MM MODULAR MATHEMATICS

Matrices & Quadratic Forms

John Bowers

BOWERS MATRICES & QUADRATIC FORMS

ARNOLD

ARNOLD

Other titles in this series

Linear Algebra
Reg Allenby

Introduction to Non-Linear Systems
John Berry

Discrete Mathematics
Amanda Chetwynd and Peter Diggle

Particle Mechanics
Chris Collinson and Tom Roper

Mathematical Modelling
John Berry and Ken Houston

Ordinary Differential Equations
William Cox

Vector Calculus
William Cox

Vectors in Two or Three Dimensions
Ann Hirst

Numbers, Sequences and Series
Keith Hirst

Groups
Camilla Jordan and David Jordan

Analysis
Ekkehard Kopp

Statistics
A Mayer and A M Sykes

Probability
John McColl

Calculus and Ordinary Differential Equations
David Pearson

Modular Mathematics Series

Matrices and Quadratic Forms

John Bowers

Formerly University of Leeds

A member of the Hodder Headline Group
LONDON

First published in Great Britain in 2000 by
Arnold, member of the Hodder Headline Group,
338 Euston Road, London NW1 3BH

http://www.arnoldpublishers.com

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN 0 340 69138 7

1 2 3 4 5 6 7 8 9 10

Commissioning Editor: Liz Gooster
Production Editor: James Rabson
Production Controller: Iain McWilliams
Cover Design: Terry Griffiths

Typeset in 10/13 Times by Heather FitzGibbon, Christchurch, Dorset.
Printed and bound in Great Britain by Redwood Books, Trowbridge, Wiltshire.

Success for all that we create
Depends on our posterity,
And so this book I dedicate
To Austin, Rose and Natalie.

Contents

Series Preface

This series is designed particularly, but not exclusively, for students reading degree programmes based on semester-long modules. Each text will cover the essential core of an area of mathematics and lay the foundation for further study in that area. Some texts may include more material than can be comfortably covered in a single module, the intention there being that the topics to be studied can be selected to meet the needs of the student. Historical contexts, real-life situations, and linkages with other areas of mathematics and more advanced topics are included. Traditional worked examples and exercises are augmented by more open-ended exercises and tutorial problems suitable for group work or self-study. Where appropriate, the use of computer packages is encouraged. The first-level texts assume only the A-level core curriculum.

Professor Chris D. Collinson
Dr Johnston Anderson
Mr Peter Holmes

Preface

This book is designed as a textbook for a second course in linear algebra, although it obviously has other uses. As there are few such textbooks most students have previously had to use parts of books aimed at more advanced students, which discuss the topics too briefly. Fortunately, I have taught second courses to students with varying interests over more than 30 years, and appreciate that there is a core of material which appears in almost all second linear algebra courses. This material appears in Chapters 6 to 13 of this book, which is intended to be a simpler alternative to those more advanced texts. But as this book is for a second course, it is necessary to explain the book's starting point as well as the kind of problems in linear algebra the book is trying to solve. As these are important for the use of the book, they are fully explained in Chapter 1, which outlines the contents. Chapter 1 also introduces a few ideas which are used throughout the book, as well as applying linear algebra to World Cup football.

One way of indicating the background knowledge needed to understand this book is to refer the reader to a textbook for a first course in linear algebra. Dr. R.B.J.T. Allenby's *Linear Algebra* is a textbook for such a course and is part of this series (*Modular Mathematics*). The choice makes sense because this book was written with the help of Reg Allenby, who read an earlier version and made many valuable, detailed comments. It is a pleasure to thank him for all the help he has given, as well as to recall all the jokes we have shared on the subject while the work was in progress, particularly concerning the construction of complex sentences. Naturally, we also agreed that the book should contain no jokes, especially puns. This is because linear algebra should always move to its objective by the shortest route.

My thanks are also due to a procession of members of Edward Arnold who have helped with the writing of this book. The first member was John Roberts, with whom I discussed a rather different book on linear algebra which provided many of the ideas for this book. Especially I wish to thank Nicki Dennis who originally commissioned this book and who has made valuable efforts to help the project to its conclusion. I also wish to thank Richard Leigh for his comments on the final manuscript and James Rabson for guiding the book through printing.

JFB

Henfield, Sussex, 2000

1 • Questions about Matrices and Quadratic Forms

Outline

In this chapter the main problems considered in this book are explained and the background knowledge needed to use the book is summarized.

Introduction

This book covers the contents of a typical second course in linear algebra, together with some of the common variations on such a course. This means that a knowledge of the core contents of a typical first course in linear algebra will be assumed. Although it is not necessary to use that particular book, there will be references to results and proofs in the textbook for a first linear algebra course in the *Modular Mathematics* series, which is *Linear Algebra* by R.B.J.T. Allenby.

In order to read this book it is necessary to know about the basic operations of matrices, and these will not be revised. However, Chapter 2 provides some reminders of this work when it introduces an easy generalization of the algebra of matrices, in which matrices are the matrix elements in the useful notation of **partitioned matrices**. Also, because the notions of linear transformations and quadratic forms do not always occur in first courses, they will be introduced in Chapters 4 and 12. The broad conclusion of a first course in linear algebra is that a knowledge of the structure of vector spaces is the key to understanding linear equations and their related algebra, therefore our title of *Matrices and Quadratic Forms* suggests a step backwards. This illusion is caused by the fact that the results on vector spaces in the earlier course are sufficient for our purposes, with the consequence that our title refers to the subjects of our further study. But, because there are several different ways of introducing vector spaces, Chapter 3 is devoted to unifying these approaches and Chapter 4 includes a few new results concerning finite-dimensional vector spaces. In fact, the theme of this book is the search for simplified forms of matrices and quadratic forms which can be used in special contexts. In some uses of matrices no simplification is possible, such as when the matrix records results of some kind, but in many cases where the matrices are used in mathematical processes they can often be assumed to be in some simple form. We can clarify this distinction and illustrate the resulting problems by looking at one example of each type of application of matrices.

Example 1

Matrices are used to display the records of football clubs by means of a league table, usually displayed in order of merit as in the following table, which belongs to qualifying Group 642 for the 1995 World Cup:

	P	W	D	L	F	A	Pts
Euphoria	3	2	1	0	7	2	7
Utopia	3	1	1	1	9	2	4
Shangrila	4	1	1	2	7	13	4
Atlantis	4	1	1	2	4	10	4

In this table the first column, headed P, contains the number of games played by the team, and this is followed by the number won (W), the number drawn (D), the number lost (L), the number of goals scored (F), the number of goals conceded (A) and finally the number of points obtained (Pts). The rows are ordered by the number of points scored. If two teams have the same number of points, the one with a greater goal difference, that is the value of F – A, has the higher place. If the goal difference is also equal, the team which has scored more goals has the higher place. This is not quite a matrix because the names of the clubs are needed to interpret it, but it can be converted into a matrix by replacing each name by the number of the team in the alphabetical list. In this matrix, which we can call the **merit-order matrix**, the first column contains the number for the club in the alphabetical list and the other columns are the same as before.

$$\mathbf{M}=\begin{pmatrix} 2 & 3 & 2 & 1 & 0 & 7 & 2 & 7 \\ 4 & 3 & 1 & 1 & 1 & 9 & 2 & 4 \\ 3 & 4 & 1 & 1 & 2 & 7 & 13 & 4 \\ 1 & 4 & 1 & 1 & 2 & 4 & 10 & 4 \end{pmatrix}$$

A method of defining a slightly different matrix for Group 642 would be to arrange the teams in alphabetical order and add a further column to indicate the position in the merit-order matrix. The only way to simplify **M** without leaving out vital information is to omit (say) the number of matches played, as that can be deduced from the number of wins, draws and losses. Although it is possible to give the information in another form, such as giving goal difference in place of goals conceded, the table cannot be otherwise transformed without removing information which is essential to appreciate the achievements of the teams. This demonstrates that the league tables can be displayed in different ways, but they cannot be much reduced in size without losing information or transformed without destroying the results they are designed to record. For example, multiplying the merit-order matrix **M** by a non-singular matrix **P** which had not been carefully selected would produce a matrix **PM** from which the table could be reconstructed, but **PM** itself would be a meaningless collection of numbers.

Example 2

Consider a system of linear equations which, to shorten the discussion, we shall assume is homogeneous. Then the system of equations can be written as $\mathbf{Ax} = \mathbf{0}$, where **A** is a matrix, **x** is a column vector of indeterminates (that is, symbols that can be regarded as

either unknowns or variables) and **0** is a zero vector. In this way, the system of homogeneous equations is fully represented by the matrix **A**. However, the real interest in a system of linear equations lies in the set of solutions, and this is a vector space V. We find V by obtaining a matrix **B** in echelon form from **A** by using elementary row operations so that the system of equations $\mathbf{Bx} = \mathbf{0}$ is equivalent to $\mathbf{Ax} = \mathbf{0}$, that is, has the same set of solutions V. To represent that the matrices **A** and **B** are (row) equivalent we shall write $\mathbf{A} \sim \mathbf{B}$, which means that **B** is obtained from **A** by a finite chain of operations of exchanging two rows, multiplying a row by a non-zero scalar or adding a multiple of one row to another. Once a system in echelon form $\mathbf{Bx} = \mathbf{0}$ is found, we can then find V by back substitution from $\mathbf{Bx} = \mathbf{0}$. Because the set of solutions V belongs to every system of linear equations equivalent to $\mathbf{Ax} = \mathbf{0}$, the family of equivalent systems of equations with solutions V is more precisely represented by the set of matrices $S = \{\mathbf{M} : \mathbf{M} \sim \mathbf{A}\}$, though a better idea is to choose a particular matrix from S. It follows that, instead of a general matrix, one of the matrices in echelon form (such as **B**) can be chosen to represent S and thence the systems of linear equations with set of solutions V. But is the matrix in echelon form **B**, associated with the system of equations $\mathbf{Ax} = \mathbf{0}$, uniquely defined by the equations? In other words, are two matrices in S necessarily equal if they are in echelon form? Unfortunately, the following example shows that the answer can be 'No'. Let k be some number and consider the following matrices

$$\mathbf{B} = \begin{pmatrix} 2 & 4 & 8 \\ 0 & 1 & 1 \\ 0 & 0 & k \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 1 \\ 0 & 0 & k \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & k \end{pmatrix}.$$

These matrices are equivalent, therefore they are the matrices of coefficients of systems of equations with the same set of solutions, but they are also in echelon form whether or not $k = 0$. In fact, if $k \neq 0$ the matrix **B** is also equivalent to the identity matrix **I**, which is also in echelon form. In fact, it is possible to choose a unique matrix from the set S. For example, there is a unique matrix in **reduced echelon form** which is equivalent to **A**, that is, a matrix in which each non-zero row starts with 1 and this number 1 is the only non-zero element in its column. Exactly one such matrix uniquely represents a system of homogeneous linear equations and all the systems equivalent to it.

Example 2 is a good illustration of the main problem for which this book finds particular solutions in special cases – that is, the finding of simpler matrices, preferably unique, to replace general matrices in certain problems which arise from applications of linear algebra.

It is not immediately obvious that there is a connection between this main problem of the book and the sections on vector spaces, linear transformations, the Cayley–Hamilton theorem (which will be stated later) and minimum polynomials, so we shall now outline the connections. In fact, as well as providing some vital techniques, these ideas are important in relating the matrices to more general mathematical problems, frequently when the elements in the problem form a vector space. We are familiar with the application to linear equations, where the set of solutions of a system of homogeneous linear equations with real coefficients in n unknowns is a vector space of n-tuples of real numbers. This vector space is a **vector space of degree n over $\mathbb{R}$** (the set of real numbers) which can also be described as a subspace of the **total vector space $\mathbb{R}^n$** of all

n-tuples of real numbers. However, further applications require a wider definition of vector spaces, and this can even be necessary within linear algebra, as the following example shows.

Example 3

Let V be the set of all 2×2 matrices with real elements. A typical element of V is $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and this can be rewritten as a column vector in the form $\mathbf{A}\sigma = (a \;\; b \;\; c \;\; d)^{\mathrm{T}}$. In this equation σ represents a mapping of V written after the element on which it acts. This notation is frequently used in this book, but the notation $s(\mathbf{A})$ is also used for this mapping when this is more convenient. It is easy to see that if $\mathbf{B} \in V$ and $r \in \mathbb{R}$ then $(\mathbf{A} + \mathbf{B})\sigma = \mathbf{A}\sigma + \mathbf{B}\sigma$ and $(r\mathbf{A})\sigma = r(\mathbf{A}\sigma)$, and therefore that V is a vector space over $\mathbb{R}$ with the same operations as the total vector space $\mathbb{R}^4$ of four-row column vectors with real elements. However, V itself cannot be regarded as being identical to $\mathbb{R}^4$ because, for example, we cannot form $\mathbf{KA}$ where $\mathbf{K}$ is a 4×4 matrix with real elements. Therefore $\mathbf{A}$ cannot be the solution of the system of linear equations $\mathbf{Kx} = \mathbf{0}$, where $\mathbf{x}$ is a column vector of indeterminates, whereas $\mathbb{R}^4$ contains the vector space of solutions of this system of equations. Conversely, there is no product in $\mathbb{R}^4$ for the vectors $\mathbf{u}$ and $\mathbf{v} \in \mathbb{R}^4$, whereas for $\mathbf{C}, \mathbf{D} \in V$ there are products $\mathbf{CD}$ and $\mathbf{DC}$ in V. When this product is taken into account the vector space V is called an **algebra** over $\mathbb{R}$.

There are two possible responses to this variety of vector spaces. One is to study each kind of vector space as it occurs in mathematical work, but this leads to much duplication of effort to provide proofs as well as difficulties in recognizing the patterns in similar proofs. These disadvantages encourage the adoption of the other approach: to derive the required results for all vector spaces from a set of common properties. In other words, we define an abstract **vector space** as a set of elements called **vectors** on which there are defined operations of addition and multiplication by scalars and which satisfy a list of required properties called the **axioms**. The obvious disadvantage of this approach is that the proofs are abstract, referring to nothing in particular, but this carries the advantage that the proofs are simpler because they are not obscured by details of calculations. We give the definition of a vector space in Chapter 3, but we also show that this definition has the strange disadvantage of being too wide for our applications to linear algebra. In order to relate a vector space V to a subspace of a total vector space, we make the extra assumption that V is **finite-dimensional**. In other words, we shall assume that a vector space V over $\mathbb{R}$ has a finite basis $B = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$, where n is a positive integer or zero. We can use this basis B to show that V is isomorphic to $\mathbb{R}^n$, that is, that V is identical to the total vector space $\mathbb{R}^n$ as far as addition and multiplication by scalars are concerned.

A disadvantage of studying vector spaces which are not of finite degree, whatever method is used, is that there is no exact analogue of the matrix for such vector spaces, although something related to a matrix can be obtained in the following way. If $\mathbf{A}$ is an $m \times n$ matrix with real elements then the equation $\mathbf{y} = \mathbf{Ax}$, where $\mathbf{x}$ and $\mathbf{y}$ are column vectors with indeterminates as elements, is a mapping from $\mathbb{R}^n$ to $\mathbb{R}^m$. If $m = n$ we may take $\mathbb{R}^m$ to be the same vector space as $\mathbb{R}^n$, so that then each $n \times n$ matrix defines a mapping $\mathbf{y} = \mathbf{Ax}$ of $\mathbb{R}^n$ into itself with the properties that $\mathbf{A}(\mathbf{c} + \mathbf{d}) = \mathbf{Ac} + \mathbf{Ad}$ and $\mathbf{A}(r\mathbf{c}) = r(\mathbf{Ac})$ for all $\mathbf{c}$ and $\mathbf{d} \in \mathbb{R}^n$ and $r \in \mathbb{R}$. To copy this idea for V, we define a **linear**

transformation of V into itself as a mapping T of V into itself such that $T(\mathbf{u}+\mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$ and $T(r\mathbf{u}) = rT(\mathbf{u})$. If we use the basis B to represent V as $\mathbb{R}^n$ then it can be shown that there is a matrix $\mathbf{A}$ such that $\mathbf{y} = T(\mathbf{x})$ if and only if $\mathbf{y} = \mathbf{Ax}$. Consequently, the linear transformation T is represented by the matrix $\mathbf{A}$, so it looks as if the linear transformations T can be used for abstract vector spaces instead of the matrices $\mathbf{A}$. But there is an important difference because the matrix form of the linear transformation depended on the use of the basis B. If a different basis is used we must multiply both the vectors by a non-singular matrix $\mathbf{P}$, because both sides of the equation have been changed by the same change of basis. Consequently, the linear transformation T is then represented by the equation $\mathbf{Py} = \mathbf{APx}$ and therefore by $\mathbf{y} = (\mathbf{P}^{-1}\mathbf{AP})\mathbf{x}$. We conclude that matrices $\mathbf{A}$ and $\mathbf{B}$ represent the same linear transformation T if and only if there is a non-singular matrix $\mathbf{P}$ such that $\mathbf{B} = \mathbf{P}^{-1}\mathbf{AP}$. Such matrices $\mathbf{A}$ and $\mathbf{B}$ are said to be **similar**. It is of interest that if some kind of geometrical or mechanical element is represented by the matrix $\mathbf{A}$ and the Cartesian coordinates of the space are changed then the matrix representing the element in the new coordinates is $\mathbf{Q}^{-1}\mathbf{AQ}$, where the change of coordinates is given by $\mathbf{y} = \mathbf{Qx}$ and $\mathbf{Q}$ is not only non-singular but also satisfies another condition, as determined in Chapter 10. These two examples imply that the determination of a unique simple matrix in the set of all matrices similar to $\mathbf{A}$ forms an important part of our main problem. Our later results show that this unique matrix can be chosen to be a diagonal matrix in many cases, but not all. An important case in which the matrix $\mathbf{D}$ representing the set of matrices similar to $\mathbf{A}$ can be chosen to be diagonal is when $\mathbf{A}$ is **symmetric**, that is, when $\mathbf{A}^{\mathrm{T}} = \mathbf{A}$.

It is helpful when trying to obtain a simple matrix $\mathbf{B}$ which is similar to a matrix $\mathbf{A}$ to investigate properties of $\mathbf{A}$ which it shares with all the matrices similar to it. Such a property is said to be **invariant under similarity**. An easy example of an invariant property of a matrix $\mathbf{A}$ is that called (rather loosely) **satisfying a polynomial**, by which we mean that there exists constants $c_0, c_1, c_2, \ldots, c_k$, not all zero, such that $f(\mathbf{A}) = c_k\mathbf{A}^k + \ldots + c_2\mathbf{A}^2 + c_1\mathbf{A} + c_0\mathbf{I} = \mathbf{0}$. That satisfying this polynomial is invariant under similarity can be expressed by the assertion that $f(\mathbf{A}) = \mathbf{0}$ if and only if $f(\mathbf{P}^{-1}\mathbf{AP}) = \mathbf{0}$ for all non-singular $n \times n$ matrices $\mathbf{P}$. This statement becomes more interesting when it is noted that every square matrix with real elements satisfies a polynomial equation. To see this we recall that every $n \times n$ matrix $\mathbf{A}$ with real elements belongs to the vector space V of all $n \times n$ matrices with real elements. Also V is of dimension n^2, as in Example 3. This implies that every set of $n^2 + 1$ elements in V is linearly dependent over $\mathbb{R}$, and therefore, with $k = n^2$, there exist real numbers $c_0, c_1, c_2, \ldots, c_k$, not all zero, such that $f(\mathbf{A}) = \mathbf{0}$, in our earlier notation. This shows that $\mathbf{A}$ satisfies at least one polynomial of degree at most n^2, and that if $\mathbf{B}$ is similar to $\mathbf{A}$ then $\mathbf{B}$ must satisfy the same polynomial. This information would be more valuable if we could name a particular polynomial that $\mathbf{A}$ satisfies, and fortunately the Cayley–Hamilton theorem (see Chapter 8) identifies such a polynomial. In fact, in Chapter 9, it is proved that there exists a unique **minimum polynomial** of $\mathbf{A}$ which is of least degree among the polynomials satisfied by $\mathbf{A}$. Furthermore, this polynomial can be found by using the Cayley–Hamilton theorem.

In this book we also attempt to solve our main problem for various classes of quadratic forms, that is, homogeneous polynomials of degree 2. Here is an example of a quadratic form in an elementary context which shows how a simpler quadratic form can be desirable, as well as showing an easy way to obtain a matrix from the quadratic form.

Example 4

An easy example of a quadratic form is $Q = x^2 + 6xy + 5y^2$. Then the equation $Q = 1$ can be taken as the equation of a conic in a Cartesian plane with coordinates (x, y) and we can express this equation in matrix form by using the following matrices:

$$\mathbf{x} = \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{and} \quad \mathbf{A} = \begin{pmatrix} 1 & 3 \\ 3 & 5 \end{pmatrix}.$$

In fact, any matrix of the form $\mathbf{B} = \begin{pmatrix} 1 & p \\ q & 5 \end{pmatrix}$ with $p + q = 6$ can be chosen here, but we have chosen **A** because it is the unique symmetric matrix of the form **B**, and we recently noted the advantage that a matrix satisfying $\mathbf{A}^{\mathrm{T}} = \mathbf{A}$ is similar to a diagonal matrix. The matrix **A** is called the **matrix associated with** Q. Then

$$\begin{aligned} \mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x} &= (x \quad y)\begin{pmatrix} 1 & 3 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = (x+3y \quad 3x+5y)\begin{pmatrix} x \\ y \end{pmatrix} \\ &= (x^2 + 6xy + 5y^2) = Q, \end{aligned}$$

where Q is regarded as a 1×1 matrix. This is a useful form of the equation, but does it help to determine what kind of conic $Q = 1$ represents? One possibility is that $Q - 1 = 0$ factorizes into linear factors, and so the figure is a pair of lines instead of being a proper conic. Fortunately, there is a theorem which states that the equation will not factorize if the determinant of the matrix of coefficients is non-zero. (Determinants are discussed in Chapter 5 of Allenby's *Linear Algebra*.) In this case the determinant is

$$\begin{vmatrix} 1 & 3 & 0 \\ 3 & 5 & 0 \\ 0 & 0 & -1 \end{vmatrix} = 4,$$

so the conic does not consist of two lines. A second possibility is that the conic has no real points on it, when it is said to be **virtual**. However, the point with coordinate $(1, 0)$ is obviously on the conic, which means that $Q = 1$ represents a parabola or an ellipse (of which a circle is a special case) or a hyperbola. A parabola differs from the others in that it has no centre, that is, a point which is the mid-point of all the chords passing through it. For $Q = 1$ the chord through (x, y) and the origin meets the conic again at $(-x, -y)$, therefore the origin is the centre of the conic, so it is not a parabola. We could decide whether the conic is an ellipse or a hyperbola if we can rotate the axes so that in the new coordinates (x', y') the equation becomes $ax'^2 + by'^2 = 1$, because the conic is an ellipse if both of the coefficients a and b are positive and a hyperbola if they are of opposite signs. Therefore we are led to the question 'Can Q be transformed into a sum of multiples of squares of the coordinates by a rotation of axes?'. We shall return to this question in Chapter 12.

Example 5

The question about Q in Example 4 can be translated into a related question about the symmetric matrix **A** associated with Q, which we can formulate approximately as

follows. Let the rotation of axes from (x, y), or $\mathbf{x}$ as a column vector, to (x', y'), or $\mathbf{x}'$ as a column vector, be given by the equation $\mathbf{x} = \mathbf{P}\mathbf{x}'$, where the matrix $\mathbf{P}$ represents a rotation of axes. Then we can obtain the equation for the conic in the new coordinates by the substitution $\mathbf{x} = \mathbf{P}\mathbf{x}'$, that is,

$$\mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x} = (\mathbf{P}\mathbf{x}')^{\mathrm{T}}\mathbf{A}(\mathbf{P}\mathbf{x}') = \mathbf{x}'^{\mathrm{T}}(\mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P})\mathbf{x}' = 1.$$

The rotation of axes determined by $\mathbf{P}$ then transforms the matrix $\mathbf{A}$ into the matrix $\mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P}$. This process changes the question about quadratic forms into the question 'If $\mathbf{A}$ is the matrix associated with a quadratic form, can a matrix $\mathbf{P}$ representing a rotation of axes be found so that $\mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P}$ is a diagonal matrix?'. The matrices which represent rotations of Cartesian axes will be determined in Chapter 10, and we solve this problem in Chapter 12.

Finally, it is time to discuss the term **field** which recurs in the results throughout the book and refers to the kind of numbers used in them. This matters because it is easy to prove that results in linear algebra vary according to the sets of numbers which are used. For example, the system of equations in the unknown integers m and n

$$\begin{aligned} 2m + 12n &= 5 \\ 8m - 9n &= 1 \end{aligned}$$

is equivalent over the integers $\mathbb{Z}$ to the system in echelon form

$$\begin{aligned} 2m + 12n &= 5 \\ 3n &= 1 \end{aligned}$$

but this second system obviously has no integer solution. On the other hand, we can deduce from the second set that the unique solution of both systems of equations over the rational numbers is $m = \frac{1}{2}$ and $n = \frac{1}{3}$. This demonstrates that the standard results in linear algebra rely on division by non-zero elements being possible. For this reason we shall consider all the equations, matrices, vector spaces and quadratic forms in this book as being 'over a field $\mathbb{F}$'. By this we mean that all the numbers are taken from the field $\mathbb{F}$, where a field $\mathbb{F}$ is a set of complex numbers which have sums, differences, products and quotients (not by 0) in $\mathbb{F}$. Although there is an abstract definition of a field which includes sets other than numbers, little will be lost by assuming that $\mathbb{F}$ is one of the following: the field of rational numbers $\mathbb{Q}$ or the field of real numbers $\mathbb{R}$ or the field of complex numbers $\mathbb{C}$. The reason why the field $\mathbb{F}$ will be referred to in the statements of most theorems (though not always in their proofs) is that some results later in the book need the field to be $\mathbb{R}$ or need it to be $\mathbb{C}$ or need $\mathbb{F}$ to satisfy a certain condition. Otherwise, naming the field only serves as a reminder that all the calculations take place inside the one set $\mathbb{F}$.

Summary

This chapter explained the purpose of the algebra which appears in this book. In particular, it introduced the main kind of problem which is solved in this book, that is, the finding of a simple matrix to use in place of a general matrix in various contexts. It was shown that the application of linear algebra to subjects other than linear equations

requires the use of abstract vector spaces and linear transformations. This led to the concept of similar matrices and the need to study characteristic and minimum polynomials of a matrix when seeking a diagonal matrix similar to a given matrix. Finally, the reasons for studying matrices over a field were given.

EXERCISES ON CHAPTER 1

1. Because of the large number of group tables in the 1995 World Cup, the Association of Sports Statisticians (or ASS) files all the group tables in a condensed form. Instead of filing the 4×8 matrix $\mathbf{M}$ for Group 642, ASS has filed the 4×3 matrix $\mathbf{L} = \mathbf{MT}$, where $\mathbf{T}$ is the 8×4 matrix given by

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

   How much of the records of the teams in Group 642 can be deduced from the matrix $\mathbf{L}$?

2. Let S be the set of all lines in a plane with a fixed set of rectangular Cartesian axes. Show that for the line $L \in S$ with equation $ax + by + c = 0$ either $a \neq 0$ or $b \neq 0$. Show that L can be represented by the set of vectors $S(L) = \{(\lambda a, \lambda b, \lambda c) : \lambda \in \mathbb{R}\}$. Show that L is represented by a unique vector in the set $U = \{(f, 1, g), (1, 0, h) : f, g, h \in \mathbb{R}\}$ and that every vector in U represents a unique line in S.

3. Which of the following statements are true (i) for $\mathbb{F} = \mathbb{Q}$, (ii) for $\mathbb{F} = \mathbb{R}$, (iii) for $\mathbb{F} = \mathbb{C}$?
   (a) $3x + 2 = 0$ has exactly one root in $\mathbb{F}$.
   (b) $x^2 = 0$ has exactly two equal roots in $\mathbb{F}$.
   (c) $x^2 - 4 = 0$ has exactly two distinct roots in $\mathbb{F}$.
   (d) $x^2 - 2 = 0$ has exactly two distinct roots in $\mathbb{F}$.
   (e) $x^2 + 2 = 0$ has exactly two roots in $\mathbb{F}$.
   (f) $x^5 - 1 = 0$ has exactly five roots in $\mathbb{F}$.

2 · Partitioned Matrices

Outline

In this chapter we consider 'partitioned' matrices, in which the elements are themselves matrices called 'submatrices' when they are used in this way. The process of inserting partitions into ordinary matrices to create partitioned matrices is then used to present results in an easier form, but is also used in a way that simplifies calculations and proofs.

Introduction

The idea of partitioning a matrix starts with the obvious way of writing a matrix like

$$\mathbf{A}=\begin{pmatrix}2&0&-1&1\\0&3&3&1\\0&0&1&0\\0&0&0&1\end{pmatrix}$$

to make it easier to read. The third and fourth rows of $\mathbf{A}$ make immediate sense if we note that the first two columns make a 2×2 zero matrix $\mathbf{0}$ and the third and fourth columns make a 2×2 identity matrix $\mathbf{I}$. Having recognized these parts of $\mathbf{A}$, we can write $\mathbf{A}$ in a briefer form by giving names to the other parts. In this case we can write $\mathbf{D}$ for the diagonal matrix $\begin{pmatrix}2&0\\0&3\end{pmatrix}$, and $\mathbf{F}$ for the matrix $\begin{pmatrix}-1&1\\3&1\end{pmatrix}$ in the first rows and last two columns of $\mathbf{A}$, in order to represent $\mathbf{A}$ as a 2×2 matrix $\mathbf{A}=\begin{pmatrix}\mathbf{D}&\mathbf{F}\\\mathbf{0}&\mathbf{I}\end{pmatrix}$ with elements that are themselves 2×2 matrices over $\mathbb{Q}$. When it is in this form we call $\mathbf{A}$ a **partitioned matrix**, a name which will be clearer later on, and we may describe the matrices $\mathbf{D}$, $\mathbf{F}$, $\mathbf{0}$ and $\mathbf{I}$ as submatrices of $\mathbf{A}$, where a **submatrix** of a matrix $\mathbf{M}$ is any matrix formed from $\mathbf{M}$ by omitting rows and columns from $\mathbf{M}$. This expression for $\mathbf{A}$ as a 2×2 partitioned matrix is easy to read, but in this chapter we shall show that this device has further advantages.

Suppose that a problem involves other matrices which are broadly similar to the matrix $\mathbf{A}$ of the Introduction, and these matrices need to be added or multiplied. For example, suppose that we also have the matrix

$$\mathbf{B}=\begin{pmatrix}1&1&4&0\\2&1&2&6\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

Then we may write $\mathbf{C}=\begin{pmatrix}1 & 1\\ 2 & 1\end{pmatrix}$ and $\mathbf{G}=\begin{pmatrix}4 & 0\\ 2 & 6\end{pmatrix}$ to obtain the 2×2 partitioned matrix with 2×2 submatrix elements $\mathbf{B}=\begin{pmatrix}\mathbf{C} & \mathbf{G}\\ \mathbf{0} & \mathbf{I}\end{pmatrix}$. Note that the identity matrix $\mathbf{I}$ and the zero matrix $\mathbf{0}$ are used as submatrices without indications of their numbers of rows and columns, unless to indicate them is essential. Consequently, $\mathbf{I}$ or $\mathbf{0}$ can appear as submatrices of several different sizes in one matrix. Also the submatrix (5) is usually written as 5, and similarly for all 1×1 submatrices.

Because addition of matrices is merely addition of corresponding elements, we can add $\mathbf{A}$ and $\mathbf{B}$ in this form as

$$\mathbf{A}+\mathbf{B}=\begin{pmatrix}\mathbf{D}+\mathbf{C} & \mathbf{F}+\mathbf{G}\\ \mathbf{0} & 2\mathbf{I}\end{pmatrix}$$

and, because the addition of the submatrices is also addition of corresponding elements, the numerical elements of this matrix that we have labelled $\mathbf{A}+\mathbf{B}$ really are those of $\mathbf{A}+\mathbf{B}$ calculated in the usual way. A calculation of $\mathbf{AB}$ as a matrix of 2×2 matrices using the usual definition of product also seems possible because all the submatrices are 2×2 matrices and so all the products and sums are defined and we have a resulting matrix

$$\mathbf{P}=\begin{pmatrix}\mathbf{D} & \mathbf{F}\\ \mathbf{0} & \mathbf{I}\end{pmatrix}\begin{pmatrix}\mathbf{C} & \mathbf{G}\\ \mathbf{0} & \mathbf{I}\end{pmatrix}=\begin{pmatrix}\mathbf{DC}+\mathbf{F0} & \mathbf{DG}+\mathbf{FI}\\ \mathbf{0C}+\mathbf{I0} & \mathbf{0G}+\mathbf{II}\end{pmatrix}=\begin{pmatrix}\mathbf{DC} & \mathbf{DG}+\mathbf{F}\\ \mathbf{0} & \mathbf{I}\end{pmatrix}.$$

This time it is not obvious that $\mathbf{P}=\mathbf{AB}$ because the sum in each submatrix of $\mathbf{P}$ is calculated in two stages. Nevertheless, it is easy to see that in this case

$$\mathbf{P}=\left(\begin{array}{cc:cc}2 & 2 & 7 & 1\\ 6 & 3 & 9 & 19\\ \hdashline 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{array}\right),$$

where the dotted lines (which we call **partitions**) delimit the submatrices, becomes $\mathbf{AB}$ when the partitions are removed. The examples of partitioned matrices that we have given so far are not typical in that the submatrices that we have used are all 2×2 matrices, whereas the familiar example of the **augmented matrix** $(\mathrm{A}\ \ \mathrm{b})$ of the system of linear equations $\mathbf{Ax}=\mathbf{b}$ is naturally partitioned in a way which (usually) gives submatrices of different sizes. It should also be noted that the number of partitions can vary from none to one less than the number of rows or columns. Moreover, the number of partitions of the rows need not equal the number of partitions of the columns. This allows a very useful partition of a matrix $\mathbf{B}$ such that the submatrices are the columns of $\mathbf{B}$, so that $\mathbf{B}=(\mathbf{b}_1\ \ \mathbf{b}_2\ \ \mathbf{b}_3\ \ \ldots\ \ \mathbf{b}_n)$ as a partitioned matrix. Then, if the product $\mathbf{AB}$ is defined, we have $\mathbf{AB}=(\mathbf{Ab}_1\ \ \mathbf{Ab}_2\ \ \mathbf{Ab}_3\ \ \ldots\ \ \mathbf{Ab}_n)$. It should also be noticed that a partitioned matrix can be obtained from a matrix $\mathbf{M}$ either by giving names to the submatrices or by defining the submatrices by means of partitions.

This discussion of the partitioning of matrices raises two questions about the addition or multiplication of two partitioned matrices. To make the questions clearer let us

introduce some notation which is only for use in this chapter. Let $\mathbf{A}\pi$ represent a matrix obtained by partitioning the matrix $\mathbf{A}$ in some way and let $\mathbf{B}\delta$ represent the matrix obtained by removing the partitions from the partitioned matrix $\mathbf{B}$. Question 1 is concerned with whether, for matrices $\mathbf{A}$ and $\mathbf{B}$ such that $\mathbf{A} + \mathbf{B}$ is defined and $\mathbf{C}$ and $\mathbf{D}$ such that $\mathbf{CD}$ is defined, the matrices can be partitioned (not necessarily in the same way) so that $\mathbf{A}\pi + \mathbf{B}\pi$ and $\mathbf{C}\pi\mathbf{D}\pi$ are defined. Question 2 asks whether $(\mathbf{A}\pi + \mathbf{B}\pi)\delta = \mathbf{A} + \mathbf{B}$ and $(\mathbf{C}\pi\mathbf{D}\pi)\delta = \mathbf{CD}$ when the operations are defined for the partitioned matrices. Satisfactory answers to these questions then prompt Question 3: do the usual rules for the addition and multiplication of matrices over a field hold for partitioned matrices? Questions 1 and 2 are answered for addition in the following theorem, which has an easy proof which we leave as an exercise.

• Theorem 1

Let $\mathbf{A}$ and $\mathbf{B}$ be $m \times n$ matrices over a field $\mathbb{F}$. Then

(i) $\mathbf{A}$ and $\mathbf{B}$ can be added as partitioned matrices if and only if their partitions are in the same positions, and

(ii) the matrix obtained by removing the partitions from the sum of $\mathbf{A}$ and $\mathbf{B}$ as partitioned matrices is $\mathbf{A} + \mathbf{B}$.

The partitioning of matrices would not be worthwhile if addition was the only operation that could be usefully performed in the partitioned form; consequently, the key to the use of partitioned matrices is the result that matrices can be multiplied in partitioned form and then the results interpreted as the product of matrices over a field. It follows that Theorem 2, which asserts these results, is important and needs to be proved, but its long proof merely verifies that the result is true in four cases which cover all possibilities. Because the proof gives no extra information or insight about the use of partitioned matrices, we shall omit it and rely on illustrating its working in the exercises.

• Theorem 2

Let $\mathbf{A}$ be an $m \times n$ matrix over a field $\mathbb{F}$ and let $\mathbf{B}$ be an $n \times p$ matrix over $\mathbb{F}$. Then

(i) if $\mathbf{A}$ and $\mathbf{B}$ have partitioned forms $\mathbf{A}\pi$ and $\mathbf{B}\pi$, the product $\mathbf{A}\pi\mathbf{B}\pi$ is defined if and only if in $\mathbf{A}\pi$ the partitions of the n columns of $\mathbf{A}$ are in the same positions as the partitions of the n rows of $\mathbf{B}$ in $\mathbf{B}\pi$, and

(ii) the matrix obtained by removing the partitions from the product $\mathbf{A}\pi\mathbf{B}\pi$ of the partitioned matrices $\mathbf{A}\pi$ and $\mathbf{B}\pi =$ is the matrix $\mathbf{AB}$ over $\mathbb{F}$.

Theorems 1 and 2 determine when either addition or multiplication of two partitioned matrices is possible, so we can combine these results to determine the most useful case, which is when the matrices can be both added and multiplied in partitioned form. The following theorem is easy to deduce from Theorems 1 and 2.

• Theorem 3

Let S be a set of matrices over a field $\mathbb{F}$ with given partitions. Then any pair of matrices in S can be both added and multiplied in partitioned form if and only if there is an

integer n such that all the matrices in S are $n \times n$ matrices over $\mathbb{F}$ with the same partitions which are symmetrical, that is, the same for the rows and the columns.

Another operation we may wish to apply to a partitioned matrix $\mathbf{A}\pi$ is to multiply $\mathbf{A}\pi$ by a scalar c, which is the operation whereby each submatrix of $\mathbf{A}\pi$ is multiplied by c. As this is achieved by multiplying each element of the submatrix by c, it is obvious that the operation $c(\mathbf{A}\pi)$ can always be performed and that $[c(\mathbf{A}\pi)]\delta = c\mathbf{A}$.

Alternatively, we can transpose partitioned matrices, although they cannot be transposed just by exchanging corresponding rows and columns like ordinary matrices. This is most easily seen by considering the transpose of a partitioned matrix $\mathbf{A}\pi$ with exactly one submatrix $\mathbf{B}$. This means that $\mathbf{A}\pi = (\mathbf{B})$ and therefore $(\mathbf{A}\pi)^{\mathrm{T}} = (\mathbf{B}^{\mathrm{T}})$. This suggests that to transpose a partitioned matrix we first transpose each submatrix and then we exchange the corresponding rows and columns. The properties of transposed partitioned matrices are summarized in the following theorem for which the proofs of parts (i) and (ii) are easy. However, the proof of Theorem 4(iii) is more difficult and makes use of the equation $(\mathbf{MN})^{\mathrm{T}} = \mathbf{N}^{\mathrm{T}}\mathbf{M}^{\mathrm{T}}$, which holds for any pair of matrices $\mathbf{M}$ and $\mathbf{N}$ with a product $\mathbf{MN}$.

• *Theorem 4*

Let $\mathbf{A}$ be an $m \times n$ matrix over a field $\mathbb{F}$ and let $\mathbf{A}\pi$ be $\mathbf{A}$ partitioned as the $r \times s$ matrix $\mathbf{A}\pi = (\mathbf{A}_{fg})$. Then the **transpose** of $\mathbf{A}\pi$ is

$$(\mathbf{A}\pi)^{\mathrm{T}} = (\mathbf{C}_{gf}) \quad \text{where} \quad \mathbf{C}_{gf} = \mathbf{A}_{fg}^{\mathrm{T}},$$

which is always defined and satisfies the following:

(i) $\mathbf{A}^{\mathrm{T}}$ is obtained by removing the partitions from $(\mathbf{A}\pi)^{\mathrm{T}}$;

(ii) if $\mathbf{B}\pi$ is an $m \times n$ matrix over $\mathbb{F}$ partitioned like $\mathbf{A}\pi$, then

$$(\mathbf{A}\pi)^{\mathrm{T}} + (\mathbf{B}\pi)^{\mathrm{T}} = (\mathbf{A}\pi + \mathbf{B}\pi)^{\mathrm{T}};$$

(iii) if $\mathbf{B}\pi$ is an $n \times p$ matrix over $\mathbb{F}$ with the same partition of the rows that $\mathbf{A}\pi$ has of the columns, then

$$(\mathbf{A}\pi\mathbf{B}\pi)^{\mathrm{T}} = (\mathbf{B}\pi)^{\mathrm{T}}(\mathbf{A}\pi)^{\mathrm{T}}.$$

Finally, we consider the inverse of a non-singular partitioned matrix. Because both the method of calculating the inverse of a matrix by elementary operations and the alternative formula for the inverse as the quotient of the adjoint by the determinant are so complicated, it is reasonable to suppose that there is no possibility of calculating the inverse of a partitioned matrix as a partitioned matrix at all. In fact, although there is no general formula for the inverse of a non-singular partitioned matrix, formulae do exist for the inverses of some special forms of partitioned matrices. Some of the possibilities are illustrated in the following tutorial problem.

TUTORIAL PROBLEM 2.1

Consider the 2×2 partitioned matrix $\mathbf{A}\pi$ given by $\mathbf{A}\pi = \begin{pmatrix} \mathbf{B} & \mathbf{F} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}$, where $\mathbf{B}$ is square and

$\mathbf{A}$ is non-singular. Show that $\mathbf{B}$ is also non-singular and that $\mathbf{A}\pi$ has the partitioned inverse matrix $\mathbf{A}^{-1}\pi$, where

$$\mathbf{A}^{-1}\pi = \begin{pmatrix} \mathbf{B}^{-1} & -\mathbf{B}^{-1}\mathbf{F} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}.$$

So far we have concentrated on the definition and existence of the algebraic operations for partitioned matrices without studying their properties, such as the associative law. The good reason for this is that all the proofs of the properties of partitioned matrices are simple revisions of the proofs for ordinary matrices. To indicate why this is true, let us look at the proof of the associative law of multiplication as applied to three 2×2 matrices over a field $\mathbb{F}$. Let

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \quad \text{and} \quad \mathbf{C} = \begin{pmatrix} t & u \\ v & w \end{pmatrix}.$$

Then the element f in the first row and first column of $(\mathbf{AB})\mathbf{C}$ is

$$f = (ap + br)t + (aq + bs)v.$$

We deduce from the right distributive law for $\mathbb{F}$ (or, if you prefer it, for the complex numbers),

$$f = [(ap)t + (br)t] + [(aq)v + (bs)v]$$

and, omitting the square brackets which are not necessary because of the associative law of addition for $\mathbb{F}$, we obtain

$$f = (ap)t + (br)t + (aq)v + (bs)v.$$

By the associative law for multiplication for $\mathbb{F}$,

$$f = a(pt) + b(rt) + a(qv) + b(sv),$$

by the commutative law for addition for $\mathbb{F}$,

$$f = a(pt) + a(qv) + b(rt) + b(sv)$$

and, by the left distributive law for $\mathbb{F}$,

$$f = a(pt + qv) + b(rt + sv).$$

Therefore f is the term in the first row and first column of $\mathbf{A}(\mathbf{BC})$, and the same can be proved for the other elements. However, the important point of this proof is that the associative law for multiplication for 2×2 matrices over $\mathbb{F}$ was proved by using only properties of the elements of the field $\mathbb{F}$ that also hold for all matrices over $\mathbb{F}$. Consequently, the same proof can be given for partitioned matrices as for matrices over $\mathbb{F}$, and therefore we omit the proof of Theorem 5.

