The Sally SERIES

Pure and Applied
UNDERGRADUATE TEXTS

42

Linear Algebra for the Young Mathematician

Steven H. Weintraub

American Mathematical Society

Linear Algebra for the Young Mathematician

The Sally Series
Pure and Applied
UNDERGRADUATE TEXTS • 42

Linear Algebra for the Young Mathematician

Steven H. Weintraub

American Mathematical Society
Providence, Rhode Island USA

2010 *Mathematics Subject Classification*. Primary 15-01.

For additional information and updates on this book, visit
www.ams.org/bookpages/amstext-42

Library of Congress Cataloging-in-Publication Data

Cataloging-in-Publication Data has been applied for by the AMS.
See http://www.loc.gov/publish/cip/.

10 9 8 7 6 5 4 3 2 1 24 23 22 21 20 19

Contents

Part II. Vector spaces with additional structure

Preface

Linear algebra is a subject that lies at the core of modern mathematics. Every mathematician, pure or applied, is intimately familiar with it. Every student of mathematics needs to become familiar with it, too.

Linear Algebra for the Young Mathematician is a careful, thorough, and rigorous introduction to linear algebra, one which emphasizes the basic ideas in the subject. Let us unpack this sentence. First of all, it is an introduction, presupposing no prior knowledge of the field. Second of all, it is careful and thorough—you should expect no less from any book. Thirdly, it is rigorous. We prove what we claim to be true. As a mathematician, you should demand this. But more than that, a good proof not only shows *that* something is true, it shows *why* it is true. This brings us to our last point. We emphasize the ideas of the subject, and provide both conceptual definitions and proofs, rather than calculational ones, so you will see and understand the logic of the field, and why its results are true. We freely admit that this conceptual approach means you will have to put more thought into learning the subject, but you will get a *lot* more out.

We presume that you, the reader, are a mathematician, but we interpret that term broadly. You could be a mathematician per se, or anyone in related fields (e.g., a statistician studying data modeling, a physicist studying quantum mechanics, or an engineer studying signal processing) with a serious interest in mathematical theory as well as in its applications to your field. We presume further that you, the reader, are a young mathematician, not necessarily in the sense of chronological years, but rather in the sense of mathematical years, i.e., that you are just starting your serious study of mathematics. The author is an old mathematician, in the sense that he has been thinking seriously about mathematics for over half a century. (Of course, this implies something about his chronological age as well.) Thus in addition to the rigorous statements in the book, we have taken considerable care, and space, to present what we think is a right viewpoint, developed over decades of thought and experience, from which to view the subject. We hope you will benefit from the wisdom we have accumulated. (Note we have said "a right viewpoint" rather than "the right viewpoint". We are not so presumptuous to claim that our viewpoint is the only right one, and you will undoubtedly go on to develop your own, which may differ. But at least we hope—indeed, expect—to provide you with a good starting point.)

What distinguishes this book from the many other introductory linear algebra books in existence? Of course, we think it is exceptionally well written. But beyond that, there are several aspects. First and foremost is our conceptual approach and our attempt to provide a viewpoint on the subject. Second is our coverage. We concentrate on the finite-dimensional case, where the results are strongest, but do not restrict ourselves to it. We consider vector spaces in general, and see to what extent results in the finite-dimensional case continue to hold in general. Of course, in the finite-dimensional case we have a very powerful computational tool, matrices, and we will learn how to do all the usual matrix computations, so that we can in practice solve the problems that arise. But we wish to emphasize, even in the finite-dimensional case: *Linear algebra is about vector spaces and linear transformations, not about matrices.* (In line with this emphasis, we do not deal with questions of how most accurately or efficiently to perform machine computations, leaving that for you to learn in a future numerical analysis course, if that is a direction you wish to pursue.) Even in the finite-dimensional case, we cover material often not covered in other introductory texts, and go further. Particularly noteworthy here is our thorough coverage of Jordan canonical form as well as the spectral theorem. Third, we wrote right at the start that linear algebra is a central subject in mathematics, and rather than having you simply have to take our word for it, we illustrate it by showing some of the connections between linear algebra and other parts of mathematics, in our case, with algebra and calculus.

On the one hand we will see that calculus "works" because the basic operations of calculus, evaluation of a function, differentiation, and definite integration, are linear transformations, and we will see how to most properly formulate some of the results of calculus in linear algebra terms. On the other hand, we will see how to use linear algebra to concretely solve some of the problems of algebra and calculus. (Some of these connections are given in separate sections of the text, while others are given as immediate applications of particular results in linear algebra.)

Here is, roughly speaking, the plan of the book.

We begin right away, in accord with our philosophy, by introducing vector spaces, in the situation of "usual" vectors (the kind you have seen in calculus), and linear transformations, in the situation of multiplication of vectors by matrices. (You will see that, throughout the book, we are much more likely to speak of "the linear transformation $\mathcal{T}_A$ that is multiplication by the matrix A" than we are to simply speak of "the matrix A".) This allows us to begin by posing the general questions we wish to answer in a relatively concrete context.

Usually, answering specific questions in linear algebra means solving systems of linear equations, and so we devote Chapter 2 entirely to that. (But, in line with our emphasis, we begin that chapter with a consideration of the geometry of linear systems, before considering the particulars of solution methods.)

The next three chapters, which deal with linear transformations, are the heart of the book. Here you will find key results in linear algebra. In Chapter 6 we turn our attention to determinants, an important theoretical and computational tool, before returning to the consideration of linear transformations in the next two chapters. Our analysis of linear transformations culminates in Jordan canonical form, which tells you all you want to know about a linear transformation (from a finite-dimensional complex vector space to itself, to be precise).

These first eight chapters (Part I of the book) deal with general vector spaces. The last two chapters (Part II) deal with vector spaces with additional structure—first that of bilinear or sesquilinear forms, and finally that of inner product spaces, culminating, in the finite-dimensional case, with the spectral theorem.

We have mentioned above that there are applications of linear algebra in various places in the text. Let us point some of them out:

Section 4.5: “Looking back at calculus”.

In Section 5.2: A common generalization of finite Taylor polynomials and the Lagrange interpolation theorem with an application to cubic splines, and partial fraction decompositions.

In Section 5.5: Numerical integration and differentiation.

Sections 7.3 and 8.4: Solutions of higher-order linear differential equations and systems of first-order linear differential equations.

Section 9.5: Diagonalizing quadratic forms, and the “second derivative test” in multivariable calculus.

In Section 10.2: The method of Gaussian quadrature.

Some remarks on numbering and notation: We use three-level numbering, so that, for example, Theorem 8.1.6 is the 6th numbered item in Section 8.1. We denote the end of proofs by $\square$, as is usual. Theorems, etc., are set in italics, so their end is denoted by the end of the italics. Definitions, etc., are set in roman type, so their end cannot be deduced from the typeface; we denote their end by $\Diamond$. Our mathematical notation is standard, though we want to point out that if A and B are sets, $A \subseteq B$ means A is a subset of B and $A \subset B$ means A is a proper subset of B (i.e., $A \subseteq B$ and $A \neq B$).

There are not enough typefaces to go around to distinguish different kinds of objects, and indeed one of the points of linear algebra is that it is logically impossible to do so. For example, we might want to regard a function $f(x)$ as a vector in a vector space—should we change notation to do so? But we will always use V to denote a vector space and we will always use $\mathcal{T}$ to denote a linear transformation.

Finally, we will remark that there is some (deliberate) repetition in the book, as in some cases we have introduced a concept in a specific situation and then generalized it later. Otherwise, the book should pretty much be read straight through, except that Section 9.4 will not be used again until Section 10.4, and that Section 9.5 will not be used in Chapter 10 at all. Also, while Chapter 8, Jordan canonical form, is the culmination of Part I, it is not necessary for the study of normal linear transformations in Part II.

There are several appendices. We use the notion of a field $\mathbb{F}$ in general, although all of our work in this book will be over the fields $\mathbb{Q}$ (the rational numbers), $\mathbb{R}$ (the real numbers), or $\mathbb{C}$ (the complex numbers). For those readers wishing to know more about fields, we have an optional Appendix A. Appendix B deals with properties of polynomials, and readers not already familiar with them will need to read it before Chapter 7, where these properties are used. We are doing algebra in this book, so we are dealing with finite sums throughout, but in analysis we need to deal with infinite sums and issues of convergence, and in the optional Appendix C we consider the basics of these. Finally, we have stated that linear algebra plays a central place in mathematics and its applications, and Appendix D is a guide to further reading for the reader who wishes to see further developments, aspects of linear algebra not treated here, or applications outside of pure mathematics.

February 2019 *Steven H. Weintraub*

Part I

Vector spaces

Chapter 1

The basics

1.1. The vector space $\mathbb{F}^n$

In this section we introduce $\mathbb{F}^n$, which is the archetype of all the spaces we will be studying.

Definition 1.1.1. Let $\mathbb{F}$ be a field. A *scalar* is an element of $\mathbb{F}$. $\Diamond$

We have stated this in general, and we treat general fields in the (optional) Appendix A. But you are undoubtedly familiar with the fields $\mathbb{Q}$ (the field of rational numbers), $\mathbb{R}$ (the field of real numbers), and $\mathbb{C}$ (the field of complex numbers). All the examples in this book will be taken from one of these three fields, so if these are the only ones you are familiar with, that will be fine. But in Part I, everything we say will be valid for any field $\mathbb{F}$, though in Part II we will specialize to $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.

Definition 1.1.2. Let $\mathbb{F}$ be a field. The *vector space* $\mathbb{F}^n$ consists of vectors $v = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$ with entries $a_1, a_2, \ldots, a_n$ any elements of $\mathbb{F}$, and with two operations:

(1) For vectors $v = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$ and $w = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$ their sum is defined to be

$$v + w = \begin{bmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{bmatrix}.$$

(2) For a scalar c and a vector $v = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$, their product is defined to be

$$cv = \begin{bmatrix} ca_1 \\ ca_2 \\ \vdots \\ ca_n \end{bmatrix}. \qquad \Diamond$$

The operation (1) is called *vector addition* and the operation (2) is called *scalar multiplication.*

If $v = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$, then $a_1, a_2, \ldots, a_n$ are called the *coefficients* (or the *entries*) of v. We see that v has n rows (each of which consists of a single entry) and one column.

First we must decide when two vectors are equal, and here the answer is the most natural one.

Definition 1.1.3. Let $v = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$ and $w = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$ be vectors in $\mathbb{F}^n$. Then $v = w$ if $a_1 = b_1,\ a_2 = b_2,\ \ldots,\ a_n = b_n$. $\Diamond$

In other words, two vectors are equal if their corresponding entries are equal.

We now single out a number of properties of vector addition and scalar multiplication.

Theorem 1.1.4. *Vector addition and scalar multiplication in $\mathbb{F}^n$ satisfy the following properties*:

(1) *If v and w are vectors in $\mathbb{F}^n$, then $v + w$ is a vector in $\mathbb{F}^n$.*

(2) *For any two vectors v and w, $v + w = w + v$.*

(3) *For any three vectors u, v, and w, $(u + v) + w = u + (v + w)$.*

(4) *There is a vector 0 such that for any vector v, $v + 0 = 0 + v = v$.*

(5) *For any vector v there is a vector $-v$ such that $v + (-v) = (-v) + v = 0$.*

(6) *If c is a scalar and v is a vector in $\mathbb{F}^n$, then cv is a vector in $\mathbb{F}^n$.*

(7) *For any scalar c and any vectors u and v, $c(u + v) = cu + cv$.*

(8) *For any scalars c and d and any vector v, $(c + d)v = cv + dv$.*

(9) *For any scalars c and d and any vector v, $c(dv) = (cd)v$.*

(10) *For any vector v, $1v = v$.*

Proof. We let the vector 0 be the vector all of whose entries are 0, $0 = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$.

Also, if $v = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$, we let $-v = \begin{bmatrix} -a_1 \\ -a_2 \\ \vdots \\ -a_n \end{bmatrix}$. Then these properties all follow in a straightforward way from the corresponding properties of elements of $\mathbb{F}$ and the fact that vector addition and scalar multiplication are both performed entry-by-entry. We leave the proof to the reader. □

Here are four more simple properties. We have listed them separately because, although they are easy to prove directly, they are in fact consequences of properties (1)–(10).

Theorem 1.1.5.

(11) *For any vector v in $\mathbb{F}^n$, $0v = 0$, the 0 vector in $\mathbb{F}^n$.*

(12) *If 0 is the 0 vector in $\mathbb{F}^n$, then for any scalar c, $c0 = 0$, the 0 vector in $\mathbb{F}^n$.*

(13) *For any vector v in $\mathbb{F}^n$, $(-1)v = -v$.*

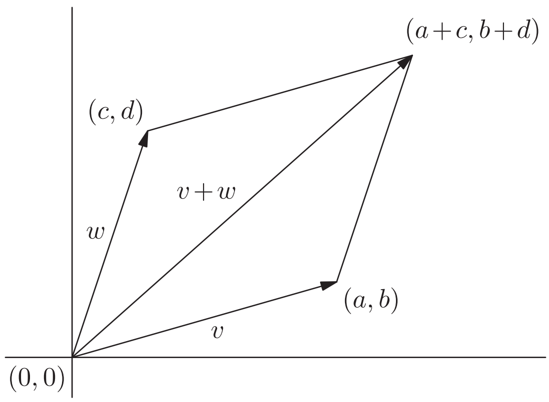
(14) *Let c be a scalar, and let v be a vector in $\mathbb{F}^n$. If $cv = 0$, then $c = 0$ or $v = 0$.*

Proof. Again we leave the proof to the reader. □

You may have already noticed that we have used the symbol 0 to mean two different things: the scalar 0 and the 0 vector in $\mathbb{F}^n$. But actually, the situation is even worse, because this vector is different for different values of n, e.g., for $n = 1$, the 0 vector is $[0]$, for $n = 2$ the 0 vector is $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$, for $n = 3$ the 0 vector is $\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, etc. Why have we done this? If you think about it, you'll see that in order to keep all of these straight we would have had to use a blizzard of different symbols to denote very similar objects. Rather than clarifying matters, that would just confuse things. (And in fact it turns out that sometimes we will want to view the same object in different contexts, so we would have two different names for the same thing, which would be even worse.) Thus we simply use the same symbol 0 for all of these objects, and rely on the context to sort them out.

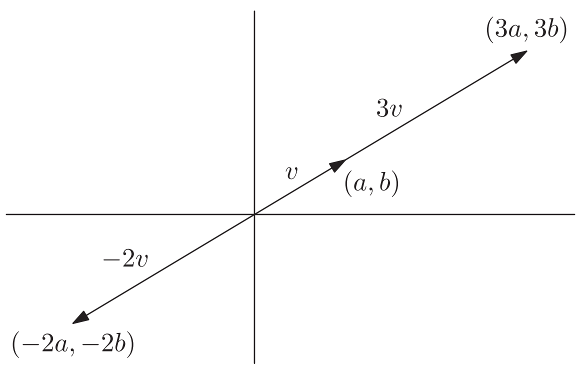
Remark 1.1.6. We have defined the operations of vector addition and scalar multiplication in $\mathbb{F}^n$ algebraically, but they have a simple geometric meaning. We shall illustrate this in $\mathbb{R}^2$, where we can draw pictures.

We shall identify the vector $\begin{bmatrix} a \\ b \end{bmatrix}$ with the "arrow" from the origin $(0, 0)$ to the point (a, b) in the plane. By "arrow" we mean the line segment between these two points, but with an arrowhead to denote that we are going from $(0, 0)$ to (a, b), not the other way around. Then vector addition is given by the "parallelogram rule".



That is, if $v = \begin{bmatrix} a \\ b \end{bmatrix}$ is the vector from the origin $(0, 0)$ to the point (a, b) and $w = \begin{bmatrix} c \\ d \end{bmatrix}$ is the vector from the origin $(0, 0)$ to the point (c, d), we form the parallelogram two of whose sides are these arrows, and then $v + w = \begin{bmatrix} a+c \\ b+d \end{bmatrix}$ is the arrow which is the diagonal of the parallelogram, going from the origin $(0, 0)$ to the other corner $(a + c, b + d)$.

Scalar multiplication of the vector v by the scalar c is given by scaling v by a factor of c along the line in which it runs. That is, we scale each of its coefficients by a factor of c.



Thus cv points along the same line as v. If c is positive, the scale factor is c and cv points in the same direction as v, while if c is negative the scale factor is $|c|$ and cv points in the opposite direction to v. $\Diamond$

We have defined $\mathbb{F}^1, \mathbb{F}^2, \mathbb{F}^3, \ldots$. We also need to define $\mathbb{F}^0$. A priori, it is not clear what this should mean. After all, what should we mean by a vector with 0 rows? It turns out that the right thing to do is this:

Definition 1.1.7. $\mathbb{F}^0$ is the vector space consisting of a single element 0. Addition is defined by $0 + 0 = 0$, and we also set $-0 = 0$. Scalar multiplication is defined by $c0 = 0$ for every c. $\Diamond$

Remark 1.1.8. As you can check, properties (1)–(14) also hold for $\mathbb{F}^0$. $\Diamond$

Remark 1.1.9. You may well ask why we have singled out these properties of $\mathbb{F}^n$. Why no more and why no fewer? Excellent question!

To answer this question let us think more broadly. Suppose we are in a situation where we are considering potential properties to require of some objects. The more properties we require, the more precise information we will have, and the stronger results we will be able to conclude. But the more properties we require, the more restricted the class of objects we consider will be, as they will have to satisfy all these properties. The fewer properties we require, the more general our objects will be, but we will have less information about them, and so the conclusion we will be able to make will not be as strong.

So where should we be in the specificity/generality scale? Over a century of mathematical practice has shown that requiring precisely properties (1) through (10) (from which, as we have remarked, properties (11) through (14) follow) is a right answer. We will see in Chapter 3 that these are exactly the properties that characterize a vector space, and vector spaces are the subject matter of linear algebra. These are the objects we will be considering in Part I of this book.

We were careful to say that requiring precisely these properties is "a" right answer rather than "the" right answer. It certainly makes sense (and is both interesting and useful) to require fewer properties. But that would carry us outside the domain of linear algebra into more general algebraic structures, and that would be outside the domain of this book.

It also certainly makes sense to require more properties. For example, you might note that we have said nothing about lengths of vectors. Indeed, in a general vector space, there is *no* notion of the length of a vector. But it is important to consider those vector spaces in which vectors *do* have lengths, and that will be the subject of Part II of this book. $\Diamond$

1.2. Linear combinations

The basic way we combine vectors in $\mathbb{F}^n$ is by taking linear combinations of them. Here is the definition.

Definition 1.2.1. Let $S = \{v_1, v_2, \ldots, v_k\}$ be a set of vectors in $\mathbb{F}^n$, and let $c_1, c_2, \ldots, c_k$ be scalars. Then

$$v = \sum_{i=1}^{k} c_i v_i = c_1 v_1 + c_2 v_2 + \cdots + c_k v_k$$

is a *linear combination* of the vectors in S. $\Diamond$

Example 1.2.2. Let $S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -2 \\ 3 \end{bmatrix}, \begin{bmatrix} 5 \\ 6 \\ 12 \end{bmatrix} \right\}$, vectors in $\mathbb{R}^3$, and let $c_1 = 3/2$, $c_2 = -5$, $c_3 = 1/2$. Then

$$c_1 v_1 + c_2 v_2 + c_3 v_3 = (3/2) \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix} - 5 \begin{bmatrix} 0 \\ -2 \\ 3 \end{bmatrix} + (1/2) \begin{bmatrix} 5 \\ 6 \\ 12 \end{bmatrix} = \begin{bmatrix} 4 \\ 16 \\ -9 \end{bmatrix}. \qquad \Diamond$$

Example 1.2.3. Let $v_1 = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$ and $v_2 = \begin{bmatrix} 2 \\ 7 \end{bmatrix}$, vectors in $\mathbb{R}^2$. Let x_1 and x_2 be (unknown) scalars and consider the equation $x_1 v_1 + x_2 v_2 = \begin{bmatrix} 2 \\ 9 \end{bmatrix}$. This is the equation

$$x_1 \begin{bmatrix} 1 \\ 3 \end{bmatrix} + x_2 \begin{bmatrix} 2 \\ 7 \end{bmatrix} = \begin{bmatrix} 2 \\ 9 \end{bmatrix},$$

which, by the definition of a linear combination, is the equation

$$\begin{bmatrix} x_1 + 2x_2 \\ 3x_1 + 7x_2 \end{bmatrix} = \begin{bmatrix} 2 \\ 9 \end{bmatrix}.$$

Remembering that two vectors are equal if their corresponding entries are equal, we see that this is the system of linear equations

$$\begin{aligned} x_1 + 2x_2 &= 2, \\ 3x_1 + 7x_2 &= 9. \end{aligned}$$

We will be making a careful and systematic study of how to solve systems of linear equations, but you have undoubtedly seen, and learned how to solve, systems of two linear equations in two unknowns before. If you solve this system, you will find it has the unique solution $x_1 = -4$, $x_2 = 3$. $\Diamond$

Now suppose our set S has an infinite number of vectors, $S = \{v_1, v_2, v_3, \ldots\}$. What should we mean by a linear combination of vectors in S? We might try the same definition: let $c_1, c_2, c_3, \ldots$ be scalars and consider

$$v = \sum_{i=1}^{\infty} c_i v_i = c_1 v_1 + c_2 v_2 + c_3 v_3 + \cdots .$$

Unfortunately, this doesn't make sense. Algebraic operations have to be finite, and here we have an infinite sum. But what does make sense are finite sums. With this in mind, we recall that adding the 0 vector doesn't change anything, i.e., $v + 0 = v$ for any v in $\mathbb{F}^n$, and also that $0w = 0$ for every vector w in $\mathbb{F}^n$, so $v + 0w = v$ for any v and w. Thus we can make sense of an infinite sum as above if only finitely many of the coefficients are nonzero—we just think of leaving out the terms with coefficient 0, and then we are left with a finite sum. We are thus led to the following definition in general.

Definition 1.2.4. Let $S = \{v_1, v_2, v_3, \ldots\}$ be a set of vectors in $\mathbb{F}^n$, and let $c_1, c_2, c_3, \ldots$ be scalars, with only finitely many $c_i \neq 0$. Then

$$\sum_i c_i v_i$$

is a *linear combination* of vectors in S. $\Diamond$

There is one very simple special case of linear combinations we need to call attention to.

Definition 1.2.5. Let $S = \{v_1, v_2, \ldots\}$ be a set of vectors in $\mathbb{F}^n$. If $c_i = 0$ for every i, then $\sum c_i v_i$ is the *trivial* linear combination of the vectors in S. Any other linear combination is *nontrivial*. $\Diamond$

It is easy to see what the value of the trivial combination must be.

Lemma 1.2.6. *Let S be any set of vectors in $\mathbb{F}^n$. Then the value of the trivial combination of the vectors in S is* 0.

Proof. If $S = \{v_1, v_2, \dots\}$, then the trivial linear combination is

$$0v_1 + 0v_2 + 0v_3 + \cdots = 0 + 0 + 0 + \cdots = 0. \qquad \square$$

We now pose two questions about linear combinations, whose importance we will see later on.

Let S be a fixed set of vectors in $\mathbb{F}^n$.

Question 1: Is the trivial combination the *only* linear combination of vectors in S that is equal to 0? If so, we say that S is *linearly independent*.

Question 2: Can *every* vector in $\mathbb{F}^n$ be expressed as a linear combination of the vectors in S? If so, we say that S *spans* $\mathbb{F}^n$.

The case in which the answer to both questions is yes is a particularly important one, and we give it a name.

Definition 1.2.7. Let S be a set of vectors in $\mathbb{F}^n$ that is linearly independent and spans $\mathbb{F}^n$. Then S is a *basis* of $\mathbb{F}^n$. $\diamondsuit$

Theorem 1.2.8. *Let e_i be the vector in $\mathbb{F}^n$ given by*

$$e_i = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \quad \textit{with } a_i = 1 \textit{ and } a_j = 0 \textit{ for } j \neq i.$$

(*In other words, e_i is the vector whose ith entry is* 1 *and all of whose other entries are* 0).

Let $\mathcal{E}_n = \{e_1, e_2, \dots, e_n\}$. Then $\mathcal{E}_n$ is a basis of $\mathbb{F}^n$.

Proof. (1) We are considering the equation $\sum x_i e_i = 0$. Writing out this equation, we see that it is

$$x_1 \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + x_n \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

which evidently only has the solution $x_1 = 0$, $x_2 = 0$, $\dots$, $x_n = 0$.

(2) We are considering the equation $\sum x_i e_i = v$, where v is *any* vector in $\mathbb{F}^n$. Let v be given by $v = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix}$. Writing out this equation, we see that it is

$$x_1 \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + x_n \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix},$$

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix},$$

which evidently has the solution $x_1 = a_1$, $x_2 = a_2$, $\ldots$, $x_n = a_n$. □

Definition 1.2.9. The set $\mathcal{E}_n$ of Theorem 1.2.8 is the *standard basis* of $\mathbb{F}^n$. ◊

We want to emphasize that questions 1 and 2 are independent questions. We have just seen that for $\mathcal{E}_n$, the answers to both questions are yes. But, as we shall see, depending on the choice of S, we may have the answers to these two questions be (yes, yes), (yes, no), (no, yes), or (no, no).

We remark that we have just answered both of these questions in an important special case. But in order for us to be able to answer these questions in general, we will have to build up some machinery. (As you might imagine, if we are calling $\mathcal{E}_n$ the standard basis, there must be other bases as well, and indeed there are.)

We shall also observe that this is another situation in which we have used the same notation to mean two different things. For example, the vector e_1 in $\mathbb{F}^2$ is the vector $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, while the vector e_1 in $\mathbb{F}^3$ is the vector $e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, and these are not the same thing. But this is another case in which it would actually create more confusion to have different notations for each of these, so we will again rely on context to tell them apart.

Finally, we need to take care of a special case. We have defined a linear combination of a set S of k vectors in $\mathbb{F}^n$ where k is a positive integer or where S has infinitely many elements. But what about the case when $k = 0$, i.e., when S is empty? We take care of that case now.

Definition 1.2.10. Let S be the empty subset of $\mathbb{F}^n$. Then the vector 0 in $\mathbb{F}^n$ is the (one and only) linear combination of the vectors in S. Furthermore, this linear combination is trivial. ◊

1.3. Matrices and the equation $Ax = b$

We begin this section by introducing matrices.

Definition 1.3.1. An m-by-n *matrix* with entries in $\mathbb{F}$ (or over $\mathbb{F}$) is an m-by-n array of numbers, each of which is in $\mathbb{F}$. $\Diamond$

Example 1.3.2. Here is a typical matrix:

$$A = \begin{bmatrix} 1 & 3 & 7 \\ 2 & 4 & 9 \end{bmatrix} \quad \text{is a 2-by-3 matrix over } \mathbb{R}. \qquad \Diamond$$

For a matrix A, we will write $A = (a_{ij})$ to mean that a_{ij} is the entry in row i, column j of the matrix A.

Example 1.3.3. For the above matrix A,

$$a_{1,1} = 1, \quad a_{1,2} = 3, \quad a_{1,3} = 7, \quad a_{2,1} = 2, \quad a_{2,2} = 4, \quad a_{2,3} = 9. \qquad \Diamond$$

Example 1.3.4. Let $m = n = 3$, and let a_{ij} be defined by $a_{ii} = 1$, $i = 1, 2, 3$, $a_{ij} = 0$ if $i \neq j$. Then $A = (a_{ij})$ is the matrix

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

Instead of viewing a matrix as composed of its entries, we may view it as composed of its columns. If $v_1, \ldots, v_n$ are vectors in $\mathbb{F}^m$, we write $A = [v_1|v_2|\ldots|v_n]$ to mean that A is the m-by-n matrix whose first column is v_1, whose second column is v_2, $\ldots$, and whose nth column is v_n.

Example 1.3.5. If A is the matrix of Example 1.3.2, writing $A = [v_1|v_2|v_3]$ we have $v_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$, $v_2 = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$, $v_3 = \begin{bmatrix} 7 \\ 9 \end{bmatrix}$. $\Diamond$

Example 1.3.6. Let $\mathcal{E} = \{e_1, e_2, e_3\}$ be the subset of $\mathbb{F}^3$ defined in Definition 1.2.9, $\mathcal{E}_3 = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$. Then $A = [e_1|e_2|e_3]$ is the matrix

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

of Example 1.3.4. $\Diamond$

Evidently, an m-by-n matrix is a rectangular array. In case $m = n$, this array is a square, and so we naturally call an n-by-n matrix a *square matrix*.

We introduce some notation.

Definition 1.3.7. We let $M_{m,n}(\mathbb{F})$ be the set of m-by-n matrices with entries in $\mathbb{F}$. In case $m = n$, we will (often) abbreviate $M_{n,n}(\mathbb{F})$ to $M_n(\mathbb{F})$. $\Diamond$

We now define the product of a matrix and a vector. We will first make the definition, then look at some examples, and then see what it is good for. In fact, we will see that the product of a matrix and a vector has several important interpretations.

Definition 1.3.8. Let $A = (a_{ij})$ be an m-by-n matrix over $\mathbb{F}$, and let $v = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$ be a vector in $\mathbb{F}^n$. Then Av is the vector in $\mathbb{F}^m$ given by

$$Av = \begin{bmatrix} a_{11}c_1 + a_{12}c_2 + \cdots + a_{1n}c_n \\ a_{21}c_1 + a_{22}c_2 + \cdots + a_{2n}c_n \\ \vdots \\ a_{m1}c_1 + a_{m2}c_2 + \cdots + a_{mn}c_n \end{bmatrix}. \qquad \diamond$$

This definition amounts to: "Lay the vector v on its side. Multiply corresponding entries of A and add. Repeat until done."

Let us see this in action.

Example 1.3.9. We wish to compute the product

$$\begin{bmatrix} 1 & 2 & 7 & 4 \\ 0 & 1 & 5 & 6 \\ 2 & 1 & 3 & 5 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \\ 0 \\ 9 \end{bmatrix}.$$

To get the first entry of the answer, we lay the vector on it side, match it up with the first row of the matrix, multiply corresponding entries and add, to obtain:

$$3 \cdot 1 + 1 \cdot 2 + 0 \cdot 7 + 9 \cdot 4 = 41.$$

Similarly for the second entry we obtain:

$$3 \cdot 0 + 1 \cdot 1 + 0 \cdot 5 + 9 \cdot 6 = 55.$$

And similarly for the third entry we obtain:

$$3 \cdot 2 + 1 \cdot 1 + 0 \cdot 3 + 9 \cdot 5 = 52.$$

Now we are done, and we have computed

$$\begin{bmatrix} 1 & 2 & 7 & 4 \\ 0 & 1 & 5 & 6 \\ 2 & 1 & 3 & 5 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \\ 0 \\ 9 \end{bmatrix} = \begin{bmatrix} 41 \\ 55 \\ 52 \end{bmatrix}. \qquad \diamond$$

Example 1.3.10. We wish to compute the product

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & -2 & 6 \\ 0 & 3 & 12 \end{bmatrix} \begin{bmatrix} 3/2 \\ -5 \\ 1/2 \end{bmatrix}. \qquad \diamond$$

This time we will combine the steps:

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & -2 & 6 \\ 0 & 3 & 12 \end{bmatrix} \begin{bmatrix} 3/2 \\ -5 \\ 1/2 \end{bmatrix} = \begin{bmatrix} (3/2) \cdot 1 + (-5) \cdot 0 + (1/2) \cdot 5 \\ (3/2) \cdot 2 + (-5) \cdot (-2) + (1/2) \cdot 6 \\ (3/2) \cdot 0 + (-5) \cdot 3 + (1/2) \cdot 12 \end{bmatrix} = \begin{bmatrix} 4 \\ 16 \\ -9 \end{bmatrix}.$$

Example 1.3.11. We may also consider the case where the entries of the vector are unknowns. We compute:

$$\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 + 2x_2 \\ 3x_1 + 7x_2 \end{bmatrix}. \qquad \Diamond$$

We record the following general computation for future use.

Lemma 1.3.12. *Let A be an m-by-n matrix and write $A = [u_1|u_2|\dots|u_n]$. Let e_i be the vector in $\mathbb{F}^n$ given in Theorem 1.2.8. Then*

$$Ae_i = u_i.$$

Proof. Direct computation. $\square$

We have said that the product of a matrix and a vector has several interpretations. Let us see what they are.

Observation 1.3.13. Interpretation I: Let us consider a system of m linear equations in n unknowns, with entries in $\mathbb{F}$. By definition, this is a system of equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

where each coefficient a_{ij} is in $\mathbb{F}$, and also where each b_i is in $\mathbb{F}$. Let

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}, \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \qquad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}.$$

A is an m-by-n matrix with entries in $\mathbb{F}$, x is the vector of unknowns, a vector with n entries (and so representing an unknown vector in $\mathbb{F}^n$), and b is the vector consisting of the entries on the right-hand side of these equations, a vector in $\mathbb{F}^m$.

Then, examining our definition of the product of a matrix and a vector (Definition 1.3.8), we see that the product Ax is just the left-hand side of this system of linear equations. We also see that the vector equation $Ax = b$ is simply an encoding (or rewriting) of this system.

Also, if $v = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$ is a vector in $\mathbb{F}^n$, then $x_1 = c_1$, $x_2 = c_2$, $\dots$, $x_n = c_n$ is a solution of this system exactly when $Av = b$ (i.e., if $Av = b$ it is a solution while if $Av \neq b$ it is not).

(Compare Example 1.3.11 and Example 1.2.3.) $\Diamond$

Observation 1.3.14. Interpretation II: Let us go back to Definition 1.3.8 and simply rewrite the answer.

$$
\begin{aligned}
Av &= \begin{bmatrix} a_{11}c_1 + a_{12}c_2 + \cdots + a_{1n}c_n \\ a_{21}c_1 + a_{22}c_2 + \cdots + a_{2n}c_n \\ \vdots \\ a_{m1}c_1 + a_{m2}c_2 + \cdots + a_{mn}c_n \end{bmatrix} \\
&= \begin{bmatrix} a_{11}c_1 \\ a_{21}c_1 \\ \vdots \\ a_{m1}c_1 \end{bmatrix} + \begin{bmatrix} a_{12}c_2 \\ a_{22}c_2 \\ \vdots \\ a_{m2}c_2 \end{bmatrix} + \cdots + \begin{bmatrix} a_{1n}c_n \\ a_{2n}c_n \\ \vdots \\ a_{mn}c_n \end{bmatrix} \\
&= c_1 \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} + c_2 \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} + \cdots + c_n \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix}
\end{aligned}
$$

We see that Av is then a linear combination of vectors. To be precise, let u_i be the vector $u_i = \begin{bmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{mi} \end{bmatrix}$ for each $i = 1, \ldots, n$. Then $Av = c_1u_1 + c_2u_2 + \cdots + c_nu_n$.

Returning to the matrix A, we see that it is just

$$
A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix},
$$

and we notice that u_i is precisely the ith column of A. In our previous notation, $A = [u_1|u_2|\ldots|u_n]$.

Summarizing, we see that Av is the linear combination of the columns A with coefficients given by the entries of v. That is,

$$
[u_1|u_2|\ldots|u_n] \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = c_1u_1 + c_2u_2 + \cdots + c_nu_n.
$$

If we now consider the equation $Ax = b$, where x is a vector of unknowns, we see that this is the equation $x_1u_1 + x_2u_2 + \cdots + x_nu_n = b$, and this equation will have a solution precisely when it is possible to express the vector b as a linear combination of the vectors $u_1, \ldots, u_n$, i.e., as a linear combination of the columns of A. Furthermore, this equation has a solution $x_1 = c_1$, $x_2 = c_2$, $\ldots$, $x_n = c_n$ precisely when $Av = b$, where $v = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$.

(Compare Example 1.3.10 and Example 1.2.2.) $\Diamond$

Observation 1.3.15. Interpretation III: Remember that in general a function $f\colon X \to Y$ is simply a rule that assigns an element of Y to each element of X, $y = f(x)$.

Let us fix an m-by-n matrix A. Then for any vector v in $\mathbb{F}^n$, we have the vector Av in $\mathbb{F}^m$. In other words, multiplication by an m-by-n matrix A gives a function from $\mathbb{F}^n$ to $\mathbb{F}^m$. This function is so important we give it a name:

$$\mathcal{T}_A \text{ is the function } \mathcal{T}_A\colon \mathbb{F}^n \to \mathbb{F}^m, \text{ given by } \mathcal{T}_A = Av.$$

Thus we see that for a vector v, Av is the value of the function $\mathcal{T}_A$ at the vector v.

For example, let A be the matrix of Example 1.3.9. Then A is a 3-by-4 matrix, so $\mathcal{T}_A$ is the function from $\mathbb{F}^4$ to $\mathbb{F}^3$. Then the computation of Example 1.3.9 shows that

$$\mathcal{T}_A\left(\begin{bmatrix} 3 \\ 1 \\ 0 \\ 9 \end{bmatrix}\right) = \begin{bmatrix} 41 \\ 55 \\ 22 \end{bmatrix}.$$

If A is the matrix of Example 1.3.10, a 3-by-3 matrix, then $\mathcal{T}_A$ is the function from $\mathbb{F}^3$ to $\mathbb{F}^3$, and the computation there shows that

$$\mathcal{T}_A\left(\begin{bmatrix} 3/2 \\ -5 \\ 1/2 \end{bmatrix}\right) = \begin{bmatrix} 4 \\ 16 \\ -9 \end{bmatrix}.$$

In general, a function is given by a rule, not necessarily by a formula. But in our case, $\mathcal{T}_A$ is in fact given by a formula. If $A = (a_{ij})$ is the m-by-n matrix whose entry in the (i,j) position is a_{ij}, and $x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ is a vector of unknowns, then $\mathcal{T}_A\colon \mathbb{F}^n \to \mathbb{F}^m$ is given by the formula in Definition 1.3.8:

$$\mathcal{T}_A(x) = \mathcal{T}_A\left(\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}\right) = A\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{bmatrix}.$$

In this interpretation, the equation $Ax = b$ is just the equation $\mathcal{T}_A(x) = b$. Thus asking whether $Ax = b$ has a solution is asking whether $\mathcal{T}_A(v) = b$ for some v in $\mathbb{F}^n$, i.e., asking whether there is some vector v in $\mathbb{F}^n$ for which the value of the function $\mathcal{T}_A$ at v is b. (Then, of course, if v is a vector with $\mathcal{T}_A(v) = b$, then v is a solution of $\mathcal{T}_A(x) = b$, while if $\mathcal{T}_A(v) \neq b$, then v is not a solution.)

For example, referring to Example 1.3.11 and Example 1.2.3, if $\mathcal{T}_A$ is the function

$$\mathcal{T}_A(x) = \mathcal{T}_A\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = A\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 + 2x_2 \\ 3x_1 + 7x_2 \end{bmatrix},$$

then $\mathcal{T}_A(x) = \begin{bmatrix} 2 \\ 9 \end{bmatrix}$ has the unique solution $x = \begin{bmatrix} -4 \\ 3 \end{bmatrix}$. $\Diamond$

Remark 1.3.16. All three of these interpretations are important, and you will need to be able to fluently translate between them. But as we will see, it is the third interpretation that is truly fundamental. $\Diamond$

1.4. The basic counting theorem

A good mathematical theory is one that reduces hard problems to easy ones. Linear algebra is such a theory. Many linear algebra problems can be reduced to simple counting. In this section we present the basic counting argument, from which all of the other counting arguments derive.

As you will see, this is a theorem about solutions of systems of linear equations. As you will also see, we will be devoting the entire next chapter to solving linear equations. So why do we do this one here? The answer is that we want to emphasize the logical simplicity of this result. In the next chapter we will be seeing how to actually go about solving systems, so there will necessarily be a lot of discussion of mechanics. Although we will try to keep our attention focused on the logical structure, the presence of the mechanics means we will run the risk of losing sight of the forest for the trees. To avoid that danger, we single out this result here.

There is another reason, and that is the logical simplicity of its proof. Not only is the statement simple, but, more importantly, its proof is logically very simple as well. By that we mean that it uses almost nothing (other than mathematical induction) beyond the basic notions themselves.

We have put this theorem in Section 4 of this chapter because we wanted to create a context for it first. But you will notice that we won't use anything from Sections 1 through 3 in either its statement or its proof—if we had wanted to, we could have put this theorem as absolutely the first thing we have said in this book.

Consider a system of m linear equations in n unknowns:

$$(*) \qquad \begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m. \end{aligned}$$

We begin with a lemma.

Lemma 1.4.1. *Let $(*')$ be a system of linear equations obtained from $(*)$ by adding a multiple of one equation to another (and leaving all the others unchanged). Then $(*)$ and $(*')$ have the same solutions.*

Proof. We leave it to the reader to check that if $(*')$ is obtained from $(*)$ by adding $c \cdot$ equation i to equation j, for some c, i, and j, then every solution of $(*)$ is also a solution of $(*')$.

But now observe that $(*)$ is obtained from $(*')$ by adding $(-c) \cdot$ equation i of $(*')$ to equation j of $(*')$. So by exactly the same logic, any solution of $(*')$ is a solution of $(*)$.

Hence $(*)$ and $(*')$ have the same solutions. $\square$

Definition 1.4.2. The system $(*)$ is *homogeneous* if $b_1 = b_2 = \cdots = b_m = 0$. Otherwise it is *inhomogeneous* (or *nonhomogeneous*). $\Diamond$

Observation 1.4.3. A homogeneous system $(*)$ always has the solution $x_1 = x_2 = \cdots = x_n = 0$. $\Diamond$

Definition 1.4.4. The solution $x_1 = x_2 = \cdots = x_n = 0$ of a homogeneous system $(*)$ is the *trivial solution*. Any other solution is a *nontrivial solution*. $\Diamond$

Here is the (absolutely, fundamentally, most) basic result.

Theorem 1.4.5 (Basic counting theorem)**.** *A homogeneous system of m linear equations in n unknowns with $n > m$ always has a nontrivial solution.*

Proof. It is convenient to introduce the following language. We will say that a linear equation $c_1x_1 + c_2x_2 + \cdots + c_nx_n = 0$ *involves* x_i if the coefficient c_i of x_i in this equation is nonzero.

We prove the theorem by induction on the number of equations m.

We begin with the case $m = 1$. So suppose we have a single homogeneous equation in $n > 1$ unknowns

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0.$$

There are two possibilities: either this equation involves x_1 or it doesn't.

If it doesn't involve x_1 it has the nontrivial solution

$$x_1 = 1, \quad x_2 = x_3 = \cdots = x_n = 0.$$

If it does involve x_1 it has the nontrivial solution

$$x_1 = -a_{12}/a_{11}, \quad x_2 = 1, \quad x_3 = \cdots = x_n = 0.$$

Now suppose the theorem is true for all homogeneous systems of m equations in n unknowns with $n > m$, and consider a homogeneous system of $m+1$ equations in n unknowns with $n > m+1$. For simplicity of notation, set $\bar{m} = m+1$. Thus we have a system

$$(*) \qquad \begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{\bar{m}1}x_1 + \cdots + a_{\bar{m}n}x_n &= 0. \end{aligned}$$

There are two possibilities: either no equation involves x_1 or at least one equation does.

If no equation involves x_1, this system has the nontrivial solution

$$x_1 = 1, \quad x_2 = \cdots = x_n = 0.$$

Suppose at least one equation does involve x_1. Choose any such equation, say equation i. Now for each $j \neq i$, add $(-a_{j1}/a_{i1})$ times equation i to equation j. If equation j does not involve x_1, this is doing nothing, as then $a_{j1} = 0$ so $-a_{j1}/a_{i1} = 0$. But if equation j does involve x_1, this is certainly doing something. To be precise, in the resulting equation

$$a'_{j1}x_1 + a'_{j2}x_2 + \cdots + a'_{jn}x_n = 0$$

we have

$$a'_{j1} = a_{j1} + (-a_{j1}/a_{i1})a_{i1} = 0.$$

Thus in system $(*')$, none of the equations involves x_1, except for equation i. In other words, system $(*')$ is a system of the form

$$(*') \qquad \begin{aligned} a'_{12}x_2 + \cdots + a'_{1n}x_n &= 0 \\ a'_{22}x_2 + \cdots + a'_{2n}x_n &= 0 \\ &\vdots \\ a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n &= 0 \\ &\vdots \\ a'_{\bar{m}2}x_2 + \cdots + a'_{\bar{m}n}x_n &= 0. \end{aligned}$$

But now notice that, omitting equation i, we have a homogeneous system of $\bar{m} - 1$ equations in the unknowns $x_2, \ldots, x_n$, i.e., a homogeneous system of m equations in the $n-1$ unknowns $x_2, \ldots, x_n$. Since $n > m+1$, $n-1 > m$, so by the inductive hypothesis this system has a nontrivial solution

$$x_2 = s_2, \quad \ldots, \quad x_n = s_n.$$

Then we see that the system $(*')$ has a nontrivial solution

$$x_1 = s_1 = (-1/a_{i1})(a_{i2}s_2 + a_{i3}s_3 + \cdots + a_{in}s_n), \quad x_2 = s_2, \quad \ldots, \quad x_n = s_n.$$

(This is nontrivial since not all of $s_2, \ldots, s_n$ are zero, so, whether or not $s_1 = 0$, not all of $s_1, \ldots, s_n$ are zero.)

But we saw in Lemma 1.4.1 that adding a multiple of one equation to another does not change the solutions. We obtained $(*')$ from $(*)$ by a sequence of these steps. Thus $(*)$ and $(*')$ have the same solutions. In particular, our nontrivial solution to $(*')$ is a nontrivial solution to $(*)$.

Thus $(*)$ has a nontrivial solution, completing the inductive step.

Hence, by induction, we conclude the theorem is true for every positive integer m. □

Here is the other side of the coin.

Theorem 1.4.6. *For any system of m linear equations in n unknowns with $n < m$ there is some right-hand side for which this system does not have a solution.*

Proof. We prove the theorem by induction on the number of unknowns n.

We begin with the case $n = 1$. So suppose we have $m > 1$ equations in one unknown. Consider the first two equations:

$$\begin{aligned} a_{11}x_1 &= b_1, \\ a_{21}x_1 &= b_2. \end{aligned}$$

If $a_{11} = 0$, then set $b_1 = 1$. This equation becomes $0 = 1$, which has no solution, and then the entire system has no solution.

If $a_{11} \neq 0$, then set $b_1 = 0$, and $b_2 = 1$. If $a_{21} = 0$, then the second equation has no solution, while if $a_{21} \neq 0$, the first equation forces $x_1 = 0$ while the second equation forces $x_1 \neq 0$, so this pair of equations, and hence the entire system, has no solution.

Now suppose the theorem is true for all systems of m equations in n unknowns with $n < m$, and consider a homogeneous system of m equations in $n+1$ unknowns with $n+1 < m$. For simplicity of notation, set $\bar{n} = n + 1$. Thus we have a system

$$(*) \qquad \begin{aligned} a_{11}x_1 + \cdots + a_{1\bar{n}}x_{\bar{n}} &= b_1 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{m\bar{n}}x_{\bar{n}} &= b_m. \end{aligned}$$

There are two possibilities: either no equation involves x_1 or at least one equation does.

If no equation involves x_1, then we may regard this system as a system in the n unknowns $x_2, \ldots, x_{\bar{n}}$, and $n < \bar{n} < m$, so by the inductive hypothesis there are values $b_1, \ldots, b_m$ for which this system has no solution.

Suppose at least one equation does involve x_1. Choose any such equation, say equation i. Set $b_i = 0$. Now for each $j \neq i$, add $(-a_{j1}/a_{i1})$ times equation i to equation j. If equation j does not involve x_1, this is doing nothing, as then $a_{j1} = 0$ so $-a_{j1}/a_{i1} = 0$. But if equation j does involve x_1, this is certainly doing something. To be precise, in the resulting equation

$$a'_{j1}x_1 + a'_{j2}x_2 + \cdots + a'_{jn}x_n = b'_j$$

we have

$$a'_{j1} = a_{j1} + (-a_{j1}/a_{i1})a_{i1} = 0 \qquad \text{and} \qquad b'_j = b_j + (-a_{j1}/a_{i1})0 = b_j.$$

Thus in system $(*')$, none of the equations involves x_1, except for equation i, and also all the entries on the right-hand side are the same as in system $(*)$. In other words, system $(*')$ is a system of the form

$$
(*') \qquad \begin{aligned}
a'_{12}x_2 + \cdots + a'_{1\bar{n}}x_{\bar{n}} &= b_1 \\
2a'_{22}x_2 + \cdots + a'_{2\bar{n}}x_{\bar{n}} &= b_2 \\
&\vdots \\
a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{i\bar{n}}x_{\bar{n}} &= 0 \\
&\vdots \\
a'_{m2}x_2 + \cdots + a'_{m\bar{n}}x_{\bar{n}} &= b_m.
\end{aligned}
$$

But now notice that, omitting equation i, we have a system of $m-1$ equations in the n unknowns $x_2, \ldots, x_{\bar{n}}$. Since $n+1 < m$, $n < m-1$, so by the inductive hypothesis there are values b_j for $j = 1, \ldots, m,\ j \neq i$ for which this system has no solution.

Then we see that the system $(*')$ has no solution for these values of b_j, and also $b_i = 0$.

But we saw in Lemma 1.4.1 that adding a multiple of one equation to another does not change the solutions. We obtained $(*')$ from $(*)$ by a sequence of these steps. Thus $(*)$ and $(*')$ have the same solutions. In particular, since $(*')$ does not have a solution, neither does $(*)$.

Thus $(*)$ does not have a solution, completing the inductive step.

Hence, by induction, we conclude the theorem is true for every positive integer n. □

Given our interpretations of the product of a matrix and a vector, we can immediately draw some conclusions from these two results.

Corollary 1.4.7. (1) *Let A be an m-by-n matrix with $n > m$. Then there is a nonzero vector v in $\mathbb{F}^n$ with $Av = 0$.*

(2) *Let A be an m-by-n matrix with $n > m$. Then there is a nonzero vector v in $\mathbb{F}^n$ with $\mathcal{T}_A(v) = 0$.*

(3) *Let $S = \{u_1, u_2, \ldots, u_m\}$ be a set of $n > m$ vectors in $\mathbb{F}^m$. Then some nontrivial linear combination of the vectors in S is equal to 0.*

Proof. We leave this translation to the reader. □

Corollary 1.4.8. (1) *Let A be an m-by-n matrix with $n < m$. Then there is a vector b in $\mathbb{F}^m$ such that $Av \neq b$ for any vector v in $\mathbb{F}^n$.*

(2) *Let A be an m-by-n matrix with $n < m$. Then there is a vector b in $\mathbb{F}^m$ such that $\mathcal{T}_A(v) \neq b$ for any vector v in $\mathbb{F}^n$.*

(3) *Let $S = \{u_1, u_2, \ldots, u_n\}$ be a set of $n < m$ vectors in $\mathbb{F}^m$. Then there is a vector b in $\mathbb{F}^m$ that cannot be expressed as a linear combination of the vectors in S.*

Proof. We also leave this translation to the reader. □

1.5. Matrices and linear transformations

We have seen that, given an m-by-n matrix A, we have the function $\mathcal{T}_A \colon \mathbb{F}^n \to \mathbb{F}^m$ defined by $\mathcal{T}_A(v) = Av$. We shall study these functions and relate them to linear transformations, which are special kinds of functions, but precisely the kinds of functions we wish to study, between vector spaces.

Let us begin by observing some properties of the product Av, where A is a matrix and v is a vector.

Lemma 1.5.1. *Let A be an m-by-n matrix.*

(1) *For any vectors v_1 and v_2 in $\mathbb{F}^n$,*
$$A(v_1 + v_2) = Av_1 + Av_2.$$
(2) *For any vector v in $\mathbb{F}^n$ and any scalar c,*
$$A(cv) = c(Av).$$
(3) *Let $v_1, \dots, v_k$ be any k vectors in $\mathbb{F}^n$, and let $c_1, \dots, c_k$ be any k scalars. Then*
$$A(c_1v_1 + c_2v_2 + \cdots + c_kv_k) = c_1(Av_1) + c_2(Av_2) + c_k(Av_k).$$

Proof. Parts (1) and (2) follow by direct computation, which we leave to the reader. To prove (3), we apply (1) and (2) repeatedly:
$$\begin{aligned} A(c_1v_1 + c_2v_2 + \cdots + c_kv_k) &= A(c_1v_1) + A(c_2v_2) + \cdots + A(c_kv_k) \\ &= c_1(Av_1) + c_2(Av_2) + \cdots + c_k(Av_k). \end{aligned}$$ □

Corollary 1.5.2. *Let A be an m-by-n matrix.*

(1) *For any vectors v_1 and v_2 in $\mathbb{F}^n$,*
$$\mathcal{T}_A(v_1 + v_2) = \mathcal{T}_A(v_1) + \mathcal{T}(v_2).$$
(2) *For any vector v on $\mathbb{F}^n$ and any scalar c,*
$$\mathcal{T}_A(cv) + c\mathcal{T}_A(v).$$

Proof. Since $\mathcal{T}_A(v) = Av$, this is simply a restatement of the lemma. □

Functions satisfying these properties are so important that we give them a name.

Definition 1.5.3. Let $\mathcal{T} \colon \mathbb{F}^n \to \mathbb{F}^m$ be a function that satisfies the following properties:

(1) For any vectors v_1 and v_2 in $\mathbb{F}^n$,
$$\mathcal{T}(v_1 + v_2) = \mathcal{T}(v_1) + \mathcal{T}(v_2).$$
(2) For any vector v in $\mathbb{F}^n$ and any scalar c,
$$\mathcal{T}(cv) = c\mathcal{T}(v).$$

Then $\mathcal{T}$ is a *linear transformation.* ◊

Corollary 1.5.4. *Let A be an m-by-n matrix. Then $\mathcal{T}_A \colon \mathbb{F}^n \to \mathbb{F}^m$ is a linear transformation.*

Proof. This is just a translation of Corollary 1.5.2 into the language of Definition 1.5.3. □

Properties (1) and (2) have a generalization.

Lemma 1.5.5. *Let $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^m$ be a linear transformation.*

(3) *Let $v_1, \ldots, v_k$ be any k vectors in $\mathbb{F}^n$, and let $c_1, \ldots, c_k$ be any k scalars. Then*

$$\mathcal{T}(c_1v_1 + c_2v_2 + \cdots + c_kv_k) = c_1\mathcal{T}(v_1) + c_2\mathcal{T}(v_2) + \cdots + c_k\mathcal{T}(v_k).$$

Proof. Applying properties (1) and (2) repeatedly, we have:

$$\begin{aligned}\mathcal{T}(c_1v_1 + c_2v_2 + \cdots + c_kv_k) &= \mathcal{T}(c_1v_1) + \mathcal{T}(c_2v_2) + \cdots + \mathcal{T}(c_kv_k)\\ &= c_1\mathcal{T}(v_1) + c_2\mathcal{T}(v_2) + \cdots + c_k\mathcal{T}(v_k).\end{aligned}$$ □

Remark 1.5.6. Before proceeding any further, we should ask why we care about linear transformations.

The answer is that $\mathbb{F}^n$ is not simply a set of vectors, but rather a structure: a set of vectors together with two operations, vector addition and scalar multiplication (which satisfies the properties of Theorem 1.1.4), and similarly for $\mathbb{F}^m$. Thus we want to consider functions that "respect" that structure, and those are precisely what we are calling linear transformations. For a linear transformation $\mathcal{T}$, (1) the value of $\mathcal{T}$ on a sum $v_1 + v_2$ of two vectors is the sum of the values of $\mathcal{T}$ on each of the vectors, and (2) the value of $\mathcal{T}$ on a scalar multiple cv of a vector v is c times its value on the vector v. ◊

We have just seen (Corollary 1.5.4) that for any matrix A, $\mathcal{T}_A$ is a linear transformation. We now see that we get all linear transformations in this way.

Theorem 1.5.7. *Let $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^m$ be a linear transformation. Then $\mathcal{T} = \mathcal{T}_A$ for some unique matrix A.*

Proof. Let $u_1 = \mathcal{T}(e_1)$, $u_2 = \mathcal{T}(e_2)$, $\ldots$, $u_n = \mathcal{T}(e_n)$, where $e_1, e_2, \ldots, e_n$ are the vectors of Definition 1.2.10. Let A be the matrix

$$A = [u_1|u_2|\ldots|u_n].$$

We claim that $\mathcal{T} = \mathcal{T}_A$.

To show this we must show that $\mathcal{T}(v) = \mathcal{T}_A(v)$ for every vector v in $\mathbb{F}^n$. We will do so by computing $\mathcal{T}(v)$ and $\mathcal{T}_A(v)$ separately and seeing that we get the same answer.

Let $v = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$. We first compute $\mathcal{T}(v)$.

Referring to the proof of Theorem 1.2.8, we see that

$$v = c_1e_1 + c_2e_2 + \cdots + c_ne_n$$

and then by property (3) of a linear transformation we have

$$\begin{aligned}\mathcal{T}(v) &= \mathcal{T}(c_1e_1 + c_2e_2 + \cdots + c_ne_n)\\ &= c_1\mathcal{T}(e_1) + c_2\mathcal{T}(e_2) + \cdots + c_n\mathcal{T}(e_n)\\ &= c_1u_1 + c_2u_2 + \cdots + c_nu_n.\end{aligned}$$

Next we compute $\mathcal{T}_A(v)$:

$$\begin{aligned}\mathcal{T}_A(v) = Av = A\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} &= [u_1|u_2|\dots|u_n]\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}\\ &= c_1u_1 + c_2u_2 + \cdots + c_nu_n\end{aligned}$$

by Observation 1.3.14.

Thus $\mathcal{T}(v)$ and $\mathcal{T}_A(v)$ are equal, as claimed.

To complete the proof, we need to show that the matrix A is unique. We do this in the standard way we show that something is unique: we suppose that there are two of them, and show they must be the same.

So suppose $\mathcal{T} = \mathcal{T}_A = \mathcal{T}_{A'}$. Write $A = [u_1|u_2|\dots|u_n]$ and $A' = [u_1'|u_2'|\dots|u_n']$.

Then for every vector v in $\mathbb{F}^n$, $\mathcal{T}(v) = \mathcal{T}_A(v) = \mathcal{T}_{A'}(v)$. In particular, this is true for $v = e_1, e_2, \dots, e_n$. Let $v = e_i$. We compute

$$\mathcal{T}(e_i) = \mathcal{T}_A(e_i) = Ae_i = u_i$$

and

$$\mathcal{T}(e_i) = \mathcal{T}_{A'}(e_i) = A'e_i = u_i'.$$

Thus $u_i' = \mathcal{T}(e_i) = u_i$, so $u_i' = u_i$ for each i. But then

$$A' = [u_1'|u_2'|\dots|u_n'] = [u_1|u_2|\dots|u_n] = A,$$

as claimed. □

Actually, the proof of Theorem 1.5.7 showed a more precise result. Not only did it show that there is some matrix A for which $\mathcal{T} = \mathcal{T}_A$, it gave a formula for that matrix.

Corollary 1.5.8. *Let $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^m$ be a linear transformation. Let A be the matrix*

$$A = [\mathcal{T}(e_1)|\mathcal{T}(e_2)|\dots|\mathcal{T}(e_n)].$$

Then $\mathcal{T} = \mathcal{T}_A$.

Proof. By the proof of Theorem 1.5.7, $\mathcal{T} = \mathcal{T}_A$ for

$$A = [u_1|u_2|\dots|u_n],$$

where $u_1 = \mathcal{T}(e_1)$, $u_2 = \mathcal{T}(e_2)$, $\dots$, $u_n = \mathcal{T}(e_n)$, so A is as claimed. □

This leads us to make a definition.

Definition 1.5.9. Let $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^m$ be a linear transformation. Let A be the matrix
$$A = [\mathcal{T}(e_1)|\mathcal{T}(e_2)|\dots|\mathcal{T}(e_n)]$$
so that $\mathcal{T} = \mathcal{T}_A$.

Then A is the *standard matrix* of $\mathcal{T}$. ◊

Let us compute a few standard matrices.

Lemma 1.5.10. *Let $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^m$ be the 0 linear transformation, given by $\mathcal{T}\left(\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}\right) = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$. Then the standard matrix of $\mathcal{T}$ is the m-by-n 0 matrix, i.e., the matrix all of whose entries are 0.*

Proof. The standard matrix of $\mathcal{T}$ is
$$[\mathcal{T}(e_1)|\dots|\mathcal{T}(e_n)] = \left[\begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}\middle|\dots\middle|\begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}\right].$$ □

Lemma 1.5.11. *Let $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^n$ be the identity linear transformation,*
$$\mathcal{T}\left(\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}\right) = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$
Then the standard matrix of $\mathcal{T}$ is the matrix I_n, the n-by-n matrix all of whose diagonal entries are 1 and all of whose off-diagonal entries are 0.

Proof. The standard matrix of $\mathcal{T}$ is
$$[\mathcal{T}(e_1)|\dots|\mathcal{T}(e_n)] = [e_1|\dots|e_n].$$ □

Definition 1.5.12. The matrix I_n is the n-by-n *identity matrix.* ◊

We write down I_n explicitly for small values of n:
$$I_1 = [1], \quad I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

We will often just write I for I_n when the value of n is known from the context.

Lemma 1.5.13. *Let $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^n$ be a linear transformation*
$$\mathcal{T}\left(\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}\right) = c\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} ca_1 \\ \vdots \\ ca_n \end{bmatrix}.$$
Then the standard matrix of $\mathcal{T}$ is the n-by-n matrix all of whose diagonal entries are c and all of whose off-diagonal entries are 0.

Proof. The standard matrix of $\mathcal{T}$ is

$$[\mathcal{T}(e_1)|\dots|\mathcal{T}(e_n)] = [ce_1|\dots|ce_n]. \qquad \square$$

A matrix of the above form (all diagonal entries equal, all off-diagonal entries 0) is known as a *scalar matrix*.

Remark 1.5.14. As we will see, the results of this section are useful in two ways.

On the one hand, we will be developing powerful techniques for calculating with and manipulating matrices, so we will be able to translate these into conclusions about linear transformations.

On the other hand, we will be thinking hard about linear transformations, and we will be able to translate our results into conclusions about matrices (with little or no computation necessary).

But on the third hand (?), we should point out that linear transformations are our main focus of interest, and sometimes it is best to keep our focus on them without bringing in matrices at all. $\Diamond$

1.6. Exercises

1. (a) Prove Theorem 1.1.4.
   (b) Prove Theorem 1.1.5.

2. Find a nontrivial solution to each of these homogeneous systems of equations:
   (a) $x_1 + 2x_2 = 0.$
   (b)
   $$\begin{aligned} x_1 - x_2 + x_3 &= 0, \\ 3x_1 - 2x_2 + 6x_3 &= 0. \end{aligned}$$
   (c)
   $$\begin{aligned} x_1 + 2x_2 - x_3 &= 0, \\ -x_1 - x_2 + x_3 + 3x_4 &= 0, \\ x_1 + 3x_2 + x_4 &= 0. \end{aligned}$$

3. In each case, find values of the right-hand side for which each of these systems has no solution:
   (a)
   $$\begin{aligned} x_1 &= b_1, \\ 2x_1 &= b_2. \end{aligned}$$
   (b)
   $$\begin{aligned} x_1 + x_2 &= b_1, \\ x_1 + 2x_2 &= b_2, \\ 2x_1 + 5x_2 &= b_3. \end{aligned}$$
   (c)
   $$\begin{aligned} x_1 + x_2 + x_3 &= b_1, \\ -x_1 + 3x_3 &= b_2, \\ x_1 + 3x_2 + 6x_3 &= b_3, \\ 2x_1 + x_2 + 4x_3 &= b_4. \end{aligned}$$

4. In each case, compute the product:

(a) $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 5 \\ 6 \end{bmatrix}$.

(b) $\begin{bmatrix} 2 & 3 & 5 \\ 1 & 4 & 9 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}$.

(c) $\begin{bmatrix} 1 & 5 \\ 2 & 6 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} 7 \\ 11 \end{bmatrix}$.

(d) $\begin{bmatrix} 1 & 3 & 7 \\ 2 & 6 & 3 \\ 5 & 0 & 8 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 6 \end{bmatrix}$.

(e) $\begin{bmatrix} 1 & 4 & 2 & 6 \\ 0 & 1 & 3 & 5 \\ 1 & 2 & 4 & 3 \\ 8 & 0 & 2 & 5 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 0 \\ 6 \end{bmatrix}$.

5. Let A be the matrix

$$A = \begin{bmatrix} 1 & 4 & 10 \\ 3 & 14 & 35 \\ 0 & 3 & 8 \end{bmatrix}.$$

Let $v_1 = \begin{bmatrix} 7 \\ -24 \\ 9 \end{bmatrix}$, $v_2 = \begin{bmatrix} -2 \\ 8 \\ 3 \end{bmatrix}$, and $v_3 = \begin{bmatrix} 0 \\ -5 \\ 2 \end{bmatrix}$. Compute Av_1, Av_2, and Av_3.

6. Let A be the matrix

$$A = \begin{bmatrix} 1286 & -321 & 180 \\ 5564 & -1389 & 780 \\ 792 & -198 & 113 \end{bmatrix}.$$

Let $v_1 = \begin{bmatrix} 1 \\ 4 \\ 0 \end{bmatrix}$, $v_2 = \begin{bmatrix} 15 \\ 65 \\ 8 \end{bmatrix}$, and $v_3 = \begin{bmatrix} 18 \\ 78 \\ 11 \end{bmatrix}$.

Show that $Av_1 = 2v_1$, $Av_2 = 3v_2$, and $Av_3 = 5v_3$.

7. (a) Let 0 be the m-by-n zero matrix. Show by direct computation that $0v = 0$ for every vector v in $\mathbb{F}^n$.

(b) Recall that I_n denotes the n-by-n identity matrix. Show by direct computation that $I_n v = v$ for every vector v in $\mathbb{F}^n$.

8. (a) Show that $S_1 = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 4 \\ 7 \end{bmatrix} \right\}$ is linearly independent and spans $\mathbb{F}^2$ (and hence is a basis for $\mathbb{F}^2$).

(b) Show that $S_2 = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 4 \\ 8 \end{bmatrix} \right\}$ is not linearly independent and does not span $\mathbb{F}^2$.

(c) Show that $S_3 = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 4 \\ 9 \end{bmatrix} \right\}$ is linearly independent and spans $\mathbb{F}^2$ (and hence is a basis for $\mathbb{F}^2$).

9. (a) Show that $T_1 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix} \right\}$ is linearly independent but does not span $\mathbb{F}^3$.

(b) Show that $T_2 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 0 \end{bmatrix} \right\}$ spans $\mathbb{F}^3$ but is not linearly independent.

(c) Show that $T_3 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix} \right\}$ is linearly independent and spans $\mathbb{F}^3$ (and hence is a basis for $\mathbb{F}^3$).

(d) Show that $T_4 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 0 \end{bmatrix} \right\}$ is not linearly independent and does not span $\mathbb{F}^3$.

10. (a) Show that $U_1 = [1]$ is a basis of $\mathbb{F}^1$.

(b) Show that $U_2 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \end{bmatrix} \right\}$ is a basis of $\mathbb{F}^2$.

(c) Show that $U_3 = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix} \right\}$ is a basis of $\mathbb{F}^3$.

(d) Show that $U_4 = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 4 \\ 5 \\ 6 \\ 0 \end{bmatrix}, \begin{bmatrix} 7 \\ 8 \\ 9 \\ 10 \end{bmatrix} \right\}$ is a basis of $\mathbb{F}^4$.

11. An n-by-n matrix $A = (a_{ij})$ is called upper triangular if all the entries below the diagonal are 0, i.e., $a_{ij} = 0$ for $i > j$. Suppose that A is an upper triangular n-by-n matrix all of whose diagonal entries are nonzero, i.e., $a_{ii} \neq 0$ for $i = 1, \ldots, n$.

Write $A = [u_1|u_2|\ldots|u_n]$. Show that $S = \{u_1, u_2, \ldots, u_n\}$ is a basis of $\mathbb{F}^n$.

12. For a vector u in $\mathbb{F}^{n-1}$, let u' be the vector in $\mathbb{F}^n$ whose first $n-1$ entries are the same as those of u, and whose nth entry is 0.

Let $S = \{u_1, \ldots, u_{n-1}\}$ be any basis of $\mathbb{F}^{n-1}$. Let v_n be any vector in $\mathbb{F}^n$ whose nth entry is nonzero. Show that $T = \{u_1', \ldots, u_{n-1}', v_n\}$ is a basis of $\mathbb{F}^n$.

13. Let $S = \{v_1, \ldots, v_n\}$ be any basis of $\mathbb{F}^n$.

(a) Let S' be the set of vectors obtained from S in one of the following ways:

(i) for some i and j, adding a times v_i to v_j, for some scalar a;

(ii) for some i, multiplying v_i by a nonzero scalar c;

(iii) for some i and j, interchanging v_i and v_j.

Show that S' is also a basis of $\mathbb{F}^n$.

(b) Now let S' be the set of vectors obtained from S in one of the following ways: for each $k = 1, \ldots, n$:

(i) for some i and j, adding a times the ith entry of v_k to the jth entry of v_k, for some scalar a;

(ii) for some i, multiplying the ith entry of v_k by a nonzero scalar c;

(iii) for some i and j, interchanging the ith and jth entries of v_k.

Show that S' is also a basis of $\mathbb{F}^n$.

14. Prove Lemma 1.4.1.

15. (a) Prove Corollary 1.4.7.

(b) Prove Corollary 1.4.8.

16. Prove Lemma 1.5.1.

17. Magic squares are a staple of recreational mathematics. An n-by-n magic square is an n-by-n array of numbers such that all the rows, all the columns, and both of the diagonals all have the same sum. One way to obtain a magic square is to choose all of the entries to be the same. Call such a magic square trivial.

(a) Every 1-by-1 magic square is trivial, as there is only one entry. It is easy to check that every 2-by-2 magic square is trivial. Show that, for every $n \geq 3$, there is a nontrivial n-by-n magic square.

Call a magic square super-magic if all the rows, columns, both diagonals, and all of the broken diagonals have the same sum.

(b) Show that every 3-by-3 super-magic square is trivial. Show that, for every $n \geq 4$, there is a nontrivial n-by-n super-magic square.

Chapter 2

Systems of linear equations

Many (most?) problems in linear algebra come down to solving a system of linear equations. So in order to be able to make much progress, we shall have to learn how to do so. Indeed, as we shall see, there is a completely effective method for solving linear systems, and that is one of the virtues of the subject: once we have translated a problem into a problem about linear systems, we can solve it.

Actually, we have already encountered linear systems in Section 1.4, where we formulated and proved our basic counting theorem. But (at the cost of some repetition) we shall not rely on that section here, but rather build up our development "from scratch".

However, before getting down to the algebraic business of solving systems, we begin with a section on their geometric meaning. This will give us a valuable picture of what is going on, and will guide our intuition in solving systems.

2.1. The geometry of linear systems

In this section we shall proceed intuitively. Unusually for a mathematics book, we will use some concepts before they are properly defined. But everything we say here will be absolutely correct, and once we properly define these concepts, you'll be able to reread this section and verify that.

We will begin by working in $\mathbb{R}^1$, $\mathbb{R}^2$, or $\mathbb{R}^3$, and we will use the usual coordinates: x in $\mathbb{R}^1$, (x, y) in $\mathbb{R}^2$, and (x, y, z) in $\mathbb{R}^3$. When we first introduced vectors, we were careful to regard them as "arrows" from the origin to their endpoints. For many purposes, it is essential to maintain the distinction between vectors and points, but for our purposes here it is convenient to simply identify a vector with its endpoint: to identify the vector $[x]$ with the point (x), the vector $\begin{bmatrix} x \\ y \end{bmatrix}$ with the point (x, y), and the vector $\begin{bmatrix} x \\ y \\ z \end{bmatrix}$ with the point (x, y, z).

We regard $\mathbb{R}^0$, a point, as 0-dimensional; $\mathbb{R}^1$, a line, as 1-dimensional; $\mathbb{R}^2$, a plane, as 2-dimensional; and 3-space $\mathbb{R}^3$ as 3-dimensional. (Dimension is a term we have yet to define. But we will see that linear algebra enables us to give a clear and unambiguous meaning to this term.)

Next we want to consider "flats" in $\mathbb{R}^n$. We are discussing things intuitively here, so we will not (and cannot yet) precisely define what we mean by this term, but we are appealing to your intuition that it should be something flat, for example, a plane in 3-space. We are about to see examples in low dimensions, but first it is convenient to define one more term.

If we have a k-dimensional "flat" in $\mathbb{R}^n$, we define its *codimension* to be $n-k$. In other words the codimension of a flat is the difference between the dimension of the ambient (or surrounding) space and the flat itself.

Reciprocally, this means if we have a codimension j flat in $\mathbb{R}^n$, it has dimension $n-j$.

To illustrate, in low dimensions we have:

A point in $\mathbb{R}^1$ has dimension 0 and codimension 1.

$\mathbb{R}^1$ itself, considering as contained in $\mathbb{R}^1$, has dimension 1 and codimension 0.

A point in $\mathbb{R}^2$ has dimension 0 and codimension 2.

A line in $\mathbb{R}^2$ has dimension 1 and codimension 1.

$\mathbb{R}^2$ itself, considering as contained in $\mathbb{R}^2$, has dimension 2 and codimension 0.

A point in $\mathbb{R}^3$ has dimension 0 and codimension 3.

A line in $\mathbb{R}^3$ has dimension 1 and codimension 2.

A plane in $\mathbb{R}^3$ has dimension 2 and codimension 1.

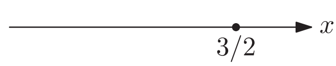
$\mathbb{R}^3$ itself, considering as contained in $\mathbb{R}^3$, has dimension 3 and codimension 0.

Now let us consider a single linear equation. Here is the basic geometric idea:

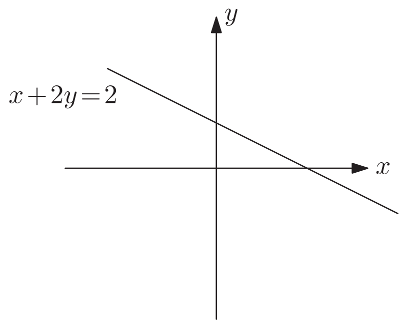
In general, the solutions of a single linear equation in n unknowns form a codimension 1 flat in $\mathbb{R}^n$ for any $n \geq 1$.

Let's see some examples of this.

(1) Let's begin with $\mathbb{R}^1$ and take a typical linear equation in one unknown, $2x = 3$. Then its solution is a point:



(2) Let's begin with $\mathbb{R}^2$ and take a typical linear equation in two unknowns, $x + 2y = 2$. Then its solution is a line:



(Note that if we begin with $\mathbb{R}^2$ and take the equation $x = 1$, we are really regarding it as an equation in two unknowns $1x + 0y = 1$, and its solution is again a line.)

(3) Let's begin with $\mathbb{R}^3$ and take a typical linear equation in three unknowns, $z = 0$. Then its solution is a plane, the (x, y)-plane in $\mathbb{R}^3$ (that is, the plane consisting of all points $(x, y, 0)$ in $\mathbb{R}^3$).

We have said "In general". How could this go wrong? Suppose, for example, we are in $\mathbb{R}^2$ and we consider the linear equation $ax + by = p$. If a and b are both 0 this becomes the equation $0 = p$, and then there are two possibilities. If $p \neq 0$, then this equation is never true, i.e., there are no values of (x, y) that make it true, and so the solutions form the empty subset of $\mathbb{R}^2$. On the other hand, if $p = 0$, then this equation is always true, i.e., every value of (x, y) makes it true, and so the solutions form the set $\mathbb{R}^2$ itself.

But as long as a and b are not both 0, the linear equation $ax + by = c$ will have as solution a line, which is a codimension 1 flat in $\mathbb{R}^2$.

Obviously $a = b = 0$ is a (very) special case, so we are justified in using the language "In general". (A mathematical synonym for "In general" is the word "Generically".) We might also think of "In general" as meaning "We expect that", i.e., in this case, if we choose a and b "at random" they won't both be zero, so we will be in this case.

So much for one linear equation in $\mathbb{R}^2$. Now what about a system of two linear equations in $\mathbb{R}^2$? Let's consider such a system:

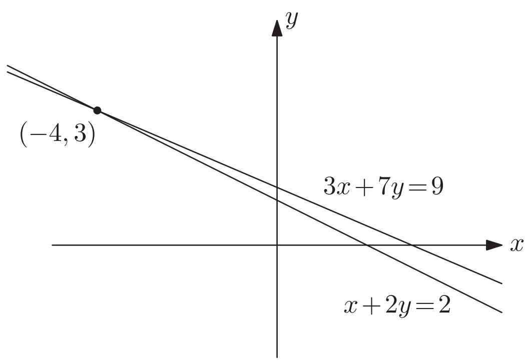
$$\begin{aligned} ax + by &= p, \\ cx + dy &= q. \end{aligned}$$

What should we expect to happen? In general, the solutions to the first equation $ax + by = p$ will form a line, and, in general, the solutions to the second equation $cx + dy = q$ will also form a line. Thus, in general, we will have two lines in the plane and then, in general, two lines will intersect in a point. Thus, in general, a linear system of two equations in two unknowns will have its solution a single point, which is a codimension 2 flat in $\mathbb{R}^2$. For example, if we have the system

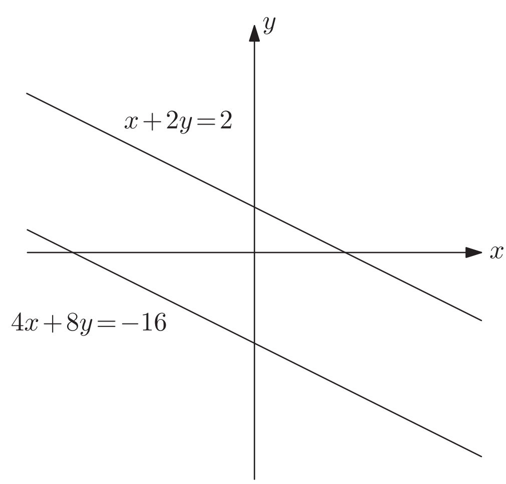
$$\begin{aligned} x + 2y &= 2, \\ 3x + 7y &= 9, \end{aligned}$$

we find that this system has the solution the point $(-4, 3)$.

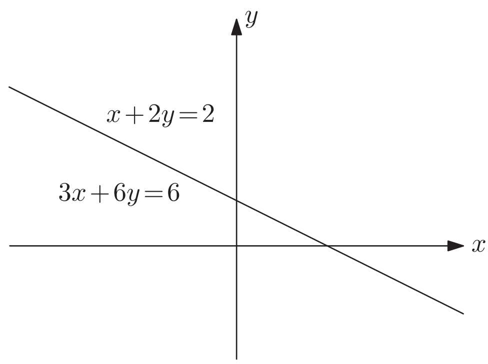
To illustrate:



Again, how could this go wrong? Again, only if something very special happens. Suppose we start with two lines. It could be that they are parallel. Then they will have no point in common, and the system will have no solution. For example:



The other way this could go wrong (assuming we had two lines to begin with) is if both lines turned out to be the same line. Then instead of getting a point for the solution of the system, we would get this whole line. For example:



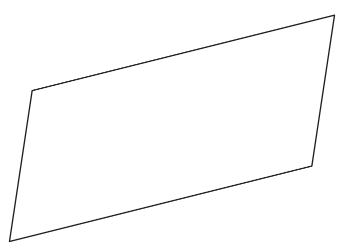
But again, these are special cases when things go wrong, and we expect things to go right.

Now let's move up from $\mathbb{R}^2$ to $\mathbb{R}^3$, and let's consider systems of linear equations. We'll simply consider what happens "in general", when things go right, rather than worrying about the various ways in which things can go wrong.

Consider first a system of one equation in three unknowns,

$$ax + by + cz = p.$$

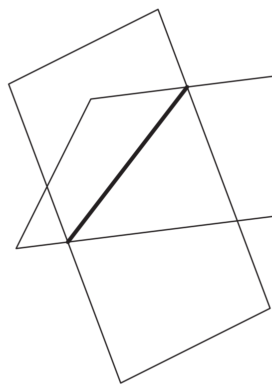
This represents a plane in $\mathbb{R}^3$, i.e., a flat of dimension 2, or more to the point, of codimension 1.



Next consider a system of two equations in three unknowns,

$$\begin{aligned} ax + by + cz &= p, \\ dx + ey + fz &= q. \end{aligned}$$

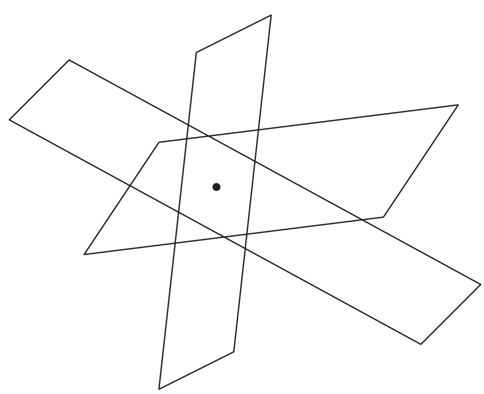
Each one of these equations represents a plane, and in general two planes will intersect in a line. Thus the solution of this system is a line in $\mathbb{R}^3$, i.e., a flat of dimension 1, or again, more to the point, of codimension 2.



And next consider a system of three equations in three unknowns,

$$\begin{aligned} ax + by + cz &= p, \\ dx + ey + fz &= q, \\ gx + hy + iz &= r. \end{aligned}$$

Each one of these represents a plane, and in general three planes will intersect in a point. Thus the solution of this system is a point in $\mathbb{R}^3$, i.e., a flat of dimension 0, or once again, more to the point, of codimension 3.



Let us do something a little silly, but something we should do to complete the picture. Suppose we consider a system of zero equations in $\mathbb{R}^n$. Then every point in $\mathbb{R}^n$ is a solution to this system, i.e., the solution is a flat in $\mathbb{R}^n$ of dimension n, or of codimension 0. Note this is true for $n = 0$ as well.

Let us put all this together. We have considered $\mathbb{R}^n$ for $n = 0, 1, 2, 3$, but that is just so we could draw pictures. Let us consider $\mathbb{F}^n$ instead, where $\mathbb{F}$ is any field and n is any nonnegative integer. The pattern we see is:

In general, the solutions of a system of k linear equations in n unknowns over a field $\mathbb{F}$ form a codimension k flat in $\mathbb{F}^n$ for any k between 0 and n.

Now let us consider homogeneous systems, i.e., systems of linear equations where the right-hand side is 0. We observe that the origin (all the unknowns $= 0$) is always a solution of any such system. Combining this observation with our previous logic first shows, for the case of a single equation:

In general, the solutions of a single homogeneous linear equation in n unknowns over a field $\mathbb{F}$ form a codimension 1 flat through the origin in $\mathbb{F}^n$ for any $n \geq 1$.

Then, following our logic for a system of homogeneous equations, we conclude:

In general, the solutions of a homogeneous system of k linear equations in n unknowns over a field $\mathbb{F}$ form a codimension k flat through the origin $\mathbb{F}^n$ for any k between 0 and n.

It is (very) worthwhile to point out a particular case of these conclusions, the case that is perhaps most important. That is the case $k = n$. In that case, a codimension n flat in $\mathbb{F}^n$ is a dimension $n - n = 0$ flat in $\mathbb{F}^n$, i.e., a single point. To say that a solution is a single point means that there is only one solution, or in other words, that the solution is unique. And then a codimension n flat through the origin in $\mathbb{F}^n$ is a single point in $\mathbb{F}^n$ passing through the origin, i.e., is the origin itself, which we have seen represents the trivial solution. Thus in particular we conclude:

In general, a system of n linear equations in n unknowns over a field $\mathbb{F}$ has a unique solution.

In general, a homogeneous system of n linear equations in n unknowns over a field $\mathbb{F}^n$ only has the trivial solution.

What about if $k > n$? Take $n = 2$. Then a system of three equations in two unknowns represents a system of three lines in the plane. The first two lines will, in general, intersect in a point. But then the third line, in general, will not pass through that point. So the solution set will be empty. If $n = 3$, a system of four equations in three unknowns represents a system of four planes in 3-space. The first three planes will, in general, intersect in a point. But then the fourth plane, in general, will not pass through that point. So again the solution set will be empty. Thus we also conclude:

In general, a system of k equations in n unknowns over a field $\mathbb{F}$, with $k > n \geq 1$, has no solution.

(Here we need to exclude $n = 0$. The reason for this will be clear soon.)

Now what about homogeneous systems when $k > n$? For a homogeneous system, every equation is represented by a flat through the origin, so no matter how many flats we have, they will all pass through the origin. In other words, the origin will always be a solution. But we should not expect there to be any other common points. Recalling that the origin is the point with all coordinates 0, and that we have called the solution to a homogeneous system with all the unknowns 0 the trivial solution, we conclude:

In general, a homogeneous system of k equations in n unknowns over a field $\mathbb{F}$, with $k > n$, has only the trivial solution.

(For $n = 0$, $\mathbb{R}^0$ consists only of a single point 0, so we are automatically in the homogeneous case, which is why we include $n = 0$ here and why we excluded it before.)

Let us now turn to a bit of language. We have the general case, what we expect "in general". What should we call the situation when we are not in the general case? "Special case" would not be a good name, as (a) it would raise the question of special in what way, and (b) special sounds specially good, when we think of it as specially bad.

Instead, we follow the practice among mathematicians of praising situations we like and damning situations we don't. Thus we adopt the (standard) terminology that the situation when we are not in the general case is the *degenerate case*, and then the situation in the general case is the *nondegenerate case*.

There is another, slightly different, way of looking at things. We have looked at the situation "statically", considering intersections of flats. Instead we may look at things "dynamically". What do we mean by this?

We start with $\mathbb{F}^n$, and regard a point in $\mathbb{F}^n$ as having n degrees of freedom. Then we look at our first linear equation. We regard that as imposing a condition, thereby cutting out degrees of freedom by 1, down from n to $n-1$. Next we look at our second condition. We regard that as imposing a further condition, thereby cutting our degrees of freedom by 1 more, down from $n-1$ to $n-2$. We keep going, so by the time we have imposed k conditions we have cut down our degrees of freedom by k, leaving $n-k$ degrees of freedom remaining. Then from this point of view we also see that a system of k equations in n unknowns will have a flat of codimension k, or of dimension $n-k$, as solutions.

Of course, this is what happens "in general". From this point of view we see that the general case is when each new condition is independent of the preceding ones, so that it imposes a genuinely new restriction.

From this point of view, the general case is when all the conditions are independent, and so we adopt (also standard) mathematical terminology and call the general case for $k \leq n$ the *independent case*.

What about when we are not in the independent case? In this case we also follow standard mathematical terminology and make a further distinction. We call a system *consistent* if it has at least one solution and *inconsistent* otherwise. As we have seen, when we are not in the general (or independent) case we may or may not have a solution. If we do, we call the system *consistent and dependent*. If we do not, we simply call it *inconsistent*.

Finally, there is one other term we have frequently used in this section, namely "flat". This is a precise mathematical object with a standard mathematical name. As we shall see, a flat through the origin is a (*vector*) *subspace*, and an arbitrary flat is an *affine subspace*.

2.2. Solving systems of equations—setting up

Suppose we have a system of linear equations $(*)$ that we wish to solve. Here is a strategy for doing so: Transform $(*)$ in another system $(*')$ which has the same solutions, but which is easier to solve. Then transform $(*')$ into another system $(*'')$ which has the same solutions but which is even easier to solve. Keep going until we arrive at a system which has the same solutions as our original system $(*)$ but which is very easy to solve. Solve that system, thereby solving $(*)$.

Here is a simple example to serve as an illustration.

Example 2.2.1. Consider the system

$$(*)\qquad \begin{aligned} x_1 + 2x_2 &= 2, \\ 3x_1 + 7x_2 &= 9. \end{aligned}$$

Let us eliminate x_1 from the second equation by adding $(-3)\cdot$the first equation to the second. We obtain:

$$(*')\qquad \begin{aligned} x_1 + 2x_2 &= 2, \\ x_2 &= 3. \end{aligned}$$

Now we have two choices how to proceed:

(1) We solve for x_2 from the second equation in $(*')$, which is immediate: $x_2 = 3$. Then we substitute this value of x_2 into the first equation and solve for x_1: $x_1 + 2(3) = 2$, $x_1 = -4$. Thus $(*)$ has the (unique) solution $x_1 = -4$, $x_2 = 3$.

(2) We eliminate x_2 from the first equation in $(*')$ by adding $(-2)\cdot$ the second equation to the first equation. We obtain:

$$(*'')\qquad \begin{aligned} x_1 \qquad &= -4, \\ x_2 &= 3. \end{aligned}$$

Now we solve this system for x_1 and x_2, which is immediate: $x_1 = -4$ and $x_2 = 3$. Thus $(*)$ has the (unique) solution $x_1 = -4$, $x_2 = 3$. $\Diamond$

Now we want to be able to solve systems of any size, not just 2-by-2 systems. So we will have to develop a systematic procedure for doing so. But the basic idea of this procedure is already to be found in this simple example.

Actually, we will be developing not one, but two, closely related procedures. The procedure that comes out of choice (1) is known as *Gaussian elimination with back-substitution* while the procedure that comes out of choice (2) is known as *Gauss-Jordan reduction.*

Now let us get down to work.

Consider a system of m equations in n unknowns with coefficients in $\mathbb{F}$:

$$(*)\qquad \begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m. \end{aligned}$$

Recall that such a system $(*)$ can be written as

$$Ax = b,$$

where A is the matrix $A = (a_{ij})$, x is the vector of unknowns $x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$, and b is the vector of the coefficients on the right-hand side, $b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$. In other words, we have translated our original system into a matrix equation. For many reasons, it is preferable to solve linear systems by working with matrices, rather than equations, translating back into equations at the very end, and that is what we shall do.

First, some language.

Definition 2.2.2. Two matrix equations $Ax = b$ and $A'x = b'$ are *equivalent* if they have the same solutions. $\Diamond$

Definition 2.2.3. Given an equation $Ax = b$ representing a system of linear equations $(*)$, the *matrix of this system* is the m-by-n matrix A, and the *augmented matrix of this system* is the m-by-$(n+1)$ matrix $[A\,|\,b]$. $\Diamond$

Definition 2.2.4. Let M be a matrix. An *elementary row operation* on M is one of the following:

(1) Multiply row i of M by $c \neq 0$.

(2) Add $c \cdot$ row i of M to row j of M.

(3) Interchange rows i and j of M.

$\Diamond$

Lemma 2.2.5. *Consider a linear system $(*)$ given by the matrix equation $Ax = b$, with augmented matrix $[A\,|\,b]$. If the matrix $[A'\,|\,b']$ is obtained from the matrix $[A\,|\,b]$ by an elementary row operation, then the matrix equations $Ax = b$ and $A'x = b'$ are equivalent.*

Proof. We first observe the effects of elementary row operations (EROs) on systems of equations.

(1) The ERO (1) has the effect of multiplying equation i of $(*)$ by $c \neq 0$.

(2) The ERO (2) has the effect of adding $c \cdot$ equation i of $(*)$ to equation j of $(*)$.

(3) The ERO (3) has the effect of interchanging equations i and j of $(*)$.

It is straightforward to check that if $(*')$ is the linear system obtained from $(*)$ by any one of these operations, every solution of $(*)$ is a solution of $(*')$. But note that if $(*')$ is obtained from $(*)$ by an ERO, then $(*)$ is obtained from $(*')$ by an ERO of the same type. (See the proof of Lemma 2.2.9 below.) Thus the two matrix systems are equivalent. $\square$

We introduce a little more language.

Definition 2.2.6. Two matrices M and $\widetilde{M}$ are *row-equivalent* if $\widetilde{M}$ can be obtained from M by a sequence of elementary row operations. $\Diamond$

Corollary 2.2.7. *Consider a linear system given by the matrix equation $Ax = b$, with augmented matrix $[A\,|\,b]$. If $[A\,|\,b]$ is row-equivalent to $[\tilde{A}\,|\,\tilde{b}]$, then this linear system is equivalent to the linear system given by the matrix equation $\tilde{A}x = \tilde{b}$.*

Proof. To say that $[A\,|\,b]$ is row-equivalent to $[\tilde{A}\,|\,\tilde{b}]$ is to say that we have a sequence

$$[A\,|\,b],\ [A'\,|\,b'],\ [A''\,|\,b''],\ \ldots,\ [\tilde{A}\,|\,\tilde{b}]$$

in which each term is obtained from the previous term by an elementary row operation. But by Lemma 2.2.5, that means that each linear system is equivalent to the next linear system, so the first linear system $Ax = b$ is equivalent to last linear system $\tilde{A} = \tilde{b}$. □

This gives our strategy for solving linear systems:

Given a linear system with augmented matrix $[A\,|\,b]$, develop a systematic procedure to transform it into a row-equivalent system $[\tilde{A}\,|\,\tilde{b}]$ that is as easy to solve as possible. Then solve that system, thereby solving the original system.

We will carry out this strategy in the next section. But before we do, let us make a remark about homogeneous systems. (Recall that a system $(*)$ as in Lemma 2.2.5 is homogeneous if the right-hand side is 0, i.e., if $b_1 = b_2 = \cdots = b_m = 0$.)

Lemma 2.2.8. *If $(*)$ is a homogeneous system, then any system $(*')$ equivalent to $(*)$ is homogeneous. In matrix terms, if a linear system has augmented matrix $[A\,|\,0]$, then any row-equivalent system must be of the form $[\tilde{A}\,|\,0]$.*

Proof. Suppose $(*)$ is homogeneous. Then it has the solution $x_1 = \cdots = x_n = 0$ (the trivial solution). But then this is a solution of $(*')$, so the right-hand side of $(*')$ must be 0 as well. □

To conclude this section, we would like to record an important observation for future reference. We introduced the notion of row-equivalence in Definition 2.2.6 and we record the following properties of it.

Lemma 2.2.9. (1) *Let M be any matrix. Then M is row-equivalent to itself.*

(2) *Let M and N be any two matrices. If M is row-equivalent to N, then N is row-equivalent to M.*

(3) *Let M, N, and P be any three matrices. If M is row-equivalent to N and N is row-equivalent to P, then M is row-equivalent to P.*

Proof. (1) M is obtained from M by the empty sequence of row operations. (Do nothing!)

(3) If there is a sequence of row operations that takes M to N and a second sequence of row operations that takes N to P, then beginning with M and performing these two sequences of row operations in order first takes us to N and then from there to P.

(2) Suppose M' is obtained from M by a single row operation. Then M is obtained from M' by reversing (or, to use the proper mathematical term, inverting)

that row operation, and that is accomplished by another row operation:

(a) The operation of multiplying row i of M by $c \neq 0$ is inverted by the operation of multiplying row i of M' by $1/c \neq 0$.

(b) The operation of adding c times row i of M to row j is inverted by the operation of adding $-c$ times row i of M' to row j.

(c) The operation of interchanging rows i and j of M is inverted by the operation of interchanging rows i and j of M'. (Interchanging two rows twice returns them to their original positions.)

Now if N is row-equivalent to M there is a sequence of row operations op_1, op_2, op_k (in that order) taking M to N. But then, if $(op_i)^{-1}$ denotes the inverse operation to op_i, the sequence of row operations $(op_k)^{-1}$, $(op_{k-1})^{-1}$, $\ldots$, $(op_1)^{-1}$ (in that order) takes N back to M. (Note that this order is opposite to the original order.) □

2.3. Solving linear systems—echelon forms

If you want to figure out the best way of getting somewhere, first you should figure out exactly where you want to go, and then you should figure out exactly how to get there.

Thus we will first, in this section, introduce echelon forms, which are systems that are particularly easy to solve, and we will see how to solve them. Then, in the next section, we will introduce our algorithm for transforming a system into echelon form.

We begin with some language and notation. Consider a system $Ax = b$ with matrix $A = (a_{ij})$. If, for some particular values of i_0 and j_0, the coefficient $a_{i_0 j_0}$ of x_{j_0} in the i_0th equation is nonzero, we will say that the i_0th equation *involves* x_{j_0}. If this coefficient may be nonzero, we will say that the i_0th equation *potentially involves* x_{j_0}. And if $a_{i_0 j_0} = 0$, we will say that the i_0th equation *does not involve* x_{j_0}.

A *leading entry* in a row of a matrix is the leftmost nonzero entry in its row.

We now introduce three forms of matrices, each more special than the previous one.

Definition 2.3.1. A matrix M is in *weak row-echelon form* if

(1) the leading entry in any row is to the right of the leading entry in the row above it; and

(2) all zero rows (if any) are at the bottom.

A matrix M is in *row-echelon form* if it is in weak row-echelon form and furthermore

(3) every leading entry is equal to 1.

A matrix M is in *reduced row-echelon form* if it is in row-echelon form and furthermore

(4) every other entry in a column containing a leading 1 is equal to 0. ◊

Example 2.3.2. The matrix $\begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$ is in weak row-echelon form; the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is in row-echelon form; and the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is in reduced row-echelon form. ◊

Example 2.3.3. The matrix

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

with a, b, and c all nonzero, is in weak row-echelon form.

The matrix

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

is in row-echelon form.

The matrix

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

is in reduced row-echelon form. ◊

Example 2.3.4. Here the matrices are intended to be square matrices (all of the same size).

The matrix

$$\begin{bmatrix} a_1 & * & * & & * \\ 0 & a_2 & * & \dots & * \\ 0 & 0 & a_3 & & * \\ & \vdots & & \ddots & \vdots \\ 0 & \dots\dots\dots & & 0 & a_n \end{bmatrix},$$

with $a_1, a_2, a_3, \dots, a_n$ all nonzero, is in weak row-echelon form.

The matrix

$$\begin{bmatrix} 1 & * & * & & * \\ 0 & 1 & * & \dots & * \\ 0 & 0 & 1 & & * \\ & \vdots & & \ddots & \vdots \\ 0 & \dots\dots & & 0 & 1 \end{bmatrix}$$

is in row-echelon form.

The matrix

$$\begin{bmatrix} 1 & 0 & 0 & & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & 0 \\ & \vdots & & \ddots & \vdots \\ 0 & \dots & \cdot & 0 & 1 \end{bmatrix}$$

is in reduced row-echelon form. $\Diamond$

Suppose that $\tilde{A}$ is in one of these three types of echelon form, and consider the system with augmented matrix $[\tilde{A}\,|\,\tilde{b}]$, i.e., the system $\tilde{A}x = b$. The entries in the ith column of $\tilde{A}$ are the coefficients of the ith variable x_i in this system. We will say that x_i is a *leading variable* if column i of $\tilde{A}$ contains a leading entry. Otherwise we will say that x_i is a *free variable*. (The reason for this language will soon become clear.) Note the distinction between leading and free variables only depends on the matrix $\tilde{A}$ (and not the vector $\tilde{b}$).

Note that if $\tilde{A}$ is in reduced row-echelon form, the only variables involved in any equation, other than the leading variable in that equation, are free variables, so a solution to $\tilde{A}x = \tilde{b}$ will directly express the leading variables in terms of the free variables. If $\tilde{A}$ is in weak row-echelon or row-echelon form, the variables involved in any equation, other than the leading variable in that equation, will either be free variables, or leading variables that have already been solved for in terms of free variables, so a solution to $\tilde{A}x = \tilde{b}$ will indirectly express the leading variables in terms of the free variables.

Note also that we are free to choose the free variables as we please (i.e., there are no restrictions on their possible values) and we will always obtain a solution in terms of them.

The key observation to make is that, in any system in any one of these echelon forms, each equation potentially involves fewer variables than the one above it.

Here is our algorithm.

Algorithm 2.3.5. Consider a system with augmented matrix $[\tilde{A}\,|\,\tilde{b}]$, where $\tilde{A}$ is in any echelon form.

If $\tilde{A}$ has any zero row for which the entry of $\tilde{b}$ in that row is nonzero, the system has no solution, i.e., is inconsistent. Stop.

Otherwise, proceed from the bottom nonzero row up. Solve for the leading entry in each row in terms of the other variables (if any) involved in the equation represented by that row.

Allow the free variables (if any) to take arbitrary values. $\Diamond$

Let us now see this algorithm in practice.

Example 2.3.6. (1) Consider the system with augmented matrix

$$[\tilde{A}_1\,|\,\tilde{b}_1] = \left[\begin{array}{cc|c} 1 & 1 & 6 \\ 0 & 2 & 4 \end{array}\right],$$

Here the system is in weak row-echelon form. It represents the system of equations

$$\begin{aligned} x_1 + \ \ x_2 &= 6, \\ 2x_2 &= 4. \end{aligned}$$

Note there are no free variables.

We work from the bottom up. Multiplying the second equation by $1/2$, we find

$$x_2 = 2.$$

Substituting in the first equation, we obtain the equation $x_1 + 2 = 6$, so

$$x_1 = 4.$$

Thus our system has the solution $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \end{bmatrix}$.

(2) Consider the system with augmented matrix $[\tilde{A}_2 \,|\, \tilde{b}_2] = \left[\begin{array}{cc|c} 1 & 1 & 6 \\ 0 & 1 & 2 \end{array}\right]$.

Here the system is in row-echelon form. It represents the system of equations

$$\begin{aligned} x_1 + x_2 &= 6, \\ x_2 &= 2. \end{aligned}$$

Note there are no free variables.

We work from the bottom up. Solving the second equation (which in this case is immediate), we find

$$x_2 = 2.$$

Substituting in the first equation, we obtain the equation $x_1 + 2 = 6$, so

$$x_1 = 4.$$

Thus our system has the solution $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \end{bmatrix}$.

(3) Consider the system with augmented matrix $[\tilde{A}_3 \,|\, \tilde{b}_3] = \left[\begin{array}{cc|c} 1 & 0 & 4 \\ 0 & 1 & 2 \end{array}\right]$.

Here the system is in reduced row-echelon form. It represents the system of equations

$$\begin{aligned} x_1 \qquad &= 4 \\ x_2 &= 2. \end{aligned}$$

Note there are no free variables.

We work from the bottom up. Solving the second equation (which is immediate), we find

$$x_2 = 2.$$

Solving the first equation (also immediate), we find

$$x_1 = 4.$$

Thus our system has the solution $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \end{bmatrix}$.

Observe that these three augmented matrices are all row-equivalent. We obtain $[\tilde{A}_2 \,|\, \tilde{b}_2]$ from $[\tilde{A}_1 \,|\, \tilde{b}_1]$ by multiplying the second row of $[\tilde{A}_1 \,|\, \tilde{b}_1]$ by $1/2$, and we obtain $[\tilde{A}_3 \,|\, \tilde{b}_3]$ from $[\tilde{A}_2 \,|\, \tilde{b}_2]$ by adding (-1) times the second row of $[\tilde{A}_2 \,|\, \tilde{b}_2]$ to the first row.

We know that row-equivalent augmented matrices represent equivalent systems, and so it is no surprise that these three systems have the same solution. $\diamondsuit$

Remark 2.3.7. Note that the matrix in (1) was in weak row-echelon form, and the matrix in (2) was in row-echelon form, while the matrix in (3) was in reduced row-echelon form. Note that we could straightforwardly solve (1), but that we could more easily solve (2), and even more easily solve (3). Of course, you can't get something for nothing, and we had to do some extra work, namely additional row operations, to get from (1) to (3).

All three solution methods are correct, but for some theoretical purposes (the first of which we will soon see) it is better to use reduced row-echelon form. For the sake of uniformity, we will use that exclusively in this book. $\diamondsuit$

Example 2.3.8. Consider the system with augmented matrix

$$\left[\begin{array}{ccccc|c} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 4 & 0 & -4 \\ 0 & 0 & 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

The fourth and fifth equations are both simply $0 = 0$, which yields no information. The top three rows of the system are

$$\begin{aligned} x_1 + 2x_2 \qquad + x_4 \qquad &= 0, \\ x_3 + 4x_4 \qquad &= -4, \\ x_5 &= 5. \end{aligned}$$

We can almost immediately solve this. We have leading variables x_1, x_3, and x_5 and free variables x_2 and x_4, and we see

$$\begin{aligned} x_1 &= \quad -2x_2 - x_4, \\ x_3 &= -4 \qquad - 4x_4, \\ x_5 &= 5, \end{aligned}$$

and our system has solution

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} -2x_2 - x_4 \\ x_2 \\ -4 - 4x_4 \\ x_4 \\ 5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -4 \\ 0 \\ 5 \end{bmatrix} + x_2 \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_4 \begin{bmatrix} -1 \\ 0 \\ -4 \\ 1 \\ 0 \end{bmatrix}. \qquad \diamondsuit$$

2.4. Solving systems of equations—the reduction process

In this section we present, and illustrate, our algorithm for transforming a linear system with augmented matrix $[A \,|\, b]$ to a system with augmented matrix $[\tilde{A} \,|\, \tilde{b}]$, where $\tilde{A}$ is in row-echelon form or reduced row-echelon form. Combining this with the previous section, we have an effective method for solving linear systems.

Here it is:

Algorithm 2.4.1. Consider the matrix of the system.

(0) Begin with the first row. Call it the current row.

(1) Look for a leading entry as far to the left in the current row or below as is possible. If that entry is in the current row, fine. Otherwise switch the current row of the augmented matrix with the row that entry is in.

Thus, after completing this step, in either case the leading entry in the current row will be as far to the left as possible, only considering the current row and rows beneath it.

(2) Multiply the current row of the augmented matrix by a constant so as to make the leading entry equal to 1.

(3) If the entry in that column in any row beneath the current row is 0, fine. Otherwise add a multiple of the current row of the augmented matrix to that row to make that entry equal to 0. Do this for every row beneath the current row.

(4) If the current row is the last row, we are done. Otherwise let the current row be the next row, and go back to step (1).

At this point the transformed matrix of the system will be in row-echelon form. If that is our goal, we are done. If our goal is to obtain a system whose matrix is in reduced row-echelon form, we have more work to do.

($0'$) Begin with the second row for which the matrix is nonzero. Call it the current row. (If the matrix has only one nonzero row, there is nothing that needs to be done.)

($1'$) Note that the current row has a leading 1 (in some column). If the entry in the column containing that leading 1 in any row above the current row is 0, fine. Otherwise, add a multiple of the current row of the augmented matrix to that row to make that entry equal to 0. Do this for every row above the current row.

($2'$) If the current row is the last nonzero row, we are done. Otherwise let the current row be the next row, and go back to step ($1'$). $\Diamond$

Remark 2.4.2. We have some flexibility in the order in which we apply these steps, and it is worth noting how we can simplify our algorithm.

Suppose we reach a stage where the matrix of the system has a zero row. There are two possibilities:

(1) The entry on the right-hand side of that row is nonzero. Then that row represents an equation $0 = a$ for some $a \neq 0$, which has no solution. Thus at this point we can simply declare that the system is inconsistent, and stop.

(2) The entry on the right-hand side of that row is 0. Then that row represents an equation $0 = 0$, which is certainly true, but yields no information. Then at this point we can simply move this row down to the bottom, leave it there and forget about it, and work on the other rows. $\Diamond$

Remark 2.4.3. As we have earlier remarked, we have two alternatives.

We may use steps (0)–(4) of Algorithm 2.4.1 to transform a system $[A\,|\,b]$ to a system $[\tilde{A}\,|\,\tilde{b}]$ with $\tilde{A}$ in row-echelon form, and then use the method of the previous section to solve the resultant system in this case. This procedure is known as *Gaussian elimination with back-substitution.*

We may use steps (0)–($2'$) of Algorithm 2.4.1 to transform a system $[A\,|\,b]$ to a system $[\tilde{A}\,|\,\tilde{b}]$ with $\tilde{A}$ in reduced row-echelon form, and then use the method of the previous section to solve the resultant system in this case. This procedure is known as *Gauss-Jordan reduction.*

Both alternatives are correct (and, of course, give the same answer in the end). As we have also earlier remarked, we will use Gauss-Jordan reduction exclusively in this book. ◊

Here are some words of advice. There are lots of tricks for speeding up the process. The author of this book has been row-reducing matrices for years, and is likely to be able to use them when solving a system. But you are a newcomer to the subject, and so you don't have much experience. You should follow our algorithm, which is a systematic procedure. If you think you see a clever trick to speed up the process, it is possible you are right, but it is more likely that you are wrong, and using your trick will make things harder somewhere down the line, with the effect of slowing down the process overall. So don't try to be clever; instead just be systematic.

Now let us see some examples of our algorithm in action.

Example 2.4.4. Consider the system

$$\begin{aligned} x_1 \qquad\;\; + \;\; 5x_3 &= 4, \\ 2x_1 - 2x_2 + \;\; 6x_3 &= 16, \\ 3x_2 + 12x_3 &= -9. \end{aligned}$$

This has the augmented matrix:

$$\left[\begin{array}{ccc|c} 1 & 0 & 5 & 4 \\ 2 & -2 & 6 & 16 \\ 0 & 3 & 12 & -9 \end{array}\right]$$

We go to work. Add (-2) row 1 to row 2:

$$\left[\begin{array}{ccc|c} 1 & 0 & 5 & 4 \\ 0 & -2 & -4 & 8 \\ 0 & 3 & 12 & -9 \end{array}\right]$$

Multiply row 2 by (-1/2):

$$\left[\begin{array}{ccc|c} 1 & 0 & 5 & 4 \\ 0 & 1 & 2 & -4 \\ 0 & 3 & 12 & -9 \end{array}\right]$$

Add (-3) row 2 to row 3:

$$\left[\begin{array}{ccc|c} 1 & 0 & 5 & 4 \\ 0 & 1 & 2 & -4 \\ 0 & 0 & 6 & 3 \end{array}\right]$$

Multiply row 3 by (1/6):

$$\left[\begin{array}{ccc|c} 1 & 0 & 5 & 4 \\ 0 & 1 & 2 & -4 \\ 0 & 0 & 1 & 1/2 \end{array}\right]$$

Add (-5) row 3 to row 1:

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 3/2 \\ 0 & 1 & 2 & -4 \\ 0 & 0 & 1 & 1/2 \end{array}\right]$$

Add (-2) row 3 to row 2:

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 3/2 \\ 0 & 1 & 0 & -5 \\ 0 & 0 & 1 & 1/2 \end{array}\right]$$

The matrix of the system is in reduced row-echelon form. It represents the equations

$$\begin{aligned} x_1 \qquad\qquad &= 3/2, \\ x_2 \qquad &= -5, \\ x_3 &= 1/2, \end{aligned}$$

which we immediately see has the solution

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 3/2 \\ -5 \\ 1/2 \end{bmatrix}. \qquad \Diamond$$

Example 2.4.5. Consider the system:

$$\begin{aligned} x_1 + 2x_2 - x_3 - 3x_4 + 3x_5 &= 19, \\ 2x_1 + 4x_2 - x_3 - 2x_4 + 8x_5 &= 44, \\ 3x_1 + 6x_2 - x_3 - x_4 + 13x_5 &= 69, \\ 5x_1 + 10x_2 - 3x_3 - 7x_4 + 21x_5 &= 117, \\ 8x_1 + 16x_2 - 5x_3 - 12x_4 + 34x_5 &= 190. \end{aligned}$$

We form the augmented matrix of this system and row-reduce:

$$\left[\begin{array}{ccccc|c} 1 & 2 & -1 & -3 & 3 & 19 \\ 2 & 4 & -1 & -2 & 8 & 44 \\ 3 & 6 & -1 & -1 & 13 & 69 \\ 5 & 10 & -3 & -7 & 21 & 117 \\ 8 & 16 & -5 & -12 & 34 & 190 \end{array}\right]$$

Here we simply give the list of elementary row operations, without writing out the intermediate matrices so obtained.

(1) Add (-2) row 1 to row 2.

(2) Add (-3) row 1 to row 3.

(3) Add (-5) row 1 to row 4.

(4) Add (-8) row 1 to row 5.

(5) Add (-2) row 2 to row 3.

(6) We observe that row 3 is $0 = 0$, so we simply move it to the bottom, and move each of rows 4 and 5 up.

(7) Add (-2) row 2 to row 3.

(8) Add (-3) row 2 to row 4.

(9) Multiply row 3 by $(1/2)$.

(10) Add (-4) row 3 to row 4.

We arrive at:

$$\left[\begin{array}{ccccc|c} 1 & 2 & -1 & -3 & 3 & 19 \\ 0 & 0 & 1 & 4 & 2 & 6 \\ 0 & 0 & 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

We pause to note at this point that even though we haven't yet solved this system, we've come far enough to be able to tell that it *has* a solution. For the matrix of the system is in row-echelon form, and whenever there is a zero row on the left (in this case, the last two rows) the entry on the right is 0.

We now continue our solution process.

(11) Add (1) row 2 to row 1.

(12) Add (-5) row 3 to row 1.

(13) Add (-2) row 3 to row 2.

We arrive at:

$$\left[\begin{array}{ccccc|c} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 4 & 0 & -4 \\ 0 & 0 & 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

This matrix is in reduced row-echelon form, and represents the system

$$\begin{aligned} x_1 + 2x_2 \qquad + x_4 \qquad &= 0, \\ x_3 + 4x_4 \qquad &= -4, \\ x_5 &= 5. \end{aligned} \qquad \Diamond$$

We now apply the method of Section 2.3 to solve this system. But in fact this system is exactly the system in Example 2.3.8, and we solved it there. So we simply record the answer:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} -2x_2 - x_4 \\ x_2 \\ -4 - 4x_4 \\ x_4 \\ 5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -4 \\ 0 \\ 5 \end{bmatrix} + x_2 \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_4 \begin{bmatrix} -1 \\ 0 \\ -4 \\ 1 \\ 0 \end{bmatrix}.$$

Note that if we start with two systems with the same matrix, though with different augmented matrices, we perform exactly the same sequence of row operations to reduce the matrices to reduced row-echelon form in order to solve the systems. With that in mind, we do the next example.

Example 2.4.6. Consider the systems:

$$\begin{aligned} x_1 + x_2 + 3x_3 &= 1 & &= 0 & &= 0, \\ 2x_1 + 2x_2 + 9x_3 &= 0 & &= 1 & &= 0, \\ 3x_1 + 2x_2 + 7x_3 &= 0, & &= 0, & &= 1. \end{aligned}$$

Thus we have three systems with the same left-hand side (i.e., the same matrix) but different right-hand sides.

Of course we could solve this system by solving for the first right-hand side, recording the row operations we used, coming back and using the same sequence of operations to solve for the second right-hand side, and coming back again to use the same sequence to solve for the third right-hand side.

But there is a better way. We form the augmented matrix

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 2 & 2 & 9 & 0 & 1 & 0 \\ 3 & 2 & 7 & 0 & 0 & 1 \end{array}\right]$$

and do row operations on it. When we have reduced the matrix to reduced row-echelon form, the first column in the right-hand side will give us the solution to the first system, the second column on the right-hand side will give us the solution to the second system, and the third column on the right-hand side will give us the solution to the third system.

We go to work. We add (-2) the first row to the second row:

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & 0 & 3 & -2 & 1 & 0 \\ 3 & 2 & 7 & 0 & 0 & 1 \end{array}\right]$$

We add (-3) the first row to the third row:

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & 0 & 3 & -2 & 1 & 0 \\ 0 & -1 & -2 & -3 & 0 & 1 \end{array}\right]$$

We interchange rows 2 and 3:

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & -1 & -2 & -3 & 0 & 1 \\ 0 & 0 & 3 & -2 & 1 & 0 \end{array}\right]$$

We multiply row 2 by (-1):

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 3 & 0 & -1 \\ 0 & 0 & 3 & -2 & 1 & 0 \end{array}\right]$$

We multiply row 3 by $(1/3)$:

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 3 & 0 & -1 \\ 0 & 0 & 1 & -2/3 & 1/3 & 0 \end{array}\right]$$

We add (-1) row 2 to row 1:

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 1 & -2 & 0 & 1 \\ 0 & 1 & 2 & 3 & 0 & -1 \\ 0 & 0 & 1 & -2/3 & 1/3 & 0 \end{array}\right]$$

We add (-1) row 3 to row 1:

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -4/3 & -1/3 & 1 \\ 0 & 1 & 2 & 3 & 0 & -1 \\ 0 & 0 & 1 & -2/3 & 1/3 & 0 \end{array}\right]$$

We add (-3) row 3 to row 2:

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -4/3 & -1/3 & 1 \\ 0 & 1 & 0 & 13/3 & -2/3 & -1 \\ 0 & 0 & 1 & -2/3 & 1/3 & 0 \end{array}\right]$$

This matrix is in reduced row-echelon form, and represents the three systems:

$$\begin{aligned} x_1 \qquad\qquad &= -4/3, &&= -1/3, &&= 1, \\ x_2 \qquad &= 13/3, &&= -2/3, &&= -1, \\ x_3 &= -2/3, &&= 1/3, &&= 0, \end{aligned}$$

and we see these three systems have solutions

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -4/3 \\ 13/3 \\ -2/3 \end{bmatrix}, \qquad = \begin{bmatrix} -1/3 \\ -2/3 \\ 1/3 \end{bmatrix}, \qquad = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}.$$

respectively. $\Diamond$

We will have many systems to solve in the future. But we will rarely go through the row-reduction process explicitly. Instead, we will simply write down the system and the solution, leaving you to go through the row operations yourself.

2.5. Drawing some consequences

In this section we will draw some consequences from and about our method of solving linear systems. The final consequence we will draw will be that the reduced row-echelon form of a matrix is unique, but the intermediate consequences we draw will be important in their own right.

Lemma 2.5.1. *Consider a linear system with augmented matrix $[A|b]$, and let this row-reduce to $[\tilde{A}|\tilde{b}]$ with $\tilde{A}$ in row-reduced echelon form.*

(1) *If there is some zero in $\tilde{A}$ for which the corresponding entry in $\tilde{b}$ is nonzero, the system $Ax = b$ does not have a solution, i.e., is inconsistent.*

(2) *If $\tilde{A}$ does not have a zero row, or if for every zero row in $\tilde{A}$ the corresponding entry in $\tilde{b}$ is zero, the system $Ax = b$ has a solution, i.e., is consistent. Furthermore, it has a solution with every free variable $= 0$.*

Proof. We recall that $Ax = b$ and $\tilde{A}x = \tilde{b}$ have the same solutions.

(1) In this situation, there is some row of $[\tilde{A}|\tilde{b}]$ that represents the equation $0 = c$ for some $c \neq 0$, and this has no solution.

(2) In this case all zero rows of $\tilde{A}$ give the equation $0 = 0$, which is always true, so this system will have the same solution as the system given by the nonzero rows.

Let $\tilde{A}$ have nonzero rows 1 through k. Each of these contains a leading 1, and let the leading 1 in row i be in column j_i. Then the augmented matrix $[\tilde{A}|\tilde{b}]$ represents the system

$$\begin{aligned} x_{j_1} + {\sum}' \tilde{a}_{1j} x_j &= \tilde{b}_1 \\ x_{j_2} + {\sum}' \tilde{a}_{2j} x_j &= \tilde{b}_2 \\ &\vdots \\ x_{j_k} + {\sum}' \tilde{a}_{kj} x_j &= \tilde{b}_k, \end{aligned}$$

where $\tilde{b}_1, \ldots, \tilde{b}_k$ are the entries of $\tilde{b}$ in rows $1, \ldots, k$, and the prime on the summation indicates that the sum is being taken *only* over free variables. But then this system certainly has the solution

$$x_{j_1} = \tilde{b}_1, \quad x_{j_2} = \tilde{b}_2, \ \ldots, \ x_{j_k} = \tilde{b}_k, \quad x_j = 0 \text{ for every free variable } x_j. \qquad \square$$

Lemma 2.5.2. *Consider a homogeneous linear system with matrix A, and let this row-reduce to $\tilde{A}$. Then this system has a unique solution for any values of the free variables. In particular, if all the free variables are 0, the only solution is $x_1 = x_2 = \cdots = x_n = 0$.*

Proof. In the notation of the proof of Lemma 2.5.1, the system becomes

$$\begin{aligned} x_{j_1} &= -\left({\sum}' \tilde{a}_{1j} x_j\right) \\ x_{j_2} &= -\left({\sum}' \tilde{a}_{2j} x_j\right) \\ &\vdots \\ x_{j_k} &= -\left({\sum}' \tilde{a}_{kj} x_j\right), \end{aligned}$$

so any given values of the free variables uniquely specify values of the leading variables. In particular, if all the free variables are 0, all the leading variables are 0 as well. $\square$

Corollary 2.5.3. *Consider a homogeneous system with matrix A, and let it row-reduce to $\tilde{A}$. Let $x_{j_1}, \ldots, x_{j_k}$ be the leading variables. Let x_{j_0} be any free variable,* *and let the* j_0*th column of* $\tilde{A}$ *be*

$$\begin{bmatrix} \tilde{a}_{1j_0} \\ \tilde{a}_{2j_0} \\ \vdots \end{bmatrix}.$$

Then the unique solution of $Ax = 0$ *with* $x_{j_0} = 1$ *and* $x_{j'} = 0$ *for every other free variable* $x_{j'}$ *is given by*

$$x_{1j_1} = -\tilde{a}_{1j_0}, \quad x_{2j_2} = -\tilde{a}_{2j_0}, \ \ldots, \ x_{kj_k} = -\tilde{a}_{kj_0},$$
$$x_{j_0} = 1, \quad x_{j'} = 0 \quad \textit{for every other free variable } x_{j'}.$$

Proof. In the notation of the previous lemma, we can write each sum $\sum' \tilde{a}_{ij}x_j$ as

$$\sum\nolimits' \tilde{a}_{ij}x_j = \tilde{a}_{ij_0}x_{j_0} + \sum\nolimits'' \tilde{a}_{ij}x_j,$$

where the second sum $\sum''$ runs over all the free variables except x_{j_0}. But then setting $x_{j_0} = 1$ and $x_j = 0$ for all other free variables x_j gives the value of the sum in this case as just $\tilde{a}_{ij_0}$, so we get the claimed solution. □

It is fair to say that we haven't really done much new so far in this section. All we've done is to make explicit the conclusions we implicitly drew from our solution method. But there's a value in doing so.

Theorem 2.5.4. *The reduced row-echelon form* $\tilde{A}$ *of any matrix* A *is unique.*

Proof. We are going to prove this theorem *not* doing any sort of manipulations on A but rather by thinking about the solutions of the homogeneous system $Ax = 0$.

We prove the theorem by induction on the number of variables n.

Suppose $n = 1$. Consider the system $Ax = 0$. Here $x = [x_1]$. We ask whether this system has the solution $x_1 = 1$. If yes, then all the entries of A are zero, and A has reduced row-echelon form $\tilde{A} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$. If no, then A has a nonzero entry, and A has reduced row-echelon form $\tilde{A} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$. Thus in either case $\tilde{A}$ is unique.

Now suppose that the theorem is true for n and consider the $n+1$ case.

Let A be m-by-$(n+1)$ and let A have a reduced row-echelon form $\tilde{A}$. Let A_n be the m-by-n matrix consisting of the first n columns of A, and let $\tilde{A}_n$ be the m-by-n matrix consisting of the first n columns of $\tilde{A}$. Note that if $\tilde{A}$ is in row-reduced echelon form, then $\tilde{A}_n$ certainly is, and in fact $\tilde{A}_n$ is a row-reduced echelon form of A_n. By the inductive hypothesis, $\tilde{A}_n$ is unique. Let $\tilde{A}_n$ have k nonzero rows. Then $\tilde{A}$ must have one of the following two forms:

(a) $\tilde{A} = [\tilde{A}_n | e_{k+1}]$ (recall e_{k+1} has a 1 in position $k+1$ and is 0 otherwise), or

(b) $\tilde{A} = [\tilde{A}_n|c]$, where $c = \begin{bmatrix} c_1 \\ \vdots \\ c_k \\ 0 \\ \vdots \\ 0 \end{bmatrix}$.

(Of course, if $k = n$ only case (b) can occur.)

We ask whether $Ax = 0$, or equivalently $\tilde{A}x = 0$, has a solution with $x_{n+1} = 1$. Note that in (a) the $(k+1)$st row of $\tilde{A}$ represents the equation $x_{n+1} = 0$, while in (b) x_{n+1} is a free variable. Thus if the answer is yes, we are in case (b), while if the answer is no, we are in case (a).

If we are in case (a), we are done—we have specified $\tilde{A}$. If we are in case (b), there is more work to do, since we need to know we can specify the vector c. Now in case (b), x_{n+1} is a free variable, so we know by Lemma 2.5.2 that this system has a unique solution with $x_{n+1} = 1$ and all other free variables (if there are any) equal to 0. Let this *unique* solution be $x_{j_1} = b_1$, $x_{j_2} = b_2$, $\dots$, $x_{j_k} = b_k$, where the leading variables are $x_{j_1}, \dots, x_{j_k}$, $x_{n+1} = 1$, and $x_j = 0$ for x_j any free variable other than x_{n+1}. But applying Corollary 2.5.3 we see that $c_1 = -b_1$, $c_2 = -b_2$, $\dots$, $c_k = -b_k$, so c is uniquely determined. Thus the theorem is true in case $n+1$.

Hence by induction it is true for every positive integer n. □

Remark 2.5.5. This theorem shows the value of weak row-echelon form. For we see that in passing from row-echelon form to row-reduced echelon form, the positions of the leading entries do not change. Thus we only need to get as far as weak row-echelon form to know where the leading entries are, and hence how many nonzero rows $\tilde{A}$ will have, as well as exactly which variables those will be. ◊

Finally, we record the following useful result.

Lemma 2.5.6. *The only n-by-n matrix that is in reduced row-echelon form with n leading entries is the matrix*

$$I_n = \begin{bmatrix} 1 & & & & \\ & 1 & & 0 & \\ & & 1 & & \\ & 0 & & \ddots & \\ & & & & 1 \end{bmatrix}$$

(*i.e., the n-by-n matrix with all diagonal entries* 1 *and all other entries* 0).

Proof. This can also be proved by an inductive argument, which we leave to the reader. □

2.6. Exercises

1. (a) Draw all possible configurations of three planes, all passing through the origin, in $\mathbb{R}^3$. In each case, decide whether the corresponding homogeneous system of three equations in three unknowns is consistent and independent or consistent and dependent.

(b) Draw all possible configurations of three planes in $\mathbb{R}^3$. In each case, decide whether the corresponding system of three equations in three unknowns is consistent and independent, consistent and dependent, or inconsistent.

2. In each case, find all solutions of the homogeneous system $Ax = 0$:

(a) $A = \begin{bmatrix} 1 & 3 \\ 4 & 14 \end{bmatrix}$.

(b) $A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 4 & 5 \\ 3 & 8 & 5 \end{bmatrix}$.

(c) $A = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix}$.

(d) $A = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & -1 \\ 3 & 5 & 7 \end{bmatrix}$.

(e) $A = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 3 & 6 & 12 & 7 \\ 5 & 11 & 21 & 18 \\ 6 & 14 & 26 & 25 \end{bmatrix}$.

(f) $A = \begin{bmatrix} 1 & 4 & 2 & 3 & 0 \\ 3 & 12 & 6 & 7 & 2 \\ 2 & 9 & 5 & 11 & -5 \\ 7 & 30 & 16 & 28 & -7 \end{bmatrix}$.

3. In each case, find all solutions to $Ax = b$:

(a) $A = \begin{bmatrix} 1 & 3 \\ 4 & 14 \end{bmatrix}$, $b = \begin{bmatrix} 3 \\ 34 \end{bmatrix}$.

(b) $A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 4 & 5 \\ 3 & 8 & 5 \end{bmatrix}$, $b = \begin{bmatrix} 4 \\ 16 \\ 12 \end{bmatrix}$.

(c) $A = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix}$, $b = \begin{bmatrix} 3 \\ 8 \\ 13 \end{bmatrix}$.

(d) $A = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & -1 \\ 3 & 5 & 7 \end{bmatrix}$, $b = \begin{bmatrix} 2 \\ 3 \\ 17 \end{bmatrix}$.

(e) $A = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 3 & 6 & 12 & 7 \\ 5 & 11 & 21 & 18 \\ 6 & 14 & 26 & 25 \end{bmatrix}$, $b = \begin{bmatrix} 5 \\ 27 \\ 31 \\ 36 \end{bmatrix}$.

(f) $A = \begin{bmatrix} 1 & 4 & 2 & 3 & 0 \\ 3 & 12 & 6 & 7 & 2 \\ 2 & 9 & 5 & 11 & -5 \\ 7 & 30 & 16 & 28 & -7 \end{bmatrix}$, $b = \begin{bmatrix} 5 \\ 27 \\ 4 \\ 41 \end{bmatrix}$.

4. Fill in the intermediate steps in Example 2.4.5.

5. Let H_3 be the matrix $H_3 = \begin{bmatrix} 1 & 1/2 & 1/3 \\ 1/2 & 1/3 & 1/4 \\ 1/3 & 1/4 & 1/5 \end{bmatrix}$. ($H_3$ is known as a "Hilbert matrix".)

Let $v = \begin{bmatrix} 11/6 \\ 13/12 \\ 47/60 \end{bmatrix} = \begin{bmatrix} 1.8333\ldots \\ 1.0833\ldots \\ 0.78333\ldots \end{bmatrix}$ and let $w = \begin{bmatrix} 1.8 \\ 1.1 \\ .78 \end{bmatrix}$.

Solve the systems $H_3x = v$ and $H_3x = w$. (The difference between the two solutions will surprise you!)

6. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a 2-by-2 matrix.

(a) Suppose that $ad - bc \neq 0$. Let $v = \begin{bmatrix} p \\ q \end{bmatrix}$ with p and q arbitrary. Show that $Ax = v$ has a unique solution, and find that solution.

(b) Suppose that $ab - bc = 0$. Show that either $Ax = v$ does not have a solution, or that $Ax = v$ has infinitely many solutions. (Thus in this case $Ax = v$ never has a unique solution.)

7. (a) Find the unique polynomial $p(x)$ of degree at most two with $p(1) = 2$, $p'(1) = 13$, and $p''(1) = 10$.

(b) Find the unique polynomial $p(x)$ of degree at most two with $p(1) = 0$, $p'(1) = -2$, and $p(2) = -3$.

(c) Find the unique polynomial $p(x)$ of degree at most two with $p(1) = 7$, $p(2) = 21$, and $p(3) = 43$.

(Compare Theorem 5.2.8.)

8. Find the unique polynomial $p(x)$ of degree at most three with $p(-1) = 10$, $p'(-1) = -20$, $p(1) = -2$, and $p'(1) = -8$. (Compare Corollary 5.2.13.)

9. A function $t(i, j)$ is defined at points (i, j) on the grid below, with the property that the value of $t(i, j)$ at any point is the average of its values at the points immediately to the right, left, above, and below it. In the following example, find the missing values:

$$\begin{array}{ccccc} & -2 & 1 & 11 & \\ & \bullet & \bullet & \bullet & \\ 1\ \bullet & \bullet & \bullet & \bullet & \bullet\ 10 \\ -2\ \bullet & \bullet & \bullet & \bullet & \bullet\ -3 \\ & \bullet & \bullet & \bullet & \\ & -3 & 2 & 0 & \end{array}$$

(This is a model of the "discrete Laplacian". See Section 4.6, Exercise 21.)

10. Prove Lemma 2.5.6.

11. Let us say that the row operation of adding a multiple of row j to row i has index (j, i) and that the row operation of multiplying row j by a nonzero constant has index (j, j). Call a sequence of these types of row operations orderly if:

(1) every row operation in the sequence has type (j, i) with $i \leq j$,

(2) the indices of the row operations are in lexicographic order.

(Indices (j_1, i_1) and (j_2, i_2) are in lexicographic order if $j_1 < j_2$ or if $j_1 = j_2$ and $i_1 < i_2$.)

Call such a sequence reverse orderly if (1) is still true but the row operations are in reverse lexicographic order.

(a) Show that every upper triangular matrix with all diagonal entries nonzero can be obtained from the identity matrix by an orderly sequence of row operations.

(b) Show that every upper triangular matrix with all diagonal entries nonzero can be obtained from the identity matrix by a reverse orderly sequence of row operations.

There will be many more linear systems for you to think about and solve in the exercises to the remaining chapters of this book.

Vector spaces

In the next few chapters we define and study vector spaces and linear transformations, and study their basic properties. This generalizes our work in Chapter 1. But, as you will see, in general vectors have nothing to do with "arrows", and many things that you would not have thought of as vectors indeed are vectors, when properly viewed. That is precisely the point: linear algebra is ubiquitous in mathematics because all sorts of mathematical objects can be regarded as vectors.

3.1. The notion of a vector space

Here is the basic definition.

Definition 3.1.1. Let $\mathbb{F}$ be a field. A *vector space* over $\mathbb{F}$, or an $\mathbb{F}$-vector space, is a set V of objects, together with two operations:

(a) vector addition: for any v, w in V, their sum $v + w$ is defined; and

(b) scalar multiplication: for any c in $\mathbb{F}$ and any v in V, the product cv is defined.
Furthermore, these operations satisfy the following properties:
  (1) If v and w are elements of V, then $v + w$ is an element of V.
  (2) For any v, w in V, $v + w = w + v$.
  (3) For any u, v, w in V, $(u + v) + w = u + (v + w)$.
  (4) There is an element 0 in V such that for any v in V, $v + 0 = 0 + v = v$.
  (5) For any v in V there is an element $-v$ in V such that $v+(-v) = (-v)+v = 0$.
  (6) If c is an element of $\mathbb{F}$ and v is an element of V, then cv is an element of V.
  (7) For any c in $\mathbb{F}$ and any u and v in V, $c(u + v) = cu + cv$.
  (8) For any c and d in $\mathbb{F}$ and any v in V, $(c + d)v = cv + dv$.
  (9) For any c and d in $\mathbb{F}$ and any v in V, $c(dv) = (cd)v$.
  (10) For any v in V, $1v = v$.

The elements of $\mathbb{F}$ are called *scalars* and the elements of V are called *vectors*. $\Diamond$

In case $\mathbb{F}$ is understood, we will often simply refer to V as a vector space.

Here are some examples of vector spaces.

Example 3.1.2. For any nonnegative integer n, $\mathbb{F}^n$ is a vector space. From Theorem 1.1.4 we know that $\mathbb{F}^n$ satisfies these properties for every $n > 0$, and as observed in Remark 1.1.8 that $\mathbb{F}^0$ does as well. ◊

Example 3.1.3. Let V be the set of vectors

$$v = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \end{bmatrix}, \quad a_1, a_2, a_3, \dots \text{ elements of } \mathbb{F}$$

(where there is an entry a_i for every positive integer i, so that v "goes on forever"). Define addition by

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \end{bmatrix} + \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \end{bmatrix} = \begin{bmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \\ \vdots \end{bmatrix}$$

and scalar multiplication by

$$c \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \end{bmatrix} = \begin{bmatrix} ca_1 \\ ca_2 \\ ca_3 \\ \vdots \end{bmatrix}.$$

The 0 vector is defined to be

$$0 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \end{bmatrix}$$

and for a vector v, $-v$ is defined by

$$-\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \end{bmatrix} = \begin{bmatrix} -a_1 \\ -a_2 \\ -a_3 \\ \vdots \end{bmatrix}.$$

It is easy to check that the proof of Theorem 1.1.4 applies here as well, so V is a vector space. V is called *big* $\mathbb{F}^\infty$. There is no standard notation for this, so we will adopt the notation $\mathbb{F}^{\infty\infty}$. ◊

Example 3.1.4. Let V be the set of vectors $V = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \end{bmatrix}$, $a_1, a_2, a_3, \dots$ elements of $\mathbb{F}$, only finitely many $a_i \neq 0$. We define addition, scalar multiplication, the vector 0, and the vector $-v$ as in Example 3.1.3.

We note that if v and w are in V, so that each only has finitely many nonzero entries, then $v + w$ has only finitely many nonzero entries, so $v + w$ is in V, that 0 is in V as it has only finitely many nonzero entries (namely, none), that if v is in V then $-v$ is in V, as if v has only finitely many nonzero entries then so does $-v$, and that if v is in V and c is any element of $\mathbb{F}$, then cv is in V, as if v has only finitely many nonzero entries then so does cv for any c. Having observed these facts, the rest of the proof of Theorem 1.1.4 applies here as well, so V is a vector space. V is called *little* $\mathbb{F}^\infty$ and we will denote it by $\mathbb{F}^\infty$. $\Diamond$

Example 3.1.5. For any positive integer n,

$$V = \{[a_1 \ \ a_2 \ \ \dots \ \ a_n]\}, \quad \text{where } a_i \in \mathbb{F} \text{ for each } i = 1, \dots, n,$$

with addition and scalar multiplication defined coordinatewise, is a vector space. We denote this vector space by ${}^t\mathbb{F}^n$.

For $n = 0$, we defined $\mathbb{F}^0 = \{0\}$ in Definition 1.1.7, and we let ${}^t\mathbb{F}^0 = \{0\}$ as well.

Similarly to Example 3.1.3, we define

$${}^t\mathbb{F}^{\infty\infty} = \{[a_1 \ \ a_2 \ \ a_3 \ \ \dots]\}, \quad a_i \text{ elements of } \mathbb{F},$$

and similarly to Example 3.1.4, we define

$${}^t\mathbb{F}^{\infty} = \{[a_1 \ \ a_2 \ \ a_3 \ \ \dots]\}, \quad a_i \text{ elements of } \mathbb{F}, \text{ only finitely many } a_i \neq 0. \qquad \Diamond$$

Example 3.1.6. (a) Let

$$\begin{aligned} P(\mathbb{F}) &= \{\text{polynomials with coefficients in } \mathbb{F}\} \\ &= \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n\}, \quad a_0, a_1, a_2, \dots \text{ in } \mathbb{F}. \end{aligned}$$

We define addition of polynomials as usual,

$$(a_0+a_1x+\cdots+a_nx^n)+(b_0+b_1x+\cdots+b_nx^n) = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n$$

and scalar multiplication as usual,

$$c(a_0 + a_1 x + \cdots + a_n x^n) = ca_0 + (ca_1)x + \cdots + (ca_n)x^n.$$

The 0 element of $P(\mathbb{F})$ is simply the 0 polynomial (i.e., the polynomial with every coefficient 0), and also $-(a_0 + a_1 x + \cdots + a_n x^n) = (-a_0) + (-a_1)x + \cdots + (-a_n)x^n$.

Then $P(\mathbb{F})$ is a vector space.

(b) Recall that the degree of the nonzero polynomial is the highest power of x that appears in the polynomial, i.e., the polynomial $a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$ has degree n. By convention, the 0 polynomial has degree $-\infty$ with $-\infty \leq d$ for any nonnegative integer d.

For any $d \geq 0$, let

$$P_d(\mathbb{F}) = \{\text{polynomials with coefficients in } \mathbb{F} \text{ of degree at most } d\}.$$

Then $P_d(\mathbb{F})$ is a vector space. $\Diamond$

Example 3.1.7. (a) Let X be any set, and let

$$V = \{f \colon X \to \mathbb{F}\},$$

i.e., the set of functions f defined on X with values in $\mathbb{F}$. We define addition of functions as usual, i.e., if $f(x)$ and $g(x)$ are functions, then their sum $(f+g)(x)$ is the function given by

$$(f+g)(x) = f(x) + g(x) \quad \text{for every } x \in X.$$

We define multiplication of functions by elements of $\mathbb{F}$ as usual, i.e., if $f(x)$ is a function and c is in $\mathbb{F}$, then $(cf)(x)$ is the function given by

$$(cf)(x) = cf(x) \quad \text{for every } x \in X.$$

The zero function is the function $0 = 0(x)$ whose value is identically 0, i.e., the function given by

$$0(x) = 0 \quad \text{for every } x \in X.$$

For a function f, the function $-f$ is the function given by

$$(-f)(x) = -f(x) \quad \text{for every } x \in X.$$

Then V is a vector space over $\mathbb{F}$.

(b) More generally, let X be any set, and let W be any vector space over $\mathbb{F}$. Let V be defined by

$$V = \{f\colon X \to W\},$$

i.e., V is the set of functions defined on X with values in W. We define vector addition, scalar multiplication, etc., similarly, noting that these make sense precisely because vector addition and scalar multiplication are defined in W, since W is a vector space.

Then V is a vector space over $\mathbb{F}$. $\Diamond$

In Section 1.1, we had four additional properties of $\mathbb{F}^n$, properties (11)–(14). We remarked there that they were consequences of properties (1)–(10). We show that now, for any vector space. Along the way, we will show some other properties as well.

Lemma 3.1.8. *Let V be a vector space over $\mathbb{F}$.*

(15) *The 0 element of V is unique, i.e., there is only one element 0 of V with the property that $0 + v = v + 0 = v$ for every $v \in V$.*

(16) *For any element v of V, the element $-v$ is unique, i.e., for every element v of V there is only one element $-v$ of V with the property that $v + (-v) = (-v) + v = 0$.*

(17) *Let w be an element of V with the property that for some vector v_0 in V, $w + v_0 = v_0$ (or $v_0 + w = v_0$). Then $w = 0$.*

Proof. We prove something is unique in the usual way, by supposing there are two of them and showing they must be the same.

(15) We have the element 0 of V with the property that $0 + v = v + 0 = v$ for every $v \in V$. Suppose we have another element $0'$ of V with the property that $0' + v = v + 0' = v$ for every $v \in V$. Then, by the property of 0, $0' + 0 = 0'$. But by the property of $0'$, $0' + 0 = 0$. Thus

$$0' = 0' + 0 = 0$$

and 0 is unique.

(16) Given the element v of V, we have the element $-v$ with the property that $(-v)+v = v+(-v) = 0$. Suppose we have another element $(-v)'$ with the property that $(-v)' + v = v + (-v)' = 0$. Then we have the following chain of equalities:

$$\begin{aligned} (-v)' + v &= 0, \\ ((-v)' + v) + (-v) &= 0 + (-v), \\ ((-v)' + v) + (-v) &= -v, \\ (-v)' + (v + (-v)) &= -v, \\ (-v)' + 0 &= -v, \\ (-v)' &= -v, \end{aligned}$$

and $-v$ is unique.

(17) We have the chain of equalities

$$\begin{aligned} w + v_0 &= v_0, \\ (w + v_0) + (-v_0) &= v_0 + (-v_0), \\ w + (v_0 + (-v_0)) &= 0, \\ w + 0 &= 0, \\ w &= 0, \end{aligned}$$

as claimed. □

Theorem 3.1.9. *Let v be a vector space over $\mathbb{F}$.*

(11) *For any vector v in V, $0v = 0$, the 0 vector in V.*

(12) *If 0 is the 0 vector in V, then for any scalar c, $c0 = 0$, the 0 vector in V.*

(13) *For any vector v in V, $(-1)v = -v$.*

Proof. (11) We have the equalities

$$0v = (0 + 0)v = 0v + 0v,$$

so by (17), $0v = 0$.

(12) We have the equalities

$$c0 = c(0 + 0) = c0 + c0,$$

so by (17), $c0 = 0$.

