \mathcal{R}$,

$$a \neq 0,\ b \neq 0 \Longrightarrow \Big(\frac{a}{b}\Big)^{-1} = \frac{b}{a}. \tag{7.1.40}$$

We have a map

$$\iota : \mathcal{R} \longrightarrow \mathbb{F}_{\mathcal{R}}, \quad \iota(a) = \frac{a}{1}, \tag{7.1.41}$$

and if $\mathcal{R}$ is an integral domain, this is an injective ring homomorphism. Note that

$$\mathcal{R} = \mathbb{Z} \Longrightarrow \mathbb{F}_{\mathcal{R}} = \mathbb{Q}. \tag{7.1.42}$$

Also, in notation introduced below (6.1.24),

$$\mathcal{R} = \mathbb{Z}[\lambda] \Longrightarrow \mathbb{F}_{\mathcal{R}} = \mathbb{Q}(\lambda). \tag{7.1.43}$$

We now turn to the implication "$\Rightarrow$" in Proposition 7.1.2. Using (7.1.41), we induce the injective ring homomorphism

$$\iota_n : M(n, \mathcal{R}) \longrightarrow M(n, \mathbb{F}_{\mathcal{R}}). \tag{7.1.44}$$

Given $A \in M(n, \mathcal{R})$,

$$\det(\iota_n A) = \iota(\det A). \tag{7.1.45}$$

Denote $\iota_n A$ by $A^{\#}$. We have

$$A : \mathcal{R}^n \longrightarrow \mathcal{R}^n, \quad A^{\#} : (\mathbb{F}_{\mathcal{R}})^n \longrightarrow (\mathbb{F}_{\mathcal{R}})^n, \tag{7.1.46}$$

and both operations are given by left multiplication by the same matrix. Suppose $u \in (\mathbb{F}_{\mathcal{R}})^n$. Then $u = (u_1, \dots, u_n)^t$ and each $u_j = a_j/b_j$ with $a_j, b_j \in \mathcal{R},\ b_j \neq 0$. Then

$$A^{\#} u = 0 \Longrightarrow Av = 0, \tag{7.1.47}$$

where

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \quad v_j = u_j \Bigl( \prod_{\ell=1}^{n} b_\ell \Bigr) = a_j \Bigl( \prod_{\ell \neq j} b_\ell \Bigr) \in \mathcal{R}. \tag{7.1.48}$$

Hence

$$A \text{ injective} \Rightarrow A^{\#} \text{ injective}. \tag{7.1.49}$$

But since $\mathbb{F}_{\mathcal{R}}$ is a field, results discussed in §6.1 give

$$A^{\#} \text{ injective} \Leftrightarrow A^{\#} \text{ surjective } \Leftrightarrow \det A^{\#} \neq 0, \tag{7.1.50}$$

and then the identity (7.1.45) finishes the proof of Proposition 7.1.2.

Contrast with the vector space case indicates that we will not be seeking a version of a decomposition of $\mathcal{R}^n$ into something like generalized eigenspaces of $A \in M(n, \mathcal{R})$ for general commutative rings with unit. Despite this, we are able to generalize the Cayley-Hamilton theorem in this setting.

**Proposition 7.1.3.** *Let $\mathcal{R}$ be a commutative ring with unit. Given $A \in M(n, \mathcal{R})$, form*

$$K_A(\lambda) = \det(\lambda I - A), \quad K_A \in \mathcal{R}[\lambda]. \tag{7.1.51}$$

*Then*

$$K_A(A) = 0. \tag{7.1.52}$$

**Proof.** We bring in the ring

$$\mathcal{R}^{\#} = \mathbb{Z}[z_{jk}, 1 \le j, k \le n] \tag{7.1.53}$$

of polynomials in the variables $z_{jk}$, with coefficients in $\mathbb{Z}$, and consider

$$Z = (z_{jk}), \quad p(Z) = (p_{hi}(Z)) = K_Z(Z), \quad p_{hi} \in \mathbb{Z}[z_{jk}, 1 \le j, k \le n]. \tag{7.1.54}$$

The Cayley-Hamilton theorem for complex matrices established in §2.3 gives

$$p(B) = 0, \quad \forall\, B \in M(n, \mathbb{C}). \tag{7.1.55}$$

Now, parallel to (6.1.26), we deduce that, for $p$ as in (7.1.54),

$$p_{hi} = 0 \ \text{ in } \ \mathbb{Z}[z_{jk}, 1 \le j, k \le n], \tag{7.1.56}$$

i.e., all the coefficients of the polynomial $p(Z)$ are zero. Now $K_A(A) = p(A)$, and if we plug in the values $a_{jk} \in \mathcal{R}$ into the polynomial $p(Z)$, we also get 0, proving the proposition. $\square$

The last few pages have concentrated on $\mathcal{R}$-modules of the form $\mathcal{R}^n$. These are special cases of finitely generated modules. We say a set $S = \{s_\alpha\}$ in an $\mathcal{R}$-module $\mathcal{M}$ generates $\mathcal{M}$ (over $\mathcal{R}$) provided each $u \in \mathcal{M}$ can be written as a finite linear combination

$$u = \sum_\alpha a_\alpha s_\alpha, \quad a_\alpha \in \mathcal{R}. \tag{7.1.57}$$

Borrowing notation from §1.3, we write

$$\mathcal{M} = \operatorname{Span} S. \tag{7.1.58}$$

If a finite set $S$ generates $\mathcal{M}$, we say $\mathcal{M}$ is finitely generated. For $\mathcal{R}^n$ we have the set of generators $\{e_j : 1 \le j \le n\}$, where $e_j \in \mathcal{R}^n$ has a 1 in the $j$th slot and zeroes elsewhere. If $\mathcal{R} = \mathbb{F}$ is a field and $V$ is an $\mathbb{F}$-module, then we know that any minimal spanning set is a basis of the vector space $V$, any two bases have the same number of elements, denoted $\dim V$, and if $\dim V = n$, then $V$ is isomorphic to $\mathbb{F}^n$. For other rings $\mathcal{R}$, a finitely generated $\mathcal{R}$-module might not be isomorphic to $\mathcal{R}^n$ for any $n$.

For a class of examples, take $n \in \mathbb{N}$, $n \ge 2$, and consider $\mathbb{Z}/(n)$. As seen in §6.1, this is a ring. It is also a $\mathbb{Z}$-module. It is clearly not isomorphic to $\mathbb{Z}^k$ for any $k \in \mathbb{N}$. Of course, it is finitely generated, by the unit 1. Suppose $n = jk$, with $j, k \ge 2$, and assume $j$ and $k$ are relatively prime, so $\gcd(j, k) = 1$. Then, by Exercise 12 of §6.1, the set $\{j, k\}$ generates $\mathbb{Z}/(n)$, over $\mathbb{Z}$. It is a minimal generating set, since neigher $\{j\}$ nor $\{k\}$ generate $\mathbb{Z}/(n)$. Thus we have different minimal generating sets of $\mathbb{Z}/(n)$ with different numbers of elements.

Recall from §6.1 that $(n) = \{nk : k \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z}$. More generally, if $\mathcal{R}$ is a commutative ring, an ideal in $\mathcal{R}$ is a set $\mathcal{I} \subset \mathcal{R}$ saisfying

$$a, b \in \mathcal{I} \Rightarrow a + b \in \mathcal{I}, \quad a \in \mathcal{I},\ b \in \mathcal{R} \Rightarrow ab \in \mathcal{I}. \tag{7.1.59}$$

As noted above (6.1.21), examples of ideals in $\mathbb{C}[\lambda]$ arose in §2.2. Namely, if $A \in M(n, \mathbb{C})$, we have the ideal

$$\mathcal{I}_A = \{p \in \mathbb{C}[\lambda] : p(A) = 0\}. \tag{7.1.60}$$

We could replace $\mathbb{C}$ by an arbitrary field, or even by an arbitrary commutative ring.

It is clear from the characterization (7.1.59) that an ideal $\mathcal{I}$ in a commutative ring $\mathcal{R}$ is an $\mathcal{R}$-module. In the case $\mathcal{R} = \mathbb{Z}$, $\mathcal{I} = (n)$ discussed above, we have $\mathcal{I}$ isomorphic to $\mathbb{Z}$, as a $\mathbb{Z}$-module. A similar circumstance happens for $\mathcal{R} = \mathbb{C}[\lambda]$, $\mathcal{I} = \mathcal{I}_A$, as in (7.1.60); such $\mathcal{I}_A$ is isomorphic to $\mathbb{C}[\lambda]$ as a $\mathbb{C}[\lambda]$-module. This is a consequence of Lemma 2.2.3, producing the minimal polynomial $m_A(\lambda)$, as in (2.2.13). In fact, Lemma 2.2.3 and Exercise 9 of §6.1 imply that $\mathbb{C}[\lambda]$ and $\mathbb{Z}$ are both *principal ideal domains* (PIDs). By definition, a commutative ring with unit $\mathcal{R}$ is a PID provided that it is an integral domain and each ideal $\mathcal{I} \subset \mathcal{R}$ has the form

$$\mathcal{I} = (b) = \{ab : a \in \mathcal{R}\}, \tag{7.1.61}$$

for some $b \in \mathcal{R}$. Whenever $\mathcal{R}$ is a PID, then each nonzero ideal $\mathcal{I}$ in $\mathcal{R}$ is isomorphic to $\mathcal{R}$, as an $\mathcal{R}$-module.

An example of a ring that is not a PID is $\mathbb{C}[x, y]$, the ring of polynomials in two variables (with coefficients in $\mathbb{C}$). Then the ideal

$$\mathcal{I} = (x, y) = \{p \in \mathbb{C}[x, y] : p(0, 0) = 0\} \tag{7.1.62}$$

is not of the form (7.1.61). As a $\mathbb{C}[x, y]$ module, this has a minimum of two generators. It is not isomorphic to $\mathbb{C}[x, y]^n$ for any $n$.

Given a commutative ring with unit $\mathcal{R}$ and an ideal $\mathcal{I} \subset \mathcal{R}$, one can also form the quotient $\mathcal{R}/\mathcal{I}$, whose elements consist of equivalence classes of elements of $\mathcal{R}$, with the equivalence relation

$$a \sim a' \Longleftrightarrow a - a' \in \mathcal{I}. \tag{7.1.63}$$

Clearly $\mathcal{R}/\mathcal{I}$ has both a natural ring structure and a natural $\mathcal{R}$-module structure.

The case $\mathcal{R} = \mathbb{Z}$, $\mathcal{I} = (n)$, yielding $\mathbb{Z}/(n)$, has been discussed. We turn to the ideal (7.1.60), and expand the scope a bit. Let $V$ be an $n$-dimensional vector space over a field $\mathbb{F}$, and let $A \in \mathcal{L}(V)$. Then set

$$\mathcal{I}_A = \{p \in \mathbb{F}[\lambda] : p(A) = 0\}. \tag{7.1.64}$$

The map $p \mapsto p(A)$ is a ring homomorphism

$$\varphi : \mathbb{F}[\lambda] \longrightarrow \mathcal{L}(V), \tag{7.1.65}$$

and the null space $\mathcal{N}(\varphi)$ of such a ring homomorphism is readily seen to be an ideal. The proof of Lemma 2.2.3 extends to yield, for any field $\mathbb{F}$,

$$\mathbb{F}[\lambda] \text{ is a PID.} \tag{7.1.66}$$

Thus

$$\mathcal{I}_A = (m_A), \tag{7.1.67}$$

for some polynomial $m_A \in \mathbb{F}[\lambda]$, called the minimal polynomial of $A$, when normalized to have leading coefficient 1. The ring homomorphism (7.1.65) induces an isomorphism

$$\tilde{\varphi} : \mathbb{F}[\lambda]/\mathcal{I}_A \xrightarrow{\approx} \mathcal{R}_A \subset \mathcal{L}(V), \tag{7.1.68}$$

where

$$\mathcal{R}_A \text{ is the ring generated by } I \text{ and } A \text{ in } \mathcal{L}(V). \tag{7.1.69}$$

In (7.1.68), $\tilde{\varphi}$ is also an isomorphism of $\mathbb{F}[\lambda]$-modules, where $\mathbb{F}[\lambda]$ acts on $\mathcal{L}(V)$ by

$$p \cdot B = p(A)B, \tag{7.1.70}$$

making $\mathcal{L}(V)$ a left $\mathbb{F}[\lambda]$-module, and this action preserves $\mathcal{R}_A$.

We move from constructions that involve ideals in a ring to constructions that involve submodules. If $\mathcal{M}$ is an $\mathcal{R}$-module, a nonempty subset $\mathcal{N} \subset \mathcal{M}$ is a submodule provided

$$a, b \in \mathcal{R},\ u, v \in \mathcal{N} \Longrightarrow au + bv \in \mathcal{N}. \tag{7.1.71}$$

Examples arise from homomorphisms of $\mathcal{R}$-modules, defined in (7.1.9)–(7.1.10). If $T \in \mathrm{Hom}_{\mathcal{R}}(\mathcal{M}_1, \mathcal{M}_2)$, we have

$$\begin{aligned} \mathcal{N}(T) &= \{u \in \mathcal{M}_1 : Tu = 0\}, \\ \mathcal{R}(T) &= \{Tu : u \in \mathcal{M}_1\}, \end{aligned} \tag{7.1.72}$$

which are submodules of $\mathcal{M}_1$ and $\mathcal{M}_2$, respectively. Whenever $\mathcal{M}$ is an $\mathcal{R}$-module and $\mathcal{N}$ is a submodule, we can form the quotient module $\mathcal{M}/\mathcal{N}$, consisting of equivalence classes of elements of $\mathcal{M}$, with the equivalence relation

$$u \sim u' \Longleftrightarrow u - u' \in \mathcal{N}, \tag{7.1.73}$$

and this has a natural $\mathcal{R}$-module structure. An $\mathcal{R}$-homomorphism $T : \mathcal{M}_1 \to \mathcal{M}_2$ induces an isomorphism

$$\widetilde{T} : \mathcal{M}_1/\mathcal{N}(T) \xrightarrow{\approx} \mathcal{R}(T) \tag{7.1.74}$$

of $\mathcal{R}$-modules. Using these concepts, we have the following description of an arbitrary finitely-generated $\mathcal{R}$-module.

**Proposition 7.1.4.** *Assume $\mathcal{M}$ is a finitely generated $\mathcal{R}$-module, with $n$ generators. Then there is an isomorphism of $\mathcal{R}$-modules*

$$\mathcal{M} \approx \mathcal{R}^n/\mathcal{N}, \tag{7.1.75}$$

*for some submodule $\mathcal{N}$ of $\mathcal{R}^n$.*

**Proof.** Let $\{u_j : 1 \le j \le n\}$ generate $\mathcal{M}$. Take the generators $\{e_j : 1 \le j \le n\}$ of $\mathcal{R}^n$ mentioned below (7.1.59), and define

$$\varphi : \mathcal{R}^n \longrightarrow \mathcal{M}, \quad \varphi\Big(\sum a_j e_j\Big) = \sum a_j u_j, \quad a_j \in \mathcal{R}. \tag{7.1.76}$$

Then $\varphi$ is a surjective $\mathcal{R}$-homomorphism, and the isomorphism (7.1.75), taking $\mathcal{N} = \mathcal{N}(\varphi)$, follows from (7.1.74). $\square$

Next we consider duals of modules. If $\mathcal{R}$ is a commutative ring with unit and $\mathcal{M}$ is an $\mathcal{R}$-module, we define the *dual module*

$$\mathcal{M}' = \mathrm{Hom}_{\mathcal{R}}(\mathcal{M}, \mathcal{R}). \tag{7.1.77}$$

It is readily verified that

$$(\mathcal{R}^n)' \approx \mathcal{R}^n. \tag{7.1.78}$$

On the other hand, the $\mathbb{Z}$-module $\mathbb{Z}/(n)$ satisfies

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}) = 0. \tag{7.1.79}$$

This example illustrates that frequently $(\mathcal{M}')'$ is not isomorphic to $\mathcal{M}$, in contrast to the case for finite dimensional vector spaces over a field. The following relative of Proposition 7.1.4 also contains (7.1.79). The proof is left to the reader.

**Proposition 7.1.5.** *Given the $\mathcal{R}$-module $\mathcal{M} = \mathcal{R}^n/\mathcal{N}$, where $\mathcal{N}$ is a submodule of $\mathcal{R}^n$,*

$$\mathcal{M}' \approx \big\{\varphi \in (\mathcal{R}^n)' : \varphi\big|_{\mathcal{N}} = 0\big\}. \tag{7.1.80}$$

More generally, extending the scope of §5.1, we can consider multi-linear maps. If $\mathcal{V}_j$ and $\mathcal{W}$ are $\mathcal{R}$-modules, we set

$$\begin{aligned} \mathcal{M}(\mathcal{V}_1, \dots, \mathcal{V}_\ell; \mathcal{W}) = \text{set of maps } \beta : \mathcal{V}_1 \times \cdots \times \mathcal{V}_\ell \to \mathcal{W} \\ \text{that are } \mathcal{R}\text{-linear in each variable,} \end{aligned} \tag{7.1.81}$$

in the sense that, for each $j \in \{1, \dots, \ell\}$,

$$\begin{aligned} &v_j, w_j \in \mathcal{V}_j,\ a, b \in \mathcal{R} \Longrightarrow \\ &\qquad \beta(u_1, \dots, av_j + bw_j, \dots, u_\ell) \\ &\qquad = a\beta(u_1, \dots, v_j, \dots, u_\ell) + b\beta(u_1, \dots, w_j, \dots, u_\ell). \end{aligned} \tag{7.1.82}$$

This has the natural structure of an $\mathcal{R}$-module. If all the $\mathcal{V}_j$ are the same, we set

$$\mathcal{M}^\ell(\mathcal{V},\mathcal{W}) = \mathcal{M}(\mathcal{V}_1,\dots,\mathcal{V}_\ell;\mathcal{W}), \quad \mathcal{V}_1 = \cdots = \mathcal{V}_\ell = \mathcal{V}. \tag{7.1.83}$$

It has two distinguished subspaces,

$$\mathrm{Sym}^\ell(\mathcal{V},\mathcal{W}), \quad \mathrm{Alt}^\ell(\mathcal{V},\mathcal{W}), \tag{7.1.84}$$

defined as in (5.1.7). In case of $\mathrm{Alt}^\ell(\mathcal{V},\mathcal{W})$, one often wants to work under the assumption that $\mathcal{R}$ has the property

$$a \in \mathcal{R},\ a \neq 0 \Longrightarrow a \neq -a. \tag{7.1.85}$$

Otherwise anomalies occur. For example,

$$\mathcal{R} = \mathbb{Z}/(2) \Longrightarrow \mathrm{Sym}^2(\mathcal{V},\mathcal{R}) = \mathrm{Alt}^2(\mathcal{V},\mathcal{R}). \tag{7.1.86}$$

In particular,

$$\mathcal{V} = \mathcal{R} = \mathbb{Z}/(2),\ \beta(u,v) = uv \Longrightarrow \beta \in \mathrm{Alt}^2(\mathcal{V},\mathcal{R}) = \mathrm{Sym}^2(\mathcal{V},\mathcal{R}). \tag{7.1.87}$$

By contrast, whenever (7.1.85) holds, if $\beta \in \mathrm{Alt}^\ell(\mathcal{V},\mathcal{W}),\ \ell \geq 2$, then

$$\beta(v_1,\dots,v_\ell) = 0 \ \text{ whenever } \ v_j = v_k \ \text{ for some } \ j \neq k. \tag{7.1.88}$$

One can use methods parallel to those of §5.2 to define tensor products of $\mathcal{R}$-modules, for a commutative ring with unit $\mathcal{R}$, as least under a certain restriction. Namely, given $\mathcal{R}$-modules $\mathcal{V}_j$, we can define

$$\mathcal{V}_1' \otimes \cdots \otimes \mathcal{V}_\ell' = \mathcal{M}(\mathcal{V}_1,\dots,\mathcal{V}_\ell;\mathcal{R}). \tag{7.1.89}$$

A problem with directly paralleling (5.2.1) to define $\mathcal{V}_1 \otimes \cdots \otimes \mathcal{V}_\ell$ is that we no longer always have the isomorphism $(\mathcal{V}_j')' \approx \mathcal{V}_j$. Thus (7.1.89) defines the tensor product over $\mathcal{R}$ only of modules that are dual modules. Sometimes we want to identify $\mathcal{R}$ explicitly, using, e.g., the notation

$$\mathcal{V}_1' \otimes_{\mathcal{R}} \mathcal{V}_2' = \mathcal{M}_{\mathcal{R}}(\mathcal{V}_1,\mathcal{V}_2;\mathcal{R}). \tag{7.1.90}$$

This does not define

$$\mathcal{V} \otimes_{\mathcal{R}} \mathcal{W}, \tag{7.1.91}$$

for general $\mathcal{R}$-modules $\mathcal{V}$ and $\mathcal{W}$, when they are not dual modules. To define (7.1.91) in this greater generality, one needs to take a different approach. One can take finite formal sums of $v_j \otimes w_j$, for $v_j \in \mathcal{V},\ w_j \in \mathcal{W}$, subject to the equivalence relation

$$v_j \otimes a w_j \sim a v_j \otimes w_j, \quad a \in \mathcal{R}. \tag{7.1.92}$$

Then $\mathcal{V} \otimes_{\mathcal{R}} \mathcal{W}$ is an $\mathcal{R}$-module, with $a(v_j \otimes w_j)$ given by (7.1.92). One can verify that this coincides with the definition given in §5.2 when $\mathcal{R}$ is a field. As examples of such a construction, we mention that, as $\mathbb{Z}$-modules,

$$\mathbb{Z}/(2) \otimes_{\mathbb{Z}} \mathbb{Z}/(2) \approx \mathbb{Z}/(2), \tag{7.1.93}$$

while

$$\mathbb{Z}/(2) \otimes_{\mathbb{Z}} \mathbb{Z}/(3) = 0, \tag{7.1.94}$$

and

$$\mathbb{Z}/(2) \otimes_{\mathbb{Z}} \mathbb{Z} = 0. \tag{7.1.95}$$

For more on tensor products of $\mathcal{R}$-modules, see Chapter 16 of [**11**].

## Exercises

1. Let $\mathcal{R}$ be a ring (with unit, by the conventions of this section). Show that the results of Exercise 1 of §6.1 hold for all $a, b \in \mathcal{R}$. Also show that

$$(-a)b = -ab = a(-b).$$

2. Let $\mathcal{M}$ be a module over the ring $\mathcal{R}$. Take $a \in \mathcal{R}, v, w \in \mathcal{M}$. Show that the results (1.1.18) hold. Show also that

$$a \cdot 0 = 0 \text{ in } \mathcal{M}, \quad a(-v) = -av.$$

3. Given commutative rings with unit, $\mathcal{R}_1$ and $\mathcal{R}_2$, define

$$\mathcal{R}_1 \oplus \mathcal{R}_2$$

as a commutative ring with unit.

4. Given $m, n \in \mathbb{N}$, both $\geq 2$, define

$$\varphi : \mathbb{Z}/(mn) \longrightarrow \mathbb{Z}/(m) \oplus \mathbb{Z}/(n),$$
$$\varphi(k) = (k \text{ mod } m, k \text{ mod } n).$$

Show that $\varphi$ is a ring homomorphism, and that $\mathcal{N}(\varphi) \subset \mathbb{Z}/(mn)$ is generated by the least common multiple of $m$ and $n$. Using Exercise 13 of §6.1, deduce that

$$\varphi \text{ is an isomorphism } \iff \gcd(m, n) = 1.$$

5. Let $m, n$ be integers $\geq 2$ that are relatively prime, i.e., have no common prime factors. Given $x \in \mathbb{Z}$, show that

$$x = a \text{ mod } m, \ x = b \text{ mod } n \Longrightarrow x = an\nu + bm\mu \text{ mod } mn,$$

where $\nu, \mu \in \mathbb{Z}$ satisfy (cf. Exercise 12 of §6.1)

$$m\mu + n\nu = 1.$$

*Hint.* Start with

$$x = mj + a, \quad x = nk + b,$$

multiply one by $n\nu$, the other by $m\mu$, and add.

6. A group of 1000 soldiers is sent into battle and some perish. After the battle, the survivors line up in columns of 32 and 15 are left over. They then rearrange themselves into columns of 31 and 7 are left over. How many soldiers survived?

REMARK. This method of counting was apparently practiced in ancient China. For this reason, the result of Exercise 4 is called the *Chinese remainder theorem.* For a generalization, see Exercise 11 in §7.2.

7. Extend the setting of Proposition 6.1.9 to treat $\det A$ for $A \in M(n, \mathcal{R})$, when $\mathcal{R}$ is a commutative ring with unit, not necessarily satisfying (7.1.16). This provides an alternative to the approach involving (7.1.19)–(7.1.25).

8. Let $\mathbb{F}$ be a field.
(a) Show that there is a unique ring homomorphism $\psi : \mathbb{Z} \to \mathbb{F}$ such that $\psi(1) = 1$.
The image $\mathcal{I}_{\mathbb{F}} = \mathcal{R}(\psi)$ is the ring in $\mathbb{F}$ generated by $\{1\}$.
(b) Show that either $\psi$ is injective or $\mathcal{N}(\psi) = (n)$ for some $n \in \mathbb{N}$, $n \geq 2$.
*Hint.* $\mathbb{Z}$ is a PID.
(c) Show that, in the latter case, $n$ must be a prime (say $n = p$).
*Hint.* In such a case, $\psi$ induces an isomorphism of $\mathbb{Z}/(n)$ with $\mathcal{I}_{\mathbb{F}}$, which is an integral domain.
REMARK. If $\mathcal{I}_{\mathbb{F}} \approx \mathbb{Z}$, we say $\mathbb{F}$ has characteristic 0. If $\mathcal{I}_{\mathbb{F}} \approx \mathbb{Z}/(p)$, we say $\mathbb{F}$ has characteristic $p$.

9. Let $\mathbb{F}$ be a field with a finite number of elements (i.e., a finite field). Show that $\mathbb{F}$ has $p^n$ elements, for some prime $p$, $n \in \mathbb{N}$.
*Hint.* Show that $\mathcal{I}_{\mathbb{F}}$ (as in Exercise 8) is isomorphic to $\mathbb{Z}/(p)$ for some prime $p$, and that $\mathbb{F}$ is a vector space over $\mathcal{I}_{\mathbb{F}}$. Say its dimension is $n$.

10. Write down a proof of (7.1.66), that $\mathbb{F}[\lambda]$ is a PID for each field $\mathbb{F}$.

11. Show that (7.1.93) provides a counterexample to the proposal that

$$\mathcal{V}_1 \otimes_{\mathcal{R}} \mathcal{V}_2 \approx \mathcal{M}_{\mathcal{R}}(\mathcal{V}_1, \mathcal{V}_2; \mathcal{R}).$$

## 7.2. Modules over principal ideal domains

Recall that a principal ideal domain (PID) is an integral domain $\mathcal{R}$ such that each ideal $\mathcal{I} \subset \mathcal{R}$ has the form (7.1.61). Throughout this section, $\mathcal{R}$ will be a PID. It will be useful to collect a few basic facts about PIDs.

**Proposition 7.2.1.** *If $\mathcal{R}$ is a PID, its set of ideals satisfies the following ascending chain condition:*

$$\begin{aligned} &\mathcal{I}_j \subset \mathcal{R} \ \ \text{ideals in } \mathcal{R},\ \mathcal{I}_1 \subset \mathcal{I}_2 \subset \cdots \subset \mathcal{I}_k \subset \cdots \\ &\Longrightarrow \mathcal{I}_\ell = \mathcal{I}_{\ell+1} = \cdots, \ \text{for some } \ell. \end{aligned} \tag{7.2.1}$$

**Proof.** If $\mathcal{I}_j$ satisfy the hypotheses of (7.2.1), then $\mathcal{I} = \cup_j \mathcal{I}_j$ is an ideal, so $\mathcal{I} = (a)$ for some $a \in \mathcal{I}$, hence $a \in \mathcal{I}_\ell$ for some $\ell$. This gives the stated conclusion in (7.2.1). □

Generally, a commutative ring with unit satisfying (7.2.1) is called a *Noetherian ring*. See Section 7.5 for basic material on this class of rings.

One consequence of Proposition 7.2.1 is that each element of a PID admits factorization into irreducibles. If $a \in \mathcal{R} \setminus 0$ is not invertible, we say $a$ is *irreducible* provided

$$a = bc, \quad b, c \in \mathcal{R} \Longrightarrow b \text{ or } c \text{ is invertible.} \tag{7.2.2}$$

**Proposition 7.2.2.** *If $\mathcal{R}$ is a PID, each $a \in \mathcal{R} \setminus 0$ that is not invertible can be written as a finite product of irreducible elements.*

**Proof.** Take such an $a$. If $a$ is irreducible, you are done. If not, write $a = b_1 b_2$, with $b_j$ not invertible. If one of them is irreducible, leave it alone. If not, factor again. The content of this proposition is that such a process must terminate in a finite number of steps. To see this, note that such a factorization $a = b_1 b_2$ as mentioned above gives ideals $(a) \subset (b_1)$ and $(a) \subset (b_2)$. If $b_1 = c_1 c_2$ is a further factorization, then one has a chain of ideals $(a) \subset (b_1) \subset (c_1)$, etc. If this factorization never terminated, we would contradict (7.2.1). □

Thus, if $\mathcal{R}$ is a PID and $a \in \mathcal{R} \setminus 0$ is not invertible, we can write

$$a = p_1 \cdots p_N, \quad p_j \in \mathcal{R} \text{ irreducible.} \tag{7.2.3}$$

If (23.94) holds, we say $p_j$ divides $a$ and write $p_j | a$. It is the case that if also

$$a = q_1 \cdots q_M, \quad q_j \in \mathcal{R} \text{ irreducible,} \tag{7.2.4}$$

then $M = N$ and, after perhaps reordering,

$$p_j = \alpha_j q_j, \quad 1 \le j \le N, \quad \alpha_j \in \mathcal{R} \text{ invertible.} \tag{7.2.5}$$

In other words, each $a \in \mathcal{R} \setminus 0$ that is not invertible has a factorization into irreducible elements, and it is essentially unique. An integral domain having this property is called a *unique factorization domain* (UFD). We are asserting that

$$\text{Each PID is a UFD.} \tag{7.2.6}$$

This is a consequence of the following.

**Lemma 7.2.3.** *If $\mathcal{R}$ is a PID and $p \in \mathcal{R}$ is irreducible, then, for $a, b \in \mathcal{R}$,*

$$p|ab \Longrightarrow p|a \quad or \quad p|b. \tag{7.2.7}$$

**Proof.** Assume $p$ does not divide $a$. The ideal generated by $p$ and $a$, $(p, a) = (\alpha)$ for some $\alpha \in \mathcal{R}$. So $p = \beta\alpha, a = \gamma\alpha$, and either $\beta$ or $\alpha$ is invertible. If $\beta$ is invertible, we can take $\alpha = p$, but this is impossible if $p$ does not divide $a$. Hence $\alpha$ is invertible. Then we can take $\alpha = 1$, so

$$1 = c_1 p + c_2 a, \quad c_j \in \mathcal{R}, \tag{7.2.8}$$

hence

$$b = (c_1 b)p + c_2(ab). \tag{7.2.9}$$

If $p|ab$, then $p$ divides the right side of (7.2.9), so $p|b$. This proves the lemma, so we have (7.2.6). □

The result that $\mathbb{Z}$ is a PID, together with (7.2.6), constitutes the *fundamental theorem of arithmetic*. See Exercise 13 for an example of an integral domain that is not a UFD and (hence) not a PID.

If $\mathcal{R}$ is a commutative ring with unit and $a \in \mathcal{R} \setminus 0$ is not invertible, we say $a$ is *prime* provided the implication (7.2.7) holds. It is easy to see that, in general

$$a \text{ prime} \Longrightarrow a \text{ irreducible}, \tag{7.2.10}$$

but the reverse implication need not always hold. Lemma 7.2.3 says the reverse implication holds if $\mathcal{R}$ is a PID. More generally, the reverse implication holds if and only if $\mathcal{R}$ is a UFD.

Next, let $\mathcal{R}$ be a PID, and assume $\mathcal{R}$ is not a field. Pick a prime $p \in \mathcal{R}$. The following result generalizes Proposition 6.1.1.

**Proposition 7.2.4.** *If $\mathcal{R}$ is a PID and $p \in \mathcal{R}$ is a prime, then $\mathcal{R}/(p)$ is a field.*

**Proof.** Pick $a \in \mathcal{R}$ such that $a \neq 0$ in $\mathcal{R}/(p)$, i.e., $a$ is not a multiple of $p$. The proof of Lemma 23.8 shows that $(p, a) = \mathcal{R}$, i.e., there exist $c_j \in \mathcal{R}$ such that (7.2.8) holds. Then the class mod $(p)$ of $c_2$ is the inverse of $a$ in $\mathcal{R}/(p)$. □

Now, on to modules. Our treatment of this topic follows [**11**]. Let $\mathcal{M}$ be a module over a PID $\mathcal{R}$. If $\mathcal{R}$ is a field, $\mathcal{M}$ is a vector space. Assume $\mathcal{R}$ is not a field, and pick a prime $p \in \mathcal{R}$. Then $p\mathcal{M}$ is a submodule of $\mathcal{M}$, and we can form the quotient module $\mathcal{M}/p\mathcal{M}$. Not only is this a module over $\mathcal{R}$, but it naturally inherits the structure of a module over $\mathcal{R}/(p)$, which by Proposition 7.2.4 is a field:

$$\mathcal{M}/p\mathcal{M} \ \text{ is a vector space over } \ \mathbb{F} = \mathcal{R}/(p). \tag{7.2.11}$$

As one example,

$$\mathcal{M} = \mathcal{R}^n \Longrightarrow \mathcal{M}/p\mathcal{M} = \mathbb{F}^n. \tag{7.2.12}$$

Since we know that the dimension of a vector space is an isomorphism invariant, we deduce from (7.2.12) the following.

**Proposition 7.2.5.** *If $\mathcal{R}$ is a PID and $\mathcal{M}$ is a module over $\mathcal{R}$, then*

$$\mathcal{M} \approx \mathcal{R}^n \ \ \textit{and} \ \ \mathcal{M} \approx \mathcal{R}^m \Longrightarrow m = n. \tag{7.2.13}$$

If (7.2.13) holds, one says $\mathcal{M}$ is a free $\mathcal{R}$-module, of dimension $n$. We have seen examples of modules that are not free. The following produces lots of modules that are free. It generalizes Proposition 1.3.4.

**Proposition 7.2.6.** *Let $\mathcal{R}$ be a PID and let $\mathcal{M}$ be a free module over $\mathcal{R}$, of dimension $n$. If $\mathcal{N}$ is a submodule of $\mathcal{M}$, then $\mathcal{N}$ is free, of dimension $\le n$.*

**Proof.** We may as well take $\mathcal{M} = \mathcal{R}^n$. Let $\{e_j : 1 \le j \le n\}$ be the standard generating set. Let $\mathcal{M}_k = \operatorname{Span}(e_1, \dots, e_k)$ and $\mathcal{N}_k = \mathcal{N} \cap \mathcal{M}_k$. Then $\mathcal{N}_1$ is a submodule of $\mathcal{M}_1 \approx \mathcal{R}$, and hence is of the form $\operatorname{Span} a_1 e_1$ for some $a_1 \in \mathcal{R}$. Thus either $\mathcal{N}_1 = 0$ or $\mathcal{N}_1 \approx \mathcal{R}$ (free of dimension 1).

Assume inductively that $\mathcal{N}_k$ is free of dimension $\le k$. Let $\mathcal{I}$ be the set of all $a \in \mathcal{R}$ such that

$$b_1 e_1 + \cdots + b_k e_k + a e_{k+1} \in \mathcal{N} \ \ \text{(hence in } \mathcal{N}_{k+1}), \tag{7.2.14}$$

for some $b_j \in \mathcal{R}$. Thus $\mathcal{I}$ is an ideal in $\mathcal{R}$, so $\mathcal{I} = (a_{k+1})$ for some $a_{k+1} \in \mathcal{R}$. If $a_{k+1} = 0$, then $\mathcal{N}_{k+1} = \mathcal{N}_k$, and the induction step is done. If $a_{k+1} \ne 0$, let $w \in \mathcal{N}_{k+1}$ be such that the coefficient of $w$ with respect to $e_{k+1}$ is $a_{k+1}$. If $x \in \mathcal{N}_{k+1}$, then the coefficient of $x$ with respect to $e_{k+1}$ is divisible by $a_{k+1}$, so there exists $c \in \mathcal{R}$ such that $x - cw \in \mathcal{N}_k$. Hence

$$\mathcal{N}_{k+1} = \mathcal{N}_k + \operatorname{Span} w. \tag{7.2.15}$$

But clearly $\mathcal{N}_k \cap \operatorname{Span} w = 0$, so this sum is direct. Again the induction step is done. $\square$

**Corollary 7.2.7.** *If $\mathcal{E}$ is a finitely generated module over a PID $\mathcal{R}$, and $\mathcal{F}$ is a submodule, then $\mathcal{F}$ is finitely generated.*

**Proof.** We have $\mathcal{E} \approx \mathcal{R}^n/\mathcal{N}$, as in Proposition 7.1.4, with a surjective homomorphism $\varphi : \mathcal{R}^n \to \mathcal{E}$, as in (7.1.76). Then $\varphi^{-1}(\mathcal{F})$ is a submodule of $\mathcal{R}^n$, so it is (free, and) finitely generated, by Proposition 7.2.6. It follows that $\mathcal{F}$ is finitely generated. □

If $\mathcal{E}$ is a finitely generated $\mathcal{R}$-module, the obstruction to its being free is given by its set of torsion elements. An element $u \in \mathcal{E}$ is a torsion element if and only if there exists $a \in \mathcal{R}$ such that $a \neq 0$ but $au = 0$. Let $\mathcal{E}_\tau$ denote the set of torsion elements of $\mathcal{E}$. It is clear that if $au = 0$ then $acu = 0$ for all $c \in \mathcal{R}$. Also, given $a, b \in \mathcal{R}$, $u, v \in \mathcal{E}$,

$$au = bv = 0 \Longrightarrow ab(u + v) = 0. \tag{7.2.16}$$

Hence $\mathcal{E}_\tau$ is a submodule of $\mathcal{E}$. Since each element of $\mathcal{E}_\tau$ is a torsion element, $\mathcal{E}_\tau$ is called a torsion module.

**Proposition 7.2.8.** *Let $\mathcal{E}$ be a finitely generated module over a PID $\mathcal{R}$. If $\mathcal{E}_\tau = 0$, then $\mathcal{E}$ is free.*

**Proof.** Let $V = \{v_1, \dots, v_n\}$ be a maximal set of elements of $\mathcal{E}$ among a given set of generators $U = \{u_1, \dots, u_m\}$ such that $V$ is linearly independent over $\mathcal{R}$. If $u \in U$, there exist $a, b_1, \dots, b_n \in \mathcal{R}$ not all 0, such that

$$au + b_1 v_1 + \cdots + b_n v_n = 0. \tag{7.2.17}$$

Then $a \neq 0$, since $V$ is linearly independent. Hence $au \in \operatorname{Span} V$. Thus, for each $j = 1, \dots, n$, there exists $a_j \in \mathcal{R}$, $\neq 0$, such that $a_j u_j \in \operatorname{Span} V$. Take $a = a_1 \cdots a_n$. Then $a\mathcal{E} \subset \operatorname{Span}(v_1, \dots, v_n)$ and $a \neq 0$.

Given that $\mathcal{E}_\tau = 0$, the map $u \mapsto au$ is an injective homomorphism of $\mathcal{E}$ into the module $\operatorname{Span}(v_1, \dots, v_n)$, which is a free module. Hence Proposition 7.2.6 implies $\mathcal{E}$ is free. □

We proceed to consider cases where $\mathcal{E}_\tau \neq 0$.

**Proposition 7.2.9.** *Let $\mathcal{E}$ be a finitely generated module over a PID $\mathcal{R}$. Then $\mathcal{E}/\mathcal{E}_\tau$ is free. Furthermore, there exists a free submodule $\mathcal{F} \subset \mathcal{E}$ such that*

$$\mathcal{E} = \mathcal{E}_\tau \oplus \mathcal{F}. \tag{7.2.18}$$

To define (7.2.18), in general a direct sum $\mathcal{M}_1 \oplus \mathcal{M}_2$ of $\mathcal{R}$-modules consists of pairs $(u_1, u_2)$ such that $u_j \in \mathcal{M}_j$, with module operations

$$(u_1, u_2) + (v_1, v_2) = (u_1 + v_1, u_2 + v_2), \quad a(u_1, u_2) = (au_1, au_2). \tag{7.2.19}$$

If $\mathcal{M}_j$ are submodules of $\mathcal{E}$, one says $\mathcal{E} = \mathcal{M}_1 \oplus \mathcal{M}_2$ provided each $u \in \mathcal{E}$ can be uniquely written as $u = u_1 + u_2$, with $u_j \in \mathcal{M}_j$.

**Proof of Proposition 7.2.9.** We first prove that $\mathcal{E}/\mathcal{E}_\tau$ is torsion free. If

$u \in \mathcal{E}$, let $u'$ denote its resudue class mod $\mathcal{E}_\tau$. Assume $b \in \mathcal{R}, b \neq 0$, and $bu' = 0$. Then $bu \in \mathcal{E}_\tau$, so there exists $c \in \mathcal{R}, c \neq 0$, such that $cbu = 0$. Now $cb \neq 0$, so $u \in \mathcal{E}_\tau$, so $u' = 0$. Hence $\mathcal{E}/\mathcal{E}_\tau$ is torsion free. It is also finitely generated. Thus Proposition 7.2.8 implies $\mathcal{E}/\mathcal{E}_\tau$ is a free, finitely-generated $\mathcal{R}$-module.

To produce the submodule $\mathcal{F}$ in (7.2.18), we bring in the following lemma.

**Lemma 7.2.10.** *Let $\mathcal{E}$ and $\mathcal{M}$ be finitely generated $\mathcal{R}$-modules, and assume $\mathcal{M}$ is free. Let $\varphi : \mathcal{E} \to \mathcal{M}$ be a surjective homomorphism. Then there exists a free submodule $\mathcal{F}$ of $\mathcal{E}$ such that $\varphi|_{\mathcal{F}}$ induces an isomorphism of $\mathcal{F}$ with $\mathcal{M}$, and such that*

$$\mathcal{E} = \mathcal{F} \oplus \mathcal{N}(\varphi). \tag{7.2.20}$$

**Proof.** We can take $\mathcal{M} = \mathcal{R}^m$. Let $\{e_1, \dots, e_m\}$ be the standard generators of $\mathcal{R}^m$. For each $j$, take $u_j \in \mathcal{E}$ such that $\varphi(u_j) = e_j$. Let

$$\mathcal{F} = \operatorname{Span}(u_1, \dots, u_m). \tag{7.2.21}$$

Then we see that $\varphi$ maps $\mathcal{F}$ isomorphically onto $\mathcal{R}^m$, so $\mathcal{F}$ is free. Now, given $u \in \mathcal{E}$, there exist $a_j \in \mathcal{R}$ such that

$$\varphi(u) = \sum a_j e_j. \tag{7.2.22}$$

Then $u - \sum a_j u_j \in \mathcal{N}(\varphi)$, so $\mathcal{E} = \mathcal{F} + \mathcal{N}(\varphi)$. But it is clear that $\mathcal{N}(\varphi) \cap \mathcal{F} = 0$, so the sum is direct. This proves the lemma. □

To finish off the proof of Proposition 7.2.9, we apply Lemma 7.2.10 to the surjective homomorphism $\mathcal{E} \to \mathcal{E}/\mathcal{E}_\tau$, whose target space has been shown to be free. Thus (7.2.20) yields (7.2.18), with $\mathcal{N}(\varphi) = \mathcal{E}_\tau$. □

In the setting of Proposition 7.2.9, we say the *rank* of $\mathcal{E}$ is given by $\dim \mathcal{E}/\mathcal{E}_\tau = \dim \mathcal{F}$.

In order to expose the structure of arbitrary finitely generated $\mathcal{R}$-modules, it remains to analyze the structure of finitely generated torsion modules. Here is a first decomposition of torsion modules.