• *Theorem 5*

Let $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ be partitioned matrices. Then the following hold whenever the operations used are defined:

(i) $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$.
(ii) $(\mathbf{A} + \mathbf{B}) + \mathbf{C} = \mathbf{A} + (\mathbf{B} + \mathbf{C})$.
(iii) The partitioned matrix $\mathbf{0}$ in which every submatrix is zero satisfies $\mathbf{A} + \mathbf{0} = \mathbf{A}$ for every matrix $\mathbf{A}$ of the same size.
(iv) $\mathbf{A} + (-1)\mathbf{A} = \mathbf{0}$.
(v) $(\mathbf{AB})\mathbf{C} = \mathbf{A}(\mathbf{BC})$.
(vi) The square partitioned matrix $\mathbf{I}$ in which every diagonal submatrix is an identity and the other submatrices are $\mathbf{0}$ satisfies $\mathbf{AI} = \mathbf{A}$ and $\mathbf{IB} = \mathbf{B}$ for every matrix $\mathbf{A}$ and $\mathbf{B}$ for which the operations are defined.
(vii) $\mathbf{A}(\mathbf{B} + \mathbf{C}) = \mathbf{AB} + \mathbf{AC}$.
(viii) $(\mathbf{B} + \mathbf{C})\mathbf{A} = \mathbf{BA} + \mathbf{CA}$.

Summary

The useful notation of a **partitioned matrix** was introduced as a matrix in which the elements are themselves matrices, which can be defined by inserting lines between some of the rows and columns of an ordinary matrix. Provided the partitions are inserted in suitable places, it is possible to add and multiply pairs of partitioned matrices. These are useful because removing the partitions after the operations produces the sum and product of the unpartitioned matrices, while the partitioning can ease the calculations in many cases. The laws for addition and multiplication of ordinary matrices hold also for partitioned matrices. Any partitioned matrix can be multiplied by a scalar or transposed, although a special definition of transposition is needed, and the relation $(\mathbf{AB})^{\mathrm{T}} = \mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}$ holds. Again, removing the partitions leads to the same expression for ordinary matrices. There is no formula or method for finding the inverse of a general partitioned matrix, but it is possible to find such a formula in special cases.

EXERCISES ON CHAPTER 2

1. Let $\mathbf{A}$ be the partitioned matrix given by

$$\mathbf{A} = \left(\begin{array}{cc:cc} 1 & 2 & 2 & 1 \\ 0 & 1 & 1 & 1 \\ \hdashline 4 & 3 & 1 & 0 \end{array}\right) = \begin{pmatrix} \mathbf{K} & \mathbf{L} \\ \mathbf{M} & \mathbf{N} \end{pmatrix}.$$

Further matrices which might be used as submatrices are:

$$\mathbf{P} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \quad \mathbf{Q} = \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 3 \end{pmatrix}, \quad \mathbf{R} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{and} \quad \mathbf{S} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Which of the following are partitioned matrices:

$$\mathbf{B} = \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{L} & \mathbf{K} \end{pmatrix}, \mathbf{C} = \begin{pmatrix} \mathbf{P} & \mathbf{Q} \\ \mathbf{R}^{\mathrm{T}} & \mathbf{N} \end{pmatrix}, \mathbf{D} = \begin{pmatrix} \mathbf{P} & \mathbf{K} \\ \mathbf{0} & \mathbf{S}^{\mathrm{T}} \end{pmatrix}, \mathbf{E} = \begin{pmatrix} 1 & \mathbf{M} \\ \mathbf{S} & \mathbf{I} \end{pmatrix},$$

$$\mathbf{F} = \begin{pmatrix} \mathbf{L} \\ \mathbf{P} \end{pmatrix}, \quad \mathbf{G} = \begin{pmatrix} \mathbf{K} & \mathbf{R} \\ \mathbf{N} & 0 \end{pmatrix} \quad \text{and} \quad \mathbf{H} = \begin{pmatrix} \mathbf{R} & \mathbf{S} \\ \mathbf{S} & \mathbf{N}^{\mathrm{T}} \end{pmatrix}?$$

Evaluate those of the following expressions which are defined as partitioned matrices and then remove the partitions and check that the result is the same as when the unpartitioned matrices are calculated:

(i) $\mathbf{A}+\mathbf{D}$ (ii) $\mathbf{AB}$ (iii) $\mathbf{AF}+\mathbf{DH}$
(iv) $\mathbf{GC}+\mathbf{D}$ (v) $\mathbf{DB}+\mathbf{GA}$ (vi) $\mathbf{EGDF}$.

There are 14 ways to partition a 3×3 matrix over a field $\mathbb{F}$, excluding the insertion of no partitions and the insertion of every possible partition. Let $\mathbf{A}\pi$ and $\mathbf{B}\rho$ be 3×3 partitioned matrices with submatrices over $\mathbb{F}$ with partitions which are not necessarily the same.

(i) For which pairs of partitions are $\mathbf{A}\pi+\mathbf{B}\rho$ and $\mathbf{A}\pi\mathbf{B}\rho$ both defined?
(ii) For which pairs of partitions are $\mathbf{A}\pi\mathbf{B}\rho$ and $\mathbf{B}\rho\mathbf{A}\pi$ both defined?

Prove Theorem 1.

Let $\mathbf{A}$ and $\mathbf{B}$ be the matrices

$$\mathbf{A}=\begin{pmatrix} 7 & 1 & 0 & 0\\ -2 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 3 & -1 & 1 & -1\end{pmatrix} \quad \text{and} \quad \mathbf{B}=\begin{pmatrix} 0 & 1 & 1 & 2\\ 1 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 2 & 1 & 0 & 0\end{pmatrix}.$$

(i) Partition $\mathbf{A}$ to make use of its special features, then partition $\mathbf{B}$ so that $\mathbf{AB}$ is defined as a partitioned matrix $(\mathbf{AB})\pi$, evaluate $(\mathbf{AB})\pi$ and check that removing the partitions yields $\mathbf{AB}$.
(ii) Partition $\mathbf{B}$ conveniently then partition $\mathbf{A}$ so that $\mathbf{AB}$ is defined as a partitioned matrix $(\mathbf{AB})\rho$, evaluate $(\mathbf{AB})\rho$ and check that removing the partitions yields $\mathbf{AB}$.

Let $\mathbf{A}$ and $\mathbf{B}$ be matrices such that $\mathbf{AB}$ and $\mathbf{BA}$ are both defined. Show that $\mathbf{AB}$ and $\mathbf{BA}$ are both defined as partitioned matrices if and only if the partitions of the rows of $\mathbf{A}$ and $\mathbf{B}$ are the same as the partitions of the columns of $\mathbf{B}$ and $\mathbf{A}$, respectively. Show also that $\mathbf{A}$ and $\mathbf{B}$ are not necessarily square and the partitions of $\mathbf{A}$ and $\mathbf{B}$ are not necessarily symmetrical.

Let $\mathbf{A}$ and $\mathbf{B}$ be matrices over a field $\mathbb{F}$ such that $\mathbf{AB}$ is defined. By partitioning $\mathbf{B}$ into its columns, show that rank $\mathbf{AB}\leq$ rank $\mathbf{B}$. Deduce that, if k is the smaller of rank $\mathbf{A}$ and rank $\mathbf{B}$, then rank $\mathbf{AB}\leq k$. Show that rank $\mathbf{AB}$ is not necessarily k. Prove that if $\mathbf{A}$ is non-singular then rank $\mathbf{AB}$ = rank $\mathbf{B}$, and, if $\mathbf{C}$ is a matrix over $\mathbb{F}$ such that $\mathbf{CA}$ is defined, then rank $\mathbf{CA}$ = rank $\mathbf{C}$.

Let $\mathbf{A}$ and $\mathbf{B}$ be the partitioned matrices

$$\mathbf{A}=\begin{pmatrix}\mathbf{K} & \mathbf{L}\\ \mathbf{M} & \mathbf{0}\end{pmatrix} \quad \text{and} \quad \mathbf{B}=\begin{pmatrix}\mathbf{I} & \mathbf{R}\\ \mathbf{0} & \mathbf{I}\end{pmatrix},$$

where

$$\mathbf{C}=\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix},\ \mathbf{L}=\begin{pmatrix}0 & 0\\ 2 & 2\end{pmatrix},\ \mathbf{M}=\begin{pmatrix}1 & 0\\ 0 & 1\\ 0 & 0\end{pmatrix} \quad \text{and} \quad \mathbf{R}=\begin{pmatrix}3 & 7\\ 2 & 5\end{pmatrix}.$$

Evaluate $\mathbf{A}^{\mathrm{T}}$, $\mathbf{B}^{\mathrm{T}}$ and $\mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}$ and check that removing the partitions from $\mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}$ yields $(\mathbf{AB})^{\mathrm{T}}$ as a matrix over $\mathbb{Q}$.

8. Let **A** be the non-singular matrix given in partitioned form as

$$\mathbf{A} = \begin{pmatrix} \mathbf{B} & \mathbf{E} & \mathbf{F} \\ \mathbf{0} & \mathbf{C} & \mathbf{G} \\ \mathbf{0} & \mathbf{0} & \mathbf{D} \end{pmatrix}$$

where **B**, **C** and **D** are square submatrices. Evaluate the inverse of **A**.

9. Prove the associative law for the multiplication of partitioned matrices.

3 · Vector Spaces

Outline

Our aim in this chapter is to present vector spaces in two different ways in order to harmonize various introductions to the subject and revise the elementary results. Examples of the direct applications of vector spaces defined as sets of ordered n-tuples of elements from a field (called vector spaces of degree n) are given to compare with the wider but subtler applications of vector spaces defined by axioms. The concepts of linear dependence, basis, dimension and subspace are then defined in terms of the axioms which are obeyed by the vectors and the elements of a field. Some important results are then reviewed, such as the basis theorem and the theorem on the dimension of a subspace. Finally, the special relationship between the dimension and the degree for vector spaces of degree n is obtained.

Introduction

There are two main ways to study vector spaces, the concrete and the abstract, and these have different advantages and disadvantages. In the concrete approach to vector spaces, a vector space is a set of ordered n-tuples of elements of $\mathbb{F}$, where n is a positive integer, which are added component by component. Such a vector space is called a 'vector space of degree n'. As a consequence, the elements are familiar, the calculations are easy and there are direct applications to linear equations and Euclidean geometry. The main disadvantage is that the results on vector spaces of degree n require generalization in order to apply even to some vector spaces which are important in linear algebra. Alternatively, what we may call 'abstract vector spaces' have the advantages that, because the vectors only have to satisfy a set of axioms and not be of any particular kind, the results can easily be applied widely outside linear algebra. Furthermore, all proofs are clearer because they are not obscured by details of calculation and there are no special results which hold only for spaces of a given degree. On the other hand, a study of abstract vector spaces includes a study of vector spaces of degree n as the principal example. In this chapter we shall review both of these methods of definition and bring out their main difference. As the results in this chapter are all aspects of results from any first linear algebra course, proofs of the results will be omitted. Instead there will be references to the theorems and propositions in *Linear Algebra* by R.B.J.T. Allenby, although those who have other textbooks for a first course will almost certainly find them in their books.

The origin of vector spaces of degree n lies in the vectors of mechanics in two or three dimensions, for which vector analysis was designed. The theory of vector spaces generalizes this but lacks the scalar (or dot) and vector (or cross) products. In fact, the scalar product will reappear in Chapter 10 when we discuss Euclidean vector spaces, but

the vector product has no place at all in vector space theory. A **vector** in mechanics is something with magnitude and direction, such as velocity or force, and, although it may have a line of action, vectors acting at a point A are usually considered. If we take A as the origin for a set of Cartesian coordinates in three dimensions, we can represent each vector $\mathbf{v}$ by the point P which lies in the direction of $\mathbf{v}$ at distance equal to the magnitude of $\mathbf{v}$. The point P then has Cartesian coordinates (a, b, c), where $a, b, c \in \mathbb{R}$, and we can represent $\mathbf{v}$ by (a, b, c). If $r \in \mathbb{R}$ and $\mathbf{w}$ is the vector represented by (d, e, f) then the laws of mechanics prove that the vector in the direction of $\mathbf{v}$ but with magnitude multiplied by r is represented by (ra, rb, rc) and the sum $\mathbf{v} + \mathbf{w}$ of the vectors $\mathbf{v}$ and $\mathbf{w}$ is represented by $(a + d, b + e, c + f)$. We may also regard the ordered triple (a, b, c) which represents the vector $\mathbf{v}$ as a vector which determines the point P, and then we call it a **position vector**. The set of all the position vectors with respect to a given set of Cartesian axes either in a plane or in space is then regarded as a vector space. However, we can make this idea more precise and make some obvious generalizations at the same time. Clearly, if the vector space is not necessarily representing something in mechanics or geometry, there is no need to restrict the definition to ordered pairs or triples, as ordered n-tuples will work just as well. Also, it would often be convenient to use $\mathbb{Q}$ or $\mathbb{C}$ instead of $\mathbb{R}$, so it is a useful idea to replace $\mathbb{R}$ in the definition by a field $\mathbb{F}$. These changes lead to the following.

• Definition 1

Let n be a positive integer and $\mathbb{F}$ be a field. The **total vector space of degree n over $\mathbb{F}$**, denoted by $\mathbb{F}^n$, is the set of all ordered n-tuples $\mathbf{v} = (a_1, a_2, a_3, ..., a_n)$ called **vectors**, where $a_1, a_2, a_3, ..., a_n \in \mathbb{F}$, with the operations of addition and multiplication by an element $c \in \mathbb{F}$ defined by

$$\mathbf{v} + \mathbf{w} = (a_1 + b_1, a_2 + b_2, a_3 + b_3, ..., a_n + b_n)$$

and

$$c\mathbf{v} = (ca_1, ca_2, ca_3, ..., ca_n),$$

where $\mathbf{w} = (b_1, b_2, b_3, ..., b_n)$.

It is frequently convenient to write the n-tuple $(a_1, a_2, a_3, ..., a_n)$ in $\mathbb{F}^n$ as the one-row matrix $\mathbf{u} = (a_1 \ a_2 \ a_3 \ .... \ a_n)$ or as the one column matrix $\mathbf{v}$, which we then call the **row vector u** or the **column vector v**. The column-vector form is very frequently used but is written in the form $\mathbf{v} = \mathbf{u}^{\mathrm{T}} = (a_1 \ a_2 \ a_3 \ ... \ a_n)^{\mathrm{T}}$ as this is more convenient. Definition 1 then defines the addition and multiplication by scalars of row or column vectors as addition and multiplication by scalars of matrices, consequently vectors in $\mathbb{F}^n$ are treated as either row or column vectors whenever it is convenient. The definition of $\mathbb{R}^3$ covers the vector space of all position vectors in space which are situated at the origin. But, although all the position vectors of points in a plane K through the origin appear to form a vector space of dimension 2, this vector space is not recognized by Definition 1 unless we set up a new set of coordinate axes in K with the same origin. This is the reason for the following definition of a wider class of vector space.

• Definition 2

Let n be a positive integer and $\mathbb{F}$ be a field. A **vector space of degree n over $\mathbb{F}$** is a non-empty set V of ordered n-tuples of elements of $\mathbb{F}$ such that

(i) $\mathbf{v} + \mathbf{w} \in V$ for all $\mathbf{v}, \mathbf{w} \in V$,
(ii) $c\mathbf{v} \in V$ for all $\mathbf{v} \in V$ and for all $c \in \mathbb{F}$,

where $\mathbf{v} + \mathbf{w}$ and $c\mathbf{v}$ are defined as in Definition 1.

With this definition the vectors in a plane or a line through the origin of Cartesian coordinates in a Euclidean geometry of dimension 2 or 3 form vector spaces of degree 2 or 3, respectively, over $\mathbb{R}$. Furthermore, the lines define vector spaces of dimension 1 and the planes define vector spaces of dimension 2, as we shall define them later. However, if K is a plane which is not through the origin, the position vectors of the points in the plane do not form a vector space, although they form a set $\{\mathbf{p} + \mathbf{x} : \mathbf{x} \in X\}$ where $\mathbf{p}$ is the position vector of a point in K with respect to the axes and X is a vector space of dimension 2 over $\mathbb{R}$. The vector space X is an example of a vector space of solutions of exactly one homogeneous linear equation and this serves to bring out the relation between the dimensions in Euclidean geometry and linear algebra: when the geometry can be represented as a vector space, the two dimensions are equal. The importance of vector spaces of degree n is brought out by the following three examples.

○ Example 1

Let V be the set of solutions of a system of homogeneous linear equations in n unknowns over a field $\mathbb{F}$. Then V can be regarded as a set of n-row column vectors over $\mathbb{F}$ which satisfy the system of equations $\mathbf{Ax} = \mathbf{0}$. Obviously $\mathbf{0} \in V$ and if $\mathbf{a}, \mathbf{b} \in V$ and $c \in \mathbb{F}$, then $\mathbf{Aa} = \mathbf{0}$ and $\mathbf{Ab} = \mathbf{0}$, therefore $\mathbf{A}(\mathbf{a} + \mathbf{b}) = \mathbf{Aa} + \mathbf{Ab} = \mathbf{0}$ and $\mathbf{A}(c\mathbf{a}) = c(\mathbf{Aa}) = \mathbf{0}$. Therefore, by Definition 2, V is a vector space of degree n over $\mathbb{F}$.

○ Example 2

Let $S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, ..., \mathbf{v}_k\}$ be a non-empty finite subset of $\mathbb{F}^n$ and let V be the set of all linear combinations of vectors in S, where a **linear combination** of the elements of S is a vector of the form

$$\sum_{j=1}^{k} c_j \mathbf{v}_j = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 + \ldots + c_k\mathbf{v}_k$$

where $c_1, c_2, c_3, ..., c_k \in \mathbb{F}$. By taking all the coefficients $c_j = 0$, it follows that $\mathbf{0} \in V$. It is easy to rearrange the sum of two linear combinations,$\mathbf{v}$ as above and $\mathbf{w} = \sum_{j=1}^{k} d_j \mathbf{v}_j$, in order to make the linear combination $\sum_{j=1}^{k} (c_j + d_j)\mathbf{v}_j$, and, for all $a \in \mathbb{F}$, the scalar product $a\mathbf{v} = \sum_{j=1}^{k} ac_j \mathbf{v}_j$ for all $a \in \mathbb{F}$ is another, therefore V is vector space of degree n over $\mathbb{F}$. V is called the **vector space over $\mathbb{F}$ spanned or generated by** S and denoted by $V = \langle S \rangle$ or by

$$V = \langle \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_k \rangle.$$

In fact, because the zero vector $\mathbf{0}$ belongs to V even if $S = \varnothing$, the **zero vector space** $\{\mathbf{0}\}$ consisting only of the zero vector can be regarded as the vector space spanned by $\varnothing$.

⊙ *Example 3*

There are two common uses of vector spaces spanned by a set of vectors which are associated with a matrix. For example, if $\mathbf{A}$ is the matrix over $\mathbb{Q}$ given by

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & -2 & 7 \\ 2 & 5 & 3 & 0 \\ 0 & -3 & -1 & 8 \end{pmatrix},$$

then the **row space** R **of** $\mathbf{A}$ is the space spanned by the rows of $\mathbf{A}$, that is,

$$R = \langle (1 \quad 1 \quad -2 \quad 7),\ (2 \quad 5 \quad 3 \quad 0),\ (0 \quad -3 \quad -1 \quad 8) \rangle$$

and the **column space** C **of** $\mathbf{A}$ is the space spanned by the columns of $\mathbf{A}$, that is,

$$C = \langle (1 \quad 2 \quad 0)^{\mathrm{T}},\ (1 \quad 5 \quad -3)^{\mathrm{T}},\ (-2 \quad 3 \quad -1)^{\mathrm{T}},\ (7 \quad 0 \quad 8)^{\mathrm{T}} \rangle.$$

Examples 1, 2 and 3 include many of the most important applications of vector spaces in linear algebra, but even inside that subject there are sets which seem to be examples of abstract vector spaces but which are not vector spaces of degree m for any integer m. For example, consider the set $\mathrm{M}_n(\mathbb{F})$ of all $n \times n$ matrices over the field $\mathbb{F}$. The operations of addition and multiplication by scalars for a matrix $\mathbf{A} \in \mathrm{M}_n(\mathbb{F})$ are the same as the vector space operations on $\mathbf{A}$ with the rows combined into a single row or the columns combined as a single column. Either of these would be a vector space of degree n^2 over $\mathbb{F}$, but in the row- or column-vector form would lose the properties of the matrices such as the matrix product. The way out of this difficulty is to widen the definition of a vector space even further in order to remove any requirement for the vectors to be of any particular kind. To this end, we list some properties of vector spaces of degree n over a field $\mathbb{F}$, which are all basic properties of matrices, and we use these properties to create a more general definition of a vector space. These properties of a vector space V of degree n over a field $\mathbb{F}$ are the **vector space axioms** (see *Linear Algebra*, Chapter 6, Axioms VS):

1 $\forall\, \mathbf{x}, \mathbf{y} \in V,\ \mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$;
2 $\forall\, \mathbf{x}, \mathbf{y}, \mathbf{z} \in V,\ (\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z})$;
3 $\exists\, \mathbf{0} \in V$ such that, $\forall\, \mathbf{x} \in V,\ \mathbf{x} + \mathbf{0} = \mathbf{x}$;
4 for each $\mathbf{x} \in V, \exists\, (-\mathbf{x}) \in V$ such that $\mathbf{x} + (-\mathbf{x}) = \mathbf{0}$;
5 $\forall\, \mathbf{x}, \mathbf{y} \in V$ and $\forall\, a \in \mathbb{F},\ a(\mathbf{x} + \mathbf{y}) = a\mathbf{x} + a\mathbf{y}$;
6 $\forall\, \mathbf{x} \in V$ and $\forall\, a, b \in \mathbb{F},\ (a + b)\mathbf{x} = a\mathbf{x} + b\mathbf{x}$;
7 $\forall\, \mathbf{x} \in V$ and $\forall\, a, b \in \mathbb{F},\ a(b\mathbf{x}) = (ab)\mathbf{x}$;
8 $\forall\, \mathbf{x} \in V,\ 1\mathbf{x} = \mathbf{x}$.

Below, in Definition 3, we can define (abstract) vector spaces by means of these axioms. Some caution is needed when defining a mathematical object by means of axioms, because it is possible to state axioms that nothing whatever satisfies. A simple

example (though not using axioms) is a non-empty subset of $\{x \in \mathbb{R} : x^2 + 1 = 0\}$. On this occasion the difficulty cannot arise because we know that all vector spaces of degree n over $\mathbb{F}$, including $\mathbb{F}^n$, satisfy the axioms.

• Definition 3

Let $\mathbb{F}$ be a field and V be a set on which the operations of **addition** and **multiplication by scalars** are defined:

(i) $\forall\, \mathbf{x}, \mathbf{y} \in V,\ \exists\, \mathbf{x} + \mathbf{y} \in V$;
(ii) $\forall\, \mathbf{x} \in V$ and $\forall\, a \in \mathbb{F},\ \exists\, a\mathbf{x} = \mathbf{x}a \in V$.

Then V is a **vector space over** $\mathbb{F}$ and its elements are called **vectors** if V satisfies the vector space axioms.

Here is an example taken from algebra which is an abstract vector space but not a vector space of degree n, for any integer n.

⊙ Example 4

The set $\mathbb{F}[x]$ of all polynomials in an indeterminate x over a field $\mathbb{F}$ is a vector space over $\mathbb{F}$ with the operations of adding polynomials and multiplying a polynomial by a scalar, as can be proved from the rules of algebra. $\mathbb{F}[x]$ cannot be regarded as a vector space of any degree n at all because the number of coefficients of the polynomials can be chosen to exceed any given integer. It follows from this that the vector space axioms admit vector spaces which are essentially different from the vector spaces of degree n. Therefore some extra axiom is needed if we wish to restrict our investigations to vector spaces which resemble vector spaces of finite degree in some abstract sense.

There is a wide range of examples of vector spaces in Chapter 6 of *Linear Algebra*. To show that the set of vector space axioms is meaningful we also need to find examples of sets which do not satisfy them. This is actually too easy, in that we can define sets that could not possibly be vector spaces. For example, although a cow has magnitude and direction and therefore can be taken to be a vector, a herd of cows spread over a real field could never be a vector space. What is really required is a set which looks like a vector space but actually is not one, such as the set of all positive functions of a real variable. This cannot be a vector space over $\mathbb{R}$ because the product of a positive function by -1 is not positive, therefore the multiplication by scalars cannot be completely defined. Alternatively, consider the following example.

⊙ Example 5

Consider the set S of all solutions of the system of linear equations over $\mathbb{Q}$ given by $2x - y = 3$ and $x + y = 3$. The column vectors $\mathbf{u} = (2 \quad 1)^{\mathrm{T}}$ and $\mathbf{v} = (1 \quad -1)^{\mathrm{T}}$ are solution vectors for this system but $\mathbf{u} + \mathbf{v} = (3 \quad 0)^{\mathrm{T}}$ is not a solution. Consequently S is not a vector space over $\mathbb{Q}$ according to Definition 3.

In the following we will define a 'subspace' to have the same relationship that a vector space of degree n over $\mathbb{F}$ has with $\mathbb{F}^n$. The parallel is very close, as is clear from the criterion that follows the definition, although not all subspaces have the special properties which hold for vector spaces of degree n.

• Definition 4

Let V be a vector space over a field $\mathbb{F}$ and let U be a non-empty subset of V. Then U is a **subspace** of V if U is a vector space over $\mathbb{F}$ with the same operations of addition and scalar multiplication as V.

• Proposition 1 (*Linear Algebra*, Chapter 7, Theorem 1)

Let V be a vector space over $\mathbb{F}$ and let U be a non-empty subset of V. Then U is a subspace of V if and only if

(i) $\mathbf{v} + \mathbf{w} \in U$ for all $\mathbf{v}, \mathbf{w} \in U$,
(ii) $c\mathbf{v} \in U$ for all $\mathbf{v} \in U$ and for all $c \in \mathbb{F}$.

The following example shows the way the idea of a subspace can be used.

☺ Example 6

Let $\mathcal{D}$ be an operator which represents differentiation with respect to a real variable x. Let W be the set of all real functions $f(x)$ of x such that $\mathcal{D}^n f(x)$ is defined for every positive integer n. Essentially, W is the set of functions which is studied in differential calculus. Let V be the subset of W which consists of all the solutions of the differential equation $(\mathcal{D}^2 - 1)y = 0$. If $f(x)$ and $g(x)$ belong to V, then, $(\mathcal{D}^2 - 1)[f(x) + g(x)] = (\mathcal{D}^2 - 1)f(x) + (\mathcal{D}^2 - 1)g(x) = 0$ by the laws of calculus, therefore $f(x) + g(x) \in V$. Similarly, for any $c \in \mathrm{R}$, $cf(x) \in V$. The zero function defined by $z(x) = 0$ for all x obviously satisfies $(\mathcal{D}^2 - 1)z(x) = 0$, therefore $V \neq \varnothing$. Consequently, by Proposition 1, V is a subspace of the vector space W.

The basic properties of a vector space can be deduced as general principles from the vector space axioms without any need to refer to the specific vector space under consideration. For example, it is easy to prove, as in *Linear Algebra*, Chapter 6, Theorem 1, that the zero vector $\mathbf{0}$ in the vector space V over the field $\mathbb{F}$ is unique and that, for any $\mathbf{v} \in V$ and $0 \in \mathbb{F}$, we have $0\mathbf{v} = \mathbf{0}$. These results can then be used to prove that, for arbitrary $\mathbf{v} \in V$, there exists exactly one vector $-\mathbf{v}$ which is equal to $(-1)\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$. Therefore the operation of **subtraction** of vectors $\mathbf{v}, \mathbf{w} \in V$ can be defined by $\mathbf{v} - \mathbf{w} = \mathbf{v} + (-\mathbf{w})$.

The vector space axioms are not the smallest possible set that could be used to define vector spaces, but they set out the basic properties of vector spaces conveniently. Actually, Axioms 1 and 2 have two useful consequences that we should note. The less obvious one is that Axiom 2 implies that no brackets are required in expressions which only use addition, so the sum $\mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{d}$ is precisely defined without including any brackets. An obvious consequence of Axiom 1 is that the order in which the vectors appear in a sum does not matter, and so $\mathbf{b} + \mathbf{c} + \mathbf{a} = \mathbf{a} + \mathbf{b} + \mathbf{c}$ whatever vector space the vectors belong to. It is less obvious that we need both these results before we can introduce the following notation for a linear combination:

$$\sum_{j=1}^{m} c_j \mathbf{v}_j = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 + \ldots + c_m\mathbf{v}_m,$$

where $c_j \in \mathbb{F}$ and $\mathbf{v}_j \in V$ for $j = 1, 2, 3, \ldots, m$.

The reason why we have tried to extend the definition of a vector space in order to include more general sets is that the concept of linear dependence, which we define next, has been so valuable in the discussion of linear equations and related topics that it is desirable to apply it in wider contexts. The generalization from total vector spaces to abstract vector spaces is then designed to allow all the original results about linear dependence to hold in the abstract vector spaces. This has not quite been achieved because, according to Example 4, some vector spaces as determined by Definition 3 differ essentially from vector spaces of degree n, and the rest of this chapter is devoted to developing the theory of vector spaces in order to express the main special property of vector spaces of degree n in a form that can be used in abstract vector spaces.

• Definition 5

Let V be a vector space over a field $\mathbb{F}$, let k be positive integer and let $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_k$ be vectors in V, not necessarily distinct. Then the set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_k\}$ is **linearly dependent over** $\mathbb{F}$ if there exist $c_1, c_2, c_3, \ldots, c_k \in \mathbb{F}$, not all of which are zero, such that $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 + \ldots + c_k\mathbf{v}_k = \mathbf{0}$. Alternatively, if the set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_k\}$ is not linearly dependent, then it is **linearly independent over** $\mathbb{F}$. That is, the set is linearly independent over $\mathbb{F}$ if the only solution of the equation $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 + \ldots + c_k\mathbf{v}_k = \mathbf{0}$, where $c_1, c_2, c_3, \ldots, c_k \in \mathbb{F}$, is $c_1 = c_2 = c_3 = \ldots = c_k = 0$.

Instead of referring to the set of vectors in Definition 5, it is often written informally that the vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_k$ are linearly dependent or independent over $\mathbb{F}$, which causes no problems provided that the property of being linearly dependent is applied only to **sets** of vectors. Definition 5 can be extended to infinite sets by saying that an infinite set S of vectors over $\mathbb{F}$ is linearly dependent over $\mathbb{F}$ if and only if a finite subset of S is linearly dependent over $\mathbb{F}$. Alternatively, S is linearly independent over $\mathbb{F}$ if and only if every finite subset of S is linearly independent over $\mathbb{F}$. The following criterion of linear dependence of sets of non-zero vectors is often used. (Any set of vectors containing $\mathbf{0}$ is linearly dependent.)

• *Proposition 2 (Linear Algebra,* Chapter 8, Theorem 1)

A set of non-zero vectors S in a vector space V over a field $\mathbb{F}$ is linearly dependent over $\mathbb{F}$ if and only if at least one of the vectors can be written as a non-zero linear combination of a finite number of the others.

A method like that used in the following example can be used to determine whether a finite set of vectors in an arbitrary vector space is linearly dependent.

○ *Example 7*

Is the set of the polynomials $S = \{p(x), q(x), r(x), s(x)\} \in \mathbb{Q}[x]$ linearly dependent over $\mathbb{Q}$, where $p(x) = x^3 + 2x^2 + 1$, $q(x) = x^2 - x + 1$, $r(x) = 2x^3 + 2x + 2$ and $s(x) = x^3 - x^2 + x + 2$? To decide this, let $t, u, v, w \in \mathbb{Q}$ and let the linear combination $tp(x) + uq(x) + vr(x) + ws(x) = 0 \in \mathbb{Q}[x]$. By equating the coefficients of x^3, x^2, x and 1, we obtain the following system of homogeneous linear equations:

$$\begin{aligned} t \quad &+2v+ \ w=0,\\ 2t+u \quad &- \ w=0,\\ -u+2v+ \ &w=0,\\ t+u+2v+2w&=0. \end{aligned}$$

We take the matrix of coefficients of this system of equations and reduce it to echelon form by elementary operations over $\mathbb{Q}$, as follows:

$$\begin{pmatrix} 1 & 0 & 2 & 1 \\ 2 & 1 & 0 & -1 \\ 0 & -1 & 2 & 1 \\ 1 & 1 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & -4 & -3 \\ 0 & -1 & 2 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & -4 & -3 \\ 0 & 0 & -2 & -2 \\ 0 & 0 & 4 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & -4 & -3 \\ 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Because the equivalent system in echelon form has fewer non-trivial equations than unknowns, there is a non-trivial solution for the system of equations, and therefore there exist values for t, u, v, w which are not all zero such that $tp(x) + uq(x) + vr(x) + ws(x) = 0$. Therefore the polynomials $p(x)$, $q(x)$, $r(x)$, $s(x)$ are linearly dependent over $\mathbb{Q}$ according to Definition 5. Unless further results are needed, there is no need to solve this system of homogeneous linear equations.

The reason why the results on vector spaces are so often used is that they combine the ideas of linear combinations and linear independence, as in the following definition.

• Definition 6

Let V be a vector space over a field $\mathbb{F}$. A **basis** of V is a spanning set of V which is linearly independent over $\mathbb{F}$.

The total vector space $\mathbb{F}^n$ has an obvious basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, ..., \mathbf{e}_n\}$, where $\mathbf{e}_j = (0, 0, 0, ..., 0, 1, 0, ..., 0)$ has 1 in the jth place, and this is called the **standard basis** of $\mathbb{F}^n$. The vector space $\mathbb{F}[x]$ of all polynomials in x over $\mathbb{F}$ has the obvious basis $\{1, x, x^2, x^3, ..., x^n, ...\}$, although this is infinite. However, each vector space has many bases. In particular, if a finite spanning set of a vector space is known, a basis can be found which is a subset of the spanning set, as in the following example.

☺ Example 8

Let V be the vector space of polynomials in $\mathbb{Q}[x]$ spanned by the set of polynomials S of Example 7. By Definition 6, S is not a basis of V because S is linearly dependent over $\mathbb{F}$ by Example 7. However, it follows from Proposition 2 that one element of S is a non-zero linear combination of the others, and this can be found by solving the system of linear equations in echelon form in Example 7 by back substitution. These equations have the general solution $w = \theta$, $v = -\theta$, $u = -\theta$, $t = \theta$ for arbitrary $\theta \in \mathbb{Q}$. We choose $\theta = 1$ and deduce that $p(x) - q(x) - r(x) + s(x) = 0$. Consequently, the polynomial $s(x)$ is

the linear combination $s(x) = -p(x) + q(x) + r(x)$ of the others, and therefore $B = \{p(x), q(x), r(x)\}$ is a spanning set for V. The working of Example 7 can then be reused to show that B is linearly dependent over $\mathbb{Q}$ if and only if there is a non-trivial solution of the homogeneous linear equations with matrix of coefficients $\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 2 \end{pmatrix}$.

As this matrix in echelon form has no zero row, the system of linear equations only has trivial solutions. Therefore B is linearly independent over $\mathbb{Q}$ and B is a basis of V by Definition 6.

The method of Example 8 can be used to construct a basis of a vector space V from a spanning set of V. The major use of a basis of a vector space comes from the following result.

• Theorem 1

Let B be a basis of the vector space V over the field $\mathbb{F}$. Then each vector $\mathbf{v} \in V$ is equal to a unique linear combination over $\mathbb{F}$ of the elements of B.

PROOF

Let $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, ..., \mathbf{b}_m\}$ be a basis of V. Suppose that for $\mathbf{v} \in V$ there exist $c_j, d_j \in \mathbb{F}$, for $j = 1, 2, 3, ..., m$, such that

$$\mathbf{v} = c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + c_3\mathbf{b}_3 + ... + c_m\mathbf{b}_m$$

and

$$\mathbf{v} = d_1\mathbf{b}_1 + d_2\mathbf{b}_2 + d_3\mathbf{b}_3 + ... + d_m\mathbf{b}_m.$$

Therefore

$$\mathbf{0} = (c_1 - d_1)\mathbf{b}_1 + (c_2 - d_2)\mathbf{b}_2 + (c_3 - d_3)\mathbf{b}_3 + ... + (c_m - d_m)\mathbf{b}_m$$

and therefore $c_j - d_j = 0$, by Definition 6, because B is linearly independent over $\mathbb{F}$. Therefore $\mathbf{v}$ is equal to the unique linear combination $c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + c_3\mathbf{b}_3 + ... + c_m\mathbf{b}_m$ of the elements of B. ●

In order to study vector spaces abstractly, we now intend to seek an abstract property which holds for all vector spaces of degree n, which are simply the subspaces of $\mathbb{F}^n$. As $\mathbb{F}^n$ has a finite basis we continue this search by studying vector spaces with finite bases. Here is the main theorem for such vector spaces, which is called the **basis theorem**.

• Theorem 2 (*Linear Algebra*, Chapter 9, Theorem 1)

Let V be a vector space over a field $\mathbb{F}$, let n be a positive integer and let V have a basis B consisting of n vectors. Then any subset of V which contains more than n elements is linearly dependent over $\mathbb{F}$.

Theorem 2 has an immediate consequence, which we state as Proposition 3, and this allows us to make the definition that follows it.

• *Proposition 3 (Linear Algebra, Chapter 9, Theorem 2)*

Let V be a vector space over the field $\mathbb{F}$ with a basis consisting of n vectors. Then every basis of V contains n vectors.

• Definition 7

Let V be a vector space over a field $\mathbb{F}$ and let n be a positive integer. Then V has **dimension** n over $\mathbb{F}$, written $\dim_{\mathbb{F}} V = n$ or $\dim V = n$, if V has a basis consisting of n vectors in V. The dimension of the zero vector space $\{\mathbf{0}\}$ over $\mathbb{F}$ is defined to be 0.

The total vector space of degree n over $\mathbb{F}$ has dimension n because $\mathbb{F}^n$ has the standard basis with n vectors, whereas $\mathbb{F}[x]$ is infinite-dimensional. The theorem which follows is an immediate consequence of Theorem 2.

• *Theorem 3 (Linear Algebra, Chapter 9, Theorem 5′)*

Let n be a positive integer, let V be a vector space of dimension n over a field $\mathbb{F}$ and let U be a subspace of V. Then U is of finite dimension m and $m \leq n$.

The following result is the required distinctive result on vector spaces of degree n. It is an immediate consequence of Theorem 3 because $\dim_{\mathbb{F}} \mathbb{F}^n = n$ and the two examples which follow show its significance.

• *Theorem 4*

Let n be a positive integer and let V be a vector space of degree n over a field $\mathbb{F}$. Then the dimension d of V is finite and $d \leq n$.

◎ *Example 9*

Let V be the solution space of m homogeneous linear equations in n unknowns over a field $\mathbb{F}$. Then V is a vector space of degree n and therefore V is of finite dimension $k \leq n$ over $\mathbb{F}$.

⊖ *Example 10*

Let $\mathbf{A}$ be an $m \times n$ matrix over the field $\mathbb{F}$. Then, as in Example 2, there is a row space R of degree n spanned by the rows of $\mathbf{A}$ and a column space C of degree m spanned by the columns of $\mathbf{A}$. By Theorem 4, $\dim_{\mathbb{F}} R = r$ is finite and $r \leq n$ and $\dim_{\mathbb{F}} C = c$ is finite and $c \leq m$. The dimension r is called the **row rank** of $\mathbf{A}$ and c is called the **column rank** of $\mathbf{A}$. By a frequently used result (*Linear Algebra*, Chapter 9, Theorem 3), $r = c$ and their common value is called the **rank** of $\mathbf{A}$ over $\mathbb{F}$.

Let V be a vector space with a finite spanning set S. The method of Example 8 can be used a finite number of times to construct a basis of V. However, as the following example shows, this method does not work for infinite-dimensional vector spaces.

○ *Example 11*

Consider $\mathbb{F}[x]$ as a vector space over the field $\mathbb{F}$. $\mathbb{F}[x]$ is spanned by any subset K which contains exactly two polynomials of each degree m for $m = 0, 1, 2, 3, \ldots$. If, alternatively, K contained exactly one polynomial of each degree m, then K would be a basis, so we wish to delete just one polynomial of each degree from K. To attempt to do this,

we assume that K is written as a sequence and we form K_0 by deleting the first constant polynomial in K. We then form K_n, $n = 1, 2, 3, \ldots$, recursively by deleting the first polynomial of degree n which occurs in k_{n-1}. The sequence K_n is therefore constructed in a finite number of steps but, no matter how large n is, an unwanted infinity of polynomials remains in K_n.

The construction of a basis of a vector space V of finite dimension n over a field $\mathbb{F}$ from a spanning set may suggest that V has relatively few bases and these are difficult to find. However, this is not true, as the following results show.

• *Proposition 4 (Linear Algebra, Chapter 8, Theorem 4)*

Let n be a positive integer, let V be a vector space of dimension n over the field $\mathbb{F}$ and let $S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_n\}$ be a linearly independent subset of V. Then S is a basis of V.

• *Proposition 5 (Linear Algebra, Chapter 9, Theorem 4)*

Let n be a positive integer, let V be a vector space of dimension n over the field $\mathbb{F}$ and let R be a subset of V which is linearly independent over $\mathbb{F}$. Then V has a finite subset T such that $R \cap T = \varnothing$ and $R \cup T$ is a basis of V.

Because $\{\mathbf{v}\}$ is a linearly independent set of vectors over $\mathbb{F}$ if and only if $\mathbf{v} \neq \mathbf{0}$, there exists a basis containing any non-zero vector in V. Therefore V has at least as many bases as non-zero vectors.

◉ *Example 12*

Let $P = \mathrm{P}_3(\mathbb{Q})$ be the vector space of polynomials of degree at most 3 over $\mathbb{Q}$ together with 0 and let $\mathbf{b}_1 = x^2 - 5x + 9$. Because $\{1, x, x^2, x^3\}$ is a basis of P, $\dim_{\mathbb{Q}} P = 4$. Because $\mathbf{b}_1 \neq \mathbf{0}$ the set $B_1 = \{\mathbf{b}_1\}$ is linearly independent over $\mathbb{Q}$ but $\langle B_1 \rangle$ is of dimension 1 and every non-zero polynomial in it is of degree 2, therefore a polynomial of degree 0 such as $\mathbf{b}_2 = 1 \notin \langle B_1 \rangle$. Therefore $B_2 = \{\mathbf{b}_1, \mathbf{b}_2\}$ is linearly independent over $\mathbb{Q}$ and $\dim_{\mathbb{Q}} \langle B_2 \rangle = 2$. Because $\langle B_2 \rangle = \{a(x^2 - 5x) + b \ : \ a, b \in \mathbb{Q}\}$ the polynomial $\mathbf{b}_3 = x + 1 \notin \langle B_2 \rangle$ therefore $B_3 = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$ is linearly independent over $\mathbb{Q}$ and $\dim_{\mathbb{Q}} \langle B_3 \rangle = 3$. Obviously $\langle B_3 \rangle$ contains no polynomial of degree 3, therefore it does not contain $\mathbf{b}_4 = x^3 + 2x^2 - 7x + 1$, consequently $B_4 = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4\}$ is a linearly independent set of four vectors in P, which is of dimension 4. By Proposition 4, B_4 is a basis of P.