(13) We have the equalities

$$(-1)v + v = (-1)v + 1v = (-1 + 1)v = 0v = 0$$

and similarly

$$v + (-1)v = 1v + (-1)v = (1 + -1)v = 0v = 0,$$

so by (16), $(-1)v = -v$. □

Theorem 3.1.10. *Let V be a vector space over $\mathbb{F}$.*

(14) *Let c be a scalar and let v be a vector in V. If $cv = 0$, then $c = 0$ or $v = 0$.*

Proof. Suppose $cv = 0$. If $c = 0$, we are done. Suppose not. Then, since $\mathbb{F}$ is a field, c has a multiplicative inverse $1/c$ in $\mathbb{F}$. We then have the chain of equalities

$$\begin{aligned} cv &= 0, \\ (1/c)cv &= (1/c)0, \\ (1/c)cv &= 0, \\ ((1/c)c)v &= 0, \\ 1v &= 0, \\ v &= 0. \end{aligned}$$

□

3.2. Linear combinations

We now introduce the notion of a linear combination of a set of vectors in a general vector space V. It is a direct generalization of the notion of a linear combination of a set of vectors in $\mathbb{F}^n$ that we introduced in Section 1.2.

Definition 3.2.1. (1) Let $S = \{v_1, \dots, v_k\}$ be a finite set of vectors in a vector space V. Then for any scalars $c_1, \dots, c_k$,

$$v = \sum_{i=1}^{k} c_i v_i = c_1 v_1 + c_2 v_2 + \cdots + c_k v_k$$

is a *linear combination* of the vectors in S.

(2) Let $S = \{v_1, v_2, \dots\}$ be an arbitrary set of vectors in a vector space V. Then for any scalars $c_1, c_2, \dots$, only finitely many of which are nonzero,

$$v = \sum c_i v_i$$

(a finite sum) is a *linear combination* of the vectors in S.

(3) If S is the empty subset of V, then the vector 0 in V is the (one and only) linear combination of the vectors in S. ◊

Definition 3.2.2. In the above situation, if $c_i = 0$ for every i, the linear combination is *trivial.* Otherwise (i.e., if $c_i \neq 0$ for at least one i) the linear combination is *nontrivial.* In (3), the (only) linear combination is *trivial.* ◊

Lemma 3.2.3. *The value of any trivial linear combination is* 0.

Proof. If every $c_i = 0$, then $v = 0v_1 + 0v_2 + \cdots = 0 + 0 + \cdots = 0$. □

In Section 1.2 we raised two questions about linear combinations of sets of vectors. Now that we have developed more machinery, we can effectively answer them.

First we introduce some standard terminology.

Definition 3.2.4. Let S be a set of vectors in a vector space V.

(1) S is *linearly independent* if the *only* linear combination of vectors in S that is equal to 0 is the trivial linear combination. That is, $S = \{v_1, v_2, \dots\}$ is linearly independent if

$$c_1 v_1 + c_2 v_2 + \cdots = 0$$

implies $c_1 = c_2 = \cdots = 0$.

(2) S *spans* V if *every* vector in V can be expressed as a linear combination of vectors in S. That is, $S = \{v_1, v_2, \dots\}$ spans V if for every $v \in V$ there are scalars $c_1, c_2, \dots$ such that

$$c_1 v_1 + c_2 v_2 + \cdots = v. \qquad \Diamond$$

(Again we recall that all sums must be finite.)

Let S be a set of vectors in the vector space V.

The two questions we ask are:

(1) Is S linearly independent?

(2) Does S span V?

Before answering these questions we introduce another perspective on linear independence. We shall say that S is *linearly dependent* if it is not linearly independent. Then we have:

Lemma 3.2.5. *Let S be a set of vectors in V. The following are equivalent*:

(1) *S is linearly dependent.*

(2) *Some vector in S can be expressed as a linear combination of the other vectors in S.*

Proof. First suppose S is linearly dependent. Then we have an equation

$$\sum c_i x_i = 0$$

with not all of the $c_i = 0$. Choose any particular i_0 for which $c_{i_0} \neq 0$. Then

$$\begin{aligned} c_{i_0} v_{i_0} + \sum_{i \neq i_0} c_i v_i &= 0, \\ c_{i_0} v_{i_0} &= -\sum_{i \neq i_0} c_i v_i, \\ v_{i_0} &= \sum_{i \neq i_0} (-c_i / c_{i_0}) v_i \end{aligned}$$

and v_{i_0} is expressed as a linear combination of the other vectors in S.

Next suppose some vector in S, say v_{i_0}, is a linear combination of the other vectors in S,

$$v_{i_0} = \sum_{i \neq i_0} c_i v_i.$$

Then

$$0 = (-1) v_{i_0} + \sum_{i \neq i_0} c_i v_i.$$

This is a nontrivial linear combination as the coefficient -1 of v_{i_0} is nonzero. Thus S is linearly dependent. $\square$

Remark 3.2.6. In view of this lemma, one way to think of a linearly dependent set is that one of the vectors in it is redundant, in the sense that it can be expressed in terms of the other vectors. Then from this point of view a linearly independent set is nonredundant, in the sense that no vector can be expressed in terms of the others. $\Diamond$

We shall call equation $\sum c_i v_i = 0$ among the vectors in S a *linear dependence relation*. If not all $c_i = 0$, we will call this *nontrivial*. Thus S is linearly dependent if and only if there is a nontrivial linear dependence relation among the vectors in S.

Example 3.2.7. In each case we ask:

(1a) Is S linearly independent?

(1b) If not, find a nontrivial linear dependence relation among the vectors of S.

(a) $S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ -3 \end{bmatrix}, \begin{bmatrix} 5 \\ 6 \\ 12 \end{bmatrix} \right\} = \{v_1, v_2, v_3\}$.

Answer. We are trying to solve $c_1v_1 + c_2v_2 + c_3v_3 = 0$. As we have already seen, this is the matrix equation $Ax = 0$, where $A = [v_1|v_2|v_3]$ and $x = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$. Thus to solve this we begin with $A = \begin{bmatrix} 1 & 0 & 5 \\ 2 & 2 & 6 \\ 0 & -3 & 12 \end{bmatrix}$ and row-reduce. In this case we don't have to carry out the row reduction all the way. We can just go far enough to obtain the matrix $\begin{bmatrix} 1 & 0 & 5 \\ 0 & 2 & -4 \\ 0 & 0 & 6 \end{bmatrix}$ in weak row-echelon form. We can already see from this matrix that every column will have a leading entry, so there are no free variables, and $Ax = 0$ has only the trivial solution. Thus S is linearly independent.

(b) $S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 4 \\ -3 \end{bmatrix}, \begin{bmatrix} 7 \\ 6 \\ 12 \end{bmatrix} \right\} = \{v_1, v_2, v_3\}$.

Answer. Just as in part (a), this is the matrix equation $Ax = 0$ with $A = [v_1|v_2|v_3]$ and $x = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$. Thus, again to solve this, we begin with $A = \begin{bmatrix} 1 & 1 & 7 \\ 2 & 4 & 6 \\ 0 & -3 & 12 \end{bmatrix}$ and row-reduce. We get part of the way, to obtain the matrix $\begin{bmatrix} 1 & 1 & 7 \\ 0 & 2 & -8 \\ 0 & 0 & 0 \end{bmatrix}$ in weak row-echelon form. We can already see from this matrix that there will be no leading entry in the third column, so there will be a free variable. Thus $Ax = 0$ will have a nontrivial solution, so S is linearly dependent.

Note that if we were only interested in question (1a) we could stop here—we have already answered it. To answer (1b) we go further, and reduce A to reduced row-echelon form. We obtain $\begin{bmatrix} 1 & 0 & 11 \\ 0 & 1 & -4 \\ 0 & 0 & 0 \end{bmatrix}$, and then we see $x = c_3 \begin{bmatrix} -11 \\ 4 \\ 1 \end{bmatrix}$ is the general solution. Since the problem as stated only asked for *a* nontrivial linear dependence relation, we could choose $c_3 = 1$ and we have the relation

$$-11\begin{bmatrix}1\\2\\0\end{bmatrix} + 4\begin{bmatrix}1\\4\\-3\end{bmatrix} + 1\begin{bmatrix}7\\6\\12\end{bmatrix} = \begin{bmatrix}0\\0\\0\end{bmatrix}$$

(which is easy to check).

(c) $S = \left\{ \begin{bmatrix}1\\0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\2\\4\end{bmatrix}, \begin{bmatrix}2\\3\\6\\1\end{bmatrix} \right\} = \{v_1, v_2, v_3\}$.

Again we row-reduce the matrix $A = \begin{bmatrix}1 & 1 & 2\\0 & 1 & 3\\1 & 2 & 6\\1 & 4 & 1\end{bmatrix}$ and we obtain a weak row-echelon form $\begin{bmatrix}1 & 1 & 2\\0 & 1 & 3\\0 & 0 & 1\\0 & 0 & 0\end{bmatrix}$. There are no free variables, so $Ax = 0$ only has the trivial solution, and S is linearly independent. (Observe that in this example, A reduces to a matrix with a 0 row, but that is *completely irrelevant.*)

(d) $S = \left\{ \begin{bmatrix}1\\0\\2\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix}, \begin{bmatrix}0\\3\\1\end{bmatrix}, \begin{bmatrix}0\\-1\\-1\end{bmatrix} \right\} = \{v_1, v_2, v_3, v_4\}$.

Again we let $A = [v_1|v_2|v_3|v_4]$ and row-reduce. $A = \begin{bmatrix}1 & 1 & 0 & 0\\0 & 1 & 3 & -1\\2 & 1 & 1 & -1\end{bmatrix}$ row-reduces to $A = \begin{bmatrix}1 & 0 & 0 & -1/2\\0 & 1 & 0 & 1/2\\0 & 0 & 1 & -1/2\end{bmatrix}$ in reduced row-echelon form, and then we see $Ax = 0$ has general solution $x = c_4\begin{bmatrix}1/2\\-1/2\\1/2\\1\end{bmatrix}$ so choosing $c_4 = 2$ (for convenience) we obtain the linear dependence relation

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

In this example we passed directly to question (1b). We could answer question (1a) with no row-reduction *at all.* See Theorem 3.2.8 below.

(e) $S = \{1+x+2x^2+4x^3, 2+3x+4x^2+6x^3, 1+x+3x^2+4x^3, 3+4x+6x^2+11x^3\} = \{v_1, v_2, v_3, v_4\}$, vectors in $P_3(\mathbb{R})$.

We wish to solve the equation $c_1v_1 + c_2v_2 + c_3v_3 + c_4v_4 = 0$, i.e., the equation

$$c_1(1 + x + 2x^2 + 4x^3) + c_2(2 + 3x + 4x^2 + 6x^3) + c_3(1 + x + 3x^2 + 4x^3) + c_4(3 + 4x + 6x^2 + 11x^3) = 0.$$

Gathering the coefficients of like powers of x together, this becomes

$$(c_1 + 2c_2 + c_3 + 3c_4) + (c_1 + 3c_2 + c_3 + 4c_4)x + (2c_1 + 4c_2 + 3c_3 + 6c_4)x^2 \\ + (4c_1 + 6c_2 + 4c_3 + 11c_4)x^3 = 0.$$

Since a polynomial is 0 exactly when all its coefficients are 0, this gives us the system of linear equations:

$$\begin{aligned} c_1 + 2c_2 + c_3 + 3c_4 &= 0, \\ c_1 + 3c_2 + c_3 + 4c_4 &= 0, \\ 2c_1 + 4c_2 + 3c_3 + 6c_4 &= 0, \\ 4c_1 + 6c_2 + 4c_3 + 11c_4 &= 0. \end{aligned}$$

This system has matrix

$$A = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 1 & 3 & 1 & 4 \\ 2 & 4 & 3 & 6 \\ 4 & 6 & 4 & 11 \end{bmatrix} \quad \text{which reduces to the matrix} \quad \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and there are no free variables, so S is linearly independent. $\Diamond$

Here is one situation in which we know the answer to question (1a) with absolutely no work.

Theorem 3.2.8. *Let S be a set of n vectors in $\mathbb{F}^m$, with $n > m$. Then S is linearly dependent.*

Proof. This is just Corollary 1.4.7(3) (which was a direct consequence of our basic counting theorem, Theorem 1.4.5). $\square$

Here is a result we will be using later.

Lemma 3.2.9. *Let A be an m-by-n matrix that is in weak row-echelon form. Suppose that A has k nonzero rows. Let them be $v_1, \dots, v_k$ and note that each v_i is a vector in the vector space ${}^t\mathbb{F}^n$. Then $\{v_1, \dots, v_k\}$ is linearly independent.*

Proof. We prove this by induction on k. If $k = 0$, then the empty set is linearly independent, and if $k = 1$, the set $\{v_1\}$ is linearly independent since $v_1 \neq 0$.

Now suppose the theorem is true for k and consider the $k + 1$ case. Suppose we have a linear combination

$$c_1v_1 + \cdots + c_{k+1}v_{k+1} = 0.$$

Let v_1 have its leading entry $a_1 \neq 0$ in column j_1. Note by the definition of weak row-echelon form that the leading entries of $v_2, v_3, \dots$ are all in columns to the right of column j_1, and so their entry in column j_1 is 0. Thus we see that the entry in column j_1 of the linear combination $c_1v_1 + \cdots + c_{k+1}v_{k+1}$ is c_1a_1. But this linear combination is equal to 0, so we must have $c_1 = 0$. Then we are left with the equation $c_2v_2 + \cdots + c_{k+1}v_{k+1} = 0$.

Now consider the matrix consisting of rows 2 through $k+1$ of A. This is also in weak row-echelon form, with k nonzero rows, so by the inductive hypothesis we have $c_2 = \cdots = c_{k+1} = 0$.

Thus our linear combination must be the trivial one, and the theorem is true in the $k+1$ case.

Hence by induction it is true for every k. □

Now we come to our second question. Again, we introduce some standard terminology first.

Definition 3.2.10. Let S be a set of vectors in a vector space V. Then $\text{Span}(S)$ is the set of all vectors in V that can be expressed as a linear combination of the vectors in V. ♢

Thus we see that $\text{Span}(S) = V$ is just another way of saying that S spans V.

Example 3.2.11. In each case we ask:

(2) Is $\text{Span}(S) = V$?

(a) $S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ -3 \end{bmatrix}, \begin{bmatrix} 5 \\ 6 \\ 12 \end{bmatrix} \right\} = \{v_1, v_2, v_3\}$.

Answer. We are trying to see whether $c_1v_1 + c_2v_2 + c_3v_3 = v$ has a solution for every v. As we have seen, this is the matrix equation $Ax = v$, where $A = [v_1|v_2|v_3]$ and $x = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$. To solve this we begin with this matrix A and row-reduce. Now this is the same set S as in Example 3.2.7(a) and so the same matrix A. Thus it reduces to the same matrix $\begin{bmatrix} 1 & 0 & 5 \\ 0 & 2 & -4 \\ 0 & 0 & 6 \end{bmatrix}$ in weak row-echelon form, and this matrix has *no* zero rows, so $Ax = v$ *always* has a solution and S spans $\mathbb{R}^3$.

(b) $S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 4 \\ -3 \end{bmatrix}, \begin{bmatrix} 7 \\ 6 \\ 12 \end{bmatrix} \right\} = \{v_1, v_2, v_3\}$.

Again we form $A = [v_1|v_2|v_3]$ and ask whether $Ax = v$ always has a solution. This is the same set as in Example 3.2.7(b) and so the same matrix A. Thus it reduces to the same matrix $\begin{bmatrix} 1 & 1 & 7 \\ 0 & 2 & -8 \\ 0 & 0 & 0 \end{bmatrix}$. Since this matrix has a 0 row, we see that $Ax = v$ *does not always* have a solution, and so S does not span $\mathbb{R}^3$.

(c) $S = \left\{ \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 6 \\ 1 \end{bmatrix} \right\} = \{v_1, v_2, v_3\}$.

Again we form $A = [v_1|v_2|v_3]$ and ask whether $Ax = v$ always has a solution. This is the same set as in Example 3.2.7(c) and so the same matrix A, which reduces to $A = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$. Since this matrix has a 0 row, S does not span V. But in fact we could answer this question with no row-reduction *at all.* See Theorem 3.2.13 below.

(d) $S = \left\{ \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ -1 \\ -1 \end{bmatrix} \right\} = \{v_1, v_2, v_3, v_4\}$.

Again we form $A = [v_1|v_2|v_3]$ and row-reduce. S is the same as in Example 3.2.7(d), so A is the same and reduces to the same matrix $A = \begin{bmatrix} 1 & 0 & 0 & -1/2 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & 1 & -1/2 \end{bmatrix}$ in reduced row-echelon form. Since this matrix does not have any 0 rows, S spans V. (In this case there is a free variable, but that is *completely irrelevant.*)

(e) $S = \{1+x+2x^2+4x^3, 2+3x+4x^2+6x^3, 1+x+3x^2+4x^3, 3+4x+6x^2+11x^3\} = \{v_1, v_2, v_3, v_4\}$, vectors in $P_3(\mathbb{R})$.

This is the same set of vectors as in Example 3.2.7(e), but now we are asking whether the equation

$$\begin{aligned} c_1(1 + x + 2x^2 + 4x^3) + c_2(2 + 3x + 4x^2 + 6x^3) + c_3(1 + x + 3x^2 + 4x^3) \\ + c_4(3 + 4x + 6x^2 + 11x^3) = b_0 + b_1x + b_2x^2 + b_3x^3 \end{aligned}$$

has a solution for every b_0, b_1, b_2, b_3. This gives the matrix equation $Ax = b$, where A is the same and $b = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}$. A row-reduces to the same matrix, which has no zero rows, so S spans $V = P_3(\mathbb{R})$. $\Diamond$

Now we can ask a more particular question. Let S be a set of vectors in V. Given a particular vector v in V, we can ask if v can be expressed as a linear combination of the vectors in S. Of course, if S spans V every vector in V can be expressed in this way, so the answer is automatically yes. But if not, then, depending on v, the answer may be yes or may be no. In fact, this is a question we already know how to answer.

Example 3.2.12. Let $S = \left\{ \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 6 \\ 1 \end{bmatrix} \right\} = \{v_1, v_2, v_3\}$ as in Example 3.2.11(c).

Let v be a vector in $\mathbb{F}^3$. We ask:

(a) Is v in $\mathrm{Span}(S)$?

(b) If so, express v as a linear combination of the vectors in S.

(a) (i) $v = \begin{bmatrix} 3 \\ 4 \\ 8 \\ 7 \end{bmatrix}$. We are asking whether $v = x_1v_1 + x_2v_2 + x_3v_3$ has a solution. The augmented matrix

$$\left[\begin{array}{ccc|c} 1 & 1 & 2 & 3 \\ 0 & 1 & 3 & 4 \\ 1 & 2 & 6 & 8 \\ 1 & 4 & 1 & 7 \end{array}\right] \quad \text{reduces to} \quad \left[\begin{array}{ccc|c} 1 & 1 & 2 & 3 \\ 0 & 1 & 3 & 4 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{array}\right]$$

so we see that this system is inconsistent and the answer to our question is no.

(ii) $v = \begin{bmatrix} 3 \\ 5 \\ 10 \\ -2 \end{bmatrix}$. This time we have a system with augmented matrix

$$\left[\begin{array}{ccc|c} 1 & 1 & 2 & 3 \\ 0 & 1 & 3 & 5 \\ 1 & 2 & 6 & 10 \\ 1 & 4 & 1 & -2 \end{array}\right] \quad \text{which reduces to} \quad \left[\begin{array}{ccc|c} 1 & 1 & 2 & 3 \\ 0 & 1 & 3 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

so we see that this system is consistent and the answer to our question is yes.

(b) Now we're asked to actually find a solution. So we continue and we see that it further reduces to

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

with solution $x_1 = 0$, $x_2 = -1$, $x_3 = 2$, and so we see

$$\begin{bmatrix} 3 \\ 5 \\ 10 \\ -2 \end{bmatrix} = (-1)\begin{bmatrix} 1 \\ 1 \\ 2 \\ 4 \end{bmatrix} + (2)\begin{bmatrix} 2 \\ 3 \\ 6 \\ 1 \end{bmatrix}. \qquad \Diamond$$

Here is one situation where we know the answer to question (2) with absolutely no work.

Theorem 3.2.13. *Let S be a set of n vectors in $\mathbb{F}^m$, with $n < m$. Then S does not span V.*

Proof. This is just Corollary 1.4.8(3). $\square$

Remark 3.2.14. Let us tabulate the results of Example 3.2.7 and Example 3.2.11.

	Is S linearly independent?	Does S span V?
(a)	Yes	Yes
(b)	No	No
(c)	Yes	No
(d)	No	Yes
(e)	Yes	Yes

As you can see, in general these questions are completely independent. Knowing the answer to one doesn't tell us anything about the answer to the other. ♢

Remark 3.2.15. While we said that in general these two questions are independent of each other, there is one important case in which they always have the *same* answer. We will prove below (Theorem 3.3.9): Let S be a set of n vectors in $\mathbb{F}^n$. Then either

(a) S is linearly independent and spans $\mathbb{F}^n$; or

(b) S is linearly dependent and does not span $\mathbb{F}^n$.

(Compare Example 3.2.7 and Example 3.2.11 parts (a) and (b)).

In fact, we will be developing the notion of the *dimension* of a vector space V, which will explain why the two answers in (a), in (d), and in (e) must be the same. ♢

We now return to considering sets of vectors in a general vector space V, thinking about the questions we have just investigated in a general context. We have the following very helpful result along these lines.

Lemma 3.2.16. *Let S be a set of vectors $S = \{v_1, v_2, \dots\}$ in a vector space V. Let S' be the set of vectors in V obtained from S by any one of the following operations*:

(a) *Replace v_i by $v_i' = cv_i$ for some $c \neq 0$.*

(b) *Replace v_j by $v_j' = v_j + cv_i$ for some c.*

(c) *Interchange v_i and v_j (i.e., set $v_i' = v_j$ and $v_j' = v_j$).*

Then

(1) *S is linearly independent if and only if S' is linearly independent*; *and*

(2) $\mathrm{Span}(S) = \mathrm{Span}(S')$.

Proof. The idea of the proof here is the same as the idea of the proof of Lemma 2.2.5, and again we leave it to the reader to fill in the details. □

3.3. Bases and dimension

In this section we introduce, and then carefully study, the notion of a basis of a vector space. It is this notion that leads us to be able to define the dimension of a vector space.

Definition 3.3.1. A set $\mathcal{B}$ of vectors in a vector space V is a *basis* of V if

(1) $\mathcal{B}$ is linearly independent; and

(2) $\mathcal{B}$ spans V. ♢

Here are some examples of bases.

Example 3.3.2. (a) The standard basis of $\mathbb{F}^n$ that we introduced in Definition 1.2.7 and which we proved was indeed a basis of $\mathbb{F}^n$ in Theorem 1.2.8.

In a similar fashion, we may let ${}^t e_i = [a_1 \;\; a_2 \;\; \dots \;\; a_n]$ be the vector in ${}^t\mathbb{F}^n$ with $a_i = 1$ and $a_j = 0$ for $j \neq i$. Then ${}^t\mathcal{E} = \{{}^t e_1, \dots, {}^t e_n\}$ is a basis of ${}^t\mathbb{F}^n$.

(b) The set $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ -3 \end{bmatrix}, \begin{bmatrix} 5 \\ 6 \\ 12 \end{bmatrix} \right\}$ is a basis of $\mathbb{R}^3$, as we proved in Example 3.2.7(a) and Example 3.2.11(a).

(c) The set $\mathcal{B} = \{1, x, x^2, \dots, x^d\}$ is a basis of $P_d(\mathbb{F})$, as any polynomial of degree at most d, $a_0 + a_1x + \cdots + a_dx^d$, is evidently a linear combination of the elements of $\mathcal{B}$, and to say a polynomial is 0 is to say its coefficients are 0, so $\mathcal{B}$ is linearly independent.

(d) The set $\mathcal{B} = \{1+x+2x^2+4x^3, 2+3x+4x^2+6x^3, 1+x+3x^2+4x^3, 3+4x+6x^2+11x^3\}$ is a basis of $P_3(\mathbb{R})$, as we saw in Example 3.2.7(e) and Example 3.2.11(e). $\diamondsuit$

We begin with an extremely important characterization of bases.

Lemma 3.3.3. *Let $\mathcal{B}$ be a set of vectors in a vector space V. Then $\mathcal{B}$ is a basis of V if and only if every vector of V can be expressed as a linear combination of the vectors in $\mathcal{B}$ in a unique way.*

Proof. Let $\mathcal{B} = \{v_1, v_2, \dots\}$. First suppose $\mathcal{B}$ is a basis of V. Let $v \in V$. Since $\mathcal{B}$ spans V, we can write $v = \sum c_iv_i$ for some scalars $\{c_i\}$. To show that this expression is unique, suppose also $v = \sum c_i'v_i$. Then $0 = v - v = \sum c_iv_i - \sum c_i'v_i = \sum(c_i - c_i')v_i$. But $\mathcal{B}$ is linearly independent, so $c_i - c_i' = 0$ for each i, i.e., $c_i' = c_i$ for each i, and the expression is unique.

On the other hand, suppose every vector of V can be expressed as a linear combination of the vectors in $\mathcal{B}$ in a unique way. Then, in particular, every vector of V can be expressed as a linear combination of the vectors in $\mathcal{B}$, so $\mathcal{B}$ spans V. Also, in particular the vector 0 can be expressed as a linear combination of the vectors in $\mathcal{B}$ in a unique way. But we certainly have the trivial linear combination $0 = \sum 0v_i$, so by uniqueness that is the only linear combination that is equal to 0, and $\mathcal{B}$ is linearly independent. $\square$

Here is a key technical lemma that will lead us directly to our first main result. As you will see, the proof is just an application of our basic counting theorem.

Lemma 3.3.4. *Let V be a vector space and suppose that V is spanned by some set $\mathcal{C}$ of m vectors. Then any set $\mathcal{D}$ of n vectors in V, with $n > m$, is linearly dependent.*

Proof. Write $\mathcal{C} = \{v_1, \dots, v_m\}$ and $\mathcal{D} = \{w_1, \dots, w_n\}$.

Since $\mathcal{C}$ spans V, every vector in $\mathcal{D}$ can be written as a linear combination of the vectors in $\mathcal{C}$. Thus for each $i = 1, \dots, n$, we have

$$w_i = a_{1i}v_1 + a_{2i}v_2 + \cdots + a_{mi}v_m = \sum_{j=1}^{m} a_{ji}v_j$$

for some $a_{1i}, a_{2i}, \dots, a_{mi}$. (These may not be unique, but that doesn't matter. Just choose any linear combination that is equal to w_i.)

We want to show that $\mathcal{D}$ is linearly dependent, i.e., that the equation

$$c_1w_1 + c_2w_2 + \cdots + c_nw_n = 0$$

has a nontrivial solution. Let us substitute the above expressions for w_i into this equation. We obtain:

$$c_1\left(\sum_{j=1}^{m} a_{j1}v_j\right) + c_2\left(\sum_{j=1}^{m} a_{j2}v_j\right) + \cdots + c_n\left(\sum_{j=1}^{m} a_{jn}v_j\right) = 0.$$

Let us gather the terms in each of the vectors v_j together. We obtain:

$$\left(\sum_{i=1}^{n} c_i a_{1i}\right)v_1 + \left(\sum_{i=1}^{n} c_i a_{2i}\right)v_2 + \cdots + \left(\sum_{i=1}^{n} c_i a_{mi}\right)v_m = 0.$$

This will certainly be the case if the coefficients of each of the vectors v_i are zero. This gives the equations:

$$\begin{aligned}\sum_{i=1}^{n} c_i a_{1i} &= 0\\ \sum_{i=1}^{n} c_i a_{2i} &= 0\\ &\vdots\\ \sum_{i=1}^{n} c_i a_{mi} &= 0.\end{aligned}$$

Writing this out, we see that this is the system

$$\begin{aligned}a_{11}c_1 + a_{12}c_2 + \cdots + a_{1n}c_n &= 0\\ a_{21}c_1 + a_{22}c_2 + \cdots + a_{2n}c_n &= 0\\ &\vdots\\ a_{m1}c_1 + a_{m2}c_2 + \cdots + a_{mn}c_n &= 0.\end{aligned}$$

But this is a homogeneous system of m equations in n unknowns, with $n > m$, so by Theorem 1.4.5 this has a nontrivial solution. □

Theorem 3.3.5. *Let V be a vector space. Then any two bases of V have the same number of elements.*

Proof. Suppose $\mathcal{B}_1$ and $\mathcal{B}_2$ are two bases of V with p and q elements, respectively. Then

(1) $\mathcal{B}_1$ is linearly independent; and
(2) $\mathcal{B}_1$ spans V,

and also

(1) $\mathcal{B}_2$ is linearly independent; and
(2) $\mathcal{B}_2$ spans V.

Thus we can apply Lemma 3.3.4 with $\mathcal{C} = \mathcal{B}_1$, $\mathcal{D} = \mathcal{B}_2$, $m = p$, and $n = q$ to conclude that $q \leq p$. But we can also apply Lemma 3.3.4 with $\mathcal{C} = \mathcal{B}_2$, $\mathcal{D} = \mathcal{B}_1$, $m = q$, and $n = p$ to conclude that $p \leq q$.

Hence $p = q$. □

Given this theorem, we can now define the dimension of vector space.

Definition 3.3.6. Let V be a vector space. If V has a basis with a finite number n of elements, then V has *dimension* n, $\dim V = n$. Otherwise V has infinite dimension, $\dim V = \infty$. ♢

Let us see some examples.

Example 3.3.7. (1) For any n, $\mathbb{F}^n$ has dimension n, as the standard basis $\mathcal{E}_n$ of $\mathbb{F}^n$ (and hence any other basis) has n elements. (For $n = 0$, $\mathbb{F}^0 = \{0\}$ has the empty set, with 0 elements, as a basis.)

(2) For any d, $P_d(\mathbb{F})$ has dimension $d+1$, as the basis $\{1, x, \ldots, x^d\}$ (and hence any other basis) has $d+1$ elements. ♢

Remark 3.3.8. Note that this definition agrees with our intuition. Geometrically speaking, $\mathbb{F}^n$ *should* be n-dimensional. So we can regard this definition as a way of making our geometric intuition precise. ♢

Recall we had our two basic questions about sets of vectors in a vector space V: is the set linearly independent and does the set span V?

We can now simply count to help us answer these questions.

Theorem 3.3.9. *Let V be a vector space of finite dimension m. Let S be a set of n vectors in V.*

(1) *If $n > m$ (possibly $n = \infty$), then S is not linearly independent.*
(2) *If $n < m$, then S does not span V.*
(3) *If $n \neq m$, then S is not a basis of V.*
(4) *If $n = m$, the following are equivalent:*
  (a) *S is a basis of V.*
  (b) *S is linearly independent.*
  (c) *S spans V.*

Proof. Since V has dimension m, it has a basis $\mathcal{B}$ consisting of m vectors.

(1) Since $\mathcal{B}$ is a basis, $\mathcal{B}$ spans V, and so this is just Lemma 3.3.4.

(2) If S spanned V, then $\mathcal{B}$ would be a linearly independent set of n vectors in a vector space spanned by S, which has $m < n$ vectors, impossible by Lemma 3.3.4.

(3) We already know this—any basis of V must have m elements. But from the point of view of (1) and (2), consider a set S of n elements that is a basis of V. From (1), we cannot have $n > m$, as then S would not be linearly independent, and from (2), we cannot have $n < m$, as then S would not span V, so we must have $n = m$.

(4) By definition, S is a basis means S is linearly independent and S spans V, so if (a) is true, then both (b) and (c) are true.

Suppose (b) is true. If S did not span V, then by Lemma 3.3.12 below we could add a vector v to S to obtain a linearly independent set of $m+1$ elements in V—impossible by (1). So (c) is true.

Suppose (c) is true. If S were not linearly independent, then by Lemma 3.3.12 below we could remove a vector from S to obtain a spanning set for V with $m-1$ elements—impossible by (2). So (b) is true.

So if either of (b) and (c) is true, then so is the other. But (b) and (c) together are just (a). □

Remark 3.3.10. In (theory and) practice, (4) is extremely useful. Suppose we have a vector space V that we know is m-dimensional and we have a set S of m vectors in V that we wish to show is a basis. A priori, this means we have to show both (b) and (c). But this theorem tells us we only have to show one of (b) and (c), and then the other is automatic. This sounds like we're cutting the amount of work in half, but it's often much better than that. Often one of (b) and (c) is relatively easy to show and the other is relatively hard, so we can just pick the easy one, show it is true, and then we're done. ◊

Theorem 3.3.11. *Let A be an n-by-n matrix. The following are equivalent*:

(a) *$Ax = b$ has a unique solution for every b in $\mathbb{F}^n$.*

(b) *$Ax = 0$ has only the trivial solution $x = 0$.*

(c) *$Ax = b$ has a solution for every b in $\mathbb{F}^n$.*

Proof. Recall we have several different interpretations of the product Ax. The theorem is stated in the context of the first interpretation (Observation 1.3.13) as representing a system of linear equations. But to prove it we shift to the second interpretation (Observation 1.3.14). In the context of this interpretation, write $A = [u_1|u_2|\dots|u_n]$. Let $S = \{u_1, \dots, u_n\}$, a set of n vectors in $\mathbb{F}^n$. If $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, then Ax is the linear combination $x_1u_1 + x_2u_2 + \cdots + x_nu_n$. Under this interpretation, (a), (b), and (c) become the conditions:

(a) Every vector in $\mathbb{F}^n$ can be written as a linear combination of the elements of S in a unique way.

(b) S is linearly independent.

(c) S spans $\mathbb{F}^n$.

But by Lemma 3.3.3, (a) is equivalent to the condition

(a) S is a basis of $\mathbb{F}^n$.

But then (a), (b), and (c) are equivalent by Theorem 3.3.9(4). □

In the following, if S is a set of vectors and v is a vector in S, $S - \{v\}$ denotes the set S with the vector v removed.

Lemma 3.3.12. (1) *Let S be a linearly independent set of vectors in V. Let v be a vector in V. Then $S \cup \{v\}$ is linearly independent if and only if v* is not *in* $\operatorname{Span}(S)$.

(2) *Let S be a set of vectors in V that spans V. Let v be a vector in S. Then $S - \{v\}$ spans V if and only if v* is *in* $\operatorname{Span}(S - \{v\})$.

Proof. We prove the contrapositive of each statement.

(1) Let $S = \{v_i\}$. If v is a linear combination of the vectors in S, then $v = \sum c_i v_i$ for some c_i, and then $(\sum c_i v_i) - v = 0$ is a linear dependence relation among the vectors in $S \cup \{v\}$. On the other hand, suppose we have a linear dependence relation $(\sum c_i v_i) + cv = 0$. We cannot have $c = 0$, as then we would have $\sum c_i v_i = 0$, and that would force all $c_i = 0$, as we are assuming S is linearly independent. But then $v = \sum(-c_i/c)v_i$ is a linear combination of the vectors in S.

(2) Let $S' = S - \{v\} = \{v_i\}$. If v is not a linear combination of the vectors in S', then we immediately see that S' does not span V. Suppose v is a linear combination of the vectors in S', say $v = \sum c_i v_i$. Let w be any vector in V. Then S spans V, so $w = (\sum d_i v_i) + dv$ for some d_i and some d. But then $w = \sum d_i v_i + d(\sum c_i v_i) = \sum(d_i + dc_i)v_i$ so S' spans V. □

This gives two other ways of looking at bases.

Corollary 3.3.13. *Let $\mathcal{B}$ be a set of vectors in a vector space V. The following are equivalent*:

(1) *$\mathcal{B}$ is a basis, i.e., $\mathcal{B}$ is linearly independent and spans V.*
(2) *$\mathcal{B}$ is a maximal linearly independent set, i.e., $\mathcal{B}$ is linearly independent but for any vector v in V, $\mathcal{B} \cup \{v\}$ is linearly dependent.*
(3) *$\mathcal{B}$ is a minimal spanning set for V, i.e., $\mathcal{B}$ spans V but for any vector $v \in \mathcal{B}$, $\mathcal{B} - \{v\}$ does not span V. (Here $\mathcal{B} - \{v\}$ denotes $\mathcal{B}$ with the vector v removed.)*

Proof. First suppose $\mathcal{B}$ is a basis. Since $\mathcal{B}$ spans V, every vector v in V is a linear combination of vectors in $\mathcal{B}$, so $\mathcal{B} \cup \{v\}$ is linearly dependent by Lemma 3.3.12. Also, $\mathcal{B}$ is linearly independent, so no vector v in $\mathcal{B}$ is a linear combination of the vectors in $\mathcal{B} - \{v\}$ (Lemma 3.2.5), so $\mathcal{B} - \{v\}$ does not span V by Lemma 3.3.12.

Now suppose $\mathcal{B}$ is a maximal linearly independent set. Then $\mathcal{B}$ is linearly independent. Also, for any vector v in V, $\mathcal{B} \cup \{v\}$ is linearly dependent, and so v is a linear combination of the vectors in $\mathcal{B}$, and so $\mathcal{B}$ spans V.

Now suppose $\mathcal{B}$ is a minimal spanning set for V. Then $\mathcal{B}$ spans V. Also, for any vector v in V, $\mathcal{B} - \{v\}$ does not span V, and so by Lemma 3.3.12, v is not a linear combination of the vectors in $\mathcal{B} - \{v\}$. Thus no vector in v is a linear combination of the other vectors in V, and so $\mathcal{B}$ is linearly independent (Lemma 3.2.5). □

Remark 3.3.14. Observe that Lemma 3.3.12 holds whether or not S is finite, and hence Corollary 3.3.13 holds whether or not $\mathcal{B}$ is finite. ◊

By definition, every finite-dimensional vector space has a (finite) basis.

Let us now prove a result which will give us a procedure for constructing a basis. In fact, it will give us two procedures.

Lemma 3.3.15. *Let V be a finite-dimensional vector space. Let R be a linearly independent set of elements in V, and let T be a set that spans V, with $R \subseteq T$. Then V has a basis S with $R \subseteq S \subseteq T$.*

First proof. Suppose V has dimension n. Then R necessarily has m elements with $m \leq n$ (and T has at least n, though possibly infinitely many, elements). We proceed as follows. We begin with $S_m = R$. Note S_m is linearly independent, by hypothesis. Now suppose we have S_k linearly independent. If every vector in T were a linear combination of the vectors in S_k, then S_k would span V. (Every vector in V can be expressed as a linear combination of the vectors in T, and then by substitution, as a linear combination of the vectors in S_k.) In that case, S_k would be linearly independent and would span V, so would be a basis of V, and we are done. Otherwise, choose any vector v in T that is not a linear combination of the vectors in S_k. Then by Lemma 3.3.12, $S_{k+1} = S_k \cup \{v\}$ is linearly independent, and $S_{k+1} \subseteq T$. Keep going. Note we have to stop (exactly) when we get to S_n because we cannot have a linearly independent set of more than n elements in a vector space of dimension n. □

Second proof. Suppose T has a finite number n of elements (in which case V is necessarily n'-dimensional for some $n' \leq n$). We proceed as follows. We begin with $S_n = T$. Note S_n spans V, by hypothesis. Now suppose we have S_k spanning V. If S_k were linearly independent, then S_k would be a basis of V, and we would be done. Otherwise there is some vector v in S_k that is a linear combination of the other vectors in S_k. In fact, we claim that there is such a vector that is not in R. To see this, consider a linear dependence relation $\sum c_i v_i$ among the vectors in S_k. This cannot just involve the vectors in R, as R is linearly independent, so there must be some vector in S_k, not in R, with a nonzero coefficient. Let $S_{k-1} = S_k - \{v\}$. Keep going. We have to stop at some point because we started with only a finite number n of vectors in T. So for some $n' \leq n$, $S_{n'}$ is a basis of V (and V has dimension n', as we already remarked). □

Remark 3.3.16. Note that the first procedure always works, but the second procedure only works if we started with a finite set T. ◊

Corollary 3.3.17. *Let V be a finite-dimensional vector space.*

(1) *If R is any linearly independent subset of V, then V has a basis S with $R \subseteq S$.*

(2) *If T is any subset of V that spans V, then V has a basis S with $S \subseteq T$.*

Proof. For (1), we can take $T = V$ in Lemma 3.3.15. For (2), we can take $R = \varnothing$, the empty set, in Lemma 3.3.15. □

Remark 3.3.18. Note that this lemma gives us a procedure for constructing a basis of a finite-dimensional vector space V. Suppose we know nothing about V. We can start with $R = \varnothing$, the empty set, and so $S_0 = \varnothing$ as well. Then we add vectors v_1, v_2, v_3 to S_0, one at a time, so $S_1 = \{v_1\}$, $S_2 = \{v_1, v_2\}$, $S_3 = \{v_1, v_2, v_3\}$, making sure that v_{k+1} is not a linear combination of the vectors in S_k, until we have to stop. And when we do, we have arrived at a basis. But this procedure also allows us to use information about V that we already know. Namely, suppose we know that some set R of vectors in V is linearly independent. Then we can start with R, add vectors one at a time, making sure we preserve linear independence at each step, until we have to stop. And when we do, we have again arrived at a basis. On the other hand, suppose we know that some finite set of vectors T spans V. Then we can throw out vectors one at a time, making sure we preserve the property of spanning V at each step, until we have to stop. And when we do, we have once again arrived at a basis. And if we know that we have a pair of sets $R \subseteq T$ with R

linearly independent and T spanning V, then we can find a basis S "between" R and T in the sense that $R \subseteq S \subseteq T$.

$\Diamond$

Let us look at some more examples of vector spaces, bases, and dimensions.

Example 3.3.19. We have already seen that the vector space $V = P_d(\mathbb{F})$ has basis $\{x^0, x^1, \ldots, x^d\}$ (where for convenience we set $x^0 = 1$) and so has dimension $d+1$. Let us look at some other bases.

(1) Let $p_i(x)$ be any polynomial of degree i. We claim $\mathcal{B} = \{p_0(x), \ldots, p_d(x)\}$ is a basis for V. (Of course, this set also has $d+1$ elements.) We leave the verification of this to the reader.

Here are some particularly useful special cases of this result.

(a) For any fixed a, $\mathcal{B} = \{1, x-a, (x-a)^2, \ldots, (x-a)^d\}$ is a basis of $P_d(\mathbb{F})$.

(b) Define $x^{(n)}$ by

$$x^{(n)} = x(x-1)\cdots(x-(n-1))$$

so that the first few of these are

$$x^{(0)} = 1, \quad x^{(1)} = x, \quad x^{(2)} = x(x-1), \quad x^{(3)} = x(x-1)(x-2), \ \ldots.$$

Then $\mathcal{B} = \{x^{(0)}, x^{(1)}, \ldots, x^{(d)}\}$ is a basis of $P_d(\mathbb{F})$.

Similarly, $\mathcal{B} = \{(x-1)^{(0)}, x^{(1)}, (x+1)^{(2)}, (x+2)^{(3)}, \ldots, (x+(d-1))^{(d)}\} = \{1, x, x(x+1), x(x+1)(x+2), \ldots\}$ is a basis of $P_d(\mathbb{F})$. $\Diamond$

Example 3.3.20. (1) Let $X = \{x_1, x_2, \ldots, x_k\}$ be a set of k elements, k a positive integer. We have seen that $V = \{f \colon X \to \mathbb{F}\}$ is a vector space.

Let $f_i \colon X \to \mathbb{F}$ be the function given by

$$f_i(x_i) = 1, \quad f_i(x_j) = 0 \quad \text{for } j \neq i.$$

Then $\mathcal{B} = \{f_1(x), f_2(x), \ldots, f_k(x)\}$ is a basis for V, and so V is k-dimensional.

(2) Let X be an infinite set and let $V = \{f \colon X \to \mathbb{F}\}$. Then V is infinite dimensional. $\Diamond$

We are going to concentrate on the case of finite-dimensional vector spaces. This is really the foundation of the subject (and hence what we should be focusing on in an introduction). It is the part of the subject most closely related to matrices. For many areas of mathematics and its applications it is the most important part. But it is not the only part, and for some areas of mathematics it is essential to study arbitrary vector spaces. In particular, this is true for developing calculus and analysis.

Thus we do want to make some remarks about the infinite-dimensional case. Let us begin with a pair of illustrative examples.

Example 3.3.21. Consider the vector space $V = \mathbb{F}^\infty$. Recall

$$\mathbb{F}^\infty = \left\{ \begin{bmatrix} a_1 \\ a_2 \\ \vdots \end{bmatrix} \right\} \quad \text{with only finitely many } a_i \neq 0.$$

Let e_i be the vector in $\mathbb{F}^\infty$ with a 1 in position i and 0 elsewhere, and let $\mathcal{E} = \{e_1, e_2, e_3, \ldots\}$. It is easy to check that $\mathcal{E}$ is linearly independent: the equation

$$c_1e_1 + \cdots + c_ne_n = 0$$

(remember that any linear combination is finite!) is the equation

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \\ 0 \\ \vdots \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \end{bmatrix}$$

which implies that each $c_i = 0$. It is also easy to check that $\mathcal{E}$ spans $\mathbb{F}^\infty$: an element of $\mathbb{F}^\infty$ is of the form

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \\ 0 \\ \vdots \end{bmatrix}$$

as, by the definition of $\mathbb{F}^\infty$, only finitely many entries can be nonzero, and this element is equal to $a_1e_1 + a_2e_2 + \cdots + a_ne_n$ (again, a linear combination is a finite sum!). Thus $\mathcal{E}$ is a basis of $\mathbb{F}^\infty$.

Now $\mathcal{E}$ evidently has infinitely many elements, so it is natural to set $\dim \mathbb{F}^\infty = \infty$. $\Diamond$

Example 3.3.22. Consider the vector space $V = \mathbb{F}^{\infty\infty}$. Recall

$$\mathbb{F}^{\infty\infty} = \left\{ \begin{bmatrix} a_1 \\ a_2 \\ \vdots \end{bmatrix} \right\}.$$

If $\mathbb{E}$ is the set of Example 3.3.21, then exactly the same proof shows that $\mathcal{E}$ is linearly independent, but (again remembering that a linear combination is a finite sum!) $\mathcal{E}$ does not span $\mathbb{F}^{\infty\infty}$, as any linear combination of the vectors in $\mathcal{E}$ has only finitely many nonzero entries. In fact, it is impossible to constructively write down a basis for V. $\Diamond$

In light of these examples, we ask: does every vector space have a basis?

This is actually a subtle logical point. Mathematics is a finite process. It is no problem to find a basis in case V is finite dimensional, as then we're making finitely many choices. But if not, we need to make infinitely many choices all at once. (I am deliberately being very vague here.) There is an axiom, the famous Axiom of Choice, that applies to situations in which we want to do this. We accept this axiom, which has the following consequence (in fact, this consequence is equivalent to it):

Axiom 3.3.23. *Every vector space has a basis.*

Given this axiom, we restate the definition of a basis.

Definition 3.3.24. Let V be a vector space. The *dimension* of V, $\dim V$, is equal to the number of elements in a basis of V, which may be $0, 1, 2, \ldots$ or ∞. $\Diamond$

Techniques for dealing with infinite sets are subtle, so we are not going to prove the following result in general (though we proved it in the finite-dimensional case in Lemma 3.3.15 and Corollary 3.3.17). We simply state it here for your future reference.

Theorem 3.3.25. *Let V be a vector space. Let R be a linearly independent set of elements in V, and let T be a set that spans V, with $R \subseteq T$. Then V has a basis S with $R \subseteq S \subseteq T$.*

In particular: if R is a linearly independent set of elements in V, then V has a basis S with $R \subseteq S$, and if T is a set of elements that spans V, then V has a basis S with $S \subseteq T$.

3.4. Subspaces

In this section we introduce the notion of a subspace. We then carefully study subspaces and related matters.

Definition 3.4.1. Let V be a vector space. Then W is a *subspace* of V if $W \subseteq V$ (i.e., W is a subset of V) and W is a vector space with the same operations of vector addition and scalar multiplication as in V. $\Diamond$

Let us see some examples.

Example 3.4.2. (a) Let V be any vector space. Then V itself is a subspace of V. Also, $\{0\}$ is a subspace of V.

(b) For any d, $P_d(\mathbb{F})$ is a subspace of $P(\mathbb{F})$. Also, for any $d_0 \leq d_1$, $P_{d_0}(\mathbb{F})$ is a subspace of $P_{d_1}(\mathbb{F})$.

(c) $\mathbb{F}^\infty$ is a subspace of $\mathbb{F}^{\infty\infty}$.

(d) Let m and n be positive integers with $n < m$. Then $\mathbb{F}^n$ is *not* a subspace of $\mathbb{F}^m$ ($\mathbb{F}^m$ consists of vectors with m entries, $\mathbb{F}^n$ consists of vectors with n entries, and these are distinct sets of objects). However

$$\left\{ \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right\}, \quad a_1, \ldots, a_n \text{ elements of } \mathbb{F},$$

is a subset of $\mathbb{F}^m$.

(e) Let X be a set. Then, as we have seen in Example 3.1.7(a),

$$V = \{f \colon X \to \mathbb{F}\}$$

is an $\mathbb{F}$-vector space. Now let $x_1 \in X$ be any fixed element of X. Then

$$W = \{f \in V \mid f(x_1) = 0\}$$

is a subspace of V. Similarly, for any fixed elements $x_1, \ldots, x_k \in X$,

$$W = \{f \in V \mid f(x_1) = f(x_2) = \cdots = f(x_k) = 0\}$$

is a subspace of V. ◊

A priori, in order to show that a subset W of V is a subspace we have to show that it satisfies all 10 properties of Definition 3.1.1. But in fact the situation is easier.

Lemma 3.4.3. *Let W be a subset of V. Then W is a subspace of V if and only if W satisfies either of the following equivalent sets of conditions*:

(4) $0 \in W$.

(1) *If $w_1, w_2 \in W$, then $w_1 + w_2 \in W$.*

(6) *If $c \in \mathbb{F}$ and $w \in W$, then $cw \in W$.*

Or

(4′) *W is nonempty.*

(1) *If $w_1, w_2 \in W$, then $w_1 + w_2 \in W$.*

(6) *If $c \in \mathbb{F}$ and $w \in W$, then $cw \in W$.*

Proof. Let us first concentrate on the first set of conditions.

We need to show that W satisfies conditions (1)–(10) of Definition 3.1.1. By hypothesis, W satisfies conditions (4), (1), and (6), so we have to check the other conditions. First, condition (5). Let w be any element of W. By condition (5) for V, we know there is an element $-w$ of V with $w + (-w) = (-w) + w = 0$. We must show that condition (5) holds for W, so we must show that in fact $-w \in W$. But by property (13) (Theorem 3.1.9), $-w = (-1)w$, and then by property (6), $-w = (-1)w$ is an element of W.

Now all the other conditions hold for all vectors in V, so they certainly hold for all vectors in W.

Now for the second set of conditions. To show these are equivalent to the first set, we show that any W satisfying either set of conditions satisfies the other.

On the one hand, suppose W satisfies (4), (1), and (6). Since $0 \in W$, W is nonempty, so W satisfies (4′), (1), and (6).

On the other hand, suppose W satisfies (4′), (1), and (6). Since W is nonempty, there is some vector $w_0 \in W$. Then by (6), $(-1)w_0 \in W$. Then by (4), $w_0 + (-1)w_0 \in W$. But we know $w_0 + (-1)w_0 = 0$, so $0 \in W$, and hence W satisfies (4), (1), and (6). □

Using this lemma it is easy to check that the subspaces given in Example 3.4.2 are indeed subspaces, as claimed.

We can now easily see that a set we introduced earlier is always a subspace.

Corollary 3.4.4. *Let V be a vector space, and let S be a set of vectors in V. Then* $\mathrm{Span}(S)$ *is a subspace of V.*

Proof. We simply check properties (4), (1), and (6).

Let $S = \{v_1, v_2, \ldots\}$.

(4) $0 = \sum 0v_i$ is a linear combination (in fact, the trivial linear combination) of the vectors in S.

(1) If $v = \sum c_i v_i$ and $w = \sum d_i v_i$ are in S, then $v + w = \sum (c_i + d_i) v_i$ is in S.

(6) If $v = \sum c_i v_i$ is in S, then $cv = \sum (cc_i) v_i$ is in S. □

Now of course a subspace W of a vector space V is itself a vector space, so it has a dimension.

Lemma 3.4.5. (1) *Let W be a subspace of V. Then* $\dim(W) \leq \dim(V)$.

(2) *If V is finite dimensional, then $W = V$ if and only if* $\dim(W) = \dim(V)$.

Proof. We leave this as an exercise for the reader. □

Now suppose we have a set S of vectors in $\mathbb{F}^m$. As we saw in Corollary 3.4.4, $W = \mathrm{Span}(S)$ is a subspace of $\mathbb{F}^m$. So we ask for the dimension of W, or, more precisely, for a basis of W.

We shall see two methods to find it.

Lemma 3.4.6. *Let $S = \{v_1, \ldots, v_n\}$ be a set of n vectors in $\mathbb{F}^m$. Form the matrix $A = [v_1 | \ldots | v_n]$. Let A' be any weak row-echelon form of A and let the leading entries of A' be in columns $j_1, \ldots, j_k$. Then* $\mathrm{Span}(S)$ *has a basis $\mathcal{B} = \{v_{j_1}, \ldots, v_{j_k}\}$ and in particular* $\mathrm{Span}(S)$ *has dimension k.*

Proof. As usual, we must show that $\mathcal{B}$ is linearly independent and spans $W = \mathrm{Span}(S)$.

As we have observed, if $\tilde{A}$ is the reduced row-echelon form of A, then the leading entries of $\tilde{A}$ are in the *same* columns $j_1, \ldots, j_k$.

First we shall show that $\mathcal{B}$ spans W. Thus suppose we have any vector v in $\mathrm{Span}(W)$. Then by definition $v = d_1 v_1 + \cdots + d_n v_n$ for some $d_1, \ldots, d_n$. That is, the equation $Ax = v$ has a solution (as we recall that Ax is a linear combination of the columns of A). But then we saw in Lemma 2.5.1 that in fact it has a solution of the form $x_{j_1} = c_{j_1}, \ldots, x_{j_k} = c_{j_k}$, and $x_j = c_j = 0$ for every other value of j. Hence, omitting the vectors whose coefficients are 0 from the linear combination, we see that $v = c_{j_1} v_{j_1} + \cdots + c_{j_k} v_{j_k}$, and so $\mathcal{B}$ spans W.

Now we show $\mathcal{B}$ is linearly independent. Suppose we have a linear dependence relation $c_{j_1} v_{j_1} + \cdots + c_{j_k} v_{j_k} = 0$. Then putting in the vectors whose coefficients are 0, we see that $0 = d_1 v_1 + \cdots + d_n v_n = Ax$ with the value of every free variable $= 0$. But we saw in Lemma 2.5.2 that this forces the values of all the variables to be 0, and so $c_{j_1} = \cdots = c_{j_k} = 0$. Thus $\mathcal{B}$ is linearly independent. □

Remark 3.4.7. Note that $\mathcal{B}$ is a subset of our *original* set S of vectors (we are taking the respective columns of our original matrix A, not of A' or $\tilde{A}$) and so this is an example of "cutting down" a spanning set to a basis. $\Diamond$

We thought about starting with the set S and forming the matrix A. But instead we could have started with the matrix A and obtained the set S by taking the columns of A. This is an important thing to do, and we give it a name.

Definition 3.4.8. Let A be an m-by-n matrix. The subspace of $\mathbb{F}^m$ spanned by the columns of A is the *column space* of A, $\mathrm{Col}(A)$. $\Diamond$

Thus we see, in this language:

Corollary 3.4.9. *Applying the procedure of Lemma* 3.4.6 *to matrix A gives a basis for, and the dimension of,* $\mathrm{Col}(A)$.

Proof. If $A = [v_1|\dots|v_n]$, then $S = \{v_1, \dots, v_n\}$ in Lemma 3.4.6. $\square$

Example 3.4.10. Find a basis for the subspace W of $\mathbb{F}^4$ spanned by

$$\left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 7 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 5 \\ 4 \\ -1 \\ 7 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 4 \\ 6 \end{bmatrix} \right\}.$$

The matrix

$$A = \begin{bmatrix} 1 & 4 & -1 & 5 & 0 \\ 2 & 1 & 0 & 4 & 1 \\ 3 & -2 & 1 & -1 & 4 \\ 7 & 0 & 1 & 7 & 6 \end{bmatrix} \qquad \text{reduces to} \qquad A' = \begin{bmatrix} 1 & 4 & -1 & 5 & 0 \\ 0 & -7 & 2 & -6 & 1 \\ 0 & 0 & 0 & -4 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

which is in weak row-echelon form. We see that there are three leading entries, so $\dim(W) = 3$. These are in columns 1, 2, and 4, so W has basis

$$\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 7 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} 5 \\ 4 \\ -1 \\ 7 \end{bmatrix} \right\}.$$

As well, W is the column space $\mathrm{Col}(A)$ of the matrix A and $\mathcal{B}$ is a basis for $\mathrm{Col}(A)$. $\Diamond$

Instead, suppose we have a set S of vectors in ${}^t\mathbb{F}^n$. We will use a different method to find a basis $\mathcal{B}$ for $W = \mathrm{Span}(S)$. Observe that with this method, the basis we find will almost never be a subset of our original spanning set S.

Lemma 3.4.11. *Let $S = \{v_1, \dots, v_m\}$ be a set of vectors in ${}^t\mathbb{F}^n$. Form the matrix A whose rows are $v_1, \dots, v_m$. Let A' be any weak row-echelon form of A. Then the nonzero rows of A' form a basis for* $\mathrm{Span}(S)$, *and in particular, if A' has k nonzero rows, the dimension of* $\mathrm{Span}(S)$ *is k.*

Proof. Write $A = \begin{bmatrix} v_1 \\ \hline \vdots \\ \hline v_m \end{bmatrix}$. Now Span$(S)$ is the subspace of ${}^t\mathbb{F}^n$ spanned by the rows of A. We now apply a sequence of elementary row operations to reduce A to A'. By Lemma 3.2.16, each elementary row operation leaves Span(S) unchanged. Thus $W = \operatorname{Span}(S)$ is also spanned by $S' = \{w_1, \ldots, w_m\}$, where $A' = \begin{bmatrix} w_1 \\ \hline \vdots \\ \hline w_m \end{bmatrix}$, i.e., where S' is the set of rows of A', i.e.,

$$\operatorname{Span}(S) = \left\{ \sum_{i=1}^{m} c_i w_i \right\}.$$

But if $w_1, \ldots, w_k$ are the nonzero rows of A', so that $w_{k+1}, \ldots, w_m$ are all zero, then $\sum_{i=1}^{m} c_i w_i = c_1 w_1 + \cdots + c_k w_k + c_{k+1} w_{k+1} + \cdots + c_m w_m = c_1 w_1 + \cdots + c_k w_k = \sum_{i=1}^{k} c_i w_i$. Thus

$$\operatorname{Span}(S) = \left\{ \sum_{i=1}^{k} c_i w_i \right\},$$

and so we have shown that if $\mathcal{B} = \{w_1, \ldots, w_k\}$, then $\mathcal{B}$ spans W. To show that $\mathcal{B}$ is a basis, we have to show that $\mathcal{B}$ is linearly independent, but that is given to us by Lemma 3.2.9. □

Again, we thought about starting with the set S and forming the matrix A. But instead we could have started with the matrix A and obtained the set S by taking the rows of A. Again, this is an important thing to do, and we give it a name.

Definition 3.4.12. Let A be an m-by-n matrix. Then the subspace of ${}^t\mathbb{F}^n$ spanned by the rows of A is the *row space* of A, Row(A). ◊

Thus we see, in this language:

Corollary 3.4.13. *Applying the procedure of Lemma* 3.4.11 *to the matrix A gives a basis for, and the dimension of,* Row(A).

Proof. If $A = \begin{bmatrix} v_1 \\ \hline \vdots \\ \hline v_m \end{bmatrix}$, then $S = \{v_1, \ldots, v_m\}$ in Lemma 3.4.11. □

Example 3.4.14. Find a basis for the subspace W of ${}^t\mathbb{F}^6$ spanned by

$$S = \left\{ \begin{bmatrix}1 & 2 & 1 & 3 & 6 & -1\end{bmatrix}, \begin{bmatrix}2 & 4 & 5 & 4 & 7 & -3\end{bmatrix}, \begin{bmatrix}0 & 0 & -6 & 4 & 9 & 3\end{bmatrix}, \begin{bmatrix}3 & 6 & 6 & 7 & 9 & 0\end{bmatrix} \right\}.$$

The matrix

$$A = \begin{bmatrix} 1 & 2 & 1 & 3 & 6 & -1 \\ 2 & 4 & 5 & 4 & 7 & -3 \\ 0 & 0 & -6 & 4 & 9 & 3 \\ 3 & 6 & 6 & 7 & 9 & 0 \end{bmatrix} \qquad \text{reduces to} \qquad A' = \begin{bmatrix} 1 & 2 & 1 & 3 & 6 & -1 \\ 0 & 0 & 3 & -2 & -5 & -1 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

which is in weak row-echelon form. We see there are three nonzero rows, so $\dim(W) = 3$. These rows are a basis of W, i.e., W has basis

$$\mathcal{B} = \left\{ \begin{bmatrix} 1 & 2 & 1 & 3 & 6 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 3 & -2 & -5 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 & -1 & 1 \end{bmatrix} \right\}.$$

As well, W is the row space $\operatorname{Row}(A)$ of the matrix A and $\mathcal{B}$ is a basis for $\operatorname{Row}(A)$. $\Diamond$

We now make a standard definition.

Definition 3.4.15. Let A be a matrix. The *row rank* of A is the dimension of the row space $\operatorname{Row}(A)$. The *column rank* of A is the dimension of the column space $\operatorname{Col}(A)$. $\Diamond$

Corollary 3.4.16. *For any matrix A, the row rank of A and the column rank of A are equal.*

Proof. Immediate from Corollary 3.4.9 and Corollary 3.4.13. $\square$

We call this common number the *rank* of A.

Remark 3.4.17. While they have the same dimension, the row space $\operatorname{Row}(A)$ and the column space $\operatorname{Col}(A)$ are completely different vector spaces and are *completely unrelated*. In fact, for *any* two subspaces, a subspace W_c of $\mathbb{F}^m$ and a subspace W_r of ${}^t\mathbb{F}^n$, with $\dim W_c = \dim W_r$, there is an m-by-n matrix A whose column space is W_c and whose row space is W_r. $\Diamond$

We now present an alternate method for finding a basis for $\operatorname{Span}(S)$, where S is a set of vectors in $\mathbb{F}^n$. To rigorously justify it we would have to involve some concepts we won't develop until the next chapter ("transpose gives an isomorphism between $\mathbb{F}^n$ and ${}^t\mathbb{F}^n$") but this method belongs here, and is so useful that we present it now. It is a method of using row operations to find a basis for $\operatorname{Span}(S)$ in this case.

The method is: we write the vectors in $\mathbb{F}^n$ in rows, rather then columns. We use the method of Lemma 3.4.11 to find a basis, and then we take those vectors in ${}^t\mathbb{F}^n$ and write them in columns.

(We could avoid this by introducing column operations, but row operations are more familiar—to everyone—and so we stick with them.)

Example 3.4.18. Let S be the set of vectors in $\mathbb{F}^4$ of Example 3.4.10,

$$S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 7 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 5 \\ 4 \\ -1 \\ 7 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 4 \\ 6 \end{bmatrix} \right\}.$$

We wish to find a basis for the subspace W of $\mathbb{F}^4$ spanned by S.

The matrix

$$A = \begin{bmatrix} 1 & 2 & 3 & 7 \\ 4 & 1 & -2 & 0 \\ -1 & 0 & 1 & 1 \\ 5 & 4 & -1 & 7 \\ 0 & 1 & 4 & 6 \end{bmatrix} \qquad \text{reduces to} \qquad A' = \begin{bmatrix} 1 & 2 & 3 & 7 \\ 0 & 1 & 4 & 6 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

which is in weak row-echelon form, and so we obtain the basis

$$B = \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 7 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 4 \\ 6 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \right\}$$

for W. And we see that $\dim(W) = 3$, agreeing (of course) with our previous calculation. $\Diamond$

Now let us see how to get new subspaces from old. There are several ways.

Lemma 3.4.19. *Let W_1 and W_2 be subspaces of the vector space V. Then $W_1 \cap W_2$ is a subspace of V.*

Proof. As usual, we verify the criteria in Lemma 3.4.3:

(4) Since $0 \in W_1$ and $0 \in W_2$, $0 \in W_1 \cap W_2$.

(1) If $w, w' \in W_1 \cap W_2$, then $w, w' \in W_1$, so $w + w' \in W_1$, and $w, w' \in W_2$, so $w + w' \in W_2$, and so $w + w' \in W_1 \cap W_2$.

(6) If $w \in W_1 \cap W_2$ and $c \in \mathbb{F}$, then $w \in W_1$, so $cw \in W_1$, and $w \in W_2$, so $cw \in W_2$, and so $cw \in W_1 \cap W_2$. $\square$

On other hand, unless $W_1 \subseteq W_2$ or $W_2 \subseteq W_1$, it is *never* the case that $W_1 \cup W_2$ is a subspace. So we have to proceed differently.

Lemma 3.4.20. *Let W_1 and W_2 be subspaces of the vector space V. Then $W_1 + W_2 = \{w_1 + w_2 \,|\, w_1 \text{ in } W_1,\ w_2 \text{ in } W_2\}$ is a subspace of V.*

Proof. Again we verify the criteria in Lemma 3.4.3:

(4) Since $0 \in W_1$, $0 \in W_2$, $0 = 0 + 0 \in W_1 + W_2$.

(1) If $w_1 + w_2 \in W_1 + W_2$ and $w_1' + w_2' \in W_1 + W_2$, then $(w_1 + w_2) + (w_1' + w_2') = (w_1 + w_1') + (w_2 + w_2') \in W_1 + W_2$.

(6) If $w_1 + w_2 \in W_1 + W_2$ and $c \in \mathbb{F}$, then $c(w_1 + w_2) = (cw_1) + (cw_2) \in W_1 + W_2$. $\square$

Let us look at a very important special case of these constructions.

Definition 3.4.21. Let V be a vector space. Suppose that U and W are two subspaces of V such that:

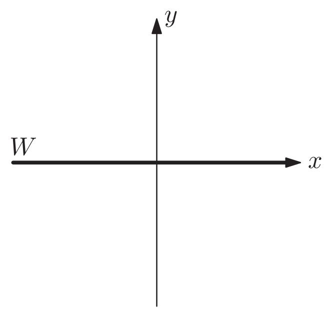
(1) $U \cap W = \{0\}$; and

(2) $U + W = V$.

Then V is the *direct sum* $V = U \oplus W$ of the subspaces U and W, and U and W are *complementary* subspaces of V, or, alternatively, each of U and W is a *complement* of the other. $\Diamond$

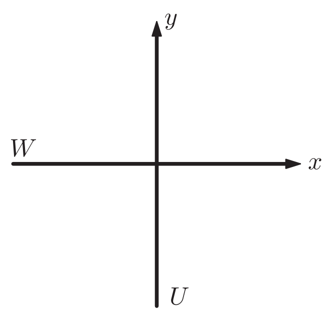
Remark 3.4.22. Before proceeding with our analysis, let us look at a picture to give us some geometric intuition. We will go back to $\mathbb{R}^2$, and we will identify a vector $\begin{bmatrix} x \\ y \end{bmatrix}$ with its endpoint (x, y).

Then $W = \left\{ \begin{bmatrix} x \\ 0 \end{bmatrix} \right\}$ is a subspace of $V = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \right\}$, and we see the picture:



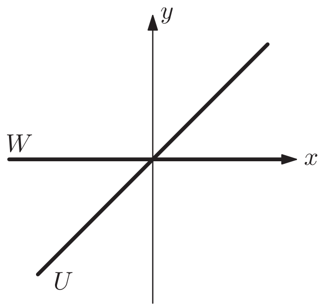
Here W is the x-axis.

Now you might think we should take $U = \left\{ \begin{bmatrix} 0 \\ y \end{bmatrix} \right\}$ as the complement of W. Certainly $U \cap W = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, and any $\begin{bmatrix} x \\ y \end{bmatrix}$ can be written as $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ y \end{bmatrix}$. Then we see the picture:



You would be correct that U is a complement of W.

But we could have made a different choice. We could choose $U = \left\{ \begin{bmatrix} y \\ y \end{bmatrix} \right\}$. Then $U \cap W = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, and any $\begin{bmatrix} x \\ y \end{bmatrix}$ can be written as $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x - y \\ 0 \end{bmatrix} + \begin{bmatrix} y \\ y \end{bmatrix}$. Then we see the picture:



Here U is a complement as well.

In fact, we could have, in this case, chosen U to be *any* line through the origin, except for the x-axis, and U would be a complement of W.

The point we want to make here is that we have lots of choices, and all are *equally good*. That is why we were careful to call U *a* complement of W rather than *the* complement. There are lots of complements, and no one is better than any other. $\Diamond$

Let us see an alternate characterization of direct sums.

Lemma 3.4.23. *Let U and W be subspaces of V. Then $V = U \oplus W$, and consequently U and W are complementary subspaces of V, if and only if every vector v in V can be written uniquely as $v = u + w$ for some vector u in U and some vector w in W.*

Proof. First suppose $V = U \oplus W$. Then in particular $V = U + W$, so every vector v in V can be written as $v = u + w$ for some vector u in U and some vector w in W. We have to show that there is only one way to do this. So suppose $v = u + w = u' + w'$ with u' in U and w' in W. Then $u - u' = w' - w$. Call this common value x. Then $x = u - u'$ so x is in U, and $x = w' - w$ so x is in W. Thus x is in $U \cap W$. But $U \cap W = \{0\}$, so $x = 0$. But then $u' = u$ and $w' = w$.

On the other hand, suppose every vector v in V can be written uniquely in the form $v = u + w$ for some u in U and w in W.

Then in particular every vector in V can be written in this form, so $V = U+W$. We must show $U \cap W = \{0\}$. So let $x \in U \cap W$. In particular, $x \in U$ and $x \in W$. Thus we can write $x = x + 0$ and $x = 0 + x$. If x were not 0, this would give us two distinct ways of writing $x = u + w$ with u in U and w in W, which is impossible. Hence x must be 0, and so $U \cap W = \{0\}$. $\square$

Now we would like to see every subspace of V indeed *has* a complement. This is a consequence of work we have already done. In fact, we will see something more precise.

Theorem 3.4.24. (1) *Let W and U be subspaces of V. Let $\mathcal{B}_1$ be a basis of W, and let $\mathcal{B}_2$ be a basis of U. If $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ is a basis of V, then $V = W \oplus U$ and so U is a complement of W (and W is a complement of U).*

(2) *Suppose that* $V = W \oplus U$. *Then for any bases* $\mathcal{B}_1'$ *of* W *and* $\mathcal{B}_2'$ *of* U, $\mathcal{B}' = \mathcal{B}_1' \cup \mathcal{B}_2'$ *is a basis of* V.

(3) *Every subspace* W *of* V *has a complement* U. *Furthermore, all complements of* W *have the same dimension.*

One way we often apply this theorem is as follows. Suppose we have a basis $\mathcal{B}$ of V, and we decompose this as a disjoint union, $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$. Then if $W = \operatorname{Span}(\mathcal{B}_1)$ and $U = \operatorname{Span}(\mathcal{B}_2)$, $V = W \oplus U$. Furthermore, if we "replace" $\mathcal{B}_1$ by $\mathcal{B}_1'$, any other basis of W, and we "replace" $\mathcal{B}_2$ by $\mathcal{B}_2'$, any other basis of U, then we may "replace" $\mathcal{B}$ by $\mathcal{B}'$ and $\mathcal{B}'$ will also be a basis of V.

Proof. (1) Let $\mathcal{B}_1 = \{w_1, w_2, \dots\}$ and $\mathcal{B}_2 = \{u_1, u_2, \dots\}$. Suppose $\mathcal{B}$ is a basis of V. Then $\mathcal{B}$ spans V, so we may write every $v \in V$ as $v = \sum c_i w_i + \sum d_j u_j$. Set $w = \sum c_i w_i$ and $u = \sum d_j u_j$. Then $w \in W$, $u \in U$, and $v = w + u$, so $V = W + U$. Now suppose $v = W \cap U$. Then $v = \sum c_i w_i$ for some c_i, and also $v = \sum d_j u_j$ for some d_j. Then $0 = v - v = \sum c_i w_i + \sum (-d_j) u_j$. But $\mathcal{B}$ is linearly independent, so $c_i = 0$ for every i (and $d_j = 0$ for every j) so $v = 0$. Thus $V = W \oplus U$.

(2) This is just about the same argument, in reverse. Suppose $V = W \oplus U$ and let $\mathcal{B}_1' = \{w_1', w_2', \dots\}$ and $\mathcal{B}_2' = \{u_1', u_2', \dots\}$ be bases of W and U. Then $V = W + U$, so any $v \in V$ can be written as $v = w + u$ with $w \in W$ and $u \in U$. But $\mathcal{B}_1'$ spans W, so $w = \sum c_i w_i'$, and $\mathcal{B}_2'$ spans U, so $u = \sum d_j u_j'$, so $v = \sum c_i w_i' + \sum d_j u_j'$ and $\mathcal{B}'$ spans V. If $0 = \sum c_i w_i' + \sum d_j u_j'$, then $\sum c_i w_i' = \sum (-d_j) u_j' = v$, say. But then $v \in W$ and also $v \in U$, and, since $W \cap U = \{0\}$, we have that $v = 0$. But $\mathcal{B}_1'$ is linearly independent, so each $c_i = 0$, and $\mathcal{B}_2'$ is linearly independent, so each $d_j' = 0$. Hence $\mathcal{B}'$ is linearly independent, and so $\mathcal{B}'$ is a basis of V.

(3) W is a vector space, so it has a basis $\mathcal{B}_1$. Extend $\mathcal{B}_1$ to a basis $\mathcal{B}$ of V, and write $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$. Then $U = \operatorname{Span}(\mathcal{B}_2)$ is a complement of W.

Now we wish to show that all complements of W have the same dimension.

Suppose that V has finite dimension n. Then this is easy: let W have dimension m. Then any basis of V has n elements and any basis of W has m elements.

Thus the basis $\mathcal{B}_1$ above has m elements, the basis $\mathcal{B}$ above has n elements, and so the basis $\mathcal{B}_2$ above, which consists of those elements of $\mathcal{B}$ that are not in $\mathcal{B}_1$, has $n - m$ elements.

Thus any complement U of W has dimension $n - m$.

This result is still true when V is infinite dimensional. We could prove this by adapting our proof that any two bases of the *same* vector space have the same number of elements (Lemma 3.3.4 and Theorem 3.3.5) to take care of two complements U and U' of W, which are *different* vector spaces but complements of the same subspace W, showing directly that U and U' must have bases with the same number of elements, and have the same dimension. But we won't do this. Instead we will defer the proof of this to the next chapter (Theorem 4.3.19) where we will be able to prove it more easily given the ideas we develop there. □

We can now make a definition.

Definition 3.4.25. Let W be a subspace of V. The *codimension* $\operatorname{codim}_V W$ of W in V is the dimension of any complement U of W in V. ◊

(We often abbreviate $\operatorname{codim}_V W$ to $\operatorname{codim} W$ when V is understood.)

Theorem 3.4.26. *Let V be a finite-dimensional vector space. Let W be a subspace of V. Then*

$$\dim W + \operatorname{codim}_V W = \dim V.$$

Proof. From the proof of Theorem 3.4.24, if $\dim V = n$ and $\dim W = m$, then any complement U of W in V has dimension $n - m$, and $m + (n - m) = n$. $\square$

Now let us ask the question: given a subspace W of V, how can we actually find a complement U of W? From the proof of Theorem 3.4.24, we see this is the same question as: given a linearly independent set of vectors in V, how can we extend it to a basis of V?

We shall give two methods. In fact, they answer a more general question.

Lemma 3.4.27. *Let W be a subspace of $\mathbb{F}^m$ which is spanned by a set $S = \{v_1, \ldots, v_n\}$. Let A be the matrix*

$$A = [v_1|\ldots|v_n|e_1|\ldots|e_m],$$

and let A' be any weak row-echelon form of A. Then the columns of A between 1 and n that have leading entries in A' are a basis for W, and the columns between $n+1$ and $n+m$ that have leading entries in A' are a basis for a complement U of W.

Proof. Since $\mathbb{F}^m$ is spanned by $\{e_1, \ldots, e_m\}$ (this just being the standard basis of $\mathbb{F}^m$), which are the last m columns of A, it is certainly spanned by $T = \{v_1, \ldots, v_n, e_1, \ldots, e_m\}$, the set of all columns of A. Thus $\mathbb{F}^m = \operatorname{Span}(T)$.

Now the matrix $A_0 = [v_1|\ldots|v_n]$ is the left n columns of the matrix A, and as we have observed, if A' is in weak row-echelon form, then so is its left n columns A'_0. Now we apply Lemma 3.4.6 twice.

Applying this to A'_0 gives that the columns of A between 1 and n that have leading entries in A' are a basis for W, and that all of the columns of A that have leading entries in A' are a basis for V. Hence those columns of A not between 1 and n, i.e., between $n+1$ and $n+m$, form a basis for a complement U of W. $\square$

Remark 3.4.28. Note this procedure works whether or not S is linearly independent. If it is, it extends S to a basis of V. $\Diamond$

Remark 3.4.29. We chose $\{e_1, \ldots, e_m\}$ purely for convenience. But, as the proof shows, we could have chosen any set of vectors in $\mathbb{F}^m$ that spans $\mathbb{F}^m$. $\Diamond$

Example 3.4.30. We return to Example 3.4.10 and ask not only to find a basis for W but also a basis for a complement U of W. Thus we form the matrix

$$A = \begin{bmatrix} 1 & 4 & -1 & 5 & 0 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 4 & 1 & 0 & 1 & 0 & 0 \\ 3 & -2 & 1 & -1 & 4 & 0 & 0 & 1 & 0 \\ 7 & 0 & 1 & 7 & 6 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and row-reduce. We arrive at

$$A' = \begin{bmatrix} 1 & 4 & -1 & 5 & 0 & 1 & 0 & 0 & 0 \\ 0 & -7 & 2 & -6 & 1 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & -4 & 2 & 1 & -2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & -1 & 1 \end{bmatrix}.$$

This has leading entries in columns 1, 2, 4, and 7, so we find that, from columns 1, 2, and 4 (as before)

$$\left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 7 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} 5 \\ 4 \\ -1 \\ 7 \end{bmatrix} \right\}$$

is a basis for W, but we also now find that W has a complement U with basis

$$\left\{ \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \right\}. \qquad \Diamond$$

This method has a practical drawback: we have to do row reduction on a large matrix in order to use it.

Here is a handier method.

Lemma 3.4.31. *Let W be a subspace of ${}^t\mathbb{F}^n$ spanned by a set $S = \{v_1, \ldots, v_m\}$. Let A be the matrix*

$$A = \begin{bmatrix} v_1 \\ \hline \vdots \\ \hline v_m \end{bmatrix}.$$

Let A' be any weak row-echelon form of A. Then the nonzero rows of A' form a basis for W. If the leading entries of A' are in columns $j_1, \ldots, j_k$, then

$$\{{}^te_j \,|\, j \neq j_1, \ldots, j_k\}$$

form a basis for a complement U of W.

Proof. By Lemma 3.4.11, the nonzero rows of A' are a basis for W. Now form the matrix A'' whose rows are the nonzero rows of A' on top, with the vectors ${}^te_j$ for those values of j not equal to $j_1, \ldots, j_k$ on the bottom. Then this matrix has a leading entry in each column (and no zero rows), so, except that the rows may be out of order, is in weak row-echelon form. Hence they form a basis for ${}^t\mathbb{F}^n$. The nonzero rows of A' form a basis of W so the remaining rows that were added form a basis for a complement U of W. $\square$

Remark 3.4.32. We just chose the set $\{{}^te_j \,|\, j \neq j_1, \ldots, j_k\}$ for convenience. We could have chosen any set of vectors which had leading entries in the columns other than $j_1, \ldots, j_k$ (one for each column). $\Diamond$

Example 3.4.33. We return to Example 3.4.14 and ask not only to find a basis for W but also a basis for a complement U of W. We form the matrix A of that example and row-reduce, and obtain the same matrix A', with leading entries in columns 1, 3, and 5. Then again W has basis

$$\left\{\begin{bmatrix}1 & 2 & 1 & 3 & 6 & -1\end{bmatrix}, \begin{bmatrix}0 & 0 & 3 & -2 & -5 & -1\end{bmatrix}, \begin{bmatrix}0 & 0 & 0 & 0 & -1 & 1\end{bmatrix}\right\},$$

but we also see that U has basis

$$\{{}^te_2, {}^te_4, {}^te_6\} = \left\{\begin{bmatrix}0 & 1 & 0 & 0 & 0 & 0\end{bmatrix}, \begin{bmatrix}0 & 0 & 0 & 1 & 0 & 0\end{bmatrix}, \begin{bmatrix}0 & 0 & 0 & 0 & 0 & 1\end{bmatrix}\right\}.$$

$\Diamond$

Again we can apply this to $\mathbb{F}^n$ by the same trick: write the vector in rows, row-reduce, find the answer, and write it in columns.

Example 3.4.34. Let W be the subspace of $\mathbb{F}^4$ spanned by the vectors of Example 3.4.18. We form the matrix A as in that example, row-reduce, and arrive at the same A', with leading entries in columns 1, 2, and 3. Thus to form a basis for ${}^t\mathbb{F}^4$ we take those rows of A' and add in ${}^te_4$.

Standing these vectors up we again obtain a basis

$$\mathcal{B} = \left\{\begin{bmatrix}1\\2\\3\\7\end{bmatrix}, \begin{bmatrix}0\\1\\4\\6\end{bmatrix}, \begin{bmatrix}0\\0\\1\\1\end{bmatrix}\right\}$$

for W, and a basis

$$\left\{\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\right\}$$

for a complement U of W. $\Diamond$

(This is not the same answer we arrived at in Example 3.4.30, but that shouldn't bother you. As we said, complements are not unique, no one complement is better than any other, and we just happened to find a different complement now than we did before.)

3.5. Affine subspaces and quotient vector spaces

For emphasis, we shall call a subspace a vector subspace. We now introduce affine subspaces. But we emphasize that an affine subspace is not a particular kind of vector subspace, but rather a generalization of a vector subspace. In other words, every vector subspace of a vector space V is an affine subspace of V, while an affine subspace of V may be, but is in general *not*, a vector subspace of V.

Definition 3.5.1. Let W be a vector subspace of V. Let t_0 be a fixed vector in V. Then

$$A = t_0 + W = \{t_0 + w \mid w \in W\}$$

is an *affine subspace* of V *parallel* to W. $\Diamond$

You can see from this definition that an affine subspace A of V is obtained by starting with a vector subspace W and "shifting" it by some vector t_0. Thus we could call an affine subspace a shifted subspace, but affine subspace is the standard mathematical term, so we will use it.

Remark 3.5.2. We could take $t_0 = 0$ and in that case A would just be W. Thus we can regard a vector subspace of V as an affine subspace of V parallel to itself. $\Diamond$

Remark 3.5.3. As we will soon see, if W_1 and W_2 are distinct vector subspaces, then no matter what elements t_1 and t_2 we choose, $A_1 = t_1 + W_1$ and $A_2 = t_2 + W_2$ are distinct affine subspaces. But we will also see (even sooner) that if we fix the vector subspace W, it may well be the case that for two distinct vectors $t_1 \neq t_2$, the affine spaces $A = t_1 + W$ and $A_2 = t_2 + W$ are the *same* affine subspaces. $\Diamond$

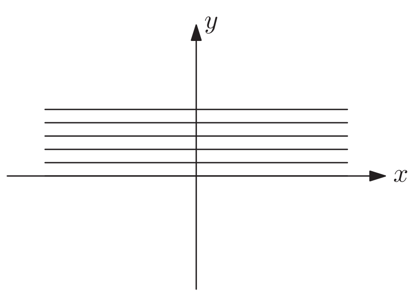
Actually, it is convenient to generalize the notion of parallelism slightly.

Definition 3.5.4. Two affine subspaces A_1 and A_2 of a vector space V are *parallel* if they are both parallel to the same vector subspace W. $\Diamond$

Remark 3.5.5. Under this definition, any affine subspace of V is parallel to itself. (Compare Remark 3.5.2.) $\Diamond$

Remark 3.5.6. We will be proving the results of this section algebraically, and so they hold in any vector space. But "parallel" is of course a geometric term. So let us first see the geometric intuition behind this definition. We will go back to $\mathbb{R}^2$, where we think of vectors as "arrows" starting at the origin, and we identify vectors with their endpoints.

As we have observed, $W = \left\{ \begin{bmatrix} x \\ 0 \end{bmatrix} \right\}$ is a subspace of $V = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \right\}$. Identifying these vectors with their endpoints, this is the x-axis in the plane, i.e., the line given by the equation $y = 0$. Now choose any vector $t_0 = \begin{bmatrix} a_0 \\ b_0 \end{bmatrix}$. Then $A_{t_0} = t_0 + W = \left\{ \begin{bmatrix} x + a_0 \\ b_0 \end{bmatrix} \right\}$ is an affine subspace of V parallel to W. But this is just the horizontal line given by the equation $y = b_0$. So we see the picture of the plane being filled up by mutually parallel (in this case horizontal) lines.



In particular, we note:

(1) any two of these lines are either identical or disjoint (i.e., have no point in common); and

(2) every point in the plane is on exactly one of these lines. $\Diamond$

With this intuition behind us, we get to work.

Lemma 3.5.7. *Let W be a subspace of V and let t_0 be any element of V. Let $A = t_0 + W$.*

(1) *If $t_0 \in W$, then $A = t_0 + W = 0 + W = W$.*

(2) *If $t_0 \notin W$, then A and W are disjoint.*

Proof. (1) Suppose $t_0 \in W$. Then any element of A is of the form $t_0 + w$ for some element of W, and since W is a subspace, this is an element of W. So $A \subseteq W$. On the other hand, let w be any element of W. Then $w = t_0 + (w - t_0) = t_0 + w'$. Now W is a subspace, so $w' \in W$, and hence w is an element of A. So $W \subseteq A$. Since each of A and W is contained in the other, they are identical.

(2) We prove the contrapositive: If A and W are not disjoint, then $t_0 \in W$. Suppose A and W are not disjoint. Then there is some vector v in $A \cap W$. In particular, v is in A, so $v = t_0 + w$ for some $w \in W$. But v is also in W. Hence $t_0 = v - w$ is in W. $\square$

Lemma 3.5.8. *Let W be a vector subspace of V. Then for any two elements t_0 and u_0 of V, $t_0 + (u_0 + W) = (t_0 + u_0) + W$.*

Proof. Any element of $t_0 + (u_0 + W)$ is of the form $t_0 + (u_0 + w)$ for some $w \in W$. But $t_0 + (u_0 + w) = (t_0 + u_0) + w$ so this element is also an element of $(t_0 + u_0) + W$, and vice-versa. $\square$

Corollary 3.5.9. *Let $A_1 = t_1 + W$ and $A_2 = t_2 + W$ be two affine subspaces parallel to the same vector subspace W. Then A_1 and A_2 are either identical or disjoint. More precisely*:

(1) *If $t_1 - t_2 \in W$ (or equivalently $t_2 - t_1 \in W$), then A_1 and A_2 are identical.*

(2) *If $t_1 - t_2 \notin W$ (or equivalently $t_2 - t_1 \notin W$), then A_1 and A_2 are disjoint.*

Proof. (1) Suppose that $t_2 - t_1 \in W$. Set $w = t_2 - t_1$ so that $t_2 = t_1 + w$ with $w \in W$. Then, using Lemma 3.5.7 and Lemma 3.5.8,

$$t_2 + W = (t_1 + w) + W = t_1 + (w + W) = t_1 + W.$$

(2) Again we prove the contrapositive. Suppose A_1 and A_2 are not disjoint and let v be a vector in $A_1 \cap A_2$. Then $v = t_1 + w$ for some w_1 in W_1, and also $v = t_2 + w_2$ for some w_2 in W. Thus $t_1 + w_1 = t_2 + w_2$ so $t_1 - t_2 = w_2 - w_1$. But W is a subspace so $w_2 - w_1 \in W$. $\square$

Corollary 3.5.10. *Let W be a vector subspace of V. Then every $v \in V$ is an element of exactly one affine subspace parallel to W.*

Proof. Since $v = v + 0$, v is in the affine subspace $v + W$. But v cannot be in any other affine subspace parallel to W, as these are all disjoint. $\square$

There is a natural notion of the dimension of an affine subspace.

Definition 3.5.11. Let A be an affine subspace of V parallel to the vector subspace W. Then for $\dim A$, the *dimension* of A, $\dim A = \dim W$. $\diamondsuit$

Remark 3.5.12. Let $\mathcal{B} = \{w_1, w_2, \ldots\}$ be a basis of W. Then, once we have chosen any t_0 in A, every element of A can be written uniquely as $t_0 + \sum c_i w_i$ for some scalars c_i. $\diamondsuit$

Lemma 3.5.13. *Let A_1 be an affine subspace of V parallel to the vector subspace W_1, and let A_2 be an affine subspace of V parallel to the vector subspace W_2. If $W_1 \neq W_2$, then $A_1 \neq A_2$.*

Proof. We prove the contrapositive: If $A_1 = A_2$, then $W_1 = W_2$. So suppose $A_1 = A_2$.

Since A_1 is parallel to W_1, $A_1 = t_1 + W_1$ for some $t_1 \in V$. Since A_2 is parallel to W_2, $A_2 = t_2 + W_2$ for some $t_2 \in V$. Thus $t_1 + W_1 = t_2 + W_2$. In particular, $t_1 + 0 = t_2 + w_2$ for some w_2 in W_2, so $t_1 - t_2 = w_2$ is an element of W_2. Similarly, $t_1 + w_1 = t_2 + 0$ for some w_1, so $t_2 - t_1 = w_1$ is an element of W_1. But $w_1 = -w_2$, and W_1 and W_2 are subspaces, so w_1 and w_2 are elements of both W_1 and W_2.

Then we have the chain of equalities, using Lemma 3.5.8 and the fact that $w_2 \in W_1$,

$$\begin{aligned}
A_1 &= A_2, \\
t_1 + W_1 &= t_2 + W_2, \\
-t_2 + [t_1 + W_1] &= -t_2 + [t_2 + W_2], \\
(-t_2 + t_1) + W_1 &= (-t_2 + t_2) + W_2, \\
w_2 + W_1 &= 0 + W_2, \\
W_1 &= W_2,
\end{aligned}$$

as claimed. $\square$

Remark 3.5.14. There is one point about affine spaces we need to emphasize. Remember that an affine subspace is $A = t_1 + W$, but the choice of t_1 is not unique; if w is *any* element of W and $t_2 = t_1 + w$, then also $A = t_2 + W$.

The point we wish to make is that there is *no* best choice; all choices are equally good. $\diamondsuit$

Beginning with a vector space V and a subspace W, we obtain another example of a vector space.

Theorem 3.5.15. *Let $V/W = \{$distinct affine subspaces of V parallel to $W\}$. Define the operation of vector addition on V/W by*

$$(t_1 + W) + (t_2 + W) = (t_1 + t_2) + W$$

and the operation of scalar multiplication on V/W by

$$c(t_1 + W) = (ct_1) + W.$$

Let the 0 element of V/W be $W = 0 + W$. Let the negative $-(t_0 + W)$ be $(-t_0) + W$. Then V/W is a vector space.

Proof. Using the properties of affine subspaces we have developed, we can verify the 10 properties of a vector space in Definition 3.1.1. □

Definition 3.5.16. The vector space V/W of Theorem 3.5.15 is called a *quotient vector space*, the quotient of the vector space V by the subspace W. ◊

3.6. Exercises

1. Verify the claims that the examples of vector spaces given in Section 3.1 are indeed vector spaces.

2. (a) For any nonnegative integer d, show that $P_d(\mathbb{F})$ is a vector space.

(b) Let $W_d = \{\text{polynomial of degree } \textit{exactly } d\}$. Show that W_d is *not* a vector space. Which axiom(s) are not satisfied?

(c) Show that $P(\mathbb{F})$ is a vector space.

3. Let $W = \left\{ v \in \mathbb{R}^n \;\middle|\; v = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \text{ with each } a_i \text{ an integer} \right\}$. Show that W is *not* a vector space. Which axiom(s) are not satisfied?

4. In each case, decide whether the given vector v is in the span of the set of vectors S. If so, express v as a linear combination of the vectors in S.

(a) $S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 4 \end{bmatrix} \right\}$, $v = \begin{bmatrix} 3 \\ 5 \\ 8 \end{bmatrix}$.

(b) $S = \left\{ \begin{bmatrix} 1 \\ 4 \\ 2 \end{bmatrix}, \begin{bmatrix} -2 \\ -3 \\ -7 \end{bmatrix} \right\}$, $v = \begin{bmatrix} 0 \\ 5 \\ -3 \end{bmatrix}$.

(c) $S = \left\{ \begin{bmatrix} 1 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 3 \end{bmatrix} \right\}$, $v = \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}$.

(d) $S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ 3 \end{bmatrix} \right\}$, $v = \begin{bmatrix} 1 \\ 3 \\ 6 \end{bmatrix}$.

(e) $S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 5 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 4 \end{bmatrix} \right\}$, $v = \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}$.

(f) $S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 4 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 1 \\ 1 \end{bmatrix} \right\}$, $v = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$.

(g) $S = \{1 + 2x + 4x^2, 4 + x + 2x^2, 2 + 5x + 7x^2\}$, $v = x^2$.

(h) $S = \{1 + 4x + x^2, 2 + 3x + x^2, 3 + 7x + 2x^2\}$, $v = 1 + x + x^2$.

5. In each case, decide whether the given set of vectors span V. If not, find a vector in V that is not in the span of the set.

(a) $\left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 5 \\ 8 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \\ 3 \end{bmatrix} \right\}$, $V = \mathbb{R}^4$.

(b) $\left\{ \begin{bmatrix} 1 \\ 3 \\ 5 \\ 9 \end{bmatrix}, \begin{bmatrix} 2 \\ 5 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \\ 2 \\ -11 \end{bmatrix}, \begin{bmatrix} 5 \\ 1 \\ 10 \\ 1 \end{bmatrix} \right\}$, $V = \mathbb{R}^4$.

(c) $\left\{ \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} -1 \\ 3 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 3 \\ 3 \\ 2 \\ 2 \end{bmatrix} \right\}$, $V = \mathbb{R}^4$.

(d) $\left\{ \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ -1 \\ -1 \end{bmatrix}, \begin{bmatrix} 3 \\ -1 \\ -1 \\ -1 \end{bmatrix} \right\}$, V the subspace of $\mathbb{R}^4$ consisting of all vectors $\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$ with $a + b + c + d = 0$.

(e) $\{1 + 3x + 4x^2 + x^3, x + 2x^2 - x^3, 2 + 6x + x^2 + 2x^3\}$, $V = P_3$.

(f) $\{1 + 2x - x^2 + 2x^3, 3 - x + 2x^2 + 3x^3, 2 - x + 2x^2 + x^3, 2x - x^2\}$, $V = P_3$.

(g) $\{1 + 3x + 2x^2 + 3x^3, 3 + 4x + x^2 + 4x^3, 2 - 3x + x^2 + 3x^3, 2 - 2x + x^2 + x^3\}$, $V = P_3$.

(h) $\{1 + 3x + x^2 + 3x^3, 2 + x + 2x^2 + 4x^3, -3 + 2x^2 + 5x^3, x^2 - x^3, x + x^2 + 3x^3\}$, $V = P_3$.

6. In each case, decide whether the given set of vectors is linearly independent. If not, find a nontrivial linear dependence relation between them.

(a) $\left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 4 \\ 4 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \\ 5 \\ 5 \end{bmatrix} \right\}$.

(b) $\left\{ \begin{bmatrix} 1 \\ 3 \\ 5 \\ 7 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \\ 6 \\ 8 \end{bmatrix}, \begin{bmatrix} 1 \\ 5 \\ 9 \\ 13 \end{bmatrix} \right\}$.

(c) $\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \\ 5 \\ 8 \end{bmatrix}, \begin{bmatrix} 1 \\ 4 \\ 7 \\ 11 \end{bmatrix} \right\}$.

(d) $\left\{ \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 4 \\ 9 \\ 16 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 5 \\ 7 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 4 \\ 8 \end{bmatrix} \right\}.$

(e) $\left\{ \begin{bmatrix} 1 \\ 2 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 4 \\ 6 \end{bmatrix}, \begin{bmatrix} 1 \\ 5 \\ 4 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 10 \\ 9 \\ 7 \end{bmatrix} \right\}.$

(f) $\{1 + 2x + 4x^2 + 6x^3, 2 + 3 + 7x^2 + 9x^3, x + x^2 + 2x^3\}$.

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

(h) $\{1 + 4x + 5x^2 + 2x^3, 2 + 3x + x^2 + 4x^3, -3 + x + x^3, 8x + 6x^2 + 7x^3\}$.

(i) $\{1 + 5x + 3x^2 + x^3, 2 + 3x + 4x^2 + 2x^3, 1 + 3x + x^2 + 4x^3, 2 + x + 3x^2 + 6x^3, 1 + 12x + 3x^2 - x^3\}$.

7. In each case, decide whether S is a basis of V.

(a) $S = \left\{ \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} -1 \\ 2 \\ 4 \end{bmatrix} \right\}, V = \mathbb{R}^3.$

(b) $S = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \right\}, V = \mathbb{R}^3.$

(c) $S = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 7 \\ 3 \end{bmatrix} \right\}, V = \mathbb{R}^3.$

(d) $S = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 5 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix} \right\}, V = \mathbb{R}^3.$

(e) $S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 4 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \\ 5 \\ 2 \end{bmatrix} \right\}, V = \mathbb{R}^4.$

(f) $S = \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 5 \\ 8 \\ 7 \end{bmatrix}, \begin{bmatrix} 3 \\ 6 \\ 10 \\ 6 \end{bmatrix}, \begin{bmatrix} 5 \\ 11 \\ 18 \\ 11 \end{bmatrix} \right\}, V = \mathbb{R}^4.$

(g) $S = \left\{ \begin{bmatrix} 1 \\ 5 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 3 \\ -1 \end{bmatrix}, \begin{bmatrix} 4 \\ 2 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 7 \\ -1 \\ -4 \\ 9 \end{bmatrix} \right\}, V = \mathbb{R}^4.$

(h) $S = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 3 \\ 8 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 4 \\ 9 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 3 \\ 7 \end{bmatrix} \right\}, V = \mathbb{R}^4.$

(i) $S = \{1 + x + x^3, 2x + 3x^2 - x^3, 1 + 3x + 7x^2\}$, $V = P_3$.

(j) $S = \{1+2x+x^2-x^3, 4+x-3x^2-5x^3, 7+4x-2x^2-5x^3, 2+x+3x^2-2x^3\}$, $V = P_3$.

(k) $S = \{1 + 2x + 2x^2 + 6x^3, 2 + 3x + 3x^2 + 6x^3, -1 + 3x + 5x^2 + 5x^3, 1 - 2x - 4x^2 + x^3\}$, $V = P_3$.

(l) $S = \{1 + 3x - 2x^2 - x^3, 3 + 5x - x^2 + 2x^3, 3 + 8x + 9x^2 - 7x^3, 3 - 2x + x^2 - 2x^3, 5 - x - x^2 - x^3\}$, $V = P_3$.

In (m), (n), (o), and (p), $V = \{f(x) \in P_3 \,|\, f(-1) = 0\}$.

(m) $S = \{3 + 2x + x^3, x + x^2\}$.

(n) $S = \{1 + 2x + 5x^2 + 4x^3, x + 3x^2 + 2x^3, 1 + 8x^2 + 9x^3\}$.

(o) $S = \{1 + 3x - 3x^2 - 5x^3, 2 + 4x - x^2 - 3x^3, 7 + 17x - 11x^2 - 21x^3\}$.

(p) $S = \{1 + 2x + 2x^2 + x^3, 2 - 3x - x^2 + 4x^3, 3 + x^2 + 4x^3, 1 + 2x + x^2\}$.

8. Answer each of the following 12 questions (two questions for each set S of vectors).

S	Does S span $\mathbb{R}^3$?	Is S linearly independent?
(a) $\left\{\begin{bmatrix}1\\0\\3\end{bmatrix}, \begin{bmatrix}0\\1\\-2\end{bmatrix}, \begin{bmatrix}2\\3\\1\end{bmatrix}, \begin{bmatrix}5\\-3\\21\end{bmatrix}\right\}$		
(b) $\left\{\begin{bmatrix}1\\2\\5\end{bmatrix}, \begin{bmatrix}1\\-1\\2\end{bmatrix}, \begin{bmatrix}-1\\7\\4\end{bmatrix}, \begin{bmatrix}1\\8\\11\end{bmatrix}\right\}$		
(c) $\left\{\begin{bmatrix}1\\3\\2\end{bmatrix}, \begin{bmatrix}1\\2\\1\end{bmatrix}, \begin{bmatrix}2\\6\\3\end{bmatrix}\right\}$		
(d) $\left\{\begin{bmatrix}1\\2\\3\end{bmatrix}, \begin{bmatrix}1\\3\\4\end{bmatrix}, \begin{bmatrix}2\\-1\\1\end{bmatrix}\right\}$		
(e) $\left\{\begin{bmatrix}1\\2\\5\end{bmatrix}, \begin{bmatrix}2\\4\\7\end{bmatrix}\right\}$		
(f) $\left\{\begin{bmatrix}2\\1\\-1\end{bmatrix}, \begin{bmatrix}6\\3\\-3\end{bmatrix}\right\}$		

9. In each case, verify that the given set R is linearly independent. Then find a basis S of V with $R \subseteq S$.

(a) $R = \left\{\begin{bmatrix}1\\4\\1\end{bmatrix}\right\}$, $V = \mathbb{R}^3$.

(b) $R = \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 3 \end{bmatrix} \right\}$, $V = \mathbb{R}^3$.

(c) $R = \left\{ \begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 \\ 6 \\ 8 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} \right\}$, $V = \mathbb{R}^3$.

(d) $R = \left\{ \begin{bmatrix} 1 \\ 2 \\ 1 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 4 \\ 7 \end{bmatrix} \right\}$, $V = \mathbb{R}^4$.

(e) $R = \left\{ \begin{bmatrix} 1 \\ 3 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 10 \\ 11 \\ 6 \end{bmatrix} \right\}$, $V = \mathbb{R}^4$.

(f) $R = \{1 + x + x^2, x + 2x^2\}$, $V = P_2$.

10. In each case, verify that the given set T spans V. Then find a basis S of V with $S \subseteq T$.

(a) $T = \left\{ \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} 7 \\ 6 \\ 2 \end{bmatrix}, \begin{bmatrix} 5 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ 2 \end{bmatrix} \right\}$, $V = \mathbb{R}^3$.

(b) $T = \left\{ \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \\ 3 \end{bmatrix}, \begin{bmatrix} 7 \\ 14 \\ 11 \end{bmatrix}, \begin{bmatrix} 5 \\ 10 \\ 9 \end{bmatrix} \right\}$, $V = \mathbb{R}^3$.

(c) $T = \left\{ \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 5 \\ 9 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \\ 6 \end{bmatrix} \right\}$, $V = \mathbb{R}^3$.

(d) $T = \{1 + x + x^2, x - x^2, 1 + 2x, x^2\}$, $V = P_2$.

11. In each case, verify that the given set R is linearly independent and that the given set T spans V. Then find a basis S of V with $R \subseteq S \subseteq T$.

(a) $R = \left\{ \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} \right\}$, $T = \left\{ \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} \right\}$, $V = \mathbb{R}^3$.

(b) $R = \left\{ \begin{bmatrix} 1 \\ 3 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 4 \end{bmatrix} \right\}$, $T = \left\{ \begin{bmatrix} 1 \\ 3 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 3 \\ 6 \\ 7 \end{bmatrix}, \begin{bmatrix} 5 \\ 9 \\ 11 \end{bmatrix}, \begin{bmatrix} 3 \\ 3 \\ 7 \end{bmatrix} \right\}$, $V = \mathbb{R}^3$.

(c) $R = \left\{ \begin{bmatrix} 1 \\ 2 \\ -1 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ -2 \end{bmatrix} \right\}$, $T = \left\{ \begin{bmatrix} 1 \\ 2 \\ -1 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ -2 \end{bmatrix}, \begin{bmatrix} 3 \\ 5 \\ -4 \end{bmatrix}, \begin{bmatrix} 6 \\ 10 \\ -7 \end{bmatrix} \right\}$, $V = \mathbb{R}^4$.

(d) $R = \left\{ \begin{bmatrix} 1 \\ 2 \\ 1 \\ -4 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ -3 \\ 0 \end{bmatrix} \right\}$, $T = \left\{ \begin{bmatrix} 1 \\ 2 \\ 1 \\ -4 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ -3 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ -1 \\ -1 \\ 0 \end{bmatrix} \right\}$,

$$V = \left\{ \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} \in \mathbb{R}^4 \,\middle|\, a+b+c+d=0 \right\}.$$

(e) $R = \{1+x, 1+x^3\}$, $T = \{1+x, 1+x^3, x-x^3, x^2+x^3\}$, $V = \{f(x) \in P_3 \,|\, f(-1) = 0\}$.

12. Let $\mathcal{E} = \{e_i\}$ be the standard basis of $\mathbb{F}^n$. Let $f_{ij} = e_i - e_j$, and let $\mathcal{F} = \{f_{ij}\}$. Let $v = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \in \mathbb{F}^n$. Show that $v \in \operatorname{Span}(\mathcal{F})$ if and only if $v_1 + \cdots + v_n = 0$.

13. Let V be the vector space $V = P_3(\mathbb{F})$.

(a) Let W_1 be the subspace $W_1 = \{p(x) \in V \,|\, p(1) = 0\}$. Find a basis for W_1.

(b) Let W_2 be the subspace $W_2 = \{p(x) \in V \,|\, p(2) = 0\}$. Find a basis for W_2.

(c) Let U_{12} be the subspace $U_{12} = \{p(x) \in V \,|\, p(1) = p(2)\}$. Find a basis for U_{12}.

(d) Let W_{12} be the subspace $W_{12} = \{p(x) \in V \,|\, p(1) = p(2) = 0\}$. Find a basis for W_{12}.

(e) Note that $W_{12} \subset W_1$, $W_{12} \subset W_2$, and $W_{12} \subset U_{12}$. More precisely, $W_{12} = U_{12} \cap W_1$ and $W_{12} = U_{12} \cap W_2$.

Extend your basis of W_{12} in (d) to a basis of U_{12}.

Extend your basis of W_{12} in (d) to a basis of W_1.

Extend your basis of W_{12} in (d) to a basis of W_2.

(f) Extend your basis of W_1 in (e) to a basis of V.

Extend your basis of W_2 in (e) to a basis of V.

14. (a) Let $\mathcal{B} = \{p_i(x)\}_{i=0,\dots,d}$ be a set of polynomials, with $\deg(p_i(x)) = i$ for each i. Show that $\mathcal{B}$ is a basis for $P_d(\mathbb{F})$.

(b) Let $\mathcal{B} = \{p_i(x)\}_{i=0,1,2,\dots}$ be a set of polynomials, with $\deg(p_i(x)) = i$ for each i. Show that $\mathcal{B}$ is a basis for $P(\mathbb{F})$.

15. (a) Fix a positive integer d. For $i = 0, \dots, d$, let $p_i(x)$ be a polynomial of degree at most d with $p_i(x)$ divisible by x^i but not by x^{i+1}. Show that $\mathcal{B} = \{p_0(x), \dots, p_d(x)\}$ is a basis for $P_d(\mathbb{F})$.

(b) For each nonnegative integer $i = 0, 1, \dots,$ let $p_i(x)$ be a polynomial that is divisible by x^i but not by x^{i+1}. Let $\mathcal{B} = \{p_0(x), p_1(x), \dots\}$. Give an example where $\mathcal{B}$ is a basis of $P(\mathbb{F})$, and an example where it is not.

16. Let $V = P(\mathbb{F})$. Let $\mathcal{B} = \{p_{i_0}(x), p_{i_1}(x), p_{i_2}(x), \dots\}$ be a set of polynomials in V with $0 \le \deg(p_{i_0}(x)) < \deg(p_{i_1}(x)) < \deg(p_{i_2}(x)) < \cdots$, and let W be the subspace of V spanned by $\mathcal{B}$. Let S be the set of nonnegative integers $\{k \,|\, k \neq i_j \text{ for any } j\}$. Show that $\operatorname{codim}_V W$ is equal to the cardinality of S.

17. Prove the following exchange (or replacement) lemma:

Let V be a vector space. Let $\mathcal{B}_0$ be a set of n vectors in V that is linearly independent. Let $\mathcal{C}$ be a set of m vectors in V that spans V. Then $n \le m$, and there is a subset $\mathcal{C}_0$ of $\mathcal{C}$ containing $m - n$ vectors such that $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{C}_0$ spans V. If $\mathcal{C}$ is also linearly independent (so that $\mathcal{C}$ is a basis of V), then $\mathcal{B}$ is also a basis of V.

(The name of this lemma comes from the fact that we can start with $\mathcal{C}$ and exchange elements of $\mathcal{B}_0$ and $\mathcal{C}$, or replace elements of $\mathcal{C}$ by elements of $\mathcal{B}_0$, so that if $\mathcal{C}$ spans V (resp., $\mathcal{C}$ is a basis of V), then the set $\mathcal{B}$ we obtain as a result of this process also spans V (resp., is also a basis of V).)

18. Let $f(x)$ be a function that does not vanish at 0 (i.e., a function with $f(0) \ne 0$).

(a) Show that $\{f(x), xf(x)\}$ is linearly independent.

(b) Show that $\{f(x), xf(x), \ldots, x^k f(x)\}$ is linearly independent for any $k \ge 0$.

Let $f(x)$ be any function that is not identically 0 (i.e., a function with $f(a) \ne 0$ for some a).

(a$'$) Show that $\{f(x), xf(x)\}$ is linearly independent.

(b$'$) Show that $\{f(x), xf(x), \ldots, x^k f(x)\}$ is linearly independent for any $k \ge 0$.

19. Let $S = \{f_1(x), f_2(x), \ldots, f_n(x)\}$ be a set of differentiable functions, and let $S' = \{f_1'(x), f_2'(x), \ldots, f_n'(x)\}$.

(a) If S is linearly independent, must S' be linearly independent?

(b) If S' is linearly independent, must S be linearly independent?

20. Verify the claims in Example 3.3.21.

21. Verify that the example of subspaces in Example 3.4.2 are indeed subspaces.

22. Prove Lemma 3.4.5.

23. Let V be a vector space and let W_1 and W_2 be subspaces of V with $W_1 \not\subseteq W_2$ and $W_2 \not\subseteq W_1$. Show that $W_1 \cup W_2$ is not a subspace of V.

24. Let V be a vector space and suppose that V is an increasing union of subspaces $V_0, V_1, V_2, \ldots$. That is, $V = \bigcup_{i=0}^{\infty} V_i$ with $V_0 \subseteq V_1 \subseteq V_2 \subseteq \cdots$. Suppose that $\mathcal{B}_i$ is a basis of V_i for each i, with $\mathcal{B}_0 \subseteq \mathcal{B}_1 \subseteq \mathcal{B}_2 \subseteq \cdots$. Show that $\mathcal{B} = \bigcup_{i=0}^{\infty} \mathcal{B}_i$ is a basis of V.

25. Let V be an infinite-dimensional vector space, and let W be a subspace of V.

(a) If $\dim W$ is finite, show $\operatorname{codim}_V W$ is infinite.

(b) If $\operatorname{codim}_V W$ is finite, show $\dim W$ is infinite.

(c) Give examples of the following:

(1) $\dim W$ is infinite, $\operatorname{codim}_V W$ is finite.
(2) $\operatorname{codim}_V W$ is infinite, $\dim W$ is finite.
(3) $\dim W$ and $\operatorname{codim}_V W$ are both infinite.

(Compare Theorem 3.4.26.)

26. Carefully prove Theorem 3.5.15 (that V/W is a vector space).

27. (a) Let V be a vector space, U a subspace of V, and A an affine subspace of V. If $B = A \cap U$ is nonempty, show that B is an affine subspace of U.

(b) In this situation, suppose that A is parallel to the subspace W of V. Show that B is parallel to $U \cap W$.

28. Let $f(x)$ be any polynomial with nonzero constant term. Let d be any non-negative integer, and let $h(x)$ be any polynomial of degree d. Show that there is a unique polynomial $g(x)$ of degree at most d such that $f(x)g(x) = h(x) + x^{d+1}k(x)$ for some polynomial $k(x)$. (This problem may most easily be solved by regarding it as a problem involving quotient vector spaces.)

29. Let $\mathbb{F}$ be a field with infinitely many elements (e.g., $\mathbb{F} = \mathbb{Q}, \mathbb{R},$ or $\mathbb{C}$).

(a) Show that a finite-dimensional vector space V over $\mathbb{F}$ is not the union of finitely many proper subspaces.

(b) Show that an arbitrary vector space V over $\mathbb{F}$ is not the union of finitely many proper subspaces.

(c) Show that a finite-dimensional vector space V over $\mathbb{F}$ is not the union of finitely many proper affine subspaces.

(d) Show that an arbitrary vector space V over $\mathbb{F}$ is not the union of finitely many proper affine subspaces.

(Hint: Do the finite-dimensional case by induction on the dimension of V. Then reduce the case of arbitrary V to the finite-dimensional case.)

Chapter 4

Linear transformations

4.1. Linear transformations I

Not only are we interested in vector spaces themselves, but we are also interested in functions between vector spaces. But let us think for a moment about what that should mean. Suppose we have two vector spaces V and W. Now V and W are each sets of vectors, so a function from V to W will certainly be a function on sets, that is, a function that takes each element of V to an element of W. But vector spaces are *more* than just sets of vectors. They are sets of vectors *with additional structure*, namely, with the operations of vector addition and scalar multiplication. So we want our functions to take this extra structure into account, to "respect" these two operations. These are the sort of functions we are interested in, and these are what are called linear transformations. We now precisely define them.

Definition 4.1.1. Let V and W be the vector spaces over a field $\mathbb{F}$. A *linear transformation* $\mathcal{T}\colon V \to W$ is a function $\mathcal{T}\colon V \to W$ that satisfies the following properties:

(1) For any two vectors v_1 and v_2 in V, $\mathcal{T}(v_1 + v_2) = \mathcal{T}(v_1) + \mathcal{T}(v_2)$.

(2) For any vector v in V and any scalar c, $\mathcal{T}(cv) = c\mathcal{T}(v)$. $\Diamond$

Here is an equivalent way of looking at linear transformations. It is that they are the functions that "respect" linear combinations.

Lemma 4.1.2. *A function $\mathcal{T}\colon V \to W$ is a linear transformation if and only if for any vectors $v_1, \ldots, v_k$ in V and any scalars $c_1, \ldots, c_k$,*

$$\mathcal{T}(c_1v_1 + c_2v_2 + \cdots + c_kv_k) = c_1\mathcal{T}(v_1) + c_2\mathcal{T}(v_2) + \cdots + c_k\mathcal{T}(v_k).$$

Proof. On the one hand, suppose $\mathcal{T}$ is a linear transformation. Then applying properties (1) and (2) repeatedly,

$$\begin{aligned}\mathcal{T}(c_1v_1 + c_2v_2 + \cdots + c_kv_k) &= \mathcal{T}(c_1v_1) + \mathcal{T}(c_2v_2) + \cdots + \mathcal{T}(c_kv_k)\\ &= c_1\mathcal{T}(v_1) + c_2\mathcal{T}(v_2) + \cdots + c_k\mathcal{T}(v_k).\end{aligned}$$

On the other hand, suppose this condition is true. Then we could take $k = 2$ and $c_1 = c_2 = 1$. Then $\mathcal{T}(v_1 + v_2) = \mathcal{T}(1v_1 + 1v_2) = 1\mathcal{T}(v_1) + 1\mathcal{T}(v_2) = \mathcal{T}(v_1) + \mathcal{T}(v_2)$. We could also take $k = 1$, $c_1 = c$, and $v_1 = v$. Then $\mathcal{T}(cv) = \mathcal{T}(c_1v_1) = c_1\mathcal{T}(v_1) = c\mathcal{T}(v)$. □

Here is one simple but basic fact about linear transformations.

Lemma 4.1.3. *Let $\mathcal{T}: V \to W$ be a linear transformation. Then $\mathcal{T}(0) = 0$.*

Proof. $\mathcal{T}(0) = \mathcal{T}(0 \cdot 0) = 0 \cdot \mathcal{T}(0) = 0$. □

(In this proof, the first, third, and fifth occurrences of 0 denote the 0 element of V, the second and fourth the scalar 0, and the last the 0 element of W.)

Let us now see a wide variety of examples.

Example 4.1.4. (a) Let $V = \mathbb{F}^n$, and let $W = \mathbb{F}^m$. Let A be an m-by-n matrix with entries in $\mathbb{F}$. Then $\mathcal{T} = \mathcal{T}_A: V \to W$ given by $\mathcal{T}_A(v) = Av$ is a linear transformation. This is Corollary 1.5.4.

(b) Let $V = P(\mathbb{F})$, the vector space of polynomials with coefficients in $\mathbb{F}$. Let $q(x)$ be any fixed polynomial. Then $\mathcal{T}: V \to V$ by $\mathcal{T}(p(x)) = p(x)q(x)$ is a linear transformation. In fact, if $q(x)$ has degree d_0, then for any d, $\mathcal{T}: P_d(\mathbb{F}) \to P_{d+d_0}(\mathbb{F})$ by $\mathcal{T}(p(x)) = p(x)q(x)$ is a linear transformation.

(c) Let V be any vector space, and let $v_1, \dots, v_k$ be any fixed elements of V. Then we have $\mathcal{T}: \mathbb{F}^k \to V$ by

$$\mathcal{T}\left(\begin{bmatrix} a_1 \\ \vdots \\ a_k \end{bmatrix}\right) = a_1v_1 + \cdots + a_kv_k.$$

(d) We observed in Example 3.1.7 that for any set X, $V = \{f: X \to \mathbb{F}\}$ has the structure of an $\mathbb{F}$-vector space. Let x_1 be any fixed element of X. Then $\mathcal{E}_{x_1}: V \to \mathbb{F}$ by $\mathcal{E}_{x_1}(f) = f(x_1)$ is a linear transformation. (We use the symbol $\mathcal{E}_{x_1}$ as this is the evaluation of the function f at the point x_1.) Similarly, for any fixed elements $x_1, \dots, x_k$ of X, we have $\mathcal{E}: V \to \mathbb{F}^k$ by $\mathcal{E}(f) = \begin{bmatrix} f(x_1) \\ f(x_2) \\ \vdots \\ f(x_k) \end{bmatrix}$.

(e) We can regard polynomials with coefficients in $\mathbb{F}$ as giving functions from $\mathbb{F}$ to $\mathbb{F}$, i.e., if $p(x)$ is a polynomial $p(x) = a_0 + a_1x + \cdots + a_nx^n$, then for any c in $\mathbb{F}$, we have $p(c) = a_0 + a_1c + \cdots + a_nc^n$. But this puts us in the situation of (d), i.e., for any fixed $c \in \mathbb{F}$ we have $\mathcal{E}_c: P(\mathbb{F}) \to \mathbb{F}$ by $\mathcal{E}_c(p(x)) = p(c)$. Then of course for any $d \geq 0$ we can also define $\mathcal{E}_c: P_d(\mathbb{F}) \to \mathbb{F}$ in this way. Similarly, for any fixed $c_1, \dots, c_k \in \mathbb{F}$ we have $\mathcal{E}: P(\mathbb{F}) \to \mathbb{F}^k$ or $\mathcal{E}: P_d(\mathbb{F}) \to \mathbb{F}^k$ by $\mathcal{E}(p(x)) = \begin{bmatrix} p(c_1) \\ p(c_2) \\ \vdots \\ p(c_k) \end{bmatrix}$.

(f) We have $\mathcal{S}_{\text{dn}}\colon \mathbb{F}^\infty \to \mathbb{F}^\infty$ and $\mathcal{S}_{\text{dn}}\colon \mathbb{F}^{\infty\infty} \to \mathbb{F}^{\infty\infty}$, and also $\mathcal{S}_{\text{up}}\colon \mathbb{F}^\infty \to \mathbb{F}^\infty$ and $\mathcal{S}_{\text{up}}\colon \mathbb{F}^{\infty\infty} \to \mathbb{F}^{\infty\infty}$ defined by

$$\mathcal{S}_{\text{dn}}\left(\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \end{bmatrix}\right) = \begin{bmatrix} 0 \\ a_1 \\ a_2 \\ \vdots \end{bmatrix}, \quad \mathcal{S}_{\text{up}}\left(\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \end{bmatrix}\right) = \begin{bmatrix} a_2 \\ a_3 \\ a_4 \\ \vdots \end{bmatrix}.$$

$\mathcal{S}_{\text{dn}}$ is "down-shift" and $\mathcal{S}_{\text{up}}$ is "up-shift". Similarly we have $\mathcal{S}_{\text{rt}}\colon {}^t\mathbb{F}^\infty \to {}^t\mathbb{F}^\infty$ and $\mathcal{S}_{\text{rt}}\colon {}^t\mathbb{F}^{\infty\infty} \to {}^t\mathbb{F}^{\infty\infty}$, and also $\mathcal{S}_{\text{lt}}\colon {}^t\mathbb{F}^\infty \to {}^t\mathbb{F}^\infty$ and $\mathcal{S}_{\text{lt}}\colon {}^t\mathbb{F}^{\infty\infty} \to {}^t\mathbb{F}^{\infty\infty}$ given by "right-shift" and "left-shift", respectively. $\Diamond$

You can see we have quite a variety of specific linear transformations. Here are two quite general ones.

Example 4.1.5. Let V be any vector space. Then we have the identity linear transformation $\mathcal{I}\colon V \to V$ given by

$$\mathcal{I}(v) = v \quad \text{for every } v \in V. \qquad \Diamond$$

Example 4.1.6. Let V and W be any two vector spaces. Then we have the zero linear transformation $\mathcal{Z}\colon V \to W$ given by

$$\mathcal{Z}(v) = 0 \quad \text{for every } v \text{ in } V. \qquad \Diamond$$

Now linear transformations are functions, and it makes sense to add functions and to multiply them by constants. But that wouldn't be very useful to us if the results were just some random functions. We want them to be linear transformations. And indeed they are:

Lemma 4.1.7. (1) *Let V and W be vector spaces, and let $\mathcal{S}\colon V \to W$ and $\mathcal{T}\colon V \to W$ be linear transformations. Let $\mathcal{U} = \mathcal{S} + \mathcal{T}$ (so that $\mathcal{U}(v) = (\mathcal{S} + \mathcal{T})(v) = \mathcal{S}(v) + \mathcal{T}(v)$ for every v in V). Then $\mathcal{U}\colon V \to W$ is a linear transformation.*

(2) *Let V and W be vector spaces, and let $\mathcal{T}\colon V \to W$ be a linear transformation. Let a be a scalar, and let $\mathcal{U} = a\mathcal{T}$ (so that $\mathcal{U}(v) = (a\mathcal{T})(v) = a\mathcal{T}(v)$ for every v in V). Then $\mathcal{U}\colon V \to W$ is a linear transformation.*

Proof. In each case we need to verify the two properties of a linear transformation, first that $\mathcal{U}(v_1 + v_2) = \mathcal{U}(v_1) + \mathcal{U}(v_2)$, and second, that $\mathcal{U}(cv) = c\mathcal{U}(v)$. These are both straightforward, and we leave them to the reader. $\Box$

Definition 4.1.8. Let V and W be fixed vector spaces. Then

$$L(V, W) = \{\text{linear transformations } \mathcal{T}\colon V \to W\}. \qquad \Diamond$$

This gives us another, and very important, example of a vector space.

Theorem 4.1.9. *For any $\mathbb{F}$-vector spaces V and W, $L(V, W)$ is an $\mathbb{F}$-vector space.*

Proof. We have to verify the 10 properties of a vector space in Definition 3.1.1.

Property (1) is given to us by Lemma 4.1.7(1), and property (6) is given to us by Lemma 4.1.7(2). The 0 element of $L(V, W)$ is the zero linear transformation $\mathcal{Z}\colon V \to W$ given by $\mathcal{Z}(v) = 0$ for every v in V, and if $\mathcal{T}\colon V \to W$ is a linear transformation, then $-\mathcal{T}\colon V \to W$ is the linear transformation defined by $(-\mathcal{T})(v) = -\mathcal{T}(v)$. Then it is routine to verify the remaining properties. □

Since $\mathcal{Z}$ is the 0 element of the vector space $L(V, W)$, we shall, as is universally done, usually denote it by 0 (yet another meaning for this symbol!).

Given any two functions $f\colon X \to Y$ and $g\colon Y \to Z$, we can compose them to get the function $gf\colon X \to Z$ defined by $(gf)(x) = g(f(x))$. Thus given linear transformations $\mathcal{S}\colon U \to V$ and $\mathcal{T}\colon V \to W$ we can compose them to get a function $\mathcal{T}\mathcal{S}\colon U \to W$. That would not be very useful if $\mathcal{T}\mathcal{S}$ were just an arbitrary function. We want $\mathcal{T}\mathcal{S}$ to be a linear transformation. And it is:

Theorem 4.1.10. *Let $\mathcal{S}\colon U \to V$ and $\mathcal{T}\colon V \to W$ be linear transformations. Then $\mathcal{T}\mathcal{S}\colon U \to W$ is a linear transformation.*

Proof. We verify the properties of a linear transformation:

(1) $\mathcal{T}\mathcal{S}(u_1+u_2) = \mathcal{T}(\mathcal{S}(u_1+u_2)) = \mathcal{T}(\mathcal{S}(u_1)+\mathcal{S}(u_2)) = \mathcal{T}(\mathcal{S}(u_1))+\mathcal{T}(\mathcal{S}(u_2)) = \mathcal{T}\mathcal{S}(u_1) + \mathcal{T}\mathcal{S}(u_2)$.

(2) $\mathcal{T}\mathcal{S}(cu) = \mathcal{T}(\mathcal{S}(cu)) = \mathcal{T}(c\mathcal{S}(u)) = c\mathcal{T}(\mathcal{S}(u)) = c\mathcal{T}\mathcal{S}(u)$. □

Let us now see some additional properties of linear transformations. We assume in this lemma that all compositions make sense.

Lemma 4.1.11. *Let $\mathcal{S}$, $\mathcal{T}$, and $\mathcal{U}$ be linear transformations. Let c be a scalar.*

(1) $\mathcal{S}(\mathcal{T}\mathcal{U}) = (\mathcal{S}\mathcal{T})\mathcal{U}$.

(2a) $(\mathcal{S}_1 + \mathcal{S}_2)\mathcal{T} = \mathcal{S}_1\mathcal{T} + \mathcal{S}_2\mathcal{T}$.

(2b) $(c\mathcal{S})\mathcal{T} = c(\mathcal{S}\mathcal{T})$.

(3a) $\mathcal{S}(\mathcal{T}_1 + \mathcal{T}_2) = \mathcal{S}\mathcal{T}_1 + \mathcal{S}\mathcal{T}_2$.

(3b) $\mathcal{S}(c\mathcal{T}) = c(\mathcal{S}\mathcal{T})$.

(4) $\mathcal{S}(c\mathcal{T}) = (c\mathcal{S})\mathcal{T} = c(\mathcal{S}\mathcal{T})$.

(5) $\mathcal{Z}\mathcal{T} = \mathcal{Z}$, $\mathcal{T}\mathcal{Z} = \mathcal{Z}$.

(6) $\mathcal{I}\mathcal{T} = \mathcal{T}$, $\mathcal{T}\mathcal{I} = \mathcal{T}$.

Proof. (1) is just a special case of the fact that composition of functions is associative.

By the definition of composition of functions, for any vector v,

$$\mathcal{S}(\mathcal{T}\mathcal{U})(v) = \mathcal{S}(\mathcal{T}(\mathcal{U}(v))) \quad \text{and} \quad (\mathcal{S}\mathcal{T})\mathcal{U}(v) = \mathcal{S}(\mathcal{T}(\mathcal{U}(v)))$$

and these are identical.

The verifications of the other properties are straightforward. □

We observed in Theorem 4.1.9 that the set of linear transformations between two vector spaces is itself a vector space. Now we observe that Lemma 4.1.11 gives us more examples of linear transformations.

Corollary 4.1.12. (1) *Let $L(U, V)$ be the vector space of linear transformations from the vector space U to the vector space V. Let $\mathcal{T}\colon V \to W$ be any fixed linear* *transformation. Then $\mathcal{P}\colon L(U,V) \to L(U,W)$ by $\mathcal{P}(\mathcal{S}) = \mathcal{T}\mathcal{S}$ is a linear transformation.*

(2) *Let $L(V,W)$ be the vector space of linear transformations from the vector space V to the vector space W. Let $\mathcal{S}\colon U \to V$ be any fixed linear transformation. Then $\mathcal{Q}\colon L(V,W) \to L(U,W)$ by $\mathcal{Q}(\mathcal{T}) = \mathcal{T}\mathcal{S}$ is a linear transformation.*

Proof. Recalling the definition of a linear transformation (Definition 4.1.1), we see that (1) is just properties (2a) and (2b) of Lemma 4.1.11, and (2) is just properties (3a) and (3b) of Lemma 4.1.11. □

4.2. Matrix algebra

In the last section we considered linear transformations in general. But in Chapter 1 we saw that any linear transformation $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^m$ is $\mathcal{T} = \mathcal{T}_A$ for some unique m-by-n matrix A, i.e., that $\mathcal{T}(v) = \mathcal{T}_A(v) = Av$ for every vector v in $\mathbb{F}^n$.

We now combine this fact with the work we did in the last section. This will have two consequences.

First, it will lead us to the correct definition of matrix operations.

Second, it will enable us to conclude the properties of matrix operations with *no* (no means zero, not just a little) additional work.

First, Theorem 1.5.7 *tells us* how we should define matrix addition and scalar multiplication.

Definition 4.2.1. Consider $L(\mathbb{F}^n, \mathbb{F}^m)$. Let $\mathcal{S}$ and $\mathcal{T}$ be elements of $L(\mathbb{F}^n, \mathbb{F}^m)$. Then $\mathcal{U} = \mathcal{S} + \mathcal{T}$ is an element of $L(\mathbb{F}^n, \mathbb{F}^m)$. By Theorem 1.5.7, $\mathcal{S}$ has a standard matrix A, $\mathcal{T}$ has a standard matrix B, and $\mathcal{U}$ has a standard matrix C. We set

$$C = A + B \quad (\text{so that } \mathcal{T}_{A+B} = \mathcal{T}_A + \mathcal{T}_B).$$

Let $\mathcal{T}$ be an element of $L(\mathbb{F}^n, \mathbb{F}^m)$, and let a be a scalar. Then $\mathcal{U} = a\mathcal{T}$ is an element of $L(\mathbb{F}^n, \mathbb{F}^m)$. By Theorem 1.5.7, $\mathcal{T}$ has a standard matrix D and $\mathcal{U}$ has a standard matrix E. We set

$$E = aD \quad \text{so that } \mathcal{T}_{aD} = a\mathcal{T}_D. \qquad \Diamond$$

Now in order to be able to use this definition, we have to be able to calculate $A + B$ and aD. But actually, we already know how to do this. Let us see what the answers are.

Theorem 4.2.2. (1) *Let A and B be m-by-n matrices. Write $A = [u_1|\dots|u_n]$ and $B = [v_1|\dots|v_n]$. Then $C = A + B$ is the m-by-n matrix given by*

$$C = [u_1 + v_1|\dots|u_n + v_n].$$

(1′) *Write $A = (a_{ij})$, $B = (b_{ij})$, and $C = (c_{ij})$. Then $C = A + B$ is the m-by-n matrix given by*

$$c_{ij} = a_{ij} + b_{ij}.$$

(2) *Let D be an m-by-n matrix and let a be a scalar. Write $D = [w_1|\dots|w_n]$. Then $E = aD$ is the m-by-n matrix given by*

$$E = [aw_1|\dots|aw_n].$$

(2′) *Write $D = (d_{ij})$, $E = (e_{ij})$. Then $E = aD$ is the m-by-n matrix given by*

$$e_{ij} = ad_{ij}.$$

Proof. (1) The standard matrix for $\mathcal{S}$ is given by

$$A = [\mathcal{S}(e_1)|\dots|\mathcal{S}(e_n)] \quad \text{so } u_1 = \mathcal{S}(e_1), \dots, u_n = \mathcal{S}(e_n),$$

and the standard matrix for $\mathcal{T}$ is given by

$$B = [\mathcal{T}(e_1)|\dots|\mathcal{T}(e_n)] \quad \text{so } v_1 = \mathcal{T}(e_1), \dots, v_n = \mathcal{T}(e_n).$$

But then the standard matrix for $\mathcal{U}$ is given by

$$\begin{aligned} C &= [\mathcal{U}(e_1)|\dots|\mathcal{U}(e_n)] \\ &= [(\mathcal{S}+\mathcal{T})(e_1)|\dots|(\mathcal{S}+\mathcal{T})(e_n)] \\ &= [\mathcal{S}(e_1)+\mathcal{T}(e_1)|\dots|\mathcal{S}(e_n)+\mathcal{T}(e_n)] \\ &= [u_1+v_1|\dots|u_n+v_n], \end{aligned}$$

as claimed.

(1′) By (1) we see that the entries in each column of C are obtained by adding the corresponding entries of u_i and v_i (as that is how we add vectors) which is just the same thing as saying that every entry of C is obtained by adding the corresponding entries of A and B.

(2) The standard matrix for $\mathcal{T}$ is given by

$$D = [\mathcal{T}(e_1)|\dots|\mathcal{T}(e_n)] \quad \text{so } w_1 = \mathcal{T}(e_1), \dots, w_n = \mathcal{T}(e_n).$$

But then the standard matrix for $\mathcal{U}$ is given by

$$\begin{aligned} E &= [\mathcal{U}(e_1)|\dots|\mathcal{U}(e_n)] \\ &= [(a\mathcal{T})(e_1)|\dots|(a\mathcal{T})(e_n)] \\ &= [a\mathcal{T}(e_1)|\dots|a\mathcal{T}(e_n)] \\ &= [aw_1|\dots|aw_n], \end{aligned}$$

as claimed.

(2′) By (2) we see that the entries in each column of E are obtained by multiplying each of the entries in the corresponding column of D by a (as that is how we take scalar multiples of vectors) which is just the same thing as saying that every entry of E is obtained by multiplying the corresponding entry of D by a. □

Remark 4.2.3. You might ask: matrix addition and scalar multiplication are obvious and easy, just do them entry-by-entry. So why didn't we just define them that way? The answer is that just because something is "obvious" and "easy" doesn't mean it's right. For example, the "obvious" and "easy" way to define matrix multiplication would also by entry-by-entry, and that's completely wrong.

So the way we should regard the situation is that we thought carefully about what matrix addition and scalar multiplication should be, and came up with the right answer. Then the fact that it's easy is just a bonus! ◊

Next, Theorem 4.1.10 *tells us* how we should define matrix multiplication.

Definition 4.2.4. Let $\mathcal{S}\colon \mathbb{F}^n \to \mathbb{F}^m$ and $\mathcal{T}\colon \mathbb{F}^m \to \mathbb{F}^p$ be linear transformations. Let $\mathcal{U} = \mathcal{T}\mathcal{S}$ be the composition of $\mathcal{T}$ and $\mathcal{S}$. By Theorem 1.5.7, $\mathcal{S}$ has a standard matrix B, and $\mathcal{T}$ has a standard matrix A. By Theorem 4.1.10, $\mathcal{U}$ is a linear transformation, so $\mathcal{U}$ has a standard matrix C. We set

$$C = AB \quad (\text{so that } \mathcal{T}_{AB} = \mathcal{T}_A\mathcal{T}_B). \qquad \diamondsuit$$

Again our first job is to calculate C.

Theorem 4.2.5. *Let A be a p-by-m matrix, and let B be an m-by-n matrix. Write $B = [u_1|\dots|u_n]$. Then $C = AB$ is the p-by-n matrix given by*

$$C = [Au_1|\dots|Au_n].$$

Proof. The standard matrix for $\mathcal{S}$ is given by

$$B = [\mathcal{S}(e_1)|\dots|\mathcal{S}(e_n)] \quad \text{so } u_1 = \mathcal{S}(e_1), \dots, u_n = \mathcal{S}(e_n).$$

To say that the standard matrix for $\mathcal{T}$ is A is to say that

$$\mathcal{T}(v) = Av \quad \text{for every } v.$$

Then the standard matrix for $\mathcal{U}$ is given by

$$\begin{aligned} C &= [\mathcal{U}(e_1)|\dots|\mathcal{U}(e_n)] \\ &= [(\mathcal{T}\mathcal{S})(e_1)|\dots|(\mathcal{T}\mathcal{S})(e_n)] \\ &= [\mathcal{T}(\mathcal{S}(e_1))|\dots|\mathcal{T}(\mathcal{S}(e_n))] \\ &= [\mathcal{T}(u_1)|\dots|\mathcal{T}(u_n)] \\ &= [Au_1|\dots|Au_n], \end{aligned}$$

as claimed. □

Remark 4.2.6. Note how this lemma gives a clear and direct formula for AB. This is without a doubt the best way to understand matrix multiplication. But, as we are about to see, the formula in terms of matrix entries is more complicated. ♢

Corollary 4.2.7. *Let $A = (a_{ij})$ be a p-by-m matrix, and let $B = (b_{ij})$ be an m-by-n matrix. Then $C = AB$ is the p-by-n matrix $C = (c_{ij})$ defined by*

$$c_{ij} = \sum_{k=1}^{m} a_{ik}b_{kj} \quad \text{for each } i = 1, \dots p,\ j = 1, \dots, n.$$

Proof. Write $C = [w_1|\dots|w_n]$. Then $w_j = Au_j$. Now

$$w_j = \begin{bmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{pj} \end{bmatrix}, \quad A = (c_{ij}), \quad \text{and} \quad u_j = \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{mj} \end{bmatrix}.$$

But then by the definition of the product Au_j (Definition 1.3.8),

$$\begin{bmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{pj} \end{bmatrix} = \begin{bmatrix} a_{11}b_{1j} + a_{12}b_{2j} + \dots + a_{1m}b_{mj} \\ a_{21}b_{1j} + a_{22}b_{2j} + \dots + a_{2m}b_{mj} \\ \vdots \\ a_{p1}b_{1j} + a_{p2}b_{2j} + \dots + a_{pm}b_{mj} \end{bmatrix}$$

so

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{im}b_{mj} = \sum_{k=1}^{m} a_{ik}b_{kj}$$

as claimed. $\square$

Example 4.2.8. We wish to compute the product

$$\begin{bmatrix} 2 & 1 & 7 \\ 3 & 0 & 5 \end{bmatrix} \begin{bmatrix} 3 & 1 & 2 & 0 \\ -1 & 6 & -5 & 4 \\ 0 & 1 & 9 & 3 \end{bmatrix}.$$

For the first column, we compute, as in Definition 1.3.8 and Example 1.3.9,

$$\begin{bmatrix} 2 & 1 & 7 \\ 3 & 0 & 5 \end{bmatrix} \begin{bmatrix} 3 \\ -1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \cdot 3 + 1 \cdot (-1) + 7 \cdot 0 \\ 3 \cdot 3 + 0 \cdot (-1) + 5 \cdot 0 \end{bmatrix} = \begin{bmatrix} 5 \\ 9 \end{bmatrix}.$$

For the second column, we compute

$$\begin{bmatrix} 2 & 1 & 7 \\ 3 & 0 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ 6 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \cdot 1 + 1 \cdot 6 + 7 \cdot 1 \\ 3 \cdot 1 + 0 \cdot 6 + 5 \cdot 1 \end{bmatrix} = \begin{bmatrix} 15 \\ 8 \end{bmatrix}.$$

For the third column, we compute

$$\begin{bmatrix} 2 & 1 & 7 \\ 3 & 0 & 5 \end{bmatrix} \begin{bmatrix} 2 \\ -5 \\ 9 \end{bmatrix} = \begin{bmatrix} 2 \cdot 2 + 1 \cdot (-5) + 7 \cdot 9 \\ 3 \cdot 2 + 0 \cdot (-5) + 5 \cdot 9 \end{bmatrix} = \begin{bmatrix} 62 \\ 51 \end{bmatrix}.$$

For the fourth column, we compute

$$\begin{bmatrix} 2 & 1 & 7 \\ 3 & 0 & 5 \end{bmatrix} \begin{bmatrix} 0 \\ 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 2 \cdot 0 + 1 \cdot 4 + 7 \cdot 3 \\ 3 \cdot 0 + 0 \cdot 4 + 5 \cdot 3 \end{bmatrix} = \begin{bmatrix} 25 \\ 15 \end{bmatrix}.$$

And so we find

$$\begin{bmatrix} 2 & 1 & 7 \\ 3 & 0 & 5 \end{bmatrix} \begin{bmatrix} 3 & 1 & 2 & 0 \\ -1 & 6 & -5 & 4 \\ 0 & 1 & 9 & 3 \end{bmatrix} = \begin{bmatrix} 5 & 15 & 62 & 25 \\ 9 & 8 & 51 & 15 \end{bmatrix}.$$ $\Diamond$

Remark 4.2.9. Our discussion has been "biased" in terms of columns as $\mathbb{F}^m$, $\mathbb{F}^n$, and $\mathbb{F}^p$ consist of column vectors. But once we have the formula in Corollary 3.5.7, we can work in terms of rows. To be precise, let $B = (b_{ij})$ be an m-by-n matrix over $\mathbb{F}$, and let $v = [d_1 \ \ d_2 \ \ \ldots \ \ d_m]$ be a vector in ${}^t\mathbb{F}^m$. Then vA is the vector in ${}^t\mathbb{F}^n$ given by

$$vA = \big[b_{11}d_1 + b_{21}d_2 + \cdots + b_{m1}d_m \quad b_{12}d_1 + b_{22}d_2 + \cdots + b_{m2}d_m \\ \ldots \quad b_{1n}d_1 + b_{2n}d_2 + \cdots + b_{mn}d_m\big].$$

(Compare Definition 1.3.8, note how the subscripts are different, and observe this rule is "stand the vector v up on its base, multiply corresponding entries and add".)

Then, breaking up our matrices by rows rather than columns, if

$$A = \begin{bmatrix} v_1 \\ \hline v_2 \\ \hline \vdots \\ \hline v_p \end{bmatrix}, \text{ then } C = AB \text{ is given by } C = \begin{bmatrix} v_1 B \\ \hline v_2 B \\ \hline \vdots \\ \hline v_p B \end{bmatrix}. \qquad \Diamond$$

We now list many properties of matrix arithmetic. They all follow either from the fact that linear transformations form a vector space (Theorem 4.1.9) or by Lemma 4.1.11.

We assume that all matrix operations make sense.

Lemma 4.2.10. (1) *Under the operations of matrix addition and scalar multiplication, $M_{m,n}(\mathbb{F})$, the set of m-by-n matrices with entries in $\mathbb{F}$, is an $\mathbb{F}$-vector space.*

(2) *Let A, B, and C be matrices. Let a and b be scalars. Let 0 be the 0 matrix, and if $A = (a_{ij})$ let $-A = (-a_{ij})$. Then:*

(1) $A + B = B + A$.
(2) $(A + B) + C = A + (B + C)$.
(3) $0 + A = A + 0 = A$.
(4) $A + (-A) = (-A) + A = 0$.
(5) $a(A + B) = aA + aB$.
(6) $(a + b)A = aA + bA$.
(7) $a(bA) = (ab)A$.
(8) $1A = A$.
(9) $0A = 0$.
(10) $a0 = 0$.
(11) $(-1)A = -A$.
(12) $A(BC) = (AB)C$.
(13) $(A + B)C = AC + BC$.
(14) $(aA)B = a(AB)$.
(15) $A(B + C) = AB + AC$.
(16) $A(aB) = a(AB)$.
(17) $A0 = 0$, $0A = 0$.
(18) $IA = A$, $AI = A$.