**Proposition 7.2.11.** *Let $\mathcal{E}$ be a finitely generated torsion module over a PID $\mathcal{R}$. Then $\mathcal{E}$ is a direct sum*

$$\mathcal{E} = \bigoplus_{p_j} \mathcal{E}(p_j), \tag{7.2.23}$$

*where, for a prime $p \in \mathcal{R}$, $\mathcal{E}(p)$ is the "p-module"*

$$\mathcal{E}(p) = \{u \in \mathcal{E} : p^k u = 0 \text{ for some } k \in \mathbb{N}\}. \tag{7.2.24}$$

*The direct sum in* (7.2.23) *is over the finite set of primes* $p_j$ *such that* $\mathcal{E}(p_j) \neq 0$.

**Proof.** Let $\{x_1, \dots, x_n\}$ generate $\mathcal{E}$. For each $j$, there exists $a_j \in \mathcal{R}$, $a_j \neq 0$, such that $a_j x_j = 0$. Set $a = a_1 \cdots a_n$. Then $a \neq 0$ and $au = 0$ for each $u \in \mathcal{E}$, i.e.,

$$\mathcal{E} = \mathcal{E}_a, \tag{7.2.25}$$

where, for each $b \in \mathcal{R}$,

$$\mathcal{E}_b = \{u \in \mathcal{E} : bu = 0\}. \tag{7.2.26}$$

If $a = p^k$, then $\mathcal{E} = \mathcal{E}_a = \mathcal{E}(p)$, and we are done. Otherwise, we factor $a = p_1^{m_1} \cdots p_k^{m_k}$. To get (7.2.23), by induction it suffices to establish the following. Assume (with $a$ as in (7.2.23))

$$\begin{aligned} &a = bc, \quad b \text{ and } c \text{ have no common prime factors,} \\ &\text{and are not invertible.} \end{aligned} \tag{7.2.27}$$

Then we claim

$$\mathcal{E} = \mathcal{E}_b \oplus \mathcal{E}_c. \tag{7.2.28}$$

To see this, note that, since $\mathcal{R}$ is a PID, the hypothesis (7.2.27) implies $(b, c) = \mathcal{R}$, so there exist $\beta, \gamma \in \mathcal{R}$ such that

$$\beta b + \gamma c = 1. \tag{7.2.29}$$

Now take $u \in \mathcal{E}$, and write

$$u = \beta b u + \gamma c u. \tag{7.2.30}$$

Then $\beta b u \in \mathcal{E}_c$ (i.e., $c\beta b u = 0$) and similarly $\gamma c u \in \mathcal{E}_b$. Furthermore, clearly $\mathcal{E}_b \cap \mathcal{E}_c = 0$, so we have (7.2.28), and, as mentioned above, the desired conclusion (7.2.23) follows inductively. $\square$

It remains to analyze the structure of each $p_j$-module $\mathcal{E}(p_j)$ in (7.2.23). We have the following.

**Proposition 7.2.12.** *In the setting of Proposition 7.2.11, each p-module* $\mathcal{E}(p)$ *satisfies*

$$\mathcal{E}(p) \approx \mathcal{R}/(p^{\nu_1}) \oplus \cdots \oplus \mathcal{R}/(p^{\nu_s}), \tag{7.2.31}$$

*with* $1 \leq \nu_1 \leq \cdots \leq \nu_s$. *The sequence* $(\nu_1, \dots, \nu_s)$ *is uniquely determined by* $\mathcal{E}(p)$.

As a preliminary to the proof, we introduce some notation. If $\mathcal{E}$ is an $\mathcal{R}$-module, we say elements $y_1, \dots, y_m \in \mathcal{E}$ are *independent* provided that whenever

$$a_1 y_1 + \cdots + a_m y_m = 0, \tag{7.2.32}$$

then each $a_j y_j = 0$. (This is different from *linear independence*, which requires that each $a_j = 0$.) An equivalent condition is that

$$\mathrm{Span}(y_1, \dots, y_m) = (y_1) \oplus \cdots \oplus (y_m), \tag{7.2.33}$$

where $(y_j) = \mathrm{Span}\, y_j$.

We next bring in a lemma, analogous to Lemma 7.2.10.

**Lemma 7.2.13.** *Let $\mathcal{E}$ be a torsion module, with the property that $p^k \mathcal{E} = 0$ for some prime $p \in \mathcal{R}$, $k \in \mathbb{N}$. Assume $u_1 \in \mathcal{E}$ and that $p^\nu u_1 = 0$ if and only if $\nu \ge k$. (We say the period of $u_1$ is $p^k$.) Set $\mathcal{E}^b = \mathcal{E}/(u_1)$. Let $y_1^b, \dots, y_\mu^b$ be independent elements of $\mathcal{E}^b$. Then for each $j$ there exists a preimage $y_j \in \mathcal{E}$ of $y_j^b$ such that the period of $y_j$ is the same as that of $y_j^b$. Furthermore, the elements $u_1, y_1, \dots, y_\mu$ are independent.*

**Proof.** Take $y^b \in \mathcal{E}^b$. Say it has period $p^n$. Let $y \in \mathcal{E}$ be a preimage of $y^b$. Then $p^n y \in (u_1)$, so

$$p^n y = p^m c u_1, \tag{7.2.34}$$

for some $m \le k$, $c \in \mathcal{R}$, not a multiple of $p$. If $m = k$, then $y$ has the same period as $y^b$. If $m < k$, then $p^m c u_1$ has period $p^{k-m}$, so $y$ has period $p^{n+k-m}$. Our hypothesis $p^k \mathcal{E} = 0$ implies $n + k - m \le k$, hence $n \le m$. Then

$$y - p^{m-n} c u_1 \tag{7.2.35}$$

is a preimage of $y^b$ whose period is $p^n$.

Having this, let $y_j \in \mathcal{E}$ be a preimage of $y_j^b$ with the same period. It remains to show that $u_1, y_1, \dots, y_\mu$ are independent. Suppose $a, a_1, \dots, a_\mu \in \mathcal{R}$ and

$$a u_1 + a_1 y_1 + \cdots + a_\mu y_\mu = 0 \quad \text{in} \quad \mathcal{E}. \tag{7.2.36}$$

Then

$$a_1 y_1^b + \cdots + a_\mu y_\mu^b = 0 \quad \text{in} \quad \mathcal{E}^b. \tag{7.2.37}$$

By hypothesis, we must have $a_j y_j^b = 0$ for each $j$. If $p^{\nu_j}$ is the period of $y_j^b$, then $p^{\nu_j} | a_j$. Thus (since as noted $y_j$ also has period $p^{\nu_j}$) $a_j y_j = 0$ for each $j$. Then (7.2.36) forces $a u_1 = 0$, proving the asserted independence. $\square$

We now tackle the proof of Proposition 7.2.12. Since $\mathcal{E}(p)$ is a submodule of a finitely generated module, it follows from Corollary 7.2.7 that $\mathcal{E}(p)$ is finitely generated. To simplify notation, we set $\mathcal{E} = \mathcal{E}(p)$. Pick $k_1 \in \mathbb{N}$ such that $p^\nu \mathcal{E} = 0$ if and only if $\nu \ge k_1$ (which is possible since $\mathcal{E}$ is finitely generated). Then pick $u_1 \in \mathcal{E}$ such that $p^\nu u_1 = 0$ if and only if $\nu \ge k_1$. Let $\mathcal{E}^b = \mathcal{E}/(u_1)$. It is convenient to bring in $\mathcal{E}_p$ and $\mathcal{E}_p^b$, where, as in (7.2.26),

$$\mathcal{E}_p = \{u \in \mathcal{E} : pu = 0\}. \tag{7.2.38}$$

Now $\mathcal{E}_p$ is an $\mathcal{R}$-submodule of $\mathcal{E}$, and (somewhat similarly to (7.2.11)) it also naturally inherits the structure of a module over $\mathcal{R}/(p)$. Ditto for $\mathcal{E}_p^b$, so

$$\mathcal{E}_p \text{ and } \mathcal{E}_p^b \text{ are vector spaces over } \mathbb{F} = \mathcal{R}/(p). \tag{7.2.39}$$

Since $\mathcal{E}$ and $\mathcal{E}^b$ are finitely generated $\mathcal{R}$-modules, the vector spaces (7.2.39) are finite dimensional. We claim that

$$\dim_{\mathbb{F}} \mathcal{E}_p^b < \dim_{\mathbb{F}} \mathcal{E}_p. \tag{7.2.40}$$

Indeed, if $y_1^b, \dots, y_\mu^b$ are linearly independent elements of $\mathcal{E}_p^b$ over $\mathbb{F}$, then Lemma 7.2.13 implies that $\dim_{\mathbb{F}} \mathcal{E}_p \ge \mu + 1$, since we can always find an element $\alpha u_1$ of $(u_1)$ having period $p$, independent of the preimages $y_1, \dots, y_\mu$.

Having (7.2.40), we establish the direct sum decomposition (7.2.31) by induction on $\dim_{\mathbb{F}} \mathcal{E}_p$. Note that $\mathcal{E}_p = 0 \Rightarrow \mathcal{E} = 0$, so

$$\mathcal{E}_p^b = 0 \Rightarrow \mathcal{E}^b = 0 \Rightarrow \mathcal{E} = (u_1) \approx \mathcal{R}/(p^{\nu_1}), \tag{7.2.41}$$

where $p^{\nu_1}$ is the period of $u_1$. To proceed, suppose we have a decomposition parallel to (7.2.31) for each $p$-module $\mathcal{F}$ such that $\dim_{\mathbb{F}} \mathcal{F}_p < \dim_{\mathbb{F}} \mathcal{E}_p$, and we want to establish this decomposition for the $p$-module $\mathcal{E}$. To start, we have such a decomposition for $\mathcal{E}^b = \mathcal{E}/(u_1)$:

$$\mathcal{E}^b = (u_2^b) \oplus \cdots \oplus (u_\ell^b), \tag{7.2.42}$$

where, for $2 \le j \le \ell$, the elements $u_j^b \in \mathcal{E}^b$ have periods $p^{k_j}$. We can arrange $k_2 \ge \cdots \ge k_\ell$. By Lemma 7.2.13, there exist preimages $u_2, \dots, u_\ell \in \mathcal{E}$, with the same periods. Furthermore, $u_1, u_2, \dots, u_\ell$ are independent, so

$$\operatorname{Span}(u_1, u_2, \dots, u_\ell) = (u_1) \oplus (u_2) \oplus \cdots \oplus (u_\ell). \tag{7.2.43}$$

It remains only to observe that the left side of (7.2.43) is equal to $\mathcal{E} = \mathcal{E}(p)$, and we have the decomposition (7.2.31).

The final uniqueness statement of Proposition 7.2.12 is a consequence of the following more general uniqueness result.

**Proposition 7.2.14.** *Let $\mathcal{E}$ be a finitely generated torsion module over a PID $\mathcal{R}$, $\mathcal{E} \ne 0$. Then $\mathcal{E}$ is isomorphic to a direct sum of factors*

$$\mathcal{R}/(q_1) \oplus \cdots \oplus \mathcal{R}/(q_k), \tag{7.2.44}$$

*where $q_1, \dots, q_k$ are non-zero elements of $\mathcal{R}$ and $q_1 | q_2 | \cdots | q_k$. The sequence of ideals $(q_1), \dots, (q_k)$ is uniquely determined by these conditions. (These ideals are called the invariants of $\mathcal{E}$.)*

**Proof.** By Proposition 7.2.11, we can write $\mathcal{E} = \mathcal{E}(p_1) \oplus \cdots \oplus \mathcal{E}(p_\ell)$, and then by Proposition 7.2.12 we can write

$$\mathcal{E}(p_j) = \bigoplus_{k=1}^m \mathcal{R}/(p_j^{r_{jk}}), \quad r_{j1} \le r_{j2} \le \cdots . \tag{7.2.45}$$

Take

$$\begin{aligned} q_1 &= p_1^{r_{11}} p_2^{r_{21}} \cdots p_\ell^{r_{\ell 1}} \\ q_2 &= p_1^{r_{12}} p_2^{r_{22}} \cdots p_\ell^{r_{\ell 2}} \\ &\vdots \\ q_m &= p_1^{r_{1m}} p_2^{r_{2m}} \cdots p_\ell^{r_{\ell m}}. \end{aligned} \tag{7.2.46}$$

We need a rectangular array here, so we might need to take some $r_{jk} = 0$, in which case $\mathcal{R}/(p_j^{r_{jk}}) = 0$. We have

$$\bigoplus_{j=1}^{\ell} \mathcal{R}/(p_j^{r_{jk}}) \approx \mathcal{R}/(q_k). \tag{7.2.47}$$

(See Exercise 11.) This gives the decomposition (7.2.44).

To prepare for the uniqueness argument, we make some preliminary remarks. Let $p \in \mathcal{R}$ be prime and suppose $\mathcal{E} = \mathcal{R}/(pb)$, $b \neq 0$. Since $\mathcal{R}$ is a UFD, is follows that $\mathcal{E}_p$ is the submodule $b\mathcal{R}/(pb)$. Now the null space of the composite map

$$\mathcal{R} \longrightarrow b\mathcal{R} \longrightarrow b\mathcal{R}/(pb) \tag{7.2.48}$$

is the ideal $(p)$, so we have an isomorphism

$$\mathcal{R}/(p) \approx b\mathcal{R}/(pb), \tag{7.2.49}$$

hence

$$\mathcal{E} = \mathcal{R}/(bp) \Longrightarrow \mathcal{E}_p \approx \mathcal{R}/(p). \tag{7.2.50}$$

By contrast, if $c \in \mathcal{R}$ is not a multiple of $p$, then

$$\mathcal{E} = \mathcal{R}/(c) \Longrightarrow \mathcal{E}_p = 0. \tag{7.2.51}$$

To proceed, let $\mathcal{E}$ have the form (7.2.44). Then an element

$$v = v_1 \oplus \cdots \oplus v_k \tag{7.2.52}$$

of $\mathcal{E}$ belongs to $\mathcal{E}_p$ if and only if $pv_j = 0$ for all $j$. Hence $\mathcal{E}_p$ is the direct sum of the null spaces of multiplication by $p$ in each term $\mathcal{R}/(q_j)$. By (7.2.50)–(7.2.51), it follows that the dimension of $\mathcal{E}_p$ as a vector space over $\mathcal{R}/(p)$ is equal to the number of terms $\mathcal{R}/(q_j)$ such that $p$ divides $q_j$.

For such $\mathcal{E}$, suppose $p$ is a prime dividing $q_1$, and hence each $q_j$, for $1 \le j \le k$. Suppose that also

$$\mathcal{E} \approx \mathcal{R}/(q_1') \oplus \cdots \oplus \mathcal{R}/(q_\ell'). \tag{7.2.53}$$

Then the computation above of $\dim_{\mathcal{R}/(p)} \mathcal{E}_p$ shows that $p$ must divide at least $k$ of the elements $q_j'$, $1 \le j \le \ell$. This forces $\ell \ge k$. By symmetry, also $k \ge \ell$, so we must have $\ell = k$. We also conclude that $p$ divides $q_j'$ for all $j$.

Now, write $q_j = pb_j$. Parallel to (7.2.49), we have $p\mathcal{R}/(pb_j) \approx \mathcal{R}/(b_j)$, so (7.2.44) implies

$$p\mathcal{E} \approx \mathcal{R}/(b_1) \oplus \cdots \oplus \mathcal{R}/(b_k), \tag{7.2.54}$$

and $b_1|\cdots|b_k$. Some of the $b_j$ might be invertible, namely those for which $(q_j) = (p)$, and then $\mathcal{R}/(b_j) = 0$. If $b_1, \dots b_\mu$ are invertible but $b_{\mu+1}$ is not invertible, we have

$$p\mathcal{E} \approx \mathcal{R}/(b_{\mu+1}) \oplus \cdots \oplus \mathcal{R}/(b_k). \tag{7.2.55}$$

One can iterate this argument, and inductively finish the uniqueness proof. ☐

## Exercises

For Exercises 1–5, we pick $\omega \in \mathbb{C} \setminus \mathbb{R}$ and form the lattice

$$\mathcal{L}_\omega = \{j\omega + k : j, k \in \mathbb{Z}\}.$$

1. Show that $\mathcal{L}_\omega$ is a ring if and only if $\omega^2 \in \mathcal{L}_\omega$. Show that this happens if and only if, after replacing $\omega$ by $\omega - \ell$ for some $\ell \in \mathbb{Z}$ (and maybe changing its sign), either

$$\omega = \sqrt{-m}, \quad m \in \mathbb{N},$$

or

$$\omega = \frac{1}{2} + \frac{1}{2}\sqrt{-D}, \quad D \in \mathbb{N},\ D = 3 \bmod 4.$$

In such a case, $\mathcal{L}_\omega = \mathbb{Z}[\omega]$. See Figure 7.2.1 for an illustration, with $D = 3$.

2. Assume $\omega \in \mathbb{C} \setminus \mathbb{R}$ is such that $\mathcal{L}_\omega = \mathbb{Z}[\omega]$. Show that if

$$\mathrm{dist}(\zeta, \mathbb{Z}[\omega]) < 1, \quad \forall\, \zeta \in \mathbb{C},$$

then $\mathbb{Z}[\omega]$ is a PID.
*Hint.* To start, given an ideal $\mathcal{I} \subset \mathbb{Z}[\omega]$, pick $\alpha \in \mathcal{I} \setminus 0$ to minimize $|\alpha|$. You want to show that $\mathcal{I} = (\alpha)$.

3. In the setting of Exercises 1–2, show that $\mathbb{Z}[\omega]$ is a PID for the following values of $\omega$:

$$\sqrt{-1}, \quad \sqrt{-2}, \quad \frac{1}{2} + \frac{1}{2}\sqrt{-D}, \quad D = 3, 7, \text{ or } 11.$$

Remark. The ring $\mathbb{Z}[\sqrt{-1}]$ is called the ring of *Gaussian integers.*

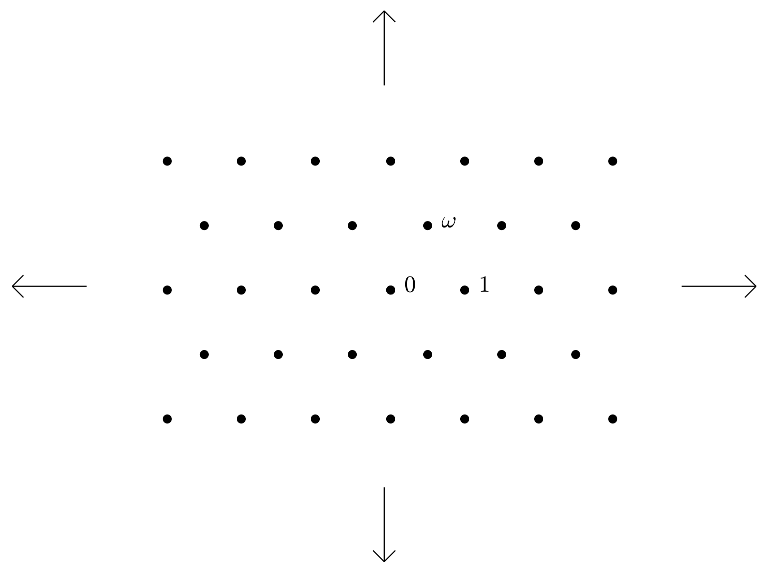


**Figure 7.2.1.** The lattice/ring $\mathcal{L}_\omega = \mathbb{Z}[\omega],\ \omega = (1 + i\sqrt{3})/2$

4. Let us set

$$\mathcal{I} = \{2j + k(1 + \sqrt{-5}) : j, k \in \mathbb{Z}\} = \{a + b\sqrt{-5} : 2 \,|\, (a - b)\}.$$

Define

$$\varphi : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}/(2), \quad \varphi(a + b\sqrt{-5}) = a - b \ (\mathrm{mod}\ 2).$$

Show that $\varphi$ is a ring homomorphism, and $\mathcal{N}(\varphi) = \mathcal{I}$. Deduce that $\mathcal{I}$ is an ideal in $\mathbb{Z}[\sqrt{-5}]$.

5. Show that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, hence not a PID.
*Hint.* One has

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

and all four of these factors are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$. To see directly that $\mathbb{Z}[\sqrt{-5}]$ is not a PID, consider the ideal $\mathcal{I}$ generated by 2 and $1 + \sqrt{-5}$ (which by Exercise 4 is a proper ideal), and show it does not have a single generator. Or use (7.2.6).

Remark. It was shown by Gauss that $\mathbb{Z}[\omega]$ is a UFD for $\omega$ as in Exercise

3, and also for

$$\omega = \frac{1}{2} + \frac{1}{2}\sqrt{-D}, \quad D = 19, 43, 67, 163.$$

It has since been shown that this list is exhaustive. See [**1**], Chapter 11, §7 for more on this.

Let $\mathcal{R}$ be a commutative ring with unit. A *proper ideal* in $\mathcal{R}$ is an ideal that is neither 0 nor $\mathcal{R}$. A *maximal ideal* in $\mathcal{R}$ is a proper ideal that is contained in no larger proper ideal.

6. If $\mathcal{R}$ is a commutative ring with unit and $\mathcal{I} \subset \mathcal{R}$ a maximal ideal, show that $\mathcal{R}/\mathcal{I}$ is a field.
*Hint.* Given $a \in \mathcal{R} \setminus \mathcal{I}$, show that the ideal generated by $a$ and $\mathcal{I}$ must be all of $\mathcal{R}$.

7. Let $\mathcal{R}$ be a PID. Let $\mathcal{I} = (a)$ be a proper ideal. Assume that, whenever $a = bc$, either $b$ or $c$ is invertible. Show that $\mathcal{I}$ is a maximal ideal.
*Hint.* If $(a) \subset (\alpha)$, then $a = \alpha\beta$.

8. Let $\mathbb{F}$ be a field, and assume $\lambda^2 + 1 = 0$ has no solution in $\mathbb{F}$. Show that Exercise 7 applies to $\mathcal{R} = \mathbb{F}[\lambda]$ and $a = q(\lambda) = \lambda^2 + 1$. Deduce that $\mathbb{F}[\lambda]/(q)$ is a field. Denote it $\mathbb{F}(\sqrt{-1})$.

9. In the setting of Exercise 8, show that there is a natural injection of $\mathbb{F}$ as a subfield of $\mathbb{F}(\sqrt{-1})$, and that $\lambda^2 + 1$ has a root in this larger field. Explain why one might write $\mathbb{F}(\sqrt{-1}) = \mathbb{F}[\sqrt{-1}]$.

10. Generalize the results of Exercises 8–9 to the case where $q(\lambda) \in \mathbb{F}[\lambda]$ is an irreducible polynomial, i.e., $q(\lambda)$ cannot be factored as a product of polynomials of lower degree, with coefficients in $\mathbb{F}$.

11. Let $\mathcal{R}$ be a PID, and take $a, b \in \mathcal{R}$, both non-invertible. Assume $a$ and $b$ have no common prime factors. Show that

$$\mathcal{R}/(ab) \approx \mathcal{R}/(a) \oplus \mathcal{R}/(b).$$

This generalizes the result of Exercise 4 in §7.1
*Hint.* As in Exercise 4 of §7.1, you want to show that if $c \in \mathbb{R}$ is a multiple of $a$ and a multiple of $b$, it must be a multiple of $ab$. Consider how these elements factor into primes.

12. Show that, in contrast to (7.1.66), the polynomial ring

$$\mathbb{Z}[\lambda] \quad \text{is not a PID.}$$

*Hint.* Consider the ideal $(2\lambda, 3\lambda^2)$.
REMARK. It is the case that $\mathbb{Z}[\lambda]$ is a UFD. More generally, given a commutative ring $\mathcal{R}$ with unit,

$$\mathcal{R} \text{ is a UFD} \Longrightarrow \mathcal{R}[\lambda] \text{ is a UFD.}$$

See Section 7.6 for a proof.

## 7.3. The Jordan canonical form revisited

Let $V$ be a finite dimensional vector space over the field $\mathbb{F}$, and let $A \in \mathcal{L}(V)$. Then $V$ gets the structure of a module over the PID $\mathcal{R} = \mathbb{F}[t]$, given by

$$p \cdot v = p(A)v, \tag{7.3.1}$$

for $v \in V,\ p \in \mathbb{F}[t]$, where if $p(t) = a_k t^k + \cdots + a_1 t + a_0$, then

$$p(A) = a_k A^k + \cdots + a_1 A + a_0 I. \tag{7.3.2}$$

The map $p \mapsto p(A)$ is a ring homomorphism $\varphi : \mathbb{F}[t] \to \mathcal{L}(V)$. Then $\mathcal{N}(\varphi)$ is an ideal in $\mathbb{F}[t]$, and since $\mathbb{F}[t]$ is a PID, we have $\mathcal{N}(\varphi) = (m_A)$, for a polynomial $m_A \in \mathbb{F}[t]$, known as the minimal polynomial of $A$, when its leading coefficient is normalized to be 1. We then have an isomorphism

$$\mathbb{F}[t]/(m_A) \approx \mathbb{F}[A], \tag{7.3.3}$$

where $\mathbb{F}[A]$ is the ring in $\mathcal{L}(V)$ generated by $I$ and $A$ (clearly a commutative ring).

We let $\mathcal{V}$ denote $V$ endowed with this structure as an $\mathbb{F}[t]$-module. Then $\mathcal{V}$ depends on both $V$ and $A$. A basis $\{v_1, \dots, v_n\}$ of $V$ over $\mathbb{F}$ also generates $\mathcal{V}$ over $\mathbb{F}[t]$, so $\mathcal{V}$ is a finitely generated $\mathbb{F}[t]$-module. The fact that $m_A(t) \cdot v = 0$ for all $v$ implies that $\mathcal{V}$ is a torsion module, over $\mathbb{F}[t]$.

Let us factor

$$m_A(t) = p_1(t)^{\nu_1} \cdots p_k(t)^{\nu_k}, \tag{7.3.4}$$

where $p_j$ are primes (i.e., irreducible polynomials) in the PID $\mathbb{F}[t]$. Then, by Proposition 7.2.11,

$$\mathcal{V} = \bigoplus_{j=1}^{k} \mathcal{V}(p_j), \tag{7.3.5}$$

where $\mathcal{V}(p_j)$ is the $p_j$-module

$$\begin{aligned} \mathcal{V}(p_j) &= \{v \in \mathcal{V} : p_j^{\nu} \cdot v = 0,\ \text{for some } \nu \in \mathbb{N}\} \\ &= \{v \in \mathcal{V} : p_j(A)^{\nu} v = 0,\ \text{for some } \nu \in \mathbb{N}\}. \end{aligned} \tag{7.3.6}$$

In fact, one has

$$\mathcal{V}(p_j) = \{v \in \mathcal{V} : p_j(A)^{\nu_j} v = 0\}, \tag{7.3.7}$$

from the proof of Proposition 7.2.11, via (7.2.27)–(7.2.28). Clearly

$$A : \mathcal{V}(p_j) \longrightarrow \mathcal{V}(p_j), \tag{7.3.8}$$

for each $j$.

If $\mathbb{F}$ is algebraically closed (e.g., $\mathbb{F} = \mathbb{C}$) then the irreducible polynomials $p_j$ in (7.3.4) have degree 1:

$$m_A(t) = (t - \lambda_1)^{\nu_1} \cdots (t - \lambda_k)^{\nu_k}, \tag{7.3.9}$$

and (7.3.5) holds with

$$\mathcal{V}(p_j) = \{v \in \mathcal{V} : (\lambda I - A)^{\nu_j} v = 0\}. \tag{7.3.10}$$

In other words, each $\mathcal{V}(p_j)$ is a generalized eigenspace of $A$, as defined (for $\mathbb{F} = \mathbb{C}$) in §2.2. In particular, we recover Propositions 2.2.5–2.2.6, in the form given in Exercise 8 of §2.2.

Returning (temporarily) to the level of generality (7.3.4), we deduce from Proposition 7.2.12 that each space $\mathcal{V}(p_j)$ can be decomposed as a direct sum of $\mathbb{F}[t]$-submodules, isomorphic to $\mathbb{F}[t]/(p_j^{\mu})$, for certain $\mu \in \mathbb{N}$. Again if $\mathbb{F}$ is algebraically closed, then $p_j(t) = t - \lambda_j$ for some $\lambda_j \in \mathbb{F}$. We then have

$$\mathcal{V}(p_j) = \bigoplus_{k=1}^{m_j} \mathcal{V}_{jk}, \quad \mathcal{V}_{jk} \approx \mathbb{F}[t]/((t-\lambda_j)^{\mu_k}), \tag{7.3.11}$$

and

$$A : \mathcal{V}_{jk} \longrightarrow \mathcal{V}_{jk}. \tag{7.3.12}$$

The following result, in conjunction with (7.3.11), covers Proposition 2.4.1, on the existence of a Jordan canonical form for $A$.

**Proposition 7.3.1.** *Let $A \in \mathcal{L}(V)$ yield the $\mathbb{F}[t]$-module $\mathcal{V}$ and take*

$$q(t) = (t-\lambda)^{\mu}, \tag{7.3.13}$$

*with $\lambda \in \mathbb{F},\ \mu \in \mathbb{N}$. Assume*

$$\mathcal{V} \approx \mathbb{F}[t]/(q). \tag{7.3.14}$$

*Then $V$ has a basis over $\mathbb{F}$ such that the matrix of $A$ with respect to this basis has the form*

$$A = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 1 & \lambda & & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & \lambda \end{pmatrix}. \tag{7.3.15}$$

**Proof.** The isomorphism $\psi : \mathbb{F}[t]/(q) \xrightarrow{\approx} \mathcal{V}$ yields $v = \psi(1) \in \mathcal{V}$ such that $\mathbb{F}[t]v = \mathcal{V}$. We claim that the elements $\psi((t-\lambda)^j) = (t-\lambda)^j \cdot v,\ 0 \le j \le \mu-1$, i.e., the elements

$$v,\ (A-\lambda I)v,\ \dots,\ (A-\lambda I)^{\mu-1}v \tag{7.3.16}$$

form a basis of $V$ over $\mathbb{F}$. This is a direct consequence of the fact that

$$1,\ t-\lambda,\ \dots,\ (t-\lambda)^{\mu-1}, \quad \text{mod } (q), \tag{7.3.17}$$

forms a basis of $\mathbb{F}[t]/(q)$ over $\mathbb{F}$. Given the basis (7.3.16), it is clear that $A$ takes the form (7.3.15). ☐

Remark. The matrix (7.3.15) is apparently the *transpose* of (2.4.1). We leave it to the reader to sort this out.

## Exercises

1. What happens to the matrix representation of $A$ in (7.3.15) when you reverse the order of the basis elements (7.3.16)?

2. Suppose $\mathbb{F} = \mathbb{R}$, $A \in \mathcal{L}(V)$, and

$$m_A(t) = t^2 + 1.$$

Show that (7.3.5) becomes

$$\mathcal{V} = \mathcal{V}(p), \quad p = m_A.$$

Show that, in the decomposition (7.2.31), with $\mathcal{E}(p)$ replaced by $\mathcal{V}(p)$, one has

$$\mathcal{V}(p) \approx \mathcal{R}/(p) \oplus \cdots \oplus \mathcal{R}/(p), \quad \mathcal{R} = \mathbb{F}[t].$$

In case $\mathcal{V} = \mathcal{R}/(p)$, show that $\dim_{\mathbb{F}} \mathcal{V} = 2$, and that a basis of $\mathcal{V}$ is given by

$$1, \quad t.$$

What is the matrix of $A$ with respect to this basis?

3. How do things change if $\mathbb{R}$ is replaced by $\mathbb{C}$ in Exercise 2?

4. Consider the ring $\mathbb{R}[t]/(t^2 + 1)$. By Lemma 7.2.3 and Proposition 7.2.4, this is a field. Which field is it:

$$\mathbb{R}, \quad \mathbb{C}, \quad \text{something else.}$$

5. Consider the ring $\mathbb{C}[t]/(t^2 + 1)$. Show that this is not a field, and find a simpler object it is isomorphic to.

## 7.4. Integer matrices and algebraic integers

Here we complement results of §6.2 with a discussion of algebraic integers. Given $a \in \mathbb{C}$, $a$ is an algebraic integer if and only if there is a polynomial

$$p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0, \quad a_j \in \mathbb{Z}, \tag{7.4.1}$$

such that $p(a) = 0$. Parallel to Proposition 6.2.2 we have

**Proposition 7.4.1.** *Given $a \in \mathbb{C}$, $a$ is an algebraic integer if and only if there exists $A \in M(n, \mathbb{Z})$ such that $a$ is an eigenvalue of $A$.*

The proof of Proposition 7.4.1 is closely parallel to that of Proposition 6.2.2. From there, arguments similar to those proving Theorem 6.2.1 give the following.

**Theorem 7.4.2.** *If $a, b \in \mathbb{C}$ are algebraic integers, so are $a + b$ and $ab$.*

In the terminology of §§6.1 and 7.1, the set $\mathcal{A}$ of algebraic numbers is a *field*, and the set $\mathcal{O}$ of algebraic integers is a *ring*.

Since $\mathcal{O} \subset \mathcal{A}$, clearly the ring $\mathcal{O}$ is an integral domain, and its quotient field is naturally contained in $\mathcal{A}$. We claim that these fields are equal. In fact, we have the following more precise result.

**Proposition 7.4.3.** *Given $x \in \mathcal{A}$, there exists $k \in \mathbb{Z}$ such that $kx \in \mathcal{O}$.*

**Proof.** Say $x$ satisfies $p(x) = 0$, with $p$ as in (6.2.1). Take $k$ to be the least common denominator of the fractions $a_j$ appearing in (6.2.1). Then $kx \in \mathcal{O}$. $\square$

It is important to know that most elements of $\mathcal{A}$ are not algebraic integers. Here is one result along that line.

**Proposition 7.4.4.** *If $x$ is both an algebraic integer and a rational number, then $x$ is an integer. That is, $x \in \mathcal{O} \cap \mathbb{Q} \Rightarrow x \in \mathbb{Z}$.*

**Proof.** Say $x \in \mathbb{Q}$ solves (7.4.1) but $x \notin \mathbb{Z}$. We can write $x = m/k$ and arrange that $m$ and $k$ be relatively prime. Now multiply (7.4.1) by $k^n$, to get

$$m^n + a_{n-1}m^{n-1}k + \cdots + a_1 m k^{n-1} + a_0 k^n = 0, \quad a_j \in \mathbb{Z}. \tag{7.4.2}$$

It follows that $k$ divides $m^n$, so (since $\mathbb{Z}$ is a UFD) $m$ and $k$ must have a common prime factor. This contradiction proves Proposition 7.4.4. $\square$

Here is an interesting geometrical consequence of Proposition 7.4.4. Consider a regular tetrahedron $\mathcal{T} \subset \mathbb{R}^3$. As one can see from Figure 7.4.1, if $\theta$

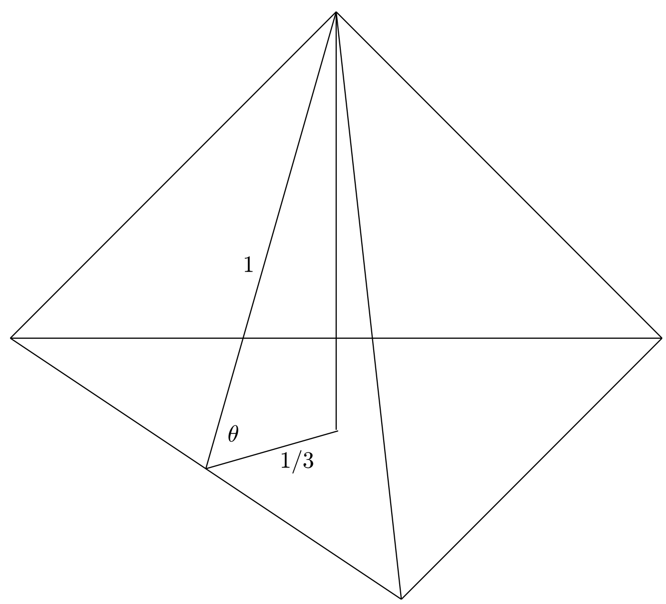


**Figure 7.4.1.** Regular tetrahedron

is the angle between two of its faces, then

$$\cos\theta = \frac{1}{3}, \quad \sin\theta = \frac{2\sqrt{2}}{3}.$$

Consequently,

$$e^{i\theta} = \frac{1}{3} + \frac{2\sqrt{2}}{3} i. \tag{7.4.3}$$

We claim that

$$\theta \text{ is not a rational multiple of } \pi. \tag{7.4.4}$$

Indeed, if $\theta = (m/k)\pi$, then $(e^{i\theta})^{2k} = 1$. However, in fact,

$$\alpha = \frac{1}{3} + \frac{2\sqrt{2}}{3} i \ \text{ is not an algebraic integer.} \tag{7.4.5}$$

Indeed, if $\alpha \in \mathcal{O}$, then also $\overline{\alpha} \in \mathcal{O}$, so $\alpha + \overline{\alpha} \in \mathcal{O}$, by Theorem 7.4.2. But $\alpha + \overline{\alpha} = 2/3$, which is not in $\mathcal{O}$, by Proposition 7.4.4.

This illustrates the fact that natural, elementary, geometric constructions can give rise to angles that are not rational multiples of $\pi$, a fact that is perhaps not much emphasized in basic geometry texts.

Remark. This observation arose in a conversation between the author and Robert Bryant, on a bus ride from MSRI down to the UC campus.

We take a further look at the algebraic number $\alpha$ in (7.4.5), which will lead to a substantial generalization of Proposition 7.4.4. We proceed as follows. Given $\alpha \in \mathcal{A}$, consider

$$\mathcal{I}_\alpha = \{p \in \mathbb{Q}[z] : p(\alpha) = 0\}. \tag{7.4.6}$$

This is an ideal, and since $\mathbb{Q}[z]$ is a PID, we have $\mathcal{I}_\alpha = (q)$ with $q \in \mathcal{I}_\alpha$ of minimal positive degree, say $q(z) = z^\ell + b_{\ell-1}z^{\ell-1} + \cdots + b_1 z + b_0$, with $b_j \in \mathbb{Q}$. We can write each $b_j$ as a quotient of integers in reduced form and multiply by the least common denominator, obtaining

$$q_0(\alpha) = 0, \quad q_0(z) = c_\ell z^\ell + c_{\ell-1}z^{\ell-1} + \cdots + c_1 z + c_0, \quad c_j \in \mathbb{Z}. \tag{7.4.7}$$

In such a situation, the integers $c_j$, $0 \le j \le \ell$, have no common factors, other than $\pm 1$. A polynomial in $\mathbb{Z}[z]$ having this property is said to be a *primitive polynomial.* The argument above shows that, for each $\alpha \in \mathcal{A}$, there is a primitive polynomial $q_0 \in \mathbb{Z}[z]$ such that $q_0$ generates $\mathcal{I}_\alpha$ in $\mathbb{Q}[z]$, and $q_0$ is uniquely determined up to a factor of $\pm 1$. We can uniquely specify it by demanding that $c_\ell > 0$. Let us write

$$q_0(z) = \Pi_\alpha(z). \tag{7.4.8}$$

For $\alpha$ as in (7.4.5), we can compute $\Pi_\alpha(z)$ as follows. Note that

$$\begin{aligned}
&\big(z-(1+2\sqrt{2}i)\big)\big(z-(1-2\sqrt{2}i)\big)\\
&\quad = \big((z-1)+2\sqrt{2}i\big)\Big((z-1)-2\sqrt{2}i\big)\\
&\quad = (z-1)^2 + 8\\
&\quad = z^2 - 2z + 9.
\end{aligned} \tag{7.4.9}$$

This polynomial has $3\alpha$ as a root, so $z^2 - (2/3)z + 1$ generates $\mathcal{I}_\alpha$ in $\mathbb{Q}[z]$, and hence

$$\alpha = \frac{1}{3} + \frac{2\sqrt{2}}{3}i \Longrightarrow \Pi_\alpha(z) = 3z^2 - 2z + 3. \tag{7.4.10}$$

The result (7.4.5) is hence also a consequence of the following.

**Proposition 7.4.5.** *Given $\alpha \in \mathcal{A}$, if $\Pi_\alpha(z)$ is not a monic polynomial (i.e., if its leading coefficient is $> 1$), then $\alpha \notin \mathcal{O}$.*

**Proof.** Assume $\alpha \in \mathcal{A}$ and

$$\Pi_\alpha(z) = b_\ell z^\ell + \cdots + b_1 z + b_0, \quad b_j \in \mathbb{Z}, \quad b_\ell > 1. \tag{7.4.11}$$

We want to contradict the possibility that $p(\alpha) = 0$ for some $p \in \mathbb{Z}[z]$ as in (7.4.1). Indeed, if $p(\alpha) = 0$, then $p \in \mathcal{I}_\alpha$, so

$$\Pi_\alpha(z)q(z) = p(z), \quad \text{for some } \ q \in \mathbb{Q}[z]. \tag{7.4.12}$$

(Note that $\mathbb{Q}[z]$ is a PID, but $\mathbb{Z}[z]$ is not.) Now write the coefficients of $q(z)$ as rational numbers in lowest terms, and multiply (7.4.12) by the least common denominator of these coefficients, call it $M$, to get

$$\Pi_\alpha(z)q_0(z) = Mp(z), \quad q_0 = Mq \in \mathbb{Z}[z]. \tag{7.4.13}$$

We see that $\Pi_\alpha(z)$ and $q_0(z)$ are primitive polynomials. The leading coefficient of both sides of (7.4.13) must be $M$, so, by (7.4.11), $M$ is an integer multiple of $b_\ell$. Thus $Mp(z)$ cannot be a primitive polynomial. This is a contradiction, in light of the following result, known as the *Gauss lemma.* □

**Theorem 7.4.6.** *Given two elements of* $\mathbb{Z}[z]$,

$$\begin{aligned} p_0(z) &= a_k z^k + \cdots + a_1 z + a_0, \quad a_j \in \mathbb{Z}, \\ q_0(z) &= b_\ell z^\ell + \cdots + b_1 z + b_0, \quad b_j \in \mathbb{Z}, \end{aligned} \tag{7.4.14}$$

*if* $p_0$ *and* $q_0$ *are both primitive polynomials, then the product* $p_0q_0$ *is also a primitive polynomial.*

**Proof.** If $p_0q_0$ is not primitive, there is a prime $\gamma \in \mathbb{Z}$ that divides all of its coefficients. The natural projection

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(\gamma) = \mathbb{F}_\gamma \tag{7.4.15}$$

gives rise to a ring homomorphism

$$\chi : \mathbb{Z}[z] \longrightarrow \mathbb{F}_\gamma[z], \tag{7.4.16}$$

and then

$$\chi(p_0)\chi(q_0) = \chi(p_0q_0) = 0 \ \text{ in } \ \mathbb{F}_\gamma[z], \tag{7.4.17}$$

while

$$\chi(p_0) \neq 0 \ \text{ and } \ \chi(q_0) \neq 0 \ \text{ in } \ \mathbb{F}_\gamma[z]. \tag{7.4.18}$$

However, we know that $\mathbb{F}_\gamma$ is a field, and this implies $\mathbb{F}_\gamma[z]$ is an integral domain, so (7.4.17)–(7.4.18) cannot both hold. This proves Theorem 7.4.6. □

Remark. The converse to Proposition 7.4.5 is obvious, so we can restate the result as follows. Given $\alpha \in \mathcal{A}$,

$$\alpha \in \mathcal{O} \Longleftrightarrow \Pi_\alpha(z) \ \text{ is a monic polynomial.} \tag{7.4.19}$$

## Exercises

1. Let $\omega \in \mathbb{C}$ be a root of unity, i.e., $\omega^n = 1$ for some $n \in \mathbb{N}$. Show that

$$\operatorname{Re}\omega \in \mathbb{Q} \Longrightarrow \operatorname{Re}\omega \in \{0, \pm\tfrac{1}{2}, \pm 1\}.$$

See how this generalizes (7.4.3)–(7.4.5).

2. Complementing the result (7.4.3)–(7.4.5) on the regular tetrahedron in $\mathbb{R}^3$, consider the other Platonic solids in $\mathbb{R}^3$ and determine whether the angles between their faces are rational multiples of $\pi$.