Summary

The concept of **linear dependence** is used in many parts of mathematics and its proper context is the **vector space**. Here we have studied vector spaces from two definitions. We defined a vector space of **degree** n as a suitable set of column vectors each containing n elements with addition and multiplication by scalars defined as for matrices, and this definition led immediately to applications to linear equations and matrices. The alternative definition we gave is abstract, assuming for a given set the existence of addition and multiplication by scalars which satisfy a convenient set of axioms. This definition has the advantage of covering many kinds of vector spaces, such as sets of polynomials or functions, and contains all the vector spaces of finite degree. However,

we discovered disadvantages of this wider definition in that it includes vector spaces which cannot be studied by the methods of linear algebra and that some of the methods of linear algebra, such as the use of matrices, cannot be applied directly to general abstract vector spaces. These difficulties led us to search for conditions, effectively an extra axiom, which would restrict the vector spaces considered to those with properties like the vector spaces of finite degree. Two concepts were important in this search. First, a **subspace** of a vector space has the same relation to an arbitrary vector space as a vector space of degree n has to the **total vector space of degree** n consisting of all column vectors with n elements. Second, a **basis** B of a vector space V, is a linearly independent subset of V such that each vector in V can be written as a linear combination of vectors in B. We ended by showing that if a vector space has a finite basis then so do all its subspaces, and consequently every vector space of degree n has a finite basis.

EXERCISES ON CHAPTER 3

1. Which of the following sets of vectors are vector spaces of degree 3 over $\mathbb{R}$?

(i) $\{x(2, 3, 1) + y(1, 4, 4) : x, y \in \mathbb{R}\}$.

(ii) $\{(x, y, z) : x, y, z \in \mathbb{R}, 3x + 4y = 1\}$.

(iii) $\{(x, y, z) : x, y, z \in \mathbb{R}, 7x - y = 0\}$.

(iv) $\{\mathbf{r} : \mathbf{r}$ ranges over the position vectors of points in the plane with equation $3x - 2y + 7z + 4 = 0\}$.

2. Prove from the vector space axioms that if V is a vector space over a field $\mathbb{F}$ and $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in V$ then

$$(\mathbf{a} + \mathbf{b}) + (\mathbf{c} + \mathbf{d}) = (\mathbf{a} + (\mathbf{c} + \mathbf{b})) + \mathbf{d}.$$

3. Which of the following are vector spaces over $\mathbb{R}$?

(i) The set of 4×4 matrices $\mathbf{A}$ over $\mathbb{R}$ such that $\mathbf{A}^{\mathrm{T}} = \mathbf{A}$ under the matrix operations of addition and multiplication by scalars.

(ii) The set of all polynomials in an indeterminate x over $\mathbb{R}$ with roots -1 and 1 under the operations of addition and multiplication by scalars for polynomials.

(iii) The set S of all real-valued functions of a real variable x with the property that, for each $f \in S$, there exist $a, b \in \mathbb{R}$ (depending on f) such that $f(x)$ is defined for all $x \in \mathbb{R}$ with $a \leq x \leq b$ under the addition and multiplication by scalars over $\mathbb{R}$ of real functions.

(iv) The set of all real-valued functions of a real variable x which are differentiable for all $x \in \mathbb{R}$ under the addition and multiplication by scalars over $\mathbb{R}$ of real functions.

4. Let V be a vector space over a field $\mathbb{F}$ and let U and W be subspaces of V. Let $U + W = \{\mathbf{u} + \mathbf{w} : \mathbf{u} \in U, \mathbf{w} \in W\}$. Show that $U \cap W$ and $U + W$ are subspaces of V.

5. Which of the following sets of vectors are linearly dependent over the field $\mathbb{F}$ in the given vector space V?

(i) $\mathbb{F} = \mathbb{Q}$, $V = \mathbb{Q}^3$; $\{(1, 0, 1), (0, 2, 2), (3, 7, 1)\}$.

(ii) $\mathbb{F} = \mathbb{R}$, $V = \mathrm{M}_4(\mathbb{R})$; $\{\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}\}$ where the 4×4 matrices are given by $\mathbf{A} = 3\mathbf{I}$,

$$\mathbf{B} = \begin{pmatrix} \mathbf{0} & \mathbf{I}_2 \\ 5\mathbf{I}_2 & \mathbf{0} \end{pmatrix}, \mathbf{C} = \mathbf{0} \text{ and } \mathbf{D} = \begin{pmatrix} 4\mathbf{I}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_2 \end{pmatrix}.$$

(iii) $\mathbb{F} = \mathbb{Q}$, $V = \mathbb{Q}[x]$; $\{p(x), q(x), r(x)\}$, where

$$p(x) = 2x^5 + x^4 + 3x^3 - x^2 + 4x - 1,$$
$$q(x) = x^5 - x^4 + 2x^3 - 2x^2 + 3x - 3,$$
$$r(x) = x^5 + 5x^4 + 4x^2 - x + 7.$$

(iv) $\mathbb{F} = \mathbb{R}$, V is the vector space of real-valued functions defined for all $x \in \mathbb{R}$; $\{e^x, \sinh x, \cosh x\}$.

6. Which of the following sets S of vectors are bases of the given vector spaces V over the field $\mathbb{F}$?

(i) $\mathbb{F} = \mathbb{Q}$, $V = \mathbb{Q}^3$; $S = \{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}$.

(ii) $\mathbb{F} = \mathbb{R}$, $V = \mathrm{P}_2(\mathbb{R})$; $S = \{x^2 + 1, x + 1, 3x^2 + 7x + 1\}$.

(iii) $\mathbb{F} = \mathbb{R}$, $V = \langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle$ where $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ are linearly independent over $\mathbb{R}$; $S = \{2\mathbf{a} + \mathbf{b} + 3\mathbf{c}, 5\mathbf{a} + 3\mathbf{b} + 4\mathbf{c}, 2\mathbf{a} + 11\mathbf{c}\}$.

(iv) $\mathbb{F} = \mathbb{R}$, $V = \{(0, y, z) : y, z \in \mathbb{R}\}$; $S = \{(0, 0, 0), (0, 0, 1), (0, 1, 1)\}$.

7. Find a basis for the vector space over $\mathbb{Q}$ spanned by $\{(2, 2, -1), (3, -1, 2), (1, 5, -4)\}$.

8. Find a matrix in echelon form which is equivalent over $\mathbb{Q}$ to $\mathbf{A}$ and so obtain the row rank of $\mathbf{A}$ over $\mathbb{Q}$, where

$$\mathbf{A} = \begin{pmatrix} 2 & 6 & -5 & 8 \\ 4 & 3 & -1 & 7 \\ -1 & 1 & 6 & 0 \\ 5 & 2 & 4 & 7 \end{pmatrix}.$$

Repeat the process with $\mathbf{A}^{\mathrm{T}}$ and so obtain the column rank of $\mathbf{A}$ over $\mathbb{Q}$. What is the rank of $\mathbf{A}$ over $\mathbb{Q}$?

9. For the vector space V_i find a basis B_i which contains the set of vectors S_i, for $i = 1, 2, 3, 4, 5$.

(i) $V_1 = \mathbb{Q}^3$, $S_1 = \{(1, 2, 3)\}$.

(ii) $V_2 = \{re^{2x} + se^{3x} : r, s \in \mathbb{R}\}$ is the vector space of solutions of the differential equation $[\mathcal{D}^2 - 5\mathcal{D} + 6]y = 0$, $S_2 = \{2e^{2x}\}$.

(iii) $V_3 = \mathbb{R}^4$, $S_3 = \{(0, 2, 5, 9), (0, 0, 0, \sqrt{2})\}$.

(iv) V_4 is the subspace of $\mathbb{Q}^4$ of the solutions of the linear equations

$$\begin{aligned} w + 2x \qquad + 5z &= 0, \\ 3y + 6z &= 0, \end{aligned}$$

and $S_4 = \varnothing$.

(v) $V_5 = \mathrm{P}_4(\mathbb{Q})$, $S_5 = \{1 + x^2, 1 + x^3, 1 + x^4\}$.

10. Let V be a vector space of dimension n over a field $\mathbb{F}$, let U be a subspace of dimension m over $\mathbb{F}$ where $0 < m < n$, and let B be a basis of U. Show that V has a basis C such that $B \subset C$. Prove that there is a subspace W of V such that $U \cap W = \{\mathbf{0}\}$ and $\dim_{\mathbb{F}} W = n - m$.

4 · Linear Transformations

Outline

In vector spaces which are not of finite degree it is not possible to multiply a vector by a matrix of a suitable size, but this difficulty can be avoided by means of linear transformations. A 'linear transformation' is a mapping of a vector space into another which preserves vector addition and multiplication by scalars. For two vector spaces of finite degree such a mapping is necessarily a mapping $\mathbf{w} = \mathbf{A}\mathbf{v}$, where $\mathbf{A}$ is a matrix, and we call this a 'matrix linear transformation'. Consequently, linear transformations provide the required generalization of matrices to abstract vector spaces. The chapter continues by obtaining properties of linear transformations of vector spaces of finite dimension. These include the proof that a vector space V of finite dimension n over a field $\mathbb{F}$ is 'isomorphic' to $\mathbb{F}^n$, which means that V and $\mathbb{F}^n$ are abstractly identical. The relations between the mappings which map V onto $\mathbb{F}^n$ are then explored. Finally, the methods of this chapter are used to obtain inequalities concerning the rank of a product of two matrices $\mathbf{AB}$ in terms of rank $\mathbf{A}$ and rank $\mathbf{B}$.

Introduction

Let $\mathbb{F}$ be any field and m and n be positive integers. Then for $\mathbf{v} \in \mathbb{F}^n$ and an $m \times n$ matrix $\mathbf{A}$ we can write down $\mathbf{Av}$, which is a vector in $\mathbb{F}^m$, by taking $\mathbf{v}$ to be a column vector. This process is useful in many applications, but it is not possible in vector spaces which are not of finite degree, even if they are of finite dimension, because the process demands that both $\mathbf{A}$ and $\mathbf{v}$ should be matrices. We can try to avoid this difficulty by using the matrix in a more general way which can be applied to all finite-dimensional vector spaces. The method we shall use is to express the matrix $\mathbf{A}$ as a mapping, by means of the equation $\mathbf{w} = \mathbf{Av}$, which transforms the vector $\mathbf{v} \in V$ into the vector $\mathbf{w} \in W$. We call the mapping $\mathbf{w} = \mathbf{Av}$ a **matrix linear transformation**. Our discussion of matrix linear transformations and the introduction of general linear transformations will revise work that occurs in first courses in linear algebra, so we shall omit some proofs by referring to *Linear Algebra* by R.B.J.T. Allenby, as in Chapter 3. We start by interpreting some simple problems in terms of matrix linear transformations.

○ Example 1

Any system of linear equations over a field $\mathbb{F}$ can be written as $\mathbf{Ax} = \mathbf{b}$, where $\mathbf{A}$ is an $m \times n$ matrix over $\mathbb{F}$, $\mathbf{b} \in \mathbb{F}^m$ and $\mathbf{x}$ is an unknown element of $\mathbb{F}^n$. The problem of solving this system can be interpreted as the search for $\mathbf{v} \in \mathbb{F}^n$ such that the matrix linear transformation $\mathbf{w} = \mathbf{Av}$ has the value $\mathbf{b} \in \mathbb{F}^m$. This interpretation is not a help towards solving the system of equations, but is helpful for transforming a more abstract problem into one about linear equations. Alternatively, for a non-singular matrix $\mathbf{P}$, we can use

the linear transformation $\mathbf{v} = \mathbf{Pu}$ to transform the system of equations into a (possibly simpler) system $\mathbf{w} = (\mathbf{AP})\mathbf{u}$ and then seek $\mathbf{u}$ such that $\mathbf{w} = \mathbf{b}$.

In order to extend this idea to abstract vector spaces, we need to find abstract properties of matrix linear transformations which can serve as an abstract definition. It is easy to see that any matrix linear transformation satisfies the conditions in the following definition.

• Definition 1

Let V and W be vector spaces over a field $\mathbb{F}$. Let T be a mapping of V into W. Then T is a **linear transformation of V into W** if, for all $\mathbf{v}, \mathbf{w} \in V$ and for all $c \in \mathbb{F}$, the following hold:

(i) $T(\mathbf{v} + \mathbf{w}) = T(\mathbf{v}) + T(\mathbf{w})$,
(ii) $T(c\mathbf{v}) = cT(\mathbf{v})$.

If the mapping T is onto W then T is a linear transformation **onto W.**

For linear transformations the mapping is usually written on the left even though the composite $U(T(\mathbf{v}))$ of linear transformations is important in some applications and this is more easily written with mapping on the right. However, this notation is compatible with the vectors of finite degree being written as column vectors and therefore matrix linear transformations being in the form $\mathbf{w} = \mathbf{Av}$. Before we find the basic properties of linear transformations, let us look at some examples.

◎ Example 2

Let $V = \mathrm{P}_3(\mathbb{Q})$ be the vector space of polynomials in x over $\mathbb{Q}$ of degree at most 3 together with 0, and let $a(x) = x^2 - 5x + 6$. Define the mapping T of V into $\mathbb{Q}[x]$ by $T(p(x)) = a(x)p(x)$ for all $p(x) \in V$. Then, for $q(x) \in V$, $T(p(x) + q(x)) = a(x)[p(x) + q(x)] = a(x)p(x) + a(x)q(x) = T(p(x)) + T(q(x))$. Also, for $c \in \mathbb{Q}$, $T(cp(x)) = a(x)cp(x) = cT(p(x))$. Therefore T is a linear transformation of V into $\mathbb{Q}[x]$ by Definition 1. Whereas T is a linear transformation, the mapping U given by $U(p(x)) = p(x) + a(x)$ is not, because for $c \in \mathbb{Q}$ we have $U(cp(x)) = cp(x) + a(x)$, which is not $cU(p(x))$ unless $c = 1$. Alternatively, for the vector space C of real continuous functions of a real variable x, neither the mapping $S(f(x)) = [f(x)]^2$ nor the mapping $R(f(x)) = \sin(f(x))$ is a linear transformation of C into itself.

• Proposition 1 (*Linear Algebra*, Chapter 10, Theorem 1)

Let V and W be vector spaces over a field $\mathbb{F}$ and let T be a linear transformation of V into W. Then:

(i) $T(\mathbf{0}) = \mathbf{0}$,
(ii) for a positive integer m, $\mathbf{v}_j \in V$ and $c_j \in \mathrm{F}$, where $j = 1, 2, 3, \ldots, m$,
$$T\left(\sum_{j=1}^{m} c_j \mathbf{v}_j\right) = \sum_{j=1}^{m} c_j T(\mathbf{v}_j);$$
(iii) for all $\mathbf{u}, \mathbf{v} \in V$, $T(\mathbf{u} - \mathbf{v}) = T(\mathbf{u}) - T(\mathbf{v})$.

Before we study linear transformations in general, let us first study linear transformations from one total vector space to another. We start with an example.

○ Example 3

Let T be the mapping of $\mathbb{R}^3$ into $\mathbb{R}^2$ defined by $T(\mathbf{v}_j) = (x_j + 5y_j + 2z_j, 2y_j - 3z_j)$ for all $\mathbf{v}_j = (x_j, y_j, z_j) \in \mathbb{R}^3$ and $j = 1, 2$. Then

$$\begin{aligned} T(\mathbf{v}_1 + \mathbf{v}_2) &= T\big((x_1 + x_2, y_1 + y_2, z_1 + z_2)\big) \\ &= \big((x_1 + x_2) + 5(y_1 + y_2) + 2(z_1 + x_2), 2(y_1 + y_2) - 3(z_1 + z_2)\big) \\ &= (x_1 + 5y_1 + 2z_1, 2y_1 - 3z_1) + (x_2 + 5y_2 + 2z_2, 2y_2 - 3z_2) \\ &= T(\mathbf{v}_1) + T(\mathbf{v}_2) \end{aligned}$$

and, for $c \in \mathbb{R}$,

$$\begin{aligned} T(c\mathbf{v}_1) &= T\big((cx_1, cy_1, cz_1)\big) \\ &= (cx_1 + 5cy_1 + 2cz_1, 2cy_1 - 3cz_1) = c(x_1 + 5y_1 + 2z_1, 2y_1 - 3z_1) \\ &= cT(\mathbf{v}_1). \end{aligned}$$

Therefore T is a linear transformation of $\mathbb{R}^3$ into $\mathbb{R}^2$, by Definition 1. But can we express T by means of a matrix? Because $\mathbf{v}_1 = (x_1 \;\; y_1 \;\; z_1)^{\mathrm{T}}$ and $T(\mathbf{v}_1) = (x_1 + 5y_1 + 2z_1 \;\; 2y_1 - 3z_1)^{\mathrm{T}}$, we can write $T(\mathbf{v}_1)$ in the form $T(\mathbf{v}_1) = x_1(1 \;\; 0)^{\mathrm{T}} + y_1(5 \;\; 2)^{\mathrm{T}} + z_1(2 \;\; -3)^{\mathrm{T}}$. Therefore, $T(\mathbf{v}_1) = \mathbf{A}\mathbf{v}_1$ for all $\mathbf{v}_1 \in \mathbb{R}^3$, where $\mathbf{A} = \begin{pmatrix} 1 & 5 & 2 \\ 0 & 2 & -3 \end{pmatrix}$. We conclude that the linear transformation from $\mathbb{R}^3$ into $\mathbb{R}^2$ in this example is a matrix linear transformation.

In fact, every linear transformation from one total vector space into another is always equal to a matrix linear transformation.

• Proposition 2

Let $\mathbb{F}$ be any field, and let n, m be positive integers and let T be any linear transformation of $\mathbb{F}^n$ into $\mathbb{F}^m$. Then there exists an $m \times n$ matrix $\mathbf{A}$ over $\mathbb{F}$ such that $T(\mathbf{v}) = \mathbf{A}\mathbf{v}$ for all $\mathbf{v} \in \mathbb{F}^n$.

PROOF

Because $\mathbb{F}^n$ has the natural ordered basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \ldots, \mathbf{e}_n\}$, where $\mathbf{e}_j$ is a zero vector except for 1 in the jth place, $\mathbf{v} \in \mathbb{F}^n$ can be written uniquely as

$$\mathbf{v} = (c_1 \;\; c_2 \;\; c_3 \;\; \ldots \;\; c_n)^{\mathrm{T}} = \sum_{j=1}^{m} c_j \mathbf{e}_j,$$

where $c_j \in \mathbb{F}$ for $j = 1, 2, 3, \ldots, n$. Therefore, by Proposition 1(ii),

$$T(\mathbf{v}) = T\left(\sum_{j=1}^{m} c_j \mathbf{e}_j\right) = \sum_{j=1}^{m} c_j T(\mathbf{e}_j).$$

Because $T(\mathbf{e}_j) \in \mathbb{F}^m$ for $j = 1, 2, 3, \ldots, n$, we can define the $m \times n$ partitioned matrix $\mathbf{A}$ over $\mathbb{F}$ by $\mathbf{A} = (T(\mathbf{e}_1)\ T(\mathbf{e}_2)\ T(\mathbf{e}_3)\ \ldots\ T(\mathbf{e}_n))$. Therefore,

$$T(\mathbf{v}) = \sum_{j=1}^{m} T(\mathbf{e}_j)c_j = \mathbf{A}(c_1 \quad c_2 \quad c_3 \quad \ldots \quad c_n)^{\mathrm{T}} = \mathbf{Av}. \qquad \bullet$$

By Proposition 2, every linear transformation of a total vector space into another is a matrix linear transformation, therefore the set of linear transformations perfectly represents the set of matrices of the appropriate size. Many of the important linear transformations operate on infinite-dimensional vector spaces and deserve great prominence. However, only the linear transformations of finite-dimensional vector spaces can be expressed in terms of matrix multiplication. Consequently we shall concentrate on finite-dimensional vector spaces, although some of our results hold for all vector spaces, such as the following.

• *Proposition 3 (Linear Algebra,* Chapter 10, Theorem 1)

Let T be a linear transformation of the vector space V over a field $\mathbb{F}$ into a vector space W over $\mathbb{F}$. Then the **image** of T is a subspace of W called the **range** $T(V)$ of T.

Because we can discuss the range $T(V)$ of a linear transformation T of a vector space V instead of the codomain of T, linear transformations can always be presented as mappings onto a vector space instead of into one without reducing their generality. The following proposition identifies a case when the range is finite-dimensional.

• *Proposition 4 (Linear Algebra,* Chapter 10, Notes 2)

Let V be a vector space of finite dimension n over the field $\mathbb{F}$ with basis $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n\}$ and let T be a linear transformation of V into W. Then:

(i) T is completely determined by $\{T(\mathbf{b}_i) : i = 1, 2, 3, \ldots, n\}$;
(ii) $T(B)$ spans $T(V)$;
(iii) $T(V)$ is of finite dimension r over $\mathbb{F}$, called the **rank** of T, and $r \leq n$.

In the case of a matrix linear transformation T, more is known about the rank of T.

• *Proposition 5 (Linear Algebra,* Chapter 10, Notes 2(iv))

Let T be the linear transformation of $\mathbb{F}^n$ into $\mathbb{F}^m$ given by $T(\mathbf{v}) = \mathbf{Av}$. Then the rank of T is the rank of the matrix $\mathbf{A}$ over $\mathbb{F}$.

In Example 1, the solution of homogeneous linear equations suggested studying the set of vectors $\mathbf{v}$ in the vector space V such that $T(\mathbf{v}) = \mathbf{0}$, where T is a linear transformation of V. In order to investigate these vectors we require the following definition.

• Definition 2

Let T be a linear transformation of a vector space V over a field $\mathbb{F}$ into a vector space W over $\mathbb{F}$. The **kernel** or **null space** K of T is the subset of V defined by $K = \{\mathbf{k} \in V : T(\mathbf{k}) = \mathbf{0} \in W\}$.

○ Example 4

Let $\mathbf{A}$ be an $m \times n$ matrix over a field $\mathbb{F}$ and let T be the matrix linear transformation of $\mathbb{F}^n$ into $\mathbb{F}^m$ given by $T(\mathbf{v}) = \mathbf{Av}$ for all $\mathbf{v} \in \mathbb{F}^n$. Then the kernel K of T is the set of all column vectors such that $\mathbf{Av} = \mathbf{0}$. Therefore K is the vector space of all solutions of the system of linear equations $\mathbf{Ax} = \mathbf{0}$. Conversely, the solutions of a system of linear equations can be expressed as the kernel of a matrix linear transformation.

In fact, Example 4 is typical in that the kernel of a linear transformation is always a subspace of the domain, as we state in the following proposition.

• Proposition 6 (*Linear Algebra*, Chapter 10, Theorem 1)

Let T be a linear transformation of a vector space V over a field $\mathbb{F}$ into a vector space W over $\mathbb{F}$. Then the kernel K of T is a subspace of V and the dimension of K is called the **nullity** of T.

If, in Proposition 6, the vector space V is of dimension n over $\mathbb{F}$ then, by Theorem 3 of Chapter 3, the dimension of the kernel of T is a non-negative integer k such that $k \leq n$. We conclude that the nullity k of any linear transformation of a vector space of finite dimension n is finite and satisfies $k \leq n$. More precise results will be obtained later by means of restrictions on the linear transformations.

Every vector in a vector space V of dimension n over a field $\mathbb{F}$ is equal to a unique linear combination of the vectors in a given basis $B = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$. Each basis vector $\mathbf{b}_j$ spans a vector space $V_j = \langle \mathbf{b}_j \rangle$ of dimension 1 over $\mathbb{F}$ and $V_j = \{c\mathbf{b}_j : c \in \mathbb{F}\}$, for $j = 1, 2, \ldots, n$. This bears a strong resemblance to the subspace W_j consisting of all the vectors $(0, 0, \ldots, 0, c_j, 0, \ldots, 0)$ in $\mathbb{F}^n$ where the only non-zero elements are in the jth place. But every vector in $\mathbb{F}^n$ is of the form

$$(c_1, c_2, \ldots, c_j, \ldots, c_n) = \sum_{j=1}^{n} (0, 0, \ldots 0, c_j, 0, \ldots, 0),$$

therefore $\mathbb{F}^n = \langle W_1, W_2, \ldots, W_n \rangle$, the space spanned by the elements of $W_1, W_2, \ldots, W_n$. However, because B spans V, we can write similarly that $V = \langle V_1, V_2, \ldots, V_n \rangle$, which suggests that V and $\mathbb{F}^n$ are very similar. Contrarily, V cannot always be equal to $\mathbb{F}^n$ because that would imply that $V = \mathbb{F}^n$ as a set, which is untrue by Example 2. Therefore the best we can hope for is that each vector $v \in V$ can be associated with exactly one n-tuple in $\mathbb{F}^n$, that is, we hope to find a **one-to-one mapping** or **bijection** θ of V onto $\mathbb{F}^n$. The existence of such a bijection is not enough in itself because we also expect the properties of the corresponding vectors to be the same, in that we require that if subset $S \subseteq V$ consists of zeros or is linearly dependent or spans the space or is a basis then the same holds for $S\theta$. All these properties are defined by linear combinations, therefore they would follow if whenever $\mathbf{w} = \sum_{j=1}^{m} c_j \mathbf{v}_j$, where $\mathbf{w}$ and $\mathbf{v}_j \in V$ and $c_j \in \mathbb{F}$ for $j = 1, 2, 3, \ldots, m$, then $\mathbf{w}\theta = \sum_{j=1}^{m} c_j(\mathbf{v}_j\theta)$. But, by Proposition 1, this is true if, for all $\mathbf{v}, \mathbf{w} \in V$ and for all $c \in \mathbb{F}$, we have $(\mathbf{v} + \mathbf{w})\theta = \mathbf{v}\theta + \mathbf{w}\theta$ and $(c\mathbf{v})\theta = c(\mathbf{v}\theta)$. Note that in these equations the sum and product by the scalar c on the left-hand side of the

equations operate in V whereas on the right-hand side they operate in $\mathbb{F}^n$, so these equations can be summarized as saying that corresponding vectors have corresponding sums and products by scalars. The abstract relation between V and $\mathbb{F}^n$ which we are now investigating is called **isomorphism**, a name for the property of having the same shape, and it is easily proved to be an equivalence relation. Let us summarize this important idea.

• Definition 3

Let V and W be vector spaces over a field $\mathbb{F}$. Then V is **isomorphic** to W, and we write $V \cong W$, if there exists a bijection θ of V onto W such that, for all $\mathbf{v}, \mathbf{w} \in V$ and for all $c \in \mathbb{F}$, the following hold:

(i) $(\mathbf{v} + \mathbf{w})\theta = \mathbf{v}\theta + \mathbf{w}\theta$;
(ii) $(c\mathbf{v})\theta = c(\mathbf{v}\theta)$.

First we give an example of an abstract vector space which is isomorphic to a total vector space.

○ Example 5

Let $P = \mathrm{P}_3(\mathbb{Q})$, the vector space of polynomials over $\mathbb{Q}$ of degree at most 3 in the indeterminate x together with the polynomial 0. If $p(x) \in P$ then $p(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ where $a_0, a_1, a_2, a_3 \in \mathbb{Q}$. This suggests that we might map $p(x)$ onto (a_0, a_1, a_2, a_3), so let us define the mapping θ of P into $\mathbb{Q}^4$ by $p(x)\theta = (a_0, a_1, a_2, a_3)$. It is immediately obvious that θ is a bijection of P onto $\mathbb{Q}^4$. Let $q(x) = b_0 + b_1x + b_2x^2 + b_3x^3 \in P$ and $c \in \mathbb{Q}$. Then

$$\begin{aligned}[p(x)+q(x)]\theta &= \left[(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+(a_3+b_3)x^3\right]\theta \\ &= (a_0+b_0, a_1+b_1, a_2+b_2, a_3+b_3) \\ &= (a_0, a_1, a_2, a_3)+(b_0, b_1, b_2, b_3) \\ &= p(x)\theta + q(x)\theta\end{aligned}$$

and

$$\begin{aligned}[cp(x)]\theta &= \left[ca_0 + ca_1x + ca_2x^2 + ca_3x^3\right]\theta \\ &= (ca_0, ca_1, ca_2, ca_3) \\ &= c(a_0, a_1, a_2, a_3) \\ &= c[p(x)\theta].\end{aligned}$$

Therefore θ is an isomorphism of P onto $\mathbb{Q}^4$ and therefore $P \cong \mathbb{Q}^4$.

• Proposition 7

Let T be a linear transformation of a vector space V over a field $\mathbb{F}$ onto a vector space W over $\mathbb{F}$. Then T is an isomorphism if and only if the kernel of T is $\{\mathbf{0}\}$.

PROOF

By Definition 3, T is an isomorphism of V onto W if and only if T is a bijection. If T is a

bijection of V onto W, there is only one $\mathbf{v} \in V$ such that $T(\mathbf{v}) = \mathbf{0}$. But, by Proposition 1(i), $T(\mathbf{0}) = \mathbf{0}$ and therefore the kernel of T is $\{\mathbf{0}\}$, by Definition 2. Conversely, suppose the kernel K of T is $\{\mathbf{0}\}$. If, for $\mathbf{u}, \mathbf{v} \in V$, $T(\mathbf{u}) = T(\mathbf{v})$ then, by Proposition 1(iii), $T(\mathbf{u} - \mathbf{v}) = T(\mathbf{u}) - T(\mathbf{v}) = \mathbf{0}$. Therefore $\mathbf{u} - \mathbf{v}$ belongs to the kernel $\{\mathbf{0}\}$ of T and consequently $\mathbf{u} = \mathbf{v}$. This proves that T is a bijection and therefore T is an isomorphism. ●

If the linear transformation T of Proposition 7 is an isomorphism, then the nullity of T is 0 and, by Proposition 4(iii), the rank of T is the dimension of V. The following theorem shows that whenever V is of finite dimension there is a relation connecting the dimension of V, the rank of T and the nullity of T.

• *Theorem 1* **The dimension theorem** (*Linear Algebra*, Chapter 10, Theorem 2)

Let $\mathbb{F}$ be a field, let V be a vector space of finite dimension n over $\mathbb{F}$, let W be a vector space over $\mathbb{F}$ and let T be a linear transformation of V onto W of rank r and nullity k. Then $r + k = n$.

The following simple deduction from the dimension theorem is important because it refers to a basic problem and therefore can be applied in a very wide range of cases. It also has an entirely elementary proof.

• *Theorem 2* (*Linear Algebra*, Chapter 10, Notes 2)

Let $\mathbf{A}$ be an $m \times n$ matrix which is of rank r over a field $\mathbb{F}$. Then the dimension of the vector space of solutions of the system of homogeneous linear equations $\mathbf{Ax} = \mathbf{0}$ is $n - r$, the **nullity** of $\mathbf{A}$, which we write as null $\mathbf{A}$.

Here are two examples of linear transformations for which the rank and nullity are calculated.

◎ *Example 6*

Let T be the matrix linear transformation from $\mathbb{Q}^3$ into $\mathbb{Q}^3$ such that, for all $\mathbf{v} \in \mathbb{Q}^3$, $T(\mathbf{v}) = \mathbf{Av}$, where $\mathbf{A} = \begin{pmatrix} 1 & 0 & 2 \\ 4 & 2 & 9 \\ 6 & 2 & 13 \end{pmatrix}$. Then the rank of T is the dimension of the range of T, which is the vector space $R = \{\mathbf{Av} : \mathbf{v} \in \mathbb{Q}^3\}$. Let us write $\mathbf{v}$ as $(x \;\; y \;\; z)^{\mathrm{T}}$ and let the columns of $\mathbf{A}$ be $\mathbf{s}$, $\mathbf{t}$, $\mathbf{u}$. Then

$$R = \left\{(\mathbf{s} \;\; \mathbf{t} \;\; \mathbf{u})(x \;\; y \;\; z)^{\mathrm{T}} \;:\; x, y, z \in \mathbb{Q}\right\}$$
$$= \{x\mathbf{s} + y\mathbf{t} + z\mathbf{u} \;:\; x, y, z \in \mathbb{Q}\},$$

which is the vector space spanned by the columns of $\mathbf{A}$. Therefore the dimension of R is the (column) rank of $\mathbf{A}$. The rank of $\mathbf{A}$ cannot be 3 because $4\mathbf{s} + \mathbf{t} - 2\mathbf{u} = \mathbf{0}$, but $\{\mathbf{s}, \mathbf{t}\}$ is linearly independent over $\mathbb{Q}$ because the vectors are not proportional. Therefore the rank of $\mathbf{A}$ and hence of T is 2. The kernel of T is $K = \{\mathbf{v} \in \mathbb{Q}^3 \;:\; \mathbf{Av} = \mathbf{0}\}$, which is the vector space of solutions of $\mathbf{Ax} = \mathbf{0}$. We reduce the matrix of coefficients $\mathbf{A}$ to echelon form as follows.

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 2 \\ 4 & 2 & 9 \\ 6 & 2 & 13 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 1 \\ 0 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

The third unknown, z, is disposable so $z = \theta$, a parameter over $\mathbb{Q}$, and, by back substitution, the other unknowns are $y = -\theta/2$ and $x = -2\theta$. Therefore $K = \{\theta(-2 \quad -1/2 \quad 1)^{\mathrm{T}} : \theta \in \mathbb{Q}\}$, which is of dimension 1 over $\mathbb{Q}$. Therefore the nullity of $\mathbf{A}$ and hence of T is 1. This verifies that the rank and nullity of T add up to 3, the dimension of $\mathbb{Q}^3$.

◎ *Example 7*

Let T be the linear transformation of $\mathbb{R}[x]$ into itself defined by $T(f(x)) = \mathfrak{D}f(x)$. By Definition 2, the kernel of T is

$$\{f(x) \in \mathbb{R}[x] \ : \ \mathfrak{D}f(x) = 0\} = \{f(x) \in \mathbb{R}[x] \ : \ f(x) = a \in \mathbb{R}\} = \mathbb{R}.$$

This is of dimension 1, therefore, by Proposition 6, the nullity of T is 1. A basis over $\mathbb{R}$ for the image of $\mathbb{R}[x]$ under T is the set $\{1, x, x^2, x^3, \ldots, x^n, \ldots\}$, therefore $T(\mathbb{R}[x])$ is of infinite dimension over $\mathbb{R}$. In fact, $T(\mathbb{R}[x]) = \mathbb{R}[x]$. Consequently, the nullity of T is certainly not the difference between the dimensions of $\mathbb{R}[x]$ and its image. It follows that the dimension theorem does not hold for the infinite-dimensional vector space $\mathbb{R}[x]$.

The standard basis $S = \{\mathbf{e}_1 = (1, 0, 0), \mathbf{e}_2 = (0, 1, 0), \mathbf{e}_3 = (0, 0, 1)\}$ of $\mathbb{R}^3$ is sensibly regarded as a typical and easily used basis, but it actually has one property that most others lack. If we refer to the second element of S, we obviously refer to $\mathbf{e}_2$, because the elements of S occur in a natural order. But what is the second element of the basis $B = \{(2, 1, 1), (1, 2, 6), (5, 4, 3)\}$ of $\mathbb{R}^3$? It is not necessarily $(1, 2, 6)$ because the basis B is merely a set, and so we might write alternatively that $B = \{(1, 2, 6), (5, 4, 3), (2, 1, 1)\}$. However, we can easily convert B into an **ordered basis** of $\mathbb{R}^3$ by putting the elements in a chosen order, such as $B = \{\mathbf{b}_1 = (1, 2, 6), \mathbf{b}_2 = (2, 1, 1), \mathbf{b}_3 = (5, 3, 4)\}$, where the elements have been placed in the ascending order of their first component, although any choice from the five other orders would be equally acceptable. In fact, for a vector space V of finite dimension n over a field $\mathbb{F}$, each basis contains n elements, by Proposition 3 of Chapter 3, and so the elements can be written out in $n!$ orders (all equally acceptable) to produce an ordered basis of V. The reason for wanting an ordered basis (instead of an ordinary one) is that an ordered basis is used in the construction that proves the following proposition.

• *Proposition 8*

Let V be a vector space of finite dimension n over a field $\mathbb{F}$ and let $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n\}$ be an ordered basis of V. Then B determines a bijection ρ of V onto $\mathbb{F}^n$, called the **representation of V with respect to B.**

PROOF

Let $\mathbf{v} \in V$. Then, by Theorem 1 of Chapter 3, there is a unique linear combination of the elements of B which is equal to $\mathbf{v}$, therefore there exist unique $c_1, c_2, c_3, \ldots, c_n \in \mathbb{F}$ such

that $\mathbf{v} = \sum_{j=1}^{n} c_j \mathbf{b}_j$. Because B is an ordered basis with the elements $\mathbf{b}_j$ ordered by $j = 1, 2, 3, \ldots, n$, there is a unique jth coefficient c_j in this linear combination. Let $\mathbf{v}\rho = (c_1, c_2, c_3, \ldots, c_n) \in \mathbb{F}^n$. Then $\mathbf{v}\rho$ is a unique element of $\mathbb{F}^n$ determined by $\mathbf{v}$ and therefore, for $\mathbf{v}$ ranging over V, ρ is a mapping of V into $\mathbb{F}^n$. For arbitrary $\mathbf{x} \in \mathbb{F}^n$ (regarded as $V\rho$), there exist unique $d_j \in \mathbb{F}$ for $j = 1, 2, 3, \ldots, n$ such that $\mathbf{x} = (d_1, d_2, d_3, \ldots, d_n)$ and therefore a unique $\mathbf{w} = \sum_{j=1}^{n} d_j \mathbf{b}_j \in V$. Therefore ρ is not only a mapping of V onto $\mathbb{F}^n$ but also a bijection, because the vector $\mathbf{w}$ is unique. Therefore ρ is the required bijection of V onto $\mathbb{F}^n$. ●

◎ Example 8

Let V be the vector space over $\mathbb{R}$ consisting of the solutions of the differential equation $(\mathfrak{D}^2 - 1)y = 0$. The standard method for solving linear differential equations gives the general solution for this equation as $y = Ae^x + Be^{-x}$, where $A, B \in \mathbb{R}$. Therefore $S = \{e^x, e^{-x}\}$ spans V. Suppose that the linear combination $ce^x + de^{-x} = 0$, where $c, d \in \mathbb{R}$. From $x = 0$ we obtain $c + d = 0$ and from $x = 1$ we obtain $ce^2 + d = 0$. Therefore $d = -c$ and $c(e^2 - 1) = 0$, consequently $c = d = 0$. We deduce that S is a basis of V.

We can now choose $B = \{b_1(x), b_2(x)\}$ as an ordered basis of V by choosing $b_1(x) = e^x$ and $b_2(x) = e^{-x}$. Then the representation of the element $f(x) = 2e^x + 3e^{-x}$ of V with respect to B is $f(x)\rho = (2, 3)$. However, we could choose an entirely different ordered basis for V. For example, $\mathfrak{D}^2 \sinh x = \sinh x$ and $\mathfrak{D}^2 \cosh x = \cosh x$, therefore $\sinh x$ and $\cosh x$ are solutions of the equation. Let $r, s \in \mathbb{R}$ such that $r \sinh x + s \cosh x = 0$. Then, by substituting $x = 0$, we have $r \sinh 0 + s \cosh 0 = 0$ and therefore $s = 0$. Next, we substitute $x = 1$ and obtain $r \sinh 1 = 0$ and therefore $r = 0$, because $\sinh 1 \neq 0$. Therefore $\{\sinh x, \cosh x\}$ is linearly independent over $\mathbb{R}$ and, by Proposition 4 of Chapter 3, it is a basis of V. By choosing $\sinh x$ to be the first element, we form the ordered basis $C = \{c_1(x) = \sinh x, c_2(x) = \cosh x\}$ and can obtain the representation of V with respect to C, which we denote by σ. To obtain the representation of the function $f(x) = 2e^x + 3e^{-x}$ with respect to C we require $r, s \in \mathbb{R}$ such that

$$f(x) = r \sinh x + s \cosh x = (re^x - re^{-x} + se^x + se^{-x})/2 = (r + s)e^x/2 + (s - r)e^{-x}/2.$$

Consequently $s + r = 4$ and $s - r = 6$ and therefore $s = 5$ and $r = -1$. We deduce that $f(x)\sigma = (-1, 5)$.

The reason for examining the representation of a vector space V of dimension n over a field $\mathbb{F}$ with respect to an ordered basis is that it provides a proof that V is isomorphic to $\mathbb{F}^n$, as we now show.

• Theorem 3

Let n be a positive integer, let V be a vector space of dimension n over a field $\mathbb{F}$ and let B be an ordered basis of V. Then the representation ρ of V with respect to B is an isomorphism of V onto $\mathbb{F}^n$.

PROOF

Let $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n\}$ be the chosen ordered basis of V. The representation ρ of V with respect to B is a bijection of V onto $\mathbb{F}^n$, by Proposition 8, so we can prove the

theorem by showing that ρ is an isomorphism. By Theorem 1 of Chapter 3, for the vectors $\mathbf{v}, \mathbf{w} \in V$, there exist unique elements $c_j, d_j \in \mathbb{F}$ for $j = 1, 2, 3, \ldots, n$ such that $\mathbf{v} = \sum_{j=1}^{n} c_j \mathbf{b}_j$ and $\mathbf{w} = \sum_{j=1}^{n} d_j \mathbf{b}_j$. Then

$$\begin{aligned}(\mathbf{v}+\mathbf{w})\rho &= \left[\sum_{j=1}^{n} c_j\mathbf{b}_j + \sum_{j=1}^{n} d_j\mathbf{b}_j\right]\rho \\ &= \left[\sum_{j=1}^{n} (c_j + d_j)\mathbf{b}_j\right]\rho \\ &= (c_1 + d_1, c_2 + d_2, c_3 + d_3, \ldots, c_n + d_n) \\ &= (c_1, c_2, c_3, \ldots, c_n) + (d_1, d_2, d_3 \ldots, d_n) \\ &= \left[\sum_{j=1}^{n} c_j\mathbf{b}_j\right]\rho + \left[\sum_{j=1}^{n} d_j\mathbf{b}_j\right]\rho \\ &= \mathbf{v}\rho + \mathbf{w}\rho\end{aligned}$$

and, for $c \in \mathbb{F}$,

$$\begin{aligned}(c\mathbf{v})\rho &= \left[c\sum_{j=1}^{n} c_j\mathbf{b}_j\right]\rho = \left[\sum_{j=1}^{n} (cc_j)\mathbf{b}_j\right]\rho \\ &= (cc_1, cc_2, cc_3, \ldots, cc_n) \\ &= c(c_1, c_2, c_3, \ldots, c_n) \\ &= c(\mathbf{v}\rho).\end{aligned}$$

Therefore, by Definition 1, ρ is an isomorphism of V onto $\mathbb{F}^n$. ●

In a finite-dimensional vector space which is not a total vector space, there is no natural choice of basis resembling the standard basis; consequently, it is sensible to use a more favourable ordered basis. If the information about the problem is already given in terms of a less convenient basis, methods for changing bases and the rules determining the consequent transformation of the vectors are needed. The following example illustrates the problem.

○ *Example 9*

Let V be the vector space over $\mathbb{R}$ of Example 8, let ρ be the representation of V with respect to the ordered basis B and σ be the representation of V with respect to the ordered basis C. Can we find a formula to express $v(x)\sigma$ in terms of $v(x)\rho$ for all $v(x) \in V$? In order to make it possible to use matrices, let us write $v\rho$ and $v\sigma$ as column vectors. Then, as in Example 8, $v(x) = pe^x + qe^{-x} \in V$, therefore we obtain $v(x)\rho = (p \quad q)^{\mathrm{T}}$ and $v(x)\sigma = (r \quad s)^{\mathrm{T}}$, where $v(x) = r \sinh x + s \cosh x$ and hence $v(x) = [(r + s)e^x + (-r + s)e^{-x}]/2$. Because $v(x)$ is equal to a unique linear combination of the basis elements e^x and e^{-x}, by Theorem 1 of Chapter 3, we deduce immediately that

$$\begin{pmatrix} p \\ q \end{pmatrix} = \mathbf{P}\begin{pmatrix} r \\ s \end{pmatrix}, \quad \text{where} \quad \mathbf{P} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Because $\det \mathbf{P} = \frac{1}{4}\left[1^2 - 1(-1)\right] = \frac{1}{2}$, the matrix $\mathbf{P}$ is non-singular, so we obtain the formulae $v(x)\rho = \mathbf{P}(v(x)\sigma)$ and $v(x)\sigma = \mathbf{P}^{-1}(v(x)\rho)$. In fact, the matrix $\mathbf{P}$ is easily deduced from the representations because, for $C = \{c_1(x), c_2(x)\}$, we have $c_1(x)\sigma = (1 \quad 0)^{\mathrm{T}}$ and $c_2(x)\rho = (0 \quad 1)^{\mathrm{T}}$, therefore $c_1(x)\rho = \left(\frac{1}{2} \quad -\frac{1}{2}\right)^{\mathrm{T}}$ and $c_2(x)\rho = \left(\frac{1}{2} \quad \frac{1}{2}\right)^{\mathrm{T}}$, and consequently $\mathbf{P} = \left(c_1(x)\rho \quad c_2(x)\rho\right)$.