Proof. These are all just translations of properties of linear transformations into matrix language.

We do (12) explicitly. Let $\mathcal{S}$ have standard matrix A, $\mathcal{T}$ have standard matrix B, and $\mathcal{U}$ have standard matrix C. Then by Lemma 4.1.11(1)

$$\mathcal{T}_A(\mathcal{T}_B\mathcal{T}_C) = (\mathcal{T}_A\mathcal{T}_B)\mathcal{T}_C.$$

But now, by the very definition of matrix multiplication, $\mathcal{T}_B\mathcal{T}_C = \mathcal{T}_{BC}$ and $\mathcal{T}_A\mathcal{T}_B = \mathcal{T}_{AB}$, so this equation becomes

$$\mathcal{T}_A\mathcal{T}_{BC} = \mathcal{T}_{AB}\mathcal{T}_C$$

and again by the very definition of matrix multiplication this becomes

$$\mathcal{T}_{A(BC)} = \mathcal{T}_{(AB)C}$$

and so

$$A(BC) = (AB)C.$$

The other properties are all simple to verify. □

Remark 4.2.11. Except for (12), it is easy to prove all of these properties simply by computing with matrices directly. But trying to prove (12) from the formula for matrix multiplication is a complicated and completely unenlightening computation that gives no idea why this should be true. ◊

Corollary 4.2.12. (1) *Let B be a fixed p-by-n matrix. Then $\mathcal{P}\colon M_{n,m}(\mathbb{F}) \to M_{p,m}(\mathbb{F})$ by $\mathcal{P}(A) = BA$ is a linear transformation.*

(2) *Let A be a fixed n-by-m matrix. Then $\mathcal{Q}\colon M_{p,n}(\mathbb{F}) \to M_{p,m}(\mathbb{F})$ by $\mathcal{Q}(B) = BA$ is a linear transformation.*

Proof. This is just a translation of Corollary 4.1.12 into matrix language. □

4.3. Linear transformations II

We now continue our study of linear transformations. We begin by seeing how bases are involved, then return to the general study, and finally reinvolve bases.

We culminate in a result of the highest importance: any two vector spaces of the same finite dimension are "isomorphic", and of different finite dimensions are not. Of course, we have to define this word, and we will, but suffice it to say right now that this means they are equivalent as vector spaces.

We have the following general result.

Theorem 4.3.1. *Let V be a vector space, and let $B = \{v_1, v_2, \dots\}$ be a basis of V. Let W be a vector space, and let $\{w_1, w_2, \dots\}$ be arbitrary vectors in W. Then there is a unique linear transformation $\mathcal{T}\colon V \to W$ with $\mathcal{T}(v_i) = w_i$. This linear transformation is given by the formula*

$$\mathcal{T}\left(\sum c_i v_i\right) = \sum c_i w_i.$$

Proof. First let us see that this formula defines a function from V to W. Let v be any vector in V. Then, since B is a basis, we may write v uniquely as $v = \sum c_i v_i$ (Lemma 3.3.3), and then $\mathcal{T}(v) = \sum c_i v_i$ defines $\mathcal{T}(v)$.

It is straightforward to check that $\mathcal{T}$ defined in this way is a linear transformation.

Now suppose $\mathcal{T}'$ is any linear transformation with $\mathcal{T}'(v_i) = w_i$. Then by linearity, $\mathcal{T}'(v) = \mathcal{T}'(\sum c_i v_i) = \sum c_i \mathcal{T}'(v_i) = \sum c_i w_i = \mathcal{T}(v)$. Since this is true for every $v \in V$, $\mathcal{T}' = \mathcal{T}$ and $\mathcal{T}$ is unique. □

Remark 4.3.2. Let us emphasize two things the theorem says.

First of all, we may choose the vectors w_i arbitrarily, so there is no restriction on the values of $\mathcal{T}(v_i)$.

Second, it says that if two linear transformations agree on a basis of V, they are identical. For if we have any two linear transformations $\mathcal{T}_1$ and $\mathcal{T}_2$ with $\mathcal{T}_1(v_i) = \mathcal{T}_2(v_i)$ for each i, then $\mathcal{T}_1(\sum c_i v_i) = \sum c_i \mathcal{T}_1(v_i) = \sum c_i \mathcal{T}_2(v_i) = \mathcal{T}_2(\sum c_i v_i)$ so $\mathcal{T}_1 = \mathcal{T}_2$.

We view the first part of this remark as giving us a way to construct linear transformations: just pick any vectors w_i and we get a linear transformation $\mathcal{T}$.

We view the second part of this remark as giving us a way to show that two linear transformations are the same: just check that they agree on the vectors in a basis of V. $\Diamond$

We now describe some general properties of linear transformations. But first we have a helpful lemma.

Lemma 4.3.3. *Let $\mathcal{T}\colon V \to W$ be a linear transformation. The following are equivalent*:

(1) *The only vector v in V with $\mathcal{T}(v) = 0$ is $v = 0$.*

(2) *If w is any vector in W and v_1 and v_2 are vectors in V with $\mathcal{T}(v_1) = \mathcal{T}(v_2) = w$, then $v_1 = v_2$.*

Proof. We know that $\mathcal{T}(0) = 0$. If (2) is true for every w in W, then it is certainly true for $w = 0$, and in that case it says that if v is any vector in V with $\mathcal{T}(v) = \mathcal{T}(0) = 0$, then $v = 0$, which is (1).

On the other hand, suppose (2) is false for some vector w_0 in W. Then there are vectors $v_1 \neq v_2$ in V with $\mathcal{T}(v_1) = \mathcal{T}(v_2) = w$. But then, by the linearity of $\mathcal{T}$, $\mathcal{T}(v_1 - v_2) = \mathcal{T}(v_1) - \mathcal{T}(v_2) = w_0 - w_0 = 0$, so $v_1 - v_2$ is a nonzero vector in V with $\mathcal{T}(v_1 - v_2) = 0$, and (1) is false. $\square$

Now we introduce some standard language.

Definition 4.3.4. Let $\mathcal{T}\colon V \to W$ be a linear transformation. Then:

(1) $\mathcal{T}$ is 1-1 if $\mathcal{T}(v_1) \neq \mathcal{T}(v_2)$ whenever $v_1 \neq v_2$.

(2) $\mathcal{T}$ is onto if for every $w \in W$ there is a $v \in V$ with $\mathcal{T}(v) = w$. $\Diamond$

Corollary 4.3.5. *$\mathcal{T}$ is* 1-1 *if and only if the only vector v with $\mathcal{T}(v) = 0$ is $v = 0$.*

Proof. This is just Lemma 4.3.3 combined with Definition 4.3.4. $\square$

A 1-1 linear transformation is often called a *monomorphism* and an onto linear transformation is often called an *epimorphism*. (It would be proper to call a general linear transformation a *homomorphism*, and that term is in use in mathematics, but it is not often used in linear algebra.) A linear transformation $\mathcal{T}$ that has an inverse as a linear transformation is called *invertible*, or an *isomorphism*.

Before proceeding any further, let us give a very simple, but very useful, example of an isomorphism.

Example 4.3.6. Let $\mathcal{T}\colon \mathbb{F}^n \to {}^t\mathbb{F}^n$ be the linear transformation

$$\mathcal{T}\left(\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}\right) = [a_1 \ \ldots \ a_n].$$

This has inverse $\mathcal{T}^{-1}\colon {}^t\mathbb{F}^n \to \mathbb{F}^n$ given by

$$\mathcal{T}^{-1}([a_1 \ \ldots \ a_n]) = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

Both $\mathcal{T}$ and $\mathcal{T}^{-1}$ are called the *transpose*. We write $\mathcal{T}(v) = {}^t v$ and also $\mathcal{T}^{-1}(v) = {}^t v$. (Thus, for example, ${}^t\begin{bmatrix} 1 \\ 0 \end{bmatrix} = [1 \ \ 0]$ and ${}^t[0 \ \ 1] = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.)

We should warn the reader that the mathematical world is divided. Some mathematicians denote the transpose of a vector v by ${}^t v$, as we do, but others denote it by v^t. ◊

Now let us consider a linear transformation $\mathcal{T}\colon V \to W$. As usual, there are two questions we can ask:

(1) Is $\mathcal{T}$ 1-1?

(2) Is $\mathcal{T}$ onto?

As usual, these are in general two completely independent questions, with completely independent answers. Let us use bases to develop a criterion for each of the answers to be yes.

Lemma 4.3.7. *Let $\mathcal{T}\colon V \to W$ be a linear transformation. Let $\mathcal{B} = \{v_1, v_2, \ldots\}$ be a basis of V.*

Write $w_1 = \mathcal{T}(v_1)$, $w_2 = \mathcal{T}(v_2)$, $\ldots$, and let $\mathcal{C} = \{w_1, w_2, \ldots\}$, a subset of W.

(1) *$\mathcal{T}$ is 1-1 if and only if the set $\mathcal{C}$ is linearly independent.*

(2) *$\mathcal{T}$ is onto if and only if the set C spans W.*

Proof. (1) To decide whether $\mathcal{T}$ is 1-1, we use Corollary 4.3.5. First suppose $\mathcal{T}$ is 1-1. Consider a linear combination $\sum c_i w_i$. Then

$$0 = \sum c_i w_i = \sum c_i \mathcal{T}(v_i) = \mathcal{T}\left(\sum c_i v_i\right).$$

But $\mathcal{T}$ is 1-1, so $\sum c_i v_i = 0$. But $\mathcal{B}$ is a basis, so $\mathcal{B}$ is linearly independent, and hence each $c_i = 0$. But that means $\mathcal{C}$ is linearly independent.

On the other hand, suppose $\mathcal{T}$ is not 1-1. Then there is some $v \neq 0$ with $\mathcal{T}(v) = 0$. Since $\mathcal{B}$ is a basis, $\mathcal{B}$ spans V, so we may write $v = \sum c_i v_i$ for some c_i, and since $v \neq 0$, not all $c_i = 0$. But then

$$0 = \mathcal{T}(v) = \mathcal{T}\left(\sum c_i v_i\right) = \sum c_i \mathcal{T}(v_i) = \sum c_i w_i$$

and $\mathcal{C}$ is not linearly independent.

(2) First suppose $\mathcal{T}$ is onto. Let w be any vector in W. Then $w = \mathcal{T}(v)$ for some vector $v \in V$. Since $\mathcal{B}$ is a basis, we may write $v = \sum c_i v_i$ for some c_i. But then

$$w = \mathcal{T}(v) = \mathcal{T}\left(\sum c_i v_i\right) = \sum c_i \mathcal{T}(v_i) = \sum c_i w_i$$

and so $\mathcal{C}$ spans W.

On the other hand, suppose $\mathcal{T}$ is not onto. Then there is some w in W for which $w \neq \mathcal{T}(v)$ for any $v \in V$. Suppose $\mathcal{C}$ spanned W. Then we could write $w = \sum c_i w_i$ for some c_i. But then, if we set $v = \sum c_i v_i$, we would have

$$\mathcal{T}(v) = \mathcal{T}\left(\sum c_i v_i\right) = \sum c_i \mathcal{T}(v_i) = \sum c_i w_i = w,$$

which is impossible. □

In the situation of the lemma, we will simply write $\mathcal{C} = \mathcal{T}(\mathcal{B})$ for short.

Let us draw several consequences from this.

Corollary 4.3.8. (1) *Let V have finite dimension n, and let W have dimension m, with $m > n$ or $m = \infty$. Then no linear transformation $\mathcal{T}\colon V \to W$ can be onto.*

(2) *Let V have finite dimension n, and let W have dimension $m < n$, or let V have dimension $n = \infty$ and let W have finite dimension m. Then no linear transformation $\mathcal{T}\colon V \to W$ can be* 1-1.

Proof. Choose a basis $\mathcal{B}$ of V and let $\mathcal{C} = \mathcal{T}(\mathcal{B})$.

(1) By Lemma 4.3.7(1), if $\mathcal{T}$ were onto we would have W spanned by $\mathcal{C}$, a set of $n < m$ vectors, which is impossible.

(2) By Lemma 4.3.7(2), if $\mathcal{T}$ were 1-1 we would have a linearly independent set $\mathcal{C}$ of $n > m$ vectors in W, which is impossible. □

Recall that in general a function $f\colon X \to Y$ is invertible if there is a function $g\colon Y \to X$ such that the compositions $gf\colon X \to X$ and $fg\colon Y \to Y$ are both the respective identity functions, i.e., $g(f(x)) = x$ for every x in X and $f(g(y)) = y$ for every $y \in Y$. In this case we say g is the inverse of f, and reciprocally that f is the inverse of g, and write $g = f^{-1}$, $f = g^{-1}$.

Recall in addition that a function $f\colon X \to Y$ is invertible if and only if it is 1-1 and onto. If that is the case, $g = f^{-1}$ is the function defined as follows. Since f is 1-1 and onto, for every $y \in Y$ there is exactly one $x \in X$ with $f(x) = y$. Then $g(y) = x$.

There is a subtle point. Suppose that $\mathcal{T}\colon V \to W$ is a linear transformation that is both 1-1 and onto. Then in particular it is a function that is both 1-1 and onto. That means that $\mathcal{T}$ has an inverse $\mathcal{T}^{-1}\colon W \to V$ *as a function*. That does not automatically mean that $\mathcal{T}$ has an inverse *as a linear* transformation. But that is indeed the case.

Lemma 4.3.9. *Let $\mathcal{T}\colon V \to W$ be a linear transformation that is both* 1-1 *and onto. Then $\mathcal{T}^{-1}\colon W \to V$ is a linear transformation.*

Proof. We must show properties (1) and (2) of Definition 3.3.1.

(1) Suppose $\mathcal{T}^{-1}(w_1) = v_1$ and $\mathcal{T}^{-1}(w_2) = v_2$. Then $\mathcal{T}(v_1) = w_1$ and $\mathcal{T}(v_2) = w_2$. Since $\mathcal{T}$ is linear, $\mathcal{T}(v_1+v_2) = \mathcal{T}(v_1)+\mathcal{T}(v_2) = w_1+w_2$. Thus $\mathcal{T}^{-1}(w_1+w_2) = v_1 + v_2 = \mathcal{T}^{-1}(w_1) + \mathcal{T}^{-1}(w_2)$.

(2) Suppose $\mathcal{T}^{-1}(w) = v$. Then $\mathcal{T}(v) = w$. Since $\mathcal{T}$ is linear, $\mathcal{T}(cv) = c\mathcal{T}(v) = cw$. Thus $\mathcal{T}^{-1}(cw) = cv = c\mathcal{T}^{-1}(w)$. □

Corollary 4.3.10. *Let $\mathcal{T}\colon V \to W$ be a* 1-1 *and onto linear transformation. Then $\mathcal{T}$ is an isomorphism.*

Proof. Since $\mathcal{T}$ is 1-1 and onto, $\mathcal{T}$ has an inverse as a function, and hence as a linear transformation by Lemma 4.3.9. □

We have the following criterion for a linear transformation to be an isomorphism.

Corollary 4.3.11. *Let $\mathcal{T}\colon V \to W$ be a linear transformation. Let $\mathcal{B}$ be a basis of V, and let $\mathcal{C} = \mathcal{T}(\mathcal{B})$. Then $\mathcal{T}$ is an isomorphism if and only if $\mathcal{C}$ is a basis of W.*

Proof. $\mathcal{C}$ is a basis of W if and only if $\mathcal{C}$ is linearly independent and spans W, so putting conclusions (1) and (2) of Lemma 4.3.7 together, we see that $\mathcal{T}$ is 1-1 and onto if and only if $\mathcal{C}$ is a basis of W. But in that case $\mathcal{T}$ is an isomorphism by Corollary 4.3.10. □

In this situation we have the following expression for the inverse of $\mathcal{T}$.

Lemma 4.3.12. *Let $\mathcal{T}\colon V \to W$ be an isomorphism. Let $\mathcal{B} = \{v_1, v_2, \dots\}$ be a basis of V, let $w_i = \mathcal{T}(v_i)$, and let $\mathcal{C} = \{w_1, w_2, \dots\}$, a basis of W. Let $\mathcal{S}$ be the unique linear transformation $\mathcal{S}\colon W \to V$ given by $\mathcal{S}(w_i) = v_i$. Then $\mathcal{S} = \mathcal{T}^{-1}$.*

Proof. First, since $\mathcal{T}$ is an isomorphism, we know that $\mathcal{C}$ is indeed a basis of W, by Corollary 4.3.11. Second, since $\mathcal{C}$ is a basis of W, we know that there is a unique such linear transformation $\mathcal{S}$, by Theorem 4.3.1.

Note then that for any $v_i \in \mathcal{B}$, $(\mathcal{S}\mathcal{T})(v_i) = \mathcal{S}(\mathcal{T}(v_i)) = \mathcal{S}(w_i) = v_i = \mathcal{I}(v_i)$ so $\mathcal{S}\mathcal{T}$ agrees with $\mathcal{I}$ on the basis $\mathcal{B}$ of V, and hence $\mathcal{S}\mathcal{T} = \mathcal{I}$ by Remark 4.3.2. Similarly, for any $w_i \in \mathcal{C}$, $(\mathcal{T}\mathcal{S})(w_i) = \mathcal{T}(\mathcal{S}(w_i)) = \mathcal{T}(v_i) = w_i = \mathcal{I}(w_i)$, so $\mathcal{T}\mathcal{S}$ agrees with $\mathcal{I}$ on the basis $\mathcal{C}$ of W, and hence $\mathcal{T}\mathcal{S} = \mathcal{I}$ by Remark 4.3.2.

Hence $\mathcal{S} = \mathcal{T}^{-1}$. □

Lemma 4.3.13. *Let $\mathcal{S}$ and $\mathcal{T}$ be isomorphisms. Then their composition $\mathcal{S}\mathcal{T}$ is an isomorphism, and $(\mathcal{S}\mathcal{T})^{-1} = \mathcal{T}^{-1}\mathcal{S}^{-1}$.*

Proof. To say that $\mathcal{S}\mathcal{T}$ is an isomorphism is to say it is invertible, and this lemma gives a formula for the inverse. So we just need to check that this formula is correct. We see

$$(\mathcal{S}\mathcal{T})(\mathcal{T}^{-1}\mathcal{S}^{-1}) = \mathcal{S}(\mathcal{T}\mathcal{T}^{-1})\mathcal{S}^{-1} = \mathcal{S}\mathcal{I}\mathcal{S}^{-1} = \mathcal{S}\mathcal{S}^{-1} = \mathcal{I}$$

and

$$(\mathcal{T}^{-1}\mathcal{S}^{-1})(\mathcal{S}\mathcal{T}) = \mathcal{T}^{-1}(\mathcal{S}^{-1}\mathcal{S})\mathcal{T} = \mathcal{T}^{-1}\mathcal{I}\mathcal{T} = \mathcal{T}^{-1}\mathcal{T} = \mathcal{I}$$

as claimed. □

Definition 4.3.14. Let V and W be vector spaces. If there is an isomorphism $\mathcal{T}\colon V \to W$, then V and W are *isomorphic.* $\Diamond$

Corollary 4.3.15. (1) *Let V and W both be vector spaces of finite dimension n. Then V and W are isomorphic. In particular, any vector space of finite dimension n is isomorphic to $\mathbb{F}^n$.*

(2) *Let V and W be vector spaces with V having finite dimension n, and with W having either finite dimension $m \neq n$ or W having infinite dimension. Then V and W are not isomorphic.*

Proof. (1) Let $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ and $\mathcal{C} = \{w_1, w_2, \ldots, w_n\}$ be bases for V and W, respectively. Then by Theorem 4.3.1 there is a linear transformation $\mathcal{T}\colon V \to W$ defined by $\mathcal{T}(v_i) = w_i$, and by Corollary 4.3.11 $\mathcal{T}$ is an isomorphism.

(2) Let $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ be a basis for V and suppose that there was an isomorphism $\mathcal{T}\colon V \to W$. Then $\mathcal{C} = \{\mathcal{T}(v_1), \mathcal{T}(v_2), \ldots, \mathcal{T}(v_n)\}$ would be a basis of W, in which case W would have dimension n. But by hypothesis it does not. $\square$

Remark 4.3.16. This is a very important result and also an illustration of how we can often reduce linear algebra problems to counting. We ask whether two vector spaces V and W are isomorphic, a priori a difficult question. But in fact, as long as at least one of the vector spaces is finite dimensional, it's easy. Just count dimensions. If V and W have the same dimension the answer is yes; if not, the answer is no. $\Diamond$

Remark 4.3.17. An isomorphism $\mathcal{T}\colon V \to W$ gives a way of pairing elements of V with elements of W by pairing the element v of V with the element $w = \mathcal{T}(v)$ of W, or equivalently by pairing the element w of W with the element $v = \mathcal{T}^{-1}(w)$ of V. Then, given this pairing, V and W have all the same properties as vector spaces. We often think of $\mathcal{T}$ as identifying elements of V with elements of W. But it is *very important* to be careful here.

To say that V and W are isomorphic is to say that elements of V and elements of W can be identified by some linear transformation $\mathcal{T}$. But it is rarely the case that there is a "canonical" (or natural) way to identify elements of V with elements of W. The identification *depends on* the choice of $\mathcal{T}$, and different choices of $\mathcal{T}$ will yield different identifications. $\Diamond$

Remark 4.3.18. We have said that V and W have the same properties as vector spaces. This means that we can often "translate" questions in V to questions in W. This can be quite useful. For example, any n-dimensional vector space V is isomorphic to $\mathbb{F}^n$. Thus we can reduce computations in V to computations in $\mathbb{F}^n$, where we have effective tools to do them, for example by the use of matrices.

But again, we want to emphasize that isomorphic vector spaces V and W are just that, isomorphic, which is *not* to say they are the same. $\Diamond$

Now we prove a result we "owe" the reader from Theorem 3.4.24. In fact, we prove something more precise.

Theorem 4.3.19. *Let V be a vector space, and let W be a subspace of V. Then all complements of W are mutually isomorphic (and hence all have the same dimension). More precisely, any complement U of W is isomorphic to the quotient vector space V/W.*

Proof. If all complements of W are isomorphic to the same vector space V/W, they are isomorphic to each other, so the second conclusion implies the first. But for the sake of simplicity, we will present a direct proof of the first conclusion.

Let U and U' be complements of W, so that $V = W \oplus U = W \oplus U'$. Let $u \in U$. Then $u = w + u'$ for some unique $w \in W$ and $u' \in U'$. Define $\mathcal{T}\colon U \to U'$ by $\mathcal{T}(u) = u'$. We check that $\mathcal{T}$ is a linear transformation:

(1) If $u_1 = w_1 + u_1'$ and $u_2 = w_2 + u_2'$, then $u_1 + u_2 = (w_1 + w_2) + (u_1' + u_2')$. If $w_1, w_2 \in W$, then $w_1 + w_2 \in W$, as W is a subspace, and if $u_1', u_2' \in U'$, then $u_1' + u_2' \in U'$ as U' is a subspace. But then we see

$$\mathcal{T}(u_1 + u_2) = u_1' + u_2' = \mathcal{T}(u_1) + \mathcal{T}(u_2).$$

(2) If $u = w + u'$, then $cu = c(w + u') = cw + cu'$. Again if $w \in W$, then $cw \in W$, and if $u' \in U'$, then $cu' \in U'$, because both are subspaces. But then we see

$$\mathcal{T}(cu) = cu' = c\mathcal{T}(u).$$

Similarly, if $u' \in U'$, then $u' = w' + u$ for some unique $w' \in W$ and $u \in U$, and we define $\mathcal{S}\colon U' \to U$ by $\mathcal{S}(u') = u$. By the same logic, $\mathcal{S}$ is a linear transformation.

We claim that $\mathcal{S} = \mathcal{T}^{-1}$, so in particular $\mathcal{T}$ is invertible, i.e., $\mathcal{T}$ is an isomorphism, and so U and U' are isomorphic.

Let $u_0 \in U$. If $u_0 = w_0 + u_0'$, then $u_0' = \mathcal{T}(u_0) = u_0 - w_0$. If $u_0' = u_0 + w_0'$, then $u_0 = \mathcal{S}(u_0') = u_0' - w_0'$. But $u_0 - w_0 = u_0' = u_0 + w_0'$ gives $w_0' = -w_0$. Then $\mathcal{S}(\mathcal{T}(u_0)) = \mathcal{S}(u_0') = u_0' - w_0' = u_0' + w_0 = u_0$ so $\mathcal{S}\mathcal{T} = \mathcal{I}$. Similarly $\mathcal{T}\mathcal{S} = \mathcal{I}$.

This proves the first conclusion. Now we prove the second.

Let U be any complement of W. Let $\overline{\mathcal{T}}$ be the linear transformation $\overline{\mathcal{T}}\colon U \to V/W$ defined by

$$\overline{\mathcal{T}}(u) = u + W.$$

We claim $\overline{\mathcal{T}}$ is an isomorphism. To show this we must first show that $\overline{\mathcal{T}}$ is a linear transformation, and then show that it is 1-1 and onto.

To show that $\overline{\mathcal{T}}$ is a linear transformation we must show that:

(1) $\overline{\mathcal{T}}(u_1 + u_2) = \overline{\mathcal{T}}(u_1) + \overline{\mathcal{T}}(u_2)$. Now $\overline{\mathcal{T}}(u_1 + u_2) = (u_1 + u_2) + W$ while $\overline{\mathcal{T}}(u_1) = u_1 + W$ and $\overline{\mathcal{T}}(u_2) = u_2 + W$. But

$$(u_1 + W) + (u_2 + W) = (u_1 + u_2) + W$$

by definition of vector addition in V/W (Theorem 3.5.15).

(2) $\overline{\mathcal{T}}(cu) = c\overline{\mathcal{T}}(u)$. Now $\overline{\mathcal{T}}(cu) = (cu) + W$ while $c\overline{\mathcal{T}}(u) = c(u + W)$. But

$$c(u + W) = (cu) + W$$

by the definition of scalar multiplication in V/W (Theorem 3.5.15).

Now we show $\overline{\mathcal{T}}$ is 1-1. To do this, we show that $\overline{\mathcal{T}}(u) = 0$ implies $u = 0$. Thus suppose $\overline{\mathcal{T}}(u) = 0$. We recall that the 0 element of V/W is $0+W$ (Theorem 3.5.15), and we also recall that $0 + W = W$, so this is the equation

$$\overline{\mathcal{T}}(u) = u + W = 0 + W = W,$$

so $u \in W$. But $U \cap W = \{0\}$, so $u = 0$.

Next we show $\overline{\mathcal{T}}$ is onto. Choose any arbitrary element $v + W$ of V/W. Then $v = u + w$ for some element u of U, and then

$$\overline{\mathcal{T}}(u) = u+W = ((u+w)+(-w))+W = (u+w)+((-w)+W) = (u+w)+W = v+W$$

(since if $w \in W$, then $-w \in W$, and then $(-w) + W = W$ by Lemma 3.5.7).

Thus $\overline{\mathcal{T}}$ is both 1-1 and onto, and hence an isomorphism. $\square$

Here is a very important example.

Example 4.3.20. Let $W = L(\mathbb{F}^n, \mathbb{F}^m)$ be the vector space of linear transformations from $\mathbb{F}^n$ to $\mathbb{F}^m$. Let $V = M_{m,n}(\mathbb{F})$ be the vector space of m-by-n matrices with entries in $\mathbb{F}$. Then V and W are isomorphic, and $\dim V = \dim W = mn$.

An isomorphism $\mathcal{M} \colon V \to W$ is given by the formula

$$\mathcal{M}(A) = \mathcal{T}_A.$$

Let us see that it is an isomorphism. It is certainly 1-1 and onto: that is just the statement that every linear transformation $\mathcal{T} \colon \mathbb{F}^n \to \mathbb{F}^m$ is $\mathcal{T} = \mathcal{T}_A$ for a unique m-by-n matrix A (Theorem 1.5.7).

What remains to be seen is that $\mathcal{M}$ is a linear transformation.

As usual, we must verify the two properties of a linear transformation (Definition 4.1.1(1) and (2)):

(1) Let A and B be two matrices. Then $\mathcal{M}(A) = \mathcal{T}_A$ and $\mathcal{M}(B) = \mathcal{T}_B$. Also, $\mathcal{M}(A + B) = \mathcal{T}_{A+B}$. But we *defined* addition of matrices by the formula $\mathcal{T}_{A+B} = \mathcal{T}_A + \mathcal{T}_B$ (Definition 4.2.1). Putting these together,

$$\mathcal{M}(A + B) = \mathcal{T}_{A+B} = \mathcal{T}_A + \mathcal{T}_B = \mathcal{M}(A) + \mathcal{M}(B).$$

(2) Let D be a matrix, and let a be a scalar. Then $\mathcal{M}(D) = \mathcal{T}_D$. Also, $\mathcal{M}(aD) = \mathcal{T}_{aD}$. But we *defined* scalar multiplication of matrices by the formula $\mathcal{T}_{aD} = a\mathcal{T}_D$ (Definition 4.2.1). Putting these together,

$$\mathcal{M}(aD) = \mathcal{T}_{aD} = a\mathcal{T}_D = a\mathcal{M}(D).$$

Thus $\mathcal{M}$ is a 1-1 onto linear transformation and hence is an isomorphism (Corollary 4.3.10).

Now since V and W are isomorphic, they have the same dimension. We can, with some work, write down a basis of W. But it is very easy to write down a basis for V. Namely, for each $1 \leq i \leq m$, $1 \leq j \leq n$, let E_{ij} be the m-by-n matrix with a 1 in the (i, j) position and 0 everywhere else. Then if $A = (a_{ij})$ is any m-by-n matrix, we can clearly write A uniquely as $A = \sum a_{ij}E_{ij}$, and so (by Lemma 3.3.3) $\mathcal{B} = \{E_{ij} \,|\, 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis of V. But $\mathcal{B}$ has mn elements, so $mn = \dim V = \dim W$. $\diamondsuit$

This illustrates Remark 4.3.18. The vector spaces $M_{24,1}(\mathbb{F})$, $M_{12,2}(\mathbb{F})$, $M_{8,3}(\mathbb{F})$, $M_{6,4}(\mathbb{F})$, $M_{4,6}(\mathbb{F})$, $M_{3,8}(\mathbb{F})$, $M_{2,12}(\mathbb{F})$, and $M_{1,24}(\mathbb{F})$ all have dimension 24, so are all isomorphic to $\mathbb{F}^{24}$. But they are all evidently different vector spaces.

Now let us rephrase the conditions that a linear transformation $\mathcal{T}$ is 1-1 and onto.

Lemma 4.3.21. *Let $\mathcal{T}\colon V \to W$ be a linear transformation.*

(1) *$\mathcal{T}$ is* 1-1 *if and only if there is a linear transformation $\mathcal{S}\colon W \to V$ with $\mathcal{ST} = \mathcal{I}$.*

(2) *$\mathcal{T}$ is onto if and only if there is a linear transformation $U\colon W \to V$ with $\mathcal{TU} = \mathcal{I}$.*

Proof. (1) Suppose $\mathcal{T}$ is 1-1. Let $\mathcal{B} = \{v_1, v_2, \dots\}$ be a basis of V. Then by Lemma 4.3.7, $\mathcal{C} = \mathcal{T}(\mathcal{B}) = \{w_1, w_2, \dots\}$ is a linearly independent set in W, so by Corollary 3.3.17 it extends to a basis of W. Write that basis as $\mathcal{C} \cup \mathcal{C}'$, where $\mathcal{C}' = \{w_1', w_2', \dots\}$. Now let $\mathcal{S}\colon W \to V$ be the linear transformation defined by $\mathcal{S}(w_i) = v_i$ and $\mathcal{S}(w_i') = 0$. (Actually, the values of $\mathcal{S}(w_i')$ are completely irrelevant, but we have to make a choice.)

Then for each vector v_i in the basis $\mathcal{B}$ of V, $\mathcal{ST}(v_i) = \mathcal{S}(\mathcal{T}(v_i)) = \mathcal{S}(w_i) = v_i = \mathcal{I}(v_i)$, so again by Remark 4.3.2, $\mathcal{ST} = \mathcal{I}$.

On the other hand, suppose there is a linear transformation $\mathcal{S}\colon W \to V$ with $\mathcal{ST} = \mathcal{I}$. Suppose $\mathcal{T}(v) = 0$. Then

$$v = \mathcal{I}(v) = \mathcal{ST}(v) = \mathcal{S}(\mathcal{T}(v)) = \mathcal{S}(0) = 0$$

and so $\mathcal{T}$ is 1-1 by Corollary 4.3.5.

(2) Suppose $\mathcal{T}$ is onto. Let $\mathcal{B} = \{v_1, v_2, \dots\}$ be a basis of V. Then by Lemma 4.3.7, $\mathcal{C} = \mathcal{T}(\mathcal{B}) = \{w_1, w_2, \dots\}$ spans W, so by Corollary 3.3.17 $\mathcal{C}$ has a subset $\mathcal{C}_0$ that is a basis of W. Now for every vector w_i in $\mathcal{C}_0$, $w_i = \mathcal{T}(v_i)$ for some vector v_i in V. (The vector v_i may not be unique, but that does not matter. Make a choice.) Let $\mathcal{U}\colon W \to V$ be the linear transformation defined by $\mathcal{U}(w_i) = v_i$. Then for each vector w_i in the basis $\mathcal{C}_0$ of W, $\mathcal{TU}(w_i) = \mathcal{T}(\mathcal{U}(w_i)) = \mathcal{T}(v_i) = w_i = \mathcal{I}(w_i)$, so again by Remark 4.3.2, $\mathcal{TU} = \mathcal{I}$.

On the other hand, suppose there is a linear transformation $\mathcal{U}\colon W \to V$ with $\mathcal{TU} = \mathcal{I}$. Then for any $w \in W$,

$$w = \mathcal{I}(w) = \mathcal{TU}(w) = \mathcal{T}(\mathcal{U}(w))$$

and so $\mathcal{T}$ is onto. □

Let is now assemble a number of results together.

Theorem 4.3.22. *Let V and W be vector spaces of the same finite dimension n. Let $\mathcal{T}\colon V \to W$ be a linear transformation. The following are equivalent*:

(1) *$\mathcal{T}$ is invertible, i.e., there exists a linear transformation $\mathcal{T}^{-1}\colon W \to V$ with $\mathcal{T}^{-1}\mathcal{T} = \mathcal{I}$ and $\mathcal{T}\mathcal{T}^{-1} = \mathcal{I}$.*

(2) *$\mathcal{T}$ is* 1-1.

(2′) *There is a linear transformation $\mathcal{S}\colon W \to V$ with $\mathcal{ST} = \mathcal{I}$. In this case $\mathcal{S} = \mathcal{T}^{-1}$.*

(3) *$\mathcal{T}$ is onto.*

(3′) *There is a linear transformation $\mathcal{U}\colon W \to V$ with $\mathcal{T}\mathcal{U} = \mathcal{I}$. In this case $\mathcal{U} = \mathcal{T}^{-1}$.*

Proof. First of all, we know that conditions (2) and (2′) are equivalent, and conditions (3) and (3′) are equivalent, by Lemma 4.3.21.

Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis of V, and let $\mathcal{C} = \mathcal{T}(\mathcal{B}) = \{w_1, \ldots, w_n\}$.

By Corollary 4.3.11 and Lemma 4.3.7, conditions (1), (2), and (3) are equivalent to:

(1) $\mathcal{C}$ is a basis of W.

(2) $\mathcal{C}$ is a linearly independent set in W.

(3) $\mathcal{C}$ spans W.

But $\mathcal{C}$ is a set of n vectors in a vector space of dimension n, so we know these conditions are all equivalent by Theorem 3.3.9(4).

Finally, suppose these conditions are all true, so that $\mathcal{T}$ has an inverse $\mathcal{T}^{-1}$. Then if $\mathcal{S}\mathcal{T} = \mathcal{I}$,

$$\mathcal{S} = \mathcal{S}\mathcal{I} = \mathcal{S}(\mathcal{T}\mathcal{T}^{-1}) = (\mathcal{S}\mathcal{T})\mathcal{T}^{-1} = \mathcal{I}\mathcal{T}^{-1} = \mathcal{T}^{-1}$$

and similarly, if $\mathcal{T}\mathcal{U} = \mathcal{I}$,

$$\mathcal{U} = \mathcal{I}\mathcal{U} = (\mathcal{T}\mathcal{T}^{-1})\mathcal{U} = \mathcal{T}^{-1}(\mathcal{T}\mathcal{U}) = \mathcal{T}^{-1}\mathcal{I} = \mathcal{T}^{-1}. \qquad \square$$

Corollary 4.3.23. *Let U, V, and W be vector spaces of the same finite dimension n. Let $\mathcal{T}\colon U \to V$ and $\mathcal{S}\colon V \to W$ so that $\mathcal{S}\mathcal{T}\colon U \to W$. If $\mathcal{S}\mathcal{T}$ is an isomorphism, then both $\mathcal{S}$ and $\mathcal{T}$ are isomorphisms.*

Proof. Since $\mathcal{S}\mathcal{T}$ is an isomorphism, it is both 1-1 and onto. Then $\mathcal{T}$ is 1-1, for if there were some nonzero vector $u \in U$ with $\mathcal{T}(u) = 0$, then we would have $\mathcal{S}\mathcal{T}(u) = \mathcal{S}(\mathcal{T}(u)) = \mathcal{S}(0) = 0$ and $\mathcal{S}$ would not be 1-1. Also, $\mathcal{S}$ is onto, for if there were some vector w with $w \neq \mathcal{S}(v)$ for any v in V, then certainly $w \neq \mathcal{S}\mathcal{T}(u) = \mathcal{S}(\mathcal{T}(u))$ for any $u \in U$.

But then both $\mathcal{S}$ and $\mathcal{T}$ are isomorphisms, by Theorem 4.3.22. $\square$

Again, the crucial step in Theorem 4.3.22 was simply counting—we had n vectors in a vector space of dimension n.

But what happens if V and W are infinite dimensional? We can't count here, but maybe there is some more complicated argument that will give us this result. In fact, there isn't. The corresponding result in the infinite-dimensional case is false, as we see from the following example.

Example 4.3.24. Consider $V = {}^t\mathbb{F}^\infty$. Recall we have right-shift $\mathcal{S}_{\mathrm{rt}}\colon V \to V$ and left-shift $\mathcal{S}_{\mathrm{lt}}\colon V \to V$ defined by $\mathcal{S}_{\mathrm{rt}}([a_1\ \ a_2\ \ a_3\ \ \ldots]) = [0\ \ a_1\ \ a_2\ \ \ldots]$ and $\mathcal{S}_{\mathrm{lt}}([a_1\ \ a_2\ \ a_3\ \ \ldots]) = [a_2\ \ a_3\ \ a_4\ \ \ldots]$.

We observe that

(1) $\mathcal{S}_{\mathrm{rt}}$ is 1-1 but not onto; and

(2) $\mathcal{S}_{\mathrm{lt}}$ is onto but not 1-1.

Hence Corollary 4.3.23 is false in this case.

We further observe

$$\begin{aligned}(3)\quad \mathcal{S}_{\mathrm{lt}}\mathcal{S}_{\mathrm{rt}}([a_1 \quad a_2 \quad a_3 \quad \ldots]) &= \mathcal{S}_{\mathrm{lt}}(\mathcal{S}_{\mathrm{rt}}([a_1 \quad a_2 \quad a_3 \quad \ldots])) \\ &= \mathcal{S}_{\mathrm{lt}}([0 \quad a_1 \quad a_2 \quad \ldots]) \\ &= [a_1 \quad a_2 \quad a_3 \quad \ldots],\end{aligned}$$

so $\mathcal{S}_{\mathrm{lt}}\mathcal{S}_{\mathrm{rt}} = \mathcal{I}$,

but

$$\begin{aligned}(4)\quad \mathcal{S}_{\mathrm{rt}}\mathcal{S}_{\mathrm{lt}}([a_1 \quad a_2 \quad a_3 \quad \ldots]) &= \mathcal{S}_{\mathrm{rt}}(\mathcal{S}_{\mathrm{lt}}([a_1 \quad a_2 \quad a_3 \quad \ldots])) \\ &= \mathcal{S}_{\mathrm{rt}}([a_2 \quad a_3 \quad a_4 \quad \ldots]) \\ &= [0 \quad a_2 \quad a_3 \quad \ldots],\end{aligned}$$

so $\mathcal{S}_{\mathrm{rt}}\mathcal{S}_{\mathrm{lt}} \neq \mathcal{I}$.

(In fact, if we let $\mathcal{R}\colon V \to V$ be the linear transformation $\mathcal{R}([a_1 \quad a_2 \quad a_3 \quad \ldots]) = [a_1 \quad 0 \quad 0 \quad 0]$, we see that $\mathcal{S}_{\mathrm{rt}}\mathcal{S}_{\mathrm{lt}} = \mathcal{I} - \mathcal{R}$.) $\Diamond$

4.4. Matrix inversion

In this section we will apply our work on isomorphisms, i.e., invertible linear transformations, to define the inverse of a matrix and to derive the properties of matrix inversion. Again, this will involve *zero* additional work.

Of course, it wouldn't be very useful to derive the properties of the inverse A^{-1} of a matrix A if we could not calculate A^{-1}. Thus we will also see how to find A^{-1}. More precisely, we will see that we already know how to find A^{-1}!

Here is the basic definition, which we first state somewhat cryptically, and then explain.

Definition 4.4.1. Let $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^n$ be a linear transformation, so that $\mathcal{T} = \mathcal{T}_A$ for a unique matrix A. If $\mathcal{T}$ is invertible, then A^{-1} is the matrix defined by $(\mathcal{T}_A)^{-1} = \mathcal{T}_{A^{-1}}$. $\Diamond$

In other words, consider $\mathcal{T} = \mathcal{T}_A$. If $\mathcal{T}$ is invertible, then it has an inverse $\mathcal{T}^{-1}\colon \mathbb{F}^n \to \mathbb{F}^n$. But then $\mathcal{T}^{-1} = \mathcal{T}_M$ for some unique matrix M, and we set $A^{-1} = M$.

Here is an alternative definition. We shall see momentarily that they are equivalent.

Definition 4.4.2. The matrix A is *invertible* if there is a matrix A^{-1} such that $AA^{-1} = A^{-1}A = I$. In this case, A^{-1} is the *inverse* of A. $\Diamond$

We now have an omnibus theorem.

Theorem 4.4.3. *Let A be an n-by-n matrix. The following are equivalent:*

(1) *The linear transformation $\mathcal{T}_A\colon \mathbb{F}^n \to \mathbb{F}^n$ defined by $\mathcal{T}_A(x) = Ax$ is invertible.*

(2) *The matrix A is invertible, i.e., there exists a matrix A^{-1} with $AA^{-1} = A^{-1}A = I$.*

(3) *There exists a matrix B with $AB = I$. In this case, $B = A^{-1}$.*

(4) *There exists a matrix C with $CA = I$. In this case, $C = A^{-1}$.*

(5) *For any $b \in \mathbb{F}^n$, the equation $Ax = b$ has a unique solution.*

(6) *For any $b \in \mathbb{F}^n$, the equation $Ax = b$ has a solution.*

(7) *The equation $Ax = 0$ only has the trivial solution $x = 0$.*

Proof. Suppose (1) is true. Then $\mathcal{T} = \mathcal{T}_A$ is invertible, i.e., $\mathcal{T}$ has an inverse $\mathcal{T}^{-1}$. But then

$$\begin{aligned}\mathcal{T}\mathcal{T}^{-1} &= \mathcal{T}^{-1}\mathcal{T} = \mathcal{I},\\ (\mathcal{T}_A)(\mathcal{T}_A)^{-1} &= (\mathcal{T}_A)^{-1}\mathcal{T}_A = \mathcal{I},\\ \mathcal{T}_A\mathcal{T}_{A^{-1}} &= \mathcal{T}_{A^{-1}}\mathcal{T}_A = \mathcal{T}_I,\\ AA^{-1} &= A^{-1}A = I,\end{aligned}$$

so (2) is true. But this chain of equalities is reversible, so if (2) is true then, (1) is true.

Now recall that $\mathcal{T}_A$ is the linear transformation given by $\mathcal{T}_A(x) = Ax$. We know that $\mathcal{T}_A$ is invertible, i.e., is an isomorphism, if and only if $\mathcal{T}_A$ is 1-1 and onto, i.e., if $\mathcal{T}_A(x) = b$ has a unique solution for every b, by Lemma 4.3.9. But $\mathcal{T}_A(x) = Ax$, so (5) is equivalent to (1).

Now the condition that $\mathcal{T}_A$ is onto is the condition that $\mathcal{T}_A(x) = b$ has a solution for every b, i.e., that $Ax = b$ has a solution for every b. This is just condition (6). But by Lemma 4.3.21, this is equivalent to there being a linear transformation $\mathcal{U}$ with $\mathcal{T}\mathcal{U} = \mathcal{I}$. Let $\mathcal{U} = \mathcal{T}_B$. Then $AB = I$. This is just condition (3).

The condition that $\mathcal{T}_A$ is 1-1 is the condition that $\mathcal{T}_A(x) = 0$ only has the trivial solution, by Corollary 4.3.5, i.e., that $Ax = 0$ only has the trivial solution $x = 0$. This is just condition (7). But by Lemma 4.3.21, this is equivalent to there being a linear transformation $\mathcal{S}$ with $\mathcal{S}\mathcal{T} = \mathcal{I}$. Let $\mathcal{S} = \mathcal{T}_C$. Then $CA = I$. This is just condition (4).

But now (and here is the punch line) since $\mathbb{F}^n$ has *finite* dimension n, by Theorem 4.3.22 conditions (1), (3), and (4) are equivalent. Thus we see all seven conditions are equivalent.

Finally, if they are all true, then also $B = A^{-1}$ and $C = A^{-1}$, again by Theorem 4.3.22. □

We also have the following theorem.

Theorem 4.4.4. *Let A and B be n-by-n matrices.*

(1) *If A and B are invertible, then AB is invertible and $(AB)^{-1} = B^{-1}A^{-1}$.*

(2) *If AB is invertible, then each of A and B is invertible.*

Proof. Part (1) is just Lemma 4.3.13 and part (2) is just Corollary 4.3.23. □

Now we come to the question of how to find the inverse of a matrix A, when it exists. To solve this problem let us think about a more general problem.

Recall that Theorem 4.3.1 told us that given a vector space V and a basis $\mathcal{B} = \{v_1, v_2, \dots\}$ of V, then for any vector space W and any choice of vectors $\mathcal{C} = \{w_1, w_2, \dots\}$ there is a unique linear transformation $\mathcal{T}\colon V \to W$ with $\mathcal{T}(v_i) = w_i$.

Let's specialize this problem. Choose $V = \mathbb{F}^n$ and $\mathcal{B} = \mathcal{E}$, the standard basis of $\mathbb{F}^n$, where $\mathcal{E} = \{e_1, e_2, \dots, e_n\}$. Let $W = \mathbb{F}^m$. Choose vectors $w_1, \dots, w_n$ in $\mathbb{F}^m$. Then there is a unique linear transformation $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^m$ with $\mathcal{T}(e_i) = w_i$ for each $i = 1, \dots, n$. We know $\mathcal{T} = \mathcal{T}_A$ for some A. What is A?

We know the answer in this case. A is the standard matrix of $\mathcal{T}$, and we know from Corollary 1.5.8 that A is given by

$$A = [\mathcal{T}(e_1) \,|\, \mathcal{T}(e_2) \,|\, \dots \,|\, \mathcal{T}(e_n)].$$

But we have just defined $\mathcal{T}$ by $\mathcal{T}(e_i) = w_i$, so we see that in this case the standard matrix of $\mathcal{T}$ is just

$$A = [w_1 | w_2 | \dots | w_n].$$

To make this concrete, suppose we want to construct a linear transformation $\mathcal{T}\colon \mathbb{F}^3 \to \mathbb{F}^2$ with $\mathcal{T}\left(\begin{bmatrix}1\\0\\0\end{bmatrix}\right) = \begin{bmatrix}2\\5\end{bmatrix}$, $\mathcal{T}\left(\begin{bmatrix}0\\1\\0\end{bmatrix}\right) = \begin{bmatrix}3\\1\end{bmatrix}$, $\mathcal{T}\left(\begin{bmatrix}0\\0\\1\end{bmatrix}\right) = \begin{bmatrix}4\\-3\end{bmatrix}$. Then $\mathcal{T} = \mathcal{T}_A$ with

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

Now let us turn our attention to linear transformations $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^n$, so we are looking at (square) n-by-n matrices. Of course, our discussion above still holds, as that was true for arbitrary m and n. But since we are trying to find the inverse of the matrix A, let us turn our viewpoint around and begin with A. Write A in columns

$$A = [u_1 | u_2 | \dots | u_n]$$

and let $\mathcal{T} = \mathcal{T}_A$, so $\mathcal{T}$ is the linear transformation defined by $\mathcal{T}(e_i) = u_i$ for $i = 1, \dots, n$.

Now remember that by Theorem 4.3.22 we only need to find a linear transformation $\mathcal{U}\colon \mathbb{F}^n \to \mathbb{F}^n$ with $\mathcal{T}\mathcal{U} = \mathcal{I}$ and then we know that $\mathcal{U} = \mathcal{T}^{-1}$, or equivalently by Theorem 4.4.3 we only need to find a matrix B with $AB = I$ to conclude that $B = A^{-1}$. Write

$$B = [v_1 | v_2 | \dots | v_n]$$

with the columns of B yet to be determined. Then $AB = I$ is the equation

$$A[v_1 | \dots | v_n] = I.$$

Now

$$A[v_1 | \dots | v_n] = [Av_1 | \dots | Av_n]$$

and

$$I = [e_1 | \dots | e_n]$$

so this equation becomes

$$[Av_1|\dots|Av_n] = [e_1|\dots|e_n],$$

i.e., it is n systems of linear equations

$$Av_1 = e_1, \quad \dots, \quad Av_n = e_n$$

(all with the same matrix A).

But we already know how to solve systems of linear equations!

Thus we have the following algorithm for finding the inverse of a matrix, when it exists.

Algorithm 4.4.5. Let A be an n-by-n matrix. For $i = 1, \dots, n$, let $x = v_i$ be a solution of $Ax = e_i$. If each of these n equations has a solution, then A^{-1} is the matrix

$$A^{-1} = [v_1|\dots|v_n].$$

If not, A is not invertible. ♢

Now as a matter of implementing our algorithm, since each of our systems $Ax = e_i$ has the same matrix, instead of solving them sequentially we can solve them simultaneously. Let us illustrate this.

Example 4.4.6. Let A be the matrix

$$A = \begin{bmatrix} 1 & 1 & 3 \\ 2 & 2 & 9 \\ 3 & 2 & 7 \end{bmatrix}.$$

We form the matrix

$$[A\,|\,I]$$

and row-reduce. When we are done, if I is invertible, A will have reduced to I (the only n-by-n matrix in reduced row-echelon form with n leading ones, by Lemma 2.5.6) and the columns on the right-hand side will be the columns of A^{-1}, or, putting it more simply, the right-hand side will be A^{-1}.

We did this computation in Example 2.4.6. We started there with

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 2 & 2 & 9 & 0 & 1 & 0 \\ 3 & 2 & 7 & 0 & 0 & 1 \end{array}\right]$$

and ended with

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -4/3 & -1/3 & 1 \\ 0 & 1 & 0 & 13/3 & -2/3 & -1 \\ 0 & 0 & 1 & -2/3 & 1/3 & 0 \end{array}\right],$$

and so we see

$$A^{-1} = \begin{bmatrix} -4/3 & -1/3 & 1 \\ 13/3 & -2/3 & -1 \\ -2/3 & 1/3 & 0 \end{bmatrix}.$$ ♢

Example 4.4.7. We find the inverse of

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{bmatrix}.$$

We form the matrix

$$A = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 0 & 1 & 0 & 0 \\ 1 & 3 & 6 & 10 & 0 & 0 & 1 & 0 \\ 1 & 4 & 10 & 20 & 0 & 0 & 0 & 1 \end{array}\right]$$

and row-reduce. Here we simply give the list of elementary row operations, without writing out the intermediate matrices so obtained.

(1) Add (-1) row 1 to row 2.
(2) Add (-1) row 1 to row 3.
(3) Add (-1) row 1 to row 4.
(4) Add (-2) row 2 to row 3.
(5) Add (-3) row 2 to row 4.
(6) Add (-3) row 3 to row 4.
(7) Add (-1) row 2 to row 1.
(8) Add (1) row 3 to row 1.
(9) Add (-2) row 3 to row 2.
(10) Add (-1) row 4 to row 1.
(11) Add (3) row 4 to row 2.
(12) Add (-3) row 4 to row 3.

We arrive at

$$A = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 4 & -6 & 4 & -1 \\ 0 & 1 & 0 & 0 & -6 & 14 & -11 & 3 \\ 0 & 0 & 1 & 0 & 4 & -11 & 10 & -3 \\ 0 & 0 & 0 & 1 & -1 & 3 & -3 & 1 \end{array}\right]$$

and so we see

$$A^{-1} = \begin{bmatrix} 4 & -6 & 4 & -1 \\ -6 & 14 & -11 & 3 \\ 4 & -11 & 10 & -3 \\ -1 & 3 & -3 & 1 \end{bmatrix}. \qquad \Diamond$$

Of course, one of the principal uses of matrix inversion is in solving linear systems.

Theorem 4.4.8. *Let A be invertible. Then the matrix equation $Ax = b$ has the unique solution $x = A^{-1}b$.*

Proof. We simply substitute:

$$A(A^{-1}b) = (AA^{-1})b = Ib = b,$$

as claimed. $\square$

Example 4.4.9. Consider the system $Ax = b$ given by

$$\begin{bmatrix} 1 & 1 & 3 \\ 2 & 2 & 9 \\ 3 & 2 & 7 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 5 \\ 1 \\ 2 \end{bmatrix}.$$

This system has solution $x = A^{-1}b$. We found A^{-1} in Example 4.4.6, and so

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -4/3 & -1/3 & 1 \\ 13/3 & -2/3 & -1 \\ -2/3 & 1/3 & 0 \end{bmatrix} \begin{bmatrix} 5 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} -5 \\ 19 \\ -1 \end{bmatrix}.$$

In fact, for $b = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$ arbitrary, the system $Ax = b$ has solution

$$x = A^{-1}b = \begin{bmatrix} -4/3 & -1/3 & 1 \\ 13/3 & -2/3 & -1 \\ -2/3 & 1/3 & 0 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} (-4/3)b_1 - (1/3)b_2 + b_3 \\ (13/3)b_1 - (2/3)b_2 - b_3 \\ (-2/3)b_1 + (1/3)b_2 \end{bmatrix}.$$

◊

Example 4.4.10. (1) Let $A = [a]$.

Set $\Delta = a$. If $\Delta \neq 0$, A has inverse $(1/\Delta)[1]$. If $\Delta = 0$, then A does not have an inverse.

(2) Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Set $\Delta = ad - bc$. If $\Delta \neq 0$, A has inverse $(1/\Delta) \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. If $\Delta = 0$, then A does not have an inverse.

(This can be derived using our algorithm, but once these formulas are written down, it is easy to check by direct matrix multiplication that $AA^{-1} = A^{-1}A = I$.) ◊

Remark 4.4.11. We observe in both these cases that there is a number Δ with the property that $\Delta \neq 0$ if and only if the matrix is invertible (and then that there is a formula for the inverse involving Δ). As we will see, Δ is the "determinant" of the matrix. ◊

Example 4.4.12. We follow the notation of Example 4.4.10. In the case when $\Delta \neq 0$, so A is invertible:

(1) If $b = [p]$ the equation $Ax = b$ has solution $x = [p/\Delta]$.

(2) If $b = \begin{bmatrix} p \\ q \end{bmatrix}$ the equation $Ax = b$ has solution

$$x = (1/\Delta) \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} (dp - bq)/\Delta \\ (-cp + aq)/\Delta \end{bmatrix}.$$

(In each case, this is just $x = A^{-1}b$.) ◊

Remark 4.4.13. Again we observe that x is given by a formula involving Δ. ◊

4.5. Looking back at calculus

We have said that calculus "works" because of linearity. Let us look back at the fundamental notions of calculus and observe that we are dealing with vector spaces and linear transformations.

Since we are dealing with calculus, in this section we let $\mathbb{F} = \mathbb{R}$ be the field of real numbers. Also, we let I denote a fixed open interval in $\mathbb{R}$ (perhaps $I = \mathbb{R}$).

To begin with, calculus deals with functions.

Definition 4.5.1. Let $F(I)$ be the set of functions $f\colon I \to \mathbb{R}$. For functions $f, g \in F(I)$, define the function $f + g \in F(I)$ by $(f + g)(x) = f(x) + g(x)$ for every $x \in I$, and for a real number c and a function $f \in F(I)$, define the function $cf \in F(I)$ by $(cf)(x) = cf(x)$ for every $x \in I$. ◊

Theorem 4.5.2. *$F(I)$ is a vector space.*

Proof. This is just a special case of Example 3.1.7. □

We are just repeating this here for emphasis—the first things calculus studies are elements of a vector space.

Definition 4.5.3. For a fixed point $a \in I$, let $\mathrm{Eval}_a\colon F(I) \to \mathbb{R}$ be evaluation at a, i.e., $\mathrm{Eval}_a(f(x)) = f(a)$. ◊

Theorem 4.5.4. *$\mathrm{Eval}_a\colon F(I) \to \mathbb{R}$ is a linear transformation.*

Proof. This is just a special case of Example 4.1.4(d). □

Again we are just repeating this for emphasis—the first thing we do with a function is evaluate it.

Now let us move on to something new.

Definition 4.5.5. Let $C(I)$ be the set of continuous functions $f\colon I \to \mathbb{R}$, with the same operations as in Definition 4.5.1. ◊

Theorem 4.5.6. *$C(I)$ is a subspace of $F(I)$.*

Proof. To show that $C(I)$ is a subspace, we need to show conditions (4), (1), and (6) of Lemma 3.4.3. That is, we need to show:

(4) The 0 function (i.e., the function given by $f(x) = 0$ for every $x \in I$) is continuous on I.

(1) If $f(x)$ and $g(x)$ are continuous functions on I, then $(f+g)(x)$ is a continuous function on I.

(6) If $f(x)$ is a continuous function on I, and c is a constant, then $(cf)(x)$ is a continuous function on I.

These are basic theorems in calculus. □

Definition 4.5.7. Let $D(I)$ be the set of differentiable functions $f\colon I \to \mathbb{R}$, with the same operations as in Definition 4.5.1. ◊

Theorem 4.5.8. *$D(I)$ is a subspace of $C(I)$.*

Proof. First we must show that $D(I)$ is a subset of $C(I)$. That is, we must show that if $f(x)$ is differentiable on I, it is continuous on I. Again this is a basic theorem in calculus.

Next, to show that $D(I)$ is a subspace, we must once again show that conditions (4), (1), and (6) of Lemma 3.4.3 hold, i.e., that:

(4) The 0 function (i.e., the function given by $f(x) = 0$ for every $x \in I$) is differentiable on I.

(1) If $f(x)$ and $g(x)$ are differentiable functions on I, then $(f+g)(x)$ is differentiable on I.

(6) If $f(x)$ is a differentiable function on I, and c is a constant, then $(cf)(x)$ is a differentiable function on I.

Again these are basic theorems in calculus. $\square$

Now what makes calculus "work" is not just the fact that the objects it studies, i.e., functions, lie in a vector space, but also, and more importantly, that the basic operations of calculus, namely evaluation of functions, differentiation, and integration, are linear transformations. We have already seen that evaluation of functions is a linear transformation in Example 4.1.4(d).

To simplify matters, before stating these properties for differentiation and integration we will introduce a new vector space.

Definition 4.5.9. $C^\infty(I)$ is the vector space consisting of functions $f(x)$ that have derivatives of all orders on I (i.e., functions $f(x)$ on I such that $f'(x)$, $f''(x)$, $f'''(x), \ldots$ are all defined on I). $\Diamond$

(The virtue of introducing $C^\infty(I)$ is that we don't have to keep track of exactly how many times a function is differentiable.) For example, $C^\infty(\mathbb{R})$ includes all polynomials, but also such functions as $f(x) = e^x$, $f(x) = \sin(x)$, $f(x) = \cos(x)$, etc.

Theorem 4.5.10. *Let* $\mathrm{Der}\colon C^\infty(I) \to C^\infty(I)$ *be differentiation, i.e.,*

$$\mathrm{Der}(f(x)) = f'(x).$$

Then Der *is a linear transformation.*

Proof. We need to show that

(1) $\mathrm{Der}(f(x)+g(x)) = \mathrm{Der}(f(x))+\mathrm{Der}(g(x))$, i.e., that $(f+g)'(x) = f'(x)+g'(x)$, and

(2) $\mathrm{Der}(cf(x)) = c\,\mathrm{Der}(f(x))$, i.e., that $(cf)'(x) = cf'(x)$.

Again these are basic theorems of calculus. $\square$

Theorem 4.5.11. *For any fixed* $a \in I$, *let* $\mathrm{Int}_a\colon C^\infty(I) \to C^\infty(I)$ *be integration starting at* a, *i.e.,*

$$\mathrm{Int}_a(f(x)) = \int_a^x f(t)\,dt.$$

Then Int_a *is a linear transformation.*

Proof. We need to show that

(1) $\mathrm{Int}_a(f(x)+g(x)) = \mathrm{Int}_a(f(x)) + \mathrm{Int}_a(g(x))$, i.e., that
$$\int_a^x (f(t)+g(t))dt = \int_a^x f(t)dt + \int_a^x g(t)dt,$$
and

(2) $\mathrm{Int}_a(cf(x)) = c\,\mathrm{Int}_a(f(x))$, i.e., that
$$\int_a^x cf(t)dt = c\int_a^x f(t)dt.$$

Once again these are basic theorems of calculus. □

Remark 4.5.12. In addition,
$$\mathrm{Der}_a\colon C^\infty(I) \to \mathbb{R} \quad \text{by} \quad \mathrm{Der}_a(f(x)) = f'(a)$$
and
$$\mathrm{Int}_{a,b}\colon C^\infty(I) \to \mathbb{R} \quad \text{by} \quad \mathrm{Int}_{a,b}(f(x)) = \int_a^b f(t)dt$$
are linear transformations.

Note $\mathrm{Der}_a(f(x))$ is the composition
$$\mathrm{Der}_a(f(x)) = \mathrm{Eval}_a(\mathrm{Der}(f(x)))$$
and $\mathrm{Int}_{a,b}(f(x))$ is the composition
$$\mathrm{Int}_{a,b}(f(x)) = \mathrm{Eval}_b(\mathrm{Int}_a(f(x))),$$
where Eval_a and Eval_b denote evaluation at $x = a$ and $x = b$, respectively.

So while we can check directly that Der_a and $\mathrm{Int}_{a,b}$ are linear transformations, this also follows from the general fact that the composition of linear transformations is a linear transformation (Theorem 4.1.10). ◊

(Our point here is not to prove these theorems—these are theorems of calculus, and we are doing linear algebra—but rather to show the context in which calculus lies.)

We need to define one more linear transformation, one that is closely related to, but not the same as, Eval_a.

Definition 4.5.13. For a fixed point $a \in I$, let $\widetilde{\mathrm{Eval}}_a\colon F(I) \to F(I)$ be the constant function $(\widetilde{\mathrm{Eval}}_a(f))(x) = f(a)$ for every $x \in I$, i.e. $\widetilde{\mathrm{Eval}}_a(f)$ is the constant function whose value at any point $x \in I$ is $f(a)$. ◊

Theorem 4.5.14 (Fundamental theorem of calculus). *Consider the linear transformations* $\mathrm{Der}\colon C^\infty(I) \to C^\infty(I)$ *and* $\mathrm{Int}_a\colon C^\infty(I) \to C^\infty(I)$. *Their compositions are given by*
$$\mathrm{Der}(\mathrm{Int}_a) = \mathcal{I},$$
$$\mathrm{Int}_a(\mathrm{Der}) = \mathcal{I} - \widetilde{\mathrm{Eval}}_a.$$

Proof. The fundamental theorem of calculus states two things.

First, suppose we begin with a function $f(x)$. Let $F(x) = \int_a^x f(t)dt$. Then $F'(x) = f(x)$. Now in our language the first of these equalities is

$$F(x) = \mathrm{Int}_a(f(x))$$

and the second is

$$f(x) = \mathrm{Der}(F(x))$$

so putting these together

$$f(x) = \mathrm{Der}(\mathrm{Int}_a(f(x))),$$

which is just saying that $\mathrm{Der}(\mathrm{Int}_a)$ is the identity linear transformation, i.e.,

$$\mathrm{Der}(\mathrm{Int}_a) = \mathcal{I}.$$

Second, suppose we begin with a function $F(x)$. Let $f(x) = F'(x)$. Then

$$F(x) - F(a) = \int_a^x f(t)dt.$$

Now in our language the first of these equalities is

$$f(x) = \mathrm{Der}(F(x))$$

and in the second equality, the right-hand side is

$$\mathrm{Int}_a(f(x))$$

while the left-hand side is

$$F(x) - F(a) = \mathcal{I}(F(x)) - \widetilde{\mathrm{Eval}}_a(F(x)) = (\mathcal{I} - \widetilde{\mathrm{Eval}}_a)(F(x)),$$

so putting these together, $\mathrm{Int}_a(\mathrm{Der})$ is *not* the identity linear transformation but instead

$$(\mathcal{I} - \widetilde{\mathrm{Eval}}_a)(F(x)) = \mathrm{Int}_a(\mathrm{Der}(f(x))),$$

which is saying that

$$\mathrm{Int}_a(\mathrm{Der}) = \mathcal{I} - \widetilde{\mathrm{Eval}}_a.$$ □

Once again, when we wrote "Proof" here, we did not mean we were proving the fundamental theorem of calculus—that is a theorem of calculus, not linear algebra—but rather showing how we can translate it into the context of linear algebra.

Remark 4.5.15. We are in an infinite-dimensional situation here, and you should compare this with Example 4.3.24. ◊

Changing the subject, let us look at some multivariable calculus. Consider a function $F\colon \mathbb{R}^n \to \mathbb{R}^m$. Let points in $\mathbb{R}^n$ be parameterized by $(x_1, \ldots, x_n)$ and points in $\mathbb{R}^m$ by $(y_1, \ldots, y_m)$. Then F is given by coordinate functions, i.e.,

$$(y_1, \ldots, y_m) = F(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)).$$

In this case F' is an m-by-n matrix with entries the partial derivatives; to be precise, if p_0 is a point in $\mathbb{R}^n$, then

$$F'(p_0) = \begin{bmatrix} \frac{\partial y_1}{\partial x_1}\Big|_{p_0} & \frac{\partial y_1}{\partial x_2}\Big|_{p_0} & \cdots & \frac{\partial y_1}{\partial x_n}\Big|_{p_0} \\ \frac{\partial y_2}{\partial x_1}\Big|_{p_0} & \frac{\partial y_2}{\partial x_2}\Big|_{p_0} & \cdots & \frac{\partial y_2}{\partial x_n}\Big|_{p_0} \\ & \vdots & & \\ \frac{\partial y_m}{\partial x_1}\Big|_{p_0} & \frac{\partial y_m}{\partial x_2}\Big|_{p_0} & \cdots & \frac{\partial y_m}{\partial x_n}\Big|_{p_0} \end{bmatrix}.$$

Similarly we may consider $G\colon \mathbb{R}^m \to \mathbb{R}^p$ where we are again parameterizing $\mathbb{R}^m$ by $(y_1, \dots, y_m)$, and we are parameterizing $\mathbb{R}^p$ by $(z_1, \dots, z_p)$. If q_0 is a point in $\mathbb{R}^m$, by exactly the same logic we have a p-by-m matrix $G'(q_0)$.

Theorem 4.5.16 (Chain rule). *Let $H\colon \mathbb{R}^n \to \mathbb{R}^p$ be the function which is the composition $H = GF$ (i.e., $H(x_1, \dots, x_n) = G(F(x_1, \dots, x_n))$). Then*

$$H'(p_0) = G'(F(p_0))F'(p_0).$$

In this theorem, the product on the right is the product of matrices. Note that the multivariable chain rule is formally identical to the single variable chain rule, i.e., the statement is identical except we are replacing real numbers by matrices. (In fact, we could think of the 1-variable case as being the case when all three matrices involved are 1-by-1.)

Proof. The usual statement and proof of the multivariable chain rule is in terms of individual partial derivatives. If $q_0 = F(p_0)$:

$$\frac{\partial z_i}{\partial x_j}\Big|_{p_0} = \frac{\partial z_i}{\partial y_1}\Big|_{q_0} \frac{\partial y_1}{\partial x_j}\Big|_{p_0} + \frac{\partial z_i}{\partial y_2}\Big|_{q_0} \frac{\partial y_2}{\partial x_j}\Big|_{p_0} + \cdots + \frac{\partial z_i}{\partial y_m}\Big|_{q_0} \frac{\partial y_m}{\partial x_j}\Big|_{p_0} \quad \text{for each } i \text{ and } j.$$

But this is just the formula for multiplying the matrices $G'(q_0)$ and $F'(p_0)$. □

4.6. Exercises

1. Verify the claims in the proof of Theorem 4.1.9.

2. Let $A_1 = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $A_2 = \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$, $A_3 = \begin{bmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{bmatrix}$.

(a) For every positive integer n, find A_1^n.

(b) For every positive integer n, find A_2^n.

(c) For every positive integer n, find A_3^n.

3. (a) Let A be a matrix with a zero row. Show that AB has a zero row for any matrix B.

(b) Let A be a matrix with a zero column. Show that CA has a zero column for any matrix C.

(c) Conclude that a matrix that has a zero row or a zero column cannot be invertible.

(d) Let A be a matrix with two rows i and j where row i of A is c times row j of A. Show that row i of AB is c times row j of AB for any matrix B.

(e) Let A be a matrix with two columns i and j where column i of A is c times column j of A. Show that column i of CA is c times column j of CA for any matrix C.

(f) Conclude that a matrix that has one row a multiple of another, or one column a multiple of another, cannot be invertible. (In particular, this is the case if the matrix has two rows that are the same, or two columns that are the same.)

4. In each case, find A^{-1}:

(a) $A = [2]$.

(b) $A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$.

(c) $A = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}$.

5. In each case, find A^{-1}:

(a) $A = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$.

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

6. In each case, find A^{-1} and use it to solve $Ax = b$:

(a) $A = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}$, $b = \begin{bmatrix} 9 \\ 22 \end{bmatrix}$.

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

(c) $A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 4 \\ 3 & 8 & 13 \end{bmatrix}$, $b = \begin{bmatrix} 2 \\ 0 \\ -4 \end{bmatrix}$.

(d) $A = \begin{bmatrix} 2 & 4 & 6 \\ 3 & 5 & 9 \\ 5 & 7 & 13 \end{bmatrix}$, $b = \begin{bmatrix} 4 \\ 6 \\ 8 \end{bmatrix}$.

(e) $A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 4 & 5 \\ 3 & 8 & 5 \end{bmatrix}$, $b = \begin{bmatrix} 6 \\ 6 \\ -12 \end{bmatrix}$.

(f) $A = \begin{bmatrix} 1 & 1 & 4 & 3 \\ 2 & 3 & 11 & 7 \\ 4 & 5 & 19 & 12 \\ 3 & 5 & 19 & 13 \end{bmatrix}$, $b = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}$.

7. Fill in the intermediate steps in Example 4.4.7.

8. The n-by-n Hilbert matrix $H_n = (h_{ij})$ is given by $h_{ij} = 1/(i+j-1)$. Thus $H_1 = [1]$, $H_2 = \begin{bmatrix} 1 & 1/2 \\ 1/2 & 1/3 \end{bmatrix}$, $H_3 = \begin{bmatrix} 1 & 1/2 & 1/3 \\ 1/2 & 1/3 & 1/4 \\ 1/3 & 1/4 & 1/5 \end{bmatrix}$, etc. Of course, $H_1^{-1} = H_1$. Find H_2^{-1} and H_3^{-1}.

9. Let $A = (a_{ij})$ be the n-by-n matrix with $a_{ij} = \min(i,j)$ for $1 \le i, j \le n$.

(a) (Cleverly) solve the matrix equation $Ax = b$ for any b.

(b) Use your answer to (a) to find A^{-1}.

10. The *commutator* $[A, B]$ of two invertible matrices A and B is defined by

$$[A, B] = ABA^{-1}B^{-1}.$$

(a) Show that $[A, B] = I$ if and only if A and B commute.

(b) Let A, B, and C be the matrices

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

Find $[A, B]$, $[B, C]$, and $[A, C]$.

11. Let $A = P^{-1}BP$ for some invertible matrix P. Show that $A^n = P^{-1}B^nP$ for every positive integer n.

Conclude that for any polynomial $f(x)$, $f(A) = P^{-1}f(B)P$.

12. We have seen that AB invertible implies both A and B invertible. Show that, in this case, $A^{-1} = B(AB)^{-1}$ and $B^{-1} = (AB)^{-1}A$.

13. The *trace* of a square matrix is the sum of its diagonal entries. Suppose that A and B are any two matrices of appropriate sizes so that both products AB and BA are defined. Show that $\mathrm{trace}(AB) = \mathrm{trace}(BA)$.

14. (a) We have defined elementary row operations (EROs) in Definition 2.2.4. For each ERO, write down a matrix E such that, for any matrix M (of the appropriate size), EM is the result of applying that ERO to M. If the ERO is of type (1), (2), or (3), as in that definition, we say that the corresponding elementary matrix E is of that type.

(b) Show that every elementary matrix is invertible, and that the inverse of an elementary matrix is an elementary matrix of the same type.

(c) Show that a matrix A is invertible if and only if it can be written as a product of elementary matrices.

15. Let A be an invertible n-by-n matrix, and let I_n denote the n-by-n identity matrix. Then, as we have seen, if we begin with

$$[A \,|\, I_n]$$

and perform row operations to transform A to I_n, this matrix becomes

$$[I_n \,|\, A^{-1}].$$

Now let B be an arbitrary n-by-p matrix (any p). If we begin with

$$[A \,|\, B]$$

and perform row operations to transform A to I_n, show that this matrix becomes

$$[I_n \,|\, A^{-1}B].$$

16. (a) Let E_0 be any fixed type (2) elementary matrix. If E is any elementary matrix, show there is an elementary matrix E' of the same type with $EE_0 = E_0E'$.

(b) Let E_0 be any fixed type (3) elementary matrix. If E is any elementary matrix, show there is an elementary matrix E' of the same type with $EE_0 = E_0E'$.

17. Define a signed row switch to be a row operation which, for some $i \neq j$, takes row i to row j and row j to -1 times row i.

(a) Write down a matrix that accomplishes a signed row switch, i.e., a matrix F such that FM is the result of applying a signed row switch to M.

(b) Show that any signed row switch may be accomplished by a sequence of type (2) elementary row operations.

(c) Show that any type (3) row operation may be accomplished by a sequence of type (2) elementary row operations followed by a single type (1) elementary row operation.

18. Let A be an invertible matrix.

(a) Show that the following are equivalent:

(i) A can be reduced to weak row-echelon form by using only elementary row operations of the form: add a multiple of row i to row j with $j > i$.

(ii) A can be written as a product $A = LU$ of a lower triangular matrix L with all diagonal entries equal to 1 and an upper triangular matrix U.

(b) In this case, show that L and U are unique.

This is known as the *LU decomposition* of the matrix A.

19. Let U be an invertible n-by-n upper triangular matrix. Write U as a block matrix

$$U = \begin{bmatrix} U' & V \\ 0 & a \end{bmatrix},$$

where U' is $(n-1)$-by-$(n-1)$. Show that

$$U^{-1} = \begin{bmatrix} (U')^{-1} & B \\ 0 & 1/a \end{bmatrix}, \quad \text{where } B = (-1/a)(U')^{-1}V.$$

(Note this gives an inductive method for finding the inverse of an upper triangular matrix.)

Formulate and prove a similar result for L an invertible n-by-n lower triangular matrix.

20. Let A be an invertible n-by-n matrix, and let $b \neq 0$.

(a) Let $B = (b_{ij})$ be an $(n+1)$-by-$(n+1)$ matrix of the form

$$B = \begin{bmatrix} A & 0 \\ * & b \end{bmatrix},$$

i.e., $b_{ij} = a_{ij}$ for $1 \leq i, j \leq n$, $b_{n+1,i}$ is arbitrary for $1 \leq i \leq n$, $b_{i,n+1} = 0$ for $1 \leq i \leq n$, and $b_{n+1,n+1} = b \neq 0$. Show that B is invertible.

(b) Now let B have the form

$$B = \begin{bmatrix} A & * \\ 0 & b \end{bmatrix}.$$

Show that B is invertible.

21. A lattice point in the plane is a point with integer coordinates. Suppose a function $t(i,j)$ is defined on lattice points (i,j) with $0 \leq i \leq m+1$ and $0 \leq j \leq n+1$ and suppose that

$$t(i,j) = (t(i,j+1) + t(i,j-1) + t(i-1,j) + t(i+1,j))/4$$

for every $1 \leq i \leq m$ and $1 \leq j \leq n$.

Suppose that the values $t(i,j)$ are assigned arbitrarily for $i = 0, m+1$ and any j and for $j = 0, n+1$ and any i. Show that there is a unique solution for $\{t(i,j)\}$.

(This is a model of the "discrete Laplacian". Here the letter t is chosen to stand for temperature. This models temperature distribution on a flat plate, where the temperature on the boundary determines the temperature on the interior.)

22. (a) Verify the computation (of partitioned matrices)

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} E & F \\ G & H \end{bmatrix} = \begin{bmatrix} AE + BG & AF + BH \\ CE + DG & CF + DH \end{bmatrix}.$$

(Carefully keep track of the order of the products, as matrix multiplication is not commutative.)

(b) Show that $\begin{bmatrix} I & B \\ 0 & I \end{bmatrix}^{-1} = \begin{bmatrix} I & -B \\ 0 & I \end{bmatrix}$ and $\begin{bmatrix} I & 0 \\ C & I \end{bmatrix}^{-1} = \begin{bmatrix} I & 0 \\ -C & I \end{bmatrix}$.

(c) If A and D are invertible, show that

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

(d) If A is invertible, show that

$$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & DA^{-1} \end{bmatrix} \begin{bmatrix} I & BA^{-1} \\ 0 & I \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}$$

and

$$\begin{bmatrix} A & 0 \\ C & D \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} \begin{bmatrix} I & 0 \\ A^{-1}C & I \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & A^{-1}D \end{bmatrix}.$$

(e) If A and D are invertible, show that

$$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{bmatrix}$$

and

$$\begin{bmatrix} A & 0 \\ C & D \end{bmatrix}^{-1} = \begin{bmatrix} A^{-1} & 0 \\ -D^{-1}CA^{-1} & D^{-1} \end{bmatrix}.$$

(f) If A is invertible, show that

$$\begin{bmatrix} I & 0 \\ -CA^{-1} & I \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} I & -A^{-1}B \\ 0 & I \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & E \end{bmatrix},$$

where $E = D - CA^{-1}B$.

(g) In (f), suppose that E is invertible. Show that

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}^{-1} = \begin{bmatrix} F & -A^{-1}BE^{-1} \\ -E^{-1}CA^{-1} & E^{-1} \end{bmatrix},$$

where $F = A^{-1} + A^{-1}BE^{-1}CA^{-1}$.

(h) If A, B, C, and D all commute (which is only possible when all four blocks are square matrices of the same size) and $AD - BC$ is invertible, show that

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} (AD-BC)^{-1} & 0 \\ 0 & (AD-BC)^{-1} \end{bmatrix} \begin{bmatrix} D & -B \\ -C & A \end{bmatrix}.$$

23. Let A be an m-by-n matrix of rank r. Show that there is an invertible m-by-m matrix P and an invertible n-by-n matrix Q, such that

$$PAQ = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}.$$

(Here I_r denotes the r-by-r identity matrix.)

24. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a set of vectors in $\mathbb{F}^m$, and let A be the matrix

$$A = [v_1|v_2|\ldots|v_n]$$

(i.e., A is the matrix whose first column is v_1, whose second column is v_2, etc.).

Show that $\mathcal{T}_A$ is 1-1 if and only if $\mathcal{B}$ is linearly independent, and that $\mathcal{T}_A$ is onto if and only if $\mathcal{B}$ spans $\mathbb{F}^m$.

25. Let A be an upper triangular n-by-n matrix and consider the linear transformation $\mathcal{T}_A \colon \mathbb{F}^n \to \mathbb{F}^n$.

(a) If all of the diagonal entries of A are nonzero, show that $\mathcal{T}_A$ is both 1-1 and onto, and hence an isomorphism.

(b) If at least one diagonal entry of A is zero, show that $\mathcal{T}_A$ is neither 1-1 nor onto.

26. Let $V = M_n(\mathbb{R})$, $n \geq 2$.

(a) Let $\mathcal{T} \colon V \to V$ be the linear transformation defined as follows. If $A = (a_{ij})$, then $B = \mathcal{T}(A) = (b_{ij})$, where $b_{ij} = (-1)^{i+j}a_{ij}$. Show there are matrices P and Q such that $\mathcal{T}_A = PAQ$ for every $A \in V$.

(b) Let $\mathcal{U} \colon V \to V$ be the linear transformation defined by

$$\mathcal{U}(A) = (A + \mathcal{T}(A))/2.$$

Show there do not exist matrices P and Q such that $\mathcal{U}(A) = PAQ$ for every $A \in V$.

27. A square matrix A is a *monomial* matrix if it has exactly one nonzero entry in each row and column. A monomial matrix is a *permutation* matrix if each of its nonzero entries is equal to 1.

Let A be a monomial matrix.

(a) Show that $A = D_1 P$ and also $A = PD_2$ for some permutation matrix P and diagonal matrices D_1 and D_2 (which may or may not be the same) all of whose diagonal entries are nonzero.

(b) Show that $A^k = D$ for some positive integer k, where D is a diagonal matrix all of whose diagonal entries are nonzero.

28. Let A be an upper triangular matrix.

(a) Show that A is invertible if and only if all of the diagonal entries of A are nonzero. In this case, show that A^{-1} is also upper triangular.

(b) Suppose that A has integer entries. Show that A^{-1} has integer entries if and only if all the diagonal entries of A are ± 1.

29. Let M be a block matrix $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, and let N be the block matrix $N = \begin{bmatrix} A & C \\ B & D \end{bmatrix}$. If M is invertible, must N be invertible?

30. Let A be a fixed n-by-n matrix with entries in $\mathbb{F}$. The *centralizer* $Z(A)$ of A is defined by $Z(A) = \{n\text{-by-}n \text{ matrices } B \text{ such that } AB = BA\}$. Show that $Z(A)$ is a subspace of $M_n(\mathbb{F})$.

31. Let A be a diagonal matrix with distinct diagonal entries.

(a) Let B be a matrix. Show that B commutes with A (i.e., $AB = BA$) if and only if B is a diagonal matrix.

(b) Let $p(x)$ be any polynomial. Then certainly $B = p(A)$ is a diagonal matrix. Show the converse. That is, let B be any diagonal matrix. Show that there is a polynomial $p(x)$ such that $B = p(A)$.

Putting these together, this shows: let A be a diagonal matrix with distinct diagonal entries. Then a matrix B commutes with A if and only if B is a polynomial in A.

(For a generalization of this, see Section 8.6, Exercise 9.)

Chapter 5

More on vector spaces and linear transformations

5.1. Subspaces and linear transformations

Two of the basic ways we obtain subspaces of vector spaces come from linear transformations. We will show this, and then see how this gives us many new examples of subspaces, as well as recovering some of the examples we already had.

Definition 5.1.1. Let $\mathcal{T}\colon V \to W$ be a linear transformation. Then

$$\operatorname{Ker}(\mathcal{T}) = \{v \in V \,|\, \mathcal{T}(v) = 0\}$$

and

$$\operatorname{Im}(\mathcal{T}) = \{w \in W \,|\, w = \mathcal{T}(v) \text{ for some } v \in V\}.$$

$\operatorname{Ker}(\mathcal{T})$ is called the *kernel* of $\mathcal{T}$ and $\operatorname{Im}(\mathcal{T})$ is called the *image* of $\mathcal{T}$. $\Diamond$

(Some authors call the image of $\mathcal{T}$ the range of $\mathcal{T}$.)

Here is the basic theorem. You will see that its proof is quite straightforward, but it has far-reaching consequences.

Theorem 5.1.2. *Let $\mathcal{T}\colon V \to W$ be a linear transformation. Then:*

(1) $\operatorname{Ker}(\mathcal{T})$ *is a subspace of* V; *and*

(2) $\operatorname{Im}(\mathcal{T})$ *is a subspace of* W.

Proof. First $\operatorname{Ker}(\mathcal{T})$. We must verify conditions (4), (1), and (6) of Lemma 3.2.3.

(4) $\mathcal{T}(0) = 0$ by Lemma 3.3.3, so $0 \in \operatorname{Ker}(\mathcal{T})$.

(1) Let $v_1, v_2 \in \operatorname{Ker}(\mathcal{T})$. Then $\mathcal{T}(v_1) = 0$ and $\mathcal{T}(v_2) = 0$. But then $\mathcal{T}(v_1 + v_2) = \mathcal{T}(v_1) + \mathcal{T}(v_2) = 0 + 0 = 0$ so $v_1 + v_2 \in \operatorname{Ker}(\mathcal{T})$.

(6) Let $v \in \operatorname{Ker}(\mathcal{T})$ and $c \in \mathbb{F}$. Then $\mathcal{T}(v) = 0$. But then $\mathcal{T}(cv) = c\mathcal{T}(v) = c0 = 0$.

Thus $\mathrm{Ker}(\mathcal{T})$ is a subspace of V.

Next $\mathrm{Im}(\mathcal{T})$. Again we verify conditions (4), (1), and (6) of Lemma 3.2.3.

(4) $0 = \mathcal{T}(0)$ by Lemma 3.3.3, so $0 \in \mathrm{Im}(\mathcal{T})$.

(1) Let $w_1, w_2 \in \mathrm{Im}(\mathcal{T})$. Then $w_1 = \mathcal{T}(v_1)$ and $w_2 = \mathcal{T}(v_2)$ for some v_1 and v_2 in V. But then $w_1 + w_2 = \mathcal{T}(v_1) + \mathcal{T}(v_2) = \mathcal{T}(v_1 + v_2)$ so $w_1 + w_2 \in \mathrm{Im}(\mathcal{T})$.

(6) Let $w \in \mathrm{Im}(\mathcal{T})$ and let $c \in \mathbb{F}$. Then $w = \mathcal{T}(v)$ for some v in V. But then $cw = c\mathcal{T}(v) = \mathcal{T}(cv)$ so $w \in \mathrm{Im}(\mathcal{T})$.

Thus $\mathrm{Im}(\mathcal{T})$ is a subspace of W. □

(Note how the linearity of $\mathcal{T}$ was used crucially in the proof.)

Let us consider the case when $\mathcal{T} = \mathcal{T}_A \colon \mathbb{F}^n \to \mathbb{F}^m$. We have these two subspaces, and we would like to find bases of each. This is a problem we have already solved!

Lemma 5.1.3. *Let $\mathcal{T} = \mathcal{T}_A \colon \mathbb{F}^n \to \mathbb{F}^m$. Then $\mathrm{Im}(\mathcal{T}) = \mathrm{Col}(A)$, the column space of A.*

Proof. Write $A = [u_1|\dots|u_n]$ and $v = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$. Then $\mathcal{T}(v) = \mathcal{T}_A(v) = Av = c_1u_1 + \dots + c_nu_n$ is just a linear combination of the columns of A, and by definition the column space of A is the set of all such linear combinations. □

Corollary 5.1.4. *The procedure of Lemma 3.4.6 gives a basis for $\mathrm{Im}(\mathcal{T}_A)$. The dimension of $\mathrm{Im}(\mathcal{T}_A)$ is the number of leading entries k in any weak row-echelon form A' of A.*

Proof. This is simply a restatement of Corollary 3.4.9. □

To see that we already know how to find a basis for $\mathrm{Ker}(\mathcal{T})$ takes a little more work. First we recall that $\mathrm{Ker}(\mathcal{T}) = \{v \,|\, \mathcal{T}_A(v) = 0\} = \{v \,|\, Av = 0\}$, i.e., $\mathrm{Ker}(\mathcal{T}_A)$ is just the set of solutions to the equation $Ax = 0$, and we considered these at length in Chapter 2.

Lemma 5.1.5. *Let A', a weak row-echelon form of the m-by-n matrix A, have k leading entries, and hence $n-k$ columns which do not have leading entries. Let these columns be $j_1, \dots, j_{n-k}$. Let $\mathcal{S} \colon \mathrm{Ker}(\mathcal{T}) \to \mathbb{F}^{n-k}$ be the linear transformation*

$$\mathcal{S}\left(\begin{bmatrix} c_1 \\ \vdots \\ c_k \end{bmatrix}\right) = \begin{bmatrix} c_{j_1} \\ \vdots \\ c_{j_{n-k}} \end{bmatrix}.$$

Then $\mathcal{S}$ is an isomorphism.

Proof. We observe that $\mathcal{S}(v)$ is the vector whose entries are the values of the free variables in a solution v of $Ax = 0$.

To show $\mathcal{S}$ is an isomorphism we must show it is 1-1 and onto. That is, we must show that for any values $c_1, \dots, c_{j_{n-k}}$, there is a unique vector v in $\mathrm{Ker}(\mathcal{T}_A)$, i.e., a unique vector v in $\mathbb{F}^n$ with $Av = 0$, and with the free variables taking those values. But that is the conclusion of Lemma 2.5.2. $\square$

Now $\mathcal{S}$ gets us the values of the free variables *from* a solution of $Ax = 0$. But that is not actually what we want to do. We want to go the other way: from the values of the free variables *to* a solution. But now that we know that $\mathcal{S}$ is an isomorphism, we can indeed go the other way: we take $\mathcal{R} = \mathcal{S}^{-1}$.

Corollary 5.1.6. *The procedure of Corollary* 2.5.3*, where we let j_0 be each of the indexes of the $n-k$ free variables in turn, gives a basis for* $\operatorname{Ker}(\mathcal{T}_A)$*. The dimension of* $\operatorname{Ker}(\mathcal{T}_A)$ *is $n-k$.*

Proof. Let $\mathcal{E} = \{e_1, \ldots, e_{n-k}\}$ be the standard basis of $\mathbb{F}^{n-k}$. Then the procedure of Corollary 2.5.3 gives a set of $n-k$ solutions $\mathcal{B} = \{v_1, \ldots, v_{n-k}\}$ of $Ax = 0$ with $v_i = \mathcal{R}(e_i)$, $i = 1, \ldots, n-k$. But $\mathcal{R}$ is an isomorphism, and $\mathcal{E}$ is a basis of $\mathbb{F}^{n-k}$, so $\mathcal{B}$ is a basis of $\operatorname{Ker}(\mathcal{T}_A)$ by Corollary 4.3.11. $\square$

As we have observed, $\operatorname{Im}(\mathcal{T}_A) = \operatorname{Col}(A)$, the column space of A. There is also another name for $\operatorname{Ker}(\mathcal{T}_A)$.

Definition 5.1.7. The *null space* $\operatorname{Null}(A)$ of the matrix A is $\operatorname{Null}(A) = \operatorname{Ker}(\mathcal{T}_A) = \{v \mid Av = 0\}$. $\Diamond$

We recall that $\operatorname{rank}(A) = \dim \operatorname{Col}(A)$. (Actually, this was our definition of column rank, but we simplified it to rank as a consequence of Corollary 3.4.16.)

Definition 5.1.8. The *nullity* $\operatorname{nullity}(A)$ of the matrix A is $\operatorname{nullity}(A) = \dim \operatorname{Null}(A)$. $\Diamond$

Example 5.1.9. Let A be the matrix

$$A = \begin{bmatrix} 1 & 4 & -1 & 5 & 0 \\ 2 & 1 & 0 & 4 & 1 \\ 3 & -2 & 1 & -1 & 4 \\ 7 & 0 & 1 & 7 & 6 \end{bmatrix}.$$

We wish to find $\operatorname{Ker}(\mathcal{T}_A)$ and $\operatorname{Im}(\mathcal{T}_A)$.

This is the matrix A of Example 3.4.10. We reduced A to A', in weak row-echelon form, with A' having leading entries in columns 1, 2, and 4. Thus we conclude

$$\operatorname{Im}(\mathcal{T}_A) = \operatorname{Col}(A) \quad \text{has basis} \quad \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 7 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} 5 \\ 4 \\ -1 \\ 7 \end{bmatrix} \right\}.$$

To find a basis for $\operatorname{Ker}(\mathcal{T}_A)$ we reduce further to $\tilde{A}$ in reduced row-echelon form, and find

$$\tilde{A} = \begin{bmatrix} 1 & 0 & 1/7 & 0 & 19/14 \\ 0 & 1 & -2/7 & 0 & 2/7 \\ 0 & 0 & 0 & 1 & -1/2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

and applying Corollary 2.5.3 we see that

$$\operatorname{Ker}(\mathcal{T}_A) = \operatorname{Null}(A) \quad \text{has basis} \quad \left\{ \begin{bmatrix} -19/14 \\ -2/7 \\ 0 \\ 1/2 \\ 1 \end{bmatrix}, \begin{bmatrix} -1/7 \\ 2/7 \\ 1 \\ 0 \\ 0 \end{bmatrix} \right\}. \qquad \Diamond$$

By definition, $\operatorname{Ker}(\mathcal{T}) = \mathcal{T}^{-1}(0)$. It is natural to ask about $\mathcal{T}^{-1}(w_0)$ for any given w_0 in W. Of course, this may be empty (i.e., there may be no v in V with $\mathcal{T}(v) = w_0$), in which case there is nothing to say. But otherwise we have the following result.

Theorem 5.1.10. *Let $\mathcal{T}: V \to W$ be a linear transformation. Let w_0 be an element of W. If $A = \mathcal{T}^{-1}(w_0)$ is nonempty, it is an affine subspace of V parallel to* $\operatorname{Ker}(\mathcal{T})$.

Proof. Let v_0 be any element of V with $\mathcal{T}(v_0) = w_0$. We claim that $A = v_0 + \operatorname{Ker}(\mathcal{T})$.

First we see that $v_0 + \operatorname{Ker}(\mathcal{T}) \subseteq A$. Let u be any element of $\operatorname{Ker}(\mathcal{T})$. Then $\mathcal{T}(v_0 + u) = \mathcal{T}(v_0) + \mathcal{T}(u) = w_0 + 0 = w_0$.

Next we see that $A \subseteq v_0 + \operatorname{Ker}(\mathcal{T})$. Let v_1 be any element of V with $\mathcal{T}(v_1) = w_0$. Then $v_1 = v_0 + (v_1 - v_0) = v_0 + u$, where $u = v_1 - v_0$. But then $\mathcal{T}(u) = \mathcal{T}(v_1 - v_0) = \mathcal{T}(v_1) - \mathcal{T}(v_0) = w_0 - w_0 = 0$ so $u \in \operatorname{Ker}(\mathcal{T})$. $\square$

Example 5.1.11. Consider the system of linear equations in Example 2.4.5. We may reinterpret that as the equation $\mathcal{T}_A(v) = Av = w_0$, where A is the matrix of the system and w_0 is the right-hand side. We solved this system, or equivalently we found $\mathcal{T}_A^{-1}(w_0)$. It consisted of all vectors of the form

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -4 \\ 0 \\ 5 \end{bmatrix} + x_2 \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_4 \begin{bmatrix} -1 \\ 0 \\ -4 \\ 1 \\ 0 \end{bmatrix},$$

and we can see that the first vector on the right-hand side is a single vector v_0, while the rest of the right-hand side is simply $\operatorname{Ker}(\mathcal{T}_A)$. $\Diamond$

5.2. Dimension counting and applications

In this section we prove the basic dimension counting theorem, and then use it to obtain some useful mathematical results that, on the face of them, don't seem to have much to do with linear algebra.

We begin with a general result.

Theorem 5.2.1. *Let $\mathcal{T}: V \to W$ be a linear transformation. Let U be any complement of* $\operatorname{Ker}(\mathcal{T})$. *Then*

$$\mathcal{T}: U \to \operatorname{Im}(\mathcal{T})$$

is an isomorphism. In particular,

$$\operatorname{codim} \operatorname{Ker}(\mathcal{T}) = \dim \operatorname{Im}(\mathcal{T}).$$

Proof. As usual, we must show $\mathcal{T}\colon U \to \mathrm{Im}(\mathcal{T})$ is 1-1 and onto.

Onto: Let $w \in \mathrm{Im}(\mathcal{T})$. Then, by definition, $w = \mathcal{T}(v)$ for some $v \in V$. Since U is a complement of $\mathrm{Ker}(\mathcal{T})$, $V = U + \mathrm{Ker}(\mathcal{T})$ so we can write v as $v = u + v'$ with v' in $\mathrm{Ker}(\mathcal{T})$. But then

$$w = \mathcal{T}(v) = \mathcal{T}(u + v') = \mathcal{T}(u) + \mathcal{T}(v') = \mathcal{T}(u) + 0 = \mathcal{T}(u).$$

1-1: Let $u \in U$ with $\mathcal{T}(u) = 0$. But that means $u \in \mathrm{Ker}(\mathcal{T})$. Since U is a complement of $\mathrm{Ker}(\mathcal{T})$, $U \cap \mathrm{Ker}(\mathcal{T}) = \{0\}$ so $u = 0$.

Finally, recall the definition of the codimension of a subspace of V: the codimension of a subspace is defined to be the dimension of a complement. Thus $\operatorname{codim} \mathrm{Ker}(\mathcal{T}) = \dim U$. But we have just shown that U and $\mathrm{Im}(\mathcal{T})$ are isomorphic, so they have the same dimension. □

Corollary 5.2.2. *Let $\mathcal{T}\colon V \to W$ be a linear transformation. Then the quotient vector space $V/\mathrm{Ker}(\mathcal{T})$ is isomorphic to $\mathrm{Im}(\mathcal{T})$.*

Proof. Recall that $V/\mathrm{Ker}(\mathcal{T})$ is the set of all affine subspaces of V parallel to $\mathrm{Ker}(\mathcal{T})$. We know that $V/\mathrm{Ker}(\mathcal{T})$ is isomorphic to any complement U of $\mathrm{Ker}(\mathcal{T})$ by Theorem 4.3.19, and we have just shown that U is isomorphic to $\mathrm{Im}(\mathcal{T})$, so $V/\mathrm{Ker}(\mathcal{T})$ is isomorphic to $\mathrm{Im}(\mathcal{T})$. But it is worth giving an explicit isomorphism.

We let $\overline{\mathcal{T}}\colon V/\mathrm{Ker}(\mathcal{T}) \to \mathrm{Im}(\mathcal{T})$ as follows. Let A be an element of $V/\mathrm{Ker}(\mathcal{T})$. Then $A = t_0 + \mathrm{Ker}(\mathcal{T})$ for some $t_0 \in V$. We set

$$\overline{\mathcal{T}}(A) = \mathcal{T}(t_0).$$

We leave it to the reader to check that $\overline{\mathcal{T}}$ is well-defined, i.e., that $\overline{\mathcal{T}}$ does not depend on the choice of t_0, that $\overline{\mathcal{T}}$ is a linear transformation, and that $\overline{\mathcal{T}}$ is both 1-1 and onto, and hence an isomorphism. □

Corollary 5.2.3 (Basic dimension counting theorem)**.** *Let $\mathcal{T}\colon V \to W$ be a linear transformation. Then*

$$\dim \mathrm{Ker}(\mathcal{T}) + \dim \mathrm{Im}(\mathcal{T}) = \dim V.$$

Proof. As we saw in Theorem 3.4.26,

$$\dim \mathrm{Ker}(\mathcal{T}) + \operatorname{codim} \mathrm{Ker}(\mathcal{T}) = \dim V.$$

But we just saw in Theorem 5.2.1 that $\operatorname{codim} \mathrm{Ker}(\mathcal{T}) = \dim \mathrm{Im}(\mathcal{T})$. □

Corollary 5.2.4. *Let A be an m-by-n matrix. Then*

$$\operatorname{rank} A + \operatorname{nullity} A = n.$$

Proof. This is just a translation of Corollary 5.2.3 into matrix language. □

Again we should observe that all these counting results can be traced back to our original and basic counting theorem, Theorem 1.4.5.

Corollary 5.2.5. *Let $\mathcal{T}\colon V \to W$ with $\dim V = n$ and $\dim W = m$. Then $\dim \mathrm{Ker}(\mathcal{T}) \geq n - m$ and $\operatorname{codim} \mathrm{Im}(\mathcal{T}) \geq m - n$.*

Proof. Clear from Corollary 5.2.3. □

Here is another result. But we want to emphasize this is *not* a new result. It is merely a handy way of encoding information we already know (Corollary 4.3.8 and Theorem 4.3.22).

Corollary 5.2.6. *Let* $\mathcal{T}\colon V \to W$ *with* $\dim V = n$ *and* $\dim W = m$.

(1) *If* $n > m$, *then* $\mathcal{T}$ *is not* 1-1.

(2) *If* $n < m$, *then* $\mathcal{T}$ *is not onto.*

(3) *If* $n = m$, *the following are equivalent*:
 (a) $\mathcal{T}$ *is* 1-1 *and onto* (*and hence an isomorphism*).
 (b) $\mathcal{T}$ *is* 1-1.
 (c) $\mathcal{T}$ *is onto.*

Proof. (1) If $n > m$, then $\dim \mathrm{Ker}(\mathcal{T}) > 0$.

(2) If $n < m$, then $\operatorname{codim} \mathrm{Im}(\mathcal{T}) > 0$.

(3) Let $k = \dim \mathrm{Ker}(\mathcal{T})$ and $i = \dim \mathrm{Im}(\mathcal{T})$.

Then by Corollary 5.2.3, $k + i = n$. But if k and i are nonnegative integers with $k + i = n$, clearly the following are equivalent:

(a) $k = 0$ and $i = n$.

(b) $k = 0$.

(c) $i = n$. □

Remark 5.2.7. In (theory and) practice, (3) is extremely useful. Suppose we have a linear transformation $\mathcal{T}\colon V \to W$ between vector spaces of the same finite dimension and we want to show that $\mathcal{T}$ is an isomorphism. A priori, this means we have to show both (b) and (c). But this theorem tells us we only have to show one of (b) and (c), and then the other is automatic. This sounds like we're cutting the amount of work in half, but it's often much better than that. Often one of (b) and (c) is relatively easy to show and the other is relatively hard, so we can just pick the easy one, show it is true, and then we're done. (Compare Remark 3.3.10.) ◊

Here is an application of dimension counting. We begin with a general result, and then we specialize it to several cases of particular interest.

We let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.

Theorem 5.2.8. *Let* n *be a positive integer, and let* $e_1, \ldots, e_n$ *be nonnegative integers. Let* $a_1, \ldots, a_n$ *be arbitrary but distinct. Set* $d + 1 = \sum_{i=1}^{n}(e_1 + 1)$.

For each $i = 1, \ldots, n$ *and each* $j = 0, \ldots, e_i$, *let* b_{ij} *be arbitrary. Then there is a unique polynomial* $p(x)$ *of degree at most* d *such that*

$$p^{(j)}(a_i) = b_{ij}, \quad i = 1, \ldots, n,\ j = 0, \ldots, e_i.$$

Proof. Recall that $P_d(\mathbb{F})$ has dimension $d+1$. Let $\mathcal{T}\colon P_d(\mathbb{F}) \to \mathbb{F}^{d+1}$ be defined by

$$\mathcal{T}(p(x)) = \begin{bmatrix} p^{(0)}(a_1) \\ \vdots \\ p^{(e_1)}(a_1) \\ \vdots \\ p^{(0)}(a_n) \\ \vdots \\ p^{(e_n)}(a_n) \end{bmatrix}.$$

$\mathcal{T}$ is a linear transformation and we claim it is an isomorphism, which then proves the theorem.

In order to show this, it suffices to show that $\mathcal{T}$ is 1-1, and in order to show this, it suffices to show that $\mathcal{T}^{-1}(0) = \{0\}$.

Thus let $p(x) \in P_d(\mathbb{F})$ be a polynomial with $\mathcal{T}(p(x)) = 0$. Then for each $i = 1, \dots, n$, $p^{(j)}(a_i) = 0$ for $j = 0, \dots, e_n$, which implies that $p(x)$ is divisible by $(x - a_i)^{e_n+1}$, and hence that $p(x)$ is divisible by the product $(x - a_1)^{e_1+1} \cdots (x - a_n)^{e_n+1}$. But this is a polynomial of degree $d+1$, and $p(x)$ has degree at most d, so this is only possible if $p(x) = 0$. □

As our first special case of this, let us go to one extreme and take $n = 1$. For simplicity, let $a = a_1$ and $b_j = b_{1j}$. Note then that $d = e_1$.

Corollary 5.2.9 (Finite Taylor expansion)**.** *Let a be arbitrary. Let $b_0, \dots, b_d$ be arbitrary. Then there is a unique polynomial $p(x)$ of degree at most d with $p^{(j)}(a) = b_j$, $j = 0, \dots, d$.*

This polynomial is

$$p(x) = \sum_{j=0}^{d} b_j \frac{(x-a)^j}{j!}$$

(*where we understand that* $(x-a)^0 = 1$).

Proof. The first claim is just a special case of Theorem 5.2.8. It remains to explicitly identify the polynomial.

For $j = 0, \dots, d$, let $q_j(x) = (x-a)^j/j!$. Then if $\mathcal{T}$ is the linear transformation of the proof of Theorem 5.2.8, $\mathcal{T}(q_j(x)) = e_j$. Thus if $\mathcal{B} = \{q_0(x), \dots, q_d(x)\}$, then $\mathcal{T}(\mathcal{B}) = \mathcal{E}$, the standard basis of $\mathbb{F}^{d+1}$. Hence $\mathcal{B}$ is a basis of $P_d(\mathbb{F})$, and every $p(x)$ in $P_d(\mathbb{F})$ has a unique expression as a linear combination of the elements of $\mathcal{B}$. Furthermore,

$$\mathcal{T}\left(\sum_{j=0}^{d} b_j q_j(x)\right) = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_d \end{bmatrix} = \mathcal{T}(p(x))$$

and $\mathcal{T}$ is an isomorphism, so $p(x) = \sum_{j=0}^{d} b_j q_j(x)$. □

Corollary 5.2.10. *For any a, $\mathcal{B} = \{1, x-a, \dots, (x-a)^d/d!\}$ is a basis of $P_d(\mathbb{F})$.*

Proof. We observed this in the course of the proof of Corollary 5.2.9. $\square$

(Of course, this corollary is a very special case of Example 3.3.21, but we just wanted to observe this special case from this viewpoint.)

As our next special case, let us go to the other extreme and take each $e_i = 0$. Then $n = d + 1$. For simplicity, we let $b_i = b_{i0}$.

Corollary 5.2.11 (Lagrange interpolation theorem)**.** *Let $a_1, \ldots, a_{d+1}$ be arbitrary but distinct. Let $b_1, \ldots, b_{d+1}$ be arbitrary. Then there is a unique polynomial of degree at most d with $p(a_i) = b_i$, $i = 1, \ldots, d + 1$.*

This polynomial is

$$p(x) = \sum_{i=1}^{d+1} b_i \frac{\prod_{j \neq i}(x - a_j)}{\prod_{j \neq i}(a_i - a_j)}.$$

Proof. The first claim is just a special case of Theorem 5.2.8. It remains to explicitly identify the polynomial.

For $i = 1, \ldots, d + 1$, let $l_i(x) = \prod_{j \neq i}(x - a_j)/\prod_{j \neq i}(a_i - a_j)$. Then if $\mathcal{T}$ is the linear transformation of the proof of Theorem 5.2.8, $\mathcal{T}(l_i(x)) = e_i$. Thus if $\mathcal{B} = \{l_1(x), \ldots, l_{d+1}(x)\}$, then $\mathcal{T}(\mathcal{B}) = \mathcal{E}$, the standard basis of $\mathbb{F}^{d+1}$. Hence $\mathcal{B}$ is a basis of $P_d(\mathbb{F})$, and every $p(x)$ in $P_d(\mathbb{F})$ has a unique expression as a linear combination of the elements of $\mathcal{B}$. Furthermore,

$$\mathcal{T}\left(\sum_{i=1}^{d+1} b_i l_i(x)\right) = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{d+1} \end{bmatrix} = \mathcal{T}(p(x))$$

and $\mathcal{T}$ is an isomorphism, so $p(x) = \sum_{i=1}^{d+1} b_i l_i(x)$. $\square$

Corollary 5.2.12. *For any distinct $a_1, \ldots, a_{d+1}$,*

$$\mathcal{B} = \left\{ \prod_{j \neq 1}(x - a_j) \Big/ \prod_{j \neq 1}(a_1 - a_j), \ldots, \prod_{j \neq d+1}(x - a_j) \Big/ \prod_{j \neq d+1}(a_{d+1} - a_j) \right\}$$

is a basis of $P_d(\mathbb{F})$.

Proof. We observed this in the course of the proof of Corollary 5.2.11. $\square$

(You've undoubtedly noticed the extreme similarity between the proof of Corollary 5.2.9 and the proof of Corollary 5.2.11.)

Here is another important special case. It is the method of *cubic splines*. We take $\mathbb{F} = \mathbb{R}$ here.

Corollary 5.2.13 (Cubic splines)**.** *Let $I = [a, b]$ be a closed interval in $\mathbb{R}$. Let $a = a_0 < a_1 < a_2 < \cdots < a_k = b$, so that I is divided into k subintervals $[a_0, a_1], [a_1, a_2], \ldots, [a_{k-1}, a_k]$. For each $i = 0, \ldots, k$ let b_{i0} and b_{i1} be arbitrary real numbers. Then there is a unique continuously differentiable function $p(x)$ defined on I with $p(a_i) = b_{i0}$ and $p'(a_i) = b_{i1}$ for each $i = 0, \ldots, k$, and with $p(x)$ given by a polynomial $p_i(x)$ of degree at most 3 on each subinterval $[a_{i-1}, a_i]$ of I.*

Proof. Applying Theorem 5.2.8 with $n = 2$, $e_1 = e_2 = 2$ and the two points at which the function is evaluated being a_{i-1} and a_i we see there is a unique polynomial $p_i(x)$ of degree at most 3 with $p_i(a_j) = b_{j0}$ and $p_i'(a_j) = b_{j1}$ for $j = i-1$ or i. Then we simply define $p(x)$ to be the function $p(x) = p_i(x)$ if $a_{i-1} \leq x \leq a_i$. Each $p_i(x)$ is continuously differentiable (as it is a polynomial) and since the left-hand and right-hand derivatives of $p(x)$ agree at each a_i by arrangement, $p(x)$ is differentiable as well. □

Remark 5.2.14. We usually think of the method of cubic splines as a method of approximating a function $f(x)$ by "simpler" functions, namely polynomials. We could certainly approximate $f(x)$ by functions that are linear on every subinterval of I, but that would give us a function that was not differentiable at the end-points of the subintervals. We could also use the Lagrange interpolation theorem to approximate $f(x)$ by a polynomial, and the polynomial would be differentiable everywhere, but there would be no reason to believe its derivative had any relation to the derivative of $f(x)$. So if we think of a "good" approximation as one that gives us the correct values of both $f(x)$ and $f'(x)$ at each of the points $a_0, \dots, a_k$, cubic splines are a good choice (and not only are they polynomials, they are polynomials of low degree). ◊

Here is an application along different lines. Again, we first prove a general theorem and then see how to use it.

We let $\mathbb{F}$ be arbitrary.

Theorem 5.2.15. *Let n be a positive integer, and let $e_1, \dots, e_n$ be positive integers. Let $a_1, \dots, a_n$ be distinct.*

Let $p(x)$ be the polynomial $(x - a_1)^{e_1}(x - a_2)^{e_2} \cdots (x - a_n)^{e_n}$ of degree $d = \sum_{i=1}^{n} e_i$. For each $i = 1, \dots, n$ and each $j = 1, \dots, e_i$, let $p_{ij}(x)$ be the polynomial $p_{ij}(x) = p(x)/(x - a_i)^j$.

Let $\mathcal{B} = \{p_{ij}(x) \,|\, i = 1, \dots, n,\ j = 1, \dots, e_i\}$. (Note that $\mathcal{B}$ has d elements.) Then $\mathcal{B}$ is a basis of $P_{d-1}(\mathbb{F})$.

Before proving this theorem, we note that it generalizes Corollary 5.2.9 and Corollary 5.2.11.

If we take $p(x) = (x - a)^{d+1}$, the elements of $\mathcal{B}$ are scalar multiples of the elements of the basis $\mathcal{B}$ of $P_d(\mathbb{F})$ of Corollary 5.2.10, and if we take $p(x) = (x - a_1) \cdots (x - a_{d+1})$, the elements of $\mathcal{B}$ are scalar multiples of the elements of the basis $\mathcal{B}$ of Corollary 5.2.11.

Proof. We proceed by complete induction on d.

If $d = 1$, then $p(x) = x - a_1$ and $p_{11}(x) = p(x)/(x - a_1) = 1$, and $\mathcal{B} = \{1\}$ is certainly a basis of $P_0(\mathbb{F})$.

Now assume the theorem is true for all polynomials $p(x)$ of degree less than d and consider a polynomial of degree d. We note that $\mathcal{B}$ has d elements and $\dim P_{d-1}(\mathbb{F}) = d$, so to show $\mathcal{B}$ is a basis we need only show it is linearly independent. Thus suppose we have a linear combination

$$q(x) = \sum c_{ij} p_{ij}(x) = 0.$$

Note that every polynomial in $\mathcal{B}$ except for $p_{ie_i}(x)$ has $(x - a_i)$ as a factor, and hence has the value 0 when $x = a_i$, and that $p_{ie_i} = \prod_{j \neq i}(x - a_j)^{e_j}$ does not, so that $p_{ie_i}(a_i) \neq 0$. Hence, setting $x = a_i$,

$$0 = q(a_i) = \sum c_{ij} p_{ij}(a_i) = c_{ie_i} p_{ie_i}(a_i)$$

and so $c_{ie_i} = 0$ for each i. Thus

$$q(x) = \sum_{j < e_i} c_{ij} p_{ij}(x) = 0.$$

But now note that for every i, every polynomial $p_{ij}(x)$ with $j < e_i$ is divisible by the polynomial $(x - a_1) \cdots (x - a_n) = q_0(x)$. Thus

$$0 = q(x) = q_0(x) \sum_{j < e_i} c_{ij} [p_{ij}(x)/q_0(x)].$$

But now note that the set of polynomials

$$\mathcal{C} = \{p_{ij}(x)/q_0(x)\}$$

is exactly the basis $\mathcal{B}$ we would obtain by starting with the polynomial $p_0(x) = (x - a_1)^{e_1 - 1}(x - a_2)^{e_2 - 1} \cdots (x - a_n)^{e_n - 1}$. Of course, $\deg p_0(x) < \deg p(x)$ so by the inductive hypothesis $\mathcal{C}$ is linearly independent, so each $c_{ij} = 0$ for $j < e_i$ as well.

Hence $\mathcal{B}$ is linearly independent as claimed. □

Corollary 5.2.16 (Partial fraction decomposition)**.** *Let*

$$p(x) = (x - a_1)^{e_1}(x - a_2)^{e_2} \cdots (x - a_n)^{e_n}$$

be a polynomial of degree $d = \sum_{i=1}^{n} e_i$. Let $q(x)$ be any polynomial of degree at most $d - 1$. Then there are unique constants $\{c_{ij}\}$ such that

$$\begin{aligned} \frac{q(x)}{p(x)} &= \frac{c_{11}}{x - a_1} + \frac{c_{12}}{(x - a_1)^2} + \cdots + \frac{c_{1e_1}}{(x - a_1)^{e_1}} \\ &+ \frac{c_{21}}{x - a_2} + \frac{c_{22}}{(x - a_2)^2} + \cdots + \frac{c_{2e_2}}{(x - a_2)^{e_2}} \\ &+ \cdots \\ &+ \frac{c_{n1}}{x - a_n} + \frac{c_{n2}}{(x - a_n)^2} + \cdots + \frac{c_{ne_n}}{(x - a_1)^{e_n}}. \end{aligned}$$

Proof. Since $\mathcal{B}$ is a basis, we may write $q(x)$ uniquely as

$$q(x) = \sum c_{ij} p_{ij}(x).$$

Now divide each side by $p(x)$. □

5.3. Bases and coordinates: vectors

In this section and the next we are guided by the following metaphor.

Bases give us coordinates, and coordinates are a language for describing vectors and linear transformations.

To explain this metaphor, let us see how human languages work. A human language is a way of giving names to objects. For example,

$$\begin{array}{lll} [*]_{\text{English}} = \text{star}, & [*]_{\text{French}} = \text{étoile}, & [*]_{\text{German}} = \text{Stern}; \\ [\to]_{\text{English}} = \text{arrow}, & [\to]_{\text{French}} = \text{flèche}, & [\to]_{\text{German}} = \text{Pfeil}. \end{array}$$

Similarly, if V is an n-dimensional vector space over a field $\mathbb{F}$, and $\mathcal{B}$ is any basis of V, then for any vector v in V we have

$$[v]_{\mathcal{B}} \quad \text{a vector in } \mathbb{F}^n,$$

the coordinate vector of v with respect to the basis $\mathcal{B}$, which we can think of as the name of the vector v in the $\mathcal{B}$ language.

As well, if $\mathcal{T}\colon V \to W$ is a linear transformation from an n-dimensional vector space V to an m-dimensional vector space W, both over the same field $\mathbb{F}$, and $\mathcal{B}$ and $\mathcal{C}$ are any bases of V and W, respectively, then we have

$$[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}} \quad \text{an } m\text{-by-}n \text{ matrix with entries in } \mathbb{F},$$

the matrix of $\mathcal{T}$ with respect to this pair of bases, which we can think of as the name of this linear transformation in the language given by this pair of bases.

Let us think about how human language works. First, when dealing with objects, sometimes it is easiest to work with them directly, but sometimes it is easiest to work with the powerful tools we human beings have developed to deal with them, i.e., words.

Similarly, when doing linear algebra, sometimes it is easiest to study vectors and linear transformations directly, but sometimes it is easiest to translate them into vectors in $\mathbb{F}^n$ and m-by-n matrices with entries in $\mathbb{F}$, where we have powerful computational tools to work with.

Also, as human beings, it is useful, and sometimes essential, for us to be able to translate between languages. Similarly, as mathematicians, it is not only useful, but often essential, for us to be able to translate between the coordinates and matrices given to us by different bases.

However, as human beings, if we have a problem in one language, and we translate it into a second language, we haven't helped solve the problem—we've just expressed it differently. In mathematics the situation is different. Often there is a preferred language in which to study a problem, and when we translate our problem into that language, it becomes much easier to solve.

Actually, we have already seen some instances of this. Let's, for example, consider $P_3(\mathbb{R})$, the vector space of polynomials of degree at most 3 with real coefficients. We have seen a number of different bases for $P_3(\mathbb{R})$. In particular, for any real number a we have the basis $\mathcal{B}_a = \{1, x-a, (x-a)^2/2, (x-a)^3/3!\}$. This is certainly the best basis to use if we want to study the behavior of a polynomial at (or near) the point $x = a$.

So if we wanted, for example, to find a cubic polynomial $f(x)$ with $f(0) = 7$, $f'(0) = 3$, $f''(0) = 2$, and $f'''(0) = 6$, we would use the basis $\mathcal{B}_0$ and immediately write down

$$f(x) = 7 + 3x + 2(x^2/2) + 6(x^3/6).$$

But if we wanted to find a cubic polynomial $g(x)$ with $g(1) = 5$, $g'(1) = 3$, $g''(1) = 4$, and $g'''(1) = 6$, it would be foolish to use the basis $\mathcal{B}_0$. Instead, we should use the basis $\mathcal{B}_1$, and immediately write down

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

However, suppose someone gave us the polynomial $g(x)$ to begin with, and asked us to study its behavior around $x = 0$. Then we should go ahead and re-express it in terms of the basis $\mathcal{B}_0$ (i.e., translate it from the $\mathcal{B}_1$-language into the $\mathcal{B}_0$-language), and when we do so, we obtain

$$g(x) = 3 + 2x + 4(x^2/2) + 6(x^3/6).$$

Conversely, if we started with $f(x)$ and we wanted to understand its behavior near $x = 1$, we should translate it from the $\mathcal{B}_0$-language to the $\mathcal{B}_1$-language to obtain

$$f(x) = 12 + 8(x-1) + 8((x-1)^2/2) + 6((x-1)^3/6).$$

We will be dealing with coordinates for vectors in this section, and matrices for linear transformations in the next section. But, looking ahead, we will simply say here that even when we are looking at $\mathbb{F}^n$, where we have a standard basis, that basis is not always the best basis to use, and instead we should be able to use the basis best adapted to our problem.

The basic idea behind coordinates is given to us by Lemma 3.3.3, which we repeat here, with slightly different wording to emphasize the point we want to make.

Lemma 5.3.1. *Let V be a vector space, and let $\mathcal{B}$ be a basis of V. Then every vector v in V can be expressed as a linear combination of the vectors in $\mathcal{B}$ in a unique way.*

This immediately leads us to the definition of coordinates.

Definition 5.3.2. Let V be an n-dimensional vector space over the field $\mathbb{F}$ and let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a basis of V. Then $[v]_{\mathcal{B}}$, the *coordinate vector of v in the $\mathcal{B}$ basis*, is given by: if $v = c_1v_1 + \cdots + c_nv_n$, then

$$[v]_{\mathcal{B}} = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

(Note that $[v]_{\mathcal{B}} \in \mathbb{F}^n$.) $\Diamond$

As we have said, we want to use coordinates to "translate" problems into ones we can more easily handle. The fact that this is a faithful translation is given to us by the following lemma.

Lemma 5.3.3. *Let V be an n-dimensional vector space over the field $\mathbb{F}$ and let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a basis of V. Then $\mathcal{T}\colon V \to \mathbb{F}^n$ given by $\mathcal{T}(v) = [v]_{\mathcal{B}}$ is an isomorphism.*

Proof. Its inverse $\mathcal{S}\colon \mathbb{F}^n \to V$ is given by

$$\mathcal{S}\left(\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}\right) = c_1 v_1 + \cdots + c_n v_n. \qquad \square$$

Example 5.3.4. (1) For any basis $\mathcal{B} = \{v_1, \ldots, v_n\}$,

$$[0]_{\mathcal{B}} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

as $0 = 0v_1 + \cdots + 0v_n$.

(2) If $\mathcal{B} = \{v_1, \ldots, v_n\}$,

$$[v_i]_{\mathcal{B}} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = e_i \quad \text{(with the 1 in the } i\text{th position)}$$

as $v_i = 0v_1 + \cdots + 1v_i + \cdots + 0v_n$. $\Diamond$

Example 5.3.5. Let $V = \mathbb{F}^n$, and let $\mathcal{E} = \{e_1, \ldots, e_n\}$ be the standard basis. If

$$v = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix},$$

then

$$\begin{aligned} v &= \begin{bmatrix} c_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ c_2 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \begin{bmatrix} 0 \\ 0 \\ \vdots \\ c_n \end{bmatrix} = c_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + c_n \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \\ &= c_1 e_1 + c_2 e_2 + \cdots + c_n e_n \end{aligned}$$

so

$$[v]_{\mathcal{E}} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}.$$

Thus a vector in $\mathbb{F}^n$ "looks like itself" in the standard basis. $\Diamond$

Example 5.3.6. Let $V = P_d(\mathbb{F})$, and let $\mathcal{B} = \{1, x, \ldots, x^d\}$. Then

$$[a_0 + a_1 x + \cdots + a_d x^d]_{\mathcal{B}} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \end{bmatrix}. \qquad \Diamond$$

Example 5.3.7. Let $V = \mathbb{F}^3$, and let $\mathcal{B}$ be the basis $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 9 \\ 7 \end{bmatrix} \right\}$ of V.

(1) If $v = \begin{bmatrix} -1 \\ 4 \\ 0 \end{bmatrix}$, find $[v]_{\mathcal{B}}$.

Answer. $[v]_{\mathcal{B}} = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$ if $v = cv_1 + cv_2 + cv_3$. Thus we have the system

$$c_1 \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} + c_2 \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} + c_3 \begin{bmatrix} 3 \\ 9 \\ 7 \end{bmatrix} = \begin{bmatrix} -1 \\ 4 \\ 0 \end{bmatrix},$$

which we solve to find $c_1 = 3$, $c_2 = 6$, $c_3 = 5$ so

$$[v_{\mathcal{B}}] = \begin{bmatrix} 3 \\ 6 \\ 5 \end{bmatrix}.$$

(2) If $[w]_{\mathcal{B}} = \begin{bmatrix} 4 \\ 0 \\ -1 \end{bmatrix}$, find w.

Answer. We see right away that

$$w = 4v_1 + 0v_2 - v_3 = 4 \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} + 0 \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} - \begin{bmatrix} 3 \\ 9 \\ 7 \end{bmatrix} = \begin{bmatrix} 1 \\ -1 \\ 5 \end{bmatrix}.$$

(Note, by Example 5.3.5, we could have phrased (1) as "If $[v]_{\mathcal{E}} = \begin{bmatrix} -1 \\ 4 \\ 0 \end{bmatrix}$, find $[v]_{\mathcal{B}}$" and we could have phrased (2) as "If $[w]_{\mathcal{B}} = \begin{bmatrix} 4 \\ 0 \\ -1 \end{bmatrix}$, find $[w]_{\mathcal{E}}$", if we had wished to do so.) $\Diamond$

Example 5.3.8. Let $\mathcal{B}$ be the basis $\{x(x-1), (x-1)(x-2), x(x-2)\}$ of $P_2(\mathbb{R})$. Let v be the vector (i.e., polynomial) $v = x^2 - 2$. We wish to find $[v]_{\mathcal{B}}$.

Answer. $[v]_{\mathcal{B}} = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$ if $v = c_1 v_1 + c_2 v_2 + c_3 v_3$.

Now for any basis $\mathcal{B}_0$, $\mathcal{T}\colon P_2(\mathbb{R}) \to \mathbb{R}^3$ by $\mathcal{T}(v) = [v]_{\mathcal{B}_0}$ is an isomorphism, so we will have $v = c_1v_1 + c_2v_2 + c_3v_3$ if and only if $[v]_{\mathcal{B}_0} = c_1[v_1]_{\mathcal{B}_0} + c_2[v_2]_{\mathcal{B}_0} + c_3[v_3]_{\mathcal{B}_0}$. Of course, we could take $\mathcal{B}_0 = \mathcal{B}$, but that wouldn't help us at all. Instead we take $\mathcal{B}_0 = \{1, x, x^2\}$. Then this becomes the equation

$$\begin{bmatrix} -2 \\ 0 \\ 1 \end{bmatrix} = c_1 \begin{bmatrix} 0 \\ -1 \\ 1 \end{bmatrix} + c_2 \begin{bmatrix} 2 \\ -3 \\ 1 \end{bmatrix} + c_3 \begin{bmatrix} 0 \\ -2 \\ 1 \end{bmatrix}$$

with solution $c_1 = 1$, $c_2 = -1$, $c_3 = 1$ so

$$[v]_{\mathcal{B}} = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}.$$

$\Diamond$

Example 5.3.9. Let $S = \{1+x+2x^2+4x^3, 2+3x+4x^2+6x^3, 1+x+3x^2+4x^3, 3+4x+6x^2+11x^3\} = \{v_1, v_2, v_3, v_4\}$, a set of four vectors in $P_3(\mathbb{R})$, a vector space of dimension 4. We ask whether S is a basis. Now for any basis $\mathcal{B}$, $\mathcal{T}\colon P_3(\mathbb{R}) \to \mathbb{R}^4$ by $\mathcal{T}(v) = [v]_{\mathcal{B}}$ is an isomorphism, so S is a basis if and only if $\mathcal{T}(S)$ is a basis. We choose $\mathcal{B} = \mathcal{B}_0 = \{1, x, x^2, x^3\}$, and then $\mathcal{T}(S) = \left\{ \begin{bmatrix} 1 \\ 1 \\ 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 4 \\ 6 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \\ 6 \\ 11 \end{bmatrix} \right\}$.

But now that we have a set of vectors in $\mathbb{R}^4$, we know how to decide whether they form a basis. We simply form the matrix A whose columns are these vectors, and row-reduce to decide whether A is invertible. We did so in Example 3.2.7(e) and found that the answer is yes—A *is* invertible. Hence we conclude that S is indeed a basis of $P_3(\mathbb{R})$. $\Diamond$

Remark 5.3.10. Referring back to Example 3.2.7(e), we were concerned with exactly the same set of vectors S there, as in Example 5.3.9, though we apparently solved the problem there without using coordinates. But in fact we did. We solved the problem there by looking at the coefficients of the various powers of x. But that is the same as taking coordinates in the $\mathcal{B}_0$ basis. So the point is that we have been using coordinates all along—and have seen how useful they are—in this particular case. Thus here we have formally introduced them, and have begun to see how useful they can be in general. $\Diamond$

Now we come to an important problem. Suppose we have two bases $\mathcal{B}$ and $\mathcal{C}$ of a vector space V, and we know $[v]_{\mathcal{B}}$, the coordinates of the vector v in the $\mathcal{B}$. How can we find $[v]_{\mathcal{C}}$, the coordinates of this vector in the $\mathcal{C}$ basis? Let us first solve this problem in principle, and then solve it in practice.

Theorem 5.3.11 (Change of basis for vectors)**.** *Let V be an n-dimensional vector space over a field $\mathbb{F}$, and let $\mathcal{B}$ and $\mathcal{C}$ be any two bases of V. Then there is an n-by-n matrix $P_{\mathcal{C}\leftarrow\mathcal{B}}$ with the property that*

$$[v]_{\mathcal{C}} = P_{\mathcal{C}\leftarrow\mathcal{B}}[v]_{\mathcal{B}} \quad \textit{for every } v \in V.$$

Let $\mathcal{B} = \{v_1, \dots, v_n\}$. Then

$$P_{\mathcal{C}\leftarrow\mathcal{B}} = \big[[v_1]_{\mathcal{C}} \big| [v_2]_{\mathcal{C}} \big| \dots \big| [v_n]_{\mathcal{C}}\big].$$

Proof. We know, by Lemma 5.3.3, that there is an isomorphism $\mathcal{T}_1\colon V \to \mathbb{F}^n$ given by $\mathcal{T}_1(v) = [v]_{\mathcal{B}}$, and similarly that there is an isomorphism $\mathcal{T}_2\colon V \to \mathbb{F}^n$ given by $\mathcal{T}_2(v) = [v]_{\mathcal{C}}$. Let $\mathcal{T}$ be the composition $\mathcal{T} = \mathcal{T}_2\mathcal{T}_1^{-1}\colon \mathbb{F}^n \to \mathbb{F}^n$. Then $\mathcal{T}$ is a linear transformation with

$$\mathcal{T}([v]_{\mathcal{B}}) = \mathcal{T}_2\mathcal{T}_1^{-1}([v]_{\mathcal{B}}) = \mathcal{T}_2(\mathcal{T}_1^{-1}([v]_{\mathcal{B}})) = \mathcal{T}_2(v) = [v]_{\mathcal{C}}.$$

But we know that any linear transformation $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^n$ is $\mathcal{T} = \mathcal{T}_P$ for some (unique) matrix P. So we let $P_{\mathcal{C}\leftarrow\mathcal{B}}$ be this matrix P.

We know that

$$P_{\mathcal{C}\leftarrow\mathcal{B}} = [P_{\mathcal{C}\leftarrow\mathcal{B}}e_1|P_{\mathcal{C}\leftarrow\mathcal{B}}e_2|\ldots|P_{\mathcal{C}\leftarrow\mathcal{B}}e_n].$$

But remember that $[v_i]_{\mathcal{B}} = e_i$. Then we see

$$P_{\mathcal{C}\leftarrow\mathcal{B}}e_i = P_{\mathcal{C}\leftarrow\mathcal{B}}[v_i]_{\mathcal{B}} = [v_i]_{\mathcal{C}}.$$ □

Definition 5.3.12. The matrix $P_{\mathcal{C}\leftarrow\mathcal{B}}$ is the *change of basis* matrix from the basis $\mathcal{B}$ to the basis $\mathcal{C}$. ◊

Let us return to our analogy of language to guide us in developing properties of change of basis matrices. We think of $P_{\mathcal{C}\leftarrow\mathcal{B}}$ as telling us how to translate from the $\mathcal{B}$-language to the $\mathcal{C}$-language.

Let us think of how we would translate between different human languages. To do so we would use a dictionary.

First suppose we wanted to translate from English to English, say. What would an English to English dictionary look like? It would be:

English	English
star	star
arrow	arrow

In fact, for any language, translating from that language to itself leaves all words unchanged, or in mathematical terms, is the identity transformation.

Next suppose we wanted to translate from English to German, or from German to English. Then we would use an English to German or a German to English dictionary, respectively. What would these two dictionaries look like? They would be:

English	German
star	Stern
arrow	Pfeil

German	English
Stern	star
Pfeil	arrow

We see that translating from German to English is the reverse of translating from English to German, and vice-versa. In mathematical terms, we would say that each of these operations is the inverse of the other.

Finally, suppose we wanted to translate from English to German, but we did not have an English to German dictionary available. If we had an English to French dictionary and a French to German dictionary, we would see

English	French
star	étoile
arrow	flèche

French	German
étoile	Stern
flèche	Pfeil

and we could accomplish our English to German translation by first doing an English to French translation and then following it by a French to German translation. In mathematical language, we would say we are taking the composition of these two intermediate translations.

Now we have a lemma which simply shows that the mathematics faithfully reflects these analogies.

Lemma 5.3.13. *Let $\mathcal{B}$, $\mathcal{C}$, and $\mathcal{D}$ be any bases of the finite-dimensional vector space V. Then:*

(1) $P_{\mathcal{B}\leftarrow\mathcal{B}} = I$ *(the identity matrix).*
(2) $P_{\mathcal{C}\leftarrow\mathcal{B}}$ *is invertible and* $P_{\mathcal{B}\leftarrow\mathcal{C}} = (P_{\mathcal{C}\leftarrow\mathcal{B}})^{-1}$.
(3) $P_{\mathcal{D}\leftarrow\mathcal{B}} = P_{\mathcal{D}\leftarrow\mathcal{C}} P_{\mathcal{C}\leftarrow\mathcal{B}}$.

Proof. (1) $P_{\mathcal{B}\leftarrow\mathcal{B}}$ has the property that

$$P_{\mathcal{B}\leftarrow\mathcal{B}}[v]_{\mathcal{B}} = [v]_{\mathcal{B}} \quad \text{for every vector } [v]_{\mathcal{B}} \text{ in } \mathbb{F}^n.$$

But that means $P_{\mathcal{B}\leftarrow\mathcal{B}}$ must be the identity matrix.

(3) On the one hand, by definition,

$$P_{\mathcal{D}\leftarrow\mathcal{B}}[v]_{\mathcal{B}} = [v]_{\mathcal{D}} \quad \text{for every vector } [v]_{\mathcal{B}} \text{ in } \mathbb{F}^n.$$

On the other hand,

$$\begin{aligned}(P_{\mathcal{D}\leftarrow\mathcal{C}} P_{\mathcal{C}\leftarrow\mathcal{B}})[v]_{\mathcal{B}} &= P_{\mathcal{D}\leftarrow\mathcal{C}}(P_{\mathcal{C}\leftarrow\mathcal{B}}[v]_{\mathcal{B}}) \\ &= P_{\mathcal{D}\leftarrow\mathcal{C}}[v]_{\mathcal{C}} \\ &= [v]_{\mathcal{D}} \quad \text{for every vector } [v]_{\mathcal{B}} \text{ in } \mathbb{F}^n\end{aligned}$$

and comparing these two answers we see we must have $P_{\mathcal{D}\leftarrow\mathcal{B}} = P_{\mathcal{D}\leftarrow\mathcal{C}} P_{\mathcal{C}\leftarrow\mathcal{B}}$.

(2) Take $\mathcal{D} = \mathcal{B}$. Then by (1) and (3) we have

$$P_{\mathcal{B}\leftarrow\mathcal{C}} P_{\mathcal{C}\leftarrow\mathcal{B}} = P_{\mathcal{B}\leftarrow\mathcal{B}} = I$$

and similarly

$$P_{\mathcal{C}\leftarrow\mathcal{B}} P_{\mathcal{B}\leftarrow\mathcal{C}} = P_{\mathcal{C}\leftarrow\mathcal{C}} = I$$

so the matrices $P_{\mathcal{B}\leftarrow\mathcal{C}}$ and $P_{\mathcal{C}\leftarrow\mathcal{B}}$ are inverses of each other. □

Now part (2) of this lemma says that any change of basis matrix must be invertible. We can also ask whether any invertible matrix is a change of basis matrix. The answer is yes, as we now see.

Lemma 5.3.14. *Let P be any invertible n-by-n matrix. Let $\mathcal{B}$ be any basis of V. Then there is a basis $\mathcal{C}$ of V with*

$$P_{\mathcal{C}\leftarrow\mathcal{B}} = P.$$

Proof. Let $Q = P^{-1}$. Write $Q = [q_1|q_2|\dots|q_n] = (q_{ij})$.

Let $\mathcal{B} = \{v_1, \dots, v_n\}$. Define $\mathcal{C} = \{w_1, \dots, w_n\}$ by

$$w_j = \sum_{i=1}^{n} q_{ij} v_i \quad \text{for each } j = 1, \dots, n,$$

so that

$$[w_j]_{\mathcal{B}} = q_j \quad \text{for each } j = 1, \dots, n.$$

Then by Theorem 5.3.11 (noting the roles of $\mathcal{B}$ and $\mathcal{C}$ have changed)

$$P_{\mathcal{B}\leftarrow\mathcal{C}} = \big[[w_1]_{\mathcal{B}}\big|[w_2]_{\mathcal{B}}\big|\dots\big|[w_n]_{\mathcal{B}}\big] = [q_1|q_2|\dots|q_n] = Q$$

and so

$$P_{\mathcal{C}\leftarrow\mathcal{B}} = Q^{-1} = P. \qquad \square$$

Now let us see in practice how to find $P_{\mathcal{C}\leftarrow\mathcal{B}}$. There are two methods: direct and indirect.

The direct method is simply to use the formula for $P_{\mathcal{C}\leftarrow\mathcal{B}}$ of Theorem 5.3.11. This formula tells us that the ith column of $P_{\mathcal{C}\leftarrow\mathcal{B}}$ is $[v_i]_{\mathcal{C}}$, the coordinate vector of v_i in the $\mathcal{C}$ basis. We know in general that finding the coordinates of a vector is simply a matter of solving a linear system, and we know how to do that.

Here is the indirect method, for $V = \mathbb{F}^n$. Let $\mathcal{B}$ be a basis of V, $\mathcal{B} = \{v_1, \dots, v_n\}$. Let $\mathcal{E}$ be the standard basis of $\mathbb{F}^n$.

1. Suppose we want to find $P_{\mathcal{E}\leftarrow\mathcal{B}}$. This is easy! We know

$$P_{\mathcal{E}\leftarrow\mathcal{B}} = \big[[v_1]_{\mathcal{E}}\big|[v_2]_{\mathcal{E}}\big|\dots\big|[v_n]_{\mathcal{E}}\big].$$

But we also know, by Example 5.3.5, that $[v_i]_{\mathcal{E}} = v_i$ ("a vector looks like itself in the standard basis"). Thus we simply see that if $\mathcal{B} = \{v_1, \dots, v_n\}$, then

$$P_{\mathcal{E}\leftarrow\mathcal{B}} = [v_1|v_2|\dots|v_n].$$

2. Suppose we want to find $P_{\mathcal{B}\leftarrow\mathcal{E}}$. We know $P_{\mathcal{B}\leftarrow\mathcal{E}} = (P_{\mathcal{E}\leftarrow\mathcal{B}})^{-1}$. But we just saw we could immediately write down $P_{\mathcal{E}\leftarrow\mathcal{B}}$, and we know to find the inverse of a matrix.

3. Suppose we want to find $P_{\mathcal{C}\leftarrow\mathcal{B}}$ in general. We introduce the standard basis $\mathcal{E}$ as an intermediate basis, and we then know

$$P_{\mathcal{C}\leftarrow\mathcal{B}} = P_{\mathcal{C}\leftarrow\mathcal{E}} P_{\mathcal{E}\leftarrow\mathcal{B}}$$

and using the last two observations we see

$$P_{\mathcal{C}\leftarrow\mathcal{B}} = (P_{\mathcal{E}\leftarrow\mathcal{C}})^{-1} P_{\mathcal{E}\leftarrow\mathcal{B}}.$$

Example 5.3.15. Let $V = \mathbb{F}^2$. Let $\mathcal{B} = \left\{\begin{bmatrix}1\\3\end{bmatrix}, \begin{bmatrix}2\\7\end{bmatrix}\right\}$, and let $\mathcal{C} = \left\{\begin{bmatrix}9\\4\end{bmatrix}, \begin{bmatrix}2\\1\end{bmatrix}\right\}$. Then we find:

$$P_{\mathcal{E}\leftarrow\mathcal{B}} = \begin{bmatrix}1 & 2\\3 & 7\end{bmatrix}, \quad P_{\mathcal{B}\leftarrow\mathcal{E}} = (P_{\mathcal{E}\leftarrow\mathcal{B}})^{-1} = \begin{bmatrix}7 & -2\\-3 & 1\end{bmatrix},$$

$$P_{\mathcal{E}\leftarrow\mathcal{C}} = \begin{bmatrix}9 & 2\\4 & 1\end{bmatrix}, \quad P_{\mathcal{C}\leftarrow\mathcal{E}} = (P_{\mathcal{E}\leftarrow\mathcal{C}})^{-1} = \begin{bmatrix}1 & -2\\-4 & 9\end{bmatrix},$$

$$P_{\mathcal{C}\leftarrow\mathcal{B}} = P_{\mathcal{C}\leftarrow\mathcal{E}} P_{\mathcal{E}\leftarrow\mathcal{B}} = \begin{bmatrix}1 & -2\\-4 & 9\end{bmatrix}\begin{bmatrix}1 & 2\\3 & 7\end{bmatrix} = \begin{bmatrix}-5 & -12\\23 & 55\end{bmatrix},$$

$$P_{\mathcal{B}\leftarrow\mathcal{C}} = P_{\mathcal{B}\leftarrow\mathcal{E}} P_{\mathcal{E}\leftarrow\mathcal{C}} = (P_{\mathcal{C}\leftarrow\mathcal{B}})^{-1} = \begin{bmatrix}55 & 12\\-23 & -5\end{bmatrix}.$$

Note that we must have

$$\begin{bmatrix} -5 & -12 \\ 23 & 55 \end{bmatrix} = P_{\mathcal{C}\leftarrow\mathcal{B}} = \left[\begin{bmatrix} 1 \\ 3 \end{bmatrix}_{\mathcal{C}} \quad \begin{bmatrix} 2 \\ 7 \end{bmatrix}_{\mathcal{C}} \right]$$

and this checks as

$$\begin{bmatrix} 1 \\ 3 \end{bmatrix} = (-5) \begin{bmatrix} 9 \\ 4 \end{bmatrix} + (23) \begin{bmatrix} 2 \\ 1 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} 2 \\ 7 \end{bmatrix} = (-12) \begin{bmatrix} 9 \\ 4 \end{bmatrix} + (55) \begin{bmatrix} 2 \\ 1 \end{bmatrix}. \qquad \Diamond$$

Remark 5.3.16. We have written the change of basis matrix from the basis $\mathcal{B}$ to the basis $\mathcal{C}$ as $P_{\mathcal{C}\leftarrow\mathcal{B}}$ as we feel this is a good mnemonic way to remember it, and because it also makes the equation $[v]_{\mathcal{C}} = P_{\mathcal{C}\leftarrow\mathcal{B}}[v]_{\mathcal{B}}$ easy to remember. It should be pointed out that some authors write $P_{\mathcal{C}\leftarrow\mathcal{B}}$ as $P_{\mathcal{B}}^{\mathcal{C}}$ and others write it as $P_{\mathcal{C}}^{\mathcal{B}}$, and you need to take particular care to note the author's notation. For if author A writes $P_{\mathcal{C}\leftarrow\mathcal{B}}$ as $P_{\mathcal{B}}^{\mathcal{C}}$, and author B writes $P_{\mathcal{C}\leftarrow\mathcal{B}}$ as $P_{\mathcal{C}}^{\mathcal{B}}$, then what author A means by $P_{\mathcal{B}}^{\mathcal{C}}$ is $P_{\mathcal{C}\leftarrow\mathcal{B}}$ but what author B means by the same symbol $P_{\mathcal{B}}^{\mathcal{C}}$ is $P_{\mathcal{B}\leftarrow\mathcal{C}}$, and these matrices are inverses of each other. $\Diamond$

We shall now use linear algebra to derive some identities for binomial coefficients.