## 7.5. Noetherian rings and Noetherian modules

Throughout this section, $\mathcal{R}$ will be a commutative ring with unit. As stated below (7.2.1), we say $\mathcal{R}$ is a Noetherian ring provided the following condition (called the ascending chain condition) holds:

$$\begin{aligned} &\mathcal{I}_j \subset \mathcal{R} \text{ ideals in } \mathcal{R}, \quad \mathcal{I}_1 \subset \mathcal{I}_2 \subset \cdots \subset \mathcal{I}_k \subset \cdots \\ &\Longrightarrow \mathcal{I}_\ell = \mathcal{I}_{\ell+1} = \cdots, \quad \text{for some } \ \ell. \end{aligned} \tag{7.5.1}$$

The content of Proposition 7.2.1 is that

$$\mathcal{R} \text{ is a PID} \Longrightarrow \mathcal{R} \text{ is Noetherian.} \tag{7.5.2}$$

In particular, $\mathcal{R}$ is Noetherian if it is a field, which is clear, since then its only ideals are 0 and $\mathcal{R}$. We will show that the polynomial rings $\mathcal{R}[x_1, \dots, x_n]$ are Noetherian whenever $\mathcal{R}$ is Noetherian, so other examples of Noetherian rings include

$$\mathbb{Z}[x_1, \dots, x_n] \ \text{ and } \ \mathbb{F}[x_1, \dots, x_n], \tag{7.5.3}$$

whenever $\mathbb{F}$ is a field. This is a deep result. First we look at some easy results.

To begin, we recall that the purpose of Proposition 7.2.1 was to apply to the factorization result, Proposition 7.2.2, which we can extend as follows. As in (7.2.2), we say that an element $a \in \mathcal{R} \setminus 0$ that is not invertible is irreducible provided

$$a = bc, \quad b, c \in \mathcal{R} \Longrightarrow b \ \text{ or } \ c \ \text{ is invertible.} \tag{7.5.4}$$

The next result extends Proposition 7.2.2.

**Proposition 7.5.1.** *If $\mathcal{R}$ is a Noetherian ring, each $a \in \mathcal{R} \setminus 0$ that is not invertible can be written as a finite product of irreducible elements.*

**Proof.** Identical to the proof of Proposition 7.2.2. □

On the other hand, (7.2.6) does not extend. We will see examples of Noetherian rings that are not UFDs.

We next present some alternative characterizations of Noetherian rings.

**Proposition 7.5.2.** *For a commutative ring $\mathcal{R}$ with unit, the following conditions are equivalent.*

$$\mathcal{R} \textit{ is Noetherian.} \tag{7.5.5}$$

$$\begin{aligned} &\textit{Each nonempty collection } \mathfrak{C} \textit{ of ideals of } \mathcal{R} \\ &\textit{has a maximal element.} \end{aligned} \tag{7.5.6}$$

$$\textit{Each ideal } \mathcal{I} \subset \mathcal{R} \textit{ is finitely generated.} \tag{7.5.7}$$

**Proof.** First we show that (7.5.5) $\Rightarrow$ (7.5.6). Let $\mathfrak{C}$ be a nonempty collection of ideals of $\mathcal{R}$. Choose $\mathcal{I}_1 \in \mathfrak{C}$. If $\mathfrak{C}$ does not have a maximal element, choose $\mathcal{I}_2 \in \mathfrak{C}$, strictly containing $\mathcal{I}_1$. Continue. Given a strictly increasing chain $\mathcal{I}_1 \subset \cdots \subset \mathcal{I}_k$, you can then choose a strictly larger ideal $\mathcal{I}_{k+1} \in \mathfrak{C}$. The resulting infinite chain contradicts (7.5.1).

The fact that (7.5.6) $\Rightarrow$ (7.5.5) is trivial.

Next we show that (7.5.6) $\Rightarrow$ (7.5.7). Let $\mathcal{I} \subset \mathcal{R}$ be an ideal, and let $\mathfrak{C}$ be the collection of finitely generated ideals contained in $\mathcal{I}$. Then $0 \in \mathfrak{C}$, so $\mathfrak{C}$ is nonempty. If (7.5.6) holds, $\mathfrak{C}$ has a maximal element, say $\mathcal{J}$ (so $\mathcal{J}$ is finitely generated). We claim $\mathcal{J} = \mathcal{I}$. If not, we can take $a \in \mathcal{I} \setminus \mathcal{J}$ and consider the ideal $\mathcal{J}_1$ generated by $\mathcal{I}$ and $a$, which must belong to $\mathfrak{C}$, yielding a contradiction.

Finally, we prove (7.5.7) $\Rightarrow$ (7.5.5). Let $\mathcal{I}_1 \subset \mathcal{I}_2 \subset \cdots \subset \mathcal{I}_k \subset \cdots$ be an increasing chain of ideals. Then $\mathcal{J} = \cup_k \mathcal{I}_k$ is an ideal. If (7.5.7) holds, $\mathcal{J}$ is finitely generated, say $\mathcal{J} = (a_1, \dots, a_\ell)$, with $a_i \in \mathcal{I}_{k_i}$. Hence $\mathcal{J} = \mathcal{I}_k$ with $k = \max k_i$. This finishes the proof of Proposition 7.5.2. $\square$

We next look at the rings $\mathbb{Z}[\omega]$ considered in Exercises 1–5 of §7.2, with

$$\omega = \sqrt{-m},\ m \in \mathbb{N}, \quad \text{or} \quad \omega = \frac{1}{2} + \frac{1}{2}\sqrt{-D},\ D \in \mathbb{N},\ D = 3 \bmod 4. \tag{7.5.8}$$

**Proposition 7.5.3.** *For each $\omega$ in* (7.5.8)*, the ring $\mathbb{Z}[\omega]$ is Noetherian.*

**Proof.** Let $\mathcal{J}$ be an ideal in $\mathbb{Z}[\omega]$. In particular, $\mathcal{J}$ is an additive subgroup of the additive group $\mathbb{Z}[\omega]$, i.e., it is a $\mathbb{Z}$-submodule of the $\mathbb{Z}$-module $\mathbb{Z}[\omega]$, which by Exercise 1 of §7.2 has two generators as a $\mathbb{Z}$-module, namely 1 and $\omega$. By Proposition 7.2.6, $\mathcal{J}$ is a finitely generated $\mathbb{Z}$-module, with at most two generators, say $a_1$ and $a_2$. It follows that $a_1$ and $a_2$ generate $\mathcal{J}$ as an ideal in $\mathbb{Z}[\omega]$, so the criterion (7.5.7) applies. $\square$

Exercise 3 of §7.2 identifies a number of cases in which these rings $\mathbb{Z}[\omega]$ are PIDs. On the other hand, by Exercise 5 of §7.2,

$$\mathbb{Z}[\sqrt{-5}] \text{ is not a UFD.} \tag{7.5.9}$$

This is therefore an example of a Noetherian ring that is not a UFD.

Remark. See Proposition 7.5.12 below for a substantial generalization of Proposition 7.5.3.

We now state and prove the celebrated *Hilbert basis theorem.*

**Theorem 7.5.4.** *If $\mathcal{R}$ is a Noetherian ring, then the polynomial ring $\mathcal{R}[x]$ is also Noetherian.*

**Proof.** We will show that each ideal $\mathcal{I} \subset \mathcal{R}[x]$ is finitely generated. To start, given such $\mathcal{I}$, define $\mathcal{J}_k \subset \mathcal{R}$ by

$$\mathcal{J}_k = \{a \in \mathcal{R} : \exists\, f \in \mathcal{I} \text{ such that } f(x) - ax^k \text{ has degree } < k\}. \tag{7.5.10}$$

One can check that each such $\mathcal{J}_k$ is an ideal in $\mathcal{R}$. Also $f \in \mathcal{R} \Rightarrow xf \in \mathcal{I}$, so $\mathcal{J}_k \subset \mathcal{J}_{k+1}$, and we have an ascending chain of ideals in $\mathcal{R}$. Thus $\mathcal{R}$ Noetherian $\Rightarrow \mathcal{J}_n = \mathcal{J}_{n+1} = \cdots$ for some $n$.

For each $m \le n$, the ideal $\mathcal{J}_m \subset \mathcal{R}$ is finitely generated, say

$$\mathcal{J}_m = (a_{m,1}, \dots, a_{m,r_m}). \tag{7.5.11}$$

Hence, for each $(m, j)$, $1 \le j \le r_m$, there is a polynomial $f_{m,j} \in \mathcal{I}$ of degree $m$, having leading coefficient $a_{m,j}$. We claim that the finite set

$$\{f_{m,j} : m \le n,\ 1 \le j \le r_m\} \tag{7.5.12}$$

generates $\mathcal{I}$.

To see this, let $f \in \mathcal{I}$ have degree $m$. Then its leading coefficient $a$ is in $\mathcal{J}_m$. If $m \ge n$, then $a \in \mathcal{J}_m = \mathcal{J}_n$, so

$$a = \sum_i b_i a_{n,i}, \quad b_i \in \mathcal{R}, \tag{7.5.13}$$

so

$$f(x) - \sum_i b_i x^{m-n} f_{n,i}(x) \text{ has degree } < m, \text{ and belongs to } \mathcal{I}. \tag{7.5.14}$$

On the other hand, if $m \le n$, then

$$a \in \mathcal{J}_m \Longrightarrow a = \sum_i b_i a_{m,i}, \quad b_i \in \mathcal{R}, \tag{7.5.15}$$

so

$$f(x) - \sum_i b_i f_{m,i}(x) \text{ has degree } < m, \text{ and belongs to } \mathcal{I}. \tag{7.5.16}$$

It follows by induction on $m$ that each $f \in \mathcal{I}$ can be written as a linear combination of the elements (7.5.12). Consequently each ideal in $\mathcal{R}[x]$ is finitely generated. This proves Theorem 7.5.4. $\square$

From here a simple inductive argument gives the following result, advertised in the first paragraph of this section.

**Corollary 7.5.5.** *If $\mathcal{R}$ is a Noetherian ring, then, for each $n \in \mathbb{N}$, the polynomial ring*

$$\mathcal{R}[x_1, \dots, x_n] \text{ is Noetherian.} \tag{7.5.17}$$

REMARK. Somewhat parallel to Theorem 7.5.4, though with a completely different proof, we have, for a commutative ring $\mathcal{R}$ with unit,

$$\mathcal{R} \text{ is a UFD} \Rightarrow \mathcal{R}[x] \text{ is a UFD.} \tag{7.5.18}$$

As a consequence, the rings (7.5.3) are also all UFDs. This is established in Section 7.6.

To proceed, we have the following.

**Corollary 7.5.6.** *If $\mathcal{R}$ is a Noetherian ring and $\mathcal{J}$ is an ideal in $\mathcal{R}[x_1, \dots, x_n]$, then*

$$\mathcal{R}[x_1, \dots, x_n]/\mathcal{J} \quad \textit{is Noetherian.} \tag{7.5.19}$$

This is a consequence of Corollary 7.5.5 and the following simple result.

**Proposition 7.5.7.** *If $\mathcal{R}$ is a Noetherian ring and $\mathcal{I}$ is an ideal in $\mathcal{R}$, then $\mathcal{R}/\mathcal{I}$ is Noetherian.*

**Proof.** Consider the natural projection $\pi : \mathcal{R} \to \mathcal{R}/\mathcal{I}$. If $\mathcal{J}$ is an ideal in $\mathcal{R}/\mathcal{I}$, then $\pi^{-1}(\mathcal{J})$ is an ideal in $\mathcal{R}$, so it is finitely generated, say $\pi^{-1}(\mathcal{J}) = (a_1, \dots, a_\ell)$. It follows that $\mathcal{J} = (b_1, \dots, b_\ell)$, with $b_j = \pi(a_j)$. □

We next introduce the concept of a *Noetherian module.* If $\mathcal{R}$ is a commutative ring with unit, an $\mathcal{R}$-module $\mathcal{M}$ is said to be a Noetherian module provided the following ascending chain condition holds:

$$\begin{aligned} &\mathcal{M}_j \subset \mathcal{M} \text{ submodules}, \quad \mathcal{M}_1 \subset \mathcal{M}_2 \subset \cdots \subset \mathcal{M}_k \subset \cdots \\ &\Longrightarrow \mathcal{M}_\ell = \mathcal{M}_{\ell+1} = \cdots, \text{ for some } \ell. \end{aligned} \tag{7.5.20}$$

Parallel to Proposition 7.5.2, we have the following equivalent characterizations.

**Proposition 7.5.8.** *If $\mathcal{M}$ is a $\mathcal{R}$-module, the following conditions are equivalent.*

$$\mathcal{M} \textit{ is a Noetherian module.} \tag{7.5.21}$$

$$\begin{aligned} &\textit{Each nonempty collection } \mathfrak{C} \textit{ of submodules of } \mathcal{M} \\ &\textit{has a maximal element.} \end{aligned} \tag{7.5.22}$$

$$\textit{Each submodule of } \mathcal{M} \textit{ is finitely generated.} \tag{7.5.23}$$

**Proof.** Essentially the same as the proof of Proposition 7.5.2. □

We now develop basic results about Noetherian modules, following the efficient presentation in §3.4 of [**18**].

**Proposition 7.5.9.** *Let $\mathcal{L}, \mathcal{M}$, and $\mathcal{N}$ be $\mathcal{R}$-modules, connected by $\mathcal{R}$-homomorphisms*

$$\mathcal{L} \xrightarrow{\alpha} \mathcal{M} \xrightarrow{\beta} \mathcal{N}. \tag{7.5.24}$$

*Assume*

$$\alpha \text{ injective}, \quad \beta \text{ surjective}, \quad \text{and } \mathcal{R}(\alpha) = \mathcal{N}(\beta). \tag{7.5.25}$$

*Then*

$$\mathcal{M} \text{ is Noetherian} \Longleftrightarrow \mathcal{L} \text{ and } \mathcal{N} \text{ are Noetherian.} \tag{7.5.26}$$

**Proof.** First, the implication $\Rightarrow$ in (7.5.26) is easy, since ascending chains of submodules in $\mathcal{L}$ and in $\mathcal{N}$ correspond one-to-one to associated ascending chains in $\mathcal{M}$.

We turn to the proof of the implication $\Leftarrow$. Let

$$\mathcal{M}_1 \subset \mathcal{M}_2 \subset \cdots \subset \mathcal{M}_k \subset \cdots \tag{7.5.27}$$

be an ascending chain of submodules of $\mathcal{M}$. We identify $\mathcal{L}$ with its image $\alpha(\mathcal{L})$ in $\mathcal{M}$. Taking intersections gives a chain

$$\mathcal{L} \cap \mathcal{M}_1 \subset \mathcal{L} \cap \mathcal{M}_2 \subset \cdots \subset \mathcal{L} \cap \mathcal{M}_k \subset \cdots \tag{7.5.28}$$

of submodules of $\mathcal{M}$ (and of $\mathcal{L}$). Also, applying $\beta$ to (7.5.27) gives an ascending chain

$$\beta(\mathcal{M}_1) \subset \beta(\mathcal{M}_2) \subset \cdots \subset \beta(\mathcal{M}_k) \subset \cdots \tag{7.5.29}$$

of submodules of $\mathcal{N}$. Given that $\mathcal{L}$ and $\mathcal{N}$ are Noetherian, the chains (7.5.28) and (7.5.29) each stabilize, so for some $\ell$,

$$\mathcal{L} \cap \mathcal{M}_\ell = \mathcal{L} \cap \mathcal{M}_{\ell+1} = \cdots, \quad \beta(\mathcal{M}_\ell) = \beta(\mathcal{M}_{\ell+1}) = \cdots. \tag{7.5.30}$$

To finish the proof, it suffices to show that, given submodules $\mathcal{M}_\ell \subset \mathcal{M}_{\ell+1} \subset \mathcal{M}$, and given (7.5.25),

$$\mathcal{L} \cap \mathcal{M}_\ell = \mathcal{L} \cap \mathcal{M}_{\ell+1} \ \text{ and } \ \beta(\mathcal{M}_\ell) = \beta(\mathcal{M}_{\ell+1}) \Longrightarrow \mathcal{M}_\ell = \mathcal{M}_{\ell+1}. \tag{7.5.31}$$

Indeed, if $x \in \mathcal{M}_{\ell+1}$, then $\beta(x) \in \beta(\mathcal{M}_{\ell+1}) = \beta(\mathcal{M}_\ell)$, so there exists $y \in \mathcal{M}_\ell$ such that $\beta(x) = \beta(y)$. Then $\beta(x - y) = 0$. Since $\mathcal{N}(\beta) = \alpha(\mathcal{L}) = \mathcal{L}$, we have

$$x - y \in \mathcal{L} \cap \mathcal{M}_{\ell+1} = \mathcal{L} \cap \mathcal{M}_\ell, \tag{7.5.32}$$

so $x \in \mathcal{M}_\ell$, and we have (7.5.31), and the proof of Proposition 7.5.9 is complete. $\square$

An alternative statement of Proposition 7.5.9 is that if $\mathcal{M}$ is an $\mathcal{R}$-module and $\mathcal{L} \subset \mathcal{M}$ a submodule,

$$\mathcal{M} \text{ is Noetherian } \Longleftrightarrow \mathcal{L} \text{ and } \mathcal{M}/\mathcal{L} \text{ are Noetherian.} \tag{7.5.33}$$

One simple application of Proposition 7.5.9 is that if $\mathcal{M}_1$ and $\mathcal{M}_2$ are $\mathcal{R}$-modules,

$$\mathcal{M}_1 \text{ and } \mathcal{M}_2 \text{ Noetherian} \Longrightarrow \mathcal{M}_1 \oplus \mathcal{M}_2 \text{ is Noetherian.} \tag{7.5.34}$$

In fact, we have natural $\mathcal{R}$-homomorphisms

$$\mathcal{M}_1 \xrightarrow{\alpha} \mathcal{M}_1 \oplus \mathcal{M}_2 \xrightarrow{\beta} \mathcal{M}_2, \tag{7.5.35}$$

satisfying the conditions of (7.5.24)–(7.5.25). Inductively, we have

$$\mathcal{M}_j \text{ Noetherian} \Longrightarrow \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_k \text{ Noetherian.} \tag{7.5.36}$$

The following is a major consequence of Propositions 7.5.8 and 7.5.9. In particular, it extends Corollary 7.2.7 from the setting of a module over a PID to that of a module over a Noetherian ring.

**Proposition 7.5.10.** *Let $\mathcal{R}$ be a Noetherian ring, and let $\mathcal{M}$ be a finitely generated $\mathcal{R}$-module. Then $\mathcal{M}$ is a Noetherian module. Consequently, each submodule $\mathcal{L}$ of $\mathcal{M}$ is finitely generated.*

**Proof.** If $\mathcal{M}$ is generated by $k$ elements, then there is a surjective homomorphism $\beta : \mathcal{R}^k \to \mathcal{M}$, so $\mathcal{M} \approx \mathcal{R}^k/\mathcal{N}$ where $\mathcal{N} = \mathcal{N}(\beta)$ is a submodule of $\mathcal{R}^k$. By (7.5.36), $\mathcal{R}^k$ is a Noetherian module, and the conclusion that $\mathcal{R}^k/\mathcal{N}$ is Noetherian follows from the implication $\Rightarrow$ in (7.5.33). Having $\mathcal{M}$ Noetherian, we deduce that each submodule $\mathcal{L}$ is finitely generated (and in fact Noetherian), by Proposition 7.5.8. □

The following result yields another proof (and indeed a substantial generalization) of Proposition 7.5.3.

**Proposition 7.5.11.** *Let $\mathcal{B}$ be a commutative ring with unit, and let $\mathcal{A}$ be a subring (with the same unit). Assume $\mathcal{A}$ is Noetherian and $\mathcal{B}$ is a finitely generated $\mathcal{A}$-module. Then $\mathcal{B}$ is a Noetherian ring.*

**Proof.** By Proposition 7.5.10, $\mathcal{B}$ is a Noetherian $\mathcal{A}$-module. Now any ascending chain of ideals in $\mathcal{B}$ is also an ascending chain of $\mathcal{A}$-modules, hence it stabilizes, so $\mathcal{B}$ is a Noetherian ring. □

Note how Proposition 7.5.11 applies to Proposition 7.5.3, with $\mathcal{A} = \mathbb{Z}$, $\mathcal{B} = \mathbb{Z}[\omega]$. Using Proposition 7.5.11, one can extend the scope of Proposition 7.5.3, from $\omega$ as in (7.5.8) to arbitrary algebraic integers. More generally, if

$$\omega_1, \dots, \omega_\ell \text{ are algebraic integers,} \tag{7.5.37}$$

then

$$\mathbb{Z}[\omega_1, \dots, \omega_\ell] \text{ is a finitely-generated } \mathbb{Z}\text{-module,} \tag{7.5.38}$$

hence a Noetherian ring. Put another way:

**Proposition 7.5.12.** *Each finitely generated subring (with unit) of the ring $\mathcal{O}$ of algebraic integers is a Noetherian ring.*

By contrast, we have the following.

**Proposition 7.5.13.** *The ring $\mathcal{O}$ of algebraic integers is not a Noetherian ring.*

**Proof.** We will show that the ascending chain

$$\mathcal{I}_k = (2, 2^{1/2}, 2^{1/3}, \dots, 2^{1/k}) \tag{7.5.39}$$

of ideals in $\mathcal{O}$ does not stabilize. Indeed,

$$\begin{aligned}
\mathcal{I}_k = \mathcal{I}_{k+1} \Longrightarrow &\\
\sum_{j=1}^{k} a_j 2^{1/j} &= 2^{1/(k+1)}, \quad a_j \in \mathcal{O} \\
\Longrightarrow 1 &= \sum_{j=1}^{k} a_j 2^{1/j-1/(k+1)} \\
&= 2^{1/k-1/(k+1)} \sum_{j=1}^{k} a_j 2^{1/j-1/k} \\
&= 2^{1/k(k+1)} \sum_{j=1}^{k} a_j 2^{(k-j)/jk} \\
\Longrightarrow\ & 2^{-1/k(k+1)} \in \mathcal{O} \\
\Longrightarrow\ & 2^{-1} \in \mathcal{O},
\end{aligned} \tag{7.5.40}$$

which is false (cf. Proposition 7.4.4). This proves Proposition 7.5.13. $\square$

## 7.6. Polynomial rings over UFDs

Our goal here is to prove that, given a commutative ring $\mathcal{R}$ with unit,

$$\mathcal{R} \text{ is a UFD} \Longrightarrow \mathcal{R}[x] \text{ is a UFD.} \tag{7.6.1}$$

We start with the following basic case.

**Proposition 7.6.1.** *The polynomial ring $\mathbb{Z}[x]$ is a UFD.*

**Proof.** Take $p(x) \in \mathbb{Z}[x]$. Thanks to Theorem 7.5.4, we can apply Proposition 7.5.1 to factor $p(x)$ into irreducible factors, say

$$p(x) = \alpha a_1(x) \cdots a_k(x), \tag{7.6.2}$$

with $\alpha \in \mathbb{Z}$ (in turn written as a product of primes in $\mathbb{Z}$) and each $a_j(x)$ irreducible in $\mathbb{Z}[x]$. In particular, the coefficients of each factor $a_j(x)$ have no common factors, i.e., $a_j(x)$ is a primitive polynomial (as defined in Section 7.4). Now suppose that also

$$p(x) = \beta b_1(x) \cdots b_\ell(x), \tag{7.6.3}$$

with $\beta \in \mathbb{Z}$ and each $b_j(x)$ an irreducible (hence primitive) polynomial in $\mathbb{Z}[x]$. By the Gauss lemma, Theorem 7.4.6, both $a_1(x) \cdots a_k(x)$ and $b_1(x) \cdots b_\ell(x)$ are primitive polynomials. It follows that both $\alpha$ and $\beta$ are the largest common factors of the coefficients of $p(x)$, so $\alpha = \beta$, up to a sign, which, when adjusted, leads to

$$a_1(x) \cdots a_k(x) = b_1(x) \cdots b_\ell(x). \tag{7.6.4}$$

Given that $\mathbb{Q}[x]$ is a PID, hence a UFD, one can readily deduce from the following result that $\ell = k$ and that these factorizations coincide, up to order and units (in this case, factors of $\pm 1$). $\square$

**Lemma 7.6.2.** *If $q(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.*

**Proof.** Irreducibility in $\mathbb{Z}[x]$ implies $q(x)$ is a primitive polynomial. If it is not irreducible in $\mathbb{Q}[x]$, we can write

$$q(x) = q_1(x) q_2(x), \quad q_j(x) \in \mathbb{Q}[x], \tag{7.6.5}$$

each factor having positive degree. Clearing denominators, we can write

$$q_j(x) = \gamma_j r_j(x), \quad \gamma_j \in \mathbb{Q}, \ r_j(x) \in \mathbb{Z}[x], \tag{7.6.6}$$

and we can arrange that each $r_j(x)$ be a primitive polynomial. Then

$$q(x) = \gamma r_1(x) r_2(x), \quad \gamma = \gamma_1 \gamma_2 \in \mathbb{Q}. \tag{7.6.7}$$

The Gauss lemma implies $r_1(x) r_2(x)$ is primitive, and we have already noted that $q(x)$ is primitive. This forces $\gamma = \pm 1$, and then (7.6.7) contradicts irreducibility of $q(x)$ in $\mathbb{Z}[x]$. Thus we have Lemma 7.6.2, which enables us to complete the proof of Proposition 7.6.1. $\square$

The argument used to prove Proposition 7.6.1 needs several modifications in order to yield (7.6.1) for a general UFD $\mathcal{R}$. To start, the argument given above to yield the factorization (7.6.2) does not work unless $\mathcal{R}$ is also a Noetherian ring. For an alternative approach, given $p(x) \in \mathcal{R}[x]$, first factor out the common prime factors of its coefficients, and write

$$p(x) = \alpha p_0(x), \quad \alpha \in \mathcal{R},\ p_0(x) \in \mathcal{R}[x], \tag{7.6.8}$$

where the coefficients of $p_0(x)$ have no common factors in $\mathcal{R}$ (again we say $p_0(x)$ is a primitive polynomial). Then let $\mathcal{F}$ denote the quotient field of $\mathcal{R}$, and write

$$p_0(x) = q_1(x) \cdots q_k(x), \quad q_j(x) \in \mathcal{F}[x], \tag{7.6.9}$$

with $q_j(x)$ irreducible in $\mathcal{F}[x]$, which is possible since $\mathcal{F}[x]$ is a PID. Next, clear out denominators to write

$$p_0(x) = \delta a_1(x) \cdots a_k(x), \quad \delta \in \mathcal{F},\ a_j(x) \in \mathcal{R}[x], \tag{7.6.10}$$

and arrange that each $a_j(x)$ is primitive, as well as irreducible in $\mathcal{F}[x]$. To proceed, we need a version of the Gauss lemma when $\mathcal{R}$ is a UFD. Here it is.

**Proposition 7.6.3.** *Assume $\mathcal{R}$ is a UFD and $p_1, p_2 \in \mathcal{R}[x]$. Then*

$$p_1 \text{ and } p_2 \text{ primitive} \Longrightarrow p_1 p_2 \text{ primitive.} \tag{7.6.11}$$

**Proof.** This is parallel to the proof of Theorem 7.4.6.
If $p_1 p_2$ is not primitive, there is a prime $\gamma \in \mathcal{R}$ that divides all its coefficients. Note that, in this setting,

$$\begin{aligned} \gamma \in \mathcal{R} \text{ prime} &\Longrightarrow \mathcal{F}_\gamma = \mathcal{R}/(\gamma) \text{ integral domain} \\ &\Longrightarrow \mathcal{F}_\gamma[x] \text{ integral domain.} \end{aligned} \tag{7.6.12}$$

Now the natural projection $\mathcal{R} \to \mathcal{F}_\gamma$ gives rise to a ring homomorphism

$$\chi : \mathcal{R}[x] \longrightarrow \mathcal{F}_\gamma[x], \tag{7.6.13}$$

and then

$$\chi(p_1)\chi(p_2) = \chi(p_1 p_2) = 0 \quad \text{in} \quad \mathcal{F}_\gamma[x], \tag{7.6.14}$$

while

$$\chi(p_1) \neq 0 \quad \text{and} \quad \chi(p_2) \neq 0 \quad \text{in} \quad \mathcal{F}_\gamma[x]. \tag{7.6.15}$$

Of course, (7.6.14)–(7.6.15) contradict (7.6.12), so (7.6.11) must hold. $\square$

Returning to (7.6.10), we see from Proposition 7.6.3 that $a_1(x)\cdots a_k(x) \in \mathcal{R}[x]$ is primitive, and since $p_0(x)$ is primitive, $\delta$ must belong to $\mathcal{R}$ and in fact must be a unit of $\mathcal{R}$. We can absorb it into $a_1(x)$ and rewrite (7.6.10) as

$$p_0(x) = a_1(x)\cdots a_k(x), \quad a_j(x) \in \mathcal{R}[x], \tag{7.6.16}$$

and each $a_j(x)$ is irreducible in $\mathcal{F}[x]$, and a fortiori in $\mathcal{R}[x]$. This gives

$$p(x) = \alpha a_1(x)\cdots a_k(x), \tag{7.6.17}$$

with $\alpha$ as in (7.6.8). We can factor $\alpha \in \mathcal{R}$ into primes, since $\mathcal{R}$ is a UFD, and in this fashion obtain a factorization of $p(x)$ into irreducible elements of $\mathcal{R}[x]$.

At this point we are in a position to establish our main result.

**Proposition 7.6.4.** *If $\mathcal{R}$ is a UFD, then $\mathcal{R}[x]$ is a UFD.*

**Proof.** Given $p(x) \in \mathcal{R}[x]$, the argument leading up to (7.6.17) gives the existence of a factorization of $p(x)$ into irreducible elements of $\mathcal{R}[x]$. To tackle uniqueness, assume also

$$p(x) = \beta b_1(x)\cdots b_\ell(x), \tag{7.6.18}$$

with $\beta \in \mathcal{R}$ and each $b_j(x)$ irreducible (hence primitive) in $\mathcal{R}[x]$. Again, by Proposition 7.6.3, $b_1(x)\cdots b_\ell(x)$ is primitive, so comparison with (7.6.17) gives

$$p(x) = \alpha p_0(x) = \beta q_0(x), \quad \alpha, \beta \in \mathcal{R},\ p_0(x), q_0(x) \in \mathcal{R}[x], \tag{7.6.19}$$

with $p_0(x)$ and $q_0(x)$ both primitive. It follows that, if one factors each of the coefficients of $p(x)$ into primes in $\mathcal{R}$, and pulls out all the factors common to all the coefficients of $p(x)$, one gets simultaneously both $\alpha$ and $\beta$, up to a unit factor. Hence $\alpha = \beta$, up to a unit factor. We can absorb that factor into $b_1(x)$, and we get

$$a_1(x)\cdots a_k(x) = b_1(x)\cdots b_\ell(x), \tag{7.6.20}$$

as in (7.6.4). To proceed, we need the following extension of Lemma 7.6.2. $\square$

**Lemma 7.6.5.** *Let $\mathcal{R}$ be a UFD, with quotient field $\mathcal{F}$. If $q(x) \in \mathcal{R}[x]$ is irreducible in $\mathcal{R}[x]$, then it is irreducible in $\mathcal{F}[x]$.*

**Proof.** The proof is parallel to that of Lemma 7.6.2, with $\mathcal{R}$ in place of $\mathbb{Z}$ and $\mathcal{F}$ in place of $\mathbb{Q}$, except that now we have (7.6.7) with $\gamma$ a unit of $\mathcal{R}$, which suffices to complete the proof. $\square$

Having Lemma 7.6.5 and the fact that $\mathcal{F}[x]$ is a UFD, we are able to argue as in the proof of Proposition 7.6.1 that $k = \ell$ and the factors on the two sides of (7.6.20) coincide, up to a rearrangement and unit factors. This yields Proposition 7.6.4.

**Corollary 7.6.6.** *If $\mathcal{R}$ is a UFD, then each polynomial ring $\mathcal{R}[x_1, \ldots, x_n]$ is a UFD.*

Chapter 8

# Special structures in linear algebra

Linear algebra gives rise to many interesting objects with special structure. We examine four such structures here. These have both classical roots and enduring significance.

In §8.1 we study the quaternions, i.e.,

$$\mathbb{H} = \{\xi = a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}, \tag{8.0.1}$$

isomorphic as a vector space over $\mathbb{R}$ to $\mathbb{R}^4$. One also writes $\xi = a + v$, where $a$ is the real part and $v = bi + cj + dk$ is the vector part. $\mathbb{H}$ is also endowed with a product, $\xi, \eta \in \mathbb{H} \Rightarrow \xi\eta \in \mathbb{H}$, an $\mathbb{R}$-bilinear map in which 1 acts as the multiplicative identity. The multiplication table for $i, j, k$ mirrors the cross product, except that, rather than $i^2 = j^2 = k^2 = 0$, we take

$$i^2 = j^2 = k^2 = -1. \tag{8.0.2}$$

This product incorporates both the dot product and the cross product for the vector parts of the factors. One basic result is the associative law:

$$\zeta(\xi\eta) = (\zeta\xi)\eta, \quad \zeta, \xi, \eta \in \mathbb{H}. \tag{8.0.3}$$

This fundamental result in turn implies some nontrivial identities involving the cross product and dot product on $\mathbb{R}^3$. It is seen that each nonzero $\xi \in \mathbb{H}$ has a multiplicative inverse. Thus $\mathbb{H}$ satisfies all the conditions of a field, except that multiplication is not commutative. One sometimes calls $\mathbb{H}$ a "noncommutative field."

Section 8.1 also looks at matrices of elements of $\mathbb{H}$,

$$M(n, \mathbb{H}) = \{A = (a_{jk}) : a_{jk} \in \mathbb{H}\}, \tag{8.0.4}$$

and a subset

$$Sp(n) = \{A \in M(n, \mathbb{H}) : A^* A = I\}. \tag{8.0.5}$$

It is seen that $Sp(n)$ is a group, and there is a natural injection

$$\mathrm{Sp}(n) \hookrightarrow O(4n), \tag{8.0.6}$$

making $Sp(n)$ a compact matrix group.

The product on $\mathbb{H}$ makes it a ring. The structure of $\mathbb{H}$ as a vector space makes this product $\mathbb{R}$-bilinear. This sets up $\mathbb{H}$ as an example of an *algebra*, studied in a general setting in §8.2. Generally, an algebra $\mathcal{A}$ over a field $\mathbb{F}$ is a vector space over $\mathbb{F}$ having a product $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$ that is $\mathbb{F}$-bilinear. Section 8.2 mainly deals with associative algebras, in which the product makes $\mathcal{A}$ a ring. Examples include matrix algebras, tensor algebras, and exterior algebras. There are also important classes of non-associative algebras, i.e., algebras for which the $\mathbb{F}$-bilinear product does not satisfy the condition of associativity. One prime class of examples is the class of Lie algebras. Another example arises in §8.4.

Section 8.3 is devoted to Clifford algebras. Given a real vector space $V$, of dimension $n$, and a quadratic form $Q$ on $V$, one defines $\mathcal{C}\ell(V, Q)$ as an associative algebra over $\mathbb{R}$, with unit, generated by $V$, and satisfying the anticommutation relations

$$uv + vu = -2Q(u, v)1, \quad u, v \in V. \tag{8.0.7}$$

We construct $\mathcal{C}\ell(V, Q)$ as a quotient of the tensor algebra of $V$, modulo an ideal, designed to capture these anticommutation relations. Then $\mathcal{C}\ell(V, Q)$ is a real vector space of dimension $2^n$. We investigates its structure, which depends on $Q$. If $Q = 0$, then we get the exterior algebra $\Lambda^* V$. We also investigate the relation between Clifford algebras and a class of first-order systems of differential operators called Dirac operators, which are important in the modern theory of partial differential equations.

Section 8.4 is devoted to a special non-associative algebra known as the algebra of octonions. This algebra, denoted $\mathbb{O}$, is an 8-dimensional real vector space, isomorphic as a vector space to $\mathbb{H} \oplus \mathbb{H}$, endowed with a multiplication that, to the degree possible, carries on the progression of how the product on $\mathbb{R}$ leads to the product on $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}$, and from there to the product on $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}$. In passing from $\mathbb{C}$ to $\mathbb{H}$, one loses commutativity of the product, and in passing from $\mathbb{H}$ to $\mathbb{O}$ one loses associativity. Nevertheless, $\mathbb{O}$ possesses an astonishingly rich structure.

One reflection of this is manifested in the rich structure of the automorphism group of $\mathbb{O}$, $\mathrm{Aut}(\mathbb{O})$, consisting of $\mathbb{R}$-linear isomorphisms $K : \mathbb{O} \to \mathbb{O}$ that preserve the product: $K(uv) = K(u)K(v)$. To describe a setting for this group, we recall the groups $SO(n)$ and $U(n)$, introduced in Chapter 3, and $Sp(n)$, introduced in §8.1. These form the "classical" compact matrix groups. In addition to this list, there are five "exceptional" compact matrix groups, denoted

$$G_2, \quad F_4, \quad E_6, \quad E_7, \quad E_8. \tag{8.0.8}$$

Results on the structure of $\mathrm{Aut}(\mathbb{O})$ established here can be shown to lead to the identity

$$\mathrm{Aut}(\mathbb{O}) = G_2. \tag{8.0.9}$$

Beyond this, the theory of the algebra $\mathbb{O}$ of octonions can be used as a key to the other exceptional groups. Further material on this can be found in [**21**].

## 8.1. Quaternions and matrices of quaternions

The space $\mathbb{H}$ of quaternions is a four-dimensional real vector space, identified with $\mathbb{R}^4$, with basis elements $1, i, j, k$, the element 1 identified with the real number 1. Elements of $\mathbb{H}$ are represented as follows:

$$\xi = a + bi + cj + dk, \tag{8.1.1}$$

with $a, b, c, d \in \mathbb{R}$. We call $a$ the real part of $\xi$ ($a = \operatorname{Re}\xi$) and $bi + cj + dk$ the vector part. We also have a multiplication on $\mathbb{H}$, an $\mathbb{R}$-bilinear map $\mathbb{H} \times \mathbb{H} \to \mathbb{H}$, such that $1 \cdot \xi = \xi \cdot 1 = \xi$, and otherwise governed by the rules

$$ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik, \tag{8.1.2}$$

and

$$i^2 = j^2 = k^2 = -1. \tag{8.1.3}$$

Otherwise stated, if we write

$$\xi = a + u, \quad a \in \mathbb{R}, \quad u \in \mathbb{R}^3, \tag{8.1.4}$$

and similarly write $\eta = b + v,\ b \in \mathbb{R},\ v \in \mathbb{R}^3$, the product is given by

$$\xi\eta = (a + u)(b + v) = (ab - u \cdot v) + av + bu + u \times v. \tag{8.1.5}$$

Here $u \cdot v$ is the dot product in $\mathbb{R}^3$, and $u \times v$ is the cross product, introduced in Exercises 5–11 of §3.4. The quantity $ab - u \cdot v$ is the real part of $\xi\eta$ and $av + bu + u \times v$ is the vector part. Note that

$$\xi\eta - \eta\xi = 2u \times v. \tag{8.1.6}$$

It is useful to take note of the following symmetries of $\mathbb{H}$.

**Proposition 8.1.1.** *Let $K : \mathbb{H} \to \mathbb{H}$ be an $\mathbb{R}$-linear transformation such that $K1 = 1$ and $K$ cyclically permutes $(i, j, k)$ (e.g., $Ki = j,\ Kj = k,\ Kk = i$). Then $K$ preserves the product in $\mathbb{H}$, i.e.,*

$$K(\xi\eta) = K(\xi)K(\eta), \quad \forall\, \xi, \eta \in \mathbb{H}. \tag{8.1.7}$$

*We say $K$ is an automorphism of $\mathbb{H}$.*

**Proof.** This is straightforward from the multiplication rules (8.1.2)–(8.1.3). $\square$

We move on to the following basic result.

**Proposition 8.1.2.** *Multiplication in $\mathbb{H}$ is associative, i.e.,*

$$\zeta(\xi\eta) = (\zeta\xi)\eta, \quad \forall\, \zeta, \xi, \eta \in \mathbb{H}. \tag{8.1.8}$$

**Proof.** Given the $\mathbb{R}$-bilinearity of the product, it suffices to check (8.1.8) when each $\zeta, \xi$, and $\eta$ is either $1, i, j$, or $k$. Since 1 is the multiplicative unit, the result (8.1.8) is easy when any factor is 1. Furthermore, one can use Proposition 8.1.1 to reduce the possibilities further; for example, one can take $\zeta = i$. We leave the final details to the reader. $\square$

Remark. In the case that $\xi = u, \eta = v$, and $\zeta = w$ are purely vectorial, we have

(8.1.9)
$$\begin{aligned} w(uv) &= w(-u \cdot v + u \times v) = -(u \cdot v)w - w \cdot (u \times v) + w \times (u \times v), \\ (wu)v &= (-w \cdot u + w \times u)v = -(w \cdot u)v - (w \times u) \cdot v + (w \times u) \times v. \end{aligned}$$

Then the identity of the two left sides is equivalent to the pair of identities

$$w \cdot (u \times v) = (w \times u) \cdot v, \tag{8.1.10}$$

$$w \times (u \times v) - (w \times u) \times v = (u \cdot v)w - (w \cdot u)v. \tag{8.1.11}$$

Compare (8.1.10) with Exercise 11 of §3.4. As for (8.1.11), it also follows from the pair of identities

$$w \times (u \times v) - (w \times u) \times v = u \times (w \times v), \tag{8.1.12}$$

and

$$u \times (w \times v) = (u \cdot v)w - (w \cdot u)v, \tag{8.1.13}$$

for which see Exercises 9–10 of §3.4. See Exercise 5 below for the converse.

In addition to the product, we also have a conjugation operation on $\mathbb{H}$:

$$\overline{\xi} = a - bi - cj - dk = a - u. \tag{8.1.14}$$

A calculation gives

$$\xi\overline{\eta} = (ab + u \cdot v) - av + bu - u \times v. \tag{8.1.15}$$

In particular,

$$\mathrm{Re}(\xi\overline{\eta}) = \mathrm{Re}(\overline{\eta}\xi) = (\xi, \eta), \tag{8.1.16}$$

the right side denoting the Euclidean inner product on $\mathbb{R}^4$. Setting $\eta = \xi$ in (8.1.15) gives

$$\xi\overline{\xi} = |\xi|^2, \tag{8.1.17}$$

the Euclidean square-norm of $\xi$. In particular, whenever $\xi \in \mathbb{H}$ is nonzero, it has a multiplicative inverse,

$$\xi^{-1} = |\xi|^{-2}\overline{\xi}. \tag{8.1.18}$$

We say a ring $\mathcal{R}$ with unit 1 is a division ring if each nonzero $\xi \in \mathcal{R}$ has a multiplicative inverse. It follows from (8.1.18) that $\mathbb{H}$ is a division ring. It

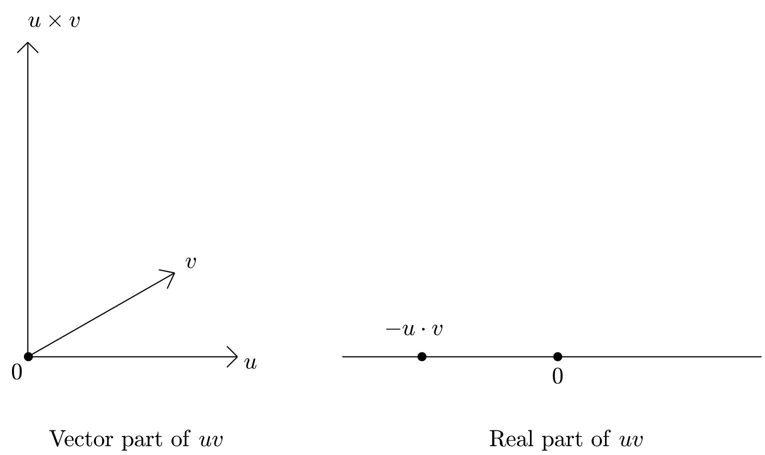


**Figure 8.1.1.** Quaternionic product of vectors in $\mathbb{R}^3$

is not a field, since multiplication in $\mathbb{H}$ is not commutative. Sometimes $\mathbb{H}$ is called a "noncommutative field."

To continue with products and conjugation, a routine calculation gives

$$\overline{\xi\eta} = \overline{\eta}\,\overline{\xi}. \tag{8.1.19}$$

Hence, via the associative law,

$$|\xi\eta|^2 = (\xi\eta)(\overline{\xi\eta}) = \xi\eta\overline{\eta}\overline{\xi} = |\eta|^2\xi\overline{\xi} = |\xi|^2|\eta|^2, \tag{8.1.20}$$

or

$$|\xi\eta| = |\xi|\,|\eta|. \tag{8.1.21}$$

Note that $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ sits in $\mathbb{H}$ as a commutative subring, for which the properties (8.1.17) and (8.1.21) are familiar.