The column vectors $c_1(x)\rho$ and $c_2(x)\rho$ can be identified in a different way because the definitions of $\sinh x$ and $\cosh x$ give us $c_1(x) = \frac{1}{2}e^x + \left(-\frac{1}{2}\right)e^{-x}$ and $c_2(x) = \frac{1}{2}e^x + \frac{1}{2}e^{-x}$, so the matrix $\mathbf{P}$ can be determined by the coefficients of the elements of C as linear combinations of the elements of B.

Example 9 suggests that in order to determine the relationships between representations of a vector space with respect to different ordered bases, we should first discover the relationships of the ordered bases with each other. We do this in the following theorem, which we then apply to find the formula which connects the different representations.

• Theorem 4

Let n be a positive integer, let V be a vector space over a field $\mathbb{F}$ and let $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n\}$ be an ordered basis of V. Then $C = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \ldots, \mathbf{c}_n\} \subseteq V$ is an ordered basis of V if and only if there exists a non-singular matrix $\mathbf{R} = (r_{ij})$ over $\mathbb{F}$ such that, for $j = 1, 2, 3, \ldots, n$, $\mathbf{c}_j = \sum_{i=1}^{n} r_{ij}\mathbf{b}_i$.

PROOF

By Proposition 4 of Chapter 3, C is a basis of V if and only if C is linearly independent over $\mathbb{F}$. Because $\mathbf{c}_j \in V$ for $j = 1, 2, 3, \ldots, n$, by Theorem 1 of Chapter 3 the vector $\mathbf{c}_j$ is equal to a unique linear combination $\mathbf{c}_j = \sum_{i=1}^{n} r_{ij}\mathbf{b}_i$ of the elements of the basis B. Therefore this linear combination uniquely defines the $n \times n$ matrix $\mathbf{R} = (r_{ij})$ over $\mathbb{F}$. Therefore, for $a_j \in \mathbb{F}$,

$$\sum_{j=1}^{n} a_j\mathbf{c}_j = \sum_{j=1}^{n} a_j\left[\sum_{i=1}^{n} r_{ij}\mathbf{b}_i\right] = \sum_{j=1}^{n}\sum_{i=1}^{n} r_{ij}a_j\mathbf{b}_i = \sum_{i=1}^{n}\left[\sum_{j=1}^{n} r_{ij}a_j\right]\mathbf{b}_i.$$

Therefore $\sum_{j=1}^{n} a_j\mathbf{c}_j = \mathbf{0}$ if and only if $\sum_{i=1}^{n}\left[\sum_{j=1}^{n} r_{ij}a_j\right]\mathbf{b}_i = \mathbf{0}$, and this holds if and only if $\sum_{j=1}^{n} r_{ij}a_j = 0$ for $i = 1, 2, 3, \ldots, n$, because B is linearly independent over $\mathbb{F}$. Let us write $\mathbf{a} = (a_1 \quad a_2 \quad a_3 \quad \ldots \quad a_n)^{\mathrm{T}}$. If $\mathbf{R}$ is non-singular, then $\mathbf{Ra} = \mathbf{0}$ implies that $\mathbf{a} = \mathbf{0}$ and therefore that C is linearly independent over $\mathbb{F}$. Conversely, if $\mathbf{R}$ is singular, then

there exists $\mathbf{a} \neq \mathbf{0}$ such that $\mathbf{Ra} = \mathbf{0}$, which implies that C is linearly dependent over $\mathbb{F}$, contrary to C being a basis of V. We conclude that C is linearly independent over $\mathbb{F}$ and therefore is an ordered basis of V if and only if $\mathbf{R}$ is non-singular. ●

We now give a name to the inverse of the matrix $\mathbf{R}$ in Theorem 4 and then show that it has further significance.

• Definition 4

The inverse matrix $\mathbf{P} = \mathbf{R}^{-1}$ of the matrix $\mathbf{R}$ in Theorem 4 is the **transition matrix** from the ordered basis B to the ordered basis C.

• Theorem 5

Let n be a positive integer, let V be a vector space of dimension n over a field $\mathbb{F}$, let B and C be ordered bases of V and let ρ and σ be the representations of V with respect to B and C. Then, for all $\mathbf{v} \in V$, $\mathbf{v}\sigma = \mathbf{P}(\mathbf{v}\rho)$, where $\mathbf{P}$ is the transition matrix from B to C.

PROOF

Write $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n\}$ and $C = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \ldots, \mathbf{c}_n\}$. Let $\mathbf{v} \in V$. Then, by Theorem 1 of Chapter 3, there exist unique $a_j \in \mathbb{F}$, for $j = 1, 2, 3, \ldots, n$, such that $\mathbf{v} = \sum_{j=1}^{n} a_j \mathbf{c}_j$, and therefore, from the proof of Theorem 3, $\mathbf{v} = \sum_{i=1}^{n} \left[\sum_{j=1}^{n} r_{ij} a_j \right] \mathbf{b}_i$, where $\mathbf{R} = (r_{ij})$ is a non-singular matrix over $\mathbb{F}$. Therefore $\mathbf{v}\sigma = (a_1 \ a_2 \ a_3 \ \ldots \ a_n)^{\mathrm{T}}$ and $\mathbf{v}\rho = (k_1 \ k_2 \ k_3 \ \ldots \ k_n)^{\mathrm{T}}$, where $k_i = \sum_{i=1}^{n} r_{ij} a_j$. Consequently, $\mathbf{v}\rho = \mathbf{R}(\mathbf{v}\sigma)$ and we conclude that $\mathbf{v}\sigma = \mathbf{P}(\mathbf{v}\rho)$, where $\mathbf{P} = \mathbf{R}^{-1}$ is the transition matrix from B to C. ●

As an application of the dimension theorem (Theorem 1), we now prove some useful results concerning the rank of the product of two matrices $\mathbf{AB}$ in terms of the ranks of $\mathbf{A}$ and $\mathbf{B}$. These results are needed in the main result (Theorem 4) of Chapter 9, although the first is so easy that its proof was set as Exercise 6 of Chapter 2.

• Proposition 9

Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times n$ matrices over a field $\mathbb{F}$. Then rank $\mathbf{AB}$ does not exceed the smaller of rank $\mathbf{A}$ and rank $\mathbf{B}$.

The next result is a generalization of the dimension theorem which gives information about a vector space which is awkwardly defined by a combination of the range of one linear transformation and the kernel of another.

• Proposition 10

Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times n$ matrices over a field $\mathbb{F}$. Then the dimension of the subspace $V = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{F}^n, \mathbf{ABx} = \mathbf{0}\}$ of $\mathbb{F}^n$ is $d = \text{rank } \mathbf{B} - \text{rank } \mathbf{AB}$.

PROOF

The vector space $U_1 = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{F}^n\}$ is the image of $\mathbb{F}^n$ under the matrix linear transformation $\mathbf{y} = \mathbf{Bx}$ into $\mathbb{F}^n$ by Proposition 3. Therefore U_1 is a vector space of dimension rank $\mathbf{B}$ over $\mathbb{F}$ by Proposition 5. Then V is the kernel of the matrix linear transformation $\mathbf{y} = \mathbf{Ax}$ of U_1 into $\mathbb{F}^n$, and consequently V is a vector space of finite dimension over $\mathbb{F}$ by Proposition 6 and its subsequent discussion. Let $q = n - \text{rank } \mathbf{B}$ and $r = n - \text{rank } \mathbf{AB}$. Then q and r are non-negative integers such that $r = n - \text{rank } \mathbf{AB} \geq n - \text{rank } \mathbf{B} = q$ by Proposition 9, therefore $0 \leq q \leq r$. We take the possible relationships between q and r separately.

First, we assume that $0 < q < r$. The vector space $U_2 = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{Bx} = \mathbf{0}\}$ is of dimension $q = n - \text{rank } \mathbf{B}$ by Theorem 2. Therefore U_2 has a basis $S_2 = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_q\}$. Similarly, $U_3 = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{ABx} = \mathbf{0}\}$ is a vector space of dimension $r = n - \text{rank } \mathbf{AB}$. But if $\mathbf{x} \in \mathbb{F}^n$ and $\mathbf{Bx} = \mathbf{0}$ then also $\mathbf{ABx} = \mathbf{0}$, so U_2 is a subspace of U_3. Therefore, by Proposition 5 of Chapter 3, there exist $\mathbf{b}_j$, for $j = q + 1, q + 2, \ldots, r$, which are not in U_2, such that $S_3 = \{\mathbf{b}_j : j = 1, 2, \ldots, q, q + 1, \ldots, r\}$ is a basis of U_3. Let $\mathbf{v} \in V$. By the definition of V, there exists $\mathbf{u} \in \mathbb{F}^n$ such that $\mathbf{v} = \mathbf{Bu}$ and $\mathbf{ABu} = \mathbf{0}$. Therefore $\mathbf{u} \in U_3$ and, because S_3 is a basis of U_3, there exist $c_j \in \mathbb{F}$, for $j = 1, 2, \ldots, q, q + 1, \ldots, r$ such that $\mathbf{u} = c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + \ldots + c_q\mathbf{b}_q + c_{q+1}\mathbf{b}_{q+1} + \ldots + c_r\mathbf{b}_r$. Therefore, because $\mathbf{b}_j \in U_2$, and consequently $\mathbf{Bb}_j = \mathbf{0}$, for $j = 1, 2, \ldots, q$, we have $\mathbf{v} = \mathbf{Bu} = c_{q+1}\mathbf{Bb}_{q+1} + c_{q+2}\mathbf{Bb}_{q+2} + \ldots + c_r\mathbf{Bb}_r$. Therefore $T = \{\mathbf{Bb}_j : j = q + 1, q + 2, \ldots, r\}$ spans V. To find the dimension of V, we need to show that T is linearly independent over $\mathbb{F}$. If there exist $d_j \in \mathbb{F}$ for $j = q + 1, q + 2, \ldots, r$ such that $d_{q+1}\mathbf{Bb}_{q+1} + d_{q+2}\mathbf{Bb}_{q+2} + \ldots + d_r\mathbf{Bb}_r = \mathbf{0}$, it follows that $\mathbf{B}(d_{q+1}\mathbf{b}_{q+1} + d_{q+2}\mathbf{b}_{q+2} + \ldots + d_r\mathbf{b}_r) = \mathbf{0}$ and therefore that $\mathbf{u} = d_{q+1}\mathbf{b}_{q+1} + d_{q+2}\mathbf{b}_{q+2} + \ldots + d_r\mathbf{b}_r \in U_2$. Because S_2 is a basis of U_2, there exist $d_j \in \mathbb{F}$, for $j = 1, 2, \ldots, q$ such that $\mathbf{u} = d_{q+1}\mathbf{b}_{q+1} + d_{q+2}\mathbf{b}_{q+2} + \ldots + d_r\mathbf{b}_r = d_1\mathbf{b}_1 + d_2\mathbf{b}_2 + \ldots + d_q\mathbf{b}_q$. However, $S_3 = \{\mathbf{b}_j : j = 1, 2, \ldots, r\}$ is a basis of U_3, therefore S_3 is linearly independent, consequently $d_{q+1} = d_{q+2} = \ldots = d_r = 0$. Therefore T is linearly independent over $\mathbb{F}$ and is a basis of V. We conclude that if $0 < q < r$ then the dimension of V is $d = r - q$.

If $0 = q = r$ then the dimension of the vector space of solutions of $\mathbf{ABx} = \mathbf{0}$ is 0 by Theorem 2, therefore $\mathbf{ABx} = \mathbf{0}$ implies $\mathbf{x} = \mathbf{0}$. Therefore $V = \{\mathbf{0}\}$ and $d = r - q = 0$.

If $0 < q = r$, then $U_2 = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{Bx} = \mathbf{0}\} \subseteq U_3$, where $U_3 = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{ABx} = \mathbf{0}\}$, and therefore, by Theorem 2, $\dim U_2 = q = r = \dim U_3$. Consequently $U_3 = U_2$ and therefore $V = U_1 \cap U_3 = U_1 \cap U_2$, where $U_1 = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{F}^n\}$. Therefore $V = \{\mathbf{0}\}$ and $d = r - q = 0$.

Finally, if $0 = q < r$ then rank $\mathbf{B} = n$. Consequently, $U_1 = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{F}^n\}$ is of dimension n over $\mathbb{F}$ and, by Proposition 4 of Chapter 3, $U_1 = \mathbb{F}^n$. Therefore $V = \mathbb{F}^n \cap U_3 = U_3$, where $U_3 = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{ABx} = \mathbf{0}\}$, therefore $d = \dim V = n - \text{rank } \mathbf{AB} = r$, by Theorem 2. Therefore $d = r - q$.

We conclude that, in all cases, the dimension of V is,

$$d = r - q = (n - \text{rank } \mathbf{AB}) - (n - \text{rank } \mathbf{B}) = \text{rank } \mathbf{B} - \text{rank } \mathbf{AB}. \quad \bullet$$

By collecting the results from Propositions 9 and 10 we obtain the following theorem which gives bounds for rank $\mathbf{AB}$ for any two $n \times n$ matrices $\mathbf{A}$ and $\mathbf{B}$.

• Theorem 6

Let **A** and **B** be $n \times n$ matrices over a field $\mathbb{F}$ and let s be the smaller of rank **A** and rank **B**. Then $s \geq \text{rank } \mathbf{AB} \geq \text{rank } \mathbf{A} + \text{rank } \mathbf{B} - n$.

PROOF

By Proposition 9, $s \geq \text{rank } \mathbf{AB}$. To prove the other inequality, we consider the vector space V of Proposition 10, which is a subspace of $W = \{ \mathbf{x} \in \mathbb{F}^n : \mathbf{Ax} = \mathbf{0} \}$. By Theorem 2, dim $W = n - \text{rank } \mathbf{A}$ and, by Proposition 10, dim $V = \text{rank } \mathbf{B} - \text{rank } \mathbf{AB}$. Also, because V is a subspace of W, dim $V \leq$ dim W, therefore rank **B** − rank **AB** $\leq n - \text{rank } \mathbf{A}$. Thence rank **A** + rank **B** $\leq$ rank **AB** + n, and we conclude that rank **AB** $\geq$ rank **A** + rank **B** − n. ●

⊙ Example 10

Let us see how Theorem 6 applies to the matrices

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 4 \\ 4 & 2 & 6 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 2 & 1 & 3 \\ 2 & -1 & 1 \\ -2 & 2 & 0 \end{pmatrix}.$$

We have

$$\mathbf{A} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & -5 & -5 \\ 0 & -6 & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & -5 & -5 \\ 0 & 0 & 0 \end{pmatrix}, \text{ therefore rank } \mathbf{A} = 2;$$

$$\mathbf{B} \sim \begin{pmatrix} 2 & 1 & 3 \\ 0 & -2 & -2 \\ 0 & 3 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 3 \\ 0 & -2 & -2 \\ 0 & 0 & 0 \end{pmatrix}, \text{ therefore rank } \mathbf{B} = 2.$$

Therefore, by Theorem 6, rank **A** + rank **B** − 3 = 1 $\leq$ rank **AB** $\leq$ 2, as this is the smaller of rank **A** and rank **B**. But

$$\mathbf{AB} = \begin{pmatrix} 0 & 5 & 5 \\ 0 & 10 & 10 \\ 0 & 14 & 14 \end{pmatrix} \sim \begin{pmatrix} 0 & 5 & 5 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \text{ therefore rank } \mathbf{AB} = 1.$$

Therefore rank **AB** equals the lower bound given by the inequality.

Now let us consider the rank of **AC**, where

$$\mathbf{C} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Because **C** is in echelon form, it is obvious that rank **C** = 2 and therefore $1 \leq$ rank **AC** ≤ 2 by the calculation we used for **AB**. However,

$$\mathbf{AC} \sim \begin{pmatrix} 1 & 2 & 0 \\ 3 & 1 & 0 \\ 4 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 \\ 0 & -5 & 0 \\ 0 & -6 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 0 \\ 0 & -5 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Because the last matrix is also in echelon form, rank $\mathbf{AC} = 2$, consequently rank $\mathbf{AC}$ equals the upper bound given by the inequality.

To investigate the extreme values that the formulae predict, let us also apply them to the $n \times n$ matrices $\mathbf{I}$ and $\mathbf{O}$. Then

$$n = 2 \times \text{rank } \mathbf{I} - n \leq \text{rank } \mathbf{I}^2 \leq \text{rank } \mathbf{I} = n$$

and

$$-n = 2 \times \text{rank } \mathbf{0} - n \leq \text{rank } \mathbf{0}^2 \leq \text{rank } \mathbf{0} = 0.$$

Summary

Matrices cannot be used to multiply vectors in vector spaces, even those of finite dimension, unless they are also of finite degree. In order to provide a substitute for the matrix, the notion of a **linear transformation** was introduced to have the basic properties of the matrix transformation $\mathbf{w} = \mathbf{Av}$ for $\mathbf{v} \in \mathbb{F}^n$ into $\mathbb{F}^m$, where $\mathbf{A}$ is an $m \times n$ matrix over the field $\mathbb{F}$. The mapping T of the vector space V over $\mathbb{F}$ into the vector space W over $\mathbb{F}$ was defined to be a linear transformation if $T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$ and $T(c\mathbf{v}) = cT(\mathbf{v})$ for all $\mathbf{u}$ and $\mathbf{v} \in V$ and all $c \in \mathbb{F}$. In fact, all linear transformations of a total vector space into another are matrix transformations, so the notion is not a generalization in this case.

We found the elementary properties of linear transformations. First, it was shown that if V is of finite dimension then its image $T(V)$, called the **range** of T, is a subspace of W of finite dimension over $\mathbb{F}$, and the dimension of W is called the **rank** of T. A property of T which is often used in these calculations is that the image of a basis of V spans $T(V)$, the image of V. The **kernel** of T, which is the set of vectors $\mathbf{k}$ in V such that $T(\mathbf{k}) = \mathbf{0}$, was shown to play a vital part in determining the range of T, and the kernel is itself a subspace of V. Therefore when V is finite-dimensional the kernel has a finite dimension, called the **nullity** of T. The main result of the chapter is the **dimension theorem**, which states that if V is a finite-dimensional vector space with linear transformation T then the sum of the rank and the nullity of T is equal to the dimension of V. The dimension theorem yields the dimension of the space of solutions of a system of homogeneous linear equations and bounds for the rank of a product of two matrices.

These results on linear transformations were then used to explore the relationship between an abstract vector space V of dimension n over a field $\mathbb{F}$ and the total vector space $\mathbb{F}^n$. Because V is not necessarily a set of ordered n-tuples, V cannot always be equal to $\mathbb{F}^n$, so a more general relation was found which indicates that two vector spaces have the same algebraic properties even though they may consist of sets of different kinds. For this reason we defined a linear transformation θ of a vector space W over a field $\mathbb{F}$ onto the vector space V over $\mathbb{F}$ to be an **isomorphism** if θ is a bijection of W onto V. If there is an isomorphism of W onto V then V and W are said to be **isomorphic**. This definition was chosen so that the image of a linear combination of vectors

$\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_k$ under θ is the same linear combination of $\mathbf{v}_1\theta, \mathbf{v}_2\theta, \mathbf{v}_3\theta, \ldots, \mathbf{v}_k\theta$. Because algebraic properties in vector spaces can all be written in terms of linear combinations, this result demonstrated that if V and W are isomorphic then they certainly have the same algebraic properties. The initial idea in our major result about isomorphism of a finite-dimensional vector space V is the observation that any basis of V can be converted into an **ordered basis** B by choosing an order in which the elements appear. The ordered basis B was then used to define a bijection ρ of V onto $\mathbb{F}^n$, called the **representation of V with respect to** B. We then showed that ρ is an isomorphism of V onto $\mathbb{F}^n$, a result we could restate by saying that every vector space of dimension n over $\mathbb{F}$ is essentially like $\mathbb{F}^n$. The disadvantage of this important result is that the representation ρ of V with respect to B is not necessarily the same as the representation σ with respect to a different basis C. However, we showed that there is a non-singular matrix $\mathbf{R}$ which determines C in terms of B and that $\mathbf{P} = \mathbf{R}^{-1}$, which is called the **transition matrix**, determines $\mathbf{v}\sigma$ for all $\mathbf{v} \in V$ by the equation $\mathbf{v}\sigma = \mathbf{P}(\mathbf{v}\rho)$.

EXERCISES ON CHAPTER 4

1. Find the range $R = \{\mathbf{Av} \in W : \mathbf{v} \in V\}$ for each of the following matrix linear transformations $\mathbf{w} = \mathbf{Av}$ of $V = \mathbb{Q}^3$ into $W = \mathbb{Q}^3$.

(i) $\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ (ii) $\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 5 & 15 \\ 0 & 0 & 0 \end{pmatrix}$

(iii) $\mathbf{A} = \begin{pmatrix} 1 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ (iv) $\mathbf{A} = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix}$.

2. Let us write the total vector space $V = \mathbb{R}^3$ in the form

$$V = \{\mathbf{v} = (a \quad b \quad c)^{\mathrm{T}} : a, b, c \in \mathbb{R}\}$$

Which of the following six mappings T of V into the total vector space $W = \mathbb{R}^m$, where m is a positive integer, is a linear transformation over $\mathbb{R}$? For each linear transformation find the $m \times 3$ matrix $\mathbf{A}$ over $\mathbb{R}$ such that $T(\mathbf{v}) = \mathbf{Av}$ for all $\mathbf{v} \in V$.

(i) $m = 3$, $T(\mathbf{v}) = (a \quad b \quad 2b)^{\mathrm{T}}$
(ii) $m = 2$, $T(\mathbf{v}) = (a + 2b \quad b + 3c)^{\mathrm{T}}$
(iii) $m = 3$, $T(\mathbf{v}) = (a + 1 \quad b + 1 \quad c + 1)^{\mathrm{T}}$
(iv) $m = 1$, $T(\mathbf{v}) = (2a + 3b + c)^{\mathrm{T}}$
(v) $m = 3$, $T(\mathbf{v}) = (a + 3b + 5c \quad 3a + 2b + c \quad 4a - 6b + 7c)^{\mathrm{T}}$
(vi) $m = 3$, $T(\mathbf{v}) = (a^3 + 2b^2 \quad b^2 - 6c \quad c)^{\mathrm{T}}$

3. Let T be a linear transformation of the vector space V over a field $\mathbb{F}$ into a vector space W over $\mathbb{F}$ and let $R = \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \ldots, \mathbf{u}_n\}$ be a finite set vectors in V which is linearly dependent over $\mathbb{F}$. Prove that $S = \{T(\mathbf{u}_1), T(\mathbf{u}_2), T(\mathbf{u}_3), \ldots, T(\mathbf{u}_n)\}$ is linearly dependent over $\mathbb{F}$.

4. In each of the following 15 cases, decide if the mapping T of the vector space V of dimension r over the field $\mathbb{F}$ into the vector space W over $\mathbb{F}$ is a linear transformation.

   (i) $V = \mathrm{P}_4(\mathbb{R})$, $\mathbb{F} = \mathbb{R}$, $r = 5$, $W = \mathrm{P}_4(\mathbb{R})$ and $T(f(x)) = (\mathfrak{D}^2 + 2)f(x)$ for all $f(x) \in V$.

   (ii) $V = \mathbb{R}^4$, $\mathbb{F} = \mathbb{R}$, $r = 4$, $W = \mathbb{R}^4$ and $T(\mathbf{v}) = (a + 2b \quad b \quad 3d \quad 2c)^{\mathrm{T}}$ for all $\mathbf{v} = (a \quad b \quad c \quad d)^{\mathrm{T}} \in V$.

   (iii) V is the vector space of real functions $f(x)$ such that $\mathfrak{D}^n f(x)$ exists for all positive integers n, $\mathbb{F} = \mathbb{R}$, r is infinite, W is the space of all real functions and $T(f(x)) = (\mathfrak{D}^2 + 3\mathfrak{D} + 2)f(x)$ for all $f(x) \in V$.

   (iv) $V = \mathbb{C}^3$, $\mathbb{F} = \mathbb{C}$, $r = 3$, $W = \mathbb{C}^2$ and $T(\mathbf{v}) = (a + 2b \quad c + 1)^{\mathrm{T}}$ for all $\mathbf{v} = (a \quad b \quad c)^{\mathrm{T}} \in V$.

   (v) V is the vector space of all real sequences, $\mathbb{F} = \mathbb{R}$, r is infinite, $W = V$, and, for each sequence $S \in V$ given by $a_1, a_2, a_3, \ldots, a_n, \ldots$, $T(S)$ is the sequence $2a_1, 2a_2, 2a_3, \ldots, 2a_k, 0, 0, 0, \ldots, 0, \ldots$, where k is a fixed positive integer.

   (vi) $V = \mathrm{P}_4(\mathbb{R})$, $\mathbb{F} = \mathbb{R}$, $r = 5$, $W = \mathrm{P}_3(\mathbb{R})$ and $T(f(x)) = ab + cx + dx^2 + ex^3$ for all $f(x) = a + bx + cx^2 + dx^3 + ex^4 \in V$.

   (vii) V is the vector space of functions of the real variable x which are continuous for all x satisfying $-1 \leq x \leq 1$, $\mathbb{F} = \mathbb{R}$, r is infinite, $W = \mathbb{R}^1 = \mathbb{R}$ and $T(f(x)) = \int_{-1}^{1} [f(x)\sin(\pi x)]\,dx$ for all $f(x) \in V$.

   (viii) $V = \mathrm{M}_3(\mathbb{R})$, the vector space of 3×3 matrices over $\mathbb{R}$, $\mathbb{F} = \mathbb{R}$, $r = 9$, W is the vector space of 2×3 matrices over $\mathbb{R}$ and $T(\mathbf{A}) = \mathbf{KA}$ where $\mathbf{K}$ is a fixed 2×3 matrix over $\mathbb{R}$.

   (ix) $V = \mathbb{Q}^3$, $\mathbb{F} = \mathbb{Q}$, $r = 3$, $W = \mathbb{Q}^4$ and $T(\mathbf{v}) = (b \quad c \quad a \quad 1)^{\mathrm{T}}$ for all $\mathbf{v} = (a \quad b \quad c)^{\mathrm{T}} \in V$.

   (x) $V = \mathbb{C}^3$, $\mathbb{F} = \mathbb{C}$, $r = 3$, $W = \mathbb{C}^2$ and $T(\mathbf{v}) = (a + 2b + 4c \quad 2a + 5b + 11c)^{\mathrm{T}}$ for all $\mathbf{v} = (a \quad b \quad c)^{\mathrm{T}} \in V$.

   (xi) $V = \langle \sin 2x, \cos 3x, x^2 - 3x + 5 \rangle$ in the vector space of all real functions of the real variable x, $\mathbb{F} = \mathbb{R}$, $r = 3$ and $T(f(x)) = \mathfrak{D}^3 f(x)$ for all $f(x) \in V$.

   (xii) $V = \mathbb{C}$, $\mathbb{F} = \mathbb{R}$, $r = 2$, $W = \mathbb{R}$ and $T(z) = |z|$ for all $z \in V$.

   (xiii) $V = \mathrm{P}_3(\mathbb{Q})$, $\mathbb{F} = \mathbb{Q}$, $r = 4$, $W = \mathbb{Q}^4$ and $T(f(x)) = (c \quad a \quad b \quad d)^{\mathrm{T}}$ for all $f(x) = a + bx + cx^2 + dx^3 \in V$.

   (xiv) V is the vector space of twice differentiable functions of a real variable x, $\mathbb{F} = \mathbb{R}$, r is infinite, $W = \mathbb{R}^1 = \mathbb{R}$ and $T(f(x)) = \int_0^1 f(x)\,dx$ for all $f(x) \in V$.

   (xv) $V = \mathbb{R}[x]$, $\mathbb{F} = \mathbb{R}$, r is infinite, W is the vector space of infinite sequences over $\mathbb{R}$ and $T(f(x))$ is the sequence of coefficients of $1, x, x^2, x^3, \ldots, x^n, \ldots$ for the polynomial $\mathfrak{D}^2 f(x)$, for each $f(x) \in V$.

5. For each linear transformation T of a vector space V of finite dimension r in Exercise 4, find the range and the rank of T.

6. For each linear transformation T of a vector space V of finite dimension r in Exercise 4, find the kernel and the nullity of T.

7. The vector space V over $\mathbb{R}$ of solutions of the differential equation $[\mathcal{D}^2 - 4\mathcal{D} + 4]y = 0$ is $V = \{(r + sx)e^{2x} : r, s \in \mathbb{R}\}$. Prove that $V \cong \mathbb{R}^2$ by finding an isomorphism of V onto $\mathbb{R}^2$.

8. Let V and W be vector spaces over a field $\mathbb{F}$, let θ be an isomorphism of V onto W and let $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n\}$ be a basis of V. Prove that $B\theta = \{\mathbf{b}_1\theta, \mathbf{b}_2\theta, \mathbf{b}_3\theta, \ldots, \mathbf{b}_n\theta\}$ is a basis of W.

9. Let V be the vector space over $\mathbb{R}$ of functions of the real variable x with ordered basis $B = \{b_1(x) = e^{2x}, b_2(x) = e^{-2x}\}$. Find the representation $a(x)\rho$ of $a(x) = 4 \sinh 2x$ with respect to B. Show that $C = \{c_1(x) = e^{-2x}, c_2(x) = 2 \cosh 2x\}$ is an ordered basis of V by finding a non-singular matrix $\mathbf{R}$ which expresses C in terms of B as in Theorem 4. Find the representation $a(x)\sigma$ of $a(x)$ with respect to C. Find the non-singular matrix $\mathbf{P}$ such that $f(x)\sigma = \mathbf{P}(f(x)\rho)$ for all $f(x) \in V$ and check that $a(x)\sigma = \mathbf{P}(a(x)\rho)$.

10. Let V be the subspace of $\mathbb{Q}^4$ with ordered basis $B = \{\mathbf{b}_1 = (2, 3, 1, 4), \mathbf{b}_2 = (1, 0, -1, 1)\}$ and let $\mathbf{a} = (5, 9, 2, 11)$. Find the representation $\mathbf{a}\rho$ of $\mathbf{a}$ with respect to B. Show that $C = \{\mathbf{c}_1 = (4, 3, -1, 6), \mathbf{c}_2 = (5, 3, -2, 7)\}$ is an ordered basis of V by finding a non-singular matrix $\mathbf{R}$ which expresses C in terms of B as in Theorem 4. Find the representation $\mathbf{a}\sigma$ of $\mathbf{a}$ with respect to C. Find the non-singular matrix $\mathbf{P}$ such that $\mathbf{v}\sigma = \mathbf{P}(\mathbf{v}\rho)$ for all $\mathbf{v} \in V$.

11. Let V be the subspace of $\mathbb{R}[x]$ with ordered basis $B = \{b_1(x) = x, b_2(x) = x^2, b_3(x) = x^4\}$. Show that $C = \{c_1(x) = x, c_2(x) = x^2 + 3x, c_3(x) = x^4 + 2x^2 + 5x\}$ is an ordered basis of V. Find the transition matrix $\mathbf{P}$ such that, for all $f(x) \in V$, we have $f(x)\sigma = \mathbf{P}(f(x)\rho)$, where ρ is the representation of V with respect to B and σ is the representation of V with respect to C.

12. Let $\mathbf{A}$ and $\mathbf{B}$ be $m \times n$ matrices over a field $\mathbb{F}$.

(i) Prove that $\text{rank}(\mathbf{A} + \mathbf{B}) \leq \text{rank}\,\mathbf{A} + \text{rank}\,\mathbf{B}$.

(ii) Show that there exists a matrix $\mathbf{C}$ such that $\text{rank}(\mathbf{A} + \mathbf{C}) = 0$.

(iii) Let $\mathbf{D}$ and $\mathbf{E}$ be $(p + q) \times (p + q)$ matrices over $\mathbb{F}$ which are partitioned as $\mathbf{D} = \begin{pmatrix} \mathbf{I}_p & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$ and $\mathbf{E} = \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_q \end{pmatrix}$, where $\mathbf{I}_p$ is a $p \times p$ identity submatrix and $\mathbf{I}_q$ is a $q \times q$ identity submatrix. Show that $\text{rank}\,(\mathbf{D} + \mathbf{E}) = \text{rank}\,\mathbf{D} + \text{rank}\,\mathbf{E}$.

13. Let $\mathbf{A}$ and $\mathbf{B}$ be 4×4 matrices over the field $\mathbb{F}$ and let $V = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{F}^4, \mathbf{ABx} = \mathbf{0}\}$. Show that $0 \leq \dim_{\mathbb{F}} V \leq \text{rank}\,\mathbf{B}$. Find the dimension of V when the matrices $\mathbf{A}$ and $\mathbf{B}$ are given by

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & -1 & 4 \\ 2 & -2 & 0 & 3 \\ 3 & 0 & -1 & 7 \\ 1 & -4 & 1 & -1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 2 & 3 & 3 & 2 \\ 1 & 2 & 0 & 1 \\ 2 & -1 & 2 & 2 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

14. Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times n$ matrices over a field $\mathbb{F}$ such that null $\mathbf{A} = p$ and null $\mathbf{B} = q$. Prove that

$$\max\{p, q\} \leq \text{null } \mathbf{AB} \leq p + q.$$

This result is called **Sylvester's law of nullity**.

5 · The Matrix Representation of Linear Transformations

Outline

In the previous chapter it was proved that every linear transformation of a total vector space into a total vector space is a matrix linear transformation. Also it was proved that any ordered basis of a vector space of finite dimension determines an isomorphism of the vector space onto the total vector space of the same dimension. Here these results are combined to prove that any linear transformation of a finite-dimensional vector space can be represented by a matrix linear transformation by the use of ordered bases in the domain and range of the transformation. The representations of the vector spaces change when the ordered bases are changed, and the rest of the chapter is devoted to finding the relationship between representations determined by different ordered bases of the domain and the codomain. From this it is deduced that if the domain and codomain are distinct vector spaces, the ordered bases can be chosen so that the matrix of the representation has a very simple form.

Introduction

We start by proving that, just as a vector space V of finite dimension n over a field $\mathbb{F}$ can be represented as a total vector space $\mathbb{F}^n$, a linear transformation T of V can be represented by a matrix linear transformation. This representation not only makes it clear that linear transformations are generalizations of matrices to finite-dimensional abstract vector spaces, but also allows matrices to be used to define linear transformations for these vector spaces. We can assume that T maps V into a vector space W of finite dimension m over $\mathbb{F}$, by Proposition 3 of Chapter 4. Then, by Theorem 3 of Chapter 4, there is an isomorphism ρ of V onto $\mathbb{F}^n$ and an isomorphism σ of W onto $\mathbb{F}^m$. Our intention is to prove that T defines a linear transformation of $\mathbb{F}^n$ onto $\mathbb{F}^m$, which, by Proposition 2 of Chapter 4, would then be a matrix linear transformation. Consider the following example.

○ Example 1

Let $V = W = \mathrm{P}_4(\mathbb{R})$, the vector space of polynomials in x over $\mathbb{R}$ of degree at most 4 together with 0. Let T be the operation of differentiation, that is, let $T(f(x)) = \mathcal{D}f(x)$, for all $f(x) \in V$. By the formulae of differential calculus, T is a linear transformation of V

into W and, as in Example 12 of Chapter 3, $B = \{1, x, x^2, x^3, x^4\}$ is a basis of V and of W. For any $f(x) \in V$, there exist $a, b, c, d, e \in \mathbb{R}$ such that $f(x) = a + bx + cx^2 + dx^3 + ex^4$. The representation $f(x)\rho$ of $f(x)$ with respect to B, found by the method of Proposition 8 of Chapter 4, is $f(x)\rho = (a \quad b \quad c \quad d \quad e)^{\mathrm{T}}$. Because $T(f(x)) = \mathcal{D}f(x)$ and $\mathcal{D}f(x) = b + 2cx + 3dx^2 + 4ex^3$, the representation σ of W with respect to B is $T(f(x))\sigma = (b \quad 2c \quad 3d \quad 4e \quad 0)^{\mathrm{T}}$. In this easy case we can see that $T(f(x))\sigma = \mathbf{A}(f(x)\rho)$, where

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The mixture of notation in $T(f(x))\sigma = \mathbf{A}(f(x)\rho)$ in Example 1, with the linear transformation T written like a function and the isomorphisms ρ and σ written in Greek letters after their variables, gives a clear impression of what we wish to prove as a theorem, but in order to prove the result it is better to write all the mappings on the same side of the variables. To clarify expressions such as $T(f(x))\sigma$, it is better to write all the mappings to the right of their variables. Consequently, we write $T(f(x))$ (temporarily) as $f(x)\tau$ and the expression for $T(f(x))\sigma$ becomes $(f(x)\tau)\sigma = f(x)\tau\sigma$. Then the desired result becomes $f(x)\tau\sigma = \mathbf{A}(f(x)\rho)$. Also we would like the equation to refer to elements of the same vector space on both sides and hence refer to $f(x)\rho \in \mathbb{R}^n$ on the left-hand side. Because ρ is a bijection, according to Definition 3 of Chapter 4, we can write $f(x) = (f(x)\rho)\rho^{-1}$. Then the required equation becomes $\mathbf{v}\rho^{-1}(\tau\sigma) = \mathbf{A}\mathbf{v}$, where $\mathbf{v}$ ranges over $\mathbb{R}^n$. Therefore we can prove the desired result provided that $\rho^{-1}(\tau\sigma)$ is a linear transformation. This follows from the following two propositions.

• Proposition 1

Let U, V and W be vector spaces over a field $\mathbb{F}$, let L be a linear transformation of U into V and let M be a linear transformation of V into W. Then the composite T of L and M, defined by $T(\mathbf{u}) = M(L(\mathbf{u}))$ for all $\mathbf{u} \in U$, is a linear transformation of U into W.

PROOF

For the proof we denote L and M by λ and μ, where $L(\mathbf{u}) = \mathbf{u}\lambda$ for all $\mathbf{u} \in U$, and $M(\mathbf{v}) = \mathbf{v}\mu$ for all $\mathbf{v} \in V$. Then $T(\mathbf{u}) = \mathbf{u}\lambda\mu$. By Definition 1 of Chapter 4, for all $\mathbf{u}_1$, $\mathbf{u}_2 \in U$,

$$\begin{aligned} T(\mathbf{u}_1 + \mathbf{u}_2) &= (\mathbf{u}_1 + \mathbf{u}_2)\lambda\mu = \big((\mathbf{u}_1 + \mathbf{u}_2)\lambda\big)\mu \\ &= (\mathbf{u}_1\lambda + \mathbf{u}_2\lambda)\mu = (\mathbf{u}_1\lambda)\mu + (\mathbf{u}_2\lambda)\mu \\ &= \mathbf{u}_1(\lambda\mu) + \mathbf{u}_2(\lambda\mu) \\ &= T(\mathbf{u}_1) + T(\mathbf{u}_2), \end{aligned}$$

where $(\mathbf{u}_j\lambda)\mu = \mathbf{u}_j(\lambda\mu)$, for $j = 1, 2$, by the definition of composition of mappings. Also by Definition 1 of Chapter 4, for all $\mathbf{u} \in U$ and $c \in \mathbb{F}$,

$$T(c\mathbf{u}) = (c\mathbf{u})\ (\lambda\mu) = [(c\mathbf{u})\lambda]\mu = [c(\mathbf{u}\lambda)]\mu = c[(\mathbf{u}\lambda)\mu] = c(\mathbf{u}\lambda\mu) = cT(\mathbf{u}).$$

Therefore T is a linear transformation of U into W.

• Proposition 2

Let R be an isomorphism of a vector space V over a field $\mathbb{F}$ onto a vector space W over $\mathbb{F}$, that is, let R be a bijection of V onto W, such that R is a linear transformation. Then the inverse R^{-1} of R is an isomorphism of W onto V.

PROOF

Because a discussion of inverse mappings involves composition, let us rewrite $R(\mathbf{v})$ as $\mathbf{v}\rho$ for all $\mathbf{v} \in V$. By definition, the inverse ρ^{-1} is a bijection of W onto V. Also, because ρ is a mapping of V onto W, for all $\mathbf{w}_1, \mathbf{w}_2 \in W$, there exists $\mathbf{v}_1, \mathbf{v}_2 \in V$ such that $\mathbf{w}_1 = \mathbf{v}_1\rho$ and $\mathbf{w}_2 = \mathbf{v}_2\rho$. Therefore, by Definition 1 of Chapter 4,

$$\begin{aligned}(\mathbf{w}_1 + \mathbf{w}_2)\rho^{-1} &= (\mathbf{v}_1\rho + \mathbf{v}_2\rho)\rho^{-1} \\ &= \big((\mathbf{v}_1 + \mathbf{v}_2)\rho\big)\rho^{-1} = (\mathbf{v}_1 + \mathbf{v}_2)(\rho\rho^{-1}) \\ &= \mathbf{v}_1 + \mathbf{v}_2 \\ &= \mathbf{w}_1\rho^{-1} + \mathbf{w}_2\rho^{-1}\end{aligned}$$

because $\mathbf{v}_1\rho = \mathbf{w}_1$ and $\mathbf{v}_2\rho = \mathbf{w}_2$. Also, by Definition 1 of Chapter 4, for $c \in \mathbb{F}$,

$$(c\mathbf{w}_1)\rho^{-1} = (c\mathbf{v}_1\rho)\rho^{-1} = \big((c\mathbf{v}_1)\rho\big)\rho^{-1} = (c\mathbf{v}_1)(\rho\rho^{-1}) = c\mathbf{v}_1.$$

But $\mathbf{v}_1\rho = \mathbf{w}_1$, therefore $(c\mathbf{w}_1)\rho^{-1} = c(\mathbf{w}_1\rho^{-1})$. We conclude that R^{-1}, which is an alternative notation for ρ^{-1}, is an isomorphism of W onto V. ●

Propositions 1 and 2, taken together, imply that isomorphism is an equivalence relation, so the relation of isomorphism can be used as an abstract equality for vector spaces. We can now prove the theorem forecast in Example 1 on matrix representation of linear transformations.