Example 5.3.17. For any fixed n, let $V = P_n(\mathbb{R})$. For any fixed real number c, let $\mathcal{B}_c$ be the basis of V given by

$$\mathcal{B}_c = \{(x+c)^0, (x+c)^1, \ldots, (x+c)^n\}.$$

Here we understand that $(x+c)^0 = 1$.

In this example, we number the rows and columns of our matrices from 0 *to* n *rather than* 1 *to* $n+1$.

Let P_c be the change of basis matrix

$$P_c = P_{\mathcal{B}_0\leftarrow\mathcal{B}_c}.$$

Write $P_c = [p_0|p_1|\ldots|p_n] = (p_{ij})$. We know

$$p_j = [(x+c)^j]_{\mathcal{B}_0} \quad \text{for } j = 0, \ldots, n.$$

But we know how to express $(x+c)^j$ in terms of powers of x. This is just the binomial theorem:

$$(x+c)^j = \sum_{i=0}^{j} \binom{j}{i} c^{j-i} x^i.$$

The ith entry in p_j is just the coefficient of x^i in this expansion. Thus we see that

$$p_{ij} = \begin{cases} \binom{j}{i} c^{j-i} & \text{for } 0 \le i \le j, \\ 0 & \text{for } i > j. \end{cases}$$

Let us write this as $p_{ij}(c)$ to make the dependence on c clear.

Now suppose $c = a + b$. We know

$$P_c = P_{\mathcal{B}_0\leftarrow\mathcal{B}_c} = P_{\mathcal{B}_0\leftarrow\mathcal{B}_a} P_{\mathcal{B}_a\leftarrow\mathcal{B}_{a+b}}.$$

But we observe that

$$P_{\mathcal{B}_a\leftarrow\mathcal{B}_{a+b}} = P_{\mathcal{B}_0\leftarrow\mathcal{B}_b}$$

as the coefficients of the expansion of $(x+(a+b))^j = ((x+a)+b)^j$ in terms of powers of $x+a$ are the same as the coefficients of the expansion of $(x+b)^j$ in terms of powers of x. Thus we see that

$$P_{a+b} = P_a P_b.$$

However, we certainly know how to multiply matrices:

$$p_{ij}(a+b) = \sum_{k=0}^{n} p_{ik}(a)p_{kj}(b).$$

Now unless $i \leq k \leq j$, at least one of the factors $p_{ik}(a)$ or $p_{kj}(b)$ will be 0. Thus we obtain

$$p_{ij}(a+b) = \sum_{k=i}^{j} p_{ik}(a)p_{kj}(b).$$

(Note this will automatically be 0 unless $i \leq j$.)

Hence, substituting, we obtain the following identities for binomial coefficients:

$$\binom{j}{i}(a+b)^{j-i} = \sum_{k=i}^{j} \binom{k}{i}\binom{j}{k} a^{k-i}b^{j-k} \quad \text{for } i \leq j.$$

Doing a little algebra, we may rewrite these identities in the equivalent form

$$(a+b)^{j-i} = (j-i)! \sum_{k=i}^{j} \frac{a^{k-i}b^{j-k}}{(k-i)!\,(j-k)!} \quad \text{for } i \leq j.$$

These are valid for all a and b, where we understand $0^0 = 1$ and $0^m = 0$ if $m > 0$.

If $i = j$, then, regardless of the values of a and b, this is just the trivial identity $1 = 1$. But if $i < j$, then these are (highly) nontrivial identities.

Let's look at two particularly interesting special cases of these identities.

First suppose $a = 1$ and $b = -1$. Then $a + b = 0$. But P_0 is the change of basis matrix $P_0 = P_{\mathcal{B}_0 \leftarrow \mathcal{B}_0}$, which is the identity matrix. Thus $p_{ij}(0) = 1$ for $i = j$ and $p_{ij}(0) = 0$ for $i < j$.

Thus we obtain the identities

$$\sum_{k=i}^{j} \frac{(-1)^{j-k}}{(k-i)!\,(j-k)!} = \begin{cases} 1 & \text{for } i = j, \\ 0 & \text{for } i < j. \end{cases}$$

Next suppose $a = 1$ and $b = 1$, so $a + b = 2$. Then we obtain the identities

$$2^{j-i} = (j-i)! \sum_{k=i}^{j} \frac{1}{(k-i)!\,(j-k)!} \quad \text{for } i \leq j. \qquad \Diamond$$

5.4. Bases and matrices: linear transformations

In the last section, we saw how, given a basis $\mathcal{B}$ of an n-dimensional vector space V, we could assign to a vector v in V its coordinate vector $[v]_{\mathcal{B}}$ in $\mathbb{F}^n$.

In this section we will see how, given a basis $\mathcal{B}$ of an n-dimensional vector space V and a basis $\mathcal{C}$ of an m-dimensional vector space W, we can assign to a linear transformation $\mathcal{T}\colon V \to W$ its matrix $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ relative to these two bases, an m-by-n matrix with entries in $\mathbb{F}$.

Again, this enables us to translate problems about linear transformations into problems about matrices.

You'll recall that any linear transformation $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^m$ was $\mathcal{T} = \mathcal{T}_A$ for some A, and we called A the standard matrix of $\mathcal{T}$. As we shall see, A is the matrix of $\mathcal{T}$ relative to the standard bases $\mathcal{E}_n$ and $\mathcal{E}_m$ of $\mathbb{F}^n$ and $\mathbb{F}^m$, respectively, i.e., $A = [\mathcal{T}_A]_{\mathcal{E}_m\leftarrow\mathcal{E}_n}$. But if we choose different bases, we will in general get a different matrix for $\mathcal{T}_A$. (This is why we were careful to call A the *standard* matrix of $\mathcal{T}$, not just the matrix of $\mathcal{T}$.)

It will be important to understand how the matrix of $\mathcal{T}$ changes as we change the bases $\mathcal{B}$ and $\mathcal{C}$, just as it was important to understand how the coordinates $[v]_{\mathcal{B}}$ of a vector v change when we change the basis $\mathcal{B}$.

Continuing our metaphor, a choice of basis gives us a language to use when talking about linear transformations. But, as we will see, there is often a best choice of basis, i.e., a best language, to use when studying a particular $\mathcal{T}$.

For example, let us consider $\mathcal{T}_1\colon \mathbb{F}^2 \to \mathbb{F}^2$ given by $\mathcal{T}_1 = \mathcal{T}_{A_1}$, where

$$A_1 = \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix},$$

and $\mathcal{T}_2\colon \mathbb{F}^2 \to \mathbb{F}^2$ given by $\mathcal{T}_2 = \mathcal{T}_{A_2}$, where

$$A_2 = \begin{bmatrix} -13 & -9 \\ 30 & 20 \end{bmatrix}.$$

Now $\mathcal{T}_1$ has an easy geometric meaning. We observe that $\mathbb{F}^2$ has standard basis $\mathcal{E} = \{e_1, e_2\}$, and that

$$\mathcal{T}_1(e_1) = \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \end{bmatrix} = 2\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

and

$$\mathcal{T}_1(e_2) = \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 5 \end{bmatrix} = 5\begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Thus $\mathcal{T}_1$ preserves the direction of e_1, but stretches it by a factor of 2, and $\mathcal{T}_1$ preserves the direction of e_2, but stretches it by a factor of 5.

On the other hand, $\mathcal{T}_2$ looks like a mess. But that appearance is deceiving, as instead of the standard basis we could take the basis $\mathcal{B} = \left\{\begin{bmatrix} 3 \\ -5 \end{bmatrix}, \begin{bmatrix} -1 \\ 2 \end{bmatrix}\right\} = \{v_1, v_2\}$, and then we would see that

$$\mathcal{T}_2(v_1) = \begin{bmatrix} -13 & -9 \\ 30 & 20 \end{bmatrix}\begin{bmatrix} 3 \\ -5 \end{bmatrix} = \begin{bmatrix} 6 \\ -10 \end{bmatrix} = 2\begin{bmatrix} 3 \\ -5 \end{bmatrix}$$

and

$$\mathcal{T}_2(v_2) = \begin{bmatrix} -13 & -9 \\ 30 & 20 \end{bmatrix}\begin{bmatrix} -1 \\ 2 \end{bmatrix} = \begin{bmatrix} -5 \\ 10 \end{bmatrix} = 5\begin{bmatrix} -1 \\ 2 \end{bmatrix}.$$

Thus we see that $\mathcal{T}_2$ has exactly the same geometry as $\mathcal{T}_1$. $\mathcal{T}_2$ preserves the direction of v_1, but stretches it by a factor of 2, and $\mathcal{T}_2$ preserves the direction of v_2, but stretches it by a factor of 5.

Thus, while we should use the basis $\mathcal{E}$ to study $\mathcal{T}_1$, we should use the basis $\mathcal{B}$ to study $\mathcal{T}_2$. (Naturally, you might ask how we found the basis $\mathcal{B}$ and the stretching factors for $\mathcal{T}_2$. This is the topic of eigenvalues and eigenvectors, which we will be devoting a lot of attention to later. But at this point we just wanted to observe that it is often useful to choose the "right" basis to study a problem.)

Here is the basic construction.

Theorem 5.4.1. *Let V be an n-dimensional vector space over $\mathbb{F}$, and let W be an m-dimensional vector space over $\mathbb{F}$. Let $\mathcal{T}\colon V \to W$ be a linear transformation.*

Let $\mathcal{B}$ be a basis of V and let $\mathcal{C}$ be a basis of W. Then there is a unique m-by-n matrix $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ such that

$$[\mathcal{T}(v)]_{\mathcal{C}} = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[v]_{\mathcal{B}} \quad \textit{for every } v \in V.$$

Let $\mathcal{B} = \{v_1, \dots, v_n\}$. Then

$$[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}} = \big[[\mathcal{T}(v_1)]_{\mathcal{C}}\big|[\mathcal{T}(v_2)]_{\mathcal{C}}\big|\dots\big|[\mathcal{T}(v_n)]_{\mathcal{C}}\big].$$

Proof. Let $\mathcal{S}_1\colon V \to \mathbb{F}^n$ be the coordinate isomorphism $\mathcal{S}_1(v) = [v]_{\mathcal{B}}$, and let $\mathcal{S}_2\colon W \to \mathbb{F}^m$ be the coordinate isomorphism $\mathcal{S}_2(w) = [w]_{\mathcal{C}}$. Then we have a linear transformation $\mathcal{T}'\colon \mathbb{F}^n \to \mathbb{F}^m$ defined by $\mathcal{T}' = \mathcal{S}_2\mathcal{T}\mathcal{S}_1^{-1}$.

Now let v be any vector in V. Then $\mathcal{S}_1(v) = [v]_{\mathcal{B}}$, so $\mathcal{S}_1^{-1}([v]_{\mathcal{B}}) = v$. But then

$$\begin{aligned}\mathcal{T}'([v]_{\mathcal{B}}) &= (\mathcal{S}_2\mathcal{T}\mathcal{S}_1^{-1})(\mathcal{S}_1(v)) \\ &= (\mathcal{S}_2\mathcal{T})(v) = \mathcal{S}_2(\mathcal{T}(v)) = [\mathcal{T}(v)]_{\mathcal{C}}.\end{aligned}$$

But $\mathcal{T}'$ is a linear transformation so there is a unique matrix A with $\mathcal{T}'([v]_{\mathcal{B}}) = \mathcal{T}_A([v]_{\mathcal{B}}) = A[v]_{\mathcal{B}}$ for every $[v]_{\mathcal{B}}$ in $\mathbb{F}^n$.

Comparing these two equations, we see

$$[\mathcal{T}(v)]_{\mathcal{C}} = A[v]_{\mathcal{B}} \quad \text{for every } v \text{ in } V$$

so we set $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}} = A$.

We know that $[v_i]_{\mathcal{B}} = e_i$ for each i. Thus

$$[\mathcal{T}(v_i)]_{\mathcal{C}} = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[v_i]_{\mathcal{B}} = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}e_i.$$

But for any matrix A, we know that

$$A = [Ae_1|Ae_2|\dots|Ae_n].$$

Hence we conclude that

$$\begin{aligned}[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}} &= \big[[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}e_1\big|[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}e_2\big|\dots\big|[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}e_n\big] \\ &= \big[[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[v_1]_{\mathcal{B}}\big|[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[v_2]_{\mathcal{B}}\big|\dots\big|[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[v_n]_{\mathcal{B}}\big] \\ &= \big[[\mathcal{T}(v_1)]_{\mathcal{C}}\big|[\mathcal{T}(v_2)]_{\mathcal{C}}\big|\dots\big|[\mathcal{T}(v_n)]_{\mathcal{C}}\big].\end{aligned}$$ □

Definition 5.4.2. In the situation of Theorem 5.4.1, the matrix $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ is the *matrix of the linear transformation $\mathcal{T}$ in* (or *with respect to*) *the bases $\mathcal{B}$ and $\mathcal{C}$* of V and W, respectively. ◊

Example 5.4.3. Let $V = \mathbb{F}^n$, and $W = \mathbb{F}^m$, and let $\mathcal{T}\colon V \to W$ be $\mathcal{T} = \mathcal{T}_A$, i.e., $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^m$ by $\mathcal{T}(v) = \mathcal{T}_A(v) = Av$.

Let $\mathcal{E}_n$ be the standard basis of $\mathbb{F}^n$, and let $\mathcal{E}_m$ be the standard basis of $\mathbb{F}^m$. Then $[\mathcal{T}]_{\mathcal{E}_m \leftarrow \mathcal{E}_n}$ is defined by

$$[\mathcal{T}(v)]_{\mathcal{E}_m} = [\mathcal{T}]_{\mathcal{E}_m \leftarrow \mathcal{E}_n}[v]_{\mathcal{E}_n},$$

i.e.,

$$[Av]_{\mathcal{E}_m} = [\mathcal{T}]_{\mathcal{E}_m \leftarrow \mathcal{E}_n}[v]_{\mathcal{E}_n}.$$

But recall from Example 5.3.5 that $[v]_{\mathcal{E}_n} = v$, and similarly $[Av]_{\mathcal{E}_m} = Av$ ("a vector looks like itself in the standard basis"). Thus we see

$$Av = [\mathcal{T}_A]_{\mathcal{E}_m \leftarrow \mathcal{E}_n} v$$

and so

$$[\mathcal{T}_A]_{\mathcal{E}_m \leftarrow \mathcal{E}_n} = A.$$

Thus the standard matrix of the linear transformation $\mathcal{T}_A$ is the matrix of $\mathcal{T}_A$ with respect to the standard bases. ("The linear transformation that is multiplication by the matrix A looks like itself in the standard bases.") $\Diamond$

Remark 5.4.4. We will often be considering a linear transformation $\mathcal{T}\colon V \to V$ and be choosing a basis $\mathcal{B}$ of V. Then we will have $[\mathcal{T}]_{\mathcal{B} \leftarrow \mathcal{B}}$. We abbreviate this by $[\mathcal{T}]_{\mathcal{B}}$ and call this the matrix of $\mathcal{T}$ in (or with respect to) the basis $\mathcal{B}$. Thus in this notation, $[\mathcal{T}(v)]_{\mathcal{B}} = [\mathcal{T}]_{\mathcal{B}}[v]_{\mathcal{B}}$ for every vector $v \in V$. $\Diamond$

Example 5.4.5. Let $V = P_4(\mathbb{R})$.

Let $\mathcal{B}$ be the basis $\{1, x, x^2, x^3, x^4\}$ of V.

Let $\mathcal{C}$ be the basis $\{1, x, x(x+1), x(x+1)(x+2), x(x+1)(x+2)(x+3)\}$ of V.

(1) Let $\mathcal{T}\colon V \to V$ be the linear transformation $\mathcal{T}(p(x)) = xp'(x)$. We compute (easily):

$$\begin{aligned}
\mathcal{T}(1) &= 0,\\
\mathcal{T}(x) &= x,\\
\mathcal{T}(x^2) &= 2x^2,\\
\mathcal{T}(x^3) &= 3x^3,\\
\mathcal{T}(x^4) &= 4x^4,
\end{aligned}$$

and so we see

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 2 & 0 & 0\\ 0 & 0 & 0 & 3 & 0\\ 0 & 0 & 0 & 0 & 4 \end{bmatrix}.$$

We also compute (with more work):

$$\begin{aligned}
\mathcal{T}(1) &= 0, \\
\mathcal{T}(x) &= x, \\
\mathcal{T}(x(x+1)) &= 2[x(x+1)] - x, \\
\mathcal{T}(x(x+1)(x+2)) &= 3[x(x+1)(x+2)] - 3[x(x+1)] - x, \\
\mathcal{T}(x(x+1)(x+2)(x+3)) &= 4[x(x+1)(x+2)(x+3)] - 6[x(x+1)(x+2)] \\
&\quad - 4[x(x+1)] - 2x,
\end{aligned}$$

and so we see

$$[\mathcal{T}]_{\mathcal{C}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & -2 \\ 0 & 0 & 2 & -3 & -4 \\ 0 & 0 & 0 & 3 & -6 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix}.$$

(2) Let $\mathcal{S}\colon V \to V$ be the linear transformation $\mathcal{S}(p(x)) = x(p(x+1) - p(x))$. We compute (easily):

$$\begin{aligned}
\mathcal{S}(1) &= 0, \\
\mathcal{S}(x) &= x, \\
\mathcal{S}(x(x+1)) &= 2[x(x+1)], \\
\mathcal{S}(x(x+1)(x+2)) &= 3[x(x+1)(x+2)], \\
\mathcal{S}(x(x+1)(x+2)(x+3)) &= 4[x(x+1)(x+2)(x+3)],
\end{aligned}$$

and so we see

$$[\mathcal{S}]_{\mathcal{C}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix}.$$

We also compute (with more work):

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

and so we see

$$[\mathcal{S}]_{\mathcal{B}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 3 & 4 \\ 0 & 0 & 0 & 3 & 6 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix}. \qquad \Diamond$$

Now let us see how to change bases for linear transformations. Once again, we shall motivate this by a consideration of human languages.

Suppose we have the transformation $\mathcal{T}$ on objects given by:

$$\mathcal{T}(*) = *** \cdots,$$
$$\mathcal{T}(\rightarrow) = \rightarrow\rightarrow\rightarrow \cdots.$$

That is, $\mathcal{T}$ takes an object to several of the same objects. Linguistically, this corresponds to taking the plural.

So suppose we want to take the plural of Stern, the German word for $*$, or Pfeil, the German word for $\rightarrow$, but we don't know how to do so. Suppose on the other hand we have a very good knowledge of English, so that we can take plurals of English words. Suppose we also have very complete German-English and English-German dictionaries at our disposal.

Then we could proceed as follows:

First we use our German-English dictionary to translate the German words into English words:

German	English
Stern	star
Pfeil	arrow

Then we use our knowledge of English to take the English plural:

star $\rightarrow$ stars

arrow $\rightarrow$ arrows

Then we use our English-German dictionary to translate the English words to German words:

English	German
stars	Sterne
arrows	Pfeile

In this way we have (correctly) found that:

The plural of the German word Stern is Sterne.
The plural of the German word Pfeil is Pfeile.

To make a long story short:

For $*$, we went Stern $\rightarrow$ star $\rightarrow$ stars $\rightarrow$ Sterne to get $*** \cdots$.
For $\rightarrow$, we went Pfeil $\rightarrow$ arrow $\rightarrow$ arrows $\rightarrow$ Pfeile to get $\rightarrow\rightarrow\rightarrow \cdots$.

This analogy is accurately reflected in the mathematics.

Theorem 5.4.6 (Change of basis for linear transformations)**.** *Let V be an n-dimensional vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. Let $\mathcal{B}$ and $\mathcal{C}$ be any two bases of V. Then*

$$[\mathcal{T}]_{\mathcal{C}} = P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}}P_{\mathcal{B}\leftarrow\mathcal{C}},$$

where $P_{\mathcal{C}\leftarrow\mathcal{B}}$ and $P_{\mathcal{B}\leftarrow\mathcal{C}}$ are change of basis matrices.

Proof. We compute, for every $[v]_{\mathcal{C}}$:

$$\begin{aligned}(P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}}P_{\mathcal{B}\leftarrow\mathcal{C}})([v]_{\mathcal{C}}) &= (P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}})(P_{\mathcal{B}\leftarrow\mathcal{C}}[v]_{\mathcal{C}})\\ &= (P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}})[v]_{\mathcal{B}}\\ &= P_{\mathcal{C}\leftarrow\mathcal{B}}([\mathcal{T}]_{\mathcal{B}}[v]_{\mathcal{B}})\\ &= P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}(v)]_{\mathcal{B}}\\ &= [\mathcal{T}(v)]_{\mathcal{C}}.\end{aligned}$$

But $[\mathcal{T}]_{\mathcal{C}}$ is the unique matrix such that for every $[v]_{\mathcal{C}}$

$$[\mathcal{T}]_{\mathcal{C}}[v]_{\mathcal{C}} = [\mathcal{T}(v)]_{\mathcal{C}},$$

so we must have that

$$[\mathcal{T}]_{\mathcal{C}} = P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}}P_{\mathcal{B}\leftarrow\mathcal{C}}. \qquad \square$$

Corollary 5.4.7. *In the situation of Theorem* 5.4.6*,*

$$\begin{aligned}[\mathcal{T}]_{\mathcal{C}} &= (P_{\mathcal{B}\leftarrow\mathcal{C}})^{-1}[\mathcal{T}]_{\mathcal{B}}P_{\mathcal{B}\leftarrow\mathcal{C}}\\ &= P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}]_{\mathcal{B}}(P_{\mathcal{C}\leftarrow\mathcal{B}})^{-1}.\end{aligned}$$

Proof. By Lemma 5.3.13, we know that

$$P_{\mathcal{B}\leftarrow\mathcal{C}} = (P_{\mathcal{C}\leftarrow\mathcal{B}})^{-1} \quad\text{and}\quad P_{\mathcal{C}\leftarrow\mathcal{B}} = (P_{\mathcal{B}\leftarrow\mathcal{C}})^{-1}. \qquad \square$$

This leads us to the following definition.

Definition 5.4.8. Two matrices A and B are *similar* if there is an invertible matrix P with $A = P^{-1}BP$ (or equivalently if there is an invertible matrix P with $B = PAP^{-1}$). ◊

Thus we conclude:

Corollary 5.4.9. *Let A and B be n-by-n matrices. Then A and B are similar if and only if they are both the matrix of the same linear transformation $\mathcal{T}$ with respect to some pair of bases $\mathcal{B}$ and $\mathcal{C}$.*

Proof. Immediate from Corollary 5.4.7 and the fact that any invertible matrix is a change of basis matrix (Lemma 5.3.14). □

Here is a reciprocal viewpoint. We say that two linear transformations $\mathcal{T}_1$ and $\mathcal{T}_2$ are *conjugate* if there is an invertible linear transformation $\mathcal{S}$ with $\mathcal{T}_1 = \mathcal{S}^{-1}\mathcal{T}_2\mathcal{S}$ (or equivalently $\mathcal{T}_2 = \mathcal{S}\mathcal{T}_1\mathcal{S}^{-1}$).

Corollary 5.4.10. *Two linear transformations $\mathcal{T}_1$ and $\mathcal{T}_2$ are conjugate if and only if there are bases $\mathcal{B}$ and $\mathcal{C}$ for which*

$$[\mathcal{T}_1]_{\mathcal{B}} = [\mathcal{T}_2]_{\mathcal{C}}.$$

Proof. If $[\mathcal{T}_1]_{\mathcal{B}} = [\mathcal{T}_2]_{\mathcal{C}}$, then by Corollary 5.4.7

$$[\mathcal{T}_1]_{\mathcal{B}} = (P_{\mathcal{C}\leftarrow\mathcal{B}})^{-1}[\mathcal{T}_2]_{\mathcal{B}}P_{\mathcal{B}\leftarrow\mathcal{C}},$$

so if we let $\mathcal{S}$ be the linear transformation with $[\mathcal{S}]_{\mathcal{B}} = P_{\mathcal{B}\leftarrow\mathcal{C}}$,

$$\begin{aligned}[\mathcal{T}_1]_{\mathcal{B}} &= [\mathcal{S}]_{\mathcal{B}}^{-1}[\mathcal{T}_2]_{\mathcal{B}}[\mathcal{S}]_{\mathcal{B}} \\ &= [\mathcal{S}^{-1}]_{\mathcal{B}}[\mathcal{T}_2]_{\mathcal{B}}[\mathcal{S}]_{\mathcal{B}} = [\mathcal{S}^{-1}\mathcal{T}_2\mathcal{S}]_{\mathcal{B}}\end{aligned}$$

and so, since a linear transformation is determined by its matrix in any basis, $\mathcal{T}_1 = \mathcal{S}^{-1}\mathcal{T}_2\mathcal{S}$.

On the other hand, if $\mathcal{T}_1 = \mathcal{S}^{-1}\mathcal{T}_2\mathcal{S}$, then

$$[\mathcal{T}_1]_{\mathcal{B}} = [\mathcal{S}]_{\mathcal{B}}[\mathcal{T}_2]_{\mathcal{B}}[\mathcal{S}]_{\mathcal{B}}^{-1}.$$

Let $\mathcal{C}$ be the basis with $P_{\mathcal{C}\leftarrow\mathcal{B}} = [\mathcal{S}]_{\mathcal{B}}$. Then

$$[\mathcal{T}_1]_{\mathcal{B}} = P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{T}_2]_{\mathcal{B}}(P_{\mathcal{C}\leftarrow\mathcal{B}})^{-1} = [\mathcal{T}_2]_{\mathcal{C}}$$

by Corollary 5.4.7. □

Remark 5.4.11. Let V be an n-dimensional vector space and let $\mathcal{S}\colon V \to V$ and $\mathcal{T}\colon V \to V$ be linear transformations. (Let A and B be n-by-n matrices.) In general, $\mathcal{ST} \neq \mathcal{TS}$, but we may ask about the relation between the two. (In general, $AB \neq BA$, but we may ask about the relation between the two.) If at least one of the two is invertible, then they are conjugate: $\mathcal{ST} = \mathcal{T}^{-1}(\mathcal{TS})\mathcal{T}$ or $\mathcal{TS} = \mathcal{S}^{-1}(\mathcal{ST})\mathcal{S}$. But otherwise they need not be. (If at least one of the two is invertible, then they are similar: $AB = B^{-1}(BA)B$ or $BA = A^{-1}(AB)A$. But otherwise they need not be.) Here is an example to illustrate this:

Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Then $AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $BA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ so they are not similar.

But we will see when we discuss Jordan canonical form in Chapter 8 below that there is a close relationship between the two. ◊

Example 5.4.12. Let $\mathcal{T}_1\colon \mathbb{F}^2 \to \mathbb{F}^2$ by $\mathcal{T}_1(v) = A_1 v$ with

$$A_1 = \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix}$$

and $\mathcal{T}_2\colon \mathbb{F}^2 \to \mathbb{F}^2$ by $\mathcal{T}_2(v) = A_2 v$ with

$$A_2 = \begin{bmatrix} -13 & -9 \\ 30 & 20 \end{bmatrix}.$$

Let $\mathcal{E} = \{e_1, e_2\} = \left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right\}$, and let $\mathcal{B} = \{v_1, v_2\} = \left\{\begin{bmatrix} 3 \\ -5 \end{bmatrix}, \begin{bmatrix} -1 \\ 2 \end{bmatrix}\right\}$.

Then, as we have computed,

$$\begin{aligned}\mathcal{T}_1(e_1) &= 2e_1, \\ \mathcal{T}_1(e_2) &= 5e_2,\end{aligned}$$

so

$$[\mathcal{T}_1]_{\mathcal{E}} = \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix},$$

and

$$\begin{aligned}\mathcal{T}_2(v_1) &= 2v_1, \\ \mathcal{T}_2(v_2) &= 5v_2,\end{aligned}$$

so

$$[\mathcal{T}_2]_{\mathcal{B}} = \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix}.$$

Thus $[\mathcal{T}_1]_{\mathcal{E}} = [\mathcal{T}_2]_{\mathcal{B}}$ so $\mathcal{T}_1$ and $\mathcal{T}_2$ are conjugate.

Furthermore

$$[\mathcal{T}_2]_{\mathcal{B}} = P_{\mathcal{B}\leftarrow\mathcal{E}}[\mathcal{T}_2]_{\mathcal{E}}P_{\mathcal{E}\leftarrow\mathcal{B}} = (P_{\mathcal{E}\leftarrow\mathcal{B}})^{-1}[\mathcal{T}_2]_{\mathcal{E}}P_{\mathcal{E}\leftarrow\mathcal{B}}.$$

But of course $[\mathcal{T}_1]_{\mathcal{E}} = A_1$ and $[\mathcal{T}_2]_{\mathcal{E}} = A_2$.

We know that we can immediately write down $P_{\mathcal{E}\leftarrow\mathcal{B}}$,

$$P_{\mathcal{E}\leftarrow\mathcal{B}} = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix},$$

so we obtain the matrix equation

$$\begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix} = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}^{-1} \begin{bmatrix} -13 & -9 \\ 30 & 20 \end{bmatrix} \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}. \qquad \Diamond$$

Example 5.4.13. We saw in Example 5.4.5 (using the notation there), that

$$[\mathcal{S}]_{\mathcal{C}} = [\mathcal{T}]_{\mathcal{B}}$$

so that $\mathcal{S}$ and $\mathcal{T}$ are conjugate.

Furthermore, note that it is straightforward to write down $P_{\mathcal{B}\leftarrow\mathcal{C}}$—we just have to multiply out the polynomials and take the coefficients of the various power of x. We find

$$P_{\mathcal{B}\leftarrow\mathcal{C}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 6 \\ 0 & 0 & 1 & 3 & 11 \\ 0 & 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

But we know that

$$[\mathcal{T}]_{\mathcal{B}} = P_{\mathcal{B}\leftarrow\mathcal{C}}[\mathcal{T}]_{\mathcal{C}}P_{\mathcal{C}\leftarrow\mathcal{B}} = P_{\mathcal{B}\leftarrow\mathcal{C}}[\mathcal{T}]_{\mathcal{C}}(P_{\mathcal{B}\leftarrow\mathcal{C}})^{-1}$$

and

$$[\mathcal{S}]_{\mathcal{C}} = P_{\mathcal{C}\leftarrow\mathcal{B}}[\mathcal{S}]_{\mathcal{B}}P_{\mathcal{B}\leftarrow\mathcal{C}} = (P_{\mathcal{B}\leftarrow\mathcal{C}})^{-1}[\mathcal{S}]_{\mathcal{B}}P_{\mathcal{B}\leftarrow\mathcal{C}}.$$

Thus we obtain the matrix equations

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 6 \\ 0 & 0 & 1 & 3 & 11 \\ 0 & 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & -2 \\ 0 & 0 & 2 & 3 & -4 \\ 0 & 0 & 0 & 3 & 6 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 6 \\ 0 & 0 & 1 & 3 & 11 \\ 0 & 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}^{-1}$$

and

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 6 \\ 0 & 0 & 1 & 3 & 11 \\ 0 & 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 3 & 4 \\ 0 & 0 & 0 & 3 & 6 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 6 \\ 0 & 0 & 1 & 3 & 11 \\ 0 & 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

$\Diamond$

5.5. The dual of a vector space

In this section we introduce dual spaces. The dual space is something we have already seen, without giving it a name, but here we investigate it intensively.

Definition 5.5.1. The *dual space* V^* of a vector space V is the vector space $V^* = L(V, \mathbb{F})$, the vector space of linear transformations $\mathcal{T}: V \to \mathbb{F}$. ◊

To see that this definition makes sense, note that $\mathbb{F}$ itself is an $\mathbb{F}$-vector space, and remember that for any two $\mathbb{F}$-vector spaces V and W, $L(V, W)$ is an $\mathbb{F}$-vector space (Theorem 4.1.9).

Definition 5.5.2. Let $\mathcal{B} = \{v_1, v_2, \dots\}$ be a basis of the vector space V. Then $\mathcal{B}^* = \{u_1^*, u_2^*, \dots\}$ is the subset of V^* defined as follows:

$$u_i^*(v_i) = 1, \quad u_i^*(v_j) = 0 \quad \text{for } j \neq i. \qquad \Diamond$$

Let us see that this definition makes sense. Since $\mathcal{B}$ is a basis of V, there is a unique linear transformation $\mathcal{T}: V \to \mathbb{F}$ taking prescribed values on the elements of $\mathcal{B}$ (Theorem 4.3.1). So for each i, there is a unique $\mathcal{T}: V \to \mathbb{F}$ with $\mathcal{T}(v_i) = 1$ and $\mathcal{T}(v_j) = 0$ for $j \neq i$, and we are calling that linear transformation u_i^*.

Lemma 5.5.3. (1) *For any basis $\mathcal{B}$ of V, $\mathcal{B}^*$ is a linearly independent set in V^*.*

(2) *If V is finite dimensional, then $\mathcal{B}^*$ is a basis of V^*.*

Proof. (1) Suppose $c_1 u_1^* + \cdots + c_k u_k^* = 0$. Of course, 0 in V^* means the function that is identically 0. Then

$$(c_1 u_1^* + \cdots + c_k u_k^*)(v) = 0 \quad \text{for every } v \in V.$$

Setting $v = v_i$, for $i = 1, \dots, k$,

$$\begin{aligned} 0 = (c_1 u_1^* + \cdots + c_k u_k^*)(v_i) &= c_1 u_1^*(v_i) + \cdots + c_i u_i^*(v_i) + \cdots + c_k u_k^*(v_i) \\ &= c_1 0 + \cdots + c_i 1 + \cdots + c_k 0 = c_i \end{aligned}$$

and so $\mathcal{B}^*$ is linearly independent.

(2) Suppose V is finite dimensional, say of dimension n, and let u^* be any element of V^*. Let $c_i = u^*(v_i)$, $i = 1, \dots, n$. Then, as the above computation shows,

$$(c_1 u_1^* + \cdots + c_k u_k^*)(v_i) = c_i = u^*(v_i), \quad i = 1, \dots, n.$$

Thus the linear transformations u^* and $c_1 u_1^* + \cdots + c_n u_n^*$ agree on the basis $\mathcal{B}$ of V, so $u^* = c_1 u_1^* + \cdots + c_n u_n^*$ by Theorem 4.3.1.

Hence $\mathcal{B}^*$ also spans V^*, so that $\mathcal{B}^*$ is a basis of V^*. □

Corollary 5.5.4. *If V is finite dimensional, then*

$$\dim V = \dim V^*$$

and hence V and V^* are isomorphic.

Proof. $\mathcal{B} = \{v_1, \dots, v_n\}$ and $\mathcal{B}^* = \{u_1^*, \dots, u_n^*\}$ have the same number of elements. □

Definition 5.5.5. If V is finite dimensional and $\mathcal{B}$ is a basis of V, the basis $\mathcal{B}^*$ of V^* constructed in Definition 5.5.2 is the *dual basis* of V. ◊

Here is a special case of this definition. If we let $V = \mathbb{F}^n$ and we let $\mathcal{B}$ be the standard basis $\mathcal{E} = \{e_1, \ldots, e_n\}$, then the dual basis $\mathcal{E}^* = \{e_1^*, \ldots, e_n^*\}$ of $(\mathbb{F}^n)^*$, defined by $e_i^*(e_j) = 1$ if $j = i$ and 0 if $j \neq i$, is the *standard basis* of $(\mathbb{F}^n)^*$.

Remark 5.5.6. If V is infinite dimensional, then $\mathcal{B}^*$ is certainly *not* a basis of V^*. For if $\mathcal{B} = \{v_1, v_2, \ldots\}$ is infinite, we have the linear transformation $u^*: V \to \mathbb{F}$ defined by $u^*(v_i) = 1$ for each i. This is *not* a linear combination of $u_1^*, \ldots, u_n^*$, as this would have to be $u_1^* + u_2^* + \cdots$, which does not make sense as a linear combination is a *finite* sum. $\Diamond$

Corollary 5.5.7. *For any vector space V, V is isomorphic to a subspace of its dual V^*.*

Proof. Let $\mathcal{B}$ be a basis of V and let $\mathcal{B}^*$ be as in Definition 5.5.2. Let U^* be the subspace of V^* spanned by $\mathcal{B}^*$. By Lemma 5.5.3, $\mathcal{B}^*$ is linearly independent, so $\mathcal{B}^*$ is a basis of U^*. But then we have an isomorphism $\mathcal{T}: V \to U^*$ defined by $\mathcal{T}(v_i) = u_i^*$ (in the notation of Definition 5.5.2) for each i. $\square$

Remark 5.5.8. It is important to note that although V and V^* are isomorphic when V is finite dimensional, there is *no* natural isomorphism between them.

Once we have chosen a basis $\mathcal{B}$ we may obtain an isomorphism $\mathcal{T}: V \to V^*$ by $\mathcal{T}(\sum c_i v_i) = \sum c_i u_i^*$, but this depends on the choice of basis. $\Diamond$

It is for this reason that we are denoting elements of V^* by u^* rather than v^*. The notation v^* would tempt you to think that starting with a vector v in V we obtain a vector v^* in V^*, and we want to remove that temptation.

Remark 5.5.9. Note that if $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\mathcal{B}^* = \{u_1^*, \ldots, u_n^*\}$, then each u_i^* depends not only on v_i but rather on *all* of the vectors in $\mathcal{B}$. $\Diamond$

We illustrate this situation with an example.

Example 5.5.10. Let $V = \mathbb{F}^2$, and let $\mathcal{E}$ be the standard basis of $\mathbb{F}^2$, $\mathcal{E} = \{e_1, e_2\} = \left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\}$. Then $\mathcal{E}$ has the dual basis $\mathcal{E}^* = \{e_1^*, e_2^*\}$ with $e_1^*(e_1) = 1$, $e_1^*(e_2) = 0$, and $e_2^*(e_1) = 0$, $e_2^*(e_2) = 1$, i.e., $e_1^*\left(\begin{bmatrix}x\\y\end{bmatrix}\right) = x$ and $e_2^*\left(\begin{bmatrix}x\\y\end{bmatrix}\right) = y$.

Now V also has the basis $\mathcal{B} = \left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}1\\-1\end{bmatrix}\right\} = \{v_1, v_2\}$. Then $\mathcal{B}^*$ has the dual basis $\mathcal{B}^* = \{u_1^*, u_2^*\}$ and you can check that $u_1^* = e_1^* + e_2^*$, $u_2^* = -e_2^*$, i.e., $u_1^*\left(\begin{bmatrix}x\\y\end{bmatrix}\right) = x + y$, $u_2^*\left(\begin{bmatrix}x\\y\end{bmatrix}\right) = -y$.

Thus even though $v_1 = e_1$, $u_1^* \neq e_1^*$. $\Diamond$

Having taken the dual once, we can take it again. We let V^{**} be the *double dual* of V, i.e., $V^{**} = (V^*)^*$ is the dual of the dual of V.

Corollary 5.5.11. (1) *V is isomorphic to a subspace of V^{**}.*

(2) *If V is finite dimensional, then V is isomorphic to V^{**}.*

Proof. This is immediate. For (1), V is isomorphic to a subspace of V^* by Corollary 5.5.7, and then applying that corollary again, V^* is isomorphic to a subspace of $(V^*)^*$, so V is isomorphic to a subspace of V^{**}. Similarly, for (2), if V is finite dimensional, then V is isomorphic to V^* by Corollary 5.5.4, and then applying that corollary again, V^* is isomorphic to $(V^*)^*$, so V is isomorphic to V^{**}. $\square$

Now the point is not just that V and V^{**} are isomorphic in the finite dimensional case. The point is that, while there is *no* natural isomorphism from V to V^*, there is a natural isomorphism (no choice of basis or anything else involved) from V to V^{**}, as we now see.

Lemma 5.5.12. *Let $\mathcal{T}\colon V \to V^{**}$ by $\mathcal{T}(v) = \mathcal{E}_v$ (evaluation at v), i.e., if $u \in V^*$, so that $u^*\colon V \to \mathbb{F}$ is a linear transformation, then $\mathcal{E}_v(u^*) = u^*(v)$. Then $\mathcal{T}$ is a* 1-1 *linear transformation. If V is finite dimensional, $\mathcal{T}$ is an isomorphism.*

Proof. First we must show that $\mathcal{T}$ is a linear transformation. (Of course, each $\mathcal{E}_v$ is a linear transformation, but that only tells us that $\mathcal{T}$ is a function from V to V^{**}. We need to show that $\mathcal{T}$ itself is linear.)

Next we must show that $\mathcal{T}$ is 1-1. As usual, we need only show that if $\mathcal{T}(v) = 0$, then $v = 0$.

We leave both of these steps to the reader.

Finally, if V is finite dimensional, then $\mathcal{T}$ is a 1-1 linear transformation between vector spaces of the same dimension, and hence an isomorphism. $\square$

We now present an interesting example of bases and dual bases that we have already seen. Then we give some interesting and useful applications.

Example 5.5.13. Let $V = P_d(\mathbb{F})$, the space of polynomials of degree at most d, with $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.

(1) We saw in Corollary 5.2.10 that for any fixed a,

$$\mathcal{B} = \{1, x-a, (x-a)^2/2, \ldots, (x-a)^d/d!\}$$

is a basis of V. Then, if we let D denote differentiation and $\mathcal{E}_a$ denote evaluation at a, the proof of Corollary 5.2.9 (the finite Taylor expansion) shows that the dual basis is $\mathcal{B}^* = \{\mathcal{E}_a, \mathcal{E}_a D, \ldots, \mathcal{E}_a D^d\}$.

(2) We saw in Corollary 5.2.12 that for any distinct $a_1, \ldots, a_{d+1}$,

$$\mathcal{B} = \left\{ \prod_{j\neq 1}(x-a_j) \Big/ \prod_{j\neq 1}(a_1-a_j), \ldots, \prod_{j\neq d+1}(x-a_j) \Big/ \prod_{j\neq d+1}(a_{d+1}-a_j) \right\}$$

is a basis of V. The proof of Corollary 5.2.11 (the Lagrange interpolation theorem) shows that the dual basis is $\mathcal{B}^* = \{\mathcal{E}_{a_1}, \ldots, \mathcal{E}_{a_{d+1}}\}$. $\Diamond$

Now let $\mathbb{F} = \mathbb{R}$ and consider a closed interval $I = [a, b]$ in $\mathbb{R}$.

Theorem 5.5.14. *Let $a_0, \ldots, a_d$ be any distinct points of I. Then there are unique real numbers $c_0, \ldots, c_d$ such that for any polynomial $p(x)$ of degree at most d,*

$$\int_a^b p(x)\,dx = \sum_{i=0}^{d} c_i p(a_i).$$

Proof. $\mathcal{T}\colon P_d(\mathbb{R}) \to \mathbb{R}$ by $\mathcal{T}(p(x)) = \int_a^b p(x)\,dx$ is a linear transformation, i.e., an element of V^*, and $\{\mathcal{E}_{a_0}, \ldots, \mathcal{E}_{a_d}\}$ is a basis of V^*, so $\mathcal{T} = \sum_{i=0}^{d} c_i \mathcal{E}_{a_i}$ for some unique $c_0, \ldots, c_d$. $\square$

Let us see how this is often applied in practice.

Example 5.5.15. Set $h = b - a$. For $d = 0$ we choose $a_0 = (a+b)/2$ to be the midpoint of I. For $d > 0$ we divide I into d subintervals of equal length h/d, so $a_i = a_0 + ih/d$, $i = 0, \ldots, d$.

Then for small values of d we have the following (more or less) well-known integration formulas:

$$\int_a^b p(x)\,dx = hp(a_0), \qquad p(x) \in P_0(\mathbb{R}),$$

$$\int_a^b p(x)\,dx = h\left(\frac{1}{2}p(a_0) + \frac{1}{2}p(a_1)\right), \qquad p(x) \in P_1(\mathbb{R}),$$

$$\int_a^b p(x)\,dx = h\left(\frac{1}{6}p(a_0) + \frac{4}{6}p(a_1) + \frac{1}{6}p(a_2)\right), \qquad p(x) \in P_2(\mathbb{R}),$$

$$\int_a^b p(x)\,dx = h\left(\frac{1}{8}p(a_0) + \frac{3}{8}p(a_1) + \frac{3}{8}p(a_2) + \frac{1}{8}p(a_3)\right), \qquad p(x) \in P_3(\mathbb{R}),$$

$$\int_a^b p(x)\,dx = h\left(\frac{7}{90}(a_0) + \frac{32}{90}(a_1) + \frac{12}{90}p(a_2) + \frac{32}{90}p(a_3) + \frac{7}{90}p(a_4)\right), \quad p(x) \in P_4(\mathbb{R}).$$

The first three of these are commonly known as the midpoint rule, the trapezoidal rule, and Simpson's rule. We shall call these the $(d+1)$-point rules for the appropriate values of d.

(While these are exact for polynomials of degree at most d, they are most often used as methods to approximate integrals, as follows. If we want to approximate $\int_a^b p(x)\,dx$, divide the interval $[a, b]$ onto k subintervals of equal length, and then apply the d-point rule to each of the subintervals $[a + (i-1)((b-a)/k), a + i((b-a)/k)]$, and add the values.)

You have probably noticed that the coefficients read the same right-to-left as left-to-right. That is easily proved from linear algebra (a direct consequence of the uniqueness of $c_0, \ldots, c_d$).

Here is a more subtle fact. For d even, the $(d+1)$-point rule is valid not only on $P_d(\mathbb{R})$, but also on $P_{d+1}(\mathbb{R})$. (For example, the midpoint rule is valid not only for constant polynomials but also for linear polynomials, Simpson's rule is valid not only for quadratic polynomials but also for cubic polynomials, etc.) From our viewpoint this is saying: let $V = P_{d+1}(\mathbb{R})$ and for d odd consider the set $\mathcal{B}' = \{\mathcal{E}_{b_0}, \ldots, \mathcal{E}_{b_{d-1}}\}$, where $b_0, \ldots, b_{d-1}$ are the points of $[a, b]$ at which $p(x)$ is evaluated for the d-point rule. $\mathcal{B}'$ is a linearly independent set, so $\operatorname{Span}(\mathcal{B}')$ is a subspace of V^* of dimension d (or of codimension 1). Then $\mathcal{T}$ is an element of this subspace. This can also be proved from linear algebra.

Finally, the values of the coefficients $c_0, \ldots, c_d$ do not follow from general principles, but rather we have to do some work to find them. This work, unsurprisingly, involves solving a linear system. $\Diamond$

Instead of integration we may consider differentiation.

Theorem 5.5.16. *Let c be any fixed point of I. Let $a_0, \ldots, a_d$ be any distinct points of I. Then there are unique real numbers $e_0, \ldots, e_d$ such that for any polynomial $p(x)$ of degree at most d,*

$$p'(c) = \sum_{i=0}^{d} e_i p(a_i).$$

Proof. $\mathcal{T}\colon P_d(\mathbb{R}) \to \mathbb{R}$ by $\mathcal{T}(p(x)) = p'(c)$ is a linear transformation, i.e., an element of V^*, and $\{\mathcal{E}_{a_0}, \ldots, \mathcal{E}_{a_d}\}$ is a basis of V^*, so $\mathcal{T} = \sum_{i=0}^{d} d_i \mathcal{E}_{a_i}$ for some unique $e_0, \ldots, e_d$. $\square$

Let us see how this is applied in practice.

Example 5.5.17. We let $I = [a, b]$ and we let c be the midpoint of I, $c = (a+b)/2$. We choose d even, so that there are an odd number of points. We choose them to be equally spaced, including the endpoints, so that c is the point in the middle of the sequence. We set $h = (b - a)/d$, and then $a_0 = a$, $a_{d/2} = c$, $a_d = b$, and a little algebra shows that $a_i = c + (i - d/2)h$, $i = 0, \ldots, d$.

For small values of d we have the differentiation formulas:

$$p'(c) = \frac{1}{h}\left[\frac{1}{2}p(c+h) - \frac{1}{2}p(c-h)\right], \qquad p(x) \in P_2(\mathbb{R}),$$

$$p'(c) = \frac{1}{h}\left[-\frac{1}{12}p(c+2h) + \frac{8}{12}p(c+h) - \frac{8}{12}p(c-h) + \frac{1}{12}p(c-2h)\right], \quad p(x) \in P_4(\mathbb{R}),$$

$$\begin{aligned} p'(c) = \frac{1}{h}\Bigg[&\frac{1}{60}p(c+3h) - \frac{9}{60}p(c+2h) + \frac{45}{60}p(c+h) - \frac{45}{60}p(c-h) \\ &+ \frac{9}{60}p(c-2h) - \frac{1}{60}p(c-3h)\Bigg], \qquad p(x) \in P_6(\mathbb{R}). \end{aligned}$$

We observe that here $\mathcal{T}$ is in the codimension 1 subspace of $P_d(\mathbb{R})$ with basis $\{\mathcal{E}_{a_0}, \ldots, \mathcal{E}_{a_{d/2-1}}, \mathcal{E}_{a_{d/2+1}}, \ldots, \mathcal{E}_{a_d}\}$.

We also remark that these formulas are often regarded as methods to approximate $p'(c)$ for a general function $p(x)$. $\Diamond$

5.6. The dual of a linear transformation

In the last section we investigated the dual of a vector space V. Now suppose we have a linear transformation $\mathcal{T}\colon V \to W$. We will construct its dual, a linear transformation $\mathcal{T}^*\colon W^* \to V^*$, and then study its properties.

As we did in the last section, we will use v to denote an element of V and u^* to denote an element of V^*. We shall also use w to denote an element of W and x^* to denote an element of W^*.

Definition 5.6.1. Let $\mathcal{T}\colon V \to W$ be a linear transformation. Its *dual* is the linear transformation $\mathcal{T}^*\colon W^* \to V^*$ defined by

$$(\mathcal{T}^*(x^*))(v) = x^*(\mathcal{T}(v)). \qquad \Diamond$$

Let us pause to see that this definition makes sense. We begin with an element x^* of W^*, so that $x^*\colon W \to \mathbb{F}$ is a linear transformation (and in particular a function). We end up with $\mathcal{T}^*(x^*)$, which we want to be an element of V^*, i.e., a linear transformation (and in particular a function) $\mathcal{T}^*(x^*)\colon V \to \mathbb{F}$. So to specify this function, we have to give its value on a typical element v of V, and that is what the formula in Definition 5.6.1 does.

Here is a basic property of the dual.

Theorem 5.6.2. *Let $\mathcal{T}\colon V \to W$ be a linear transformation.*

(1) *$\mathcal{T}$ is* 1-1 *if and only if $\mathcal{T}^*$ is onto.*

(2) *$\mathcal{T}$ is onto if and only if $\mathcal{T}^*$ is* 1-1.

(3) *$\mathcal{T}$ is an isomorphism if and only if $\mathcal{T}^*$ is an isomorphism.*

Proof. (1) Suppose that $\mathcal{T}$ is 1-1. Let $\mathcal{B}$ be a basis of V, $\mathcal{B} = \{v_1, v_2, \dots\}$. Then $\mathcal{C} = \mathcal{T}(\mathcal{B}) = \{w_1, w_2, \dots\}$ is a linearly independent set in W, so extends to a basis $\{w_1, w_2, \dots\} \cup \{w_1', w_2', \dots\}$ of W. Now let u^* be an arbitrary element of V^*. Define the element x^* of W^* by $x^*(w_i) = u^*(v_i)$ and $x^*(w_j') = 0$ (Theorem 4.3.1).

Then we see

$$(\mathcal{T}^*(x^*))(v_i) = x^*(\mathcal{T}(v_i)) = x^*(w_i) = u^*(v_i)$$

so $\mathcal{T}^*(x^*)$ agrees with u^* on the basis $\mathcal{B}$ of V, and hence $\mathcal{T}^*(x^*) = u^*$ (Theorem 4.3.1 again).

Suppose that $\mathcal{T}$ is not 1-1. Then there is some $v_0 \neq 0$ with $\mathcal{T}(v_0) = 0$. Then for any x^* in W^*,

$$(\mathcal{T}^*(x^*))(v_0) = x^*(\mathcal{T}(v_0)) = x^*(0) = 0.$$

But, as we have already seen, for any $v_0 \neq 0$ in V there is some u_0^* in V^* with $u_0^*(v_0) = 1 \neq 0$. Thus we cannot have $\mathcal{T}^*(x^*) = u_0^*$ and so $\mathcal{T}^*$ is not onto.

(2) Suppose that $\mathcal{T}$ is onto. Let $x^* \in W^*$ with $\mathcal{T}^*(x^*) = 0$ (the 0 function on V). We want to show that $x^* = 0$ (the 0 function on W). So suppose $\mathcal{T}^*(x^*) = 0$. Then

$$0 = (\mathcal{T}^*(x^*))(v) = x^*(\mathcal{T}(v)) \quad \text{for every } v \in V.$$

Now let w be any element of W. Since $\mathcal{T}$ is onto, $w = \mathcal{T}(v)$ for some $v \in V$. But then

$$x^*(w) = x^*(\mathcal{T}(v)) = 0$$

and since this is true for every w in W, $x^* = 0$.

Suppose that $\mathcal{T}$ is not onto. Then $\operatorname{Im}(\mathcal{T})$ is a proper subspace of W. Let $\operatorname{Im}(\mathcal{T})$ have basis $\{w_1, w_2, \dots\}$. Extend this to a basis $\{w_1, w_2, \dots\} \cup \{w_1', w_2', \dots\}$ of W. Now let x_0^* be the element of W^* defined by $x_0^*(w_i) = 0$, $x_0^*(w_j') = 1$. Since there is at least one w_j', $x_0^* \neq 0$. But then for any $v \in V$,

$$(\mathcal{T}^*(x_0^*))(v) = x_0^*(\mathcal{T}(v)) = 0$$

as $\mathcal{T}(v) = w$ is in $\operatorname{Im}(\mathcal{T})$, so $w = \sum c_i w_i$ for some c_i, and then $x_0^*(w) = \sum c_i x_0^*(w_i) = 0$. Hence $\mathcal{T}^*(x_0^*) = 0$ (the 0 function) but $x_0^* \neq 0$, so $\mathcal{T}^*$ is not 1-1.

(3) Since a linear transformation is an isomorphism if and only if it is both 1-1 and onto, this follows immediately from (1) and (2). $\square$

We have the following dimension count.

Theorem 5.6.3. *Let $\mathcal{T}\colon V \to W$ be a linear transformation. Then*

$$\dim \operatorname{Im}(\mathcal{T}) = \dim \operatorname{Im}(\mathcal{T}^*),$$
$$\operatorname{codim} \operatorname{Ker}(\mathcal{T}) = \operatorname{codim} \operatorname{Ker}(\mathcal{T}^*).$$

Proof. Since for any linear transformation the codimension of its kernel is equal to the dimension of its image (Theorem 5.2.1), the second statement is just a rephrasing of the first.

Thus we concentrate on proving the first. In order to do so, we will have to keep track of a number of subspaces.

Let $V_1 = \operatorname{Ker}(\mathcal{T})$. Then V_1 is a subspace of V. Let V_2 be any complement of V_1, so $V = V_1 \oplus V_2$.

Let $W_2 = \operatorname{Im}(\mathcal{T})$. Then W_2 is a subspace of W. Let W_1 be any complement of W_2, so that $W = W_1 \oplus W_2$.

Let $\mathcal{B}_2 = \{v_1, v_2, \dots\}$ be a basis of V_2, and let $\mathcal{B}_1 = \{\tilde{v}_1, \tilde{v}_2, \dots\}$ be a basis of $V_1 = \operatorname{Ker}(\mathcal{T})$. Then $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ is a basis of V.

By Theorem 5.2.1, $\mathcal{T}\colon V_2 \to W_2$ is an isomorphism. Then $\mathcal{C}_2 = \mathcal{T}(\mathcal{B}_2)$ is a basis of W_2, i.e., if $w_1 = \mathcal{T}(v_1)$, $w_2 = \mathcal{T}(v_2)$, $\dots$, then $\mathcal{C}_2 = \{w_1, w_2, \dots\}$ is a basis of $W_2 = \operatorname{Im}(\mathcal{T})$. Let $\mathcal{C}_1 = \{\tilde{w}_1, \tilde{w}_2, \dots\}$ be a basis of W_1, so that $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ is a basis of W. (Note that while $\mathcal{C}_2$ was obtained from $\mathcal{B}_2$, $\mathcal{C}_1$ and $\mathcal{B}_1$ have nothing to do with each other.)

Let $u_i^* \in V^*$ be defined by

$$u_i^*(v_i) = 1, \quad u_i^*(v_j) = 0 \quad \text{if } j \neq i, \quad u_i^*(\tilde{v}_j) = 0 \quad \text{for every } j.$$

Similarly, let $x_i^* \in W^*$ be defined by

$$x_i^*(w_i) = 1, \quad x_i^*(w_j) = 0 \quad \text{if } j \neq i, \quad x_i^*(\tilde{w}_j) = 0 \quad \text{for every } j.$$

We claim that $\mathcal{T}^*(x_i^*) = u_i^*$ for each i. To see this, we merely have to check that they agree on any basis of V. We choose the basis $\mathcal{B}$.

First

$$\mathcal{T}^*(x_i^*)(v_i) = x_i^*(\mathcal{T}(v_i)) = x_i^*(w_i) = 1 = u_i^*(v_i)$$

and for $j \neq i$

$$\mathcal{T}^*(x_i^*)(v_j) = x_i^*(\mathcal{T}(v_j)) = x_i^*(w_j) = 0 = u_i^*(v_j).$$

Second, for any j,

$$\mathcal{T}^*(x_i^*)(\tilde{v}_j) = x_i^*(\mathcal{T}(\tilde{v}_j)) = x_i^*(0) = 0 = u^*(\tilde{v}_j).$$

Now $\mathcal{B}_2 = \{v_1, v_2, \dots\}$ is a linearly independent set and so the proof of Lemma 5.5.3(1) shows that $\mathcal{C}_2^* = \{u_1^*, u_2^*, \dots\}$ is a linearly independent set as well.

Suppose that $\mathcal{B}_2$ has finitely many elements, $\mathcal{B}_2 = \{v_1, \dots, v_k\}$, so that $\mathcal{C}_2^* = \{u_1^*, \dots, u_k^*\}$ has k elements as well. We claim that $\mathcal{C}_2^*$ spans $\operatorname{Im}(\mathcal{T}^*)$. If so, $\mathcal{C}_2^*$ is then a basis for $\operatorname{Im}(\mathcal{T}^*)$. But then $k = \dim V_2 = \dim W_2 = \dim \operatorname{Im}(\mathcal{T})$ and $k = \dim \operatorname{Im}(\mathcal{T}^*)$ so $\dim \operatorname{Im}(\mathcal{T}) = \dim \operatorname{Im}(\mathcal{T}^*)$.

To prove the claim, consider any $u^* \in \mathrm{Im}(\mathcal{T}^*)$. Then $u^* = \mathcal{T}^*(x^*)$ for some $x^* \in W^*$.

Define $c_1, \ldots, c_k$ by $c_i = u^*(v_i)$, $i = 1, \ldots, k$. Let

$$t^* = c_1 u_1^* + \cdots + c_k u_k^*.$$

First note that t^* makes sense as $\mathcal{C}_2^*$ is finite so this is a finite sum. We now compute:

$$\begin{aligned} t^*(v_i) &= (c_1 u_1^* + \cdots + c_k u_k^*)(v_i) \\ &= c_1 u_1^*(v_i) + \cdots + c_i u_i^*(v_i) + \cdots + c_k u_k^*(v_i) \\ &= c_i = u^*(v_i) \end{aligned}$$

(as $u_i^*(v_i) = 1$ and $u_j^*(v_i) = 0$ for $j \neq i$), and so t^* and u^* agree on every element of the basis $\mathcal{B}_2$.

Also,

$$t^*(\tilde{v}_j) = (c_1 u_1^* + \cdots + c_k u_k^*)(\tilde{v}_j) = 0$$

as $u_i^*(\tilde{v}_j) = 0$ for every i, and, since $V_1 = \mathrm{Ker}(\mathcal{T})$,

$$u^*(\tilde{v}_j) = \mathcal{T}^*(x^*)(\tilde{v}_j) = x^*(\mathcal{T}(\tilde{v}_j)) = x^*(0) = 0$$

so t^* and u^* agree on every element of the basis $\mathcal{B}_1$.

Thus t^* and u^* agree on every element of $\mathcal{B}$, so

$$u^* = t^* = c_1 u_1^* + \cdots + c_k u_k^*$$

and hence $\mathcal{C}_2$ spans $\mathrm{Im}(\mathcal{T}^*)$, completing the proof in this case.

If $\mathcal{B}_2$ has infinitely many elements, then $\mathcal{C}_2^*$ has infinitely many elements, so $\mathrm{Im}(\mathcal{T}^*)$ contains an infinite linearly independent set, so $\dim \mathrm{Im}(\mathcal{T}^*) = \infty$. But to say that $\mathcal{B}_2$ has infinitely many elements is to say that $\dim V_2 = \infty$. But $\mathcal{T}\colon V_2 \to W_2 = \mathrm{Im}(\mathcal{T})$ is an isomorphism, so $\dim W_2 = \infty$ as well. Thus in this case we also see that $\dim \mathrm{Im}(\mathcal{T}) = \dim \mathrm{Im}(\mathcal{T}^*)$. □

Corollary 5.6.4. *Let $\mathcal{T}\colon V \to W$ be a linear transformation. Then*

$$\begin{aligned} \dim \mathrm{Ker}(\mathcal{T}) &= \operatorname{codim} \mathrm{Im}(\mathcal{T}^*), \\ \dim \mathrm{Ker}(\mathcal{T}^*) &= \operatorname{codim} \mathrm{Im}(\mathcal{T}). \end{aligned}$$

Proof. For simplicity, we shall just prove this in case V and W are finite dimensional, when we have a simple dimension count.

Let $\dim V = n$ and $\dim W = m$. Then $\dim V^* = n$ and $\dim W^* = m$. Let $r = \dim \mathrm{Im}(\mathcal{T}) = \dim \mathrm{Im}(\mathcal{T}^*)$. Then by Corollary 5.2.3, $n - r = \dim \mathrm{Ker}(\mathcal{T}) = \operatorname{codim} \mathrm{Im}(\mathcal{T}^*)$ and $m - r = \dim \mathrm{Ker}(\mathcal{T}^*) = \operatorname{codim} \mathrm{Im}(\mathcal{T})$. □

Here are some general facts about duals.

Lemma 5.6.5. (1) *Let $\mathcal{T}_1\colon V \to W$ and $\mathcal{T}_2\colon V \to W$ be linear transformations, and let c_1 and c_2 be scalars. Then $(c_1\mathcal{T}_1 + c_2\mathcal{T}_2)^* = c_1\mathcal{T}_1^* + c_2\mathcal{T}_2^*$.*

(2) *Let $\mathcal{I}\colon V \to V$ be the identity transformation. Then $\mathcal{I}^* = \mathcal{I}$, the identity transformation $\mathcal{I}\colon V^* \to V^*$.*

(3) *Let $\mathcal{T}\colon U \to V$ and $\mathcal{S}\colon V \to W$ be linear transformations. Then $(\mathcal{S}\mathcal{T})^* = \mathcal{T}^*\mathcal{S}^*$.*

(4) *Let $\mathcal{T}: V \to W$ be a linear transformation. Suppose that $\mathcal{T}$ and $\mathcal{T}^*$ are both invertible. Then $(\mathcal{T}^*)^{-1} = (\mathcal{T}^{-1})^*$.*

Proof. (1) Let x^* be any element of W^*. Then by properties of linear transformations,

$$\begin{aligned}(c_1\mathcal{T}_1 + c_2\mathcal{T}_2)^*(x^*) &= x^*(c_1\mathcal{T}_1 + c_2\mathcal{T}_2)\\ &= c_1x^*(\mathcal{T}_1) + c_2x^*(\mathcal{T}_2)\\ &= c_1\mathcal{T}_1^*(x^*) + c_2\mathcal{T}_2^*(x^*).\end{aligned}$$

(2) By the definition of $\mathcal{I}^*$, for any x^* in W^*

$$\mathcal{I}^*(x^*) = x^*(\mathcal{I}) = x^* = \mathcal{I}(x^*).$$

(3) By the definition of $(\mathcal{S}\mathcal{T})^*$, for any x^* in W^*

$$\begin{aligned}(\mathcal{S}\mathcal{T})^*(x^*) = x^*(\mathcal{S}\mathcal{T}) &= (x^*(\mathcal{S}))(\mathcal{T})\\ &= \mathcal{T}^*(x^*(\mathcal{S})) = \mathcal{T}^*(\mathcal{S}^*(x^*)) = (\mathcal{T}^*\mathcal{S}^*)(x^*).\end{aligned}$$

(4) $(\mathcal{T}^*)^{-1}$ is defined by the equations $(\mathcal{T}^*)^{-1}\mathcal{T}^* = \mathcal{I}$ and $\mathcal{T}^*(\mathcal{T}^*)^{-1} = \mathcal{I}$. But from (2) and (3)

$$\mathcal{I} = \mathcal{I}^* = (\mathcal{T}\mathcal{T}^{-1})^* = (\mathcal{T}^{-1})^*\mathcal{T}^* \quad\text{and}\quad \mathcal{I} = \mathcal{I}^* = (\mathcal{T}^{-1}\mathcal{T})^* = \mathcal{T}^*(\mathcal{T}^{-1})^*$$

so we see $(\mathcal{T}^*)^{-1} = (\mathcal{T}^{-1})^*$. □

We can now define, and see the meaning of, the transpose of a matrix.

Definition 5.6.6. Let $A = (a_{ij})$ be an m-by-n matrix. Its *transpose* ${}^tA = (b_{ij})$ is the n-by-m matrix given by $b_{ji} = a_{ij}$ for each $i = 1, \ldots, m$ and $j = 1, \ldots, n$. ◊

Thus we see that ${}^tA$ is obtained by "flipping" the rows and columns of A, i.e., the first row of ${}^tA$ is the first column of A (or equivalently the first column of ${}^tA$ is the first row of A), similarly for the second, third, etc.

Now suppose we have a linear transformation $\mathcal{T}: V \to W$, where V and W are both finite dimensional, and we choose bases $\mathcal{B}$ and $\mathcal{C}$ of V and W, respectively. Then we have the matrix of this linear transformation with respect to these bases, $P = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$.

But then we can also consider $\mathcal{T}^*: W^* \to V^*$, and choose the dual bases $\mathcal{C}^*$ and $\mathcal{B}^*$ of W^* and V^*, respectively. Then we also have the matrix of this linear transformation with respect to these bases, $Q = [\mathcal{T}^*]_{\mathcal{B}^*\leftarrow\mathcal{C}^*}$.

Theorem 5.6.7. *Let $P = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ be the m-by-n matrix $P = (p_{ij})$, and let $Q = [\mathcal{T}^*]_{\mathcal{B}^*\leftarrow\mathcal{C}}$ be the n-by-m matrix $Q = (q_{ij})$. Then $Q = {}^tP$.*

Proof. Let $P = (p_{ij})$ and $Q = (q_{ij})$. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$, $\mathcal{C} = \{w_1, \ldots, w_m\}$, $\mathcal{B}^* = \{u_1^*, \ldots, u_n^*\}$, and $\mathcal{C}^* = \{x_1^*, \ldots, x_m^*\}$.

By the definition of $\mathcal{T}^*$, for each i and j

$$\mathcal{T}^*(x_i)^*(v_j) = x_i^*(\mathcal{T}(v_j)).$$

Now recall that

$$[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}} = \big[[\mathcal{T}(v_1)]_{\mathcal{C}}\big|[\mathcal{T}(v_2)]_{\mathcal{C}}\big|\ldots\big|[\mathcal{T}(v_n)]_{\mathcal{C}}\big]$$

so $[\mathcal{T}(v_j)]$ is the jth column of this matrix,

$$[\mathcal{T}(v_j)]_{\mathcal{C}} = \begin{bmatrix} p_{1j} \\ p_{2j} \\ \vdots \\ p_{mj} \end{bmatrix},$$

i.e.,

$$\mathcal{T}(v_j) = \sum_k p_{kj} w_k,$$

and then

$$x_i^*(\mathcal{T}(v_j)) = x_i^*\Big(\sum_k p_{kj} w_k\Big) = p_{ij}$$

as $x_i^*(w_k) = 1$ if $k = i$ and 0 if $k \neq i$.

Also recall that

$$[\mathcal{T}^*]_{\mathcal{B}^* \leftarrow \mathcal{C}^*} = \big[[\mathcal{T}(x_1^*)]_{\mathcal{B}^*}\big|[\mathcal{T}(x_2^*)]_{\mathcal{B}^*}\big|\ldots\big|[\mathcal{T}(x_m^*)]_{\mathcal{B}^*}\big]$$

so $[\mathcal{T}(x_i^*)]_{\mathcal{B}^*}$ is the ith column of this matrix,

$$[\mathcal{T}(x_i^*)]_{\mathcal{B}^*} = \begin{bmatrix} q_{1i} \\ q_{2i} \\ \vdots \\ q_{ni} \end{bmatrix},$$

i.e.,

$$\mathcal{T}(x_i^*) = \sum_k q_{ki} u_k^*$$

and then

$$\mathcal{T}(x_i^*)(v_j) = \Big(\sum_k q_{ki} u_k^*\Big)(v_j) = q_{ji}$$

as $u_k^*(v_i) = 1$ if $k = i$ and 0 if $k \neq i$.

Thus we see $q_{ji} = p_{ij}$ for every i and j, as claimed. □

Now consider the case where $V = \mathbb{F}^n$, $W = \mathbb{F}^m$, $\mathcal{B} = \mathcal{E}_n$ is the standard basis of $\mathbb{F}^n$, and $\mathcal{C} = \mathcal{E}_m$ is the standard basis of $\mathbb{F}^m$. Then $\mathcal{B}^* = \mathcal{E}_n^*$ and $\mathcal{C}^* = \mathcal{E}_m^*$ are the standard bases of $(\mathbb{F}^n)^*$ and $(\mathbb{F}^m)^*$. Recall that the standard matrix of $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^m$ is the matrix $[\mathcal{T}]_{\mathcal{E}_m \leftarrow \mathcal{E}_n}$. We define the *standard matrix* of $\mathcal{T}^*\colon (\mathbb{F}^m)^* \to (\mathbb{F}^n)^*$ to be the matrix $[\mathcal{T}^*]_{\mathcal{E}_n^* \leftarrow \mathcal{E}_m^*}$. Thus we see that if $\mathcal{T}$ has standard matrix A, then $\mathcal{T}^*$ has standard matrix ${}^tA$.

We have the following properties of the transpose.

Lemma 5.6.8. (1) *If A and B are matrices, ${}^t(A+B) = {}^tA + {}^tB$.*

(2) *If A is a matrix and c is a scalar, ${}^t(cA) = c\,{}^tA$.*

(3) *If A and B are matrices, ${}^t(AB) = {}^tB\,{}^tA$.*

(4) *The matrix A is invertible if and only if the matrix ${}^tA$ is invertible, and $({}^tA)^{-1} = {}^t(A^{-1})$. (We write this common value as ${}^tA^{-1}$.)*

Proof. This is just a restatement of Lemma 5.6.5 in terms of matrices. □

We also have a conceptual proof of a result we showed quite some time ago (Corollary 3.4.16) by computational means.

Corollary 5.6.9. *For any matrix A,* row rank(A) = column rank(A).

Proof. Let $\mathcal{T}$ have standard matrix A, so that $\mathcal{T}^*$ has standard matrix ${}^tA$. The column rank of A is the dimension of the column space of A, which is the dimension of $\mathrm{Im}(\mathcal{T})$.

The column rank of ${}^tA$ is the dimension of the column space of ${}^tA$, which is the dimension of $\mathrm{Im}(\mathcal{T}^*)$.

We know that $\dim \mathrm{Im}(\mathcal{T}) = \dim \mathrm{Im}(\mathcal{T}^*)$ by Theorem 5.6.3.

But given the relation between A and ${}^tA$, where ${}^tA$ is obtained from A by interchanging rows and columns, the column space of ${}^tA$ is just the row space of A. □

Remark 5.6.10. We should note (once again) that the mathematical world is divided. Some mathematicians denote the transpose of A by ${}^tA$, as we do, while others denote it by A^t. ◊

5.7. Exercises

1. For each of the following matrices A, find a basis for $\mathrm{Ker}(\mathcal{T}_A)$ and a basis for $\mathrm{Im}(\mathcal{T}_A)$:

(a) $A = \begin{bmatrix} 1 & 1 & 0 \\ 2 & 3 & 1 \\ 1 & 4 & 3 \end{bmatrix}$.

(b) $A = \begin{bmatrix} 1 & 2 & 4 \\ 1 & 2 & 4 \\ 3 & 6 & 12 \end{bmatrix}$.

(c) $A = \begin{bmatrix} 1 & 1 & 2 & 0 & 1 \\ 2 & 3 & 5 & 1 & 5 \\ 1 & 2 & 3 & 1 & 4 \\ 4 & 5 & 9 & 1 & 7 \end{bmatrix}$.

(d) $A = \begin{bmatrix} 1 & 1 & 2 & 1 & 2 \\ 3 & 5 & 8 & 5 & 10 \\ 1 & 2 & 3 & 3 & 5 \\ 4 & 2 & 6 & 6 & 8 \end{bmatrix}$.

(e) $A = \begin{bmatrix} 1 & 2 & 1 & 5 & 1 \\ 2 & 2 & 2 & 6 & 0 \\ 1 & 1 & 2 & 4 & 0 \\ 3 & 4 & 4 & 11 & 0 \end{bmatrix}$.

(f) $A = \begin{bmatrix} 1 & 2 & 3 & 5 \\ 2 & 4 & 6 & 13 \\ 1 & 3 & 5 & 9 \\ 3 & 6 & 9 & 18 \\ 3 & 7 & 10 & 20 \end{bmatrix}$.

(g) $A = \begin{bmatrix} 1 & 2 & 3 & 5 \\ 1 & 1 & 2 & 2 \\ 0 & 3 & 3 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 2 & 3 & 0 \end{bmatrix}$.

(h) $A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ -1 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ -1 & 3 & 2 & -1 \\ -2 & 4 & 2 & -2 \end{bmatrix}$.

2. Let V be a vector space, and let V_1 and V_2 be subspaces of V with $V = V_1 \oplus V_2$. Let $\mathcal{C} = \{v_i\}$ be a set of vectors in V. For each i, let $v_i = v_i^1 + v_i^2$ for unique vectors $v_i^1 \in V_1$ and $v_i^2 \in V_2$. Suppose that $\mathcal{C}$ spans V. Show that $\mathcal{C}^1 = \{v_i^1\}$ spans V_1 and $\mathcal{C}^2 = \{v_i^2\}$ spans V_2. Suppose that $\mathcal{C}$ is linearly dependent. Show that $\mathcal{C}^1$ and $\mathcal{C}^2$ are also linearly dependent.

3. (a) Let U and W be finite-dimensional subspaces of the vector space V. Show that

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W).$$

(b) Let n be any nonnegative integer. Let i and j be any integers with $0 \le i \le n$, $0 \le j \le n$. Let k be any integer with $i \le k$, $j \le k$, $k \le i + j$, and $k \le n$.

Give an example of a vector space V with $\dim(V) = n$, subspaces U and W with $\dim(U) = i$ and $\dim(W) = j$, and $\dim(U + W) = k$.

4. Let $V = P(\mathbb{R})$. Then V has subspaces

$$V_{\text{even}} = \{p(x) \in V \,|\, p(-x) = p(x)\} \quad \text{and} \quad V_{\text{odd}} = \{p(x) \in V \,|\, p(-x) = -p(x)\}.$$

(a) Show that $V = V_{\text{even}} \oplus V_{\text{odd}}$.

(b) Let $\mathcal{B} = \{1, x, x^2, \dots\}$. $\mathcal{B}$ is a basis for V. Let $\mathcal{B}_{\text{even}} = \{1, x^2, x^4, \dots\}$ and $\mathcal{B}_{\text{odd}} = \{x, x^3, x^5, \dots\}$. Show that $\mathcal{B}_{\text{even}}$ is a basis for V_{even} and that $\mathcal{B}_{\text{odd}}$ is a basis for V_{odd}.

5. Let $V = M_n(\mathbb{R})$. A matrix A in V is *symmetric* if $A = {}^tA$ and *skew-symmetric* if ${}^tA = -A$. Let $V_+ = \{\text{symmetric matrices in } V\}$ and $V_- = \{\text{skew-symmetric matrices in } V\}$.

(a) Show that V_+ and V_- are subspaces of V.

(b) Show that $V = V_+ \oplus V_-$.

(c) Find $\dim(V_+)$ and $\dim(V_-)$.

(d) Find bases for V_+ and V_-.

6. Let $\mathcal{B}$ and $\mathcal{C}$ be the bases of $\mathbb{F}^2$ given by

$$\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 5 \end{bmatrix} \right\} \quad \text{and} \quad \mathcal{C} = \left\{ \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ -2 \end{bmatrix} \right\}.$$

Find the change of basis matrices $P_{\mathcal{C} \leftarrow \mathcal{B}}$ and $P_{\mathcal{B} \leftarrow \mathcal{C}}$.

7. (a) Let $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 9 \end{bmatrix} \right\}$, a basis of $\mathbb{F}^2$. Let $T\colon \mathbb{F}^2 \to \mathbb{F}^2$ be given by $T(v) = Av$, where $A = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}$. Find $[T]_{\mathcal{B}}$.

(b) Let $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 \\ 11 \end{bmatrix} \right\}$, a basis of $\mathbb{F}^2$. Let $T\colon \mathbb{F}^2 \to \mathbb{F}^2$ be given by $T(v) = Av$, where $A = \begin{bmatrix} -52 & 10 \\ -257 & 53 \end{bmatrix}$. Find $[T]_{\mathcal{B}}$.

Do both parts of this problem both directly and by using change of basis matrices.

8. Let $\mathcal{E}$ be the standard basis of $\mathbb{F}^3$, and let $\mathcal{B}$ be the basis

$$\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 \\ 7 \\ 12 \end{bmatrix}, \begin{bmatrix} 5 \\ 12 \\ 20 \end{bmatrix} \right\}.$$

(a) If $v = \begin{bmatrix} 5 \\ 8 \\ 13 \end{bmatrix}$, find $[v]_{\mathcal{B}}$.

(b) If $[v]_{\mathcal{B}} = \begin{bmatrix} 7 \\ 4 \\ -3 \end{bmatrix}$, find v.

(c) If $\mathcal{T}\colon \mathbb{F}^3 \to \mathbb{F}^3$ has $[\mathcal{T}]_{\mathcal{E}} = \begin{bmatrix} 1 & 3 & 6 \\ 2 & 4 & 7 \\ 3 & 8 & 9 \end{bmatrix}$, find $[\mathcal{T}]_{\mathcal{B}}$.

(d) If $\mathcal{T}\colon \mathbb{F}^3 \to \mathbb{F}^3$ has $[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} 6 & 1 & 2 \\ 4 & 3 & 5 \\ 1 & 8 & 0 \end{bmatrix}$, find $[\mathcal{T}]_{\mathcal{E}}$.

Do each part of this problem both directly and by using change of basis matrices.

9. Now let $\mathcal{B}$ be the basis of $P_2(\mathbb{F})$,

$$\mathcal{B} = \{1 + x^2, x + x^2, 1 + 2x^2\}.$$

(a) If $v = x^2$, find $[v]_{\mathcal{B}}$.

(b) If $[v]_{\mathcal{B}} = \begin{bmatrix} 0 \\ -1 \\ 1 \end{bmatrix}$, find v.

(c) If $\mathcal{T}\colon \mathbb{F}^3 \to \mathbb{F}^3$ by $\mathcal{T}(f(x)) = f(x+1)$, find $[\mathcal{T}]_{\mathcal{B}}$.

(d) If $\mathcal{T}\colon \mathbb{F}^3 \to \mathbb{F}^3$ by $\mathcal{T}(f(x)) = f'(x)$, find $[\mathcal{T}]_{\mathcal{B}}$.

Do each part of this problem both directly and by using change of basis matrices.

10. Let $V = M_n(\mathbb{F})$, the vector space of n-by-n matrices with coefficients in $\mathbb{F}$. For a fixed matrix $A \in V$, let $\mathcal{T}\colon V \to V$ by $\mathcal{T}(B) = AB - BA$.

(a) Show that $\mathcal{T}$ is a linear transformation.

(b) Let $n = 2$, and let $E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $E_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, and $E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$. Then $\mathcal{B} = \{E_{11}, E_{12}, E_{21}, E_{22}\}$ is a basis of V. Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$. Find $[\mathcal{T}]_{\mathcal{B}}$, the matrix of $\mathcal{T}$ in the basis $\mathcal{B}$.

(c) Let $n = 2$. Show that there are matrices A and B with $AB - BA = C = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$ if and only if $c_{11} + c_{22} = 0$.

(d) Let n be arbitrary. Show that there are matrices A and B with $AB - BA = C$ if and only if the sum of the diagonal entries of C is 0.

11. Let V and W be finite dimensional vector spaces, and let $\mathcal{T}\colon V \to W$ be a linear transformation. Let $\mathcal{B}$ and $\mathcal{B}'$ be bases of V, and let $\mathcal{C}$ and $\mathcal{C}'$ be bases of W. Show that:

(a) $[\mathcal{T}]_{\mathcal{C}' \leftarrow \mathcal{B}} = P_{\mathcal{C}' \leftarrow \mathcal{C}}[\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}}$.

(b) $[\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}'} = [\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}} P_{\mathcal{B} \leftarrow \mathcal{B}'}$.

(c) $[\mathcal{T}]_{\mathcal{C}' \leftarrow \mathcal{B}'} = P_{\mathcal{C}' \leftarrow \mathcal{C}}[\mathcal{T}]_{\mathcal{C} \leftarrow \mathcal{B}} P_{\mathcal{B} \leftarrow \mathcal{B}'}$.

12. (a) Let V and W be vector spaces.

Let $\mathcal{L}_V = \{\text{linear transformations } \mathcal{T}\colon V \to V\}$ and $\mathcal{L}_W = \{\text{linear transformations } \mathcal{T}\colon W \to W\}$.

As we have seen, $\mathcal{L}_V$ and $\mathcal{L}_W$ are vector spaces.

Suppose that V and W are isomorphic and let $\mathcal{S}\colon V \to W$ be an isomorphism. Let $\mathcal{R}\colon \mathcal{L}_V \to \mathcal{L}_W$ by

$$\mathcal{R}(\mathcal{T}) = \mathcal{S}\mathcal{T}\mathcal{S}^{-1}.$$

Show that $\mathcal{R}$ is an isomorphism.

(b) Translate this result into matrix language, in the finite-dimensional case, to show: Let $X = M_n(\mathbb{F})$, the space of n-by-n matrices over $\mathbb{F}$. Let B be a fixed n-by-n matrix over $\mathbb{F}$. Then $\mathcal{R}\colon X \to X$ by $\mathcal{R}(A) = BAB^{-1}$ is an isomorphism.

13. Let V be an n-dimensional vector space with basis $\mathcal{B} = \{v_1, \ldots, v_n\}$. Let $\mathcal{C} = \{w_1, \ldots, w_n\}$ be any set of n vectors in V. Show that $\mathcal{C}$ is a basis of V if and only if the matrix

$$\big([w_1]_{\mathcal{B}} \big| [w_2]_{\mathcal{B}} \big| \ldots \big| [w_n]_{\mathcal{B}}\big)$$

is invertible.

14. Let us call two bases $\mathcal{B} = \{v_1, \ldots, v_n\}$ and $\mathcal{C} = \{w_1, \ldots, w_n\}$ of $\mathbb{F}^n$ *matched* if $\operatorname{Span}(\{v_1, \ldots, v_i\}) = \operatorname{Span}(\{w_1, \ldots, w_i\})$ for each $i = 1, \ldots, n$. Show that $\mathcal{B}$ and $\mathcal{C}$ are matched if and only if the change of basis matrix $P_{\mathcal{C} \leftarrow \mathcal{B}}$ is upper triangular.

15. Let $V = P_d(\mathbb{R})$. Let $\mathcal{E} = \{1, x, \ldots, x^d\}$, and let $\mathcal{B} = \{x^{(0)}, x^{(1)}, \ldots, x^{(d)}\}$. Both $\mathcal{E}$ and $\mathcal{B}$ are bases of V. Let ${}_1S$ be the change of basis matrix $P_{\mathcal{E} \leftarrow \mathcal{B}}$ and let ${}_2S$ be the change of basis matrix $P_{\mathcal{B} \leftarrow \mathcal{E}}$. Both of these $(d+1)$-by-$(d+1)$ matrices are upper triangular. *Number the rows and columns of these matrices* 0 *to* d.

Let ${}_1s_n^m$ be the entry in row m and column n of ${}_1S$ for $m \leq n$. The numbers $\{{}_1s_n^m\}$ are called Stirling numbers of the first kind.

Let ${}_2s_n^m$ be the entry in row m and column n of ${}_2S$ for $m \leq n$. The numbers $\{{}_2s_n^m\}$ are called Stirling numbers of the second kind.

Compute these matrices in case $d = 5$, thereby finding the Stirling numbers ${}_1s_n^m$ and ${}_2s_n^m$ for $m, n \leq 5$.

16. Let $V = P_d(\mathbb{R})$. For any integer i, let $\mathcal{B}_i = \{(x+i)^0, (x+i)^1, \ldots, (x+i)^d\}$, a basis of V.

(a) For any integer a, find the change of basis matrix $P_a = P_{\mathcal{B}_0 \leftarrow \mathcal{B}_a}$.

(b) Show that, for any integer k, $P_{\mathcal{B}_k \leftarrow \mathcal{B}_{a+k}} = P_a$.

(c) Show that for any integers a and b, $P_{a+b} = P_a P_b = P_b P_a$, and in particular $P_a = (P_1)^a$.

(d) Show that, for $a \neq 0$, $P_a = D_a^{-1} P_1 D_a$, where D_a is the diagonal matrix with diagonal entries $1, a, a^2, \ldots, a^d$.

(e) Use part (c) to derive identities among binomial coefficients. For example, use $a = 1$ and $b = -1$ to show, for any fixed i, $0 \leq i \leq d$,

$$\sum_{j=i}^{d} \binom{j-1}{i-1}\binom{d-1}{j-1}(-1)^{d-j} = \begin{cases} 0, & i < d, \\ 1, & i = d. \end{cases}$$

Also, for example, use $a = 1$ and $b = 1$ to show, for any fixed i, $0 \leq i \leq d$,

$$\sum_{j=i}^{d} \binom{j-1}{i-1}\binom{d-1}{j-1} = \binom{d-1}{i-1} 2^{d-i}.$$

Suggestion: Before doing this exercise for d in general, try it for various small values of d.

17. Let A be an n-by-n matrix of rank r.

(a) Show that A is similar to a matrix with exactly r nonzero columns.

(b) Show that A is similar to a matrix with exactly r nonzero rows.

(c) Show that A is similar to a matrix with exactly r nonzero rows and exactly r nonzero columns.

(d) Show that A is similar to a matrix of the form $\begin{bmatrix} M & 0 \\ 0 & 0 \end{bmatrix}$, where M is r-by-r, if and only if $\operatorname{Ker}(A) \cap \operatorname{Im}(A) = \{0\}$.

18. In each case, $\mathcal{T}\colon V \to W$ is a linear transformation, where $\dim(V) = n$, $\dim(W) = m$, $\operatorname{rank}(\mathcal{T}) = r$, and $\operatorname{nullity}(\mathcal{T}) = k$. Fill in the missing entries of the table. If there is no linear transformation consistent with the given data, write "I" for impossible. If the missing entry cannot be determined from the given data, write "U" for undetermined.

	n	m	r	k
(a)		7	3	2
(b)	6		5	1
(c)	7	4		6
(d)	8	3	6	
(e)	8		5	2
(f)	7	8	4	

19. (a) Let V be a finite-dimensional vector space, and let $\mathcal{T}: V \to V$ be a linear transformation. Show that the following are equivalent:

(1) $V = \mathrm{Ker}(\mathcal{T}) + \mathrm{Im}(\mathcal{T})$.

(2) $\mathrm{Ker}(\mathcal{T}) \cap \mathrm{Im}(\mathcal{T}) = \{0\}$.

(3) $V = \mathrm{Ker}(\mathcal{T}) \oplus \mathrm{Im}(\mathcal{T})$.

(b) Give an example where (1), (2), and (3) are all true, and an example where they are all false.

(c) Now let V be infinite dimensional. Give examples where (1), (2), and (3) are all true, (1), (2), and (3) are all false, (1) is true but (2), and hence (3), are false, and where (2) is true but (1), and hence (3), are false. (Of course, if (3) is true, then (1) and (2) are both true.)

20. (a) Let V be an n-dimensional vector space, and let W be an m-dimensional vector space. Let $\mathcal{T}: V \to W$ be a linear transformation. Set $i = \dim \mathrm{Im}(\mathcal{T})$ and $k = \dim \mathrm{Ker}(\mathcal{T})$. We know that $i + k = n$. Also, since $\mathrm{Im}(\mathcal{T})$ is a subspace of W, we know $i \leq m$.

Show that these are only restrictions on i and k. That is, let n and m be nonnegative integers, and let V be an n-dimensional vector space and W an m-dimensional vector space. Let i and k be any two nonnegative integers such that

$$i + k = n \quad \text{and} \quad i \leq m.$$

Show that there is a linear transformation $\mathcal{T}: V \to W$ with

$$\dim \mathrm{Im}(\mathcal{T}) = i \quad \text{and} \quad \dim \mathrm{Ker}(\mathcal{T}) = k.$$

(b) More precisely, in this situation let U be any subspace of V with $\dim U = k$, and let X be any subspace of W with $\dim W = i$. Show that there is a linear transformation $\mathcal{T}: V \to W$ with $\mathrm{Ker}(\mathcal{T}) = U$ and $\mathrm{Im}(\mathcal{T}) = X$.

(c) Show this has the following translation into matrix language. Let m and n be any positive integers. Let V_1 be any subspace of $\mathbb{F}^n$, and let W_1 be any subspace of $\mathbb{F}^m$ with $\dim V_1 + \dim W_1 = n$. Then there is an m-by-n matrix A whose null space is V_1 and whose column space is W_1.

21. In each case, find a matrix A such that $\mathcal{B}$ is a basis for $\mathrm{Ker}(\mathcal{T}_A)$ and $\mathcal{C}$ is a basis for $\mathrm{Im}(\mathcal{T}_A)$:

(a) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 1 \\ -2 \end{bmatrix} \right\}$, $\mathcal{C} = \left\{ \begin{bmatrix} 2 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 5 \end{bmatrix} \right\}$.

(b) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 5 \\ 7 \end{bmatrix} \right\}, \mathcal{C} = \left\{ \begin{bmatrix} 3 \\ 6 \\ 1 \end{bmatrix} \right\}.$

(c) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \\ 6 \end{bmatrix} \right\}, \mathcal{C} = \left\{ \begin{bmatrix} 2 \\ 4 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 2 \\ 5 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 4 \end{bmatrix} \right\}.$

(d) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 1 \\ 5 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 4 \\ 3 \end{bmatrix} \right\}, \mathcal{C} = \left\{ \begin{bmatrix} 4 \\ 2 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 5 \\ 1 \\ 8 \\ 6 \end{bmatrix} \right\}.$

(e) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 3 \\ 5 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 5 \\ 10 \end{bmatrix} \right\}, \mathcal{C} = \left\{ \begin{bmatrix} 3 \\ 5 \\ 2 \\ 7 \end{bmatrix} \right\}.$

(f) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 1 \\ 0 \\ 1 \end{bmatrix} \right\}, \mathcal{C} = \left\{ \begin{bmatrix} 1 \\ 4 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right\}.$

(g) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 3 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 3 \\ 2 \end{bmatrix} \right\}, \mathcal{C} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \right\}.$

(h) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 0 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 4 \end{bmatrix} \right\}, \mathcal{C} = \left\{ \begin{bmatrix} 2 \\ 1 \\ 5 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 4 \\ 8 \end{bmatrix} \right\}.$

In each case, find a 5-by-5 matrix A such that $\mathcal{B}$ is a basis for $\mathrm{Ker}(\mathcal{T}_A)$ and $\mathcal{C}$ is a basis for $\mathrm{Im}(\mathcal{T}_A)$:

(i) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 4 \\ 2 \\ 3 \end{bmatrix} \right\}, \mathcal{C} = \left\{ \begin{bmatrix} 4 \\ 9 \\ 18 \\ 8 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \\ 9 \\ 9 \\ 7 \end{bmatrix}, \begin{bmatrix} 5 \\ 7 \\ 16 \\ 15 \\ 12 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 7 \\ 6 \\ 4 \end{bmatrix} \right\}.$

(j) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 4 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 4 \\ 9 \\ 18 \\ 8 \\ 3 \end{bmatrix} \right\}, \mathcal{C} = \left\{ \begin{bmatrix} 3 \\ 4 \\ 9 \\ 9 \\ 7 \end{bmatrix}, \begin{bmatrix} 5 \\ 7 \\ 16 \\ 15 \\ 12 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 7 \\ 6 \\ 4 \end{bmatrix} \right\}.$

(k) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 4 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 4 \\ 9 \\ 18 \\ 8 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \\ 9 \\ 9 \\ 7 \end{bmatrix} \right\}, \mathcal{C} = \left\{ \begin{bmatrix} 5 \\ 7 \\ 16 \\ 15 \\ 12 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 7 \\ 6 \\ 4 \end{bmatrix} \right\}.$

(l) $\mathcal{B} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 4 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 4 \\ 9 \\ 18 \\ 8 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \\ 9 \\ 9 \\ 7 \end{bmatrix}, \begin{bmatrix} 5 \\ 7 \\ 16 \\ 15 \\ 12 \end{bmatrix} \right\}, \mathcal{C} = \left\{ \begin{bmatrix} 1 \\ 2 \\ 7 \\ 6 \\ 4 \end{bmatrix} \right\}.$

(In all cases, the given sets $\mathcal{B}$ and $\mathcal{C}$ are linearly independent).

22. (a) Let V be an n-dimensional vector space, and let U_1 and U_2 be any two subspaces of V with $\dim U_1 = \dim U_2$. Show that there is an automorphism $\mathcal{T}$ of V, that is, an isomorphism $\mathcal{T}: V \to V$, with $\mathcal{T}(U_1) = U_2$.

(b) More precisely, in this situation let $\mathcal{R}: U_1 \to U_2$ be any isomorphism. Show that there is an automorphism $\mathcal{T}$ of V with $\mathcal{T}|U_1 = \mathcal{R}$.

(c) In this situation, let W_1 be any complement of U_1 in V and let W_2 be any complement of U_2 in V (again with $\dim U_1 = \dim U_2$). Show that there is an automorphism $\mathcal{T}$ of V with $\mathcal{T}(U_1) = U_2$ and $\mathcal{T}(W_1) = W_2$.

(d) More precisely, in this situation let $\mathcal{R}: U_1 \to U_2$ and $\mathcal{S}: U_1 \to U_2$ be any isomorphisms. Show that there is a unique automorphism $\mathcal{T}$ of V with $\mathcal{T}|U_1 = \mathcal{R}$ and $\mathcal{T}|W_1 = \mathcal{S}$.

23. (a) Let A be an n-by-n matrix. Show that there is a nonzero polynomial $p(x)$ of degree at most n^2 with $p(A) = 0$.

(b) Let A be an n-by-n matrix and let v be a vector in $\mathbb{F}^n$. Show there is a nonzero polynomial $p_v(x)$ of degree at most n with $p_v(A)v = 0$.

(In fact, as we will see later, there is a nonzero polynomial $p(x)$ of degree at most n with $p(A) = 0$. Then, of course, for this polynomial $p(x)$, $p(A)v = 0$ for every v in $\mathbb{F}^n$.)

24. Let V be a vector space, and let $\{\mathcal{P}_1, \ldots, \mathcal{P}_n\}$ be a set of linear transformations with the following properties:

(1) $\mathcal{P}_1 + \cdots + \mathcal{P}_n = \mathcal{I}$.

(2) $\mathcal{P}_i^2 = \mathcal{P}_i$ for each i.

(3) $\mathcal{P}_i\mathcal{P}_j = 0$ whenever $i \neq j$.

(a) Let $W_i = \mathrm{Im}(\mathcal{P}_i)$. Show that $V = W_1 \oplus \cdots \oplus W_n$.

(b) Show that the following are two examples of this situation:

(1) $V = \mathbb{F}^n$ and for some fixed k,

$$\mathcal{P}_1\left(\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}\right) = \begin{bmatrix} v_1 \\ \vdots \\ v_k \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \mathcal{P}_2\left(\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}\right) = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ v_{k+1} \\ \vdots \\ v_n \end{bmatrix}.$$

(2) $V = \mathbb{F}^n$ and for each $i = 1, \ldots, n$,

$$\mathcal{P}_i\left(\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}\right) = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ v_i \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

25. Let $\mathcal{S}\colon V \to V$ and $\mathcal{T}\colon V \to V$ be linear transformations.

(a) If $v \in \operatorname{Ker}(\mathcal{T})$, show that $v \in \operatorname{Ker}(\mathcal{ST})$.

(b) Give an example to show that if $v \in \operatorname{Ker}(\mathcal{T})$, it is not necessarily the case that $v \in \operatorname{Ker}(\mathcal{TS})$.

(c) If $v \in \operatorname{Im}(\mathcal{ST})$, show that $v \in \operatorname{Im}(\mathcal{S})$.

(d) Give an example to show that if $v \in \operatorname{Im}(\mathcal{ST})$, it is not necessarily the case that $v \in \operatorname{Im}(\mathcal{T})$.

26. (a) Let $\mathcal{T}\colon U \to V$ and $\mathcal{S}\colon V \to W$ be linear transformations between finite-dimensional vector spaces. Show that $\operatorname{rank}(\mathcal{ST}) \leq \min(\operatorname{rank}(\mathcal{S}), \operatorname{rank}(\mathcal{T}))$.

(b) For any nonnegative integers k, m, and n, with $k \leq \min(m, n)$, give an example of linear transformations $\mathcal{T}\colon U \to V$ and $\mathcal{S}\colon V \to W$ with $\operatorname{rank}(\mathcal{S}) = m$, $\operatorname{rank}(\mathcal{T}) = n$, and $\operatorname{rank}(\mathcal{ST}) = k$.

(c) Show that in fact

$$\operatorname{rank}(\mathcal{S}) + \operatorname{rank}(\mathcal{T}) - \dim(V) \leq \operatorname{rank}(\mathcal{ST}) \leq \min(\operatorname{rank}(\mathcal{S}), \operatorname{rank}(\mathcal{T})).$$

(d) For any nonnegative integers k, m, n, and p, with $p \leq m + n$ and $k \leq \min(m, n, p)$, give an example of a pair of linear transformations $\mathcal{T}\colon U \to V$ and $\mathcal{S}\colon V \to W$ with $\operatorname{rank}(\mathcal{S}) = m$, $\operatorname{rank}(\mathcal{T}) = n$, $\dim(V) = p$, and $\operatorname{rank}(\mathcal{ST}) = m + n - p$.

27. (a) Let A be an m-by-n matrix, and let B be an n-by-m matrix. Then $C = AB$ is an m-by-m matrix and $D = BA$ is an n-by-n matrix. Suppose that $m > n$. Show that it is impossible for C to be the identity matrix I_m.

(b) Give an example to show that, for any $m \geq n$, it is possible for D to be the identity matrix I_n.

28. (a) Define the s-rank of a matrix M to be the smallest nonnegative integer s such that M is a sum of matrices $M = A_1 + \cdots + A_s$ with each A_i a matrix of rank 1. Show that the s-rank of M is equal to the rank of M.

(b) Define the t-rank of a matrix M to be the smallest nonnegative integer $t = t_1 + \cdots + t_k$, where M is a sum of matrices $M = A_1 + \cdots + A_k$ with A_i a matrix of rank t_i for each i. Show that the t-rank of M is equal to the rank of M.

(These are not standard definitions.)

29. Let V be a finite-dimensional vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. Show that $\operatorname{rank}(\mathcal{T}^2) = \operatorname{rank}(\mathcal{T})$ if and only if $\operatorname{Ker}(\mathcal{T}) \cap \operatorname{Im}(\mathcal{T}) = \{0\}$.

30. Let V be an n-dimensional vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. $\mathcal{T}$ is *nilpotent* if $\mathcal{T}^k = 0$ for some positive integer k. In this case, the smallest positive integer k for which $\mathcal{T}^k = 0$ is called the *index of nilpotence* of $\mathcal{T}$.

(a) Show that $1 \le k \le n$.

(b) Show by example that for every k between 1 and n, there is a nilpotent linear transformation whose index of nilpotence is k.

31. Let V be a finite-dimensional vector space, and let $\mathcal{T}\colon V \to V$ be a nilpotent linear transformation. Show that V has a basis $\mathcal{B}$ with $[T]_{\mathcal{B}}$ a strictly upper triangular matrix, i.e., a triangular matrix with all diagonal entries equal to 0.

32. Let V be n-dimensional, and let $\mathcal{T}\colon V \to V$ be a nilpotent linear transformation with index of nilpotence n. Show that V has a basis $\mathcal{B}$ with

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & 0 & 1 & & 0 \\ \vdots & \vdots & 0 & & 0 \\ & & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix}.$$

(In this matrix, every entry immediately above the diagonal is 1 and all the other entries are 0.)

33. (a) Let $\mathcal{R}\colon V \to V$ be a nilpotent linear transformation with index of nilpotence i, and let $\mathcal{S}\colon V \to V$ be a nilpotent linear transformation with index of nilpotence j. Suppose that $\mathcal{R}$ and $\mathcal{S}$ commute. Show that $\mathcal{T} = \mathcal{R} + \mathcal{S}$ is a nilpotent linear transformation with index of nilpotence $k \le i + j$.

(b) Give an example where $\mathcal{R}\colon V \to V$ is a nilpotent linear transformation and $\mathcal{S}\colon V \to V$ is a nilpotent linear transformation with $\mathcal{R}$ and $\mathcal{S}$ not commuting where $\mathcal{R} + \mathcal{S}$ is nilpotent, and one where $\mathcal{R} + \mathcal{S}$ is not.

34. Let $\mathcal{T}$ be a nilpotent linear transformation.

(a) Show that $\mathcal{I} - \mathcal{T}$ is invertible.

(b) More generally, suppose that $\mathcal{S}$ is an invertible linear transformation that commutes with $\mathcal{T}$ (i.e., $\mathcal{ST} = \mathcal{TS}$). Show that $\mathcal{S} - \mathcal{T}$ is invertible.

(c) Give a counterexample to (b) when $\mathcal{S}$ does not commute with $\mathcal{T}$.

35. (a) Let $\mathcal{S}\colon V \to W$ and $\mathcal{T}\colon V \to W$ be linear transformations. Show that

$$|\operatorname{rank}(\mathcal{S}) - \operatorname{rank}(\mathcal{T})| \leq \operatorname{rank}(\mathcal{S} + \mathcal{T}) \leq \operatorname{rank}(\mathcal{S}) + \operatorname{rank}(\mathcal{T}).$$

(b) Let a, b, m, and n be any nonnegative integers. Let k be any integer with $|a - b| \leq k \leq a + b$ and also $k \leq m$ and $k \leq n$. Give an example of a pair of linear transformations $\mathcal{S}\colon V \to W$, $\mathcal{T}\colon V \to W$ with $\dim(V) = m$, $\dim(W) = n$, $\operatorname{rank}(\mathcal{S}) = a$, $\operatorname{rank}(\mathcal{T}) = b$, and $\operatorname{rank}(\mathcal{S} + \mathcal{T}) = k$.

(Thus, if we let $\mathcal{R} = \mathcal{S} + \mathcal{T}\colon V \to W$, then $\operatorname{rank}(\mathcal{R}) \leq \min(m, n)$ and in addition to that restriction, the only restriction on $\operatorname{rank}(\mathcal{R})$ is that given in part (a).)

36. Let V be a vector space and $\mathcal{T}\colon V \to V$ a fixed linear transformation. Let $\mathcal{C} = \{v_i\}$ be a set of vectors in V. Define the $\mathcal{T}$-Span of $\mathcal{C}$ to be

$$\mathcal{T}\text{-Span}(\mathcal{S}) = \operatorname{Span}(\{p(\mathcal{T})(v_i) \,|\, v_i \in \mathcal{C}, p(x) \in \mathbb{F}[x]\}).$$

Define the $\mathcal{T}$-rank of V to be the minimal number of elements in a set $\mathcal{C}$ that $\mathcal{T}$-spans V.

(a) Show that if $\mathcal{T} = c\mathcal{I}$ for any c (including $c = 0$ and $c = 1$), $\mathcal{T}\text{-rank}(V) = \dim V$.

(b) For every positive integer n, give an example of a vector space V of dimension n with $\mathcal{T}$-rank k for each integer k with $1 \leq k \leq n$.

(c) Give an example of an infinite-dimensional vector space V with $\mathcal{T}$-rank 1.

Note we have defined the $\mathcal{T}$-rank of V to be the minimal number of elements in a set $\mathcal{C}$ that $\mathcal{T}$-spans V and *not* the number of elements in a minimal set $\mathcal{C}$ that $\mathcal{T}$-spans V (i.e., a set $\mathcal{C}$ that $\mathcal{T}$-spans V but no proper subset of $\mathcal{C}$ $\mathcal{T}$-spanning V).

(d) Give an example of two minimal $\mathcal{T}$-spanning sets $\mathcal{C}_1$ and $\mathcal{C}_2$ of V with different numbers of elements.

37. Let V be a vector space and $\mathcal{S}\colon V \to V$ and $\mathcal{T}\colon V \to V$ commuting linear transformations (i.e., $\mathcal{ST} = \mathcal{TS}$). If $\mathcal{S}$ is invertible, show that $\mathcal{S}^{-1}$ commutes with $\mathcal{T}$. (Similarly, if $\mathcal{T}$ is invertible, then $\mathcal{T}^{-1}$ commutes with $\mathcal{S}$, and if both are invertible, $\mathcal{S}^{-1}$ commutes with $\mathcal{T}^{-1}$.)

38. Let V be a vector space, and let $\mathcal{T}\colon V \to V$ be an invertible linear transformation.

(a) If V is finite dimensional, show that $\mathcal{T}^{-1}$ is a polynomial in $\mathcal{T}$.

(b) Give an example to show this need not be true if V is infinite dimensional.

39. Let V be a finite-dimensional vector space, and let $\mathcal{T}: V \to V$ be a linear transformation. Let $U_i = \operatorname{Im}(\mathcal{T}^i)$, $i = 0, 1, 2, \ldots$, and $W_i = \operatorname{Ker}(\mathcal{T}^i)$, $i = 0, 1, 2, \ldots$.

(a) Show that $U_0 \supseteq U_1 \supseteq U_2 \supseteq \cdots$. Let $r_i = \dim(U_i)$. Then $r_0 \geq r_1 \geq r_2 \geq \cdots$. Show there is an integer p such that $r_0 > r_1 > \cdots > r_p$ and $r_{p+1} = r_{p+2} = r_{p+3} = \cdots$.

(b) Show that $W_0 \subseteq W_1 \subseteq W_2 \subseteq \cdots$. Let $k_i = \dim(W_i)$. Then $k_0 \leq k_1 \leq k_2 \leq \cdots$. Show there is an integer q such that $k_0 < k_1 < \cdots < k_q$ and $k_{q+1} = k_{q+2} = k_{q+3} = \cdots$.

(c) Show that the integers p of part (a) and q of part (b) are equal.

40. Let V be a vector space, and let $\mathcal{T}: V \to V$ be a linear transformation. Of course, if $\mathcal{T}$ is invertible, then, setting $\mathcal{S} = \mathcal{T}^{-1}$, we have $\mathcal{T}\mathcal{S} = \mathcal{I}$ and hence $\mathcal{T}\mathcal{S}\mathcal{T} = \mathcal{T}$. Show that this last fact is true whether or not $\mathcal{T}$ is invertible. That is, show that for *any* linear transformation $\mathcal{T}: V \to V$ there is a linear transformation $\mathcal{S}: V \to V$ with $\mathcal{T}\mathcal{S}\mathcal{T} = \mathcal{T}$.

41. Let V be the vector space of doubly infinite sequences of real numbers, i.e.,

$$V = \{s = (\ldots, a_{-2}, a_{-1}, a_0, a_1, a_2, \ldots) \mid a_i \in \mathbb{R} \text{ for each } i\}.$$

For a set of fixed real numbers $R = \{r_0, \ldots, r_k\}$ with $r_0 \neq 0$ and $r_k \neq 0$, we will say that s satisfies the linear recurrence determined by R if

$$r_0 a_i + r_1 a_{i+1} + \cdots + r_k a_{i_k} = 0 \quad \text{for every } i = \ldots, -2, -1, 0, 1, 2, \ldots.$$

Let W be the subspace

$$W = \{s \in V \mid s \text{ satisfies the linear recurrence determined by } R\}.$$

Show that W is a subspace of V of dimension k. Find a basis of W.

(As an example, we may take $R = \{-1, -1, 1\}$, which gives the linear recurrence $-a_i - a_{i+1} + a_{i+2} = 0$, i.e., $a_{i+2} = a_i + a_{i+1}$, the linear recurrence satisfied by the Fibonacci numbers.)

42. Let $V = P(\mathbb{R})$, the space of all real polynomials.

(a) Let $\mathcal{T}: V \to V$ by $\mathcal{T}(p(x)) = xp'(x)$. Show that $\mathcal{T}$ is neither 1-1 nor onto.

(b) Let $\mathcal{S}: V \to V$ by $\mathcal{S}(p(x)) = p(x) + p'(x)$. Show that $\mathcal{S}$ is both 1-1 and onto.

43. (a) Let $V = P_d(\mathbb{R})$, the space of all real polynomials of degree at most d. Let $\mathcal{S}: V \to V$ be a linear transformation with the property that $\deg \mathcal{S}(p(x)) = \deg p(x)$ for every polynomial $p(x) \in V$. Show that $\mathcal{S}$ is an isomorphism.

(b) Now let $V = P(\mathbb{R})$, the space of all real polynomials, and let $\mathcal{S}: V \to V$ be a linear transformation with the same property. Show that, here too, $\mathcal{S}$ is an isomorphism.

44. (a) Let V be a (necessarily infinite-dimensional) vector space, and let $\mathcal{T}: V \to V$ be a linear transformation that is onto, but with $\operatorname{Ker}(\mathcal{T})$ 1-dimensional. Let v_1 be any nonzero vector in $\operatorname{Ker}(\mathcal{T})$. Show that, for any positive integer k, $\operatorname{Ker}(\mathcal{T}^k)$ is k-dimensional with basis $\{v_1, \ldots, v_k\}$, where $\mathcal{T}(v_i) = v_{i-1}$ for $i = 2, \ldots, k$.

(b) Let W be a (necessarily infinite-dimensional) vector space, and let $\mathcal{S}\colon W \to W$ be a linear transformation that is 1-1, but with $\mathrm{Im}(\mathcal{S})$ a subspace of W of codimension 1. Let w_1 be any vector not in $\mathrm{Im}(\mathcal{S})$. Show that, for any positive integer k, $\mathrm{Im}(\mathcal{S}^k)$ is a subspace of W of codimension k, having a complement with basis $\{w_1, \ldots, w_k\}$, where $\mathcal{S}(w_i) = w_{i+1}$ for $i = 1, \ldots, k-1$.

45. (a) A complex number α is called *algebraic* if it is a root of polynomial $p(x)$ with rational coefficients. For example, $\alpha = \sqrt{2} + \sqrt{3}$ is algebraic as $p(\alpha) = 0$, where $p(x)$ is the polynomial $p(x) = x^4 - 10x^2 + 1$. Show that the following are equivalent:

(1) α is algebraic.

(2) The $\mathbb{Q}$-vector space spanned by $\{1, \alpha, \alpha^2, \alpha^3, \ldots\}$ is finite dimensional.

(b) Let α be a nonzero complex number. Show that the following are equivalent:

(1) α is algebraic.

(2) $1/\alpha = q(\alpha)$ for some polynomial $q(x)$ with rational coefficients.

Let α be algebraic. Then there is a unique monic polynomial $p_\alpha(x)$ of smallest degree with $p_\alpha(\alpha) = 0$.

(c) Let $p_\alpha(x)$ have degree d. Show that the dimension of the $\mathbb{Q}$-vector space spanned by $\{1, \alpha, \alpha^2, \ldots\}$ is equal to d. This integer d is called the *degree* of the algebraic number α.

46. Let $V_n, V_{n-1}, \ldots, V_0$ be a sequence of finite-dimensional vector spaces, and let $\mathcal{T}_i\colon V_i \to V_{i-1}$ be a linear transformation for each i, $1 \le i \le n$. The sequence

$$\{0\} \to V_n \xrightarrow{\mathcal{T}_n} V_{n-1} \xrightarrow{\mathcal{T}_{n-1}} V_{n-2} \to \cdots \to V_1 \xrightarrow{\mathcal{T}_1} V_0 \to \{0\}$$

is *exact* if

(1) $\mathcal{T}_n$ is a monomorphism,

(2) $\mathrm{Ker}(\mathcal{T}_{i-1}) = \mathrm{Im}(\mathcal{T}_i)$ for each $i = 2, \ldots, n$,

(3) $\mathcal{T}_1$ is an epimorphism.

(Note that there is a unique linear transformation $\mathcal{T}_{n+1}\colon \{0\} \to V_n$ given by $\mathcal{T}_{n+1}(0) = 0$, and there is a unique linear transformation $\mathcal{T}_0\colon V_0 \to \{0\}$ given by $\mathcal{T}_0(v) = 0$ for every $v \in V_0$. Using these, we could rephrase the three conditions above as the single condition $\mathrm{Ker}(\mathcal{T}_{i-1}) = \mathrm{Im}(\mathcal{T}_i)$ for each $i = 1, \ldots, n+1$.)

Show the following:

(a1) If $\{0\} \to V_0 \to \{0\}$ is an exact sequence, then $V_0 = \{0\}$.

(a2) If $\{0\} \to V_1 \xrightarrow{\mathcal{T}_0} V_0 \to \{0\}$ is an exact sequence, then $\mathcal{T}_0\colon V_1 \to V_0$ is an isomorphism.

(a3) If $\{0\} \to V_2 \xrightarrow{\mathcal{T}_1} V_1 \xrightarrow{\mathcal{T}_0} V_0 \to \{0\}$ is an exact sequence, then V_0 is isomorphic to the quotient V_1/B_1, where $B_1 = \mathrm{Im}(\mathcal{T}_1)$. (Note that $\mathcal{T}_1\colon V_2 \to B_1$ is an isomorphism.)

An exact sequence as in (a3) is called a *short* exact sequence.

(b) Given an exact sequence as above, show that

$$\sum_{i=0}^{n}(-1)^i \dim(V_i) = 0.$$

A sequence

$$\{0\} \to V_n \xrightarrow{\mathcal{T}_n} V_{n-1} \xrightarrow{\mathcal{T}_{n-1}} V_{n-2} \to \cdots \to V_1 \xrightarrow{\mathcal{T}_1} V_0 \to \{0\}$$

is *half-exact* if $\mathrm{Ker}(\mathcal{T}_{i-1}) \supseteq \mathrm{Im}(\mathcal{T}_i)$ for each $i = 2, \ldots, n$. (With $\mathcal{T}_{n+1}$ and $\mathcal{T}_0$ as above, note it is automatically the case that $\mathrm{Ker}(\mathcal{T}_{i-1}) \supseteq \mathrm{Im}(\mathcal{T}_i)$ for $i = 1$ and for $i = n+1$.)

For a half-exact sequence, define subspaces Z_i and B_i of V_i by

$$Z_i = \mathrm{Ker}(\mathcal{T}_{i-1}), \quad B_i = \mathrm{Im}(\mathcal{T}_i) \quad \text{for } i = 0, \ldots, n.$$

Then $B_i \subseteq Z_i$ for each i, so we may define

$$H_i = Z_i/B_i \quad \text{for } i = 0, \ldots, n.$$

(c) Show that

$$\sum_{i=0}^{n}(-1)^i \dim(H_i) = \sum_{i=0}^{n}(-1)^i \dim(V_i).$$

This common value is called the *Euler characteristic* of the sequence.

47. Let V be an n-dimensional vector space, and let $\mathcal{T}\colon V \to W$ be a linear transformation. Prove the basic dimension counting theorem (Corollary 5.2.3) as follows. Let $\mathrm{Ker}(\mathcal{T})$ be k-dimensional, and let $\mathcal{B}_0 = \{v_1, \ldots, v_k\}$ be a basis of $\mathrm{Ker}(\mathcal{T})$. Extend $\mathcal{B}_0$ to a basis $\mathcal{B} = \{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ of V. Let $\mathcal{C} = \{\mathcal{T}(v_{k+1}), \ldots, \mathcal{T}(v_n)\}$. Show that $\mathcal{C}$ is a basis of $\mathrm{Im}(\mathcal{T})$.

(Then $\dim\ \mathrm{Ker}(\mathcal{T}) + \dim\ \mathrm{Im}(\mathcal{T}) = k + (n-k) = n = \dim\ V$.)

48. Complete the proof of Corollary 5.2.2. That is: let $\mathcal{T}\colon V \to W$ be a linear transformation.

Let $V_0 = \mathrm{Ker}(\mathcal{T})$, a subspace of V, and let $W_0 = \mathrm{Im}(\mathcal{T})$, a subspace of W. Let $\overline{\mathcal{T}}\colon V/V_0 \to W_0$ be defined by $\overline{\mathcal{T}}(v + V_0) = \mathcal{T}(v)$.

(a) Show that $\overline{\mathcal{T}}$ is well-defined (i.e., independent of the choice of v).

(b) Show that $\overline{\mathcal{T}}$ is a linear transformation.

(c) Show that $\overline{\mathcal{T}}\colon V/V_0 \to W_0$ is an isomorphism.

49. Let $\mathcal{T}\colon V \to W$ be a linear transformation, and let U be a subspace of $V_0 = \mathrm{Ker}(\mathcal{T})$.

Let $\overline{\mathcal{T}}\colon V/U \to W$ be defined by $\overline{\mathcal{T}}(v+U) = \mathcal{T}(v)$. Show that $\overline{\mathcal{T}}$ is a well-defined linear transformation. Furthermore, let $\mathcal{P}\colon V \to V/U$ be defined by $\mathcal{P}(v) = v + U$. Show that $\mathcal{T} = \overline{\mathcal{T}}\mathcal{P}$ (i.e., that $\mathcal{T}(v) = \overline{\mathcal{T}}(\mathcal{P}(v))$ for every vector $v \in V$).

50. Let V be a vector space, and let T and U be subspaces of V. Let $\mathcal{P}\colon T \to V/U$ by $\mathcal{P}(t) = t + U$, where $t \in T$.

(a) Show that $\mathrm{Ker}(\mathcal{P}) = T \cap U$.

(b) Show that $\mathrm{Im}(\mathcal{P}) = (T+U)/U$.

(c) Conclude that $T/(T \cap U)$ is isomorphic to $(T+U)/U$.

51. Let V be a vector space, and let T and U be subspaces of V with $T \subseteq U$. Show that V/U is isomorphic to $(V/T)/(U/T)$.

52. Let V be a vector space, and let T be a subspace of V. To any subspace U of V that contains T we can associate the subspace $a(U) = U/T$ of V/T. Show that a gives a 1-1 correspondence,

$$\{\text{subspaces of } V \text{ containing } T\} \xrightarrow{a} \{\text{subspaces of } V/T\}.$$

53. Let $\mathcal{T}\colon V \to V$ be a linear transformation, and let U be a subspace of V with $\mathcal{T}(U) \subseteq U$. (Such a subspace is said to be $\mathcal{T}$-*invariant*.)

(a) Show that $\overline{\mathcal{T}}\colon V/U \to V/U$ defined by $\overline{\mathcal{T}}(v_0+U) = \mathcal{T}(v_0)+U$ is well-defined (i.e., is independent of the choice of v_0) and is a linear transformation.

(b) Let $\mathcal{S}$ be the restriction of $\mathcal{T}$ to U, so that $\mathcal{S}\colon U \to U$. Show that $\mathcal{T}$ is an isomorphism if and only if $\mathcal{S}$ and $\overline{\mathcal{T}}$ are isomorphisms.

(c) Suppose that V is finite dimensional, and let U be a subspace of V. Let $\mathcal{B}_0$ be a basis of U and extend $\mathcal{B}_0$ to a basis $\mathcal{B}$ of V, so that $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{C}$. Let $\mathcal{T}\colon V \to V$ be a linear transformation. Find a condition on $[\mathcal{T}]_{\mathcal{B}}$ that is necessary and sufficient for U to be $\mathcal{T}$-invariant.

(d) Let $\mathcal{P}\colon V \to V/U$ by $\mathcal{P}(v) = v+U$, and let $\overline{\mathcal{C}} = \mathcal{P}(\mathcal{C})$. In this situation, relate $[\mathcal{T}]_{\mathcal{B}}$ to $[\mathcal{S}]_{\mathcal{B}_0}$ and $[\overline{\mathcal{T}}]_{\overline{\mathcal{C}}}$.

54. (a) In the notation of Exercise 53, show that $\mathcal{T}$ is nilpotent if and only if $\mathcal{S}$ and $\overline{\mathcal{T}}$ are nilpotent.

(b) Let $\mathcal{S}$ have index of nilpotence i, $\overline{\mathcal{T}}$ have index of nilpotence j, and $\mathcal{T}$ have index of nilpotence k. Show that $\max(i,j) \le k \le i+j$.

55. Let $\mathcal{T}\colon V \to V$ be a linear transformation, and let U be a subspace of V with $\mathcal{T}(U) \subseteq U$. Let $\mathcal{S}$ be the restriction of $\mathcal{T}$ to U, so that $\mathcal{S}\colon U \to U$. Suppose that $\mathcal{T}$ is an isomorphism.

(a) If V is finite dimensional, show that $\mathcal{S}$ is an isomorphism.

(b) Give a counterexample in case V is infinite dimensional.

56. Complete the proof of Lemma 5.5.12.

57. Let $V = M_{m,n}(\mathbb{F})$.

(a) For a fixed matrix B, define $\mathcal{S}_B(A) = \mathrm{trace}(A\,{}^tB)$, where the *trace* of a square matrix is defined to be the sum of its diagonal entries. Show that $\mathcal{S}_B \in V^*$.

(b) Show that $\mathcal{T}\colon V \to V^*$ by $\mathcal{T}(B) = \mathcal{S}_B$ is an isomorphism.

(c) Let $\mathcal{B} = \{E_{ij}\}$ be the basis of V with E_{ij} the matrix having an entry of 1 in the (i,j) position and all other entries 0. Let $\mathcal{B}^* = \{E_{ij}^*\}$ be the dual basis. Show that $\mathcal{T}(E_{ij}) = E_{ij}^*$.

58. Let $V = P_3(\mathbb{R})$, and let $\mathcal{E} = \{1, x, x^2, x^3\}$ be the standard basis of V. Let $\mathcal{E}^*$ be the dual basis of V^*. Let $\mathcal{B}^* = \{b_0, b_1, b_2, b_3\}$ be the basis of V^* given by $b_i(f(x)) = f^{(i)}(0)$. Let $\mathcal{C}^* = \{c_0, c_1, c_2, c_3\}$ be the basis of V^* given by $c_i(f(x)) = f(i)$.

(a) Find the change of basis matrices $P_{\mathcal{E}^* \leftarrow \mathcal{B}^*}$ and $P_{\mathcal{B}^* \leftarrow \mathcal{E}^*}$.

(b) Find the change of basis matrices $P_{\mathcal{E}^* \leftarrow \mathcal{C}^*}$ and $P_{\mathcal{C}^* \leftarrow \mathcal{E}^*}$.

We may identify V with V^{**}. Under this identification:

(c) Find the dual basis $\mathcal{B}$ of $\mathcal{B}^*$.

(d) Find the dual basis $\mathcal{C}$ of $\mathcal{C}^*$.

Let $\mathcal{T}_i \colon V \to V$, $i = 1, \ldots, 4$, be the following linear transformations:

$$\begin{aligned}
\mathcal{T}_1(f(x)) &= f'(x), \\
\mathcal{T}_2(f(x)) &= f(x+1), \\
\mathcal{T}_3(f(x)) &= xf'(x), \\
\mathcal{T}_4(f(x)) &= x(f(x+1) - f(x)).
\end{aligned}$$

(e) Find $[\mathcal{T}_i]_{\mathcal{E}}$ for $i = 1, \ldots, 4$.

(f) Find $[\mathcal{T}_i^*]_{\mathcal{B}^*}$ for $i = 1, \ldots, 4$.

(g) Find $[\mathcal{T}_i^*]_{\mathcal{C}^*}$ for $i = 1, \ldots, 4$.

59. Let $V = P_3(\mathbb{R})$, the vector space of polynomials of degree at most 3. Let V^* be the dual space of V.

(a) For $i = 1, 2, 3, 4$, let $a_i(p(x)) = \int_0^i p(x)\,dx$. Show that $\{a_1, a_2, a_3, a_4\}$ is a basis of V^*.

(b) Let $b_0(p(x)) = p(0)$ and for $i = 1, 2, 3$ let $c_i(p(x)) = p'(i)$. Show that $\{b_0, c_1, c_2, c_3\}$ is a basis of V^*.

Now let $V = P_d(\mathbb{R})$, the vector space of polynomials of degree at most d. Let V^* be the dual space of V.

(c) Let $r_1, \ldots, r_{d+1}$ be any $d+1$ distinct nonzero real numbers, and let $a_i(p(x)) = \int_0^{r_i} p(x)\,dx$.

Show that $\{a_1, \ldots, a_{d+1}\}$ is a basis of V^*.

(d) Let r_0 be any real number, and let $r_1, \ldots, r_d$ be any d distinct real numbers. Let $b_0(p(x)) = p(r_0)$ and $c_i(p(x)) = p'(r_i)$. Show that $\{b_0, c_1, \ldots, c_d\}$ is a basis of V^*.

60. (a) Let $V = P_2(\mathbb{R})$, and let V^* be the dual space of V. Let $a_i(f(x)) = \int_0^i f(x)\,dx$. Then $\mathcal{B} = \{a_1, a_2, a_3\}$ is a basis of V^*. Express each of the following elements of V^* as a linear combination of the elements of $\mathcal{B}$.

(i) $b(f(x)) = \int_0^4 f(x)\,dx$.

(ii) $b(f(x)) = \int_0^1 xf(x)\,dx$.

(iii) $b(f(x)) = f(0)$.

(iv) $b(f(x)) = f'(1)$.

(b) Identifying V with V^{**}, the dual of V^*, find the basis of V that is dual to the basis $\mathcal{B}$ of V^*.

61. Referring to Example 5.5.15:

(a) Show that, for any value of d, $c_{d-i} = c_i$ for each $i = 0, \ldots, d$.

(b) Show that, for any even value of d, the $(d+1)$-point rule is exact on $P_{d+1}(\mathbb{R})$.

(c) Find the values of $c_0, \ldots, c_d$ in the cases $d = 0, 1, 2, 3, 4$.

62. Referring to Example 5.5.17:

(a) Show that, for any even value of d, $c_{d-i} = -c_i$ for each $i = 0, \ldots, d$ (and hence that $c_{d/2} = 0$), where c_i is the coefficient of $p(a_i)$ in the expansions.

(b) Find the values of $c_0, \ldots, c_d$ in the cases $d = 2, 4, 6$.

Chapter 6

The determinant

In this chapter we study the determinant of a square matrix. (Determinants are only defined for square matrices.)

The determinant of a square matrix A has a geometric interpretation as a signed volume. This leads us to begin with a heuristic discussion of properties we would like volume to have. Then we go on to show there is a unique function, the determinant, having these properties. And then, once we have developed the determinant, we go on to study it further.

At the end of this chapter, we will recall how determinants appear in calculus, in the guise of Jacobians.

In this chapter we think about determinants from a geometric viewpoint. In the next chapter we will see that they are an essential algebraic tool.

6.1. Volume functions

In this section we want to present a purely heuristic discussion of what a volume function should be. We will arrive at a pair of properties that a volume function should have.

Then in the next section we will start with these properties and show how to rigorously construct volume functions, chief among them the determinant.

Since we are thinking geometrically, we will consider that we are in $\mathbb{R}^n$ for some n, and think of a vector as an "arrow" from the origin to its endpoint.

Before going any further, we want to point out why it is essential to consider signed volume rather than ordinary (i.e., nonnegative) volume. We can already see this in $\mathbb{R}^1$, where volume is just length. We would like lengths to add, i.e., if v_1, v_2, and v_3 are three vectors in $\mathbb{R}^1$ with $v_3 = v_1 + v_2$, we would like to have that the length of v_3 is the sum of the lengths of v_1 and v_2. If $v_1 = [5]$ and $v_2 = [3]$, this is no problem: $v_3 = [8]$ has length 8 and sure enough $5 + 3 = 8$. But if $v_1 = [5]$ and $v_2 = [-3]$ and we are considering ordinary length, this is a problem: $v_3 = [2]$ has length 2 and $5 + 3 \neq 2$. However, if we consider signed length, then v_1 has length 1, v_2 has length -3, and v_3 has length 2, and sure enough $5 + (-3) = 2$. So that is what we will do. And we notice that in each case, if v_i is obtained from $e_i = [1]$ by "scaling" by a factor of c_i, i.e., $v_i = c_i e_1$, then the signed length "scales" by exactly that factor, i.e., the signed length of v_i is c_i times the signed length of e_1 (which is 1).

Thus henceforth we consider signed volume without further ado, and we use the word volume to mean signed volume.

Now let A be an n-by-n matrix and write $A = [v_1|v_2|\ldots|v_n]$. The columns $v_1, \ldots, v_n$ of A determine an n-parallelepiped, the n-dimensional analog of a parallelogram.

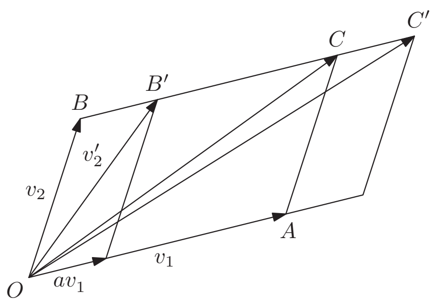
What properties should $\mathrm{Vol}([v_1|\ldots|v_n])$, the volume of this parallelepiped, have? We have two very basic ones.

(1) If we are in $\mathbb{R}^1$, then, as we have just seen, if we scale the edge v_1 by a factor of c, we should multiply the volume by a factor of c. That is, $\mathrm{Vol}([cv_1]) = c\,\mathrm{Vol}([v_1])$. Now the same logic should hold in n dimensions if we leave $v_2, \ldots, v_n$ unchanged throughout the process, so we should have $\mathrm{Vol}([cv_1|v_2|v_3|\ldots|v_n]) = c\,\mathrm{Vol}([v_1|v_2|\ldots|v_n])$. And then it certainly should not matter which vector we single out, so we should have

$$\mathrm{Vol}([v_1|\ldots|cv_i|\ldots|v_n]) = c\,\mathrm{Vol}([v_1|\ldots|v_i|\ldots|v_n]).$$

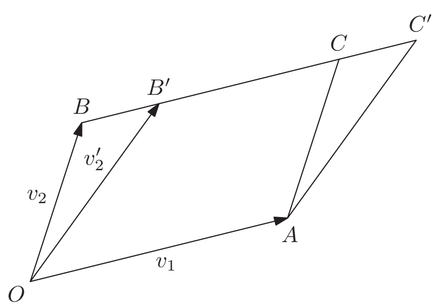
(2) Suppose we are in the plane $\mathbb{R}^2$ and we wish to compare the 2-dimensional volume (i.e., area) of the parallelogram determined by vectors v_1 and v_2 with that of the parallelogram determined by vectors v_1 and $v_2' = v_2 + av_1$.

Here is a picture of how we obtain these two parallelograms:



$v_2' = v_2 + av_1$
C is the endpoint of $v_1 + v_2$
C' is the endpoint of $v_1 + v_2'$

To simplify this picture let us remove some of the edges. We obtain this picture:



P =Parallelogram $OACB$
determined by v_1 and v_2
P' =Parallelogram $OAC'B'$
determined by v_1 and v_2'

But now we notice that triangles $OB'B$ and $AC'C$ are congruent, and then

$$\begin{aligned}\text{Area}(P') &= \text{Area}(OAC'B') \\ &= \text{Area}(OACB') + \text{Area}(AC'C) \\ &= \text{Area}(OACB') + \text{Area}(OB'B) \\ &= \text{Area}(OACB) = \text{Area}(P).\end{aligned}$$

In other words, $\text{Vol}([v_1|v_2 + av_1]) = \text{Vol}([v_1|v_2])$. Now the same logic should hold in n dimensions if we leave $v_3, \ldots, v_n$ unchanged throughout the process, so we should have $\text{Vol}([v_1|v_2+av_1|v_3|\ldots|v_n]) = \text{Vol}([v_1|v_2|\ldots|v_n])$. And then it certainly should not matter which two vectors we single out, so we should have

$$\text{Vol}([v_1|\ldots|v_i + av_j|\ldots|v_n]) = \text{Vol}([v_1|\ldots|v_n]).$$

It is convenient to consider all volume functions that satisfy these two properties. But in the end we will want to "normalize" our volume functions. That is, we will want to find a particular volume function Vol_1 which satisfies:

(3) The volume of the unit cube is 1, i.e.,

$$\text{Vol}_1([e_1|e_2|\ldots|e_n]) = 1.$$

Again we point out that we are forced to consider volume, that is, signed volume, if we wish to obtain a natural notion, rather than nonnegative volume, which might be the first notion that occurs to you. (But of course, we may obtain nonnegative volume simply by taking the absolute value of volume.)

We will then see that there is a unique function Vol_1, the *determinant*, i.e., the determinant is the function $\det(A) = \text{Vol}_1(A)$. (Then we will also see that any fixed volume function Vol is given by $\text{Vol}(A) = \det(A)\,\text{Vol}(I)$, so that any volume function is just a scaled version of the determinant.)

Of course, there is some volume function that satisfies (1) and (2): we have the trivial volume function defined by $\text{Vol}(A) = 0$ for every matrix A. That would not be very interesting (or useful). Otherwise, at this point we do not yet know that there is any nontrivial volume function. But let us be optimistic, and proceed in the hope that one exists.

It turns out that properties (1) and (2) are equivalent to two other properties.

Lemma 6.1.1. *The following two sets of properties of a volume function are equivalent (i.e., any function that satisfies one set of properties satisfies the other).*

(1) $\text{Vol}([v_1|\ldots|cv_i|\ldots|v_n]) = c\,\text{Vol}([v_1|\ldots|v_n])$; *and*

(2) $\text{Vol}([v_1|\ldots|v_i + cv_j|\ldots|v_n]) = \text{Vol}([v_1|\ldots|v_n])$

and

(A) (Alternation) *If A has two columns equal, say columns i and j, then* $\text{Vol}(A) = 0$*, i.e.,*

$$\text{Vol}([v_1|\ldots|v_i|\ldots|v_i|\ldots|v_n]) = 0; \quad \textit{and}$$

(M) (Multilinearity) *If some column v_i is a linear combination $v_i = c_1u_1 + c_2u_2$, then*

$$\begin{aligned}\mathrm{Vol}([v_1|\dots|v_i|\dots|v_n]) &= \mathrm{Vol}([v_1|\dots|c_1u_1+c_2u_2|\dots|v_n]) \\ &= c_1\,\mathrm{Vol}([v_1|\dots|u_1|\dots|v_n]) + c_2\,\mathrm{Vol}([v_1|\dots|u_2|\dots|v_n])\end{aligned}$$

(*i.e.*, Vol *is a linear function of each column of A, providing the other columns are left fixed*).

Proof. First we show that any function satisfying (A) and (M) satisfies (1) and (2), which is easy, and then we show that any function satisfying (1) and (2) satisfies (A) and (M), which is considerably more work.

Suppose Vol satisfies (A) and (M). Then

$$\begin{aligned}\mathrm{Vol}([v_1|\dots|cv_i|\dots|v_n]) &= \mathrm{Vol}([v_1|\dots|cv_i+0\cdot 0|\dots|v_n]) \\ &= c\,\mathrm{Vol}([v_1|\dots|v_n]) + 0\,\mathrm{Vol}([v_1|\dots|0|\dots|v_n]) \\ &= c\,\mathrm{Vol}([v_1|\dots|v_i|\dots|v_n])\end{aligned}$$

and

$$\begin{aligned}\mathrm{Vol}([v_1|\dots|v_i+cv_j|\dots|v_n]) &= \mathrm{Vol}([v_1|\dots|v_j|\dots|1v_i+cv_j|\dots|v_n]) \\ &= 1\,\mathrm{Vol}([v_1|\dots|v_j|\dots|v_i|\dots|v_n]) \\ &\quad + c\,\mathrm{Vol}([v_1|\dots|v_j|\dots|v_j|\dots|v_n]) \\ &= 1\,\mathrm{Vol}([v_1|\dots|v_j|\dots|v_i|\dots|v_n]) + c0 \\ &= \mathrm{Vol}([v_1|\dots|v_j|\dots|v_i|\dots|v_n])\end{aligned}$$

and so we see that Vol satisfies (1) and (2).

Now suppose Vol satisfies (1) and (2). Then

$$\begin{aligned}\mathrm{Vol}([v_1|\dots|v_i|\dots|v_i|\dots|v_n]) &= \mathrm{Vol}([v_1|\dots|v_i|\dots|0+v_i|\dots|v_n]) \\ &= \mathrm{Vol}([v_1|\dots|v_i|\dots|0|\dots|v_n]) \\ &= \mathrm{Vol}([v_1|\dots|v_i|\dots|0\cdot 0|\dots|v_n]) \\ &= 0\,\mathrm{Vol}([v_1|\dots|v_i|\dots|0|\dots|v_n]) \\ &= 0\end{aligned}$$

so Vol satisfies (A).

Now we must show (M). In order to simplify the notation, we shall just show this in case $i = n$, where we are dealing with the last column.

We begin with a general observation. Suppose that $\{v_1, \dots, v_n\}$ are not linearly independent. Then we know that $v_i = \sum_{j\neq i} c_j v_j$ for some i and for some scalars. For simplicity, let us suppose $i = n$. Then

$$\begin{aligned}\mathrm{Vol}([v_1|\dots|v_n]) &= \mathrm{Vol}([v_1|\dots|c_1v_1+\cdots+c_{n-1}v_{n-1}]) \\ &= \mathrm{Vol}([v_1|\dots|0+c_1v_1+\cdots+c_{n-1}v_{n-1}]) \\ &= \mathrm{Vol}([v_1|\dots|0+c_1v_1+\cdots+c_{n-2}v_{n-2}]) \\ &= \cdots \\ &= \mathrm{Vol}([v_1|\dots|0]) = 0.\end{aligned}$$

In other words:

If $\{v_1, \ldots, v_n\}$ is not linearly independent, then $\mathrm{Vol}([v_1|\ldots|v_n]) = 0$.

We now return to the proof of (M). Suppose $v_n = a_1u_1 + a_2u_2$. There are several possibilities:

If $\{v_1, \ldots, v_{n-1}\}$ is not linearly independent, then no matter what the last column w is, $\mathrm{Vol}([v_1|\ldots|v_{n-1}|w]) = 0$. Then certainly

$$\mathrm{Vol}([v_1|\ldots|v_n]) = a_1 \mathrm{Vol}([v_1|\ldots|v_{n-1}|u_1]) + a_2 \mathrm{Vol}([v_1|\ldots|v_{n-1}|u_2])$$

as this is just the equation $0 = a_1 0 + a_2 0$.

Suppose $\{v_1, \ldots, v_{n-1}\}$ is linearly independent but $\{v_1, \ldots, v_{n-1}, u_1\}$ is not. Then, as above, $\mathrm{Vol}([v_1|\ldots|v_{n-1}|u_1]) = 0$. But also, by the same logic,

$$\begin{aligned}\mathrm{Vol}([v_1|\ldots|v_{n-1}|a_1u_1 + a_2u_2]) &= \mathrm{Vol}([v_1|\ldots|v_{n-1}|a_2u_2]) \\ &= a_2 \mathrm{Vol}([v_1|\ldots|v_{n-1}|u_2])\end{aligned}$$

so

$$\mathrm{Vol}([v_1|\ldots|v_{n-1}|a_1u_1+a_2u_2]) = a_1 \mathrm{Vol}([v_1|\ldots|v_{n-1}|u_1])+a_2 \mathrm{Vol}([v_1|\ldots|v_{n-1}|u_2]).$$

Finally (and this is the most interesting case), suppose $\{v_1, \ldots, v_{n-1}, u_1\}$ is linearly independent. Then it also spans $\mathbb{R}^n$. In particular, we may write u_2 as a linear combination of these vectors, $u_2 = c_1v_1 + \cdots + c_{n-1}v_{n-1} + bu_1$. Then

$$\begin{aligned}&\mathrm{Vol}([v_1|\ldots|v_{n-1}|a_1u_1 + a_2u_2]) \\ &\quad= \mathrm{Vol}([v_1|\ldots|v_{n-1}|a_1u_1 + a_2(c_1v_1 + \cdots + c_{n-1}v_{n-1} + bu_1)]) \\ &\quad= \mathrm{Vol}([v_1|\ldots|v_{n-1}|(a_1 + a_2b)u_1 + a_2c_1v_1 + \cdots + a_2c_{n-1}v_{n-1}]) \\ &\quad= \mathrm{Vol}([v_1|\ldots|v_{n-1}|(a_1 + a_2b)u_1]) = (a_1 + a_2b) \mathrm{Vol}([v_1|\ldots|v_{n-1}|u_1]).\end{aligned}$$

But

$$\mathrm{Vol}([v_1|\ldots|v_{n-1}|a_1u_1]) = a_1 \mathrm{Vol}([v_1|\ldots|v_{n-1}|u_1])$$

and

$$\begin{aligned}\mathrm{Vol}([v_1|\ldots|v_{n-1}|a_2u_2]) &= \mathrm{Vol}([v_1|\ldots|v_{n-1}|a_2bu_1 + a_2c_1v_1 + \cdots + a_2c_{n-1}v_{n-1}]) \\ &= \mathrm{Vol}([v_1|\ldots|v_{n-1}|a_2bu_1]) \\ &= a_2b \mathrm{Vol}([v_1|\ldots|v_{n-1}|u_1])\end{aligned}$$

so

$$\mathrm{Vol}([v_1|\ldots|v_{n-1}|a_1u_1+a_2u_2]) = a_1 \mathrm{Vol}([v_1|\ldots|v_{n-1}|u_1])+a_2 \mathrm{Vol}([v_1|\ldots|v_{n-1}|u_2]).$$

□

Before proceeding any further, let us see why property (A) is called alternating.