Let us examine (8.1.21) when $\xi = u$ and $\eta = v$ are purely vectorial. We have (as illustrated in Figure 8.1.1)

$$uv = -u \cdot v + u \times v. \tag{8.1.22}$$

Hence, directly,

$$|uv|^2 = (u \cdot v)^2 + |u \times v|^2, \tag{8.1.23}$$

while (8.1.21) implies

$$|uv|^2 = |u|^2|v|^2. \tag{8.1.24}$$

As seen in Exercise 1 of §3.4, if $\theta$ is the angle between $u$ and $v$ in $\mathbb{R}^3$,

$$u \cdot v = |u|\,|v|\,\cos\theta. \tag{8.1.25}$$

Hence (8.1.23) implies

$$|u \times v|^2 = |u|^2|v|^2 \sin^2\theta. \tag{8.1.26}$$

Compare Exercise 7 of §3.4.

We next consider the set of unit quaternions:

$$Sp(1) = \{\xi \in \mathbb{H} : |\xi| = 1\}. \tag{8.1.27}$$

Using (8.1.18) and (8.1.21), we see that $Sp(1)$ is a group under multiplication. It sits in $\mathbb{R}^4$ as the unit sphere $S^3$. We compare $Sp(1)$ with the group $SU(2)$, consisting of $2 \times 2$ complex matrices of the form

$$U = \begin{pmatrix} \xi & -\overline{\eta} \\ \eta & \overline{\xi} \end{pmatrix}, \quad \xi, \eta \in \mathbb{C}, \quad |\xi|^2 + |\eta|^2 = 1. \tag{8.1.28}$$

The group $SU(2)$ is also in natural one-to-one correspondence with $S^3$. Furthermore, we have:

**Proposition 8.1.3.** *The groups $SU(2)$ and $Sp(1)$ are isomorphic under the correspondence*

$$U \mapsto \xi + j\eta, \tag{8.1.29}$$

*for $U$ as in* (8.1.28).

**Proof.** The correspondence (8.1.29) is clearly bijective. To see it is a homomorphism of groups, we calculate:

$$\begin{pmatrix} \xi & -\overline{\eta} \\ \eta & \overline{\xi} \end{pmatrix} \begin{pmatrix} \xi' & -\overline{\eta}' \\ \eta' & \overline{\xi}' \end{pmatrix} = \begin{pmatrix} \xi\xi' - \overline{\eta}\eta' & -\xi\overline{\eta}' - \overline{\eta}\overline{\xi}' \\ \eta\xi' + \overline{\xi}\eta' & -\eta\overline{\eta}' + \overline{\xi}\overline{\xi}' \end{pmatrix}, \tag{8.1.30}$$

given $\xi, \eta \in \mathbb{C}$. Noting that, for $a, b \in \mathbb{R}$, $j(a + bi) = (a - bi)j$, we have

$$\begin{aligned} (\xi + j\eta)(\xi' + j\eta') &= \xi\xi' + \xi j\eta' + j\eta\xi' + j\eta j\eta' \\ &= \xi\xi' - \overline{\eta}\eta' + j(\eta\xi' + \overline{\xi}\eta'). \end{aligned} \tag{8.1.31}$$

Comparison of (8.1.30) and (8.1.31) verifies that (8.1.29) yields a homomorphism of groups. □

We next define the map

$$\pi : Sp(1) \longrightarrow \mathcal{L}(\mathbb{R}^3) \tag{8.1.32}$$

by

$$\pi(\xi)u = \xi u \xi^{-1} = \xi u \overline{\xi}, \quad \xi \in Sp(1),\ u \in \mathbb{R}^3 \subset \mathbb{H}. \tag{8.1.33}$$

To justify (8.1.32), we need to show that if $u$ is purely vectorial, so is $\xi u\overline{\xi}$. In fact, by (8.1.19),

$$\zeta = \xi u\overline{\xi} \Longrightarrow \overline{\zeta} = \overline{\overline{\xi}}\,\overline{u}\,\overline{\xi} = -\xi u\overline{\xi} = -\zeta, \tag{8.1.34}$$

so that is indeed the case. By (8.1.21),

$$|\pi(\xi)u| = |\xi|\,|u|\,|\overline{\xi}| = |u|, \quad \forall\, u \in \mathbb{R}^3,\ \xi \in Sp(1), \tag{8.1.35}$$

so in fact

$$\pi : Sp(1) \longrightarrow SO(3), \tag{8.1.36}$$

and it follows easily from the definition (8.1.33) that if also $\zeta \in Sp(1)$, then $\pi(\xi\zeta) = \pi(\xi)\pi(\zeta)$, so (8.1.36) is a group homomorphism. It is readily verified that

$$\operatorname{Ker}\pi = \{\pm 1\}. \tag{8.1.37}$$

Note that we can extend (8.1.32) to

$$\pi : Sp(1) \longrightarrow \mathcal{L}(\mathbb{H}), \quad \pi(\xi)\eta = \xi\eta\overline{\xi}, \quad \xi \in Sp(1),\ \eta \in \mathbb{H}, \tag{8.1.38}$$

and again $\pi(\xi\zeta) = \pi(\xi)\pi(\zeta)$ for $\xi, \zeta \in Sp(1)$. Furthermore, each map $\pi(\xi)$ is a ring homomorphism, i.e.,

$$\pi(\xi)(\alpha\beta) = (\pi(\xi)\alpha)(\pi(\xi)\beta), \quad \alpha, \beta \in \mathbb{H},\ \xi \in Sp(1). \tag{8.1.39}$$

Since $\pi(\xi)$ is invertible, this is a group of ring automorphisms of $\mathbb{H}$. The reader is invited to draw a parallel to the following situation. Define

$$\tilde{\pi} : SO(3) \longrightarrow \mathcal{L}(\mathbb{H}), \quad \tilde{\pi}(T)(a+u) = a + Tu, \tag{8.1.40}$$

given $a+u \in \mathbb{H},\ a \in \mathbb{R},\ u \in \mathbb{R}^3$. It is a consequence of the identity (3.4.34), i.e., $T(u \times v) = Tu \times Tv$, for $u, v \in \mathbb{R}^3$, that

$$\tilde{\pi}(T)(\alpha\beta) = (\tilde{\pi}(T)\alpha)(\tilde{\pi}(T)\beta), \quad \alpha, \beta \in \mathbb{H},\ T \in SO(3). \tag{8.1.41}$$

Thus $SO(3)$ acts as a group of automorphisms of $\mathbb{H}$. (Note that Proposition 8.1.1 is a special case of this.) We claim this is the same group of automorphisms as described in (8.1.38)–(8.1.39), via (8.1.36). This is a consequence of the fact that $\pi$ in (8.1.36) is surjective. We mention that the automorphism $K$ in Proposition 8.1.1 has the form (8.1.38) with

$$\xi = \frac{1}{2}(1 + i + j + k).$$

To proceed, we consider $n \times n$ matrices of quaternions:

$$A = (a_{jk}) \in M(n, \mathbb{H}), \quad a_{jk} \in \mathbb{H}. \tag{8.1.42}$$

If $\mathbb{H}^n$ denotes the space of column vectors of length $n$, whose entries are quaternions, then $A \in M(n, \mathbb{H})$ acts on $\mathbb{H}^n$ by the usual formula. Namely, if $\xi = (\xi_j)^t,\ \xi_j \in \mathbb{H}$, we have

$$(A\xi)_j = \sum_k a_{jk}\xi_k. \tag{8.1.43}$$

Note that

$$A : \mathbb{H}^n \longrightarrow \mathbb{H}^n \tag{8.1.44}$$

is $\mathbb{R}$-linear, and commutes with the *right action* of $\mathbb{H}$ on $\mathbb{H}^n$, defined by

$$(\xi b)_j = \xi_j b, \quad \xi \in \mathbb{H}^n,\ b \in \mathbb{H}. \tag{8.1.45}$$

Composition of such matrix operations on $\mathbb{H}^n$ is given by the usual matrix product. If $B = (b_{jk})$, then

$$(AB)_{jk} = \sum_\ell a_{j\ell} b_{\ell k}. \tag{8.1.46}$$

We define a conjugation on $M(n, \mathbb{H})$. With $A$ given by (8.1.42),

$$A^* = (\overline{a}_{kj}). \tag{8.1.47}$$

Clearly $(A^*)^* = A$. A calculation using (8.1.19) gives

$$(AB)^* = B^* A^*. \tag{8.1.48}$$

We are ready to define the groups $Sp(n)$ for $n > 1$:

$$Sp(n) = \{A \in M(n, \mathbb{H}) : A^* A = I\}. \tag{8.1.49}$$

Note that $A^*$ is a left inverse of the $\mathbb{R}$-linear map $A : \mathbb{H}^n \to \mathbb{H}^n$ if and only if it is a right inverse (by real linear algebra). In other words, given $A \in M(n, \mathbb{H})$,

$$A^* A = I \Longleftrightarrow AA^* = I. \tag{8.1.50}$$

In particular,

$$A \in Sp(n) \Longleftrightarrow A^* \in Sp(n) \Longleftrightarrow A^{-1} \in Sp(n). \tag{8.1.51}$$

Also, given $A, B \in Sp(n)$,

$$(AB)^* AB = B^* A^* AB = B^* B = I. \tag{8.1.52}$$

Hence $Sp(n)$, defined by (8.1.49), is a group.

For another perspective, we put a quaternionic inner product on $\mathbb{H}^n$ as follows. If $\xi = (\xi_j)^t, \eta = (\eta_j)^t \in \mathbb{H}^n$, set

$$\langle \xi, \eta \rangle = \sum_j \overline{\eta}_j \xi_j. \tag{8.1.53}$$

From (8.1.16), we have

$$\mathrm{Re}\langle \xi, \eta \rangle = (\xi, \eta), \tag{8.1.54}$$

where the right side denotes the Euclidean inner product on $\mathbb{H}^n = \mathbb{R}^{4n}$. Now, if $A \in M(n, \mathbb{H})$, $A = (a_{jk})$, then

$$\begin{aligned} \langle A\xi, \eta \rangle &= \sum_{j,k} \overline{\eta}_j a_{jk} \xi_k \\ &= \sum_{j,k} \overline{\overline{a}_{jk} \eta_j} \xi_k \\ &= \langle \xi, A^* \eta \rangle. \end{aligned} \tag{8.1.55}$$

Hence

$$\langle A\xi, A\eta \rangle = \langle \xi, A^* A\eta \rangle. \tag{8.1.56}$$

In particular, given $A \in M(n, \mathbb{H})$, we have $A \in Sp(n)$ if and only if $A : \mathbb{H}^n \to \mathbb{H}^n$ preserves the quaternionic inner product (8.1.53). Given (8.1.54), we have

$$Sp(n) \hookrightarrow O(4n). \tag{8.1.57}$$

## Exercises

1. Fill in the details for the proof of Proposition 8.1.2.

2. Work out a proof of (8.1.19). Show that, if $\xi = a + u, \eta = b + v$,

$$\begin{aligned}\overline{\xi}\,\overline{\eta} &= ab - u \cdot v - av - ab + u \times v \\ &= \overline{\eta\xi}.\end{aligned}$$

3. Take $z = a + ib,\ w = c + id \in \mathbb{C}$, so $\xi$ in (8.1.1) becomes

$$\xi = z + wj.$$

If also $\eta = u + vj,\ u, v \in \mathbb{C}$, show that the multiplication law for $\mathbb{H}$ becomes

$$\xi\eta = (zu - w\overline{v}) + (w\overline{u} + zv)j.$$

*Hint.* $jv = \overline{v}j$.

4. Define $\mathbb{R}$-linear maps,

$$\alpha : \mathbb{C}^2 \longrightarrow \mathbb{H}, \quad \beta : \mathbb{C}^2 \longrightarrow \mathcal{L}(\mathbb{C}^2),$$

by

$$\alpha\begin{pmatrix} z \\ w \end{pmatrix} = z + wj, \quad \beta\begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} z & -w \\ \overline{w} & \overline{z} \end{pmatrix}.$$

Note that $\alpha$ is an $\mathbb{R}$-linear isomorphism, so we have the $\mathbb{R}$-linear map

$$\gamma = \beta \circ \alpha^{-1} : \mathbb{H} \longrightarrow \mathcal{L}(\mathbb{C}^2).$$

Modify the proof of Proposition 8.1.3 to show that

$$\xi, \eta \in \mathbb{H} \longrightarrow \gamma(\xi\eta) = \gamma(\xi)\gamma(\eta).$$

Thus $\gamma$ effects an $\mathbb{R}$-linear ring isomorphism of $\mathbb{H}$ onto a subring of $\mathcal{L}(\mathbb{C}^2)$.

5. Supplement the implication (8.1.12)–(8.1.13) $\Rightarrow$ (8.1.11). with the converse implication.
*Hint.* To start, given (8.1.11), permute letters to supplement this with

$$\begin{aligned} w \times (v \times u) - (w \times v) \times u &= (v \cdot u)w - (w \cdot v)u, \\ u \times (w \times v) - (u \times w) \times v &= (w \cdot v)u - (u \cdot w)v. \end{aligned} \tag{8.1.58}$$

Then add (8.1.58) to (8.1.11) to obtain (8.1.13).

**Exponentiation of quaternions**

6. Following arguments in §3.7, show that

$$e^{t\xi} = \sum_{k=0}^{\infty} \frac{t^k}{k!}\xi^k$$

is a convergent power series for all $t \in \mathbb{R},\ \xi \in \mathbb{H}$, and that we have

$$\frac{d}{dt}e^{t\xi} = \xi e^{t\xi}.$$

7. Show that

$$e^{(s+t)\xi} = e^{s\xi}e^{t\xi}, \quad \forall\, s,t \in \mathbb{R},\ \xi \in \mathbb{H},$$

and if also $\eta \in \mathbb{H}$,

$$\xi\eta = \eta\xi \Longrightarrow e^{t(\xi+\eta)} = e^{t\xi}e^{t\eta}.$$

8. Show that if $u \in \mathbb{R}^3 \subset \mathbb{H},\ u \neq 0$, then, for $t \in \mathbb{R}$,

$$e^{tu} = \Bigl(\cos t|u|\Bigr) + \Bigl(\sin t|u|\Bigr)\frac{u}{|u|},$$

and, if $\xi = a + u$,

$$e^{t\xi} = e^{ta}\Bigl[\Bigl(\cos t|u|\Bigr) + \Bigl(\sin t|u|\Bigr)\frac{u}{|u|}\Bigr].$$

9. Show that, for $t \in \mathbb{R}$,

$$u \in \mathbb{R}^3 \subset \mathbb{H} \Longrightarrow e^{tu} \in Sp(1),$$

using either Exercise 6 or

$$\overline{e^{t\xi}} = e^{t\bar{\xi}}.$$

**Quaternionic matrix exponential**

10. Parallel to Exercise 6, show that, for $A \in M(n,\mathbb{H})$,

$$e^{tA} = \sum_{k=0}^{\infty} \frac{t^k}{k!}A^k \in M(n,\mathbb{H})$$

is a convergent power series for $t \in \mathbb{R}$, and that we have

$$\frac{d}{dt}e^{tA} = Ae^{tA}.$$

11. Show that

$$e^{(s+t)A} = e^{sA}e^{tA}, \quad \forall\, s,t \in \mathbb{R},\ A \in M(n,\mathbb{H}),$$

and, if also $B \in M(n, \mathbb{H})$,

$$AB = BA \Longrightarrow e^{t(A+B)} = e^{tA}e^{tB}.$$

12. Defining $A^* \in M(n, \mathbb{H})$ as in (8.1.47), show that, for $t \in \mathbb{R}$,

$$\left(e^{tA}\right)^* = e^{tA^*}.$$

13. Let us set

$$\mathfrak{sp}(n) = \{A \in M(n, \mathbb{H}) : A^* = -A\}.$$

Show that

$$A \in \mathfrak{sp}(n),\ t \in \mathbb{R} \Longrightarrow e^{tA} \in Sp(n),$$

and that

$$A, B \in \mathfrak{sp}(n) \Longrightarrow [A, B] \in \mathfrak{sp}(n).$$

## 8.2. Algebras

Let $\mathbb{F}$ be a field. An *algebra* $\mathcal{A}$ over $\mathbb{F}$ has the following structure:

$$\mathcal{A} \text{ is a vector space over } \mathbb{F}, \tag{8.2.1}$$

$$\begin{gathered}\mathcal{A} \text{ is a ring, and the product } (u,v) \mapsto uv \text{ is} \\ \text{an } \mathbb{F}\text{-bilinear map } \mathcal{A} \times \mathcal{A} \to \mathcal{A}.\end{gathered} \tag{8.2.2}$$

Hence, if $a \in \mathbb{F},\ u,v \in \mathcal{A}$,

$$a(uv) = (au)v = u(av). \tag{8.2.3}$$

We say $\mathcal{A}$ is a *commutative algebra* if $u,v \in \mathcal{A} \Rightarrow uv = vu$. If (8.2.1)–(8.2.2) hold and $\mathcal{A}$ is a ring with unit (call it $1_{\mathcal{A}}$, temporarily) we call $\mathcal{A}$ an algebra with unit, and simply denote the unit by 1 (the same symbol as used for the unit in $\mathbb{F}$).

A number of rings we have seen before have natural structures as algebras, such as $M(n,\mathbb{F})$ and $\mathbb{F}[t]$, which are algebras over the field $\mathbb{F}$. If $\mathcal{A}$ is an algebra over $\mathbb{F}$, then $M(n,\mathcal{A})$ and $\mathcal{A}[t]$ are algebras over $\mathbb{F}$. On the other hand, the rings $M(n,\mathbb{Z}), \mathbb{Z}[t]$, and $\mathbb{Z}/(n)$ (when $n$ is not a prime) are not algebras over a field. The ring $\mathbb{H}$ of quaternions, introduced in §8.1, is an algebra over $\mathbb{R}$ (hence $\mathbb{H}$ is often called the algebra of quaternions). Note that $\mathbb{H}$ is not an algebra over $\mathbb{C}$.

If $V$ is an $n$-dimensional vector space over $\mathbb{F}$, the ring

$$\Lambda^* V = \bigoplus_{k=0}^{n} \Lambda^k V, \tag{8.2.4}$$

where $\Lambda^0 V = \mathbb{F},\ \Lambda^1 V = V$, and $\Lambda^k V$ is as in (5.3.64), with the wedge product, described in §21, is an algebra over $\mathbb{F}$ (called the exterior algebra of $V$). We can also write

$$\Lambda^* V = \bigoplus_{k=0}^{\infty} \Lambda^k V, \tag{8.2.5}$$

keeping in mind that $\Lambda^k V = 0$ for $k > n = \dim V$. Recall that

$$\alpha \in \Lambda^i V,\ \beta \in \Lambda^j V \Longrightarrow \alpha \wedge \beta \in \Lambda^{i+j} V. \tag{8.2.6}$$

Another algebra over $\mathbb{F}$ associated with such an $n$-dimensional vector space is the *tensor algebra*, defined by

$$\otimes^* V = \bigoplus_{k=0}^{\infty} \otimes^k V, \tag{8.2.7}$$

where

$$\otimes^0 V = \mathbb{F}, \quad \otimes^1 V = V, \quad \otimes^2 V = V \otimes V, \tag{8.2.8}$$

and, for $k \geq 3$,

$$\otimes^k V = V \otimes \cdots \otimes V \quad (k \text{ factors}), \tag{8.2.9}$$

defined as in §5.2, i.e., $\otimes^k V = V_1 \otimes \cdots \otimes V_k$ with each $V_j = V$. That is to say, an element $\alpha \in \otimes^k V$ is a $k$-linear map

$$\alpha : V' \times \cdots \times V' \longrightarrow \mathbb{F}. \tag{8.2.10}$$

If also $\beta \in \otimes^\ell V$, then $\alpha \otimes \beta \in \Lambda^{k+\ell} V$ is defined by

$$\alpha \otimes \beta(w_1, \dots, w_k, w_{k+1}, \dots, w_{k+\ell}) = \alpha(w_1, \dots, w_k)\, \beta(w_{k+1}, \dots, w_{k+\ell}), \tag{8.2.11}$$

for $w_j \in V'$. As opposed to (8.2.5), if $V \neq 0$, all the terms $\otimes^k V$ are nonzero. We define the countable direct sum

$$\mathcal{V} = \bigoplus_{k=0}^{\infty} V_k \tag{8.2.12}$$

of vector spaces $V_k$ to consist of elements

$$(v_0, v_1, v_2, \dots, v_j, \dots), \quad v_j \in V_j, \tag{8.2.13}$$

such that only finitely many $v_j$ are nonzero. This is a vector space, with vector operations

$$\begin{aligned} &(v_0, v_1, \dots, v_j, \dots) + (v_0', v_1', \dots, v_j', \dots) \\ &\quad = (v_0 + v_0', v_1 + v_1', \dots, v_j + v_j', \dots), \\ &a(v_0, v_1, \dots, v_j, \dots) = (av_0, av_1, \dots, av_j, \dots). \end{aligned} \tag{8.2.14}$$

In such a fashion, $\otimes^* V$ is a vector space (of infinite dimension) over $\mathbb{F}$, and the product (8.2.11) makes it an algebra over $\mathbb{F}$.

This tensor algebra possesses the following *universal property*:

**Proposition 8.2.1.** *Let $\mathcal{A}$ be an algebra over $\mathbb{F}$ with unit, $V$ an $n$-dimensional vector space over $\mathbb{F}$, and let*

$$M : V \longrightarrow \mathcal{A} \tag{8.2.15}$$

*be a linear map. Them $M$ extends uniquely to a homomorphism of algebras (i.e., an $\mathbb{F}$-linear ring homomorphism)*

$$\widetilde{M} : \otimes^* V \longrightarrow \mathcal{A}. \tag{8.2.16}$$

**Proof.** The extension is given by $\widetilde{M}(1) = 1$ and

$$\widetilde{M}(v_1 \otimes \cdots \otimes v_k) = M(v_1) \cdots (Mv_k), \quad v_j \in V. \tag{8.2.17}$$

Verifying that this yields an algebra homomorphism is straightforward from the definitions. $\square$

In case $\mathcal{A} = \Lambda^* V$, with $V = \Lambda^1 V$, Proposition 8.2.1 yields

$$\widetilde{M} : \otimes^* V \longrightarrow \Lambda^* V. \tag{8.2.18}$$

Clearly this is surjective. Furthermore,

$$\begin{gathered}\mathcal{N}(\widetilde{M}) = \mathcal{I}, \text{ the 2-sided ideal in } \oplus^* V \text{ generated by} \\ \{v \otimes w + w \otimes v : v, w \in V\}.\end{gathered} \tag{8.2.19}$$

Hence

$$\Lambda^* V \approx \otimes^* V / \mathcal{I}. \tag{8.2.20}$$

Next, let $\mathcal{A}$ be an algebra and $V$ a vector space over $\mathbb{F}$, both finite dimensional, and form the tensor product $\mathcal{A} \otimes V$, seen from §5.2 to be a vector space over $\mathbb{F}$. In fact, $\mathcal{A} \otimes V$ has the natural structure of an $\mathcal{A}$-module, given by

$$a(b \otimes v) = (ab) \otimes v, \quad a, b \in \mathcal{A},\ v \in V. \tag{8.2.21}$$

One important class of examples arises with $\mathbb{F} = \mathbb{R}$, $\mathcal{A} = \mathbb{C}$, and $V$ a real vector space, yielding the *complexification*,

$$V_{\mathbb{C}} = \mathbb{C} \otimes V. \tag{8.2.22}$$

This is a $\mathbb{C}$-module, hence a vector space over $\mathbb{C}$. We might write the right side of (8.2.22) as $\mathbb{C} \otimes_{\mathbb{R}} V$, to emphasize what field we are tensoring over. To illustrate the role of $\mathbb{F}$ in the notation $\mathcal{A} \otimes_{\mathbb{F}} V$, we note that

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}^n \approx \mathbb{C}^{2n}, \quad \text{but} \ \ \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}^n \approx \mathbb{C}^n. \tag{8.2.23}$$

Specializing to the case where $V = \mathcal{B}$ is also an algebra over $\mathbb{F}$, we have

$$\mathcal{A} \otimes \mathcal{B}, \tag{8.2.24}$$

which also has the structure of an algebra over $\mathbb{F}$, with product defined by

$$(a \otimes b)(a' \otimes b') = (aa') \otimes (bb'). \tag{8.2.25}$$

In particular, with $\mathbb{F} = \mathbb{R}$ and $\mathcal{A} = \mathbb{C}$, we have for an $\mathbb{R}$-algebra $\mathcal{B}$ the complexification

$$\mathcal{B}_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} \mathcal{B}. \tag{8.2.26}$$

An example is

$$M(n, \mathbb{R})_{\mathbb{C}} = M(n, \mathbb{C}). \tag{8.2.27}$$

Here is an interesting tensor product computation, which will make an appearance in Section 8.3:

**Proposition 8.2.2.** *We have* $\mathbb{H} \otimes \mathbb{H} \approx \mathcal{L}(\mathbb{H})$, *or equivalently*

$$\mathbb{H} \otimes \mathbb{H} \approx M(4, \mathbb{R}), \tag{8.2.28}$$

*as algebras over* $\mathbb{R}$.

**Proof.** We define $\alpha : \mathbb{H} \otimes \mathbb{H} \to \mathcal{L}(\mathbb{H})$ as follows. For $\xi, \eta, \zeta \in \mathbb{H}$, set

$$\alpha(\xi \otimes \eta)\zeta = \xi\zeta\overline{\eta}. \tag{8.2.29}$$

This extends by linearity to produce a linear map $\alpha : \mathbb{H} \otimes \mathbb{H} \to \mathcal{L}(\mathbb{H})$. Note that $\alpha(1 \otimes 1) = I$. We also have

$$\begin{aligned} \alpha(\xi\xi' \otimes \eta\eta')\zeta &= (\xi\xi')\zeta(\overline{\eta\eta'}) \\ &= (\xi\xi')\zeta(\overline{\eta}'\overline{\eta}) \\ &= \xi(\xi'\zeta\overline{\eta}')\overline{\eta} \\ &= \xi(\alpha(\xi' \otimes \eta')\zeta)\overline{\eta} \\ &= \alpha(\xi \otimes \eta)\alpha(\xi' \otimes \eta')\zeta, \end{aligned} \tag{8.2.30}$$

from which it follows that $\alpha$ is a homomorphism of algebras.

It remains to prove that $\alpha$ is bijective. Since $\dim \mathbb{H}\otimes\mathbb{H} = \dim M(4, \mathbb{R}) = 16$, it suffices to prove *one* of the following:

$$\mathcal{N}(\alpha) = 0, \quad \text{or} \quad \mathcal{R}(\alpha) = \mathcal{L}(\mathbb{H}). \tag{8.2.31}$$

Note that $\mathcal{N}(\alpha)$ is a two-sided ideal in $\mathbb{H} \otimes \mathbb{H}$ and $\mathcal{R}(\alpha)$ is a subalgebra of $\mathcal{L}(\mathbb{H})$. It is the case that $\mathbb{H} \otimes \mathbb{H}$ has no proper two-sided ideals (the reader might try to prove this), which would imply $\mathcal{N}(\alpha) = 0$, but this is not the route we will take. Instead, we propose to show that $\mathcal{R}(\alpha) = \mathcal{L}(\mathbb{H})$, via a path through some other interesting results. $\square$

To start, let $\beta$ denote the restriction of $\alpha$ to $\xi, \eta \in Sp(1)$, the group of unit quaternions. Note that

$$\xi, \eta \in Sp(1) \Longrightarrow |\xi\zeta\overline{\eta}| = |\zeta|, \tag{8.2.32}$$

so

$$\beta : Sp(1) \times Sp(1) \longrightarrow SO(4), \tag{8.2.33}$$

and, by (8.2.30), it is a group homomorphism. Clearly if $(\xi, \eta) \in \operatorname{Ker}\beta$, then (taking $\zeta = 1$) we must have $\xi\overline{\eta} = 1$, hence $\eta = \xi$. Next, $(\xi, \overline{\xi}) \in \operatorname{Ker}\beta$ If and only if $\xi$ commutes with each $\zeta \in \mathbb{H}$. This forces $\xi = \pm 1$. Thus

$$\operatorname{Ker}\beta = \{(1, 1), (-1, -1)\}, \tag{8.2.34}$$

so $\beta$ is a two-to-one map. At this point, it is convenient to have in hand some basic concepts about Lie groups (such as described in the first few chapters of [**25**]). Namely, $Sp(1)$ has dimension 3 (recall from (8.1.27) the identification of $Sp(1)$ with the 3-sphere $S^3$), and $SO(4)$ has dimension 6. From (8.2.34) it can be deduced that the range of $\beta$ in (8.2.33) is a 6-dimensional subgroup of $SO(4)$. It is also the case that $SO(4)$ is connected, and any 6-dimensional subgroup must be all of $SO(4)$. Thus $\beta$ in (8.2.33) is onto. We record this progress.

**Lemma 8.2.3.** *The group homomorphism $\beta$ in* (8.2.33) *is two-to-one and onto.*

It follows that the range $\mathcal{R}(\alpha)$ is a subalgebra of $\mathcal{L}(\mathbb{R}^4)$ that contains $SO(4)$. The following result finishes off the proof of Proposition 8.2.2.

**Lemma 8.2.4.** *For $n \geq 3$, the algebra of linear transformations of $\mathbb{R}^n$ generated by $SO(n)$ is equal to $\mathcal{L}(\mathbb{R}^n)$.*

**Proof.** Denote this algebra by $\mathcal{A}$, and note that $\mathcal{A}$ is actually the linear span of $SO(n)$. (For $n = 2$, $\mathcal{A}$ is commutative, and the conclusion fails.) Using the inner product $\langle A, B\rangle = \operatorname{Tr} A^t B$ on $\mathcal{L}(\mathbb{R}^n)$, suppose there exists $A \in \mathcal{L}(\mathbb{R}^n)$ that is orthogonal to $\mathcal{A}$. Then

$$\operatorname{Tr}(UA) = 0 \tag{8.2.35}$$

for all $U \in SO(n)$.

For the moment, assume $n$ is odd. Then $U \in O(n)$ implies either $U$ or $-U$ belongs to $SO(n)$, so (G.35) holds for all $U \in O(n)$. By Proposition 3.6.2, we can write

$$A = KP, \quad K \in O(n),\ P \text{ positive semidefinite.} \tag{8.2.36}$$

Taking $U = K^{-1}$ in (8.2.35) yields

$$\operatorname{Tr} P = 0, \quad \text{hence} \ \ P = 0, \quad \text{hence} \ \ A = 0. \tag{8.2.37}$$

We hence have Lemma 8.2.4 for $n$ odd. □

In order to produce an argument that works for $n \geq 4$ even, we bring in the following. Let $G_m$ denote the subgroup of $SO(m)$ consisting of rotations that preserve the cube

$$Q_m = \{x \in \mathbb{R}^m : |x_j| \leq 1,\ \text{for } 1 \leq j \leq m\}.$$

The action of an element of $G_m$ is uniquely determined by how it permutes the vertices of $Q_m$, so $G_m$ is a finite group. Now take

$$P = \frac{1}{o(G_m)} \sum_{T \in G_m} T \in \mathcal{L}(\mathbb{R}^m). \tag{8.2.38}$$

**Proposition 8.2.5.** *For $m \geq 2$, $P = 0$.*

**Proof.** Since $T \in G_m \Rightarrow T^{-1} = T^t \in G_m$, we see that

$$P = P^t. \tag{8.2.39}$$

If we multiply both sides of (8.2.38) on the left by $U \in G_m$, we get the sum over the same set of terms on the right, so

$$UP = P, \quad \forall\, U \in G_m. \tag{8.2.40}$$

Averaging both sides of (8.2.40) over $U \in G_m$ yields

$$P^2 = P. \tag{8.2.41}$$

Thus $P$ is an orthogonal projection on $\mathbb{R}^m$, and, by (8.2.40), each vector $v$ in the range of $P$ satisfies

$$Uv = v, \quad \forall\, U \in G_m. \tag{8.2.42}$$

Now the only $v \in \mathbb{R}^m$ satisfying (8.2.42) is $v = 0$, so $P = 0$. □

We return to Lemma 8.2.4, and give a demonstration valid for all $n \ge 3$. To start, note that

$$T \in G_{n-1} \Longrightarrow \begin{pmatrix} T & \\ & 1 \end{pmatrix} \in SO(n). \tag{8.2.43}$$

By Proposition 8.2.5, as long as $n \ge 3$,

$$\frac{1}{o(G_{n-1})} \sum_{T \in G_{n-1}} \begin{pmatrix} T & \\ & 1 \end{pmatrix} = \begin{pmatrix} 0 & \\ & 1 \end{pmatrix}, \tag{8.2.44}$$

where the upper left 0 is the zero matrix in $M(n-1, \mathbb{R})$. It follows that the right side of (8.2.44) (call it $P_1$) belongs to $\mathcal{A}$. Hence

$$I - 2P_1 = \begin{pmatrix} I & \\ & -1 \end{pmatrix} \in \mathcal{A}, \tag{8.2.45}$$

where the upper left $I$ in the last matrix is the identity in $M(n-1, \mathbb{R})$. This is an element of $O(n)$ with negative determinant! It follows that $O(n) \subset \mathcal{A}$. From here, the argument involving (8.2.35) (now known to hold for all $U \in O(n)$), proceeding to (8.2.36)–(8.2.37), works, and we have Lemma 8.2.4 for all $n \ge 3$. □

We return to generalities. As we have defined the concept of an algebra $\mathcal{A}$, it must have the associative property (6.1.6), i.e.,

$$u, v, w \in \mathcal{A} \Longrightarrow u(vw) = (uv)w. \tag{8.2.46}$$

For emphasis, we sometimes call $\mathcal{A}$ an *associative algebra*. This terminology is apparently redundant, but it is useful in face of the fact that there are important examples of "non-associative algebras," which satisfy most of the properties we require of an algebra, but lack the property (8.2.46). We close this section with a brief mention of some significant classes of nonassociative algebras.

**Lie algebras**

The paradigm cases of Lie algebras arise as follows. Let $V$ be a vector space over $\mathbb{F}$. A linear subspace $L$ of $\mathcal{L}(V)$ is a Lie algebra of transformations on $V$ provided

$$A, B \in L \Longrightarrow [A, B] \in L, \tag{8.2.47}$$

where

$$[A, B] = AB - BA. \tag{8.2.48}$$

We define the action ad of $L$ on itself by

$$\mathrm{ad}(A)B = [A, B]. \tag{8.2.49}$$

It is routine to verify that

$$\mathrm{ad}([A, B]) = \mathrm{ad}(A)\ \mathrm{ad}(B) - \mathrm{ad}(B)\ \mathrm{ad}(A). \tag{8.2.50}$$

This is equivalent to the identity

$$[[A, B], C] = [A, [B, C]] - [B, [A, C]], \tag{8.2.51}$$

for all $A, B, C \in \mathcal{L}(V)$. The identity (8.2.50) (or (8.2.51)) is called the *Jacobi identity*.

With this in mind, we define a Lie algebra $L$ (over a field $\mathbb{F}$) to be a vector space over over $\mathbb{F}$, equipped with an $\mathbb{F}$-bilinear map

$$\lambda : L \times L \longrightarrow L, \quad \lambda(A, B) = [A, B], \tag{8.2.52}$$

satisfying

$$[A, B] = -[B, A], \tag{8.2.53}$$

and the Jacobi identity (8.2.49)–(8.2.50), for all $A, B, C \in L$.

Examples of Lie algebras that are subalgebras of $\mathcal{L}(V)$ include

$$\mathrm{Skew}(V) = \{T \in \mathcal{L}(V) : T^* = -T\}, \tag{8.2.54}$$

where $V$ is a real or complex inner product space (cf. Exercise 8 of §3.3). Further examples include

$$\{T \in \mathcal{L}(V) : \mathrm{Tr}\, T = 0\}, \tag{8.2.55}$$

when $V$ is a finite dimensional vector space over $\mathbb{F}$,

$$\{T \in \mathcal{L}(\mathbb{F}^n) : T \text{ is upper triangular}\}, \tag{8.2.56}$$

and

$$\{T \in \mathcal{L}(\mathbb{F}^n) : T \text{ is strictly upper triangular}\}. \tag{8.2.57}$$

A variant of $\mathcal{L}(V)$ with a natural Lie algebra structure is $M(n, \mathcal{A})$, where $\mathcal{A}$ is a commutative, associative algebra that is a finite dimensional vector space over $\mathbb{F}$.

It follows from Exercises 5–9 of §3.4 that $\mathbb{R}^3$, with the cross product, is a Lie algebra, isomorphic to $\mathrm{Skew}(\mathbb{R}^3)$.

There are a number of important Lie algebras of differential operators that arise naturally. We mention one here, namely the 3-dimensional space of operators on $C^\infty(\mathbb{R})$ spanned by $X_1, X_2$, and $X_3$, where

$$X_1 f(x) = f'(x), \quad X_2 f(x) = x f(x), \quad X_3 f(x) = f(x). \tag{8.2.58}$$

By the Leibniz identity,

$$[X_1, X_2] = X_3, \tag{8.2.59}$$

and, obviously,

$$[X_j, X_3] = 0. \tag{8.2.60}$$

This Lie algebra is isomorphic to the Lie algebra of strictly upper triangular $3 \times 3$ real matrices, spanned by

$$Y_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad Y_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad Y_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \tag{8.2.61}$$

Parallel to (8.2.59)–(8.2.60), we have

$$[Y_1, Y_2] = Y_3, \quad [Y_j, Y_3] = 0. \tag{8.2.62}$$

A result known as Ado's theorem says that every finite dimensional Lie algebra is isomorphic to a Lie algebra of matrices. A proof can be found in [**17**].

The study of Lie algebras goes hand in hand with the study of Lie groups. More thorough introductions to this important area can be found in [**17**] and in [**25**].

### Jordan algebras

The paradigms for Jordan algebras are the spaces

$$\mathrm{Herm}(n, \mathbb{F}) = \{(a_{jk}) \in M(n, \mathbb{F}) : a_{kj} = \overline{a}_{jk}\}, \tag{8.2.63}$$

for $n \geq 2$, with $\mathbb{F} = \mathbb{R}, \mathbb{C}$, or $\mathbb{H}$, endowed with the product

$$A \circ B = \frac{1}{2}(AB + BA), \tag{8.2.64}$$

an $\mathbb{R}$-bilinear map $\mathrm{Herm}(n, \mathbb{F}) \times \mathrm{Herm}(n, \mathbb{F}) \to \mathrm{Herm}(n, \mathbb{F})$. Note that the product is commutative ($A \circ B = B \circ A$), but it is not associative. There is, however, the following vestige of associativity:

$$A \circ (B \circ A^2) = (A \circ B) \circ A^2. \tag{8.2.65}$$

An algebra over $\mathbb{R}$, i.e., a finite dimensional real vector space $V$ with product given as a bilinear map $V \times V \to V$, that is commutative and satisfies (8.2.65) is called a Jordan algebra. Another example of a Jordan algebra is

$$\mathrm{Herm}(3, \mathbb{O}), \tag{8.2.66}$$

where $\mathbb{O}$ is the space of octonions, introduced in §8.4, again with the product (8.2.64), where the right side makes use of the product on $\mathbb{O}$. We refer to [**15**] and [**21**] for further material on Jordan algebras, whose introduction was stimulated by developments in quantum mechanics.

## 8.3. Clifford algebras

Let $V$ be a finite dimensional, real vector space and $Q : V \times V \to \mathbb{R}$ a symmetric bilinear form. The Clifford algebra $\mathcal{C}\ell(V,Q)$ is an associative algebra, with unit 1, generated by $V$, and satisfying the anticommutation relations

$$uv + vu = -2Q(u,v) \cdot 1, \quad \forall\, u,v \in V. \tag{8.3.1}$$

Formally, we construct $\mathcal{C}\ell(V,Q)$ as

$$\mathcal{C}\ell(V,Q) = \otimes^* V/\mathcal{I}, \tag{8.3.2}$$

where $\otimes^* V$ is the tensor algebra:

$$\otimes^* V = \mathbb{R} \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots, \tag{8.3.3}$$

and

$$\begin{aligned} \mathcal{I} &= \text{two-sided ideal generated by} \\ &\quad \{u \otimes v + v \otimes u + 2Q(u,v)1 : u,v \in V\} \\ &= \text{two-sided ideal generated by} \\ &\quad \{e_j \otimes e_k + e_k \otimes e_j + 2Q(e_j,e_k)1\}, \end{aligned} \tag{8.3.4}$$

where $\{e_j\}$ is a basis of $V$. Note that

$$Q = 0 \Longrightarrow \mathcal{C}\ell(V,Q) \approx \Lambda^* V \quad \text{(the exterior algebra).} \tag{8.3.5}$$

Here is a fundamental property of $\mathcal{C}\ell(V,Q)$.

**Proposition 8.3.1.** *Let $\mathcal{A}$ be an associative algebra with unit, and let*

$$M : V \longrightarrow \mathcal{A} \tag{8.3.6}$$

*be a linear map satisfying*

$$M(u)M(v) + M(v)M(u) = -2Q(u,v)1, \tag{8.3.7}$$

*for each $u,v \in V$ (or equivalently for all $u = e_j,\ v = e_k$, where $\{e_j\}$ is a basis of $V$). Then $M$ extends to a homomorphism*

$$M : \mathcal{C}\ell(V,Q) \longrightarrow \mathcal{A}, \quad M(1) = 1. \tag{8.3.8}$$

**Proof.** Given (8.3.6), there is a homomorphism $\widetilde{M} : \otimes^* V \to \mathcal{A}$ extending $M$, with $\widetilde{M}(1) = 1$. The relation (8.3.7) implies $\widetilde{M} = 0$ on $\mathcal{I}$, so it descends to $\otimes^* V/\mathcal{I} \to \mathcal{A}$, giving (8.3.8). $\square$

From here on we require $Q$ to be nondegenerate. Thus each Clifford algebra $\mathcal{C}\ell(V,Q)$ we consider will be isomorphic to one of the following. Take $V = \mathbb{R}^n$, with standard basis $\{e_1,\dots,e_n\}$, take $p,q \ge 0$ such that $p+q = n$, and take $Q(u,v) = \sum_{j \le p} u_j v_j - \sum_{j>p} u_j v_j$, where $u = \sum u_j e_j$ and $v = \sum v_j e_j$. In such a case, $\mathcal{C}\ell(V,Q)$ is denoted $\mathcal{C}\ell(p,q)$.

We also define the complexification of $\mathcal{C}\ell(V,Q)$:

$$\mathbb{C}\ell(V,Q) = \mathbb{C} \otimes \mathcal{C}\ell(V,Q). \tag{8.3.9}$$

(We tensor over $\mathbb{R}$.) Note that taking $e_j \mapsto ie_j$ for $p+1 \le j \le n$ gives, whenever $p+q=n$,

$$\mathbb{C}\ell(p,q) \approx \mathbb{C}\ell(n,0), \quad \text{which we denote } \ \mathbb{C}\ell(n). \tag{8.3.10}$$

Use of the anticommutator relations (8.3.1) show that if $\{e_1,\dots,e_n\}$ is a basis of $V$, then each element $u \in \mathcal{C}\ell(V,Q)$ can be written in the form

$$u = \sum_{i_\nu = 0 \text{ or } 1} a_{i_1\cdots i_n} e_1^{i_1} \cdots e_n^{i_n}, \tag{8.3.11}$$

or, equivalently, in the form

$$u = \sum_{k=0}^{n} \sum_{j_1<\cdots<j_k} \tilde{a}_{j_1\cdots j_k} e_{j_1} \cdots e_{j_k}. \tag{8.3.12}$$

(By convention the $k=0$ summand in (8.3.12) is $\tilde{a}_\emptyset \cdot 1$.) In other words, we see that

$$\{e_{j_1} \cdots e_{j_k} : 0 \le k \le n, \ j_1 < \cdots < j_k\} \tag{8.3.13}$$

spans $\mathcal{C}\ell(V,Q)$. Again, by convention, the subset of (8.3.13) for which $k=0$ is $\{1\}$. It is very useful to know that the following is true.