• Theorem 1

Let $\mathbb{F}$ be a field, let V and W be vector spaces of finite dimension n and m, respectively, over $\mathbb{F}$ and let T be a linear transformation of V onto W. Let ρ be the representation of V with respect to the ordered basis B and let σ be the representation of W with respect to the ordered basis C. Then there exists an $m \times n$ matrix $\mathbf{A}$ over $\mathbb{F}$ such that, for all $\mathbf{v} \in V$,

$$T(\mathbf{v})\sigma = \mathbf{A}(\mathbf{v}\rho).$$

PROOF

Let us rewrite $T(\mathbf{v})$ as $\mathbf{v}\tau$, for all $\mathbf{v} \in V$. Then

$$T(\mathbf{v})\sigma = (\mathbf{v}\tau)\sigma = \mathbf{v}(\tau\sigma) = \big[\mathbf{v}(\rho\rho^{-1})\big](\tau\sigma) = (\mathbf{v}\rho)\big[\rho^{-1}(\tau\sigma)\big] = (\mathbf{v}\rho)\big[(\rho^{-1}\tau)\sigma\big]$$

because ρ is a bijection and the product of mappings is associative. By Theorem 3 of Chapter 4, ρ is an isomorphism of V onto $\mathbb{F}^n$ and therefore, by Proposition 2, ρ^{-1} is an isomorphism of $\mathbb{F}^n$ onto V. Consequently, as τ is a linear transformation of V into W, by

Proposition 1, $\rho^{-1}\tau$ is a linear transformation of $\mathbb{F}^n$ into W. Again, by Theorem 3 of Chapter 4, σ is an isomorphism of W onto $\mathbb{F}^m$, therefore, by Proposition 1, $(\rho^{-1}\tau)\sigma$ is a linear transformation of $\mathbb{F}^n$ into $\mathbb{F}^m$.Therefore, by Proposition 2 of Chapter 4, there exists an $m \times n$ matrix $\mathbf{A}$ over $\mathbb{F}$ such that, for all $\mathbf{x} \in \mathbb{F}^n$, $\mathbf{x}[(\rho^{-1}\tau)\sigma] = \mathbf{Ax}$. Consequently, as ρ maps V into $\mathbb{F}^n$, for all $\mathbf{v} \in V$, $(\mathbf{v}\rho)[(\rho^{-1}\tau)\sigma] = \mathbf{A}(\mathbf{v}\rho)$. Therefore, for all $\mathbf{v} \in V$, $T(\mathbf{v})\sigma = \mathbf{A}(\mathbf{v}\rho)$. ●

We call the matrix $\mathbf{A}$ of Theorem 1, or the matrix linear transformation it defines, the **representation of the linear transformation T with respect to the ordered bases B and C.** The existence of this representation shows that linear transformations are analogues of matrices for all vector spaces of finite dimension. In the following example the representations of a linear transformation with respect to two different ordered bases are found.

○ Example 2

Consider the vector space $V = \langle e^x, e^{-x} \rangle$ of Example 8 in Chapter 4. There we chose two ordered bases $B = \{b_1(x) = e^x, b_2(x) = e^{-x}\}$ and $C = \{c_1(x) = \sinh x, c_2(x) = \cosh x\}$. Let T be the linear transformation of V into itself defined by $T(f(x)) = \mathcal{D}f(x)$.

First we represent T with respect to the ordered basis B and represent V by the representation ρ with respect to B as both domain and codomain. For $f(x) = pe^x + qe^{-x} \in V$, where $p, q \in \mathbb{R}$, we have $f(x)\rho = (p \quad q)^{\mathrm{T}}$. Also $T(f(x)) = \mathcal{D}f(x) = pe^x - qe^{-x}$, so $T(f(x))\rho = \quad (p \quad -q)^{\mathrm{T}}$. Therefore, by the proof of Proposition 2 of Chapter 4,

$$T(f(x))\rho = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}(f(x)\rho).$$

Now we represent T with respect to the ordered basis C of V and represent V by the representation σ with respect to C as both domain and codomain. Then we write $f(x) = pe^x + qe^{-x} = r \sinh x + s \cosh x$. Because $\sinh x = (e^x - e^{-x})/2$ and $\cosh x = (e^x + e^{-x})/2$, we deduce that $f(x) = \frac{1}{2}(r+s)e^x + \frac{1}{2}(s-r)e^{-x}$. Therefore, $r + s = 2p$ and $s - r = 2q$, whence $r = p - q$ and $s = p + q$. Consequently,

$$f(x) = (p-q)\sinh x + (p+q)\cosh x \quad \text{and} \quad f(x)\sigma = \begin{pmatrix} p-q \\ p+q \end{pmatrix}.$$

Therefore

$$T(f(x)) = \mathcal{D}f(x) = (p-q)\cosh x + (p+q)\sinh x,$$

and consequently

$$T(f(x))\sigma = \begin{pmatrix} p+q \\ p-q \end{pmatrix}.$$

Hence

$$T(f(x))\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}(f(x)\sigma),$$

by the proof of Proposition 2 of Chapter 4.

We conclude that T is represented by the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ with respect to the ordered basis B but by the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with respect to the ordered basis C.

A linear transformation of $\mathbb{F}^n$ into $\mathbb{F}^m$ corresponds to a unique $m \times n$ matrix over $\mathbb{F}$, by Proposition 2 of Chapter 4. Essentially, this is because a total vector space has a standard basis and every vector in it has a natural expression as a column vector. However, for a linear transformation T of a vector space V of dimension n over a field $\mathbb{F}$ into a vector space W of dimension m over $\mathbb{F}$, T corresponds to a set of matrices $R = \{\mathbf{A}(B, C)\}$, where B ranges over the ordered bases of V and C ranges over the ordered bases of W and $\mathbf{A}(B, C)$ is determined by these bases as in Theorem 1. Proposition 5 of Chapter 3 shows that there is a wide range of choices for B and for C, therefore R is an infinite set. This suggests that it may be possible to choose a simple matrix in R to represent T uniquely. However, in the case where $W = V$, the linear transformation T corresponds to $S = \{\mathbf{A}(B)\}$, where B ranges over the ordered bases of V and $\mathbf{A}(B)$ is the representation of T with respect to the ordered basis B for V as both domain and codomain. Because S is probably a more restricted set than R, the finding of a representative matrix is likely to be more difficult. Whether $W = V$ or not, our first problem is to determine the sets R and S by finding the effects of changing the ordered bases for V and W. The following result, which is easier to prove than to state, relates the matrix representation of T with respect to new bases to its representation with respect to B and C.

• *Proposition 3*

Let T be a linear transformation of the vector space V of finite dimension n over a field $\mathbb{F}$ into the vector space W of the finite dimension m over $\mathbb{F}$. Let ρ be the representation of V with respect to the ordered basis B and let σ be the representation of W with respect to the ordered basis C. Let $\mathbf{A}$ be the matrix which represents T with respect to the ordered bases B and C, in that

$$T(\mathbf{v})\sigma = \mathbf{A}(\mathbf{v}\rho) \qquad \text{for all } \mathbf{v} \in V.$$

Let B' be an ordered basis of V, let $\mathbf{P}$ be the transition matrix from B' to B and let ρ' be the representation of V with respect to B'. Let C' be an ordered basis of W, let $\mathbf{Q}$ be the transition matrix from C' to C and let σ' be the representation of W with respect to the ordered basis C'. Let $\mathbf{G}$ be the matrix which represents T with respect to the ordered bases B' and C' in that

$$T(\mathbf{v})\sigma' = \mathbf{G}(\mathbf{v}\rho') \qquad \text{for all } \mathbf{v} \in V.$$

Then

$$\mathbf{G} = \mathbf{Q}^{-1}\mathbf{A}\mathbf{P}.$$

PROOF

By Theorem 5 of Chapter 4, the representation ρ of V with respect to the ordered basis B

is related by the transition matrix $\mathbf{P}$ to the representation ρ' with respect to the ordered basis B' by the equation

$$\mathbf{v}\rho = \mathbf{P}(\mathbf{v}\rho') \qquad \text{for all } \mathbf{v} \in V.$$

Similarly, the representation σ of W with respect to the ordered basis C is related by the transition matrix $\mathbf{Q}$ to the representation σ' with respect to the ordered basis C' by the equation

$$\mathbf{w}\sigma = \mathbf{Q}(\mathbf{w}\sigma') \qquad \text{for all } \mathbf{w} \in W.$$

Because $\mathbf{A}$ is the representation of T with respect to the ordered bases B of V and C of W, we have

$$T(\mathbf{v})\sigma = \mathbf{A}(\mathbf{v}\rho).$$

Therefore

$$T(\mathbf{v})\sigma = \mathbf{AP}(\mathbf{v}\rho')$$

and, because $T(\mathbf{v}) \in W$,

$$\mathbf{Q}[T(\mathbf{v})\sigma'] = \mathbf{AP}(\mathbf{v}\rho').$$

Therefore

$$T(\mathbf{v})\sigma' = \mathbf{Q}^{-1}\mathbf{AP}(\mathbf{v}\rho')$$

and consequently T is represented by $\mathbf{G} = \mathbf{Q}^{-1}\mathbf{AP}$ with respect to the ordered bases B' and C'.

●

For the matrix $\mathbf{G} = \mathbf{Q}^{-1}\mathbf{AP}$ in Proposition 3, the matrices $\mathbf{P}$ and $\mathbf{Q}$ can be chosen freely by suitable choice of bases of V and W provided that $W \neq V$, according to Theorem 4 of Chapter 4. Let $\mathbf{Q}^{-1}$ be chosen so that $\mathbf{Q}^{-1}\mathbf{A}$ is a matrix $\mathbf{R}$ in reduced echelon form, as defined in Allenby, *Linear Algebra*, Chapter 2, Definition 3. Then let $\mathbf{P}$ be chosen so that $(\mathbf{RP})^{\mathrm{T}} = \mathbf{P}^{\mathrm{T}}\mathbf{R}^{\mathrm{T}}$ is also in reduced echelon form. It can be proved that, with these choices of $\mathbf{P}$ and $\mathbf{Q}$, the transformation T in Proposition 3 can be represented by a matrix $\mathbf{N}$, where $\mathbf{N}$ has the partitioned form $\mathbf{N} = \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$. Here the identity submatrix is an $r \times r$ matrix and $r = \text{rank } \mathbf{A}$. The actual matrix $\mathbf{N}$ varies according to the relations of m, n and r. By Theorem 4 of Chapter 3, $r \leq m$ and $r \leq n$, which leaves the following possibilities. If $r = 0$, then $\mathbf{N} = \mathbf{0}$, so we now assume that $r > 0$. If $r = m = n$, then $\mathbf{N} = \mathbf{I}$. If $r = m < n$, then $\mathbf{N} = (\mathbf{I} \quad \mathbf{0})$. If $r = n < m$, then $\mathbf{N} = \begin{pmatrix} \mathbf{I} \\ \mathbf{0} \end{pmatrix}$. However, if $r < m$ and $r < n$ then $\mathbf{N} = \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$. In all these cases, the matrix $\mathbf{N}$ is called the **normal form** of the matrix $\mathbf{A}$, where the word 'normal' does not mean 'usual' but 'perpendicular', which refers to angles which occur in certain applications of the result. However, it would be more useful to know the bases of V and W which lead to the normal form of the matrix which represents the linear transformation rather than to determine it by the matrices $\mathbf{P}$ and $\mathbf{Q}$. This information is given in the proof of the following result.

• Proposition 4

Let T be a linear transformation of rank r of the vector space V of finite dimension n over a field $\mathbb{F}$ into a vector space W of finite dimension m over $\mathbb{F}$. Let B be an ordered basis of V. Then we have an ordered basis C of V and an ordered basis D of W such that T is represented with respect to C and D by the matrix in normal form $\mathbf{N} = \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$, where the submatrix $\mathbf{I}$ is an $r \times r$ matrix, except when $r = 0$ in which case $\mathbf{N} = \mathbf{0}$.

PROOF

Let $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n\}$. then, by Proposition 4 of Chapter 4,

$$T(B) = \{T(\mathbf{b}_1), T(\mathbf{b}_2), T(\mathbf{b}_3), \ldots, T(\mathbf{b}_n)\}$$

spans the range $T(V)$ of T, which is a vector subspace of dimension r in W. By using the method of Example 8 of Chapter 3, we can find a subset

$$D_1 = \{\mathbf{d}_1 = T(\mathbf{b}_{j(1)}), \mathbf{d}_2 = T(\mathbf{b}_{j(2)}), \ldots, \mathbf{d}_r = T(\mathbf{b}_{j(r)})\}$$

which is an ordered basis of $T(V)$, where the integers $j(i)$ satisfy $1 \leq j(1) < j(2) < \ldots < j(r) \leq n$. By Proposition 5 of Chapter 3, there is a subset $D_2 = \{\mathbf{d}_{r+1}, \mathbf{d}_{r+2}, \ldots, \mathbf{d}_n\}$ of W such that

$$D = \{\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_r, \mathbf{d}_{r+1}, \ldots, \mathbf{d}_n\}$$

is an ordered basis of W. Now construct C from B by $C = C_1 \cup C_2$, where

$$C_1 = \{\mathbf{c}_1 = \mathbf{b}_{j(1)}, \mathbf{c}_2 = \mathbf{b}_{j(2)}, \mathbf{c}_3 = \mathbf{b}_{j(3)}, \ldots, \mathbf{c}_r = \mathbf{b}_{j(r)}\},$$

and $C_2 = \{\mathbf{c}_{r+1}, \mathbf{c}_{r+2}, \ldots, \mathbf{c}_n\}$ can be chosen to form a basis of the kernel of T by the proof of Theorem 1 of Chapter 4. Then $T(\mathbf{c}_i) = \mathbf{d}_i$ for $i = 1, 2, 3, \ldots, r$, and $T(\mathbf{c}_i) = \mathbf{0}$ for $i = r+1, r+2, \ldots, n$. Let $\mathbf{v}\rho = (f_1 \ f_2 \ \ldots \ f_n)^{\mathrm{T}}$ be the representation of $\mathbf{v} \in V$ with respect to C. Then, by Proposition 8 of Chapter 4, $\mathbf{v} = \sum_{i=1}^{n} f_i \mathbf{c}_i$. By Proposition 1(ii) of Chapter 4, $T(\mathbf{v}) = \sum_{i=1}^{n} f_i T(\mathbf{c}_i) = \sum_{i=1}^{r} f_i \mathbf{d}_i$, because $T(\mathbf{c}_i) = \mathbf{0}$ for $i = r+1, r+2, \ldots, n$. Let σ be the representation of W with respect to D. Then

$$T(\mathbf{v})\sigma = (f_1 \ f_2 \ \ldots \ f_r \ 0 \ 0 \ \ldots \ 0)^{\mathrm{T}}.$$

Let us write $\mathbf{v}\rho = \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{pmatrix}$, where $\mathbf{v}_1 = (f_1 \ f_2 \ f_3 \ \ldots \ f_r)^{\mathrm{T}}$. Therefore

$$T(\mathbf{v})\sigma = \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{pmatrix} = \mathbf{N}(\mathbf{v}\rho),$$

where $\mathbf{I}$ is an $r \times r$ identity matrix unless $r = 0$, when $\mathbf{N} = \mathbf{0}$. ●

There is no such simple result when $W = V$ and the same basis is chosen for W as for V, when the linear transformation T maps V into itself. Then a change of basis for V automatically changes the basis for W, so that in Proposition 3 the matrix $\mathbf{Q}^{-1}$ is

replaced by $\mathbf{P}^{-1}$. The following theorem states this important special case of Proposition 3 when $W = V$.

• Theorem 2

Let T be a linear transformation of the vector space V of finite dimension n over a field $\mathbb{F}$ into itself. Let ρ be the representation of V with respect to the ordered basis B and let $\mathbf{A}$ be the matrix which represents T with respect to the ordered basis B in that

$$T(\mathbf{v})\rho = \mathbf{A}(\mathbf{v}\rho) \qquad \text{for all } \mathbf{v} \in V.$$

Let B' be an ordered basis of V, let $\mathbf{P}$ be the transition matrix from B' to B and let ρ' be the representation of V with respect to B'. Let $\mathbf{C}$ be the matrix which represents T with respect to the ordered basis B' in that

$$T(\mathbf{v})\rho' = \mathbf{C}(\mathbf{v}\rho') \qquad \text{for all } \mathbf{v} \in V.$$

Then

$$\mathbf{C} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}.$$

○ Example 3

In Example 2 the linear transformation T of $V = \langle e^x, e^{-x} \rangle$ over $\mathbb{R}$ into itself was defined by $T(f(x)) = \mathfrak{D}f(x)$ for all $f(x) \in V$. The linear transformation T is represented by the matrix $\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with respect to the ordered basis $C = \{c_1(x) = \sinh x, c_2(x) = \cosh x\}$.

If this were the only basis that we knew for V, we might hope that with respect to a different ordered basis T might be represented by a simpler matrix, such as a diagonal matrix. In fact, we know from Example 2 that T is represented by the matrix $\mathbf{G} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ with respect to the ordered basis $B = \{b_1(x) = e^x, b_2(x) = e^{-x}\}$. Theorem 2 tells us how to change the representation from $\mathbf{A}$ to $\mathbf{G}$ by changing the basis from C to B. To do this we find the transition matrix $\mathbf{P}$ from B to C (the reverse order is not a mistake) and form $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}$. By Definition 4 of Chapter 4, $\mathbf{P} = \mathbf{R}^{-1}$, where $\mathbf{R}$ is given by Theorem 4 of Chapter 4 as the matrix of coefficients which determines the elements of B in terms of the elements of C. Consequently, $\mathbf{P}$ is the matrix of coefficients which determines C in terms of B, that is, for $j = 1,2$, $c_j(x) = \sum_{i=1}^{2} p_{ij} b_i(x)$. By the definitions of the hyperbolic functions, $c_1(x) = \frac{1}{2}e^x - \frac{1}{2}e^{-x}$ and $c_2(x) = \frac{1}{2}e^x + \frac{1}{2}e^{-x}$. Therefore $\mathbf{P} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$. By one of the usual calculations for the inverse, $\mathbf{P}^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$.

Therefore

$$\mathbf{P}^{-1}\mathbf{AP} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

That is, $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{G}$, as we expected.

This illustrates how to transform the matrix representing a linear transformation when the ordered basis required for the new representation is known, but it does not show how to find the matrix $\mathbf{P}$ to obtain some desired form for the important matrix $\mathbf{P}^{-1}\mathbf{AP}$, where $\mathbf{P}$ is non-singular. In fact, Theorem 2 changes the problem of finding the relations between representations of a linear transformation of a finite-dimensional vector space into a problem about matrices alone. The matrix problem is that of finding a non-singular matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{AP}$ has some required form. Consequently, we shall devote the next chapter to studying the relationship between $\mathbf{A}$ and $\mathbf{P}^{-1}\mathbf{AP}$.

Summary

In Chapter 4 it was proved that any finite-dimensional vector space V over a field $\mathbb{F}$ is isomorphic to a total vector space over F, the representation of V with respect to an ordered basis B of V. Some elementary properties of linear transformations and the result, in Chapter 4, that every linear transformation of a total vector space over $\mathbb{F}$ into a total vector space over $\mathbb{F}$ is a matrix linear transformation are used to prove that any linear transformation T of V into the vector space W over $\mathbb{F}$ with finite ordered basis C is a matrix linear transformation of the representation of V with respect to B into the representation of W with respect to C. This transformation, or its matrix $\mathbf{A}$, is the **representation of the linear transformation T with respect to the ordered bases B and C.** Because the representation of T depends on the ordered bases, the set S of matrices which represent T with respect to all possible pairs of ordered bases when $W \neq V$ is

$$S = \{\mathbf{Q}^{-1}\mathbf{AP} \ : \ \det \mathbf{P} \neq 0, \ \det \mathbf{Q} \neq 0\}.$$

Provided that $W \neq V$, there is a simple process, which starts from any ordered basis of V, to construct ordered bases B of V and C of W such that T is represented by the matrix $\mathbf{N}$ with respect to B and D, where $\mathbf{N}$ is in **normal form**, that is $\mathbf{N} = \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$, where some of the submatrices may not be present for a given matrix $\mathbf{A}$. However, if T is a linear transformation of the vector space V into itself and T is represented by the matrix $\mathbf{A}$ with respect to the ordered basis B, then the set R of matrices which represent T with respect to all possible ordered bases is $R = \{\mathbf{P}^{-1}\mathbf{AP} \ : \ \det \mathbf{P} \neq 0\}$. The next chapter is devoted to the more difficult problem of trying to find a simple matrix in the set R.

EXERCISES ON CHAPTER 5

1. Let L and M be linear transformations of the vector space V over the field $\mathbb{F}$ into the vector space W over $\mathbb{F}$. Show that the mapping $L + M$ is a linear transformation of V into W, where

$$(L + M)(\mathbf{v}) = L(\mathbf{v}) + M(\mathbf{v}) \qquad \text{for all } \mathbf{v} \in V.$$

Let $V = \mathbb{F}^n$, let $W = \mathbb{F}^m$ and let the matrices of L and M be $\mathbf{P}$ and $\mathbf{Q}$, respectively. What is the matrix of $L + M$?

2. Let U, V and W be finite-dimensional vector spaces over a field $\mathbb{F}$ and let $a, b \in \mathbb{F}$. Let K and L be linear transformations of U into V, let M be a linear transformation of V into W and let N be an isomorphism of V onto W. Which of the following expressions define linear transformations, where $X(Y)$ is defined by $X(Y)\mathbf{z} = X(Y(\mathbf{z}))$ for mappings X, Y and vector $\mathbf{z}$?

(i) $aK + bL$ (ii) $M(K + L)$ (iii) $L^{-1}(K)$
(iv) $K - L$ (v) $KL(N)$ (vi) $N^{-1}(M(L))$
(vii) $L(K) + M$ (viii) $(aM)(N^{-1}) + (aM)$

3. Let $\mathbb{F}$ be a field, let L be a linear transformation of $\mathbb{F}^n$ into $\mathbb{F}^m$ with matrix $\mathbf{A}$ and let M be a linear transformation of $\mathbb{F}^m$ into $\mathbb{F}^k$ with matrix $\mathbf{B}$. Show that the linear transformation given by $M(L)\mathbf{v}$ for all $\mathbf{v} \in \mathbb{F}^n$, has matrix $\mathbf{BA}$.

4. In each of the following cases, find the matrix representation of the linear transformation T of the vector space V over the field $\mathbb{F}$ into the vector space W over $\mathbb{F}$ with respect to the ordered basis B of V and the ordered basis C of W. The elements of the ordered bases are written in ascending order.

(i) $\mathbb{F} = \mathbb{Q}$, $V = \mathrm{P}_2(\mathbb{Q})$, $W = \mathrm{P}_4(\mathbb{Q})$, $T(f(x)) = (5 + 3x + x^2)f(x)$ for all $f(x) \in V$, $B = \{1, x, x^2\}$ and $C = \{1, x, x^2, x^3, x^4\}$.

(ii) $\mathbb{F} = \mathbb{Q}$, $V = \mathbb{Q}^4$, $W = \mathrm{M}_2(\mathbb{Q})$, $T(\mathbf{v}) = \begin{pmatrix} 1 & 4 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for all $\mathbf{v} = (a \;\; b \;\; c \;\; d)^{\mathrm{T}} \in V$,

B is a standard basis and $C = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right\}$.

(iii) $\mathbb{F} = \mathbb{R}$, $V = \mathrm{P}_2(\mathbb{R})$, $W = \mathbb{R}^3$, $T(f(x)) = (c \;\; a \;\; b)^{\mathrm{T}}$, where $(\mathfrak{D}^2 + \mathfrak{D} + 1)f(x) = a + bx + cx^2$, $B = \{1, x, x^2\}$ and C is the standard basis.

(iv) $\mathbb{F} = \mathbb{R}$, V and W are subspaces of the vector space of real functions of a real variable x, $T(f(x)) = \mathfrak{D}f(x)$ for all $f(x) \in V$, $B = \{\cos x, 1, x, x^2\}$ and $C = \{\sin x, 1, x\}$.

(v) $\mathbb{F} = \mathbb{R}$, V is a subspace of the vector space of real functions of a real variable x, $W = V$, $T(f(x)) = (\mathfrak{D}^2 + 3\mathfrak{D} + 1)f(x)$ and $B = \{e^{3x}, \sinh 2x, \cosh 2x\}$.

5. In each of the following cases, choose ordered bases to construct a matrix representation of the linear transformation T of the vector space V over the field $\mathbb{F}$ into the vector space W over $\mathbb{F}$.

(i) $\mathbb{F} = \mathbb{Q}$, $V = P_3(\mathbb{Q})$, $W = P_6(\mathbb{Q})$ and $T(f(x)) = a + 2bx + bx^2 + 3cx^3 + cx^4 + 4dx^5 + dx^6$ for all $f(x) = a + bx + cx^2 + dx^3 \in V$.

(ii) $\mathbb{F} = \mathbb{C}$, $V = M_2(\mathbb{C})$, $W = \mathbb{C}^2$ and $T(\mathbf{A}) = (b \quad c)^T$ for all $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in V$.

(iii) $\mathbb{F} = \mathbb{R}$, $V = W = \langle \sin x, x \sin x, \cos x, x \cos x \rangle$ and $T(f(x)) = (\mathcal{D}^2 + 1)f(x)$ for all $f(x) \in V$.

6. Let V be the kernel of the matrix linear transformation S of $\mathbb{R}^4$ into itself with matrix

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 2 & 3 \\ 3 & 2 & 1 & 4 \\ 1 & -2 & -3 & -2 \\ 4 & 4 & 3 & 7 \end{pmatrix}.$$

Let T be the linear transformation of V into $\mathbb{R}[x]$ defined by $T(\mathbf{v}) = (1 + 2x^2 + 3x^4)(a + bx + cx^2 + dx^3)$ for all $\mathbf{v} = (a \quad b \quad c \quad d)^T \in V$. Find a matrix over $\mathbb{R}$ which represents T.

7. Let V be the vector space of real functions of a real variable x over $\mathbb{R}$ with the ordered basis $B_1 = \{e^x, e^{-x}\}$ and let W be the vector space of degree 3 over $\mathbb{R}$ with ordered basis $C_1 = \{(1, 2, 5), (2, 5, 1)\}$. Let T be the linear transformation of V into W which is represented by the matrix $\mathbf{A}_1$ with respect to the ordered bases B_1 and C_1, where $\mathbf{A}_1 = \begin{pmatrix} 5 & 4 \\ 2 & 2 \end{pmatrix}$. In all the ordered bases the elements are written in ascending order.

(i) Find the matrix $\mathbf{A}_2$ which represents T with respect to the ordered basis $B_2 = \{\sinh x, \cosh x\}$ of V and the ordered basis $C_2 = \{(3, 7, 6), (4, 9, 11)\}$ of W.

(ii) Find the matrix $\mathbf{A}_3$ which represents T with respect to the ordered basis $B_3 = \{2e^x + e^{-x}, 3e^x + 2e^{-x}\}$ of V and the ordered basis $C_3 = \{(-1, -3, 4), (-1, -4, 13)\}$ of W.

8. For each of the following linear transformations T of the vector space V over the field $\mathbb{F}$ into the vector space W over $\mathbb{F}$, find an ordered basis B of V and an ordered basis C of W such that T is represented by a normal-form matrix with respect to B and C.

(i) $\mathbb{F} = \mathbb{Q}$, V and W are distinct copies of $\mathbb{Q}^3$, and T is the matrix linear transformation defined by $\mathbf{A} = \begin{pmatrix} 1 & -2 & -1 \\ 2 & 2 & 3 \\ 3 & 0 & 2 \end{pmatrix}$.

(ii) $\mathbb{F} = \mathbb{R}$, V and W are distinct copies of $P_3(\mathbb{R})$, and $T(f(x)) = \mathcal{D}f(x)$ for all $f(x) \in V$.

(iii) $\mathbb{F} = \mathbb{R}$, $V = \langle x \cosh x, 1, x, x^2 \rangle$, $W = \langle \cosh x, x \sinh x, 1, x, x^2 \rangle$ and $T(f(x)) = \mathcal{D}f(x)$ for all $f(x) \in V$.

9. In each of the following cases, find the matrix representation of the linear transformation T of the vector space V over the field $\mathbb{F}$ into itself with respect to the ordered basis B, in which the elements are written in ascending order.

(i) $\mathbb{F} = \mathbb{Q}$, $V = \{\mathbf{v} = (a + b, 2a - b, 3a + b) : a, b \in \mathbb{Q}\}$, $T(\mathbf{v}) = (4a - 3b, 5a, 6a - 5b)$ and $B = \{(0, 3, 2), (1, -1, 1)\}$.

(ii) $\mathbb{F} = \mathbb{R}$, $V = \mathrm{M}_2(\mathbb{R})$, $T\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ and

$$\mathbf{B} = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right\}.$$

(iii) $\mathbb{F} = \mathbb{R}$, V $_4(\mathbb{R})$, $T(f(x)) = (x^2\mathfrak{D}^2 + x\mathfrak{D} + 1)f(x)$ for all $f(x) \in V$ and $B = \{1, x, x^2, x^3, x^4\}$.

6 · Similar Matrices

Outline

The square matrix **B** is said to be 'similar' to the square matrix **A** if there exists a non-singular matrix **P** such that $\mathbf{B} = \mathbf{P}^{-1}\mathbf{AP}$. Similarity is an equivalence relation, and this chapter starts a search for a unique simple matrix in each equivalence class. A preliminary discussion supports the hypothesis that this simple matrix might be a diagonal matrix. For a given square matrix **A**, the diagonal matrices **D** such that **D** might be equal to $\mathbf{P}^{-1}\mathbf{AP}$, where **P** is non-singular, are identified. Each diagonal element of such a diagonal matrix **D** is the coefficient d_i, for $i = 1, 2, 3, \ldots, n$, called an 'eigenvalue', such that $\mathbf{Av} = d_i\mathbf{v}$ for some column vector **v**, an 'eigenvector'. Furthermore, the eigenvectors are the columns of the non-singular matrix **P**, if such a matrix exists. A method for finding the eigenvalues of a matrix is given and the calculation of the eigenvectors associated with an eigenvalue is investigated.

Introduction

The importance of the relation between the square matrices **A** and $\mathbf{P}^{-1}\mathbf{AP}$, where **P** is a non-singular matrix, is revealed by Theorem 2 of Chapter 5, which shows that the matrices represent the same linear transformation of this relation with respect to different ordered bases. There are other applications to geometry (one of which we give later), mechanics, algebra and many other subjects which would take too long to explain. In this chapter we investigate the relation between **A** and $\mathbf{P}^{-1}\mathbf{AP}$ by means of matrix calculations without referring to linear transformations. We start by giving the relation a name.

• Definition 1

Let $\mathbb{F}$ be a field, let n be a positive integer and let **A** and **B** be $n \times n$ matrices over $\mathbb{F}$. Then **B** is **similar** to **A** if there exists a non-singular matrix **P** over $\mathbb{F}$ such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{B}$.

The relation between similar matrices is called **similarity**. Although only applicable to square matrices, similarity can be used in the same way as isomorphism of vector spaces because of the following result.

• Proposition 1

Similarity is an equivalence relation on the set of $n \times n$ matrices over a field $\mathbb{F}$.

PROOF

First, every square matrix **A** over a field $\mathbb{F}$ is similar to itself, because $\mathbf{A} = \mathbf{I}^{-1}\mathbf{AI}$. Second, if the square matrix **B** over $\mathbb{F}$ is similar to **A** then **A** is similar to **B** because, by

Definition 1, there exists a non-singular matrix $\mathbf{P}$ over $\mathbb{F}$ such that $\mathbf{B} = \mathbf{P}^{-1}\mathbf{AP}$ and therefore $\mathbf{A} = \mathbf{PBP}^{-1}$. That is, $\mathbf{A} = \mathbf{Q}^{-1}\mathbf{BQ}$ where $\mathbf{Q}$ is the non-singular matrix $\mathbf{P}^{-1}$. Third, if $\mathbf{B}$ is similar to $\mathbf{A}$, and the square matrix $\mathbf{C}$ over $\mathbb{F}$ is similar to $\mathbf{B}$, then $\mathbf{C}$ is similar to $\mathbf{A}$. This holds because, by Definition 1, there exists a non-singular matrix $\mathbf{R}$ over $\mathbb{F}$ such that $\mathbf{C} = \mathbf{R}^{-1}\mathbf{BR}$ and we have $\mathbf{B} = \mathbf{P}^{-1}\mathbf{AP}$. Therefore $\mathbf{C} = \mathbf{R}^{-1}(\mathbf{P}^{-1}\mathbf{AP})\mathbf{R} = (\mathbf{R}^{-1}\mathbf{P}^{-1})\mathbf{A}(\mathbf{PR}) = (\mathbf{PR})^{-1}\mathbf{A}(\mathbf{PR})$. We conclude that similarity satisfies the three conditions required for it to be an equivalence relation. ●

Let $\mathbf{A}$ be any $n \times n$ matrix over a field $\mathbb{F}$. Then the set of matrices $S(\mathbf{A}) = \{\mathbf{P}^{-1}\mathbf{AP} : \det \mathbf{P} \neq 0\}$ is the **similarity class** of $\mathbf{A}$. Because of Proposition 1, a matrix $\mathbf{B}$ is similar to $\mathbf{A}$ if and only if $\mathbf{B} \in S(\mathbf{A})$. Further, if $\mathbf{B} \in S(\mathbf{A})$ then $S(\mathbf{B}) = S(\mathbf{A})$. What is more important in applications, $S(\mathbf{A})$ is the set of all matrices which represent the same linear transformation T of a vector space V of dimension n over $\mathbb{F}$ into itself as $\mathbf{A}$, according to Theorem 2 of Chapter 5. Consequently, it is desirable to find a simple matrix, preferably unique, which belongs to $S(\mathbf{A})$ and can be used to represent T.

To simplify a search for a simple matrix in $S(\mathbf{A})$, let us assume that $\mathbf{A}$ is non-singular. Let us first consider the possibility that a simple matrix can be chosen in $S(\mathbf{A})$ just as for a linear transformation onto a different vector space. In fact, for a linear transformation X of a vector space V of dimension n over $\mathbb{F}$ into a different vector space W of dimension n over $\mathbb{F}$, we can choose bases of V and W such that X is represented by a matrix $\mathbf{N}$ in normal form, by Proposition 4 of Chapter 5. As $\mathbf{N}$ is non-singular and, as in Proposition 4 of Chapter 5, the rank of the identity submatrix $\mathbf{I}$ in $\mathbf{N}$ is rank $\mathbf{N}$, we have $\mathbf{N} = \mathbf{I}$, so the equivalent result to Proposition 4 would be that if $\mathbf{A}$ is non-singular then $\mathbf{I} \in S(\mathbf{A})$. This seems unlikely, so let us ask the following, slightly more general question instead.

QUESTION 1

Let $\mathbf{A}$ be a square matrix over a field $\mathbb{F}$. Is there a non-singular matrix $\mathbf{P}$ over $\mathbb{F}$ such that $\mathbf{P}^{-1}\mathbf{AP} = c\mathbf{N}$, where $c \in \mathbb{F}$ and $\mathbf{N}$ is in normal form, that is, $\mathbf{N} = \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$?

☺ Example 1

Let $\mathbf{A}$ be any non-singular matrix over a field $\mathbb{F}$ such that $\mathbf{A}$ is similar to a matrix $c\mathbf{N}$ where $\mathbf{N}$ is in normal form, as in Question 1. Then, by Definition 1, there exists a non-singular matrix $\mathbf{P}$ such that $c\mathbf{N} = \mathbf{P}^{-1}\mathbf{AP}$. Because the matrices $\mathbf{P}$, $\mathbf{A}$ and $\mathbf{P}^{-1}$ are non-singular, so is $\mathbf{N}$. Also by Proposition 4 of Chapter 5, the rank of the identity submatrix $\mathbf{I}$ in $\mathbf{N}$ is rank $\mathbf{N}$, therefore $\mathbf{N} = \mathbf{I}$. Therefore $\mathbf{P}^{-1}\mathbf{AP} = c\mathbf{I}$ and thence $\mathbf{A} = \mathbf{P}(c\mathbf{I})\mathbf{P}^{-1} = (c\mathbf{I})\mathbf{PP}^{-1} = c\mathbf{I}$. We conclude that a non-singular matrix $\mathbf{A}$ is similar to a scalar multiple of a matrix in normal form if and only if $\mathbf{A}$ is scalar.

A feature of Example 1 is that if $\mathbf{A}$ is a scalar matrix, then $S(\mathbf{A}) = \{\mathbf{P}^{-1}\mathbf{AP} : \det \mathbf{P} \neq 0\} = \{\mathbf{A}\}$. The following tutorial problem shows that there are only two possibilities for the number of matrices in a similarity class.

TUTORIAL PROBLEM 6.1

(i) Let **A** be a 2×2 matrix over $\mathbb{Q}$. By considering $\mathbf{P}^{-1}\mathbf{AP}$ as **P** ranges over some elementary matrices, or otherwise, show that the set of all matrices which are similar to **A** is either infinite or consists of **A** alone.

(ii) Let **A** be an $n \times n$ matrix over $\mathbb{Q}$. By considering 2×2 submatrices of **A** which each contain two diagonal elements of **A**, or otherwise, show that the set of all matrices which are similar to **A** is either infinite or consists of **A** alone.

(iii) Does this result hold for matrices over $\mathbb{R}$?

Example 1 also shows that Question 1 has a negative answer for non-singular matrices, and therefore we need to find a more general form of matrix **K** which might be similar to a given square matrix. The calculations of Example 1 show that it is essential that **K** must not have the property that **KP = PK** for all non-singular matrices **P**. On the other hand, we would like **K** to be as simple as possible, so we first look for the smallest change to a scalar multiple of a matrix in normal form in order that $\mathbf{KP} \neq \mathbf{PK}$ for at least one non-singular matrix **P**. The obvious simplest generalization of such a scalar multiple is a diagonal matrix, so let us try to answer the following question.

QUESTION 2

Is every square matrix **A** over a field $\mathbb{F}$ similar to a diagonal matrix over F?

To start our answer to this question, let us look at the matrix $\mathbf{B} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, which certainly does not resemble a diagonal matrix. However, in Example 2 in Chapter 5 it was shown that **B** represents the same linear transformation as the matrix $\mathbf{C} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ but with respect to a different ordered basis. Therefore, by Theorem 2 of Chapter 5, **B** is similar to the diagonal matrix **C**. We can now follow up this encouraging start by trying to answer Question 2 for a 2×2 matrix **A** which has no special features, apart from having been very carefully selected to make the calculations easy.

○ *Example 2*

Is the matrix $\mathbf{A} = \begin{pmatrix} -16 & 6 \\ -45 & 17 \end{pmatrix}$ over $\mathbb{Q}$ similar to a diagonal matrix over $\mathbb{Q}$? By Definition 1, **A** is similar to a diagonal matrix **D** if and only if there exists a non-singular matrix **P** such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$, and this is equivalent to **AP = PD**. Rather than use the fact that **A** is a 2×2 matrix, let us try to use the fact that the matrix **D** has a distinctive form.

As **D** is diagonal we can write $\mathbf{D} = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$, where $c, d \in \mathbb{Q}$. Multiplying **P** by **D** has the effect of multiplying the first column of **P** by c and the second by d, so let us partition **P** into its columns as $\mathbf{P} = (\mathbf{u} \quad \mathbf{v})$. Then the equation **AP = PD** is equivalent to

$$\mathbf{A}(\mathbf{u} \quad \mathbf{v}) = (\mathbf{u} \quad \mathbf{v})\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = (c\mathbf{u} \quad d\mathbf{v}).$$

Therefore $\mathbf{A}$ is similar to $\mathbf{D}$ if and only if there exists a non-singular matrix $(\mathbf{u} \quad \mathbf{v})$ such that $(\mathbf{Au} \quad \mathbf{Av}) = (c\mathbf{u} \quad d\mathbf{v})$. This is true if and only if there exists a set of vectors $\{\mathbf{u}, \mathbf{v}\}$ which is linearly independent over $\mathbb{Q}$ such that $\mathbf{Au} = c\mathbf{u}$ and $\mathbf{Av} = d\mathbf{v}$. These equations are merely systems of linear equations $(\mathbf{A} - c\mathbf{I})\mathbf{u} = \mathbf{0}$ and $(\mathbf{A} - d\mathbf{I})\mathbf{v} = \mathbf{0}$ except that we do not know the coefficients c and d. In fact, the problem is to find a set of two linearly independent vectors $\mathbf{w}$ which satisfy the equation $(\mathbf{A} - q\mathbf{I})\mathbf{w} = \mathbf{0}$ for suitable values of $q \in \mathbb{Q}$. Consequently, if we write $\mathbf{w} = (x \quad y)^{\mathrm{T}}$, we transform this problem into that of solving the system of equations in x, y and q given by

$$\begin{aligned} (-16 - q)x + \quad & 6y = 0, \\ -45x + (17 - q)y &= 0 \end{aligned}$$

We need a linearly independent set of solution vectors, so we must have non-trivial solutions of these homogeneous equations. By the well-known theorem, the homogeneous linear equations have a non-trivial solution if and only if the determinant of matrix of coefficients is 0. Consequently,

$$\begin{vmatrix} -16 - q & 6 \\ -45 & 17 - q \end{vmatrix} = 0.$$

By evaluating this determinant we obtain the equation $-(16 + q)(17 - q) + 270 = 0$, that is, $q^2 - q - 2 = 0$. The solutions 2 and -1 of this equation supply two values for the unknown coefficient in our system of linear equations, which can then be solved.

For $q = 2$, the linear equations become $-18x + 6y = 0$ and $-45x + 15y = 0$, so this system is equivalent to the single equation $y - 3x = 0$. By choosing $x = 1$, we obtain the vector $\mathbf{u} = (1 \quad 3)^{\mathrm{T}}$ such that $\mathbf{Au} = 2\mathbf{u}$.

For $q = -1$, the linear equations become $-15x + 6y = 0$ and $-45x + 18y = 0$, so this system of equations is equivalent to the single equation $5x - 2y = 0$. By choosing $y = 5$, we obtain the vector $\mathbf{v} = (2 \quad 5)^{\mathrm{T}}$ such that $\mathbf{Av} = -\mathbf{v}$.

Now let $\mathbf{P}$ be the matrix $(\mathbf{u} \quad \mathbf{v})$. The determinant of $\mathbf{P}$ is -1, so $\mathbf{P}$ is a non-singular matrix and, by the first part of these calculations, $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$, where $\mathbf{D} = \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}$.

Therefore we have shown that $\mathbf{A}$ is similar to a diagonal matrix over $\mathbb{Q}$.

Example 2 is consistent with a positive answer to Question 2. Also it suggests a method for obtaining a non-singular matrix $\mathbf{P}$ for a 2×2 matrix $\mathbf{A}$ such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$, where $\mathbf{D}$ is diagonal. Furthermore, the method actually determines the diagonal matrix $\mathbf{D}$. We found the method by considering 2×2 matrices, but it might generalize for an $n \times n$ matrix $\mathbf{A}$ provided the non-singular matrix $\mathbf{P}$ were partitioned into its columns as $\mathbf{P} = (\mathbf{c}_1 \quad \mathbf{c}_2 \quad \mathbf{c}_3 \quad \ldots \quad \mathbf{c}_n)$. The calculations in Example 2 look as if they could be reused to prove that

$$(\mathbf{Ac}_1 \quad \mathbf{Ac}_2 \quad \mathbf{Ac}_3 \quad \ldots \quad \mathbf{Ac}_n) = (d_1\mathbf{c}_1 \quad d_2\mathbf{c}_2 \quad d_3\mathbf{c}_3 \quad \ldots \quad d_n\mathbf{c}_n),$$

where $d_1, d_2, d_3, \ldots, d_n$ are the diagonal elements of $\mathbf{D}$. In fact, this equation will be proved in Theorem 1 of Chapter 7, so it appears that the method can be applied to any

square matrix. In the example (and in the proposed general method), a column $\mathbf{v} \neq \mathbf{0}$ of $\mathbf{P}$ was associated with a corresponding diagonal element q of $\mathbf{D}$ by the equation $\mathbf{Av} = q\mathbf{v}$, so we give a name to this relationship.

• Definition 2

Let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$. A column vector $\mathbf{v} \neq \mathbf{0}$ with n rows is an **eigenvector** of $\mathbf{A}$ if there exists $b \in \mathbb{F}$ such that $\mathbf{Av} = b\mathbf{v}$. Then $\mathbf{v}$ is an eigenvector associated with the **eigenvalue** b of $\mathbf{A}$.