Lemma 6.1.2. *Let* Vol *be a function satisfying* (A). *Then*

$$\mathrm{Vol}([v_1|\ldots|v_j|\ldots|v_i|\ldots|v_n]) = -\mathrm{Vol}([v_1|\ldots|v_i|\ldots|v_j|\ldots|v_n]),$$

i.e., interchanging two columns multiplies Vol *by* -1.

Proof.

$$\begin{aligned}
0 &= \mathrm{Vol}([v_1|\dots|v_i+v_j|\dots|v_i+v_j|\dots|v_n]) \\
&= \mathrm{Vol}([v_1|\dots|v_i|\dots|v_i+v_j|\dots|v_n]) \\
&\qquad + \mathrm{Vol}([v_1|\dots|v_j|\dots|v_i+v_j|\dots|v_n]) \\
&= \mathrm{Vol}([v_1|\dots|v_i|\dots|v_i|\dots|v_n]) \\
&\qquad + \mathrm{Vol}([v_1|\dots|v_i|\dots|v_j|\dots|v_n]) \\
&\qquad + \mathrm{Vol}([v_1|\dots|v_j|\dots|v_i|\dots|v_n]) \\
&\qquad + \mathrm{Vol}([v_1|\dots|v_j|\dots|v_j|\dots|v_n]) \\
&= 0 + \mathrm{Vol}([v_1|\dots|v_i|\dots|v_j|\dots|v_n]) \\
&\qquad + \mathrm{Vol}([v_1|\dots|v_j|\dots|v_i|\dots|v_n]) + 0
\end{aligned}$$

so

$$\mathrm{Vol}([v_1|\dots|v_j|\dots|v_i|\dots|v_n]) = -\,\mathrm{Vol}([v_1|\dots|v_i|\dots|v_j|\dots|v_n]). \qquad \square$$

We now have the following important result.

Theorem 6.1.3. *Suppose that the function* det *exists (i.e., that there is a volume function with* $\mathrm{Vol}(I) = 1$*). Then*

$$\det(A) \neq 0 \quad \textit{if and only if } A \textit{ is invertible.}$$

Proof. Suppose that A is not invertible. Then the columns $\{v_1, \dots, v_n\}$ of A are not linearly independent. Then we saw in the course of the proof of Lemma 6.1.1 that $\det([v_1|\dots|v_n]) = \det(A) = 0$.

Now suppose that A is invertible. Then the columns $\{v_1, \dots, v_n\}$ of A span $\mathbb{F}^n$. Set $A_0 = A$, for convenience.

Let us introduce the notation $x \sim y$ to mean that x is a nonzero multiple of y (or equivalently that y is a nonzero multiple of x). Otherwise stated, $x \sim y$ if either both are nonzero or both are zero.

Consider the nth standard unit vector e_n. Since the columns of A_0 span $\mathbb{F}^n$, we can write $e_n = \sum_{i=1}^n c_i v_i$ for some c_i. Since $e_n \neq 0$, not all c_i can be 0. If $c_n \neq 0$, fine; don't do anything and set $A_1 = A_0$. Otherwise, choose some value of k with $c_k \neq 0$ and let A_1 be the matrix obtained from A_0 by interchanging columns k and n of A_0. In either case, $\det(A_0) \sim \det(A_1)$.

(Re)label the columns of A_1 as $\{v_1 \dots, v_n\}$. Then, solving for v_n, we find $v_n = (1/c_n)e_n - \sum_{i=1}^{n-1}(c_i/c_n)v_i$. Thus

$$\begin{aligned}
\det(A_1) = \det([v_1|\dots|v_n]) &= \det\left([v_1|\dots|v_{n-1}|(1/c_n)e_n - \sum_{i=1}^{n-1}(c_i/c_n)v_i]\right) \\
&= \det([v_1|\dots|v_{n-1}|(1/c_n)e_n]) \\
&= (1/c_n)\det([v_1|\dots|v_{n-1}|e_n]) \\
&\sim \det(A_2),
\end{aligned}$$

where A_2 is the matrix $A_2 = [v_1|\dots|v_{n-1}|e_n]$.

Thus $\det(A) = \det(A_0) \sim \det(A_2)$. Now the columns of A_2 still span $\mathbb{F}^n$. Hence we can write the $(n-1)$st standard unit vector e_{n-1} as a linear combination $e_{n-1} = \sum_{i=1}^{n-1} c_i v_i + c_n e_n$. Again not all c_i can be zero, and in fact some c_i with $1 \leq i \leq n-1$ must be nonzero as we obviously cannot have $e_{n-1} = c_n e_n$ for any c_n. If $c_{n-1} \neq 0$, fine; don't do anything and set $A_3 = A_2$. Otherwise, choose some value of k between i and $n-1$ with $c_k \neq 0$ and let A_3 be the matrix obtained from A_2 by interchanging columns k and $n-1$ of A_2. In either case, $\det(A_3) \sim \det(A_2)$. (Re)label the columns of A_3 as $\{v_1, \ldots, v_{n-1}, e_n\}$. Then solving for v_{n-1}, we find $v_{n-1} = (1/c_{n-1})e_{n-1} - \sum_{i=1}^{n-2}(c_i/c_{n-1})v_i - (c_{n-1}/c_n)e_n$. Then we similarly find

$$\begin{aligned}\det(A_3) &= \det([v_1|\ldots|v_{n-1}|e_n]) \\ &= (1/c_{n-1})\det([v_1|\ldots|v_{n-2}|e_{n-1}|e_n]) \sim \det(A_4),\end{aligned}$$

where A_4 is the matrix $A_4 = [v_1|\ldots|v_{n-2}|e_{n-1}|e_n]$. Thus $\det(A) = \det(A_0) \sim \det(A_4)$.

Proceeding in this way, we find

$$\begin{aligned}\det(A) = \det(A_0) &\sim \det([v_1|\ldots|v_n]) \\ &\sim \det([v_1|\ldots|v_{n-1}|e_n]) \\ &\sim \det([v_1|\ldots|v_{n-2}|e_{n-1}|e_n]) \\ &\sim \det([v_1|\ldots|v_{n-3}|e_{n-2}|e_{n-1}|e_n]) \\ &\sim \cdots \\ &\sim \det([e_1|e_2|\ldots|e_n]) = \det(I) = 1\end{aligned}$$

so $\det(A) \neq 0$. □

Remark 6.1.4. Note how this theorem accords perfectly with the intuition of determinant as n-dimensional volume. If A is *not* invertible, the parallelepiped determined by the columns of A lies in some subspace of $\mathbb{F}^n$ of dimension at most $n-1$, so should have n-dimensional volume of 0. But if A *is* invertible, this parallelepiped includes some "solid" piece of $\mathbb{F}^n$, so should have a nonzero n-dimensional volume. ◊

Remark 6.1.5. Let us change our point of view from a "static" to a "dynamic" one. Let $B = [w_1|\ldots|w_n]$ be an n-by-n matrix. Instead of regarding $\det(B)$ as the volume of the parallelepiped determined by the columns of B, we could proceed as follows. We know that $B = [Be_1|Be_2|\ldots|Be_n]$, so that $w_i = Be_i = \mathcal{T}_B(e_i)$. Thus we could regard $\det(B) = \det(B)\cdot 1 = \det(B)\det([e_1|\ldots|e_n])$ as the factor by which the volume 1 of the standard unit cube is multiplied under the linear transformation $\mathcal{T}_B$ taking this unit cube, i.e., the parallelepiped P_I determined by the vectors $e_1, \ldots, e_n$, to the parallelepiped P_B determined by $\mathcal{T}_B(e_1), \ldots, \mathcal{T}_B(e_n)$.

Similarly, $\det(A)$ is the factor by which the volume of the parellelepiped P_I is multiplied by under the linear transformation $\mathcal{T}_A$ which takes it to the parallelepiped P_A. But a linear transformation is homogeneous in the sense that it multiplies the volume of any n-dimensional solid by the *same* factor, so we should also have the volume of the image of the parallelepiped P_B under $\mathcal{T}_A$ being $\det(A)$ times the volume of P_B, i.e., the volume of $\mathcal{T}_A(P_B)$ should be $\det(A)\cdot \mathrm{volume}(P_B) = \det(A)\det(B)$. But $\mathcal{T}_A(P_B) = \mathcal{T}_A(\mathcal{T}_B(I)) = \mathcal{T}_{AB}(I)$ is $\det(AB)\cdot 1 = \det(AB)$.

Thus we would expect from geometry that $\det(AB) = \det(A)\det(B)$, and we will indeed prove that this is true (Corollary 6.2.5). $\Diamond$

6.2. Existence, uniqueness, and properties of the determinant

We now show the determinant exists.

Theorem 6.2.1. *There is a function* $\det\colon M_n(\mathbb{F}) \to \mathbb{F}$ *satisfying properties* (1), (2), *and* (3), *or* (A), (M), *and* (3), *of the last section.*

Proof. We prove this by induction on n.

For $n = 1$ we have the function $\det([a]) = a$.

Now assume the theorem is true for $n-1$ and consider n-by-n matrices.

For an entry a_{st} in the (s,t) position of an n-by-n matrix A, we let its minor M_{st} be the $(n-1)$-by-$(n-1)$ matrix obtained by deleting the row and column containing this entry (i.e., by deleting row s and column t).

We claim that for any fixed value of p, $1 \le p \le n$, the function defined by

$$\det(A) = \sum_{q=1}^{n} (-1)^{p+q} a_{pq} \det(M_{pq})$$

is such a function. To see that this is true, we must verify the properties.

Property (M): Suppose $A = [v_1|\dots|v_i|\dots|v_n] = (a_{st})$ with $v_i = c_1w_1 + c_2w_2$. Let $B_1 = [v_1|\dots|w_1|\dots|v_n]$ and $B_2 = [v_1|\dots|w_2|\dots|v_n]$. Then we must show $\det(A) = c_1\det(B_1) + c_2\det(B_2)$.

Let the pth entry of u_1 be b_1 and let the pth entry of u_2 be b_2. Then $a_{pi} = c_1b_1 + c_2b_2$. If N^1_{pq} is the (p,q) minor of B_1 and N^2_{pq} is the (p,q) minor of B_2, then, since B_1 and B_2 agree with A except in column i,

$$\det(B_1) = \sum_{q \ne i} (-1)^{p+q} \det(N^1_{pq}) + (-1)^{p+i} b_1 \det(M_{pi}),$$
$$\det(B_2) = \sum_{q \ne i} (-1)^{p+q} \det(N^2_{pq}) + (-1)^{p+i} b_2 \det(M_{pi}).$$

Let u_i be the vector obtained from v_i by deleting its pth entry. Let x^1_i be the vector obtained from w_1 by deleting its pth entry, and let x^2_i be the vector obtained from w_2 by deleting its pth entry. Then $u_i = c_1x^1_i + c_2x^2_i$.

For every $q \ne i$, M_{pq} has a column equal to u_i, with the corresponding column of N^1_{pq} equal to x^1_i, and the corresponding column of N^2_{pq} equal to x^2_i, and all other columns of M_{pq}, N^1_{pq}, and N^2_{pq} agree. Thus, by induction,

$$\det(M_{pq}) = c_1\det(N^1_{pq}) + c_2\det(N^2_{pq}).$$

But then

$$\begin{aligned} c_1 \det(B_1) + c_2 \det(B_2) &= \sum_{q \neq i} (-1)^{p+q} a_{pq} (c_1 \det(N^1_{pq}) + c_2 \det(N^2_{pq})) \\ &\quad + (-1)^{p+i} (c_1 b_1 + c_2 b_2) \det(M_{pi}) \\ &= \sum_{q \neq i} (-1)^{p+q} a_{pq} \det(M_{pq}) + (-1)^{p+i} a_{pi} \det(M_{pi}) \\ &= \det(A). \end{aligned}$$

Property (A): Suppose $A = [v_1| \dots |v_n] = (a_{st})$ with $v_i = v_j = w$. Then

$$\det(A) = \sum_{q \neq i,j} (-1)^{p+q} a_{pq} \det(M_{pq}) + (-1)^{p+i} a_{pi} \det(M_{pi}) + (-1)^{p+j} a_{pj} \det(M_{pj}).$$

Now for $q \neq i, j$, M_{pq} has two equal columns, so by induction we have that $\det(M_{pq}) = 0$.

Let x be the vector obtained from w by deleting its pth entry. Then we see (assuming $i < j$)

$$\begin{aligned} M_{pi} &= [v_1|v_2| \dots |v_{i-1}|v_{i+1}| \dots |w| \dots |v_n], \\ M_{pj} &= [v_1|v_2| \dots |w| \dots |v_{j-1}|v_{j+1}| \dots |v_n]. \end{aligned}$$

Thus M_{pi} and M_{pj} have exactly the same columns, but in a different order. To be precise, w is the ith column of M_{pj} but is the $(j-1)$st (not the jth) column of M_{pi}.

So to get from M_{pj} to M_{pi}, we must first interchange w and v_{i+1}, to make w into column $i+1$, and that multiplies the determinant by (-1) (by Lemma 6.1.2). Then we must interchange w and v_{i+2}, to move w into column $i+2$, and that multiplies the determinant by another factor of (-1). We keep going until w is in column $j-1$, at which point we have arrived at M_{pi}. In doing so we have performed $j-1-i$ column interchanges, so we have multiplied the determinant by $(-1)^{j-1-i}$, i.e., we have that

$$\det(M_{pi}) = (-1)^{j-1-i} \det(M_{pj}).$$

Of course, since $v_i = v_j = w$, we also have $a_{pi} = a_{pj}$. Hence

$$\begin{aligned} \det(A) = (-1)^{p+i} (a_{pj} (-1)^{j-1-i} \det(M_{pj})) + (-1)^{p+j} a_{pj} \det(M_{pj}) \\ = a_{pj} \det(M_{pj}) [(-1)^{p+j-1} + (-1)^{p+j}]. \end{aligned}$$

But $(-1)^{p+j-1} + (-1)^{p+j} = (-1)^{p+j-1}(1 + (-1)) = 0$ so $\det(A) = 0$.

(3) If $A = I$, then $a_{pq} = 0$ for $q \neq 0$ and $a_{pp} = 1$. Also, the minor A_{pp} is just the $(n-1)$-by-$(n-1)$ identity matrix. Then by induction we have

$$\det(A) = (-1)^{p+p} \det(A_{pp}) = 1. \qquad \square$$

Corollary 6.2.2. *Let A be an n-by-n matrix. Then* $\det(A) \neq 0$ *if and only if A is invertible.*

Proof. We proved this in Theorem 6.1.3 under the assumption that det exists, and now by Theorem 6.2.1 we know that it does. $\square$

We have just shown we have a determinant function. Now we would like to show it is unique. In fact we will show something more.

Theorem 6.2.3. *For any a, there is a unique volume function* Vol_a *satisfying properties* (1) *and* (2), *or* (A) *and* (M), *and with* $\mathrm{Vol}_a(I) = a$. *This function is* $\mathrm{Vol}_a(A) = \det(A)\,\mathrm{Vol}_a(I)$.

Proof. We note that any function $\mathrm{Vol}_a(A) = a\det(A)$ for fixed a satisfies properties (1) and (2). So there exists a function Vol_a for any a.

Now we want to show it is unique.

Suppose A is not invertible. Then the proof of Theorem 6.1.3 showed that for any volume function, $\mathrm{Vol}(A) = 0$. Thus

$$0 = \mathrm{Vol}_a(A) = 0 \cdot \mathrm{Vol}_a(I) = \det(A)\,\mathrm{Vol}_a(I).$$

Now suppose A is invertible. Then there is a sequence of column operations taking I to A. Let us say that A has distance at most k from I if there is a sequence of k such column operations.

Let f_1 and f_2 be any two functions satisfying (1) and (2), with $f_1(I) = f_2(I) = a$. We prove that $f_1(A) = f_2(A)$ for every matrix A by induction on k.

If $k = 0$, then $A = I$, and $f_1(I) = f_2(I)$, by definition.

Now suppose the theorem is true for $k-1$, and let A have distance at most k from I. Let B be the matrix obtained from I by applying the first $k-1$ column operations. By the inductive hypothesis, $f_1(B) = f_2(B)$. But now A is obtained from B by performing a single column operation. But then $f_1(A) = df_1(B)$ and $f_2(A) = df_2(B)$ for the same value of d, as this value of d is given by either (1), (2), or Lemma 6.1.2. Thus $f_1(A) = f_2(A)$ and by induction we are done. □

Here is a useful special case.

Corollary 6.2.4. *Let $A = (a_{ij})$ be an upper triangular, lower triangular, or diagonal n-by-n matrix. Then $\det(A) = a_{11}a_{22}\cdots a_{nn}$ is the product of its diagonal entries.*

Proof. By induction on n. If $n = 1$, $\det([a]) = a$.

Now suppose the corollary is true for all $(n-1)$-by-$(n-1)$ matrices. Let A be an n-by-n matrix of one of these forms, $A = (a_{ij})$. If A is upper triangular, expand by minors of the last row. If A is lower triangular, expand by minors of the first row. If A is diagonal, do either. In the first case we see that $\det(A) = a_{nn}\det(A_{nn})$ and in the second case we see that $\det(A) = a_{11}\det(A_{11})$. But both A_{nn} and A_{11} are triangular (or diagonal), so their determinants are the product of their diagonal entries. Then by induction we are done. □

Corollary 6.2.5. *Let A and B be n-by-n matrices. Then*

$$\det(AB) = \det(A)\det(B).$$

Proof. Define a function $D(B)$ by $D(B) = \det(AB)$.

It is easy to check that $D(B)$ satisfies properties (1) and (2), so is a volume function. But then by Theorem 6.2.3

$$\det(AB) = D(B) = \det(B)D(I) = \det(B)\det(AI) = \det(B)\det(A). \qquad \square$$

Corollary 6.2.6. *Let A be an invertible n-by-n matrix. Then $\det(A^{-1}) = \det(A)^{-1}$.*

Proof. If A is invertible, $AA^{-1} = I$. Then

$$1 = \det(I) = \det(AA^{-1}) = \det(A)\det(A^{-1}). \qquad \square$$

Corollary 6.2.7. *If the matrices A and B are similar, then $\det(A) = \det(B)$.*

Proof. If $A = P^{-1}BP$, then

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

Theorem 6.2.8. *For any matrix A, $\det({}^tA) = \det(A)$.*

We defer the proof of this theorem to the next section.

Corollary 6.2.9. *The function $\det\colon M_n(\mathbb{F}) \to \mathbb{F}$ is the unique function satisfying properties* (1) *and* (2), *or properties* (A) *and* (M), *with columns replaced by rows, and property* (3).

Proof. $\det({}^tA) = \det(A)$ and the rows of A are the columns of ${}^tA$. $\square$

Corollary 6.2.10. *Let A be an n-by-n matrix. Then:*

(1) *For any p, $\det(A) = \sum_{q=1}^{n}(-1)^{p+q}a_{pq}\det(A_{pq})$.*
(2) *For any q, $\det(A) = \sum_{p=1}^{n}(-1)^{p+q}a_{pq}\det(A_{pq})$.*
(3) *For any $s \neq p$, $0 = \sum_{q=1}^{n}(-1)^{p+q}a_{pq}\det(A_{sq})$.*
(4) *For any $t \neq q$, $0 = \sum_{p=1}^{n}(-1)^{p+q}a_{pq}\det(A_{pt})$.*

Formula (1) is known as expansion by minors of the pth row, and formula (2) is known as expansion by minors of the qth column. Together they are known as *Laplace expansion.*

Proof. We proved (1) in the course of proving Theorem 6.2.1. Then (2) follows from the fact that $\det({}^tA) = \det(A)$, and also that $\det({}^tM_{ij}) = \det(M_{ij})$ and the fact that the rows of A are the columns of ${}^tA$.

(3) is true as the right-hand side is the expansion by minors of the matrix B that agrees with A except that row s of B is equal to row p of A. Since B has two equal rows (rows p and s) it is not invertible and so $\det(B) = 0$.

(4) is true similarly: the right-hand side is the expansion by minors of the determinant of a matrix B with two equal columns, and such a matrix is not invertible so $\det(B) = 0$. $\square$

6.3. A formula for the determinant

In the last section we defined the determinant recursively. That is, we defined the determinant of an n-by-n matrix in terms of the determinants of $(n-1)$-by-$(n-1)$ matrices, using Laplace expansion. Then the determinant of an $(n-1)$-by-$(n-1)$ matrix was defined in terms of the determinants of $(n-2)$-by-$(n-2)$ matrices, using Laplace expansion, etc.

In this section we will derive a direct formula for the determinant of an n-by-n matrix in terms of its entries. We will adopt an approach that builds on our work in the last section. (While it is possible to derive this formula from scratch, that would essentially involve redoing a good bit of work we have already done.)

Definition 6.3.1. A *permutation* of $\{1,\ldots,n\}$ is a reordering of this set. More precisely, a permutation of $S=\{1,\ldots,n\}$ is given by a 1-1 function $\sigma\colon S\to S$, where $(1,2,3,\ldots,n)$ is taken to $(\sigma(1),\sigma(2),\sigma(3),\ldots,\sigma(n))$. $\Diamond$

Lemma 6.3.2. *There are exactly* $n!$ *permutations* $\sigma\colon\{1,\ldots,n\}\to\{1,\ldots,n\}$.

Proof. To specify σ, we specify the values of $\sigma(1),\ldots,\sigma(n)$. There are n choices for $\sigma(1)$; once $\sigma(1)$ has been chosen there are $n-1$ choices for $\sigma(2)$; once $\sigma(1)$ and $\sigma(2)$ have been chosen there are $n-2$ choices for $\sigma(3)$; etc. In the end there are $n(n-1)(n-2)\cdots 1=n!$ choices for σ. $\square$

Definition 6.3.3. An n-by-n *permutation matrix* P is a matrix with a single nonzero entry of 1 in each row and column. More precisely, the permutation matrix P_σ attached to the permutation σ is the matrix with an entry of 1 in each of the positions $(\sigma(1),1),(\sigma(2),2),\ldots,(\sigma(n),n)$ and all other entries 0. $\Diamond$

Remark 6.3.4. Observe that the matrix P_σ is given by

$$P_\sigma=[e_{\sigma(1)}|e_{\sigma(2)}|\ldots|e_{\sigma(n)}]. \qquad \Diamond$$

Lemma 6.3.5. *Let* P_σ *be a permutation matrix. Then* $\det(P_\sigma)=\pm 1$.

Proof. By induction on n.

For $n=1$, the only permutation matrix is $[1]$, and $\det([1])=1$. Now suppose the lemma is true for all $(n-1)$-by-$(n-1)$ permutation matrices, and consider an n-by-n permutation matrix P_σ.

Case I: $\sigma(n)=n$. In this case there is an entry of 1 in the (n,n) position. In this case, do nothing. Set $\sigma'=\sigma$, so $P_{\sigma'}=P_\sigma$ and $\det(P_{\sigma'})=\det(P_\sigma)$.

Case II: $\sigma(n)\neq n$. In this case $\sigma(q)=n$ for some $q\neq n$. Then there is an entry of 1 in the (q,n) position. Interchange columns q and n, to obtain a matrix with an entry of 1 in the (n,n) position. Then the matrix so obtained is another permutation matrix, i.e., is P_σ for some σ' with $\sigma'(n)=n$. In this case, $\det(P_{\sigma'})=-\det(P_\sigma)$ by Lemma 6.1.2.

Thus, regardless of which case we are in, $\det(P_\sigma)=\pm\det(P_{\sigma'})$.

Now expand $\det(P_{\sigma'})$ by minors of the last row. Every entry in the last row is 0 except for the entry in position (n,n), which is 1. Thus $\det(P_{\sigma'})=\det(Q)$, where Q is the (n,n) minor of $P_{\sigma'}$. But Q is an $(n-1)$-by-$(n-1)$ permutation matrix, so $\det(Q)=\pm 1$. But then $\det(P_\sigma)=\pm 1$ as well.

Then by induction we are done. $\square$

Now we have the following formula for the determinant of an n-by-n matrix.

Theorem 6.3.6. *Let $A = (a_{ij})$ be an n-by-n matrix. Then*

$$\det(A) = \sum_{\text{permutations } \sigma} \det(P_\sigma) a_{\sigma(1),1} a_{\sigma(2),2} \cdots a_{\sigma(n),n}.$$

Proof. Regard each of the entries a_{ij} of A as a variable. As we have observed, there are $n!$ permutations, so this sum has $n!$ terms.

Claim. *In any expansion by minors, there are $n!$ terms.*

Proof of claim. By induction. Certainly true for $n = 1$. Assume true for $n - 1$. Then expansion by minors yields n determinants of $(n-1)$-by-$(n-1)$ matrices, each of which has $(n-1)!$ terms, for a total of $n(n-1)! = n!$ terms. □

Claim. *Every term in any expansion by minors is $\varepsilon_\sigma a_{\sigma(1),1} a_{\sigma(2),2} \cdots a_{\sigma(n),n}$ for some permutation σ and some $\varepsilon_\sigma = \pm 1$, and every such term appears in the expansion.*

Proof of claim. By induction. Certainly true for $n = 1$. Assume true for $n - 1$ and consider an expansion

$$\det(A) = \sum_{q=1}^{n} (-1)^{p+q} a_{pq} \det(A_{pq}).$$

Now for different values q_1 and q_2 of q, the terms with $q = q_1$ in the sum all have the factor a_{pq_1} for some p, while the terms with $q = q_2$ in the sum all have the factor a_{pq_2} for some p; in particular none of the terms for $q \neq q_1$ duplicates any term for $q = q_1$. Thus the n terms for $q = 1, \ldots, n$ in the sum are all distinct. Now for any fixed value of p and q consider $\det(A_{pq})$. By induction, this is a sum of $(n-1)!$ terms of the matrix $A_{p,q}$. The entries of this matrix are all entries of A, none of which are in row p or column q of A. Furthermore, by induction, each term in $\det(A_{pq})$ is of the form $\pm a_{i_1 j_1} a_{i_2 j_2} \cdots a_{i_{n-1} j_{n-1}}$, where $i_1, i_2, \ldots, i_{n-1}$ are all distinct, none of which equal p, and $j_1, \ldots, j_{n-1}$ are all distinct, none of which equal q. Thus each term yields a term $\pm a_{i_1 j_1} a_{i_2 j_2} \cdots a_{i_{n-1} j_{n-1}} a_{pq}$ in the sum for $\det(A)$. But this term is just $\varepsilon_\sigma a_{\sigma(1),1} \cdots a_{\sigma(n),n}$ (after rearranging the order of the factors) with $\varepsilon_\sigma = \pm 1$ for some permutation σ. Furthermore, since there are $n!$ such terms and they are all distinct, and the sum for $\det(A)$ has $n!$ terms, each of them appears. □

We thus have proved the theorem except for identifying the value of ε_σ, so it only remains to show $\varepsilon_\sigma = \det(P_\sigma)$.

To do this, we consider the determinant of the matrix P_σ. Then if $P_\sigma = (p_{ij})$

$$\begin{aligned}\det(P_\sigma) &= \sum_{\text{permutations } \rho} e_\rho p_{\rho(1),1} p_{\rho(2),2} \cdots p_{\rho(n),n} \\ &= \varepsilon_\sigma p_{\sigma(1),1} p_{\sigma(2),2} \cdots p_{\sigma(n),n} \\ &\quad + \sum_{\rho \neq \sigma} \varepsilon_\rho p_{\rho(1),1} p_{\rho(2),2} \cdots p_{\rho(n),n}.\end{aligned}$$

But now P_σ is defined by $p_{\sigma(1),1} = 1$, $p_{\sigma(2),2} = 1$, $\ldots$, $p_{\sigma(n),n} = 1$. On the other hand, if $\rho \neq \sigma$, then $\rho(k) \neq \sigma(k)$ for some k, and so $p_{\rho(k),k} = 0$. Thus the above sum becomes

$$\det(P_\sigma) = \varepsilon_\sigma(1) + \sum_{\rho \neq \sigma} \varepsilon_\rho(0) = \varepsilon(\sigma),$$

completing the proof. □

Logically speaking, we are done. But aesthetically speaking, we are not. Our formula for $\det(A)$ involves the determinants $\det(P_\sigma)$ of the permutation matrices P_σ, these determinants being ± 1.

In would be desirable to obtain a formula for this sign that did not involve determinants, but which was obtained more directly from the permutation σ. We do that now.

We are regarding permutations as functions $\sigma\colon S \to S$, where $S = \{1, \ldots, n\}$. Then we define multiplication of permutations to be composition of functions: $\sigma_2\sigma_1$ is the permutation defined by $(\sigma_2\sigma_1)(k) = \sigma_2(\sigma_1(k))$ for $k \in S$.

We note that we have the identity permutation ι that is the identity function: $\iota(k) = k$ for every k in S.

We also note that each permutation σ is invertible as a function, so $\sigma^{-1}\colon S \to S$ and σ^{-1} is also a permutation. With our definition of multiplication as composition of functions, $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \iota$. Also, since multiplication of permutations is composition of functions, it is associative: $\sigma_3(\sigma_2\sigma_1) = (\sigma_3\sigma_2)\sigma_1$. (These properties together show that, for any fixed n, the set of permutations form a *group*, this group being known as the *symmetric group* on n objects.)

We define a *transposition* to be a permutation τ that interchanges two elements of S but leaves the others fixed: for $i \neq j$, $\tau = \tau(i, j)$ is defined by $\tau(i) = j$, $\tau(j) = i$, $\tau(k) = k$ for $k \neq i, j$. We observe that $\tau^2 = \iota$.

Lemma 6.3.7. *Any permutation can be written as a* (*possibly empty*) *product of transpositions.*

Proof. By induction by n.

If $n = 1$, the only permutation is the identity ι.

If $n = 2$, there are exactly two permutations σ. Either $\sigma(1) = 1$ and $\sigma(2) = 2$, in which case $\sigma = \iota$, or $\sigma(1) = 2$ and $\sigma(2) = 1$ in which case σ is the transposition $\sigma = \tau(1, 2)$.

Now for the inductive step. Assume the lemma is true for $n - 1$.

If $\rho\colon \{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ is a permutation, define the permutation $\tilde{\rho}\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ by $\tilde{\rho}(k) = \rho(k)$ if $1 \leq k \leq n-1$, and $\tilde{\rho}(n) = n$. Note that if ρ is a transposition, so is $\tilde{\rho}$.

Consider a permutation $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$.

Case I: $\sigma(n) = n$. In this case let $\rho\colon \{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ be the permutation defined by $\rho(k) = \sigma(k)$ for $1 \leq k \leq n-1$. By the inductive hypothesis ρ is a product of transpositions, $\rho = \tau_j \cdots \tau_2\tau_1$. But then $\sigma = \tilde{\rho} = \tilde{\tau}_j \cdots \tilde{\tau}_2\tilde{\tau}_1$ is a product of transpositions.

Case II: $\sigma(n) = k \neq n$. Then

$$\sigma = \iota\sigma = \tau(k,n)^2\sigma = \tau(k,n)(\tau(k,n)\sigma) = \tau(k,n)\sigma',$$

where σ' is the product $\tau(k,n)\sigma$. But then $\sigma'(n) = (\tau(k,n)\sigma)(n) = \tau(k,n)(\sigma(n)) = \tau(k,n)k = n$. Thus by case I, σ' is a product of transpositions $\sigma' = \tilde{\tau}_j \cdots \tilde{\tau}_1$, and then $\sigma = \tau(k,n)\tilde{\tau}_j \cdots \tilde{\tau}_i$ is a product of transpositions. $\square$

Now it is certainly *not* true that any permutation can be written as a product of transpositions in a unique way. For example, the identity permutation ι is the empty product, or the product of zero transpositions. But since $\tau^2 = \iota$ for any transposition τ, we also have $\iota = \tau^2$ written as a product of two transpositions.

As a more interesting example, take the permutation σ of $\{1,2,3\}$ given by $\sigma(1) = 3,\ \sigma(2) = 2,\ \sigma(3) = 1$. On the one hand, $\sigma = \tau(1,3)$, a single transposition, but on the other hand, $\sigma = \tau(2,3)\tau(1,3)\tau(1,2)$, a product of three transpositions. (Remember that we compose permutations right-to-left.)

While the number of transpositions involved in writing a permutation σ as a product of transpositions is not well-defined, the parity of this number is. As we shall now see, this follows from the fact that the determinant is well-defined. Later we will give an independent argument, which also gives a handy method for finding it.

First, a general lemma.

Lemma 6.3.8. *Let σ_1 and σ_2 be two permutations. Then*

$$P_{\sigma_2\sigma_1} = P_{\sigma_2}P_{\sigma_1}.$$

Proof. Direct calculation. $\square$

Lemma 6.3.9. *If a permutation σ is written as the product of t transpositions, then* $\det(P_\sigma) = (-1)^t$.

Proof. Write $\sigma = \tau_t\tau_{t-1}\cdots\tau_2\tau_1$. Then $P_\sigma = P_{\tau_t}\cdots P_{\tau_1}$, and so

$$\det(P_\sigma) = \det(P_{\tau_t})\cdots\det(P_{\tau_1}).$$

Now for any transposition τ, P_τ is obtained from the identity matrix by interchanging two columns (and leaving the other columns alone) so by Lemma 6.1.2, $\det(P_\tau) = -1$. Hence, substituting, we see that $\det(P_\sigma) = (-1)^t$. $\square$

This justifies the following definition.

Definition 6.3.10. Let σ be a permutation. Then

$$\operatorname{sign}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is the product of an even number of transpositions,} \\ -1 & \text{if } \sigma \text{ is the product of an odd number of transpositions.} \end{cases} \quad \diamond$$

Putting these together, we have the following formula for the determinant.

Theorem 6.3.11. *Let $A = (a_{ij})$ be an n-by-n matrix. Then*

$$\det(A) = \sum_{\text{permutations } \sigma} \operatorname{sign}(\sigma) a_{\sigma(1),1}a_{\sigma(2),2}\cdots a_{\sigma(n),n}.$$

Proof. Immediate from Theorem 6.3.6, Lemma 6.3.9, and Definition 6.3.10. $\square$

Now for our other method of finding the sign of a permutation σ:

Definition 6.3.12. Let $\sigma\colon \{1,\ldots,n\} \to \{1,\ldots,n\}$ be a permutation. Write down the sequence

$$\sigma(1)\ \sigma(2)\ \cdots\ \sigma(n).$$

The number of *inversions* in σ is the number of instances where a larger number precedes a smaller number in this sequence. $\Diamond$

Lemma 6.3.13. *Let σ be a permutation. If the number of inversions in σ is even (resp., odd), then any way of writing σ as a product of transpositions involves an even (resp., odd) number of transpositions, in which case* $\operatorname{sign}(\sigma) = +1$ *(resp.,* $\operatorname{sign}(\sigma) = -1$*). In particular,* $\operatorname{sign}(\sigma)$ *is well-defined.*

For example, consider the permutation given by $\sigma(1) = 5$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 1$, $\sigma(5) = 2$. We write down the sequence

$$5\ 3\ 4\ 1\ 2.$$

We count: 5 precedes 3, 4, 1, and 2, giving four inversions. 3 precedes 1 and 2, giving two inversions. 4 precedes 1 and 2, giving two inversions. Thus we have a total of eight inversions. We also observe $\sigma = \tau(4,5)\tau(3,5)\tau(2,5)\tau(1,4)$, a product of four transpositions. (Of course, other factorizations are possible.)

Proof. The identity permutation ι is even (the product of 0 transpositions) and has 0 inversions.

We will show that if σ is any permutation and τ is any transposition, then the number of inversions in $\tau\sigma$ differs from the number of inversions in σ by an odd number.

Let $\tau = \tau(i,k)$ with $i < k$. Suppose that $\sigma(i) = p$ and $\sigma(k) = r$. Thus in the reordering of $\{1,\ldots,n\}$ given by σ, i is in position p and k is in position r. In the reordering given by $\tau\sigma$, the positions of i and k are interchanged, and all other entries stay the same. Suppose first that $p < r$.

Let us now compare inversions in σ and $\tau\sigma$. The number of inversions of any entry in position $< p$ or $> r$ does not change. For any entry between positions $p-1$ and $r-1$, if that entry is either $< i$ or $> k$, the number of inversions of that entry also does not change.

Thus suppose we have m entries between positions $p-1$ and $r-1$ that are greater than i but less than k. Consider any such entry j. In σ, i comes before j and j comes before k, so neither of these is an inversion. But in $\tau\sigma$, k comes before j and j comes before i, so both of these are inversions. Hence the number of inversions increases by $2m$. But also i comes before j in σ, which is not an inversion, but j comes before i in $\tau\sigma$, which is an inversion. Hence the number of inversions in $\tau\sigma$ is $2m+1$ more than the number of inversions in σ, an odd number.

If, on the other hand, $r < p$, the same argument shows that the number of inversions in $\tau\sigma$ is $2m+1$ less than the number of inversions in σ, also a change by an odd number. $\square$

We now present a proof of Theorem 6.2.8.

Proof of Theorem 6.2.8. Let ${}^tA = (b_{ij})$. Then by Theorem 6.3.6,

$$\det({}^tA) = \sum_{\text{permutations } \sigma} \det(P_\sigma) b_{\sigma(1),1}, b_{\sigma(2),2} \cdots b_{\sigma(n),n}.$$

Now by the definition of ${}^tA$, $b_{ij} = a_{ji}$ for every i, j. Thus

$$\det({}^tA) = \sum_{\text{permutations } \sigma} \det(P_\sigma) a_{1,\sigma(1)}, a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

Now there is some k_1 with $\sigma(k_1) = 1$; then $\sigma^{-1}(1) = k_1$. Then there is some k_2 with $\sigma(k_2) = 2$; then $\sigma^{-1}(k_2) = 2$; etc. Thus we may rewrite this sum as

$$\det({}^tA) = \sum_{\text{permutations } \sigma} \det(P_\sigma) a_{\sigma^{-1}(1),1}, a_{\sigma^{-1}(2),2} \cdots a_{\sigma^{-1}(n),n}.$$

Let $\rho = \sigma^{-1}$. Then $\sigma = \rho^{-1}$. Note that as σ ranges over all permutations, so does $\rho = \sigma^{-1}$. Then this sum is

$$\det({}^tA) = \sum_{\text{permutations } \rho} \det(P_{\rho^{-1}}) a_{\rho(1),1}, a_{\rho(2),2} \cdots a_{\rho(n),n}.$$

Now

$$1 = \det(I) = \det(P_\iota) = \det(P_{\rho\rho^{-1}}) = \det(P_\rho)\det(P_{\rho^{-1}})$$

so either $\det(P_\rho) = \det(P_{\rho^{-1}}) = 1$ or $\det(P_\rho) = \det(P_{\rho^{-1}}) = -1$. Whichever is the case, $\det(P_\rho) = \det(P_{\rho^{-1}})$ and so this sum is

$$\det({}^tA) = \sum_{\text{permutations } \rho} \det(P_\rho) a_{\rho(1),1}, a_{\rho(2),2} \cdots a_{\rho(n),n} = \det(A). \qquad \square$$

6.4. Practical evaluation of determinants

Suppose we have an n-by-n matrix A and we want to find $\det(A)$. Proceeding in a completely straightforward manner, we could do this in one of the following ways:

(1) Use Laplace expansion to write $\det(A)$ as a sum of multiples of n determinants of $(n-1)$-by-$(n-1)$ matrices, then use Laplace expansion to write each of these determinants as a sum of multiples of $n-1$ determinants of $(n-2)$-by-$(n-2)$ matrices, and continue, eventually arriving at an expression for $\det(A)$ involving $n!$ terms.

(2) Use the formula we have developed in the last section to calculate $\det(A)$, this formula having $n!$ terms.

Suppose $n = 10$. Then $n! = 3{,}628{,}800$. Obviously this would be impossible to do by hand, so your reaction would be to simply put it on a computer.

Suppose $n = 60$. A standard estimate for 60! shows that if every atom in the sun were a computer capable of calculating a term in a nanosecond (a billionth of a second, or about the amount of time it takes a beam of light to travel one foot), it would take over 100,000,000 years to calculate a determinant.

Nevertheless, a computer can actually calculate the determinant of a 60-by-60 matrix in (far less time than) the blink of an eye. That is because we program it with an intelligent way to do so. Here is an oversimplified version of the algorithm: Add multiples of rows to other rows to transform a matrix A into a matrix B with a leading entry in each row and column (if possible; if not $\det(A) = 0$) and then $\det(A) = \det(B)$ is the product of the leading entries times an appropriate sign.

In this section we will see an optimized (for human beings) variant of this procedure. We will be using both row and column operations. And, while I have stressed the value of being systematic, in evaluating determinants we want to be opportunistic, taking advantage of good luck when we find it. In fact, the key to the procedure is to make our luck even better.

The basic procedure is as follows. Use row or column operations to transform a column or row into one with at most one nonzero entry, and then expand by minors of that row or column to obtain a smaller determinant, and evaluate the same way, etc. Throughout this procedure take advantage of entries that are already 0.

We present some illustrative examples.

Example 6.4.1.

$$\begin{vmatrix} 2 & 3 & 2 & 9 \\ 8 & 2 & 6 & 1 \\ 4 & 1 & -1 & 3 \\ -6 & 4 & 4 & 22 \end{vmatrix} = \begin{vmatrix} 2 & 3 & 2 & 9 \\ 0 & -10 & -2 & -35 \\ 4 & 1 & -1 & 3 \\ -6 & 4 & 4 & 22 \end{vmatrix} = \begin{vmatrix} 2 & 3 & 2 & 9 \\ 0 & -10 & -2 & -35 \\ 0 & -5 & -5 & -15 \\ -6 & 4 & 4 & 22 \end{vmatrix}$$

$$= \begin{vmatrix} 2 & 3 & 2 & 9 \\ 0 & -10 & -2 & -35 \\ 0 & -5 & -5 & -15 \\ 0 & 13 & 10 & 49 \end{vmatrix}$$

(expanding by minors of the first column)

$$= 2\begin{vmatrix} -10 & -2 & -35 \\ -5 & -5 & -15 \\ 13 & 10 & 49 \end{vmatrix}$$

(pulling out a factor to simplify the arithmetic)

$$= 2(-5)\begin{vmatrix} -10 & -2 & -35 \\ 1 & 1 & 3 \\ 13 & 10 & 49 \end{vmatrix} = 2(-5)\begin{vmatrix} 0 & 8 & -5 \\ 1 & 1 & 3 \\ 13 & 10 & 49 \end{vmatrix} = 2(-5)\begin{vmatrix} 0 & 8 & -5 \\ 1 & 1 & 3 \\ 0 & -3 & 10 \end{vmatrix}$$

(expanding by minors of the first column)

$$= 2(-5)(-1)\begin{vmatrix} 8 & 5 \\ -3 & 10 \end{vmatrix} = 2(-5)(-1)\begin{vmatrix} 8 & 5 \\ 13 & 0 \end{vmatrix}$$

(expanding by minors of the second column)

$$= 2(-5)(-1)|13| = 2(-5)(-1)(13) = 650.$$ ◊

Example 6.4.2. $\begin{vmatrix} 5 & 16 & 8 & 7 \\ 0 & 6 & 3 & 0 \\ 2 & -3 & 4 & 9 \\ 2 & 3 & 1 & 6 \end{vmatrix}$ (taking advantage of the fact that the second row only has two nonzero entries) $= \begin{vmatrix} 5 & 0 & 8 & 7 \\ 0 & 0 & 3 & 0 \\ 2 & -11 & 4 & 9 \\ 2 & 1 & 1 & 6 \end{vmatrix}$ (expanding by minors of the second row) $= (-3)\begin{vmatrix} 5 & 0 & 7 \\ 2 & -11 & 9 \\ 2 & 1 & 6 \end{vmatrix}$ (taking advantage of the fact that the second column only has two nonzero entries) $= (-3)\begin{vmatrix} 5 & 0 & 7 \\ 24 & 0 & 75 \\ 2 & 1 & 6 \end{vmatrix}$ (expanding by minors of the second column) $= (-3)(-1)\begin{vmatrix} 5 & 7 \\ 24 & 75 \end{vmatrix} = (-3)(-1)(5(75) - 7(24)) = 621.$ $\Diamond$

6.5. The classical adjoint and Cramer's rule

For $n = 1$ the results of this section are trivial. For $n = 2$, we already know them (see Example 4.4.10 and Remark 4.4.11). For $n \geq 3$ the methods of this section should *never* (repeat, *never*) be used. We present them partly for historical reasons, and partly because they have some theoretical consequences, one of which we will draw.

Definition 6.5.1. Let $A = (a_{ij})$ be a square matrix. Its *classical adjoint* $B = (b_{ij})$ is the matrix defined by

$$b_{ij} = \det(A_{ji}). \qquad \Diamond$$

(Here A_{ji} is the minor. Note the order of the subscripts.)

Theorem 6.5.2. *Suppose A is invertible. Then if B is the classical adjoint of A,*

$$A^{-1} = (1/\det(A))B.$$

Proof. From Corollary 6.2.10 we see that

$$AB = BA = \det(A)I. \qquad \square$$

Theorem 6.5.3 (Cramer's rule)**.** *Suppose A is invertible. Then the unique solution to the matrix equation $Ax = b$ is the vector $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ given by*

$$x_i = \det(A_i(b))/\det(A),$$

where $A_i(b)$ is the matrix obtained from A by replacing its ith column by b.

Proof. Let $\mathcal{T}\colon \mathbb{F}^n \to \mathbb{F}^n$ be given by

$$\mathcal{T}(b) = \text{the unique solution to } Ax = b.$$

Let $\mathcal{S}\colon \mathbb{F}^n \to \mathbb{F}^n$ be given by

$$\mathcal{S}(b) = \text{the vector given by Cramer's rule}.$$

Then $\mathcal{T}$ and $\mathcal{S}$ are both linear transformations. We claim $\mathcal{S} = \mathcal{T}$. In order to show this, we know it suffices to show that $\mathcal{S}$ and $\mathcal{T}$ agree on any basis $\mathcal{B}$ of $\mathbb{F}^n$.

Write $A = [u_1 | \dots | u_n]$. Since A is invertible, its columns form a basis for $\mathbb{F}^n$, so we choose $\mathcal{B} = \{u_1, \dots, u_n\}$.

On one hand, we know $Ae_i = u_i$, so $\mathcal{T}(u_i) = e_i$.

On the other hand, if $b = u_i$, then $A_i(b) = A$, so Cramer's rule gives $x_i = 1$, and $A_j(b)$ is a matrix with two identical columns (columns i and j) for $j \neq i$, so Cramer's rule gives $x_j = 0$ for $j \neq i$. Thus $\mathcal{S}(u_i) = e_i$. □

Remark 6.5.4. The classical adjoint should never be used for $n \geq 3$ as in order to compute it we must compute a single n-by-n determinant ($\det(A)$) and n^2 $(n-1)$-by-$(n-1)$ determinants ($\det(A_{ji})$) for each (j, i)), and this is hopelessly inefficient. Similarly, Cramer's rule should never be used as in order to use it we must compute $n+1$ n-by-n determinants ($\det(A)$ and $\det(A_i(b))$ for each i), and this is hopelessly inefficient. ♢

Here is the one useful corollary we will draw.

Corollary 6.5.5. *Let A be an invertible matrix with integer entries. The following are equivalent:*

(1) $\det(A) = \pm 1$.

(2) A^{-1} *has integer entries.*

(3) *For every vector b with integer entries, the unique solution of $Ax = b$ has integer entries.*

Proof. We leave this as an exercise for the reader. □

6.6. Jacobians

In this section we recall where determinants appear in (single and) multivariable calculus.

Here is the change of variable theorem for integrals in multivariable calculus.

Theorem 6.6.1. *Let B be a closed, bounded region in $\mathbb{R}^n$ (parameterized by $y_1, \ldots, y_n$), and let $g\colon B \to \mathbb{R}$ be a continuous function. Let A be a closed, bounded region in $\mathbb{R}^n$ (parameterized by $x_1, \ldots, x_n$), and let $F\colon A \to B$ be a differentiable function with a differentiable inverse. Then*

$$\int \cdots \int_B g(y_1, \ldots, y_n)\, dy_1 \cdots dy_n$$
$$= \int \cdots \int_A g(F(x_1, \ldots, x_n))\, |\det(F'(x_1, \ldots, x_n))|\, dx_1 \cdots dx_n.$$

Notice the appearance of the determinant. This determinant is known as the *Jacobian* of the function F. The reason it appears in this theorem is exactly because $\det(F')$ is the factor by which F' multiplies volume. Here we have the absolute value because in the situation of this theorem we are thinking about unsigned volume. In particular, if we take $g(y_1, \ldots, y_n) = 1$, we obtain

$$\mathrm{Vol}(B) = \int \cdots \int_B dy_1 \cdots dy_n = \int \cdots \int_A |\det(F'(x_1, \ldots, x_n))|\, dx_1 \cdots dx_n,$$

where by $\mathrm{Vol}(B)$ we mean unsigned volume.

In fact we already saw this in single variable calculus, but we didn't notice it. Here is the change of variable formula in single variable calculus.

Theorem 6.6.2. *Let J be the closed interval $J = [c, d]$ in $\mathbb{R}$ (parameterized by y), and let $g\colon J \to \mathbb{R}$ be a continuous function. Let I be the closed interval $I = [a, b]$ in $\mathbb{R}$ (parameterized by x), and let $f\colon I \to J$ be a differentiable function with a differentiable inverse. Then*

$$\int_c^d g(y)\,dy = \int_{f^{-1}(c)}^{f^{-1}(d)} g(f(x))f'(x)\,dx.$$

The factor $f'(x)$ appears for the same reason: $f'(x)$ is really here as $f'(x) = \det([f'(x)])$.

Now you may (in fact, you should) be bothered by the fact that we have an absolute value sign in the multivariable case but not in the single variable case.

Here is the reason. There are two possibilities: either $f'(x) > 0$, in which case $f(x)$ is increasing, so $f(a) = c$ and $f(b) = d$, or $f'(x) < 0$, in which case $f(x)$ is decreasing, so $f(a) = d$ and $f(b) = c$. Then in the first case we have

$$\int_c^d g(y)\,dy = \int_a^b g(f(x))f'(x)\,dx$$

while in the second case we have

$$\begin{aligned}\int_c^d g(y)\,dy &= \int_b^a g(f(x))f'(x)\,dx = -\int_a^b g(f(x))f'(x)\,dx\\ &= \int_a^b g(f(x))(-f'(x))\,dx,\end{aligned}$$

so in either case we may rewrite the formula as

$$\int_I g(y)\,dy = \int_J g(f(x))|f'(x)|\,dx.$$

(Actually, with more care, we can attach signs to our integrals in a natural way so that the formula in the multivariable case becomes the analog of the formula in the single variable case but with $\det(F'(x_1, \ldots, x_n))$ instead of $|\det(F'(x_1, \ldots, x_n))|$. But to do so would be to carry us far afield.)

While we will not prove these theorems here—we are doing linear algebra here, not calculus—let us see an interesting geometric application.

Example 6.6.3. (1) Let B be an elliptical disk in the (y_1, y_2)-plane, i.e., the region in the (y_1, y_2)-plane bounded by the ellipse $\left(\frac{y_1}{a_1}\right)^2 + \left(\frac{y_2}{a_2}\right)^2 = 1$ (with $a_1, a_2 > 0$), and let A be the unit disk in the (x_1, x_2)-plane, i.e., the region in the (x_1, x_2)-plane bounded by the unit circle $x_1^2 + x_2^2 = 1$. Let $F\colon A \to B$ be the linear function

$$(y_1, y_2) = F(x_1, x_2) = (a_1x_1, a_2x_2).$$

Then

$$\operatorname{Area}(B) = \iint_B dy_1\,dy_2 = \iint_A |\det(F'(x_1, x_2))|\,dx_1dx_2.$$

But

$$F'(x_1, x_2) = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix}$$

so $\det(F'(x_1, x_2)) = a_1a_2$. Thus

$$\text{Area}(B) = \iint_A a_1a_2\, dx_1dx_2 = a_1a_1 \iint_A dx_1dx_2 = \pi a_1a_2,$$

and we have found a formula for the area of an elliptical disk in the plane.

(2) Let B be an ellipsoidal ball in (y_1, y_2, y_3)-space, i.e., the region in (y_1, y_2, y_3)-space bounded by the ellipsoid $\left(\frac{y_1}{a_1}\right)^2 + \left(\frac{y_2}{a_2}\right)^2 + \left(\frac{y_3}{a_3}\right)^2 = 1$ (with $a_1, a_2, a_3 > 0$), and let A be the unit ball in (x_1, x_2, x_3)-space, i.e., the region in (x_1, x_2, x_3)-space bounded by the unit sphere $x_1^2 + x_2^2 + x_3^2 = 1$. Let $F\colon A \to B$ be the linear function

$$(y_1, y_2, y_3) = f(x_1, x_2, x_3) = (a_1x_1, a_2x_2, a_3x_3).$$

Then, similarly, $\det(F'(x_1, x_2, x_3)) = a_1a_2a_3$, so the volume of the ellipsoidal ball B is given by

$$\begin{aligned}\text{Vol}(B) = \iiint_B dy_1dy_2dy_3 &= \iiint_A (a_1a_2a_3)\, dx_1dx_2dx_3 \\ &= a_1a_2a_3 \iiint_A dx_1dx_2dx_3 = a_1a_2a_3 \operatorname{Vol}(A) = \frac{4}{3}\pi(a_1a_2a_3).\end{aligned}$$

Clearly the analogs hold in higher dimension as well. $\Diamond$

6.7. Exercises

1. Find the determinants of the following matrices:

(a) $\begin{bmatrix} 1 & 3 \\ 4 & 14 \end{bmatrix}$.

(b) $\begin{bmatrix} 1 & 2 & 3 \\ 1 & 4 & 5 \\ 3 & 8 & 5 \end{bmatrix}$.

(c) $\begin{bmatrix} 0 & 1 & 2 \\ 1 & 1 & 1 \\ 2 & 3 & 4 \end{bmatrix}$.

(d) $\begin{bmatrix} 2 & 4 & 6 \\ 3 & 5 & 9 \\ 5 & 7 & 13 \end{bmatrix}$.

(e) $\begin{bmatrix} 5 & 0 & 0 & 1 \\ 2 & 3 & 1 & -2 \\ 2 & -7 & 0 & 1 \\ 11 & -2 & -1 & 4 \end{bmatrix}$.

(f) $\begin{bmatrix} 1 & 4 & 2 & 3 \\ 3 & 12 & 6 & 5 \\ 2 & 9 & 5 & 11 \\ 6 & 24 & 14 & 25 \end{bmatrix}$.

(g) $\begin{bmatrix} 7 & 2 & 4 & 0 & 2 \\ 5 & 1 & 2 & 0 & 4 \\ 6 & 0 & 1 & 2 & 2 \\ 7 & 0 & 0 & 4 & 3 \\ 3 & 1 & 5 & 0 & 7 \end{bmatrix}$.

2. Let $A_n = (a_{ij})$ be the n-by-n matrix with $a_{ii} = 2$, $i = 1, \ldots, n$, $a_{ij} = 1$ if $j = i+1$ or $j = i-1$, and $a_{ij} = 0$ otherwise. Thus

$$A_1 = [2], \quad A_2 = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}, \quad A_4 = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{bmatrix}, \quad \text{etc.}$$

(a) Find $\det(A_n)$ for $n = 1, 2, 3, 4$.

(b) Find $\det(A_n)$ in general.

Let B_{2n} be the $2n$-by-$2n$ matrix with $b_{ii} = 2$, $i = 1, \ldots, n$, $b_{ii} = 0$, $i = n+1$, $b_{ii} = -2$, $i = n+2, \ldots, 2n$, $b_{ij} = 1$ if $j = i+1$ or $j = i-1$, and $b_{ij} = 0$ otherwise. Thus

$$B_2 = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}, \quad B_4 = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -2 \end{bmatrix}, \quad B_6 = \begin{bmatrix} 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{bmatrix}, \quad \text{etc.}$$

(c) Find $\det(B_{2n})$ for $n = 1, 2, 3, 4$.

(d) Find $\det(B_{2n})$ in general.

3. Let E_8 be the 8-by-8 matrix

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

Find $\det(E_8)$.

4. The matrix C below is called a circulant matrix:

$$\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-2} \\ \vdots & & & & \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}.$$

Show that $\det(C) = \prod_{k=0}^{n-1} \sum_{j=0}^{n-1} c_j e^{2\pi kji/n}$. (Here $i = \sqrt{-1}$.) Hint: Regard the c_i as variables and the determinant as a polynomial in these variables.

5. The matrix V below is called a van der Monde matrix:

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \dots & x_3^{n-1} \\ \vdots & & & & \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{bmatrix}.$$

Show that $\det(V) = \prod_{1 \le j < i \le n}(x_i - x_j)$. Hint: Regard the x_i as variables and the determinant as a polynomial in these variables.

6. For each element f of $\mathbb{F}$, let v_f be the vector in $\mathbb{F}^{\infty\infty}$ given by

$$v_f = \begin{bmatrix} 1 \\ f \\ f^2 \\ f^3 \\ \vdots \end{bmatrix}.$$

Show that $S = \{v_f \,|\, f \in \mathbb{F}\}$ is a linearly independent subset of $\mathbb{F}^{\infty\infty}$.

7. Let $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ be a block matrix.

(a) If A is invertible, show that

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

where E is the matrix $E = D - CA^{-1}B$.

(b) If A is invertible and A and C commute, show that

$$\det(M) = \det(AD - CB).$$

If A is invertible and A and B commute, show that

$$\det(M) = \det(DA - CB).$$

8. We have seen that, for any matrix A, row rank(A) = column rank(A). Define the determinantal rank of A by $r = \det \operatorname{rank}(A)$ if r is the largest positive integer such that A has an r-by-r submatrix (where the rows and columns forming this submatrix may be *any* r rows and *any* r columns) whose determinant is nonzero. Show that

$$\det \operatorname{rank}(A) = \operatorname{row\,rank}(A) = \operatorname{column\,rank}(A).$$

9. Prove Corollary 6.5.5.

10. Completely analogously to Definition 2.2.4, we may define three types of elementary column operations on a matrix A: (1) multiply a column of A by a nonzero constant c; (2) add a multiple of one column of A to another; (3) interchange two columns of A. Then we may call two matrices column-equivalent if one may be obtained from the other by a sequence of elementary column operations. Completely analogously to Section 4.6, Exercise 17, we may show that if two matrices are column-equivalent, one may be obtained from the other by a sequence of type (1) and type (2) elementary column operations (i.e., type (3) elementary column

operations are never necessary). Now consider matrices with real entries and call two such matrices positive column-equivalent if one can be obtained from the other by a sequence of elementary column operations of types (1) and (2) where in every elementary column operation of type (1) $c > 0$.

Let A be an invertible matrix. Show that A is positive column-equivalent to the identity matrix I if and only if $\det(A) > 0$ and, more generally, that if A and B are both invertible matrices (of the same size), then A and B are positive column-equivalent if and only if $\det(A)$ and $\det(B)$ have the same sign.

Chapter 7

The structure of a linear transformation

Let V be a vector space over a field $\mathbb{F}$, and let $\mathcal{T}\colon V \to V$ be a linear transformation. Our objective in this chapter and the next is to understand the geometric structure of $\mathcal{T}$.

Referring back to our metaphor of a basis as giving us a language in which to describe vectors and linear transformations, we are looking for the language in which the geometric behavior of $\mathcal{T}$ will become most apparent. This is the language of (generalized) eigenvectors, and the description of $\mathcal{T}$ will involve its eigenvalues. (Of course, these terms are yet to be defined.) In the simplest case, if we choose the proper basis $\mathcal{B}$, the matrix $[\mathcal{T}]_{\mathcal{B}}$ will be diagonal. In the general case, $[\mathcal{T}]_{\mathcal{B}}$ will not quite be so simple, but, providing a certain algebraic condition is satisfied, $[\mathcal{T}]_{\mathcal{B}}$ will be in a particular form known as Jordan canonical form.

We will begin this chapter by considering eigenvalues and eigenvectors—actually we saw them already in several examples in Chapter 5—and computing some concrete examples.

Then we will be more general and consider some questions about decomposing the vector space V, keeping in mind the linear transformation $\mathcal{T}$. This will give us some crude information about $\mathcal{T}$.

It turns out that this crude information is already enough for us to be able to use linear algebra to effectively solve certain differential equations. So we will then turn our attention to this application.

Then we will return to linear algebra and study the case of diagonalizable linear transformations. This case is relatively straightforward, but there is a lot to say about it.

We will then derive a variety of structural information about linear transformations, in particular, further information about eigenvalues and (generalized) eigenvectors, and will handle the case of triangularizable linear transformations.

Jordan canonical form is of the utmost importance, but is also quite involved, and so we save it until the next chapter.

At the end of the next chapter we give an application of our work to (once again, concretely) solve systems of differential equations. We delay it until then to have it all in one place. But you can skip ahead after reading this chapter to see how to solve the diagonalizable case.

7.1. Eigenvalues, eigenvectors, and generalized eigenvectors

We begin with the basic definition.

Definition 7.1.1. Let $\mathcal{T}\colon V \to V$ be a linear transformation. Then a scalar $\lambda \in \mathbb{F}$ is an *eigenvalue* of $\mathcal{T}$ if there is a nonzero vector $v \in V$ with $\mathcal{T}(v) = \lambda v$. In this case the vector v is called an *eigenvector* of $\mathcal{T}$ and λ and v are said to be *associated.* $\Diamond$

(The terms *characteristic value*/*characteristic vector* are sometimes used instead of eigenvalue/eigenvector.)

Note that $\mathcal{T}(v) = \lambda v$ is equivalent to $\mathcal{T}(v) = \lambda\mathcal{I}(v)$ which is itself equivalent to $(\mathcal{T} - \lambda\mathcal{I})(v) = 0$ and that is equivalent to $v \in \operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I})$. Thus we see we have an alternate definition.

Definition 7.1.2. Let $\mathcal{T}\colon V \to V$ be a linear transformation. Then a scalar $\lambda \in \mathbb{F}$ is an *eigenvalue* of $\mathcal{T}$ if there is a nonzero vector v with $(\mathcal{T} - \lambda\mathcal{I})(v) = 0$, or equivalently if $\operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I}) \neq \{0\}$. Such a vector v is an *eigenvector* of $\mathcal{T}$ and λ and v are *associated.* In this situation

$$E_\lambda = \operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I})$$

is the *eigenspace* of $\mathcal{T}$ *associated* to the eigenvalue λ. $\Diamond$

Thus we observe that the eigenspace of $\mathcal{T}$ associated to λ consists of all of the eigenvectors of $\mathcal{T}$ associated to λ together with the 0 vector.

Having defined eigenvalues/vectors of linear transformations, we can now easily do so for matrices.

Definition 7.1.3. Let A be an n-by-n matrix with entries in $\mathbb{F}$. Then the eigenvalues/eigenvectors/eigenspaces of A are the eigenvalues/eigenvectors/eigenspaces of the linear transformation $\mathcal{T}_A\colon \mathbb{F}^n \to \mathbb{F}^n$.

Equivalently, a scalar $\lambda \in \mathbb{F}$ is an *eigenvalue* of A if there is a nonzero vector $v \in \mathbb{F}$ with $(A - \lambda I)(v) = 0$, or equivalently if the nullspace $\operatorname{Null}(A - \lambda I) \neq \{0\}$. Such a vector v is an *eigenvector* of A and λ and v are associated. In this situation $E_\lambda = \operatorname{Null}(A - \lambda I)$ is the *eigenspace* of A associated to λ. $\Diamond$

Remark 7.1.4. We observe that for a linear transformation $\mathcal{T}$, the 0 eigenspace E_0 is just $\operatorname{Ker}(\mathcal{T})$. Similarly, for a matrix A, the 0 eigenspace E_0 is just the nullspace $\operatorname{Null}(A)$. $\Diamond$

Let us now see some examples.

Example 7.1.5. Let A be the matrix

$$A = \begin{bmatrix} -13 & -9 \\ 30 & 20 \end{bmatrix}.$$

We considered this matrix in Chapter 5 (see Example 5.4.12). We computed

$$A\begin{bmatrix}3\\-5\end{bmatrix}=2\begin{bmatrix}3\\-5\end{bmatrix}\qquad\text{and}\qquad A\begin{bmatrix}-1\\2\end{bmatrix}=5\begin{bmatrix}-1\\2\end{bmatrix}$$

and so 2 is an eigenvalue of A and $\begin{bmatrix}3\\-5\end{bmatrix}$ is an associated eigenvector, and 5 is an eigenvalue of A and $\begin{bmatrix}-1\\2\end{bmatrix}$ is an associated eigenvector. As we shall see, the eigenspace E_2 of A is 1-dimensional, with basis $\left\{\begin{bmatrix}3\\-5\end{bmatrix}\right\}$, and the eigenspace E_5 of A is also 1-dimensional, with basis $\left\{\begin{bmatrix}-1\\2\end{bmatrix}\right\}$. $\diamondsuit$

You may (in fact, you should) ask how we found those eigenvalues and eigenvectors. Be patient—we will see how to do so in a little while.

Example 7.1.6. Let $V = {}^t\mathbb{F}^{\infty\infty}$. Then we have right-shift $\mathcal{S}_{\mathrm{rt}}\colon V \to V$ by $\mathcal{S}_{\mathrm{rt}}([a_1, a_2, \dots]) = [0, a_1, a_2, \dots]$. It is easy to check that for any $c \in \mathbb{F}$, the equation $\mathcal{S}_{\mathrm{rt}}(v) = cv$ only has the solution $v = [0, 0, 0, \dots]$, the 0 vector in V, so $\mathcal{S}_{\mathrm{rt}}$ has no eigenvalues. On the other hand, we have left-shift $\mathcal{S}_{\mathrm{lt}}\colon V \to V$ by $\mathcal{S}_{\mathrm{lt}}([a_1, a_2, \dots]) = [a_2, a_3, \dots]$ and the equation $\mathcal{S}_{\mathrm{lt}} = cv$ has solution $v = [a, ac, ac^2, \dots] = a[1, c, c^2, \dots]$ for any $c \in \mathbb{F}$, and these are all the solutions, so every $c \in \mathbb{F}$ is an eigenvalue of $\mathcal{S}_{\mathrm{lt}}$ with associated eigenspace E_c 1-dimensional with basis $\{[1, c, c^2, \dots]\}$. $\diamondsuit$

Example 7.1.7. (1) Let $V = P^\infty(\mathbb{R})$, and let $\mathcal{T}\colon V \to V$ by $\mathcal{T}(p(x)) = xp'(x)$. Then, for every nonnegative integer f we have $\mathcal{T}(x^f) = x(fx^{f-1}) = fx^f$ so we see that f is an eigenvalue of $\mathcal{T}$ and x^f is an associated eigenvector.

(2) Let $V = P^\infty(\mathbb{R})$, and let $\mathcal{S}\colon V \to V$ by $\mathcal{S}(p(x)) = x(p(x+1) - p(x))$. Then for every nonnegative integer f we have $\mathcal{S}((x+f-1)^{(f)}) = x((x+f)^{(f)} - (x+f-1)^{(f)}) = x(f(x+f-1)^{(f-1)}) = f(x+f-1)^{(f)}$ so we see that f is an eigenvalue of $\mathcal{S}$ and $(x+f-1)^{(f)}$ is an associated eigenvector. (See Example 5.4.5. The polynomial $x^{(f)}$ was defined in Example 3.3.19.) $\diamondsuit$

Example 7.1.8. Let I be an open interval in $\mathbb{R}$, and let $V = C^\infty(I)$. We have the linear transformation $\mathcal{D}\colon V \to V$, $\mathcal{D}(f(x)) = f'(x)$. Then $\mathrm{Ker}(\mathcal{D}) = \{f(x) \mid f'(x) = 0\}$ is just the constant functions, so $E_0 = \mathrm{Ker}(\mathcal{D})$ is 1-dimensional with basis $\{1\}$. More generally, for any real number c,

$$\begin{aligned}E_c = \mathrm{Ker}(\mathcal{D} - c\mathcal{I}) &= \{f(x) \mid (\mathcal{D} - c\mathcal{I})(f(x)) = 0\}\\ &= \{f(x) \mid f'(x) - cf(x) = 0\} = \{f(x) \mid f'(x) = cf(x)\}.\end{aligned}$$

We recognize that the functions $f(x) = ae^{cx}$ for any $a \in \mathbb{R}$ are solutions to this equation, and in fact that these are the only solutions. Thus E_c is 1-dimensional with basis $\{e^{cx}\}$ for every $c \in \mathbb{R}$.

We can also consider the vector space V over $\mathbb{C}$ of all complex-valued infinitely differentiable functions on I. Then for any complex number c, we have the functions $f(x) = ae^{cx}$ for any $a \in \mathbb{C}$, with derivative $f'(x) = cae^{cx}$, and again E_c is 1-dimensional with basis $\{e^{cx}\}$ for every $c \in \mathbb{C}$. $\diamondsuit$

Looking ahead to future developments, we want to define generalized eigenvectors.

Definition 7.1.9. Let V be a vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. Let λ be an eigenvalue of $\mathcal{T}$. Then a nonzero vector v in V is a *generalized eigenvector* of *index* f of $\mathcal{T}$ if f is the smallest positive integer such that

$$(\mathcal{T} - \lambda\mathcal{I})^f(v) = 0.$$

We define the subspace E_λ^f of V by

$$E_\lambda^f = \{v \in V \mid (\mathcal{T} - \lambda\mathcal{I})^f(v) = 0\}$$

and the *generalized eigenspace* by

$$E_\lambda^\infty = \{v \in V \mid (\mathcal{T} - \lambda\mathcal{I})^f(v) = 0 \text{ for some } f\}. \qquad \Diamond$$

We observe that a generalized eigenvector of index 1 is just an eigenvector.

Equivalently, $E_\lambda^1 = E_\lambda$ by definition. We also observe that $v \in E_\lambda^f$ if v is a generalized eigenvector of index *at most* f, or $v = 0$, and thus we see that $E_\lambda = E_\lambda^1 \subseteq E_\lambda^2 \subseteq E_\lambda^3 \subseteq \cdots \subseteq E_\lambda^\infty$.

Lemma 7.1.10. (1) *For any f, E_λ^f is a subspace of V.*

(2) *E_λ^∞ is a subspace of V.*

Proof. (1) E_λ^f is the kernel of a linear transformation.

(2) We verify the conditions for E_λ^∞ to be a subspace. First, $0 \in E_\lambda^\infty$ as for $f = 0$ (or for any f), $(\mathcal{T} - \lambda\mathcal{I})^f(0) = 0$. Second, if $v \in E_\lambda^\infty$, then $(\mathcal{T} - \lambda\mathcal{I})^f(v) = 0$ for some f, in which case $(\mathcal{T} - \lambda\mathcal{I})^f(cv) = c(\mathcal{T} - \lambda\mathcal{I})^f(v) = c0 = 0$ so $cv \in E_\lambda^\infty$. Third, if $v_1 \in E_\lambda^\infty$, so that $(\mathcal{T} - \lambda\mathcal{I})^{f_1}(v_1) = 0$ for some f_1, and if $v_2 \in E_\lambda^\infty$, so that $(\mathcal{T} - \lambda\mathcal{I})^{f_2}(v_2) = 0$ for some f_2, then, choosing $f = \max(f_1, f_2)$, $(\mathcal{T} - \lambda\mathcal{I})(v_1 + v_2) = (\mathcal{T} - \lambda\mathcal{I})^f(v_1) + (\mathcal{T} - \lambda\mathcal{I})^f(v_2) = 0 + 0 = 0$ so $v_1 + v_2 \in E_\lambda^\infty$. $\square$

Remark 7.1.11. Note that, starting with v_f, a generalized eigenvector of index f associated to the eigenvalue λ, we can take $v_{f-1} = (\mathcal{T} - \lambda\mathcal{I})(v_f)$ to get a generalized eigenvector of index $f - 1$ associated to λ, then take $v_{f-2} = (\mathcal{T} - \lambda\mathcal{I})(v_{f-1})$ to get a generalized eigenvector of index $f - 2$ associated to λ, etc. In this way we get a "chain" of generalized eigenvectors

$$v_f, v_{f-1}, \dots, v_1$$

of indices $f, f-1, \dots, 1$, with $(\mathcal{T} - \lambda\mathcal{I})(v_j) = v_{j-1}$ for $j > 1$, and $(\mathcal{T} - \lambda\mathcal{I})(v_1) = 0$. This will be very important for us when we consider Jordan canonical form. $\Diamond$

Let us see some examples.

Example 7.1.12. Let A be the matrix

$$A = \begin{bmatrix} -27 & 36 \\ -25 & 33 \end{bmatrix}.$$

Then

$$(A - 3I)\begin{bmatrix} 6 \\ 5 \end{bmatrix} = \begin{bmatrix} -30 & 36 \\ -25 & 30 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix},$$

so 3 is an eigenvalue of A and $\begin{bmatrix} 6 \\ 5 \end{bmatrix}$ is an associated eigenvector. In fact, E_3^1 is 1-dimensional with basis $\left\{ \begin{bmatrix} 6 \\ 5 \end{bmatrix} \right\}$. Then

$$(A - 3I) \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -30 \\ -25 \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

but

$$(A - 3I)^2 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = (A - 3I)(A - 3I) \begin{bmatrix} 1 \\ 0 \end{bmatrix} = (A - 3I) \begin{bmatrix} -30 \\ -25 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix},$$

so $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is a generalized eigenvector of index 2 associated to the eigenvalue 3. (We observe that $(A - 3I) \begin{bmatrix} 1 \\ 0 \end{bmatrix} = -5 \begin{bmatrix} 6 \\ 5 \end{bmatrix} \in E_3^1$ as we expect.) In fact, you can check that $(A - 3I)^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, so $E_3^2 = \mathbb{F}^2$ is 2-dimensional, and any $v \in \mathbb{F}^2$ that is not in E_3^1, i.e., that is not a scalar multiple of $\begin{bmatrix} 6 \\ 5 \end{bmatrix}$, is a generalized eigenvector of index 2 associated to the eigenvalue 3. ♢

Again you may ask how we found this eigenvalue and these (generalized) eigenvectors, and again we will see in a little while.

Example 7.1.13. Referring to Example 7.1.6, let $\mathcal{S}_{\mathrm{lt}} \colon {}^t\mathbb{F}^{\infty\infty} \to {}^t\mathbb{F}^{\infty\infty}$ be left-shift. We saw that for any $c \in \mathbb{F}$, we had the eigenvector (= generalized eigenvector of index 1) $v_1 = [1, c, c^2, c^3, \dots]$, and $\{v_1\}$ was a basis for E_c^1. You can check that

$$v_2 = [0, 1, 2c, 3c^2, 4c^3, \dots]$$

is a generalized eigenvector of index 2, and E_c^2 is 2-dimensional with basis $\{v_1, v_2\}$. You can also check that

$$v_3 = [0, 0, 1, 3c, 6c^2, 10c^3, \dots]$$

is a generalized eigenvector of index 3, and E_c^3 is 3-dimensional with basis $\{v_1, v_2, v_3\}$. In fact, for any f, E_c^f is f-dimensional with basis $\{v_1, v_2, \dots, v_f\}$, and these vectors form a chain as in Remark 7.1.11. ♢

Example 7.1.14. Referring to Example 7.1.8, for any $f \geq 1$, if $p(x) = x^{f-1}$, then $\mathcal{D}(p(x)) = (f-1)x^{f-2}$, $\mathcal{D}^2(p(x)) = (f-1)(f-2)x^{f-3}$, $\dots$, $\mathcal{D}^{f-1}(p(x)) = (f-1)!$, and $\mathcal{D}^f(p(x)) = 0$. Thus $p(x)$ is a generalized eigenvector of $\mathcal{D}$ of index f, associated to the eigenvector 0. It turns out that E_0^f is f-dimensional, with basis

$$\{1, x, \dots, x^{f-1}\}.$$

More generally, for any $f \geq 1$, if $p(x) = x^{f-1}e^{cx}$, then $(\mathcal{D} - c\mathcal{I})(p(x)) = (f-1)x^{f-2}e^{cx}$, $(\mathcal{D} - c\mathcal{I})^2(p(x)) = (f-1)(f-2)x^{f-3}e^{cx}$, $\dots$, $(\mathcal{D} - c\mathcal{I})^{f-1}(p(x)) = (f-1)!\, e^{cx}$, and $(\mathcal{D} - c\mathcal{I})^f(p(x)) = 0$. Thus $p(x)$ is a generalized eigenvector of $\mathcal{D}$ of index f, associated to the eigenvalue c. In turns out that E_c^f is f-dimensional, with basis

$$\{e^{cx}, xe^{cx}, \dots, x^{f-1}e^{cx}\}.$$

♢

7.2. Polynomials in $\mathcal{T}$

Let V be an $\mathbb{F}$-vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. In this section we establish some general facts, which we will then specifically apply in the next sections.

We will be using a number of properties of polynomials, and we have gathered these properties together in Appendix B, which the reader should consult as necessary.

We let $\mathbb{F}[x]$ denote the set of polynomials with coefficients in $\mathbb{F}$.

Let $p(x) \in \mathbb{F}[x]$, $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then $p(\mathcal{T})\colon V \to V$ is the linear transformation $p(\mathcal{T}) = a_n\mathcal{T}^n + a_{n-1}\mathcal{T}^{n-1} + \cdots + a_1\mathcal{T} + a_0\mathcal{I}$. (For an n-by-n matrix A, $p(A) = a_nA^n + a_{n-1}A^{n-1} + \cdots + a_1A + a_0I$.)

We can already see that a discussion of polynomials in $\mathcal{T}$ is relevant to our work in this chapter, as we have already encountered them in the last section. For we can rewrite our definition of the eigenspace E_λ of $\mathcal{T}$ as

$$E_\lambda = \mathrm{Ker}(p(\mathcal{T})), \quad \text{where } p(x) \text{ is the polynomial } p(x) = x - \lambda,$$

and similarly

$$E_\lambda^f = \mathrm{Ker}(p(\mathcal{T})), \quad \text{where } p(x) \text{ is the polynomial } p(x) = (x-\lambda)^f.$$

We know that in general linear transformations do not commute. But the first thing to see is that two linear transformations that are polynomials in the same linear transformation do commute. In fact, we show something a little more precise.

Lemma 7.2.1. *Let $p(x), q(x) \in \mathbb{F}[x]$, and let $r(x) = p(x)q(x)$. Then for any linear transformation $\mathcal{T}$, $p(\mathcal{T})q(\mathcal{T}) = q(\mathcal{T})p(\mathcal{T}) = r(\mathcal{T})$.*

Proof. Let $p(x) = a_nx^n + \cdots + a_0$, and let $q(x) = b_mx^m + \cdots + b_0$. Then a typical term a_jx^j of $p(x)$ and a typical term b_kx^k of $q(x)$ contribute $a_jb_kx^{j+k}$ to $r(x)$.

But $(a_j\mathcal{T}^j)(b_k\mathcal{T}^k) = a_jb_k\mathcal{T}^{j+k} = (b_k\mathcal{T}^k)(a_j\mathcal{T}^j)$ by linearity. □

Now we get down to work.

Lemma 7.2.2. *Let V be a finite-dimensional vector space, $\dim V = n$, over the field $\mathbb{F}$, and let $\mathcal{T}\colon V \to V$ be a linear transformation. Let $v \in V$ be any fixed vector of V. Then there is a unique monic polynomial $\bar{m}(x) = m_{\mathcal{T},v}(x)$ of smallest degree such that $\bar{m}(\mathcal{T})(v) = 0$. The degree of the polynomial $\bar{m}(x)$ is at most n. Furthermore, if $p(x)$ is any polynomial with $p(\mathcal{T})(v) = 0$, then $\bar{m}(x)$ divides $p(x)$.*

Proof. First let us see that there is some nonzero monic polynomial $\tilde{m}(x)$ such that $\tilde{m}(\mathcal{T})(v) = 0$. To this end, consider the set of vectors

$$\{\mathcal{I}(v), \mathcal{T}(v), \mathcal{T}^2(v), \ldots, \mathcal{T}^n(v)\}.$$

This is a set of $n+1$ vectors in the n-dimensional vector space V, so must be linearly dependent. Thus there are $c_0, \ldots, c_n$, not all zero, with

$$c_n\mathcal{T}^n(v) + c_{n-1}\mathcal{T}^{n-1}(v) + \cdots + c_1\mathcal{T}(v) + c_0\mathcal{I}(v) = 0.$$

Let k be the largest value of i such that $c_i \neq 0$. Set $a_i = c_i/c_k$ for $i \leq k$. Then

$$\mathcal{T}^k(v) + a_{k-1}\mathcal{T}^{k-1}(v) + \cdots + a_1\mathcal{T}(v) + a_0\mathcal{I}(v) = 0$$

so if $\tilde{m}(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0$, then $\tilde{m}(\mathcal{T})(v) = 0$.

Now consider {all monic polynomials $q(x)$ with $q(\mathcal{T})(v) = 0$}. This set is nonempty, as we have just shown that $\tilde{m}(x)$ is such a polynomial. So there is some polynomial $\bar{m}(x)$ in this set of smallest degree, and this degree is at most n.

Now suppose $p(x)$ is any polynomial with $p(\mathcal{T})(v) = 0$. By the division algorithm for polynomials,

$$p(x) = \bar{m}(x)q(x) + r(x)$$

for some unique polynomials $q(x)$ and $r(x)$, with $r(x) = 0$ or $\deg(r(x)) < \deg(\bar{m}(x))$. But then

$$\begin{aligned} 0 = p(\mathcal{T})(v) &= (\bar{m}(\mathcal{T})q(\mathcal{T}) + r(\mathcal{T}))(v) \\ &= q(\mathcal{T})\bar{m}(\mathcal{T})(v) + r(\mathcal{T})(v) \\ &= q(\mathcal{T})(0) + r(\mathcal{T})(v) = r(\mathcal{T})(v). \end{aligned}$$

Thus if $r(x)$ is not the zero polynomial, then, dividing $r(x)$ by its leading coefficient, we obtain a monic polynomial $r_1(x)$ with $\deg(r_1(x)) < \deg(m(x))$ and $r_1(\mathcal{T})(v) = 0$, contradicting the minimality of the degree of $m(x)$. Hence $r(x) = 0$, and $p(x) = \bar{m}(x)q(x)$, i.e., $\bar{m}(x)$ divides $p(x)$.

This also shows that $\bar{m}(x)$ is unique, as if $p(x)$ had the same degree as $\bar{m}(x)$ and was also monic, the only way $\bar{m}(x)$ could divide $p(x)$ is if they were equal. □

Definition 7.2.3. The polynomial $m_{\mathcal{T},v}(x)$ of Lemma 7.2.2 is the $\mathcal{T}$-*annihilator* of v. ◊

We can immediately see a relationship between $\mathcal{T}$-annihilators and (generalized) eigenvectors.

Lemma 7.2.4. (1) *Let $\mathcal{T} : V \to V$ be a linear transformation, and let v be a nonzero vector of V. Then v is an eigenvector of $\mathcal{T}$ with associated eigenvalue λ if and only if its $\mathcal{T}$-annihilator $m_{\mathcal{T},v}(x) = x - \lambda$.*

(2) *More generally, v is a generalized eigenvector of index f of $\mathcal{T}$ with associated eigenvalue λ if and only if its $\mathcal{T}$-annihilator $m_{\mathcal{T},v}(x) = (x - \lambda)^f$.*

Proof. (1) If $m_{\mathcal{T},v}(x) = x - \lambda$, then by the definition of the $\mathcal{T}$-annihilator, $m_{\mathcal{T},v}(\mathcal{T})(v) = 0$, i.e., $(\mathcal{T} - \lambda\mathcal{I})(v) = 0$, and v is an eigenvector of $\mathcal{T}$ with associated eigenvalue λ. On the other hand, if v is an eigenvector of $\mathcal{T}$ with associated eigenvalue λ, then $(\mathcal{T} - \lambda\mathcal{I})(v) = 0$, i.e., $p(\mathcal{T})(v) = 0$ where $p(x) = x - \lambda$. But $m_{\mathcal{T},v}(x)$ is the unique monic polynomial of smallest degree with $m_{\mathcal{T},v}(\mathcal{T})(v) = 0$. Since $p(x)$ has degree 1, which is as small as possible (since $v \neq 0$) and is monic, we must have $m_{\mathcal{T},v}(x) = p(x) = x - \lambda$.

(2) If $m_{\mathcal{T},v}(x) = (x - \lambda)^f$, then $m_{\mathcal{T},v}(\mathcal{T})(v) = 0$, i.e., $(\mathcal{T} - \lambda\mathcal{I})^f(v) = 0$, so v is a generalized eigenvector of index at most f with associated eigenvalue λ. But for any $j < f$, $(x - \lambda)^j$ has degree $j < f$, so by the minimality of the degree of $m_{\mathcal{T},v}(x)$, $(\mathcal{T} - \lambda\mathcal{I})^j(v) \neq 0$. Hence v has index exactly f. On the other hand, if v is a generalized eigenvector of index f associated to the eigenvalue λ, then if

$p(x) = (x-\lambda)^f$, $p(\mathcal{T})(v) = (\mathcal{T}-\lambda\mathcal{I})^f(v) = 0$. Then $m_{\mathcal{T},v}(x)$ divides $p(x)$, so $m_{\mathcal{T},v}(x)$ must be $(x-\lambda)^j$ for some $j \leq f$. But if $j < f$, $(\mathcal{T}-\lambda\mathcal{I})^j(v) \neq 0$, because v has index f, so we must have $j = f$ and $m_{\mathcal{T},v}(x) = p(x) = (x-\lambda)^f$. □

Here is an important conclusion we can draw.

Corollary 7.2.5. (1) *Let $\mathcal{T}\colon V \to V$ be a linear transformation. Let $\lambda_1, \ldots, \lambda_k$ be distinct eigenvalues of $\mathcal{T}$, and for each i, let w_i be a generalized eigenvector associated to the eigenvalue λ_i. Then $\{w_1, \ldots, w_k\}$ is linearly independent.*

(2) *More generally, let $\mathcal{C}_i$ be a linearly independent set of generalized eigenvectors associated to the eigenvalue λ_i for each i. Then $\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_k$ is linearly independent.*

Proof. (1) Let w_i have index f_i. Suppose

$$v = c_1w_1 + c_2w_2 + \cdots + c_kw_k = 0.$$

Let $p_i(x) = \prod_{j\neq i}(x-\lambda_j)^{f_j}$. Thus $p_i(x)$ is divisible by $(x-\lambda_j)^{f_j} = m_{\mathcal{T},w_j}(x)$ for every $j \neq i$, but $p_i(x)$ is not divisible by $(x-\lambda_i)^{f_i} = m_{\mathcal{T},w_i}(x)$, and so $p_i(\mathcal{T})(w_j) = 0$ for every $j \neq i$, but $u_i = p_i(\mathcal{T})(w_i) \neq 0$. Then

$$0 = p_i(\mathcal{T})(v) = c_1p_i(\mathcal{T})(w_1) + \cdots + c_kp_i(\mathcal{T})(w_k) = c_iu_i$$

so $c_i = 0$ for each i, and hence $\{w_1, \ldots, w_k\}$ is linearly independent.

(2) Let $\mathcal{C}_i = \{w_i^1, w_i^2, \ldots\}$ for each i. Suppose

$$c_1^1w_1^1 + c_1^2w_1^2 + \cdots + c_k^1w_k^1 + c_k^2w_k^2 + \cdots = 0.$$

Let $w_1 = c_1^1w_1^1 + c_1^2w_1^2 + \cdots$, $\ldots$, $w_k = c_k^1w_k^1 + c_k^2w_k^2 + \cdots$. Then each w_i is a generalized eigenvector of $\mathcal{T}$ associated to the eigenvalue λ_i, and $w_1 + \cdots + w_k = 0$. Hence, by part (1), $w_1 = \cdots = w_k = 0$, i.e., $c_i^1w_i^1 + c_i^2w_i^2 + \cdots = 0$ for each i. But each $\mathcal{C}_i$ is linearly independent, so $c_i^1 = c_i^2 = \cdots = 0$ for each i, and so $\mathcal{C}$ is linearly independent. □

Here is one way (certainly not the only way) we can get a linearly independent set of generalized eigenvectors all associated to the same eigenvalue of $\mathcal{T}$.

Lemma 7.2.6. *Let λ be an eigenvalue of $\mathcal{T}$, and let $u_1, \ldots, u_j$ be generalized eigenvectors of $\mathcal{T}$ of indices $f_1, \ldots, f_j$ associated to the eigenvalue λ, with the indices $f_1, \ldots, f_j$ distinct. Then $\{u_1, \ldots, u_j\}$ is linearly independent.*

Proof. Reordering the vectors if necessary, we may assume $f_1 > f_2 > \cdots > f_j$. Now suppose

$$u = c_1u_1 + c_2u_2 + \cdots + c_ju_j = 0.$$

Note that $v_1 = (\mathcal{T}-\lambda\mathcal{I})^{f_1-1}(u_1) \neq 0$, but

$$(\mathcal{T}-\lambda\mathcal{I})^{f_1-1}(u_2) = \cdots = (\mathcal{T}-\lambda\mathcal{I})^{f_1-1}(u_j) = 0.$$

Then

$$0 = (\mathcal{T}-\lambda\mathcal{I})^{f_1-1}(u) = c_1v_1 + c_20 + \cdots + c_j0 = c_1v_1$$

with $v_1 \neq 0$, so $c_1 = 0$ and our relation is

$$u = c_2u_2 + \cdots + c_ju_j = 0.$$

Now repeat the argument using $(\mathcal{T} - \lambda\mathcal{I})^{f_2-1}$ instead of $(\mathcal{T} - \lambda\mathcal{I})^{f_1-1}$ to get $c_2 = 0$, etc., to conclude that $c_1 = \cdots = c_j = 0$ and $\{u_1, \ldots, u_j\}$ is linearly independent. $\square$

This gives the following precise conclusion.

Corollary 7.2.7. *In the situation of Corollary 7.2.5, for each i let $w_{i1}, \ldots, w_{ij_i}$ be generalized eigenvectors associated to the eigenvalue λ_i, with all the indices of these generalized eigenvectors distinct for each $i = 1, \ldots, k$. Then $\{w_{11}, \ldots, w_{1j_1}, w_{21}, \ldots, w_{2j_2}, \ldots, w_{k1}, \ldots, w_{kj_k}\}$ is linearly independent.*

Proof. Immediate from Lemma 7.2.6 and Corollary 7.2.5(2). $\square$

We are going to continue with our study of linear transformations in this section—it would not make sense to stop here. But the work we have done so far is already enough for us to be able to solve certain differential equations. We give this application in the next section. So if you are particularly interested in differential equations, you could skip ahead to that section now and then come back.

Theorem 7.2.8. *Let V be a finite-dimensional vector space, $\dim(V) = n$, over the field $\mathbb{F}$, and let $\mathcal{T}\colon V \to V$ be a linear transformation. Then there is a unique monic polynomial $m(x) = m_{\mathcal{T}}(x)$ of smallest degree such that $m(\mathcal{T}) = 0$. The degree of the polynomial $m(x)$ is at most n^2. Furthermore, if $p(x)$ is any polynomial with $p(\mathcal{T}) = 0$, then $m(x)$ divides $p(x)$.*

We will see, with considerably more work (see Corollary 7.2.14 below), that the degree of $m(x)$ is at most n.

Proof. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be any basis of V. For each i, let $m_i(x) = m_{\mathcal{T},v_i}(x)$. Then set

$$m_{\mathcal{T}}(x) = \operatorname{lcm}(m_1(x), \ldots, m_n(x)).$$

First we claim that $m(\mathcal{T}) = 0$. To see this, let $v \in V$ be arbitrary. Then we can write v as $v = c_1v_1 + \cdots + c_nv_n$ for some $c_1, \ldots, c_n$. Now for each i, $m(\mathcal{T})(v_i) = 0$ as $m(x)$ is a multiple of $m_i(x)$. Then

$$\begin{aligned} m(\mathcal{T})(v) &= m(\mathcal{T})(c_1v_1 + \cdots + c_nv_n) \\ &= c_1m(\mathcal{T})(v_1) + \cdots + c_nm(\mathcal{T})(v_n) \\ &= c_10 + \cdots + c_n0 = 0. \end{aligned}$$

Now suppose $p(x)$ is any polynomial with $p(\mathcal{T}) = 0$. Then $p(\mathcal{T})(v_i) = 0$ for each i, so, by Lemma 7.2.2 $m_i(x)$ divides $p(x)$. But then their least common multiple $m(x)$ divides $p(x)$.

And again this shows $m(x)$ is unique: if $p(x)$ is a monic polynomial of the same degree as $m(x)$, the only way $m(x)$ could divide $p(x)$ is if they were equal. $\square$

Definition 7.2.9. The polynomial $m_{\mathcal{T}}(x)$ of Theorem 7.2.8 is the *minimal polynomial* of $\mathcal{T}$. $\Diamond$

For an n-by-n matrix A, we define the A-*annihilator* of the vector v in $\mathbb{F}^n$ to be the $\mathcal{T}_A$-annihilator of v, and the *minimal polynomial* of the matrix A to be the minimal polynomial of the linear transformation $\mathcal{T}_A$. More simply, $m_{A,v}(x)$ is the unique monic polynomial of smallest degree with $m_{A,v}(A)v = 0$, and $m_A(x)$ is the unique monic polynomial of smallest degree with $m_A(A) = 0$.

Example 7.2.10. (1) If $\mathcal{T} = 0$, then $m_{\mathcal{T}}(x) = 1$, of degree 0.

(2) If $\mathcal{T} = c\mathcal{I}$ with $c \neq 0$, then $m_{\mathcal{T}}(x) = x - c$, of degree 1. $\Diamond$

Example 7.2.11. (1) Let A be the matrix of Example 7.1.5, and let $\mathcal{B} = \left\{\begin{bmatrix} 3 \\ -5 \end{bmatrix}, \begin{bmatrix} -1 \\ 2 \end{bmatrix}\right\} = \{v_1, v_2\}$. As we saw, v_1 is an eigenvector of A with associated eigenvalue 2, so $m_{A,v_1}(x) = x - 2$, and v_2 is an eigenvector of A with associated eigenvalue 5, so $m_{A,v_2}(x) = x - 5$. You can easily check that $\mathcal{B}$ is a basis of $\mathbb{F}^2$, but you don't even have to—this is automatic from Corollary 7.2.5. Then the minimal polynomial is

$$m_A(x) = \operatorname{lcm}(x-2, x-5) = (x-2)(x-5) = x^2 - 7x + 10.$$

(You can check by matrix arithmetic that $A^2 - 7A + 10I = 0$.)

(2) Let A be the matrix of Example 7.1.12, and let $\mathcal{B} = \left\{\begin{bmatrix} 6 \\ 5 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right\} = \{v_1, v_2\}$. As we saw, v_1 is an eigenvector (or equivalently, a generalized eigenvector of index 1) of A with associated eigenvalue 3, so $m_{A,v_1}(x) = x - 3$, and v_2 is a generalized eigenvector of index 2 with associated eigenvalue 3, so $m_{A,v_2}(x) = (x-3)^2$. You can easily check that $\mathcal{B}$ is a basis of $\mathbb{F}^2$, but you don't even have to—this is automatic from Corollary 7.2.7. Then the minimal polynomial is

$$m_A(x) = \operatorname{lcm}(x-3, (x-3)^2) = (x-3)^2 = x^2 - 6x + 9.$$

(You can check by matrix arithmetic that $A^2 - 6A + 9I = 0$.) $\Diamond$

Here is an example to show that we have to restrict our attention to finite-dimensional vector spaces.

Example 7.2.12. Let $V = {}^t\mathbb{F}^\infty$ and consider $\mathcal{S}_{\mathrm{lt}} \colon V \to V$, left-shift. For any $v \in V$, $v = [0, 0, 0, \ldots]$, in which case $m_{\mathcal{T},v}(x) = 1$, or $v = [a_1, a_2, \ldots, a_f, 0, 0, 0, \ldots]$ with $a_f \neq 0$ for some f, in which case $m_{\mathcal{T},v}(x) = x^f$. Thus for every vector $v \in V$, $m_{\mathcal{T},v}(x)$ exists, but there is no polynomial $m_{\mathcal{T}}(x)$ with $m_{\mathcal{T}}(\mathcal{T}) = 0$ (as that polynomial would have to be divisible by x^f for every f). If we consider $\mathcal{S}_{\mathrm{rt}} \colon V \to V$, right-shift, then for *no* $v \neq 0$ is there a polynomial $m_{\mathcal{T},v}(x)$ with $m_{\mathcal{T},v}(\mathcal{T})(v) = 0$, and so there is certainly no polynomial $m_{\mathcal{T}}(x)$ with $m_{\mathcal{T}}(\mathcal{T}) = 0$. $\Diamond$

Theorem 7.2.13. *Let V be a finite-dimensional vector space, and let $\mathcal{T} \colon V \to V$ be a linear transformation. Then there is some vector v_0 in V for which $m_{\mathcal{T}}(x) = m_{\mathcal{T},v_0}(x)$, i.e., for which the minimal polynomial of $\mathcal{T}$ is equal to the $\mathcal{T}$-annihilator of the vector v_0.*

Proof. Factor $m_{\mathcal{T}}(x)$ as

$$m_{\mathcal{T}}(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k},$$

where $p_1(x), \ldots, p_k(x)$ are distinct irreducible monic polynomials.

Claim. *For each j, there is a vector w_j in V with $m_{\mathcal{T},w_j}(x) = p_j(x)^{e_j}$.*

Proof. Choose a basis $\{v_1, \ldots, v_n\}$ of V. We know

$$m_{\mathcal{T}}(x) = \operatorname{lcm}(m_1(x), \ldots, m_n(x)),$$

where $m_i(x) = m_{\mathcal{T},v_i}(x)$. Thinking about the factorizations of $m_1(x), \ldots, m_n(x)$, there must be some i for which $m_i(x)$ has $p_j(x)^{e_j}$ as a factor, so $m_i(x) = p_j(x)^{e_j} q(x)$ for some polynomial $q(x)$. Then let $w_j = q(\mathcal{T})(v_i)$. □

Claim. *If u_1 and u_2 are any two vectors in V with $m_{\mathcal{T},u_1}(x)$ and $m_{\mathcal{T},u_2}(x)$ relatively prime, and $u = u_1 + u_2$, then*

$$m_{\mathcal{T},u}(x) = m_{\mathcal{T},u_1}(x) m_{\mathcal{T},u_2}(x).$$

Proof. Write $r_1(x) = m_{\mathcal{T},u_1}(x)$, $r_2(x) = m_{\mathcal{T},u_2}(x)$, and $r(x) = m_{\mathcal{T},u}(x)$, for convenience. Then we want to show $r(x) = r_1(x) r_2(x)$.

First observe that

$$\begin{aligned}
r_1(\mathcal{T})r_2(\mathcal{T})(u) &= r_1(\mathcal{T})r_2(\mathcal{T})(u_1 + u_2) \\
&= r_1(\mathcal{T})r_2(\mathcal{T})(u_1) + r_1(\mathcal{T})r_2(\mathcal{T})(u_2) \\
&= r_2(\mathcal{T})r_1(\mathcal{T})(u_1) + r_1(\mathcal{T})r_2(\mathcal{T})(u_2) \\
&= r_2(\mathcal{T})(0) + r_1(\mathcal{T})(0) \\
&= 0 + 0 = 0.
\end{aligned}$$

This tells us that $r(x)$ divides $r_1(x)r_2(x)$. We now show that $r_1(x)r_2(x)$ divides $r(x)$. We know $r(\mathcal{T})(u) = 0$. But then

$$\begin{aligned}
0 = r(\mathcal{T})(u) &= r_2(\mathcal{T})r(\mathcal{T})(u) \\
&= r(\mathcal{T})r_2(\mathcal{T})(u) \\
&= r(\mathcal{T})r_2(\mathcal{T})(u_1 + u_2) \\
&= r(\mathcal{T})r_2(\mathcal{T})(u_1) + r(\mathcal{T})r_2(\mathcal{T})(u_2) \\
&= r(\mathcal{T})r_2(\mathcal{T})(u_1) + r(\mathcal{T})(0) \\
&= r(\mathcal{T})r_2(\mathcal{T})(u_1) + 0 = r(\mathcal{T})r_2(\mathcal{T})(u_1),
\end{aligned}$$

so we see that $r_1(x)$ divides $r(x)r_2(x)$. Since $r_1(x)$ and $r_2(x)$ are relatively prime, we have that $r_1(x)$ divides $r(x)$. By the same logic, $r_2(x)$ divides $r(x)$, but, again because $r_1(x)$ and $r_2(x)$ are relatively prime, $r_1(x)r_2(x)$ divides $r(x)$. □

With these claims now taken care of, we finish the proof of the theorem.

We have w_1 with $m_{\mathcal{T},w_1}(x) = p_1(x)^{e_1}$. We also have w_2 with $m_{\mathcal{T},w_2}(x) = p_2(x)^{e_2}$. Since these polynomials are relatively prime, we know $m_{\mathcal{T},w_1+w_2}(x) = p_1(x)^{e_1} p_2(x)^{e_2}$. But then we have w_3 with $m_{\mathcal{T},w_3}(x) = p_3(x)^{e_3}$, which is relatively prime to $p_1(x)^{e_1} p_2(x)^{e_2}$, so $m_{\mathcal{T},w_1+w_2+w_3}(x) = p_1(x)^{e_1} p_2(x)^{e_2} p_3(x)^{e_3}$. Keep going. At the end, if we set $v_0 = w_1 + w_2 + \cdots + w_k$, $m_{\mathcal{T},v_0}(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_k(x)^{e_k} = m_{\mathcal{T}}(x)$. □

Corollary 7.2.14. *If V has dimension n, then the minimal polynomial $m_{\mathcal{T}}(x)$ has degree at most n.*

Proof. We just saw that $m_{\mathcal{T}}(x) = m_{\mathcal{T},v_0}(x)$ for some vector v_0, and we observed earlier (Lemma 7.2.2) that for any vector v, the degree of the polynomial $m_{\mathcal{T},v}(x)$ is at most n. □

We now introduce another polynomial, the characteristic polynomial, that is intimately related to eigenvalues.

Definition 7.2.15. (1) Let A be an n-by-n matrix with entries in $\mathbb{F}$. The *characteristic polynomial* $c_A(x)$ is the polynomial

$$c_A(x) = \det(xI - A).$$

(2) Let V be a finite-dimensional vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. Let $\mathcal{B}$ be any basis of V, and let $A = [\mathcal{T}]_{\mathcal{B}}$ be the matrix of $\mathcal{T}$ in the $\mathcal{B}$ basis. Then the *characteristic polynomial* $c_{\mathcal{T}}(x)$ of $\mathcal{T}$ is the polynomial $c_{\mathcal{T}}(x) = c_A(x) = \det(xI - A)$. ◊

Now the definition of $c_A(x)$ certainly makes sense, but there is a potential problem with the definition of $c_{\mathcal{T}}(x)$. We want it to just depend on $\mathcal{T}$, but it appears to depend on A, which depends on the choice of basis $\mathcal{B}$. So the first thing we have to see is that this potential problem is not an actual problem.

Lemma 7.2.16. *The characteristic polynomial $c_{\mathcal{T}}(x)$ is well-defined, i.e., it only depends on the linear transformation $\mathcal{T}$, not the choice of basis $\mathcal{B}$.*

Proof. Let $\mathcal{C}$ be any other basis of V, and let $B = [\mathcal{T}]_{\mathcal{C}}$. Then A and B are similar, so $B = PAP^{-1}$ for some invertible matrix P. But then

$$\begin{aligned} xI - B &= xI - PAP^{-1} = x(PIP^{-1}) - PAP^{-1} = P(xI)P^{-1} - PAP^{-1} \\ &= P(xI - A)P^{-1}, \end{aligned}$$

i.e., $xI - B$ is similar to $xI - A$. But then $\det(xI - B) = \det(xI - A)$ by Corollary 6.2.7. □

Remark 7.2.17. (1) Let A be the n-by-n matrix $A = (a_{ij})$. Referring to our expression for the determinant (Theorem 6.3.11), we see that $\det(xI - A)$ has one term that is the product of the diagonal entries of the matrix $xI - A$, which is $(x - a_{11})(x - a_{22}) \cdots (x - a_{nn})$. Note the highest power of x in this expression is x^n, and it has a coefficient of 1. We also see that the highest power of x in any other term of $\det(xI - A)$ is less than n. Thus we conclude that $\det(xI - A)$ is a monic polynomial of degree n.

(2) One of the virtues of the characteristic polynomial is that we can actually compute it—after all, it is a determinant, and we know how to compute determinants.

(3) In doing theoretical work, it is preferable to deal with $xI - A$, because $\det(xI - A)$ is monic. But for computations it is much more preferable to deal with $A - xI$, and that is what we shall do. ◊

Here is the basic result that gets the ball rolling.

Theorem 7.2.18. *The eigenvalues of $\mathcal{T}$ are the roots of the characteristic polynomial $c_{\mathcal{T}}(x)$.*

Proof. Let λ be a root of $c_{\mathcal{T}}(x)$. Then $\det(\lambda I - A) = 0$, so $\lambda I - A$ is not invertible. Now $\lambda I - A = [\lambda\mathcal{I} - \mathcal{T}]_{\mathcal{B}}$, so $\lambda\mathcal{I} - \mathcal{T}$ is not invertible. In particular this means $\mathrm{Ker}(\lambda\mathcal{I} - \mathcal{T}) \neq \{0\}$. Let v be any nonzero vector in $\mathrm{Ker}(\lambda\mathcal{I} - \mathcal{T})$. Then

$$\begin{aligned}(\lambda\mathcal{I} - \mathcal{T})(v) &= 0,\\ \lambda\mathcal{I}(v) - \mathcal{T}(v) &= 0,\\ \lambda v - \mathcal{T}(v) &= 0,\\ \lambda v &= \mathcal{T}(v),\end{aligned}$$

and so we see that λ is an eigenvalue of $\mathcal{T}$.

Conversely, suppose that λ is an eigenvalue of $\mathcal{T}$ and let v be an associated eigenvector. Then by definition $\lambda v = \mathcal{T}(v)$ and the same argument shows that $(\lambda\mathcal{I} - \mathcal{T})(v) = 0$, so $v \in \mathrm{Ker}(\lambda\mathcal{I} - \mathcal{T})$. By the definition of an eigenvector, $v \neq 0$, so we see that $\mathrm{Ker}(\lambda\mathcal{I} - \mathcal{T}) \neq \{0\}$, and hence $\lambda\mathcal{I} - \mathcal{T}$ is not invertible. But then $\det(\lambda\mathcal{I} - \mathcal{T}) = 0$, i.e., $c_{\mathcal{T}}(\lambda) = 0$, and λ is a root of $c_{\mathcal{T}}(x)$. □

Example 7.2.19. Let A be as in Example 7.1.5 or Example 7.2.11(1),

$$A = \begin{bmatrix} -13 & -9 \\ 30 & 20 \end{bmatrix}.$$

Then

$$\begin{aligned} c_A(c) = \det(xI - A) &= \det\left(\begin{bmatrix} x+13 & 9 \\ -30 & x-20 \end{bmatrix}\right) \\ &= x^2 - 7x + 10 = (x-2)(x-5) \end{aligned}$$

so A has eigenvalues $\lambda = 2$ and $\lambda = 5$.

The eigenspace $E_2 = \mathrm{Null}(A - 2I) = \mathrm{Null}\left(\begin{bmatrix} -15 & -9 \\ 30 & 18 \end{bmatrix}\right)$, and we know how to find this—row reduction, of course. When we do so, we find it is 1-dimensional with basis $\left\{\begin{bmatrix} 3 \\ -5 \end{bmatrix}\right\}$. Similarly, $E_5 = \mathrm{Null}(A - 5I) = \mathrm{Null}\left(\begin{bmatrix} -18 & -9 \\ 30 & 15 \end{bmatrix}\right)$ is 1-dimensional with basis $\left\{\begin{bmatrix} -1 \\ 2 \end{bmatrix}\right\}$. ◊

Example 7.2.20. Let A be as in Example 7.1.12 or Example 7.2.11(2),

$$A = \begin{bmatrix} -27 & 36 \\ -25 & 33 \end{bmatrix}.$$

Then

$$\begin{aligned} c_A(x) = \det(xI - A) &= \det\left(\begin{bmatrix} x+27 & -36 \\ 25 & x-33 \end{bmatrix}\right) \\ &= x^2 - 6x + 9 = (x-3)^2 \end{aligned}$$

so A has the eigenvalue $\lambda = 3$.

The eigenspace $E_3 = \mathrm{Null}(A - 3I) = \mathrm{Null}\left(\begin{bmatrix} -30 & 36 \\ -25 & 30 \end{bmatrix}\right)$ is 1-dimensional with basis $\left\{\begin{bmatrix} 6 \\ 5 \end{bmatrix}\right\}$.

We also compute E_3^2, the vector space of generalized eigenvectors of index at most 2 associated to the eigenvalue 3. $E_3^2 = \mathrm{Null}((A-3I)^2) = \mathrm{Null}\left(\begin{bmatrix} -30 & 36 \\ -25 & 30 \end{bmatrix}^2\right)$. We compute that $\begin{bmatrix} -30 & 36 \\ -25 & 30 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ so $E_3^2 = \mathbb{F}^2$ is 2-dimensional. We have our choice of bases, so we could just extend $\left\{\begin{bmatrix} 6 \\ 5 \end{bmatrix}\right\}$ to $\left\{\begin{bmatrix} 6 \\ 5 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right\}$. ♢

7.3. Application to differential equations

We now pause in our investigation of the structure of linear transformations to see how the work we have done so far provides us with a method—a practical method, not just a theoretical one—for solving certain differential equations. But before we get to the practical method, we will need a theoretical result.

We let I be an interval in $\mathbb{R}$ and we assume, for simplicity, that all our functions are C^∞. We will allow them to take complex values, so we will initially be dealing with vector spaces over $\mathbb{C}$. Thus we let V be the vector space of complex-valued C^∞ functions on I. But we will come back and relate this to real-valued functions later in the section.

We let D denote differentiation, i.e., $D(f(x)) = f'(x)$.

Lemma 7.3.1. *Let $a_n(x), \dots, a_0(x)$ be functions in V, and let*

$$\mathcal{L} = a_n(x)D^n + \cdots + a_0(x)$$

(so that $\mathcal{L}(f(x)) = a_n(x)f^{(n)}(x) + \cdots + a_0(x)f(x)$). Then $\mathcal{L}\colon V \to V$ is a linear transformation.

Proof. D is a linear transformation, and hence so is D^k for any k; multiplication by a fixed function is a linear transformation; the sum of linear transformations is a linear transformation. □

Definition 7.3.2. $\mathcal{L}$ as in Lemma 7.3.1 is called a *linear differential operator of order n.* ♢

This name is easy to understand. It is called linear as it is a linear transformation and differential as it involves derivatives. Its order is n as that is the highest derivative that appears. Finally, operator is a traditional mathematical term for a transformation that takes a function to another function.

Here is the basic result from differential equations that we will use.

Theorem 7.3.3. *Let $\mathcal{L} = a_n(x)D^n + \cdots + a_0(x)$ be a linear differential operator and suppose that $a_n(x) \neq 0$ for every $x \in I$. Let $g(x)$ be any function in V. Let x_0 be any point in I, and let $y_0, \dots, y_{n-1}$ be arbitrary complex numbers. Then there is a unique function $f(x)$ in V with*

$$\mathcal{L}(f(x)) = g(x), \quad f(x_0) = y_0, \quad f'(x_0) = y_1, \ \dots, \ f^{(n-1)}(x_0) = y_{n-1}.$$

Now let us translate this theorem into linear algebra.

Theorem 7.3.4. *Let $\mathcal{L}$ be as in Theorem* 7.3.3. *Then* $\mathrm{Ker}(\mathcal{L})$ *is an n-dimensional subspace of V and for any $g(x)$ in V, $\{f(x)\,|\,\mathcal{L}(f(x)) = g(x)\}$ is an affine subspace of V parallel to* $\mathrm{Ker}(\mathcal{L})$.

Proof. Since $\mathcal{L}$ is a linear transformation, we know that $\mathrm{Ker}(\mathcal{L})$ is a subspace of V. We also know that $\{f(x)\,|\,\mathcal{L}(f(x)) = g(x)\}$ is either empty or an affine subspace of V parallel to $\mathrm{Ker}(\mathcal{L})$ and Theorem 7.3.3 tells us it is nonempty.

The most important part of the conclusion is that $\mathrm{Ker}(\mathcal{L})$ has dimension n. To see this, let $\mathcal{T}\colon \mathrm{Ker}(\mathcal{L}) \to \mathbb{C}^n$ by

$$\mathcal{T}(f(x)) = \begin{bmatrix} f(x_0) \\ f'(x_0) \\ \vdots \\ f^{(n-1)}(x_0) \end{bmatrix}.$$

Then $\mathcal{T}$ is onto, because the theorem says that for any vector $y = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix}$ in $\mathbb{C}^n$, there is a function in $\mathrm{Ker}(\mathcal{L})$ (i.e., a function with $\mathcal{L}(f(x)) = 0$, with $\mathcal{T}(f(x)) = y$), and it is 1-1 because the theorem says that this function is unique. Thus $\mathcal{T}$ is an isomorphism and so $\dim \mathrm{Ker}(\mathcal{L}) = \dim \mathbb{C}^n = n$. ☐

Corollary 7.3.5. (1) *Let $\mathcal{B} = \{f_1(x), \dots, f_n(x)\}$ be a basis of* $\mathrm{Ker}(\mathcal{L})$. *Then any $f(x)$ in V with $\mathcal{L}(f(x)) = 0$ can be expressed uniquely as $f(x) = c_1 f_1(x) + \cdots + c_n f_n(x)$ for some constants $c_1, \dots, c_n$.*

(2) *Let $f_0(x)$ be any fixed function with $\mathcal{L}(f_0(x)) = g(x)$. Then any $f(x)$ in V with $\mathcal{L}(f(x)) = g(x)$ can be expressed uniquely as*

$$f(x) = f_0(x) + c_1 f_1(x) + \cdots + c_n f_n(x) \quad \textit{for some constants } c_1, \dots, c_n.$$

Thus we see from this corollary that linear algebra reduces the problem of finding the general solution of $\mathcal{L}(f(x)) = 0$ to that of finding n linearly independent solutions $f_1(x), \dots, f_n(x)$. (Since $f_1(x), \dots, f_n(x)$ are n linearly independent elements of the vector space $\mathrm{Ker}(\mathcal{L})$, which is n-dimensional, they are automatically a basis.) It reduces the problem of finding the general solution of $\mathcal{L}(f(x)) = g(x)$ to finding $f_1(x), \dots, f_n(x)$, and in addition finding a single solution $f_0(x)$ of the nonhomogeneous equation. In the language of differential equations, a (any) single such function with $\mathcal{L}(f_0(x)) = g(x)$ is called a *particular solution*.

Now suppose we have n solutions $f_1(x), \dots, f_n(x)$. How can we tell if they're a basis? Here's how.

Lemma 7.3.6. *Let $f_1(x), \dots, f_n(x)$ be solutions to $\mathcal{L}(f(x)) = 0$. Then the following conditions are equivalent:*

(1) $\mathcal{B} = \{f_1(x), \dots, f_n(x)\}$ *is linearly independent and thus a basis for* $\mathrm{Ker}(\mathcal{L})$.

(2) *For any $x_0 \in I$, the vectors*

$$\left\{ \begin{bmatrix} f_1(x_0) \\ f_1'(x_0) \\ \vdots \\ f_1^{(n-1)}(x) \end{bmatrix}, \begin{bmatrix} f_2(x_0) \\ f_2'(x_0) \\ \vdots \\ f_2^{(n-1)}(x) \end{bmatrix}, \ldots, \begin{bmatrix} f_n(x_0) \\ f_n'(x_0) \\ \vdots \\ f_n^{(n-1)}(x) \end{bmatrix} \right\}$$

are linearly independent, and thus a basis for $\mathbb{C}^n$.

(3) *For any $x_0 \in I$, the matrix*

$$A_{x_0} = \begin{bmatrix} f_1(x_0) & \ldots & f_n(x_0) \\ f_1'(x_0) & \ldots & f_n'(x_0) \\ \vdots & & \vdots \\ f_n^{(n-1)}(x_0) & \ldots & f_n^{(n-1)}(x_0) \end{bmatrix}$$

is invertible.

(4) *For any $x_0 \in I$, $W(x_0) = \det(A_{x_0}) \neq 0$.*

Proof. No work—we already know this.

(1) is equivalent to (2) as the linear transformation $\mathcal{T}$ in the proof of Theorem 7.3.4 is an isomorphism, so $\mathcal{T}(\mathcal{B})$ is a basis if and only if $\mathcal{B}$ is a basis.

(2) is equivalent to (3), as we have seen.

(3) is equivalent to (4), as we have also seen. $\square$

In the theory of differential equations, $W(x_0)$ is known as the *Wronskian* of the functions $f_1(x), \ldots, f_n(x)$ at x_0. (Since the point x_0 is arbitrary, this lemma also tells us that either $W(x_0) \neq 0$ for every x_0 in I, or that $W(x_0) = 0$ for every x_0 in I.)

Now I promised you that we would have a practical, not just a theoretical, method for solving certain differential equations. Here it is.

Definition 7.3.7. $\mathcal{L}$ is a constant coefficient linear differential operator if each of the functions $a_i(x)$ is a constant, $a_i(x) = a_i$. $\diamondsuit$

Theorem 7.3.8. *Let*

$$\mathcal{L} = a_n D^n + a_{n-1} D^{n-1} + \cdots + a_1 D + a_0$$

be a constant coefficient linear differential operator with $a_n \neq 0$. Factor $p(D) = a_n D^n + \cdots + a_0$ as $p(D) = a_n(D - \lambda_1)^{e_1} \cdots (D - \lambda_k)^{e_k}$. Then a basis for $\operatorname{Ker}(\mathcal{L})$ *is given by*

$$\mathcal{B} = \{e^{\lambda_1 x}, \ldots, x^{e_1 - 1} e^{\lambda_1 x}, e^{\lambda_2 x}, \ldots, x^{e_2 - 1} e^{\lambda_2 x}, \ldots, e^{\lambda_k x}, \ldots, x^{e_k - 1} e^{\lambda_k x}\}$$

and so the general solution of $\mathcal{L}(f(x)) = 0$ is given by

$$f(x) = c_{1\,0} e^{\lambda_1 x} + \cdots + c_{1\,e_1 - 1} x^{e_1 - 1} e^{\lambda_1 x} + \cdots + c_{k\,0} e^{\lambda_k x} + \cdots + c_{k\,e_k - 1} x^{e_k - 1} e^{\lambda_k x}.$$

Proof. No work—we already know this! Since $p(D)$ has degree n, $e_1 + \cdots + e_k = n$. $\mathcal{B}$ has $e_1 + \cdots + e_k = n$ elements. Thus to show $\mathcal{B}$ is a basis, we need only show $\mathcal{B}$ is linearly independent. But we already observed that $x^j e^{\lambda x}$ is a generalized eigenvector of index j associated to the eigenvalue λ of D. Thus the elements of

$\mathcal{B}$ are all generalized eigenvectors with no two having the same index, and so $\mathcal{B}$ is linearly independent by Corollary 7.2.7. $\square$

(Note there was no need to compute any Wronskians or anything else in this proof—the linear independence of $\mathcal{B}$ is guaranteed.)

Corollary 7.3.9. *In the situation of Theorem* 7.3.8*, let* A_{x_0} *be the matrix in Lemma* 7.3.6 *for the basis* $\mathcal{B}$ *of Theorem* 7.3.8*, and let* $\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$ *be the unique solution of* $A_{x_0}\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} y_0 \\ \vdots \\ y_{n-1} \end{bmatrix}$*; equivalently let* $\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = A_{x_0}^{-1}\begin{bmatrix} y_0 \\ \vdots \\ y_{n-1} \end{bmatrix}$*. Then* $\mathcal{L}(f(x)) = 0$*,* $f(x_0) = y_0, \ldots, f^{(n-1)}(x_0) = y_{n-1}$ *has the unique solution*

$$f(x) = c_1 e^{\lambda_1 x} + \cdots + c_n x^{e_k - 1} e^{\lambda_k x}.$$

Proof. Since $\mathcal{B}$ is a basis, we know A_{x_0} is an invertible matrix (by Lemma 7.3.6—again no need to compute Wronskians) and applying the linear transformation $\mathcal{T}$ of the proof of Theorem 7.3.4 to this basis gives precisely the columns of A_{x_0}, so for these unique values of $c_1, \ldots, c_n$, $f(x)$ is the unique solution of $\mathcal{L}(f(x)) = 0$ with $f(x_0) = y_0, \ldots, f^{(n-1)}(x_0) = y_{n-1}$. $\square$

Example 7.3.10. (1) Let $\mathcal{L} = D^3(D-2)^2(D-4)$. We wish to find all functions $f(x)$ that are solutions to the differential equation $\mathcal{L}(f(x)) = 0$.

Answer. $\mathcal{B} = \{1, x, x^2, e^{2x}, xe^{2x}, e^{4x}\}$ is a basis for $\operatorname{Ker}(\mathcal{L})$, so $f(x) = c_1 + c_2 x + c_3 x^2 + c_4 e^{2x} + c_5 x e^{2x} + c_6 e^{4x}$ with $c_1, \ldots, c_6$ arbitrary.

(2) We wish to find the unique function $f(x)$ with $\mathcal{L}(f(x)) = 0$ and $f(0) = 6$, $f'(0) = 7$, $f''(0) = 22$, $f'''(0) = 68$, $f''''(0) = 256$, and $f'''''(0) = 1008$.

Answer. Using the basis $\mathcal{B}$ above we form the matrix A_0 and then we solve

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 2 & 1 & 4 \\ 0 & 0 & 2 & 4 & 4 & 16 \\ 0 & 0 & 0 & 8 & 12 & 64 \\ 0 & 0 & 0 & 16 & 32 & 256 \\ 0 & 0 & 0 & 32 & 80 & 1024 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \end{bmatrix} = \begin{bmatrix} 6 \\ 7 \\ 22 \\ 68 \\ 256 \\ 1008 \end{bmatrix}$$

and find $c_1 = 3$, $c_2 = 0$, $c_3 = 1$, $c_4 = 2$, $c_5 = -1$, and $c_6 = 1$, so $f(x) = 3 + x^2 + 2e^{2x} - xe^{2x} + e^{4x}$. $\Diamond$

Our solution method has one blemish. Suppose $p(D)$ is a polynomial with real coefficients. It may have complex roots, which means our solution will be expressed in terms of complex functions. We would like to express it in terms of real functions.

To this end, note that if $\lambda = a + bi$ is a root of the real polynomial $p(D)$, then its complex conjugate $\bar{\lambda} = a - bi$ is a root of $p(D)$ of the same multiplicity. Now consider the 2-dimensional vector space W with basis $\{e^{\lambda x}, e^{\bar{\lambda}x}\}$. We have that

$$\begin{aligned} e^{\lambda x} &= e^{(a+bi)x} = e^{ax}(\cos(bx) + i\sin(bx)) = e^{ax}\cos(bx) + ie^{ax}\sin(bx), \\ e^{\bar{\lambda}x} &= e^{(a-bi)x} = e^{ax}(\cos(-bx) + i\sin(-bx)) = e^{ax}\cos(bx) - ie^{ax}\sin(bx). \end{aligned}$$

Hence

$$\begin{aligned} e^{ax}\cos(bx) &= \frac{1}{2}e^{\lambda x} + \frac{1}{2}e^{\bar{\lambda}x}, \\ e^{ax}\sin(bx) &= \frac{1}{2i}e^{\lambda x} + \frac{-1}{2i}e^{\bar{\lambda}x}. \end{aligned}$$

Hence $e^{ax}\cos(bx)$ and $e^{ax}\sin(bx)$ are also in W, and since $e^{\lambda x}$ and $e^{\bar{\lambda}x}$ are linear combinations of them, they span W and hence (since there are two of them), $\{e^{ax}\cos(bx), e^{ax}\sin(bx)\}$ is also a basis of W.

Thus in our basis $\mathcal{B}$ for $\mathrm{Ker}(\mathcal{L})$, we may replace the pair of functions $e^{\lambda x}, e^{\bar{\lambda}x}$ by the pair of functions $e^{ax}\cos(bx), e^{ax}\sin(bx)$ wherever it occurs.

Example 7.3.11. Let $\mathcal{L} = p(D) = (D^2 - 4D + 13)(D - 2)$. Then, by the quadratic formula, $D^2 - 4D + 13$ has roots $2 \pm 3i$, so that

$$p(D) = (D - (2 + 3i))(D - (2 - 3i))(D - 2).$$

Hence $\mathrm{Ker}(p(D))$ has basis $\{e^{(2+3i)x}, e^{(2-3i)x}, e^{2x}\}$, but then it also has basis $\{e^{2x}\cos(3x), e^{2x}\sin(3x), e^{2x}\}$ so $\mathcal{L}(f(x)) = 0$ has general solution $f(x) = c_1e^{2x}\cos(3x) + c_2e^{2x}\sin(3x) + c_3e^{2x}$. $\Diamond$

Finally, this method can also be used to solve nonhomogeneous equations $\mathcal{L}(f(x)) = g(x)$ when $\mathcal{L} = p(D)$ and there is also some polynomial $q(D)$ with $g(x) \in \mathrm{Ker}(q(D))$. For then we have

$$\begin{aligned} p(D)(f(x)) &= g(x), \\ p(D)q(D)(f(x)) &= q(D)(g(x)), \\ r(D) &= 0, \end{aligned}$$

where $r(D)$ is the polynomial $r(D) = p(D)q(D)$. This tells us the "form" of the answer but not the exact answer itself, as we lose information when we apply $q(D)$, but it is then only a little work to find the exact answer.

Example 7.3.12. (1) We wish to solve $(D^2 - 1)(f(x)) = 32xe^{-3x}$. We recognize that $(D + 3)^2(xe^{-3x}) = 0$ so we consider solutions of $(D^2 - 1)(D + 3)^2(f(x)) = 0$. Of course, $D^2 - 1 = (D - 1)(D + 1)$ so we see that a basis for this solution space is $\{e^x, e^{-x}, e^{-3x}, xe^{-3x}\}$. We look for a single solution (a "particular solution") of $(D^2 - 1)(f(x)) = xe^{-3x}$. Since there is no point in duplicating functions in $\mathrm{Ker}((D^2 - 1))$, we look for a solution of the form $f(x) = a_1e^{-3x} + a_2xe^{-3x}$. Then by explicit calculation we find

$$(D^2 - 1)(f(x)) = (8a_1 - 6a_2)e^{-3x} + 8a_2xe^{-3x} = 32xe^{-3x}$$

yielding the linear system

$$\begin{aligned} 8a_1 - 6a_2 &= 0, \\ 8a_2 &= 32, \end{aligned}$$

which we easily solve to find $a_1 = 3$, $a_2 = 4$, and so $f(x) = 3e^{-3x} + 4xe^{-3x}$. Then the general solution of $\mathcal{L}(f(x)) = g(x)$ is

$$f(x) = c_1e^x + c_2e^{-x} + 3e^{-3x} + 4xe^{-3x}.$$

(2) We wish to solve $(D^2+D)(f(x)) = e^{-x}$. We recognize that $(D+1)(e^{-x}) = 0$ so $(D^2 + D)(D + 1)(f(x)) = 0$. Of course, $D^2 + D = D(D + 1)$ so we see that a basis for the solution space is $\{1, e^{-x}, xe^{-x}\}$. Again there is no point in duplicating functions in $\mathrm{Ker}(D(D + 1))$, so we look for a solution of the form $f(x) = a_1xe^{-x}$. Then by explicit calculation we find

$$(D^2 + D)(a_1xe^{-x}) = -a_1e^{-x} = e^{-x}$$

so $a_1 = -1$ and $f(x) = -xe^{-x}$ is a particular solution. Then the general solution of $(D^2 + D)(f(x)) = e^{-x}$ is

$$f(x) = c_1 + c_2e^{-x} - xe^{-x}.$$

$\Diamond$

Finally, we can combine the last two examples.

Example 7.3.13. Find the unique solution of $(D^2 - 1)(f(x)) = 32xe^{-3x}$ with $f(0) = 7$, $f'(0) = 9$.

Answer. We know $f(x) = c_1e^x + c_2e^{-x} + 3e^{-3x} + 4xe^{-3x}$, from which we easily compute $f'(x) = c_1e^x - c_2e^{-x} - 5e^{-3x} - 12xe^{-3x}$. Then $f(0) = 7$, $f'(0) = 9$ gives the linear system

$$\begin{aligned} c_1 + c_2 + 3 &= 7, \\ c_1 - c_2 - 5 &= 9, \end{aligned} \qquad \text{or} \qquad \begin{aligned} c_1 + c_2 &= 4, \\ c_1 - c_2 &= 14, \end{aligned}$$

which we easily solve to find $c_1 = 9$, $c_2 = -5$ and so

$$f(x) = 9e^x - 5e^{-x} + 3e^{-3x} + 4xe^{-3x}.$$

$\Diamond$

7.4. Diagonalizable linear transformations

In this section we consider the simplest sort of linear transformations, the diagonalizable ones. These are an important type of linear transformation, and it is worthwhile to study them separately, before moving to the general situation.

We begin with some illustrative examples, but first a couple of definitions.

Definition 7.4.1. Let λ be an eigenvalue of $\mathcal{T}$. The *algebraic multiplicity* $\text{alg-mult}(\lambda)$ of λ is the highest power of $x - \lambda$ that divides the characteristic polynomial $c_{\mathcal{T}}(x)$. $\Diamond$

Definition 7.4.2. Let λ be an eigenvalue of $\mathcal{T}$. The *geometric multiplicity* $\text{geom-mult}(\lambda)$ of λ is the dimension of associated eigenspace $E_\lambda = \mathrm{Ker}(\lambda\mathcal{I} - \mathcal{T})$. $\Diamond$

The word *multiplicity* by itself is used to mean algebraic multiplicity.

In these examples, we simply give the characteristic polynomial, as it can be messy to compute. We also remember that we know (and have had plenty of practice) how to find bases for the nullspace of matrices—via row reduction—so we simply give the answers. To have everything in the same place, we include information about the minimal polynomial, though we don't yet know how to find it.

Example 7.4.3. (1) Let

$$A = \begin{bmatrix} 1 & 4 & -2 \\ -10 & 6 & 0 \\ -14 & 11 & -1 \end{bmatrix} \quad \text{with} \quad c_A(x) = (x-1)(x-2)(x-3).$$

Thus the eigenvalues are $\lambda = 1$, $\lambda = 2$, and $\lambda = 3$. To find the respective eigenspaces we row-reduce $A - I$, $A - 2I$, and $A - 3I$, respectively. We find:

Eigenvalue	alg-mult	geom-mult	basis for eigenspace
1	1	1	$\left\{ \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix} \right\}$
2	1	1	$\left\{ \begin{bmatrix} 2 \\ 5 \\ 9 \end{bmatrix} \right\}$
3	1	1	$\left\{ \begin{bmatrix} 3 \\ 10 \\ 17 \end{bmatrix} \right\}$

The minimal polynomial $m_A(x) = (x-1)(x-2)(x-3)$.

(2) Let

$$A = \begin{bmatrix} -3 & 4 & -2 \\ -15 & 14 & -6 \\ -20 & 16 & -6 \end{bmatrix} \quad \text{with} \quad c_A(x) = (x-1)(x-2)^2.$$

Then we find:

Eigenvalue	alg-mult	geom-mult	basis for eigenspace
1	1	1	$\left\{ \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \right\}$
2	2	2	$\left\{ \begin{bmatrix} 2 \\ 0 \\ -5 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} \right\}$

The minimal polynomial $m_A(x) = (x-1)(x-2)$.

(3) Let

$$A = \begin{bmatrix} -12 & 1 & 2 \\ -44 & 4 & 7 \\ -72 & 4 & 13 \end{bmatrix} \quad \text{with} \quad c_A(x) = (x-1)(x-2)^2.$$

Then we find:

Eigenvalue	alg-mult	geom-mult	basis for eigenspace
1	1	1	$\left\{\begin{bmatrix}1\\3\\5\end{bmatrix}\right\}$
2	2	1	$\left\{\begin{bmatrix}3\\10\\16\end{bmatrix}\right\}$

The minimal polynomial $m_A(x) = (x-1)(x-2)^2$. ◊

Lemma 7.4.4. *Let λ be an eigenvalue of the linear transformation $\mathcal{T}$ (or the matrix A). Then*

$$1 \leq \text{geom-mult}(\lambda) \leq \text{alg-mult}(\lambda).$$

In particular, if $\text{alg-mult}(\lambda) = 1$, *then* $\text{geom-mult}(\lambda) = 1$.

Proof. Since λ is an eigenvalue of $\mathcal{T}$, the eigenspace $E_\lambda \neq \{0\}$, so $1 \leq \dim(E_\lambda) = \text{geom-mult}(\lambda)$.

Let $g = \text{geom-mult}(\lambda)$, and let $\{v_1, \dots, v_g\}$ be a basis of E_λ. Extend this set to a basis $\mathcal{B} = \{v_1, \dots, v_g, v_{g+1}, \dots, v_n\}$ of V. Now $\mathcal{T}(v_i) = \lambda v_i$ for $i = 1, \dots, g$, so

$$[\mathcal{T}]_{\mathcal{B}} = \left[\begin{array}{ccc|c} \lambda & & 0 & \\ & \ddots & & B \\ 0 & & \lambda & \\ & 0 & & D \end{array}\right],$$

where there are g λ's along the diagonal, and B and D are unknown. But then

$$[x\mathcal{I} - \mathcal{T}]_{\mathcal{B}} = \left[\begin{array}{ccc|c} x-\lambda & & 0 & \\ & \ddots & & -B \\ 0 & & x-\lambda & \\ & 0 & & xI - D \end{array}\right]$$

and so, consecutively expanding by minors of the first g columns, we see

$$c_{\mathcal{T}}(x) = (x-\lambda)^g \det(xI - D)$$

so $\text{alg-mult}(\lambda) \geq g$, i.e., $\text{geom-mult}(\lambda) \leq \text{alg-mult}(\lambda)$.

We have phrased this in terms of $\mathcal{T}$, but the same proof works for the matrix A by taking $\mathcal{T} = \mathcal{T}_A$. □

Before proceeding any further, there is a subtle point about polynomials we need to address.

Let $\mathbb{F} = \mathbb{Q}$, and let $A = \begin{bmatrix} 0 & 1 \\ 4 & 0 \end{bmatrix}$. Then $c_A(x) = x^2 - 4 = (x-2)(x+2)$ so A has eigenvalues $\lambda = 2$ and $\lambda = -2$. Fine.

But now let $\mathbb{F} = \mathbb{Q}$ and $A = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$. Then $c_A(x) = x^2 - 2$ and this polynomial has no roots in $\mathbb{Q}$. Thus this matrix has no eigenvalues in $\mathbb{Q}$. However, if $\mathbb{F} = \mathbb{R}$, then $c_A(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ so A has eigenvalues $\lambda = \sqrt{2}$ and $\lambda = -\sqrt{2}$. Fine.

But now let $\mathbb{F} = \mathbb{R}$ and $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Then $c_A(x) = x^2 + 1$ and this polynomial has no roots in $\mathbb{R}$. Thus this matrix has no eigenvalues in $\mathbb{R}$. However, if $\mathbb{F} = \mathbb{C}$, then $c_A(x) = x^2 + 1 = (x + i)(x - i)$ so A has eigenvalues $\lambda = i$ and $\lambda = -i$. Fine.

These examples illustrate the point that whether a polynomial has roots in $\mathbb{F}$ (and hence whether a linear transformation has eigenvalues in $\mathbb{F}$) depends on the field $\mathbb{F}$.

In this regard we have the fundamental theorem of algebra.

Theorem 7.4.5 (Fundamental theorem of algebra)**.** *Let $p(x) = a_n x^n + \cdots + a_0$ be any polynomial with complex coefficients. Then $p(x)$ has n roots in $\mathbb{C}$ (counting multiplicities) or equivalently $p(x)$ splits into a product of linear factors in $\mathbb{C}$,*

$$p(x) = a_n(x - r_1) \cdots (x - r_n)$$

for some complex numbers $r_1, \ldots, r_n$.

This property is so important we give it a name.

Definition 7.4.6. A field $\mathbb{E}$ is *algebraically closed* if every polynomial $p(x)$ with coefficients in $\mathbb{E}$ splits into a product of linear factors in $\mathbb{E}$. $\Diamond$

Thus in this language the fundamental theorem of algebra simply states that the field of complex numbers $\mathbb{C}$ is algebraically closed.

We also have the following theorem.

Theorem 7.4.7. *Any field $\mathbb{F}$ is contained in an algebraically closed field $\mathbb{E}$.*

For example, $\mathbb{Q} \subseteq \mathbb{C}$, $\mathbb{R} \subseteq \mathbb{C}$, and of course $\mathbb{C} \subseteq \mathbb{C}$.

Now consider a particular linear transformation $\mathcal{T}$ or a matrix A. We saw several examples (Example 7.4.3) where c_A splits into a product of linear factors in $\mathbb{Q}$, and so we were able to find eigenvalues and eigenvectors. But if not, there may not be enough eigenvalues—indeed, there may be none—and then we are dead in the water. Thus we will want to have:

Hypothesis (S). *The characteristic polynomial $c_{\mathcal{T}}$ (or $c_A(x)$) splits into a product of linear factors in $\mathbb{F}$. This hypothesis is automatically satisfied if $\mathbb{F}$ is algebraically closed, for example, if $\mathbb{F} = \mathbb{C}$.*

(The "S" in Hypothesis (S) stands for "splits".)

Observe that if $c_{\mathcal{T}}(x)$ (or $c_A(x)$) satisfies Hypothesis (S), we may (and usually will) gather like terms together and write this polynomial as

$$(x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k} \quad \text{with } \lambda_1, \ldots, \lambda_k \text{ distinct.}$$

Then $\lambda_1, \ldots, \lambda_k$ are the eigenvalues of $\mathcal{T}$ (or of A), and $e_1, \ldots, e_k$ are their algebraic multiplicities.

We can now define and completely characterize diagonalizable linear transformations.

Definition 7.4.8. (1) Let $\mathcal{T}: V \to V$ be a linear transformation, with V an n-dimensional vector space over field $\mathbb{F}$. Then $\mathcal{T}$ is *diagonalizable* if V has a basis $\mathcal{B}$ in which the matrix $[\mathcal{T}]_{\mathcal{B}}$ is a diagonal matrix.

(2) Let A be an n-by-n matrix with coefficients in $\mathbb{F}$. A is *diagonalizable* if it is similar over $\mathbb{F}$ to a diagonal matrix, i.e., if there is an invertible matrix P with entries in $\mathbb{F}$ such that $P^{-1}AP$ is a diagonal matrix. $\Diamond$

Theorem 7.4.9. (1) *Let $\mathcal{T}: V \to V$ be a linear transformation, with V an n-dimensional vector space over field $\mathbb{F}$. Then $\mathcal{T}$ is diagonalizable if and only if V has a basis $\mathcal{B}$ of eigenvectors of $\mathcal{T}$.*

(2) *If $\mathcal{T}$ does not satisfy Hypothesis* (S), *$\mathcal{T}$ is not diagonalizable.*

(3) *The following are equivalent*:

(a) *$\mathcal{T}$ is diagonalizable.*

(b) *The sum of the geometric multiplicities of the eigenvalues of $\mathcal{T}$ is $n = \dim V$.*

(c) *$\mathcal{T}$ satisfies Hypothesis* (S) *and for each eigenvalue λ of $\mathcal{T}$,*

$$\text{geom-mult}(\lambda) = \text{alg-mult}(\lambda).$$

(d) *$\mathcal{T}$ satisfies Hypothesis* (S) *and for each eigenvalue λ of $\mathcal{T}$, every generalized eigenvector of $\mathcal{T}$ associated to λ has index* 1, *i.e., is an eigenvector of $\mathcal{T}$ associated to λ, or, equivalently, the generalized eigenspace E_λ^∞ is just the eigenspace E_λ.*

(e) *The minimal polynomial $m_{\mathcal{T}}(x)$ is a product of distinct linear factors.*

Remark 7.4.10. Note that Hypothesis (S) was not part of the assumptions in (b) or (e), so, by (2), we see that if $\mathcal{T}$ satisfies (b) or (e), it automatically satisfies Hypothesis (S). $\Diamond$

Before proving this theorem, let us point out an important special case.

Corollary 7.4.11. *Let $\mathcal{T}: V \to V$ be a linear transformation and suppose $c_{\mathcal{T}}(x) = (x - \lambda_1) \cdots (x - \lambda_n)$ with $\lambda_1, \ldots, \lambda_n$ distinct. Then $\mathcal{T}$ is diagonalizable.*

Proof. In this case $c_{\mathcal{T}}(x)$ satisfies Hypothesis (S), by assumption, and furthermore, by assumption, every eigenvalue has algebraic multiplicity 1. Then, by Lemma 7.4.4, every eigenvalue has geometric multiplicity 1 as well. Thus (c) is true, and hence (a) is true. $\Box$

Proof of Theorem 7.4.9. (1) Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis of V consisting of eigenvectors of $\mathcal{T}$, and let $r_1, \ldots, r_n$ be the (not necessarily distinct) associated eigenvalues. Then $\mathcal{T}(v_i) = r_i v_i$ so $[\mathcal{T}(v_i)]_{\mathcal{B}} = r_i e_i$. Then

$$[\mathcal{T}]_{\mathcal{B}} = \big[[\mathcal{T}(v_1)]_{\mathcal{B}} \big| \ldots \big| [\mathcal{T}(v_n)]_{\mathcal{B}}\big] = \begin{bmatrix} r_1 & & 0 & & 0 \\ 0 & & \vdots & & 0 \\ \vdots & \ldots & r_i & \ldots & \vdots \\ & & \vdots & & \\ 0 & & 0 & & r_n \end{bmatrix}$$

is diagonal. Conversely, if $[\mathcal{T}]_{\mathcal{B}}$ has this form, then for each i, $[\mathcal{T}(v_i)]_{\mathcal{B}} = r_i e_i$ so $\mathcal{T}(v_i) = r_i v_i$ and v_i is an eigenvector.