**Proposition 8.3.2.** *The set* (8.3.13) *is a basis of* $\mathcal{C}\ell(V,Q)$.

This is true for all $Q$, but we will restrict attention to nondegenerate $Q$. Since we know that (8.3.13) spans, the assertion is that the dimension of $\mathcal{C}\ell(p,q)$ is $2^n$ when $p+q=n$. By (8.3.10), it suffices to show this for $\mathcal{C}\ell(n,0)$, and we can assume $\{e_1,\dots,e_n\}$ is the standard orthonormal basis of $\mathbb{R}^n$ Note that the assertion for $Q=0$ corresponding to Proposition 8.3.2 is that

$$\{e_{j_1} \wedge \cdots \wedge e_{j_k} : 0 \le k \le n, j_1 < \cdots < j_k\} \ \text{ is a basis of } \ \Lambda^*\mathbb{R}^n, \tag{8.3.14}$$

where $\{e_1,\dots,e_n\}$ is the standard basis of $\mathbb{R}^n$. We will use this in our proof of Proposition 8.3.2. See §5.3 for a proof of (8.3.14).

Given that (8.3.14) is true, we can define a linear map

$$\alpha : \Lambda^*\mathbb{R}^n \longrightarrow \mathcal{C}\ell(n,0) \tag{8.3.15}$$

by $\alpha(1) = 1$ and

$$\alpha(e_{j_1} \wedge \cdots \wedge e_{j_k}) = e_{j_1} \cdots e_{j_k}, \tag{8.3.16}$$

when $1 \le j_1 < \cdots < j_k \le n$. The content of Proposition 8.3.2 is that $\alpha$ is a linear isomorphism. On the way to proving this, we construct a representation of $\mathcal{C}\ell(n,0)$ on $\Lambda^*\mathbb{R}^n$, of interest in its own right.

To construct this representation, i.e., homomorphism of algebras

$$M : \mathcal{C}\ell(n,0) \longrightarrow \mathcal{L}(\Lambda^*\mathbb{R}^n), \tag{8.3.17}$$

we begin with a linear map

$$M : \mathbb{R}^n \longrightarrow \mathcal{L}(\Lambda^*\mathbb{R}^n), \tag{8.3.18}$$

defined on the basis $\{e_1, \dots, e_n\}$ as follows. Define

$$\wedge_j : \Lambda^k\mathbb{R}^n \longrightarrow \Lambda^{k+1}\mathbb{R}^n, \quad \iota_j : \Lambda^k\mathbb{R}^n \longrightarrow \Lambda^{k-1}\mathbb{R}^n \tag{8.3.19}$$

by

$$\wedge_j(e_{j_1} \wedge \cdots \wedge e_{j_k}) = e_j \wedge e_{j_1} \wedge \cdots \wedge e_{j_k}, \tag{8.3.20}$$

and

$$\begin{aligned} &\iota_j(e_{j_1} \wedge \cdots \wedge e_{j_k}) \\ &= (-1)^{\ell-1} e_{j_1} \wedge \cdots \wedge \widehat{e_{j_\ell}} \wedge \cdots \wedge e_{j_k} \quad \text{if } j = j_\ell, \\ &\qquad\qquad 0 \qquad\qquad\qquad\qquad \text{if } j \notin \{j_1, \dots, j_k\}. \end{aligned} \tag{8.3.21}$$

Here the symbol $\widehat{e_{j_\ell}}$ signifies that $e_{j_\ell}$ is removed from the product.

Remark. If $\Lambda^*\mathbb{R}^n$ has the inner product such that (8.3.14) is an orthonormal basis, then $\iota_j$ is the adjoint of $\wedge_j$.

A calculation (cf. (5.3.52)–(5.3.53)) gives the following anticommutator relations for these operators:

$$\begin{aligned} \wedge_j \wedge_k + \wedge_k \wedge_j &= 0, \\ \iota_j \iota_k + \iota_k \iota_j &= 0, \\ \wedge_j \iota_k + \iota_k \wedge_j &= \delta_{jk}. \end{aligned} \tag{8.3.22}$$

Now we define $M$ in (8.3.18) by

$$M(e_j) = M_j = \wedge_j - \iota_j. \tag{8.3.23}$$

From (8.3.22) we get

$$M_j M_k + M_k M_j = -2\delta_{jk}. \tag{8.3.24}$$

Hence Proposition 8.3.1 applies to give the homomorphism of algebras (8.3.17), with $M(1) = I$, the identity operator.

We can now prove Proposition 8.3.2. We define a linear map

$$\beta : \mathcal{C}\ell(n,0) \longrightarrow \Lambda^*\mathbb{R}^n, \quad \beta(u) = M(u)1. \tag{8.3.25}$$

Recalling the map $\alpha$ from (8.3.15)–(8.3.16), we have

$$\begin{aligned} \beta \circ \alpha(e_{j_1} \wedge \cdots \wedge e_{j_k}) &= M(e_{j_1} \cdots e_{j_k})1 \\ &= M(e_{j_1}) \cdots M(e_{j_k})1. \end{aligned} \tag{8.3.26}$$

Now $M(e_{j_k})1 = e_{j_k}$, $M(e_{j_{k-1}})e_{j_k} = e_{j_{k-1}} \wedge e_{j_k}$ if $j_{k-1} < j_k$, and inductively we see that

$$j_1 < \cdots < j_k \Longrightarrow M(e_{j_1}) \cdots M(e_{j_k})1 = e_{j_1} \wedge \cdots \wedge e_{j_k}. \tag{8.3.27}$$

It follows that $\alpha$ and $\beta$ are inverses, and that each is a linear isomorphism. This proves Proposition 8.3.2 (granted (8.3.14)).

We next characterize $\mathcal{C}\ell(p,q)$ for small $p$ and $q$. For starters, $\mathcal{C}\ell(1,0)$ and $\mathcal{C}\ell(0,1)$ are linear spaces of the form

$$\{a + be_1 : a, b \in \mathbb{R}\}. \tag{8.3.28}$$

In $\mathcal{C}\ell(1,0)$, $e_1^2 = -1$, so

$$\mathcal{C}\ell(1,0) \approx \mathbb{C}, \quad e_1 \leftrightarrow i. \tag{8.3.29}$$

Meanwhile, in $\mathcal{C}\ell(0,1)$, $e_1^2 = 1$, so $\mathcal{C}\ell(0,1)$ is of the form

$$\begin{gathered} \{\alpha f_+ + \beta f_- : \alpha, \beta \in \mathbb{R}\} \\ f_\pm = \frac{1 \pm e_1}{2} \Rightarrow f_\pm^2 = f_\pm,\ f_+ f_- = f_- f_+ = 0, \end{gathered} \tag{8.3.30}$$

and we have

$$\mathcal{C}\ell(0,1) \approx \mathbb{R} \oplus \mathbb{R} \approx C_{\mathbb{R}}(\{+,-\}), \tag{8.3.31}$$

the space of real valued functions on the two-point set $\{+,-\}$.

Next, $\mathcal{C}\ell(2,0), \mathcal{C}\ell(1,1)$, and $\mathcal{C}\ell(0,2)$ are linear spaces of the form

$$\{a + be_1 + ce_2 + de_1e_2 : a, b, c, d \in \mathbb{R}\}. \tag{8.3.32}$$

In $\mathcal{C}\ell(2,0)$, $e_1^2 = e_2^2 = (e_1e_2)^2 = -1$, and also $e_2(e_1e_2) = e_1$, while $(e_1e_2)e_1 = e_2$, which are the algebraic relations satisfied by $i, j, k$ in the algebra $\mathbb{H}$ of quaternions, defined in §8.1. Hence

$$\mathcal{C}\ell(2,0) \approx \mathbb{H} = \{a + bi + cj + dk\}. \tag{8.3.33}$$

In $\mathcal{C}\ell(0,2)$, $e_1^2 = e_2^2 = 1$, while $(e_1e_2)^2 = -1$. Meanwhile $e_2(e_1e_2) = -e_1$ and $(e_1e_2)e_1 = -e_2$, and we have

$$\begin{aligned} &\mathcal{C}\ell(0,2) \approx \mathrm{M}(2,\mathbb{R}) \\ &= \left\{ aI + b\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + c\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + d\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}. \end{aligned} \tag{8.3.34}$$

It turns out that also

$$\mathcal{C}\ell(1,1) \approx M(2,\mathbb{R}). \tag{8.3.35}$$

We leave this to the reader.

Using (8.3.31) and (8.3.34), we find the complexified algebras

$$\mathbb{C}\ell(1) \approx \mathbb{C} \oplus \mathbb{C}, \quad \mathbb{C}\ell(2) \approx \mathrm{M}(2,\mathbb{C}). \tag{8.3.36}$$

These results are special cases of the following:

**Proposition 8.3.3.** *The complex Clifford algebras* $\mathbb{C}\ell(n)$ *have the properties*

$$\begin{aligned}\mathbb{C}\ell(2k) &\approx \mathrm{M}(2^k, \mathbb{C}),\\ \mathbb{C}\ell(2k+1) &\approx \mathrm{M}(2^k, \mathbb{C}) \oplus \mathrm{M}(2^k, \mathbb{C}).\end{aligned} \tag{8.3.37}$$

Proposition 8.3.3 follows inductively from (8.3.36) and the following result.

**Proposition 8.3.4.** *For* $n \in \mathbb{N}$, *we have isomorphisms of algebras*

$$\mathbb{C}\ell(n+2) \approx \mathbb{C}\ell(n) \otimes \mathbb{C}\ell(2). \tag{8.3.38}$$

In turn, Proposition 8.3.4 follows from:

**Proposition 8.3.5.** *For* $n \in \mathbb{N}$, *we have isomorphisms of algebras*

$$\mathcal{C}\ell(n,0) \otimes \mathcal{C}\ell(0,2) \approx \mathcal{C}\ell(0,n+2). \tag{8.3.39}$$

It remains to prove (8.3.39). To do this, we construct a homomorphism of algebras

$$M : \mathcal{C}\ell(0,n+2) \longrightarrow \mathcal{C}\ell(n,0) \otimes \mathcal{C}\ell(0,2). \tag{8.3.40}$$

Once it is checked that $M$ is onto, a dimension count guarantees it is an isomorphism.

To produce (8.3.40), we start with a linear map

$$M : \mathbb{R}^{n+2} \longrightarrow \mathcal{C}\ell(n,0) \otimes \mathcal{C}\ell(0,2), \tag{8.3.41}$$

defined by

$$\begin{aligned}Me_j &= M_j = e_j \otimes e_{n+1}e_{n+2}, \quad 1 \le j \le n,\\ Me_j &= M_j = 1 \otimes e_j, \qquad j = n+1, n+2.\end{aligned} \tag{8.3.42}$$

Here we take $\{e_1, \dots, e_n\}$ to generate $\mathcal{C}\ell(n,0)$ and $\{e_{n+1}, e_{n+2}\}$ to generate $\mathcal{C}\ell(0,2)$. To extend $M$ in (8.3.41) to (8.3.40), we need to establish the anticommutation relations

$$M_jM_k + M_kM_j = 2\delta_{jk}, \quad 1 \le j,k \le n+2. \tag{8.3.43}$$

To get this for $1 \le j,k \le n$, we use the computations

$$\begin{aligned}&(e_{n+1}e_{n+2})^2 = -e_{n+1}^2 e_{n+2}^2 = -1,\\ &(e_j \otimes e_{n+1}e_{n+2})(e_k \otimes e_{n+1}e_{n+2})\\ &\quad = e_je_k \otimes (e_{n+1}e_{n+2})^2 = -e_je_k \otimes 1,\end{aligned} \tag{8.3.44}$$

which yield

$$\begin{aligned}1 \le j,k \le n \Rightarrow M_jM_k + M_kM_j &= -(e_je_k \otimes 1 + e_ke_j \otimes 1)\\ &= 2\delta_{jk},\end{aligned} \tag{8.3.45}$$

as desired. Next we have

$$
\begin{aligned}
&1 \le j \le n \Longrightarrow \\
&M_j M_{n+1} + M_{n+1} M_j \\
&= (e_j \otimes e_{n+1}e_{n+2})(1 \otimes e_{n+1}) + (1 \otimes e_{n+1})(e_j \otimes e_{n+1}e_{n+2}) \\
&= e_j \otimes e_{n+1}e_{n+2}e_{n+1} + e_j \otimes e_{n+1}e_{n+1}e_{n+2} \\
&= 0,
\end{aligned}
\tag{8.3.46}
$$

since $e_{n+1}e_{n+2} = -e_{n+2}e_{n+1}$. Similarly one gets $M_j M_{n+2} + M_{n+2} M_j = 0$ for $1 \le j \le n$. Next,

$$
M_{n+1}M_{n+1} = (1 \otimes e_{n+1})(1 \otimes e_{n+1}) = 1 \otimes e_{n+1}^2 = 1, \tag{8.3.47}
$$

and similarly $M_{n+2}M_{n+2} = 1$. Finally,

$$
\begin{aligned}
&M_{n+1}M_{n+2} + M_{n+2}M_{n+1} \\
&= (1 \otimes e_{n+1})(1 \otimes e_{n+2}) + (1 \otimes e_{n+2})(1 \otimes e_{n+1}) \\
&= 1 \otimes (e_{n+1}e_{n+2} + e_{n+2}e_{n+1}) \\
&= 0.
\end{aligned}
\tag{8.3.48}
$$

This establishes (8.3.43). Hence, by Proposition 8.3.1, $M$ extends to the algebra homomorphism (8.3.40) (with $M1 = I$). It is routine to verify that the elements on the right side of (8.3.42) generate $\mathcal{C}\ell(n,0) \otimes \mathcal{C}\ell(0,2)$, so $M$ in (8.3.40) is onto, hence an isomorphism. This completes the proof of Proposition 8.3.5, hence Propositions 8.3.3–8.3.4.

Remark. The following companions to (8.3.39),

$$
\begin{aligned}
\mathcal{C}\ell(0,n) \otimes \mathcal{C}\ell(2,0) &\approx \mathcal{C}\ell(n+2,0), \\
\mathcal{C}\ell(p,q) \otimes \mathcal{C}\ell(1,1) &\approx \mathcal{C}\ell(p+1,q+1),
\end{aligned}
\tag{8.3.49}
$$

have essentially the same proof. From (8.3.39) and (8.3.49) it follows that

$$
\mathcal{C}\ell(n+8,0) \approx \mathcal{C}\ell(n,0) \otimes \mathcal{C}\ell(0,2) \otimes \mathcal{C}\ell(2,0) \otimes \mathcal{C}\ell(0,2) \otimes \mathcal{C}\ell(2,0). \tag{8.3.50}
$$

Meanwhile, by (8.3.33)–(8.3.34),

$$
\mathcal{C}\ell(0,2) \otimes \mathcal{C}\ell(2,0) \approx \mathrm{M}(2,\mathbb{R}) \otimes \mathbb{H}. \tag{8.3.51}
$$

This, together with the isomorphism (cf. Proposition 8.2.2)

$$
\mathbb{H} \otimes \mathbb{H} \approx \mathrm{M}(4,\mathbb{R}), \tag{8.3.52}
$$

leads to

$$
\mathcal{C}\ell(n+8,0) \approx \mathcal{C}\ell(n,0) \otimes \mathrm{M}(16,\mathbb{R}). \tag{8.3.53}
$$

See [**13**] for more details.

**Dirac operators**

A major motivation for studying Clifford algebras arises from the connection with a class of first order differential operators known as *Dirac operators*, which we describe here.

Let $V$ be a real or complex vector space. We define an operator $\mathcal{D}$ on smooth functions on $\mathbb{R}^n$ with values in $V$ by

$$\mathcal{D}u = \sum_{j=1}^{n} \gamma_j \, \partial_j u, \quad \partial_j u = \frac{\partial u}{\partial x_j}, \tag{8.3.54}$$

where $\gamma_j \in \mathcal{L}(V)$ are assumed to satisfy the anticommutation relations

$$\gamma_j \gamma_k + \gamma_k \gamma_j = -2\eta_{jk} I, \tag{8.3.55}$$

where

$$\begin{aligned} \eta_{jk} = \ & 0 \quad \text{if } \ j \neq k, \\ & 1 \quad \text{if } \ j = k \in \{1, \dots, p\}, \\ & -1 \ \text{if } \ j = k \in \{p+1, \dots, n\}. \end{aligned} \tag{8.3.56}$$

Here we pick $p \in \{0, \dots, n\}$, so $(\eta_{jk})$ provides an inner product on $\mathbb{R}^n$ of signature $(p, q)$, $p = n - p$. By Proposition 8.3.1, there is a homomorphism of algebras

$$\gamma : \mathcal{C}\ell(p, q) \longrightarrow \mathcal{L}(V) \tag{8.3.57}$$

such that, if $\{e_1, \dots, e_n\}$ is the standard basis of $\mathbb{R}^n$,

$$\gamma(e_j) = \gamma_j. \tag{8.3.58}$$

The operator $\mathcal{D}$ has the following important property:

$$\begin{aligned} \mathcal{D}^2 u &= \sum_{j,k=1}^{n} \gamma_j \gamma_k \partial_j \partial_k u \\ &= \frac{1}{2} \sum_{j,k=1}^{n} (\gamma_j \gamma_k + \gamma_k \gamma_j) \partial_j \partial_k u \\ &= -\sum_{j,k=1}^{n} \eta_{jk} \, \partial_j \partial_k u \\ &= -\sum_{j=1}^{p} \partial_j^2 u + \sum_{j=p+1}^{n} \partial_j^2 u. \end{aligned} \tag{8.3.59}$$

In particular,

$$(8.3.60)\qquad \begin{aligned} (p,q)=(n,0) &\Longrightarrow \mathcal{D}^2u=-\sum_{j=1}^n \partial_j^2 u=-\Delta u,\\ (p,q)=(0,n) &\Longrightarrow \mathcal{D}^2u=\sum_{j=1}^n \partial_j^2 u=\Delta u, \end{aligned}$$

where $\Delta$ is the Laplace operator, acting (componentwise) on $V$-valued functions on $\mathbb{R}^n$,

$$(8.3.61)\qquad \Delta u=\sum_{j=1}^n \partial_j^2 u.$$

A canonical example of such a Dirac operator arises when

$$(8.3.62)\qquad V=\mathcal{C}\ell(p,q),\quad 0\le p,q\le n,\ p+q=n,$$

with $\gamma_j\in\mathcal{L}(V)$ defined by Clifford multiplication, $\gamma_j(v)=e_jv$, where $\{e_j\}$ is the standard basis of $\mathbb{R}^n$, $v\in\mathcal{C}\ell(p,q)$ (alternatively, $V=\mathbb{C}\ell(n)$). Such an operator $\mathcal{D}$ is called the Clifford Dirac operator, of signature $(p,q)$. In such a case, one has (H.53) where $\gamma_j$ can be taken to be $N\times N$ matrices, where, by Proposition 8.3.2,

$$(8.3.63)\qquad N=\dim \mathbb{C}\ell(n)=2^n,$$

for example,

$$(8.3.64)\qquad n=3\Longrightarrow N=8,\quad n=4\Longrightarrow N=16.$$

However, there are other vector spaces $V$, of lower dimension, for which there are Dirac operators. In particular, by Proposition 8.3.3, one can have Dirac operators acting on functions with values in $\mathbb{C}^M$, where

$$(8.3.65)\qquad M=2^k,\quad \text{if}\ \ n=2k\ \ \text{or}\ \ 2k+1.$$

For example,

$$(8.3.66)\qquad n=3\Longrightarrow M=2,\quad n=4\Longrightarrow M=4.$$

We now give an explicit inductive construction of $M\times M$ matrices $\gamma_1,\dots,\gamma_n$, satisfying anticommutation relations of the form (8.3.55), starting with the trivial case $n=1$ (so $M=1$):

$$(8.3.67)\qquad \alpha_1=1.$$

Here $\alpha_1^2=1$; we could multiply by $i$ to get $\alpha_1^2=-1$. Generally, suppose you have $M\times M$ matrices $\alpha_1,\dots,\alpha_n$, satisfying (8.3.55). We form the following $(2M)\times(2M)$ matrices:

$$(8.3.68)\qquad \beta_j=\begin{pmatrix} & -\alpha_j\\ \alpha_j & \end{pmatrix},\quad 1\le j\le n,\quad \beta_{n+1}=\begin{pmatrix} & I\\ I & \end{pmatrix}.$$

For $1 \le j, k \le n$, we have

$$\beta_j \beta_k = \begin{pmatrix} -\alpha_j \alpha_k & \\ & -\alpha_j \alpha_k \end{pmatrix}, \tag{8.3.69}$$

so

$$\beta_j \beta_k + \beta_k \beta_j = -\begin{pmatrix} \alpha_j \alpha_k + \alpha_k \alpha_j & \\ & \alpha_j \alpha_k + \alpha_k \alpha_j \end{pmatrix} = 2\eta_{jk} I. \tag{8.3.70}$$

Meanwhile, for $1 \le j \le n$,

$$\beta_j \beta_{n+1} = \begin{pmatrix} -\alpha_j & \\ & \alpha_j \end{pmatrix} = -\beta_{n+1} \beta_j, \tag{8.3.71}$$

and, of course,

$$\beta_{n+1}^2 = I. \tag{8.3.72}$$

We call this construction Method I.

Applying this to (8.3.67) gives

$$\beta_1 = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}, \quad \beta_2 = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \tag{8.3.73}$$

so (8.3.55) holds with $\eta_{11} = 1,\ \eta_{22} = -1$. Multiplying one or both $\beta_j$ by $i$ gives other signatures.

We could iterate Method I, producing a triple of $4 \times 4$ matrices. However, according to (8.3.66), we want to look for a triple of $2 \times 2$ matrices.

Again we produce a general construction, which we call Method II. Assume that $n + 1$ is *even*, and you have matrices $\beta_j,\ 1 \le j \le n + 1$, of the form (8.3.68), with the same anticommutation relations as $\mathcal{C}\ell(p, q)$, with $p + q = n + 1$. Now set

$$\begin{aligned} \beta_{n+2} &= \beta_1 \beta_2 \cdots \beta_{n+1} \\ &= (-1)^{(n-1)/2} \begin{pmatrix} -\alpha_1 \cdots \alpha_n & \\ & \alpha_1 \cdots \alpha_n \end{pmatrix}. \end{aligned} \tag{8.3.74}$$

We have

$$\beta_{n+2}^2 = \begin{pmatrix} (\alpha_1 \cdots \alpha_n)^2 & \\ & (\alpha_1 \cdots \alpha_n)^2 \end{pmatrix} = \pm I, \tag{8.3.75}$$

and

$$\beta_j \beta_{n+2} = -\beta_{n+2} \beta_j, \quad \text{for} \ \ 1 \le j \le n + 1. \tag{8.3.76}$$

To see (8.3.76), note that pushing $\beta_j$ from the far left, in $\beta_j \beta_1 \cdots \beta_{n+1}$, to the far right, in $\beta_1 \cdots \beta_{n+1} \beta_j$, produces $n$ sign changes, and in the current setting $n$ is odd.

Applying Method II (with $n+1=2$) to (8.3.73) yields

$$\beta_1 = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}, \quad \beta_2 = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \quad \beta_3 = \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}, \tag{8.3.77}$$

which have the same anticommutation relations as $\mathcal{C}\ell(1,2)$. Multiplying $\beta_1$ by $i$ and $\beta_3$ by $-1$ and reordering, we have the *Pauli matrices*,

$$\sigma_1 = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} & i \\ -i & \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}, \tag{8.3.78}$$

which have the same anticommutation relations as $\mathcal{C}\ell(0,3)$.

We now apply Method I to the Pauli matrices (8.3.78), yielding the following $4 \times 4$ matrices

$$\gamma_j = \begin{pmatrix} & -\sigma_j \\ \sigma_j & \end{pmatrix}, \quad 1 \le j \le 3, \quad \gamma_4 = \begin{pmatrix} & I \\ I & \end{pmatrix}. \tag{8.3.79}$$

These are called the *Dirac matrices.* They have the same anticommutation relations as $\mathcal{C}\ell(3,1)$. The associated Dirac operator $\mathcal{D}$ satisfies

$$\mathcal{D}^2 = \frac{\partial^2}{\partial t^2} - \Delta, \quad t = x_4, \quad \Delta = \partial_1^2 + \partial_2^2 + \partial_3^2. \tag{8.3.80}$$

Solving the initial value problem

$$\mathcal{D}u = 0, \quad u(x,0) = f(x), \tag{8.3.81}$$

is equivalent to solving

$$\frac{\partial^2 u}{\partial t^2} - \Delta u = 0, \quad u(x,0) = f(x), \ \partial_t u(x,0) = g(x), \tag{8.3.82}$$

where

$$g(x) = -\gamma_4^{-1} \sum_{j=1}^{3} \gamma_j \partial_j f(x). \tag{8.3.83}$$

Of course, $\gamma_4^{-1} = \gamma_4$, and, for $1 \le j \le 3$,

$$-\gamma_4^{-1}\gamma_j = \begin{pmatrix} -\sigma_j & \\ & \sigma_j \end{pmatrix}. \tag{8.3.84}$$

Methods of solving the "wave equation" (8.3.82) can be found in Chapter 3 of [**26**].

From here, we can obtain a 5-tuple of $4\times4$ matrices, via Method II, which have the same anticommutator relations as $\mathcal{C}\ell(p,q)$, with $p+q=5$. We then alternate the use of Method I and Method II to produce higher dimensional Clifford algebras of matrices, yielding Dirac operators on smooth vector-valued functions on $\mathbb{R}^n$, for larger $n$.

## Exercises

1. Given a Clifford algebra $\mathcal{C}\ell(V,Q)$ $(\dim V < \infty)$, and $u \in \mathcal{C}\ell(V,Q)$, show that the power series

$$e^{tu} = \sum_{k=0}^{\infty} \frac{t^k}{k!} u^k$$

converges for all $t \in \mathbb{R}$, defining $e^{tu}$ as a smooth function of $t$ with values in $\mathcal{C}\ell(V,Q)$ satisfying

$$\frac{d}{dt} e^{tu} = u e^{tu}.$$

2. In the setting of Exercise 1, assume $V$ is an inner product space and $Q(u,u) = |u|^2$. Show that

$$u \in V \Longrightarrow e^{tu} = \bigl(\cos t|u|\bigr) + \frac{\sin t|u|}{|u|} u.$$

*Hint.* Set $Y(t) = e^{tu}$ and show that

$$Y''(t) = -|u|^2 Y(t), \quad Y(0) = 1,\ Y'(0) = u.$$

Compare this result with Exercise 8 of §8.1.

3. Let $\sigma_j$ denote the Pauli matrices:

$$\sigma_1 = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} & i \\ -i & \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}.$$

Show that $\{i\sigma_1, i\sigma_2, i\sigma_3\}$ have the same anticommutation relations as $\mathcal{C}\ell(3,0)$. Using this and Exercise 2, compute

$$e^{it(a_1\sigma_1 + a_2\sigma_2 + a_3\sigma_3)}, \quad a_j \in \mathbb{R}.$$

## 8.4. Octonions

The set of octonions (also known as Cayley numbers) is a special but intriguing example of a nonassociative algebra. This space is

$$\mathbb{O} = \mathbb{H} \oplus \mathbb{H}, \tag{8.4.1}$$

with product given by

$$(\alpha, \beta) \cdot (\gamma, \delta) = (\alpha\gamma - \overline{\delta}\beta, \delta\alpha + \beta\overline{\gamma}), \quad \alpha, \beta, \gamma, \delta \in \mathbb{H}, \tag{8.4.2}$$

with conjugation $\delta \mapsto \overline{\delta}$ on $\mathbb{H}$ defined as in §8.1. We mention that, with $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}$, the product in $\mathbb{H}$ is also given by (8.4.2), with $\alpha, \beta, \gamma, \delta \in \mathbb{C}$. Furthermore, with $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}$, the product in $\mathbb{C}$ is given by (8.4.2), with $\alpha, \beta, \gamma, \delta \in \mathbb{R}$. In the setting of $\mathbb{O} = \mathbb{H} \oplus \mathbb{H}$, the product in (8.4.2) is clearly $\mathbb{R}$-bilinear, but it is neither commutative nor associative. However, it does retain a vestige of associativity, namely

$$x(yz) = (xy)z \quad \text{whenever any two of } x, y, z \in \mathbb{O} \text{ coincide.} \tag{8.4.3}$$

We define a conjugation on $\mathbb{O}$:

$$x = (\alpha, \beta) \Longrightarrow \overline{x} = (\overline{\alpha}, -\beta). \tag{8.4.4}$$

We set $\operatorname{Re} x = (x + \overline{x})/2 = (\operatorname{Re} \alpha, 0)$. Note that $a = \operatorname{Re} x$ lies in the center of $\mathbb{O}$ (i.e., commutes with each element of $\mathbb{O}$), and $\overline{x} = 2a - x$. It is straightforward to check that

$$x, y \in \mathbb{O} \Longrightarrow \operatorname{Re} xy = \operatorname{Re} yx. \tag{8.4.5}$$

We have a decomposition

$$x = a + u, \quad a = \operatorname{Re} x, \ u = x - \operatorname{Re} x = \operatorname{Im} x, \tag{8.4.6}$$

parallel to (8.1.4). Again we call $u$ the vector part of $x$, and we say that $u \in \operatorname{Im}(\mathbb{O})$. If also $y = b + v$, then

$$xy = ab + av + bu + uv, \tag{8.4.7}$$

with a similar formula for $yx$, yielding

$$xy - yx = uv - vu. \tag{8.4.8}$$

We now define the inner product

$$\langle x, y \rangle = \operatorname{Re}(x\overline{y}), \quad x, y \in \mathbb{O}. \tag{8.4.9}$$

To check symmetry, note that if $x = a + u, \ y = b + v$,

$$\langle x, y \rangle = ab - \operatorname{Re}(uv), \tag{8.4.10}$$

and (8.4.5) then implies

$$\langle x, y \rangle = \langle y, x \rangle. \tag{8.4.11}$$

In fact, (8.4.9) yields the standard Euclidean inner product on $\mathbb{O} \approx \mathbb{R}^8$, with square norm $|x|^2 = \sqrt{\langle x, x\rangle}$. We have

$$x = (\alpha, \beta) \Longrightarrow x\overline{x} = (\alpha\overline{\alpha} + \overline{\beta}\beta, 0) = (|x|^2, 0). \tag{8.4.12}$$

As a consequence, we see that

$$x \in \mathbb{O},\ x \neq 0,\ y = |x|^{-2}\overline{x} \Longrightarrow xy = yx = 1, \tag{8.4.13}$$

where $1 = (1, 0)$ is the multiplicative unit in $\mathbb{O}$.

Returning to conjugation on $\mathbb{O}$, we have, parallel to (8.1.19),

$$x, y \in \mathbb{O} \Longrightarrow \overline{xy} = \overline{y}\,\overline{x}, \tag{8.4.14}$$

via a calculation using the definition (8.4.2) of the product. Using the decomposition $x = a + u,\ y = b + v$, this is equivalent to $\overline{uv} = vu$, and since $\overline{uv} = 2\,\mathrm{Re}(uv) - uv = -2\langle u, v\rangle - uv$, this is equivalent to

$$u, v \in \mathrm{Im}(\mathbb{O}) \Longrightarrow uv + vu = -2\langle u, v\rangle. \tag{8.4.15}$$

In turn, (8.4.15) follows from expanding $(u+v)(u+v)$ and using $w^2 = -|w|^2$ for $w \in \mathrm{Im}(\mathbb{O})$, with $w = u, v$, and $u+v$. In light of (8.4.15), we can perceive a Clifford algebra action arising, via Proposition 8.3.1, but we will not dwell on this here. (Proposition 8.4.3 would also be needed.) We next establish the following parallel to (8.1.21).

**Proposition 8.4.1.** *Given $x, y \in \mathbb{O}$,*

$$|xy| = |x|\,|y|. \tag{8.4.16}$$

**Proof.** To begin, we bring in the following variant of (8.4.3),

$$x, y \in \mathbb{O} \Longrightarrow (xy)(yx) = ((xy)y)x, \tag{8.4.17}$$

which can be verified from the definition (8.4.2) of the product. Taking into account $\overline{x} = 2a - x,\ \overline{y} = 2b - y$, and (8.4.14), we have

$$\begin{aligned} (xy)(\overline{xy}) &= (xy)(\overline{y}\,\overline{x}) = ((xy)\overline{y})\overline{x} \\ &= (x|y|^2)\overline{x} = |x|^2|y|^2, \end{aligned} \tag{8.4.18}$$

which gives (8.4.16), since $|xy|^2 = (xy)(\overline{xy})$. $\square$

Continuing to pursue parallels with §8.1, we define a cross product on $\mathrm{Im}(\mathbb{O})$ as follows. Given $u, v \in \mathrm{Im}(\mathbb{O})$, set

$$u \times v = \frac{1}{2}(uv - vu). \tag{8.4.19}$$

By (8.4.5), this is an element of $\mathrm{Im}(\mathbb{O})$. Also, if $x = a + u, y = b + v$,

$$xy - yx = 2u \times v. \tag{8.4.20}$$

Compare (8.1.6). Putting together (8.4.15) and (8.4.19), we have

$$uv = -\langle u, v\rangle + u \times v, \quad u, v \in \mathrm{Im}(\mathbb{O}). \tag{8.4.21}$$

Hence

$$|uv|^2 = |\langle u, v\rangle|^2 + |u \times v|^2. \tag{8.4.22}$$

Now (8.4.16) implies $|uv|^2 = |u|^2|v|^2$, and of course $\langle u, v\rangle = |u|\,|v| \cos\theta$, where $\theta$ is the angle between $u$ and $v$. Hence, parallel to (8.1.26),

$$|u \times v|^2 = |u|^2|v|^2|\sin\theta|^2, \quad \forall\, u, v \in \mathrm{Im}(\mathbb{O}). \tag{8.4.23}$$

We have the following complement.

**Proposition 8.4.2.** *If* $u, v \in \mathrm{Im}(\mathbb{O})$*, then*

$$w = u \times v \Longrightarrow \langle w, u\rangle = \langle w, v\rangle = 0. \tag{8.4.24}$$

**Proof.** We know that $w \in \mathrm{Im}(\mathbb{O})$. Hence, by (8.4.21),

$$\begin{aligned} \langle w, v\rangle &= \langle uv, v\rangle = \mathrm{Re}((uv)\overline{v}) \\ &= \mathrm{Re}(u(v\overline{v})) = |v|^2 \,\mathrm{Re}\, u = 0, \end{aligned} \tag{8.4.25}$$

the third identity by (8.4.3) (applicable since $\overline{v} = -v$). The proof that $\langle w, u\rangle = 0$ is similar. □

Returning to basic observations about the product (8.4.2), we note that it is uniquely determined as the $\mathbb{R}$-bilinear map $\mathbb{O} \times \mathbb{O} \to \mathbb{O}$ satisfying

$$\begin{aligned} (\alpha, 0) \cdot (\gamma, 0) &= (\alpha\gamma, 0), \quad & (0, \beta) \cdot (\gamma, 0) &= (0, \beta\overline{\gamma}), \\ (\alpha, 0) \cdot (0, \delta) &= (0, \delta\alpha), \quad & (0, \beta) \cdot (0, \delta) &= (-\overline{\delta}\beta, 0), \end{aligned} \tag{8.4.26}$$

for $\alpha, \beta, \gamma, \delta \in \mathbb{H}$. In particular, $\mathbb{H} \oplus 0$ is a subalgebra of $\mathbb{O}$, isomorphic to $\mathbb{H}$. As we will see, $\mathbb{O}$ has lots of subalgebras isomorphic to $\mathbb{H}$. First, let us label the "standard" basis of $\mathbb{O}$ as

$$\begin{aligned} 1 &= (1, 0), \quad & e_1 &= (i, 0), \quad & e_2 &= (j, 0), \quad & e_3 &= (k, 0), \\ f_0 &= (0, 1), \quad & f_1 &= (0, i), \quad & f_2 &= (0, j), \quad & f_3 &= (0, k), \end{aligned} \tag{8.4.27}$$

and describe the associated multiplication table. The mutiplication table for $1, e_1, e_2, e_3$ is the same as (8.1.2)–(8.1.3), of course. We also have $f_\ell^2 = -1$ and all the distinct $e_\ell$ and $f_m$ anticommute. These results are special cases of the fact that

$$u, v \in \mathrm{Im}(\mathbb{O}),\ |u| = 1,\ \langle u, v\rangle = 0 \Longrightarrow u^2 = -1 \ \text{ and } \ uv = -vu, \tag{8.4.28}$$

which is a consequence of (8.4.15).

To proceed with the multiplication table for $\mathbb{O}$, note that (8.4.26) gives

$$(\alpha, 0) f_0 = (0, \alpha), \tag{8.4.29}$$

so

$$e_\ell f_0 = f_\ell, \quad 1 \le \ell \le 3. \tag{8.4.30}$$

By (8.4.28), $f_0 e_\ell = -f_\ell$. Using the notation $\varepsilon_1 = i, \varepsilon_2 = j, \varepsilon_3 = k \in \mathbb{H}$, we have

$$e_\ell f_m = (\varepsilon_\ell, 0) \cdot (0, \varepsilon_m) = (0, \varepsilon_m \varepsilon_\ell), \quad 1 \le \ell, m \le 3, \tag{8.4.31}$$

and the multiplication table (8.1.2)–(8.1.3) gives the result as $-f_0$ if $\ell = m$, and $\pm f_\mu$ if $\ell \neq m$, where $\{\ell, m, \mu\} = \{1, 2, 3\}$. Again by (I.28), $f_m e_\ell = -e_\ell f_m$. To complete the multiplication table, we have

$$f_0 f_m = (0, 1) \cdot (0, \varepsilon_m) = (\varepsilon_m, 0) = e_m, \quad 1 \le m \le 3, \tag{8.4.32}$$

and

$$f_\ell f_m = (0, \varepsilon_\ell) \cdot (0, \varepsilon_m) = (\varepsilon_m \varepsilon_\ell, 0) = e_m e_\ell, \quad 1 \le \ell, m \le 3. \tag{8.4.33}$$

The following is a succinct summary of the results described above on the multiplication table for $\mathbb{O}$. In each row listed in (8.4.34), consisting of three elements (say $u_j$), $\mathrm{Span}\{1, u_1, u_2, u_3\}$ is an algebra, isomorphic to $\mathbb{H}$ under $i \mapsto u_1, j \mapsto u_2, k \mapsto u_3$.

$$\begin{array}{ccc} i & j & k \\ e_1 & e_2 & e_3 \\ e_\ell & f_0 & f_\ell \\ f_1 & e_3 & f_2 \\ f_2 & e_1 & f_3 \\ f_3 & e_2 & f_1 \end{array} \tag{8.4.34}$$

Following [**5**], we depict in Figure 8.4.1 a diagram of this multiplication table. In each case, one has a triple recorded in (8.4.34), lying along a line (or a circle), equipped with an arrow indicating the appropriate order.

We turn to the task of constructing subalgebras of $\mathbb{O}$. To start, pick

$$u_1 \in \mathrm{Im}(\mathbb{O}), \quad \text{such that} \quad |u_1| = 1. \tag{8.4.35}$$

By (8.4.28), $u_1^2 = -1$, and we have the subalgebra of $\mathbb{O}$,

$$\mathrm{Span}\{1, u_1\} \approx \mathbb{C}. \tag{8.4.36}$$

To proceed, pick

$$u_2 \in \mathrm{Im}(\mathbb{O}), \quad \text{such that} \quad |u_2| = 1 \text{ and } \langle u_1, u_2 \rangle = 0, \tag{8.4.37}$$

and set

$$u_3 = u_1 u_2. \tag{8.4.38}$$

By (8.4.28),

$$u_2^2 = -1, \text{ and } u_2 u_1 = -u_1 u_2 = -u_3. \tag{8.4.39}$$

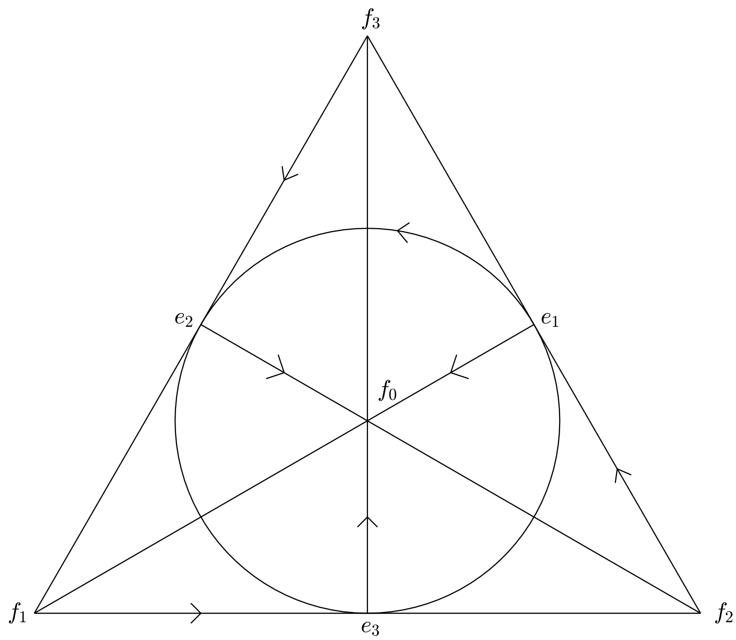


**Figure 8.4.1.** Multiplication table schematic for $\mathbb{O}$

Note that

$$\operatorname{Re} u_3 = \operatorname{Re}(u_1 u_2) = -\langle u_1, u_2 \rangle = 0. \tag{8.4.40}$$

Also, by (8.4.16), $|u_3| = 1$, so

$$1 = u_3 \overline{u}_3 = -u_3^2. \tag{8.4.41}$$

Furthermore, by (8.4.3),

$$\begin{aligned} u_1 u_3 &= u_1(u_1 u_2) = (u_1 u_1) u_2 = -u_2, \quad \text{and} \\ u_3 u_2 &= (u_1 u_2) u_2 = u_1 (u_2 u_2) = -u_1. \end{aligned} \tag{8.4.42}$$

Let us also note that

$$u_3 = u_1 \times u_2. \tag{8.4.43}$$

Hence, by Proposition 8.4.2,

$$\langle u_3, u_1 \rangle = \langle u_3, u_2 \rangle = 0, \tag{8.4.44}$$

and, again by (8.4.28), $u_3 u_1 = -u_1 u_3$ and $u_2 u_3 = -u_3 u_2$. Thus we have for each such choice of $u_1$ and $u_2$ a subalgebra of $\mathbb{O}$,

$$\operatorname{Span}\{1, u_1, u_2, u_3\} \approx \mathbb{H}. \tag{8.4.45}$$

At this point we can make the following observation.

**Proposition 8.4.3.** *Given any two elements $x_1, x_2 \in \mathbb{O}$, the algebra $\mathcal{A}$ generated by $1, x_1$, and $x_2$ is isomorphic to either $\mathbb{R}, \mathbb{C}$, or $\mathbb{H}$. In particular, it is associative.*

**Proof.** Consider $V = \operatorname{Span}\{1, x_1, x_2\}$. If $\dim V = 1$, then $\mathcal{A} \approx \mathbb{R}$. If $\dim V = 2$, the argument yielding (8.4.36) gives $\mathcal{A} \approx \mathbb{C}$. If $\dim V = 3$, then $\operatorname{Im} x_1$ and $\operatorname{Im} x_2$ are linearly independent. We can pick orthonormal elements $u_1$ and $u_2$ in their span. Then $\mathcal{A}$ is the algebra generated by $1, u_1$, and $u_2$, and the analysis (8.4.35)–(8.4.45) gives $\mathcal{A} \approx \mathbb{H}$. $\square$

The last assertion of Proposition 8.4.3 contains (8.4.3) and (8.4.17) as special cases. The failure of $\mathbb{O}$ to be associative is clearly illustrated by (8.4.31), which implies

$$e_\ell(e_m f_0) = (e_m e_\ell) f_0, \quad \text{for } \ 1 \le \ell, m \le 3, \tag{8.4.46}$$

so

$$e_\ell(e_m f_0) = -(e_\ell e_m) f_0, \quad \text{if } \ \ell \neq m. \tag{8.4.47}$$

Bringing in also (8.4.33) yields

$$f_\ell(e_m f_0) = e_m e_\ell, \quad \text{while } \ (f_\ell e_m) f_0 = e_\ell e_m. \tag{8.4.48}$$

We next explore how the subalgebra

$$\mathcal{A} = \operatorname{Span}\{1, u_1, u_2, u_3\}, \tag{8.4.49}$$

from (I.44), interacts with its orthogonal complement $\mathcal{A}^\perp$. Pick

$$v_0 \in \mathcal{A}^\perp, \quad |v_0| = 1. \tag{8.4.50}$$

Note that $v_0 \in \Im(\mathbb{O})$. Taking a cue from (8.4.30), we set

$$v_\ell = u_\ell v_0, \quad 1 \le \ell \le 3. \tag{8.4.51}$$

Note that $\Re v_\ell = -\langle u_\ell, v_0 \rangle = 0$, so $v_\ell \in \Im(\mathbb{O})$. We claim that

$$\{v_0, v_1, v_2, v_3\} \ \text{ is an orthonormal set in } \ \mathbb{O}. \tag{8.4.52}$$

To show this, we bring in the following operators. Given $x \in \mathbb{O}$, define the $\mathbb{R}$-linear maps

$$L_x, R_x : \mathbb{O} \longrightarrow \mathbb{O}, \quad L_x y = xy, \ R_x y = yx. \tag{8.4.53}$$

By (I.16), for $y \in \mathbb{O}$,

$$|x| = 1 \Longrightarrow |L_x y| = |R_x y| = |y|. \tag{8.4.54}$$

Hence $L_x$ and $R_x$ are orthogonal transformations. Since the unit sphere in $\mathbb{O}$ is connected, $\det L_x$ and $\det R_x$ are $\equiv 1$ for such $x$, so

$$|x| = 1 \Longrightarrow L_x, R_x \in SO(\mathbb{O}). \tag{8.4.55}$$

Hence $R_{v_0} \in SO(\mathbb{O})$. Since

$$v_0 = R_{v_0} 1, \quad v_\ell = R_{v_0} u_\ell \ \text{ for } \ 1 \le \ell \le 3, \tag{8.4.56}$$

we have (8.4.52). We next claim that

$$v_\ell \perp u_m, \quad \forall\, \ell, m \in \{1,2,3\}. \tag{8.4.57}$$

In fact, since $L_{u_\ell} \in SO(\mathbb{O})$,

$$\begin{aligned} \langle v_\ell, u_m \rangle &= \langle u_\ell v_0, u_m \rangle = \langle u_\ell (u_\ell v_0), u_\ell u_m \rangle \\ &= \langle (u_\ell u_\ell) v_0, u_\ell u_m \rangle = -\langle v_0, u_\ell u_m \rangle = 0, \end{aligned} \tag{8.4.58}$$

the third identity by (8.4.3).