The terms 'eigenvector' and 'eigenvalue' are taken from the German terms *Eigenvektor* and *Eigenwert* and imply that the vector and the number belong to the matrix. They are sometimes replaced by equivalent English terms **characteristic vector** and **characteristic root** of $\mathbf{A}$. There is no unique eigenvector associated with a given eigenvalue b, but the set of eigenvectors associated with b is the set of non-trivial solutions of the equations $\mathbf{Ax} = b\mathbf{x}$. It is better to change these equations by writing $b\mathbf{x} = (b\mathbf{I})\mathbf{x}$ and so converting them into $\mathbf{Ax} - b\mathbf{Ix} = \mathbf{0}$ and thence into the system of homogeneous linear equations $(\mathbf{A} - b\mathbf{I})\mathbf{x} = \mathbf{0}$. In the method of Example 2 we require the matrix of coefficients to have determinant 0, that is, we need $\det(\mathbf{A} - b\mathbf{I}) = 0$. As we treat this as an equation to be solved for b, we replace the scalar b by an indeterminate. This indeterminate is traditionally denoted by λ and this leads to the equation $\det(\mathbf{A} - \lambda\mathbf{I}) = 0$. The matrix $\mathbf{A} - \lambda\mathbf{I}$ has scalar elements in all positions except the main diagonal, where the element in the jth row is of the form $c_{jj} - \lambda$ with $c_{jj} \in \mathbb{F}$. It follows that $\det(\mathbf{A} - \lambda\mathbf{I})$ is a polynomial in λ of degree at most n. Indeed, this polynomial is of degree exactly n because there is exactly one term of degree n, namely $(c_{11} - \lambda)(c_{22} - \lambda) \ldots (c_{nn} - \lambda)$, in the expansion of the determinant by the first row. We now give a name to this polynomial.

• Definition 3

Let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$ and let λ be an indeterminate. The **characteristic polynomial** $\chi(\lambda)$ of $\mathbf{A}$ is the polynomial of degree n in λ defined by $\chi(\lambda) = \det(\mathbf{A} - \lambda\mathbf{I})$ and $\chi(\lambda) = 0$ is the **characteristic equation** of $\mathbf{A}$.

If the characteristic polynomials of several matrices are being considered, the characteristic polynomial of $\mathbf{A}$ is denoted by $\chi_{\mathbf{A}}(\lambda)$. The following theorem shows that the characteristic equation determines the eigenvalues of a matrix $\mathbf{A}$, which were formerly called the 'latent roots'. This is probably why the indeterminate in $\chi(\lambda)$ was originally chosen to be λ (the Greek letter corresponding to 'l'). A Greek letter was probably chosen in order to avoid confusion with the indeterminates which appear in the equations $(\mathbf{A} - \lambda\mathbf{I})\mathbf{x} = \mathbf{0}$.

• Theorem 1

Let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$. Then $b \in \mathbb{F}$ is an eigenvalue of $\mathbf{A}$ if and only if b is a root of the characteristic polynomial of $\mathbf{A}$.

PROOF
The scalar b is an eigenvalue of $\mathbf{A}$ if and only if there is a non-trivial solution $\mathbf{v}$ of the system of linear equations $(\mathbf{A} - b\mathbf{I})\mathbf{x} = \mathbf{0}$, and this holds if and only if the determinant of the matrix of coefficients is 0, that is, $\det(\mathbf{A} - b\mathbf{I}) = 0$. By Definition 3, this is equivalent to $\chi(b) = 0$. Therefore the eigenvalues of $\mathbf{A}$ are exactly the roots in $\mathbb{F}$ of the characteristic polynomial of $\mathbf{A}$. ●

A weak feature of Theorem 1 is that it requires the eigenvalue b to be an element of the field $\mathbb{F}$ in order that the associated eigenvectors should be over $\mathbb{F}$. That this is a serious weakness is shown by the following example.

⊙ Example 3

Let $\mathbf{A}(k) = \begin{pmatrix} 0 & k \\ 1 & 0 \end{pmatrix}$, where $k \in \mathbb{Q}$. Then $\mathbf{A}(k)$ is over $\mathbb{Q}$ and the characteristic polynomial of $\mathbf{A}(k)$ is $\chi(\lambda) = \lambda^2 - k$. The eigenvalues of $\mathbf{A}(k)$ are therefore the roots of $\chi(\lambda)$, that is, $\pm\sqrt{k}$. Whether these roots are in $\mathbb{Q}$ and therefore the eigenvectors are over $\mathbb{Q}$ depends on the value of k. Let us look at three cases.

For $\mathbf{A}(1)$ the eigenvalues are $\pm 1 \in \mathbb{Q}$ so the equations $(\mathbf{A} - \lambda\mathbf{I})\mathbf{x} = \mathbf{0}$ are over $\mathbb{Q}$. Indeed, for $\lambda = 1$ the equations for the eigenvectors are $\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \mathbf{0}$, that is, $-x + y = 0$ and $x - y = 0$. This pair of equations is equivalent to the single equation $x - y = 0$, for which the solution vectors are $(\theta \quad \theta)^{\mathrm{T}}$, where θ is a parameter. By choosing the parameter θ in $\mathbb{Q}$, such as $\theta = 1$, we find the eigenvector $(1 \quad 1)^{\mathrm{T}}$ over $\mathbb{Q}$ associated with the eigenvalue 1. Similarly, for $\lambda = -1$ the equations for the eigenvectors are $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \mathbf{0}$, that is, $x + y = 0$ twice. The solution vectors are therefore $(-\phi \quad \phi)^{\mathrm{T}}$, where ϕ is a parameter. By choosing the parameter ϕ in $\mathbb{Q}$, such as $\phi = -1$, we find the eigenvector $(1 \quad -1)^{\mathrm{T}}$ over $\mathbb{Q}$ associated with the eigenvalue -1. We therefore see that for $k = 1$ the matrix $\mathbf{A}(k)$ has eigenvalues in $\mathbb{Q}$ and the eigenvectors can be chosen to be over $\mathbb{Q}$. In fact, we proved this result by a direct calculation in Example 3 of Chapter 5.

For $\mathbf{A}(2)$ over $\mathbb{Q}$ the eigenvalues are $\pm\sqrt{2}$, which are not in $\mathbb{Q}$, although they are in $\mathbb{R}$. For $\lambda = \sqrt{2}$ the equations for the eigenvectors are $\begin{pmatrix} -\sqrt{2} & 2 \\ 1 & -\sqrt{2} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \mathbf{0}$, that is, $-\sqrt{2}x + 2y = 0$ and $x - \sqrt{2}y = 0$. These are equivalent to the single equation $x - \sqrt{2}y = 0$ over $\mathbb{R}$. The solution vectors are therefore $\left(\sqrt{2}\theta \quad \theta\right)^{\mathrm{T}}$, where θ is a parameter. By choosing θ in $\mathbb{R}$, such as $\theta = \sqrt{2}$, we find the eigenvector $\left(2 \quad \sqrt{2}\right)^{\mathrm{T}}$ over $\mathbb{R}$ associated with the eigenvalue $\sqrt{2}$. Similarly, for the eigenvalue $-\sqrt{2}$ we can find the associated eigenvector $\left(2 \quad -\sqrt{2}\right)^{\mathrm{T}}$ over $\mathbb{R}$ for the matrix $\mathbf{A}(2)$. Consequently,

if we consider $\mathbf{A}(2)$ to be a matrix over $\mathbb{R}$ the eigenvalues of $\mathbf{A}(2)$ are in $\mathbb{R}$ and we can find eigenvectors over $\mathbb{R}$ for $\mathbf{A}(2)$ associated with them.

For $\mathbf{A}(-1)$ over $\mathbb{Q}$ the eigenvalues are $\pm i$, which are in neither $\mathbb{Q}$ nor $\mathbb{R}$, but they are in $\mathbb{C}$. By the methods used for $\mathbf{A}(1)$ and $\mathbf{A}(2)$ we can find the eigenvector $(1 \quad i)^T$ over $\mathbb{C}$ associated with the eigenvalue i of $\mathbf{A}(-1)$ and the eigenvector $(1 \quad -i)^T$ over $\mathbb{C}$ associated with the eigenvalue $-i$ of $\mathbf{A}(-1)$. Therefore we need to consider $\mathbf{A}(-1)$ to be a matrix over $\mathbb{C}$ if we wish to obtain eigenvalues in the same field and eigenvectors associated with them over the same field.

The difficulty that is made clear in Example 3 is that a matrix over a field $\mathbb{F}$ does not necessarily have eigenvalues in $\mathbb{F}$. The only step of the process in Example 3 in which the field is not preserved is the solution of the characteristic equation. However, by the **fundamental theorem of algebra**, any polynomial of degree n over $\mathbb{C}$ has exactly n roots in $\mathbb{C}$ provided that the roots are counted according to their multiplicity. For example, $(x-1)(x-i)^2(x+5)^3$ is of degree 6 with 6 roots: 1, i, i, -5, -5, -5. This theorem is false for both $\mathbb{R}$ and $\mathbb{Q}$. Therefore, one way to ensure that eigenvalues exist in the same field as the matrix, and hence that there are eigenvectors over this field associated with the eigenvalue, would be to assume that all matrices are over $\mathbb{C}$. Some books on linear algebra assume instead that the field $\mathbb{F}$ being used is 'algebraically closed'. This phrase means that $\mathbb{F}$ is a field for which the fundamental theorem of algebra is true, and so implies that $\mathbb{F}$ might be $\mathbb{C}$ but cannot be $\mathbb{R}$ or $\mathbb{Q}$. If an $n \times n$ matrix $\mathbf{A}$ is over $\mathbb{C}$, it has n eigenvalues in $\mathbb{C}$ and therefore its eigenvectors are also over $\mathbb{C}$. However, some theorems in later chapters show that, for the matrices over $\mathbb{R}$ in certain sets, all the eigenvalues are in $\mathbb{R}$ and therefore their eigenvectors can be chosen to be over $\mathbb{R}$. Because of this, we shall use the alternative method of including, when it is needed, an assumption that all the eigenvalues of the matrix $\mathbf{A}$ over $\mathbb{F}$ belong to $\mathbb{F}$. For a matrix $\mathbf{A}$ for which this assumption holds, the eigenvectors belong to a finite-dimensional vector space over $\mathbb{F}$, as we prove in the following theorem. However, Theorem 2 in the next chapter gives a much better upper limit for the dimension of this vector space.

• *Theorem 2*

Let n be a positive integer, let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$ and let $b \in \mathbb{F}$ be an eigenvalue of $\mathbf{A}$. Then the set V_b of eigenvectors of $\mathbf{A}$ associated with b which are over $\mathbb{F}$ together with $\mathbf{0}$ is a vector space over $\mathbb{F}$ and $\dim_{\mathbb{F}} V_b \leq n$.

PROOF

The set V_b is a subset of $\mathbb{F}^n$ because its definition requires the eigenvectors of $\mathbf{A}$ in it to be over $\mathbb{F}$. Therefore, by Definition 2, $V_b = \{ \mathbf{x} \in \mathbb{F}^n, \mathbf{0} : \mathbf{Ax} = b\mathbf{x}, \mathbf{x} \neq \mathbf{0} \}$. Because $\mathbf{A0} = b\mathbf{0}$, the set $V_b = \{ \mathbf{y} \in \mathbb{F}^n : \mathbf{Ay} = b\mathbf{y} \} = \{ \mathbf{y} \in \mathbb{F}^n : (\mathbf{A} - b\mathbf{I})\mathbf{y} = \mathbf{0} \}$. Therefore V_b is the set of solutions of $(\mathbf{A} - b\mathbf{I})\mathbf{y} = \mathbf{0}$ and, by Theorem 2 of Chapter 4, V_b is a vector space of dimension k over $\mathbb{F}$, where $k = n - \text{rank}(\mathbf{A} - b\mathbf{I})$. Because $0 \leq \text{rank}(\mathbf{A} - b\mathbf{I}) \leq n$, we have $k \leq n$. ●

Before we try to answer Question 2, it is sensible to discover what properties are not changed when we replace a matrix by a similar matrix. For example, we might ask

whether the property of being diagonal is preserved. However, in Example 2 we found a matrix **A** which is similar to a diagonal matrix **D** although **A** has an element outside the main diagonal which is not 0. Therefore, by Proposition 1, **D** is similar to the non-diagonal matrix **A**. Consequently, the property of being diagonal is not invariant under similarity, whereas, by Example 1, the property of being a scalar matrix is invariant. So we ask the following.

QUESTION 3

Which properties of a matrix **A** also hold for the similar matrix $\mathbf{P}^{-1}\mathbf{AP}$?

The following proposition describes some of the properties which are invariant under similarity.

• *Proposition 2*

Let n be a positive integer and let **A**, **B** and **P** be $n \times n$ matrices over $\mathbb{F}$ such that **P** is non-singular and $\mathbf{B} = \mathbf{P}^{-1}\mathbf{AP}$. Then:

(i) rank **B** = rank **A**;
(ii) **B** has the same characteristic polynomial as **A**;
(iii) **B** has the same eigenvalues in $\mathbb{F}$ with the same multiplicities as **A**;
(iv) if **u** is an eigenvector over $\mathbb{F}$ of **A** associated with the eigenvalue $c \in \mathbb{F}$, then $\mathbf{P}^{-1}\mathbf{u}$ is an eigenvector over $\mathbb{F}$ of **B** associated with the eigenvalue c;
(v) $\mathbf{B}^k = \mathbf{P}^{-1}\mathbf{A}^k\mathbf{P}$ for all positive integers k;
(vi) if **A** is non-singular, $\mathbf{B}^m = \mathbf{P}^{-1}\mathbf{A}^m\mathbf{P}$ for all $m \in \mathbb{Z}$.

PROOF

(i) By Proposition 5 of Chapter 4, rank **A** = rank T, where T is the linear transformation of $\mathbb{F}^n$ into $\mathbb{F}^n$ defined by $\mathbf{y} = \mathbf{Ax}$. By Theorem 2 of Chapter 5, there is an ordered basis of $\mathbb{F}^n$ such that T is represented by the matrix $\mathbf{B} = \mathbf{P}^{-1}\mathbf{AP}$. This means that T has the equation $\mathbf{y}' = \mathbf{Bx}'$ in this representation and therefore that rank **B** = rank T = rank **A**.

(ii) Because **P** is non-singular, $\det \mathbf{P} \in \mathbb{F}$ is not 0. Also, because the determinant of a product of matrices is the product of the determinants, that $\mathbf{P}^{-1}\mathbf{P} = \mathbf{I}$ implies that $(\det \mathbf{P}^{-1})(\det \mathbf{P}) = \det \mathbf{I} = 1$. Consequently $(\det \mathbf{P})^{-1} = \det \mathbf{P}^{-1}$. Let the characteristic polynomial of **A** be $\chi(\lambda)$. From these two results and Definition 3 we deduce that the characteristic polynomial of $\mathbf{B} = \mathbf{P}^{-1}\mathbf{AP}$ is

$$\begin{aligned}
\det(\mathbf{B} - \lambda\mathbf{I}) &= \det(\mathbf{P}^{-1}\mathbf{AP} - \lambda\mathbf{P}^{-1}\mathbf{IP}) \\
&= \det\left(\mathbf{P}^{-1}(\mathbf{A} - \lambda\mathbf{I})\mathbf{P}\right) \\
&= (\det \mathbf{P}^{-1})\big(\det(\mathbf{A} - \lambda\mathbf{I})\big)\,(\det \mathbf{P}) \\
&= (\det \mathbf{P}^{-1})\chi(\lambda)(\det \mathbf{P}) \\
&= (\det \mathbf{P})^{-1}\chi(\lambda)(\det \mathbf{P}) \\
&= \chi(\lambda).
\end{aligned}$$

(iii) By Theorem 1, $c \in \mathbb{F}$ is an eigenvalue of $\mathbf{A}$ if and only if c is a root of $\chi(\lambda)$. The multiplicity of the eigenvalue c is its multiplicity as a root of $\chi(\lambda)$. By (ii), $\chi(\lambda)$ is also the characteristic polynomial of $\mathbf{B}$, therefore the eigenvalues of $\mathbf{B}$ and their multiplicities are the same as for $\mathbf{A}$.

(iv) By Definition 2, $\mathbf{u}$ is an eigenvector associated with c if and only if $\mathbf{u} \neq \mathbf{0}$ and $\mathbf{Au} = c\mathbf{u}$. Because $\mathbf{P}$ is non-singular, we deduce that $\mathbf{P}^{-1}\mathbf{Au} = c\mathbf{P}^{-1}\mathbf{u}$ and therefore that $\mathbf{P}^{-1}\mathbf{A}(\mathbf{P}\mathbf{P}^{-1})\mathbf{u} = c\mathbf{P}^{-1}\mathbf{u}$. This implies that $(\mathbf{P}^{-1}\mathbf{AP})(\mathbf{P}^{-1}\mathbf{u}) = c(\mathbf{P}^{-1}\mathbf{u})$, which means that $\mathbf{B}(\mathbf{P}^{-1}\mathbf{u}) = c(\mathbf{P}^{-1}\mathbf{u})$. The vector $\mathbf{P}^{-1}\mathbf{u} \neq \mathbf{0}$, because otherwise $\mathbf{u} = \mathbf{0}$ contrary to Definition 2, therefore $\mathbf{P}^{-1}\mathbf{u}$ is an eigenvector of $\mathbf{B}$ associated with the eigenvalue c.

(v) By definition, $\mathbf{B}^{-1} = \mathbf{P}^{-1}\mathbf{A}^1\mathbf{P}$. Let us assume inductively that $\mathbf{B}^k = \mathbf{P}^{-1}\mathbf{A}^k\mathbf{P}$. Then $\mathbf{B}^{k+1} = \mathbf{B}^k\mathbf{B} = (\mathbf{P}^{-1}\mathbf{A}^k\mathbf{P})(\mathbf{P}^{-1}\mathbf{AP}) = \mathbf{P}^{-1}\mathbf{A}^k(\mathbf{P}\mathbf{P}^{-1})\mathbf{AP} = \mathbf{P}^{-1}\mathbf{A}^k\mathbf{IAP} = \mathbf{P}^{-1}\mathbf{A}^{k+1}\mathbf{P}$, therefore (v) holds by the principle of induction.

(vi) Because $\mathbf{A}$ is non-singular, $\det \mathbf{A} \neq 0$ and therefore $\det \mathbf{B} = \det \mathbf{P}^{-1}\mathbf{AP} = (\det \mathbf{P})^{-1}(\det \mathbf{A})(\det \mathbf{P}) \neq 0$, so $\mathbf{B}$ is non-singular. Obviously $\mathbf{B}^0 = \mathbf{I} = \mathbf{P}^{-1}\mathbf{IP} = \mathbf{P}^{-1}\mathbf{A}^0\mathbf{P}$. For $m = -k$, where k is a positive integer, $\mathbf{B}^m = (\mathbf{B}^k)^{-1} = (\mathbf{P}^{-1}\mathbf{A}^k\mathbf{P})^{-1}$ by (v). Therefore $\mathbf{B}^m = \mathbf{P}^{-1}\mathbf{A}^{-k}\mathbf{P}$, by the formula $(\mathbf{XY})^{-1} = \mathbf{Y}^{-1}\mathbf{X}^{-1}$, and therefore $\mathbf{B}^m = \mathbf{P}^{-1}\mathbf{A}^m\mathbf{P}$. ●

Proposition 2(v) provides quick calculations for the powers of a matrix which is similar to a diagonal matrix, as in the following example.

◎ *Example 4*

Let us calculate $\mathbf{A}^7$, where $\mathbf{A} = \begin{pmatrix} -16 & 6 \\ -45 & 17 \end{pmatrix}$ as in Example 2. In Example 2 we found the non-singular matrix $\mathbf{P} = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$ and the diagonal matrix $\mathbf{D} = \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}$ such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$. It follows that $\mathbf{A} = \mathbf{PDP}^{-1}$ and thence, by Proposition 2(v), that $\mathbf{A}^7 = \mathbf{PD}^7\mathbf{P}^{-1}$. Because $\mathbf{D}$ is diagonal, $\mathbf{D}^7$ is the diagonal matrix for which the diagonal elements are the seventh powers of the diagonal elements of $\mathbf{D}$. Therefore $\mathbf{D}^7$ is the diagonal matrix with diagonal elements 128 in the first row and -1 in the second. However, to complete the calculation of $\mathbf{A}^7$ from this formula we also need to find $\mathbf{P}^{-1} = \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}$ by a standard method. Then

$$\mathbf{A}^7 = \mathbf{PD}^7\mathbf{P}^{-1} = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 128 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 128 & -2 \\ 384 & -5 \end{pmatrix}\begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix} = \begin{pmatrix} -646 & 258 \\ -1935 & 773 \end{pmatrix}.$$

This method has obvious advantages, but it has the weakness that $\mathbf{D}$, $\mathbf{P}$ and $\mathbf{P}^{-1}$ need to be calculated first.

The following theorem shows that the diagonal elements of a diagonal matrix $\mathbf{D}$ which is similar to a given matrix $\mathbf{A}$ are determined by the characteristic polynomial of $\mathbf{A}$.

• Theorem 3

Let **A** be a square matrix over $\mathbb{F}$ that is similar to a diagonal matrix **D** over $\mathbb{F}$ and let $\chi(\lambda)$ be the characteristic polynomial of **A**. Then the diagonal elements of **D** are the eigenvalues of **A** with the same multiplicities as in $\chi(\lambda)$.

PROOF

Let the diagonal elements of **D** be $d_1, d_2, d_3, \ldots, d_n$. Then the characteristic polynomial of **D** is the product of the diagonal elements of $\mathbf{D} - \lambda\mathbf{I}$. That is

$$\begin{aligned}\det(\mathbf{D} - \lambda\mathbf{I}) &= (d_1 - \lambda 1)(d_2 - \lambda 1)(d_3 - \lambda 1)\ldots(d_n - \lambda 1)\\ &= (d_1 - \lambda)(d_2 - \lambda)(d_3 - \lambda)\ldots(d_n - \lambda),\end{aligned}$$

Therefore $d_1, d_2, d_3, \ldots, d_n$ are precisely the eigenvalues of **D** and consequently precisely the eigenvalues of **A** by Proposition 2(iii). ●

Theorem 3 asserts that the diagonal elements of the diagonal matrix **D** are uniquely determined but **D** is not necessarily unique because the order of these elements in the main diagonal is not also determined. However, if the eigenvalues of the matrix **A** are all equal to 1 and **A** is similar to the diagonal matrix **D**, then **D** = **I**, by Theorem 2. But Example 1 shows that the only matrix similar to **I** is **I** itself. Therefore a matrix $\mathbf{A} \neq \mathbf{I}$ with all eigenvalues 1 is an example of a square matrix which is not similar to a diagonal matrix. Does such a matrix exist?

◎ Example 5

Let us consider the 2×2 matrix $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and, to make sure that it has two eigenvalues, let us consider **A** as a matrix over $\mathbb{C}$. Let us suppose that **A** is similar to a diagonal matrix, and therefore that there exist a non-singular matrix **P** over $\mathbb{C}$ and a diagonal matrix **D** over $\mathbb{C}$ such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$. Then $\mathbf{A} - \lambda\mathbf{I} = \begin{pmatrix} 1-\lambda & 1 \\ 0 & 1-\lambda \end{pmatrix}$ and therefore the characteristic polynomial of **A** is $\chi(\lambda) = \det(\mathbf{A} - \lambda\mathbf{I}) = (\lambda - 1)^2$. Therefore the eigenvalues of **A** are 1, 1 and, by Theorem 3, **D** = **I**. But **A** is non-singular and therefore is a non-singular matrix which is similar to **I**. Consequently, by Example 1, **A** = **I**, which is obviously false. We conclude that **A** is not similar to a diagonal matrix over $\mathbb{C}$. Because $\mathbb{C}$ contains $\mathbb{R}$ and $\mathbb{Q}$, this means that **A** is also not similar to a diagonal matrix over either $\mathbb{R}$ or $\mathbb{Q}$. A similar calculation can be used to show that if $\mathbf{B} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ and $b \neq 0$ then the only diagonal matrix to which **B** can be similar is $a\mathbf{I}$, and Example 1 then shows that $\mathbf{B} = a\mathbf{I}$, which is false. This shows that there exist square matrices which are not similar to diagonal matrices, although our examples **A** and **B** look as if they ought not be similar to a diagonal matrix. However, this appearance is not shared with the matrix $\mathbf{C} = \begin{pmatrix} 22 & 49 \\ -9 & -20 \end{pmatrix}$. Nevertheless, $\mathbf{C} = \mathbf{P}^{-1}\mathbf{AP}$, where $\mathbf{P} = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$. Therefore if **C** is

similar to a diagonal matrix then so is **A**, by Proposition 1. Because we have shown that **A** is not similar to a diagonal matrix, we deduce that **C** is a less obvious example of a square matrix which is not similar to a diagonal matrix.

That Example 5 shows that Question 2 has a negative answer suggests that we should abandon our attempt to find a diagonal matrix similar to a given matrix. However, Example 2 provided a method of constructing the diagonal matrix (if it exists), Theorem 3 identifies the possible diagonal matrices and Example 4 illustrates the uses of the diagonal matrix. Consequently, instead of trying to answer an unrelated question, we transform Question 2 into the following.

QUESTION 4

Is there a necessary and sufficient condition for a square matrix to be similar to a diagonal matrix?

We shall give a preliminary answer to Question 4 in the next chapter, but this answer gives a criterion that requires a relatively long calculation. In consequence, we shall use this as a step towards a theorem in Chapter 9 which gives an easier criterion for a matrix to be similar to a diagonal matrix. For those matrices which are not similar to diagonal matrices there is a fairly simple form of matrix **J** which is obtained from a matrix **A** and is similar to **A**. The matrix **J** is in fact constructed in such a way that it is a diagonal matrix whenever **A** is similar to a diagonal matrix. However, we shall leave the description and construction of the matrix **J** to more advanced books on linear algebra.

Summary

The square matrix **B** is **similar** to the square matrix **A** if there exists a non-singular matrix **P** such that $\mathbf{B} = \mathbf{P}^{-1}\mathbf{AP}$. Similarity of matrices is an equivalence relation, therefore the set of $n \times n$ matrices over a field is decomposed into a set of disjoint similarity classes. In this chapter we started a search for a simple representative for each similarity class. It was proved that this representative could not be assumed to be a scalar multiple of a matrix in normal form, but an example suggested that we should search for a diagonal matrix similar to the given matrix. This example also suggested how such a diagonal matrix might be found for a matrix **A** using a matrix constructed with eigenvectors of **A**, where an **eigenvector** of **A** is a vector $\mathbf{u} \neq \mathbf{0}$ such that $\mathbf{Au} = b\mathbf{u}$, where the scalar b is an **eigenvalue** of **A**. Further, the eigenvalues of the $n \times n$ matrix **A** are the roots of the **characteristic polynomial** $\chi(\lambda)$ of **A**, where λ is an indeterminate and $\chi(\lambda) = \det(\mathbf{A} - \lambda\mathbf{I})$. Unfortunately, not all the roots of the characteristic polynomial are in the field $\mathbb{F}$ which **A** is over, although the roots always belong to $\mathbb{F}$ if $\mathbb{F} = \mathbb{C}$. It was shown that the eigenvalues and characteristic polynomial of a matrix are the same for similar matrices. This result can be used for a quick calculation of a power of **A** provided that **A** is similar to a diagonal matrix. Furthermore, if **A** is similar to a diagonal matrix **D**, the diagonal elements of **D** are exactly the eigenvalues of **A**. Disappointingly, these results pointed the way to an example that showed that some square matrices with repeated eigenvalues are not similar to diagonal matrices. Consequently, the question

posed for the next chapter is 'What is a necessary and sufficient condition for a square matrix over $\mathbb{F}$ to be similar to a diagonal matrix over $\mathbb{F}$?'

EXERCISES ON CHAPTER 6

1. Let $\mathbf{A}=\begin{pmatrix}2 & 3\\ 0 & 1\end{pmatrix}$, $\mathbf{B}=\begin{pmatrix}0 & 1\\ 2 & 0\end{pmatrix}$ and $\mathbf{D}=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$.

(i) By finding a suitable non-singular matrix, show that **A** is similar to **D**.
(ii) Show that **B** is not similar to **D**.
(iii) Is **A** similar to **B**?

2. Let **A** be a matrix for which $\mathbf{A}^2=\mathbf{A}$ and which is similar to a diagonal matrix **D**. Show that each diagonal element of **D** is either 1 or 0.

3. Find all the eigenvectors of the following matrices:

(i) $\mathbf{A}=\begin{pmatrix}-14 & -10\\ 21 & 15\end{pmatrix}$, (ii) $\mathbf{B}=\begin{pmatrix}-2 & -5\\ 4 & 7\end{pmatrix}$,

(iii) $\mathbf{C}=\begin{pmatrix}11 & 14\\ -7 & -9\end{pmatrix}$, (iv) $\mathbf{D}=\begin{pmatrix}37 & 25\\ -49 & -33\end{pmatrix}$,

(v) $\mathbf{E}=\begin{pmatrix}9 & 10\\ -5 & -5\end{pmatrix}$.

4. Find all the eigenvectors of the following matrices.

(i) $\mathbf{A}=\begin{pmatrix}2 & -2 & 3\\ 1 & 1 & 1\\ 1 & 3 & -1\end{pmatrix}$, (ii) $\mathbf{B}=\begin{pmatrix}1 & 1 & -2\\ 0 & 1 & 0\\ 0 & -1 & 3\end{pmatrix}$,

(iii) $\mathbf{C}=\begin{pmatrix}0 & 1 & 0\\ -1 & 0 & 0\\ 0 & 0 & 3\end{pmatrix}$, (iv) $\mathbf{D}=\begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 0\\ 0 & 0 & 2\end{pmatrix}$.

5. All polynomials in one indeterminate over $\mathbb{R}$ factorize over $\mathbb{R}$ into a product of linear and quadratic factors. Prove that if c is a repeated eigenvalue of a 3×3 matrix **A** over $\mathbb{R}$ then $c\in\mathbb{R}$. Let $\chi(\lambda)$ be the characteristic polynomial of **A**. Prove that if c is a repeated eigenvalue of **A** then c is a root of both $\chi(\lambda)$ and $\mathcal{D}_\lambda\chi(\lambda)$, where $\mathcal{D}_\lambda$ represents differentiation with respect to λ.

6. Use the results of Exercise 5 to determine which of the following matrices have repeated eigenvalues.

(i) $\mathbf{A}=\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ -21 & -11 & 9\end{pmatrix}$, (ii) $\mathbf{B}=\begin{pmatrix}26 & 61 & 4\\ -12 & -28 & 3\\ 0 & 0 & -1\end{pmatrix}$,

(iii) $\mathbf{C} = \begin{pmatrix} 2 & 0 & 1 \\ 6 & 3 & -3 \\ 4 & 0 & -1 \end{pmatrix}$, (iv) $\mathbf{D} = \begin{pmatrix} -2 & 1 & 0 \\ -3 & 1 & 1 \\ 37 & -18 & 7 \end{pmatrix}$,

(v) $\mathbf{E} = \begin{pmatrix} 3 & 2 & 1 \\ 0 & 42 & 185 \\ 0 & -10 & -44 \end{pmatrix}$.

7. Which of the following matrices are similar to the matrix

$$\mathbf{M} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}?$$

(i) $\mathbf{A} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$, (ii) $\mathbf{B} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 \end{pmatrix}$,

(iii) $\mathbf{C} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, (iv) $\mathbf{D} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$,

(v) $\mathbf{E} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$.

8. Find a pair of 2×2 matrices $\mathbf{A}$ and $\mathbf{B}$ over $\mathbb{C}$ which have the following properties:

(i) rank $\mathbf{A}$ = rank $\mathbf{B}$ = 2;
(ii) $\mathbf{A}$ and $\mathbf{B}$ have the same characteristic polynomial;
(iii) $\mathbf{A}$ is not similar to $\mathbf{B}$.

9. Show that the 2×2 matrix $\mathbf{A} = \begin{pmatrix} 0 & 4 \\ -1 & -4 \end{pmatrix}$ is not similar to a diagonal matrix.

7 Diagonalizable Matrices

Outline

The main theorem of this chapter is that an $n \times n$ matrix is similar to a diagonal matrix if and only if there exists a linearly independent set of n eigenvectors of the matrix. A practical deduction from this criterion is that if none of the eigenvalues of a square matrix is a repeated root of its characteristic polynomial then the matrix is similar to a diagonal matrix. For repeated eigenvalues, a bound for the dimension of a vector space of eigenvectors is obtained in terms of the multiplicity of the associated eigenvalue. This leads to an elementary criterion for a matrix to be similar to a diagonal matrix. Examples are given to illustrate the range of possibilities allowed by these results.

Introduction

We start by giving a name to the property which we shall be investigating throughout this chapter.

• Definition 1

A square matrix $\mathbf{A}$ over a field $\mathbb{F}$ is **diagonalizable over** $\mathbb{F}$ if there exist a non-singular matrix $\mathbf{P}$ over $\mathbb{F}$ and a diagonal matrix $\mathbf{D}$ over $\mathbb{F}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$.

Let us now summarize what we learned about diagonalizable matrices in Chapter 6. We discovered that not all square matrices are diagonalizable, so that the main problem is to find a necessary and sufficient condition for a square matrix $\mathbf{A}$ to be diagonalizable (Question 4). If the matrix $\mathbf{A}$ over $\mathbb{F}$ is similar to the diagonal matrix $\mathbf{D}$, then the diagonal elements of $\mathbf{D}$ are the eigenvalues of $\mathbf{A}$ (Theorem 3). However, the eigenvalues of $\mathbf{A}$ need not belong to $\mathbb{F}$ (Example 3), although they certainly belong to $\mathbb{C}$ if $\mathbb{F} = \mathbb{Q}$ or $\mathbb{R}$. We also found that the eigenvalues of $\mathbf{A}$ are the roots of the characteristic polynomial of $\mathbf{A}$ (Theorem 1), which allows the eigenvectors of $\mathbf{A}$ to be calculated (Example 2). We restart this discussion with an example.

◎ Example 1

Let us consider the matrix $\mathbf{A} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 0 \end{pmatrix}$ over $\mathbb{Q}$. First we find the eigenvalues of $\mathbf{A}$ by solving the characteristic equation $\det(\mathbf{A} - \lambda\mathbf{I}) = 0$, according to Theorem 1 of Chapter 6. Because the matrix is upper triangular, in that all elements below the main

diagonal are 0, the determinant is the product of the diagonal elements. Therefore the equation is $(1-\lambda)(2-\lambda)(-\lambda)=0$ and consequently the eigenvalues of $\mathbf{A}$ are 1, 2, 0. In order to study the non-singular matrices $\mathbf{P}$ over $\mathbb{Q}$ such that $\mathbf{P}^{-1}\mathbf{AP}=\mathbf{D}$, we start by finding all the eigenvectors of $\mathbf{A}$. For the eigenvalue λ, the eigenvectors are the solution vectors of the system of linear equations $(\mathbf{A}-\lambda\mathbf{I})\mathbf{v}=\mathbf{0}$, that is, for $\mathbf{v}=(x \quad y \quad z)^{\mathrm{T}}$,

$$\begin{pmatrix} 1-\lambda & -1 & 0 \\ 0 & 2-\lambda & 2 \\ 0 & 0 & -\lambda \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

When written in equation form this becomes

$$(1-\lambda)x-y=0, \qquad (2-\lambda)y+2z=0, \qquad -\lambda z=0.$$

For $\lambda=1$ the equations become $y=0$, $y+2z=0$ and $-z=0$, which are equivalent to $y=z=0$. The solutions of these equations are $x=\theta$, $y=z=0$, where θ is a non-zero parameter over $\mathbb{Q}$.

For $\lambda=2$ the equations become $x+y=0$, $2z=0$, $2z=0$, for which the solutions are $x=-\phi$, $y=\phi$, $z=0$, where ϕ is a non-zero parameter over $\mathbb{Q}$.

For $\lambda=0$, the equations become $x-y=0$, $y+z=0$, $0=0$, for which the solutions are $x=y=-\psi$, $z=\psi$, where ψ is a nonzero parameter over $\mathbb{Q}$.

According to the calculations of Example 2 in Chapter 6, we form matrices $\mathbf{P}$ with the eigenvectors associated with 1, 2, 0 as the columns. For the parameters $\theta, \phi, \psi \in \mathbb{C}$, these matrices are $\mathbf{P}=\begin{pmatrix} \theta & -\phi & -\psi \\ 0 & \phi & -\psi \\ 0 & 0 & \psi \end{pmatrix}$. Can $\theta, \phi, \psi \in \mathbb{C}$ be chosen so that $\mathbf{P}$ is non-singular? To test this, let $a, b, c \in \mathbb{C}$ and

$$a\begin{pmatrix} \theta \\ 0 \\ 0 \end{pmatrix}+b\begin{pmatrix} -\phi \\ \phi \\ 0 \end{pmatrix}+c\begin{pmatrix} -\psi \\ -\psi \\ \psi \end{pmatrix}=0.$$

Then

$$(a\theta)\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}+(b\phi)\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}+(c\psi)\begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix}=0,$$

which is an equation in which the indeterminate parameters can be absorbed by the coefficients a, b, c. This implies that the choice of parameters has no effect whatever provided none are 0, consequently they can all be given convenient non-zero values, such as 1. Here we let $\theta=\phi=\psi=1$ and obtain

$$\begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix}+\begin{pmatrix} -b \\ b \\ 0 \end{pmatrix}+\begin{pmatrix} -c \\ -c \\ c \end{pmatrix}=\mathbf{0},$$

that is,

$$a-b-c=0, \qquad b-c=0, \qquad c=0.$$

Solving these equations by back substitution, we obtain $a = b = c = 0$. Therefore the columns of the chosen matrix $\mathbf{P} = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$ are linearly independent and consequently $\mathbf{P}$ is non-singular. The usual calculation for the inverse of a matrix gives us $\mathbf{P}^{-1} = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Therefore

$$\mathbf{P}^{-1}\mathbf{AP} = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

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

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

Therefore $\mathbf{P}$ is one of the matrices over $\mathbb{Q}$ such that $\mathbf{P}^{-1}\mathbf{AP}$ is the diagonal matrix $\mathbf{D}$. Because $\mathbf{P}$ is over $\mathbb{Q}$, so is $\mathbf{P}^{-1}$ and therefore, as $\mathbf{A}$ is over $\mathbb{Q}$, the diagonal matrix $\mathbf{D} = \mathbf{P}^{-1}\mathbf{AP}$ is also over $\mathbb{Q}$. Of course, by Theorem 3 of Chapter 6, the diagonal elements of $\mathbf{D}$ are the eigenvalues of $\mathbf{A}$.

The diagonalizable matrix $\mathbf{A}$ in Example 1 has the special property that it is a 3×3 matrix with three distinct eigenvalues. We shall explore the significance of this later, but we first study a different property of $\mathbf{A}$. In common with the 2×2 matrix in Example 2 of Chapter 6, $\mathbf{A}$ is an $n \times n$ matrix with a set of n linearly independent eigenvectors, and these eigenvectors form the columns of the non-singular matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{AP}$ is diagonal. This construction holds for all square matrices, as is proved in the following theorem which provides a necessary and sufficient condition for a square matrix to be diagonalizable. The criterion is mainly of theoretical interest, but the theorem also establishes the construction for the non-singular matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{AP}$ is a diagonal matrix.

• *Theorem 1*

Let n be a positive integer and let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$. Then there exists a non-singular $n \times n$ matrix $\mathbf{P}$ over $\mathbb{F}$ such that $\mathbf{P}^{-1}\mathbf{AP}$ is diagonal if and only if the columns of $\mathbf{P}$ form a set of eigenvectors of $\mathbf{A}$ over $\mathbb{F}$ which is linearly independent over $\mathbb{F}$.

PROOF

If there exist a non-singular matrix $\mathbf{P}$ over $\mathbb{F}$ and a diagonal matrix $\mathbf{D}$ over $\mathbb{F}$ such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$, then, by Theorem 3 of Chapter 6, the diagonal elements of $\mathbf{D}$ are the eigenvalues of $\mathbf{A}$. Consequently, we shall discuss whether $\mathbf{A}$ is similar to a particular one of

the diagonal matrices with the eigenvalues of **A** as diagonal elements, that is, $\mathbf{D} = (\lambda_j \delta_{jk})$ where $\delta_{jk} = 0$ if $j \neq k$, $\delta_{jk} = 1$ if $j = k$ and $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n$ are the eigenvalues of **A** with the repeated eigenvalues occurring with their correct multiplicities. (The other possible diagonal matrices have the same diagonal elements in a different order.) Then there exists a non-singular matrix $\mathbf{P} = (p_{ij})$ over $\mathbb{F}$ such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$ if and only if there exists a non-singular matrix **P** with columns $\mathbf{c}_j$, for $j = 1, 2, 3, \ldots, n$, over $\mathbb{F}$ such that

$$\mathbf{A}(\mathbf{c}_1 \ \mathbf{c}_2 \ \mathbf{c}_3 \ \ldots \ \mathbf{c}_n) = (\mathbf{c}_1 \ \mathbf{c}_2 \ \mathbf{c}_3 \ \ldots \ \mathbf{c}_n)\mathbf{D}.$$

This holds if and only if there are linearly independent column vectors $\mathbf{c}_j = (p_{1j} \ p_{2j} \ p_{3j} \ \ldots \ p_{nj})^{\mathrm{T}}$ over $\mathbb{F}$ such that

$$(\mathbf{Ac}_1 \ \mathbf{Ac}_2 \ \mathbf{Ac}_3 \ \ldots \ \mathbf{Ac}_n) = (\mathbf{c}_1 \ \mathbf{c}_2 \ \mathbf{c}_3 \ \ldots \ \mathbf{c}_n)\mathbf{D}.$$

This equation holds if and only if there are linearly independent column vectors $\mathbf{c}_j$ over $\mathbb{F}$, for $j = 1, 2, 3, \ldots, n$, such that

$$\begin{aligned}(\mathbf{Ac}_1 \ \mathbf{Ac}_2 \ \mathbf{Ac}_3 \ \ldots \ \mathbf{Ac}_n) &= (p_{ij})(\lambda_j \delta_{jk}) \\ &= \left(\sum_{j=1}^{n} p_{ij} \lambda_j \delta_{jk} \right) \\ &= (p_{ik} \lambda_k) \qquad \text{as } \delta_{jk} = 0 \text{ or } 1 \\ &= (\lambda_1 \mathbf{c}_1 \ \lambda_2 \mathbf{c}_2 \ \lambda_3 \mathbf{c}_3 \ \ldots \ \lambda_n \mathbf{c}_n).\end{aligned}$$

This holds if and only if $\mathbf{Ac}_j = \lambda_j \mathbf{c}_j$ for $j = 1, 2, 3, \ldots, n$, and $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \ldots, \mathbf{c}_n$ are linearly independent over $\mathbb{F}$. By Definition 2 of Chapter 6, this is equivalent to the existence of a set of eigenvectors of **A**, one for each eigenvalue λ_j, for $j = 1, 2, 3, \ldots, n$, which is linearly independent over $\mathbb{F}$. ●

This necessary and sufficient condition for a matrix to be diagonalizable has the disadvantage that using it requires an almost complete calculation of the required non-singular matrix. However, it is also a good basis for attempts to answer the following question.

QUESTION 1

Are there any easily used sets of conditions for a square matrix **A** to be diagonalizable?

As Theorem 1 tells us, to answer Question 1 we should look for a set of conditions for the existence of a full linearly independent set of eigenvectors of **A**. Example 1 suggests that this might hold and **A** be diagonalizable provided that the eigenvalues of **A** are distinct. This suggestion is supported by Example 5 of Chapter 6, in which a non-diagonalizable matrix has repeated eigenvalues. We shall return to that conjecture later in the chapter, but first we shall explore the influence of the **multiplicity** of an eigenvalue, that is, the number of times it occurs as a root of the characteristic polynomial. For any eigenvalue of a square matrix, the following theorem gives an upper bound for

the dimension of the vector space of eigenvectors in terms of the multiplicity of the eigenvalue. From this we can deduce an upper bound for the dimension of a vector space spanned by all the eigenvectors of the matrix.