(2) We may calculate $\mathcal{T}$ by using any basis. Assume $\mathcal{T}$ is diagonalizable and choose a basis $\mathcal{B}$ of eigenvectors. Then

$$\begin{aligned} c_{\mathcal{T}}(x) = \det([x\mathcal{I} - \mathcal{T}]_{\mathcal{B}}) &= \det\left(\begin{bmatrix} x - r_1 & & & & \\ & \ddots & & & \\ & & x - r_i & & \\ & & & \ddots & \\ & & & & x - r_n \end{bmatrix}\right) \\ &= (x - r_1)\cdots(x - r_n) \end{aligned}$$

and $\mathcal{T}$ satisfies Hypothesis (S). Hence if $\mathcal{T}$ does not satisfy Hypothesis (S), $\mathcal{T}$ cannot be diagonalizable.

(3) Assume $\mathcal{T}$ is diagonalizable, i.e., that (a) is true. Then we can easily see that (b) through (e) are true, as follows. Rewrite $c_{\mathcal{T}}(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k}$ with $\lambda_1, \ldots, \lambda_k$ distinct. Then, reordering the basis $\mathcal{B}$ if necessary, we see that

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & \lambda_1 & & & & \\ & & & \ddots & & & \\ & & & & \lambda_k & & \\ & & & & & \ddots & \\ & & & & & & \lambda_k \end{bmatrix},$$

where there are e_1 entries of λ_1, $\ldots$, e_k entries of λ_k.

Then for each i, $M_i = [\mathcal{T} - \lambda_i \mathcal{I}]_{\mathcal{B}}$ is a diagonal matrix with e_i diagonal entries equal to 0 and all the other diagonal entries nonzero, so $\operatorname{Ker}(\mathcal{T} - \lambda_i \mathcal{I})$ has dimension e_i. But that says the geometric multiplicity of λ_i is equal to e_i, which is its algebraic multiplicity, so (c) is true. Also, $n = e_1 + \cdots + e_k$ (as $c_{\mathcal{T}}(x)$ has degree n), and this is the sum of the geometric multiplicities, so (b) is also true. Furthermore, for each i every power M_i^j of M_i also has the same e_i diagonal entries equal to 0 and all the other diagonal entries not equal to 0, so $\operatorname{Ker}((\mathcal{T} - \lambda_i \mathcal{I})^j) = \operatorname{Ker}(\mathcal{T} - \lambda_i \mathcal{I})$ for every j, and (d) is true.

Finally, the product $M_1 \cdots M_k = 0$ (and no proper subproduct is 0), i.e., $(\mathcal{T} - \lambda_1 \mathcal{I}) \cdots (\mathcal{T} - \lambda_k \mathcal{I}) = 0$, and $m_{\mathcal{T}}(x) = (x - \lambda_1) \cdots (x - \lambda_k)$ is a product of distinct linear factors, so (e) is true.

Now suppose (b) is true. Let W_i be the eigenspace associated to the eigenvalue λ_i, and let W_i have dimension f_i. Choose a basis $\mathcal{B}_i$ for W_i. Of course, $\mathcal{B}_i$ has f_i elements. Since W_i is an eigenspace, each vector in $\mathcal{B}_i$ is an eigenvector. Then, by Corollary 7.2.5(2), $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$ is linearly independent. But $f_1 + \cdots + f_k = n$, so $\mathcal{B}$ is a basis of V. Thus V has a basis of eigenvectors, so $\mathcal{B}$ is diagonalizable, and (a) is true.

Suppose (c) is true, and let W_i be as in (b). Then by hypothesis $f_i = e_i$, so $f_1 + \cdots + f_k = e_1 + \cdots + e_k = n$, and hence (b) is true, and then (a) is true.

Suppose (d) is true. Then $c_{\mathcal{T}}(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k}$, and $c_{\mathcal{T}}(x)$ has degree n, so $e_1 + \cdots + e_k = n$. We now use a result we will prove later: if λ is an eigenvalue of $\mathcal{T}$, then the algebraic multiplicity of λ is equal to the dimension of the generalized eigenspace of λ (Corollary 7.5.3), i.e., $e_i = \dim E^{\infty}_{\lambda_i}$ for each i.

Thus $\dim E^{\infty}_{\lambda_1} + \cdots + \dim E^{\infty}_{\lambda_k} = n$. But we are also assuming that $E^{\infty}_{\lambda_i} = E_{\lambda_i}$ for each i, so $\dim E^{\infty}_{\lambda_i} = \dim E_{\lambda_i} = \text{geom-mult}(\lambda_i)$ for each i, so $\sum \text{geom-mult}(\lambda_i) = n$ and (b) is true, and hence (a) is true.

Finally, suppose (e) is true. We are assuming that $m_{\mathcal{T}}(x)$ is a product of linear factors, $m_{\mathcal{T}}(x) = (x - \lambda_1) \cdots (x - \lambda_k)$. We again use a result we will prove later: the polynomials $m_{\mathcal{T}}(x)$ and $c_{\mathcal{T}}(x)$ have the same irreducible factors (Theorem 7.5.9(2)). Thus $c_{\mathcal{T}}(x)$ is a product of linear factors, $c_{\mathcal{T}}(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k}$, i.e., $\mathcal{T}$ satisfies Hypothesis (S).

Also, let λ_i be any eigenvalue of $\mathcal{T}$, and let v be any associated generalized eigenvector, of index h. Then the $\mathcal{T}$-annihilator of v is $m_{\mathcal{T},v}(x) = (x - \lambda_i)^h$. But we know that $m_{\mathcal{T},v}(x)$ divides the minimal polynomial $m_{\mathcal{T}}(x) = (x - \lambda_1) \cdots (x - \lambda_k)$, so we must have $h = 1$. That is, every generalized eigenvector is in fact an eigenvector. Thus (d) is true, and hence (a) is true, completing the proof. □

Let's see how to concretely express this in terms of matrices.

Corollary 7.4.12. *Let A be an n-by-n matrix and suppose that $c_A = (x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k}$. Suppose further that for each i, the dimension of the eigenspace W_i associated to the eigenvalue λ_i is equal to e_i. Then A is similar to the diagonal matrix*

$$D = \begin{bmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & \lambda_1 & & & & \\ & & & \ddots & & & \\ & & & & \lambda_k & & \\ & & & & & \ddots & \\ & & & & & & \lambda_k \end{bmatrix},$$

where there are e_i entries of λ_i for each i.

More precisely, let $\mathcal{B}_i = \{v^i_1, \ldots, v^i_{e_i}\}$ be any basis of W_i for each i, and let P be the matrix

$$P = [v^1_1 | \ldots | v^1_{e_1} | \ldots | v^k_1 | \ldots | v^k_{e_k}].$$

Then

$$D = P^{-1}AP \quad (\textit{or, equivalently, } A = PDP^{-1}).$$

Proof. Let $\mathcal{T} = \mathcal{T}_A$. Then we are assuming (c) of Theorem 7.4.9, so we conclude that $\mathcal{T}$ is diagonalizable, i.e., there is a basis $\mathcal{B}$ in which $[\mathcal{T}]_{\mathcal{B}}$ is diagonal. But the proof of that theorem shows that that diagonal matrix is exactly the matrix D. Thus we see that A is similar to D.

More precisely, that proof shows that we may choose $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$. Hence we have (Theorem 5.4.6, Corollary 5.4.7)

$$[\mathcal{T}]_{\mathcal{B}} = P_{\mathcal{B} \leftarrow \mathcal{E}} [\mathcal{T}]_{\mathcal{E}} P_{\mathcal{E} \leftarrow \mathcal{B}}$$

i.e.

$$D = P^{-1} A P$$

where $P = P_{\mathcal{E} \leftarrow \mathcal{B}}$ is the change of basis matrix from $\mathcal{B}$ to $\mathcal{E}$. But we also know that (Theorem 5.3.11, Example 5.3.5) P is the matrix whose columns are the vectors in $\mathcal{B}$. $\square$

Example 7.4.13. (1) The matrix A of Example 7.4.3(1) satisfies (c), so is diagonalizable. Furthermore, given the table there, we see

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 10 \\ 4 & 9 & 17 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 4 & -2 \\ -10 & 6 & 0 \\ -14 & 11 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 10 \\ 4 & 9 & 17 \end{bmatrix}.$$

(2) The matrix A of Example 7.4.3(2) satisfies (c), so is diagonalizable. Furthermore, given the table there, we see

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 0 \\ 3 & 0 & 1 \\ 4 & -5 & 2 \end{bmatrix}^{-1} \begin{bmatrix} -3 & 4 & -2 \\ -15 & 14 & -6 \\ -20 & 16 & -6 \end{bmatrix} \begin{bmatrix} 1 & 2 & 0 \\ 3 & 0 & 1 \\ 4 & -5 & 2 \end{bmatrix}. \qquad \Diamond$$

Note that our theory gives these concrete numerical results with no further computations at all, once we have found the eigenvalues and bases for the eigenspaces. Of course, you can check these claims by direct computation, if you wish. It is tedious to check $D = P^{-1}AP$ directly, as that involves computing P^{-1}, but (assuming that P is invertible) this matrix equation is equivalent to the matrix equation $PD = AP$, which is much easier to check.

7.5. Structural results

In this section we prove a number of structural results about linear transformations. Among them is the famous Cayley-Hamilton theorem.

Not only are these results a useful intermediate step toward the analysis of general linear transformations, but they provide valuable information in themselves.

We have algebraic invariants of a linear transformation—the minimal and characteristic polynomials. We have geometric invariants—eigenvalues and (generalized) eigenvectors. We have already seen that they are closely connected. We begin with some results that make the connections even more precise.

Lemma 7.5.1. *Let V be a finite-dimensional vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. Let λ be an eigenvalue of $\mathcal{T}$. Then there is a smallest positive integer f such that $E_\lambda^\infty = E_\lambda^f$. This f is the smallest positive integer such that $\dim(E_\lambda^f) = \dim(E_\lambda^{f+1})$. Furthermore, this integer f is the exponent of $(x - \lambda)$ in the minimal polynomial $m_{\mathcal{T}}(x)$ of $\mathcal{T}$.*

This lemma is useful both ways: we can compute $\dim(E_\lambda^1), \dim(E_\lambda^2), \ldots,$ and as soon as this sequence of dimensions becomes constant, we know we have found f, the exponent of $(x - \lambda)$ in $m_{\mathcal{T}}(x)$. On the other hand, if we have found the minimal polynomial $m_{\mathcal{T}}(x)$, then we know what the value of f is, so we know the smallest integer f with $E_\lambda^\infty = E_\lambda^f$.

Proof. We know that $E_\lambda^1 \subseteq E_\lambda^2 \subseteq \cdots \subseteq E_\lambda^f \subseteq E_\lambda^{f+1} \subseteq \cdots \subseteq V$ so we have $\dim(E_\lambda^1) \leq \dim(E_\lambda^2) \leq \cdots \leq \dim(E_\lambda^f) \leq \dim(E_\lambda^{f+1}) \leq \cdots \leq \dim(V)$. Since $\dim(V)$ is finite, this sequence of dimensions cannot always be increasing, so it must pause somewhere.

Let it pause for the first time at f, so

$$\dim(E_\lambda^{f-1}) < \dim(E_\lambda^f) = \dim(E_\lambda^{f+1}).$$

Then E_λ^{f-1} is a proper subspace of E_λ^f, so there is some generalized eigenvector of index f. On the other hand, since $\dim(E_\lambda^f) = \dim(E_\lambda^{f+1})$, we have that $E_\lambda^f = E_\lambda^{f+1}$. We show that in fact not only does it pause at f, it stops at f. We show that $E_\lambda^f = E_\lambda^{f+1} = E_\lambda^{f+2} = \cdots$ and so $E_\lambda^\infty = E_\lambda^f$.

Suppose $v \in E_\lambda^{f+2}$. Then $(\mathcal{T} - \lambda\mathcal{I})^{f+2}(v) = 0$. Set $w = (\mathcal{T} - \lambda\mathcal{I})(v)$. Then $0 = (\mathcal{T} - \lambda\mathcal{I})^{f+2}(v) = (\mathcal{T} - \lambda\mathcal{I})^{f+1}(\mathcal{T} - \lambda\mathcal{I})(v) = (\mathcal{T} - \lambda\mathcal{I})^{f+1}(w)$, and so $w \in E_\lambda^{f+1}$. But $E_\lambda^{f+1} = E_\lambda^f$, so in fact $w \in E_\lambda^f$.

But that means $(\mathcal{T} - \lambda\mathcal{I})^f(w) = 0$ so $(\mathcal{T} - \lambda\mathcal{I})^{f+1}(v) = (\mathcal{T} - \lambda\mathcal{I})^f(\mathcal{T} - \lambda\mathcal{I})(v) = (\mathcal{T} - \lambda\mathcal{I})^f(w) = 0$, so in fact $v \in E_\lambda^{f+1}$, and so $E_\lambda^{f+2} = E_\lambda^{f+1}$. Repeating this argument starting with $v \in E_\lambda^{f+3}$ shows $E_\lambda^{f+3} = E_\lambda^{f+2}$, etc.

Now we have to relate this to the minimal polynomial. Suppose the exponent of $x - \lambda$ in $m_{\mathcal{T}}(x)$ is j, i.e., $(x - \lambda)^j$ is a factor of $m_{\mathcal{T}}(x)$ but $(x - \lambda)^{j+1}$ is not. We want to show that $j = f$.

On the one hand, we know there is some generalized eigenvector v of index f associated to λ, so its $\mathcal{T}$-annihilator is $m_{\mathcal{T},v}(x) = (x - \lambda)^f$. Now $m_{\mathcal{T}}(\mathcal{T}) = 0$, so in particular $m_{\mathcal{T}}(\mathcal{T})(v) = 0$. But we know that $m_{\mathcal{T},v}(x)$ divides any polynomial $p(x)$ for which $p(\mathcal{T})(v) = 0$, so $(x - \lambda)^f$ divides $m_{\mathcal{T}}(x)$ and so $j \geq f$.

On the other hand, we have seen how to find $m_{\mathcal{T}}(x)$. Choose any basis $\{v_1, \ldots, v_k\}$ of V, and then

$$m_{\mathcal{T}}(x) = \operatorname{lcm}(m_{\mathcal{T},v_1}(x), m_{\mathcal{T},v_2}(x), \ldots, m_{\mathcal{T},v_k}(x)).$$

So if $m_{\mathcal{T}}(x)$ has a factor $(x - \lambda)^j$, there must be some v_i with $m_{\mathcal{T},v_i}(x)$ having a factor of $(x - \lambda)^j$. Write $m_{\mathcal{T},v_i}(x) = (x - \lambda)^j q(x)$. Let $w = q(\mathcal{T})(v_i)$. Then

$$(\mathcal{T} - \lambda\mathcal{I})^j(w) = (\mathcal{T} - \lambda\mathcal{I})^j q(\mathcal{T})(v_i) = m_{\mathcal{T},v_i}(v_i) = 0$$

but

$$(\mathcal{T} - \lambda\mathcal{I})^{j-1}(w) = (\mathcal{T} - \lambda\mathcal{I})^{j-1} q(\mathcal{T})(v_i) \neq 0$$

as the polynomial $(x - \lambda)^{j-1}$ has degree less than that of $m_{\mathcal{T},v_i}(x)$. Hence w is a generalized eigenvector of index j associated to the eigenvalue λ, and so $f \geq j$. Since $j \leq f$ and $f \leq j$, we must have $j = f$. $\square$

For our next step, we can find the geometric meaning of the algebraic multiplicity. We shall derive it from the following result, which we shall use in a different (but related) context below.

Lemma 7.5.2. *Let $\mathcal{T}\colon V \to V$ be a linear transformation. Let λ be an eigenvalue of $\mathcal{T}$ with algebraic multiplicity e. Then V has a basis $\mathcal{B}$ in which*

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} A & * \\ 0 & D \end{bmatrix},$$

where A is an e-by-e upper triangular matrix all of whose diagonal entries are equal to λ, and D is an $(n-e)$-by-$(n-e)$ matrix that does not have λ as an eigenvalue.

Proof. By induction on n. If $n = 1$, $[\mathcal{T}]_{\mathcal{B}} = [\lambda]$ and there is nothing to prove.

Assume true for $n-1$ and let V have dimension n. Choose an eigenvector v_1 associated to the eigenvalue λ, and extend v_1 to a basis $\mathcal{B}' = \{v_1, \dots, v_n\}$ of V. Then

$$M = [\mathcal{T}]_{\mathcal{B}'} = \begin{bmatrix} \lambda & * & \\ 0 & & \\ \vdots & D_1 & \\ 0 & & \end{bmatrix}$$

and then we compute that

$$c_{\mathcal{T}}(x) = c_M(x) = (x-\lambda)\det(xI - D_1),$$

and so D_1 is an $(n-1)$-by-$(n-1)$ matrix having λ as an eigenvalue of algebraic multiplicity $e-1$. If $e = 1$, we are done: M is of the required form (as then D_1 does not have λ as an eigenvalue).

Let W be the subspace of V spanned by $\mathcal{B}_1' = \{v_1\}$, and let U be the subspace of V spanned by $\mathcal{B}_2' = \{v_2, \dots, v_n\}$, so that $V = W \oplus U$. While $\mathcal{T}(W) \subseteq W$, it is not necessarily the case that $\mathcal{T}(U) \subseteq U$. (It would be the case if the entries $*$ were all zero, but that may well not be the case.) However, we do have the linear transformation $\mathcal{P}\colon V \to U$ defined by $\mathcal{P}(v_1) = 0$ and $\mathcal{P}(v_i) = v_i$ for $i > 1$; more simply $\mathcal{P}(c_1v_1 + c_2v_2 + \dots + c_nv_n) = c_2v_2 + \dots + c_nv_n$. Let $\mathcal{S}$ be the composition $\mathcal{S} = \mathcal{P}\mathcal{T}\colon U \to U$, so that $[\mathcal{S}]_{\mathcal{B}_2'} = D_1$. Then by induction U has a basis $\mathcal{B}_2$ in which

$$[\mathcal{S}]_{\mathcal{B}_2} = \begin{bmatrix} A' & * \\ 0 & D \end{bmatrix},$$

where A' is an $(e-1)$-by-$(e-1)$ upper triangular matrix with all diagonal entries equal to λ, and D does not have λ as an eigenvalue.

Now let $\mathcal{B} = \mathcal{B}_1' \cup \mathcal{B}_2$ and note that $\mathcal{B}$ is a basis of V (Theorem 3.4.24). Let $M = [\mathcal{T}]_{\mathcal{B}}$.

Then

$$M = \big[[\mathcal{T}(v)]_{\mathcal{B}} \mid [\mathcal{T}(u_2)]_{\mathcal{B}} \mid \dots \mid [\mathcal{T}(u_n)]_{\mathcal{B}}\big],$$

where $\mathcal{B}_2 = \{u_2, \dots, u_n\}$. We still have $\mathcal{T}(v_1) = \lambda v_1$. For each $i = 2, \dots, e$, we have, since A' is upper triangular with diagonal entries equal to λ, $\mathcal{S}(u_i) = c_2u_2 + \dots + c_{i-1}u_{i-1} + \lambda u_i$ for some unknown $c_2, \dots, c_{i-1}$. But $\mathcal{S} = \mathcal{P}\mathcal{T}$ so that says $\mathcal{T}(u_i) = c_1u_1 + c_2u_2 + \dots + c_{i-1}u_{i-1} + \lambda u_i$, where c_1 is unknown as well. But that says $[\mathcal{T}(u_i)]_{\mathcal{B}}$ is a vector with unknown entries in positions 1 through $i-1$,

λ in position i, and 0's in positions $i+1, \dots, n$, i.e., the first i columns of $[\mathcal{T}]_\mathcal{B}$ are of the form

$$\begin{bmatrix} \lambda & * & * & & * \\ 0 & \lambda & * & & * \\ 0 & 0 & \lambda & & \vdots \\ \vdots & \vdots & \vdots & \dots & \lambda \\ & & & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix} = \begin{bmatrix} A \\ \\ 0 \\ \end{bmatrix}$$

as claimed. □

Corollary 7.5.3. *Let $\mathcal{T} \colon V \to V$ be a linear transformation. Let λ be an eigenvalue of $\mathcal{T}$ with algebraic multiplicity e. Then*

(1) *$E_\lambda^e = E_\lambda^\infty$, so that every generalized eigenvector associated to λ has index at most e; and*

(2) *$e = \dim E_\lambda^\infty$, i.e., the algebraic multiplicity of the eigenvalue λ is equal to the dimension of its associated generalized eigenspace.*

Proof. Choose a basis $\mathcal{B}$ of V with $[\mathcal{T}]_\mathcal{B}$ as in the last lemma. Then

$$M = [\mathcal{T} - \lambda\mathcal{I}]_\mathcal{B} = \begin{bmatrix} N & * \\ 0 & F \end{bmatrix},$$

where N is an e-by-e triangular matrix with all of its diagonal entries equal to 0, and $F = D - \lambda I$. Note that F is invertible because λ is *not* an eigenvalue of F. (The characteristic polynomial of D does *not* have λ as a root, so $\det(\lambda I - D) \neq 0$ and so this matrix is invertible.)

Now it is easy to compute that if N is an e-by-e upper triangular matrix with all of its entries equal to 0, then $N^e = 0$. Thus we see

$$M^e = \begin{bmatrix} 0 & * \\ 0 & F^e \end{bmatrix}$$

and since F is invertible, so is F^e, so $\mathrm{Null}(M^e)$ has dimension e. But in fact for any $j \geq e$ we have

$$M^j = \begin{bmatrix} 0 & * \\ 0 & F^j \end{bmatrix}$$

and so $\mathrm{Null}(M^j) = \mathrm{Null}(M)$ for any $j \geq e$. Thus

$$E_\lambda^e = E_\lambda^{e+1} = E_\lambda^{e+2} = \cdots \quad \text{so} \quad E_\lambda^\infty = E_\lambda^e$$

and $e = \dim E_\lambda^e = \dim E_\lambda^\infty$. □

Corollary 7.5.4. *Let $\mathcal{B} = \{v_1, \dots, v_e, v_{e+1}, \dots, v_n\}$ be a basis of $\mathcal{B}$ in which $[\mathcal{T}]_\mathcal{B}$ is as in Lemma 7.5.2. Then*

$$\mathcal{B}_1 = \{v_1, \dots, v_e\}$$

is a basis for the generalized eigenspace E_λ^∞ of $\mathcal{T}$ associated to the eigenvalue λ.

Proof. The proof of the last lemma not only showed that (in the notation of the proof) $E_\lambda^\infty = E_\lambda^e = \mathrm{Null}(M^e)$ had dimension e, it identified that subspace:

$$M^e = \begin{bmatrix} 0 & * \\ 0 & F^e \end{bmatrix}$$

with F invertible, so $\mathrm{Ker}(M) = \begin{bmatrix} c_1 \\ \vdots \\ c_e \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ for $c_1, \ldots, c_e \in \mathbb{F}$, i.e., $v \in E_\lambda$ if and only if $[v]_\mathcal{B} = \begin{bmatrix} c_1 \\ \vdots \\ c_e \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, i.e., $v \in E_\lambda$ if and only if $v = c_1 v_1 + \cdots + c_e v_e$ for some $c_1, \ldots, c_e \in \mathbb{F}$, and so $\mathcal{B}_1 = \{v_1, \ldots, v_e\}$ is a basis for $E_\lambda^e = E_\lambda^\infty$. □

Our goal is to find a basis $\mathcal{B}$ of V in which $[\mathcal{T}]_\mathcal{B}$ is as simple as possible. We will do this in stages. Here is a first stage.

Definition 7.5.5. Let V be a finite-dimensional $\mathbb{F}$-vector space, and let $\mathcal{T} \colon V \to V$ be a linear transformation. Then $\mathcal{T}$ is *triangularizable* over $\mathbb{F}$ if there is a basis $\mathcal{B}$ of V in which $B = [\mathcal{T}]_\mathcal{B}$ is upper triangular. An n-by-n matrix A with coefficients in $\mathbb{F}$ is *triangularizable* over $\mathbb{F}$ if there exists an invertible matrix P with coefficients in $\mathbb{F}$ such that the matrix $B = P^{-1}AP$ (which will then also have coefficients in $\mathbb{F}$) is upper triangular. ◇

Theorem 7.5.6. *The linear transformation $\mathcal{T}$ (or the matrix A) is triangularizable over $\mathbb{F}$ if and only if its characteristic polynomial $c_\mathcal{T}(x)$ (or $c_A(x)$) satisfies Hypothesis* (S).

Proof. First suppose $\mathcal{T}$ is triangularizable. Let $\mathcal{B}$ be a basis in which $B = [\mathcal{T}]_\mathcal{B}$ is upper triangular. Let $B = (b_{ij})$. Of course, all entries of B are in $\mathbb{F}$. But then $xI - B$ is also upper triangular with its diagonal entries being $x - b_{11}$, $x - b_{22}$, …, $x - b_{nn}$. But the determinant of an upper triangular matrix is the product of its diagonal entries, so $c_\mathcal{T}(x) = \det(xI - B) = (x - b_{11}) \cdots (x - b_{nn})$ is a product of linear factors, i.e., satisfies Hypothesis (S).

Conversely, suppose that $\mathcal{T}$ satisfies Hypothesis (S), so that $c_\mathcal{T}(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k}$ with $\lambda_1, \ldots, \lambda_k$ distinct.

First observe that if v is in the generalized eigenspace $E_{\lambda_i}^\infty$ of λ_i, so that $(\mathcal{T} - \lambda_i \mathcal{I})^f(v) = 0$ for some f, then

$$(\mathcal{T} - \lambda_i \mathcal{I})^f(\mathcal{T}(v)) = \mathcal{T}((\mathcal{T} - \lambda_i \mathcal{I})^f(v)) = \mathcal{T}(0) = 0,$$

so that $\mathcal{T}(v)$ is in $E_{\lambda_i}^\infty$ as well.

Now apply Lemma 7.5.2 successively, first with $\lambda = \lambda_1$ and $e = e_1$ to get a basis $\mathcal{B}_1$ of the generalized eigenspace $E^\infty_{\lambda_1}$ of λ_1 (by Corollary 7.5.4), then with $\lambda = \lambda_2$ and $e = e_2$ to get a basis $\mathcal{B}_2$ of the generalized eigenspace $E^\infty_{\lambda_2}$ of λ_2, etc. Thus we obtain $\mathcal{B}_1, \dots, \mathcal{B}_k$.

Each $\mathcal{B}_i$ is linearly independent and so we see from Corollary 7.2.5(2) that $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$ is linearly independent as well. But $\mathcal{B}$ has $e_1 + \cdots + e_k = n$ elements, so we conclude that $\mathcal{B}$ is a basis of V. Then

$$[\mathcal{T}]_\mathcal{B} = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}$$

with $A_1, \dots, A_k$ upper triangular matrices. □

Examining this proof, we see not only did it show that if $c_\mathcal{T}(x)$ satisfies Hypothesis (S), then $\mathcal{T}$ is triangularizable, but in fact it gave more precise information. We record that information.

Corollary 7.5.7. *Let $\mathcal{T}\colon V \to V$ be a linear transformation and suppose that $\mathcal{T}$ satisfies Hypothesis* (S). *Write $c_\mathcal{T}(x)$ as $c_\mathcal{T}(x) = (x-\lambda_1)^{e_1} \cdots (x-\lambda_k)^{e_k}$ with $\lambda_1, \dots, \lambda_k$ distinct. Then*

(1) *V is the direct sum of the generalized eigenspaces*

$$V = E^\infty_{\lambda_1} \oplus \cdots \oplus E^\infty_{\lambda_k}$$

and each of these subspaces is invariant under $\mathcal{T}$, i.e., $\mathcal{T}(E^\infty_{\lambda_i}) \subseteq E^\infty_{\lambda_i}$ for each i.

(2) *V has a basis $\mathcal{B}$ in which*

$$[\mathcal{T}]_\mathcal{B} = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix},$$

where A_i is an upper triangular e_i-by-e_i matrix with all diagonal entries equal to λ_i for each $i = 1, \dots, k$.

Proof. We showed this in the course of proving Theorem 7.5.6. □

With this result in hand, we can now prove the Cayley-Hamilton theorem.

Theorem 7.5.8 (Cayley-Hamilton theorem)**.** *Let $\mathcal{T}\colon V \to V$ be a linear transformation* (*or let A be an n-by-n matrix*)*. Let $c_\mathcal{T}(x)$ be its characteristic polynomial. Then $c_\mathcal{T}(\mathcal{T}) = 0$* (*alternatively, $c_A(A) = 0$*)*.*

Proof. First suppose that $\mathcal{T}$ satisfies Hypothesis (S). Let $c_{\mathcal{T}}(x) = (x-\lambda_1)^{e_1}\cdots(x-\lambda_k)^{e_k}$ and choose a basis $\mathcal{B}$ of V such that $[\mathcal{T}]_{\mathcal{B}}$ has the form in Corollary 7.5.7(2),

$$B = [\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}.$$

Then

$$B_1 = [\mathcal{T} - \lambda_1\mathcal{I}] = \begin{bmatrix} N_1 & & & \\ & M_{21} & & \\ & & \ddots & \\ & & & M_{k1} \end{bmatrix},$$

where $N = A_1 - \lambda_1 I$ is an e_1-by-e_1 upper triangular matrix with all diagonal entries equal to 0, and $M_{i1} = A_i - \lambda_1 I$ for $i > 1$.

Thus

$$B_1^{e_1} = \begin{bmatrix} 0 & & & \\ & M_{21}^{e_1} & & \\ & & \ddots & \\ & & & M_{k1}^{e_1} \end{bmatrix}$$

Similarly

$$B_2^{e_2} = \begin{bmatrix} M_{12}^{e_2} & & & \\ & 0 & & \\ & & \ddots & \\ & & & M_{k2}^{e_2} \end{bmatrix}$$

$$\vdots$$

$$B_k^{e_k} = \begin{bmatrix} M_{1k}^{e_k} & & & \\ & M_{2k}^{e_k} & & \\ & & \ddots & \\ & & & 0 \end{bmatrix}$$

and so

$$\begin{aligned} [c_{\mathcal{T}}(\mathcal{T})]_{\mathcal{B}} &= [(\mathcal{T} - \lambda_1\mathcal{I})^{e_1}\cdots(\mathcal{T} - \lambda_k\mathcal{I})^{e_k}]_{\mathcal{B}} \\ &= [(\mathcal{T} - \lambda_1\mathcal{I})^{e_1}]_{\mathcal{B}}\cdots[(\mathcal{T} - \lambda_k\mathcal{I})^{e_k}]_{\mathcal{B}} \\ &= B_1 B_2 \cdots B_k = 0 \end{aligned}$$

and so

$$c_{\mathcal{T}}(\mathcal{T}) = 0.$$

Alternatively, A is similar to the matrix B, $A = PBP^{-1}$ for some P, and we know then that $c_A(x) = c_B(x)$, so

$$c_A(A) = Pc_A(B)P^{-1} = Pc_B(B)P^{-1} = P(0)P^{-1} = 0.$$

Now consider the general case. Choose any basis $\mathcal{B}$ of V. If $c_{\mathcal{T}}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then $c_A(A) = A^n + a_{n-1}A^{n-1} + \cdots + a_0 I$, and if $c_A(A) = 0$, then $[c_{\mathcal{T}}(\mathcal{T})]_{\mathcal{B}} = c_A(A) = 0$, so $c_{\mathcal{T}}(\mathcal{T}) = 0$. Thus we only need to show that $c_A(A) = 0$.

Now A is a matrix with entries in $\mathbb{F}$. But, as we have mentioned, $\mathbb{F}$ is contained in some field $\mathbb{E}$ that is algebraically closed. Regarded as a matrix in $\mathbb{E}$, A satisfies Hypothesis (S) (as by the definition of being algebraically closed, every polynomial with coefficients in $\mathbb{E}$ splits into a product of linear factors). Then by the first case, $c_A(A) = 0$ is the 0 matrix, the matrix with coefficients in $\mathbb{E}$, all of whose entries are 0. But this is also the 0 matrix in $\mathbb{F}$, so $c_A(A) = 0$ as a matrix equation in $\mathbb{F}$, or $[c_{\mathcal{T}}(\mathcal{T})]_{\mathcal{B}} = 0$ and $c_{\mathcal{T}}(\mathcal{T}) = 0$ as a linear transformation $\mathcal{T}: V \to V$. □

We can now obtain a precise relationship between the minimal polynomial and the characteristic polynomial of $\mathcal{T}$.

Theorem 7.5.9. *Let $\mathcal{T}: V \to V$ be a linear transformation.*

(1) *The minimal polynomial $m_{\mathcal{T}}(x)$ divides the characteristic polynomial $c_{\mathcal{T}}(x)$.*

(2) *The minimal polynomial $m_{\mathcal{T}}(x)$ and the characteristic polynomial $c_{\mathcal{T}}(x)$ have the same irreducible factors.*

Proof. (1) By the Cayley-Hamilton theorem, $c_{\mathcal{T}}(\mathcal{T}) = 0$, and we know $m_{\mathcal{T}}(x)$ divides any polynomial $p(x)$ with $p(\mathcal{T}) = 0$ (Theorem 7.2.8).

(2) First suppose $\mathbb{F}$ is algebraically closed. Then every irreducible factor is linear. Let $x - \lambda$ be a factor of $c_{\mathcal{T}}(x)$. Then λ is an eigenvalue of $\mathcal{T}$, so there is an associated eigenvector v. Then v has $\mathcal{T}$-annihilator $m_{\mathcal{T},v}(x) = x - \lambda$ as well. But $m_{\mathcal{T}}(\mathcal{T}) = 0$, so $m_{\mathcal{T}}(\mathcal{T})(v) = 0$, and $m_{\mathcal{T},v}(x)$ divides every polynomial $p(x)$ for which $p(\mathcal{T})(v) = 0$, so $x - \lambda$ is a factor of $m_{\mathcal{T}}(x)$.

Now consider $\mathbb{F}$ in general, and let $f(x)$ be any irreducible factor of $c_{\mathcal{T}}(x)$. Again let $\mathbb{E}$ be an algebraically closed field containing $\mathbb{F}$, and regard $f(x)$ as a polynomial in $\mathbb{E}$. Then $f(x)$ has a factor $x - \lambda$ for some λ. Write $m_{\mathcal{T}}(x) = g_1(x) \cdots g_j(x)$, a product of irreducible polynomials in $\mathbb{F}[x]$. Then, as polynomials in $\mathbb{E}[x]$, by case (1), $x - \lambda$ divides $m_{\mathcal{T}}(x)$, so (as $x - \lambda$ is certainly irreducible) it must divide one of the factors $g_i(x)$ of $m_{\mathcal{T}}(x)$. Thus $f(x)$ and $g_i(x)$ have the common factor of $x - \lambda$ in $\mathbb{E}[x]$, so are not relatively prime in $\mathbb{E}[x]$. That implies that they are not relatively prime in $\mathbb{F}[x]$ either, and since $f(x)$ is irreducible, that implies that $f(x)$ divides $g_i(x)$. □

7.6. Exercises

1. In each case, decide whether A is diagonalizable. If so, find an invertible matrix P and a diagonal matrix D with $A = PDP^{-1}$.

(a) $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 3 \\ 0 & 0 & 3 \end{bmatrix}$.

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

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

(d) $A = \begin{bmatrix} 5 & 1 & 0 & -1 \\ 0 & 6 & 0 & -1 \\ 0 & 0 & 7 & -2 \\ 0 & 0 & 0 & 5 \end{bmatrix}$.

(e) $A = \begin{bmatrix} 4 & 0 & 4 & 0 \\ 2 & 1 & 3 & 0 \\ -1 & 0 & 0 & 0 \\ 3 & 0 & 4 & 1 \end{bmatrix}$.

(f) $A = \begin{bmatrix} 4 & -3 & -4 & 3 \\ 4 & -3 & -8 & 7 \\ -4 & 4 & 6 & -4 \\ -4 & 4 & 2 & 0 \end{bmatrix}$, $c_A(x) = x(x-1)(x-2)(x-4)$.

(g) $A = \begin{bmatrix} -4 & -3 & 0 & 9 \\ 2 & 2 & 1 & -2 \\ 2 & 0 & 3 & -2 \\ -6 & -3 & 0 & 11 \end{bmatrix}$, $c_A(x) = (x-2)^2(x-3)(x-5)$.

(h) $A = \begin{bmatrix} 4 & 2 & 1 & -6 \\ -16 & 4 & -16 & 0 \\ -6 & -1 & -3 & 4 \\ -6 & 1 & -6 & 2 \end{bmatrix}$, $c_A(x) = x^2(x-3)(x-4)$.

(i) $A = \begin{bmatrix} -9 & 8 & -16 & -10 \\ 4 & -7 & 16 & 4 \\ 2 & -5 & 11 & 2 \\ 12 & -8 & 16 & 13 \end{bmatrix}$, $c_A(x) = (x-1)^2(x-3)^2$.

(j) $A = \begin{bmatrix} 5 & 0 & 2 & 1 \\ 0 & 2 & 1 & 1 \\ -2 & 0 & 0 & -2 \\ 2 & -2 & 5 & 7 \end{bmatrix}$, $c_A(x) = (x-3)^2(x-4)^2$.

2. Show that the *only* diagonalizable n-by-n matrix A with a single eigenvalue λ (necessarily of multiplicity n) is the matrix $A = \lambda I$. (Of course, this matrix is already diagonal.)

3. For fixed a and b, define the (a, b)-Fibonacci numbers F_n by

$$F_0 = a, \quad F_1 = b, \quad F_{n+2} = F_{n+1} + F_n \text{ for } n \geq 0.$$

(The $(0, 1)$ Fibonacci numbers are the ordinary Fibonacci numbers

$$F_0 = 0, \quad F_1 = 1, \quad F_2 = 1, \quad F_3 = 2, \quad F_4 = 3, \quad F_5 = 5, \quad F_6 = 8, \ldots .)$$

Observe that

$$\begin{bmatrix} F_{n+1} \\ F_{n+2} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} F_n \\ F_{n+1} \end{bmatrix}$$

and hence that

$$\begin{bmatrix} F_n \\ F_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^n \begin{bmatrix} F_0 \\ F_1 \end{bmatrix} \quad \text{for every } n \geq 0.$$

Use this observation to find a formula for F_n.

4. Let V be a finite-dimensional vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. If $\mathcal{T}$ is diagonalizable, show that $\mathcal{T}^k$ is diagonalizable for every positive integer k.

5. Let V be a finite-dimensional vector space over the complex numbers, and let $\mathcal{T}\colon V \to V$ be a linear transformation. Suppose that $\mathcal{T}^k$ is diagonalizable for some positive integer k.

(a) If $\mathcal{T}$ is invertible, show that $\mathcal{T}$ is diagonalizable.

(b) Show by example that if $\mathcal{T}$ is not invertible, $\mathcal{T}$ may not be diagonalizable.

6. Let V be a finite-dimensional complex vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. Show that $\mathcal{T}$ is diagonalizable if and only if

$$\operatorname{Ker}(\mathcal{T} - a\mathcal{I}) \cap \operatorname{Im}(\mathcal{T} - a\mathcal{I}) = \{0\}$$

for every complex number a.

7. (a) Let V be a finite-dimensional vector space, and let $\mathcal{R}\colon V \to V$ and $\mathcal{S}\colon V \to V$ be diagonalizable linear transformations. Suppose that $\mathcal{R}$ and $\mathcal{S}$ commute. Show that $\mathcal{R} + \mathcal{S}$ is diagonalizable.

(b) Give an example of a vector space V and diagonalizable linear transformations $\mathcal{R}$ and $\mathcal{S}$ that do not commute where $\mathcal{R}+\mathcal{S}$ is diagonalizable, and an example where $\mathcal{R} + \mathcal{S}$ is not diagonalizable.

8. Let V be a finite-dimensional vector space, and let $\mathcal{S}\colon V \to V$ and $\mathcal{T}\colon V \to V$ be diagonalizable linear transformations. $\mathcal{S}$ and $\mathcal{T}$ are said to be *simultaneously diagonalizable* if there is a basis $\mathcal{B}$ of V with $[\mathcal{S}]_{\mathcal{B}}$ and $[\mathcal{T}]_{\mathcal{B}}$ both diagonal. Show that $\mathcal{S}$ and $\mathcal{T}$ are simultaneously diagonalizable if and only if $\mathcal{S}$ and $\mathcal{T}$ commute (i.e., if and only if $\mathcal{S}\mathcal{T} = \mathcal{T}\mathcal{S}$).

9. Let $M_n(a, b)$ be the n-by-n matrix all of whose diagonal entries are equal to a and all of whose off-diagonal entries are equal to b.

(a) Find the eigenvalues of $M_n(a, b)$, their algebraic and geometric multiplicities, and bases for the eigenspaces.

(b) Find an invertible matrix P and a diagonal matrix D such that $M_n(a, b) = PDP^{-1}$.

(c) Use the result of (b) to find the determinant of $M_n(a, b)$ and the characteristic polynomial of $M_n(a, b)$.

(Note that this problem asks you to do (a) and (b) first, and then (c). This illustrates that it is sometimes (often?) more useful to think about eigenvalues and eigenvectors directly rather than to compute characteristic polynomials and determinants.)

10. Let V be a finite-dimensional vector space, and let $\mathcal{T}: V \to V$ be a linear transformation. Suppose that $\mathcal{T}$ is both diagonalizable and nilpotent. Show that $\mathcal{T} = 0$.

11. (a) Show that there are infinitely many linear transformations $\mathcal{T}: \mathbb{C}^2 \to \mathbb{C}^2$ with $\mathcal{T}^2 = 0$. Show that up to similarity there are exactly two such.

(b) Show that there are infinitely many linear transformations $\mathcal{T}: \mathbb{C}^2 \to \mathbb{C}^2$ with $\mathcal{T}^2 = \mathcal{I}$. Show that up to similarity, there are exactly three such.

12. Let V be a finite-dimensional vector space, and let $\mathcal{T}: V \to V$ be a linear transformation. For a vector $v \in V$, let $m_{\mathcal{T},v}(x)$ be the unique monic polynomial of smallest degree with $m_{\mathcal{T},v}(\mathcal{T})(v) = 0$.

(a) Show that $m_{\mathcal{T},v}(x)$ divides the minimal polynomial $m_{\mathcal{T}}(x)$ of $\mathcal{T}$.

(b) The $\mathcal{T}$-Span of v is $\mathcal{T}\text{-Span}(v) = \{p(\mathcal{T})(v) \,|\, p(x) \in \mathbb{F}[x]\}$. Show that $\dim \mathcal{T}\text{-Span}(v) = \text{degree of } m_{\mathcal{T},v}(x)$.

13. Recall that the *trace* of a square matrix is the sum of its diagonal entries.

(a) Let A and B be similar matrices. Show that $\det(B) = \det(A)$ and that $\operatorname{trace}(B) = \operatorname{trace}(A)$.

(b) Let A be a complex matrix. Show that the determinant of A is equal to the product of the eigenvalues of A (with multiplicities) and that the trace of A is equal to the sum of the eigenvalues of A (with multiplicities).

14. Let A be a fixed m-by-m complex matrix, and let B be a fixed n-by-n complex matrix.

(a) Show that the equation $AX = XB$ has a nonzero solution if and only if A and B have a common eigenvalue. (Here X is an m-by-n complex matrix.)

(b) Use part (a) to show that the equation $AX - XB = C$ has a unique solution for every complex m-by-n matrix C if and only if A and B do not have a common eigenvalue. This equation is known as *Sylvester's equation*.

15. Let $\mathcal{T}: V \to V$ be a linear transformation that satisfies Hypothesis (S). Let the distinct eigenvalues of $\mathcal{T}$ be $\lambda_1, \ldots, \lambda_k$. Then, as we have seen, $V = E^\infty_{\lambda_1} \oplus \cdots \oplus E^\infty_{\lambda_k}$.

(a) Let U be any $\mathcal{T}$-invariant subspace of V. Show that $U = U_1 \oplus \cdots \oplus U_k$, where $U_i = U \cap E^\infty_{\lambda_i}$ for each i.

(b) Show that every $\mathcal{T}$-invariant subspace U of V has a $\mathcal{T}$-invariant complement if and only if $\mathcal{T}$ is diagonalizable.

16. Let V be the complex vector space of trigonometric polynomials, i.e., the complex vector space with basis

$$\{1, \cos(x), \sin(x), \cos(2x), \sin(2x), \cos(3x), \sin(3x), \ldots\}.$$

Let $\mathcal{T}: V \to V$ by $\mathcal{T}(f(x)) = f'(x)$. Find the eigenvalues of $\mathcal{T}$ and bases for the eigenspaces of $\mathcal{T}$.

17. Solve each of the following constant coefficient linear differential equations. In all cases, express your answer in terms of real functions.

(a) $(D-1)(D-2)(D-3)(f(x)) = 0$.

(b) $(D-2)^2(D-5)(f(x)) = 0$.

(c) $(D^2-4D+13)(f(x)) = 0$.

(d) $D^2(D+1)^3(f(x)) = 0$.

(e) $(D^2-6D+25)(f(x)) = 0$.

(f) $(D^2+1)^2(D-2)(D+3)(f(x)) = 0$.

(g) $(D-2)(D-5)(f(x)) = 6e^{4x}$.

(h) $D^2(D+1)(f(x)) = 12+6x$.

(i) $(D+2)^2(f(x)) = 19\cos(3x) - 22\sin(3x)$.

18. Solve each of the following initial value problems. (An initial value problem is a differential equation with specified initial values.) In all cases, express your answer in terms of real functions.

(a) $(D^2-4)(f(x)) = 0$, $f(0) = 8$, $f'(0) = -4$.

(b) $D(D-2)(D-3)(f(x)) = 0$, $f(0) = 6$, $f'(0) = 13$, $f''(0) = 18$.

(c) $D(D-1)^2(f(x)) = 5e^x$, $f(0) = 9$, $f'(0) = 12$, $f''(0) = 14$.

(b) $(D-3)(D^2+4)(f(x)) = 0$, $f(0) = -1$, $f'(0) = 9$, $f''(0) = 5$.

Chapter 8

Jordan canonical form

In this chapter, we turn our attention to Jordan canonical form. We suppose that we have a linear transformation $\mathcal{T}: V \to V$, where V is a finite-dimensional vector space over a field $\mathbb{F}$, and that $\mathcal{T}$ satisfies our Hypothesis (S). (We remind the reader that if $\mathbb{F}$ is algebraically closed, and in particular if $\mathbb{F} = \mathbb{C}$, the field of complex numbers, then Hypothesis (S) is automatically satisfied, so this is no further restriction.) We show that V has a basis $\mathcal{B}$, called a *Jordan basis*, in which $J = [\mathcal{T}]_{\mathcal{B}}$, the matrix of $\mathcal{T}$ in the $\mathcal{B}$ basis, is a matrix in *Jordan canonical form* (JCF).

As we will see, the Jordan canonical form J of a linear transformation $\mathcal{T}$ makes its geometric structure crystal clear. (To mix metaphors, we have regarded a basis as giving us a language in which to express linear transformations, and a Jordan basis $\mathcal{B}$ of V is a *best* language in which to understand $\mathcal{T}$.) By the geometric structure of $\mathcal{T}$ we mean, as we have been studying, its (generalized) eigenvectors and the relationships between them.

We will see that the generalized eigenvectors of a linear transformation fall into "chains", and that the JCF encodes the chains. Actually, we will introduce the eigenstructure picture (ESP) of a linear transformation $\mathcal{T}$, a pictorial structure that makes the situation particularly easy to understand, and it will be immediate how to pass from the ESP of $\mathcal{T}$ to the JCF of $\mathcal{T}$, and vice-versa.

Once we have established that Jordan canonical form exists, we will develop a simple algorithm for finding it (provided we have factored the characteristic polynomial). This algorithm will simply be counting dimensions (or counting nodes in the ESP)! We will also develop an algorithm for finding a Jordan basis.

In the last chapter we considered, in particular, the case of diagonalizable linear transformations, i.e., the case where V has a basis $\mathcal{B}$ (of eigenvectors) in which $D = [\mathcal{T}]_{\mathcal{B}}$ is diagonal. In this case, $\mathcal{B}$ is a Jordan basis and the JCF of $\mathcal{T}$ is D. In other words, if $\mathcal{T}$ is diagonalizable, then $D = [\mathcal{T}]_{\mathcal{B}}$ is as simple as it could possibly be. But it is too much to hope for that every $\mathcal{T}$ is diagonalizable—indeed we have already seen examples where that is not the case—but *every* $\mathcal{T}$ (satisfying Hypothesis (S)) has a Jordan canonical form $J = [\mathcal{T}]_{\mathcal{B}}$ that is almost as simple.

JCF is of the highest importance in itself. But we will also give a particular application that tells us the relationship between linear transformations $\mathcal{ST}$ and $\mathcal{TS}$.

We saw earlier how to use linear algebra to solve higher-order linear differential equations. We will see, as an application of diagonalizability/JCF, how to solve systems of first-order differential equations.

Finally, you might ask what happens if $\mathcal{T}$ does not satisfy Hypothesis (S). In this case there is a generalization of JCF, which we briefly describe in the last section of this chapter.

8.1. Chains, Jordan blocks, and the (labelled) eigenstructure picture of $\mathcal{T}$

Definition 8.1.1. Let $\mathcal{T}\colon V \to V$ be a linear transformation. A set of vectors $\{u_1, \ldots, u_h\}$ in V is a *chain* of length h associated to the eigenvalue λ if u_h is a generalized eigenvector of index h of $\mathcal{T}$ with associated eigenvalue λ, and for each $i = 2, \ldots, h$, $u_{i-1} = (\mathcal{T} - \lambda\mathcal{I})(u_i)$. $\Diamond$

Remark 8.1.2. (1) We observe that a chain is completely determined by the vector u_h, which we call the vector at the *top* of the chain.

(2) For each $i = 1, \ldots, h-1$, $u_i = (\mathcal{T} - \lambda\mathcal{I})^{h-i}(u_h)$.

(3) For each $i = 1, \ldots, h$, u_i is a generalized eigenvector of index i associated to the eigenvalue λ.

(4) $\{u_1, \ldots, u_h\}$ is linearly independent by Lemma 7.2.6. $\Diamond$

Lemma 8.1.3. *Let $\mathcal{T}\colon V \to V$ be a linear transformation. Then V has a basis $\mathcal{B} = \{u_1, \ldots, u_h\}$ that is a chain of length h associated to the eigenvalue λ if and only if*

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & & \\ & & & & 1 \\ & & & & \lambda \end{bmatrix},$$

an h-by-h matrix with all diagonal entries equal to λ, all entries immediately above the diagonal equal to 1, and all other entries equal to 0.

Proof. We know that the ith column of $[\mathcal{T}]_{\mathcal{B}}$ is the coordinate vector $[\mathcal{T}(u_i)]_{\mathcal{B}}$. But if $u_{i-1} = (\mathcal{T} - \lambda\mathcal{I})(u_i) = \mathcal{T}(u_i) - \lambda u_i$, we have that $\mathcal{T}(u_i) = u_{i-1} + \lambda u_i$, so $[\mathcal{T}]_{\mathcal{B}}$ is as claimed, and vice-versa. (If $i = 1$, $(\mathcal{T} - \lambda\mathcal{I})(u_1) = 0$ so $\mathcal{T}(u_1) = \lambda u_1$.) $\square$

Definition 8.1.4. (1) *A* matrix as in the conclusion of Lemma 8.1.3 is an h-by-h *Jordan block*.

(2) An n-by-n matrix J is in *Jordan canonical form (JCF)* if J is a block diagonal matrix

$$J = \begin{bmatrix} J_1 & & \\ & J_2 & \\ & & \ddots \end{bmatrix} \qquad \Diamond$$

with each J_i a Jordan block.

Remark 8.1.5. Note that a diagonal matrix is a matrix in Jordan canonical form in which every Jordan block is 1-by-1. $\Diamond$

Here is the theorem to which we are heading.

Theorem 8.1.6 (Existence and essential uniqueness of Jordan canonical form)**.** *Let $\mathcal{T}\colon V \to V$, $\dim V = n$, be a linear transformation satisfying Hypothesis* (S). *Then V has a basis $\mathcal{B}$ in which $J = [\mathcal{T}]_{\mathcal{B}}$ is in Jordan canonical form.*

The matrix J is unique up to the order of the blocks.

We can immediately translate this into matrix language.

Theorem 8.1.7. *Let A be an n-by-n matrix satisfying Hypothesis* (S). *Then A is similar to a matrix J in Jordan canonical form,*

$$J = P^{-1}AP$$

for some invertible matrix P. The matrix J is unique up to the order of the blocks.

Definition 8.1.8. A basis $\mathcal{B}$ as in Theorem 8.1.6 is a *Jordan basis* of V. If P is as in Theorem 8.1.7, a basis $\mathcal{B}$ of $\mathbb{F}^n$ consisting of the columns of P is a *Jordan basis* of $\mathbb{F}^n$. $\Diamond$

(The basis $\mathcal{B}$ will never be unique.)

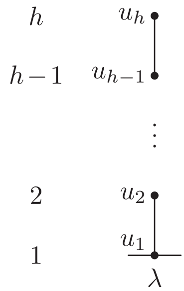
Remark 8.1.9. We observe that if the first block in the JCF of $\mathcal{T}$ is h_1-by-h_1, the first h_1 vectors in a Jordan basis $\mathcal{B}$ form a chain of length h_1; if the second block is h_2-by-h_2, then the next h_2 vectors in $\mathcal{B}$ form a chain of length h_2, etc. Thus a Jordan basis $\mathcal{B}$ is a union of chains.

Conversely, we observe that if $\mathcal{B}$ is a union of chains, $J = [\mathcal{T}]_{\mathcal{B}}$ is in Jordan canonical form.

In particular, we also see that if A is similar to J, $J = P^{-1}AP$, then P is a matrix whose columns are the vectors in a Jordan basis, i.e., P is a matrix whose columns are generalized eigenvectors, ordered in chains. $\Diamond$

We now develop the (labelled) eigenstructure picture of a linear transformation —its lESP (or its ESP, without the labels).

We picture a chain of length h as in Lemma 8.1.3 as:



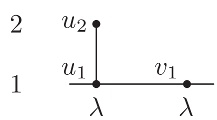
Here the column on the left is indicating the height of the node ($\bullet$) and each u_i is labelling the corresponding node. Below the base we have the associated eigenvalue λ.

(Given this picture, it is natural to think of the index of a generalized eigenvector as its height. But index, rather than height, is the standard mathematical term, so we will continue to use it.)

Thus, in view of Remark 8.1.2, we may encode both the Jordan canonical form of $\mathcal{T}$ and the Jordan basis $\mathcal{B}$ by the *labelled eigenstructure picture* (lESP) of $\mathcal{T}$, obtained by juxtaposing all the pictures of the chains. We may encode the Jordan canonical form of $\mathcal{T}$ alone by its *eigenstructure picture* (ESP), which consists of the picture without the labels. (In theory, we get the lESP first and erase the labels to get the ESP. In practice, we get the ESP first and then figure out what the labels should be.)

We will not give a formal definition, as that would involve a blizzard of notation. Rather, we give a few examples to make the situation clear.

An lESP of

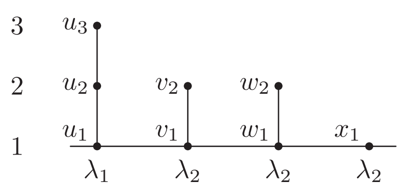


corresponds to a JCF of

$$\begin{bmatrix} \lambda & 1 & \\ & \lambda & \\ & & \lambda \end{bmatrix}$$

and a Jordan basis $\{u_1, u_2, v_1\}$ (in that order).

An lESP of



corresponds to a JCF of

$$\begin{bmatrix} \lambda_1 & 1 & & & & & & \\ & \lambda_1 & 1 & & & & & \\ & & \lambda_1 & & & & & \\ & & & \lambda_2 & 1 & & & \\ & & & & \lambda_2 & & & \\ & & & & & \lambda_2 & 1 & \\ & & & & & & \lambda_2 & \\ & & & & & & & \lambda_2 \end{bmatrix}$$

and a Jordan basis $\{u_1, u_2, u_3, v_1, v_2, w_1, w_2, x_1\}$.

An lESP with all nodes at height 1 corresponds to a diagonalizable linear transformation. If $c_{\mathcal{T}}(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k}$ and $\mathcal{T}$ is diagonalizable, then $\mathcal{T}$ has lESP

$$1 \qquad \begin{array}{c} v_1 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad v_n \\ \bullet\text{———}\bullet\text{——}\bullet\text{———}\bullet\text{————}\bullet\text{———}\bullet \\ \underbrace{\lambda_1 \ \cdots \ \lambda_1}_{e_1} \quad \underbrace{\lambda_2 \ \cdots \ \lambda_2}_{e_2} \quad \cdots \quad \underbrace{\lambda_k \ \cdots \ \lambda_k}_{e_k} \end{array}$$

with $\mathcal{B} = \{v_1, \ldots, v_n\}$ a basis of eigenvectors.

Remark 8.1.10. Suppose that $c_{\mathcal{T}}(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k}$. We observe:

(1) The algebraic multiplicity e_i of λ_i, which is the dimension of the associated generalized eigenspace (Corollary 7.5.3), is equal to the sum of the sizes of Jordan blocks with diagonals λ_i, or alternatively the total number of nodes in the chains associated to λ_i.

(2) Since each chain contains exactly one eigenvector, the vector at the bottom of the chain, these vectors form a basis for the associated eigenspace. Thus the geometric multiplicity of λ_i, which is the dimension of the eigenspace of λ_i, is equal to the number of Jordan blocks with diagonals λ_i, or alternatively the number of chains associated to λ_i.

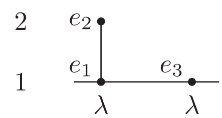
(3) The minimal polynomial $m_{\mathcal{T}}(x) = (x - \lambda_1)^{f_1} \cdots (x - \lambda_k)^{f_k}$, where f_i is the size of the largest Jordan block with diagonal λ_i, or alternatively the maximum height of a chain associated to λ_i. $\Diamond$

8.2. Proof that $\mathcal{T}$ has a Jordan canonical form

Since JCF is subtle, before proving it let's think about how we might go about doing it. Suppose we had a matrix

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

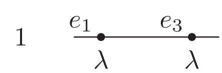
Of course, A is already in JCF, and we have a Jordan basis $\mathcal{B} = \{e_1, e_2, e_3\}$, and a labelled ESP:



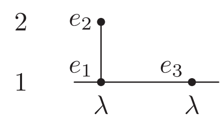
But suppose we didn't already know that, and we were trying to *show* that we had a Jordan basis and hence that A was similar to a matrix in JCF.

We might try to work the bottom up. First we could find a basis for E^1_λ, the generalized eigenspace of index at most 1.

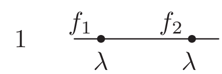
Sure enough we could choose the basis $\{e_1, e_3\}$ to get the picture:



and then e_1 is at the bottom of a chain whose top is e_2, i.e., we can find v with $(A - \lambda I)v = e_1$, namely $v = e_2$, so moving up to the next level we get:



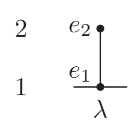
and we are done—perfect. But of course there are many choices of basis so instead suppose we chose the basis $\{f_1, f_2\}$ for E^1_λ, where $f_1 = e_1 + e_3$ and $f_2 = e_3$, to get the same picture:



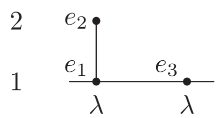
Now when we try to move up to the next level, we're stuck, as there is no vector v with $(A - \lambda I)v = f_1$, or with $(A - \lambda I)v = f_2$, so we can't move up from either of these nodes.

This shows that moving up is not a good strategy.

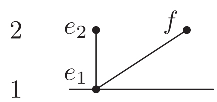
Thus instead we should try moving down. We begin by looking for a vector at the top of a chain—not just any chain, since we are trying to move down, but a vector at the top of a highest chain. We find such a vector, e_2, at height 2, and then we get the rest of the chain. The vector below it in the chain is $(A - \lambda I)e_2 = e_1$. Hence we have the picture:



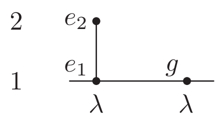
Now we have a linearly independent set, i.e., a partial basis, $\{e_1, e_2\}$ of $\mathbb{F}^3$ and we want to extend it to be a (full) basis. Since $\mathbb{F}^3$ is 3-dimensional, we simply choose another linearly independent vector. Suppose we choose e_3. Then we get, for the lESP,



(as $(A - \lambda I)e_3 = 0$ so e_3 is an eigenvector, and again we are done—perfect). But of course, we could have made another choice. Suppose we chose $f = e_2 + e_3$. Then $\{e_1, e_2, f\}$ is still a basis of $\mathbb{F}^3$. But now when we compute $(A - \lambda I)f$ we find $(A - \lambda I)f = e_1$. So the picture we see is



Thus f is a "crooked" vector. We want to "straighten" it out, and we can do so by modifying our choice. We modify f to $g = f - e_2$ (and we see $g = e_3$) to obtain



and we are done—perfect.

Thus our proof will show that we can always straighten out a crooked vector; indeed, it will show us how to do so.

(It is true that Ecclesiastes, or, to give him his Hebrew name, Koheleth, wrote "What is crooked cannot be made straight", but he was not discussing linear algebra when he did so.)

Having described the strategy of our proof, we now go ahead and carry it out.

Proof of Theorem 8.1.6. We first consider the case where we only have a single eigenvalue, so $c_{\mathcal{T}}(x) = (x - \lambda)^n$. (As we will see, given our previous results, all the work in proving the theorem goes into this case.)

We begin by following the strategy of the proof of Lemma 7.5.2, but instead of starting with a single eigenvector we start with a single Jordan block.

We proceed by induction on n.

Let $\mathcal{T}$ have minimal polynomial $m_{\mathcal{T}}(x) = (x - \lambda)^f$, with $f \leq n$. (We know the minimal polynomial must be of this form.)

Choose a vector $v = v_f$ with $m_{\mathcal{T},v}(x) = (x - \lambda)^f$. Form the chain $v_1, \ldots, v_f$ as in Definition 8.1.1, and let W be the subspace of V with basis $\mathcal{B}_0 = \{v_1, \ldots, v_f\}$.

If $f = n$, then $W = V$ and by Lemma 8.1.3, setting $\mathcal{B} = \mathcal{B}_0$, $[\mathcal{T}]_{\mathcal{B}}$ consists of a single n-by-n Jordan block associated to λ, and we are done.

Otherwise extend $\mathcal{B}_0$ to a basis $\mathcal{B}' = \{v_1, \dots, v_f, \dots, v_n\}$ of V. Then

$$M = [\mathcal{T}]_{\mathcal{B}'} = \begin{bmatrix} J_1 & * \\ 0 & D_1 \end{bmatrix}$$

with J_1 an f-by-f Jordan block associated to λ, and with D_1 an $(n-f)$-by-$(n-f)$ matrix with characteristic polynomial $c_{D_1}(x) = (x-\lambda)^{n-f}$.

Let U be the subspace of V spanned by $\mathcal{B}'_2 = \{v_{f+1}, \dots, v_n\}$. If all the entries $*$ were 0, then we would have $\mathcal{T}(U) \subseteq U$ and we could apply induction to replace $\mathcal{B}'_2$ by another basis $\mathcal{B}''_2$ with $[\mathcal{T}']_{\mathcal{B}''_2}$ in Jordan canonical form, where $\mathcal{T}'$ is simply the restriction of $\mathcal{T}$ to U, $\mathcal{T}' \colon U \to U$, and then if $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}''$, $[\mathcal{T}]_{\mathcal{B}}$ would be in Jordan canonical form as well, and we would be done.

But there is no reason to believe that all of the entries $*$ are zero, and that may well not be the case.

We have the linear transformation $\mathcal{P} \colon V \to U$ defined by $\mathcal{P}(v_i) = 0$ for $i = 1, \dots, f$ and $\mathcal{P}(v_i) = v_i$ for $i = f+1, \dots, n$; more simply,

$$\mathcal{P}(c_1v_1 + \cdots + c_fv_f + c_{f+1}v_{f+1} + \cdots + c_nv_n) = c_{f+1}v_{f+1} + \cdots + c_nv_n.$$

Let $\mathcal{S}$ be the composition $\mathcal{S} = \mathcal{P}\mathcal{T} \colon U \to U$, so that $[\mathcal{S}]_{\mathcal{B}'_2} = D_1$. Then by induction U has a basis $\mathcal{B}''_2 = \{u_1, \dots, u_{n-1}\}$ in which

$$[\mathcal{S}]_{\mathcal{B}''_2} = \begin{bmatrix} J_2 & & \\ & J_3 & \\ & & \ddots \end{bmatrix}$$

is a matrix in Jordan canonical form.

Now let $\mathcal{B}'' = \mathcal{B}_0 \cup \mathcal{B}''_2$ and note that $\mathcal{B}$ is a basis of V (Theorem 3.4.24). Let $M_1 = [\mathcal{T}]_{\mathcal{B}''}$.

Then $M_1 = \big[[\mathcal{T}(v_1)]_{\mathcal{B}''} | \dots | [\mathcal{T}(v_f)]_{\mathcal{B}''} | [\mathcal{T}(u_1)]_{\mathcal{B}''} | \dots | [\mathcal{T}(u_{n-f})]_{\mathcal{B}''}\big]$, where $\mathcal{B}'' = \{v_1, \dots, v_f, u_1, \dots, u_{n-f}\}$. We have not changed the first f columns. As for the rest of the columns, we know what $\mathcal{S}(u_i)$ is for each i. But $\mathcal{S}(u_i) = \mathcal{P}\mathcal{T}(u_i)$ so that says that we must have $\mathcal{T}(u_i) = c_1v_1 + \cdots + c_fv_f + \mathcal{S}(u_i)$ for some unknown $c_1, \dots, c_f$ (depending on i, of course). Thus we see that

$$M_1 = \begin{bmatrix} J_1 & B_{12} & B_{13} & \dots \\ & J_2 & & 0 \\ & & J_3 & \\ & 0 & & \ddots \end{bmatrix}$$

for some unknown matrices B_{12}, B_{13}, etc.

Now at this stage in the proof of Lemma 7.5.2 we were done, because there we were just looking for a matrix in upper triangular form, so it didn't matter what the unknown entries were.

But here that is not good enough. To get M_1 in JCF we would have to have $B_{12} = B_{13} = \cdots = 0$, and that may not be the case. Indeed, there is no reason to expect that to be the case, as we chose $u_1, \dots, u_{n-f}$ almost at random (subject only to the condition that $\mathcal{B}''$ be a basis). In other words, $u_1, \dots, u_{n-f}$ may be crooked, and we will have to straighten them out.

You'll notice that we chose $v = v_f$ with $m_{\mathcal{T}}(x) = (x-\lambda)^f$, so that $m_{\mathcal{T},v}(x) = (x-\lambda)^f$ was of as high a degree as possible, or equivalently, that the size of the J_1 Jordan block was as large as possible. So far we have not used that in the proof, but now we are about to make crucial use of it.

Suppose that J_2 is an h-by-h Jordan block. Then J_2 is the restriction of $\mathcal{T}$ to the subspace with basis $\{u_1, \dots, u_h\}$, the first h vectors in the basis $\mathcal{B}_2''$ of U. Certainly $h \leq f$.

(Case I) $h = f$: Let $x_f = u_f$ and form a chain $x_1, \dots, x_f$. Replace the vectors $u_1, \dots, u_f$ in $\mathcal{B}''$ by the vectors $x_1, \dots, x_f$ to get a new basis

$$\mathcal{B}''' = \{v_1, \dots, v_f, x_1, \dots, x_f, \dots\}$$

of V. ($\mathcal{B}'''$ is a basis of V by Theorem 3.4.24 again, as each x_i differs from the corresponding u_i by a linear combination of $v_1, \dots, v_f$, i.e., by an element of W. In making this replacement we may have changed U to a different complement of W, that with basis $\{x_1, \dots, x_f, \dots\}$, but that is irrelevant.) We have changed our basis, so we have changed the matrix of $\mathcal{T}$, but the only change to this matrix is to replace the block B_{12} by a new block B_{12}'.

We claim that the vectors $x_1, \dots, x_f$ are "straight", i.e., that when we express $\mathcal{T}(x_i)$ as a linear combination of the vectors in $\mathcal{B}'''$, the coefficients of $v_1, \dots, v_f$ are all zero, and so the entries in the block $\mathcal{B}_{12}'$ are all zero, which is what we need.

Let's note that $x_2, \dots, x_f$ are automatically straight, as for $i = 2, \dots, f$, since we have chosen these vectors to be in a chain, $(\mathcal{T} - \lambda\mathcal{I})(x_i) = x_{i-1}$, i.e., $\mathcal{T}(x_i) = x_{i-1} + \lambda x_i$ and this expression does not involve $v_1, \dots, v_f$. Also

$$\begin{aligned}
\mathcal{T}(x_1) &= ((\mathcal{T} - \lambda\mathcal{I}) + \lambda\mathcal{I})(x_1) \\
&= (\mathcal{T} - \lambda\mathcal{I})(x_1) + \lambda x_1 \\
&= (\mathcal{T} - \lambda\mathcal{I})(\mathcal{T} - \lambda\mathcal{I})^{f-1}(x_f) + \lambda x_1 \\
&= (\mathcal{T} - \lambda\mathcal{I})^f(x_f) + \lambda x_1 = 0 + \lambda x_1 = \lambda x_1
\end{aligned}$$

which also does not involve $v_1, \dots, v_f$, so in this case we are done.

(Case II) $h < f$: We could follow exactly the same strategy as Case I to get $x_2, \dots, x_h$ straight, but then when we got to the last step we would not necessarily have x_1 straight. But we know two things:

$$(\mathcal{T} - \lambda\mathcal{I})(x_1) = c_1 v_1 + \cdots + c_f v_f \quad \text{for some } c_1, \dots, c_f$$

(these coefficients being the entries in the first column of B_{12}); and

$$\begin{aligned}
(\mathcal{T} - \lambda\mathcal{I})^{f-h}(\mathcal{T} - \lambda\mathcal{I})(x_1) &= (\mathcal{T} - \lambda\mathcal{I})^{f-h}(\mathcal{T} - \lambda\mathcal{I})(\mathcal{T} - \lambda\mathcal{I})^{h-1}(x_h) \\
&= (\mathcal{T} - \lambda\mathcal{I})^f(x_h) = 0.
\end{aligned}$$

In other words, $(\mathcal{T} - \lambda\mathcal{I})(x_1)$ is a generalized eigenvector of index at most $f - h$, so we must have

$$(\mathcal{T} - \lambda\mathcal{I})(x_1) = c_1 v_1 + \cdots + c_{f-h} v_{f-h},$$

i.e., all the coefficients $c_{f-h+1}, \dots, c_f$ are zero.

Thus in this case we do not use $x_h = u_h$; instead we "straighten" x_h by choosing

$$y_h = x_h - (c_1 v_{h+1} + c_2 v_{h+2} + \cdots + c_{f-h} v_f) = x_h - v.$$

(Again here we are crucially using $f \geq h$.) We then form the chain $y_1, \ldots, y_h$ as before. Again it is automatically the case that $y_2, \ldots, y_h$ are "straight", since $\mathcal{T}(y_i) = y_{i-1} + \lambda y_i$ for $i \geq 2$, but now, remembering that $v_1, \ldots, v_f$ form a chain,

$$\begin{aligned}(\mathcal{T} - \lambda\mathcal{I})(y_1) &= (\mathcal{T} - \lambda\mathcal{I})(\mathcal{T} - \lambda\mathcal{I})^{h-1}(y_h)\\ &= (\mathcal{T} - \lambda\mathcal{I})(\mathcal{T} - \lambda\mathcal{I})^{h-1}(x_h - v)\\ &= (\mathcal{T} - \lambda\mathcal{I})(\mathcal{T} - \lambda\mathcal{I})^{h-1}(x_h) - (\mathcal{T} - \lambda\mathcal{I})(\mathcal{T} - \lambda\mathcal{I})^{h-1}(v)\\ &= (\mathcal{T} - \lambda\mathcal{I})(x_1) + (\mathcal{T} - \lambda\mathcal{I})^{h}(v)\\ &= (c_1 v_1 + \cdots + c_{f-h} v_{f-h}) - (c_1 v_1 + \cdots + c_{f-h} v_{f-h}) = 0\end{aligned}$$

so $\mathcal{T}(y_1) = \lambda y_1$.

Hence in the basis $\{v_1, \ldots, v_f, y_1, \ldots, y_h, \ldots\}$ the matrix of $\mathcal{T}$ has the block $B''_{12} = 0$.

In this process we have not changed any other block in the matrix of $\mathcal{T}$ at all. So we may similarly modify our basis to make the block $B''_{13} = 0$, etc. Thus in the end we arrive at a basis $\mathcal{B}$ with

$$M = [\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} J_1 & & \\ & J_2 & \\ & & \ddots \end{bmatrix}$$

in Jordan canonical form.

Finally, suppose we have more than one eigenvalue, so that $c_{\mathcal{T}}(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k}$. We saw that V has a basis $\mathcal{B}'$ in which $[\mathcal{T}]_{\mathcal{B}'}$ was block diagonal with each block corresponding to a generalized eigenspace (Corollary 7.5.7). Writing $\mathcal{B}' = \mathcal{B}'_1 \cup \cdots \cup \mathcal{B}'_k$, where each $\mathcal{B}'_i$ is a basis for the corresponding generalized eigenspace, replacing each $\mathcal{B}'_i$ by a basis $\mathcal{B}_i$ in which the restriction of $\mathcal{T}$ to that generalized eigenspace is in JCF, and taking $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$, we get a basis $\mathcal{B}$ with $[\mathcal{T}]_{\mathcal{B}}$ in JCF. (More simply said, if $[\mathcal{T}]_{\mathcal{B}'}$ is block diagonal and we change basis to a basis $\mathcal{B}$ so that each diagonal block is in JCF, i.e., consists of a sequence of Jordan blocks, then $[\mathcal{T}]_{\mathcal{B}}$ consists of a sequence of Jordan blocks, i.e., $[\mathcal{T}]_{\mathcal{B}}$ is in JCF.)

This completes the proof that $\mathcal{T}$ has a JCF. Our theorem also states that the JCF is unique up to order of the blocks. That will be an immediate consequence of our algorithm for determining JCF, so we defer its proof. But we outline an alternate proof, not using this algorithm, in Section 8.6, Exercise 5. □

8.3. An algorithm for Jordan canonical form and a Jordan basis

In this section we present an algorithm for determining the JCF of a linear transformation $\mathcal{T}$, assuming we have factored its characteristic polynomial as $c_{\mathcal{T}}(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k}$, so that we know its eigenvalues.

Actually, our algorithm will determine the ESP of $\mathcal{T}$, but from that we immediately obtain its JCF.

Afterwards, we will see how to elaborate on this algorithm to find the lESP of $\mathcal{T}$, and hence a Jordan basis.

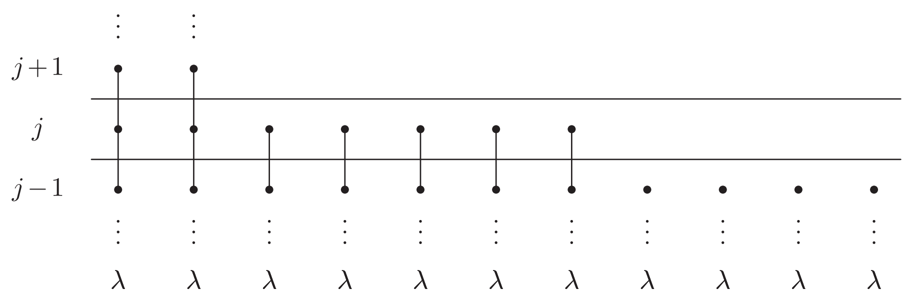
(In principle, our proof of the existence of JCF gives an algorithm for finding both JCF and a Jordan basis, but that algorithm is not at all a practical one—once we know JCF exists, there is a much better way to proceed.)

Consider the ESP of a linear transformation $\mathcal{T}$, which has nodes arranged in chains. Clearly to find the ESP, it suffices to find where the nodes at the top of the chains are. So that is what we do.

We work one eigenvalue at a time, so fix an eigenvalue λ.

We envision starting at the top and working our way down. From this point of view, the nodes at the top of chains are "new" nodes, while the ones that are not at the top of chains lie under nodes we have already seen, so we regard them as "old" nodes. Thus our task is to find all the new nodes.

Suppose we are in the middle of this process, at some height j. Then we see the picture:



Let us set

$$d_j^{\text{new}}(\lambda) = \text{the number of new nodes at height } j \text{ for } \lambda.$$

This is exactly what we hope to find. We find it in stages.

Let us next set

$$d_j^{\text{ex}}(\lambda) = \text{the number of (all) nodes at height (exactly) } j \text{ for } \lambda, \text{ and}$$
$$d_j(\lambda) = \text{the number of (all) nodes at height at most } j \text{ for } \lambda.$$

Clearly a node is at height exactly j if it is at height at most j but not at height at most $j-1$, so we see right away

$$d_j^{\text{ex}}(\lambda) = d_j(\lambda) - d_{j-1}(\lambda) \quad \text{for each } j.$$

(In order to make this work for $j = 1$ we set $d_0(\lambda) = 0$, which is true—there are no nodes at height 0 or below.)

Now how many of these nodes at height j are new? Clearly the number of new nodes is the total number of nodes minus the number of old nodes. But every old node lies immediately below some node at level $j+1$, so we see

$$d_j^{\text{new}}(\lambda) = d_j^{\text{ex}}(\lambda) - d_{j+1}^{\text{ex}}(\lambda) \quad \text{for each } j.$$

(This is true at the top as well, for in that case there are no nodes at a higher height.)

Thus you see we can find $d_j^{\text{new}}(\lambda)$ for every j, and hence the ESP of $\mathcal{T}$, providing we can find $d_j(\lambda)$. But if we were to label the nodes, the labels (i.e., vectors) at height at most λ would be a basis for the generalized eigenspace E_λ^j of generalized eigenvectors of index (i.e., height) at most j. But the dimension of this eigenspace is the number of elements in any basis, i.e., the number of nodes, and so we see

$$d_j(\lambda) = \dim E_\lambda^j \quad \text{for each } j,$$

and this is something we know how to find.

Thus we have obtained the portion of the ESP corresponding to the eigenvalue λ. Do this for each eigenvalue of $\mathcal{T}$, and then we are done.

We now summarize this algorithm.

Algorithm 8.3.1 (Algorithm for Jordan canonical form)**.** Let $\mathcal{T}\colon V \to V$ have characteristic polynomial $c_{\mathcal{T}}(x) = (x-\lambda_1)^{e_1}\cdots(x-\lambda_k)^{e_k}$. For each $i = 1,\ldots,k$:

1. (Set $\lambda = \lambda_i$ and $e = e_i$, to simplify the notation.) For $j = 1, 2, \ldots$ compute

$$d_j(\lambda) = \dim E_\lambda^j.$$

Stop when any of the following equivalent conditions are first reached:

(a) $d_j(\lambda) = e$, the algebraic multiplicity of λ.

(b) $d_{j+1}(\lambda) = d_j(\lambda)$.

(c) $j = f$, where f is the exponent of $x - \lambda$ in $m_{\mathcal{T}}(x)$.

2. (Set $d_{f+1}^{\mathrm{ex}}(\lambda) = 0$ and $d_0(\lambda) = 0$ to simplify the notation.) For $j = f, f-1, \ldots, 1$ compute

$$d_j^{\mathrm{ex}}(\lambda) = d_j(\lambda) - d_{j-1}(\lambda)$$

and

$$d_j^{\mathrm{new}}(\lambda) = d_j^{\mathrm{ex}}(\lambda) - d_{j-1}^{\mathrm{ex}}(\lambda) = 2d_j(\lambda) - (d_{j+1}(\lambda) + d_{j-1}(\lambda)).$$

Then for each $j = 1,\ldots,f$, the portion of the ESP of $\mathcal{T}$ corresponding to λ has $d_j^{\mathrm{new}}(\lambda)$ chains of height j. $\Diamond$

Remark 8.3.2. We may equivalently phrase the conclusion of this algorithm as:

Then for each $j = 1,\ldots,f$, the JCF of $\mathcal{T}$ has $d_j^{\mathrm{new}}(\lambda)$ j-by-j Jordan blocks with diagonal entry λ. $\Diamond$

Conclusion of the proof of Theorem 8.1.6. We have shown that $\mathcal{T}$ has a JCF. We need to show the JCF is unique up to the order of the blocks. But this algorithm shows that the number and sizes of the Jordan blocks are determined by

$$\dim E_\lambda^j$$

for each eigenvalue λ of $\mathcal{T}$ and each integer j, and this is well-defined (i.e., depends on $\mathcal{T}$ alone and not on any choices). $\square$

Now we turn to the problem of finding the lESP. Since we have already found the ESP, this is a matter of finding the labels on the nodes.

Of course, once we have found these labels (i.e., vectors), arranging them into chains will give us a Jordan basis $\mathcal{B}$.

Again we work one eigenvalue λ at a time.

Again let us work from the top down, and imagine ourselves in the middle of the process, at height j, where we see the same picture as before.

The vectors labelling the new nodes at level j are part of a basis for E_λ^j. The other vectors in the basis are of two kinds:

(1) The labels on old nodes at level j. We know exactly what these are, as (since we are working from the top down) we know the labels on (all of) the nodes at level $j+1$, so if a node at level $j+1$ is labelled by a vector u_{j+1}, the node at level j below it is the next vector in its chain, $u_j = (\mathcal{T} - \lambda\mathcal{I})(u_{j+1})$.

(2) The labels on the nodes at all levels below j. Of course, we don't know these yet—but it doesn't matter! These vectors are a basis for the space E_λ^{j-1}, and any basis is as good as any other. We certainly know how to find a basis of E_λ^{j-1}, so we use that basis instead.

Thus if we take the union of the labels on old nodes at level j with any basis of E_λ^{j-1}, this will be part of a basis for E_λ^j. Then we extend it to a basis of E_λ^j, and the labels on the new nodes will just be the new vectors we have added to form the basis. Given this logic, we now formulate our algorithm.

Algorithm 8.3.3 (Algorithm for a Jordan basis)**.** Let $\mathcal{T}\colon V \to V$ have characteristic polynomial $c_{\mathcal{T}}(x) = (x-\lambda_1)^{e_1}\cdots(x-\lambda_k)^{e_k}$. For each $i = 1, \ldots, j$:

(Set $\lambda = \lambda_i$, to simplify the notation. Let f be the highest height of a generalized eigenvector. Set $F_\lambda^{f+1} = \{0\}$ and $E_\lambda^0 = \{0\}$, also to simplify the notation.)

For $j = f, f-1, \ldots, 1$:

Let F_λ^{f+1} have basis $\{u_{j+1}^1, \ldots, u_{j+1}^r\}$. Set $u_j^i = (\mathcal{T} - \lambda\mathcal{I})(u_{j+1}^i)$ for each $i = 1, \ldots, r$.

Let E_λ^{j-1} have basis $\{v^1, \ldots, v^s\}$. (We do not care what the heights of the individual vectors in this basis are.)

Extend $\{u_j^1, \ldots, u_j^r, v^1, \ldots, v^s\}$ to a basis

$$\mathcal{B} = \{u_j^1, \ldots, u_j^r, v^1, \ldots, v^s, w_j^1, \ldots w_j^t\}$$

of E_λ^j. Then

$$\{w_j^1, \ldots, w_j^t\}$$

are the labels on the new nodes at height j.

Let $F_\lambda^j = \{u_j^1, \ldots, u_j^r, w_j^1, \ldots, w_j^t\}$ (these being the labels on all the nodes at level j) and move down to the next lower value of j.

When we have finished we have obtained vectors labelling all the nodes in the ESP, i.e., we have found the lESP. Order these vectors into chains to obtain a Jordan basis $\mathcal{B}$. $\Diamond$

Remark 8.3.4. Note that while we have to compute the vectors $\{v^1, \ldots, v^s\}$ for each j, these vectors may not (and usually will not) in the end be part of the Jordan basis. $\Diamond$

We illustrate our algorithm with several examples.

Example 8.3.5. (1) Consider

$$A = \begin{bmatrix} 7 & 0 & 0 & 0 & -2 \\ -5 & 2 & -1 & 1 & 2 \\ -5 & 1 & 5 & -1 & 2 \\ -15 & 1 & 3 & 2 & 6 \\ 10 & 0 & 0 & 0 & -2 \end{bmatrix}$$

with $c_A(x) = (x-3)^4(x-2)$.

For $\lambda = 2$, we have that E_2^1 is 1-dimensional with basis

$$\left\{ \begin{bmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 5 \end{bmatrix} \right\}.$$

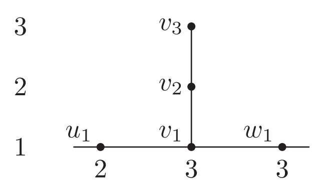
Let $\lambda = 3$. We see that

E_3^1 has basis $\left\{ \begin{bmatrix} 1 \\ -3 \\ 2 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \right\}$ so is 2-dimensional;

E_3^2 has basis $\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -2 \\ 1 \\ 0 \\ 0 \end{bmatrix} \right\}$ so is 3-dimensional;

E_3^3 has basis $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \right\}$ so is 4-dimensional.

Hence we see that A has lESP



with the labels yet to be determined.

For $\lambda = 2$, we take $u_1 = \begin{bmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 5 \end{bmatrix}$.

For $\lambda = 3$, working from the top down, we choose v_3 to be any vector that extends the above basis of E_3^2 to a basis of E_3^3. We choose

$$v_3 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Then

$$v_2 = (A - 3I)(v_3) = \begin{bmatrix} 0 \\ 1 \\ -1 \\ -1 \\ 0 \end{bmatrix} \quad \text{and} \quad v_1 = (A - 3I)(v_2) = \begin{bmatrix} 0 \\ -1 \\ 0 \\ -1 \\ 0 \end{bmatrix}.$$

We extend $\{v_1\}$ to a basis $\{v_1, w_1\}$ of E_3^1. Given the basis above, we can choose

$$w_1 = \begin{bmatrix} 1 \\ -3 \\ 2 \\ 0 \\ 2 \end{bmatrix},$$

and we have found all the labels.

To summarize, A has JCF

$$\begin{bmatrix} 2 & & & & \\ & 3 & 1 & & \\ & & 3 & 1 & \\ & & & 3 & \\ & & & & 3 \end{bmatrix},$$

$\mathcal{B}$ is the Jordan basis $\{u_1, v_1, v_2, v_3, w_1\}$ for these values of the vectors, and $J = P^{-1}AP$, where P is the matrix whose columns are the vectors in $\mathcal{B}$. Also, we see $m_A(x) = (x-3)^3(x-2)$.

(2) Consider

$$A = \begin{bmatrix} -18 & 3 & 78 & -48 & 24 \\ -12 & 2 & 65 & -40 & 16 \\ -16 & 0 & 0 & 0 & 24 \\ -26 & 0 & 0 & 0 & 39 \\ -12 & 2 & 52 & -32 & 16 \end{bmatrix}$$

with $c_A(x) = x^5$.

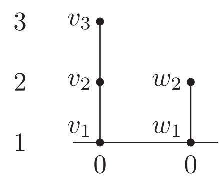
We compute

$$E_0^1 \text{ has basis } \left\{ \begin{bmatrix} 0 \\ 0 \\ 8 \\ 13 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ 0 \\ 0 \\ 2 \end{bmatrix} \right\} \text{ so is 2-dimensional;}$$

$$E_0^2 \text{ has basis } \left\{ \begin{bmatrix} 0 \\ 0 \\ 8 \\ 13 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right\} \text{ so is 4-dimensional;}$$

$E_0^3 = \mathbb{F}^5$ so is 5-dimensional.

Hence we see that A has lESP



with the labels yet to be determined.

To find v_3 we extend the above basis for E_0^2 to a basis for $E_0^3 = \mathbb{F}^5$. We choose

$$v_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

Then

$$v_2 = (A - 0I)v_3 = \begin{bmatrix} 78 \\ 65 \\ 0 \\ 0 \\ 52 \end{bmatrix} \qquad \text{and} \qquad v_1 = (A - 0I)v_2 = \begin{bmatrix} 39 \\ 26 \\ 0 \\ 0 \\ 26 \end{bmatrix}.$$

(Of course, $A - 0I = A$; we are just writing $A - 0I$ for emphasis.)

Now to find w_2 we extend

$$\left\{ \begin{bmatrix} 78 \\ 65 \\ 0 \\ 0 \\ 52 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 8 \\ 13 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ 0 \\ 0 \\ 2 \end{bmatrix} \right\}$$

to a basis of E_0^2. (Note the first vector above is v_2 and the last two vectors are the basis we found for E_0^1.) We choose

$$w_2 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

and then

$$w_1 = (A - 0I)w_2 = \begin{bmatrix} 24 \\ 16 \\ 24 \\ 39 \\ 16 \end{bmatrix},$$

and we have found all the labels.

To summarize, A has JCF

$$J = \begin{bmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & & \\ & & & 0 & 1 \\ & & & & 0 \end{bmatrix},$$

$\mathcal{B}$ is the Jordan basis $\{v_1, v_2, v_3, w_1, w_2\}$ for these values of the vectors, and $J = P^{-1}AP$, where P is the matrix whose columns are the vectors in $\mathcal{B}$. Also, we see $m_A(x) = x^3$. $\Diamond$

8.4. Application to systems of first-order differential equations

In this section we show how to apply our results to solve systems of first-order linear differential equations. First we give some theory, and then we turn to practice. We will be brief with the theory, as it is entirely analogous to what we have considered before for a single higher-order differential equation.

We let I be an open interval in $\mathbb{R}$, and we let V be the $\mathbb{C}$-vector space

$$V = \left\{ X(t) = \begin{bmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{bmatrix} \;\middle|\; \text{each } x_i(t) \text{ is a complex-valued } C^\infty \text{ function on } I \right\}.$$

Theorem 8.4.1. *Let $A(t) = (a_{ij}(t))$ be an n-by-n matrix with each $a_{ij}(t)$ a complex-valued C^∞ function on I. Let $B(t) = \begin{bmatrix} b_1(t) \\ \vdots \\ b_n(t) \end{bmatrix}$ be any element of V. Let t_0 be any point in I, and let $X_0 = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$ be any vector in $\mathbb{C}^n$.*

Then the equation

$$X'(t) = A(t)X(t) + B(t), \quad X(t_0) = X_0$$

has a unique solution.

Translated into linear algebra, this theorem says:

Theorem 8.4.2. *In the situation of Theorem 8.4.1, let*

$$\mathcal{L}(X(t)) = X'(t) - A(t)X(t).$$

Then $\mathrm{Ker}(\mathcal{L})$ *is an* n*-dimensional subspace of* V*, and for any* $B(t)$*,*

$$\{X(t)\,|\,\mathcal{L}(X(t)) = B(t)\}$$

is an affine subspace of V *parallel to* $\mathrm{Ker}(\mathcal{L})$*.*

Thus to solve the homogeneous equation $\mathcal{L}(X(t)) = 0$, i.e., the equation $X'(t) = A(t)X(t)$, we merely have to find a basis for the solution space, and then take linear combinations.

Lemma 8.4.3. *For* $i = 1, \ldots, n$*, let*

$$X^i(t) = \begin{bmatrix} x_1^i(t) \\ \vdots \\ x_n^i(t) \end{bmatrix}$$

be a vector in $\mathrm{Ker}(\mathcal{L})$*. The following are equivalent:*

(1) $\{X^1(t), \ldots, X^n(t)\}$ *is a basis for* $\mathrm{Ker}(\mathcal{L})$*.*

(2) *For some* t_0 *in* I*,* $\{X^1(t_0), \ldots, X^n(t_0)\}$ *is linearly independent.*

(3) *For every* t_0 *in* I*,* $\{X^1(t_0), \ldots, X^n(t_0)\}$ *is linearly independent.*

Remark 8.4.4. Of course, condition (1) is equivalent to the condition that the matrix

$$\mathcal{X}(t) = \left[X^1(t)|\cdots|X^n(t)\right]$$

is nonsingular, and that will be true if and only if its determinant $\det(\mathcal{X}(t)) \neq 0$. (By condition (2), that will be true if and only if $\det(\mathcal{X}(t_0)) \neq 0$ for some t_0.) $\Diamond$

Remark 8.4.5. If the matrix $\mathcal{X}(t)$ is nonsingular, then the general solution of $X'(t) = A(t)X(t)$ will be given by

$$X(t) = \mathcal{X}(t)C,$$

where $C = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$ is an arbitrary vector of constants. $\Diamond$

Now we turn to practice. We suppose that A has constant entries, $A = (a_{ij})$.

One case is very easy to solve.

Lemma 8.4.6. *Let* D *be the diagonal matrix*

$$D = \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{bmatrix}.$$

Then

$$X'(t) = DX(t)$$

has solution

$$X(t) = \begin{bmatrix} e^{d_1 t} & & \\ & \ddots & \\ & & e^{d_n t} \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \mathcal{X}(t)C.$$

Proof. Writing out this system, we see it is just the system

$$x_1'(t) = d_1 x_1(t)$$
$$\dots$$
$$x_n'(t) = d_n x_n(t),$$

a system which is completely "uncoupled", i.e., in which we have n differential equations, with the ith equation just involving the function $x_i(t)$ and none of the others. Thus we can solve each equation individually and just assemble the answers. But the differential equation

$$x'(t) = dx(t)$$

simply has the general solution

$$x(t) = ce^{dt},$$

where c is an arbitrary constant. □

This now gives us a method of solving $X'(t) = AX(t)$ whenever A is diagonalizable.

Method 8.4.7. To solve $X'(t) = AX(t)$ when A is diagonalizable:

(1) Find a diagonal matrix D and an invertible matrix P such that $D = P^{-1}AP$, or equivalently $A = PDP^{-1}$.

(2) Substitute in the original differential equation:

$$X'(t) = PDP^{-1}X(t),$$
$$P^{-1}X'(t) = DP^{-1}X(t).$$

(3) Set $Y(t) = P^{-1}X(t)$ and observe that $Y'(t) = (P^{-1}X(t))' = P^{-1}X'(t)$ as P^{-1} is a matrix of constants. Substitute to obtain

$$Y'(t) = DY(t).$$

(4) Solve this system for $Y(t)$ to obtain

$$Y(t) = \mathcal{Y}(t)C.$$

(5) Then

$$\begin{aligned} X(t) &= PY(t) \\ &= \mathcal{X}(t)C, \end{aligned}$$

where

$$\mathcal{X}(t) = P\mathcal{Y}(t).$$ ◊

Remark 8.4.8. Note that in applying this method, we never actually had to evaluate P^{-1}. All we had to do was find P and D. ◊

Example 8.4.9. Consider the system $X'(t) = AX(t)$, where

$$A = \begin{bmatrix} 1 & 4 & -2 \\ -10 & 6 & 0 \\ -14 & 11 & -1 \end{bmatrix}.$$

We saw in Example 7.4.13(2) that A is diagonalizable, $D = P^{-1}AP$, with

$$D = \begin{bmatrix} 1 & & \\ & 2 & \\ & & 3 \end{bmatrix} \quad \text{and} \quad P = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 10 \\ 4 & 9 & 17 \end{bmatrix}.$$

We solve $Y'(t) = DY(t)$ to obtain

$$Y(t) = \mathcal{Y}(t)C = \begin{bmatrix} e^t & & \\ & e^{2t} & \\ & & e^{3t} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

and then

$$X(t) = PY(t) = \mathcal{X}(t)C$$

with

$$\mathcal{X}(t) = P\mathcal{Y}(t),$$

i.e.,

$$\mathcal{X}(t) = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 10 \\ 4 & 9 & 17 \end{bmatrix} \begin{bmatrix} e^t & & \\ & e^{2t} & \\ & & e^{3t} \end{bmatrix} = \begin{bmatrix} e^t & 2e^{2t} & 3e^{3t} \\ 2e^t & 5e^{2t} & 10e^{3t} \\ 4e^t & 9e^{2t} & 17e^{3t} \end{bmatrix}$$

and then

$$X(t) = \mathcal{X}(t) \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} c_1e^t + 2c_2e^{2t} + 3c_3e^{3t} \\ 2c_1e^t + 5c_2e^{2t} + 10c_3e^{3t} \\ 4c_1e^t + 9c_2e^{2t} + 17c_3e^{3t} \end{bmatrix}. \qquad \Diamond$$

Now we turn to the general case. Here we have to begin by looking at the situation where A is a single Jordan block and proving the analog of Lemma 8.4.6.

Lemma 8.4.10. *Let J be an h-by-h Jordan block associated to the eigenvalue λ, i.e., the h-by-h matrix*

$$J = \begin{bmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & & \\ & & & & 1 \\ & & & & \lambda \end{bmatrix}.$$

Then

$$X'(t) = JX(t)$$

has solution

$$X(t) = \begin{bmatrix} e^{\lambda t} & te^{\lambda t} & (t^2/2)e^{\lambda t} & \dots & (t^{h-1}/(h-1)!)e^{\lambda t} \\ & e^{\lambda t} & te^{\lambda t} & & \vdots \\ & & e^{\lambda t} & & \vdots \\ & & & \ddots & te^{\lambda t} \\ & & & & e^{\lambda t} \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ \vdots \\ \\ c_h \end{bmatrix} = \mathcal{X}(t)C.$$

Proof. Again when we write this system out we see it is

$$\begin{aligned} x_1'(t) &= \lambda x_1(t) + x_2(t) \\ &\vdots \\ x_{h-1}'(t) &= \lambda x_{h-1}(t) + x_h(t) \\ x_h'(t) &= \lambda x_h(t) \end{aligned}$$

i.e.,

$$\begin{aligned} x_1'(t) - \lambda x_1(t) &= x_2(t) \\ &\vdots \\ x_{h-1}'(t) - \lambda x_{h-1}(t) &= x_h(t) \\ x_h'(t) - \lambda x_h(t) &= 0. \end{aligned}$$

This system is no longer uncoupled, but note we can solve from the bottom up: the last equation just involves $x_h(t)$, so we can solve for it, then substitute in the next-to-the-last equation to obtain an equation just involving $x_{h-1}(t)$, and solve for it, etc. It is then routine to verify that we obtain $X(t)$ as claimed. □

Given this lemma, we have a method for solving $X'(t) = AX(t)$ which uses the exact same strategy as the diagonalizable case.

Method 8.4.11. To solve $X'(t) = AX(t)$ in general:

(1) Find a matrix J in JCF and an invertible matrix P such that $J = P^{-1}AP$, or equivalently $A = PJP^{-1}$.

(2) Substitute to obtain
$$P^{-1}X'(t) = JP^{-1}X(t).$$

(3) Set $Y(t) = P^{-1}X(t)$ and substitute to obtain
$$Y'(t) = JY(t).$$

(4) Solve to obtain
$$Y(t) = \mathcal{Y}(t)C.$$

(5) Then
$$X(t) = PY(t) = \mathcal{X}(t)C, \quad \text{where } \mathcal{X}(t) = PY(t).$$ ◊

Example 8.4.12. Consider the system $X'(t) = AX(t)$, where

$$A = \begin{bmatrix} 1 & 4 & -4 \\ -2 & 7 & 4 \\ -1 & 2 & 1 \end{bmatrix}.$$

You may check that $J = P^{-1}AP$ with

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

We solve $Y'(t) = JY(t)$ to obtain

$$Y(t) = \mathcal{Y}(t)C = \begin{bmatrix} e^{3t} & te^{3t} & \\ & e^{3t} & \\ & & e^{3t} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

and then

$$\mathcal{X}(t) = P\mathcal{Y}(t) = \begin{bmatrix} -2 & 1 & 0 \\ -2 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} e^{3t} & te^{3t} & \\ & e^{3t} & \\ & & e^{3t} \end{bmatrix} = \begin{bmatrix} -2e^{3t} & -2te^{3t} + e^{3t} & 0 \\ -2e^{3t} & -2te^{3t} & e^{3t} \\ e^{3t} & te^{3t} & e^{3t} \end{bmatrix}$$

and then

$$X(t) = \mathcal{X}(t) \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} (-2c_1 + c_2)e^{3t} - 2c_2te^{3t} \\ (-2c_1 + c_3)e^{3t} - 2c_2te^{3t} \\ (c_1 + c_3)e^{3t} + c_2te^{3t} \end{bmatrix}. \qquad \Diamond$$

As before, this method can be refined to always express the solution in terms of real-valued functions whenever all the entries of A are real, and also to handle some nonhomogeneous systems, but we will stop here.

8.5. Further results

We have two goals in this section.

First, we will derive some results—which should be better known than they are—about the relationship between linear transformations $\mathcal{ST}$ and $\mathcal{TS}$, for any pair of linear transformations $\mathcal{S}$ and $\mathcal{T}$ (for which both compositions make sense).

Second, we will outline a generalization of Jordan canonical form to linear transformations that do not satisfy Hypothesis (S). But this is only of secondary importance, so we will simply state the results without providing full details.

Suppose $\mathcal{S}\colon V \to V$ and $\mathcal{T}\colon V \to V$ are two linear transformations. As we have observed, if at least one of $\mathcal{S}$ and $\mathcal{T}$ is invertible, then $\mathcal{ST}$ and $\mathcal{TS}$ are conjugate, but if neither is invertible, they may not be. (Expressed in terms of matrices, if we choose a basis $\mathcal{B}$ of V, and set $A = [\mathcal{S}]_{\mathcal{B}}$ and $B = [\mathcal{T}]_{\mathcal{B}}$, then if at least one of A and B is invertible, AB and BA are similar, but if neither is invertible, they need not be.) We can ask, in general, what is the relationship between $\mathcal{ST}$ and $\mathcal{TS}$ (or between AB and BA)?

It turns out that exactly the same arguments enable us to deal with a more general situation, so we do that.

The key to our result is the following lemma.

Lemma 8.5.1. *Let $\mathcal{T}\colon V \to W$ and $\mathcal{S}\colon W \to V$ be linear transformations (so that $\mathcal{ST}\colon V \to V$ and $\mathcal{TS}\colon W \to W$ are both defined). Then for any polynomial $p(x) = a_dx^d + \cdots + a_0$ with constant term $a_0 \neq 0$,*

$$\dim \operatorname{Ker}(p(\mathcal{ST})) = \dim \operatorname{Ker}(p(\mathcal{TS})).$$

Proof. First let us see that if v is any vector in $\operatorname{Ker}(p(\mathcal{ST}))$, then $\mathcal{T}(v)$ is a vector in $\operatorname{Ker}(p(\mathcal{TS}))$. (This is true for any polynomial $p(x)$, whether or not its constant term is nonzero.) To this end, let us first observe

$$\begin{aligned}
\mathcal{I}\mathcal{T} &= \mathcal{T}\mathcal{I},\\
(\mathcal{T}\mathcal{S})\mathcal{T} &= \mathcal{T}(\mathcal{S}\mathcal{T}),\\
(\mathcal{T}\mathcal{S})^2\mathcal{T} &= (\mathcal{T}\mathcal{S})(\mathcal{T}\mathcal{S})\mathcal{T} = \mathcal{T}(\mathcal{S}\mathcal{T})(\mathcal{S}\mathcal{T}) = \mathcal{T}(\mathcal{S}\mathcal{T})^2,\\
&\cdots\\
(\mathcal{T}\mathcal{S})^d\mathcal{T} &= \mathcal{T}(\mathcal{S}\mathcal{T})^d.
\end{aligned}$$

But then

$$\begin{aligned}
p(\mathcal{T}\mathcal{S})(\mathcal{T}(v)) &= a_d(\mathcal{T}\mathcal{S})^d\mathcal{T}(v) + \cdots + a_1(\mathcal{T}\mathcal{S})\mathcal{T}(v) + a_0\mathcal{I}\mathcal{T}(v)\\
&= a_d\mathcal{T}(\mathcal{S}\mathcal{T})^d(v) + \cdots + a_1\mathcal{T}(\mathcal{S}\mathcal{T})(v) + a_0\mathcal{T}\mathcal{I}(v)\\
&= \mathcal{T}(a_d(\mathcal{S}\mathcal{T})^d(v) + \cdots + a_1(\mathcal{S}\mathcal{T})(v) + a_0\mathcal{I}(v))\\
&= \mathcal{T}(0) = 0.
\end{aligned}$$

Now let $\{v_1, \ldots, v_s\}$ be any basis for $\mathrm{Ker}(p(\mathcal{S}\mathcal{T}))$. We claim that in this case $\{\mathcal{T}(v_1), \ldots, \mathcal{T}(v_s)\}$ is linearly independent. To see this, suppose that

$$c_1\mathcal{T}(v_1) + \cdots + c_s(\mathcal{T}_s) = 0.$$

Then

$$\mathcal{T}(c_1v_1 + \cdots + c_sv_s) = 0$$

and so certainly

$$\mathcal{S}\mathcal{T}(c_1v_1 + \cdots + c_sv_s) = 0.$$

Thus, setting $v = c_1v_1 + \cdots + c_sv_s$, we have $\mathcal{S}\mathcal{T}(v) = 0$, i.e., $v \in \mathrm{Ker}(\mathcal{S}\mathcal{T})$. But then

$$0 = p(\mathcal{S}\mathcal{T})(v) = a_d(\mathcal{S}\mathcal{T})^d(v) + \cdots + a_1(\mathcal{S}\mathcal{T})(v) + a_0\mathcal{I}v = a_0v$$

and since we are assuming $a_0 \neq 0$, we must have $v = 0$, i.e., $c_1v_1 + \cdots + c_sv_s = 0$. But $\{v_1, \ldots, v_s\}$ was a basis of $\mathrm{Ker}(p(\mathcal{S}\mathcal{T}))$, hence linearly independent, so $c_1 = \cdots = c_s = 0$ as claimed.

Hence we see that $\mathrm{Ker}(p(\mathcal{T}\mathcal{S}))$ contains a linearly independent set of s vectors, so $\dim \mathrm{Ker}(p(\mathcal{T}\mathcal{S})) \geq s = \dim \mathrm{Ker}(p(\mathcal{S}\mathcal{T}))$. Reversing the roles of $\mathcal{S}$ and $\mathcal{T}$ shows $\dim \mathrm{Ker}(p(\mathcal{S}\mathcal{T})) \geq \dim \mathrm{Ker}(p(\mathcal{T}\mathcal{S}))$, so they are equal. □

Theorem 8.5.2. *Let $\mathcal{T}: V \to W$ and $\mathcal{S}: W \to V$ be linear transformations.*

(1) *Suppose that $\mathbb{F}$ is algebraically closed, so that every linear transformation satisfies Hypothesis* (S). *Then $\mathcal{S}\mathcal{T}$ and $\mathcal{T}\mathcal{S}$ have the same nonzero eigenvalues and furthermore for every common eigenvalue $\lambda \neq 0$, $\mathcal{S}\mathcal{T}$ and $\mathcal{T}\mathcal{S}$ have the same ESP at λ (i.e., the same number of Jordan blocks with the same sizes associated to λ).*

(2) *If $\dim V = \dim W = n$, then $\mathcal{S}\mathcal{T}$ and $\mathcal{T}\mathcal{S}$ have the same characteristic polynomial, $c_{\mathcal{S}\mathcal{T}}(x) = c_{\mathcal{T}\mathcal{S}}(x)$. If $\dim V = n$ and $\dim W = m$, with $n > m$ (resp., $n < m$), then $c_{\mathcal{S}\mathcal{T}}(x) = x^{n-m}c_{\mathcal{T}\mathcal{S}}(x)$ (resp., $c_{\mathcal{T}\mathcal{S}}(x) = x^{m-n}c_{\mathcal{S}\mathcal{T}}(x)$).*

Proof. (1) As our algorithm for JCF shows, the portion of the ESP of a linear transformation $\mathcal{R}$ at an eigenvalue $\lambda \neq 0$ is entirely determined by $\dim \mathrm{Ker}((x-\lambda)^d)$ for every d, and these dimensions are all equal for $\mathcal{R}_1 = \mathcal{S}\mathcal{T}$ and $\mathcal{R}_2 = \mathcal{T}\mathcal{S}$ by Lemma 8.5.1.

(2) Passing to the algebraic closure of $\mathbb{F}$ if necessary, we know that $c_{\mathcal{ST}}(x) = x^{n-k}p_1(x)$, where $p_1(x)$ consists of the product of all other irreducible factors of $c_{\mathcal{ST}}(x)$, and similarly $c_{\mathcal{TS}}(x) = x^{m-k}p_2(x)$. But by part (1), $p_1(x) = p_2(x)$ (and k is the common sum of the algebraic multiplicities of the nonzero eigenvalues). □

We give an example, using matrices, where we can easily calculate characteristic polynomials and find eigenvalues. For emphasis, we give an example where AB and BA have different sizes.

Example 8.5.3. Let A be the matrix $A = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \end{bmatrix}$, and let B be the matrix $B = \begin{bmatrix} 2 & 3 \\ 1 & 4 \\ 1 & 1 \end{bmatrix}$. Then

$$AB = \begin{bmatrix} 6 & 11 \\ 5 & 12 \end{bmatrix} \quad \text{and} \quad BA = \begin{bmatrix} 7 & 8 & 5 \\ 6 & 9 & 5 \\ 3 & 3 & 2 \end{bmatrix}.$$

You can check that AB has eigenvalues 1, 17 and that BA has eigenvalues 0, 1, 17. ◊

Now for our second goal.

Definition 8.5.4. (1) Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a monic polynomial of degree n. The *companion matrix* of $f(x)$ is the n-by-n matrix

$$C(f(x)) = \begin{bmatrix} -a_{n-1} & 1 & 0 & & 0 \\ -a_{n-2} & 0 & 1 & & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_1 & 0 & 0 & & 1 \\ -a_0 & 0 & 0 & & 0 \end{bmatrix}.$$

(The 1's are immediately above the diagonal.)

(2) More generally, let h be a positive integer. A *generalized Jordan block* associated to $f(x)$ is the nh-by-nh matrix

$$\tilde{J} = C_h(f(x)) = \begin{bmatrix} C(f(x)) & N & & \\ & C(f(x)) & & \\ & & \ddots & N \\ & & & C(f(x)) \end{bmatrix},$$

where $C(f(x))$ is the companion matrix of $f(x)$ (a d-by-d matrix), there are h diagonal blocks, and each of the $h-1$ blocks N immediately above the diagonal is an n-by-n matrix with 1 in the lower left-hand corner (i.e., in position $(n,1)$) and all other entries 0. ◊

Lemma 8.5.5. (1) *Let $A = C(f(x))$, where $f(x)$ is a monic polynomial of degree n. Then*

$$m_{A,e_n}(x) = m_A(x) = c_A(x) = f(x).$$

(2) *More generally, let $A = C_h(f(x))$. Then*

$$m_{A,e_{nh}}(x) = m_A(x) = c_A(x) = f(x)^h.$$

Proof. We leave this as an exercise for the reader. □

Remark 8.5.6. Observe that if $f(x) = x - \lambda$, then $C(f(x)) = [\lambda]$, so the Jordan h-block associated to $x - \lambda$ is simply an h-by-h Jordan block with all diagonal entries equal to λ. ♢

Theorem 8.5.7. *Let $\mathcal{T}\colon V \to V$ be a linear transformation. Factor the characteristic polynomial $c_{\mathcal{T}}$ as $c_{\mathcal{T}} = f_1(x)^{d_1} \cdots f_k(x)^{d_k}$, a product of powers of distinct irreducible polynomials. Then V has a basis $\mathcal{B}$ in which*

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} \tilde{J}_1 & & \\ & \tilde{J}_2 & \\ & & \ddots \end{bmatrix}$$

in which each $\tilde{J}_i$ is $C_h(f(x))$ for some h and for some $f(x) = f_1(x), \ldots, f_k(x)$.

Furthermore, $[\mathcal{T}]_{\mathcal{B}}$ is unique up to the order of the blocks.

Definition 8.5.8. A matrix as in the conclusion of this theorem is said to be in generalized Jordan canonical form. ♢

We conclude by noting how Theorem 8.5.2 generalizes to this situation.

Theorem 8.5.9. *Let $\mathcal{T}\colon V \to W$ and $\mathcal{S}\colon W \to V$ be linear transformations. Then in the generalized JCF's of $\mathcal{S}\mathcal{T}$ and $\mathcal{T}\mathcal{S}$, the generalized Jordan blocks associated to all irreducible polynomials other than the polynomial x correspond.*

8.6. Exercises

1. In each case, find

(1) the characteristic polynomial $c_A(x)$ (when it is not already given),

(2) the eigenvalues, their algebraic and geometric multiplicities,

(3) the minimal polynomial $m_A(x)$,

(4) the JCF of A and a Jordan basis for $\mathbb{R}^n$.

(a) $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 3 \\ 0 & 0 & 3 \end{bmatrix}$.

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

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

(d) $A = \begin{bmatrix} 5 & 1 & 0 & -1 \\ 0 & 6 & 0 & -1 \\ 0 & 0 & 7 & -2 \\ 0 & 0 & 0 & 5 \end{bmatrix}$.

(e) $A = \begin{bmatrix} 4 & 0 & 4 & 0 \\ 2 & 1 & 3 & 0 \\ -1 & 0 & 0 & 0 \\ 3 & 0 & 4 & 1 \end{bmatrix}$.

(f) $A = \begin{bmatrix} 4 & -3 & -4 & 3 \\ 4 & -3 & -8 & 7 \\ -4 & 4 & 6 & -4 \\ -4 & 4 & 2 & 0 \end{bmatrix}$, $c_A(x) = x(x-1)(x-2)(x-4)$.

(g) $A = \begin{bmatrix} -4 & -3 & 0 & 9 \\ 2 & 2 & 1 & -2 \\ 2 & 0 & 3 & -2 \\ -6 & -3 & 0 & 11 \end{bmatrix}$, $c_A(x) = (x-2)^2(x-3)(x-5)$.

(h) $A = \begin{bmatrix} 4 & 2 & 1 & -6 \\ -16 & 4 & -16 & 0 \\ -6 & -1 & -3 & 4 \\ -6 & 1 & 6 & 2 \end{bmatrix}$, $c_A(x) = x^2(x-3)(x-4)$.

(i) $A = \begin{bmatrix} -9 & 8 & -16 & -10 \\ 4 & -7 & 16 & 4 \\ 2 & -5 & 11 & 2 \\ 12 & -8 & 16 & 13 \end{bmatrix}$, $c_A(x) = (x-1)^2(x-3)^2$.

(j) $A = \begin{bmatrix} 5 & 0 & 2 & 1 \\ 0 & 2 & 1 & 1 \\ -2 & 0 & 0 & -2 \\ 2 & -2 & 5 & 7 \end{bmatrix}$, $c_A(x) = (x-3)^2(x-4)^2$.

(k) $A = \begin{bmatrix} 2 & 1 & -2 & 0 \\ -4 & -6 & -15 & -4 \\ 1 & 2 & 8 & 1 \\ 8 & 15 & 23 & 10 \end{bmatrix}$, $c_A(x) = (x-2)^2(x-5)^2$.

(l) $A = \begin{bmatrix} -7 & -20 & -40 & -100 \\ 4 & 11 & 16 & 40 \\ -4 & -8 & -13 & -40 \\ 2 & 4 & 8 & 23 \end{bmatrix}$, $c_A(x) = (x-2)^3(x-5)$.

(m) $A = \begin{bmatrix} 2 & 1 & 0 & -1 \\ -3 & 6 & -4 & -1 \\ -1 & 1 & 0 & 0 \\ -2 & 6 & -4 & -1 \end{bmatrix}$, $c_A(x) = (x-1)^3(x-4)$.

(n) $A = \begin{bmatrix} -1 & 4 & -4 & 4 \\ 2 & -3 & 4 & -4 \\ -6 & 12 & -11 & 12 \\ -10 & 20 & -20 & 21 \end{bmatrix}$, $c_A(x) = (x-1)^3(x-3)$.

(o) $A = \begin{bmatrix} 8 & 64 & -14 & -49 \\ -1 & -8 & 2 & 7 \\ 0 & 0 & 4 & 16 \\ 0 & 0 & -1 & -4 \end{bmatrix}$, $c_A(x) = x^4$.

(p) $A = \begin{bmatrix} 4 & 1 & -1 & 2 \\ -2 & 7 & -2 & 4 \\ 3 & -3 & 8 & -6 \\ 2 & -2 & 2 & 1 \end{bmatrix}$, $c_A(x) = (x-5)^4$.

(q) $A = \begin{bmatrix} 7 & -2 & -1 & 3 \\ 1 & 3 & 0 & 1 \\ 1 & -1 & 4 & 1 \\ -2 & 1 & 1 & 2 \end{bmatrix}$, $c_A(x) = (x-4)^4$.

(r) $A = \begin{bmatrix} 3 & 1 & -3 & 1 & 2 \\ -1 & 2 & -5 & 1 & 4 \\ 1 & 1 & -7 & 1 & 5 \\ -2 & -2 & 16 & -1 & -10 \\ 2 & 2 & -16 & 2 & 11 \end{bmatrix}$, $c_A(x) = (x-1)^2(x-2)^3$.

(s) $A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ -4 & 1 & 1 & 2 & 2 \\ -6 & -3 & 3 & 1 & 3 \\ -2 & -1 & 0 & 4 & 1 \\ -10 & -3 & 1 & 4 & 8 \end{bmatrix}$, $c_A(x) = (x-3)^3(x-4)^2$.

(t) $A = \begin{bmatrix} 3 & -7 & 6 & -4 & 1 & 4 \\ -2 & -2 & 3 & -1 & 3 & 2 \\ -2 & -5 & 6 & -1 & 3 & 2 \\ 2 & -3 & 3 & -1 & -1 & -3 \\ -2 & -8 & 6 & -3 & 6 & 4 \\ 2 & -1 & 1 & -2 & -1 & 4 \end{bmatrix}$, $c_A(x) = (x-1)(x-3)^5$.

2. For each of the matrices A in the preceding problem, find the general solution of the system of first-order linear differential equations $X' = AX$.

3. Let $L(D)$ be a constant coefficient linear differential operator of the form

$$L(D) = D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0.$$

Consider the equation $L(D)(y) = 0$.

Let Y be the vector $\begin{bmatrix} y \\ y' \\ \vdots \\ y^{(n-1)} \end{bmatrix}$.

Show that this equation is equivalent to the system

$$Y' = AY,$$

where A is the companion matrix of the polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

(In other words, we see here that a single higher-order linear differential equation can be expressed as a system of first-order linear differential equations. This is true more generally.)

4. In each case below, you are given some of the following information for a linear transformation $\mathcal{T}\colon V \to V$, V a vector space over $\mathbb{C}$:

(1) the characteristic polynomial of $\mathcal{T}$,

(2) the minimal polynomial of $\mathcal{T}$,

(3) the algebraic multiplicity of each eigenvalue of $\mathcal{T}$,

(4) the geometric multiplicity of each eigenvalue of $\mathcal{T}$.

Find the remaining information and also the ESP or JCF of $\mathcal{T}$. In many cases there is more than one possibility. Find all of them.

(a) char. poly. $= (x-2)^4(x-3)^2$.

(b) char. poly. $= (x-7)^5$.

(c) char. poly. $= (x-3)^4(x-5)^4$, min. poly. $= (x-3)^2(x-5)^2$.

(d) char. poly. $= x(x-4)^7$, min. poly. $= x(x-4)^3$.

(e) char. poly. $= x^2(x-2)^4(x-6)^2$, min. poly. $= x(x-2)^2(x-6)^2$.

(f) char. poly. $= (x-3)^4(x-8)^2$, geom. mult.$(3) = 2$, geom. mult.$(8) = 1$.

(g) char. poly. $= x(x-1)^4(x-2)^5$, geom. mult.$(1) = 2$, geom. mult.$(2) = 2$.

(h) $\dim(V) = 5$, geom. mult.$(7) = 3$.

(i) $\dim(V) = 6$, min. poly. $= (x+3)^2(x+1)^2$.

(j) $\dim(V) = 6$, min. poly. $= (x+1)^4$.

(k) $\dim(V) = 8$, min. poly. $= (x+4)^6(x+5)$.

(l) $\dim(V) = 8$, min. poly. $= (x-2)^5(x-3)^3$.

(m) $\dim(V) = 6$, min. poly. $= x-1$.

(n) char. poly. $= (x-5)(x-7)(x-11)(x-13)$.

(o) $\dim(V) = 5$, min. poly. $= (x-1)^3$, geom. mult.$(1) = 3$.

(p) $\dim(V) = 7$, min. poly. $= (x-2)^3$, geom. mult.$(2) = 3$.

5. (a) Let V be a finite-dimensional vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation with $c_{\mathcal{T}}(x) = (x-\lambda)^k$. Let $d_j = \dim \operatorname{Ker}((\mathcal{T} - \lambda\mathcal{I})^j)$, and let b_j be the number of Jordan blocks of size j in a Jordan canonical form of $\mathcal{T}$ for each $j = 1, \ldots, k$. Show that:

$$1b_1 + 2b_2 + \cdots + jb_j + jb_{j+1} + \cdots + jb_k = d_j \text{ for each } j = 1, \ldots, k.$$

(b) Let b be the vector whose entries are $b_1, \ldots, b_k$, and let d be the vector whose entries are $d_1, \ldots, d_k$. Show that the equations in (a) give the matrix equation $Ab = d$, where $A = (a_{ij})$ is the k-by-k matrix with $a_{ij} = \min(i, j)$.

(c) Show that the matrix A is invertible.

(d) Conclude that d uniquely determines b.

(e) Solve the equation $Ab = d$ to obtain formulas for $\{b_j\}$ in terms of $\{d_j\}$.

(f) Conclude from (d) that if $\mathcal{T}\colon V \to V$, $\dim V = n$, is a linear transformation satisfying Hypothesis (S), then the Jordan canonical form of $\mathcal{T}$ is unique up to the order of the blocks.

6. Let V be a finite-dimensional complex vector space, and let $\mathcal{S}\colon V \to V$ and $\mathcal{T}\colon V \to V$ be linear transformations. Show that $\mathcal{S}$ and $\mathcal{T}$ are similar if and only if

$$\dim \operatorname{Ker}((\mathcal{S} - a\mathcal{I})^k) = \dim \operatorname{Ker}((\mathcal{T} - a\mathcal{I})^k)$$

for every complex number a and every positive integer k.

7. Let $V_n = P_n$, the space of polynomials of degree at most n.

(a) Let $\mathcal{T}\colon V_n \to V_n$ by $\mathcal{T}(p(x)) = xp'(x)$. Show that $\mathcal{T}$ is diagonalizable and find a diagonal matrix D with $D = [\mathcal{T}]_{\mathcal{B}}$ in some basis $\mathcal{B}$ of V_n.

(b) Let $\mathcal{S}\colon V_n \to V_n$ by $\mathcal{S}(p(x)) = p(x) + p'(x)$. If $n = 0$, then $\mathcal{S} = \mathcal{I}$ is the identity. Suppose $n > 0$. Show that $\mathcal{S}$ is not diagonalizable. Find a matrix J in Jordan canonical form with $J = [\mathcal{S}]_{\mathcal{B}}$ in some basis $\mathcal{B}$ of V_n.

8. Let $A \in M_n(\mathbb{C})$ be a matrix. Show that A is similar to ${}^tA$.

9. Let $A \in M_n(\mathbb{C})$. The *centralizer* $Z(A)$ of A is

$$Z(A) = \{B \in M_n(\mathbb{C}) \mid AB = BA\}.$$

Observe that $Z(A)$ is a subspace of $M_n(\mathbb{C})$.

(a) Show that the following are equivalent:

(i) $\dim Z(A) = n$.

(ii) $\deg(m_A(x)) = n$.

(iii) $Z(A) = \{$matrices in $M_n(\mathbb{C})$ that are polynomials in $A\}$.

(b) If these conditions are not satisfied, show that $\dim Z(A) > n$.

10. Find all possible values of $\dim Z(A)$ for a fixed 3-by-3 complex matrix A.

11. Let V be a finite-dimensional $\mathbb{F}$-vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. Suppose that $\mathcal{T}$ satisfies Hypothesis (S). Show that there is a diagonalizable linear transformation $\mathcal{R}\colon V \to V$ and a nilpotent linear transformation $\mathcal{S}\colon V \to V$ such that:

(1) $\mathcal{T} = \mathcal{R} + \mathcal{S}$.

(2) $\mathcal{R}$, $\mathcal{S}$, and $\mathcal{T}$ all commute.

Furthermore, show that

(3) $\mathcal{R} = p(\mathcal{T})$ and $\mathcal{S} = q(\mathcal{T})$ for some polynomials $p(x)$ and $q(x)$ in $\mathbb{F}[x]$.

(4) $\mathcal{R}$ and $\mathcal{S}$ are unique.

12. Let V be a finite-dimensional $\mathbb{F}$-vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. For a set of vectors $\mathcal{C}$ in V, we defined $\mathcal{T}$-span$(\mathcal{C})$ in Chapter 5, Exercise 36. If $\mathcal{C} = \{v\}$ consists of a single vector v, we write $\mathcal{T}$-span(v) for $\mathcal{T}$-span$(\mathcal{C})$. We say that V is $\mathcal{T}$-cyclic if there is some vector $v_0 \in V$ with $V = \mathcal{T}$-span(v_0). Suppose that $\mathcal{T}$ satisfies Hypothesis (S).

(a) Show that the following are equivalent:

(i) V is $\mathcal{T}$-cyclic.

(ii) $m_{\mathcal{T}}(x) = c_{\mathcal{T}}(x)$.

(iii) For each eigenvalue λ of $\mathcal{T}$, there is a single Jordan block associated to the eigenvalue λ.

(b) In this situation, let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of $\mathcal{T}$. For each $i = 1, \ldots, k$, let v_i be a generalized eigenvector of highest index associated to λ_i. Show that we may take $v_0 = v_1 + \cdots + v_k$.

(In fact, the equivalence of (i) and (ii) in (a) is true for all $\mathcal{T}$, i.e., even if $\mathcal{T}$ does not satisfy Hypothesis (S).)

13. More generally, let V be an n-dimensional $\mathbb{F}$-vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation that satisfies Hypothesis (S). Give upper and lower bounds for the number of elements in a minimal $\mathcal{T}$-spanning set of V in terms of the Jordan canonical form of $\mathcal{T}$.

14. Let M be an m-by-m complex matrix and write $M = A + iB$, where A and B are real m-by-m matrices. Set $n = 2m$ and let N be the n-by-n real block matrix $N = \begin{bmatrix} A & -B \\ B & A \end{bmatrix}$.

(a) If M has (not necessarily distinct) eigenvalues $\{\lambda_1, \ldots, \lambda_m\}$, show that N has (not necessarily distinct) eigenvalues $\{\lambda_1, \overline{\lambda_1}, \ldots, \lambda_m, \overline{\lambda_m}\}$.

(b) Show that the JCF of N can be obtained from the JCF of M as follows. Let $J_1, \ldots, J_k$ be the Jordan blocks in the JCF of M. Replace each J_i by the pair of Jordan blocks J_i and $\overline{J_i}$.

15. Let A be an m-by-m complex matrix, and let B be an n-by-n complex matrix. Show that every complex block matrix $\begin{bmatrix} A & C \\ 0 & B \end{bmatrix}$ is similar to the block matrix $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$ if and only if A and B have no common eigenvalues (cf. Chapter 7, Exercise 14).

16. Prove Lemma 8.5.5.

Acknowledgment. While our algorithm for Jordan canonical form and a Jordan basis is certainly not new, its formulation in terms of ESP and lESP first appeared, to the author's knowledge, in Steven H. Weintraub, *Jordan Canonical Form: Theory and Practice*, Morgan and Claypool, 2009.

Part II

Vector spaces with additional structure

Hitherto we have considered vector spaces in complete generality. Now we turn our attention to vector spaces which have additional structure, and to linear transformations between them. In this more special situation, we will see that the extra structure gives us stronger results.

While it is possible (and indeed interesting) to proceed more generally, for simplicity, and because these are the most interesting and useful cases, we shall restrict our attention to the cases $\mathbb{F} = \mathbb{R}$ (the field of real numbers) or $\mathbb{F} = \mathbb{C}$ (the field of complex numbers).

Chapter 9

Forms on vector spaces

9.1. Forms in general

We wish to consider bilinear forms on real vector spaces and sesquilinear forms on complex vector spaces. We shall simply call these "forms" for short. ("Bi" is a prefix that means two, while "sesqui" is a prefix that means one and a half.) The difference between the real and complex cases is that we have conjugation in the complex case. Thus we begin by discussing conjugation in complex vector spaces.

We first recall the properties of complex conjugation.

Lemma 9.1.1. *Let $z = a + bi$ be a complex number, and $\bar{z} = a - bi$ its complex conjugate. Then:*

(1) $\bar{\bar{z}} = z$.

(2) $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$.

(3) $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$.

(4) $z = \bar{z}$ *if and only if* z *is a real number.*

(5) $z\bar{z}$ *is a nonnegative real number and* $z\bar{z} = 0$ *if and only if* $z = 0$.

(6) *If* $z \neq 0$, $(\bar{z})^{-1} = \overline{(\bar{z}^{-1})}$.

Definition 9.1.2. Let V be a complex vector space. Then a *conjugation* on V is a function $c\colon V \to V$, where, denoting $c(v)$ by $\bar{v}$:

(1) $\bar{\bar{v}} = v$ for every $v \in V$.

(2) $\overline{v_1 + v_2} = \bar{v}_1 + \bar{v}_2$ for every $v_1, v_2 \in V$.

(3) $\overline{zv} = \bar{z}\bar{v}$ for every $z \in \mathbb{C}$ and every $v \in V$. ◊

Example 9.1.3. (a) If $V = \mathbb{C}^n$, then V has conjugation defined by:

$$\text{If } v = \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}, \text{ then } \bar{v} = \begin{bmatrix} \bar{z}_1 \\ \vdots \\ \bar{z}_n \end{bmatrix}.$$

Similarly if $V = \mathbb{C}^\infty$ or $\mathbb{C}^{\infty\infty}$.

(b) If $V = \{f\colon X \to \mathbb{C}\}$ for some set X, then V has conjugation defined by:

$$\bar{f}(x) = \overline{f(x)} \quad \text{for every } x \in X. \qquad \Diamond$$

Of course, we know what a linear transformation is. We need a slight variant.

Definition 9.1.4. Let V be a complex vector space with a conjugation. Then $\mathcal{T}\colon V \to V$ is *conjugate linear* if:

(1) $\mathcal{T}(v_1 + v_2) = \mathcal{T}(v_1) + \mathcal{T}(v_2)$ for every $v_1, v_2 \in V$.

(2) $\mathcal{T}(zv) = \bar{z}\mathcal{T}(v)$ for every $z \in \mathbb{C}$, $v \in V$. $\Diamond$

Now we come to the basic definition.

Definition 9.1.5. Let V be a vector space over $\mathbb{R}$. A *bilinear form* is a function $\varphi\colon V \times V \to \mathbb{R}$ that is linear in each entry. That is, writing $\varphi(x, y) = \langle x, y\rangle$,

(1) $\langle c_1x_1 + c_2x_2, y\rangle = c_1\langle x_1, y\rangle + c_2\langle x_2, y\rangle$ for every $c_1, c_2 \in \mathbb{R}$ and every $x_1, x_2, y \in V$; and

(2) $\langle x, c_1y_1 + c_2y_2\rangle = c_1\langle x, y_1\rangle + c_2\langle x, y_2\rangle$ for every $c_1, c_2 \in \mathbb{R}$ and every $x, y_1, y_2 \in V$.

Let V be a vector space over $\mathbb{C}$ with a conjugation. A *sesquilinear form* is a function $\varphi\colon V \times V \to \mathbb{C}$ that is linear in the first entry and conjugate linear in the second entry. That is, writing $\varphi(x, y) = \langle x, y\rangle$,

(1) $\langle c_1x_1 + c_2x_2, y\rangle = c_1\langle x_1, y\rangle + c_2\langle x_2, y\rangle$ for every $c_1, c_2 \in \mathbb{C}$ and every $x_1, x_2, y \in V$; and

(2) $\langle x, c_1y_1 + c_2y_2\rangle = \bar{c}_1\langle x, y_1\rangle + \bar{c}_2\langle x, y_2\rangle$ for every $c_1, c_2 \in \mathbb{C}$ and every $x, y_1, y_2 \in V$. $\Diamond$

Example 9.1.6. (a) Let $V = \mathbb{R}^n$. If

$$x = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \quad \text{and} \quad y = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix},$$

then

$$\langle x, y\rangle = {}^t x y.$$

Let $V = \mathbb{C}^n$. If

$$x = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \quad \text{and} \quad y = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix},$$

then

$$\langle x, y\rangle = {}^t x \bar{y}.$$

In each case, this is the familiar "dot product" ($\langle x, y\rangle = a_1b_1 + \cdots + a_nb_n$ in the real case, and $\langle x, y\rangle = a_1\bar{b}_1 + \cdots + a_n\bar{b}_n$ in the complex case).

Strictly speaking, $\langle x, y\rangle$ given by this definition is a 1-by-1 matrix, but we identify that matrix with its entry.

(b) More generally, let A be any fixed n-by-n matrix (with real entries in case $V = \mathbb{R}^n$ and complex entries in case $V = \mathbb{C}^n$). Then

$$\langle x, y\rangle = {}^t\!xAy \quad \text{if } V = \mathbb{R}^n,$$
$$\langle x, y\rangle = {}^t\!xA\bar{y} \quad \text{if } V = \mathbb{C}^n.$$

In particular, if A is a diagonal matrix with diagonal entries $w_1, \ldots, w_n$, then

$$\langle x, y\rangle = a_1b_1w_1 + \cdots + a_nb_nw_n \quad \text{if } V = \mathbb{R}^n,$$
$$\langle x, y\rangle = a_1\bar{b}_1w_1 + \cdots + a_n\bar{b}_nw_n \quad \text{if } V = \mathbb{C}^n.$$

(c) If $V = \mathbb{R}^\infty$ or $\mathbb{C}^\infty$, then we can similarly define

$$\langle x, y\rangle = \sum_{i=1}^{\infty} x_iy_i \quad \text{or} \quad \langle x, y\rangle = \sum_{i=1}^{\infty} x_i\bar{y}_i$$

and this makes sense, as since x and y each only have finitely many nonzero entries, this is a finite sum. Note, however, that these formulas do *not* define forms in $\mathbb{R}^{\infty\infty}$ or $\mathbb{C}^{\infty\infty}$, as infinite sums do not make sense.

(d) Let V be the vector space of real-valued (resp., complex-valued) continuous functions on $[0, 1]$. Then

$$\langle f(x), g(x)\rangle = \int_0^1 f(x)g(x)\,dx \quad \text{in the real case,}$$
$$\langle f(x), g(x)\rangle = \int_0^1 f(x)\bar{g}(x)\,dx \quad \text{in the complex case.}$$

More generally, let $w(x)$ be any fixed real-valued (resp., complex-valued) continuous function on $[0, 1]$. Then

$$\langle f(x), g(x)\rangle = \int_0^1 f(x)g(x)w(x)\,dx \quad \text{in the real case,}$$
$$\langle f(x), g(x)\rangle = \int_0^1 f(x)\bar{g}(x)w(x)\,dx \quad \text{in the complex case.}$$

On the other hand, if V is the vector space of real-valued (resp., complex-valued) continuous functions on $\mathbb{R}$,

$$\langle f(x), g(x)\rangle = \int_{-\infty}^{\infty} f(x)g(x)\,dx,$$
$$\langle f(x), g(x)\rangle = \int_{-\infty}^{\infty} f(x)\bar{g}(x)\,dx$$

do *not* define forms on V, as the integrals in general will not be defined. $\Diamond$

We saw how to obtain forms on $\mathbb{R}^n$ or $\mathbb{C}^n$ from matrices in Example 9.1.6(b). Now let us see that every form is obtained in this way.

Lemma 9.1.7. *Let $V = \mathbb{R}^n$ or $V = \mathbb{C}^n$, and let $\varphi(x, y) = \langle x, y\rangle$ be a form on V. Then there is a unique matrix A such that*

$$\langle x, y\rangle = {}^t\!xAy \quad \textit{in the real case,}$$
$$\langle x, y\rangle = {}^t\!xA\bar{y} \quad \textit{in the complex case}$$

for every $x, y \in V$.

Proof. Let $A = (a_{ij})$ and define a_{ij} by

$$a_{ij} = \langle e_i, e_j\rangle.$$

Then $\langle x, y\rangle = {}^t\!xAy$ or $\langle x, y\rangle = {}^t\!xA\bar{y}$ whenever x and y are both unit vectors, and then it follows from (conjugate) linearity that this is still true when x and y are arbitrary vectors in V. □

Definition 9.1.8. The matrix A of Lemma 9.1.7 is the *standard* matrix of the form φ. ♢

Lemma 9.1.9. *Let V be a finite-dimensional real or complex vector space, and let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a basis of V. Let $\varphi(x, y) = \langle x, y\rangle$ be a form on V. Then there is a unique matrix $[\varphi]_{\mathcal{B}}$ with*

$$\langle x, y\rangle = {}^t[x]_{\mathcal{B}}[\varphi]_{\mathcal{B}}[y]_{\mathcal{B}} \quad \textit{in the real case}$$

or

$$\langle x, y\rangle = {}^t[x]_{\mathcal{B}}[\varphi]_{\mathcal{B}}[\bar{y}]_{\mathcal{B}} \quad \textit{in the complex case}$$

for every $x, y \in V$ (where $[x]_{\mathcal{B}}$ and $[y]_{\mathcal{B}}$ are the coordinate vectors of x and y in the basis $\mathcal{B}$). This matrix is given by $[\varphi]_{\mathcal{B}} = A = (a_{ij})$, where

$$a_{ij} = \langle v_i, v_j\rangle.$$

Proof. If $x = v_i$, then $[x]_{\mathcal{B}} = e_i$, and if $y = [v_j]$, then $[y]_{\mathcal{B}} = e_j$, so we are back in the situation of Lemma 9.1.7:

$$\langle v_i, v_j\rangle = {}^t e_i A e_j = a_{ij} \quad \text{for every } i, j$$

and, again, since this is true for all pairs of basis vectors it is true for all pairs of vectors in V. □

Definition 9.1.10. The matrix $[\varphi]_{\mathcal{B}}$ of Lemma 9.1.9 is the matrix of the form φ in the basis $\mathcal{B}$. ♢

Remark 9.1.11. We observe that if $V = \mathbb{R}^n$ or $V = \mathbb{C}^n$, the matrix of φ in the standard basis $\mathcal{E}$ of V is the standard matrix of φ. ♢

Example 9.1.12. Let $V = \mathbb{R}^n$ or $\mathbb{C}^n$, and let $\varphi(x, y) = \langle x, y\rangle = {}^t\!xy$ or ${}^t\!x\bar{y}$ be the familiar dot product of Example 9.1.6(a). Let $\mathcal{E} = \{e_1, \dots, e_n\}$ be the standard basis of V. Then $\varphi(e_i, e_i) = 1$ and $\varphi(e_i, e_j) = 0$ for $i \neq j$. Thus we see that $[\varphi]_{\mathcal{E}} = I$, i.e., that the standard matrix of φ is the identity matrix I. ♢

Again, following our previous logic, we would like to see how the matrix of the form φ changes when we change the basis of V.

Theorem 9.1.13. *Let V be a finite-dimensional real or complex vector space, and let $\varphi(x, y) = \langle x, y\rangle$ be a form on V. Let $\mathcal{B}$ and $\mathcal{C}$ be bases for V. Then if $[\varphi]_{\mathcal{B}}$ and $[\varphi]_{\mathcal{C}}$ are the matrices of the form φ in the bases $\mathcal{B}$ and $\mathcal{C}$, respectively,*

$$[\varphi]_{\mathcal{B}} = {}^tP_{\mathcal{C}\leftarrow\mathcal{B}}[\varphi]_{\mathcal{C}}P_{\mathcal{C}\leftarrow\mathcal{B}} \quad \text{in the real case}$$

or

$$[\varphi]_{\mathcal{B}} = {}^tP_{\mathcal{C}\leftarrow\mathcal{B}}[\varphi]_{\mathcal{C}}\bar{P}_{\mathcal{C}\leftarrow\mathcal{B}} \quad \text{in the complex case,}$$

where $P_{\mathcal{C}\leftarrow\mathcal{B}}$ is the change of basis matrix from the basis $\mathcal{B}$ to the basis $\mathcal{C}$.

Proof. We shall do the complex case. The real case follows by simply forgetting the conjugation.

By the definition of $[\varphi]_{\mathcal{C}}$, we have

$$\langle x, y\rangle = {}^t[x]_{\mathcal{C}}[\varphi]_{\mathcal{C}}[\bar{y}]_{\mathcal{C}} \quad \text{for every } x, y \in V.$$

Now by the definition of the change of basis matrix,

$$[x]_{\mathcal{C}} = P_{\mathcal{C}\leftarrow\mathcal{B}}[x]_{\mathcal{B}} \quad \text{and} \quad [y]_{\mathcal{C}} = P_{\mathcal{C}\leftarrow\mathcal{B}}[y]_{\mathcal{B}}.$$

Substituting, we see

$$\begin{aligned}\langle x, y\rangle &= {}^t(P_{\mathcal{C}\leftarrow\mathcal{B}}[x]_{\mathcal{B}})[\varphi]_{\mathcal{C}}(\overline{P_{\mathcal{C}\leftarrow\mathcal{B}}[y]_{\mathcal{B}}}) \\ &= {}^t[x]_{\mathcal{B}}\,{}^tP_{\mathcal{C}\leftarrow\mathcal{B}}[\varphi]_{\mathcal{C}}\bar{P}_{\mathcal{C}\leftarrow\mathcal{B}}[\bar{y}]_{\mathcal{B}}.\end{aligned}$$

But by the definition of $[\varphi]_{\mathcal{B}}$,

$$\langle x, y\rangle = {}^t[x]_{\mathcal{B}}[\varphi]_{\mathcal{B}}[\bar{y}]_{\mathcal{B}} \quad \text{for every } x, y \in V.$$

Comparing these two formulas, we see

$$[\varphi]_{\mathcal{B}} = {}^tP_{\mathcal{C}\leftarrow\mathcal{B}}[\varphi]_{\mathcal{C}}\bar{P}_{\mathcal{C}\leftarrow\mathcal{B}}.$$ □

This leads us to make the following definition.

Definition 9.1.14. Two real matrices A and B are *congruent* if there is an invertible real matrix P with $A = {}^tPBP$. Two complex matrices A and B are *conjugate congruent* if there is an invertible complex matrix P with $A = {}^tPB\bar{P}$. ◊

Corollary 9.1.15. *Two real matrices A and B are congruent (resp., two complex matrices A and B are conjugate congruent) if and only if they are matrices of the same form φ with respect to some pair of bases.*

Proof. This follows directly from Theorem 9.1.13, Definition 9.1.14, and the fact that every invertible matrix is a change of basis matrix. □

Remark 9.1.16. Note that here we have a *different* interpretation of matrices than we did before. Earlier, we viewed a matrix as the matrix of a linear transformation. Now we view a matrix as the matrix of a form. Thus it should come as no surprise that we have a *different* change of basis formula here than we did earlier. ◊

Example 9.1.17. Let $V = \mathbb{R}^2$ or $\mathbb{C}^2$, let $\mathcal{B} = \{v_1, v_2\}$ be a basis of V, and let φ be the form on V with

$$[\varphi]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

(thus $\varphi(v_1, v_1) = 0$, $\varphi(v_1, v_2) = 1$, $\varphi(v_2, v_1) = 1$, and $\varphi(v_2, v_2) = 0$). Let $\mathcal{C}$ be the basis $\{w_1, w_2\}$ with

$$w_1 = (1/\sqrt{2})v_1 + (1/\sqrt{2})v_2,$$
$$w_2 = (1/\sqrt{2})v_1 - (1/\sqrt{2})v_2.$$

Then we have, by Theorem 9.1.13, that

$$[\varphi]_{\mathcal{C}} = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1\sqrt{2} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1\sqrt{2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(or we can directly compute that $\varphi(w_1, w_1) = 1$, $\varphi(w_1, w_2) = 0$, $\varphi(w_2, w_1) = 0$, and $\varphi(w_2, w_2) = -1$). ◊

We know what it means to write a vector space V as the direct sum of two subspaces, $V = W_1 \oplus W_2$. We should see the analog when forms are involved. This requires us to make a definition first.