It follows that

$$\mathcal{A}^\perp = \operatorname{Span}\{v_0, v_1, v_2, v_3\}. \tag{8.4.59}$$

Consequently

$$\{1, u_1, u_2, u_3, v_0, v_1, v_2, v_3\} \ \text{ is an orthonormal basis of } \ \mathbb{O}. \tag{8.4.60}$$

Results above imply that

$$R_{v_0} : \mathcal{A} \xrightarrow{\approx} \mathcal{A}^\perp. \tag{8.4.61}$$

Such an argument applies to any unit length $v \perp \mathcal{A}$. Consequently

$$x \in \mathcal{A},\ y \in \mathcal{A}^\perp \Longrightarrow xy \in \mathcal{A}^\perp. \tag{8.4.62}$$

Noting that if also $x \in \operatorname{Im}(\mathbb{O})$ then $xy = -yx$, we readily deduce that

$$x \in \mathcal{A},\ y \in \mathcal{A}^\perp \Longrightarrow yx \in \mathcal{A}^\perp. \tag{8.4.63}$$

Furthermore, since $|x| = 1 \Rightarrow L_x, R_x \in SO(\mathbb{O})$, we have

$$x \in \mathcal{A}^\perp \Longrightarrow L_x, R_x : \mathcal{A}^\perp \longrightarrow \mathcal{A}, \tag{8.4.64}$$

hence

$$x, y \in \mathcal{A}^\perp \Longrightarrow xy \in \mathcal{A}. \tag{8.4.65}$$

Note that for the special case

$$\mathcal{H} = \mathbb{H} \oplus 0, \quad \mathcal{H}^\perp = 0 \oplus \mathbb{H}, \tag{8.4.66}$$

the results (8.4.62)–(8.4.65) follow immediately from (8.4.26).

We have the following important result about the correspondence between the bases (8.4.27) and (8.4.60) of $\mathbb{O}$.

**Proposition 8.4.4.** *Let $u_\ell, v_\ell \in \operatorname{Im}(\mathbb{O})$ be given as in* (8.4.49)–(8.4.51). *Then the orthogonal transformation $K : \mathbb{O} \to \mathbb{O}$, defined by*

$$K1 = 1, \quad Ke_\ell = u_\ell, \quad Kf_\ell = v_\ell, \tag{8.4.67}$$

*preserves the product on $\mathbb{O}$:*

$$K(xy) = K(x)K(y), \quad \forall\, x, y \in \mathbb{O}. \tag{8.4.68}$$

*That is to say, $K$ is an automorphism of $\mathbb{O}$.*

**Proof.** What we need to show is that $\{u_1, u_2, u_3, v_0, v_1, v_2, v_3\}$ has the same multiplication table as $\{e_1, e_2, e_3, f_0, f_1, f_2, f_3\}$. That products involving only $\{u_\ell\}$ have such behavior follows from the arguments leading to (8.4.45). That $e_\ell f_0 = f_\ell$ is paralleled by $u_\ell v_0 = v_\ell$, for $1 \le \ell \le 3$, is the definition (8.4.51). It remains to show that the products $u_\ell v_m$ and $v_\ell v_m$ mirror the products $e_\ell f_m$ and $f_\ell f_m$, as given in (8.4.31)–(8.4.33).

First, we have, for $1 \le m \le 3$,

$$v_0 v_m = -v_m v_0 = -(u_m v_0) v_0 = -u_m(v_0 v_0) = u_m, \tag{8.4.69}$$

mirroring (8.4.32). Mirroring the case $\ell = m$ of (8.4.31), we have

$$u_\ell v_\ell = u_\ell(u_\ell v_0) = (u_\ell u_\ell) v_0 = -v_0. \tag{8.4.70}$$

The analogue of (8.4.31) for $\ell = m$ is simple, thanks to (8.4.15):

$$v_\ell v_\ell = -1. \tag{8.4.71}$$

It remains to establish the following:

$$u_\ell v_m = (u_m u_\ell) v_0, \quad v_\ell v_m = u_m u_\ell, \quad \text{for } \ 1 \le \ell, m \le 3, \ \ell \ne m. \tag{8.4.72}$$

Expanded out, the required identities are

$$u_\ell(u_m v_0) = (u_m u_\ell) v_0, \quad 1 \le \ell, m \le 3, \ \ell \ne m, \tag{8.4.73}$$

and

$$(u_\ell v_0)(u_m v_0) = u_m u_\ell, \quad 1 \le \ell, m \le 3, \ \ell \ne m. \tag{8.4.74}$$

□

Such identities as (8.4.73)–(8.4.74) are closely related to an important class of identities known as "Moufang identities," which we now introduce.

**Proposition 8.4.5.** *Given $x, y, z \in \mathbb{O}$,*

$$(xyx)z = x(y(xz)), \quad z(xyx) = ((zx)y)x, \tag{8.4.75}$$

*and*

$$(xy)(zx) = x(yz)x. \tag{8.4.76}$$

Regarding the paucity of parentheses here, we use the notation $xwx$ to mean

$$xwx = (xw)x = x(wx), \tag{8.4.77}$$

the last identity by (8.4.3). Note also that the two identities in (8.4.75) are equivalent, respectively, to

$$L_{xyx} = L_x L_y L_x, \quad \text{and} \quad R_{xyx} = R_x R_y R_x. \tag{8.4.78}$$

A proof of Proposition 8.4.5 will be given later in this section. We now show how (8.4.75)–(8.4.76) can be used to establish (8.4.73)–(8.4.74).

We start with (8.4.74), which is equivalent to

$$(v_0 u_\ell)(u_m v_0) = u_\ell u_m. \tag{8.4.79}$$

In this case, (8.4.76) yields

$$\begin{aligned}(v_0 u_\ell)(u_m v_0) &= v_0(u_\ell u_m)v_0 \\ &= -(u_\ell u_m)v_0 v_0 \quad (\text{if } \ell \neq m) \\ &= u_\ell u_m,\end{aligned} \tag{8.4.80}$$

via a couple of applications of (8.4.15). This gives (8.4.74).

Moving on, applying $L_{v_0}$, we see that (8.4.73) is equivalent to

$$v_0(u_\ell(u_m v_0)) = v_0(u_m u_\ell)v_0, \tag{8.4.81}$$

hence to

$$v_0(u_\ell(v_0 u_m)) = v_0(u_\ell u_m)v_0. \tag{8.4.82}$$

Now the first identity in (8.4.75) implies that the left side of (8.4.82) is equal to

$$(v_0 u_\ell v_0)u_m = u_\ell u_m, \tag{8.4.83}$$

the latter identity because $v_0 u_\ell v_0 = -u_\ell v_0 v_0 = u_\ell$. On the other hand, if $\ell \neq m$, then

$$v_0(u_\ell u_m)v_0 = -(u_\ell u_m)v_0 v_0 = u_\ell u_m, \tag{8.4.84}$$

agreeing with the right side of (8.4.83). Thus we have (8.4.82), hence (8.4.73).

Rather than concluding that Proposition 8.4.4 is now proved, we must reveal that the proof of Proposition 8.4.5 given below actually uses Proposition 8.4.4. Therefore, it is necessary to produce an alternative endgame to the proof of Proposition 8.4.4.

We begin by noting that the approach to the proof of Proposition 8.4.4 described above uses the identities (8.4.75)–(8.4.76) with

$$x = v_0, \quad y = u_\ell, \quad z = u_m, \quad \ell \neq m, \tag{8.4.85}$$

hence $xy = -v_\ell, zx = v_m, yz = \pm u_h,\ \{h, \ell, m\} = \{1, 2, 3\}$. Thus the application of the first identity of (8.4.75) in (8.4.83) is justified by the following special case of (8.4.78):

**Proposition 8.4.6.** *If* $\{u, v\} \in \mathrm{Im}(\mathbb{O})$ *is an orthonormal set, then*

$$L_{uvu} = L_v = L_u L_v L_u. \tag{8.4.86}$$

**Proof.** Under these hypotheses, $u^2 = -1$ and $uv = -vu$. Bringing in (8.4.3), we have

$$uvu = -u^2v = v, \tag{8.4.87}$$

which gives the first identity in (8.4.86). We also have

$$a \in \mathrm{Im}(\mathbb{O}) \Longrightarrow L_a^2 = L_{a^2} = -|a|^2 I, \tag{8.4.88}$$

the first identity by (8.4.3). Thus

$$\begin{aligned} -2I = L^2_{(u+v)} &= (L_u + L_v)(L_u + L_v) \\ &= L_u^2 + L_v^2 + L_u L_v + L_v L_u, \end{aligned} \tag{8.4.89}$$

so

$$L_u L_v = -L_v L_u, \tag{8.4.90}$$

and hence

$$L_u L_v L_u = -L_v L_u^2 = L_v, \tag{8.4.91}$$

giving the second identity in (8.4.86). □

As for the application of (8.4.76) to (8.4.80), we need the special case

$$(uv)(wu) = u(vw)u, \tag{8.4.92}$$

for $u = v_0, v = u_\ell, w = u_m, \ell \neq m, 1 \le \ell, m \le 3$ (so $uv = -v_\ell$), in which cases

$$\{u, v, w, uv\},\ \{u, vw\} \subset \mathrm{Im}(\mathbb{O}),\ \text{are orthonormal sets.} \tag{8.4.93}$$

In such a case, $u(vw)u = -(vw)u^2 = vw$, so it suffices to show that

$$(uv)(wu) = vw, \tag{8.4.94}$$

for

$$\{u, v, w, uv\} \subset \mathrm{Im}(\mathbb{O}), \quad \text{orthonormal.} \tag{8.4.95}$$

When (8.4.95) holds, we say $\{u, v, w\}$ is a *Cayley triangle*. The following takes care of our needs.

**Proposition 8.4.7.** *Assume $\{u, v, w\}$ is a Cayley triangle. Then*

$$v(uw) = -(vu)w, \tag{8.4.96}$$

$$\langle uv, uw \rangle = 0, \quad \textit{so } \{u, v, uw\} \textit{ is a Cayley triangle}, \tag{8.4.97}$$

*and* (8.4.94) *holds.*

**Proof.** To start, the hypotheses imply

$$vu = -uv, \quad vw = -wv, \quad uw = -wu, \quad (vu)w = -w(vu), \tag{8.4.98}$$

so

$$\begin{aligned} v(uw) + (vu)w &= -v(wu) - w(vu) \\ &= (v^2 + w^2)u - (v + w)(vu + wu) \\ &= (v + w)^2 u - (v + w)((v + w)u) \\ &= 0, \end{aligned} \tag{8.4.99}$$

and we have (8.4.96). Next,

$$\langle uv, uw \rangle = \langle L_u v, L_u w \rangle = \langle u, w \rangle = 0, \tag{8.4.100}$$

since $L_u \in SO(\mathbb{O})$. Thus $\{u, v, uw\}$ is a Cayley triangle. Applying (8.4.96) to this Cayley triangle (and bringing in (8.4.3)) then gives

$$\begin{aligned} (vu)(uw) &= -v(u(uw)) \\ &= -v(u^2 w) \\ &= vw, \end{aligned} \tag{8.4.101}$$

yielding (8.4.94). □

At this point, we have a complete proof of Proposition 8.4.4.

### The automorphism group of $\mathbb{O}$

The set of automorphisms of $\mathbb{O}$ is denoted $\mathrm{Aut}(\mathbb{O})$. Note that $\mathrm{Aut}(\mathbb{O})$ is a group, i.e.,

$$K_j \in \mathrm{Aut}(\mathbb{O}) \Longrightarrow K_1 K_2,\ K_j^{-1} \in \mathrm{Aut}(\mathbb{O}). \tag{8.4.102}$$

Clearly $K \in \mathrm{Aut}(\mathbb{O}) \Rightarrow K1 = 1$. The following result will allow us to establish a converse to Proposition 8.4.4.

**Proposition 8.4.8.** *Assume* $K \in \mathrm{Aut}(\mathbb{O})$. *Then*

$$K : \mathrm{Im}(\mathbb{O}) \longrightarrow \mathrm{Im}(\mathbb{O}). \tag{8.4.103}$$

*Consequently*

$$K\overline{x} = \overline{Kx}, \quad \forall\, x \in \mathbb{O}, \tag{8.4.104}$$

*and*

$$|Kx| = |x|, \quad \forall\, x \in \mathbb{O}, \tag{8.4.105}$$

*so* $K : \mathbb{O} \to \mathbb{O}$ *is an orthogonal transformation.*

**Proof.** To start, we note that, given $x \in \mathbb{O}$, $x^2$ is real if and only if either $x$ is real or $x \in \operatorname{Im}(\mathbb{O})$. Now, given $u \in \operatorname{Im}(\mathbb{O})$,

$$(Ku)^2 = K(u^2) = -|u|^2 K1 = -|u|^2 \quad \text{(real)}, \tag{8.4.106}$$

so either $Ku \in \operatorname{Im}(\mathbb{O})$ or $Ku = a$ is real. In the latter case, we have $K(a^{-1}u) = 1$, so $a^{-1}u = 1$, so $u = a$, contradicting the hypothesis that $u \in \operatorname{Im}(\mathbb{O})$. This gives (8.4.103). The result (8.4.104) is an immediate consequence. Thus, for $x \in \mathbb{O}$,

$$|Kx|^2 = (Kx)(\overline{Kx}) = (Kx)(K\overline{x}) = K(x\overline{x}) = |x|^2, \tag{8.4.107}$$

giving (8.4.105). ∎

Now, given $K \in \operatorname{Aut}(\mathbb{O})$, define $u_1, u_2$, and $v_0$ by

$$u_1 = Ke_1, \quad u_2 = Ke_2, \quad v_0 = Kf_0. \tag{8.4.108}$$

By Proposition 8.4.8, these are orthonormal elements of $\operatorname{Im}(\mathbb{O})$. Also, $\mathcal{A} = K(\mathcal{H})$, spanned by $1, u_1, u_2$, and $u_1u_2 = u_1 \times u_2$, is a subalgebra of $\mathbb{O}$, and $v_0 \in \mathcal{A}^\perp$. These observations, together with Proposition 8.4.4, yield the following.

**Proposition 8.4.9.** *The formulas* (8.4.108) *provide a one-to-one correspondence between the set of automorphisms of* $\mathbb{O}$ *and*

$$\begin{aligned} &\text{the set of ordered orthonormal triples } (u_1, u_2, v_0) \text{ in } \operatorname{Im}(\mathbb{O}) \\ &\text{such that } v_0 \text{ is also orthogonal to } u_1 \times u_2, \text{ that is,} \\ &\text{the set of Cayley triangles in } \operatorname{Im}(\mathbb{O}). \end{aligned} \tag{8.4.109}$$

It can be deduced from (8.4.109) that $\operatorname{Aut}(\mathbb{O})$ is a Lie group of dimension 14.

We return to the Moufang identities and use the results on $\operatorname{Aut}(\mathbb{O})$ established above to prove them.

**Proof of Proposition 8.4.5.** Consider the first identity in (8.4.75), i.e.,

$$(xyx)z = x(y(xz)), \quad \forall\, x, y, z \in \mathbb{O}. \tag{8.4.110}$$

We begin with a few simple observations. First, (8.4.110) is clearly true if any one of $x, y, z$ is scalar, or if any two of them coincide (thanks to Proposition 8.4.3). Also, both sides of (8.4.110) are linear in $y$ and in $z$. Thus, it suffices to treat (8.4.110) for $y, z \in \operatorname{Im}(\mathbb{O})$. Meanwhile, multiplying by a real number and applying an element of $\operatorname{Aut}(\mathbb{O})$, we can assume $x = a + e_1$, for some $a \in \mathbb{R}$.

To proceed, (8.4.110) is clear for $y \in \operatorname{Span}(1, x)$, so, using the linearity in $y$, and applying Proposition 8.4.9 again, we can arrange that $y = e_2$. Given this, (8.4.110) is clear for $z \in \mathcal{H} = \operatorname{Span}(1, e_2, e_2, e_3 = e_1e_2)$. Thus, using linearity of (8.4.110) in $z$, it suffices to treat $z \in \mathcal{H}^\perp$, and again applying an element of $\mathrm{Aut}(\mathbb{O})$, we can assume $z = f_1$.

At this point, we have reduced the task of proving (8.4.110) to checking it for

$$x = a + e_1, \quad y = e_2, \quad z = f_1, \quad a \in \mathbb{R}, \tag{8.4.111}$$

and this is straightforward. Similar arguments applied to the second identity in (8.4.75), and to (8.4.76), reduce their proofs to a check in the case (8.4.111). □

We next look at some interesting subgroups of $\mathrm{Aut}(\mathbb{O})$. Taking $Sp(1)$ to be the group of unit quaternions, as in (8.1.27), we have group homomorphisms

$$\alpha, \beta : Sp(1) \longrightarrow \mathrm{Aut}(\mathbb{O}), \tag{8.4.112}$$

given by

$$\begin{aligned} \alpha(\xi)(\zeta, \eta) &= (\xi\zeta\overline{\xi}, \xi\eta\overline{\xi}), \\ \beta(\xi)(\zeta, \eta) &= (\zeta, \xi\eta), \end{aligned} \tag{8.4.113}$$

where $\zeta, \eta \in \mathbb{H}$ define $(\zeta, \eta) \in \mathbb{O}$. As in (8.1.33)–(8.1.39), for $\xi \in Sp(1)$, $\pi(\xi)\zeta = \xi\zeta\overline{\xi}$ gives an automorphism of $\mathbb{H}$, and it commutes with conjugation in $\mathbb{H}$, so the fact that $\alpha(\xi)$ is an automorphism of $\mathbb{O}$ follows from the definition (8.4.2) of the product in $\mathbb{O}$. The fact that $\beta(\xi)$ is an automorphism of $\mathbb{O}$ also follows directly from (8.4.2). Parallel to (8.1.37),

$$\mathrm{Ker}\,\alpha = \{\pm 1\} \subset Sp(1), \tag{8.4.114}$$

so the image of $Sp(1)$ under $\alpha$ is a subgroup of $\mathrm{Aut}(\mathbb{O})$ isomorphic to $SO(3)$. Clearly $\beta$ is one-to-one, so it yields a subgroup of $\mathrm{Aut}(\mathbb{O})$ isomorphic to $Sp(1)$.

These two subgroups of $\mathrm{Aut}(\mathbb{O})$ do not commute with each other. In fact, we have, for $\xi_j \in Sp(1)$, $(\zeta, \eta) \in \mathbb{O}$,

$$\begin{aligned} \alpha(\xi_1)\beta(\xi_2)(\zeta, \eta) &= (\xi_1\zeta\overline{\xi}_1, \xi_1\xi_2\eta\overline{\xi}_1), \\ \beta(\xi_2)\alpha(\xi_1)(\zeta, \eta) &= (\xi_1\zeta\overline{\xi}_1, \xi_2\xi_1\eta\overline{\xi}_1). \end{aligned} \tag{8.4.115}$$

Note that, since $\xi_2\xi_1 = \xi_1(\overline{\xi}_1\xi_2\xi_1)$,

$$\beta(\xi_2)\alpha(\xi_1) = \alpha(\xi_1)\beta(\overline{\xi}_1\xi_2\xi_1). \tag{8.4.116}$$

It follows that

$$G_{\mathcal{H}} = \{\alpha(\xi_1)\beta(\xi_2) : \xi_j \in Sp(1)\} \tag{8.4.117}$$

is a subgroup of $\mathrm{Aut}(\mathbb{O})$. It is clear from (8.4.113) that each automorphism $\alpha(\xi_1), \beta(\xi_2)$, and hence each element of $G_{\mathcal{H}}$, preserves $\mathcal{H}$ (and also $\mathcal{H}^\perp$). The converse also holds:

**Proposition 8.4.10.** *The group $G_{\mathcal{H}}$ is the group of all automorphisms of $\mathbb{O}$ that preserve $\mathcal{H}$.*

**Proof.** Indeed, suppose $K \in \mathrm{Aut}(\mathbb{O})$ preserves $\mathcal{H}$. Then $K|_{\mathcal{H}}$ is an automorphism of $\mathcal{H} \approx \mathbb{H}$. Arguments in the paragraph containing (8.1.38)–(8.1.41) imply that there exists $\xi_1 \in Sp(1)$ such that $K|_{\mathcal{H}} = \alpha(\xi_1)|_{\mathcal{H}}$, so $K_0 = \alpha(\xi_1)^{-1}K \in \mathrm{Aut}(\mathbb{O})$ is the identity on $\mathcal{H}$. Now $K_0 f_1 = (0, \xi_2)$ for some $\xi_2 \in Sp(1)$, and it then follows from Proposition I.7 that $K_0 = \beta(\xi_2)$. Hence $K = \alpha(\xi_1)\beta(\xi_2)$, as desired. □

For another perspective on $G_{\mathcal{H}}$, we bring in

$$\tilde{\alpha} : Sp(1) \longrightarrow \mathrm{Aut}(\mathbb{O}), \quad \tilde{\alpha}(\xi) = \beta(\overline{\xi})\alpha(\xi). \tag{8.4.118}$$

Note that

$$\tilde{\alpha}(\xi)(\zeta, \eta) = (\xi\zeta\overline{\xi}, \eta\overline{\xi}), \tag{8.4.119}$$

so $\tilde{\alpha}$ is a group homomorphism. Another easy consequence of (8.4.119) is that $\tilde{\alpha}(\xi_1)$ and $\beta(\xi_2)$ commute, for each $\xi_j \in Sp(1)$. We have a surjective group homomorphism

$$\tilde{\alpha} \times \beta : Sp(1) \times Sp(1) \longrightarrow G_{\mathcal{H}}. \tag{8.4.120}$$

Note that $\mathrm{Ker}(\tilde{\alpha} \times \beta) = \{(1,1), (-1,-1)\}$, with 1 denoting the unit in $\mathbb{H}$. Comparison with (8.2.33)–(8.2.34) and Lemma 8.2.3 gives

$$G_{\mathcal{H}} \approx SO(4). \tag{8.4.121}$$

We now take a look at one-parameter families of automorphisms of $\mathbb{O}$, of the form

$$K(t) = e^{tA}, \quad A \in \mathcal{L}(\mathbb{O}), \tag{8.4.122}$$

where $e^{tA}$ is the matrix exponential, introduced in §3.7. To see when such linear transformations on $\mathbb{O}$ are automorphisms, we differentiate the identity

$$K(t)(xy) = (K(t)x)(K(t)y), \quad x, y \in \mathbb{O}, \tag{8.4.123}$$

obtaining

$$A(xy) = (Ax)y + x(Ay), \quad x, y \in \mathbb{O}. \tag{8.4.124}$$

When (8.4.124) holds, we say

$$A \in \mathrm{Der}(\mathbb{O}). \tag{8.4.125}$$

**Proposition 8.4.11.** *Given $A \in \mathcal{L}(\mathbb{O})$, $e^{tA} \in \mathrm{Aut}(\mathbb{O})$ for all $t \in \mathbb{R}$ if and only if $A \in \mathrm{Der}(\mathbb{O})$.*

**Proof.** The implication $\Rightarrow$ was established above. For the converse, suppose $A$ satisfies (8.4.124). Take $x, y \in \mathbb{O}$, and set

$$X(t) = (e^{tA}x)(e^{tA}y). \tag{8.4.126}$$

Applying $d/dt$ gives

$$\begin{aligned} \frac{dX}{dt} &= (Ae^{tA}x)(e^{tA}y) + (e^{tA}x)(Ae^{tA}y) \\ &= A\big((e^{tA}x)(e^{tA}y)\big) \\ &= AX(t), \end{aligned} \tag{8.4.127}$$

the second identity by (8.4.124). Since $X(0) = xy$, it follows from the uniqueness argument in (3.7.11)–(3.7.16) that

$$X(t) = e^{tA}(xy), \tag{8.4.128}$$

so indeed $e^{tA} \in \mathrm{Aut}(\mathbb{O})$. □

The set $\mathrm{Der}(\mathbb{O})$ has the following structure.

**Proposition 8.4.12.** $\mathrm{Der}(\mathbb{O})$ *is a linear subspace of* $\mathcal{L}(\mathbb{O})$ *satisfying*

$$A, B \in \mathrm{Der}(\mathbb{O}) \Longrightarrow [A, B] \in \mathrm{Der}(\mathbb{O}), \tag{8.4.129}$$

*where* $[A, B] = AB - BA$. *That is,* $\mathrm{Der}(\mathbb{O})$ *is a Lie algebra.*

**Proof.** That $\mathrm{Der}(\mathbb{O})$ is a linear space is clear from the defining property (8.4.124). Furthermore, if $A, B \in \mathrm{Der}(\mathbb{O})$, then, for all $x, y \in \mathbb{O}$,

$$\begin{aligned} AB(xy) &= A((Bx)y) + A(x(By)) \\ &= (ABx)y + (Bx)(Ay) + (Ax)(By) + x(ABy), \end{aligned} \tag{8.4.130}$$

and similarly

$$BA(xy) = (BAx)y + (Ax)(By) + (Bx)(Ay) + x(BAy), \tag{8.4.131}$$

so

$$[A, B](xy) = ([A, B]x)y + x([A, B]y), \tag{8.4.132}$$

and we have (8.4.129). □

By Proposition 8.4.8, if $A \in \mathrm{Der}(\mathbb{O})$, then $e^{tA}$ is an orthogonal transformation for each $t \in \mathbb{R}$. As in Exercise 9 of §3.7, we have

$$(e^{tA})^* = e^{tA^*}, \tag{8.4.133}$$

so

$$A \in \mathrm{Der}(\mathbb{O}) \Longrightarrow A^* = -A, \tag{I.128}$$

i.e., $A$ is skew-adjoint. It is clear that

$$A \in \mathrm{Der}(\mathbb{O}) \Longrightarrow A : \mathrm{Im}(\mathbb{O}) \to \mathrm{Im}(\mathbb{O}), \tag{8.4.134}$$

and since $\mathrm{Im}(\mathbb{O})$ is odd dimensional, the structural result Proposition 3.3.4 implies

$$A \in \mathrm{Der}(\mathbb{O}) \Longrightarrow \mathcal{N}(A) \cap \mathrm{Im}(\mathbb{O}) \neq 0. \tag{8.4.135}$$

As long as $A \neq 0$, we can also deduce from Proposition 3.3.4 that $\mathrm{Im}(\mathbb{O})$ contains a two-dimensional subspace with orthonormal basis $\{u_1, u_2\}$, invariant under $A$, and with repect to which $A$ is represented by a $2 \times 2$ block

$$\begin{pmatrix} 0 & -\lambda \\ \lambda & 0 \end{pmatrix}. \tag{8.4.136}$$

Then, by (I.118),

$$\begin{aligned} A(u_1 u_2) &= (Au_1)u_2 + u_1(Au_2) \\ &= \lambda u_2^2 - \lambda u_1^2 \\ &= 0, \end{aligned} \tag{8.4.137}$$

so $u_1 u_2 = u_1 \times u_2 \in \mathcal{N}(A) \cap \mathrm{Im}(\mathbb{O})$. As in (8.4.37)–(8.4.45), $\mathrm{Span}\{1, u_1, u_2, u_3 = u_1 u_2\} = \mathcal{A}$ is a subalgebra of $\mathbb{O}$ isomorphic to $\mathbb{H}$. We see that $A$ preserves $\mathcal{A}$, so the associated one-parameter group of automorphisms $e^{tA}$ preserves $\mathcal{A}$.

Using Proposition 8.4.9, we can pick $K \in \mathrm{Aut}(\mathbb{O})$ taking $\mathcal{A}$ to $\mathcal{H}$, and deduce the following.

**Proposition 8.4.13.** *Given* $A \in \mathrm{Der}(\mathbb{O})$*, there exists* $K \in \mathrm{Aut}(\mathbb{O})$ *such that*

$$K e^{tA} K^{-1} \in G_{\mathcal{H}}, \quad \forall\, t \in \mathbb{R}. \tag{8.4.138}$$

Note that then

$$K e^{tA} K^{-1} = e^{t\widetilde{A}}, \quad \widetilde{A} = KAK^{-1} \in \mathrm{Der}(\mathbb{O}), \tag{8.4.139}$$

and (8.4.138) is equivalent to

$$\widetilde{A} : \mathcal{H} \longrightarrow \mathcal{H}, \quad \widetilde{A} \in \mathrm{Der}(\mathbb{O}), \tag{8.4.140}$$

which also entails $\widetilde{A} : \mathcal{H}^\perp \to \mathcal{H}^\perp$, since $\widetilde{A}$ is skew-adjoint. When (8.4.140) holds, we say

$$\widetilde{A} \in D_{\mathcal{H}}. \tag{8.4.141}$$

Going further, suppose we have $d$ commuting elements of $\mathrm{Der}(\mathbb{O})$:

$$A_j \in \mathrm{Der}(\mathbb{O}), \quad A_j A_k = A_k A_j, \quad j, k \in \{1, \dots, d\}. \tag{8.4.142}$$

A modification of the arguments leading to Proposition 3.3.4 yields a two-dimensional subspace of $\mathrm{Im}(\mathbb{O})$, with orthonormal basis $\{u_1, u_2\}$, invariant under each $A_j$, with respect to which each $A_j$ is represented by a $2\times 2$ block as in (8.4.136), with $\lambda$ replaced by $\lambda_j$ (possibly 0). As in (8.4.137),

$$A_j(u_1u_2) = 0, \quad 1 \le j \le d, \tag{8.4.143}$$

so each $A_j$ preserves $\mathcal{A} = \operatorname{Span}\{1, u_1, u_2, u_3 = u_1u_2\}$, and so does each one-parameter group of automorphisms $e^{tA_j}$. Bringing in $K \in \operatorname{Aut}(\mathbb{O})$, taking $\mathcal{A}$ to $\mathcal{H}$, we have the following variant of Proposition 8.4.13.

**Proposition 8.4.14.** *Given commuting $A_j \in \operatorname{Der}(\mathbb{O})$, $1 \le j \le d$, there exists $K \in \operatorname{Aut}(\mathbb{O})$ such that*

$$Ke^{tA_j}K^{-1} \in G_{\mathcal{H}}, \quad \forall\, t \in \mathbb{R},\ j \in \{1, \dots, d\}. \tag{8.4.144}$$

As a consequence, we have

$$\widetilde{A}_j = KA_jK^{-1} \in D_{\mathcal{H}}, \quad \widetilde{A}_j\widetilde{A}_k = \widetilde{A}_k\widetilde{A}_j, \quad 1 \le j, k \le d. \tag{8.4.145}$$

Consequently, $e^{t\widetilde{A}_j}$ are mutually commuting one-parameter subgroups of $G_{\mathcal{H}}$, i.e.,

$$e^{t_j\widetilde{A}_j} \in G_{\mathcal{H}}, \quad e^{t_j\widetilde{A}_j}e^{t_k\widetilde{A}_k} = e^{t_k\widetilde{A}_k}e^{t_j\widetilde{A}_j}, \quad 1 \le j, k \le d. \tag{8.4.146}$$

One can produce *pairs* of such commuting groups, as follows. Take

$$\tilde{\alpha}(\xi_1(t_1)),\ \beta(\xi_2(t_2)) \in G_{\mathcal{H}}, \tag{8.4.147}$$

with $\beta$ as in (8.4.112)–(8.4.113), $\tilde{\alpha}$ as in (8.4.118)–(8.4.119), and $\xi_\nu(t)$ one-parameter subgroups of $Sp(1)$, for example

$$\xi_\nu(t) = e^{t\omega_\nu}, \quad \omega_\nu \in \operatorname{Im}(\mathbb{H}) = \operatorname{Span}\{i, j, k\}. \tag{8.4.148}$$

The exponential $e^{t\omega_\nu}$ is amenable to a treatment parallel to that given in §3.7, as seen in exercises at the end of §8.1. Mutual commutativity in (8.4.147) follows from the general mutual commutativity of $\tilde{\alpha}$ and $\beta$. The following important structural information on $\operatorname{Aut}(\mathbb{O})$ says $d = 2$ is as high as one can go.

**Proposition 8.4.15.** *If $A_j \in \operatorname{Der}(\mathbb{O})$ are mutually commuting, for $j \in \{1, \dots, d\}$, and if $\{A_j\}$ is linearly independent in $\mathcal{L}(\mathbb{O})$, then $d \le 2$.*

**Proof.** To start, we obtain from $A_j$ the mutually commuting one-parameter groups $Ke^{tA_j}K^{-1}$, subgroups of $G_{\mathcal{H}}$. Taking inverse images under the two-to-one surjective homomorphism (8.4.120), we get mutually commuting one-parameter subgroups $\gamma_j(t)$ of $Sp(1) \times Sp(1)$, which can be written

$$\gamma_j(t) = \begin{pmatrix} e^{\omega_j t} & \\ & e^{\sigma_j t} \end{pmatrix}, \quad \omega_j, \sigma_j \in \operatorname{Im}(\mathbb{H}), \quad 1 \le j \le d. \tag{8.4.149}$$

Parallel to Proposition 3.7.6, this commutativity requires $\{\omega_j : 1 \le j \le d\}$ to commute in $\mathbb{H}$ and it also requires $\{\sigma_j : 1 \le j \le d\}$ to commute in

$\mathbb{H}$. These conditions in turn require each $\omega_j$ to be a real multiple of some $\omega^\# \in \mathrm{Im}(\mathbb{H})$ and each $\sigma_j$ to be a real multiple of some $\sigma^\# \in \mathrm{Im}(\mathbb{H})$.

Now the linear independence of $\{A_j : 1 \le j \le d\}$ in $\mathrm{Der}(\mathbb{O})$ implies the linear independence of $\{(\omega_j, \sigma_j) : 1 \le j \le d\}$ in $\mathrm{Im}(\mathbb{H}) \oplus \mathrm{Im}(\mathbb{H})$, and this implies $d \le 2$. $\square$

We turn to the introduction of another interesting subgroup of $\mathrm{Aut}(\mathbb{O})$. Note that, by Proposition 8.4.9, given any unit $u_1 \in \mathrm{Im}(\mathbb{O})$, there exists $K \in \mathrm{Aut}(\mathbb{O})$ such that $Ke_1 = u_1$. Consequently, $\mathrm{Aut}(\mathbb{O})$, acting on $\mathrm{Im}(\mathbb{O})$ as a group of orthogonal transformations, acts *transitively* on the unit sphere $S$ in $\mathrm{Im}(\mathbb{O}) \approx \mathbb{R}^7$, i.e., on $S \approx S^6$. Referring to (A.3.30)–(A.3.31), we are hence interested in the group

$$\{K \in \mathrm{Aut}(\mathbb{O}) : Ke_1 = e_1\} = \mathcal{G}_{e_1}. \tag{8.4.150}$$

We claim that

$$\mathcal{G}_{e_1} \approx SU(3). \tag{8.4.151}$$

As preparation for the demonstration, note that each $K \in \mathcal{G}_{e_1}$ is an orthogonal linear transformation on $\mathbb{O}$ that leaves invariant $\mathrm{Span}\{1, e_1\}$, and hence it also leaves invariant the orthogonal complement

$$V = \mathrm{Span}\{1, e_1\}^\perp = \mathrm{Span}\{e_2, e_3, f_0, f_1, f_2, f_3\}, \tag{8.4.152}$$

a linear space of $\mathbb{R}$-dimension 6. We endow $V$ with a complex structure. Generally, a complex structure on a real vector space $V$ is an $\mathbb{R}$-linear map $J : V \to V$ such that $J^2 = -I_V$. One can check that this requires $\dim_{\mathbb{R}} V$ to be even, say $2k$. Then $(V, J)$ has the structure of a complex vector space, with

$$(a + ib)v = av + bJv, \quad a, b \in \mathbb{R},\ v \in V. \tag{8.4.153}$$

One has $\dim_{\mathbb{C}}(V, J) = k$. If $V$ is a real inner product space, with inner product $\langle\ ,\ \rangle$, and if $J$ is orthogonal (hence skew-adjoint) on $V$, then $(V, J)$ gets a natural Hermitian inner product

$$(u, v) = \langle u, v\rangle + i\langle u, Jv\rangle, \tag{8.4.154}$$

satisfying (3.1.5)–(3.1.7). If $T : V \to V$ preserves $\langle\ ,\ \rangle$ and commutes with $J$, then it also preserves $(\ ,\ )$, so it is a unitary transformation on $(V, J)$.

We can apply this construction to $V$ as in (8.4.152), with

$$Jv = L_{e_1} v = e_1 v, \tag{8.4.155}$$

noting that $L_{e_1}$ is an orthogonal map on $\mathbb{O}$ that preserves $\mathrm{Span}\{1, e_1\}$, and hence also preserves $V$. To say that an $\mathbb{R}$-linear map $K : V \to V$ is $\mathbb{C}$-linear is to say that $K(e_1 v) = e_1 K(v)$, for all $v \in V$. Clearly this holds if $K \in \mathrm{Aut}(\mathbb{O})$ and $Ke_1 = e_1$. Thus each element of $\mathcal{G}_{e_1}$ defines a complex linear orthogonal (hence unitary) transformation on $V$, and we have an injective group homomorphism

$$\mathcal{G}_{e_1} \longrightarrow U(V,J). \tag{8.4.156}$$

Note that the 6 element real orthonormal basis of $V$ in (8.4.152) yields the 3 element orthonormal basis of $(V,J)$,

$$\{e_2, f_0, f_2\}, \tag{8.4.157}$$

since

$$e_3 = e_1 e_2, \quad f_1 = e_1 f_0, \quad f_3 = -e_1 f_2, \tag{8.4.158}$$

the latter two identities by (8.4.30)–(8.4.31). This choice of basis yields the isomorphism

$$U(V,J) \approx U(3). \tag{8.4.159}$$

We aim to identify the image of $\mathcal{G}_{e_1}$ in $U(3)$ that comes from (8.4.156) and (8.4.159).

To accomplish this, we reason as follows. From Proposition 8.4.9 it follows that there is a natural one-to-one correspondence between the elements of $\mathcal{G}_{e_1}$ and

$$\begin{aligned}&\text{the set of ordered orthonormal pairs } \{u_2, v_0\} \text{ in } V\\ &\text{such that also } v_0 \perp e_1 u_2,\end{aligned} \tag{8.4.160}$$

or, equivalently,

$$\text{the set of ordered orthonormal pairs } \{u_2, v_0\} \text{ in } (V,J), \tag{8.4.161}$$

where $(V,J)$ carries the Hermitian inner product (8.4.154). In fact, the correspondence associates to $K \in \mathcal{G}_{e_1}$ (i.e., $K \in \mathrm{Aut}(\mathbb{O})$ and $Ke_1 = e_1$) the pair

$$u_2 = Ke_2, \quad v_0 = Kf_0. \tag{8.4.162}$$

Then the image of $\mathcal{G}_{e_1}$ in $U(V,J)$ in (8.4.156) is uniquely determined by the action of $K$ on the third basis element in (8.4.157), as

$$Kf_2 = K(e_2 f_0) = K(e_2)K(f_0) = u_2 v_0 = u_2 \times v_0, \tag{8.4.163}$$

where we recall from (8.4.30) that $f_2 = e_2 f_0$, and the last identity in (8.4.163) follows from (8.4.21).

From (8.4.160)–(8.4.161), it can be deduced that $\mathcal{G}_{e_1}$ is a compact, connected Lie group of dimension 8. Then (8.4.155) and (8.4.158) present $\mathcal{G}_{e_1}$ as isomorphic to a subgroup (call it $\widetilde{\mathcal{G}}$) of $U(3)$ that is a compact, connected Lie group of dimension 8. Meanwhile, $\dim U(3) = 9$, so $\widetilde{\mathcal{G}}$ has codimension 1. We claim that this implies

$$\widetilde{\mathcal{G}} = SU(3). \tag{8.4.164}$$

We sketch a proof of (8.4.164), using some elements of Lie group theory.

To start, one can show that a connected, codimension-one subgroup of a compact, connected Lie group must be *normal* (recall the definition from (A.3.17)). Hence $\widetilde{\mathcal{G}}$ is a normal subgroup of $U(3)$. As in (A.3.27)–(A.3.29), this implies $U(3)/\widetilde{\mathcal{G}}$ is a group. This quotient is a compact Lie group of dimension 1, hence isomorphic to $S^1 = \{z \in \mathbb{C} : |z| = 1\}$, and the projection $U(3) \to U(3)/\widetilde{\mathcal{G}}$ produces a continuous, surjective group homomorphism

(8.4.165) $$\vartheta : U(3) \longrightarrow S^1, \quad \operatorname{Ker} \vartheta = \widetilde{\mathcal{G}}.$$

Now a complete list of such homomorphisms is given by

(8.4.166) $$\vartheta_j(K) = (\det K)^j, \quad j \in \mathbb{Z} \setminus 0,$$

and in such a case, $\operatorname{Ker} \vartheta_j$ has $|j|$ connected components. Then connectivity of $\widetilde{\mathcal{G}}$ forces $\vartheta = \vartheta_{\pm 1}$ in (8.4.165), which in turn gives (8.4.164).

It is useful to take account of various subgroups of $\operatorname{Aut}(\mathbb{O})$ that are conjugate to $G_{\mathcal{H}}$ (given by (8.4.117)) or to $\mathcal{G}_{e_1}$ (given by (8.4.150)). In particular, when $\mathcal{A} \subset \mathbb{O}$ is a four-dimensional subalgebra, we set

(8.4.167) $$G_{\mathcal{A}} = \{K \in \operatorname{Aut}(\mathbb{O}) : K(\mathcal{A}) \subset \mathcal{A}\},$$

and if $u \in \operatorname{Im}(\mathbb{O}), |u| = 1$, we set

(8.4.168) $$\mathcal{G}_u = \{K \in \operatorname{Aut}(\mathbb{O}) : Ku = u\}.$$

We see that each group $G_{\mathcal{A}}$ is conjugate to $G_{\mathcal{H}}$, and isomorphic to $SO(4)$, and each group $\mathcal{G}_u$ is conjugate to $\mathcal{G}_{e_1}$, and isomorphic to $SU(3)$.