• *Theorem 2* The eigenvalue multiplicity theorem

Let $f \in \mathbb{F}$ be an eigenvalue of multiplicity m of the $n \times n$ matrix $\mathbf{A}$ over a field $\mathbb{F}$. Then the vector space spanned by the eigenvectors of $\mathbf{A}$ associated with f is of dimension $n - \text{rank}(\mathbf{A} - f\mathbf{I})$, where

$$n - \text{rank}(\mathbf{A} - f\mathbf{I}) \leq m.$$

PROOF

For the eigenvalue f, the eigenvectors are the solutions of the system of equations $(\mathbf{A} - f\mathbf{I})\mathbf{x} = \mathbf{0}$. Therefore the dimension s of the vector space of eigenvectors over $\mathbb{F}$ is $s = n - \text{rank}(\mathbf{A} - f\mathbf{I})$, by Theorem 2 of Chapter 4. In all cases $s > 0$ because $\det(\mathbf{A} - f\mathbf{I}) = 0$ by Theorem 1 of Chapter 6 and therefore $\text{rank}(\mathbf{A} - f\mathbf{I}) < n$. If $s = n$ then $\text{rank}(\mathbf{A} - f\mathbf{I}) = 0$, therefore $\mathbf{A} = f\mathbf{I}$, $m = n$ and $s \leq m$ in this case.

Therefore we can assume that $0 < s < n$. Because s is the dimension of the vector space V of solutions of $(\mathbf{A} - f\mathbf{I})\mathbf{x} = \mathbf{0}$, V has a basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_s\}$. By Proposition 5 of Chapter 3, there exist $\mathbf{b}_{s+1}, \mathbf{b}_{s+2}, \ldots, \mathbf{b}_n$ such that $B = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_s, \mathbf{b}_{s+1}, \ldots, \mathbf{b}_n\}$ is a basis of $\mathbb{F}^n$. Let $\mathbf{B}$ be the $n \times n$ matrix over $\mathbb{F}$ of which the columns are the vectors in the basis B. That is,

$$\mathbf{B} = (\mathbf{b}_1 \quad \mathbf{b}_2 \quad \ldots \quad \mathbf{b}_s \quad \mathbf{b}_{s+1} \quad \ldots \quad \mathbf{b}_n).$$

Then, because $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_s\}$ is a basis of V, $(\mathbf{A} - f\mathbf{I})\mathbf{b}_j = \mathbf{0}$, for $j = 1, 2, \ldots, s$. Let us write $\mathbf{c}_j = (\mathbf{A} - f\mathbf{I})\mathbf{b}_j$, for $j = s + 1, s + 2, \ldots, n$. Then we obtain

$$\begin{aligned}(\mathbf{A} - f\mathbf{I})\mathbf{B} &= \big((\mathbf{A} - f\mathbf{I})\mathbf{b}_1 \quad \ldots \quad (\mathbf{A} - f\mathbf{I})\mathbf{b}_s \quad \ldots \quad (\mathbf{A} - f\mathbf{I})\mathbf{b}_n\big) \\ &= (\mathbf{0} \quad \mathbf{0} \quad \ldots \quad \mathbf{0} \quad \mathbf{c}_{s+1} \quad \mathbf{c}_{s+2} \quad \ldots \quad \mathbf{c}_n).\end{aligned}$$

Because B is a basis of $\mathbb{F}^n$, $\mathbf{B}$ is a non-singular matrix and therefore

$$\begin{aligned}\mathbf{C} = \mathbf{B}^{-1}(\mathbf{A} - f\mathbf{I})\mathbf{B} &= \mathbf{B}^{-1}(\mathbf{0} \quad \mathbf{0} \quad \ldots \quad \mathbf{0} \quad \mathbf{c}_{s+1} \quad \mathbf{c}_{s+2} \quad \ldots \quad \mathbf{c}_n) \\ &= (\mathbf{0} \quad \ldots \quad \mathbf{0} \quad \mathbf{B}^{-1}\mathbf{c}_{s+1} \quad \ldots \quad \mathbf{B}^{-1}\mathbf{c}_n).\end{aligned}$$

We deduce that the first s columns of the matrix $\mathbf{C}$ are zero. The characteristic polynomial of $\mathbf{C}$ is given by $\chi(\lambda) = \det(\mathbf{C} - \lambda\mathbf{I})$ where the first s columns of the determinant are $(-\lambda \ 0 \ \ldots \ 0)^{\mathrm{T}}$, $(0 \ -\lambda \ \ldots \ 0)^{\mathrm{T}}$, $\ldots$, $(0 \ 0 \ \ldots \ -\lambda \ 0 \ \ldots \ 0)^{\mathrm{T}}$. If we evaluate $\det(\mathbf{C} - \lambda\mathbf{I})$ by expanding the determinants by the first column we obtain $\chi(\lambda) = (-\lambda)^s\phi(\lambda)$, where $\phi(\lambda)$ is a polynomial in λ. The matrix $\mathbf{C}$ is similar to $\mathbf{A} - f\mathbf{I}$ and therefore, by Proposition 2(ii) of Chapter 6, the characteristic polynomial of $\mathbf{A} - f\mathbf{I}$ is also $\chi(\lambda)$. This shows that $\det(\mathbf{A} - f\mathbf{I} - \lambda\mathbf{I}) = (-\lambda)^s\phi(\lambda)$. Let us change this equation by replacing λ by $\lambda = x - f$. Then $\det(\mathbf{A} - f\mathbf{I} - \lambda\mathbf{I}) = \det(\mathbf{A} - x\mathbf{I})$ and therefore the characteristic polynomial of $\mathbf{A}$ is $\det(\mathbf{A} - x\mathbf{I}) = (f - x)^s\psi(x)$, where $\psi(x)$ is a polynomial in x. We conclude that the eigenvalue f of $\mathbf{A}$ has multiplicity at least s and therefore $s \leq m$. ●

○ Example 2

For $b, c \in \mathbb{Q}$, let the matrix $\mathbf{A}(b, c)$ over $\mathbb{Q}$ be $\mathbf{A}(b,c) = \begin{pmatrix} 2 & b & 0 \\ 0 & 2 & c \\ 0 & 0 & 2 \end{pmatrix}$. Then, by expanding the determinants successively by the first column, $\det(\mathbf{A}(b, c) - \lambda\mathbf{I}) = (2 - \lambda)^3$, therefore $\mathbf{A}(b, c)$ has eigenvalue 2 with multiplicity 3. In this case the eigenvalue multiplicity theorem tells us only that the vector space $V(b, c)$ of eigenvectors is of dimension not exceeding 3. But this is not sensational news, because $V(b, c)$ is a subspace of $\mathbb{F}^3$ and therefore the dimension of $V(b, c)$ cannot exceed 3 by Theorem 4 of Chapter 3! So what is the dimension d of $V(b, c)$?

From the proof of Theorem 2 of Chapter 6, $V(b, c)$ is the vector space of solutions of $(\mathbf{A}(b, c) - 2\mathbf{I})\mathbf{x} = \mathbf{0}$. Therefore, by Theorem 2 of Chapter 4, the dimension $d = \dim_{\mathbb{F}} V(b, c)$ is given by $d = 3 - \text{rank}(\mathbf{A}(b, c) - 2\mathbf{I})$, which we can evaluate case by case.

If $b = c = 0$ then $\mathbf{A}(0, 0) = 2\mathbf{I}$ therefore $\mathbf{A}(0, 0) - 2\mathbf{I} = \mathbf{0}$, which is of rank 0. Therefore $d = 3$ in this case.

If $b \neq 0$ but $c = 0$ then $\mathbf{A}(b,0) - 2\mathbf{I} = \begin{pmatrix} 0 & b & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, which is of rank 1. Therefore $d = 2$ in this case, and the same holds when $b = 0$ but $c \neq 0$.

Finally, if $b \neq 0$ and $c \neq 0$ then $\mathbf{A}(b,c) - 2\mathbf{I} = \begin{pmatrix} 0 & b & 0 \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}$, which is of rank 2. Therefore $d = 1$ in this case, and we conclude that the dimension of the vector space of eigenvectors of $\mathbf{A}(b, c)$ can vary from 1 to 3 according to the values of b and c.

The eigenvalue multiplicity theorem gives an upper bound for the dimension of the vector space of eigenvectors associated with a given eigenvalue in all cases. However, if the eigenvalue has multiplicity 1, then Theorem 2 actually determines the dimension of the vector space of eigenvectors, as the following result shows.

• Proposition 1

Let $f \in \mathbb{F}$ be an unrepeated eigenvalue of the $n \times n$ matrix $\mathbf{A}$ over the field $\mathbb{F}$. Then the vector space of eigenvectors of $\mathbf{A}$ associated with f is of dimension 1 over $\mathbb{F}$.

PROOF

By Definition 2 of Chapter 6, that f is an eigenvalue implies that $\mathbf{A}$ has an eigenvector $\mathbf{v} \neq \mathbf{0}$, therefore the dimension d of the vector space of eigenvectors of $\mathbf{A}$ associated with f is at least 1. By Theorem 2 we have $d \leq 1$, therefore $d = 1$. •

Theorem 1 suggests that a square matrix is diagonalizable if the vector space of solutions of the systems of equations for the eigenvectors has sufficient rank. The eigenvalue multiplicity theorem shows that the vector space of eigenvectors associated with an eigenvalue has bounded dimension. Combining these two results suggests the following result.

• Theorem 3

Let $\mathbf{A}$ be an $n \times n$ matrix over the field $\mathbb{F}$. Then $\mathbf{A}$ is diagonalizable over $\mathbb{F}$ if and only if all the eigenvalues of $\mathbf{A}$ belong to $\mathbb{F}$ and, for each eigenvalue λ of $\mathbf{A}$, the dimension of the vector space of eigenvectors of $\mathbf{A}$ associated with λ is equal to the multiplicity of λ as a root of the characteristic polynomial.

PROOF

Suppose that $\mathbf{A}$ is diagonalizable over $\mathbb{F}$. Then there exist a non-singular matrix $\mathbf{P}$ over $\mathbb{F}$ and a diagonal matrix $\mathbf{D}$ over $\mathbb{F}$ such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$. It follows that the diagonal elements of $\mathbf{D}$, which are the eigenvalues of $\mathbf{A}$ by Theorem 3 of Chapter 6, belong to $\mathbb{F}$. Let the eigenvalue λ of $\mathbf{A}$ have multiplicity k. Then exactly k of the diagonal elements of $\mathbf{D}$ are equal to λ, therefore $\mathbf{D} - \lambda\mathbf{I}$ has k zero rows and the other rows are non-zero multiples of rows of $\mathbf{I}$. Consequently, $\text{rank}(\mathbf{D} - \lambda\mathbf{I}) = \text{rank}(\mathbf{P}^{-1}\mathbf{AP} - \lambda\mathbf{I}) = n - k$. Because $\mathbf{P}$ and $\mathbf{P}^{-1}$ are non-singular and multiplying by a non-singular matrix does not change the rank of a matrix, $\text{rank}(\mathbf{A} - \lambda\mathbf{I}) = \text{rank}\ \mathbf{P}^{-1}(\mathbf{A} - \lambda\mathbf{I})\mathbf{P} = n - k$. It follows from Theorem 2 of Chapter 4 that the vector space of solutions of the system of linear equations $(\mathbf{A} - \lambda\mathbf{I})\mathbf{x} = \mathbf{0}$ has dimension k over $\mathbb{F}$, as required.

Conversely, suppose that all the eigenvalues of $\mathbf{A}$ belong to $\mathbb{F}$ and, for each eigenvalue λ of $\mathbf{A}$, the dimension of the vector space of eigenvectors of $\mathbf{A}$ associated with λ is the multiplicity of λ as a root of the characteristic polynomial of $\mathbf{A}$. Let $\rho_1, \rho_2, \rho_3, \ldots, \rho_k$ be all the distinct eigenvalues of $\mathbf{A}$, and let the vector space V_j of eigenvectors of $\mathbf{A}$ associated with ρ_j (together with $\mathbf{0}$) have basis B_j, for $j = 1, 2, 3, \ldots, k$. Let $B = \bigcup_{j=1}^{k} B_j$. By hypothesis, the dimension of V_j is the multiplicity of ρ_j, therefore the number of vectors in B is the sum s of the multiplicities of ρ_j, for $j = 1, 2, 3, \ldots, k$. But s is the number of roots of the characteristic polynomial of $\mathbf{A}$, which all belong to $\mathbb{F}$ by hypothesis. Because $\mathbf{A}$ is an $n \times n$ matrix, its characteristic polynomial is of degree n, therefore $s = n$. Consequently, B is a set of n eigenvectors of $\mathbf{A}$. In order to use Theorem 1, we now need to show that B is linearly independent over $\mathbb{F}$. Therefore we consider any zero linear combination $\mathbf{w} = \mathbf{0}$ of the vectors in B. To simplify the notation for later calculations, let us choose an arbitrary value p of $j = 1, 2, 3, \ldots, k$ and concentrate our attention on the part of the sum $\mathbf{w}$ which contains the elements of B_p. We may write $B_p = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_m\}$, where m is the multiplicity of ρ_p. Then $\mathbf{w} = \ldots + c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + c_3\mathbf{b}_3 + c_m\mathbf{b}_m + \ldots$, where $c_j \in \mathbb{F}$ for $j = 1, 2, 3, \ldots, m$. However, $\mathbf{v}_p = c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + c_3\mathbf{b}_3 + c_m\mathbf{b}_m \in V_p$ and is an eigenvector of $\mathbf{A}$ associated with ρ_p unless $\mathbf{v}_p = \mathbf{0}$. Therefore $\mathbf{w} = \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 + \ldots + \mathbf{v}_k = \mathbf{0}$, where $\mathbf{v}_j \in V_j$ is defined in terms of B_j in the same way as $\mathbf{v}_p$. In order to use the fact that $\mathbf{v}_j$ is either $\mathbf{0}$ or an eigenvector of $\mathbf{A}$ associated with ρ_j, we consider $(\rho_q\mathbf{I} - \mathbf{A})\mathbf{v}_j$, for $j, q = 1, 2, 3, \ldots, k$. Then $(\rho_q\mathbf{I} - \mathbf{A})\mathbf{v}_j = \rho_q\mathbf{v}_j - \mathbf{A}\mathbf{v}_j = \rho_q\mathbf{v}_j - \rho_j\mathbf{v}_j = (\rho_q - \rho_j)\mathbf{v}_j$. In this expression the multiplier $\rho_q - \rho_j \neq 0$ unless $j = q$ because $\rho_1, \rho_2, \rho_3, \ldots, \rho_k$ are distinct. Let $\mathbf{R}$ be the product of all the matrices $\rho_q\mathbf{I} - \mathbf{A}$ for $q \neq p$, that is, for $q = 1, 2, \ldots, p-1, p+1, \ldots, k$. Then, for $j = 1, 2, 3, \ldots, k$,

$$\begin{aligned}\mathbf{R}\mathbf{v}_j &= (\rho_1\mathbf{I}-\mathbf{A})(\rho_2\mathbf{I}-\mathbf{A})\ldots(\rho_{p-1}\mathbf{I}-\mathbf{A})(\rho_{p+1}\mathbf{I}-\mathbf{A})\ldots(\rho_k\mathbf{I}-\mathbf{A})\mathbf{v}_j \\ &= (\rho_1\mathbf{I}-\mathbf{A})\ldots(\rho_{p-1}\mathbf{I}-\mathbf{A})(\rho_{p+1}\mathbf{I}-\mathbf{A})\ldots(\rho_{k-1}\mathbf{I}-\mathbf{A})\mathbf{v}_j(\rho_k-\rho_j) \\ &= (\rho_1\mathbf{I}-\mathbf{A})\ldots(\rho_{p-1}\mathbf{I}-\mathbf{A})(\rho_{p+1}\mathbf{I}-\mathbf{A})\ldots(\rho_{k-2}\mathbf{I}-\mathbf{A})\mathbf{v}_j(\rho_{k-1}-\rho_j)(\rho_k-\rho_j) \\ &= \mathbf{v}_j(\rho_1-\rho_j)(\rho_2-\rho_j)\ldots(\rho_{p-1}-\rho_j)(\rho_{p+1}-\rho_j)\ldots(\rho_k-\rho_j\end{aligned}$$

and we write this as $\mathbf{R}\mathbf{v}_j = r_j\mathbf{v}_j$. For $j \neq p$ the coefficient r_j has the factor $\rho_j - \rho_j$ therefore $r_j = 0$, but for $j = p$ the coefficient $r_p \neq 0$. Therefore $\mathbf{R}\mathbf{w} = \mathbf{R}\mathbf{v}_1 + \ldots + \mathbf{R}\mathbf{v}_p + \ldots + \mathbf{R}\mathbf{v}_k = r_p\mathbf{v}_p$ and, because $\mathbf{R}\mathbf{w} = \mathbf{0}$ and $r_p \neq 0$, we deduce that $\mathbf{v}_p = \mathbf{0}$. But $\mathbf{v}_p = c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + c_3\mathbf{b}_3 + c_m\mathbf{b}_m$ and the basis B_p of V_p is linearly independent over $\mathbb{F}$, therefore $c_1 = c_2 = c_3 = \ldots = c_m = 0$. Consequently, all the coefficients related to the eigenvalue ρ_p of $\mathbf{A}$ are 0. However, ρ_p is an arbitrary eigenvalue of $\mathbf{A}$, therefore all the coefficients of the elements of B in $\mathbf{w}$ are 0. Therefore B is a linearly independent set of n eigenvectors over $\mathbb{F}$ of $\mathbf{A}$, and consequently $\mathbf{A}$ is diagonalizable over $\mathbb{F}$ by Theorem 1. ●

Theorem 3 shares the disadvantage of Theorem 1 that to apply it most of the calculation to find the matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}$ is diagonal must be completed. However, Theorem 3 does reduce the amount of work by removing the need to check that the columns of $\mathbf{P}$ are linearly independent. It also helps to prove the following theorem, which gives an easy condition which implies that a matrix is diagonalizable.

• Theorem 4

Let $\mathbf{A}$ be an $n \times n$ matrix over $\mathbb{F}$ with n distinct eigenvalues over $\mathbb{F}$. Then $\mathbf{A}$ is diagonalizable over $\mathbb{F}$.

PROOF

Let d be an eigenvalue of $\mathbf{A}$. Then, by hypothesis, $d \in \mathbb{F}$ and d has multiplicity 1 as an eigenvalue of $\mathbf{A}$. Therefore, by Proposition 1, the vector space of eigenvectors associated with d (together with $\mathbf{0}$) has dimension 1 over $\mathbb{F}$. Because this holds for every eigenvalue of $\mathbf{A}$, the matrix $\mathbf{A}$ satisfies the conditions of Theorem 3. We conclude that $\mathbf{A}$ is diagonalizable over $\mathbb{F}$. ●

It is not always true that a matrix over $\mathbb{F}$ with distinct eigenvalues is diagonalizable over $\mathbb{F}$ because the eigenvalues of $\mathbf{A}$ may not belong to $\mathbb{F}$. Example 3 of Chapter 6 contains a matrix of this kind. What we have shown is that all square matrices over $\mathbb{C}$ are diagonalizable over $\mathbb{C}$ except for some of those with multiple eigenvalues. The following three examples demonstrate some of the possibilities concerning the diagonalization of 3×3 matrices.

○ Example 3

Is the matrix $\mathbf{A} = \begin{pmatrix} 5 & 0 & 13 \\ 1 & 3 & 4 \\ -2 & 0 & -5 \end{pmatrix}$ diagonalizable?

The characteristic polynomial of $\mathbf{A}$ is $\chi(\lambda) = \det(\mathbf{A} - \lambda\mathbf{I})$, and therefore, on evaluating the determinant by the second column,

$$\chi(\lambda)=\begin{vmatrix}5-\lambda & 0 & 13\\ 1 & 3-\lambda & 4\\ -2 & 0 & -5-\lambda\end{vmatrix}=(3-\lambda)\begin{vmatrix}5-\lambda & 13\\ -2 & -5-\lambda\end{vmatrix}$$
$$=(3-\lambda)(\lambda^2+1)=(3-\lambda)(\lambda-\mathrm{i})(\lambda+\mathrm{i}).$$

Therefore the eigenvalues of **A** are 3, i and –i and therefore **A** is diagonalizable over $\mathbb{C}$ by Theorem 4. However, **A** is not diagonalizable over $\mathbb{Q}$ by Theorem 3.

TUTORIAL PROBLEM 7.1

Find a diagonal matrix **D** over $\mathbb{C}$ and a non-singular matrix **P** over $\mathbb{C}$ such that $\mathbf{P}^{-1}\mathbf{AP}=\mathbf{D}$, where **A** is the matrix in Example 3.

○ *Example 4*

Is the matrix $\mathbf{A}=\begin{pmatrix}-3 & 2 & 2\\ -12 & 7 & 6\\ 0 & 0 & 1\end{pmatrix}$ diagonalizable over $\mathbb{Q}$?

The characteristic polynomial of **A** is $\chi(\lambda)=\det(\mathbf{A}-\lambda\mathbf{I})$, and therefore, on evaluating the determinant by the last row,

$$\chi(\lambda)=\begin{vmatrix}-3-\lambda & 2 & 2\\ -12 & 7-\lambda & 6\\ 0 & 0 & 1-\lambda\end{vmatrix}=(1-\lambda)\begin{vmatrix}-3-\lambda & 2\\ -12 & 7-\lambda\end{vmatrix}$$
$$=(1-\lambda)\left[(\lambda+3)(\lambda-7)+24\right]$$
$$=(1-\lambda)(\lambda^2-4\lambda+3)$$
$$=(1-\lambda)(\lambda-1)(\lambda-3).$$

Therefore the eigenvalues of **A** are 1, 1 and 3, and therefore **A** has a double eigenvalue. Consequently, we need to use Theorem 3 in order to find out whether **A** is diagonalizable over $\mathbb{Q}$. As it follows from Proposition 1 that **A** has a vector space of eigenvectors associated with the single eigenvalue 3 of dimension 1, it is sensible to start by finding the eigenvectors associated with 1. The eigenvectors of **A** associated with 1 are the non-zero solutions of the system of linear equations with the matrix of coefficients

$$\mathbf{A}-\mathbf{I}=\begin{pmatrix}-4 & 2 & 2\\ -12 & 6 & 6\\ 0 & 0 & 0\end{pmatrix}\sim\begin{pmatrix}-4 & 2 & 2\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}$$

and therefore they are the solutions of the single equation $4x-2y-2z=0$. For parameters θ and ϕ over $\mathbb{Q}$ which are not both 0, the solutions of this equation are $x=(\theta+\phi)/2$, $y=\theta$ and $z=\phi$. As there are two parameters in this solution, we can obtain a linearly independent set of two eigenvectors by choosing the pairs of parameters $\theta=2$, $\phi=0$ and $\theta=0$, $\phi=2$. This yields the two eigenvectors $(1\ \ 1\ \ 0)^{\mathrm{T}}$ and $(1\ \ 0\ \ 1)^{\mathrm{T}}$ of **A** associated with 1, which obviously form a linearly independent set.

Therefore the vector space of eigenvectors of **A** associated with 1 has dimension 2. Consequently, we deduce from Theorem 3 that **A** is diagonalizable over $\mathbb{Q}$.

Example 5

Is the matrix $\mathbf{A} = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$ diagonalizable ?

The characteristic polynomial of **A** is $\chi(\lambda) = \det(\mathbf{A} - \lambda\mathbf{I})$, and therefore

$$\chi(\lambda) = \begin{vmatrix} -\lambda & 1 & 2 \\ 0 & -\lambda & 3 \\ 0 & 0 & -\lambda \end{vmatrix}.$$

On evaluating the determinant by the last row we obtain $\chi(\lambda) = -\lambda^3$. Therefore the eigenvalues of **A** are 0, 0, 0, so it is not obvious that **A** is diagonalizable. Indeed, if **A** is diagonalizable, by Theorem 3 of Chapter 6, the diagonal matrix is **0** and therefore there exists a non-singular matrix **P** such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{0}$. From this we can deduce that $\mathbf{A} = \mathbf{P0P}^{-1} = \mathbf{0}$, which is obviously false. Consequently, **A** is not diagonalizable.

Theorems 3 and 4 are useful in deciding whether a matrix is diagonalizable, but they certainly have not answered the following question. We shall give a moderately good set of conditions which answer the question in Chapter 9.

QUESTION 2

Is there an easily applied set of conditions which refers to a square matrix **A** over a field $\mathbb{F}$ and which is necessary and sufficient for **A** to be diagonalizable over $\mathbb{F}$?

Summary

We call an $n \times n$ matrix **A** **diagonalizable over** $\mathbb{F}$ if there is a non-singular matrix **P** over $\mathbb{F}$ such that $\mathbf{P}^{-1}\mathbf{AP}$ is a diagonal matrix **D**. But the diagonal elements of **D** are the eigenvalues of **A**, which are the roots of the characteristic polynomial $\chi(\lambda)$ of **A**. Consequently, because the matrix **D** can exist only if $\chi(\lambda)$ has n roots in $\mathbb{F}$ (not necessarily distinct) we limited our discussion to matrices over a field $\mathbb{F}$ which have n eigenvalues in $\mathbb{F}$. It was proved that the vector space spanned by the eigenvectors associated with an eigenvalue has dimension bounded by the multiplicity of the eigenvalue as a root of the characteristic polynomial. This result was used in the proof of the theorem which asserted that a square matrix is diagonalizable over $\mathbb{F}$ if and only if the vector space of eigenvectors associated with each eigenvalue has dimension equal to the multiplicity of the eigenvalue. We deduced from this that an $n \times n$ matrix is diagonalizable over $\mathbb{F}$ if it has n distinct eigenvalues over $\mathbb{F}$.

EXERCISES ON CHAPTER 7

1. Let V be a vector space over the field $\mathbb{F}$, let the subset $\{\mathbf{u}, \mathbf{v}, \mathbf{w}, \mathbf{x}\}$ of V be linearly independent over $\mathbb{F}$ and let a, b, c, d be non-zero elements of $\mathbb{F}$. Prove that $\{a\mathbf{u}, b\mathbf{v}, c\mathbf{w}, d\mathbf{x}\}$ is linearly independent over $\mathbb{F}$.

2. For each matrix in Exercise 3 of Chapter 6 find, if possible, a set of two eigenvectors which is linearly independent over a field which contains the eigenvalues of **A**.

3. For each matrix in Exercise 4 of Chapter 6 find, if possible, a set of three eigenvectors which is linearly independent over a field which contains the eigenvalues of **A**. Also, for each matrix **M** for which it is possible, find a matrix **P** such that $\mathbf{P}^{-1}\mathbf{MP}$ is a diagonal matrix.

4. For each matrix **M** in Exercise 3 for which there is a non-singular matrix **P** such that $\mathbf{P}^{-1}\mathbf{MP}$ is a diagonal matrix, find the inverse of **P** and calculate $\mathbf{M}^5$.

5. Let **A**, **B** and **D** be $n \times n$ matrices over a field $\mathbb{F}$ such that $\mathbf{D} = (m_j\delta_{jk})$, $\mathbf{BA} = \mathbf{DB}$ and the rows of **B** are the row vectors $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \ldots, \mathbf{r}_n$. Show that $\mathbf{r}_j\mathbf{A} = m_j\mathbf{r}_j$ for $j = 1, 2, 3, \ldots, n$.

6. Let **A** be a square matrix over $\mathbb{R}$, let $\lambda, \mu \in \mathbb{R}$ and let **u**, **v** be eigenvectors of **A** associated with the eigenvalue λ. Show that if $b, c \in \mathbb{R}$ and $b\mathbf{u} + c\mathbf{v}$ is an eigenvector of **A** associated with μ,then $\mu = \lambda$.

7. Which of the matrices in Exercise 6 of Chapter 6 is diagonalizable over $\mathbb{C}$?

8. For each eigenvalue λ of each matrix **M** in Exercise 4 of Chapter 6, find the multiplicity m of λ, $k = \text{null}(\mathbf{M} - \lambda\mathbf{I})$ and $m - k$.

8 · The Cayley–Hamilton Theorem

Outline

This chapter is devoted to the surprising result called the Cayley–Hamilton theorem. The theorem states that if $\mathbf{A}$ is an $n \times n$ matrix and its characteristic polynomial $\chi(\lambda)$ is written as

$$\chi(\lambda) \equiv (-1)^n \left[\lambda^n + c_{n-1}\lambda^{n-1} + \ldots + c_2\lambda^2 + c_1\lambda + c_0\right],$$

then

$$\mathbf{A}^n + c_{n-1}\mathbf{A}^{n-1} + \ldots + c_2\mathbf{A}^2 + c_1\mathbf{A} + c_0\mathbf{I} = \mathbf{0}.$$

The way the theorem was discovered is considered and its relevance to the investigation of similar matrices is established before its proof is constructed. Finally, some applications of the Cayley–Hamilton theorem are considered.

Introduction

In this chapter we shall refer to substituting matrices into polynomials, although this is not strictly possible. For example, if we substitute the 2×2 matrix $\mathbf{A}$ for the indeterminate x in the polynomial $x^2 + 2x + 3$ we obtain $\mathbf{A}^2 + 2\mathbf{A} + 3$, which makes no sense because $\mathbf{A}^2 + 2\mathbf{A}$ is a 2×2 matrix and 3 is a number. However, the difficulty is overcome if we first multiply the polynomial by the 2×2 identity matrix $\mathbf{I}$ to yield $x^2\mathbf{I} + 2x\mathbf{I} + 3\mathbf{I}$ into which we can substitute $\mathbf{A}$ to obtain the matrix $\mathbf{A}^2 + 2\mathbf{A} + 3\mathbf{I}$. Alternatively, we could replace the indeterminate x by an **indeterminate** 2×2 **matrix** $\mathbf{X}$ to produce the **matrix polynomial** $\mathbf{X}^2 + 2\mathbf{X} + 3\mathbf{I}$. However, if it happened that $\mathbf{A}^2 + 2\mathbf{A} + 3\mathbf{I} = \mathbf{0}$ it would be misleading to describe $\mathbf{A}$ as a root of the polynomial. Instead, if for the $n \times n$ matrix $\mathbf{A}$ over the field $\mathbb{F}$ and the polynomial

$$f(x) \equiv a_m x^m + a_{m-1}x^{m-1} + \ldots + a_2x^2 + a_1x + a_0$$

over $\mathbb{F}$ we have

$$f(\mathbf{A}) = a_m\mathbf{A}^m + a_{m-1}\mathbf{A}^{m-1} + \ldots + a_2\mathbf{A}^2 + a_1\mathbf{A} + a_0\mathbf{I} = \mathbf{0}$$

then we say that $\mathbf{A}$ **satisfies the polynomial** $f(x)$. In Chapter 1 we proved that for any $n \times n$ matrix over a field $\mathbb{F}$ there exists a polynomial $p(x)$ over $\mathbb{F}$ which is satisfied by $\mathbf{A}$ and for which the degree $\deg p(x) \leq n^2$. The weaknesses of this result (which will be superseded in this chapter) are that the degree of $p(x)$ appears to be inconveniently large and that $p(x)$ has not been identified. Consequently, we need to find a polynomial $q(x)$ which is satisfied by $\mathbf{A}$ and we hope that $\deg q(x)$ is closer to n than to n^2. Let us start with an example, which will also indicate why such a polynomial can be very useful.

○ Example 1

We can find a polynomial $g(x)$ over $\mathbb{Q}$ of degree at most 4, which is satisfied by the matrix $\mathbf{A} = \begin{pmatrix} 11 & 17 \\ -6 & -10 \end{pmatrix}$ as follows. Let $g(x) = b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$, where b_j is an unknown in $\mathbb{Q}$ for $j = 0, 1, 2, 3, 4$, and then substitute $\mathbf{A}$ in $g(x)$ to obtain the equation

$$g(\mathbf{A}) = b_4\mathbf{A}^4 + b_3\mathbf{A}^3 + b_2\mathbf{A}^2 + b_1\mathbf{A} + b_0\mathbf{I} = \mathbf{0}.$$

This equation can be split into four homogeneous linear equations over $\mathbb{Q}$ in the five unknowns b_j, $j = 0, 1, 2, 3, 4$, for which a non-trivial solution can be found to give a polynomial satisfied by $\mathbf{A}$. However, instead of this long method, we shall calculate powers of $\mathbf{A}$ and look for special features. In fact, a special feature appears immediately because $\mathbf{A}^2 = \begin{pmatrix} 19 & 17 \\ -6 & -2 \end{pmatrix}$ has the same elements off the main diagonal as $\mathbf{A}$. Consequently $\mathbf{A}^2 - \mathbf{A}$ is the diagonal matrix $\begin{pmatrix} 8 & 0 \\ 0 & 8 \end{pmatrix} = 8\mathbf{I}$, therefore $\mathbf{A}^2 - \mathbf{A} - 8\mathbf{I} = \mathbf{0}$. We conclude that $\mathbf{A}$ satisfies the quadratic polynomial $x^2 - x - 8$ over $\mathbb{Q}$.

The main use of a polynomial satisfied by a matrix is to give an easy calculation of a high power of the matrix as an alternative to multiplying the matrix recursively by itself. Suppose that we need $\mathbf{A}^5$ in this case. Then we know that $\mathbf{A}^2 = \mathbf{A} + 8\mathbf{I}$, therefore $\mathbf{A}^3 = \mathbf{A}(\mathbf{A} + 8\mathbf{I}) = \mathbf{A}^2 + 8\mathbf{A} = (\mathbf{A} + 8\mathbf{I}) + 8\mathbf{A} = 9\mathbf{A} + 8\mathbf{I}$. Similarly, $\mathbf{A}^4 = 9\mathbf{A}^2 + 8\mathbf{A} = 17\mathbf{A} + 72\mathbf{I}$ and $\mathbf{A}^5 = 17\mathbf{A}^2 + 72\mathbf{A} = 89\mathbf{A} + 136\mathbf{I}$. The technique used for calculating $\mathbf{A}^5$ can also be used to calculate a polynomial expression in the matrix. Any discussion of the relative speeds of this calculation and a direct calculation of $\mathbf{A}^5$ by matrix multiplication must take into account how easily the polynomial can be found.

This example illustrates why it would be useful to discover a general method for identifying a polynomial $f(x)$ satisfied by a given $n \times n$ matrix $\mathbf{A}$, and why it would be preferable if the degree of $f(x)$ were small. Fortunately, in 1858 Arthur Cayley had suggested a polynomial of degree n that an $n \times n$ matrix might satisfy long before the problem of finding it was posed. (This had to wait until after 1918, when the definition of a vector space was given.)

So what was Cayley trying to do when he suggested a polynomial that might be satisfied by a given square matrix? He did not say what problem he was studying, but at the time he was certainly interested in 2×2 and 3×3 matrices associated with geometrical problems and would have wished to diagonalize them. Although we have no further evidence to support this idea, it is reasonable to conjecture that he was really trying to answer Question 2 of Chapter 7. Specifically, he was probably searching for a condition which was satisfied by all diagonalizable matrices, and therefore he discovered the following result.

• Proposition 1

Let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$ which is diagonalizable over $\mathbb{F}$. Then $\mathbf{A}$ satisfies its characteristic polynomial.

PROOF

Because **A** is diagonalizable over $\mathbb{F}$, there exist a non-singular matrix **P** over $\mathbb{F}$ and a diagonal matrix **D** over $\mathbb{F}$ such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$. By Theorem 3 of Chapter 6, the diagonal elements $d_1, d_2, d_3, \ldots, d_n$ of **D** are the eigenvalues of **A**. By Theorem 1 of Chapter 6, the eigenvalues of **A** are the roots of the characteristic polynomial $\chi(\lambda)$ of **A** and therefore

$$\chi(\lambda) \equiv (-1)^n(\lambda - d_1)(\lambda - d_2)(\lambda - d_3)(\lambda - d_n)$$

because the leading coefficient of $\chi(\lambda)$ is $(-1)^n$, as can be proved from Definition 3 of Chapter 6. Consequently, if we substitute the matrix **D** into $\chi(\lambda)$ we obtain

$$\chi(\mathbf{D}) = (-1)^n(\mathbf{D} - d_1\mathbf{I})(\mathbf{D} - d_2\mathbf{I})(\mathbf{D} - d_3\mathbf{I})\ldots(\mathbf{D} - d_n\mathbf{I}).$$

The first row of the matrix $\mathbf{M}_1 = \mathbf{D} - d_1\mathbf{I}$ is zero. Let us assume inductively that the first k rows of the matrix

$$\mathbf{M}_k = (\mathbf{D} - d_1\mathbf{I})(\mathbf{D} - d_2\mathbf{I})(\mathbf{D} - d_3\mathbf{I}) \ldots (\mathbf{D} - d_k\mathbf{I})$$

are zero. Then the first k rows of $\mathbf{M}_{k+1}$ are also zero. But the $(k+1)$th column of the diagonal matrix $\mathbf{D} - d_{k+1}\mathbf{I}$ is also zero, and therefore the $(k+1)$th column of $\mathbf{M}_{k+1}$ is zero. Because $\mathbf{M}_{k+1}$ is a diagonal matrix, the $(k+1)$th row of $\mathbf{M}_{k+1}$ is zero, therefore the first $k+1$ rows of $\mathbf{M}_{k+1}$ are zero. It follows from the principle of induction that $\chi(\mathbf{D}) = (-1)^n\mathbf{M}_n = \mathbf{0}$. Let us write

$$\chi(\lambda) \equiv (-1)^n\left[\lambda^n + c_{n-1}\lambda^{n-1} + \ldots + c_2\lambda^2 + c_1\lambda + c_0\right].$$

Then we have shown that

$$\chi(\mathbf{D}) = (-1)^n\left[\mathbf{D}^n + c_{n-1}\mathbf{D}^{n-1} + \ldots + c_2\mathbf{D}^2 + c_1\mathbf{D} + c_0\mathbf{I}\right] = \mathbf{0}.$$

Because $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$, we deduce from Proposition 2(v) of Chapter 6 that $\mathbf{P}^{-1}\mathbf{A}^k\mathbf{P} = \mathbf{D}^k$ for $k = 1, 2, 3, \ldots, n$, and therefore that

$$(-1)^n\left[\mathbf{P}^{-1}\mathbf{A}^n\mathbf{P} + c_{n-1}\mathbf{P}^{-1}\mathbf{A}^{n-1}\mathbf{P} + \ldots + c_2\mathbf{P}^{-1}\mathbf{A}^2\mathbf{P} + c_1\mathbf{P}^{-1}\mathbf{AP} + c_0\mathbf{I}\right] = \mathbf{0}.$$

Because $\mathbf{I} = \mathbf{P}^{-1}\mathbf{IP}$, this can be written as

$$(-1)^n\mathbf{P}^{-1}\left[\mathbf{A}^n + c_{n-1}\mathbf{A}^{n-1} + \ldots + c_2\mathbf{A}^2 + c_1\mathbf{A} + c_0\mathbf{I}\right]\mathbf{P} = \mathbf{0})$$

and therefore

$$\chi(\mathbf{A}) = (-1)^n\left[\mathbf{A}^n + c_{n-1}\mathbf{A}^{n-1} + \ldots + c_2\mathbf{A}^2 + c_1\mathbf{A} + c_0\mathbf{I}\right] = \mathbf{P0P}^{-1} = \mathbf{0}.$$

We conclude that **A** satisfies its characteristic polynomial. ●

This looks like good progress towards an answer to Question 2 of Chapter 7, except that we have not investigated how the criterion applies to square matrices which are not diagonalizable. Here is such an example.

○ Example 2

We showed in Example 5 of Chapter 6 that the 2×2 matrix $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has repeated eigenvalue 1 and is not diagonalizable. Is $\chi(\mathbf{A}) = \mathbf{0}$, where $\chi(\lambda) \equiv \lambda^2 - 2\lambda + 1$ is the characteristic polynomial of $\mathbf{A}$? To find out, we calculate

$$\mathbf{A}^2 - 2\mathbf{A} + \mathbf{I} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{0}.$$

Example 2 shows that satisfying the characteristic polynomial is not a necessary and sufficient condition for a matrix to be diagonalizable. Therefore we ask which 2×2 matrices satisfy their characteristic polynomials. To answer this, we solve this problem.

TUTORIAL PROBLEM 8.1

Show that any 2×2 matrix over any field satisfies its characteristic polynomial.

In 1858 Cayley published his solution of Tutorial Problem 8.1 and also stated that he had proved the same result for a 3×3 matrix, but, very sensibly, he did not publish this long calculation. In 1853 Hamilton had already proved a similar result for 'quaternions', which can be regarded as extended complex numbers (with three basic quaternions i, j, k for which $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$) or as elements of a certain algebra of 4×4 matrices over $\mathbb{R}$. Hamilton's proof used techniques which would not be effective in the general case, so it does not help us to find a proof of the result for general $n \times n$ matrices. Any attempt to prove that each 4×4 matrix satisfies its characteristic polynomial by direct calculation will soon indicate that the proof of the general case must make use of the principles on which the calculation is based rather than the calculation itself. The following proof of the general result, which is called the **Cayley–Hamilton theorem**, was discovered at a later date and makes use of some formulae, most of them well known, for the evaluation of determinants. For the $n \times n$ matrix $\mathbf{A} = (a_{ij})$ over a field $\mathbb{F}$, the **cofactor** of a_{ij}, which is denoted by $\text{cof}_{ij}\mathbf{A}$, is the product of $(-1)^{i+j}$ and the determinant of the matrix obtained from $\mathbf{A}$ by omitting the ith row and the jth column. The determinant of $\mathbf{A}$ is then **evaluated by the pth row** by means of the formula

$$\det \mathbf{A} = \sum_{j=1}^{n} a_{pj} \, \text{cof}_{pj}\mathbf{A}.$$

The cofactors are used in the definition of the **adjoint of A**, which is denoted by adj $\mathbf{A}$ and given by the formula

$$\text{adj } \mathbf{A} = (\text{cof}_{ij}\mathbf{A})^{\mathrm{T}}.$$

This gives the formula

$$\mathbf{A}(\text{adj } \mathbf{A}) = (\det \mathbf{A})\mathbf{I} \qquad \text{for any square matrix } \mathbf{A}.$$

The adjoint also appears in the formula

$$\mathbf{A}^{-1} = \frac{\text{adj } \mathbf{A}}{\det \mathbf{A}}, \qquad \text{provided that} \quad \det \mathbf{A} \neq 0.$$

○ *Example 3*

The general proof of the Cayley–Hamilton theorem requires the evaluation of the determinant $\det(\mathbf{A}-\lambda\mathbf{I})$, so let us look at $\operatorname{adj}(\mathbf{A}-\lambda\mathbf{I})$ for the 3×3 matrix $\mathbf{A}=\begin{pmatrix} 5 & 0 & 13 \\ 1 & 3 & 14 \\ -2 & 0 & -5 \end{pmatrix}$.

In Example 3 of Chapter 7 we found that the characteristic polynomial of $\mathbf{A}$ is

$$\chi(\lambda)\equiv -(\lambda-3)(\lambda^2+1)\equiv -\lambda^3+3\lambda^2-\lambda+3.$$

(Polynomials $f(x)$ and $g(x)$ are equivalent, and we write $f(x)\equiv g(x)$, when they are equal for all values of x when it is regarded as a variable.) Then

$$\begin{aligned}
\operatorname{adj}(\mathbf{A}-\lambda\mathbf{I}) &\equiv \operatorname{adj}\begin{pmatrix} 5-\lambda & 0 & 13 \\ 1 & 3-\lambda & 4 \\ -2 & 0 & -5-\lambda \end{pmatrix} \\
&\equiv \begin{pmatrix} \lambda^2+2\lambda-15 & \lambda-3 & -2\lambda+6 \\ 0 & \lambda^2+1 & 0 \\ 13\lambda-39 & 4\lambda-7 & \lambda^2-8\lambda+15 \end{pmatrix}^{\mathrm{T}} \\
&\equiv \begin{pmatrix} \lambda^2+2\lambda-15 & 0 & 13\lambda-39 \\ \lambda-3 & \lambda^2+1 & 4\lambda-7 \\ -2\lambda+6 & 0 & \lambda^2-8\lambda+15 \end{pmatrix} \\
&\equiv \lambda^2\mathbf{I}+\lambda\mathbf{B}+\mathbf{C},
\end{aligned}$$

where

$$\mathbf{B}=\begin{pmatrix} 2 & 0 & 13 \\ 1 & 0 & 4 \\ -2 & 0 & -8 \end{pmatrix}, \qquad \mathbf{C}=\operatorname{adj}\mathbf{A}=\begin{pmatrix} -15 & 0 & -39 \\ -3 & 1 & -7 \\ 6 & 0 & 15 \end{pmatrix}.$$

We can therefore calculate $\chi(\lambda)\equiv\det(\mathbf{A}-\lambda\mathbf{I})$ again by the formula

$$\begin{aligned}
\mathbf{I}\det(\mathbf{A}-\lambda\mathbf{I}) &\equiv (\mathbf{A}-\lambda\mathbf{I})\operatorname{adj}(\mathbf{A}-\lambda\mathbf{I}) \\
&\equiv (\mathbf{A}-\lambda\mathbf{I})(\lambda^2\mathbf{I}+\lambda\mathbf{B}+\mathbf{C}) \\
&\equiv -\lambda^3\mathbf{I}+\lambda^2(\mathbf{A}-\mathbf{B})+\lambda(\mathbf{AB}-\mathbf{C})+\mathbf{A}\operatorname{adj}\mathbf{A} \\
&\equiv -\lambda^3\mathbf{I}+3\lambda^2\mathbf{I}-\lambda\mathbf{I}+3\mathbf{I},
\end{aligned}$$

where

$$\mathbf{AB}=\begin{pmatrix} -16 & 0 & -39 \\ -3 & 0 & -7 \\ 6 & 0 & 14 \end{pmatrix}.$$

We shall now prove that for any square matrix $\mathbf{A}$ the adjoint of $(\mathbf{A}-\lambda\mathbf{I})$ can be expressed as a polynomial in λ with matrix coefficients.