Definition 9.1.18. Let V be a vector space with a form φ. Two subspaces W_1 and W_2 are *orthogonal* if $0 = \varphi(w_1, w_2) = \varphi(w_2, w_1)$ for every $w_1 \in W_1$, $w_2 \in W_2$. ◊

Definition 9.1.19. Let V be a vector space with a form φ. Then V is the *orthogonal direct sum* of two subspaces W_1 and W_2, $V = W_1 \perp W_2$, if V is the direct sum $V = W_1 \oplus W_2$, and the two subspaces W_1 and W_2 are orthogonal. ◊

In case V is finite dimensional, we can express this concretely using the matrix of a form.

Lemma 9.1.20. *Let V be a finite-dimensional vector space with a form φ, and let W_1 and W_2 be subspaces of V with $V = W_1 \oplus W_2$. Let W_1 have basis $\mathcal{B}_1$ and W_2 have basis $\mathcal{B}_2$, and let $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$, a basis of V. Let φ_1 be the restriction of φ to W_1, and set $A_1 = [\varphi_1]_{\mathcal{B}_1}$. Let φ_2 be the restriction of φ to W_2, and set $A_2 = [\varphi_2]_{\mathcal{B}_2}$. Then $V = W_1 \perp W_2$ if and only if*

$$[\varphi]_{\mathcal{B}} = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}.$$

Proof. The condition that the upper right-hand block be 0 is exactly the condition that $\varphi(w_1, w_2) = 0$ for every $w_1 \in W_1$, $w_2 \in W_2$, and the condition that the lower left-hand block be 0 is exactly the condition that $\varphi(w_2, w_1) = 0$ for every $w_1 \in W_1$, $w_2 \in W_2$. □

Example 9.1.21. Let $V = \mathbb{R}^n$ or $\mathbb{C}^n$, and let φ be the usual dot product. Let $\mathcal{E}$ be the standard basis of V, and let W_i be the subspace generated by e_i. Let φ_i be the restriction of φ to W_i. Then $V = W_1 \perp \cdots \perp W_n$ and each φ_i has matrix $[1]$.

In the case of Example 9.1.6(b), where A is a diagonal matrix, then (using the notation of that example) $V = W_1 \perp \cdots \perp W_n$ with φ_i having matrix $[w_i]$. ◊

We know what it means for two vector spaces to be isomorphic. Now we have the extra structure of forms on our vector spaces, so we want to have a notion of isomorphism for vector spaces with forms. These should be, first of all, isomorphisms of vector spaces, but in addition should make the forms "correspond". We are thus led to the following definition.

Definition 9.1.22. Let V and W both be vector spaces over $\mathbb{R}$ or $\mathbb{C}$, with V having a form φ and W having a form ψ. A linear transformation $\mathcal{T}\colon V \to W$ is an *isometry* if

$$\psi(\mathcal{T}(v_1), \mathcal{T}(v_2)) = \varphi(v_1, v_2) \quad \text{for every } v_1, v_2 \in V.$$

$\mathcal{T}$ is an *isometric isomorphism* if it is both an isometry and an isomorphism.

V with the form φ and W with the form ψ are *isometrically isomorphic* if there is an isometric isomorphism between them. $\diamondsuit$

In the finite-dimensional case, where we can represent linear transformations by matrices, we have the following criterion for $\mathcal{T}$ to be an isometric isomorphism. (Notice the similarity between this theorem and Theorem 9.1.13.)

Theorem 9.1.23. *Let V and W both be finite-dimensional vector spaces over $\mathbb{R}$ or $\mathbb{C}$, with V having a form φ and W having a form ψ. Let V have basis $\mathcal{B}$ and W have basis $\mathcal{C}$. Let $\mathcal{T}\colon V \to W$ be a linear transformation. Then $\mathcal{T}$ is an isometric isomorphism if and only if $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ is an invertible matrix with*

$$[\varphi]_{\mathcal{B}} = {}^t[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[\psi]_{\mathcal{C}}[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}} \quad \textit{in the real case}$$

or

$$[\varphi]_{\mathcal{B}} = {}^t[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[\psi]_{\mathcal{C}}[\bar{\mathcal{T}}]_{\mathcal{C}\leftarrow\mathcal{B}} \quad \textit{in the complex case.}$$

Proof. First, $\mathcal{T}$ is an isomorphism if and only if $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ is an invertible matrix.

Now if $w = \mathcal{T}(v)$, then by the definition of $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$, $[w]_{\mathcal{C}} = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[v]_{\mathcal{B}}$.

Then substitute, as in the proof of Theorem 9.1.13, to obtain the analogous result here. $\square$

There is an important case in which an isometry is automatically an isometric isomorphism.

Lemma 9.1.24. *Let φ be a nonsingular form on an n-dimensional vector space V, and let ψ be a form on an n-dimensional vector space W. Let $\mathcal{T}\colon V \to W$ be an isometry. Then $\mathcal{T}$ is an isometric isomorphism. Furthermore, ψ is also nonsingular.*

Proof. Let $y \in V$. Then by nonsingularity there is an $x \in V$ with $\varphi(x, y) \neq 0$. Since $\mathcal{T}$ is an isometry, $\psi(\mathcal{T}(x), \mathcal{T}(y)) = \varphi(x, y) \neq 0$. In particular, that implies that $\mathcal{T}(y) \neq 0$. Thus $\operatorname{Ker}(\mathcal{T}) = \{0\}$. Since $\mathcal{T}$ is a linear transformation between finite-dimensional vector spaces of the same dimension, this implies $\mathcal{T}$ is an isomorphism.

Now let $y' \in W$. Then $y' = \mathcal{T}(y)$ for some $y \in V$. Let $x \in V$ with $\varphi(x, y) \neq 0$ and set $x' = \mathcal{T}(x)$. Then $\psi(x', y') = \psi(\mathcal{T}(x), \mathcal{T}(y)) = \varphi(x, y) \neq 0$ and so ψ is nonsingular. $\square$

Example 9.1.25. Here is an example to show we need finite dimensionality. Let $V = {}^t\mathbb{R}^\infty$ (or ${}^t\mathbb{C}^\infty$) with the form φ defined by $\varphi([x_1, x_2, \ldots], [y_1, y_2, \ldots]) = \sum x_i y_i$ (or $\sum x_i \bar{y}_i$). Then we have right-shift $\mathcal{S}_{\mathrm{rt}}\colon V \to V$ by $\mathcal{S}_{\mathrm{rt}}[x_1, x_2, \ldots] = [0, x_1, x_2, \ldots]$, and $\varphi(\mathcal{S}_{\mathrm{rt}}(x), \mathcal{S}_{\mathrm{rt}}(y)) = \varphi(x, y)$ for every $x, y \in V$, but $\mathcal{S}_{\mathrm{rt}}$ is not an isomorphism. $\diamondsuit$

9.2. Usual types of forms

We now restrict our attention to the types of forms usually encountered in mathematics.

Definition 9.2.1. Let V be a vector space over $\mathbb{R}$. Let $\varphi(x,y) = \langle x,y\rangle$ be a bilinear form on V. Then

$$\varphi \text{ is } \textit{symmetric} \text{ if } \varphi(x,y) = \varphi(y,x) \text{ for every } x,y \in V,$$
$$\varphi \text{ is } \textit{skew-symmetric} \text{ if } \varphi(x,y) = -\varphi(y,x) \text{ for every } x,y \in V.$$

Let V be a vector space over $\mathbb{C}$. Let $\varphi(x,y) = \langle x,y\rangle$ be a sesquilinear form on V. Then

$$\varphi \text{ is } \textit{Hermitian} \text{ if } \varphi(x,y) = \overline{\varphi(y,x)} \text{ for every } x,y \in V,$$
$$\varphi \text{ is } \textit{skew-Hermitian} \text{ if } \varphi(x,y) = -\overline{\varphi(y,x)} \text{ for every } x,y \in V. \qquad \Diamond$$

Lemma 9.2.2. *In the situation of Definition* 9.2.1*, suppose that V is finite dimensional. Let $\mathcal{B}$ be a basis of V, and let $A = [\varphi]_{\mathcal{B}}$. Then:*

(1) *φ is symmetric if and only if ${}^tA = A$.*
(2) *φ is skew-symmetric if and only if ${}^tA = -A$.*
(3) *φ is Hermitian if and only if ${}^t\bar{A} = A$.*
(4) *φ is skew-Hermitian if and only if ${}^t\bar{A} = -A$.*

Proof. We shall do the Hermitian case. The other cases are similar. By the definition of $[\varphi]_{\mathcal{B}}$,

$$\varphi(x,y) = {}^t[x]_{\mathcal{B}} A[\bar{y}]_{\mathcal{B}}$$

remembering that the right-hand side is really a 1-by-1 matrix, and we are identifying that matrix with its entry. Similarly,

$$\varphi(y,x) = {}^t[y]_{\mathcal{B}} A[\bar{x}]_{\mathcal{B}}$$

so

$$\overline{\varphi(y,x)} = {}^t[\bar{y}]_{\mathcal{B}} \bar{A}[x]_{\mathcal{B}}$$

and so

$${}^t\overline{\varphi(y,x)} = {}^t[x]_{\mathcal{B}} {}^t\bar{A}[\bar{y}]_{\mathcal{B}}.$$

But the transpose of a 1-by-1 matrix is itself. Thus, if φ is Hermitian, i.e., if

$$\varphi(x,y) = \overline{\varphi(y,x)} = {}^t\overline{\varphi(y,x)},$$

then comparing these two expressions shows that

$${}^t\bar{A} = A,$$

and conversely that if A satisfies this condition, then φ is Hermitian. $\square$

This leads us to the following definition.

Definition 9.2.3. A real matrix is *symmetric* if ${}^tA = A$ and *skew-symmetric* if ${}^tA = -A$. A complex matrix is *Hermitian* if ${}^tA = \bar{A}$ and *skew-Hermitian* if ${}^tA = -\bar{A}$. $\Diamond$

Remark 9.2.4. Observe that if φ is symmetric, $\varphi(x, x)$ is an arbitrary real number, while if φ is skew-symmetric, we must have $\varphi(x, x) = 0$. If φ is Hermitian we must have $\varphi(x, x)$ real, while if φ is skew-Hermitian we must have $\varphi(x, x)$ zero or pure imaginary.

Similarly, the diagonal entries of a symmetric matrix are arbitrary, while the diagonal entries of a skew-symmetric matrix must be 0. Also, the diagonal entries of a Hermitian matrix must be real and the diagonal entries of a skew-Hermitian matrix must be zero or pure imaginary. $\diamondsuit$

Lemma 9.2.5. *Let V be a vector space, and let φ be a form on V. Let V^* be the dual space of V.*

(a) *In the real case, the function $\alpha_\varphi \colon V \to V^*$ defined by $\alpha_\varphi(y)(x) = \varphi(x, y)$ is a linear transformation.*

(b) *In the complex case, the function $\alpha_\varphi \colon V \to V^*$ defined by $\alpha_\varphi(y)(x) = \varphi(x, y)$ is a conjugate linear transformation.*

Proof. Let y be any fixed element of V. Then we have the function $\mathcal{T}_y \colon V \to \mathbb{F}$ (where $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, as the case may be) defined by $\mathcal{T}_y(x) = \varphi(x, y)$ and we claim that $\mathcal{T}_y$ is a linear transformation. This follows from the fact that φ is linear in the first entry:

$$\begin{aligned}
\mathcal{T}_y(c_1x_1 + c_2x_2) &= \varphi(c_1x_1 + c_2x_2, y) \\
&= c_1\varphi(x_1, y) + c_2\varphi(x_2, y) \\
&= c_1\mathcal{T}_y(x_1) + c_2\mathcal{T}_y(x_2).
\end{aligned}$$

Thus $\mathcal{T}_y$ is a linear transformation from V to $\mathbb{F}$, i.e., $\mathcal{T}_y$ is an element of V^*.

Thus we see that, for each fixed y, $\mathcal{T}_y$ is an element of V^*, so we have a function $\alpha_\varphi \colon V \to V^*$ defined by $\alpha_\varphi(y) = \mathcal{T}_y$. We are further claiming that in the real case α_φ is a linear transformation and in the complex case α_φ is a conjugate linear transformation. This follows from the fact that φ is linear (in the real case) or conjugate linear (in the complex case) in the second entry:

$$\begin{aligned}
\alpha_\varphi(c_1y_1 + c_2y_2)(x) &= \mathcal{T}_{c_1y_1+c_2y_2}(x) \\
&= \varphi(x, c_1y_1 + c_2y_2) \\
&= \overline{c_1}\varphi(x, y_1) + \overline{c_2}\varphi(x, y_2) \\
&= \overline{c_1}\mathcal{T}_{y_1}(x) + \overline{c_2}\mathcal{T}_{y_2}(x) \\
&= (\overline{c_1}\mathcal{T}_{y_1} + \overline{c_2}\mathcal{T}_{y_2})(x) \\
&= (\overline{c_1}\alpha_\varphi(y_1) + \overline{c_2}\alpha_\varphi(y_2))(x)
\end{aligned}$$

and since this is true for every $x \in V$,

$$\alpha_\varphi(c_1y_1 + c_2y_2) = \overline{c_1}\alpha_\varphi(y_1) + \overline{c_2}\alpha_\varphi(y_2). \qquad \square$$

Definition 9.2.6. The form φ on V is *nonsingular* if $\alpha_\varphi \colon V \to V^*$ is 1-1. $\diamondsuit$

Lemma 9.2.7. *The form φ in V is nonsingular if and only if for every nonzero $y \in V$ there is an $x \in V$ with $\varphi(x, y) \neq 0$.*

Proof. Suppose φ is nonsingular. Then if $y \neq 0$, $\alpha_\varphi(y)\colon V \to \mathbb{F}$ is not the zero linear transformation, and so there is an $x \in V$ with $\alpha_\varphi(y)(x) \neq 0$. But $\alpha_\varphi(y)(x) = \varphi(x, y)$, so $\varphi(x, y) \neq 0$ for these values of x and y.

On the other hand, if for each $y \neq 0$ there is an x with $\varphi(x, y) \neq 0$, then $\alpha_\varphi(y)(x) \neq 0$ so $\alpha_\varphi(y)$ is not the zero linear transformation, i.e., $\alpha_\varphi(y) \neq 0$, and so α_φ is 1-1. □

In the finite-dimensional case we have a stronger result.

Lemma 9.2.8. *Let V be finite dimensional. The following are equivalent*:

(a) *φ is nonsingular.*

(b) *$\alpha_\varphi\colon V \to V^*$ is an isomorphism in the real case and a conjugate isomorphism in the complex case, i.e., α_φ is* 1-1 *and onto in either case.*

(c) *Every $\mathcal{T}$ in V^* is $\mathcal{T} = \alpha_\varphi(y)$ for some unique $y \in V$.*

(d) *The matrix of φ in any basis of V is nonsingular.*

Proof. Clearly (b) implies (a). But recall that, if V is finite dimensional, $\dim V^* = \dim V$, and recall also that a 1-1 linear transformation between vector spaces of the same finite dimension must be onto as well. It is straightforward to check that this is true for conjugate linear transformations as well. Thus (a) implies (b), and so these two conditions are equivalent.

Now (c) is just a restatement of (b): to say that every $\mathcal{T}$ in V^* is $\mathcal{T} = \alpha_\varphi(y)$ for some y is to say that α_φ is onto, and to say that y is unique is to say that α_φ is 1-1.

Finally, we show that (d) and (a) are equivalent. Choose any basis $\mathcal{B}$ for V and let $A = [\varphi]_\mathcal{B}$ be the matrix of φ in that basis.

Suppose that the matrix A is nonsingular. Let y be any nonzero element of V. Then $A[y]_\mathcal{B} \neq 0$ (or, in the complex case, $A[\bar{y}]_\mathcal{B} \neq 0$). In particular, the ith entry c of $A[y]_\mathcal{B}$ (or $A[\bar{y}]_\mathcal{B}$) is nonzero for some i. But then if $[x]_\mathcal{B} = e_i$, $\varphi(x, y) = c \neq 0$. Thus φ is nonsingular by Lemma 9.2.7.

On the other hand, suppose that the matrix A is singular. Then there is a nonzero vector y in V such that $A[y]_\mathcal{B} = 0$ (or $A[\bar{y}]_\mathcal{B} = 0$). But then, for that vector y, $\varphi(x, y) = 0$ for every $x \in V$. □

Remark 9.2.9. Suppose that V is finite dimensional. Then V^* has the same dimension as V, so V and V^* are isomorphic. But we have emphasized in our earlier work that there is *no* natural identification between them. However, if we have a nonsingular form φ on V, the situation is *exactly the opposite.* For we see from Lemma 9.2.8(b) that φ *gives us* an identification α_φ of V with V^*. (Of course, this identification depends on the choice of the nonsingular form φ—different choices will give us different identifications.) ◊

If φ is one of the four types of form as in Definition 9.2.1, we shall say that φ is a *usual* form. (This is not standard mathematical language.) These are the sorts of forms we will consider henceforth.

Remark 9.2.10. We observe that if φ is a usual form, and x and y are any two vectors in V, then $\varphi(x, y) = 0$ if and only if $\varphi(y, x) = 0$. ◊

9.3. Classifying forms I

In this and the next section we wish to classify usual forms on finite-dimensional vector spaces. Thus, *throughout these two sections we assume that V is finite dimensional and φ is a usual form.*

We begin with some results that are interesting in their own right.

Definition 9.3.1. Let W be a subspace of V. Its *orthogonal subspace* $W^\perp$ is the subspace

$$W^\perp = \{v \in V \mid \varphi(v, w) = \varphi(w, v) = 0 \text{ for all } w \in W\}. \qquad \Diamond$$

Lemma 9.3.2. *Let W be a subspace of V, and let ψ be the restriction of φ to W. If ψ is nonsingular, then $V = W \perp W^\perp$. Let $\psi^\perp$ be the restriction of φ to $W^\perp$. If φ is nonsingular as well, then $\psi^\perp$ is nonsingular.*

Proof. By definition, W and $W^\perp$ are orthogonal so in order to show that $V = W \perp W^\perp$, we need only show that $V = W \oplus W^\perp$. And to show this, we show that $W \cap W^\perp = \{0\}$ and that $V = W + W^\perp$.

$W \cap W^\perp = \{0\}$: Let $v_0 \in W \cap W^\perp$. Then $v_0 \in W^\perp$, so $\varphi(w, v_0) = 0$ for every $w \in W$. But $v_0 \in W$ as well, and $\psi(w, v_0) = \varphi(w, v_0)$ for every $w \in W$. Thus $\psi(w, v_0) = 0$ for every $w \in W$. But we are assuming that ψ is nonsingular, so that forces $v_0 = 0$.

$V = W + W^\perp$: Let $v_0 \in V$. As we have seen, $\mathcal{T}(w) = \varphi(w, v_0)$ is a linear transformation $\mathcal{T}\colon V \to \mathbb{F}$. But by the nonsingularity of ψ, there is some $w_0 \in W$ with $\mathcal{T}(w) = \psi(w, w_0) = \varphi(w, w_0)$ for every $w \in W$. Then, if we set $w_1 = v_0 - w_0$,

$$\varphi(w, w_1) = \varphi(w, v_0 - w_0) = \varphi(w, v_0) - \varphi(w, w_0) = 0$$

for every $w \in W$. But this says $w_1 \in W^\perp$, and then $v_0 = w_0 + w_1$ with $w_0 \in W$ and $w_1 \in W^\perp$.

Suppose now that φ is nonsingular. Let $v_1 \in W^\perp$. Then there is some vector $v_0 \in V$ with $\varphi(v_0, v_1) \neq 0$. Write $v_0 = w_0 + w_1$ with $w_0 \in W$ and $w_1 \in W^\perp$. Then $\varphi(w_0, v_1) = 0$ as $w_0 \in W$ and $v_1 \in W^\perp$, so

$$0 \neq \varphi(v_0, v_1) = \varphi(w_0 + w_1, v_1) = \varphi(w_0, v_1) + \varphi(w_1, v_1) = \varphi(w_1, v_1) = \psi^\perp(w_1, v_1)$$

so $w_1 \in W^\perp$ with $\psi^\perp(w_1, v_1) \neq 0$ and so $\psi^\perp$ is nonsingular. $\square$

Example 9.3.3. Let $V = \mathbb{R}^2$ or $\mathbb{C}^2$, and let φ be the form with $[\varphi]_{\mathcal{E}} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ (so φ is symmetric or Hermitian). Let W_1 be the subspace spanned by the unit vector $\{e_1\}$, W_2 be the subspace spanned by the unit vector $\{e_2\}$, and W_3 be the subspace spanned by the vector $\{e_1 + e_2\}$. Then the restriction of φ to the subspace W_1 has matrix $[1]$, so is nonsingular, $W_1^\perp = W_2$, and indeed $V = W_1 \perp W_1^\perp$. Similarly, the restriction of φ to W_2 has matrix $[-1]$, so is nonsingular, $W_2^\perp = W_1$, and indeed $V = W_2 \perp W_2^\perp$.

But we also compute that

$$\varphi(e_1 + e_2, e_1 + e_2) = \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = 0$$

and so the restriction of φ to W_3 has matrix $[0]$, and this form is singular. But we also see that $W_3^\perp = W_3$, so $V \neq W_3 \perp W_3^\perp$. (Indeed, it is neither the case that $W_3 \cap W_3^\perp = \{0\}$ nor the case that $W_3 + W_3^\perp = V$.) $\diamondsuit$

Remark 9.3.4. We shall (soon) see important cases where it is automatic that the restriction of φ to W is nonsingular, so in those cases $V = W \perp W^\perp$ for every subspace W of V. $\diamondsuit$

Remark 9.3.5. Let W be a subspace of a vector space V. Then W has a complement U, i.e., $V = W \oplus U$. In our earlier work we emphasized that any complement of W is as good as any other, i.e., that there is no best choice. But if we have a form, the situation changes. Namely, if we have a usual form φ and W is a subspace with the restriction of φ to W nonsingular, then we do have a natural choice, the subspace $W^\perp$. In this situation $W^\perp$ is called the *orthogonal complement* of W in V. $\diamondsuit$

Corollary 9.3.6. *Let W be a subspace of V and suppose that the restriction ψ of φ to W and the restriction $\psi^\perp$ of φ to $W^\perp$ are both nonsingular. Then φ is nonsingular and $(W^\perp)^\perp = W$.*

Proof. Let $v \in V$, $v \neq 0$. Write $v = w_0 + w_1$, with $w_0 \in W$ and $w_1 \in W^\perp$. Since $v \neq 0$, at least one of w_0 and w_1 is nonzero. Suppose that $w_0 \neq 0$. Since ψ is nonsingular, there is a w_0' in W with $\psi(w_0', w_0) = \varphi(w_0', w_0) \neq 0$. But then

$$\varphi(w_0', v) = \varphi(w_0', w_0 + w_1) = \varphi(w_0', w_0) + \varphi(w_0', w_1) = \varphi(w_0', w_0) \neq 0,$$

and similarly if $w_1 \neq 0$.

Now note that if $w_1 \in W^\perp$, then for any $w_0 \in W$, $\varphi(w_0, w_1) = 0$. This says that $W \subseteq (W^\perp)^\perp$.

By Lemma 9.3.2, $V = W \perp W^\perp$ and also $V = W^\perp \perp (W^\perp)^\perp$. But then we must have $(W^\perp)^\perp = W$, since both are orthogonal complements of $W^\perp$. $\square$

We now restrict our attention to symmetric and Hermitian forms.

Of course, if V is a real vector space and φ is a symmetric form in V, then $\varphi(x, x)$ is real for every $x \in V$. But recall also that if V is a complex vector space and φ is a Hermitian form in V, then $\varphi(x, x)$ is real for every $x \in V$ as well.

Definition 9.3.7. Let φ be a symmetric form on a real vector space V or a Hermitian form on a complex vector space V. Then φ is *positive definite* if $\varphi(x, x) > 0$ for every $x \in V$, $x \neq 0$, and φ is *negative definite* if $\varphi(x, x) < 0$ for every $x \in V$, $x \neq 0$. Also, φ is *indefinite* if $\varphi(x_1, x_1) > 0$ for some $x_1 \in V$ and $\varphi(x_2, x_2) < 0$ for some $x_2 \in V$. $\diamondsuit$

We begin with a simple but useful observation.

Lemma 9.3.8. *Suppose that φ is either a positive definite or a negative definite symmetric or Hermitian form on the finite-dimensional vector space V. Let W be any subspace of V, and let ψ be the restriction of φ to W. Then ψ is nonsingular.*

Proof. Let $y \in W$, $y \neq 0$. We must find some $x \in W$ with $\psi(x, y) \neq 0$. But we may simply choose $x = y$, as $\psi(y, y) = \varphi(y, y) \neq 0$. $\square$

Example 9.3.9. Let V be $\mathbb{R}^n$ or $\mathbb{C}^n$. The dot product (Example 9.1.6(a)) is positive definite. The negative of the dot product is negative definite. (Note the standard matrix of the dot product is I and the standard matrix of its negative is $-I$.) $\Diamond$

Now the point is that this simple example is essentially the only one.

Lemma 9.3.10. *Let φ be a positive definite (resp., negative definite) symmetric or Hermitian form on a finite-dimensional vector space V over $\mathbb{R}$ or $\mathbb{C}$. Then φ is isometrically isomorphic to the dot product (resp., the negative of the dot product).*

Proof. We do the positive definite case. The negative definite case is essentially the same argument.

We proceed by induction on $n = \dim V$.

Suppose $n = 1$. Let $x_1 \in V$, $x_1 \neq 0$. Then $\varphi(x_1, x_1) = r$ is a positive real number. Let $y_1 = x_1/\sqrt{r}$. Then $\varphi(y_1, y_1) = 1$ so if $\mathcal{B} = \{y_1\}$, $[\varphi]_{\mathcal{B}} = [1]$.

Now suppose the theorem is true for all vector spaces and forms of dimension $n-1$ and let V have dimension n.

Choose any element x_1 of V. Let $\varphi(x_1, x_1) = r$ and set $y_1 = x_1/\sqrt{r}$ as before, so $\varphi(y_1, y_1) = 1$. Let W be the subspace of V spanned by y_1 (or x_1), and let $\mathcal{B}_1 = \{y_1\}$, so that, if ψ is the restriction of φ to W, $[\psi]_{\mathcal{B}_1} = [1]$.

Now W is a nonsingular subspace, so $V = W \perp W^\perp$. Then $W^\perp$ has dimension $n-1$, and the restriction $\bar{\psi}$ of φ to $W^\perp$ is positive definite, so by induction $W^\perp$ has a basis $\mathcal{B}_2 = \{y_2, \ldots, y_n\}$ with $[\psi]_{\mathcal{B}_2} = I_{n-1}$, the $(n-1)$-by-$(n-1)$ identity matrix. But then if $\mathcal{B} = \{y_1, \ldots, y_n\}$, $[\varphi]_{\mathcal{B}} = I$, the n-by-n identity matrix.

Hence by induction the theorem is true for all n. $\square$

9.4. Classifying forms II

We now consider general symmetric and Hermitian, and also general skew-symmetric, forms.

Definition 9.4.1. Let φ be a usual form on V. Then the *radical* V_0 of V is

$$V_0 = \{y \in V \mid \varphi(x, y) = \varphi(y, x) = 0 \text{ for every } x \in V\}. \qquad \Diamond$$

Remark 9.4.2. We observe that the radical of V is $\{0\}$ if and only if φ is nonsingular (by Lemma 9.2.7). $\Diamond$

The radical is the completely uninteresting part of V. Let us see that we can "split it off".

Theorem 9.4.3. *Let φ be a usual form on V. Let V_0 be the radical of V. Then for any complement U of V_0, $V = V_0 \perp U$. Furthermore, if U_1 and U_2 are any two complements of V_0, and φ_1 and φ_2 are the restrictions of φ to U_1 and U_2, respectively, then U_1 and U_2 are isometrically isomorphic. Furthermore, the quotient vector space V/V_0 has a form $\bar{\varphi}$ defined on it as follows. If $v_1 + V_0$ and $v_2 + V_0$ are any two elements of V/V_0, then $\bar{\varphi}(v_1 + V_0, v_2 + V_0) = \varphi(v_1, v_2)$. Furthermore, if U is any complement of V_0, U is isometrically isomorphic to V/V_0.*

Proof. First of all, by the definition of a complement, we have $V = V_0 \oplus U$. Since V_0 is the radical of V, it is certainly orthogonal to U. Then $V = V_0 \perp U$.

Now recall from Theorem 4.3.19 that any two complements of V_0 are mutually isomorphic. Recall the proof of that theorem. Let $u_1 \in U_1$. Then $u_1 = v_0 + u_2$ for some unique $v_0 \in V_0$ and $u_2 \in U$. Define $\mathcal{T}\colon U_1 \to U_2$ by $\mathcal{T}(u_1) = u_2$. Then $\mathcal{T}$ is an isomorphism. We leave it to the reader to show that in our situation here this linear transformation $\mathcal{T}$ is an isometry.

To see that the form $\bar{\varphi}$ on V/V_0 is well-defined, we must show that it does not depend on the choice of v_1 and v_2. We leave this to the reader as well.

Now also recall that from the proof of Theorem 4.3.19 that $\overline{\mathcal{T}}\colon U \to V/V_0$ given by $\overline{\mathcal{T}}(u) = u + V_0$ is an isomorphism. But then

$$\bar{\varphi}(\overline{\mathcal{T}}(u_1), \overline{\mathcal{T}}(u_2)) = \bar{\varphi}(u_1 + V_0, u_2 + V_0) = \varphi(u_1, u_2)$$

so $\overline{\mathcal{T}}$ is also an isometry. □

We can now define two invariants of a usual form.

Definition 9.4.4. Let φ be a usual form on a finite-dimensional vector space V. Then the *dimension* of φ is the dimension of V, and the *rank* of φ is the codimension of the radical of φ. ♢

Remark 9.4.5. We observe that φ is nonsingular if and only if its rank is equal to its dimension. More generally, we observe that φ has dimension n and rank r if and only if V has a basis $\mathcal{B}$ in which

$$A = [\varphi]_{\mathcal{B}} = \begin{bmatrix} 0 & 0 \\ 0 & B \end{bmatrix},$$

where A is an n-by-n matrix and B is a nonsingular r-by-r matrix. ♢

Now we wish to deal with general symmetric and Hermitian forms. To do so, we first prove a calculational lemma.

Lemma 9.4.6. *Let V be a finite-dimensional vector space over $\mathbb{R}$ or $\mathbb{C}$, and let φ be a nonsingular symmetric or Hermitian form. Then there is a vector y in V with $\varphi(y, y) = \pm 1$.*

Proof. Let x_1 be an arbitrary nonzero vector in V. If $\varphi(x_1, x_1) \neq 0$, set $z = x_1$. Otherwise, since φ is nonsingular, there is a vector x_2 in V with $\varphi(x_1, x_2)$ a nonzero real number. If $\varphi(x_2, x_2) \neq 0$, set $z = x_2$. Otherwise, $\varphi(x_1 + x_2, x_1 + x_2) \neq 0$, so set $z = x_1 + x_2$. Then set $y = z/\sqrt{|\varphi(z, z)|}$. □

Theorem 9.4.7. *Let V be a finite-dimensional vector space over $\mathbb{R}$ or $\mathbb{C}$, and let φ be a symmetric or Hermitian form on V. There are unique nonnegative integers z, p, and q such that φ is isometrically isomorphic to the form on $\mathbb{R}^n$ or $\mathbb{C}^n$ with matrix*

$$\begin{bmatrix} 0_z & & \\ & I_p & \\ & & -I_q \end{bmatrix},$$

where 0_z is the z-by-z 0 matrix, I_p is the p-by-p identity matrix, and $-I_q$ is the negative of the q-by-q identity matrix.

These integers z, p, and q are given by:

$z =$ *the dimension of the radical of V.*

$p =$ *largest dimension of a subspace of V on which φ is positive definite.*

$q =$ *largest dimension of a subspace of V on which φ is negative definite.*

Proof. We will first show that such integers z, p, and q exist, and afterward identify them.

Let V_0 be the radical of V. Let V' be any complement of V_0, and let φ' be the restriction of φ to V'. While V' is not unique all choices of V' give isomorphic forms φ'. Let $\mathcal{B}_0$ be a basis of V_0. If $\dim V_0 = z$, and φ_0 is the restriction of φ to V_0, then $[\varphi_0]_{\mathcal{B}_0} = 0_z$. Also, as we have seen, $V = V_0 \perp V'$.

Let $r = \dim V'$. Then r is the rank of φ, and φ' is nonsingular. We proceed by induction on r.

If $r = 0$, then $V' = \{0\}$ and $p = q = 0$.

Now let $r \geq 1$. Let y be a vector in V' as in Lemma 9.4.6. Let $e = \varphi(y, y) = \pm 1$. Let W be the subspace generated by y. Then the restriction of φ' to W is nonsingular, so $V' = W \perp W^{\perp}$.

The restriction of φ' to $W^{\perp}$ is isometrically isomorphic to

$$\begin{bmatrix} I_{p_1} & \\ & -I_{q_1} \end{bmatrix},$$

by the inductive hypothesis, so φ' is isometrically isomorphic to

$$\begin{bmatrix} e & & \\ & I_{p_1} & \\ & & -I_{q_1} \end{bmatrix}.$$

Thus if $e = 1$, $p = p_1 + 1$ and $q = q_1$, while if $e = -1$, $p = p_1$ and $q = q_1 + 1$.

Thus by induction we are done.

We now identify z, p, and q. Let $\mathcal{B}$ be a basis for V with $[\varphi]_{\mathcal{B}}$ as in the conclusion of the theorem. Write $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_+ \cup \mathcal{B}_-$, where $\mathcal{B}_0$ consists of the first z vectors in the basis, $\mathcal{B}_+$ consists of the next p, and $\mathcal{B}_-$ consists of the last q. Let V_0, V_+, and V_- be the subspaces spanned by $\mathcal{B}_0$, $\mathcal{B}_+$, and $\mathcal{B}_-$ and let φ_0, φ_+, and φ_- be the restrictions of φ to these three subspaces. Then $V = V_0 \perp V_+ \perp V_-$. Also, φ_0 is trivial (identically 0), φ_+ is positive definite, and φ_- is negative definite.

Now z is the dimension of V_0, and V_0 is just the radical of V. We claim that p is the largest dimension of a subspace of V on which the form φ is positive definite and q is the largest dimension of a subspace of V on which the form φ is negative definite.

To see this, note that $p+q = r$. Let p' and q' be these largest dimensions. Since V_+ has dimension p and V_- has dimension q, we have $p' \geq p$ and $q' \geq q$. Suppose there was a subspace V'_+ of dimension $p' > p$ on which φ was positive definite. Then $\dim V'_+ + \dim V_- = p' + q > r$, so that means that $\dim V'_+ \cap V_- = (p' + q) - r > 0$, i.e., that $V'_+ \cap V_- \neq \{0\}$. Let x be a nonzero vector in $V'_+ \cap V_-$. Then on the one hand, $x \in V'_+$, so $\varphi(x, x) > 0$, and on the other hand, $x \in V_-$, so $\varphi(x, x) < 0$, and these contradict each other. Hence $p' = p$, and by the same logic $q' = q$. $\square$

Theorem 9.4.8. *Let V and W be finite-dimensional vector spaces, both over either $\mathbb{R}$ or $\mathbb{C}$, and let φ and ψ be both symmetric or Hermitian forms on V and W, respectively. Let z_φ, p_φ, and q_φ be the integers associated to φ as in Theorem* 9.4.7, *and similarly for z_ψ, p_ψ, and q_ψ. Then V and W are isometrically isomorphic if and only if $z_\varphi = z_\psi$, $p_\varphi = p_\psi$, and $q_\varphi = q_\psi$.*

Proof. If $z_\varphi = z_\psi = z$, $p_\varphi = p_\psi = p$, and $q_\varphi = q_\psi = q$, then V and W are both isometrically isomorphic to the same form, namely the one in the conclusion of Theorem 9.4.7, and hence to each other.

On the other hand, from the characterizations of the integers z, p, and q in the conclusion of Theorem 9.4.7, they are clearly the same for isometrically isomorphic forms. $\square$

In common mathematical language, the classification is stated a bit differently.

Definition 9.4.9. In the notation of Theorem 9.4.7, the *signature* σ of φ is $\sigma = p - q$. $\Diamond$

Theorem 9.4.10. *A symmetric form φ on a finite-dimensional real vector space V, or a Hermitian form on a finite-dimensional complex vector space V, is determined up to isometric isometry by its dimension, rank, and signature.*

Proof. The integers z, p, and q determine the integers n, r, and σ ($n = z + p + q$, $r = p + q$, $\sigma = p - q$), but also the integers n, r, and σ determine the integers z, p, and q ($z = n - r$, $p = (r + \sigma)/2$, $q = (r - \sigma)/2$). $\square$

Let us now derive a handy result that will enable us to determine whether a symmetric or Hermitian form φ is positive or negative definite. In fact, it will also allow us in most cases to easily find the signature of φ. First we make a standard definition.

Definition 9.4.11. Let A be a symmetric or Hermitian matrix. The form φ_A is the form on $\mathbb{C}^n$ whose standard matrix is A. The matrix A is positive definite/negative definite/indefinite according as the form φ_A is positive definite/negative definite/indefinite. Furthermore, the *signature* of A is the signature of the form φ_A. $\Diamond$

Theorem 9.4.12. *Let A be a nonsingular real symmetric or complex Hermitian matrix. Let $\delta_0(A) = 1$ and for $k = 1, \ldots, n$, let δ_k be the determinant of the upper left-hand k-by-k submatrix A_k of A.*

Then:

(1) *A is positive definite if and only if $\delta_k > 0$ for $k = 1, \ldots, n$.*

(2) *A is negative definite if and only if $\delta_{k-1}(A)$ and $\delta_k(A)$ have opposite signs for $k = 1, \ldots, n$, i.e., if and only if $(-1)^k \delta_k(A) > 0$ for $k = 1, \ldots, n$.*

(3) *Suppose that $\delta_k(A) \neq 0$ for $k = 1, \ldots, n$. Then A has signature $\sigma = r - s$, where*

$$\begin{gathered} r \text{ is the number of values of } k \text{ between } 1 \text{ and } n \text{ for which} \\ \delta_{k-1}(A) \text{ and } \delta_k(A) \text{ have the same sign; and} \\ s \text{ is the number of values of } k \text{ between } 1 \text{ and } n \text{ for which} \\ \delta_{k-1}(A) \text{ and } \delta_k(A) \text{ have opposite signs.} \end{gathered}$$

Proof. First let us observe that if A is positive definite or negative definite, so is each A_k, and in particular, each A_k is nonsingular, so $\delta_k(A) \neq 0$ for each k. Given that observation, we see that (1) and (2) are special cases of (3):

If each $\delta_k(A) > 0$, then $r = n$ and $s = 0$, so A has signature n, i.e., is positive definite, while if $(-1)^k \delta_k(A) > 0$ for each k, then $r = 0$ and $s = n$, so A has signature $-n$, i.e., is negative definite.

We proceed by induction on n.

In case $n = 1$, if $A = [a_{11}]$, then φ_A is positive definite, i.e., has index 1, if $a_{11} > 0$, and is negative definite, i.e., has index -1, if $a_{11} < 0$.

Now suppose the theorem is true for $n - 1$ and let A be n-by-n. Let $V = \mathbb{C}^n$, and let W be the subspace of $\mathbb{C}^n$ consisting of all vectors whose last coordinate is 0. Then the restriction of φ to W has matrix A_{n-1}, the upper left $(n-1)$-by-$(n-1)$ submatrix of A. Note that the restriction of φ to W is nonsingular if and only if $\delta_{n-1}(A) = \det(A_{n-1}) \neq 0$. Assuming that is the case, we may, by Lemma 9.3.2, decompose V as $V = W \perp W^\perp$.

Now $W^\perp$ is 1-dimensional; choose a nonzero vector v_n in $W^\perp$. Let $\mathcal{B}$ be the basis $\mathcal{B} = \{e_1, \ldots, e_{n-1}, v_n\}$ of V. Then

$$B = [\varphi]_{\mathcal{B}} = \begin{bmatrix} A_{n-1} & 0 \\ 0 & b_{nn} \end{bmatrix}$$

and $b_{nn} = \varphi(v_n, v_n) \neq 0$ since φ is nonsingular.

But now recall, by Theorem 9.1.13, that $A = {}^t\!PB\bar{P}$, where $P = P_{\mathcal{B} \leftarrow \mathcal{E}}$ is the change of basis matrix, and so, setting $z = \det(P)$,

$$\begin{aligned} \delta_n(A) = \det(A) &= \det({}^t\!P)\det(B)\det(\bar{P}) \\ &= z\bar{z}\det(B) = |z|^2 \det(B) \\ &= |z|^2 \det(A_{n-1}) b_{nn} = |z|^2 \delta_{n-1}(A) b_{nn} \end{aligned}$$

has the same sign as $\delta_{n-1}(A) b_{nn}$, as $|z|^2 > 0$ for any complex number z.

Now suppose A_{n-1} has signature $\sigma_1 = r_1 - s_1$. Then, by the inductive hypothesis, W has a subspace W_+ of dimension r_1 on which φ is positive definite and a subspace W_- of dimension s_1 on which φ is negative definite, so $W = W_+ \perp W_-$ and $V = W_+ \perp W_- \perp W^\perp$.

Now there are two possibilities. If $b_{nn} > 0$, then φ is positive definite on the subspace $W_+ \perp W^\perp$ and negative definite on the subspace W_-, in which case $r = r_1 + 1$, $s = s_1$, and A has signature $\sigma = \sigma_1 + 1$. But in this case $\delta_n(A)$ has the same sign as $\delta_{n-1}(A)$, so, compared to A_{n-1}, there is one more value of k, namely $k = n$, for which $\delta_{k-1}(A)$ and $\delta_k(A)$ have the same sign, so the count in (3) also shows $\sigma = \sigma_1 + 1$. On the other hand, if $b_{nn} < 0$, then φ is positive definite on W_+, negative definite on $W_- \perp W^\perp$, so $r = r_1$, $s = s_1 + 1$, $\sigma = \sigma_1 - 1$. But in this case $\delta_n(A)$ has the opposite sign as $\delta_{n-1}(A)$, so there is one more value of k for which $\delta_{k-1}(A)$ and $\delta_k(A)$ have opposite signs, so the count in (3) shows $\sigma = \sigma_1 - 1$. Thus in either case the count in (3) is correct, as claimed. $\square$

Remark 9.4.13. If φ is positive definite or negative definite, then, as we observed in the course of the proof, Theorem 9.4.12 always applies. (Thus in particular we see that if $\delta_k(A) = 0$ for some $k < n$, then A is indefinite.) But in the indefinite case, (3) may not. For example, suppose $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Then $\delta_1(A) = 0$ (but in this case it is easy to check that φ_A is isometrically isomorphic to φ_B with $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, and Theorem 9.4.12(3) applies to B). But see Section 9.7, Exercise 14. $\diamondsuit$

Example 9.4.14. Let $n = 2$, and let $A = \begin{bmatrix} a & b \\ \bar{b} & d \end{bmatrix}$. You can easily check that in this case, Theorem 9.4.12 gives:

A is positive definite if $a > 0$ and $\det(A) > 0$.

A is negative definite if $a < 0$ and $\det(A) > 0$.

A is indefinite if $\det(A) < 0$. $\diamondsuit$

While this theorem is a handy computational tool, it does not tell us *why* A should be positive or negative definite, or have the signature that it does. We will see the true reason for this, and more, in the next chapter.

In our last few results, we have dealt with nonsingular forms. Of course, not every form is nonsingular. So let us consider the (possibly) singular case.

Definition 9.4.15. Let φ be a symmetric form on a real vector space, or a Hermitian form on a complex vector space. Then φ is *positive semidefinite* if $\varphi(x, x) \geq 0$ for every $x \in V$, φ is *negative semidefinite* if $\varphi(x, x) \leq 0$ for every $x \in V$, and φ is *indefinite* if there are vectors x_1 and x_2 in V with $\varphi(x_1, x_1) > 0$ and $\varphi(x_2, x_2) < 0$. $\diamondsuit$

Lemma 9.4.16. *Let φ be a symmetric form on a real vector space or a Hermitian form on a complex vector space.*

(a) *Suppose that φ is nonsingular. Then φ is positive* (*resp., negative*) *semidefinite if and only if φ is positive* (*resp., negative*) *definite.*

(b) *In general, let V_0 be the radical of V, let U be any complement of V_0, and let φ' be the restriction of φ to U. Then φ is positive semidefinite/negative semidefinite/indefinite if and only if φ' is positive definite/negative definite/indefinite.*

Proof. We leave this as an exercise for the reader. $\square$

Now let us classify skew-symmetric forms on finite-dimensional real vector spaces. Here the idea is similar, but the situation is easier.

We begin with an easy preliminary result, which is actually the key to the whole situation.

Lemma 9.4.17. (a) *Let V be a 1-dimensional real vector space. Then any skew-symmetric form on φ is trivial (i.e., identically zero).*

(b) *Let V be a 2-dimensional real vector space, and let φ be a nonsingular skew-symmetric form on V. Then V has a basis $\mathcal{B}$ in which*

$$[\varphi]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Proof. (a) Let x be any nonzero vector in V. Then $\varphi(x,x) = 0$ by skew-symmetry. Since V is 1-dimensional, x spans V, so $\varphi(x,y) = 0$ for any $x, y \in V$.

(b) Let x_1 be any nonzero vector in V. Since φ is nonsingular, there is a vector y in V with $\varphi(x,y) = a \neq 0$. Let $y_1 = (1/a)y$. Then $\varphi(x_1,x_1) = 0$, $\varphi(x_1,y_1) = 1$, so by skew-symmetry $\varphi(y_1,x_1) = -1$, and $\varphi(y_1,y_1) = 0$. Now y_1 cannot be a multiple of x_1, as if it were we would have $\varphi(x_1,y_1) = 0$, so $\mathcal{B} = \{x_1, y_1\}$ is a linearly independent set of two vectors in V, a vector space of dimension 2, so is a basis for V, and then $[\varphi]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. □

Theorem 9.4.18. *Let V be a finite-dimensional vector space over $\mathbb{R}$, and let φ be a skew-symmetric form on V. There are unique nonnegative integers z and s such that φ is isometrically isomorphic to the form on $\mathbb{R}^n$ with basis*

$$\begin{bmatrix} 0_z & & \\ & 0_s & I_s \\ & -I_s & 0_s \end{bmatrix}.$$

Proof. We follow the same strategy as in the proof of Theorem 9.4.7.

Let V_0 be the radical of V, let V' be any complement of V_0, let φ_0 be the restriction of φ to V_0, and let φ' be the restriction of φ to V'. Then if $\mathcal{B}_0$ is a basis of V_0, $[\varphi_0]_{\mathcal{B}_0} = 0_z$, where z is the dimension of V_0. Also, $V = V_0 \perp V'$.

Let $r = \dim V'$. Then r is the rank of φ, and φ' is nonsingular. We proceed by induction on r.

If $r = 0$, then $V' = \{0\}$ and $s = 0$.

If $r = 1$, then V' is 1-dimensional. But by Lemma 9.4.17, this cannot occur, as φ' must be trivial, so cannot be nonsingular.

If $r = 2$, then V' is 2-dimensional and so V' has a basis $\mathcal{B}$ with $[\varphi]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ by Lemma 9.4.17.

Now let $r > 2$. Let x be any nonzero vector in V'. Since φ is nonsingular, there is a vector y in V' with $\varphi(x,y) \neq 0$, and since φ is skew-symmetric, x and y are linearly independent. Let W be the subspace generated by x and y. Then, as in Lemma 9.4.17, W has a basis $\mathcal{B}_1 = \{x_1, y_1\}$ in which φ_1, the restriction of φ' to W, has matrix $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. This also means that φ_1 is nonsingular, so $V' = W_1 \perp W_2$, and the restriction φ_2 of φ' to W_2 is nonsingular as well. But then by induction W_2 has a basis $\mathcal{B}_2 = \{x_2, \ldots, x_s, y_2, \ldots, y_s\}$ with

$$[\varphi_2]_{\mathcal{B}_2} = \begin{bmatrix} 0_{s-1} & I_{s-1} \\ -I_{s-1} & 0_{s-1} \end{bmatrix}.$$

Let $\mathcal{B} = \{x_1, x_2, \ldots, x_s, y_1, y_2, \ldots, y_s\}$. Then

$$[\varphi']_{\mathcal{B}} = \begin{bmatrix} 0_s & I_s \\ -I_s & 0_s \end{bmatrix}$$

and by induction we are done.

Now z is unique, as z is the dimension of the radical of V. Also, r is unique, as it is the rank of φ, and $2s = r$, i.e., $s = r/2$, so s is unique as well. □

Theorem 9.4.19. *Let V and W be finite-dimensional real vector spaces, and let φ and ψ be skew-symmetric forms on V and W, respectively. Then V and W are isometrically isomorphic if and only if they have the same dimension and rank.*

Proof. The integers z and s determine the dimension n and rank r, as $r = 2s$ and $n = z + r = z + 2s$, and vice-versa, as $z = n - r$ and $s = r/2$. If V and W have the same rank and dimension they are both isometrically isomorphic to the same form as in Theorem 9.4.18. On the other hand, if they are isometrically isomorphic, they certainly have the same dimension n, and their radicals have the same dimension z, so they have the same rank $r = n - z$. □

The following special case is worth pointing out.

Corollary 9.4.20. *Let V be a finite-dimensional vector space over $\mathbb{R}$. If there is a nonsingular skew-symmetric form on V, then the dimension of V must be even. If the dimension of V is even, then any two nonsingular skew-symmetric forms on V are isometrically isomorphic.*

Proof. In our previous notation, if $z = 0$, then $n = r = 2s$ must be even. But if n is even and $z = 0$, then $r = n$. □

9.5. The adjoint of a linear transformation

In this section we fix a vector space V and a nonsingular form φ on V, and a vector space W and a nonsingular form ψ on W. We assume that either V and W are both real, so that φ and ψ are both bilinear, or that V and W are both complex, so that φ and ψ are both sesquilinear.

We will do all our proofs in the complex case, as we will need to keep track of the conjugations. But they all work in the real case as well, just forgetting about the conjugations.

Definition 9.5.1. Let $\mathcal{T}\colon V \to W$ be a linear transformation. Its *adjoint* $\mathcal{T}^*\colon W \to V$ is the linear transformation given by the formula

$$\psi(\mathcal{T}(x), y) = \varphi(x, \mathcal{T}^*(y))$$

assuming such a linear transformation exists. ◊

This is a sort of conditional definition, since $\mathcal{T}^*$ may or may not exist. But before we deal with the question of whether it does, let us see that it is a linear transformation.

Lemma 9.5.2. *If $\mathcal{T}^*$ exists, then $\mathcal{T}^*\colon W \to V$ is a well-defined linear transformation.*

Proof. Let y_0 be any fixed element of W, and let $\mathcal{S}\colon V \to \mathbb{F}$ ($\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$) be defined by

$$\mathcal{S}(x) = \psi(\mathcal{T}(x), y_0).$$

We leave it to the reader to check that $\mathcal{S}(x_1 + x_2) = \mathcal{S}(x_1) + \mathcal{S}(x_2)$ and that $\mathcal{S}(cx) = c\mathcal{S}(x)$. Thus $\mathcal{S}$ is a linear transformation from V to $\mathbb{F}$, i.e., an element of the dual space V^*. Now the nonsingularity of φ means that the map $\alpha_\varphi\colon V \to V^*$ is 1-1, so there is at most one vector $z_0 \in V$ with $\alpha_\varphi(z_0) = \mathcal{S}$. But $\alpha_\varphi(z_0)(x) = \varphi(x, z_0)$.

Thus, if z_0 exists, it is unique, and then $\mathcal{S}(x) = \alpha_\varphi(z_0)(x)$ is the equation

$$\psi(\mathcal{T}(x), y_0) = \varphi(x, z_0)$$

so, setting $z_0 = \mathcal{T}^*(y_0)$, we have a well-defined function $\mathcal{T}^*\colon W \to V$.

Proceeding on the assumption that $\mathcal{T}^*$ exists, we leave it to the reader to show that, by the definition of $\mathcal{T}^*$ and (conjugate) linearity, $\varphi(x, \mathcal{T}^*(y_1 + y_2)) = \varphi(x, \mathcal{T}^*(y_1)) + \varphi(x, \mathcal{T}^*(y_2))$ for every $x \in V$ and every $y_1, y_2 \in W$, so, since φ is nonsingular, $\mathcal{T}^*(y_1 + y_2) = \mathcal{T}^*(y_1) + \mathcal{T}^*(y_2)$, and also that $\varphi(x, \mathcal{T}^*(cy_0)) = c\varphi(x, \mathcal{T}^*(y_0))$ for every $x \in V$, every $y_0 \in W$, and every $c \in \mathbb{F}$, so, again since φ is nonsingular, $\mathcal{T}^*(cy_0) = c\mathcal{T}^*(y_0)$.

Thus $\mathcal{T}^*$ is a linear transformation, as claimed. □

Lemma 9.5.3. *If V is finite dimensional, then $\mathcal{T}^*$ always exists.*

Proof. Referring to the proof of Lemma 9.5.2, and in the notation of that proof, in the finite-dimensional case if φ is nonsingular, then the map $\alpha_\varphi\colon V \to V^*$ is both 1-1 *and* onto (Lemma 9.2.8), so for any $\mathcal{S}$ there is *always* a unique z_0 with $\alpha_\varphi(z_0) = \mathcal{S}$, so the equation $\mathcal{T}^*(y_0) = z_0$ defines a function $\mathcal{T}\colon W \to V$ for every $y_0 \in W$. □

Remark 9.5.4. In Section 5.6, given a linear transformation $\mathcal{T}\colon V \to W$, we defined its dual $\mathcal{T}^*\colon W^* \to V^*$. Thus we are using $\mathcal{T}^*$ to mean two different things: dual and adjoint. Unfortunately, this is standard mathematical notation, so we are stuck with it. However, in the remainder of this chapter and in the next chapter, we will *always* be using $\mathcal{T}^*$ to denote the adjoint, and *never* the dual. (We also emphasize that the dual just depends on the vector spaces V and W, but the adjoint also depends on the forms φ and ψ—if we change φ and ψ the adjoint changes.) ◊

The adjoint is admittedly a subtle (and tricky) concept. Let us see how to calculate it, and that will enable us to give some concrete examples.

Lemma 9.5.5. *Let V and W be finite dimensional, and let $\mathcal{B}$ and $\mathcal{C}$ be bases for V and W, respectively. Then $[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ and $[\mathcal{T}^*]_{\mathcal{B}\leftarrow\mathcal{C}}$ are related by the equation*

$${}^t[\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[\psi]_{\mathcal{C}} = [\varphi]_{\mathcal{B}}[\overline{\mathcal{T}^*}]_{\mathcal{B}\leftarrow\mathcal{C}}$$

and so

$$[\mathcal{T}^*]_{\mathcal{B}\leftarrow\mathcal{C}} = [\varphi]_{\mathcal{B}}^{-1}\,{}^t[\bar{\mathcal{T}}]_{\mathcal{C}\leftarrow\mathcal{B}}[\bar{\psi}]_{\mathcal{C}}.$$

Proof. This is a matter of carefully tracing through what the matrices of linear transformations and forms mean.

For simplicity, let us set $M = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ and $N = [\mathcal{T}^*]_{\mathcal{B}\leftarrow\mathcal{C}}$.

First we compute $\psi(\mathcal{T}(x), y)$. By the definition of $[\psi]_{\mathcal{C}}$,

$$\psi(\mathcal{T}(x), y) = {}^t[\mathcal{T}(x)]_{\mathcal{C}}[\psi]_{\mathcal{C}}[\bar{y}]_{\mathcal{C}}.$$

Now, also by definition, $[\mathcal{T}(x)]_{\mathcal{C}} = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}[x]_{\mathcal{B}} = M[x]_{\mathcal{B}}$, so

$$\begin{aligned}\psi(\mathcal{T}(x), y) &= {}^t(M[x]_{\mathcal{B}})[\psi]_{\mathcal{C}}[\bar{y}]_{\mathcal{C}}\\ &= {}^t[x]_{\mathcal{B}}\,{}^tM[\psi]_{\mathcal{C}}[\bar{y}]_{\mathcal{C}}.\end{aligned}$$

Similarly, we compute

$$\varphi(x, \mathcal{T}^*(y)) = {}^t[x]_{\mathcal{B}}[\varphi]_{\mathcal{B}}[\overline{\mathcal{T}^*(y)}]_{\mathcal{B}}$$

and $[\mathcal{T}^*(y)]_{\mathcal{B}} = [\mathcal{T}^*]_{\mathcal{B}\leftarrow\mathcal{C}}[y]_{\mathcal{C}} = N[y]_{\mathcal{C}}$, so

$$\begin{aligned}\varphi(x, \mathcal{T}^*(y)) &= {}^t[x]_{\mathcal{B}}[\varphi]_{\mathcal{B}}(\overline{N[y]_{\mathcal{C}}})\\ &= {}^t[x]_{\mathcal{B}}[\varphi]_{\mathcal{B}}\bar{N}[\bar{y}]_{\mathcal{C}}.\end{aligned}$$

But by the definition of the adjoint, $\psi(\mathcal{T}(x), y) = \psi(x, \mathcal{T}^*(y))$ for every x, y, so, comparing these two expressions, we see

$${}^tM[\psi]_{\mathcal{C}} = [\varphi]_{\mathcal{B}}\bar{N}. \qquad \square$$

Thus in the finite-dimensional case, not only does $\mathcal{T}^*$ always exist, but we have a formula for it. This formula looks rather mysterious in general, but its meaning will become clear in some particular cases.

Example 9.5.6. Let $V = \mathbb{R}^n$ (or $\mathbb{C}^n$) and $W = \mathbb{R}^m$ (or $\mathbb{C}^m$), and let φ and ψ be the "dot product" on V and W, respectively. Let $\mathcal{E}_n$ and $\mathcal{E}_m$ be the standard bases for V and W, respectively. Then, as we have seen, $[\varphi]_{\mathcal{E}_n} = I_n$ and $[\psi]_{\mathcal{E}_m} = I_m$ (the n-by-n and m-by-m identity matrices, respectively). Also, we recall that $[\mathcal{T}]_{\mathcal{E}_m\leftarrow\mathcal{E}_n}$ is the standard matrix of $\mathcal{T}$, and similarly $[\mathcal{T}^*]_{\mathcal{E}_n\leftarrow\mathcal{E}_m}$ is the standard matrix of $\mathcal{T}^*$. Let us set $A = [\mathcal{T}]_{\mathcal{E}_m\leftarrow\mathcal{E}_n}$ (so that $\mathcal{T} = \mathcal{T}_A$) and $A^* = [\mathcal{T}^*]_{\mathcal{E}_n\leftarrow\mathcal{E}_m}$ (so that $\mathcal{T}^* = \mathcal{T}_{A^*}$). Then we see

$$A^* = {}^t\bar{A}$$

(and of course, in the real case, $\bar{A} = A$, so in this case $A^* = {}^tA$). $\Diamond$

Now let's specialize a little more. Let $W = V = \mathbb{R}^n$ (or $\mathbb{C}^n$), and let $\psi = \varphi$ be the dot product, so now we have a linear transformation $\mathcal{T}\colon V \to V$ and its adjoint is another linear transformation $\mathcal{T}^*\colon V \to V$.

Definition 9.5.7. In this situation $\mathcal{T}$ is *self-adjoint* if $\mathcal{T}^* = \mathcal{T}$. $\Diamond$

Lemma 9.5.8. *In this situation $\mathcal{T}$ is self-adjoint if and only if its standard matrix is symmetric* (*in the real case*) *or Hermitian* (*in the complex case*).

Proof. We just saw in Example 9.5.6 that $A^* = {}^t\bar{A}$. But if $A^* = A$, that becomes simply the equation $A = {}^t\bar{A}$. $\square$

We are then led to the following definition.

Definition 9.5.9. A matrix A is *self-adjoint* if $A^* = {}^t\bar{A}$. $\diamondsuit$

Then we have:

Corollary 9.5.10. *A real matrix A is self-adjoint if and only if it is symmetric. A complex matrix A is self-adjoint if and only if it is Hermitian.*

Proof. This is just a translation of Lemma 9.5.8 into matrix language. $\square$

In preparation for our next lemma, we introduce some standard language.

Definition 9.5.11. Let A be a matrix with $A^* = A^{-1}$. If A is real, A is called *orthogonal.* If A is complex, A is called *unitary.* $\diamondsuit$

Lemma 9.5.12. *In this situation, $\mathcal{T}$ is an isometric isomorphism if and only if its standard matrix is orthogonal (in the real case) or unitary (in the complex case).*

Proof. First recall that, in this situation, if $\mathcal{T}$ is an isometry, then it is an isometric isomorphism (Lemma 9.1.24). To say that $\mathcal{T}$ is an isometry is to say that $\varphi(\mathcal{T}(x), \mathcal{T}(y)) = \varphi(x, y)$ for every $x, y \in V$. But in the standard basis the dot product is just $\varphi(x, y) = {}^tx\bar{y}$. Thus, if $\mathcal{T}$ has standard matrix A, we simply compute

$$\varphi(\mathcal{T}(x), \mathcal{T}(y)) = {}^t[Ax][\overline{Ay}] = {}^tx{}^tA\bar{A}\bar{y} = {}^tx\bar{y} = \varphi(x, y)$$

so we see ${}^tA\bar{A} = I$; conjugating, ${}^t\bar{A}A = I$.

From Example 9.5.6 we see that this is the equation $A^*A = I$, i.e., $A^* = A^{-1}$. $\square$

Remark 9.5.13. Concretely, it is easy to tell when A is orthogonal/unitary. Write $A = [v_1| \dots |v_n]$. Then the (i, j) entry of ${}^tA\bar{A}$ is ${}^tv_i\bar{v}_j = \varphi(v_i, v_j)$. So A is orthogonal/unitary if and only if $\varphi(v_i, v_i) = 1$ for each $i = 1, \dots, n$ and $\varphi(v_i, v_j) = 0$ whenever $j \neq i$. $\diamondsuit$

Now let us derive some properties of adjoints.

Lemma 9.5.14. (1) *The identity linear transformation $\mathcal{I}: V \to V$ always has an adjoint, and $\mathcal{I}^* = \mathcal{I}$.*

(2) *Suppose that $\mathcal{T}_1: V \to W$ and $\mathcal{T}_2: V \to W$ both have adjoints. Then $\mathcal{T}_1 + \mathcal{T}_2: V \to W$ has an adjoint and $(\mathcal{T}_1 + \mathcal{T}_2)^* = \mathcal{T}_1^* + \mathcal{T}_2^*$.*

(3) *Suppose that $\mathcal{T}: V \to W$ has an adjoint. Then for any scalar c, $c\mathcal{T}$ has an adjoint and $(c\mathcal{T})^* = \bar{c}\mathcal{T}^*$.*

(4) *Suppose that $\mathcal{S}: V \to W$ and $\mathcal{T}: W \to X$ both have adjoints. Then the composition $\mathcal{T}\mathcal{S}: V \to X$ has an adjoint and $(\mathcal{T}\mathcal{S})^* = \mathcal{S}^*\mathcal{T}^*$.*

(5) *Suppose that $\mathcal{T}: V \to V$ has an adjoint. Then for any polynomial $p(x)$, $p(\mathcal{T})$ has an adjoint, and $(p(\mathcal{T}))^* = \bar{p}(\mathcal{T}^*)$.*

(6) *Suppose that φ and ψ have the same type. If $\mathcal{T}: V \to W$ has an adjoint, then $\mathcal{T}^*: W \to V$ has an adjoint, and $(\mathcal{T}^*)^* = \mathcal{T}$.*

Proof. (1) Clearly $\varphi(x,y)=\varphi(\mathcal{I}(x),y)=\varphi(x,\mathcal{I}(y))$ so $\mathcal{I}^*=\mathcal{I}$.

(2) We have the equalities

$$\begin{aligned}\varphi(x,(\mathcal{T}_1+\mathcal{T}_2)^*(y))=\psi((\mathcal{T}_1+\mathcal{T}_2)(x),y)&=\psi(\mathcal{T}_1(x),y)+\psi(\mathcal{T}_2(x),y)\\&=\varphi(x,\mathcal{T}_1^*(y))+\varphi(x,\mathcal{T}_2^*(y))\\&=\varphi(x,(\mathcal{T}_1^*+\mathcal{T}_2^*)(y)).\end{aligned}$$

(3) We have the equalities

$$\begin{aligned}\varphi(x,(c\mathcal{T})^*(y))&=\psi((c\mathcal{T})(x),y)=\psi(c\mathcal{T}(x),y)\\&=c\psi(\mathcal{T}(x),y)=c\varphi(x,\mathcal{T}^*(y))\\&=\bar{\bar{c}}\varphi(x,\mathcal{T}^*(y))=\varphi(x,\bar{c}\mathcal{T}^*(y))=\varphi(x,(\bar{c}\mathcal{T}^*)(y)).\end{aligned}$$

(4) Let X have the form ρ. Then

$$\begin{aligned}\rho(\mathcal{S}\mathcal{T}(v),x)&=\rho(\mathcal{S}(\mathcal{T}(v)),x)=\psi(\mathcal{T}(v),\mathcal{S}^*(x))\\&=\varphi(v,\mathcal{T}^*(\mathcal{S}^*(x)))=\varphi(v,(\mathcal{T}^*\mathcal{S}^*)(x)).\end{aligned}$$

(5) This is a direct consequence of (1) through (4).

(6) We do the case where both φ and ψ are Hermitian. Let $\mathcal{S}=\mathcal{T}^*$, so that, by the definition of adjoint, $\varphi(\mathcal{T}(x),y)=\varphi(x,\mathcal{S}(y))$. Now $\mathcal{S}$ has an adjoint $\mathcal{R}=\mathcal{S}^*$ if and only if $\varphi(\mathcal{S}(y),x)=\psi(y,\mathcal{R}(x))$. But

$$\varphi(\mathcal{S}(y),x)=\overline{\varphi(x,\mathcal{S}(y))}=\overline{\psi(\mathcal{T}(x),y)}=\overline{\overline{\psi(y,\mathcal{T}(x))}}=\psi(y,\mathcal{T}(x))$$

so we see that $\mathcal{R}=\mathcal{T}$, i.e., that $\mathcal{S}^*=\mathcal{T}$, i.e., that $(\mathcal{T}^*)^*=\mathcal{T}$. □

Corollary 9.5.15. *Let $\mathcal{T}\colon V\to W$ be a linear transformation with $\dim V=\dim W$ finite. Suppose that $\mathcal{T}$ is an isomorphism. Then $(\mathcal{T}^*)^{-1}=(\mathcal{T}^{-1})^*$. In particular, $\mathcal{T}^*$ is an isomorphism.*

Proof. Since V and W are finite dimensional, both $\mathcal{T}$ and $\mathcal{T}^{-1}$ have adjoints. Then

$$\mathcal{I}=\mathcal{I}^*=(\mathcal{T}\mathcal{T}^{-1})^*=(\mathcal{T}^{-1})^*\mathcal{T}^*\quad\text{and}\quad\mathcal{I}=\mathcal{I}^*=(\mathcal{T}^{-1}\mathcal{T})^*=\mathcal{T}^*(\mathcal{T}^{-1})^*$$

so $(\mathcal{T}^*)^{-1}=(\mathcal{T}^{-1})^*$. □

Theorem 9.5.16. *Let V and W be finite dimensional. Let $\mathcal{T}\colon V\to W$ be a linear transformation. Then*

$$\dim\operatorname{Im}(\mathcal{T})=\dim\operatorname{Im}(\mathcal{T}^*).$$

Proof. Let $\operatorname{Im}(\mathcal{T})$ have dimension k, and choose a basis $\mathcal{C}_0=\{w_1,\ldots,w_k\}$ for $W_0=\operatorname{Im}(\mathcal{T})$. Let $w_i=\mathcal{T}(x_i)$ for each $i=1,\ldots,k$. Then $\mathcal{C}_0$ is linearly independent so $\mathcal{B}_0=\{x_1,\ldots,x_k\}$ is linearly independent as well. Extend $\mathcal{C}_0$ to a basis $\mathcal{C}$ of W, and let $\mathcal{C}^*$ be the dual basis of W^* (Lemma 5.5.3). Let $\mathcal{C}_0^*=\{w_1^*,\ldots,w_k^*\}$ consist of the first k elements of $\mathcal{C}^*$.

Now ψ is nonsingular, so, by Lemma 9.2.8, there is a unique y_i in W such that $w_i^*=\alpha_\psi(y_i)$ for each $i=1,\ldots,k$. Let $z_i=\mathcal{T}^*(y_i)$ for each $i=1,\ldots,k$. We claim that $\mathcal{D}=\{z_1,\ldots,z_k\}$ is a linearly independent subset of V, which shows that $\dim\operatorname{Im}(\mathcal{T}^*)\geq\dim\operatorname{Im}(\mathcal{T})$.

To see this, let us evaluate $\varphi(x_i, z_j)$ for each i and j. We have

$$\begin{aligned}\varphi(x_i, z_j) = \varphi(x_i, \mathcal{T}^*(y_j)) = \psi(\mathcal{T}(x_i), y_j) = \psi(w_i, y_j)\\ = \alpha_\psi(y_j)(w_i) = w_j^*(w_i) = 1 \text{ if } j = i \text{ and } 0 \text{ if } j \neq i.\end{aligned}$$

Now suppose $\sum c_j z_j = 0$. Then for each i we have $0 = \varphi(x_i, \sum c_j z_j) = \sum \varphi(x_i, c_j z_j) = \sum \bar{c}_j \varphi(x_i, z_j) = \bar{c}_i$ so $\bar{c}_i = 0$ for each i, and then $c_i = 0$ for each i, so $\mathcal{D}$ is linearly independent.

Now by the same logic, $\dim \operatorname{Im}(\mathcal{T}^{**}) \geq \dim \operatorname{Im}(\mathcal{T}^*)$. But by Lemma 9.5.14(6), in case φ and ψ have the same type, $\mathcal{T}^{**} = \mathcal{T}$, so we get $\dim \operatorname{Im}(\mathcal{T}) \geq \dim \operatorname{Im}(\mathcal{T}^*)$, and they are equal. (If one of φ and ψ is symmetric and the other is skew-symmetric, or one is Hermitian and the other is skew-Hermitian, then $\mathcal{T}^{**} = -\mathcal{T}$ and we get the same dimension count.) □

Corollary 9.5.17. *Let $\mathcal{T}\colon V \to W$ be a linear transformation with $\dim V = \dim W$ finite. Then*

$$\dim \operatorname{Ker}(\mathcal{T}) = \dim \operatorname{Ker}(\mathcal{T}^*).$$

Proof. We know

$$\dim \operatorname{Ker}(\mathcal{T}) + \dim \operatorname{Im}(\mathcal{T}) = \dim V$$

and

$$\dim \operatorname{Ker}(\mathcal{T}^*) + \dim \operatorname{Im}(\mathcal{T}^*) = \dim W,$$

and we have just seen that $\dim \operatorname{Im}(\mathcal{T}) = \dim \operatorname{Im}(\mathcal{T}^*)$. □

Now let us look at some examples on infinite-dimensional spaces. For simplicity we stick to the real case.

Example 9.5.18. (a) Let $V = {}^t\mathbb{R}^\infty$, and let φ be the symmetric form

$$\varphi([x_1, x_2, \ldots], [y_1, y_2, \ldots]) = \sum_{i=1}^{\infty} x_i y_i.$$

Let $\mathcal{S}_{\mathrm{rt}}$ be right-shift and $\mathcal{S}_{\mathrm{lt}}$ be left-shift. Then

$$\begin{aligned}\varphi(\mathcal{S}_{\mathrm{rt}}([x_1, x_2, \ldots]), [y_1, y_2, \ldots]) &= \varphi([0, x_1, \ldots], [y_1, y_2, \ldots])\\ &= 0y_1 + x_1 y_2 + \cdots\\ &= \sum_{i=1}^{\infty} x_i y_{i+1}\end{aligned}$$

and

$$\begin{aligned}\varphi([x_1, x_2, \ldots], \mathcal{S}_{\mathrm{lt}}([y_1, y_2, \ldots])) &= \varphi([x_1, x_2, \ldots], [y_2, y_3, \ldots])\\ &= x_1 y_2 + x_2 y_3 + \cdots\\ &= \sum_{i=1}^{\infty} x_i y_{i+1}\end{aligned}$$

and these are equal. Thus $\mathcal{S}_{\mathrm{lt}}^* = \mathcal{S}_{\mathrm{rt}}$. Then Lemma 9.5.14(6) gives that $\mathcal{S}_{\mathrm{rt}}^* = \mathcal{S}_{\mathrm{lt}}$, though this is easy to check directly. Observe that

$$\mathcal{S}_{\mathrm{rt}}^* \mathcal{S}_{\mathrm{rt}} = \mathcal{S}_{\mathrm{lt}} \mathcal{S}_{\mathrm{rt}} = \mathcal{I} \quad \text{but} \quad \mathcal{S}_{\mathrm{rt}} \mathcal{S}_{\mathrm{rt}}^* = \mathcal{S}_{\mathrm{rt}} \mathcal{S}_{\mathrm{lt}} \neq \mathcal{I}$$

and similarly

$$\mathcal{S}_{\mathrm{lt}}\mathcal{S}_{\mathrm{lt}}^* = \mathcal{S}_{\mathrm{lt}}\mathcal{S}_{\mathrm{rt}} = \mathcal{I} \quad \text{but} \quad \mathcal{S}_{\mathrm{lt}}^*\mathcal{S}_{\mathrm{lt}} = \mathcal{S}_{\mathrm{rt}}\mathcal{S}_{\mathrm{lt}} \neq \mathcal{I}.$$

(b) Let V be the vector space of doubly infinite sequences of real numbers, arranged in a row, $V = \{[\dots, x_{-2}, x_{-1}, x_0, x_1, x_2, \dots]\}$, only finitely many of which are nonzero, and let $\varphi([\dots, x_{-1}, x_0, x_1, \dots], [\dots, y_{-1}, y_0, y_1, \dots]) = \sum_{i=-\infty}^{\infty} x_i y_i$. Then we similarly have right shift $\mathcal{S}_{\mathrm{rt}} \colon V \to V$ and left shift $\mathcal{S}_{\mathrm{lt}} \colon V \to V$. Again $\mathcal{S}_{\mathrm{rt}}^* = \mathcal{S}_{\mathrm{lt}}$ and $\mathcal{S}_{\mathrm{lt}}^* = \mathcal{S}_{\mathrm{rt}}$, but now

$$\mathcal{S}_{\mathrm{rt}}^*\mathcal{S}_{\mathrm{rt}} = \mathcal{S}_{\mathrm{lt}}\mathcal{S}_{\mathrm{rt}} = \mathcal{I} = \mathcal{S}_{\mathrm{rt}}\mathcal{S}_{\mathrm{lt}} = \mathcal{S}_{\mathrm{rt}}\mathcal{S}_{\mathrm{rt}}^*$$

and

$$\mathcal{S}_{\mathrm{lt}}\mathcal{S}_{\mathrm{lt}}^* = \mathcal{S}_{\mathrm{lt}}\mathcal{S}_{\mathrm{rt}} = \mathcal{I} = \mathcal{S}_{\mathrm{rt}}\mathcal{S}_{\mathrm{lt}} = \mathcal{S}_{\mathrm{lt}}^*\mathcal{S}_{\mathrm{lt}}.$$

(c) Let $V = {}^t\mathbb{R}^\infty$, and let $\mathcal{T} \colon V \to V$ be given by

$$\mathcal{T}([x_1, x_2, \dots]) = \left[\sum_{i=1}^{\infty} x_i, 0, 0, \dots\right].$$

We claim that $\mathcal{T}$ does not have an adjoint. For suppose it had an adjoint $\mathcal{T}^* \colon V \to V$. Let $y = [1, 0, 0, \dots]$ and let $z = [z_1, z_2, \dots] = \mathcal{T}^*(y)$. Since z is in V, it has only finitely many nonzero entries. Choose any value of k for which $z_k = 0$ and let $x = [0, 0, \dots, 1, 0, \dots]$ with the 1 in position k. Then for these values of x and y,

$$\varphi(\mathcal{T}(x), y) = \varphi([1, 0, \dots], [1, 0, \dots]) = 1$$

but

$$\varphi(x, \mathcal{T}^*(y)) = \varphi(x, z) = \varphi([0, \dots, 0, 1, 0, \dots], [z_1, z_2, \dots]) = z_k = 0,$$

a contradiction.

(d) Let V be the vector space of all C^∞ functions on the interval $[0, 1]$, and let φ be the form on V given by

$$\varphi(f(x), g(x)) = \int_0^1 f(x)g(x)\,dx.$$

Let $D \colon V \to V$ be differentiation, $D(f(x)) = f'(x)$. We claim that D does not have an adjoint. Suppose it did. Then we would have

$$\varphi(Df(x), g(x)) = \varphi(f(x), D^*g(x))$$

for every pair of functions $f(x), g(x)$ in V.

Let $g_0(x)$ be the function $g_0(x) = 1$, and let $h_0(x) = D^*g_0(x)$. Then

$$\varphi(Df(x), g_0(x)) = \int_0^1 f'(x)\,dx = f(x)|_0^1 = f(1) - f(0)$$

and

$$\varphi(f(x), D^*g_0(x)) = \int_0^1 f(x)h_0(x)\,dx$$

and these must be equal for every function $f(x)$.

First take $f(x) = x$. Then we see $1 = \int_0^1 xh_0(x)\,dx$ so in particular $h_0(x)$ is not the zero function.

Next take $f(x) = x^2(x-1)^2h_0(x)$. Then we see $0 = \int_0^1 x^2(x-1)^2h_0(x)^2\,dx$. But the integrand is always nonnegative and is not identically zero, so this is impossible.

(e) Let W be the subspace of V,

$$W = \{f(x) \in V \mid f^{(k)}(1) = f^{(k)}(0) \text{ for every } k = 0, 1, 2, \dots\},$$

with the same form φ on W, and again let $D\colon W \to W$ be differentiation, $Df(x) = f'(x)$. We claim that D has an adjoint on W, and in fact $D^* = -D$, i.e., $D^*f(x) = -f'(x)$. To see this we must verify that $\varphi(Df(x), g(x)) = \varphi(f(x), -Dg(x))$, or equivalently that

$$\varphi(Df(x), g(x)) - \varphi(f(x), -Dg(x)) = 0$$

for every pair of functions $f(x)$ and $g(x)$ in W. Recall that $D(f(x)g(x)) = Df(x)g(x) + f(x)Dg(x)$. (This is just the product rule for differentiation.) Then, from the fundamental theorem of calculus, we see

$$\begin{aligned}
\varphi(Df(x), g(x)) - \varphi(f(x), -Dg(x)) &= \varphi(Df(x), g(x)) + \varphi(f(x), Dg(x)) \\
&= \int_0^1 Df(x)g(x)\,dx + \int_0^1 f(x)Dg(x)\,dx \\
&= \int_0^1 (Df(x)g(x) + f(x)Dg(x))\,dx \\
&= f(x)g(x)|_0^1 = f(1)g(1) - f(0)g(0) = 0
\end{aligned}$$

as $f(1) = f(0)$ and $g(1) = g(0)$, as $f(x)$ and $g(x)$ are in W. ◊

9.6. Applications to algebra and calculus

In this section we see two applications of our work, one to algebra and one to calculus.

We assume in this section that we are in the real case.

Definition 9.6.1. A *quadratic form* Φ in n variables $x_1, \dots, x_n$ is a function

$$\Phi(x_1, \dots, x_n) = \sum_{i=1}^n a_{ii}x_i^2 + \sum_{i<j} b_{ij}x_ix_j. \qquad \Diamond$$

Example 9.6.2. Here are three quadratic forms:

(a) $\Phi_a(x_1, x_2) = 4x_1^2 + 12x_1x_2 + 25x_2^2$.

(b) $\Phi_b(x_1, x_2) = 4x_1^2 + 12x_1x_2 + 9x_2^2$.

(c) $\Phi_c(x_1, x_2) = 4x_1^2 + 12x_1x_2$. ◊

Lemma 9.6.3. *Let Φ be as in Definition 9.6.1. For $i < j$, set $a_{ji} = a_{ij} = b_{ij}/2$. Let A be the matrix $A = (a_{ij})$, a symmetric matrix, and let φ be the symmetric bilinear form on $\mathbb{R}^n$ given by $\varphi(x, y) = {}^t\!xAy$. If $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, then $\Phi(x_1, \dots, x_n) = \varphi(x, x)$.*

Proof. This is just the calculation

$$\begin{bmatrix} x_1 & \dots & x_n \end{bmatrix} \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \sum_{i,j} a_{ij}x_ix_j. \qquad \square$$

Definition 9.6.4. The matrix A as in Lemma 9.6.3 for the form Φ is the *matrix of* Φ. $\Diamond$

Example 9.6.5. Referring to Example 9.6.2:

(a) The matrix of Φ_a is $A_a = \begin{bmatrix} 4 & 6 \\ 6 & 25 \end{bmatrix}$.

(b) The matrix of Φ_b is $A_b = \begin{bmatrix} 4 & 6 \\ 6 & 9 \end{bmatrix}$.

(c) The matrix of Φ_c is $A_c = \begin{bmatrix} 4 & 6 \\ 6 & 0 \end{bmatrix}$. $\Diamond$

Here is our application.

Theorem 9.6.6. *Let Φ be a quadratic form in the variables $x_1, \dots, x_n$. Then there is an invertible linear change of variables*

$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = P \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

with P an invertible matrix, and real numbers $c_1, \dots, c_n$, each of which is 1, 0, *or* -1, *such that*

$$\Phi(y_1, \dots, y_n) = \sum_{i=1}^{n} c_i y_i^2.$$

Proof. By Theorem 9.4.7, $\mathbb{R}^n$ has a basis $\mathcal{B}$ with $[\varphi]_{\mathcal{B}}$ a diagonal matrix with all diagonal entries either 1, 0, or -1. $\square$

Example 9.6.7. Referring back to Example 9.6.2 again:

(a) $\Phi_a(x_1, x_2) = (2x_1 + 3x_2)^2 + (4x_2)^2 = y_1^2 + y_2^2$ with $y_1 = 2x_1 + 3x_2$, $y_2 = 4x_2$.

(b) $\Phi_b(x_1, x_2) = (2x_1 + 3x_2)^2 = y_1^2$ with $y_1 = 2x_1 + 3x_2$, $y_2 = x_2$.

(c) $\Phi_c(x_1, x_2) = (2x_1 + 3x_2)^2 - (3x_2)^2 = y_1^2 - y_2^2$ with $y_1 = 2x_1 + 3x_2$, $y_2 = 3x_2$. $\Diamond$

Remark 9.6.8. The way we usually think of this is that there is a linear change of variables that eliminates all of the "cross" terms $x_i x_j$ for $i \neq j$. $\Diamond$

The following special case is worth pointing out.

Definition 9.6.9. The quadratic form Φ is *positive definite* if $\Phi(x_1, \dots, x_n) > 0$ whenever $(x_1, \dots, x_n) \neq (0, \dots, 0)$. $\Diamond$

Theorem 9.6.10. *Let Φ be a positive definite quadratic form in the variables $x_1, \dots, x_n$. Then there is an invertible change of variables as in Theorem* 9.6.6 *in which $\Phi = \sum_{i=1}^{n} y_i^2$ is a sum of n linearly independent squares.*

Proof. This is the conclusion of Lemma 9.3.10 (or the case of Theorem 9.6.6 where $c_i = 1$ for $i = 1, \dots, n$). $\square$

Example 9.6.11. The form Φ_a of Example 9.6.2(a) is positive definite and we expressed Φ_a as a sum of two squares in Example 9.6.7(a). $\Diamond$

Now we have an application to calculus. Let R be a region in $\mathbb{R}^n$, and let $F\colon R \to \mathbb{R}$ be a C^2 function. If p is a point in R, then the derivative $F'(p)$ is the 1-by-n matrix

$$F'(p) = [F_1(p), \dots, F_n(p)],$$

where the subscripts denote partial derivatives. Then a is a critical point of F if $F'(a) = 0$, and we have the following theorem of calculus.

Theorem 9.6.12. *Suppose that a is a local maximum or local minimum of F. Then a is a critical point of F.*

Now suppose that a is a critical point. We would like to know whether a is a local maximum, local minimum, or neither. We have a second derivative test. To state it we must first make a definition.

Definition 9.6.13. In this situation, the *Hessian matrix* $H(p)$ of F at the point p is the n-by-n matrix whose (i, j) entry is the second partial derivative $F_{ij}(p)$. $\Diamond$

We observe that $H(p)$ is a symmetric matrix by Clairaut's theorem (equality of mixed partials).

Theorem 9.6.14. *Let a be a critical point of the function F. Let φ be the symmetric bilinear form on $\mathbb{R}^n$ whose standard matrix is $H(a)$. Then:*

(a) *If φ is positive definite, then a is a local minimum of F.*

(b) *If φ is negative definite, then a is a local maximum of F.*

(c) *If φ is indefinite, then a is neither a local minimum nor a local maximum of F.*

This is a theorem of calculus, not linear algebra, so we will not prove it here. But we want to point out that this is the right way to look at the second derivative test (especially since it is often not formulated in these terms).

9.7. Exercises

1. Let A be a symmetric matrix. Show that there is a diagonal matrix D such that $A + D$ is positive definite.

2. Let A and B be positive definite symmetric matrices. Show that $A+B$ is positive definite. (In particular, if A is positive definite and D is a diagonal matrix with all entries positive, then $A + D$ is positive definite.)

3. Let A be a positive definite symmetric n-by-n matrix, and let v be an arbitrary vector in $\mathbb{R}^n$. Let $A'(a)$ be the $(n+1)$-by-$(n+1)$ matrix

$$A'(a) = \begin{bmatrix} A & v \\ {}^t v & a \end{bmatrix}.$$

Show that there is a real number a_0 such that $A'(a)$ is positive definite whenever $a > a_0$, that $A'(a_0)$ is positive semidefinite, and that $A'(a)$ is indefinite whenever $a < a_0$.

4. (a) Let $A = (a_{ij})$ be a symmetric matrix with real entries. A is *diagonally dominant* if

$$a_{ii} > \sum_{j \neq i} |a_{ij}| \quad \text{for each } i.$$

Show that every diagonally dominant matrix A is positive definite.

(b) Suppose that

$$a_{ii} \geq \sum_{j \neq i} |a_{ij}| \quad \text{for each } i.$$

Show that A is positive semidefinite.

In particular, in this case, if A is nonsingular, then A is positive definite.

5. Let A be a positive definite Hermitian matrix. Show that A can be written uniquely as $A = LL^*$, where L is a lower triangular matrix with diagonal entries positive real numbers. This is known as the *Cholesky decomposition* of A.

6. Find the rank and signature of each of the following matrices:

(a) $A = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}$.

(b) $A = \begin{bmatrix} 1 & 3 \\ 3 & 10 \end{bmatrix}$.

(c) $A = \begin{bmatrix} 2 & 3 & 1 \\ 3 & 7 & 2 \\ 1 & 2 & 3 \end{bmatrix}$.

(d) $A = \begin{bmatrix} 2 & 3 & 3 \\ 3 & 6 & 0 \\ 3 & 0 & 18 \end{bmatrix}$.

7. Let A be a real symmetric matrix, and let c be a nonzero real number.

(a) Show that $\sigma(cA) = \operatorname{sign}(c)\sigma(A)$.

(b) Let A_c be the matrix obtained from A by multiplying all the diagonal entries of A by c and leaving the other entries unchanged.

(i) Suppose that A is not a diagonal matrix (so that $A_c \neq cA$). Suppose all the diagonal entries of A are positive. Show that there is some positive value of c for which A_c is positive definite and that there is some positive value of c for which A_c is not positive definite.

(ii) If all of the diagonal entries of A are 0, then $A_{-1} = A_1$, so certainly $\sigma(A_{-1}) = \sigma(A_1)$. Find an example of a matrix A not all of whose diagonal entries are 0 with $\sigma(A_{-1}) = \sigma(A_1)$.

Note that (b) shows that in general it is not the case that $\sigma(A_c) = \operatorname{sign}(c)\sigma(A)$.

8. Find the signatures of each of the following symmetric matrices:

(a) $A = (a_{ij})$, $i, j = 1, \dots, n$, with

$$\begin{aligned} a_{ii} &= 2, \quad && i = 1, \dots, n, \\ a_{ij} &= 1, && \text{if } |i-j| = 1, \\ a_{ij} &= 0, && \text{otherwise.} \end{aligned}$$

(b) $A = (a_{ij})$, $i, j = 1, \dots, n$, with

$$\begin{aligned} a_{ii} &= 2, \quad && i = 1, \dots, k, \\ a_{ii} &= 0, && i = k+1, \\ a_{ii} &= -2, && i = k+2, \dots, n, \\ a_{ij} &= 1 && \text{if } |i-j| = 1, \\ a_{ij} &= 0 && \text{otherwise.} \end{aligned}$$

(c) $$E_8 = \begin{bmatrix} 2 & 1 & & & & & & \\ 1 & 2 & 1 & & & & & \\ & 1 & 2 & 1 & & & & \\ & & 1 & 2 & 1 & & & \\ & & & 1 & 2 & 1 & 0 & 1 \\ & & & & 1 & 2 & 1 & 0 \\ & & & & 0 & 1 & 2 & 1 \\ & & & & 1 & 0 & 1 & 2 \end{bmatrix}.$$

9. Diagonalize the following quadratic forms:

(a) $4x^2 + 10xy + 13y^2$.

(b) $3x^2 - 2xy - 8y^2$.

(c) $41x^2 + 24xy + 34y^2$.

10. Let φ be an indefinite symmetric form on a real vector space V, or an indefinite Hermitian form on a complex vector space V. Let x and y be vectors in V with $\varphi(x, x) > 0$ and $\varphi(y, y) < 0$. Find a nonzero linear combination z of x and y with $\varphi(z, z) = 0$.

11. (a) Let φ be a nonsingular symmetric form on a real vector space V, or a nonsingular Hermitian form on a complex vector space V. Suppose that there is some nonzero vector x in V with $\varphi(x, x) = 0$. By the nonsingularity of φ, there must be a vector y in V with $\varphi(x, y) \neq 0$. Find linear combinations z_+ and z_- of x and y with $\varphi(z_+, z_+) > 0$ and $\varphi(z_-, z_-) < 0$. (Thus, in this case φ is indefinite.)

(b) Use this to prove Lemma 9.4.16.

12. (a) Let φ be a form on a complex vector space V. Show that φ is skew-Hermitian if and only if $\psi = i\varphi$ is Hermitian.

(b) Use this to classify skew-Hermitian forms on finite-dimensional complex vector spaces.

13. Fill in the details of the proof of Theorem 9.4.3.

14. In the setting, and notation, of Theorem 9.4.12: suppose that it is never the case that both $\delta_{k-1}(A) = 0$ and $\delta_k(A) = 0$. Let $\varepsilon_k(A) = +1$ if $\delta_k(A) > 0$, $\varepsilon_k(A) = -1$ if $\delta_k(A) < 0$, and $e_k(A) = -e_{k-1}(A)$ if $\delta_k(A) = 0$. Show that A has signature $\sigma = r - s$, where r is the number of values of k between 1 and n for which $\varepsilon_{k-1}(A)$ and $\varepsilon_k(A)$ have the same sign and s is the number of values of k between 1 and n for which $\varepsilon_{k-1}(A)$ and $\varepsilon_k(A)$ have opposite signs.

15. Let V be an n-dimensional real (resp., complex) vector space, and let φ be a symmetric bilinear (resp., Hermitian sesquilinear) form on V. Suppose that V has an m-dimensional subspace W such that the restriction of φ to W is identically 0.

(a) If $m > n/2$, show that φ must be singular.

(b) If φ is nonsingular and $m = n/2$, show that φ has signature 0.

16. Fill in the details of the proof of Lemma 9.5.2.

17. In the setting, and notation, of Section 9.5, suppose that V and W are finite-dimensional vector spaces. Let $\mathcal{B}$ be a basis of V, and let $\mathcal{C}$ be a basis of W. Let $M = [\varphi]_{\mathcal{B}}$ and $N = [\psi]_{\mathcal{C}}$. Let $A = [\mathcal{T}]_{\mathcal{C}\leftarrow\mathcal{B}}$ and $B = [\mathcal{T}^*]_{\mathcal{B}\leftarrow\mathcal{C}}$.

(a) Express B in terms of M, N, and A. (Note that this gives a definition of the adjoint $\mathcal{T}^*$ of $\mathcal{T}$ purely in terms of matrices, and in particular provides a computational proof of Lemmas 9.5.2 and 9.5.3 in this case.)

(b) Now let $C = [\mathcal{T}^{**}]_{\mathcal{C}\leftarrow\mathcal{B}}$. Express C in terms of B. Suppose φ and ψ have the same type. Show that $C = A$, thereby providing a computational proof that $\mathcal{T}^{**} = \mathcal{T}$ in this case (cf. Lemma 9.5.14(6)).

18. Let $V = P_n(\mathbb{R})$ with the inner product

$$\langle f(x), g(x)\rangle = \int_0^1 f(x)g(x)\,dx.$$

Let $D\colon V \to V$ be the linear transformation $D(f(x)) = f'(x)$. For $n = 0, 1, 2, 3$, find D^*, the adjoint of D.

19. (a) Let V be a *real* vector space. Show that {bilinear forms on V} is a *real* vector space.

(b) Let V be a *complex* vector space. Show that {sesquilinear forms on V} is a *complex* vector space.

(c) Let V be a *complex* vector space. Show that {Hermitian forms on V} and {skew-Hermitian forms on V} are both *real* vector spaces.

20. Let V be a finite-dimensional real vector space, $\dim(V) = n$, and let $f^*, g^* \in V^*$, the dual space of V. Define $L_{f^*,g^*}(v, w)$ by

$$L_{f^*,g^*}(v, w) = f^*(v)g^*(w).$$

(a) Show that $L_{f^*,g^*}(v, w)$ is a bilinear form on V.

(b) Let $\{b_1, \dots, b_n\}$ be a basis of V, and let $\{b_1^*, \dots, b_n^*\}$ be the dual basis of V^*. Show that

$$\{L_{b_i^*,b_j^*} \mid i = 1, \dots, n, j = 1, \dots, n\}$$

is a basis for {bilinear forms on V} (and hence that this vector space has complex dimension n^2).

(c) Let
$$L^+_{f^*,g^*}(v,w) = L_{f^*,g^*}(v,w) + L_{g^*,f^*}(v,w)$$
and
$$L^-_{f^*,g^*}(v,w) = L_{f^*,g^*}(v,w) - L_{g^*,f^*}(v,w).$$
Show that $L^+_{f^*,g^*}$ is a symmetric bilinear form and that $L^-_{f^*,g^*}(v,w)$ is a skew-symmetric bilinear form on V.

(d) Show that
$$\{L^+_{b_i^*,b_j^*} \,|\, 1 \leq i \leq j \leq n\}$$
is a basis for {symmetric bilinear forms on V} (and hence that this space has dimension $n(n+1)/2$) and that
$$\{L^-_{b_i^*,b_j^*} \,|\, 1 \leq i < j \leq n\}$$
is a basis for {skew-symmetric bilinear forms on V} (and hence that this space has dimension $n(n-1)/2$).

21. Let V be a finite-dimensional complex vector space, $\dim(V) = n$, and let $f^*, g^* \in V^*$, the dual space of V. Define $\tilde{L}_{f^*,g^*}(v,w)$ by
$$\tilde{L}_{f^*,g^*}(v,w) = f^*(v)\bar{g}^*(w).$$

(a) Show that $\tilde{L}_{f^*,g^*}(v,w)$ is a Hermitian form on V.

(b) Let $\{b_1, \ldots, b_n\}$ be a basis of V, and let $\{b_1^*, \ldots, b_n^*\}$ be the dual basis. Show that
$$\{\tilde{L}_{b_i^*,b_j^*} \,|\, 1 \leq i \leq n, 1 \leq j \leq n\}$$
is a basis for {sesquilinear forms on V} (and hence that this complex vector space has complex dimension n^2).

(c) Let
$$\tilde{L}^+_{f^*,g^*}(v,w) = \tilde{L}_{f^*,g^*}(v,w) + \tilde{L}_{g^*,f^*}(v,w)$$
and
$$\tilde{L}^-_{f^*,g^*}(v,w) = \tilde{L}_{f^*,g^*}(v,w) - \tilde{L}_{g^*,f^*}(v,w).$$
Show that $\tilde{L}^+_{f^*,g^*}$ is a Hermitian form and that $\tilde{L}^-_{f^*,g^*}$ is a skew-Hermitian form.

(d) Show that
$$\{\tilde{L}^+_{b_i^*,b_i^*} \,|\, i = 1, \ldots, n\} \cup \{\tilde{L}^+_{b_i^*,b_j^*}, i\tilde{L}^+_{b_i^*,b_j^*} \,|\, 1 \leq i < j \leq n\}$$
is a basis for {Hermitian forms on V} (and hence that this real vector space has real dimension n^2) and that
$$\{i\tilde{L}^-_{b_i^*,b_i^*} \,|\, i = 1, \ldots, n\} \cup \{\tilde{L}^-_{b_i^*,b_j^*}, i\tilde{L}^-_{b_i^*,b_j^*} \,|\, 1 \leq i < j \leq n\}$$
is a basis for {skew-Hermitian forms on V} (and hence that this real vector space has real dimension n^2).

Chapter 10

Inner product spaces

10.1. Definition, examples, and basic properties

In this chapter we specialize our attention from arbitrary bilinear forms (over $\mathbb{R}$) or sesquilinear forms (over $\mathbb{C}$) to ones that are positive definite.

Definition 10.1.1. Let V be a real (resp., complex) vector space, and let $\varphi(x, y) = \langle x, y\rangle$ be a positive definite symmetric bilinear (resp., Hermitian sesquilinear) form on V. Then φ is an *inner product* and V is an *inner product space.* $\Diamond$

We will (almost) exclusively use the notation $\langle x, y\rangle$ in this chapter.

Remark 10.1.2. Some authors call any nonsingular symmetric bilinear/Hermitian sesquilinear form an inner product, so beware. $\Diamond$

Given that we have an inner product, we can define the length (or norm, to use the right technical term) of a vector.

Definition 10.1.3. Let x be a vector in the inner product space V. Then the *norm* of x is $\|x\| = \sqrt{\langle x, x\rangle}$. $\Diamond$

Example 10.1.4. We refer back to, and use the notation of, Example 9.1.6.

(a) The "dot product" $\langle x, y\rangle = {}^t x y$ (in the real case) or $\langle x, y\rangle = {}^t x \bar{y}$ (in the complex case) is an inner product, and $\|x\| = \sqrt{a_1^2 + \cdots + a_n^2}$ (in the real case) or $\|x\| = \sqrt{|a_1|^2 + \cdots + |a_n|^2}$ (in the complex case), on $\mathbb{R}^n$ (or $\mathbb{C}^n$).

(b) Let A be any positive definite symmetric (real) or Hermitian (complex) n-by-n matrix, and let $V = \mathbb{R}^n$ (or $\mathbb{C}^n$) with $\langle x, y\rangle = {}^t x A y$ (or $\langle x, y\rangle = {}^t x A \bar{y}$). Then V is an inner product space. In particular, this is the case if A is a diagonal matrix with diagonal entries $w_1, \ldots, w_n$, all of which are positive real numbers.

(c) $V = \mathbb{R}^\infty$ with $\langle x, y\rangle = \sum_{i=1}^{\infty} x_i y_i$, or $V = \mathbb{C}^\infty$ with $\langle x, y\rangle = \sum_{i=1}^{\infty} x_i \bar{y}_i$, is an inner product space.

(d) If V is the vector space of real-valued (resp., complex-valued) continuous functions in $[0,1]$ with

$$\langle f(x), g(x)\rangle = \int_0^1 f(x)g(x)\,dx \quad \text{in the real case,}$$
$$\langle f(x), g(x)\rangle = \int_0^1 f(x)\bar{g}(x)\,dx \quad \text{in the complex case,}$$

then V is an inner product space, and

$$\|f(x)\| = \left(\int_0^1 |f(x)|^2\,dx\right)^{1/2}.$$

More generally, if $w(x)$ is any real-valued continuous function on $[0,1]$ with $w(x) \geq 0$ for every x in $[0,1]$, and such that there is no subinterval $[a,b]$ of $[0,1]$ (with $a < b$) on which $w(x) = 0$, then

$$\langle f(x), g(x)\rangle = \int_0^1 f(x)g(x)w(x)\,dx \quad \text{in the real case,}$$
$$\langle f(x), g(x)\rangle = \int_0^1 f(x)g(x)\bar{w}(x)\,dx \quad \text{in the complex case}$$

are inner products on V. $\Diamond$

Remark 10.1.5. As these examples make clear, the same vector space can have (infinitely) many different inner products. Thus, to be precise, in Definition 10.1.1 we should have said the pair $(V, \langle,\rangle)$ is an inner product space. But we are following common mathematical practice in just saying V is an inner product space, when the inner product $\langle,\rangle$ is understood. $\Diamond$

As you can see, we have been almost repeating ourselves by stating things first in the real and then in the complex case. In the future we will almost always simply state and prove things in the complex case; then the statements and proofs will apply to the real case simply by forgetting the conjugation. There will be a few times, though, when we will have to handle the real and complex cases separately.

Let us see that, just knowing the norms of vectors, we can recover the inner products of any pair of vectors.

Lemma 10.1.6 (Polarization identities)**.** (a) *Let V be a real inner product space. Then for any x, y in V,*

$$\langle x, y\rangle = (1/4)\|x+y\|^2 - (1/4)\|x-y\|^2.$$

(b) *Let V be a complex inner product space. Then for any x, y in V,*

$$\langle x, y\rangle = (1/4)\|x+y\|^2 + (i/4)\|x+iy\|^2 - (1/4)\|x-y\|^2 - (i/4)\|x-iy\|^2.$$

Proof. Direct calculation. $\square$

Now let us see some important properties of norms of vectors.

Lemma 10.1.7. *Let V be an inner product space.*

(a) *For any vector x in V, $\|x\| \geq 0$, and $\|x\| = 0$ if and only if $x = 0$.*

(b) *For any vector x in V and any scalar c, $\|cx\| = |c| \, \|x\|$.*

(c) (Cauchy-Schwartz-Buniakowsky inequality) *For any two vectors x and y in V, $|\langle x, y\rangle| \leq \|x\| \, \|y\|$, with equality if and only if $\{x, y\}$ is linearly dependent.*

(d) (Triangle inequality) *For any two vectors x and y in V, $\|x+y\| \leq \|x\|+\|y\|$, with equality if and only if $x = 0$ or $y = 0$, or $y = px$ (or equivalently $x = qy$) for some positive real number p (or q).*

Proof. (a) and (b) are immediate.

(c) If $x = 0$ or $y = 0$, then we get $0 = 0$; if $y = cx$, then $|\langle x, y\rangle| = |\langle x, cx\rangle| = |\bar{c}\langle x, x\rangle| = |\bar{c}| \, \|x\|^2 = |c| \, \|x\|^2$, and $\|x\| \, \|y\| = \|x\|(|c| \, \|x\|) = |c| \, \|x\|^2$ and we also have equality. That takes care of the case when $\{x, y\}$ is linearly dependent.

Suppose $\{x, y\}$ is linearly independent. Then $x - cy \neq 0$ for any c, so $\|x - cy\| \neq 0$. But then

$$\begin{aligned} 0 < \|x - cy\|^2 = \langle x - cy, x - cy\rangle &= \langle x, x\rangle + \langle -cy, x\rangle + \langle x, -cy\rangle + \langle cy, cy\rangle \\ &= \langle x, x\rangle - c\langle y, x\rangle - \bar{c}\langle x, y\rangle + |c|^2\langle y, y\rangle \\ &= \langle x, x\rangle - c\overline{\langle x, y\rangle} - \bar{c}\langle x, y\rangle + |c|^2\langle y, y\rangle. \end{aligned}$$

Now set $c = \langle x, y\rangle/\langle y, y\rangle$. Then this inequality becomes

$$\begin{aligned} 0 &< \langle x, x\rangle - 2\langle x, y\rangle\overline{\langle x, y\rangle}/\langle y, y\rangle + (\langle x, y\rangle\overline{\langle x, y\rangle}/\langle y, y\rangle^2)(\langle y, y\rangle) \\ &= \langle x, x\rangle - 2\langle x, y\rangle\overline{\langle x, y\rangle}/\langle y, y\rangle + \langle x, y\rangle\overline{\langle x, y\rangle}/\langle y, y\rangle \\ &= \langle x, x\rangle - \langle x, y\rangle\overline{\langle x, y\rangle}/\langle y, y\rangle = \|x\|^2 - |\langle x, y\rangle|^2/\|y\|^2 \end{aligned}$$

and so

$$\begin{aligned} &|\langle x, y\rangle|^2/\|y\|^2 < \|x\|^2, \\ &|\langle x, y\rangle|^2 < \|x\|^2\|y\|^2 \end{aligned}$$

yielding the result.

(d) We have that

$$\begin{aligned} \|x + y\|^2 &= \langle x + y, x + y\rangle \\ &= \langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle + \langle y, y\rangle \\ &= \langle x, x\rangle + \langle x, y\rangle + \overline{\langle x, y\rangle} + \langle y, y\rangle. \end{aligned}$$

Now for any complex number c, $c + \bar{c} = 2\,\mathrm{Re}(c) \leq 2|c|$. Applying this to the two middle terms gives

$$\begin{aligned} \|x + y\|^2 &\leq \langle x, x\rangle + 2|\langle x, y\rangle| + \langle y, y\rangle \\ &= \|x\|^2 + 2|\langle x, y\rangle| + \|y\|^2. \end{aligned}$$

But now, by the Cauchy-Schwartz-Buniakowsky inequality, $|\langle x, y\rangle| \leq \|x\| \, \|y\|$, so we see

$$\begin{aligned} \|x + y\|^2 &\leq \|x\|^2 + 2\|x\| \, \|y\| + \|y\|^2 \\ &= (\|x\| + \|y\|)^2 \end{aligned}$$

yielding the inequality.

When can we have equality? Certainly if $x = 0$ or $y = 0$ we do. Suppose not. In order to have $\|x+y\| = \|x\| + \|y\|$ each of the above two inequalities must be equalities. For the Cauchy-Schwartz-Buniakowsky inequality to be an equality we must have that $\{x, y\}$ is linearly dependent, so we must have $y = px$ for some complex number p. But for the first inequality to be an equality we must have $\langle x, y\rangle + \overline{\langle y, x\rangle} = 2|\langle x, y\rangle|$. Setting $y = px$ and remembering that $\langle x, x\rangle = \|x\|^2$ is a positive real number,

$$\begin{aligned}\langle x, y\rangle + \overline{\langle x, y\rangle} &= \langle x, px\rangle + \overline{\langle x, px\rangle} = \bar{p}\langle x, x\rangle + \overline{\bar{p}\langle x, x\rangle} \\ &= \bar{p}\langle x, x\rangle + p\langle x, x\rangle = (p+\bar{p})\langle x, x\rangle\end{aligned}$$

while

$$2|\langle x, y\rangle| = 2|\langle x, px\rangle| = 2|\bar{p}\langle x, x\rangle| = 2|\bar{p}|\langle x, x\rangle$$

so we must have $p + \bar{p} = 2|\bar{p}| = 2|p|$, which is true if and only if p is a positive real number. □

Here is a useful application.

Corollary 10.1.8. (a) *Let $a_1, \dots, a_n$ and $b_1, \dots, b_n$ be two sequences of n complex numbers. Then*

$$\left|\sum_{i=1}^{n} a_i \bar{b}_i\right|^2 \le \left(\sum_{i=1}^{n} |a_i|^2\right)\left(\sum_{i=1}^{n} |b_i|^2\right).$$

(b) *Let $f(x)$ and $g(x)$ be continuous functions on $[0, 1]$. Then*

$$\left(\int_0^1 f(x)\bar{g}(x)\,dx\right)^2 \le \left(\int_0^1 |f(x)|^2\,dx\right)\left(\int_0^1 |g(x)|^2\,dx\right).$$

Proof. These are the Cauchy-Schwartz-Buniakowsky inequality applied to the inner product spaces V of Example 10.1.4(a) and (b), respectively. □

Definition 10.1.9. Let V be an inner product space. A vector x in V is a *unit vector* if $\|x\| = 1$. A set of vectors $\mathcal{S} = \{x_1, x_2, \dots\}$ is *orthogonal* if $\langle x_i, x_j\rangle = 0$ for $i \neq j$. It is *orthonormal* if $\langle x_i, x_j\rangle = 1$ for $i = j$ and 0 for $i \neq j$, i.e., if it is an orthogonal set of unit vectors. A basis $\mathcal{B}$ of V is an *orthogonal* (resp., *orthonormal*) *basis* of V if it is both a basis and an orthogonal (resp., orthonormal) set. ◊

Lemma 10.1.10. *Let $\mathcal{S} = \{x_1, x_2, \dots\}$ be an orthogonal set of nonzero vectors in V. If $x = \sum c_i x_i$ is a linear combination of the vectors in $\mathcal{S}$, then $c_i = \langle x, x_i\rangle/\|x_i\|^2$ for each i. In particular, if $\mathcal{S}$ is an orthonormal set, then $c_i = \langle x, x_i\rangle$ for every i.*

Furthermore, in this situation $\|x\| = \sum_i |c_i|^2\|x_i\|^2 = \sum_i |\langle x, x_i\rangle|^2\|x_i\|^2$ and if $\mathcal{S}$ is orthonormal, $\|x\| = \sum_i |c_i|^2 = \sum_i |\langle x, x_i\rangle|^2$.

Proof. We simply compute

$$\langle x, x_i\rangle = \left\langle \sum_j c_j x_j, x_i \right\rangle = \sum_j c_j\langle x_j, x_i\rangle = c_i\langle x_i, x_i\rangle = c_i\|x_i\|^2.$$

We also compute

$$\langle x, x\rangle = \left\langle \sum_j c_j x_j, \sum_i c_i x_i \right\rangle = \sum_{j,i} c_j \bar{c}_i \langle x_j, x_i\rangle = \sum_i |c_i|^2 \|x_i\|^2. \qquad \square$$

Corollary 10.1.11. *If $\mathcal{S} = \{x_1, x_2, \dots\}$ is an orthogonal set of nonzero vectors in V, then $\mathcal{S}$ is linearly independent.*

Proof. By the above lemma, if $0 = \sum c_i x_i$, then $c_i = 0$ for each i. $\square$

Now $\mathcal{B}$ is a basis of V if and only if every vector in V is a unique linear combination of the vectors in $\mathcal{B}$. If $\mathcal{B}$ is orthogonal, then this lemma gives us the linear combination.

Corollary 10.1.12. *Let $\mathcal{B} = \{x_1, x_2, \dots\}$ be an orthogonal basis of V. Then for any vector x in V,*

$$x = \sum_i (\langle x, x_i\rangle / \|x_i\|^2) x_i.$$

In particular, if $\mathcal{B}$ is orthonormal,

$$x = \sum_i \langle x, x_i\rangle x_i.$$

Proof. We know $x = \sum c_i x_i$ and Lemma 10.1.10 gives the value of each c_i. $\square$

Corollary 10.1.13 (Bessel's inequality)**.** *Let $\mathcal{S} = \{x_1, \dots, x_n\}$ be a finite orthogonal set of nonzero vectors in V. For any $x \in V$,*

$$\sum_{i=1}^n \langle x, x_i\rangle / \|x_i\|^2 \le \|x\|^2$$

with equality if and only if $x = \sum_{i=1}^n (\langle x, x_i\rangle / \|x_i\|^2) x_i$. In particular, if $\mathcal{S}$ is orthonormal,

$$\sum_{i=1}^n |\langle x, x_i\rangle|^2 \le \|x\|$$

with equality if and only if $x = \sum_{i=1}^n \langle x, x_i\rangle x_i$.

Proof. Let $y = \sum_{i=1}^n (\langle x, x_i\rangle / \|x_i\|^2) x_i$ and set $z = x - y$. Then, as we have just seen, $\langle x, x_i\rangle = \langle y, x_i\rangle$ for each i, so $\langle z, x_i\rangle = 0$ for each i, and so $\langle z, y\rangle = 0$. But then

$$\begin{aligned}\|x\|^2 = \|y + z\|^2 = \langle y + z, y + z\rangle &= \langle y, y\rangle + \langle y, z\rangle + \langle z, y\rangle + \langle z, z\rangle \\ &= \langle y, y\rangle + \langle z, z\rangle = \|y\|^2 + \|z\|^2 \ge \|y\|^2\end{aligned}$$

with equality if and only if $z = 0$, i.e., if $x = y$. But

$$\|y\|^2 = \sum_{i=1}^n (\overline{\langle x, x_i\rangle / \|x_i\|^2})^2 \|x_i\|^2 = \sum_{i=1}^n |\langle x, x_i\rangle|^2 / \|x_i\|^2. \qquad \square$$

Example 10.1.14. If $V = \mathbb{R}^n$ or $\mathbb{C}^n$ and $\langle , \rangle$ is the dot product, then the standard basis $\mathcal{E} = \{e_1, \dots, e_n\}$ is an orthonormal basis of V. We already know that any $x = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ is given by $x = a_1 e_1 + \cdots + a_n e_n$. But we see directly that $\langle x, e_i \rangle = a_i$ for each i, verifying Lemma 10.1.10 in this case. $\Diamond$

As a matter of standard notation, if c is a nonzero scalar and x is a vector, we will often write $(1/c)x$ as x/c.

We make the following simple observation.

Lemma 10.1.15. *If x is any nonzero vector in V, then $x/\|x\|$ is a unit vector.*

Proof. Let $c = 1/\|x\|$. Then $\|cx\| = |c|\,\|x\| = 1$. $\square$

This leads to the following definition.

Definition 10.1.16. Let x be a nonzero vector in V. Then $y = N(x) = x/\|x\|$ is the *normalization* of x. If $\{x_1, x_2, \dots\}$ is any orthogonal set of nonzero vectors in V, its *normalization* is the orthonormal set $\{y_1, y_2, \dots\}$, where $y_i = N(x_i)$ for each i. $\Diamond$

We briefly consider a generalization of inner product spaces.

Definition 10.1.17. Let V be a vector space over $\mathbb{R}$ or $\mathbb{C}$. A *norm* on V is a function $\|\cdot\|$ from V to $\mathbb{R}$ with the properties:

(i) $\|0\| = 0$ and $\|x\| > 0$ if $x \neq 0$,

(ii) $\|cv\| = |c|\|x\|$ for any scalar c and x in V,

(iii) $\|x + y\| \leq \|x\| + \|y\|$ for any x and y in V.

The pair $(V, \|\cdot\|)$ is a *normed vector space.* $\Diamond$

Theorem 10.1.18. *Let $(V, \langle , \rangle)$ be a real or complex inner product space and set $\|x\| = \sqrt{\langle x, x \rangle}$. Then $(V, \|\cdot\|)$ is a normed vector space.*

Proof. Properties (i) and (ii) are immediate, and property (iii) is the triangle inequality (Lemma 10.1.7(d)). $\square$

Remark 10.1.19. On the one hand, we have emphasized in this book that we are doing algebra, and so all of our linear combinations are finite sums. On the other hand, we have also emphasized that linear algebra applies throughout mathematics, and in doing analysis, we are often interested in infinite sums. In order for those to make sense, we need a notion of convergence, and that is given to us by a norm. Indeed, different norms can define different vector spaces, or give different notions of convergence on the same vector space. For the interested reader, we include a short appendix which is an introduction to some of the considerations involved. $\Diamond$

10.2. Subspaces, complements, and bases

We continue to suppose that V is an inner product space with inner product $\varphi(x, y) = \langle x, y \rangle$.

Of course, an inner product is a special kind of symmetric or Hermitian form, and we have already investigated these in general. We want to begin by recalling some of our previous results and seeing how we can strengthen them in our situation.

Lemma 10.2.1. *Let W be any subspace of V. Then W is nonsingular in the sense of Definition* 9.2.6.

Proof. By Lemma 9.2.7, W is nonsingular if and only if for any nonzero $y \in W$ there is an $x \in W$ with $\langle x, y \rangle \neq 0$. But we can simply choose $x = y$, as $\langle y, y \rangle > 0$ for any $y \neq 0$. □

Definition 10.2.2. Two subspaces W_1 and W_2 of V are *orthogonal* if $\langle x, y \rangle = 0$ for every $x \in W_1$, $y \in W_2$.

V is the *orthogonal direct sum* of two subspaces W_1 and W_2, $V = W_1 \perp W_2$, if V is the direct sum $V = W_1 \oplus W_2$, and W_1 and W_2 are orthogonal. In this case W_2 is the *orthogonal complement* of W_1, and vice-versa. ◊

Definition 10.2.3. Let W be a subspace of V. Its *orthogonal subspace* $W^\perp$ is the subspace
$$W^\perp = \{x \in V \mid \langle x, y \rangle = 0 \text{ for every } y \in W\}. \qquad \Diamond$$

Lemma 10.2.4. (a) *Let W be an arbitrary subspace of V. Then*

(i) $W \cap W^\perp = \{0\}$,

(ii) $W \subseteq (W^\perp)^\perp$.

(b) *Let W be a finite-dimensional subspace of V. Then $V = W \perp W^\perp$, so that $W^\perp$ is the orthogonal complement of W.*

(c) *If $V = W \perp W^\perp$, then $W = (W^\perp)^\perp$.*

Proof. (a) (i) If $x \in W \cap W^\perp$, then, since $x \in W$ and $x \in W^\perp$, $\langle x, x \rangle = 0$. But that implies $x = 0$.

(ii) From Definition 10.2.3 we see that every $y \in W$ is orthogonal to every x in $W^\perp$, so $W \subseteq (W^\perp)^\perp$.

(b) We proved this in Lemma 9.3.2. Let us recall: first, we have just seen that $W \cap W^\perp = \{0\}$, so we only need to show $W + W^\perp = V$. Let $v_0 \in V$. Then $\mathcal{T}(w) = \langle w, v_0 \rangle$ is a linear transformation $\mathcal{T}\colon W \to \mathbb{F}$. Since W is nonsingular and W is finite dimensional, by Lemma 9.2.8 there is some $w_0 \in W$ with $\mathcal{T}(w) = \langle w, w_0 \rangle$ for every $w \in W$. Let $w_1 = v_0 - w_0$. Then
$$\langle w, w_1 \rangle = \langle w, v_0 - w_0 \rangle = \langle w, v_0 \rangle - \langle w, w_0 \rangle = 0 \quad \text{for every } w \in W,$$
so $w_1 \in W^\perp$. But then $v_0 = w_0 + w_1$, with $w_0 \in W$ and $w_1 \in W^\perp$.

(c) Let z be any element of $(W^\perp)^\perp$. Since $V = W \perp W^\perp$, we can write z (uniquely) as $z = w_0 + w_1$, with $w_0 \in W$ and $w_1 \in W^\perp$. Since $z \in (W^\perp)^\perp$, $\langle z, w \rangle = 0$ for every $w \in W^\perp$. In particular, $\langle z, w_1 \rangle = 0$. But then
$$0 = \langle z, w_1 \rangle = \langle w_0 + w_1, w_1 \rangle = \langle w_0, w_1 \rangle + \langle w_1, w_1 \rangle = 0 + \langle w_1, w_1 \rangle = \langle w_1, w_1 \rangle$$
so $w_1 = 0$. But then $z = w_0 \in W$. □

In general, if W is infinite dimensional, it may or may not be the case that $V = W \perp W^\perp$. We illustrate both possibilities.

Example 10.2.5. (a) Let $V = {}^t\mathbb{R}^\infty$ with

$$\langle [x_1, x_2, x_3, \ldots], [y_1, y_2, y_3, \ldots] \rangle = \sum x_i y_i.$$

Let W be the subspace $W = \{[x_1, 0, x_3, 0, x_5, 0, \ldots]\}$. Then $W^\perp$ is the subspace $W^\perp = \{[0, x_2, 0, x_4, 0, x_6, \ldots]\}$ and $V = W \perp W^\perp$.

(b) Let V be the subspace of ${}^t\mathbb{R}^{\infty\infty}$ given by

$$V = \{[x_1, x_2, x_3, \ldots] \mid |x_i| \text{ are bounded}\},$$

i.e., for each element of V there is an M with $|x_i| < M$ for every i. Let V have the inner product

$$\langle [x_1, x_2, x_3, \ldots], [y_1, y_2, y_3, \ldots] \rangle = \sum x_i y_i / 2^i.$$

Let $W = {}^t\mathbb{R}^\infty$, a proper subspace of V. Then $W^\perp = \{[0, 0, 0, \ldots]\}$. To see this, suppose $y = [y_1, y_2, y_3, \ldots] \in W^\perp$. Now $e_i = [0, 0, \ldots, 1, 0, \ldots]$, with the 1 in position i, is in W. But then $\langle y, e_i \rangle = y_i / 2^i = 0$, and this must be true for every i. Thus $V \neq W \perp W^\perp$. (Also, $(W^\perp)^\perp = V$ so $W \neq (W^\perp)^\perp$.) $\Diamond$

Remark 10.2.6. As we have earlier observed, a subspace W will in general have (infinitely) many complements, none of which is to be preferred. But if V is an inner product space, and W is a subspace with $V = W \perp W^\perp$, then W does have a distinguished complement, its orthogonal complement $W^\perp$. $\Diamond$

Definition 10.2.7. Suppose $V = W \perp W^\perp$. Then Π_W, the *orthogonal projection* of V onto W, is the linear transformation given as follows.

Write $z \in V$ uniquely as $z = w_0 + w_1$, with $w_0 \in W$ and $w_1 \in W^\perp$. Then $\Pi_W(z) = w_0$. $\Diamond$

We observe some properties of orthogonal projections.

Lemma 10.2.8. *Suppose $V = W \perp W^\perp$. Then:*

(a) $\Pi_W(z) = z$ *if and only if* $z \in W$, *and* $\Pi_W(z) = 0$ *if and only if* $z \in W^\perp$.

(b) $\Pi_W + \Pi_{W^\perp} = \mathcal{I}$ (*the identity*).

(c) $\Pi_W^2 = \Pi_W$ *and* $\Pi_{W^\perp}^2 = \Pi_{W^\perp}$. *Also* $\Pi_W \Pi_{W^\perp} = 0$ *and* $\Pi_{W^\perp} \Pi_W = 0$.

Proof. These properties all follow directly from the definition. $\square$

Recall by Lemma 10.2.4 that if W is finite dimensional, it is always the case that $V = W \perp W^\perp$. In this situation we have the following formula.

Lemma 10.2.9. *Let W be a finite-dimensional subspace of V, and let $\mathcal{B} = \{x_1, \ldots, x_k\}$ be an orthogonal basis of W. Then for any $z \in V$*

$$\Pi_W(z) = \sum_{i=1}^{k} (\langle z, x_i \rangle / \|x_i\|)^2 x_i.$$

In particular, if $\mathcal{B}$ is an orthonormal basis of W,

$$\Pi_W(z) = \sum_{i=1}^{k} \langle z, x_i \rangle x_i.$$

Proof. Write $z = w_0 + w_1$ with $w_0 \in W$ and $w_1 \in W$. Then $\Pi_W(z) = w_0$. We know from Corollary 10.1.12 that

$$w_0 = \sum_{i=1}^{k} (\langle w_0, x_i \rangle / \|x\|)^2 x_i.$$

But $\langle z, x_i \rangle = \langle w_0 + w_1, x_i \rangle = \langle w_0, x_i \rangle + \langle w_1, x_i \rangle = \langle w_0, x_i \rangle$, as $\langle w_1, x_i \rangle = 0$ since $w_1 \in W^{\perp}$. $\square$

Now we have often referred to orthogonal or orthonormal bases. Let us first see, as a direct consequence of our previous work, that in the finite-dimensional case they always exist.

Theorem 10.2.10. *Let W be any subspace of V. Then W has an orthonormal basis.*

Proof. Let φ be the form defined on W by $\varphi(x, y) = \langle x, y \rangle$ for every $x, y \in W$, i.e., φ is just the restriction of the dot product to W. Then φ is positive definite. (Since $\langle x, x \rangle > 0$ for every $x \neq 0$ in V, $\langle x, x \rangle > 0$ for every $x \neq 0$ in W.) Thus, by Lemma 9.3.10 and Example 9.1.12, W has a basis $\mathcal{S} = \{x_1, \dots, x_k\}$ in which $[\varphi]_{\mathcal{S}} = I$, the identity matrix. But that simply means that $\langle x_i, x_i \rangle = 1$ for each i, and $\langle x_i, x_j \rangle = 0$ for each $i \neq j$, i.e., $\mathcal{S}$ is orthonormal. $\square$

Now let us see a second, independent, proof. This proof has several advantages: it is simpler, it is more general, and it provides a concrete procedure for constructing orthonormal bases.

(In the statement of this theorem we implicitly assume, in the infinite-dimensional case, that the elements of $\mathcal{B}$ are indexed by the positive integers.)

Theorem 10.2.11. *Let W be a subspace of V of finite or countably infinite dimension, and let $\mathcal{B} = \{x_1, x_2, \dots\}$ be an arbitrary basis of W. Then there is an orthonormal basis $\mathcal{C} = \{z_1, z_2, \dots\}$ of W. This basis has the additional property that* $\mathrm{Span}(\{z_1, \dots, z_i\}) = \mathrm{Span}(\{x_1, \dots, x_i\})$ *for each i.*

Proof. We define the vectors z_i inductively as follows.

We let $y_1 = x_1$ and $z_1 = y_1/\|y_1\|$.

If $y_1, \dots, y_{i-1}$ are defined, we let

$$y_i = x_i - \sum_{k=1}^{i-1} (\langle x_i, y_k \rangle / \|y_k\|^2) y_k \quad \text{and} \quad z_i = y_i/\|y_i\|.$$

We claim that $\{y_1, y_2, \dots\}$ is orthogonal. The set $\{y_1\}$ is orthogonal—there is nothing to prove as y_1 is the only vector in this set.

Suppose that $\{y_1, \dots, y_{i-1}\}$ is orthogonal. Then for any j between 1 and $i-1$,

$$\begin{aligned}\langle y_i, y_j\rangle &= \left\langle x_i - \sum_{k=1}^{i-1}(\langle x_i, y_k\rangle/\|y_k\|^2)y_k, y_j\right\rangle \\ &= \langle x_i, y_j\rangle - \sum_{k=1}^{i-1}\langle x_i, y_k\rangle/\|y_k\|^2\langle y_k, y_j\rangle \\ &= \langle x_i, y_j\rangle - (\langle x_i, y_j\rangle/\|y_j\|^2)(\|y_j\|^2) = 0\end{aligned}$$

as $\langle y_k, y_j\rangle = 0$ for $k \neq j$ by orthogonality. Hence $\{y_1, \dots, y_i\}$ is orthogonal.

Thus by induction the set $\{y_1, \dots, y_i\}$ is orthogonal for any i, and that means, even if there are infinitely many vectors, that the set $\{y_1, y_2, \dots\}$ is orthogonal, as given any two vectors y_j and y_k in this set they lie in some finite subset, namely in $\{y_1, \dots, y_i\}$ with $i = \max(j, k)$.

Then if $\{y_1, y_2, \dots\}$ is orthogonal, $\{z_1, z_2, \dots\}$ is orthonormal, as each z_i is a multiple of y_i and $\|z_i\| = 1$ for each i.

Finally, from the construction of y_i we see that y_i is of the form $y_i = x_i + c_1y_1 + \cdots + c_{i-1}y_{i-1}$ for some scalars $c_1, \dots, c_{i-1}$ for each i, so $\operatorname{Span}(\{z_1, \dots, z_i\}) = \operatorname{Span}(\{y_1, \dots, y_i\}) = \operatorname{Span}(\{x_1, \dots, x_i\})$ for each i. □

Remark 10.2.12. The procedure in this proof is known as the *Gram-Schmidt procedure.* ◊

We can rephrase the Gram-Schmidt procedure in terms of our earlier constructions.

Corollary 10.2.13. *Let W and $\mathcal{B}$ be as in Theorem* 10.2.11*. Set $W_0 = \{0\}$ and for each $i > 0$ set $W_i = \operatorname{Span}(x_1, \dots, x_i)$. Then if $\mathcal{C}$ is as in Theorem* 10.2.11*, and N is the normalization map of Definition* 10.1.16*,*

$$z_i = N\big(\Pi_{W_{i-1}^\perp}(x_i)\big)$$

for each $i = 1, 2, \dots$.

Proof. We recognize from Theorem 10.2.11 that

$$y_i = x_i - \Pi_{W_{i-1}}(x_i) = (\mathcal{I} - \Pi_{W_{i-1}})(x_i)$$

and from Lemma 10.2.8 that $\mathcal{I} - \Pi_{W_{i-1}} = \Pi_{W_{i-1}^\perp}$. (Note that each W_{i-1} is finite dimensional so always has an orthogonal complement.) Then, recalling the definition of the normalization map N, $z_i = N(y_i)$. □

Example 10.2.14. Let $V = \mathbb{R}^3$, and let $\mathcal{B} = \left\{\begin{bmatrix}1\\2\\2\end{bmatrix}, \begin{bmatrix}2\\1\\1\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}\right\}$ be a basis of V. We use the Gram-Schmidt procedure to convert $\mathcal{B}$ to an orthonormal basis $\mathcal{C}$ of $\mathbb{R}^3$.

We begin with $x_1 = \begin{bmatrix}1\\2\\2\end{bmatrix}$. Then $y_1 = x_1 = \begin{bmatrix}1\\2\\2\end{bmatrix}$ and $z_1 = y_1/\|y_1\| = \begin{bmatrix}1/3\\2/3\\2/3\end{bmatrix}$.

Next consider $x_2 = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}$. Then $y_2 = x_2 - (\langle x_2, y_1\rangle / \|y_1\|^2)y_1$,

$$y_2 = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix} - \left(\left\langle \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} \right\rangle /9 \right) \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix} - (2/3) \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 4/3 \\ -1/3 \\ -1/3 \end{bmatrix},$$

and $z_2 = y_2/\|y_2\| = \begin{bmatrix} 4\sqrt{2}/6 \\ -\sqrt{2}/6 \\ -\sqrt{2}/6 \end{bmatrix}$.

Next consider $x_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$. Then $y_3 = x_3 - (\langle x_3, y_1\rangle / \|y_1\|^2)y_1 - (\langle x_3, y_2\rangle / \|y_2\|^2)y_2$,

$$\begin{aligned} y_3 &= \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} - \left(\left\langle \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} \right\rangle /9 \right) \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} - \left(\left\langle \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 4/3 \\ -1/3 \\ -1/3 \end{bmatrix} \right\rangle /2 \right) \begin{bmatrix} 4/3 \\ -1/3 \\ -1/3 \end{bmatrix} \\ &= \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} - (1/3) \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} - (1/2) \begin{bmatrix} 4/3 \\ -1/3 \\ -1/3 \end{bmatrix} = \begin{bmatrix} 0 \\ -1/2 \\ -1/2 \end{bmatrix}, \end{aligned}$$

and $z_3 = y_3/\|y_3\| = \begin{bmatrix} 0 \\ -\sqrt{2}/2 \\ \sqrt{2}/2 \end{bmatrix}$.

Thus $\mathcal{C} = \left\{ \begin{bmatrix} 1/3 \\ 2/3 \\ 2/3 \end{bmatrix}, \begin{bmatrix} 4\sqrt{2}/6 \\ -2\sqrt{2}/6 \\ -2\sqrt{2}/6 \end{bmatrix}, \begin{bmatrix} 0 \\ -\sqrt{2}/2 \\ \sqrt{2}/2 \end{bmatrix} \right\}$. $\Diamond$

Remark 10.2.15. It is sometimes useful to modify the Gram-Schmidt procedure by changing the normalization, so that the vectors z_i have prescribed norms, not all of which may be 1. $\Diamond$

Example 10.2.16. Let $V = \{$real polynomials $f(x)\}$ with inner product

$$\langle f(x), g(x)\rangle = \int_{-1}^{1} f(x)g(x)\,dx.$$

Let $\mathcal{B} = \{1, x, x^2, \dots\}$. We apply the Gram-Schmidt procedure to obtain an orthogonal basis $\{P_0(x), P_1(x), P_2(x), \dots\}$ for V, except we normalize so that $\langle P_n(x), P_n(x)\rangle = 2/(2n+1)$. Direct calculation shows that the first few of these polynomials are given by

$$\begin{aligned}
P_0(x) &= 1, \\
P_1(x) &= x, \\
P_2(x) &= \frac{1}{2}(3x^2 - 1), \\
P_3(x) &= \frac{1}{2}(5x^3 - x), \\
P_4(x) &= \frac{1}{8}(35x^4 - 30x^2 + 3), \\
P_5(x) &= \frac{1}{8}(63x^5 - 70x^3 + 15x).
\end{aligned}$$ ◊

Remark 10.2.17. The polynomials $P_n(x)$ are known as the *Legendre polynomials.* ◊

(In our application below we will not care about the normalizations, but this is the classical definition.)

Let us now see an application of our work to calculus. Fix an odd value of n and for convenience set $n = 2k-1$. Let $V = \mathcal{P}_n = \{$real polynomials $f(x)$ of degree at most $n\}$. We recall that V is a vector space of dimension $n+1 = 2k$. We saw earlier (Theorem 5.5.14) that given any $2k$ distinct points $x_1, \dots, x_{2k}$ in an interval $[a, b]$, there were "weights" $c_1, \dots, c_{2k}$ such that

$$\int_a^b f(x)\,dx = \sum_{i=1}^{2k} c_i f(x_i)$$

for every $f(x) \in V$.

Now suppose we allow the points to vary. If we have k points and k weights, that gives us $2k$ "degrees of freedom", and V has dimension $2k$, so we might hope that by choosing the points appropriately, we might get a similar integration formula, valid for every $f(x) \in V$. That is, we might hope that we can find the value of the integral by taking an appropriately weighted sum of the values of $f(x)$ at only k points, instead of $2k$ points.

However, if you set up the problem, you will see that it is a nonlinear problem, and so there is no guarantee that it is possible to solve it.

We will now see, introducing an inner product, not only that it is possible to solve it, but in fact how to do so—how to concretely obtain the k points and k weights.

We will start off by specializing the problem to the interval $[-1, 1]$. (Once we have solved it for that interval, it is easy to solve it in general.) We give V the inner product

$$\langle f(x), g(x) \rangle = \int_{-1}^{1} f(x)g(x)\,dx.$$

We summarize the answer to our problem in the following theorem, where we also give more precise information.

Theorem 10.2.18. *Let $P_k(x)$ denote the kth Legendre polynomial.*

(a) *$P_k(x)$ is a polynomial of degree k, for every k.*

(b) *If k is even, $P_k(x)$ is even (i.e., $P_k(-x) = P_k(x)$), and if k is odd, $P_k(x)$ is odd (i.e., $P_k(-x) = -P_k(x)$).*

(c) *$P_k(x)$ has k roots in the interval $(-1,1)$. If $k = 2j$ is even, write these roots in ascending order as*

$$r_{-j}, \ldots, r_{-1}, r_1, \ldots, r_j.$$

If $k = 2j+1$ is odd, write these roots in ascending order as

$$r_{-j}, \ldots, r_{-1}, r_0, r_1, \ldots, r_j.$$

(d) *$r_{-i} = -r_i$ for $i = 1, \ldots, j$, and $r_0 = 0$ if k is odd.*

(e) *For each i, let $q_i(x) = \prod_{m \neq i}(x - r_m)^2$. Let $c_i = (1/q_i(r_i)) \int_{-1}^{1} q_i(x)\, dx$. Then $c_i > 0$ for each i, and $c_{-i} = c_i$ for $i = 1, \ldots, j$. Also, $\sum_{i=-j}^{j} c_i = 2$.*

(f) *For any polynomial $f(x)$ of degree at most $n = 2k-1$,*

$$\int_{-1}^{1} f(x)\, dx = \sum c_i f(r_i).$$

Proof. (a) By induction on k. For $k = 0$, $P_0(x) = 1$ has degree 0. Assume $P_i(x)$ has degree i for each $i < k$. Now $P_k(x)$ is obtained from x^k by applying the Gram-Schmidt procedure, and examining that procedure we see it yields $P_k(x) = a_k x^k + a_{k-1}P_{k-1}(x) + \cdots + a_0 P_0(x)$ for some $a_k \neq 0$ and some $a_{k-1}, \ldots, a_0$, so this is a polynomial of degree k.

(b) $P_k(x)$ is orthogonal to each of $P_0(x), \ldots, P_{k-1}(x)$, so is orthogonal to the subspace W spanned by $P_0(x), \ldots, P_{k-1}(x)$. But this subspace is just $W = \mathcal{P}_{k-1}$, the space of polynomials of degree at most $k-1$. Then $V = W \perp W^\perp$ and $W^\perp$ is 1-dimensional, generated by $P_k(x)$.

Now let $f(x) \in W$. The change-of-variable $y = -x$ shows

$$\int_{-1}^{1} f(x) P_k(-x)\, dx = \int_{-1}^{1} f(-y) P_k(y)\, dy = 0$$

as if $f(x) \in W$, then $f(-y) \in W$ (as $f(-y)$ is polynomial of the same degree as $f(x)$). In other words, $P_k(-x) \in W^\perp$, and so $P_k(-x)$ is a multiple of $P_k(x)$, $P_k(-x) = aP_k(x)$ for some a. But it is easy to check that this is only possible when $a = 1$ if k is even, and when $a = -1$ if k is odd.

(c) Let $s_1, \ldots, s_i$ be the roots of $P_k(x)$ in the interval $(-1,1)$ of odd multiplicity. Then $P_k(x)$ changes sign at $s_1, \ldots, s_i$ but nowhere else in $[-1,1]$. Let $f(x) = (x - s_1)\cdots(x - s_i)$. Then $f(x)P_k(x)$ has constant sign (always nonnegative or always nonpositive) on $[-1,1]$ and is not identically zero. Hence

$$0 \neq \int_{-1}^{1} f(x) P_k(x)\, dx = \langle f(x), P_k(x) \rangle.$$

But $P_k(x)$ is orthogonal to every polynomial of degree at most $k-1$, so $f(x)$ must have degree k, so $i = k$ and $P_k(x)$ has k roots (necessarily all of multiplicity one) in $(-1,1)$.

(d) Since $P_k(x) = \pm P_k(-x)$, if $P_k(r_i) = 0$, then $P_k(-r_i) = 0$. Also, if k is odd, $P_k(0) = P_k(-0) = -P_k(0)$, so $P_k(0) = 0$.

(f) We show this is true for some constants c_i; afterwards we will evaluate the constants and show (e).

We know from Theorem 5.5.14 that there exist unique constants c_i such that

$$\int_{-1}^{1} f(x)\,dx = \sum c_i f(r_i),$$

where $f(x)$ is any polynomial of degree at most $k-1$, i.e., for any $f(x)$ in the subspace $\mathcal{P}_{k-1}$ of $V = \mathcal{P}_{2k-1}$. We want to show this equality holds on all of V. It suffices to prove it on any basis of V. We choose the basis

$$\{1, x, \ldots, x^{k-1}, P_k(x), xP_k(x), \ldots, x^{k-1}P_k(x)\}.$$

(Note this is a basis of V as these polynomials have degrees $0, 1, \ldots, 2k-1$.) Now for the first k elements of this basis, we know (writing 1 as x^0 for convenience)

$$\int_{-1}^{1} f(x)\,dx = \sum c_i f(r_i), \quad f(x) = x^t,\ t = 0, \ldots, k-1,$$

as that is how we defined the constants c_i. But for the last k elements of this basis we have, on the one hand,

$$\int_{-1}^{1} f(x)\,dx = \int_{-1}^{1} x^t P_k(x)\,dx = \langle x^t, P_k(x)\rangle = 0 \quad \text{by orthogonality},$$

and on the other hand

$$\sum c_i f(r_i) = \sum c_i 0 = 0$$

as $f(x) = x^t P_k(x)$, $t = 0, \ldots, k-1$, has $P_k(x)$ as a factor, and $P_k(r_i) = 0$ for each i as these are the roots of $P_k(x)$.

(e) Note that $q_i(x) = \prod_{m \neq i}(x - r_m)^2$ has degree $2k-2$, so is in V, and thus

$$\int_{-1}^{1} q_i(x)\,dx = \sum c_m q_i(r_m) = c_i q_i(r_i)$$

as $q_i(r_m) = 0$ for $m \neq i$, giving the value of c_i. Note that $q_i(x)$ is a square, so $q_i(r_i) > 0$ and $\int_{-1}^{1} q_i(x)\,dx > 0$. Hence $c_i > 0$.

Also note that for $i > 0$ we can write $q_i(x)$ as

$$q_i(x) = (x - r_{-i})^2 \prod_{\substack{m \geq 0 \\ m \neq i}} (x - r_m)^2 (x - r_{-m})^2$$

and from this it is easy to see that $q_{-i}(-x) = q_i(x)$ for every x (since $r_{-m} = -r_m$ for each m), so $q_{-i}(-r_i) = q_i(r_i)$, and also

$$\int_{-1}^{1} q_i(x)\,dx = \int_{-1}^{1} q_{-i}(-x)\,dx = \int_{-1}^{1} q_{-i}(y)\,dy$$

(again using the change-of-variable $y = -x$), so $c_{-i} = c_i$.

Finally, for $f(x) = 1$ we have $2 = \int_{-1}^{1} f(x)dx = \sum_i c_i f(r_i) = \sum_i c_i$. $\square$

We now give a table of the values of r_i and c_i for small values of n. In view of the theorem, we restrict ourselves to $i \geq 0$.

Remark 10.2.19. For $n = 1$: $r_0 = 0$, $c_0 = 2$.

For $n = 3$: $r_1 = \sqrt{1/3}$, $c_1 = 1$.

For $n = 5$: $r_0 = 0$, $c_0 = 8/9$; $r_1 = \sqrt{3/5}$, $c_1 = 5/9$.

For $n = 7$: $r_1 = \sqrt{(15 - 2\sqrt{30})/35}$, $c_1 = (18 + \sqrt{30})/36$;

$r_2 = \sqrt{(15 + 2\sqrt{30})/35}$, $c_2 = (18 - \sqrt{30})/36$.