It is of interest to look at $\mathcal{G}_u \cap \mathcal{G}_v$, where $u$ and $v$ are unit elements of $\operatorname{Im}(\mathbb{O})$ that are not collinear. Then

(8.4.169) $$\mathcal{G}_u \cap \mathcal{G}_v = \{K \in \operatorname{Aut}(\mathbb{O}) : K = I \text{ on } \operatorname{Span}\{u, v\}\}.$$

Now we can write $\operatorname{Span}\{u, v\} = \operatorname{Span}\{u_1, u_2\}$, with $u_1 = u, u_2 \perp u_1$, and note that $Ku_j = u_j \Rightarrow K(u_1u_2) = u_1u_2$, so (8.4.169) is equal to

(8.4.170) $$\mathcal{G}_{\mathcal{A}} = \{K \in \operatorname{Aut}(\mathbb{O}) : K = I \text{ on } \mathcal{A}\},$$

where $\mathcal{A} = \operatorname{Span}\{1, u_1, u_2, u_1u_2\}$ is a four-dimensional subalgebra of $\mathbb{O}$. Clearly

(8.4.171) $$\mathcal{G}_{\mathcal{A}} \subset G_{\mathcal{A}}, \quad \text{and} \quad \mathcal{G}_{\mathcal{A}} \approx Sp(1) \approx SU(2).$$

In fact, $\mathcal{G}_{\mathcal{A}}$ is conjugate to $\mathcal{G}_{\mathcal{H}} = \beta(Sp(1))$, with $\beta$ as in (8.4.112)–(8.4.113).

Extending (8.4.152), we have associated to each unit $u \in \operatorname{Im}(\mathbb{O})$ the space

(8.4.172) $$V_u = \operatorname{Span}\{1, u\}^{\perp},$$

and $L_u : V_u \to V_u$ gives a complex structure $J_u = L_u|_{V_u}$, so $(V_u, J_u)$ is a three-dimensional complex vector space. Parallel to (8.4.156), we have an injective group homomorphism

$$\mathcal{G}_u \longrightarrow U(V_u, J_u), \tag{8.4.173}$$

whose image is a codimension-one subgroup isomorphic to $SU(3)$. Associated to the family $(V_u, J_u)$ is the following interesting geometrical structure. Consider the unit sphere $S \approx S^6$ in $\mathrm{Im}(\mathbb{O})$. There is a natural identification of $V_u$ with the tangent space $T_uS$ to $S$ at $u$:

$$T_uS = V_u, \tag{8.4.174}$$

and the collection of complex structures $J_u$ gives $S$ what is called an *almost complex structure*. Now an element $K \in \mathrm{Aut}(\mathbb{O})$ acts on $S$, thanks to Proposition 8.4.8. Furthermore, for each $u \in S$,

$$K : V_u \longrightarrow V_{Ku} \tag{8.4.175}$$

is an isometry, and it is $\mathbb{C}$-linear, since

$$v \in V_u \Longrightarrow K(uv) = K(u)K(v). \tag{8.4.176}$$

Thus $\mathrm{Aut}(\mathbb{O})$ acts as a group of rotations on $S$ that preserve its almost complex structure. In fact, this property characterizes $\mathrm{Aut}(\mathbb{O})$. To state this precisely, we bring in the following notation. Set

$$\iota : \mathrm{Aut}(\mathbb{O}) \longrightarrow SO(\mathrm{Im}(\mathbb{O})), \quad \iota(K) = K\Big|_{\mathrm{Im}(\mathbb{O})}. \tag{8.4.177}$$

This is an injective group homomorphism, whose image we denote

$$A^b(\mathbb{O}) = \iota\, \mathrm{Aut}(\mathbb{O}). \tag{8.4.178}$$

The inverse of the isomorphism $\iota : \mathrm{Aut}(\mathbb{O}) \to A^b(\mathbb{O})$ is given by

$$\begin{gathered} j\Big|_{A^b(\mathbb{O})}, \quad j : SO(\mathrm{Im}(\mathbb{O})) \to SO(\mathbb{O}), \\ j(K_0)(a+u) = a + K_0 u. \end{gathered} \tag{8.4.179}$$

Our result can be stated as follows.

**Proposition 8.4.16.** *The group* $\Gamma$ *of rotations on* $\mathrm{Im}(\mathbb{O})$ *that preserve the almost complex structure of* $S$ *is equal to* $A^b(\mathbb{O})$*, hence isomorphic to* $\mathrm{Aut}(\mathbb{O})$*.*

**Proof.** We have seen that $A^b(\mathbb{O}) \subset \Gamma$. It remains to prove that $\Gamma \subset A^b(\mathbb{O})$, so take $K_0 \in \Gamma$, and set $K = j(K_0)$, as in (8.4.179). We need to show that $K \in \mathrm{Aut}(\mathbb{O})$. First, one readily checks that, if $K = j(K_0)$, then

$$K \in \mathrm{Aut}(\mathbb{O}) \Longleftrightarrow K(uv) = K(u)K(v),\ \forall\, u, v \in \mathrm{Im}(\mathbb{O}), \tag{8.4.180}$$

and furthermore we can take $|u| = 1$. Now the condition $K_0 \in \Gamma$ implies

$$K_0(uv) = K_0(u)K_0(v), \quad \forall\, u \in \mathrm{Im}(\mathbb{O}),\ v \in V_u. \tag{8.4.181}$$

To finish the argument, we simply note that if $K_0 \in \Gamma$ and $K = j(K_0)$, and if $u$ is a unit element of $\mathrm{Im}(\mathbb{O})$ and $v \in V_u$, then for all $a \in \mathbb{R}$,

$$\begin{aligned} K(u(au+v)) &= K(-a+uv) \\ &= -a + K_0(uv) \\ &= -a + K_0(u)K_0(v), \end{aligned} \tag{8.4.182}$$

while

$$\begin{aligned} (Ku)(K(au+v)) &= (K_0u)(aK_0u + K_0v) \\ &= a(K_0u)^2 + (K_0u)(K_0v) \\ &= -a + K_0(u)K_0(v). \end{aligned} \tag{8.4.183}$$

This finishes the proof. □

Results discussed above provide an introduction to the structure of $\mathrm{Aut}(\mathbb{O})$. In the theory of Lie groups, $\mathrm{Aut}(\mathbb{O})$ has been shown to be isomorphic to a group denoted $G_2$. The "2" comes from Proposition 8.4.15. For further material on octonions and their automorphisms, and other concepts introduced in this appendix, we refer to [**21**], [**16**], and [**25**], and also to the survey article [**3**], and to Chapter 6 of [**8**].

*Appendix A*

# Complementary results

Here we collect some results of use in various spots in the main text.

In Appendix A.1 we prove the Fundamental Theorem of Algebra, which says that every nonconstant polynomial $p(z)$ with complex coefficients has a complex root, a result needed in our work on eigenvalues of a matrix $A \in M(n, \mathbb{C})$. In brief, the proof starts with the observation that $|p(z)| \to \infty$ as $|z| \to \infty$. This leads to the existence of $z_0 \in \mathbb{C}$ such that $|p(z_0)|$ is minimal. Finally, we show that if $p(z)$ is a nonconstant polynomial and $|p(z_0)|$ is minimal, then $p(z_0) = 0$.

In Appendix A.2 we explore the notion of "averaging" a set of rotations, i.e., elements $A_1, \dots, A_N \in SO(n)$. We define the "R-average" of this set as a minimizer of

$$\psi(X) = \sum_{j=1}^{N} \|X - A_j\|^2, \tag{A.0.1}$$

over $X \in SO(n)$. Here we use the Hilbert-Schmidt norm. We analyze the R-average by means of the polar decomposition of $\overline{A} = A_1 + \cdots + A_N$.

Appendix A.3 presents results on *groups*, examples of which arise at several points in the text. Groups treated here include finite groups, such as the set $S_n$ of permutations of $n$ objects, which made an appearance in the treatment of determinants, and also infinite groups, particularly matrix groups, such as $O(n)$ and $U(n)$. One result discussed here is that if $G$ is a finite group, with $n$ elements (we say $o(G) = n$) and $H \subset G$ is a subgroup, then $o(H)$ divides $o(G)$. From this we draw the corollary that if $o(G) = n$ and $g \in G$, then

$$g^n = e, \tag{A.0.2}$$

the identity element of $G$. Applying this to the multiplicative group of nonzero elements of $\mathbb{Z}/(p)$ yields

$$a^{p-1} = 1, \quad \text{mod } p, \tag{A.0.3}$$

whenever $p$ is a prime and $a \in \mathbb{Z}$ is not a multiple of $p$. We discuss an application of this identity to a popular method of encryption.

Appendix A.4 treats algebraic extensions of fields. Given a field $\mathbb{F}$ and a polynomial $P \in \mathbb{F}[x]$ with no root in $\mathbb{F}$, we construct a new field $\widetilde{\mathbb{F}}$, as a quotient of the polynomial ring $\mathbb{F}[x]$ by a certain ideal. This new field has the property that there is a natural inclusion $\mathbb{F} \hookrightarrow \widetilde{\mathbb{F}}$, and $\widetilde{\mathbb{F}}$ has a root of $P$. Furthermore, $\widetilde{\mathbb{F}}$ is a vector space over $\mathbb{F}$ and $\dim_{\mathbb{F}} \widetilde{\mathbb{F}} < \infty$. Applying such a construction to $\mathbb{F} = \mathbb{Z}/(p)$, we obtain other finite fields. Every finite field has $p^n$ elements, for some prime $p$ and $n \in \mathbb{N}$. Conversely, for each such $p$ and $n$, we produce a field with $p^n$ elements, and show it is unique, up to isomorphism. These results form a natural complement to the material in Chapter 6. However, their derivation makes essential use of material from the first two sections of Chapter 7, so this appendix seems to be where they fit best.

## A.1. 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 A.1.1.** *If $p(z)$ is a nonconstant polynomial (with complex coefficients), then $p(z)$ must have a complex root.*

**Proof.** We have, for some $n \geq 1$, $a_n \neq 0$,

$$\begin{aligned} p(z) &= a_n z^n + \cdots + a_1 z + a_0 \\ &= a_n z^n \bigl(1 + R(z)\bigr), \quad |z| \to \infty, \end{aligned} \tag{A.1.1}$$

where

$$|R(z)| \leq \frac{C}{|z|}, \quad \text{for } \ |z| \ \text{ large.} \tag{A.1.2}$$

This implies

$$\lim_{|z|\to\infty} |p(z)| = \infty. \tag{A.1.3}$$

Picking $R \in (0, \infty)$ such that

$$\inf_{|z|\geq R} |p(z)| > |p(0)|, \tag{A.1.4}$$

we deduce that

$$\inf_{|z|\leq R} |p(z)| = \inf_{z\in\mathbb{C}} |p(z)|. \tag{A.1.5}$$

Since $D_R = \{z : |z| \leq R\}$ is closed and bounded and $p$ is continuous, there exists $z_0 \in D_R$ such that

$$|p(z_0)| = \inf_{z\in\mathbb{C}} |p(z)|. \tag{A.1.6}$$

The theorem hence follows from: ☐

**Lemma A.1.2.** *If $p(z)$ is a nonconstant polynomial and* (A.1.6) *holds, then $p(z_0) = 0$.*

**Proof.** Suppose to the contrary that

$$p(z_0) = a \neq 0. \tag{A.1.7}$$

We can write

$$p(z_0 + \zeta) = a + q(\zeta), \tag{A.1.8}$$

where $q(\zeta)$ is a (nonconstant) polynomial in $\zeta$, 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.,

$$q(\zeta) = b\zeta^k + \zeta^{k+1} r(\zeta), \quad |r(\zeta)| \leq C, \quad \zeta \to 0, \tag{A.1.9}$$

so, with $\zeta = \varepsilon\omega,\ \omega \in S^1 = \{\omega : |\omega| = 1\}$,

$$p(z_0 + \varepsilon\omega) = a + b\omega^k\varepsilon^k + (\varepsilon\omega)^{k+1} r(\varepsilon\omega), \quad \varepsilon \searrow 0. \tag{A.1.10}$$

Pick $\omega \in S^1$ such that

$$\frac{b}{|b|}\omega^k = -\frac{a}{|a|}, \tag{A.1.11}$$

which is possible since $a \neq 0$ and $b \neq 0$. Then

$$p(z_0 + \varepsilon\omega) = a\Big(1 - \Big|\frac{b}{a}\Big|\varepsilon^k\Big) + (\varepsilon\omega)^{k+1} r(\varepsilon\omega), \tag{A.1.12}$$

with $r(\zeta)$ as in (A.1.9), which contradicts (A.1.6) for $\varepsilon > 0$ small enough. Thus (A.1.7) is impossible. This proves Lemma A.1.2, hence Theorem A.1.1. □

Now that we have shown that $p(z)$ in (A.1.1) must have one root, we can show it has $n$ roots (counting multiplicity).

**Proposition A.1.3.** *For a polynomial $p(z)$ of degree $n$, as in* (A.1.1)*, there exist $r_1, \dots, r_n \in \mathbb{C}$ such that*

$$p(z) = a_n(z - r_1) \cdots (z - r_n). \tag{A.1.13}$$

**Proof.** We have shown that $p(z)$ has one root; call it $r_1$. Dividing $p(z)$ by $z - r_1$, we have

$$p(z) = (z - r_1)\tilde{p}(z) + q, \tag{A.1.14}$$

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 (A.1.14) yields $q = 0$, i.e.,

$$p(z) = (z - r_1)\tilde{p}(z). \tag{A.1.15}$$

Since $\tilde{p}(z)$ is a polynomial of degree $n - 1$, the result (A.1.13) follows by induction on $n$. □

Remark 1. The numbers $r_j,\ 1 \le j \le n$, in (A.1.13) are the roots of $p(z)$. If $k$ of them coincide (say with $r_\ell$), we say $r_\ell$ is a root of multiplicity $k$. If $r_\ell$ is distinct from $r_j$ for all $j \neq \ell$, we say $r_\ell$ is a simple root.

Remark 2. In complex analysis texts one can find proofs of the fundamental theorem of algebra that are a little shorter than the proof given above, but that depend on more advanced techniques.

## A.2. Averaging rotations

Suppose $A_1, \dots, A_N$ are rotation matrices on $n$-dimensional Euclidean space $\mathbb{R}^n$, i.e., $A_j \in SO(n)$. We want to identify an element of $SO(n)$ that represents an "average" of these rotations $A_j$.

Part of our task is to produce a reasonable definition of "average" in this context. If we simply average over all of $M(n, \mathbb{R})$, we would have

$$\frac{1}{N}\overline{A}, \quad \overline{A} = A_1 + \cdots + A_N. \tag{A.2.1}$$

However, typically this element of $M(n, \mathbb{R})$ does not belong to $SO(n)$. To formulate a notion of average that will work for averaging over sets that are not linear spaces, we start with the observation that $\overline{A}/N$ is obtained as the minimizer of

$$\psi(X) = \sum_{j=1}^{N} \|X - A_j\|^2, \tag{A.2.2}$$

if we minimize over all $X \in M(n, \mathbb{R})$. Here we take the Hilbert-Schmidt norm,

$$\|T\|^2 = \mathrm{Tr}\ T^*T. \tag{A.2.3}$$

Guided by this, we make the following

**Definition.** Given $A_1, \dots, A_N \in SO(n)$, an element $X \in SO(n)$ that minimizes (A.2.2) over $SO(n)$ is said to be an R-average of $\{A_j : 1 \le j \le N\}$.

Certainly (A.2.2) has a minimum, over $SO(n)$, though the minimizer might or might not be unique, as we will see in examples below. If the minimizer is unique, we say it is *the* R-average.

We proceed to establish some properties of the R-average. We show that it is determined by $\overline{A} = A_1 + \cdots + A_N$. How it is determined depends on whether the determinant of $\overline{A}$ is positive, negative, or zero. We will give a number of examples of collections of elements of $SO(3)$ and compute their R-averages.

**The R-average**

We tackle the problem of computing R-averages of sets of elements of $SO(n)$. To analyze (A.2.2), write

$$\begin{aligned} \|X - A_j\|^2 &= \mathrm{Tr}\,(X^* - A_j^*)(X - A_j) \\ &= \mathrm{Tr}\,(X^*X - X^*A_j - A_j^*X + A_j^*A_j) \\ &= 2n - 2\ \mathrm{Tr}\ A_j^*X, \end{aligned} \tag{A.2.4}$$

using $X^*X = A_j^*A_j = I$. Hence we have

$$\psi(X) = 2nN - 2\ \mathrm{Tr}\ \overline{A}^*X, \quad \overline{A} = A_1 + \cdots + A_N. \tag{A.2.5}$$

Thus the problem of minimizing (A.2.2) over $X \in SO(n)$ is equivalent to the following problem:

$$\text{Maximize} \quad \mathrm{Tr}\ \overline{A}^*X \quad \text{over} \quad X \in SO(n). \tag{A.2.6}$$

We break the analysis into several cases:

Case I. $\overline{A}$ is invertible.
Take the polar decomposition of $\overline{A}$:

$$\overline{A} = UP, \tag{A.2.7}$$

with $U$ orthogonal and $P$ positive definite. This polar decomposition is unique; in particular $P = (\overline{A}^*\overline{A})^{1/2}$. Then we are considering

$$\mathrm{Tr}\ \overline{A}^*X = \mathrm{Tr}\ PU^*X. \tag{A.2.8}$$

Case IA. $\det \overline{A} > 0$.
In this case $U \in SO(n)$, so $U^*X$ runs over $SO(n)$ in (A.2.8) as $X$ runs over $SO(n)$, so the following result is useful.

**Lemma A.2.1.** *If $P$ is positive-definite on $\mathbb{R}^n$ and $V \in SO(n)$, then*

$$\mathrm{Tr}\ PV \le \mathrm{Tr}\ P, \tag{A.2.9}$$

*with identity if and only if $V = I$.*

**Proof.** Let $v_1, \dots, v_n$ be an orthonormal basis of $\mathbb{R}^n$, consisting of eigenvectors of $P$, $Pv_j = \lambda_j v_j$, $\lambda_j > 0$. Then

$$\mathrm{Tr}\ PV = \sum_j (PVv_j, v_j) = \sum_j \lambda_j (Vv_j, v_j). \tag{A.2.10}$$

We have $(Vv_j, v_j) \le 1$, with equality if and only if $Vv_j = v_j$, given $V \in SO(n)$, and this proves the lemma. □

**Corollary A.2.2.** *In Case IA, the minimum for* (A.2.2) *over $X \in SO(n)$ is achieved at one point:*

$$X = U, \tag{A.2.11}$$

*with $U \in SO(n)$ given by the polar decomposition* (A.2.7).

Case IB. det $\overline{A} < 0$.
In this case $U$ in (A.2.7) is orthogonal but det $U = -1$; we say $U \in O^-(n)$. Then $U^*X$ runs over $O^-(n)$ in (A.2.8) as $X$ runs over $SO(n)$, so the following result is useful.

**Lemma A.2.3.** *If $P$ is positive-definite on $\mathbb{R}^n$, with eigenvalues satisfying $0 < \lambda_1 \le \lambda_2 \le \cdots \le \lambda_n$, and $V \in O^-(n)$, then*

$$\text{Tr } PV \le \lambda_n + \cdots + \lambda_2 - \lambda_1. \tag{A.2.12}$$

*If $\{v_j\}$ is an orthonormal basis such that $Pv_j = \lambda_j v_j$, the maximum is achieved when $Vv_j = v_j$ for $j \ge 2$ and $Vv_1 = -v_1$.*

**Proof.** First suppose $V$ is stationary for $\varphi : O^-(n) \to \mathbb{R}$, $\varphi(X) = \text{Tr } PX$. Differentiating $\varphi(Ve^{sZ})$ at $s = 0$, we deduce that Tr $PVZ = 0$ for all $Z \in \text{Skew}(n)$, hence $PV$ is symmetric, so $PV = V^*P$. Hence $PV^2 = V^*PV$. In particular Tr $PV^2 =$ Tr $P$, and $V^2 \in SO(n)$, so Lemma A.2.1 implies $V^2 = I$. Hence $V^* = V$, so $PV = VP$.

The proof of Lemma A.2.3 is now straightforward if $P$ has only simple eigenvalues. In such a case $Vv_j = \pm v_j$, and the maximum of Tr $PV$ is assumed only for $V$ described in the lemma.

A similarly straightforward argument extends the treatment to the case where $P$ has multiple eigenvalues. We describe the result. Suppose the distinct eigenvalues of $P$ are $\lambda_1 = \mu_1 < \cdots < \mu_k = \lambda_n$. Let $E_j$ be the $\mu_j$-eigenspace. Then $V : E_j \to E_j$ for each $j$. For $j > 1$, $V|_{E_j}$ is the identity if (A.2.12) is maximized, and $V|_{E_1}$ must be a reflection across some hyperplane in $E_1$, so it has one eigenvalue equal to $-1$. □

For $\mu > 1$, the set of $(\mu - 1)$-dimensional linear subspaces of $\mathbb{R}^\mu$ is called the $(\mu - 1)$-dimensional real projective space, and is denoted $\mathbb{RP}^{\mu-1}$.

**Corollary A.2.4.** *In Case IB, the minimum for* (A.2.2) *over $X \in SO(n)$ is achieved at*

$$X = UV, \tag{A.2.13}$$

*where $U \in O^-(n)$ is given by the polar decomposition* (A.2.7) *and $V \in O^-(n)$ is the identity on $E_j$ for all $j > 1$ and an orthogonal reflection on $E_1$. Thus the minimizer $X$ is unique if dim $E_1 = 1$. If dim $E_1 = \mu > 1$, the set of minimizers for* (A.2.2) *is in one-to-one correspondence with $\mathbb{RP}^{\mu-1}$.*

Case II. $\overline{A}$ is not invertible.
We can still write

$$\overline{A} = UP. \tag{A.2.14}$$

This time $P = (\overline{A}^*\overline{A})^{1/2}$ is positive semi-definite, with null space $\mathcal{N}(P) = \mathcal{N}(\overline{A})$. The factor $U$ is a uniquely defined orthogonal linear map from the range $\mathcal{R}(P)$ to $\mathcal{R}(\overline{A})$. We can extend $U$ to provide an orthogonal linear map from $\mathcal{N}(P) = \mathcal{R}(P)^\perp$ to $\mathcal{R}(\overline{A})^\perp$. Several such choices can be made. Make one choice, and arrange that $U \in SO(n)$. Again we are considering a function of the form (A.2.8); the only difference is that now $P$ is only positive semi-definite. Hence the following lemma is useful.

**Lemma A.2.5.** *If $P$ is positive semi-definite on $\mathbb{R}^n$ and $V \in SO(n)$, then*

$$\text{Tr } PV \le \text{Tr } P, \tag{A.2.15}$$

*with equality if and only if $V|_{\mathcal{R}(P)} = I$.*

The proof is a simple analogue of the proof of Lemma A.2.1.

**Corollary A.2.6.** *In Case II, the minimum for* (A.2.2) *over $X \in SO(n)$ is achieved at*

$$X = UV, \tag{A.2.16}$$

*where $U \in SO(n)$ is as described above for* (A.2.14) *and $V$ is any element of $SO(n)$ such that $V = I$ on $\mathcal{R}(P)$. If dim $\mathcal{N}(\overline{A}) = 1$, then necessarily $V = I$ on $\mathbb{R}^n$ and $X$ is unique. If dim $\mathcal{N}(\overline{A}) = \mu > 1$ then the set of minimizers for* (A.2.2) *is in one-to-one correspondence with $SO(\mu)$.*

Remark. While the analysis above includes cases for which the R-average is not unique, we mention that this situation has probability zero in the set of random collections $\{A_1, \dots, A_N\} \subset SO(n)$.

### Examples

We illustrate the results established above with some examples. Let $Q$ be the unit cube in $\mathbb{R}^3$, centered at the origin, with edges parallel to the coordinate axes. Let $G$ be the group of rotations of $\mathbb{R}^3$ preserving $Q$. It is known that $G$ is a group of order 24, isomorphic to the symmetric group $S_4$. Furthermore, $G$ is generated by rotations $R_{xy}, R_{yz}$, and $R_{zx}$, where $R_{xy}$ is counterclockwise rotation by 90° in the $xy$-plane, etc. We will select various subsets of $G$.

Example 1. Let $A_1 = R_{xy},\ A_2 = R_{yz},\ A_3 = R_{zx}$. Then

$$\overline{A} = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix}, \quad \det \overline{A} = 4. \tag{A.2.17}$$

A calculation gives $\overline{A} = UP$ with

$$P = \frac{1}{3}\begin{pmatrix} 5 & -1 & -1 \\ -1 & 5 & -1 \\ -1 & -1 & 5 \end{pmatrix}, \quad U = \frac{1}{3}\begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix}. \tag{A.2.18}$$

This element $U \in SO(3)$ is the unique minimizer for (A.2.2), so $U$ is the R-average of $A_1, A_2, A_3$.

Example 2. Let $A_1, \dots, A_{24}$ enumerate all the elements of the group $G$ described above. We claim that

$$\overline{A} = A_1 + \cdots + A_{24} = 0. \tag{A.2.19}$$

Indeed, for each $\ell$, $\{A_\ell A_j : 1 \le j \le 24\} = G$, so $A_\ell \overline{A} = \overline{A}$. Hence $v \in \mathbb{R}^3, w = \overline{A}v \Rightarrow A_\ell w = w$ for each $A_\ell$, in particuler for $A_1, A_2, A_3$ in Example 1. This forces $w = 0$.

In this case, the function $\psi : SO(3) \to \mathbb{R}$ defined by (A.2.2) is constant, and hence achieves its minimum at each point of $SO(3)$. Thus the R-average of this set of rotations is completely arbitrary, an expression that this set of rotations is evenly distributed in $SO(3)$.

Example 3. Let $A_1, \dots, A_{23}$ enumerate all the elements of $G$ except the identity. Then

$$\overline{A} = A_1 + \cdots + A_{23} = -I, \quad \det \overline{A} = -1. \tag{A.2.20}$$

We hence have $\overline{A} = UP$ with $P = I,\ U = -I$. Corollary A.2.4 applies and we see that the minimum for (A.2.2) over $X \in SO(3)$ is achieved precisely when

$$X = -R, \tag{A.2.21}$$

where $R$ is an arbitrary reflection across some 2D plane in $\mathbb{R}^3$. This set of minimizers is in one-to-one correspondence with $\mathbb{RP}^2$.

Example 4. Let $A_1, \dots, A_{21}$ enumerate all the elements of $G$ except the three rotations $R_{xy}, R_{yz}$, and $R_{zx}$ considered in Example 1. Hence (by (A.2.17) and (A.2.19)),

$$\overline{A} = A_1 + \cdots + A_{21} = -\begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix}, \quad \det \overline{A} = -4. \tag{A.2.22}$$

(Anti)parallel to (A.2.18), we have $\overline{A} = UP$ with $P$ as in (A.2.18) and

$$U = -\frac{1}{3}\begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix} \in O^-(3). \tag{A.2.23}$$

We note that the eigenvalues of $P$ are $\lambda_1 = 1, \lambda_2 = 2, \lambda_3 = 2$; in particular

$$P(e_1 + e_2 + e_3) = e_1 + e_2 + e_3, \tag{A.2.24}$$

where $\{e_j\}$ is the standard orthonormal basis of $\mathbb{R}^3$. Corollary A.2.4 applies and we see that (A.2.2) has the unique minimizer,

$$X = UV, \tag{A.2.25}$$

where $U$ is as in (A.2.7) and $V \in O^-(3)$ has the property

$$V(e_1 + e_2 + e_3) = -(e_1 + e_2 + e_3), \tag{A.2.26}$$

with $V = I$ on the orthogonal complement of the span of this vector. In other words,

$$V = \frac{1}{3}\begin{pmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{pmatrix}, \tag{A.2.27}$$

and hence the R-average in this case is

$$X = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}. \tag{A.2.28}$$

**Covariance**

We mention a covariance property of the R-average. Namely, let

$$A_1, \dots, A_N \in SO(n),$$

take $U \in SO(n)$, and set $B_j = UA_j \in SO(n)$. Then $X$ is an R-average of $A_1, \dots, A_N$ if and only if $UX$ is an R-average of $B_1, \dots, B_N$. This is an obvious consequence of the definition in terms of (A.2.2). Similarly the R-average is covariant with respect to $A_j \mapsto A_j U$ for $U \in SO(n)$, and with respect to $A_j \mapsto VA_jW$, for $V, W \in O^-(n)$.

## A.3. Groups

In addition to fields and vector spaces, and more generally rings and modules, discussed in the body of the text, there have appeared objects with another algebraic structure, that of a *group*, which we briefly discuss in this appendix. By definition a group is a set $G$, endowed with an operation of multiplication; that is, given $a, b \in G$, then $ab$ is defined in $G$. The following laws have to hold, for all $a, b, c \in G$:

$$\text{(A.3.1)} \qquad \text{Associative law} \ : \ (ab)c = a(bc),$$

$$\text{(A.3.2)} \qquad \text{Identity element} \ : \ \exists\, e \in G, \ ea = ae = a,$$

$$\text{(A.3.3)} \qquad \text{Inverse} \ : \ \exists\, a^{-1} \in G, \ a^{-1}a = aa^{-1} = e.$$

If, in addition, we have

$$\text{(A.3.4)} \qquad ab = ba, \quad \forall\, a, b \in G,$$

we say $G$ is a *commutative group* (also called an *Abelian group*). We mention that inverses have to be unique. Indeed, if $a \in G$ has a left inverse $b$ and a right inverse $b'$, i.e., $ba = e, \ ab' = e$, then we have

$$\text{(A.3.5)} \qquad \begin{aligned} b(ab') &= be = b, \quad \text{and} \\ (ba)b' &= eb' = b', \end{aligned}$$

but the two left sides are equal, by (A.3.1), so $b = b'$. The reader can also verify that if $e$ and $e' \in G$ both satisfy (A.3.2), then $e = e'$ (consider $ee'$).

A master source of groups arises as follows. Let $X$ be a set, and let $\Pi(X)$ denote the set of all maps

$$\text{(A.3.6)} \qquad \varphi : X \longrightarrow X \ \text{ that are ont-to-one and onto.}$$

We define the group operation by composition: $\varphi\psi(x) = \varphi(\psi(x))$. Then (A.3.1)–(A.3.3) hold, with $e \in \Pi(X)$ the identity map, $e(x) \equiv x$, and $\varphi^{-1}$ the mapping inverse to $\varphi$. When $X = \{1, \dots, n\}$, this group is the *permutation group* $S_n$, introduced in (1.5.20). Also one calls $S_n$ the *symmetric group* on $n$ symbols.

If $H$ is a subset of $\Pi(X)$ having the property that

$$\text{(A.3.7)} \qquad e \in H, \quad \text{and} \ \ a, b \in H \Longrightarrow a^{-1}, \, ab \in H,$$

then $H$ is a group. More generally, if $G$ is a group and $H \subset G$ satisfies (A.3.7), then $H$ is a group. We say $H$ is a *subgroup* of $G$.

A number of special sets of matrices arising in the text are groups. These include

$$\text{(A.3.8)} \qquad G\ell(n, \mathbb{F}),$$

the group of invertible $n \times n$ matrices (with coefficients in $\mathbb{F}$), introduced near the end of §1.5, the subgroups

$$U(n), \quad SU(n) \tag{A.3.9}$$

of $G\ell(n, \mathbb{C})$, and the subgroups

$$O(n), \quad SO(n) \tag{A.3.10}$$

of $G\ell(n, \mathbb{R})$, introduced in §3.4. When $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, $G\ell(n, \mathbb{F})$ is an open subset of the vector space $M(n, \mathbb{F})$, and the group operations of multiplication, $G\ell(n, \mathbb{F}) \times G\ell(n, \mathbb{F}) \to G\ell(n, \mathbb{F})$ and inverse $G\ell(n, \mathbb{F}) \to G\ell(n, \mathbb{F})$ can be seen to be smooth maps. The groups (A.3.9)–(A.3.10) are smooth surfaces in $M(n, \mathbb{C})$, and $M(n, \mathbb{R})$, respectively, and the group operations are also smooth. Groups with such structure are called *Lie groups*. For this, methods of multidimensional calculus are available to produce a rich theory. One can consult [**25**] for material on this.

Most of the groups listed above are not commutative. If $n \geq 3$, $S_n$ is not commutative. If $n \geq 2$, none of the groups listed in (A.3.8)–(A.3.10) are commutative, except $SO(2)$. The case $n = 1$ of (A.3.8) is also denoted

$$\mathbb{F}^* = \{a \in \mathbb{F} : a \neq 0\}. \tag{A.3.11}$$

For any field $\mathbb{F}$, $\mathbb{F}^*$ is a commutative group. Whenever $\mathcal{R}$ is a ring with unit,

$$\mathcal{R}^* = \{a \in \mathbb{R} : a \text{ is invertible}\} \tag{A.3.12}$$

is a group (typically not commutative, if $\mathcal{R}$ is not a commutative ring). When $\mathcal{R} = M(n, \mathbb{F})$, $\mathcal{R}^*$ becomes (A.3.8).

When $G$ is commutative, one sometimes (but not always) wants to write the group operation as $a + b$, rather than $ab$. Then we call $G$ a commutative additive group. This concept was introduced in §6.1, and we recall that fields, and more generally rings, are commutative additive groups, endowed with an additional multiplicative structure.

If $G$ and $K$ are groups, a map $\varphi : G \to K$ is called a (group) *homomorphism* provided it preserves the group operations, i.e.,

$$a, b \in G \Longrightarrow \varphi(ab) = \varphi(a)\varphi(b). \quad \varphi(e) = e', \tag{A.3.13}$$

where $e'$ is the identity element of $K$. The second condition is actually redundant, since $\varphi(e) = \varphi(e \cdot e) = \varphi(e)\varphi(e)$ forces $\varphi(e) = e'$. Note that $\varphi(a^{-1}) = \varphi(a)^{-1}$, since $\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e)$. Examples of group homomorphisms include

$$\det : G\ell(n, \mathbb{F}) \longrightarrow \mathbb{F}^*, \tag{A.3.14}$$

arising from Proposition 1.5.1, thanks to Propositions 1.5.3 and 1.5.6, and

$$\text{sgn} : S_n \longrightarrow \{1, -1\}, \tag{A.3.15}$$

introduced in (1.5.23), thanks to (1.5.24)–(1.5.28).

A group homomorphism $\varphi : G \to K$ yields a special subgroup of $G$,

$$\operatorname{Ker}\varphi = \{a \in G : \varphi(a) = e\}. \tag{A.3.16}$$

In such a case, $\operatorname{Ker}\varphi$ has the property of being a *normal subgroup* of $G$, where a subgroup $H$ of $G$ is said to be a normal subgroup provided

$$h \in H,\ g \in G \Longrightarrow g^{-1}hg \in H. \tag{A.3.17}$$

In the cases (A.3.14) and (A.3.15), these subgroups are

$$\begin{gathered} S\ell(n,\mathbb{F}) = \{A \in G\ell(n,\mathbb{F}) : \det A = 1\}, \quad \text{and} \\ A_n = \{\tau \in S_n : \operatorname{sgn}\tau = 1\}. \end{gathered} \tag{A.3.18}$$

The group $A_n$ is called the *alternating group.*

A group homomorphism

$$\varphi : G \longrightarrow G\ell(n,\mathbb{F}) \tag{A.3.19}$$

is called a *representation* of $G$ on the vector space $\mathbb{F}^n$. More generally (formally, if not substantially) if $V$ is an $n$-dimensional vector space over $\mathbb{F}$, we denote by $G\ell(V)$ the group of invertible linear transformations on $V$, and call a homomorphism

$$\varphi : G \longrightarrow G\ell(V) \tag{A.3.20}$$

a representation of $G$ on $V$. One way these representations arise is as follows. Suppose $X$ is a set, with $n$ elements, and $G$ acts on $X$, i.e., there is a group homomorphism $G \to \Pi(X)$. Let $V$ be the space of all functions $f : X \to \mathbb{F}$, which is an $n$-dimensional vector space over $\mathbb{F}$. Then we define a representation $\pi$ of $G$ on $V$ by

$$\pi(a)f(x) = f(a^{-1}x), \quad a \in G,\ x \in X,\ f : X \to \mathbb{F}. \tag{A.3.21}$$

The study of representations of groups provides fertile ground for use of linear algebra. We whet the reader's appetite with one example. If $\varphi$ and $\psi$ are representations of $G$ on finite dimensional vector spaces $V$ and $W$, respectively, there is a tensor product representation $\varphi \otimes \psi$ of $G$ on $V \otimes W$, satisfying

$$\varphi \otimes \psi(g)(v \otimes w) = \varphi(g)v \otimes \psi(g)w, \quad g \in G,\ v \in V,\ w \in W. \tag{A.3.22}$$

For further material on group representations, we refer to [**25**], [**20**], and Chapter 18 of [**11**].

If $G$ is a group and $H \subset G$ a subgroup, we define the *coset space* $G/H$ as follows. An element of $G/H$ consists of an equivalence class of elements of $G$, with equivalence relation

$$g \sim g' \Longrightarrow g' = gh \ \text{ for some } \ h \in H. \tag{A.3.23}$$

Equivalently, an element of $G/H$ is a subset of $G$ of the form

$$gH = \{gh : h \in H\}, \tag{A.3.24}$$

for some $g \in G$. Note that $gH = g'H$ if and only if (E.23) holds. There is a natural action of $G$ on the space $X = G/H$, namely

$$g \cdot (g'H) = gg'H. \tag{A.3.25}$$

We see that this action is transitive, where generally the action of $G$ on a set $X$ is *transitive* if and only if

$$\forall\, x, x \in X, \quad gx = x' \ \text{ for some } \ g \in G. \tag{A.3.26}$$

The coset space $G/H$ gets a group structure provided $H$ is normal, i.e., provided (A.3.17) holds. Then we can define

$$(gH)(g'H) = gg'H, \tag{A.3.27}$$

and use (A.3.17) to show that this puts a well defined group structure on $G/H$. In such a case, we get a group homomorphism

$$\pi : G \longrightarrow G/H, \quad \pi(g) = gH, \tag{A.3.28}$$

and

$$\operatorname{Ker} \pi = H. \tag{A.3.29}$$

Let us look further at transitive group actions. Whenever a group $G$ acts transitively on $X$, we can fix $p \in X$ and set

$$H = \{g \in G : g \cdot p = p\}. \tag{A.3.30}$$

Then $H$ is a subgroup of $G$, and the map

$$F : G/H \longrightarrow X, \quad F(gH) = g \cdot p, \tag{A.3.31}$$

is well defined, one-to-one, and onto. As an example of this, take

$$G = SO(n), \quad X = S^{n-1}, \quad p = e_n, \tag{A.3.32}$$

where $S^{n-1} = \{x \in \mathbb{R}^n : |x| = 1\}$ is the unit sphere and $e_n$ is the $n$th standard basis vector in $\mathbb{R}^n$. The group $SO(n)$ acts transitively on $S^{n-1}$, and one can show that the set of elements of $SO(n)$ that fix $e_n$ consists of those matrices

$$\begin{pmatrix} h & \\ & 1 \end{pmatrix}, \quad h \in SO(n-1).$$

As another example, take

$$G = S_n, \quad X = \{1, \dots, n\}, \quad p = n. \tag{A.3.33}$$

Then the set of elements of $S_n$ that fix $p$ consists of permutations of $\{1, \dots, n-1\}$, and we get a subgroup $H \approx S_{n-1}$. For other transitive actions of $S_n$, one can fix $k \in \mathbb{N}$, $1 < k < n$, and consider

$$X_{k,n} = \text{ collection of all subsets of } \{1, \dots, n\} \text{ with } k \text{ elements.} \tag{A.3.34}$$

Then $S_n$ naturally acts on each set $X_{k,n}$, and each such action is transitive. Note that the number of elements of $X_{k,n}$ is given by the binomial coefficient

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{A.3.35}$$

The procedure (A.3.27) gives a representation of $S_n$ on $\mathbb{R}^{\binom{n}{k}}$. In such a case, if $p = \{1, \dots, k\}$, a permutation $\tau \in S_n$ fixes $p$ under this action if and only if $\tau$ acts as a permutation on $\{1, \dots k\}$ and as a permutation on $\{k+1, \dots, n\}$. Thus the subgroup $H$ of $S_n$ fixing such $p$ satisfies

$$H \approx S_k \times S_{n-k}, \tag{A.3.36}$$

where, if $H_1$ and $H_2$ are groups, $H_1 \times H_2$ consists of pairs $(h_1, h_2)$, $h_j \in H_j$, with group law $(h_1, h_2) \cdot (h_1', h_2') = (h_1 h_1', h_2 h_2')$.

Groups we have discussed above fall into two categories. One consists of groups such as those listed in (A.3.8)–(A.3.10), called Lie groups. Another consists of *finite groups*, i.e., groups with a finite number of elements. We end this appendix with some comments on finite groups, centered around the notion of *order*. If $G$ is a finite group, set $o(G)$ equal to the number of elements of $G$. More generally, if $X$ is a finite set, set

$$o(X) = \text{ number of elements of } X. \tag{A.3.37}$$

In the group setting we have, for example,

$$o(S_n) = n!, \quad o(\mathbb{Z}/(n)) = n, \quad G = (\mathbb{Z}/(p))^* \Rightarrow o(G) = p-1, \tag{A.3.38}$$

where in the second case $\mathbb{Z}/(n)$ is an additive commutative group, and the third case is a special case of (A.3.11). The following is a simple but powerful classical observation.

Let $G$ be a finite group and $H$ a subgroup. The description of $G/H$ given above shows that $G$ is partitioned into $o(G/H)$ cosets $gH$, and each coset has $o(H)$ elements. Hence

$$o(G) = o(H) \cdot o(G/H). \tag{A.3.39}$$

In particular,

$$H \text{ subgroup of } G \Longrightarrow o(H) \text{ divides } o(G). \tag{A.3.40}$$

This innocent-looking observation has lots of interesting consequences.

For example, gien $g \in G$, $g \neq e$, let

$$\Gamma(g) = \{g^k : k \in \mathbb{Z}\} \tag{A.3.41}$$

be the subgroup of $G$ generated by $g$. Since $G$ is finite, so is $\Gamma(g)$, so there exist $k, \ell \in \mathbb{Z}$ such that $g^k = g^\ell$, hence there exists $j = k - \ell \in \mathbb{Z}$ such that $g_j = e$. It is clear that the set of such $j$ is a subgroup of $\mathbb{Z}$ (hence an ideal in $\mathbb{Z}$), so it is generated by its smallest positive element, call it $\gamma$. Then

$$\Gamma(g) = \{e, g, \dots, g^{\gamma-1}\}, \quad \text{so} \;\; o(\Gamma(g)) = \gamma, \;\; \text{and} \;\; g^\gamma = e. \tag{A.3.42}$$

It follows that $g^{j\gamma} = e$ for all $j \in \mathbb{Z}$. By (A.3.40), $\gamma$ divides $o(G)$. This proves the following.

**Proposition A.3.1.** *If $G$ is a finite group and $g \in G$, then*

$$k = o(G) \Longrightarrow g^k = e. \tag{A.3.43}$$

An interesting corollary of this result arises for

$$G = (\mathbb{Z}/(p))^*, \quad o(G) = p - 1. \tag{A.3.44}$$

Then Proposition A.3.1 implies that

$$a^{p-1} = 1 \mod p, \tag{A.3.45}$$

when $p$ is a prime and $a \neq 0$ mod $p$. See Exercise 3 of §6.1 (addressing (6.1.27)) for an application of this result. More generally, one can consider

$$G = (\mathbb{Z}/(n))^*, \tag{A.3.46}$$

whose elements consist of (equivalence classes mod $n$ of) integers $k$ such that $\gcd(k, n) = 1$. Applying Proposition A.3.1 to (A.3.46) yields a generalization of (A.3.45), whose formulation we leave to the reader.

The identity (A.3.45) also plays an important role in a certain type of "public key encryption." We end this appendix with a brief description of how this works, filling in the mathematical details of a nontechnical discussion given in Chapter 9 of [**14**]. The ingredients consist of the following

A. Secret data: $p, q$ (distinct large primes) $\beta \in \mathbb{N}$.

B. Public data: $pq$, $\alpha \in \mathbb{N}$ (the "key").

C. Message: $a \in \{1, \dots, pq\}$.

D. Encrypted message: $b = a^\alpha$ mod $pq$.

E. Decrypted message: $b^\beta = a$ mod $pq$.

The secret number $\beta$ has the crucial property that

$$\alpha\beta = 1 \bmod (p-1)(q-1). \tag{A.3.47}$$

The identity of $\beta$ could be deduced easily from knowledge of $p, q$ and $\alpha$, but not so easily from the knowledge merely of $pq$ and $\alpha$ (assuming that it is hard to factor $pq$).

Here is how a person who knows the public data encrypts a message and sends it to a recipient who knows the secret data. Let us say Bill knows the secret data and lots of people know the public data. Joe wants to send a message (digitized as $a$) to Bill. Joe knows the public data. (So do the members of the nefarious international spy organization, Nosy Snoopers, Inc., from whom Joe wants to shield the message.) Joe takes the message $a$ and uses the public data to produce the encrypted message $b$. Then Joe sends the message $b$ to Bill. There is a serious possibility that nosy snoopers will intercept this encrypted message.

Bill uses the secret data to convert $b$ to $a$, thus decrypting the secret message. To accomplish this decryption, Bill makes use of the secret number $\beta$, which is not known to Joe, nor to the nosy snoopers (unless they are capable of factoring the number $pq$ into its prime factors). As indicated above, Bill computes $b^\beta$ mod $pq$, and, so we assert, this produces the original message.

The mathematical result behind how this works is the following.

**Theorem A.3.2.** *Let $p$ and $q$ be distinct primes. Assume that $\alpha$ and $\beta$ are two positive integers satisfying* (A.3.47)*. Then*

$$a^{\alpha\beta} = a \quad \bmod pq, \quad \forall\, a \in \mathbb{Z}. \tag{A.3.48}$$

The key step in the proof is the following.

**Lemma A.3.3.** *In the setting of Theorem A.3.2,*

$$a^{(p-1)(q-1)}a = a \quad \bmod pq. \tag{A.3.49}$$

**Proof.** As in (A.3.45), we have

$$a^{p-1} = 1 \bmod p, \quad \text{if } \ a \neq 0 \bmod p, \tag{A.3.50}$$

so

$$a^{(p-1)(q-1)} = 1 \bmod p, \quad \text{if } \ a \neq 0 \bmod p. \tag{A.3.51}$$

Thus

$$a^{(p-1)(q-1)}a = a \bmod p, \quad \forall\, a \in \mathbb{Z}, \tag{A.3.52}$$

since this holds trivially if $a = 0 \bmod p$, and otherwise follows from (A.3.51). Similarly

$$a^{(p-1)(q-1)}a = a \bmod q, \tag{A.3.53}$$

and together (A.3.52) and (A.3.53) imply (A.3.49). □

Having (A.3.49), we can multiply repeatedly by $a^{(p-1)(q-1)}$, and obtain

$$a^{m(p-1)(q-1)+1} = a \bmod pq, \quad \forall\, a \in \mathbb{Z}, \tag{A.3.54}$$

whenever $m$ is a positive integer. This yields (A.3.48), proving Theorem A.3.2.

The success of this as an encryption device rests on the observation that, while the task of producing $k$-digit primes $p$ and $q$ (say with the initial $k/2$ digits arbitrarily specified) increases in complexity with $k$, the difficulty of the task of factoring the product $pq$ of two such into its prime factors increases much faster with $k$. (Warning: this is an observation, not a theorem.) Anyway, for this scheme to work, one wants $p$ and $q$ to be fairly large (say with several hundred digits), and hence $\alpha$ and $\beta$ need to be fairly large. Hence one needs to take $a$ (having numerous digits) and raise it, mod $n = pq$, to quite a high power. This task is not as daunting as it might first appear. Indeed, to compute $a^\ell \bmod n$ with $\ell = 2^k$, one just needs to square $a \bmod n$ and do this squaring $k$ times. For more general $\ell \in \mathbb{N}$, take its dyadic expansion $\ell = 2^i + 2^j + \cdots + 2^k$ and follow your nose.

To be sure, producing such primes $p$ and $q$ as described above requires some effort. The Prime Number Theorem (cf. [**30**], §4.4) provides a rough guide to how large a string of integers one needs to search for primes. Regarding the task of finding a prime in such a string, the interested reader can look up items like "primality testing" on such sources as Wikipedia or Google.

We sign off here, and refer the reader to Chapter 1 of [**11**] and Chapter 6 of [**4**] for further material on finite groups.

## A.4. Finite fields and other algebraic field extensions

Certain subfields of $\mathbb{C}$ that are finite-dimensional vector spaces over $\mathbb{Q}$ have been considered in §6.1 (around (6.1.28)–(6.1.37)) and §6.2. Here we construct such finite extensions of a general field $\mathbb{F}$, and show how this construction yields a string of finite fields, when applied to $\mathbb{F} = \mathbb{F}_p = \mathbb{Z}/(p)$.

To start, let $\mathbb{F}$ be a field, and let $P \in \mathbb{F}[x]$, the polynomial ring, which, we recall, is a PID. Then $P$ generates an ideal $(P)$, and

$$\mathbb{F}[x]/(P) \tag{A.4.1}$$

is a ring. If $P(x) = a_n x^n + \cdots + a_0,\ n \ge 1,\ a_n \neq 0$, then $\mathbb{F}[x]/(P)$ is a vector space of dimension $n$ over $\mathbb{F}$. To state the following result on when $\mathbb{F}[x]/(P)$ is a field, we recall from §7.2 that $P \in \mathbb{F}[x]$ is said to be *irreducible* provided it has no factors in $\mathbb{F}[x]$ of positive degree $< \deg P$.

**Proposition A.4.1.** *If $P \in \mathbb{F}[x]$ is irreducible, then the ring $\mathbb{F}[x]/(P)$ is a field.*

**Proof.** By Proposition 7.2.4, if $\mathcal{R}$ is a PID and $P \in \mathcal{R}$ is prime, then $\mathcal{R}/(P)$ is a field. Furthermore, as noted just before Proposition 7.2.4, for such $\mathcal{R}$, an element $P \in \mathcal{R}$ is prime if and only if it is irreducible. □

We have the natural projection

$$\pi : \mathbb{F}[x] \longrightarrow \mathbb{F}[x]/(P) = \mathbb{F}_{(P)}, \tag{A.4.2}$$

the latter identity defining $\mathbb{F}_{(P)}$. The natural inclusion $\mathbb{F} \hookrightarrow \mathbb{F}[x]$, composed with $\pi$, yields an injective ring homomorphism

$$\iota : \mathbb{F} \hookrightarrow \mathbb{F}_{(P)}. \tag{A.4.3}$$

Loosely, we say $\mathbb{F} \subset \mathbb{F}_{(P)}$. Note that we can regard $P$ as an element of $\mathbb{F}_{(P)}[x]$, and

$$\xi = \pi(x) \Longrightarrow \xi \in \mathbb{F}_{(P)} \ \text{ and } \ P(\xi) = 0. \tag{A.4.4}$$

Thus $P$ is not irreducible in $\mathbb{F}_{(P)}[x]$. We have a factorization

$$P(x) = (x - \xi) P_1(x), \quad P_1 \in \mathbb{F}_{(P)}[x], \tag{A.4.5}$$

where $P_1$ is a polynomial of degree $n - 1$. If $n = 2$, then $P_1$ is linear, $P_1(x) = a_2(x - \eta)$, with $\eta \in \mathbb{F}_{(P)}$, and we have

$$P(x) = a_2(x - \xi)(x - \eta) = a_2(x^2 - (\xi + \eta)x + \xi\eta), \tag{A.4.6}$$

which implies

$$\xi + \eta,\ \xi\eta \in \mathbb{F}. \tag{A.4.7}$$

Note in particular that $\eta \neq \xi$, if $2 \neq 0$ in $\mathbb{F}$, since otherwise we would have $\xi = \eta \in \mathbb{F}$, and $P$ would not be irreducible in $\mathbb{F}[x]$. If $n = 3$, then either $P_1$ factors into linear factors or it is irreducible in $\mathbb{F}_{(P)}[x]$. If $n \geq 4$, $P_1$ might have neither property, but it will have a factorization $P_1 = P_{11} \cdots P_{1\mu}$ with $P_{1\nu}$ irreducible in $\mathbb{F}_{(P)}[x]$. Then the construction described above yields a field $\mathbb{F}_{(P)}[x]/(P_{11})$, and one can continue this process.

Let us consider some examples, starting with $x^2 + 1$, which is clearly irreducible over $\mathbb{Q}[x]$. The construction above via (A.4.1), with $\mathbb{F} = \mathbb{Q}$, yields a field isomorphic to $\mathbb{Q}[i]$, introduced in (6.1.30). On the other hand, the situation can differ for the field $\mathbb{F}_p = \mathbb{Z}/(p)$, when $p \in \mathbb{N}$ is a prime. For example,

$$x^2 + 1 = x^2 - 1 = (x + 1)(x - 1) = (x - 1)^2 \quad \text{in} \quad \mathbb{F}_2[x]. \tag{A.4.8}$$

More generally,

$$x^2 + 1 \;\text{ is irreducible in }\; \mathbb{F}_p[x] \Leftrightarrow -1 = b^2 \;\text{ has no solution }\; b \in \mathbb{F}_p, \tag{A.4.9}$$

and, still more generally, given $a \in \mathbb{Z}$,

$$x^2 - a \;\text{ is irreducible in }\; \mathbb{F}_p[x] \Longleftrightarrow a = b^2 \;\text{ has no solution }\; b \in \mathbb{F}_p. \tag{A.4.10}$$

For each prime $p \geq 3$ in $\mathbb{N}$, there exists $a \in \mathbb{Z}$ such that the condition for irreducibility in (A.4.10) is satisfied, and one then obtains via (A.4.1) a field that is a vector space of dimension 2 over $\mathbb{F}_p$, i.e., a field with $p^2$ elements. We denote such a field by $\mathbb{F}_{p^2}$. (Justification for this notation will be given below, in Proposition A.4.7.) For $p = 2$, there is no irreducible polynomial of the form (A.4.10), but

$$x^2 + x + 1 \;\text{ is irreducible in }\; \mathbb{F}_2[x], \tag{A.4.11}$$

since such $P(x)$ is nowhere vanishing on $\mathbb{F}_2$, so has no linear factors. Thus one can use this polynomial in (A.4.1) to construct a field (denoted $\mathbb{F}_4$) with 4 elements.

We next consider the cubic polynomial

$$x^3 - 3, \tag{A.4.12}$$

which is irreducible in $\mathbb{Q}[x]$. As a polynomial over $\mathbb{C}$, this has the three complex roots

$$r_1 = 3^{1/3}, \quad r_2 = 3^{1/3} e^{2\pi i/3}, \quad r_3 = 3^{1/3} e^{-2\pi i/3}. \tag{A.4.13}$$

In each case, the ring $\mathbb{Q}[r_j]$ is (by Proposition 6.1.3) a field, and one readily verifies that the field $\mathbb{Q}_{(x^3-3)}$ given by (A.4.1) is isomorphic to each of them. However, these are distinct subfields of $\mathbb{C}$. For example, $\mathbb{Q}[r_1] \subset \mathbb{R}$, but $\mathbb{Q}[r_2]$ and $\mathbb{Q}[r_3]$ do not have this property. Using

$$x^3 - r^3 = (x - r)(x^2 + rx + r^2), \tag{A.4.14}$$

we have

$$x^3 - 3 = (x - 3^{1/3})(x^2 + 3^{1/3}x + 3^{2/3}), \tag{A.4.15}$$

and

$$x^2 + 3^{1/3}x + 3^{2/3} \quad \text{is irreducible in} \quad \mathbb{Q}[3^{1/3}][x], \tag{A.4.16}$$

since this polynomial has no roots in $\mathbb{Q}[3^{1/3}]$ (the roots are $r_2$ and $r_3$, which are not in $\mathbb{R}$), and hence no linear factor in $\mathbb{Q}[3^{1/3}][x]$. Upon applying (A.4.1) with $\mathbb{F} = \mathbb{Q}[3^{1/3}]$ and $P(x)$ as in (A.4.16), one obtains a field isomorphic to

$$\mathbb{Q}(r_1, r_2, r_3) = \mathbb{Q}[3^{1/3}, e^{2\pi i/3}], \tag{A.4.17}$$

which has dimension 2 over $\mathbb{Q}[3^{1/3}]$, hence dimension 6 over $\mathbb{Q}$.

Moving on from $\mathbb{Q}$ to $\mathbb{F}_p$, and generalizing a bit, in parallel with (A.4.10), we see that if $p \in \mathbb{N}$ is a prime,

$$x^3 - a \ \text{ is irreducible in } \ \mathbb{F}_p[x] \Longleftrightarrow a = b^3 \ \text{ has no solution } \ b \in \mathbb{F}_p. \tag{A.4.18}$$

Now, there exists $a \in \mathbb{F}_p$ such that the condition (A.4.18) holds

$$\begin{aligned} &\Longleftrightarrow b \mapsto b^3, \text{mapping } \mathbb{F}_p \to \mathbb{F}_p, \text{ is not onto} \\ &\Longleftrightarrow \ \text{this map is not one-to-one} \\ &\Longleftrightarrow \exists\, \beta \neq 1 \ \text{ in } \mathbb{F}_p \text{ such that } \ \beta^3 = 1 \\ &\Longleftrightarrow x^2 + x + 1 \ \text{ has a root} \neq 1 \text{ in } \ \mathbb{F}_p, \end{aligned} \tag{A.4.19}$$

the last equivalence by $x^3 - 1 = (x - 1)(x^2 + x + 1)$. Note that the last condition clearly fails for $p = 2$ and 3. Also, for primes $p \geq 5$, the calculation $x^2 + x + 1 = (x + 1/2)^2 + 3/4$ shows that the last condition in (A.4.19) is

$$\Longleftrightarrow x^2 + 3 \ \text{ has a root in } \ \mathbb{F}_p. \tag{A.4.20}$$

Now there are infinitely many primes $p$ for which (A.4.20) holds and infinitely many for which it fails. Rather than pursue this further, we change course, and look for irreducible cubic polynomials in $\mathbb{F}_p[x]$ of the form

$$x^3 + x^2 - a, \quad a \in \mathbb{F}_p. \tag{A.4.21}$$

Note that $x^3 + x^2$ takes the same values at $x = 0$ and $x = -1$, so the map $b \mapsto b^3 + b^2$ is not one-to-one as a map $\mathbb{F}_p \to \mathbb{F}_p$, and hence it is not onto, so there exists $a \in \mathbb{F}_p$ such that $x^3 + x^2 - a$ has no root, hence no linear factor, and for such $a$, (A.4.21) is irreducible in $\mathbb{F}_p[x]$. Thus we get a field (denoted $\mathbb{F}_{p^3}$) with $p^3$ elements.

Now we consider the quartic polynomial

$$x^4 - 3, \tag{A.4.22}$$

which is irreducible in $\mathbb{Q}[x]$. As a polynomial over $\mathbb{C}$, this has the 4 complex roots

$$r_1 = 3^{1/4}, \quad r_2 = -3^{1/4}, \quad r_3 = 3^{1/4}i, \quad r_4 = -3^{1/4}i. \tag{A.4.23}$$

In each case, the ring $\mathbb{Q}[r_j]$ is a field, isomorphic to the field $\mathbb{Q}_{(x^4-3)}$ given via (A.4.1). However (compare the case (A.4.13)), we have two distinct subfields of $\mathbb{C}$, namely $\mathbb{Q}[r_1] = \mathbb{Q}[-r_1]$ (in $\mathbb{R}$) and $\mathbb{Q}[r_3] = \mathbb{Q}[r_4]$ (not in $\mathbb{R}$). Using

$$x^4 - r^4 = (x^2 - r^2)(x^2 + r^2) = (x + r)(x - r)(x^2 + r^2), \tag{A.4.24}$$

we have

$$x^4 - 3 = (x - 3^{1/4})(x + 3^{1/4})(x^2 + 3^{1/2}), \tag{A.4.25}$$

and (cf. (A.4.16))

$$x^2 + 3^{1/2} \ \text{ is irreducible in } \ \mathbb{Q}[3^{1/4}][x], \tag{A.4.26}$$

since this polynomial has no roots in $\mathbb{Q}[3^{1/4}]$, and hence no linear factor in $\mathbb{Q}[3^{1/4}][x]$. Upon applying (A.4.1) with $\mathbb{F} = \mathbb{Q}[3^{1/4}]$ and $P(x)$ as in (A.4.26), we obtain a field isomorphic to

$$\mathbb{Q}(r_1, r_2, r_3, r_4) = \mathbb{Q}[3^{1/4}, i], \tag{A.4.27}$$

which has dimension 2 over $\mathbb{Q}[3^{1/4}]$, and hence dimension 8 over $\mathbb{Q}$. Note that (A.4.25) gives an example of (A.4.5) with

$$P_1(x) = (x + 3^{1/4})(x^2 + 3^{1/2}), \tag{A.4.28}$$

which is neither irreducible nor a product of linear factors in $\mathbb{Q}[3^{1/4}][x]$.

Moving back to $\mathbb{F} = \mathbb{F}_p$, and generalizing (A.4.22) to $x^4 - a$, we are led to the following question, for a prime $p \in \mathbb{N}$:

$$\text{When is } x^4 - a \text{ irreducible in } \ \mathbb{F}_p[x]? \tag{A.4.29}$$

This question is more subtle than those treated in (A.4.10) and (A.4.18), since a polynomial of degree 4 can be reducible without containing a linear factor (it can have 2 factors, each quadratic). For example,

$$a = \beta^2 \bmod p \Longrightarrow x^4 - a = (x^2 + \beta)(x^2 - \beta) \text{ in } \mathbb{F}_p[x]. \tag{A.4.30}$$

(Then the issue of irreducibility of $x^2 \pm \beta$ in $\mathbb{F}_p[x]$ is settled as in (A.4.10).) More generally, expanding

$$(x^2 + \alpha x + \beta)(x^2 + \gamma x + \delta), \tag{A.4.31}$$

with coefficients in a field $\mathbb{F}$, we see (A.4.31) has the form $x^4 - a$, $a \in \mathbb{F}$, if and only if

$$\alpha + \gamma = 0, \quad \delta + \alpha\gamma + \beta = 0, \quad \alpha\delta + \beta\gamma = 0, \ \text{in } \mathbb{F}. \tag{A.4.32}$$

These conditions imply $\alpha(\beta - \delta) = 0$, hence either $\alpha = 0$ or $\beta = \delta$. The first case yields

$$(x^2 + \beta)(x^2 - \beta) = x^4 - a, \quad \text{with} \ \ a = \beta^2, \tag{A.4.33}$$

as in (A.4.30). The second case yields $\alpha^2 = 2\beta$, hence, if $\mathbb{F}$ does not have characteristic 2 (i.e., if $2 \neq 0$ in $\mathbb{F}$),

$$\Bigl(x^2 + \alpha x + \frac{\alpha^2}{2}\Bigr)\Bigl(x^2 - \alpha x + \frac{\alpha^2}{2}\Bigr) = x^4 - a, \quad \text{with} \ \ a = -\frac{\alpha^4}{4}. \tag{A.4.34}$$

We have the following conclusion.

**Proposition A.4.2.** *Given a field $\mathbb{F}$ whose characteristic is not 2, and given $a \in \mathbb{F}$, the polynomial $x^4 - a$ is reducible in $\mathbb{F}[x]$ if and only if one of the following holds:*

$$x^4 - a \ \ \textit{has a linear factor, i.e.,} \ a = b^4 \ \textit{for some} \ \ b \in \mathbb{F}, \tag{A.4.35}$$

$$a = \beta^2 \ \ \textit{for some} \ \ \beta \in \mathbb{F}, \tag{A.4.36}$$

$$a = -\tfrac{\alpha^4}{4} \ \ \textit{for some} \ \ \alpha \in \mathbb{F}. \tag{A.4.37}$$

*(Actually,* (A.4.35) $\Rightarrow$ (A.4.36)*, so* (A.4.35) *can be ignored.)*

The notion of the characteristic of a field was introduced in Exercise 7 of §7.1, and we recall it here. Given a field $\mathbb{F}$, there is a unique ring homomorphism $\psi : \mathbb{Z} \to \mathbb{F}$ such that $\psi(1) = 1$. The image $\mathcal{I}_{\mathbb{F}} = \psi(\mathbb{Z})$ is the ring in $\mathbb{F}$ generated by $\{1\}$. Since $\mathbb{Z}$ is a PID, either $\psi$ is injective or $\mathcal{N}(\psi) = (n)$ for some $n \in \mathbb{N}$, $n \geq 2$. Then $\psi$ induces an isomorphism of $\mathbb{Z}/(n)$ with $\mathcal{I}_{\mathbb{F}}$, so $n$ must be a prime, say $n = p$. If $\psi$ is injective, we say $\mathbb{F}$ has characteristic 0. If $\mathcal{N}(\psi) = (p)$, then $\mathcal{I}_{\mathbb{F}}$ is a subfield of $\mathbb{F}$, isomorphic to $\mathbb{F}_p$, and we say $\mathbb{F}$ has characteristic $p$.

It is easy to see that $x^4 - a$ is reducible in $\mathbb{F}_2[x]$ for all $a \in \mathbb{F}_2$. On the other hand, Proposition A.4.2 is applicable to $\mathbb{F}_p$ for all primes $p \geq 3$. In such a case, $x^4 - a$ is irreducible in $\mathbb{F}_p[x]$ whenever

$$a = \beta^2 \ \ \text{has no solution} \ \ \beta \in \mathbb{F}_p, \ \text{and} \tag{A.4.38}$$

$$-4a = \alpha^4 \ \ \text{has no solution} \ \ \alpha \in \mathbb{F}_p. \tag{A.4.39}$$

Note that if $-1$ is a square in $\mathbb{F}_p$, then (A.4.38) $\Rightarrow$ (A.4.39). (Interest in this situation also arose in (A.4.9) and in Exercise 5 of §6.1.) Now

$$\begin{gathered} \{\beta^2 : \beta \in \mathbb{F}_p \setminus 0\} \ \ \text{has cardinality} \ \ \frac{p-1}{\nu_p}, \ \ \text{and} \\ \Bigl\{-\frac{\alpha^4}{4} : \alpha \in \mathbb{F}_p \setminus 0\Bigr\} \ \ \text{has cardinality} \ \ \frac{p-1}{\mu_p}, \end{gathered} \tag{A.4.40}$$

where

$$\nu_p = \#\{\gamma \in \mathbb{F}_p : \gamma^2 = 1\}, \quad \mu_p = \#\{\gamma \in \mathbb{F}_p : \gamma^4 = 1\}. \tag{A.4.41}$$

Clearly, for primes $p \geq 3$, $\nu_p = 2$ and

$$\begin{aligned} \mu_p = 4 \quad &\text{if } -1 \text{ is a square in } \mathbb{F}_p, \\ 2 \quad &\text{if } -1 \text{ is not a square in } \mathbb{F}_p. \end{aligned} \tag{A.4.42}$$

This, by the way, suggests the answer to Exercise 5 of §6.1: given a prime $p \geq 3$,

$$-1 \ \text{ is a square in } \ \mathbb{F}_p \Longleftrightarrow 4|(p-1). \tag{A.4.43}$$

When $-1$ is not a square in $\mathbb{F}_p$, the two sets in (A.4.40) are disjoint, and hence cover $\mathbb{F}_p \setminus 0$. We deduce the following.

**Proposition A.4.3.** *For a prime $p \geq 3$, there exits $a \in \mathbb{F}_p$ such that $x^4 - a$ is irreducible in $\mathbb{F}_p[x]$ if and only if $p = 1$ mod 4.*

The arguments above illustrate that looking for irreducible polynomials in $\mathbb{F}[x]$ of a specific form can be an interesting and challenging task. We leave this pursuit, and turn to a task that extends the scope of our initial application of Proposition A.4.1.

Namely, we take a field $\mathbb{F}$ and a polynomial $P \in \mathbb{F}[x]$, not necessarily irreducible, and desire to extend $\mathbb{F}$ to a new field $\widetilde{\mathbb{F}}$, finite dimensional over $\mathbb{F}$, such that $P(x)$ factors into linear factors over $\widetilde{\mathbb{F}}$. Thus, if $P(x) = x^n + \cdots + a_0$ (we may as well take $a_n = 1$), we want

$$P(x) = (x - \xi_1) \cdots (x - \xi_n), \quad \xi_j \in \widetilde{F}. \tag{A.4.44}$$

The construction is quite similar to what was done in the paragraph following Proposition A.4.1. Since $\mathbb{F}[x]$ is a PID, $P(x)$ has a factorization $P(x) = Q_1(x) \cdots Q_M(x)$, with $Q_j \in \mathbb{F}[x]$ irreducible. Then, by Proposition A.4.1,

$$\mathbb{F}[x]/(Q_1) = \mathbb{F}_{(Q_1)} \tag{A.4.45}$$

is a field, in which $Q_1$ has a root $\xi_1$ (parallel to (A.4.4)) and a factorization $Q_1(x) = (x - \xi_1)\widetilde{Q}_1(x)$ (parallel to (A.4.5)), with $\widetilde{Q}_1 \in \mathbb{F}_{(Q_1)}[x]$. Then, with $P_1 = \widetilde{Q}_1 Q_2 \cdots Q_M \in \mathbb{F}_{(Q_1)}$, we have

$$P(x) = (x - \xi_1) P_1(x), \quad \xi_1 \in \mathbb{F}_{(Q_1)}, \quad P_1 \in \mathbb{F}_{(Q_1)}[x], \tag{A.4.46}$$

and $P_1$ has degree $n - 1$. We can iterate this a finite number of times to obtain (A.4.44), with $\widetilde{\mathbb{F}}$ obtained from $\mathbb{F}$ by a finite number of constructions of the form (A.4.1). Let us define

$$\mathbb{F}[\xi_1, \ldots, \xi_n] \subset \widetilde{\mathbb{F}} \tag{A.4.47}$$

as the subset of $\widetilde{\mathbb{F}}$ consisting of polynomials in $\xi_1, \ldots, \xi_n$, with coefficients in $\mathbb{F}$. Clearly $\mathbb{F}[\xi_1, \ldots, \xi_n]$ is a ring, and a finite-dimensional vector space over $\mathbb{F}$. In fact, it is a field, thanks to the following extension of Proposition 6.1.3.

**Proposition A.4.4.** *Let $\mathbb{F}$ and $\widetilde{\mathbb{F}}$ be fields and $\mathcal{R}$ a ring, satisfying*

$$\mathbb{F} \subset \mathcal{R} \subset \widetilde{\mathbb{F}}. \tag{A.4.48}$$

*If $\mathcal{R}$ is a finite dimensional vector space over $\mathbb{F}$, then $\mathcal{R}$ is a field.*

**Proof.** Simple variant of the proof of Proposition 6.1.3. □

We say $\mathbb{F}[\xi_1, \dots, \xi_n]$, arising in (A.4.44)–(A.4.47), is a *root field* of $P(x)$ over $\mathbb{F}$. Note that one can relabel $\{\xi_1, \dots, \xi_n\}$ as $\{\zeta_{jk}\}$, with

$$Q_j(x) = (x - \zeta_{j1}) \cdots (x - \zeta_{j\mu_j}), \quad \mu_j = \text{ order of } Q_j, \quad \zeta_{jk} \in \widetilde{\mathbb{F}}. \tag{A.4.49}$$

Note that constructing $\mathbb{F}[\xi_1, \dots, \xi_n]$ involved some arbitrary choices. Another choice could lead to

$$P(x) = (x - \xi_1') \cdots (x - \xi_n'), \quad \xi_j' \in \widetilde{\mathbb{F}}', \tag{A.4.50}$$

and to the field

$$\mathbb{F}[\xi_1', \dots, \xi_n'] \subset \widetilde{\mathbb{F}}'. \tag{A.4.51}$$

We have the following important uniqueness result.

**Proposition A.4.5.** *There is an isomorphism $\mathbb{F}[\xi_1, \dots, \xi_n] \approx \mathbb{F}[\xi_1', \dots, \xi_n']$ that is the identity on $\mathbb{F}$ and takes $\xi_j \mapsto \xi_{\sigma(j)}'$, for some permutation $\sigma$ of $\{1, \dots, n\}$.*

To establish Proposition A.4.5, we start with the following complement to Proposition A.4.1.

**Lemma A.4.6.** *Assume that $P \in \mathbb{F}[x]$ is irreducible and that there is a field $\widetilde{\mathbb{F}} \supset \mathbb{F}$ and $\xi \in \widetilde{\mathbb{F}}$ such that $P(\xi) = 0$. Consider the ring $\mathbb{F}[\xi] \subset \widetilde{\mathbb{F}}$ (which, by Proposition A.4.4, is a field). Then there is a natural isomorphism*

$$\mathbb{F}[\xi] \approx \mathbb{F}_{(P)} = \mathbb{F}[x]/(P). \tag{A.4.52}$$

**Proof.** The map $x \mapsto \xi$ yields a natural surjective ring homomorphism

$$\psi : \mathbb{F}[x] \longrightarrow \mathbb{F}[\xi]. \tag{A.4.53}$$

Then the null space $\mathcal{N}(\psi)$ is an ideal in $\mathbb{F}[x]$, and it must be a principal ideal. Now $P(\xi) = 0 \Rightarrow P \in \mathcal{N}(\psi)$, so $\mathcal{N}(\psi) \supset (P)$. The irreducibility of $P$ in $\mathbb{F}[x]$ implies $\mathcal{N}(\psi) = (P)$, and gives (A.4.52). □

NOTE. A corollary of Lemma A.4.6 is that, if $P \in \mathbb{F}[x]$ is irreducible, and if if there exists another field $\widetilde{\mathbb{F}}' \supset \mathbb{F}$ and $\xi' \in \widetilde{\mathbb{F}}'$ such that $P(\xi') = 0$, yielding $\mathbb{F}[\xi'] \subset \widetilde{\mathbb{F}}'$, then $\mathbb{F}[\xi]$ and $\mathbb{F}[\xi']$ are isomorphic, via $\xi \mapsto \xi'$.

**Proof of Proposition A.4.5.** We use induction on

$$m = \dim_{\mathbb{F}} \mathbb{F}[\xi_1, \dots, \xi_n] \tag{A.4.54}$$

(for arbitrary $\mathbb{F}$). The result is trivial for $m = 1$, since then $P(x)$ factors into linear factors in $\mathbb{F}[x]$, uniquely (up to order). Suppose $m > 1$. Then $P(x)$ has an irreducible factor $Q(x)$ of degree $d > 1$. Let $\xi$ be a root of $Q$ in $\mathbb{F}[\xi_1, \dots, \xi_n]$ and $\xi'$ a root of $Q$ in $\mathbb{F}[\xi'_1, \dots, \xi'_n]$ (say $\xi = \xi_j,\ \xi' = \xi'_{\sigma(j)}$). By Lemma A.4.6, $\xi \mapsto \xi'$ provides an isomorphism from $\mathbb{F}[\xi]$ to $\mathbb{F}[\xi']$. Now $\mathbb{F}[\xi_1, \dots, \xi_n]$ is an extension of $\mathbb{F}[\xi_j]$, and

$$\dim_{\mathbb{F}[\xi_j]} \mathbb{F}[\xi_1, \dots, \xi_n] = \frac{m}{d}, \tag{A.4.55}$$

while $\mathbb{F}[\xi'_1, \dots, \xi'_n]$ is an extension of $\mathbb{F}[\xi']$, which we can identify with $\mathbb{F}[\xi]$. Thus induction finishes the proof. $\square$

In light of Proposition A.4.5, we say $\mathbb{F}[\xi_1, \dots, \xi_n]$ in (A.4.46)–(A.4.47) is *the* root field of $P(x)$ over $\mathbb{F}$, and denote it by

$$\mathcal{R}(P, \mathbb{F}). \tag{A.4.56}$$

Note that if $\mathbb{K}$ is a field and $P \in \mathbb{F}[x]$,

$$\mathbb{F} \subset \mathbb{K} \subset \mathcal{R}(P, \mathbb{F}) \Longrightarrow \mathcal{R}(P, \mathbb{K}) = \mathcal{R}(P, \mathbb{F}). \tag{A.4.57}$$

We return to the search for and description of fields with $p^n$ elements. Momentarily postponing the existence question, let us set $q = p^n$, where $p \in \mathbb{N}$ is a prime and $n \in \mathbb{N}$, and suppose $\mathbb{F}_q$ is a field with $q$ elements. As we have seen, $\mathbb{F}_q$ contains, in a unique fashion, a subfield isomorphic to $\mathbb{F}_p = \mathbb{Z}/(p)$, and $\dim_{\mathbb{F}_p} \mathbb{F}_q = n$. To look further into the structure of $\mathbb{F}_q$, we note that $\mathbb{F}_q \setminus 0$ is a multiplicative group with $q - 1$ elements, so, by Proposition A.3.1,

$$a \in \mathbb{F}_q \setminus 0 \Longrightarrow a^{q-1} = 1 \Longrightarrow a^q = a, \tag{A.4.58}$$

the latter identity also holding for $a = 0$. Thus each element of $\mathbb{F}_q$ is a root of the polynomial $x^q - x$. Since this has at most $q$ roots, we must have

$$x^q - x = \prod_{j=1}^{q} (x - a_j), \quad \mathbb{F}_q = \{a_j : 1 \le j \le q\}. \tag{A.4.59}$$

These considerations lead to the following result.

**Proposition A.4.7.** *If $p \in \mathbb{N}$ is a prime, $n \in \mathbb{N}$, and $q = p^n$, then*

$$\mathcal{R}(x^q - x, \mathbb{F}_p) \tag{A.4.60}$$

*is a field with $q$ elements. Furthermore, each field with $q$ elements is isomorphic to* (A.4.60). *We denote this field by $\mathbb{F}_q$.*

**Proof.** First, we need to show that the field (A.4.60) has $q$ elements if $q = p^n$. For this, it suffices to show that $P(x) = x^q - x$ has no multiple roots. In fact, if $\xi$ is a multiple root of $P(x)$, then $x - \xi$ is also a factor of $P'(x)$ in $\mathcal{R}(x^q - x, \mathbb{F}_p)$, so $P'(\xi) = 0$. But in $\mathbb{F}_p[x]$, $P'(x) = qx^{q-1} - 1 = -1$, so it has no roots. Consequently, $x^q - x$ has $q$ distinct roots in $\mathcal{R}(x^q - x, \mathbb{F}^p)$.

The sum and difference of two roots are also roots, since

$$(a \pm b)^p = a^p \pm b^p \tag{A.4.61}$$

in any field of characteristic $p$, and hence, inductively, given roots $a$ and $b$,

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} = a \pm b. \tag{A.4.62}$$

The product $ab$ is also a root, since $(ab)^q = a^q b^q = ab$. The set of all $q$ roots of $x^q - x$ is therefore a subring of $\mathcal{R}(x^q - x, \mathbb{F}_p)$, hence a subfield (by Proposition A.4.4). Since it contains all the roots, it must equal $\mathcal{R}(x^q - x, \mathbb{F}_p)$. □

The proof of Proposition A.4.7 motivates us to consider more generally when a polynomial $P \in \mathbb{F}[x]$ has multiple roots in $\mathcal{R}(P, \mathbb{F})$. This brings in the derivative

$$D : \mathbb{F}[x] \longrightarrow \mathbb{F}[x], \tag{A.4.63}$$

an $\mathbb{F}$-linear map defined by

$$Dx^n = nx^{n-1}, \tag{A.4.64}$$

the formula one sees in basic calculus, but here in a more general setting. We also use the notation $P' = DP$. As in calculus, one verifies that $D$ is a derivation, i.e.,

$$D(PQ) = P'Q + PQ', \quad \forall\, P, Q \in \mathbb{F}[x]. \tag{A.4.65}$$

Of course, $D$ acts on polynomials over any field, such as $\mathcal{R}(P, \mathbb{F})$. If $P$ factors as in (A.4.44), then $P'$ is, by (A.4.65), a sum of $n$ terms, the $j$th term obtained from (A.4.44) by omitting the factor $x - \xi_j$. Consequently, if $\xi_j = \xi_k$ is a double root of $P$,

$$P \text{ and } P' \text{ are both multiples of } x - \xi_j, \text{ in } \mathcal{R}(P, \mathbb{F}). \tag{A.4.66}$$

This observation leads to the following result.

**Proposition A.4.8.** *If $P \in \mathbb{F}[x]$ is irreducible, then all the roots of $P$ in $\mathcal{R}(P, \mathbb{F})$ are simple unless $P' = 0$.*

**Proof.** If $P$ is irreducible, and $P'$ (whose degree is less than that of $P$) is not 0 in $\mathbb{F}[x]$, then the ideal generated by $P$ and $P'$ has a single generator, which divides $P$, so is 1. Thus there exist $Q_0, Q_1 \in \mathbb{F}[x]$ such that

$$Q_0(x)P(x) + Q_1(x)P'(x) = 1. \tag{A.4.67}$$

This identity also holds in $\mathcal{R}(P, \mathbb{F})$, of course, and it contradicts (A.4.66). □

If the leading term of $P(x)$ is $a_n x^n,\ n \geq 1,\ a_n \neq 0$, then the leading term of $P'(x)$ is $n a_n x^{n-1}$, which is nonvanishing unless $n = 0$ in $\mathbb{F}$. Thus we have:

**Corollary A.4.9.** *If $\mathbb{F}$ has characteristic $0$ and $P \in \mathbb{F}[x]$ is irreducible, then all the roots of $P$ in $\mathcal{R}(P, \mathbb{F})$ are simple.*

Here is an example of a field $\mathcal{F}$ of characteristic $p$ and an irreducible $P \in \mathcal{F}[x]$ that has a multiple root in $\mathcal{R}(P, \mathcal{F})$. Namely, let $p \in \mathbb{N}$ be a prime and set $\mathcal{K} = \mathbb{F}_p(t)$, the quotient field of the polynomial ring $\mathbb{F}_p[t]$ (which is an integral domain). Then set

$$\mathcal{F} = \mathbb{F}_p(t^p), \tag{A.4.68}$$

the subfield of $\mathcal{K}$ generated by $t^p$. Then take

$$P(x) = x^p - t^p, \quad P \in \mathcal{F}[x], \tag{A.4.69}$$

which is irreducible over $\mathcal{F}$, though not over $\mathcal{K}$. In this case, we have

$$P(x) = x^p - t^p = (x - t)^p \ \text{ in } \ \mathcal{K}[x], \tag{A.4.70}$$

so $\mathcal{K} = \mathcal{R}(P, \mathcal{F})$, and $P$ has just one root, of multiplicity $p$, in $\mathcal{R}(P, \mathcal{F})$.

By contrast, there is the following complement to Corollary A.4.9.

**Proposition A.4.10.** *If $\mathbb{F}$ is a finite field and $P \in \mathbb{F}[x]$ is irreducible, then all roots of $P$ in $\mathcal{R}(P, \mathbb{F})$ are simple.*

A useful ingredient in the proof of Proposition A.4.10 is the following.

**Lemma A.4.11.** *If $\mathbb{F} = \mathbb{F}_q,\ q = p^n$, then*

$$\psi : \mathbb{F} \longrightarrow \mathbb{F}, \quad \psi(a) = a^p \quad \textit{is bijective.} \tag{A.4.71}$$

**Proof.** In fact, if $\psi^n = \psi \circ \cdots \circ \psi$ is the $n$-fold composition, then

$$\psi^n(a) = a^{p^n} = a, \quad \forall\, a \in \mathbb{F}, \tag{A.4.72}$$

by (A.4.58), so $\psi^n$ is bijective. This forces $\psi$ to be bijective. $\square$

**Proof of Proposition A.4.10.** By Proposition A.4.8, it suffices to show that if $q = p^n,\ P \in \mathbb{F}_q[x]$, and $P' = 0$, then $P$ is not irreducible. Indeed, if $P' = 0$, then $P(x)$ must have the form

$$P(x) = a_k x^{kp} + a_{k-1} x^{(k-1)p} + \cdots + a_1 x^p + a_0. \tag{A.4.73}$$

By Lemma A.4.11, we can write each $a_j = b_j^p$ for some $b_j \in \mathbb{F}_q$, and then identities parallel to, and following by induction from, (A.4.61) give

$$P(x) = Q(x)^p, \quad Q(x) = b_k x^k + b_{k-1} x^{k-1} + \cdots + b_1 x + b_0, \tag{A.4.74}$$

proving that $P(x)$ is not irreducible. $\square$

Remark. The identity (A.4.61) for elements of $\mathbb{F}_q$ also implies that $\psi$ in (A.4.71) satisfies

$$\psi : \mathbb{F}_q \longrightarrow \mathbb{F}_q \text{ is a ring homomorphism.} \tag{A.4.75}$$

Being bijective, $\psi$ is hence an automorphism of $\mathbb{F}_q$. Also the analogue of (A.4.58) for $q = p$ implies that $\psi$ is the identity on $\mathbb{F}_p \subset \mathbb{F}_q$. One writes

$$\psi \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p). \tag{A.4.76}$$

Generally, if we have fields $\mathbb{F} \subset \mathcal{F}$, an element

$$\varphi \in \mathrm{Gal}(\mathcal{F}/\mathbb{F}) \tag{A.4.77}$$

is an automorphism of $\mathcal{F}$ that leaves the elements of $\mathbb{F}$ fixed. The set $\mathrm{Gal}(\mathcal{F}/\mathbb{F})$ is a group, called the Galois group of $\mathcal{F}$ over $\mathbb{F}$. Galois theory is a very important topic in algebra, which the reader who has gotten through this appendix will be prepared to study, in sources like [**1**], [**4**], and [**11**]. It is tempting to say a little more about Galois theory here, but we have to stop somewhere.

# Bibliography


[1] M. Artin, *Algebra*, Prentice-Hall, Englewood Cliffs, NJ, 1991.

[2] M. Atiyah and I. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading MA, 1969.

[3] J. Baez, The octonions, *Bull. AMS* 39 (2002), 145–205.

[4] G. Birkhoff and S. MacLane, *Survey of Modern Algebra*, Macmillan, New York, 1953.

[5] T. Dray and C. Manogue, *The Geometry of the Octonions*, World Scientific, NJ, 2015.

[6] G. Golub and C. van Loan, *Matrix Computations*, Johns Hopkins Univ. Press, 1996.

[7] W. Greub, *Multilinear Algebra*, Springer-Verlag, New York, 1978.

[8] F. R. Harvey, *Spinors and Calibrations*, Academic Press, New York, 1990.

[9] K. Hofmann and R. Kunze, *Linear Algebra*, Prentice Hall, New Jersey, 1971.

[10] R. Horn and C. Johnson, *Matrix Analysis*, Cambridge Univ. Press, Cambridge UK, 1985.

[11] S. Lang, *Algebra*, Addison-Wesley, Reading MA, 1965.

[12] S. Lang, *Linear Algebra*, Springer, New York, 1987.

[13] H. B. Lawson and M. L. Michelson, *Spin Geometry*, Princeton Univ. Press, Princeton NJ, 1989.

[14] J. MacCormick, *9 Algorithms that Changed the Future*, Princeton Univ. Press, Princeton NJ, 2012.

[15] K. McCrimmon, Jordan algebras and their applications, *Bull. AMS* 84 (1978), 612–627.

[16] I. Porteous, *Clifford Algebras and Classical Groups*, Cambridge Univ. Press, 1995.

[17] C. Procesi, *Lie Groups – an Approach through Invariants and Representations*, Springer, New York, 2007.

[18] M. Reid, *Undergraduate Commutative Algebra*, LMS Student Texts #29, Cambridge Univ. Press, Cambridge UK, 1995.

[19] E. Seneta, *Non-negative Matrices and Markov Chains*, Springer-Verlag, New York, 1981.

[20] B. Simon, *Representations of Finite and Compact Groups*, Amer. Math. Soc., Providence RI, 1996.

[21] T. Springer and F. Veldkamp, *Octonions, Jordan Algebras, and Exceptional Groups*, Springer, Berlin, 2000.

[22] G. Strang, *Linear Algebra and its Applications* (4th ed.), Brooks/Cole, Belmont, CA, 2006.

[23] M. Taylor, *Introduction to Analysis in One Variable*, Amer. Math. Soc., Providence RI, to appear.

[24] M. Taylor, *Introduction to Analysis in Several Variables (Advanced Calculus)*, Amer. Math. Soc., Providence RI, to appear.

[25] M. Taylor, *Lectures on Lie Groups*, Lecture Notes, available at AMS Open Math Notes.

[26] M. Taylor, *Partial Differential Equations*, Vols. 1–3, Springer, New York, 1996 (2nd ed., 2011).

[27] M. Taylor, *Introduction to Differential Equations*, Amer. Math. Soc., Providence RI, 2011.

[28] M. Taylor, *Differential Geometry*, Lecture Notes, 2019.

[29] M. Taylor, *Measure Theory and Integration*, Amer. Math. Soc., Providence RI, 2006.

[30] M. Taylor, *Introduction to Complex Analysis*, GSM #202, Amer. Math. Soc., Providence RI, 2019.

[31] L. Trefethen and D. Bau, *Numerical Linear Algebra*, SIAM, 1997.

# Index