For $n = 9$: $r_0 = 0$, $c_0 = 128/225$;

$r_1 = \sqrt{(35 - 2\sqrt{70})/63}$, $c_1 = (322 + 13\sqrt{70})/900$;

$r_2 = \sqrt{(35 + 2\sqrt{70})/63}$, $c_2 = (322 - 13\sqrt{70})/900$. ◊

Remark 10.2.20. Instead of the interval $[-1, 1]$, we may consider any interval $[a, b]$ by performing a linear change of variable. (To be precise, $y = (x + 1)(b - a)/2 + a$ takes $[-1, 1]$ to $[a, b]$, and $x = 2(y - a)/(b - a) - 1$ takes $[a, b]$ back to $[-1, 1]$.)

Then for the polynomials, we have that $\{P_n(2(x-a)/(b-a)-1)\}$ are orthogonal on $[a, b]$, and

$$\int_a^b P_n(2(x - a)/(b - a) - 1)^2 \, dx = (b - a)/(n + 1).$$

In particular, for the interval $[0, 1]$ we get the "shifted" Legendre polynomials

$$\{P_n^*(x) = P_n(2x - 1)\} \quad \text{with} \quad \int_0^1 P_n^*(x)^2 \, dx = 1/(n + 1).$$

For the integrals, the point r_i in $[-1, 1]$ is taken to the point $(r_i+1)(b-a)/2+a = r_i'$, and the factor c_i is taken to the factor $c_1(b - a)/2 = c_i'$; i.e.,

$$\int_a^b f(x) \, dx = \sum c_i' f(r_i')$$

for every polynomial $f(x)$ of degree at most n.

In particular, for the interval $[0, 1]$, $r_i' = (r_i + 1)/2$ and $c_i' = c_i/2$. ◊

Remark 10.2.21. This method of exactly integrating polynomials of degree at most n may also be regarded as a method of approximately integrating arbitrary functions. It is know as *Gaussian quadrature.* ◊

10.3. Two applications: symmetric and Hermitian forms, and the singular value decomposition

In this section we present two applications of our ideas. Logically speaking, this section should follow Section 10.4. Then part of what we do here would be superfluous, as it would simply be a special case of our results there, or follow from the spectral theorem, the main theorem of that section. But the considerations there are rather subtle, and the results here are important ones, so we think it is worthwhile to give relatively simple direct arguments in this case.

We will be considering matrices with $A = A^*$. This means, in the language of Section 9.5, that the linear transformation $\mathcal{T}_A$ is self-adjoint ($\mathcal{T}_A^* = \mathcal{T}_A$). But that section was also a subtle one, and in the interests of simplicity we will also avoid using anything from that section (including the language).

If A is a matrix, we let $A^* = {}^t\bar{A}$. We observe that $A = A^*$ if either A is real symmetric or complex Hermitian. Indeed, we may regard a real symmetric matrix as a complex Hermitian matrix that just happens to have real entries.

We also observe that for any matrix A, $A^{**} = A$.

We also recall our standard language: the eigenvalues/eigenvectors/generalized eigenvectors of A are those of the linear transformation $\mathcal{T}_A$.

Lemma 10.3.1. *Let A be an n-by-n matrix. Then*

$$\langle Ax, y\rangle = \langle x, A^*y\rangle \quad \text{for every } x, y \in \mathbb{C}^n.$$

In particular, if $A = A^*$, then

$$\langle Ax, y\rangle = \langle x, Ay\rangle \quad \text{for every } x, y \in \mathbb{C}^n.$$

Proof. We simply compute

$$\langle Ax, y\rangle = {}^t(Ax)\bar{y} = {}^tx\,{}^tA\bar{y} \qquad \text{and} \qquad \langle x, {}^t\bar{A}y\rangle = {}^t x(\overline{{}^t\bar{A}y}) = {}^tx\,{}^tA\bar{y},$$

and these are equal. □

Theorem 10.3.2. *Let A be an n-by-n matrix with $A = A^*$. Then:*

(1) *Every eigenvalue of A is real.*

(2) *Every generalized eigenvector of A is an eigenvector.*

(3) *Eigenvectors associated to distinct eigenvalues of A are orthogonal.*

Proof. These are all computations.

(1) Let λ be an eigenvalue of A and let x be an associated eigenvector. Then $Ax = \lambda x$, and then

$$\lambda\langle x, x\rangle = \langle \lambda x, x\rangle = \langle Ax, x\rangle = \langle x, Ax\rangle = \langle x, \lambda x\rangle = \bar{\lambda}\langle x, x\rangle$$

(where the third equality is Lemma 10.3.1), and so, since $\langle x, x\rangle \neq 0$, $\lambda = \bar{\lambda}$.

(2) Suppose $(A - \lambda I)^2 x = 0$. We show $(A - \lambda I)x = 0$. For simplicity, let $B = A - \lambda I$. Note that $B^* = {}^t(\overline{A - \lambda I}) = {}^t(\bar{A} - \bar{\lambda} I) = {}^t(\bar{A} - \lambda I)$ (as $\lambda = \bar{\lambda}$) $= {}^t\bar{A} - \lambda\,{}^tI = {}^t\bar{A} - \lambda I = A - \lambda I = B$. Then

$$0 = \langle B^2 x, x\rangle = \langle B(Bx), x\rangle = \langle Bx, Bx\rangle \quad \text{so} \quad Bx = 0$$

(where the third equality is again Lemma 10.3.1).

(3) Let λ and μ be distinct eigenvalues of A, and let x be an eigenvector associated to λ and y an eigenvector associated to μ. Then λ and μ are both real, by (1), so $\lambda = \bar{\lambda}$, $\mu = \bar{\mu}$. Then

$$\lambda\langle x, y\rangle = \langle \lambda x, y\rangle = \langle Ax, y\rangle = \langle x, Ay\rangle = \langle x, \mu y\rangle = \bar{\mu}\langle x, y\rangle = \mu\langle x, y\rangle$$

(where once again the third equality is Lemma 10.3.1), so $\langle x, y\rangle = 0$. □

Corollary 10.3.3. (a) *Let A be a real symmetric matrix. Then $\mathbb{R}^n$ has an orthonormal basis consisting of eigenvectors of A.*

(b) *Let A be a complex Hermitian matrix. Then $\mathbb{C}^n$ has an orthonormal basis consisting of eigenvectors of A.*

Proof. To begin with, regard A as a complex matrix. Then, by Theorem 10.3.2(3), we know that A is diagonalizable, so that, if $\lambda_1, \ldots, \lambda_k$ are the distinct eigenvalues of A, then $\mathbb{C}^n = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}$, where E_λ is the complex eigenspace of A corresponding to the eigenvalue λ.

By Theorem 10.3.2(1), every eigenvalue of A is a real number. If λ is an eigenvalue of A, then $E_\lambda = \operatorname{Ker}(A - \lambda I)$. But if A is real and λ is real, $A - \lambda I$ is real, so $\operatorname{Ker}(A - \lambda I)$ has a basis consisting of real vectors (think about how we found a basis for the nullspace of a matrix in Chapter 2), so in this case we see that we also have $\mathbb{R}^n = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k}$, where now E_λ is the real eigenspace of A corresponding to the eigenvalue λ.

Now, in either case, E_{λ_i} has an orthonormal basis $\mathcal{B}_i$, by Theorem 10.2.11, for each i. By Theorem 10.3.2(3), the subspaces E_{λ_i} and E_{λ_j} are orthogonal whenever $i \neq j$. Thus $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$ is an orthonormal basis for $\mathbb{R}^n$ or $\mathbb{C}^n$, as the case may be. □

Definition 10.3.4. (a) A real n-by-n matrix P is *orthogonal* if its columns form an orthonormal basis of $\mathbb{R}^n$.

(b) A complex n-by-n matrix P is *unitary* if its columns form an orthonormal basis of $\mathbb{C}^n$. ◊

Lemma 10.3.5. (a) *A real matrix P is orthogonal if and only if ${}^tP = P^{-1}$.*

(b) *A complex matrix P is unitary if and only if ${}^tP = \bar{P}^{-1}$.*

Proof. Suppose P is orthogonal/unitary. Let $P = [x_1|\cdots|x_n]$. Then the (i, j) entry of ${}^tP\bar{P}$ is $\langle x_i, x_j\rangle$. But since the columns of P are orthonormal, $\langle x_i, x_j\rangle = 1$ if $i = j$ and 0 if $i \neq j$, and so we see ${}^tP\bar{P} = I$. On the other hand, if ${}^tP\bar{P} = I$, then this computation shows that P is orthogonal/unitary. □

Corollary 10.3.6. (a) *Let A be a real symmetric n-by-n matrix. Then A is orthogonally diagonalizable, i.e., there exists an orthogonal matrix P such that $P^{-1}AP = D$, a diagonal matrix.*

(b) *Let A be a complex Hermitian n-by-n matrix. Then A is unitarily diagonalizable, i.e., there exists a unitary matrix P such that $P^{-1}AP = D$, a diagonal matrix.*

In both cases, the matrix D is real.

Proof. Since A is diagonalizable, we know that in any basis consisting of eigenvectors, $P^{-1}AP = D$ is diagonal, where P is the matrix whose columns are the eigenvectors.

But by Theorem 10.2.11, we can choose the basis to be orthonormal, and then by Definition 10.3.4, the matrix P is orthogonal (in the real case) or unitary (in the complex case). Finally, the diagonal entries of D are the eigenvalues of A, and these are all real, by Theorem 10.3.2. □

We now arrive at the application to which we have been heading.

Theorem 10.3.7. *Let A be a real symmetric or complex Hermitian n-by-n matrix, and let $\varphi = \varphi_A$ be the bilinear form on $\mathbb{R}^n$, or the sesquilinear form on $\mathbb{C}^n$, given by $\varphi(x,y) = {}^t\!xAy$ or $\varphi(x,y) = {}^t\!xA\bar{y}$, respectively. Then, in the notation of Theorem* 9.4.7*,*

$$\begin{aligned} &z \text{ is the number of zero eigenvalues of } A,\\ &p \text{ is the number of positive eigenvalues of } A,\\ &q \text{ is the number of negative eigenvalues of } A, \end{aligned}$$

counted according to multiplicity.

Proof. We do the proof in the complex case.

Thus suppose that A is complex Hermitian. By Corollary 10.3.6, there is a unitary matrix P such that $P^{-1}AP = D$ is diagonal, and then

$$\bar{P}^{-1}\bar{A}\bar{P} = (\overline{P^{-1}AP}) = \bar{D} = D.$$

Then the columns of $\bar{P}$ are eigenvectors of $\bar{A}$. Again, ordering them so that the first z_0 diagonal entries of D are zero, the next p_0 are positive, and the last q_0 are negative, and letting U_0 be the subspace of $\mathbb{C}^n$ spanned by the first z_0 columns of $\bar{P}$, U_+ be the subspace spanned by the next p_0 columns of $\bar{P}$, and U_- be the subspace spanned by the last q_0 columns of $\bar{P}$, we have $\mathbb{C}^n = U_0 \oplus U_+ \oplus U_-$ with $\dim(U_0) = z_0$, $\dim(U_+) = p_0$, $\dim(U_-) = q_0$. Note that the numbers z_0, p_0, and q_0, which a priori are the multiplicities of zero/positive/negative eigenvalues *of* $\bar{A}$, are also the multiplicities of zero/positive/negative eigenvalues *of* A, as $\bar{A}$ and A are both similar to the *same* diagonal matrix D.

However, since P is unitary, ${}^tP = \bar{P}^{-1}$. Thus ${}^tP\bar{A}\bar{P} = D$.

Let $\bar{\varphi}$ be the form on $\mathbb{C}^n$ defined by $\bar{\varphi}(x,y) = {}^t\!x\bar{A}y$. Then ${}^tP\bar{A}\bar{P} = D$ means that, letting $\mathcal{B}$ be the basis of $\mathbb{C}^n$ consisting of the columns of P (*not* of $\bar{P}$), the matrix $[\bar{\varphi}]_{\mathcal{B}}$ (*not* the matrix $[\varphi]_{\mathcal{B}}$) is just $[\bar{\varphi}]_{\mathcal{B}} = D$. Then, since eigenvectors corresponding to different eigenspaces are orthogonal, we see that $\mathbb{C}^n = V_0 \perp V_+ \perp V_-$ (*not* $U_0 \perp U_+ \perp U_-$), where V_0, V_+, V_- are the subspaces of $\mathbb{C}^n$ spanned by the first z_0, next p_0, and last q_0 columns of P, and the restrictions of $\bar{\varphi}$ (*not* φ) to V_0, V_+, V_- are identically zero, positive definite, and negative definite, respectively.

Now of course $\dim(V_0) = z_0 = \dim(U_0)$, $\dim(V_+) = p_0 = \dim(U_+)$, $\dim(U_-) = q_0 = \dim(V_-)$. But in fact, more is true. Since each of V_0, V_+, and V_- is spanned by certain columns of P, and each of U_0, U_+, and U_- is spanned by the same columns of $\bar{P}$, we have $U_0 = \bar{V}_0$, $U_+ = \bar{V}_+$, $U_- = \bar{V}_-$, and then $V_0 = \bar{U}_0$, $V_+ = \bar{U}_+$, $V_- = \bar{U}_-$ as well.

Finally, notice that for any vector x in V,

$$\bar{\varphi}(\bar{x},\bar{x}) = {}^t\bar{x}\bar{A}x = (\overline{{}^t\!xA\bar{x}}) = \overline{\varphi(x,x)} = \varphi(x,x).$$

Thus, since $\bar{\varphi}$ is identically zero, positive definite, and negative definite on V_0, V_+, V_-, respectively, then φ is identically zero, positive definite, and negative definite on U_0, U_+, U_-, respectively. Thus we see in this case as well, in the above notation

$$z \geq z_0, \quad p \geq p_0, \quad \text{and} \quad q \geq q_0.$$

We claim all these inequalities are in fact equalities.

Suppose $\mathbb{C}^n$ had a subspace W_+ of dimension $p > p_0$ with φ restricted to W_+ positive definite.

Since $z_0 + p_0 + q_0 = n$, $p + (z_0 + q_0) > n$, so $W_+ \cap (V_0 \oplus V_-)$ would have positive dimension. Let w be a nonzero vector in W_+ and write $w = v_0 + v_-$ with v_0 in V_0 and v_- in V_-. Then on the one hand $\varphi(w, w) > 0$, as w is in W_+, and on the other hand, remembering that in fact V_0 and V_- are orthogonal, $\varphi(w, w) = \varphi(v_0 + v_-, v_0 + v_-) = \varphi(v_0, v_0) + \varphi(v_-, v_-) \leq 0$, a contradiction. Hence $p = p_0$. By the same argument, $q = q_0$. But $z + p + q = n$ as well, so $z = z_0$. □

We have gone through this argument very carefully, step-by-step, as it is rather tricky. But let us emphasize part of our conclusion. To do so, it is convenient to introduce some nonstandard language.

Definition 10.3.8. Let A be a real symmetric or complex Hermitian matrix. The *zero space* of A is the zero eigenspace of A, the *positive space* of A is the direct sum of the eigenspaces corresponding to positive eigenvalues of A, and the *negative space* of A is the direct sum of the eigenspaces corresponding to negative eigenvalues of A. ♢

Corollary 10.3.9. (a) *Let A be a real symmetric matrix. Then the restriction of φ_A to the zero/positive/negative spaces of A is identically zero/positive definite/negative definite.*

(b) *Let A be a complex Hermitian matrix. Then the restriction of φ_A to the zero/positive/negative spaces of $\bar{A}$ is identically zero/positive definite/negative definite.*

Proof. This is precisely what we showed in the course of the proof of Theorem 10.3.7. □

Example 10.3.10. (a) Let $A = \begin{bmatrix} 73 & -36 \\ -36 & 52 \end{bmatrix}$. We compute that A has eigenvalues $\lambda = 25$ and $\lambda = 100$. For $\lambda = 25$ we find an eigenvector $w_1 = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$ which we normalize to $x_1 = \begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix}$.

For $\lambda = 100$ we find an eigenvector $w_2 = \begin{bmatrix} -4 \\ 3 \end{bmatrix}$ which we normalize to $x_2 = \begin{bmatrix} -4/5 \\ 3/5 \end{bmatrix}$.

Hence we see that $P^{-1}AP = D$, where

$$D = \begin{bmatrix} 25 & 0 \\ 0 & 100 \end{bmatrix} \quad \text{is diagonal, and}$$

$$P = \begin{bmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{bmatrix} \quad \text{is orthogonal.}$$

(b) Let $A = \begin{bmatrix} 9 & 12 \\ 12 & 16 \end{bmatrix}$. We compute that A has eigenvalues $\lambda = 25$ and $\lambda = 0$. For $\lambda = 25$ we obtain the same normalized eigenvector x_1, and for $\lambda = 0$ we obtain the same normalized eigenvector x_2.

Hence we see that $P^{-1}AP = D$, where

$$D = \begin{bmatrix} 25 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{is diagonal, and}$$
$$P \text{ is the same matrix as in (a).}$$

(c) Let $A = \begin{bmatrix} -7 & 24 \\ 24 & 7 \end{bmatrix}$. We compute that A has eigenvalues $\lambda = 25$ and $\lambda = -25$. For $\lambda = 25$ we obtain the same normalized eigenvector x_1, and for $\lambda = -25$ we obtain the same normalized eigenvector x_2.

Hence we see that $P^{-1}AP = D$, where

$$D = \begin{bmatrix} 25 & 0 \\ 0 & -25 \end{bmatrix} \quad \text{is diagonal, and}$$
$$P \text{ is the same matrix as in (a).}$$ ◊

We already saw in Section 9.6 that we could diagonalize quadratic forms. We can now do this in a more precise way. (Note here we are using x_i's and y_i's to denote variables, not vectors.)

Corollary 10.3.11. *Let Φ be a quadratic form in the variables $x_1, \ldots, x_n$. Then there is an orthogonal (in the real case) or unitary (in the complex case) change of variables*

$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = Q \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

and unique real numbers $d_1, \ldots, d_n$ such that

$$\Phi(y_1, \ldots, y_n) = \sum_{i=1}^{n} d_i y_i^2.$$

Proof. Let A be the matrix of Φ, so that

$$\Phi(x, x) = {}^t x A \bar{x}.$$

As we have just seen, $A = PDP^{-1}$ with P orthogonal/unitary, so

$$\begin{aligned} \Phi(x, x) &= {}^t x (PDP^{-1}) \bar{x} \\ &= ({}^t x P) D (P^{-1} \bar{x}). \end{aligned}$$

Set $Q = \bar{P}^{-1}$ and $y = Qx$. Since P is orthogonal/unitary, so is Q, and then $\Phi(y, y) = {}^t y D \bar{y}$. □

Example 10.3.12. We refer to Example 10.3.10.

(a) Let $\Phi(x_1, x_2) = 73x_1^2 - 72x_1x_2 + 52x_2^2$. Then Φ has matrix $A = \begin{bmatrix} 73 & -36 \\ -36 & 52 \end{bmatrix}$, so we see that, setting $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 3/5 & 4/5 \\ -4/5 & 3/5 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} (3/5)x_1 + (4/5)x_2 \\ (-4/5)x_1 + (3/5)x_2 \end{bmatrix}$,

$$\Phi(y_1, y_2) = 25y_1^2 + 100y_2^2, \quad \text{or, in terms of our original variables,}$$

$$\Phi(x_1, x_2) = 25\left(\frac{3}{5}x_1 + \frac{4}{5}x_2\right)^2 + 100\left(-\frac{4}{5}x_1 + \frac{3}{5}x_2\right)^2.$$

(b) Let $\Phi(x_1, x_2) = 9x_1^2 + 24x_1x_2 + 16x_2^2$. Then Φ has matrix $A = \begin{bmatrix} 9 & 12 \\ 12 & 16 \end{bmatrix}$, so with the same change of variables, $\Phi(y_1, y_2) = 25y_1^2$, i.e.,

$$\Phi(x_1, x_2) = 25\left(\frac{3}{5}x_1 + \frac{4}{5}x_2\right)^2.$$

(c) Let $\Phi(x_1, x_2) = -7x_1^2 + 48x_1x_2 + 7x_2^2$. Then Φ has matrix $A = \begin{bmatrix} -7 & 24 \\ 24 & 7 \end{bmatrix}$, so with the same change of variables, $\Phi(y_1, y_2) = 25y_1^2 - 25y_2^2$, i.e.,

$$\Phi(x_1, x_2) = 25\left(\frac{3}{5}x_1 + \frac{4}{5}x_2\right)^2 - 25\left(-\frac{4}{5}x_1 + \frac{3}{5}x_2\right)^2. \qquad \Diamond$$

We now turn to a completely different application.

Lemma 10.3.13. *Let A be an arbitrary (not necessarily square) matrix. Let B be the matrix $B = A^*A$. Then $B = B^*$. Also,* $\operatorname{Ker}(B) = \operatorname{Ker}(A)$.

Proof. First we compute $B^* = (A^*A)^* = A^*A^{**} = A^*A = B$. Next, if $Ax = 0$, then certainly $Bx = A^*Ax = A^*(Ax) = A^*(0) = 0$. On the other hand, if $Bx = 0$, then, using Lemma 10.3.1,

$$0 = \langle x, Bx\rangle = \langle x, A^*Ax\rangle = \langle Ax, Ax\rangle$$

so $Ax = 0$. $\square$

Now suppose B is any matrix with $B = B^*$. We can ask when there is a matrix A with $B = A^*A$. The answer is simple.

Lemma 10.3.14. *Let B be a matrix (resp., an invertible matrix) with $B = B^*$. Then there is a matrix A, with $B = A^*A$, if and only if B is positive semidefinite (resp., positive definite). If so, then there is such a matrix A with $A = A^*$.*

Proof. Suppose that $B = A^*A$. Since $B = B^*$, we know that B will be positive semidefinite if and only if all of its eigenvalues are nonnegative. Thus, let λ be any eigenvalue of B, and let x be an associated eigenvector. Then

$$\lambda\langle x, x\rangle = \langle \lambda x, x\rangle = \langle Bx, x\rangle = \langle A^*Ax, x\rangle = \langle Ax, A^{**}x\rangle = \langle Ax, Ax\rangle \geq 0$$

so $\lambda \geq 0$.

On the other hand, suppose that B is positive semidefinite. We know that $B = {}^t\!PD\bar{P}$ for some unitary matrix P and some diagonal matrix D, and furthermore that D has nonnegative diagonal entries.

Let E be the diagonal matrix whose entries are the square roots of the entries of D. Then

$$\begin{aligned} B &= {}^t\!PD\bar{P} \\ &= (\bar{P})^{-1}D\bar{P} \\ &= (\bar{P})^{-1}E^2\bar{P} \\ &= ((\bar{P})^{-1}E\bar{P})((\bar{P})^{-1}E\bar{P}) \\ &= ({}^t\!PE\bar{P})({}^t\!PE\bar{P}) \\ &= A^*A \end{aligned}$$

with $A = {}^t\!PE\bar{P} = A^*$.

Finally, we know that a positive semidefinite matrix is positive definite if and only if it is invertible. □

We may now make the following definition.

Definition 10.3.15. Let $\mathcal{T}: V \to W$ be a linear transformation with $\dim V = n$, $\dim W = m$, and $\dim \operatorname{Im}(\mathcal{T}) = r$. Let A be the matrix of $\mathcal{T}$ with respect to any pair of bases of V and W. Let $\lambda_1, \ldots, \lambda_r$ be the (not necessarily distinct) nonzero eigenvalues of $B = A^*A$, all of which are necessarily positive real numbers. (There are exactly r of these since $\dim \operatorname{Ker}(\mathcal{T}^*\mathcal{T}) = \dim \operatorname{Ker}(\mathcal{T})$, and hence $\dim \operatorname{Im}(\mathcal{T}^*\mathcal{T}) = \dim \operatorname{Im}(\mathcal{T})$.) Order them so that $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r$. Then $\sigma_1 = \sqrt{\lambda_1}, \ldots, \sigma_r = \sqrt{\lambda_r}$ are the *singular values* of $\mathcal{T}$. ◊

We then have the following theorem, known as the *singular value decomposition* of $\mathcal{T}$. In case $\mathcal{T} = \mathcal{T}_A$, we simply call this the singular value decomposition of A.

Theorem 10.3.16 (Singular value decomposition)**.** *Let $\mathcal{T}: V \to W$ be as in Definition* 10.3.15*. Then there are orthonormal bases $\mathcal{B} = \{x_1, \ldots, x_n\}$ of V and $\mathcal{C} = \{y_1, \ldots, y_m\}$ of W such that*

$$\mathcal{T}(x_i) = \sigma_i y_i, \quad i = 1, \ldots, r, \quad \textit{and} \quad \mathcal{T}(x_i) = 0 \quad \textit{for } i > r.$$

Proof. Since $\mathcal{T}^*\mathcal{T}$ is self-adjoint, we know that there is an orthonormal basis $\mathcal{B} = \{x_1, \ldots, x_n\}$ of V consisting of eigenvectors of $\mathcal{T}^*\mathcal{T}$, with

$$\mathcal{T}^*\mathcal{T}(x_i) = \lambda_i x_i \text{ for } i = 1, \ldots, r, \text{ and } \mathcal{T}^*\mathcal{T}(x_i) = 0 \text{ for } i > r.$$

Set

$$y_i = (1/\sigma_i)\mathcal{T}(x_i) \quad \text{for } i = 1, \ldots, r.$$

We compute

$$\begin{aligned} \langle y_i, y_i \rangle &= \langle (1/\sigma_i)\mathcal{T}(x_i), (1/\sigma_i)\mathcal{T}(x_i) \rangle \\ &= (1/\lambda_i)\langle \mathcal{T}(x_i), \mathcal{T}(x_i) \rangle = (1/\lambda_i)\langle x_i, \mathcal{T}^*\mathcal{T}(x_i) \rangle \\ &= (1/\lambda_i)\langle x_i, \lambda_i x_i \rangle = \langle x_i, x_i \rangle = 1 \end{aligned}$$

and for $i \neq j$

$$\begin{aligned}\langle y_i, y_j\rangle &= \langle (1/\sigma_i)\mathcal{T}(x_i), (1/\sigma_j)\mathcal{T}(x_j)\rangle \\ &= (1/(\sigma_i\sigma_j))\langle \mathcal{T}(x_i), \mathcal{T}(x_j)\rangle = (1/(\sigma_i\sigma_j))\langle x_i, \mathcal{T}^*\mathcal{T}(x_j)\rangle \\ &= (1/(\sigma_i\sigma_j))\langle x_i, \lambda_j x_j\rangle = (\lambda_j/(\sigma_i\sigma_j))\langle x_i, x_j\rangle = 0.\end{aligned}$$

Then extend $\{y_1, \ldots, y_n\}$ to an orthonormal basis of W. □

Example 10.3.17. (a) Let $A = \begin{bmatrix} 8 & -6 \\ 3 & 4 \end{bmatrix}$. We wish to find the singular value decomposition of A. We begin by computing

$$B = A^*A = \begin{bmatrix} 8 & 3 \\ -6 & 4 \end{bmatrix}\begin{bmatrix} 8 & -6 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 73 & -36 \\ -36 & 52 \end{bmatrix}.$$

This matrix B is the same matrix as in Example 10.3.10(a), so we may reuse our computations there. We found the eigenvalues of B there, which we rearrange in descending order as $\lambda_1 = 100$, $\lambda_2 = 25$. Thus we see that A has singular values $\sigma_1 = 10$ and $\sigma_2 = 5$. The basis $\mathcal{B}$ of $\mathbb{R}^2$ is then the orthonormal basis of eigenvectors

$$\mathcal{B} = \left\{ \begin{bmatrix} -4/5 \\ 3/5 \end{bmatrix}, \begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix} \right\}.$$

We compute

$$(1/10)\begin{bmatrix} 8 & -6 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} -4/5 \\ 3/5 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \end{bmatrix}, \quad (1/5)\begin{bmatrix} 8 & -6 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

so $\mathcal{C}$ is the orthonormal basis of $\mathbb{R}^2$,

$$\mathcal{C} = \left\{ \begin{bmatrix} -1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\} \quad \text{and then, of course,}$$

$$\begin{bmatrix} 8 & -6 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} -4/5 \\ 3/5 \end{bmatrix} = 10\begin{bmatrix} -1 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 8 & -6 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix} = 5\begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

(b) Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$. We wish to find the singular value decomposition of A. We begin by computing

$$B = A^*A = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 5 \end{bmatrix}.$$

We compute $\lambda_1 = 3 + \sqrt{5}$ and $\lambda_2 = 3 - \sqrt{5}$, so A has singular values $\sigma_1 = \sqrt{3+\sqrt{5}}$ and $\sigma_2 = \sqrt{3-\sqrt{5}}$. For λ_1 we find an eigenvector $w_1 = \begin{bmatrix} -(2-\sqrt{5}) \\ 1 \end{bmatrix}$ which we normalize to

$$x_1 = \begin{bmatrix} -(2-\sqrt{5})\sqrt{\frac{1}{10-4\sqrt{5}}} \\ \sqrt{\frac{1}{10-4\sqrt{5}}} \end{bmatrix}$$

and for λ_2 we find an eigenvector $w_2 = \begin{bmatrix} -(2+\sqrt{5}) \\ 1 \end{bmatrix}$ which we normalize to

$$x_2 = \begin{bmatrix} -(2+\sqrt{5})\sqrt{\frac{1}{10+4\sqrt{5}}} \\ \sqrt{\frac{1}{10+4\sqrt{5}}} \end{bmatrix}.$$

Then $Ax_1 = \sigma_1 y_1$ and $Ax_2 = \sigma_2 y_2$, where

$$y_1 = (1/\sqrt{3+\sqrt{5}}) \begin{bmatrix} (-1+\sqrt{5})\sqrt{\frac{1}{10-4\sqrt{5}}} \\ 2\sqrt{\frac{1}{10-4\sqrt{5}}} \end{bmatrix},$$

$$y_2 = (1/\sqrt{3-\sqrt{5}}) \begin{bmatrix} (-1-\sqrt{5})\sqrt{\frac{1}{10+4\sqrt{5}}} \\ 2\sqrt{\frac{1}{10+4\sqrt{5}}} \end{bmatrix}. \qquad \Diamond$$

Example 10.3.18. (a) We already saw in Example 10.3.17(a) that

$$\begin{aligned} \Phi(x_1, x_2) &= 73x_1^2 - 72x_1x_2 + 52x_2^2 \\ &= 25\left(\frac{3}{5}x_1 + \frac{4}{5}x_2\right)^2 + 100\left(-\frac{4}{5}x_1 + \frac{3}{5}x_2\right)^2. \end{aligned}$$

(b) We observe that $\begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = x_1^2 + 2x_1x_2 + 5x_2^2$ so our computations in Example 10.3.17(b) show that

$$\begin{aligned} \Phi(x_1, x_2) &= x_1^2 + 2x_1x_2 + 5x_2^2 \\ &= (3+\sqrt{5})\left[-(2-\sqrt{5})\sqrt{\frac{1}{10-4\sqrt{5}}}\,x_1 + \sqrt{\frac{1}{10-4\sqrt{5}}}\,x_2\right]^2 \\ &+ (3-\sqrt{5})\left[-(2+\sqrt{5})\sqrt{\frac{1}{10+4\sqrt{5}}}\,x_1 + \sqrt{\frac{1}{10+4\sqrt{5}}}\,x_2\right]^2. \end{aligned} \qquad \Diamond$$

Remark 10.3.19. We want to emphasize that the singular values of A are the square roots of the eigenvalues of $B = A^*A$, *not* the eigenvalues of A itself. For example, in Example 10.3.17(a) we found that A had singular values 10 and 5, whereas the eigenvalues of A are, as you may easily compute, $6 \pm i\sqrt{14}$, so that A does not even have any real eigenvalues. Furthermore, in Example 10.3.17(b) we found that A had singular values $\sqrt{3+\sqrt{5}}$ and $\sqrt{3-\sqrt{5}}$ while A itself also has real eigenvalues, but they are 2 and 1. $\Diamond$

Now that we have found the singular value decomposition of a linear transformation $\mathcal{T}$, or a matrix A, you might well ask what does it mean and why do we care? In turns out that it has a very simple and important geometric meaning.

Let us leave linear algebra aside for the moment and do some geometry. For simplicity we will stick to the real case.

Recall that, for any $a > 0$ and $b > 0$,

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} \leq 1$$

is the equation of an elliptical disk in the plane. (We allow $a = b$, in which case this is an ordinary (circular) disk.) This elliptical disk has two principal axes, the x-axis and the y-axis, and its "semilengths" along these axes, which are perpendicular to each other, are a and b, respectively. (In case $a = b$ we could take the principal axes to be any two perpendicular directions, and then both "semilengths" would be the radius of the disk.)

Similarly, for $a > 0$, $b > 0$, $c > 0$,

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} \leq 1$$

is the equation for an ellipsoidal ball in $\mathbb{R}^3$. Assuming for simplicity that a, b, and c are all distinct, we have three principal axes, the x-axis, the y-axis, and the z-axis, and its semilengths along these axes, which again are all mutually perpendicular, are a, b, and c.

We could also consider

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} \leq 1, \quad z = 0$$

which defines an elliptical disk in $\mathbb{R}^3$, where we again have principal axes the x-axis and the y-axis, but now we have semilengths a and b along the x-axis and the y-axis, and this elliptical disk lies in the plane in $\mathbb{R}^3$ perpendicular to the z-axis.

Let us rewrite this equation for an ellipsoidal ball in $\mathbb{R}^3$ in a way that is more complicated but leads directly to a generalization. If e_1, e_2, and e_3 are the standard unit vectors, the equation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} \leq 1$$

becomes

$$\frac{1}{a^2}\langle xe_1, xe_1\rangle + \frac{1}{b^2}\langle ye_2, ye_2\rangle + \frac{1}{c^2}\langle ze_3, ze_3\rangle \leq 1.$$

From this point of view we can see there is nothing magical about e_1, e_2, e_3. They just happen to form an orthonormal basis of $\mathbb{R}^3$. We are thus led to the following definition.

Definition 10.3.20. Let $\{w_1, \ldots, w_m\}$ be an orthonormal basis for $\mathbb{R}^m$. Let $a_1, \ldots, a_r$ be positive real numbers. Then

$$\frac{1}{a_1^2}\langle t_1 w_1, t_1 w_1\rangle + \cdots + \frac{1}{a_r^2}\langle t_r w_r, t_r w_r\rangle = 1,$$
$$\langle t_{r+1} w_{r+1}, t_{r+1} w_{r+1}\rangle = \cdots = \langle t_m w_m, t_m w_m\rangle = 0$$

is an r-dimensional ellipsoidal ball in $\mathbb{R}^m$ with principal axes $w_1, \ldots, w_r$ and semilengths $a_1, \ldots, a_r$ along these axes. $\lozenge$

Theorem 10.3.21. *Let $\mathcal{T}$ be a linear transformation between real vector spaces as in Theorem* 10.3.16 (*the singular value decomposition*). *Then the image of the unit ball in $\mathbb{R}^n$ is an r-dimensional ellipsoidal ball as in Definition* 10.3.20.

Proof. From Theorem 10.3.16, we see that $\mathbb{R}^n$ has an orthogonal basis $\mathcal{B} = \{x_1, \ldots, x_n\}$, and so the unit ball in $\mathbb{R}^n$ is just given by

$$t_1^2 + \cdots + t_n^2 = \langle t_1 x_1, t_1 x_1\rangle + \cdots + \langle t_n x_n, t_n x_n\rangle \leq 1,$$

and $\mathbb{R}^m$ has an orthogonal basis $\mathcal{C} = \{y_1, \ldots, y_m\}$ with $\mathcal{T}(x_i) = \sigma_i y_i$, $i = 1, \ldots, r$, and $\mathcal{T}(x_i) = 0$, $i = r+1, \ldots, n$, so the image of this unit ball is just

$$\mathcal{T}\left(\begin{bmatrix} t_1 x_1 \\ \vdots \\ t_n x_n \end{bmatrix}\right) = \begin{bmatrix} t_1 \sigma_1 y_1 \\ \vdots \\ t_r \sigma_r y_r \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

and so we see

$$\frac{1}{\sigma_1^2}\langle t_1 y_1, t_1 y_1 \rangle + \cdots + \frac{1}{\sigma_r^2}\langle t_r y_r, t_r y_r \rangle \le 1,$$
$$\langle t_{r+1} y_{r+1}, t_{r+1} y_{r+1} \rangle = \cdots = \langle t_m y_m, t_m y_m \rangle = 0$$

as claimed. □

Remark 10.3.22. The way the singular value decomposition is often viewed is as follows. Suppose $\mathcal{T}$ has singular values $\sigma_1, \ldots, \sigma_r$ and suppose the last $r-s$ of these are "small", i.e.,

$$\varepsilon > \sigma_{s+1} > \cdots > \sigma_r$$

for some ε. Then the image of the unit ball under $\mathcal{T}$ is

$$\begin{aligned} &\frac{1}{\sigma_1^2}\langle t_1 y_1, t_1 y_1 \rangle + \cdots + \frac{1}{\sigma_s^2}\langle t_s y_s, t_s y_s \rangle \\ &\qquad + \frac{1}{\sigma_{s+1}^2}\langle t_{s+1} y_{s+1}, t_{s+1} y_{s+1} \rangle + \cdots + \frac{1}{\sigma_r^2}\langle t_r y_r, t_r y_r \rangle \le 1, \\ &\qquad\qquad \langle t_i y_i, t_i y_i \rangle = 0 \quad \text{for } i > r. \end{aligned}$$

But notice that $\frac{1}{\sigma_i^2} > \frac{1}{\varepsilon^2}$ for $i = s+1, \ldots, r$, so this forces $|t_{s+1}| < \varepsilon, \ldots, |t_r| < \varepsilon$, and of course $t_{r+1} = \cdots = t_m = 0$.

So this is saying that this r-dimensional ellipsoidal ball lies very close to the s-dimensional ellipsoidal ball defined by

$$\frac{1}{\sigma_1^2}\langle t_1 y_1, t_1 y_1 \rangle + \cdots + \frac{1}{\sigma_s^2}\langle t_s y_s, t_s y_s \rangle \le 1,$$
$$\langle t_i y_i, t_i y_i \rangle = 0 \quad \text{for } i > s.$$

◊

10.4. Adjoints, normal linear transformations, and the spectral theorem

We continue to suppose that V is an inner product space. We will now consider properties of adjoints. Recall that if V_1 and V_2 are finite dimensional, then any linear transformation $\mathcal{T}\colon V_1 \to V_2$ has an adjoint $\mathcal{T}^*$, but otherwise $\mathcal{T}\colon V_1 \to V_2$ may not (Lemma 9.5.3).

Recall also that if $\mathcal{T}$ has an adjoint $\mathcal{T}^*$, then $\mathcal{T}^*$ has an adjoint $\mathcal{T}^{**}$, and furthermore $\mathcal{T}^{**} = \mathcal{T}$ (Lemma 9.5.14(6)).

Recall also that in the finite-dimensional case, $\dim \operatorname{Im}(\mathcal{T}) = \dim \operatorname{Im}(\mathcal{T}^*)$, and if in this case $\dim V_1 = \dim V_2$, then $\dim \operatorname{Ker}(\mathcal{T}) = \dim \operatorname{Ker}(\mathcal{T}^*)$ as well (Theorem 9.5.16 and Corollary 9.5.17).

After considering adjoints in general we will define and study "normal" linear transformations $\mathcal{T}\colon V \to V$. In case $\dim V$ is finite, our study will culminate in the spectral theorem.

Lemma 10.4.1. *Let $\mathcal{T}\colon V_1 \to V_2$ be a linear transformation and suppose that $\mathcal{T}$ has an adjoint $\mathcal{T}^*$. Then:*

(1) $\operatorname{Ker}(\mathcal{T}^*) = \operatorname{Im}(\mathcal{T})^\perp$ *and* $\operatorname{Ker}(\mathcal{T}) = \operatorname{Im}(\mathcal{T}^*)^\perp$.

(2) *If V_1 and V_2 are finite dimensional,*

$$\operatorname{Im}(\mathcal{T}) = \operatorname{Ker}(\mathcal{T}^*)^\perp \quad \textit{and} \quad \operatorname{Im}(\mathcal{T}^*) = \operatorname{Ker}(\mathcal{T})^\perp.$$

Proof. (1) We show $\operatorname{Ker}(\mathcal{T}^*) \subseteq \operatorname{Im}(\mathcal{T})^\perp$ and $\operatorname{Im}(\mathcal{T})^\perp \subseteq \operatorname{Ker}(\mathcal{T}^*)$. Suppose $y \in \operatorname{Ker}(\mathcal{T}^*)$. Then $\mathcal{T}^*(y) = 0$. Thus for every $x \in V$,

$$0 = \langle x, 0\rangle = \langle x, \mathcal{T}^*(y)\rangle = \langle \mathcal{T}(x), y\rangle$$

so $y \in \operatorname{Im}(\mathcal{T})^\perp$.

Suppose $y \in \operatorname{Im}(\mathcal{T})^\perp$. Then $\langle x, y\rangle = 0$ for every $x \in \operatorname{Im}(\mathcal{T})$. In particular, we may choose $x = \mathcal{T}(\mathcal{T}^*(y))$. Then

$$0 = \langle \mathcal{T}(\mathcal{T}^*(y)), y\rangle = \langle \mathcal{T}^*(y), \mathcal{T}^*(y)\rangle$$

so $\mathcal{T}^*(y) = 0$, i.e., $y \in \operatorname{Ker}(\mathcal{T}^*)$.

Applying the same argument to $\mathcal{T}^*$, we obtain $\operatorname{Ker}(\mathcal{T}^{**}) = \operatorname{Im}(\mathcal{T}^*)^\perp$. But $\mathcal{T}^{**} = \mathcal{T}$.

(2) This follows directly from (1). We know that if V is finite dimensional and W is any subspace of V, then $(W^\perp)^\perp = W$ (Lemma 10.2.4(b)). Thus

$$\operatorname{Ker}(\mathcal{T}^*)^\perp = (\operatorname{Im}(\mathcal{T})^\perp)^\perp = \operatorname{Im}(\mathcal{T})$$

and

$$\operatorname{Ker}(\mathcal{T})^\perp = (\operatorname{Im}(\mathcal{T}^*)^\perp)^\perp = \operatorname{Im}(\mathcal{T}^*). \qquad \square$$

Henceforth we will be considering the situation $\mathcal{T}\colon V \to V$, a linear transformation from the vector space V to itself. In this situation $\mathcal{T}$ is sometimes called a *linear operator* on V.

Before proceeding further, there are some subtleties we have to deal with.

Let V be finite dimensional, and let $\mathcal{T}\colon V \to V$ be a linear transformation.

First suppose that V is a complex vector space. We will say that $\mathcal{T}$ is *real* if there is some orthonormal basis $\mathcal{B}$ of V in which $A = [\mathcal{T}]_\mathcal{B}$ is a matrix with real entries.

Next suppose that V is a real vector space. Then of course $A = [\mathcal{T}]_\mathcal{B}$ has real entries for every basis $\mathcal{B}$ of V, and we will say that $\mathcal{T}$ is real in this case as well. But we may regard A as a complex matrix whose entries just happen to be real numbers, and so we may speak of the complex eigenvalues (and eigenvectors) of A and the Jordan canonical form of A, and consider those as eigenvalues and the Jordan canonical form of $\mathcal{T}$.

As an example, let us consider $\mathcal{T} = \mathcal{T}_{A_1}\colon \mathbb{R}^2 \to \mathbb{R}^2$, where $A_1 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$. Calculation shows that $\mathcal{T}$ has characteristic polynomial $p_\mathcal{T}(x) = x^2 - 3x + 1$ with roots the real numbers $(3 \pm \sqrt{5})/2$, so $\mathcal{T}$ has two real eigenvalues. Thus all the eigenvalues of $\mathcal{T}$ are real. In this case there is no problem. On the other hand, consider $\mathcal{T} = \mathcal{T}_{A_2} \colon \mathbb{R}^2 \to \mathbb{R}^2$, where $A_2 = \begin{bmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{bmatrix}$. Calculation shows that $\mathcal{T}$ has characteristic polynomial $p_{\mathcal{T}}(x) = x^2 - x + 1$ which has no real roots. Now since $\mathbb{R}^2$ is a *real* vector space, this means that $\mathcal{T}$ has no eigenvalues. Then, logically speaking, in this case all the eigenvalues of $\mathcal{T}$ are real as well. However, we could regard the matrix A_2 as a complex matrix defining the linear transformation $\mathcal{T} = \mathcal{T}_{A_2} \colon \mathbb{C}^2 \to \mathbb{C}^2$ and then $\mathcal{T}$ would have the same characteristic polynomial with complex roots $1/2 \pm i(\sqrt{3}/2)$, so not all of its eigenvalues are real.

We will say that in the case of A_1, all of its complex eigenvalues are real, while in the case of A_2, not all of its complex eigenvalues are real.

With these conventions and language in mind, we can now proceed.

Theorem 10.4.2. *Let V be finite dimensional, and let $\mathcal{T} \colon V \to V$ be a linear transformation.*

(a) *If λ is an eigenvalue of $\mathcal{T}$, then $\bar{\lambda}$ is an eigenvalue of $\mathcal{T}^*$. Furthermore, the algebraic/geometric multiplicity of λ as an eigenvalue of $\mathcal{T}$ is the same as the algebraic/geometric multiplicity of $\bar{\lambda}$ as an eigenvalue of $\mathcal{T}^*$. Also, the characteristic and minimal polynomials of $\mathcal{T}$ and $\mathcal{T}^*$ are related by*

$$c_{\mathcal{T}^*}(x) = \overline{c_{\mathcal{T}}(x)} \quad \textit{and} \quad m_{\mathcal{T}^*}(x) = \overline{m_{\mathcal{T}}(x)}.$$

If J is the Jordan canonical form of $\mathcal{T}$, then $\bar{J}$ is the Jordan canonical form of $\mathcal{T}^*$.

(b) *If $\mathcal{T}$ is real, then $c_{\mathcal{T}^*}(x) = c_{\mathcal{T}}(x)$ and $m_{\mathcal{T}^*}(x) = m_{\mathcal{T}}(x)$. Furthermore, $\mathcal{T}$ and $\mathcal{T}^*$ have the same Jordan canonical form.*

Proof. As a special case of Lemma 9.5.14(5), for any complex number λ, $(\mathcal{T} - \lambda\mathcal{I})^* = \mathcal{T}^* - \bar{\lambda}\mathcal{I}$, and also $((\mathcal{T} - \lambda\mathcal{I})^k)^* = (\mathcal{T}^* - \bar{\lambda}\mathcal{I})^k$ for any positive integer k. Then λ is an eigenvalue of $\mathcal{T}$ if and only if $\dim \operatorname{Ker}(\mathcal{T} - \lambda\mathcal{I}) \neq 0$, which by Corollary 9.5.17 is equivalent to $\dim \operatorname{Ker}((\mathcal{T} - \lambda\mathcal{I})^*) = \dim \operatorname{Ker}(\mathcal{T}^* - \bar{\lambda}\mathcal{I}) \neq 0$, which is true if and only if $\bar{\lambda}$ is an eigenvalue of $\mathcal{T}^*$. Furthermore, by the same logic, $\dim \operatorname{Ker}((\mathcal{T} - \lambda\mathcal{I})^k) = \dim \operatorname{Ker}((\mathcal{T}^* - \bar{\lambda}\mathcal{I})^k)$ for every λ and every k, and this sequence of dimensions determines the geometric multiplicity, the algebraic multiplicity, the ESP of $\mathcal{T}$ at λ and the ESP of $\mathcal{T}^*$ at $\bar{\lambda}$, and the JCF of $\mathcal{T}$ and the JCF of $\mathcal{T}^*$.

As for (b), recall we can use any matrix of $\mathcal{T}$ to determine all of these items, so we choose an orthonormal basis $\mathcal{B}$ of V and let $A = [\mathcal{T}]_{\mathcal{B}}$.

Since $\mathcal{B}$ is orthonormal, we know that $[\mathcal{T}^*]_{\mathcal{B}} = {}^t\!A$ by Lemma 9.5.5. Now the first claim in (b) is easy to see. $c_{\mathcal{T}}(x) = \det(xI - A)$ and $c_{\mathcal{T}^*}(x) = \det(xI - {}^t\!A) = \det({}^t(xI - A))$ and these are equal. Also, for any polynomial $p(x)$, $p({}^t\!A) = p(A)$, so $p(A) = 0$ if and only if $p({}^t\!A) = 0$. But $m_{\mathcal{T}}(x) = m_A(x)$ (resp., $m_{\mathcal{T}^*}(x) = m_{{}^t\!A}(x)$) is the *unique* monic polynomial of lowest degree with $m_A(A) = 0$ (resp., $m_{{}^t\!A}({}^t\!A) = 0$) so we must have $m_{\mathcal{T}}(x) = m_{\mathcal{T}^*}(x)$.

Now we also know that if A is a matrix with real entries and λ is any complex number, $\dim \operatorname{Ker}(A - \lambda I)^k = \dim \operatorname{Ker}(A - \bar{\lambda} I)^k$ for every k, and ${}^t(A - \lambda I) = {}^t\!A - \lambda I$, ${}^t(A - \bar{\lambda} I) = {}^t\!A - \bar{\lambda} I$, so $\dim \operatorname{Ker}(A - \lambda I)^k = \dim \operatorname{Ker}({}^t\!A - \bar{\lambda} I)^k$ for every k. In other words, the ESP of A at λ is the same as the ESP of A at $\bar{\lambda}$, and both of these are the same as the ESP of ${}^tA$ at λ, which is the same as the ESP of ${}^tA$ at $\bar{\lambda}$, so in particular A and ${}^tA$ have the same JCF. □

We now come to our basic definition.

Definition 10.4.3. Let $\mathcal{T}\colon V \to V$ be a linear transformation. Then $\mathcal{T}$ is *normal* if $\mathcal{T}$ has an adjoint $\mathcal{T}^*$ and $\mathcal{T}$ and $\mathcal{T}^*$ commute, i.e., $\mathcal{T}\mathcal{T}^* = \mathcal{T}^*\mathcal{T}$. ◊

This definition is certainly not very intuitive, but let us see three important classes of normal linear transformations.

Definition 10.4.4. A linear transformation $\mathcal{T}\colon V \to V$ is *self-adjoint* if $\mathcal{T}$ has an adjoint $\mathcal{T}^*$ and $\mathcal{T}^* = \mathcal{T}$. ◊

Lemma 10.4.5. *Let $\mathcal{T}\colon V \to V$ be a self-adjoint linear transformation. Then $\mathcal{T}$ is normal and every complex eigenvalue of $\mathcal{T}$ is real.*

Proof. Certainly $\mathcal{T}$ is normal in this case. Now suppose that λ is a complex eigenvalue of $\mathcal{T}$, and let x be an associated eigenvector. Then

$$\lambda\langle x, x\rangle = \langle \lambda x, x\rangle = \langle \mathcal{T}(x), x\rangle = \langle x, \mathcal{T}^*(x)\rangle = \langle x, \mathcal{T}(x)\rangle = \langle x, \lambda x\rangle = \bar{\lambda}\langle x, x\rangle$$

so $\lambda = \bar{\lambda}$, i.e., λ is real. □

Lemma 10.4.6. *Let W be a subspace of V and suppose that W has an orthogonal complement $W^\perp$. Let $\Pi = \Pi_W : V \to V$ be orthogonal projection onto W. Then Π is self-adjoint.*

Proof. For $x \in V$, write $x = x_1 + x_2$ with $x_1 \in W$, $x_2 \in W^\perp$, and for $y \in V$, write $y = y_1 + y_2$ with $y_1 \in W$, $y_2 \in W^\perp$. Then

$$\langle \Pi(x), y\rangle = \langle x_1, y\rangle = \langle x_1, y_1 + y_2\rangle = \langle x_1, y_1\rangle + \langle x_1, y_2\rangle = \langle x_1, y_1\rangle$$

and

$$\langle x, \Pi(y)\rangle = \langle x, y_1\rangle = \langle x_1 + x_2, y_1\rangle = \langle x_1, y_1\rangle + \langle x_2, y_1\rangle = \langle x_1, y_1\rangle$$

and these are equal. □

As we will see from the spectral theorem, in the finite-dimensional case these projections are the "building blocks" for all normal linear transformations.

Lemma 10.4.7. *Let $\mathcal{T}\colon V \to V$ be an isometric isomorphism. Then $\mathcal{T}^* = \mathcal{T}^{-1}$, and so $\mathcal{T}$ is normal. Furthermore, every complex eigenvalue λ of $\mathcal{T}$ has absolute value* 1.

Proof. Let $x, y \in V$. Let $z = \mathcal{T}^{-1}(y)$, so $y = \mathcal{T}(z)$. Then

$$\langle x, \mathcal{T}^{-1}(y)\rangle = \langle x, z\rangle = \langle \mathcal{T}(x), \mathcal{T}(z)\rangle = \langle \mathcal{T}(x), y\rangle.$$

Hence $\mathcal{T}^* = \mathcal{T}^{-1}$ and $\mathcal{T}$ is normal.

Now let λ be a complex eigenvalue of $\mathcal{T}$, and let x be an associated eigenvector. Then $\mathcal{T}(x) = \lambda x$, so $x = \mathcal{T}^{-1}(\lambda x) = \lambda \mathcal{T}^{-1}(x)$, and so $\mathcal{T}^{-1}(x) = (1/\lambda)x$. But then

$$\begin{aligned}\lambda\langle x, x\rangle &= \langle \lambda x, x\rangle = \langle \mathcal{T}(x), x\rangle = \langle x, \mathcal{T}^*(x)\rangle \\ &= \langle x, \mathcal{T}^{-1}(x)\rangle = \langle x, (1/\lambda)x\rangle = (1/\bar{\lambda})\langle x, x\rangle\end{aligned}$$

so $\lambda = 1/\bar{\lambda}$, i.e., $\lambda\bar{\lambda} = |\lambda|^2 = 1$. □

Definition 10.4.8. If V is a real inner product space, an isometric isomorphism $\mathcal{T} \colon V \to V$ is called *orthogonal.* If V is a complex inner product space, an isometric isomorphism $\mathcal{T} \colon V \to V$ is called *unitary.* ◊

Now here are some constructions of new normal transformations from old.

Lemma 10.4.9. *If $\mathcal{T} \colon V \to V$ is normal, then $\mathcal{T}^*$ is normal.*

Proof. We need to know that $\mathcal{T}^*$ indeed has an adjoint, but by Lemma 9.5.14(6) it does, and in fact $(\mathcal{T}^*)^* = \mathcal{T}$. □

Lemma 10.4.10. *If $\mathcal{T} \colon V \to V$ is normal, then for any polynomial $p(x)$, $p(\mathcal{T})$ is normal, and $(p(\mathcal{T}))^* = \bar{p}(\mathcal{T}^*)$. If $\mathcal{T}$ is self-adjoint, then for any polynomial $p(x)$ with real coefficients, $p(\mathcal{T})$ is self-adjoint.*

Proof. This is the conclusion of Lemma 9.5.14(5). □

Now we come to some basic properties of normal linear transformations.

Lemma 10.4.11. *Let $\mathcal{T} \colon V \to V$ be a normal linear transformation. Then:*

(1) $\|\mathcal{T}(x)\| = \|\mathcal{T}^*(x)\|$ *for every $x \in V$. Consequently,* $\mathrm{Ker}(\mathcal{T}) = \mathrm{Ker}(\mathcal{T}^*)$.

(2) $\mathrm{Ker}(\mathcal{T}) = \mathrm{Im}(\mathcal{T})^\perp$ *and* $\mathrm{Ker}(\mathcal{T}^*) = \mathrm{Im}(\mathcal{T}^*)^\perp$.

(3) *Every generalized eigenvector of $\mathcal{T}$ is an eigenvector of $\mathcal{T}$.*

(4) *The vector $x \in V$ is an eigenvector of $\mathcal{T}$ with associated eigenvalue λ if and only if x is an eigenvector of $\mathcal{T}^*$ with associated eigenvalue $\bar{\lambda}$.*

(5) *Eigenspaces of distinct eigenvalues of $\mathcal{T}$ are orthogonal.*

Proof. (1) We have the chain of equalities

$$\begin{aligned}\|\mathcal{T}(x)\|^2 = \langle \mathcal{T}(x), \mathcal{T}(x)\rangle = \langle x, \mathcal{T}^*\mathcal{T}(x)\rangle = \langle x, \mathcal{T}\mathcal{T}^*(x)\rangle &= \langle x, \mathcal{T}^{**}\mathcal{T}^*(x)\rangle \\ = \langle \mathcal{T}^*(x), \mathcal{T}^*(x)\rangle &= \|\mathcal{T}^*(x)\|^2.\end{aligned}$$

Also, $x \in \mathrm{Ker}(\mathcal{T})$ means $\mathcal{T}(x) = 0$, which is equivalent to $\|\mathcal{T}(x)\| = 0$, so $\|\mathcal{T}^*(x)\| = 0$, and so $\mathcal{T}^*(x) = 0$, i.e., $x \in \mathrm{Ker}(\mathcal{T}^*)$, and vice-versa.

(2) From Lemma 10.4.1 we know that $\mathrm{Im}(\mathcal{T})^\perp = \mathrm{Ker}(\mathcal{T}^*)$ and $\mathrm{Im}(\mathcal{T}^*)^\perp = \mathrm{Ker}(\mathcal{T})$. But by (1), $\mathrm{Ker}(\mathcal{T}^*) = \mathrm{Ker}(\mathcal{T})$.

(3) We need to show that if $(\mathcal{T} - \lambda\mathcal{I})^2(x) = 0$, then $(\mathcal{T} - \lambda\mathcal{I})x = 0$ for any λ and any $x \in V$. Let $\mathcal{S} = \mathcal{T} - \lambda\mathcal{I}$. Then $\mathcal{S}$ is normal, as $\mathcal{S}^* = \mathcal{T}^* - \bar{\lambda}\mathcal{I}$, by Lemma 9.5.14. Let $w = \mathcal{S}(x)$. Then evidently $w \in \mathrm{Im}(\mathcal{S})$. But also $\mathcal{S}(w) = 0$ so $w \in \mathrm{Ker}(\mathcal{S})$. Thus $w \in \mathrm{Ker}(\mathcal{S}) \cap \mathrm{Im}(\mathcal{S}) = \{0\}$ by (2).

(4) We have that $x \in \mathrm{Ker}(\mathcal{S})$ where again $\mathcal{S} = \mathcal{T} - \lambda\mathcal{I}$. Then $x \in \mathrm{Ker}(\mathcal{S}^*)$ by (1). But $\mathcal{S}^* = (\mathcal{T} - \lambda\mathcal{I})^* = \mathcal{T}^* - \bar{\lambda}\mathcal{I}$, by Lemma 9.5.14.

(5) Let x_1 be an eigenvector of $\mathcal{T}$ with associated eigenvalue λ_1, and let x_2 be an eigenvector of $\mathcal{T}$ with associated eigenvalue $\lambda_2 \neq \lambda_1$. Then $\mathcal{T}(x_1) = \lambda_1 x_1$ and $\mathcal{T}(x_2) = \lambda_2 x_2$. But then, by (4), $\mathcal{T}^*(x_2) = \bar{\lambda}_2 x_2$. Then

$$\lambda_1\langle x_1, x_2\rangle = \langle \lambda_1 x_1, x_2\rangle = \langle \mathcal{T}(x_1), x_2\rangle = \langle x_1, \mathcal{T}^*(x_2)\rangle = \langle x_1, \bar{\lambda}_2 x_2\rangle = \lambda_2\langle x_1, x_2\rangle$$

so we must have $\langle x_1, x_2\rangle = 0$. □

Corollary 10.4.12. *Let V be finite dimensional, and let $\mathcal{T}: V \to V$ be a normal linear transformation. Then* $\operatorname{Im}(\mathcal{T}) = \operatorname{Im}(\mathcal{T}^*)$.

Proof. In this case, by Lemma 10.4.1(2) and Lemma 10.4.11(2),

$$\operatorname{Im}(\mathcal{T}) = \operatorname{Ker}(\mathcal{T}^*)^\perp = \operatorname{Ker}(\mathcal{T})^\perp = \operatorname{Im}(\mathcal{T}^*).$$ □

In the finite-dimensional case, we can summarize the basic structure of normal linear transformations (in the complex case) or self-adjoint linear transformations (in the real case) in the *spectral theorem.*

Theorem 10.4.13 (Spectral theorem)**.** (a) *Let V be a finite-dimensional complex vector space, and let $\mathcal{T}: V \to V$ be a linear transformation. The following are equivalent*:

(1) *$\mathcal{T}$ is normal.*

(2) *There are subspaces $W_1, \dots, W_k$ of V with $V = W_1 \perp \cdots \perp W_k$ and distinct complex numbers $\lambda_1, \dots, \lambda_k$ such that*

$$\mathcal{T} = \lambda_1 \Pi_{W_1} + \cdots + \lambda_k \Pi_{W_k},$$

where Π_{W_i} is the orthogonal projection of V onto W_i.

(3) *V has an orthonormal basis of eigenvectors of $\mathcal{T}$.*

(b) *Let V be a finite-dimensional real vector space, and let $\mathcal{T}: V \to V$ be a linear transformation. The following are equivalent*:

(1) *$\mathcal{T}$ is self-adjoint.*

(2) *There are subspaces $W_1, \dots, W_k$ of V with $V = W_1 \perp \cdots \perp W_k$ and distinct real numbers $\lambda_1, \dots, \lambda_k$ such that*

$$\mathcal{T} = \lambda_1 \Pi_{W_1} + \cdots + \lambda_k \Pi_{W_k},$$

where Π_{W_i} is the orthogonal projection of V onto W_i.

(3) *V has an orthonormal basis of eigenvectors of $\mathcal{T}$.*

Proof. First suppose that V is a complex vector space and that $\mathcal{T}$ is normal. Let $\lambda_1, \dots, \lambda_k$ be the distinct eigenvalues of $\mathcal{T}$, and let $W_1, \dots, W_k$ be the associated eigenspaces. Then by Lemma 10.4.11,

$$V = W_1 \perp \cdots \perp W_k.$$

Writing $v \in V$ uniquely as $v = w_1 + \cdots + w_k$ with $w_i \in W_i$,

$$\begin{aligned}\mathcal{T}(v) = \mathcal{T}(w_1 + \cdots + w_k) &= \mathcal{T}(w_1) + \cdots + \mathcal{T}(w_k)\\ &= \lambda_1 w_1 + \cdots + \lambda_k w_k\\ &= \lambda_1 \Pi_{W_1}(v) + \cdots + \lambda_k \Pi_{W_k}(v).\end{aligned}$$

Letting $\mathcal{B}_i$ be an orthonormal basis of W_i (which exists by Theorem 10.2.10 or Theorem 10.2.11), if $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$, then $\mathcal{B}$ is an orthonormal basis of V. Thus if (1) is true, then (2) and (3) are true. Also, this identification of the subspaces W_i and the complex numbers λ_i shows that (2) and (3) are equivalent.

On the other hand, suppose (2) (or (3)) is true.

Then

$$\mathcal{T} = \lambda_1 \Pi_{W_1} + \cdots + \lambda_k \Pi_{W_k}$$

so

$$\begin{aligned}\mathcal{T}^* &= \bar{\lambda}_1 \Pi_{W_1}^* + \cdots + \bar{\lambda}_k \Pi_{W_k}^* \\ &= \bar{\lambda}_1 \Pi_{W_1} + \cdots + \bar{\lambda}_k \Pi_{W_k}\end{aligned}$$

by Lemma 10.4.6. Since $\Pi_{W_i}^2 = \Pi_{W_i}$ and $\Pi_{W_i}\Pi_{W_j} = 0$ for $i \neq j$, we see that

$$\mathcal{T}\mathcal{T}^* = \mathcal{T}^*\mathcal{T} = |\lambda_1|^2 \Pi_{W_1} + \cdots + |\lambda_k|^2 \Pi_{W_k},$$

and in particular that $\mathcal{T}$ and $\mathcal{T}^*$ commute, so $\mathcal{T}$ is normal.

In the real case, we first note that all of the complex eigenvalues of $\mathcal{T}$ are real, by Lemma 10.4.5. Then the rest of the proof is the same. □

Corollary 10.4.14. (1) *In the situation, and notation, of Theorem* 10.4.13*,*

$$\mathcal{T}^* = \bar{\lambda}_1 \Pi_{W_1} + \cdots + \bar{\lambda}_k \Pi_{W_k}.$$

(2) *Let V be a finite-dimensional complex/real vector space, and let $\mathcal{T}\colon V \to V$ be a normal/self-adjoint linear transformation. Then $\mathcal{T}^*$ is a polynomial in $\mathcal{T}$.*

Proof. We proved (1) in the course of proving Theorem 10.4.13. Following the notation of the proof, note that if $v = w_1 + \cdots + w_k$,

$$\begin{aligned}(\mathcal{T} - \lambda_2\mathcal{I}) \cdots (\mathcal{T} - \lambda_k\mathcal{I})(v) &= (\lambda_1 - \lambda_2) \cdots (\lambda_1 - \lambda_k) w_1 \\ &= (\lambda_1 - \lambda_2) \cdots (\lambda_1 - \lambda_k) \Pi_{W_1}(v)\end{aligned}$$

so Π_{W_1} is a polynomial in $\mathcal{T}$, and so are $\Pi_{W_2}, \ldots, \Pi_{W_k}$. Then $\mathcal{T}^*$ is a polynomial in $\mathcal{T}$ as well. □

We can reformulate the spectral theorem in matrix terms. To do so, we need a definition first.

Definition 10.4.15. An n-by-n real matrix with ${}^tP = P^{-1}$ is *orthogonal*. An n-by-n matrix with ${}^tP = \bar{P}^{-1}$ is *unitary*. ◊

Theorem 10.4.16. (a) *Let A be an n-by-n complex matrix. The following are equivalent*:

(1) *A is normal, i.e., A commutes with A^*.*

(2) *There is a unitary matrix P and a diagonal matrix D with $A = {}^tPD\bar{P} = \bar{P}^{-1}D\bar{P}$.*

(b) *Let A be an n-by-n real matrix. The following are equivalent*:

(1) *A is symmetric.*

(2) *There is an orthogonal matrix P and a diagonal matrix D with real entries with $A = {}^tPDP = P^{-1}DP$.*

Proof. The linear transformation $\mathcal{T}_A$ is normal if and only if A is normal, and it is easy to check that P is unitary if and only if its columns are orthonormal, so this is a direct translation of the spectral theorem, and similarly in the real case. $\square$

Let us make some observations about unitary/orthogonal linear transformations/matrices.

Corollary 10.4.17. *Let V be a finite-dimensional complex/real vector space, and let $\mathcal{T}\colon V \to V$ be a linear transformation. The following are equivalent*:

(1) *$\mathcal{T}$ is unitary/orthogonal.*

(2) *$\mathcal{T}$ is normal and every complex eigenvalue λ of $\mathcal{T}$ is a complex number with $|\lambda| = 1$.*

Proof. By definition, a unitary/orthogonal linear transformation is normal. From the formula $\mathcal{T} = \lambda_1 \Pi_{W_1} + \cdots + \lambda_k \Pi_{W_k}$ of Theorem 10.4.13, it is easy to see that $\mathcal{T}$ is an isometry, and hence an isometric isomorphism, if and only if $|\lambda_i| = 1$ for each i. (Compare Lemma 10.4.7.) $\square$

Remark 10.4.18. It is *not* necessarily the case that if P is an orthogonal matrix, then all the complex eigenvalues of P are real. For example, for any value of θ the matrix

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

is orthogonal, but its complex eigenvalues are $\cos(\theta) \pm i \sin(\theta)$, which are not real unless $\sin(\theta) = 0$.

However, if P is an orthogonal matrix all of whose eigenvalues are real, they must be real numbers λ with $|\lambda|^2 = 1$, i.e., they must all be $\lambda = \pm 1$. In this case we see from Corollary 10.4.17 that $\mathcal{T}_P^* = \mathcal{T}_P$, i.e., that $\mathcal{T}_P$ is self-adjoint. $\Diamond$

Corollary 10.4.19. *Let V be a finite-dimensional complex/real vector space, and let $\mathcal{B}$ be an orthonormal basis of V. Let $\mathcal{C}$ be another basis of V, and let $P = [P]_{\mathcal{B} \leftarrow \mathcal{C}}$ be the change of basis matrix. The following are equivalent*:

(1) *P is unitary/orthogonal.*

(2) *$\mathcal{C}$ is orthonormal.*

Proof. Let $\mathcal{B} = \{v_1, \dots, v_n\}$ and $\mathcal{C} = \{w_1, \dots, w_n\}$. Then $\mathcal{T}\colon V \to V$ by $\mathcal{T}(v_i) = w_i$ is an isometry, and hence an isometric isomorphism, if and only if $\mathcal{C}$ is orthonormal. $\square$

We have a final application of the spectral theorem. If $\mathcal{S}$ and $\mathcal{T}$ are isometries, and hence isometric isomorphisms, then so are $\mathcal{S}\mathcal{T}$ and $\mathcal{T}^{-1}$. If $\mathcal{T}$ is normal/self-adjoint and invertible, then if V is finite dimensional, from Corollary 9.5.15 so is $\mathcal{T}^{-1}$. It is not in general the case that if $\mathcal{S}$ and $\mathcal{T}$ are normal/self-adjoint, so is $\mathcal{S}\mathcal{T}$. But in one case it is.

Corollary 10.4.20. *Let V be a finite-dimensional vector space, and let $\mathcal{S}\colon V \to V$ and $\mathcal{T}\colon V \to V$ be normal linear transformations. Suppose that $\mathcal{S}$ and $\mathcal{T}$ commute. Then $\mathcal{S}$ and $\mathcal{T}^*$, $\mathcal{S}^*$ and $\mathcal{T}$, and $\mathcal{S}^*$ and $\mathcal{T}^*$ also commute. Also, $\mathcal{S}\mathcal{T}$ is normal. Furthermore, if $\mathcal{S}$ and $\mathcal{T}$ are both self-adjoint, then $\mathcal{S}\mathcal{T}$ is self-adjoint.*

Proof. The self-adjoint case is immediate. If $\mathcal{S} = \mathcal{S}^*$ and $\mathcal{T} = \mathcal{T}^*$, then $(\mathcal{S}\mathcal{T})^* = \mathcal{T}^*\mathcal{S}^* = \mathcal{T}\mathcal{S} = \mathcal{S}\mathcal{T}$ is self-adjoint.

Suppose, in general, that $\mathcal{S}$ and $\mathcal{T}$ are normal. Then, by Corollary 10.4.14, there are polynomials $p(x)$ and $q(x)$ with $\mathcal{S}^* = p(\mathcal{S})$ and $\mathcal{T}^* = q(\mathcal{T})$. But then $\mathcal{S}$ commutes with $q(\mathcal{T})$, $\mathcal{T}$ commutes with $p(\mathcal{S})$, and $p(\mathcal{S})$ and $q(\mathcal{T})$ commute. But then also

$$(\mathcal{S}\mathcal{T})^*(\mathcal{S}\mathcal{T}) = \mathcal{T}^*\mathcal{S}^*\mathcal{S}\mathcal{T} = \mathcal{S}\mathcal{T}\mathcal{T}^*\mathcal{S}^* = (\mathcal{S}\mathcal{T})(\mathcal{S}\mathcal{T})^*$$

so $\mathcal{S}\mathcal{T}$ is normal. □

We make one final comparison between arbitrary linear transformations and normal ones. First we have a result of Schur.

Lemma 10.4.21. *Let V be a finite-dimensional vector space, and let $\mathcal{T}: V \to V$ be a linear transformation. If V is real, assume all the complex eigenvalues of $\mathcal{T}$ are real. Then V has an orthonormal basis $\mathcal{C}$ in which $A = [\mathcal{T}]_{\mathcal{C}}$ is upper triangular.*

Proof. We know that V has a basis $\mathcal{B} = \{x_1, \ldots, x_n\}$ in which $B = [\mathcal{T}]_{\mathcal{B}}$ is upper triangular. Let $B = (b_{ij})$. Then for each i, $\mathcal{T}(x_i) = \sum_{j \le i} b_{ij} x_j$, i.e., $\mathcal{T}(x_i) \in \operatorname{Span}(\{x_1, \ldots, x_i\})$ for each $i = 1, \ldots, n$. Apply the Gram-Schmidt procedure (Theorem 10.2.11) to $\mathcal{B}$ to obtain a new basis $\mathcal{C} = \{z_1, \ldots, z_n\}$ of V. Then $\mathcal{C}$ is orthonormal, by construction, and $\operatorname{Span}(\{z_1, \ldots, z_i\}) = \operatorname{Span}(\{x_1, \ldots, x_i\})$ for each i. Thus $\mathcal{T}(z_i) = \sum_{j \le i} a_{ij} z_j$ and so $A = (a_{ij})$ is upper triangular. □

Corollary 10.4.22. *Let V be a finite-dimensional vector space, and let $\mathcal{T}: V \to V$ be a linear transformation. If V is real, assume all the complex eigenvalues of $\mathcal{T}$ are real. Let $\mathcal{C}$ be an orthonormal basis of V with $A = [\mathcal{T}]_{\mathcal{C}}$ upper triangular. Then $\mathcal{T}$ is normal if and only if A is diagonal.*

Proof. Since $\mathcal{C}$ is orthonormal, $[\mathcal{T}^*]_{\mathcal{C}} = A^* = {}^t\bar{A}$. On the one hand, if A is upper triangular, then A^* is lower triangular. On the other hand, by Corollary 10.4.14, $A^* = p(A)$ for some polynomial $p(x)$, so if A is upper triangular, then A^* is also upper triangular. Thus A^* must be both upper and lower triangular, i.e., diagonal, and then $A = (A^*)^*$ is diagonal as well. Conversely, if A is diagonal, then $A^* = {}^t\bar{A}$ is also diagonal, so A and A^* certainly commute, and $\mathcal{T}$ is normal. □

Remark 10.4.23. While we have completely determined the structure of normal linear transformations in the finite-dimensional case, and while Lemma 10.4.11 is true whether or not V is finite dimensional, this in general is far from telling us the answer in the infinite-dimensional case. In fact, there is no similar structure theorem in the infinite-dimensional case, as if V is infinite dimensional, a linear transformation $\mathcal{T}: V \to V$ need not have any eigenvalues at all.

For example, let V be the vector space of doubly infinite sequences of Example 9.5.18(b). Then $\mathcal{S}_{\mathrm{rt}}$ and $\mathcal{S}_{\mathrm{lt}}$ are both isometric isomorphisms, and indeed $\mathcal{S}_{\mathrm{rt}} = \mathcal{S}_{\mathrm{lt}}^{-1}$, but neither $\mathcal{S}_{\mathrm{rt}}$ nor $\mathcal{S}_{\mathrm{lt}}$ has any eigenvalues.

Similarly, let $V = {}^t\mathbb{R}^\infty$ as in Example 9.5.18(b), and note, as our computations there show, that neither $\mathcal{S}_{\mathrm{rt}}$ nor $\mathcal{S}_{\mathrm{lt}}$ is normal. But $\mathcal{T} = \mathcal{S}_{\mathrm{rt}} + \mathcal{S}_{\mathrm{lt}}$ is normal (in fact, self-adjoint), and $\mathcal{T}$ does not have any eigenvalues. ◊

10.5. Exercises

1. Apply the Gram-Schmidt procedure to convert each of the following bases for $\mathbb{R}^n$, with the standard inner product (dot product), to orthonormal bases.

(a) $\mathcal{B} = \left\{ \begin{bmatrix} 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 6 \end{bmatrix} \right\}$.

(b) $\mathcal{B} = \left\{ \begin{bmatrix} 2 \\ 6 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \end{bmatrix} \right\}$.

(c) $\mathcal{B} = \left\{ \begin{bmatrix} 9 \\ 12 \\ 20 \end{bmatrix}, \begin{bmatrix} 4 \\ 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 6 \\ 3 \end{bmatrix} \right\}$.

(d) $\mathcal{B} = \left\{ \begin{bmatrix} 2 \\ 6 \\ 3 \end{bmatrix}, \begin{bmatrix} 4 \\ 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 9 \\ 12 \\ 20 \end{bmatrix} \right\}$.

(As this problem demonstrates, the result of Gram-Schmidt depends on the order of the vectors.)

2. Let $\mathbb{R}^3$ have the standard inner product. In each case, find the orthogonal projections of the vector v onto the subspace spanned by the set S.

(a) $S = \left\{ \begin{bmatrix} 3 \\ 4 \\ 12 \end{bmatrix} \right\}$, $v = \begin{bmatrix} 3 \\ 1 \\ 0 \end{bmatrix}$.

(b) $S = \left\{ \begin{bmatrix} 8 \\ 9 \\ 12 \end{bmatrix}, \begin{bmatrix} -1 \\ 2 \\ 2 \end{bmatrix} \right\}$, $v = \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$.

3. Let $P_2(\mathbb{R})$ have the inner product

$$\langle f(x), g(x) \rangle = \int_{-1}^{1} f(x)g(x)\,dx.$$

In each case, find the orthogonal projection of the vector v onto the subspace spanned by the set S.

(a) $S = \{1\}$, $v = 1 + 2x + 3x^2$.

(b) $S = \{x\}$, $v = 1 + 2x + 3x^2$.

(c) $S = \{1, x\}$, $v = 1 + 2x + 3x^2$.

4. (a) Let $V = \mathbb{R}^2$ with the standard inner product. Let a and b be real numbers with $a^2 + b^2 = 1$. Let $w_1 = \begin{bmatrix} a \\ b \end{bmatrix}$ and $w_2 = \begin{bmatrix} -b \\ a \end{bmatrix}$. Let $\varepsilon = \pm 1$.

Show that $\mathcal{B} = \{w_1, \varepsilon w_2\}$ is an orthonormal basis of V, and that every orthonormal basis of V is of this form.

(b) Let $V = \mathbb{C}^2$ with the standard inner product. Let a and b be complex numbers with $a\bar{a} + b\bar{b} = 1$. Let $w_1 = \begin{bmatrix} a \\ b \end{bmatrix}$ and $w_2 = \begin{bmatrix} -\bar{b} \\ \bar{a} \end{bmatrix}$. Let ε be a complex number with $\varepsilon\bar{\varepsilon} = 1$.

Show that $\mathcal{B} = \{w_1, \varepsilon w_2\}$ is an orthonormal basis of V, and that every orthonormal basis of V is of this form.

5. (a) Let $V = \mathbb{R}^2$ with the standard inner product. Let a and b be real numbers with $a^2 + b^2 = 1$. Let $w_1 = \begin{bmatrix} a \\ b \end{bmatrix}$ and $w_2 = \begin{bmatrix} -b \\ a \end{bmatrix}$.

Then $\mathcal{B} = \{w_1, w_2\}$ is an orthonormal basis of V. Let W_1 be the subspace of V spanned by w_1, and let W_2 be the subspace of V spanned by w_2. Let $\Pi_1 \colon V \to W_1$ and $\Pi_2 \colon V \to W_2$ be the orthogonal projections. Let E_1 be the matrix of Π_1, and E_2 the matrix of Π_2, both in the standard bases. Show that

$$E_1 = \begin{bmatrix} a^2 & ab \\ ab & b^2 \end{bmatrix} \quad \text{and} \quad E_2 = \begin{bmatrix} b^2 & -ab \\ -ab & a^2 \end{bmatrix}.$$

(b) Let $V = \mathbb{C}^2$ with the standard inner product. Let a and b be complex numbers with $a\bar{a} + b\bar{b} = 1$. Let $w_1 = \begin{bmatrix} a \\ b \end{bmatrix}$ and $w_2 = \begin{bmatrix} -\bar{b} \\ \bar{a} \end{bmatrix}$.

Then $\mathcal{B} = \{w_1, w_2\}$ is an orthonormal basis of V. Let W_1 be the subspace of V spanned by w_1, and let W_2 be the subspace of V spanned by w_2. Let $\Pi_1 \colon V \to W_1$ and $\Pi_2 \colon V \to W_2$ be the orthogonal projections. Let E_1 be the matrix of Π_1, and E_2 the matrix of Π_2, both in the standard bases. Show that

$$E_1 = \begin{bmatrix} a\bar{a} & a\bar{b} \\ \bar{a}b & b\bar{b} \end{bmatrix} \quad \text{and} \quad E_2 = \begin{bmatrix} b\bar{b} & -a\bar{b} \\ -\bar{a}b & a\bar{a} \end{bmatrix}.$$

6. (a) Let $w = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ be a fixed nonzero vector in $V = \mathbb{R}^n$ (with the standard inner product), and let W be the subspace spanned by w. Let $\Pi_W \colon V \to W$ be the orthogonal projection of V onto W. Find $[\Pi_W]_{\mathcal{E}}$, the matrix of Π_W in the standard basis $\mathcal{E}$ of V.

(b) Same problem with $V = \mathbb{C}^n$.

7. Let A be any invertible matrix with real (resp., complex) entries. Show there is an orthogonal (resp., unitary) matrix Q and an upper triangular matrix R all of whose diagonal entries are positive real numbers such that $A = QR$. Furthermore, show that the matrices Q and R are unique. (This is called the *QR decomposition* of A.)

8. Let V be an inner product space, and let W be a subspace. Let $\Pi \colon V \to W$ be orthogonal projection. Let $v \in V$, and let $v_0 = \Pi(v)$.

(a) Show that $v - v_0 \in W^{\perp}$.

(b) If W has orthonormal basis $\mathcal{B} = \{w_1, \ldots, w_k\}$, show that

$$v_0 = \langle v, w_1 \rangle w_1 + \cdots + \langle v, w_k \rangle w_k.$$

(c) Let w be any vector in W. Show that $\|v - v_0\| \leq \|v - w\|$ with equality if and only if $w = v_0$.

This gives the point of view that of all vectors in W, v_0 is the unique best approximation to v.

9. Prove the polarization identities (Lemma 10.1.6).

10. Let V be a real or complex inner product space. Let $v_1, v_2, \dots, v_n$ be any n vectors in V. Show that

$$(1/2^n) \sum \|\varepsilon_1 v_1 + \cdots + \varepsilon_n v_n\|^2 = \sum_{i=1}^{n} \|v_i\|^2,$$

where the sum on the left-hand side is taken over all 2^n possible choices $\varepsilon_1 = \pm 1, \dots, \varepsilon_n = \pm 1$. (For $n = 2$ this is known as the *parallelogram law.*)

11. We defined a general notion of a norm $\|\cdot\|$ on a real or complex vector space V in Definition 10.1.17.

(a) Given a norm $\|\cdot\|$ on V, we may define $\langle x, y\rangle$ by the polarization identities (Lemma 10.1.6). Show that $\langle x, y\rangle$ defined in this way is an inner product on V if and only if the parallelogram law holds for $\|\cdot\|$.

(b) Let $V = \mathbb{R}^n$ or $\mathbb{C}^n$ and define a norm on V as follows. If $v = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$, then $\|v\| = \max(|a_1|, |a_2|, \dots, |a_n|)$. Show that this norm does not satisfy the parallelogram law.

12. Let $V = P_d(\mathbb{R})$ with inner product

$$\langle f(x), g(x)\rangle = \int_0^1 f(x)g(x)w(x)\,dx$$

with $w(x) \geq 0$ for all x and with $w(x)$ not identically zero on any subinterval of $[0, 1]$.

Let $\mathcal{B} = \{p_0(x), \dots, p_d(x)\}$ be any basis of V with $\deg(p_i(x)) = i$ for each i (for example, $\mathcal{B} = \{1, x, \dots, x^d\}$), and let $\mathcal{C} = \{q_0(x), \dots, q_d(x)\}$ be the basis of V obtained by applying the Gram-Schmidt procedure to $\mathcal{B}$. Of course, the exact elements of $\mathcal{C}$ depend on the "weight" $w(x)$. But show that for *any* $w(x)$, $\deg(q_i(x)) = i$ for each i.

Similarly, if $\mathcal{B}' = \{p_d(x), \dots, p_0(x)\}$ is a basis of V with $p_i(x)$ exactly divisible by x^i for each i (for example, $\mathcal{B}' = \{x^d, x^{d-1}, \dots, 1\}$) and $\mathcal{C}' = \{q'_d(x), \dots, q'_0(x)\}$ is obtained by applying the Gram-Schmidt procedure to $\mathcal{B}'$, show that $q'_i(x)$ is exactly divisible by x^i for each i.

13. Let $P_3(\mathbb{R})$ have inner product

$$\langle f(x), g(x)\rangle = \int_{-1}^1 f(x)g(x)w(x)\,dx.$$

Let $\mathcal{B} = \{1, x, x^2, x^3\}$ be a basis for $P_3(\mathbb{R})$. Use the Gram-Schmidt procedure to convert $\mathcal{B}$ into an orthogonal basis $\mathcal{B}' = \{p_0(x), p_1(x), p_2(x), p_3(x)\}$ except instead of normalizing so that each $p_i(x)$ has norm 1, normalize them as given.

(a) $w(x) = 1$, $p_i(1) = 1$, $i = 0, \ldots, 3$.

(b) $w(x) = 1/\sqrt{1-x^2}$, $p_i(1) = 1$, $i = 0, \ldots, 3$.

(c) $w(x) = \sqrt{1-x^2}$, $p_i(1) = i+1$, $i = 0, \ldots, 3$.

The polynomials so obtained are known as the Legendre polynomials, the Chebyshev polynomials of the first kind, and the Chebyshev polynomials of the second kind, respectively.

(d), (e), (f): As in (a), (b), (c), except now $\mathcal{B} = \{x^3, x^2, x, 1\}$.

14. (a) Let A be an n-by-n matrix such that $A^2 = A$. Show that $\mathbb{R}^n = \operatorname{Ker}(A) \oplus \operatorname{Im}(A)$.

(b) Now suppose that A is real symmetric (resp., complex Hermitian). Show that $\mathbb{R}^n = \operatorname{Ker}(A) \perp \operatorname{Im}(A)$ (resp., $\mathbb{C}^n = \operatorname{Ker}(A) \perp \operatorname{Im}(A)$).

15. Let V and W be finite-dimensional inner product spaces, and let $\mathcal{T}\colon V \to W$ be a linear transformation. Let $w_0 \in W$ and suppose that $U = \{v \in V \mid \mathcal{T}(v) = w_0\}$ is nonempty (in which case it is an affine subspace of V).

(a) Show that there is a unique vector $u_0 \in U \cap \operatorname{Im}(\mathcal{T}^*)$.

(b) Show that for any vector $u \in U$, $\|u\| \geq \|u_0\|$ with equality if and only if $u = u_0$.

Thus we see that if $\mathcal{T}(v) = w_0$ has a solution, it has a unique solution of minimal norm.

16. Let V and W be inner product spaces, and let $\mathcal{T}\colon V \to W$ be a linear transformation. The *pseudo-inverse* of $\mathcal{T}$ is the linear transformation $\mathcal{S}\colon W \to V$ defined as follows.

Write $V = \operatorname{Ker}(\mathcal{T}) \perp \operatorname{Ker}(\mathcal{T})^\perp$ and $W = \operatorname{Im}(\mathcal{T}) \perp \operatorname{Im}(\mathcal{T})^\perp$, let $\mathcal{T}'$ be the restriction of $\mathcal{T}$ to $\operatorname{Im}(\mathcal{T})^\perp$, and note that $\mathcal{T}'\colon \operatorname{Ker}(\mathcal{T})^\perp \to \operatorname{Im}(\mathcal{T})$ is an isomorphism. Let $\Pi\colon W \to \operatorname{Im}(\mathcal{T})$ be the projection. Then

$$\mathcal{S} = (\mathcal{T}')^{-1}\Pi.$$

Alternatively, $\mathcal{S}$ is defined as follows. Let $w \in W$. Then we may write w uniquely as $w = w_0 + w_1$ with $w_0 \in \operatorname{Im}(\mathcal{T})$ and $w_1 \in \operatorname{Im}(\mathcal{T})^\perp$. There is a unique element $v_0 \in \operatorname{Ker}(\mathcal{T})^\perp$ with $\mathcal{T}(v_0) = w_0$. Then

$$\mathcal{S}(w) = v_0.$$

In the above notation, show that w_0 is the element of W such that $\|w - w_0\|$ is minimal, and that v_0 is the element of V with $\mathcal{T}(v_0) = w_0$ having $\|v_0\|$ minimal.

17. Let A be a real m-by-n matrix, so that $\mathcal{T}_A\colon \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation. Give $\mathbb{R}^n$ and $\mathbb{R}^m$ the standard inner products ("dot-product"). Then the pseudo-inverse of the matrix A is the matrix B with $\mathcal{S} = \mathcal{T}_B$, where $\mathcal{S}$ is the pseudo-inverse of $\mathcal{T}_A$ as defined in the previous problem.

In each case, compute B and (in the notation of the previous problem) find v_0 and w_0.

(a) $A = \begin{bmatrix} 1 & 3 \\ 2 & 6 \end{bmatrix}$, $w = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

(b) $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 7 \end{bmatrix}$, $w = \begin{bmatrix} 3 \\ 7 \\ 10 \end{bmatrix}$.

(c) $A = \begin{bmatrix} 1 & 2 \\ 3 & 7 \\ 5 & 11 \end{bmatrix}$, $w = \begin{bmatrix} 9 \\ 19 \end{bmatrix}$.

(d) $A = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix}$, $w = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$.

(e) $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 4 & 8 & 12 \end{bmatrix}$, $w = \begin{bmatrix} 1 \\ 4 \\ 9 \end{bmatrix}$.

18. Let $A = \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $C = AB = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$.

(a) Find the pseudo-inverses D of A, E of B, and F of C.

(b) Calculate that $F \neq ED$.

(Thus, as opposed to inverses, it is not always the case that the pseudo-inverse of a product is the product of the pseudo-inverses in the reverse order.)

19. Let $V = P_3$ with the inner product

$$\langle f, g \rangle = \int_{-1}^{1} f(x)g(x)\,dx.$$

Let $D\colon V \to V$ be differentiation, $D(f(x)) = f'(x)$. Find the pseudo-inverses of D, D^2, and D^3.

20. Let A be a positive semidefinite real symmetric/complex Hermitian matrix. Show that A has a unique positive semidefinite real symmetric/complex Hermitian square root. That is, show that there is a unique positive semidefinite real symmetric/complex Hermitian matrix B with $B^2 = A$.

21. (a) Orthogonally diagonalize the following symmetric matrices:

(i) $A = \begin{bmatrix} 1 & 2 \\ 2 & 7 \end{bmatrix}$.

(ii) $A = \begin{bmatrix} 225 & 180 & 240 \\ 180 & 944 & -408 \\ 240 & -408 & 706 \end{bmatrix}$, $c_A(x) = x(x-625)(x-1250)$.

(iii) $A = \begin{bmatrix} 3600 & -300 & 1200 \\ -300 & 3775 & 900 \\ 1200 & 900 & 400 \end{bmatrix}$, $c_A(x) = (x+225)(x-4000)^2$.

(b) Unitarily diagonalize the following Hermitian matrix:

$$A = \begin{bmatrix} 1 & 2i \\ -2i & 7 \end{bmatrix}.$$

22. Let $\mathcal{T}: V \to W$. Referring to the singular value decomposition, we see that we have bases $\mathcal{B}$ of V and $\mathcal{C}$ of W, but they are not well-defined, i.e., there are choices involved.

Consider $\mathcal{T}^*: W \to V$. We may similarly choose bases $\mathcal{B}^*$ of W and $\mathcal{C}^*$ of V. Show that it is possible to choose $\mathcal{B}^* = \mathcal{C}$ and $\mathcal{C}^* = \mathcal{B}$. Then conclude that $\mathcal{T}^*$ has the same singular values as $\mathcal{T}$.

23. We have stated the singular value decomposition for linear transformations.

(a) Show that this translates into the singular value decomposition for matrices as follows. Let A be an m-by-n matrix. Let $\lambda_1, \ldots, \lambda_r$ be the nonzero eigenvalues of A^*A, and let $\sigma_i = \sqrt{\lambda_i}$, $i = 1, \ldots, r$. Let S be the m-by-n matrix whose first r diagonal entries are $\sigma_1, \ldots, \sigma_r$, and all of whose other entries are 0. Then there is a unitary m-by-m matrix P and a unitary n-by-n matrix Q, such that $A = PSQ^*$.

(b) Identify the matrices P and Q in terms of the other data in the singular value decomposition.

(Of course, Q is unitary if and only if Q^* is, but the singular value decomposition for matrices is most naturally stated using Q^*.)

24. Let A and B be similar matrices. Then of course they have the same eigenvalues. Show by example that A and B can have different singular values. Give an example where A and B are both diagonalizable, and one where they are not.

25. (a) Let A be any matrix. Show that A and A^* have the same singular values. Also, given a singular value decomposition of A, find a singular value decomposition of A^*.

(b) Let A be any invertible matrix. Show that the singular values of A^{-1} are the inverses (i.e., reciprocals) of the singular values of A. Also, given a singular value decomposition of A, find a singular value decomposition of A^{-1}.

26. Let A be a real symmetric/complex Hermitian matrix. Then, by Corollary 10.3.6, A is orthogonally/unitarily diagonalizable. Write $A = PDP^{-1}$ as in that corollary. Of course, we may choose D so that the absolute values of its diagonal entries are in decreasing order.

(a) If A is positive semidefinite, show that this factorization of A is a singular value decomposition of A.

(b) For a general real symmetric/complex Hermitian matrix A, find a singular value decomposition of A from this factorization of A.

27. Let A be a real symmetric/complex Hermitian matrix. It follows from Exercise 20 that there is a unique positive semidefinite real symmetric/complex Hermitian matrix B with $B^2 = A^2$. Given a singular value decomposition of A, find a singular value decomposition of B.

28. In each case, find a singular value decomposition $A = PSQ^*$ of the matrix A.

(a) $A = \begin{bmatrix} 3 & 2 \\ 1 & 2 \end{bmatrix}$.

(b) $A = \begin{bmatrix} -5 & -9 \\ 4 & 7 \end{bmatrix}$.

(c) $A = \begin{bmatrix} 1 & -2 \\ 3 & 5 \end{bmatrix}$.

(d) $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \\ 1 & 1 \end{bmatrix}$.

(e) $A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 2 & 1 \end{bmatrix}$.

(Hint: Use your answer to (d) to get an answer to (e).)

29. Show that the spectral theorem for normal linear transformations has the following transformation into matrix language.

Let A be a complex n-by-n matrix (resp., a real n-by-n matrix) with $A{}^t\bar{A} = {}^t\bar{A}A$ (resp., $A = {}^tA$). Then there are distinct complex (resp., real) numbers $\lambda_1, \dots, \lambda_k$ and complex (resp., real) matrices $E_1, \dots, E_k$ such that

(1a) $I = E_1 + \cdots + E_k$,

(1b) $E_i = {}^t\bar{E}_i$, $E_i^2 = E_i$, $E_iE_j = 0$ for $i \neq j$,

(2) $A = \lambda_1 E_1 + \cdots + \lambda_k E_k$.

This is called the spectral decomposition of the matrix A.

30. Let $\mathcal{E} = \{e_1, \dots, e_n\}$ be the standard basis of $\mathbb{C}^n$, and let A be the matrix $A = [e_n|e_1|\dots|e_{n-1}]$. (Observe that A is a permutation matrix, and is also the companion matrix of the polynomial $x^n - 1$.) Regarding A as a complex matrix, observe that A is unitary.

(a) Let $\mathcal{T} = \mathcal{T}_A \colon \mathbb{C}^n \to \mathbb{C}^n$. In (a)(2) of Theorem 10.4.13, the spectral theorem for $\mathcal{T}$, find the λ_i and the W_i.

(b) In (a)(2) of Theorem 10.4.16, the spectral theorem for A, find P and D.

(c) In (2) of Exercise 29, the spectral decomposition of A, find the λ_i and E_i.

31. Find the spectral decompositions of each of the following normal matrices.

(a) $A = \begin{bmatrix} 1 & 4 \\ 4 & 9 \end{bmatrix}$.

(b) $A = \begin{bmatrix} 1 & 4i \\ -4i & 9 \end{bmatrix}$.

(c) $A = \begin{bmatrix} 9+32i & 12-12i \\ 12-12i & 16+18i \end{bmatrix}$.

(d) $A = \begin{bmatrix} 625+1152i & 336 \\ -336 & 625+98i \end{bmatrix}$.

(e) $A = \begin{bmatrix} 225 & 180 & 240 \\ 180 & 944 & -408 \\ 240 & -408 & 706 \end{bmatrix}$, $c_A(x) = x(x - 625)(x - 1250)$.

(f) $A = \begin{bmatrix} 3600 & -300 & 1200 \\ -300 & 3775 & 900 \\ 1200 & 900 & 400 \end{bmatrix}$, $c_A(x) = (x + 225)(x - 4000)^2$.

Appendix A

Fields

In the first section of this (optional) appendix we introduce the notion of a field and give several examples. In the second section we (very briefly) consider fields as vector spaces.

A.1. The notion of a field

Here is the basic definition.

Definition A.1.1. A *field* $\mathbb{F}$ is a set of objects with two operations, addition and multiplication, having the following properties:

(1) If a and b are elements of $\mathbb{F}$, then $a+b$ is an element of $\mathbb{F}$.

(2) For any $a,\ b$ in $\mathbb{F}$, $a+b=b+a$.

(3) For any $a,\ b,\ c$ in $\mathbb{F}$, $(a+b)+c=a+(b+c)$.

(4) There is an element 0 in $\mathbb{F}$ such that for any a in $\mathbb{F}$, $a+0=0+a=a$.

(5) For any a in $\mathbb{F}$ there is an element $-a$ in $\mathbb{F}$ such that $a+(-a)=(-a)+a=0$.

(6) If a and b are elements of $\mathbb{F}$, then ab is an element of $\mathbb{F}$.

(7) For any $a,\ b$ in $\mathbb{F}$, $ab=ba$.

(8) For any $a,\ b,\ c$ in $\mathbb{F}$, $(ab)c=a(bc)$.

(9) There is an element $1\neq 0$ in $\mathbb{F}$ such that for any a in $\mathbb{F}$, $a1=1a=a$.

(10) For any $a\neq 0$ in $\mathbb{F}$ there is an element a^{-1} in $\mathbb{F}$ such that $aa^{-1}=a^{-1}a=1$.

(11) For any $a,\ b,\ c$ in $\mathbb{F}$, $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$. ◊

Here are some familiar fields. (In each case, we use the "usual" operations of addition and multiplication.)

Example A.1.2. (a) $\mathbb{F}=\mathbb{Q}=\{a/b\,|\,a,\ b \text{ integers}, b\neq 0\}$, the field of *rational numbers.*

(b) $\mathbb{F}=\mathbb{R}$, the field of *real numbers.*

(c) $\mathbb{F} = \mathbb{C} = \{a + bi \,|\, a,\ b \in \mathbb{R}\}$, the field of *complex numbers*. Here $i^2 = -1$. $\Diamond$

Here is a way of getting new fields from old.

Example A.1.3. Let $\mathbb{F}$ be a field, and let D be an element of $\mathbb{F}$ that is not a square in $\mathbb{F}$. Then $\mathbb{E} = \mathbb{F}(\sqrt{D}) = \{a + b\sqrt{D} \,|\, a,\ b \in \mathbb{F}\}$ is a field with the following operations:

$$
\begin{aligned}
(a_1 + b_1\sqrt{D}) + (a_2 + b_2\sqrt{D}) &= (a_1 + a_2) + (b_1 + b_2)\sqrt{D}, \\
(a_1 + b_1\sqrt{D})(a_2 + b_2\sqrt{D}) &= a_1a_2 + a_1b_2\sqrt{D} + a_2b_1\sqrt{D} + b_1b_2(\sqrt{D})^2 \\
&= (a_1a_2 + b_1b_2D) + (a_1b_2 + a_2b_1)\sqrt{D}, \\
(a + b\sqrt{D})^{-1} &= \frac{1}{a + b\sqrt{D}} = \frac{1}{a + b\sqrt{D}} \cdot \frac{a - b\sqrt{D}}{a - b\sqrt{D}} = \frac{a - b\sqrt{D}}{a^2 - b^2D} \\
&= \frac{a}{a^2 - b^2D} + (\frac{-b}{a^2 - b^2D})\sqrt{D}.
\end{aligned}
$$

If $\mathbb{F} = \mathbb{R}$ and $D = -1$, then $\mathbb{E} = \mathbb{R}(\sqrt{-1})$ is just $\mathbb{C}$. But we could also choose, for example, $\mathbb{F} = \mathbb{Q}$ and $D = 2$ to obtain the field $\mathbb{Q}(\sqrt{2})$. $\Diamond$

For those of you who know some number theory, here is another example.

Example A.1.4. Let p be a prime, and let $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ with addition given by addition (mod p) and multiplication given by multiplication (mod p). Then $\mathbb{F}_p$ is a field. Note $\mathbb{F}_p$ has p elements. $\Diamond$

Remark A.1.5. We observe that the integers $\mathbb{Z}$ do *not* form a field. They do not satisfy property (10): if n is a nonzero integer, $n \neq \pm 1$, then n does not have a multiplicative inverse in $\mathbb{Z}$. $\Diamond$

A.2. Fields as vector spaces

Definition A.2.1. Let $\mathbb{F}$ and $\mathbb{E}$ be fields with $\mathbb{F} \subseteq \mathbb{E}$. Then we say that $\mathbb{F}$ is a *subfield* of $\mathbb{E}$, or that $\mathbb{E}$ is an *extension (field)* of $\mathbb{F}$. $\Diamond$

It is then easy to check:

Lemma A.2.2. *Let $\mathbb{E}$ be an extension of $\mathbb{F}$. Then $\mathbb{E}$ is an $\mathbb{F}$-vector space.*

Thus we may define:

Definition A.2.3. Let $\mathbb{E}$ be an extension of $\mathbb{F}$. The *degree* of this extension is the dimension of $\mathbb{E}$ as an $\mathbb{F}$-vector space. $\Diamond$

Example A.2.4. (a) Let $\mathbb{E} = \mathbb{F}(\sqrt{D})$ as in Example A.1.3. Then $\mathbb{E}$ has basis $\mathcal{B} = \{1, \sqrt{D}\}$ as an $\mathbb{F}$-vector space, so $\mathbb{E}$ is an extension of $\mathbb{F}$ of degree 2. In particular, $\mathbb{C}$ is an extension of $\mathbb{R}$ of degree 2.

(b) Although we will not prove it here, $\mathbb{R}$ and $\mathbb{C}$ are both infinite-dimensional $\mathbb{Q}$-vector spaces. $\Diamond$

We also see:

Lemma A.2.5. *Let $\mathbb{E}$ be an extension of $\mathbb{F}$. Let e_0 be any fixed element of E. Then $\mathcal{T}\colon \mathbb{E} \to \mathbb{E}$ defined by $\mathcal{T}(e) = ee_0$ is an $\mathbb{F}$-linear transformation.*

Example A.2.6. (a) Let $\mathbb{E} = \mathbb{F}(\sqrt{D})$ as in Example A.1.3, and let $\mathbb{E}$ have the basis $\mathcal{B} = \{1, \sqrt{D}\}$ of Example A.2.4. Let $e_0 = c + d\sqrt{D}$, and let $\mathcal{T}\colon \mathbb{E} \to \mathbb{E}$ by $\mathcal{T}(a + b\sqrt{D}) = (a + b\sqrt{D})(c + d\sqrt{D})$. Then the matrix of $\mathcal{T}$ in the basis $\mathcal{B}$ is

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} c & dD \\ d & c \end{bmatrix}.$$

(b) Now let $\mathcal{T}\colon \mathbb{E} \to \mathbb{E}$ by $\mathcal{T}(a + b\sqrt{D}) = a - b\sqrt{D}$. Then the matrix of $\mathcal{T}$ in the basis $\mathcal{B}$ is

$$[\mathcal{T}]_{\mathcal{B}} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

($\mathcal{T}$ is called *conjugation* in $\mathbb{E}$. In the case of $C = \mathbb{R}(i)$ this is just the familiar complex conjugation.) $\Diamond$

Obviously there is much more to say about extension fields, and linear algebra plays an important role in saying it. We refer the reader to our guide to further reading.

Polynomials

In this appendix we present and derive a number of results about polynomials we have used during this text.

B.1. Statement of results

We recall that $\mathbb{F}[x]$ denotes the set of polynomials with coefficients in the field $\mathbb{F}$. The degree of a nonzero polynomial is the highest power of x appearing in the polynomial; by convention the degree of the 0 polynomial is $-\infty$. A nonzero polynomial is *monic* if the coefficient of the highest power of x appearing in the polynomial is 1.

We begin with a nonstandard but useful definition, which will also establish some notation.

Definition B.1.1. Let $p(x) \in \mathbb{F}[x]$ be a nonzero polynomial, $p(x) = a_n x^n + \cdots + a_0$. Its *normalization* $\tilde{p}(x)$ is the monic polynomial $\tilde{p}(x) = (1/a_n)p(x)$. $\Diamond$

We have the division algorithm for polynomials.

Theorem B.1.2. *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{F}[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ with*

$$f(x) = g(x)q(x) + r(x) \quad \textit{and} \quad \deg r(x) < \deg g(x) \ \textit{or}\ r(x) = 0.$$

Theorem B.1.3. *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{F}[x]$, not both 0. Then there is a unique monic polynomial $h(x)$ of highest degree that divides both $f(x)$ and $g(x)$. Furthermore*:

(1) *There are polynomials $a(x)$ and $b(x)$ such that*

$$h(x) = f(x)a(x) + g(x)b(x).$$

(2) *Every polynomial that divides both $f(x)$ and $g(x)$ divides $h(x)$.*

Definition B.1.4. The polynomial $h(x)$ of Theorem B.1.2 is the *greatest common divisor* of $f(x)$ and $g(x)$, $h(x) = \gcd(f(x), g(x))$. $\Diamond$

Definition B.1.5. Two polynomials $f(x)$ and $g(x)$ in $\mathbb{F}[x]$, not both 0, are *relatively prime* if their gcd is 1. $\Diamond$

We have Euclid's lemma for polynomials.

Lemma B.1.6 (Euclid's lemma for polynomials)**.** *Let $a(x)$ divide the product $b(x)c(x)$. If $a(x)$ and $b(x)$ are relatively prime, then $a(x)$ divides $c(x)$.*

Corollary B.1.7. *Let $a(x)$ and $b(x)$ be relatively prime. If $a(x)$ divides $c(x)$ and $b(x)$ divides $c(x)$, then their product $a(x)b(x)$ divides $c(x)$.*

Corollary B.1.8. *Let $a(x)$ and $b(x)$ be relatively prime, and let $a(x)$ and $c(x)$ be relatively prime. Then $a(x)$ and $b(x)c(x)$ are relatively prime.*

Lemma B.1.9. *Let $f(x)$ and $g(x)$ be nonzero polynomials in $\mathbb{F}[x]$. Then there is a unique monic polynomial $k(x)$ of lowest degree that is a multiple of both $f(x)$ and $g(x)$. Furthermore, every polynomial that is a multiple of both $f(x)$ and $g(x)$ is a multiple of $k(x)$.*

Definition B.1.10. The polynomial $k(x)$ of Lemma B.1.9 is the *least common multiple* of $f(x)$ and $g(x)$, $k(x) = \operatorname{lcm}(f(x), g(x))$. $\Diamond$

Definition B.1.11. A nonconstant polynomial $f(x)$ is *irreducible* if $f(x)$ cannot be written as the product of two nonconstant polynomials $g(x)$ and $h(x)$. $\Diamond$

Lemma B.1.12. *Let $f(x)$ be an irreducible polynomial. If $f(x)$ divides the product $g(x)h(x)$, then $f(x)$ divides $g(x)$ or $f(x)$ divides $h(x)$.*

Remark B.1.13. Theorem B.1.3, Lemma B.1.6, Corollary B.1.7, Corollary B.1.8, Lemma B.1.9, and Lemma B.1.12 all are true for any finite number of polynomials, not just two. The proof is by using induction. (In fact, Theorem B.1.3 is true for any set of polynomials, but we will not need that fact here.) $\Diamond$

We then have unique factorization for polynomials.

Theorem B.1.14 (Unique factorization for polynomials)**.** *Let $p(x)$ be a nonzero polynomial. Then there is a unique constant c and unique irreducible monic polynomials $f_1(x), \dots, f_t(x)$ such that*

$$p(x) = cf_1(x) \cdots f_t(x).$$

Alternatively, there is a unique constant c, unique distinct irreducible polynomials $f_1(x), \dots, f_s(x)$, and unique positive integers $e_1, \dots, e_s$ such that

$$p(x) = cf_1(x)^{e_1} \cdots f_s(x)^{e_s}.$$

(*Here unique means unique up to the order of the factors.*)

Remark B.1.15. In case $p(x) = c$, a nonzero constant polynomial, then there are no factors $f_1(x), \dots, f_t(x)$ and we just have $p(x) = c$. $\Diamond$

Finally, suppose $\mathbb{F}$ is a subfield of the field $\mathbb{E}$. Then any polynomial in $\mathbb{F}[x]$ is a polynomial in $\mathbb{E}[x]$. We have a result that compares the situation in $\mathbb{F}[x]$ to the situation in $\mathbb{E}[x]$.

Theorem B.1.16. (1) *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{F}[x]$ with $g(x) \neq 0$. Then $g(x)$ divides $f(x)$ as polynomials in $\mathbb{F}[x]$ if and only if $g(x)$ divides $f(x)$ as polynomials in $\mathbb{E}[x]$.*

(2) *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{F}[x]$, not both 0. Then the* gcd *of $f(x)$ and $g(x)$ as polynomials in $\mathbb{F}[x]$ is equal to the* gcd *of $f(x)$ and $g(x)$ as polynomials in $\mathbb{E}[x]$. In particular, $f(x)$ and $g(x)$ are relatively prime in $\mathbb{F}[x]$ if and only if they are relatively prime in $\mathbb{E}[x]$.*

(3) *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{F}[x]$ with $f(x)$ irreducible. If $f(x)$ and $g(x)$ have a common nonconstant factor in $\mathbb{E}[x]$, then $f(x)$ divides $g(x)$ in $\mathbb{F}[x]$.*

B.2. Proof of results

Proof of Theorem B.1.2. First we prove existence, then we prove uniqueness. Let $f(x)$ have degree n and $g(x)$ have degree m. We prove this by induction on n, for any fixed m.

If $f(x) = 0$ or $n < m$, we have

$$f(x) = g(x)0 + f(x)$$

so we can choose $q(x) = 0$ and $r(x) = f(x)$.

Suppose the theorem is true for all polynomials of degree $< n$, and let $f(x)$ have degree $n \geq m$. If $f(x) = a_n x^n + \cdots$ and $g(x) = b_m x^m + \cdots$, then $f_1(x) = f(x) - (a_n/b_m)x^{n-m}g(x)$ has the coefficient of x^n equal to 0, so is either 0 or a polynomial of degree $< n$. Hence by the inductive hypothesis

$$f_1(x) = g(x)q_1(x) + r(x)$$

for some polynomial $q_1(x)$ and some polynomial $r(x)$ with $r(x) = 0$ or $\deg r(x) < m$. But then

$$f(x) = g(x)q(x) + r(x),$$

where $q(x) = (a_n/b_m)x^{n-m} + q_1(x)$, as claimed.

Now for uniqueness. Suppose $f(x) = g(x)q(x) + r(x)$ and $f(x) = g(x)q'(x) + r'(x)$ with $r(x) = 0$ or $\deg r(x) < \deg g(x)$, and with $r'(x) = 0$ or $\deg r'(x) < \deg g(x)$. Then $g(x)q(x) + r(x) = g(x)q'(x) + r'(x)$ so $g(x)(q(x) - q'(x)) = r'(x) - r(x)$. If $r'(x) \neq r(x)$, then the right-hand side of this equation is a nonzero polynomial of degree $< \deg g(x)$, and the left-hand side of this equation is a nonzero multiple of $g(x)$, so has degree $\geq \deg g(x)$, and that is impossible. Hence we must have $r'(x) = r(x)$, and then $q'(x) = q(x)$ as well. □

Proof of Theorem B.1.3. First suppose that one of the polynomials divides the other, say $g(x)$ divides $f(x)$. (Note this includes the case $f(x) = 0$.) Write $g(x) = b_m x^m + \cdots$. Then $h(x)$ is just the normalization of $g(x)$, and

$$h(x) = f(x)0 + g(x)(1/b_m).$$

Otherwise, let $f(x)$ have degree n. We proceed by induction on $k = \min(m, n) = \min(\deg f(x), \deg g(x))$. Reorder the polynomials, if necessary, so that $k = m$. By the division algorithm, we have

$$f(x) = g(x)q(x) + r(x),$$

where $r(x)$ has degree $j < m$, or $r(x) = 0$. If $r(x) = 0$, then $g(x)$ divides $f(x)$, and we have already handled that case. Suppose $r(x) \neq 0$. From the above equation, we see that any common divisor of $g(x)$ and $r(x)$ is a divisor of $f(x)$, and, rewriting it as $r(x) = f(x) - g(x)q(x)$, we see that any common divisor of $f(x)$ and $g(x)$ is a divisor of $r(x)$. Hence we see that $f(x)$ and $g(x)$, and $g(x)$ and $r(x)$, have exactly the same common divisors. But $j = \min(m, j) = \min(\deg g(x), \deg r(x)) < k$, so by the inductive hypothesis $g(x)$ and $r(x)$ have a gcd $h(x)$, so $h(x)$ is also a gcd of $f(x)$ and $g(x)$.

Also, by the inductive hypothesis, there are polynomials $c(x)$ and $d(x)$ with $h(x) = g(x)c(x) + r(x)d(x)$. But then

$$\begin{aligned} h(x) &= g(x)c(x) + r(x)d(x) \\ &= g(x)c(x) + (f(x) - g(x)q(x))d(x) \\ &= f(x)a(x) + g(x)b(x), \end{aligned}$$

where

$$a(x) = d(x), \quad b(x) = c(x) - q(x)d(x).$$

Also, from the equation $h(x) = f(x)a(x) + g(x)b(x)$, we see that every polynomial that divides both $f(x)$ and $g(x)$ divides $h(x)$.

Finally, suppose we had two gcds $h(x)$ and $h'(x)$. Then $h(x)$ and $h'(x)$ would be two monic polynomials, each of which divides the other. Thus we must have $h'(x) = h(x)$, i.e., $h(x)$ is unique. □

Proof of Lemma B.1.6. Since $a(x)$ and $b(x)$ are relatively prime, we may write

$$1 = a(x)s(x) + b(x)t(x)$$

for some polynomials $s(x)$ and $t(x)$. Multiplying by $c(x)$, we have

$$c(x) = a(x)c(x)s(x) + b(x)c(x)t(x).$$

Now $a(x)$ certainly divides the first term on the right-hand side, and, since we are assuming $a(x)$ divides the product $b(x)c(x)$, it divides the second term as well. Hence $a(x)$ divides their sum, which is $c(x)$. □

Proof of Corollary B.1.7. Since $b(x)$ divides $c(x)$, we may write $c(x) = b(x)d(x)$. Then $a(x)$ divides $b(x)d(x)$ and $a(x)$ is relatively prime to $b(x)$, so $a(x)$ divides $d(x)$, i.e., $d(x) = a(x)e(x)$. But then $c(x) = a(x)b(x)e(x)$, i.e., $a(x)b(x)$ divides $c(x)$. □

Proof of Corollary B.1.8. Since $a(x)$ and $b(x)$ are relatively prime, we may write

$$1 = a(x)d(x) + b(x)e(x)$$

and since $a(x)$ and $c(x)$ are relatively prime, we may write

$$1 = a(x)f(x) + c(x)g(x).$$

Multiplying, we have

$$\begin{aligned} 1 &= (a(x)d(x) + b(x)e(x))(a(x)f(x) + c(x)g(x)) \\ &= a(x)s(x) + (b(x)c(x))t(x), \end{aligned}$$

where

$$s(x) = d(x)a(x)f(x) + d(x)c(x)g(x) + b(x)e(x)f(x), \quad t(x) = e(x)g(x);$$

thus $\gcd(a(x), b(x)c(x))$ divides 1 and hence must equal 1. □

Proof of Lemma B.1.9. There is certainly some monic polynomial that is a common multiple of $f(x)$ and $g(x)$, namely the normalization of their product $f(x)g(x)$. Hence there is such a polynomial $k(x)$ of lowest degree. Let $m(x)$ be any common multiple of $f(x)$ and $g(x)$. Then

$$m(x) = k(x)q(x) + r(x)$$

with $r(x) = 0$ or $\deg r(x) < \deg k(x)$. But we see from this equation that $r(x)$ is also a common multiple of $f(x)$ and $g(x)$. But $k(x)$ is a multiple of lowest degree, so we must have $r(x) = 0$ and $k(x)$ divides $m(x)$.

Again, $k(x)$ is unique, as if we had another lcm $k'(x)$, $k(x)$ and $k'(x)$ would divide each other so would have to be equal. □

Proof of Lemma B.1.12. Suppose that $f(x)$ divides $g(x)h(x)$.

Let $e(x) = \gcd(f(x), g(x))$. Then, in particular, $e(x)$ is a divisor of $f(x)$. But $f(x)$ is irreducible, so that means either $e(x) = 1$ or $e(x) = \tilde{f}(x)$, the normalization of $f(x)$. If $e(x) = \tilde{f}(x)$, then $\tilde{f}(x)$, and hence $f(x)$, divides $g(x)$. If $e(x) = 1$, then $f(x)$ and $g(x)$ are relatively prime, so $f(x)$ divides $g(x)$. □

Proof of Theorem B.1.14. First we show existence of the factorization, then uniqueness.

Existence: We proceed by induction on $n = \deg p(x)$.

If $n = 0$, then $p(x) = a_0$, and we are done.

Assume the theorem is true for all polynomials of degree $< n$, and let $p(x)$ have degree n. If $p(x)$ is irreducible, then $p(x) = a_n\tilde{p}(x)$ (where a_n is the coefficient of x^n in $p(x)$) and we are done.

Otherwise, $p(x) = s(x)t(x)$ with $s(x)$ and $t(x)$ polynomials of lower degree. But then, by the inductive hypothesis,

$$\begin{aligned} s(x) &= cf_1(x)\cdots f_k(x), \\ t(x) &= dg_1(x)\cdots g_l(x) \end{aligned}$$

for irreducible monic polynomials $f_1(x), \ldots, g_l(x)$, and then

$$p(x) = (cd)f_1(x)\cdots f_k(x)g_1(x)\cdots g_l(x),$$

and by induction we are done.

Uniqueness. Again we proceed by induction on the degree of $p(x)$. Suppose we have two factorization of $p(x)$ into irreducibles,

$$\begin{aligned} p(x) &= cf_1(x)\cdots f_k(x) \\ &= dg_1(x)\cdots g_l(x). \end{aligned}$$

Clearly $c = d$ (as this is the coefficient of the highest power of x in $p(x)$).

Now the irreducible polynomial $f_1(x)$ divides the product $g_1(x)\cdots g_l(x)$, so by Lemma B.1.12 (and Remark B.1.13) must divide one of the factors; reordering if necessary we may assume that $f_1(x)$ divides $g_1(x)$. But $g_1(x)$ is irreducible, so we must have $g_1(x) = f_1(x)$. But then, setting $q(x) = p(x)/f_1(x) = p(x)/g_1(x)$, we have

$$\begin{aligned} q(x) &= cf_2(x) \cdots f_k(x) \\ &= dg_2(x) \cdots g_l(x) \end{aligned}$$

so, by the inductive hypothesis, we must have $l = k$, and after possible reordering, $g_2(x) = f_2(x), \ldots, g_k(x) = f_k(x)$, and by induction we are done. □

Proof of Theorem B.1.16. (1) By the division algorithm, in $\mathbb{F}[x]$, we have

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

with $q(x)$ a polynomial in $\mathbb{F}[x]$, and $r(x)$ a polynomial in $\mathbb{F}[x]$, with $r(x) = 0$ or $\deg r(x) < \deg g(x)$, and this expression is *unique* as polynomials in $\mathbb{F}[x]$.

But we also have the division algorithm in $\mathbb{E}[x]$, yielding

$$f(x) = g(x)q'(x) + r'(x)$$

with $q'(x)$ and $r'(x)$ polynomials in $\mathbb{E}[x]$ with $r'(x) = 0$ or $\deg r'(x) < \deg g(x)$, and this expression is also *unique* as polynomials in $\mathbb{E}[x]$. But the first expression $f(x) = g(x)q(x) + r(x)$ *is* an expression in $\mathbb{E}[x]$ (since every polynomial in $\mathbb{F}[x]$ is a polynomial in $\mathbb{E}[x]$) so by uniqueness in $\mathbb{E}[x]$ we must have $q'(x) = q(x)$ and $r'(x) = r(x)$.

In particular, $r(x) = 0$, i.e., $g(x)$ divides $f(x)$ in $\mathbb{F}[x]$, if and only if $r'(x) = 0$, i.e., $g(x)$ divides $f(x)$ in $\mathbb{E}[x]$.

(2) Let $h(x)$ be the gcd of $f(x)$ and $g(x)$ as polynomials in $\mathbb{F}[x]$, and let $h'(x)$ be the gcd of $f(x)$ and $g(x)$ as polynomials in $\mathbb{E}[x]$. Then on the one hand $h(x)$ is a polynomial in $\mathbb{E}[x]$ that is a common divisor of $f(x)$ and $g(x)$, so $h(x)$ divides $h'(x)$. But on the other hand, we have

$$h(x) = f(x)a(x) + g(x)b(x)$$

and $h'(x)$ divides both $f(x)$ and $g(x)$, so $h'(x)$ divides $h(x)$. Hence $h(x)$ and $h'(x)$ must be equal.

(3) Let $h(x)$ be the gcd of $f(x)$ and $g(x)$ in $\mathbb{F}[x]$, and let $h'(x)$ be the gcd of $f(x)$ and $g(x)$ in $\mathbb{E}[x]$. As we have just seen, $h(x) = h'(x)$.

Now $f(x)$ is irreducible, and $h(x)$ divides $f(x)$, so either $h(x) = 1$ or $h(x) = f(x)$. But by assumption $h'(x) \neq 1$. Hence $h(x) \neq 1$, so $h(x) = f(x)$ and then $f(x)$ divides $g(x)$ in $\mathbb{F}[x]$. □

Normed vector spaces and questions of analysis

In this appendix we give a brief introduction to some of the issues that arise when doing analysis on normed vector spaces. Our objective here is simply to show that there are a variety of interesting questions, and to give some examples that illustrate them.

C.1. Spaces of sequences

We recall that we defined a normed vector space in Definition 10.1.17.

Definition C.1.1. Let $(V, \|\cdot\|)$ be a normed vector space. A sequence of vectors $x_1, x_2, \ldots$ in V is a *Cauchy sequence* if for every $\varepsilon > 0$ there exists an N such that $\|x_m - x_n\| < \varepsilon$ whenever $m,\ n > N$. $\Diamond$

Definition C.1.2. Let $(V, \|\cdot\|)$ be a normed vector space. A sequence of vectors $x_1, x_2, \ldots$ in V *converges* to a vector x in V if for every $\varepsilon > 0$ there exists an N such that $\|x - x_n\| < \varepsilon$ whenever $n > N$.

A series of vectors $w_1, w_2, \ldots$ has *sum* v, i.e., $v = \sum_i^\infty w_i$, if its sequence of partial sums $x_1, x_2, \ldots$ defined by $x_i = \sum_{j=1}^i w_j$ converges to v. $\Diamond$

First let us see how different norms on the same vector space V give us different notions of Cauchy sequences and convergent sequences.

Example C.1.3. (a) Let $V = {}^t\mathbb{F}^\infty$ and define a norm $\|\cdot\|$ on V by

$$\|[a_1, a_2, \ldots]\| = \sum_{i=1}^\infty |a_i|.$$

Let $e_i = [0, 0, \ldots, 1, 0, \ldots]$, with the 1 in position i. Then the sequence $e_1, e_2, \ldots$ is not a Cauchy sequence.

(b) Let $V = {}^t\mathbb{F}^\infty$ and define a norm $\|\cdot\|$ on V by

$$\|[a_1, a_2, \ldots]\| = \sum_{i=1}^{\infty} |a_i|/2^i.$$

Then the sequence $e_1, e_2, \ldots$ is a Cauchy sequence, and converges to $[0, 0, \ldots]$. $\Diamond$

Next let us see that in general there is a difference between Cauchy sequences and convergent sequences.

Example C.1.4. (a) Let V be the subspace of ${}^t\mathbb{F}^{\infty\infty}$ defined by

$$V = \{[a_1, a_2, \ldots] \mid \{|a_i|\} \text{ is bounded}\}.$$

Observe that $W = {}^t\mathbb{F}^\infty$ is a subspace of V. We give V, and W, the norm

$$\|[a_1, a_2, \ldots]\| = \sup(\{|a_i|\}).$$

Let f_i be the vector in W given by $f_i = \sum_{j=1}^{i} e_i/2^i$. Then the sequence $\{f_1, f_2, \ldots\}$ is a Cauchy sequence in W, but does not converge in W.

(b) The same sequence $\{f_1, f_2, \ldots\}$ is a Cauchy sequence in V, and converges in V to the vector $[a_1, a_2, \ldots]$ with $a_i = 1/2^i$ for each i. $\Diamond$

Definition C.1.5. Let $(V, \|\cdot\|)$ be a normed vector space, and let W be a subspace of V. Then W is *dense* in V if for every v in V and every $\varepsilon > 0$ there is a w in W with $\|v - w\| < \varepsilon$. $\Diamond$

Example C.1.6. Let V and W be as in Example C.1.4 but now with norm

$$\|[a_1, a_2, \ldots]\| = \sum_{i=1}^{\infty} |a_i|/2^i.$$

Then W is a dense subspace of V. $\Diamond$

We have a whole family of standard spaces:

Definition C.1.7. Let $p \geq 1$ be a real number. We let $(\ell^p, \|\cdot\|)$ be the normed vector space defined by

$$\ell^p = \{[a_1, a_2, \ldots] \in {}^t\mathbb{F}^{\infty\infty} \mid \sum_{i=1}^{\infty} |a_i|^p < \infty\}$$

with norm

$$\|[a_1, a_2, \ldots]\| = \left(\sum_{i=1}^{\infty} |a_i|^p\right)^{1/p}.$$

We let $(\ell^\infty, \|\cdot\|)$ be the normed vector space defined by

$$\ell^\infty = \{[a_1, a_2, \ldots] \in {}^t\mathbb{F}^{\infty\infty} \mid \{|a_i|\} \text{ is bounded}\}$$

with norm

$$\|[a_1, a_2, \ldots]\| = \sup(\{|a_i|\}).$$ $\Diamond$

In one case we have more structure on ℓ^p.

Lemma C.1.8. *For $v = [a_1, a_2, \ldots]$ and $w = [b_1, b_2, \ldots]$ in ℓ^2, define $\langle v, w\rangle$ by*

$$\langle v, w\rangle = \langle [a_1, a_2, \ldots], [b_1, b_2, \ldots]\rangle = \sum_i a_i \overline{b_i}.$$

Then $\langle , \rangle$ is an inner product on V and $\|v\| = \sqrt{\langle v, v\rangle}$ agrees with the definition of $\|\cdot\|$ in Definition C.1.5 *above for $p = 2$.*

We now have a standard definition.

Definition C.1.9. Let $(V, \|\cdot\|)$ be a normed vector space in which every Cauchy sequence converges. Then V is *complete.* A complete normed vector space is called a *Banach space.* A complete inner product space is called a *Hilbert space.* $\Diamond$

We then have:

Theorem C.1.10. *For $p \geq 1$ or $p = \infty$, the space ℓ^p is complete. Thus, ℓ^p is a Banach space for every $p \geq 1$ or $p = \infty$, and ℓ^2 is a Hilbert space.*

C.2. Spaces of functions

One very important direction in analysis is to study how well general functions can be approximated by a given set of functions. This kind of question fits naturally in our framework. Let us set this up.

Definition C.2.1. Let $(V, \langle , \rangle)$ be an inner product space and consider an orthogonal set of nonzero vectors $\mathcal{B} = \{v_n\}_{n\in\mathcal{N}}$, where $\mathcal{N}$ is some indexing set, in V. For any v in V, let

$$a_n = \langle v, v_n\rangle / \|v_n\|^2.$$

Then $\{a_n\}_{n\in\mathcal{N}}$ are the *Fourier coefficients* of v with respect to $\mathcal{B}$. $\Diamond$

Let W be the subspace of V with basis $\mathcal{B}$. (Note that $\mathcal{B}$ is automatically linearly independent, by Corollary 10.1.11.) If v is in W, then v is a linear combination of elements of $\mathcal{B}$, and, remembering that linear combinations are finite, only finitely many a_n are nonzero. In this case $v = \sum_n a_n v_n$ (Corollary 10.1.12). But if not, there will be infinitely many nonzero a_n and we have an infinite series $\sum_n a_n v_n$ which we may hope converges to v.

Now let us look at particular cases of this set-up.

Lemma C.2.2. *Let $\mathcal{C}^0([0, 1])$ be the vector space of continuous complex-valued functions of the real variable x for x in the interval* $[0, 1]$.

(a) *This space has an inner product $\langle , \rangle_2$ given by*

$$\langle f(x), g(x)\rangle_2 = \int_0^1 f(x)\overline{g(x)}dx$$

which gives a norm $\|\cdot\|_2$.

(b) *This space has a different norm $\|\cdot\|_\infty$ given by*

$$\|f(x)\|_\infty = \sup_{x\in[0,1]} |f(x)|.$$

Note that in the norm $\|\cdot\|_\infty$, convergence in $\mathcal{C}[0,1]$ is uniform convergence. We recall that uniform convergence implies pointwise convergence.

We observe that $\mathcal{C}^0([0,1])$ has a subspace $\mathcal{C}^1([0,1])$ that consists of complex-valued functions of the real variable x that are continuously differentiable at all points $x \in [0,1]$, with the same norms.

We choose our notation below to emphasize the points we want to make here, but it is not standard.

Definition C.2.3. Let $V^0 = \mathcal{C}^0([0,1])$ with inner product $\langle , \rangle_2$ and let $V^1 = \mathcal{C}^1([0,1])$. Let $\tilde{V}^0 = \{f(x) \in V^0 \,|\, f(1) = f(0)\}$, and let $\tilde{V}^1 = \{f(x) \in \tilde{V}^0 \,|\, f'(1) = f'(0)\}$.

(a) Let $\mathcal{B}_{\mathrm{poly}} = \{P_n^*(x) \,|\, n = 0, 1, \ldots\}$, where $\{P_n^*(x)\}$ are the shifted Legendre polynomials of Remark 10.2.20, and let $W_{\mathrm{poly}} = \mathrm{Span}_{\mathbb{C}}(\mathcal{B}_{\mathrm{poly}})$. (Here $\mathrm{Span}_{\mathbb{C}}$ means we are taking all linear combinations with complex coefficients, so W_{poly} is a complex subspace of the complex vector space V.) Of course, W_{poly} is just the vector space of all complex polynomials, regarded as functions on $[0,1]$.

(b) Let $\mathcal{B}_{\mathrm{trig}} = \{e^{2n\pi i x} \,|\, n \text{ an integer}\}$, an orthonormal set, and let $W_{\mathrm{trig}} = \mathrm{Span}_{\mathbb{C}}(\mathcal{B}_{\mathrm{trig}})$. The elements of W are called *trigonometric polynomials*, although they are not polynomials in the usual sense. (The connection with trigonometry comes from Euler's formula $e^{i\theta} = \cos(\theta) + i\sin(\theta)$.) $\Diamond$

Theorem C.2.4. (a) *Let $V = V^0$, and let $\mathcal{B} = \mathcal{B}_{\mathrm{poly}} = \{b_0(x), b_1(x), \ldots\}$. Let $f(x) \in V$, and let $\{a_n\}$ be the Fourier coefficients of $f(x)$ with respect to $\mathcal{B}$. Then*

$$f(x) = \sum_{n=0}^{\infty} a_n b_n(x) \text{ in the } \|\cdot\|_2 \text{ norm,}$$

i.e., the sequence $\sum_{k=0}^{n} a_k b_k(x)$ converges to $f(x)$ in V.

(b) *Let $V = \tilde{V}^0$, and let $\mathcal{B} = \mathcal{B}_{\mathrm{trig}} = \{\ldots, b_{-1}(x), b_0(x), b_1(x), \ldots\}$. Let $f(x) \in V$, and let $\{a_n\}$ be the Fourier coefficients of $f(x)$ with respect to $\mathcal{B}$. Then*

$$f(x) = \sum_{n=i\infty}^{\infty} a_n b_n(x) \text{ in the } \|\cdot\|_2 \text{ norm,}$$

i.e., the sequence $\sum_{k=-n}^{n} a_k b_k(x)$ converges to $f(x)$ in V.

But in fact more is true!

Theorem C.2.5. *In the situation of Theorem* C.2.4*:*

(a1) *If $f(x) \in V^1$ and $\mathcal{B} = \mathcal{B}_{\mathrm{poly}}$, then*

$$f(x) = \sum_{n=0}^{\infty} a_n b_n(x) \text{ in the } \|\cdot\|_\infty \text{ norm,}$$

i.e., the sequence $\sum_{k=0}^{n} a_k b_k(x)$ converges to $f(x)$ uniformly on $[0,1]$.

(b1) *If $f(x) \in \tilde{V}^1$ and $\mathcal{B} = \mathcal{B}_{\mathrm{trig}}$, then*

$$f(x) = \sum_{n=-\infty}^{\infty} a_n b_n(x) \text{ in the } \|\cdot\|_\infty \text{ norm,}$$

i.e., the sequence $\sum_{k=-n}^{n} a_k b_k(x)$ *converges to* $f(x)$ *uniformly on* $[0,1]$.

(a2) *If* $f(x) \in V^0$ *and* $\mathcal{B} = \mathcal{B}_{\text{poly}}$*, then for any* $\varepsilon > 0$ *there is a nonnegative integer* N *and a set* $\{a'_n\}_{0 \le n \le N}$ *such that*

$$\|f(x) - \sum_{n=0}^{N} a'_n b_n(x)\|_\infty < \varepsilon.$$

(b2) *If* $f(x) \in \tilde{V}^0$ *and* $\mathcal{B} = \mathcal{B}_{\text{trig}}$*, then for any* $\varepsilon > 0$ *there is a nonnegative integer* N *and a set* $\{a'_n\}_{-N \le n \le N}$ *such that*

$$\|f(x) - \sum_{n=-N}^{N} a'_n b_n(x)\|_\infty < \varepsilon.$$

Remark C.2.6. Note that Theorem C.2.4 says that W_{poly} is dense in V^0 in the $\|\cdot\|_2$ norm, and that W_{trig} is dense in $\tilde{V}^0$ in the $\|\cdot\|_2$ norm, and Theorem C.2.5 says that W_{poly} is dense in V^0 in the $\|\cdot\|_\infty$ norm, and that W_{trig} is dense in $\tilde{V}^0$ in the $\|\cdot\|_\infty$ norm. $\Diamond$

As you can see, there are subtle questions of analysis here, and these results can be generalized far beyond spaces of continuous, or continuously differentiable, functions. Questions about approximating quite general functions by trigonometric polynomials are at the heart of traditional *Fourier analysis*. We leave all of this for the interested reader to investigate further. (We caution the reader that, in the language of Fourier analysis, a maximal orthogonal set $\mathcal{B}$ of nonzero vectors in an inner product space V is often called an orthogonal basis of V, although it is *not* a basis of V in the sense of linear algebra, unless $\mathcal{B}$ is finite.)

Appendix D

A guide to further reading

In this appendix we present a short guide to books concerning aspects of linear algebra and its applications not treated here.

A wide-ranging book on linear algebra, covering both topics treated here and many topics not treated here, but from a rather more analytic than algebraic viewpoint is:

• Harry Dim, *Linear Algebra in Action*, second edition, American Mathematical Society, 2013.

Two books dealing with questions of numerical analysis in linear algebra are:

• Lloyd N. Trefethen and David Bau III, *Numerical Linear Algebra*, Society for Industrial and Applied Mathematics, 1997.

• James W. Demmel, *Applied Numerical Linear Algebra*, Society for Industrial and Applied Mathematics, 1997.

A third book going further into numerical methods is:

• Uri M. Ascher and Chen Grief, *A First Course in Numerical Methods*, Society for Industrial and Applied Mathematics, 2011.

A book that, among other things, lays the foundation for the study of normed vector spaces essential to analysis (the "L^p spaces") is:

• Edwin Hewitt and Karl Stromberg, *Real and Abstract Analysis*, Springer, 1965.

A book that presents the foundation of Hilbert spaces and operators on them is:

• Paul R. Halmos, *Introduction to Hilbert Space and the Theory of Spectral Multiplicity*, second edition, Dover Publications, 2017 (reprint of Chelsea, 1957).

Two books on Fourier analysis that build on linear algebra are:

• T. W. Körner, *Fourier Analysis*, Cambridge University Press, 1988.

• Gerald B. Folland, *Fourier Analysis and its Applications*, American Mathematical Society, 2009.

In signal processing, both the trigonometric polynomials of classical Fourier analysis and “wavelets”, a different orthonormal set, are commonly used (with each approach having its advantages and disadvantages). Two books here are:

• Michael W. Frazier, *An Introduction to Wavelets through Linear Algebra*, Springer, 1999.

• Roe W. Goodman, *Discrete Fourier and Wavelet Transforms*, World Scientific, 2016.

There are extensive applications of linear algebra and matrix theory in statistics. Two books that deal with this are:

• Franklin A. Graybill, *Matrices with Applications in Statistics*, Wadsworth, 1969.

• R. B. Bapat, *Linear Algebra and Linear Methods*, third edition, Springer, 2012.

Quantum theory is a “linear” theory, and the mathematical basis of quantum theory is the study of linear operators in Hilbert space. A book that makes this clear is:

• Keith Hannabuss, *An Introduction to Quantum Theory*, Oxford University Press, 1997.

A book that unifies many problems in optimization theory under a linear algebra framework is:

• David G. Luenberger, *Optimization by Vector Space Methods*, Wiley, 1969.

Linear algebra can be used to great effect in Galois theory, which is the study of algebraic extensions of fields. Two books that adopt this approach are:

• Emil Artin, *Galois Theory*, second edition, Dover Publications, 1988 (reprint of Notre Dame University Press, 1944).

• Steven H. Weintraub, *Galois Theory*, second edition, Springer, 2009.

Modules are a generalization of vector spaces, and they are treated in:

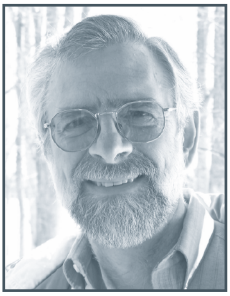
• William A. Adkins and Steven H. Weintraub, *Algebra: An Approach via Module Theory*, Springer, 1992.

Finally, we have restricted our computational examples and exercises here to ones that could reasonably be done by hand computation (matrices that are not too large, and answers that mostly, and almost always in Part I, have integer entries). A certain amount of hand computation breeds familiarity and gives insight. But the sort of “heavy-duty” computations done in applications are best done by (or can only be done by) computer, and the standard mathematics packages, Maple, MATLAB, and Mathematica, all have routines to do them. We simply refer the reader to the documentation for those packages.

Index

Published Titles in This Series

42 **Steven H. Weintraub,** Linear Algebra for the Young Mathematician, 2019
40 **Heiko Knospe,** A Course in Cryptography, 2019
39 **Andrew D. Hwang,** Sets, Groups, and Mappings, 2019
38 **Mark Bridger,** Real Analysis, 2019
37 **Mike Mesterton-Gibbons,** An Introduction to Game-Theoretic Modelling, Third Edition, 2019
36 **Cesar E. Silva,** Invitation to Real Analysis, 2019
35 **Álvaro Lozano-Robledo,** Number Theory and Geometry, 2019
34 **C. Herbert Clemens,** Two-Dimensional Geometries, 2019
33 **Brad G. Osgood,** Lectures on the Fourier Transform and Its Applications, 2019
32 **John M. Erdman,** A Problems Based Course in Advanced Calculus, 2018
31 **Benjamin Hutz,** An Experimental Introduction to Number Theory, 2018
30 **Steven J. Miller,** Mathematics of Optimization: How to do Things Faster, 2017
29 **Tom L. Lindstrøm,** Spaces, 2017
28 **Randall Pruim,** Foundations and Applications of Statistics: An Introduction Using R, Second Edition, 2018
27 **Shahriar Shahriari,** Algebra in Action, 2017
26 **Tamara J. Lakins,** The Tools of Mathematical Reasoning, 2016
25 **Hossein Hosseini Giv,** Mathematical Analysis and Its Inherent Nature, 2016
24 **Helene Shapiro,** Linear Algebra and Matrices, 2015
23 **Sergei Ovchinnikov,** Number Systems, 2015
22 **Hugh L. Montgomery,** Early Fourier Analysis, 2014
21 **John M. Lee,** Axiomatic Geometry, 2013
20 **Paul J. Sally, Jr.,** Fundamentals of Mathematical Analysis, 2013
19 **R. Clark Robinson,** An Introduction to Dynamical Systems: Continuous and Discrete, Second Edition, 2012
18 **Joseph L. Taylor,** Foundations of Analysis, 2012
17 **Peter Duren,** Invitation to Classical Analysis, 2012
16 **Joseph L. Taylor,** Complex Variables, 2011
15 **Mark A. Pinsky,** Partial Differential Equations and Boundary-Value Problems with Applications, Third Edition, 1998
14 **Michael E. Taylor,** Introduction to Differential Equations, 2011
13 **Randall Pruim,** Foundations and Applications of Statistics, 2011
12 **John P. D'Angelo,** An Introduction to Complex Analysis and Geometry, 2010
11 **Mark R. Sepanski,** Algebra, 2010
10 **Sue E. Goodman,** Beginning Topology, 2005
9 **Ronald Solomon,** Abstract Algebra, 2003
8 **I. Martin Isaacs,** Geometry for College Students, 2001
7 **Victor Goodman and Joseph Stampfli,** The Mathematics of Finance, 2001
6 **Michael A. Bean,** Probability: The Science of Uncertainty, 2001
5 **Patrick M. Fitzpatrick,** Advanced Calculus, Second Edition, 2006
4 **Gerald B. Folland,** Fourier Analysis and Its Applications, 1992
3 **Bettina Richmond and Thomas Richmond,** A Discrete Transition to Advanced Mathematics, 2004
2 **David Kincaid and Ward Cheney,** Numerical Analysis: Mathematics of Scientific Computing, Third Edition, 2002
1 **Edward D. Gaughan,** Introduction to Analysis, Fifth Edition, 1998



Linear Algebra for the Young Mathematician is a careful, thorough, and rigorous introduction to linear algebra. It adopts a conceptual point of view, focusing on the notions of vector spaces and linear transformations, and it takes pains to provide proofs that bring out the essential ideas of the subject. It begins at the beginning, assuming no prior knowledge of the subject, but goes quite far, and it includes many topics not usually treated in introductory linear algebra texts, such as Jordan canonical form and the spectral theorem. While it concentrates on the finite-dimensional case, it treats the infinite-dimensional case as well. The book illustrates the centrality of linear algebra by providing numerous examples of its application within mathematics. It contains a wide variety of both conceptual and computational exercises at all levels, from the relatively straightforward to the quite challenging.

Readers of this book will not only come away with the knowledge that the results of linear algebra are true, but also with a deep understanding of why they are true.

ISBN 978-1-4704-5084-7

9 781470 450847

AMSTEXT/42

For additional information and updates on this book, visit
www.ams.org/bookpages/amstext-42

AMS
www.ams.org

This series was founded by the highly respected mathematician and educator, Paul J. Sally, Jr.