• Proposition 2

Let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$ and let λ be an indeterminate. Then there exist $n \times n$ matrices $\mathbf{B}_0, \mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_{n-1}$ over $\mathbb{F}$ such that

$$\operatorname{adj}(\mathbf{A} - \lambda\mathbf{I}) \equiv \mathbf{B}_0 + \lambda\mathbf{B}_1 + \lambda^2\mathbf{B}_2 + \ldots + \lambda^{n-1}\mathbf{B}_{n-1}.$$

PROOF

Write $\mathbf{B} = \mathbf{A} - \lambda\mathbf{I}$. For $i, j = 1, 2, 3, \ldots, n$, we write $\mathbf{B}(i, j)$ for the matrix $\mathbf{B}$ with the ith row and the jth column omitted. Because λ occurs to the first power in each diagonal element of $\mathbf{B}$ but in no other elements, λ occurs to the first power in at most one element (not necessarily diagonal) in each row of $\mathbf{B}(i, j)$. Each term in the sum that makes up $\det \mathbf{B}(i, j)$ is a product of ± 1 and one element from each row of $\mathbf{B}(i, j)$, therefore the term has no power of λ greater than $n - 1$. Consequently, $\det \mathbf{B}(i, j)$ is a polynomial of degree at most $n - 1$ in λ. In fact, $\det \mathbf{B}(i, i)$ is of degree $n - 1$ in λ but $\det \mathbf{B}(i, j)$ is of degree at most $n - 2$ in λ if $j \neq i$. Therefore $\operatorname{cof}_{ij} \mathbf{B} = (-1)^{i+j} \det \mathbf{B}(i, j)$ is a polynomial of degree at most $n - 1$ in λ. It follows that $\operatorname{adj} \mathbf{B}$ can be written as

$$\begin{aligned}\operatorname{adj} \mathbf{B} &\equiv \left(c_{ij}(0) + \lambda c_{ij}(1) + \lambda^2 c_{ij}(2) + \ldots + \lambda^{n-1} c_{ij}(n-1)\right) \\ &\equiv \left(c_{ij}(0)\right) + \left(\lambda c_{ij}(1)\right) + \left(\lambda^2 c_{ij}(2)\right) + \ldots + \left(\lambda^{n-1} c_{ij}(n-1)\right) \\ &\equiv \mathbf{B}_0 + \lambda\mathbf{B}_1 + \lambda^2\mathbf{B}_2 + \ldots + \lambda^{n-1}\mathbf{B}_{n-1},\end{aligned}$$

where $\mathbf{B}_p = (c_{ij}(p))$ for $p = 0, 1, 2, \ldots, n - 1$. ●

We are now ready to prove the Cayley–Hamilton theorem for all square matrices.

• Theorem I The Caley–Hamilton theorem

Every square matrix satisfies its own characteristic polynomial.

PROOF

Let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$, let the characteristic polynomial of $\mathbf{A}$ be $\chi(\lambda) \equiv c_0 + c_1\lambda + c_2\lambda^2 + \ldots + c_n\lambda^n$ and let $\mathbf{B} = \mathbf{A} - \lambda\mathbf{I}$. Then $\chi(\lambda)\mathbf{I} \equiv (\det \mathbf{B})\mathbf{I} \equiv \mathbf{B}(\operatorname{adj} \mathbf{B})$ by the formula concerning determinants. Therefore, by Proposition 2, there exist $n \times n$ matrices $\mathbf{B}_0, \mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_{n-1}$ over $\mathbb{F}$ such that

$$\begin{aligned}c_0\mathbf{I} + c_1\lambda\mathbf{I} + c_2\lambda^2\mathbf{I} + \ldots + c_n\lambda^n\mathbf{I} &\equiv (\mathbf{A} - \lambda\mathbf{I})(\mathbf{B}_0 + \lambda\mathbf{B}_1 + \lambda^2\mathbf{B}_2 + \ldots + \lambda^{n-1}\mathbf{B}_{n-1}) \\ &\equiv \mathbf{A}\mathbf{B}_0 + \lambda(\mathbf{A}\mathbf{B}_1 - \mathbf{B}_0) + \lambda^2(\mathbf{A}\mathbf{B}_2 - \mathbf{B}_1) + \ldots \\ &\quad + \lambda^{n-1}(\mathbf{A}\mathbf{B}_{n-1} - \mathbf{B}_{n-2}) - \lambda^n\mathbf{B}_{n-1}.\end{aligned}$$

By equating the coefficients of λ in this equation we obtain $\mathbf{A}\mathbf{B}_0 = c_0\mathbf{I}$, $\mathbf{A}\mathbf{B}_1 - \mathbf{B}_0 = c_1\mathbf{I}$, $\mathbf{A}\mathbf{B}_2 - \mathbf{B}_1 = c_2\mathbf{I}$, …, $\mathbf{A}\mathbf{B}_{n-1} - \mathbf{B}_{n-2} = c_{n-1}\mathbf{I}$ and $-\mathbf{B}_{n-1} = c_n\mathbf{I}$. We multiply these equations by $\mathbf{I}, \mathbf{A}, \mathbf{A}^2, \ldots, \mathbf{A}^n$, respectively, to obtain $\mathbf{A}\mathbf{B}_0 + \mathbf{0} = c_0\mathbf{I}$, $\mathbf{A}^2\mathbf{B}_1 - \mathbf{A}\mathbf{B}_0 = c_1\mathbf{A}$, $\mathbf{A}^3\mathbf{B}_2 - \mathbf{A}^2\mathbf{B}_1 = c_2\mathbf{A}^2$, …, $\mathbf{A}^n\mathbf{B}_{n-1} - \mathbf{A}^{n-1}\mathbf{B}_{n-2} = c_{n-1}\mathbf{A}^{n-1}$ and $\mathbf{0} - \mathbf{A}^n\mathbf{B}_{n-1} = c_n\mathbf{A}^n$. On adding these equations, we find that the first term on the left-hand side cancels with the second term on the left-hand side of the next equation, so the sum of the equations is

$$\mathbf{0} = c_0\mathbf{I} + c_1\mathbf{A} + c_2\mathbf{A}^2 + \ldots + c_n\mathbf{A}^n = \chi(\mathbf{A}).$$ ●

For the matrix in Example 1 we found a polynomial that the matrix satisfied and used it to give easy expression for higher powers of the matrix. We now prove that the Cayley–Hamilton theorem allows this method to be applied to any square matrix.

• *Proposition 3*

Let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$. Then:

(i) for any positive integer m, the matrix $\mathbf{A}^m$ is either $\mathbf{0}$ or equal to a polynomial in $\mathbf{A}$ of degree at most $n-1$ over $\mathbb{F}$;

(ii) for any polynomial $f(x) \in \mathbb{F}[x]$ there exists $g(x) \in \mathbb{F}[x]$ such that $g(x)$ is either 0 or of degree at most $n-1$ over $\mathbb{F}$ and $f(\mathbf{A}) = g(\mathbf{A})$;

(iii) if $\mathbf{A}$ is non-singular then $\mathbf{A}^{-1}$ is equal to a polynomial in $\mathbf{A}$ of degree at most $n-1$ over $\mathbb{F}$;

(iv) if $\mathbf{A}$ is non-singular then, for any polynomial $p(x) \in \mathbb{F}[x]$, there exists $q(x) \in \mathbb{F}[x]$ such that $q(x)$ is either 0 or of degree at most $n-1$ over $\mathbb{F}$ and $p(\mathbf{A}^{-1}) = q(\mathbf{A})$.

PROOF

The characteristic polynomial of $\mathbf{A}$ is given by $\chi(\lambda) \equiv \det(\mathbf{A} - \lambda\mathbf{I}) \equiv c_0 + c_1\lambda + c_2\lambda^2 + \ldots + c_n\lambda^n$, where $c_j \in \mathbb{F}$ for $j = 0, 1, 2, \ldots, n$. By substituting $\lambda = 0$ in $\chi(\lambda)$ we discover that $c_0 = \det \mathbf{A}$. Also, because λ only occurs in the diagonal elements $a_{jj} - \lambda$ of $\mathbf{A} - \lambda\mathbf{I}$, where $j = 1, 2, 3, \ldots, n$, the only term of degree n in $\chi(\lambda)$ is $(-1)^n\lambda^n$, so $c_n = (-1)^n$.

(i) $\mathbf{A}^m$ is itself a polynomial in $\mathbf{A}$ of degree at most $n-1$ over $\mathbb{F}$ if $m < n$. By the Cayley–Hamilton theorem, $c_0\mathbf{I} + c_1\mathbf{A} + c_2\mathbf{A}^2 + \ldots + c_n\mathbf{A}^n = \mathbf{0}$ therefore $\mathbf{A}^n = (-1)^{n-1}[c_0\mathbf{I} + c_1\mathbf{A} + c_2\mathbf{A}^2 + \ldots + c_{n-1}\mathbf{A}^{n-1}]$ because $c_n = (-1)^n$. Consequently, either $\mathbf{A}^n = \mathbf{0}$ or $\mathbf{A}^n$ is equal to a polynomial in $\mathbf{A}$ of degree at most $n-1$ over $\mathbb{F}$.

Let us assume inductively for the positive integer m such that $m \geq n$ that either $\mathbf{A}^m = \mathbf{0}$ or $\mathbf{A}^m = d_0\mathbf{I} + d_1\mathbf{A} + d_2\mathbf{A}^2 + \ldots + d_{n-1}\mathbf{A}^{n-1}$, where $d_j \in \mathbb{F}$ for $j = 0, 1, 2, \ldots, n-1$. If $\mathbf{A}^m = \mathbf{0}$ then also $\mathbf{A}^{m+1} = \mathbf{0}$. Otherwise

$$\begin{aligned}
\mathbf{A}^{m+1} &= d_0\mathbf{A} + d_1\mathbf{A}^2 + d_2\mathbf{A}^3 + \ldots + d_{n-1}\mathbf{A}^n \\
&= d_0\mathbf{A} + d_1\mathbf{A}^2 + d_2\mathbf{A}^3 + \ldots + d_{n-2}\mathbf{A}^{n-1} \\
&\qquad + (-1)^{n-1}d_{n-1}\left[c_0\mathbf{I} + c_1\mathbf{A} + c_2\mathbf{A}^2 + \ldots + c_{n-1}\mathbf{A}^{n-1}\right] \\
&= (-1)^{n-1}d_{n-1}c_0\mathbf{I} + \left[d_0 + (-1)^{n-1}d_{n-1}c_1\right]\mathbf{A} + \left[d_1 + (-1)^{n-1}d_{n-1}c_2\right]\mathbf{A}^2 \\
&\qquad + \ldots + \left[d_{n-2} + (-1)^{n-1}d_{n-1}c_{n-1}\right]\mathbf{A}^{n-1},
\end{aligned}$$

which is either $\mathbf{0}$ or a polynomial in $\mathbf{A}$ of degree at most $n-1$ over $\mathbb{F}$. Therefore, by the principle of induction, for all positive integers m, $\mathbf{A}^m$ is either $\mathbf{0}$ or equal to a polynomial in $\mathbf{A}$ of degree at most $n-1$ over $\mathbb{F}$.

(ii) By (i), any polynomial $f(\mathbf{A})$ in $\mathbf{A}$ over $\mathbb{F}$ is a sum of multiples of zero matrices and polynomials in $\mathbf{A}$ of degree at most $n-1$ over $\mathbb{F}$ and therefore $f(\mathbf{A}) = g(\mathbf{A})$, where $g(x) \in \mathbb{F}[x]$ is either 0 or is a polynomial of degree at most $n-1$ over $\mathbb{F}$.

(iii) If $\mathbf{A}$ is non-singular then $\mathbf{A}^{-1} \neq \mathbf{0}$ exists and $\mathbf{A}$ satisfies $\chi(\lambda)$, so $c_0\mathbf{I} + c_1\mathbf{A} + c_2\mathbf{A}^2 + \ldots + c_n\mathbf{A}^n = \mathbf{0}$ where $c_0 = \det \mathbf{A} \neq 0$. By multiplying this equation by $\mathbf{A}^{-1}$ we obtain $c_0\mathbf{A}^{-1} + c_1\mathbf{I} + c_2\mathbf{A} + \ldots + c_n\mathbf{A}^{n-1} = \mathbf{0}$ and therefore

$$\mathbf{A}^{-1} = -(c_1/c_0)\mathbf{I} - (c_2/c_0)\mathbf{A} - \ldots - (c_n/c_0)\mathbf{A}^{n-1} = g(\mathbf{A}).$$

where $g(\mathbf{A})$ is a polynomial in $\mathbf{A}$ of degree at most $n-1$ over $\mathbb{F}$.

(iv) Let $p(\mathbf{A}^{-1})$ be a polynomial in $\mathbf{A}^{-1}$ over $\mathbb{F}$. By (iii), $p(\mathbf{A}^{-1}) = p(g(\mathbf{A}))$, which is a polynomial in $\mathbf{A}$ over $\mathbb{F}$. Therefore, by (ii), for $p(g(x))$ there exists $q(x) \in \mathbb{F}[x]$ such that $q(x)$ is either 0 or of degree at most $n-1$ over $\mathbb{F}$ and $p(\mathbf{A}^{-1}) = p(g(\mathbf{A})) = q(\mathbf{A})$. ●

The following example shows how easy it is to calculate matrix polynomials by the methods of Proposition 3.

○ *Example 4*

In Example 4 of Chapter 7 we found that the matrix $\mathbf{A} = \begin{pmatrix} -3 & 2 & 2 \\ -12 & 7 & 6 \\ 0 & 0 & 1 \end{pmatrix}$ over $\mathbb{Q}$ has eigenvalues 1, 1, 3 and that $\mathbf{A}$ is diagonalizable over $\mathbb{Q}$. Now let us use the methods of Proposition 3 to evaluate the polynomial in $\mathbf{A}$ given by $f(\mathbf{A}) = \mathbf{A}^4 - 4\mathbf{A}^3 + 4\mathbf{A}^2 - 4\mathbf{A} + 3\mathbf{I}$ and also evaluate $\mathbf{A}^{-1}$.

Because the eigenvalues of $\mathbf{A}$ are 1, 1, 3, the characteristic polynomial of $\mathbf{A}$ is $\chi(\lambda) \equiv -(\lambda - 1)^2(\lambda - 3) \equiv -\lambda^3 + 5\lambda^2 - 7\lambda + 3$. Therefore, by the Cayley–Hamilton theorem, $-\mathbf{A}^3 + 5\mathbf{A}^2 - 7\mathbf{A} + 3\mathbf{I} = \mathbf{0}$. We start by expressing each of $\mathbf{A}^3$ and $\mathbf{A}^4$ either as $\mathbf{0}$ or as a polynomial of degree at most 2 in $\mathbf{A}$. We have that $\mathbf{A}^3 = 5\mathbf{A}^2 - 7\mathbf{A} + 3\mathbf{I}$, and we can calculate $\mathbf{A}^4$ by $\mathbf{A}^4 = \mathbf{A} \times \mathbf{A}^3$. Therefore

$$\begin{aligned} \mathbf{A}^4 &= 5\mathbf{A}^3 - 7\mathbf{A}^2 + 3\mathbf{A} \\ &= 5(5\mathbf{A}^2 - 7\mathbf{A} + 3\mathbf{I}) - 7\mathbf{A}^2 + 3\mathbf{A} \\ &= 18\mathbf{A}^2 - 32\mathbf{A} + 15\mathbf{I}. \end{aligned}$$

We then deduce that

$$\begin{aligned} f(\mathbf{A}) &= \mathbf{A}^4 - 4\mathbf{A}^3 + 4\mathbf{A}^2 - 4\mathbf{A} + 3\mathbf{I} \\ &= 18\mathbf{A}^2 - 32\mathbf{A} + 15\mathbf{I} - 4(5\mathbf{A}^2 - 7\mathbf{A} + 3\mathbf{I}) + 4\mathbf{A}^2 + 3\mathbf{I} \\ &= 2\mathbf{A}^2 - 8\mathbf{A} + 6\mathbf{I}. \end{aligned}$$

We can now calculate $f(\mathbf{A})$ completely by evaluating

$$\mathbf{A}^2 = \begin{pmatrix} -3 & 2 & 2 \\ -12 & 7 & 6 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} -15 & 8 & 8 \\ -48 & 25 & 24 \\ 0 & 0 & 1 \end{pmatrix}$$

and then, by summing up,

$$\begin{aligned} f(\mathbf{A}) &= 2\mathbf{A}^2 - 8\mathbf{A} + 6\mathbf{I} \\ &= \begin{pmatrix} -30 & 16 & 16 \\ -96 & 50 & 48 \\ 0 & 0 & 2 \end{pmatrix} + \begin{pmatrix} 24 & -16 & -16 \\ 96 & -56 & -48 \\ 0 & 0 & -8 \end{pmatrix} + 6\mathbf{I} = \mathbf{0}. \end{aligned}$$

Thus $f(\mathbf{A})$ is both equal to $\mathbf{0}$ and also equal to the polynomial $2\mathbf{A}^2 - 8\mathbf{A} + 6\mathbf{I}$. Indeed, this implies that $2\mathbf{A}^2 - 8\mathbf{A} + 6\mathbf{I} = \mathbf{0}$ and therefore that $f(\mathbf{A}) = \mathbf{A}^2 - 4\mathbf{A} + 3\mathbf{I} = \mathbf{0}$. Consequently, $f(\mathbf{A})$ is expressible by more than one quadratic polynomial in $\mathbf{A}$ as well as by $\mathbf{0}$. However, our significant discovery is that a diagonalizable matrix with repeated roots may satisfy a polynomial of lower degree than its characteristic polynomial. In this case, $\mathbf{A}$ satisfies $\lambda^2 - 4\lambda + 3 \equiv (\lambda - 1)(\lambda - 3)$, which divides the characteristic polynomial $\chi(\lambda) \equiv -(\lambda - 1)^2(\lambda - 3)$ of $\mathbf{A}$.

The matrix $\mathbf{A}$ is non-singular because, by Definition 3 of Chapter 6, a square matrix is singular if and only if 0 is an eigenvalue. From the Cayley–Hamilton theorem we learn that $\chi(\mathbf{A}) = -\mathbf{A}^3 + 5\mathbf{A}^2 - 7\mathbf{A} + 3\mathbf{I} = \mathbf{0}$. Therefore $3\mathbf{I} = \mathbf{A}^3 - 5\mathbf{A}^2 + 7\mathbf{A}$ and, by multiplying by $\mathbf{A}^{-1}/3$, we obtain $\mathbf{A}^{-1} = [\mathbf{A}^2 - \mathbf{A} + 7\mathbf{I}]/3$. However, in this case, there is an easier way to obtain $\mathbf{A}^{-1}$. Instead of starting with $\chi(\mathbf{A}) = \mathbf{0}$, we can start with $\mathbf{A}^2 - 4\mathbf{A} + 3\mathbf{I} = \mathbf{0}$. This gives us $3\mathbf{I} = -\mathbf{A}^2 + 4\mathbf{A}$ and therefore we multiply this equation by $\mathbf{A}^{-1}/3$ and obtain

$$\mathbf{A}^{-1} = \frac{4\mathbf{I} - \mathbf{A}}{3} = \frac{1}{3}\begin{pmatrix} 7 & -2 & -2 \\ 12 & -3 & -6 \\ 0 & 0 & 3 \end{pmatrix}.$$

The calculation for $\mathbf{A}^{-1}$ in Example 4 looks very short, but it conceals the fact that the process of finding the characteristic polynomial by evaluating a determinant is longer than the process for finding the inverse of a matrix by elementary operations. However, it provides a very quick method of evaluating the inverse whenever the characteristic polynomial needs to be found for some other application. A more significant feature of the matrix in Example 4 is the existence of polynomials satisfied by the matrix $\mathbf{A}$ which are of degree less than 3, which is the degree of the characteristic polynomial of $\mathbf{A}$. A consequence of this is the fact that polynomial expressions of degree less than 3 are not necessarily unique. This raises two questions about an $n \times n$ matrix $\mathbf{A}$ over a field $\mathbb{F}$. The first is whether there is always a polynomial over $\mathbb{F}$ of degree less than n satisfied by $\mathbf{A}$. The other is whether there exists an integer k less than n such that polynomial expressions of degree less than k are always unique. We shall take up these problems again in the next chapter.

Summary

We say that a matrix $\mathbf{A}$ over a field $\mathbb{F}$ **satisfies the polynomial**

$$f(x) \equiv d_0 + d_1 x + d_2 x^2 + \ldots + d_m x^m$$

over $\mathbb{F}$ if

$$f(\mathbf{A}) = d_0\mathbf{I} + d_1\mathbf{A} + d_2\mathbf{A}^2 + \ldots + d_m\mathbf{A}^m = \mathbf{0}.$$

We discovered in Chapter 1 that for every $n \times n$ matrix $\mathbf{A}$ over a field $\mathbb{F}$ there is a polynomial $f(x)$ of degree less than or equal to n^2 over $\mathbb{F}$ which is satisfied by $\mathbf{A}$. In this chapter this result was improved by identifying a polynomial $f(x)$ which is of degree n and can be calculated directly from $\mathbf{A}$. In fact, the **Cayley–Hamilton theorem** asserts that any $n \times n$ matrix $\mathbf{A}$ over a field $\mathbb{F}$ satisfies its characteristic polynomial $\chi(\lambda) \equiv \det(\mathbf{A} - \lambda\mathbf{I})$. The proof of this theorem forms the most important part of this

chapter. However, we found an example of an $n \times n$ matrix which satisfied polynomials of degree less than n. If the matrix $\mathbf{A}$ is non-singular and $\chi(\lambda)$ has already been calculated, then $\chi(\lambda)$ can be used for a very quick calculation of $\mathbf{A}^{-1}$ by expressing it as a polynomial of degree not exceeding $n-1$ in $\mathbf{A}$ over $\mathbb{F}$. In all cases, $\chi(\lambda)$ can be used to express any polynomial in $\mathbf{A}$ as either $\mathbf{0}$ or as a polynomial $h(\mathbf{A})$ in $\mathbf{A}$ of degree less than n over $\mathbb{F}$, although $h(\mathbf{A})$ may not be unique.

EXERCISES ON CHAPTER 8

1. For each of the following matrices over $\mathbb{Q}$ find a polynomial of degree less than 5 over $\mathbb{Q}$ which is satisfied by the matrix:

(i) $\mathbf{A} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$, (ii) $\mathbf{B} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, (iii) $\mathbf{C} = \begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix}$,

(iv) $\mathbf{D} = \begin{pmatrix} 17 & 24 \\ -12 & -17 \end{pmatrix}$, (v) $\mathbf{E} = \begin{pmatrix} 3 & 0 \\ 1 & 3 \end{pmatrix}$.

2. For each of the following matrices over $\mathbb{R}$ find a polynomial of degree less than 10 over $\mathbb{R}$ which is satisfied by the matrix, and thence evaluate the inverse of the matrix if it is defined:

(i) $\mathbf{A} = \begin{pmatrix} 4 & 3 & 3 \\ 2 & 3 & 2 \\ -7 & -7 & -6 \end{pmatrix}$, (ii) $\mathbf{B} = \begin{pmatrix} 4 & 2 & 1 \\ 2 & 7 & 2 \\ 1 & 2 & 4 \end{pmatrix}$,

(iii) $\mathbf{C} = \begin{pmatrix} 4 & 13 & -6 \\ -1 & -3 & 2 \\ 1 & 3 & -1 \end{pmatrix}$, (iv) $\mathbf{D} = \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

3. For each of the following matrices $\mathbf{M}$ find the characteristic polynomial $\chi(\lambda)$ of $\mathbf{M}$ and verify that $\mathbf{M}$ satisfies $\chi(\lambda)$:

(i) $\mathbf{A} = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ -2 & -2 & -1 \end{pmatrix}$, (ii) $\mathbf{B} = \begin{pmatrix} 1 & 1 & -1 \\ -3 & -3 & 3 \\ -2 & -2 & 2 \end{pmatrix}$,

(iii) $\mathbf{C} = \begin{pmatrix} -2 & 8 & 6 \\ -4 & 10 & 6 \\ 4 & -8 & -4 \end{pmatrix}$.

4. Show directly that the matrix $\mathbf{A} = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & k \end{pmatrix}$ over $\mathbb{R}$ satisfies its characteristic polynomial.

5. Find the adjoint of the matrix $\mathbf{A} = \begin{pmatrix} x & 1 & -3 \\ -1 & y & 2 \\ 3 & -2 & z \end{pmatrix}$ over $\mathbb{R}$, where x, y and z are indeterminates, and calculate $\mathbf{A}(\text{adj } \mathbf{A})$.

6. Find an expression as a polynomial of degree less than 3 for the polynomial $\mathbf{P}(\mathbf{M}) = \mathbf{M}^4 + 2\mathbf{M}^3 - \mathbf{I}$ for each matrix $\mathbf{M}$ in Exercise 3.

7. For the matrix $\mathbf{C}$ in Exercise 3, show that $\mathbf{C}^4 = 8\mathbf{C}$, and thence calculate $\mathbf{C}^4$. Also calculate $\mathbf{C}^2 + 6\mathbf{C}$ and $2\mathbf{C}^2 + 4\mathbf{C}$. Prove that there exist polynomials in $\mathbf{C}$ for which the expressions as polynomials of degree less than 3 in $\mathbf{C}$ are not unique. Also show that for the same polynomials the expressions as polynomials of degree exactly 2 in $\mathbf{C}$ are not unique.

8. Let $\mathbf{A}$ be a matrix over a field $\mathbb{F}$ which satisfies the polynomial $f(x) \equiv x^2 + bx + c$ over $\mathbb{F}$. Show that $\mathbf{A}^2$ satisfies the polynomial $g(x) \equiv x^2 + (2c - b^2)x + c^2$. Show that $f(x)$ and $g(x)$ are the same polynomial if and only if either $b = c = 0$ or $b = c = 1$.

9. The Minimum Polynomial

Outline

The discussion of the characteristic polynomial of an $n \times n$ matrix revealed that the matrix might satisfy a polynomial of lower degree than n. In order to investigate this, a polynomial with leading coefficient 1 of least degree such that it is satisfied by a matrix is defined to be a 'minimum polynomial' of the polynomial of the matrix. It is shown for a given matrix that the minimum polynomial is unique and divides every polynomial which is satisfied by the matrix. The Cayley–Hamilton theorem implies that the minimum polynomial divides the characteristic polynomial. It is also proved that every eigenvalue of the matrix is a root of the minimum polynomial, which enables the minimum polynomial to be found. Applications of the minimum polynomial include calculations for unique polynomial expressions for high powers of the matrix and a criterion for a matrix to be diagonalizable.

Introduction

The attempts to use the characteristic polynomial of a square matrix in Chapter 8 prompted two questions about an $n \times n$ matrix over a field $\mathbb{F}$ which provide the motivation for this chapter. First, we answer the following question.

QUESTION 1

Is there a polynomial of degree less than n over $\mathbb{F}$ which is satisfied by the matrix $\mathbf{A}$?

To answer Question 1 we define a certain polynomial $\mu(x)$ in a way which ensures that it exists, is satisfied by the matrix $\mathbf{A}$ and is of degree less than or equal to the degree of the characteristic equation of $\mathbf{A}$. However, this definition does not appear to ensure that $\mu(x)$ is unique and does not provide a method for finding $\mu(x)$. Consequently, we start by finding properties of $\mu(x)$, and these show that $\mu(x)$ is indeed unique.

• Definition 1

Let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$. Then a polynomial $\mu(x)$ of degree at least 1 over $\mathbb{F}$ with leading coefficient 1 in an indeterminate x is a **minimum polynomial** of $\mathbf{A}$ if $\mu(x)$ is of least degree among the polynomials satisfied by $\mathbf{A}$.

○ Example 1

Let us consider the matrix

$$\mathbf{A} = \begin{pmatrix} -3 & 2 & 2 \\ -12 & 7 & 6 \\ 0 & 0 & 1 \end{pmatrix}$$

over $\mathbb{Q}$ of Example 4 in Chapter 8. We found that $\mathbf{A}$ is diagonalizable with eigenvalues 1, 1, 3, so the characteristic polynomial of $\mathbf{A}$ is $\chi(\lambda) \equiv -(\lambda - 1)^2(\lambda - 3) \equiv -\lambda^3 + 5\lambda^2 - 7\lambda + 3$. We also discovered that $2\mathbf{A}^2 - 8\mathbf{A} + 6\mathbf{I} = \mathbf{0}$; consequently, $\mathbf{A}$ satisfies the polynomial $f(x) \equiv 2x^2 - 8x + 6$ over $\mathbb{Q}$, therefore $-\chi(x)$, which has leading coefficient 1, is not of least degree among the polynomials satisfied by $\mathbf{A}$. But $f(x)$ cannot be a minimum polynomial because the leading coefficient is 2, so let us divide $f(x)$ by 2 to give the polynomial $g(x) = x^2 - 4x + 3$ which has leading coefficient 1 and is satisfied by $\mathbf{A}$. So is $g(x)$ a minimum polynomial of $\mathbf{A}$? According to Definition 1, $g(x)$ is a minimum polynomial provided that $\mathbf{A}$ does not satisfy a polynomial $h(x) \equiv x - b$ of degree 1 with leading coefficient 1 over $\mathbb{Q}$. If $\mathbf{A}$ satisfies $h(x)$ then $h(\mathbf{A}) = \mathbf{A} - b\mathbf{I} = \mathbf{0}$ and therefore

$$h(\mathbf{A}) = \begin{pmatrix} 3-b & 2 & 2 \\ -12 & 7-b & 6 \\ 0 & 0 & 1-b \end{pmatrix} = \mathbf{0},$$

which is obviously not true because the element in the first row and second column is not 0. Therefore $g(x)$ is a minimum polynomial for $\mathbf{A}$, and all other minimum polynomials must be quadratic by Definition 1. However, $g(x) = (x - 1)(x - 3)$, so $g(x)$ divides $\chi(x)$. If this holds for every minimum polynomial, it can be used for finding them.

In the next result we prove that the minimum polynomial of a matrix $\mathbf{A}$ is unique, which justifies denoting it by $\mu(x)$, or by $\mu_{\mathbf{A}}(x)$ if more than one matrix is being considered. This suggests that $\mu(x)$ is an alternative to $\chi(x)$ in certain applications. However, there is no standard notation for the minimum polynomial of a matrix.

• Theorem 1

Let $\mathbf{A}$ be a square matrix over a field $\mathbb{F}$ with a minimum polynomial $\mu(x)$. Then $\mu(x)$ is the unique minimum polynomial of $\mathbf{A}$ and $\mathbf{A}$ satisfies a polynomial $f(x)$ over $\mathbb{F}$ if and only if $\mu(x)$ divides $f(x)$.

PROOF

Let $p(x) \neq \mu(x)$ be a minimum polynomial of $\mathbf{A}$. Then $p(x)$, like $\mu(x)$, is of least degree m among the polynomials over $\mathbb{F}$ satisfied by $\mathbf{A}$ and has leading coefficient 1. Therefore $p(\mathbf{A}) = \mu(\mathbf{A}) = \mathbf{0}$, $p(x) = x^m + bx^{m-1} + \ldots$ and $\mu(x) = x^m + cx^{m-1} + \ldots$. Because $p(x) \neq \mu(x)$, the polynomial $g(x) = p(x) - \mu(x) \neq 0$ and also $g(x) = (b - c)x^{m-1} + \ldots$, therefore $g(x)$ is of degree less than m over $\mathbb{F}$. But $g(\mathbf{A}) = p(\mathbf{A}) - \mu(\mathbf{A}) = \mathbf{0}$, so $\mathbf{A}$ satisfies $g(x)$, contrary to $\mu(x)$ being of least degree among polynomials over $\mathbb{F}$ satisfied by $\mathbf{A}$. This shows that $\mu(x)$ is the unique minimum polynomial of $\mathbf{A}$. Let $f(x) \in \mathbb{F}[x]$ such that $\mu(x)$ divides $f(x)$. Then there exists $h(x) \in \mathbb{F}[x]$ such that $f(x) = \mu(x)h(x)$ and therefore $f(x)\mathbf{I} = [\mu(x)\mathbf{I}][h(x)\mathbf{I}]$. It follows that $f(\mathbf{A}) = \mu(\mathbf{A})h(\mathbf{A}) = \mathbf{0}$, therefore $\mathbf{A}$ satisfies $f(x)$.

Conversely, suppose that $\mathbf{A}$ satisfies $f(x) \in \mathbb{F}[x]$. If we divide $f(x)$ by $\mu(x)$ we obtain the quotient $q(x)$ (which may be 0) and remainder $r(x)$; this remainder either has degree less than the degree of $\mu(x)$ or is the zero polynomial. Then $r(x) = f(x) - q(x)\mu(x)$ and, because $\mu(x)$ divides $q(x)\mu(x)$, $q(\mathbf{A})\mu(\mathbf{A}) = \mathbf{0}$. Because $\mathbf{A}$ satisfies $f(x)$, $f(\mathbf{A}) = \mathbf{0}$, therefore $r(\mathbf{A}) = f(\mathbf{A}) - q(\mathbf{A})\mu(\mathbf{A}) = \mathbf{0}$. If the degree of $r(x)$ is less than the degree of $\mu(x)$, then that $\mathbf{A}$ satisfies $r(x)$ contradicts that the degree is least among the polynomials satisfied by $\mathbf{A}$. Consequently, $r(x)$ is the zero polynomial, therefore $f(x) = q(x)\mu(x)$. ●

The following consequence of Theorem 1 and the Cayley–Hamilton theorem is very often used.

• Proposition 1

For any square matrix $\mathbf{A}$ over a field $\mathbb{F}$, the minimum polynomial of $\mathbf{A}$ divides the characteristic polynomial of $\mathbf{A}$.

PROOF

By the Cayley–Hamilton theorem (Theorem 1 of Chapter 8), $\mathbf{A}$ satisfies its characteristic polynomial $\chi(x)$. Therefore, by Theorem 1, the minimum polynomial of $\mathbf{A}$ divides $\chi(x)$. ●

Not only does the minimum polynomial divide the characteristic polynomial of the same matrix, but the properties of the two polynomials are related. For example, the following tutorial problem resembles Proposition 2 of Chapter 6.

TUTORIAL PROBLEM 9.1

Let $\mathbf{A}$ and $\mathbf{B}$ be similar $n \times n$ matrices over a field $\mathbb{F}$. Show that $\mathbf{A}$ and $\mathbf{B}$ have the same minimum polynomial over $\mathbb{F}$.

Before we look at the uses of the minimum polynomial of a matrix, we need to find a reasonable process for finding it. The following example illustrates one of the difficulties.

○ Example 2

What is the minimum polynomial $\mu(x)$ of the matrix where $\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ over $\mathbb{Q}$?

Expansion of $\det(\mathbf{A} - \lambda\mathbf{I})$ by its second row gives the characteristic polynomial as

$$\begin{aligned} \chi(\lambda) &= (2-\lambda)\begin{vmatrix} 1-\lambda & 1 \\ 1 & 1-\lambda \end{vmatrix} \\ &= (2-\lambda)(1-2\lambda+\lambda^2-1) \\ &= (2-\lambda)\lambda(\lambda-2). \end{aligned}$$

Consequently $\chi(x) = -x(x-2)^2$. By Proposition 1, $\mu(x)$ divides $\chi(x)$ and therefore the irreducible factors of $\mu(x)$, that is, those which have no proper polynomial factors, are

among those of $\chi(x)$. Because $\mathbf{A}$ satisfies it, $\mu(x)$ cannot be a constant polynomial, therefore $\mu(x)$ has at least one irreducible factor. Also, the leading coefficient of $\mu(x)$ is 1, so the irreducible factors of $\mu(x)$ may be assumed to be some of x, $x-2$, $x-2$. Therefore $\mu(x)$ is one of the following polynomials over $\mathbb{Q}$: x, $x-2$, $x(x-2)$, $(x-2)^2$, $x(x-2)^2$. To find which one of these polynomials is $\mu(x)$, we substitute $\mathbf{A}$ in each one, starting from the lowest degree, until we find a polynomial which is satisfied. However, this list is a long one for such an easy case, so perhaps we can shorten it by showing that every distinct irreducible factor of $\chi(x)$ divides $\mu(x)$. Although we shall not complete the proof of this result, it follows from the following theorem.

• Theorem 2

Let $\mathbf{A}$ be an $n \times n$ matrix with minimum polynomial $\mu(x)$ over a field $\mathbb{F}$. Then every eigenvalue of $\mathbf{A}$ is a root of $\mu(x)$.

PROOF

Because $\mu(x)$ has leading coefficient 1 and is of degree at least 1, we have a positive integer m and $c_0, c_1, c_2, \ldots, c_{m-1} \in \mathbb{F}$ such that

$$\mu(x) \equiv c_0 + c_1 x + c_2 x^2 + \ldots + c_{m-1} x^{m-1} + x^m.$$

Let λ be an eigenvalue of $\mathbf{A}$. Then there exists an eigenvector $\mathbf{v}$ of $\mathbf{A}$ associated with λ. That means that $\mathbf{v} \neq \mathbf{0}$ is an n-row column vector such that $\mathbf{Av} = \lambda\mathbf{v}$. By Definition 1, $\mathbf{A}$ satisfies $\mu(x)$, therefore

$$\mu(\mathbf{A}) = c_0\mathbf{I} + c_1\mathbf{A} + c_2\mathbf{A}^2 + \ldots + c_{m-1}\mathbf{A}^{m-1} + \mathbf{A}^m = \mathbf{0}.$$

If we multiply this equation on the right by the eigenvector $\mathbf{v}$ we obtain

$$\mu(\mathbf{A})\mathbf{v} = c_0\mathbf{Iv} + c_1\mathbf{Av} + c_2\mathbf{A}^2\mathbf{v} + \ldots + c_{m-1}\mathbf{A}^{m-1}\mathbf{v} + \mathbf{A}^m\mathbf{v} = \mathbf{0}.$$

Let us assume inductively for a positive integer k that $\mathbf{A}^k\mathbf{v} = \lambda^k\mathbf{v}$. Then $\mathbf{A}^{k+1}\mathbf{v} = \mathbf{A}(\mathbf{A}^k\mathbf{v}) = \mathbf{A}(\lambda^k\mathbf{v}) = \lambda^k\mathbf{Av} = \lambda^{k+1}\mathbf{v}$, therefore, by the principle of induction, $\mathbf{A}^k\mathbf{v} = \lambda^k\mathbf{v}$ for all positive integers k. Therefore we have

$$\begin{aligned}\mathbf{0} = \mu(\mathbf{A})\mathbf{v} &= c_0\mathbf{v} + c_1\lambda\mathbf{v} + c_2\lambda^2\mathbf{v} + \ldots + c_{m-1}\lambda^{m-1}\mathbf{v} + \lambda^m\mathbf{v} \\ &= (c_0 + c_1\lambda + c_2\lambda^2 + \ldots + c_{m-1}\lambda^{m-1} + \lambda^m)\mathbf{v} \\ &= \mu(\lambda)\mathbf{v}.\end{aligned}$$

Because $\mathbf{v} \neq \mathbf{0}$, it follows that $\mu(\lambda) = 0$. ●

⊙ Example 3

Now we can complete Example 2 more easily by using Theorem 2. In Example 2 we found that $\chi(\lambda) = -\lambda(\lambda-2)^2$, therefore the eigenvalues of $\mathbf{A}$ are 0 and 2. By Theorem 2, both 0 and 2 are roots of $\mu(x)$, whence x and $x-2$ must divide $\mu(x)$. Therefore only the following members of the list in Example 2 are possible minimum polynomials for $\mathbf{A}$: $x(x-2)$ and $-\chi(x) = x(x-2)^2$. To find out which polynomial is $\mu(x)$ we start with the one of lower degree and test whether it is satisfied by $\mathbf{A}$. However, we obtain

$$\mathbf{A}(\mathbf{A}-2\mathbf{I})=\begin{pmatrix}1&1&1\\0&2&0\\1&1&1\end{pmatrix}\begin{pmatrix}-1&1&1\\0&0&0\\1&1&-1\end{pmatrix}=\begin{pmatrix}0&2&0\\0&0&0\\0&2&0\end{pmatrix}\neq\mathbf{0}.$$

Therefore $\mathbf{A}$ does not satisfy $x(x-2)$, so the minimum polynomial of $\mathbf{A}$ is $-\chi(x)$, which $\mathbf{A}$ satisfies by the Cayley–Hamilton theorem.

The result in the following tutorial problem shows that it is easy to find the minimum polynomial of a square matrix $\mathbf{A}$ over a field for which all the eigenvalues are distinct and belong to $\mathbb{F}$.

TUTORIAL PROBLEM 9.2

Let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$ with minimum polynomial $\mu(x)$ and characteristic polynomial $\chi(x)$. Prove that if $\mathbf{A}$ has n distinct eigenvalues in $\mathbb{F}$ then $\mu(x) = (-1)^n\chi(x)$.

Now that we know enough about the minimum polynomial $\mu_{\mathbf{A}}(x)$ of a matrix $\mathbf{A}$ in order to be able to find it, Definition 1 effectively answers Question 1. This brings us to the second question prompted by the work in Chapter 8.

QUESTION 2

Let $\mathbf{A}$ be an $n \times n$ matrix over $\mathbb{F}$. Is there a polynomial $g(x)$ over $\mathbb{F}$ with the following properties: (i) $\mathbf{A}$ satisfies $g(x)$; (ii) $\deg g(x) = m$, where $m \leq n$; (iii) for any positive integer m, $g(x)$ can be used as in Proposition 3 of Chapter 8 to construct a unique polynomial $s(x)$ over $\mathbb{F}$ such that $\deg s(x) \leq m - 1$ and $\mathbf{A}^m = s(\mathbf{A})$?

That the minimum polynomial $\mu(x)$ of a matrix $\mathbf{A}$ is unique and is of least degree among the polynomials satisfied by $\mathbf{A}$ suggests the following theorem, which shows that $\mu(x)$ is the polynomial $g(x)$ of Question 2.

• Theorem 3

Let $\mathbf{A}$ be a square matrix with minimum polynomial $\mu(x)$ of degree k over a field $\mathbb{F}$. Then:

(i) for any polynomial $f(x) \in \mathbb{F}[x]$ there exists a unique polynomial $g(x) \in \mathbb{F}[x]$ such that $g(x)$ is 0 or of degree less than k over $\mathbb{F}$ and $f(\mathbf{A}) = g(\mathbf{A})$;

(ii) if $\mathbf{A}$ is non-singular then there exists a unique polynomial $p(x) \in \mathbb{F}[x]$ such that $p(x)$ is of degree less than k over $\mathbb{F}$ and $\mathbf{A}^{-1} = p(\mathbf{A})$;

(iii) if $\mathbf{A}$ is non-singular then, for any polynomial $q(x) \in \mathbb{F}[x]$, there exists a unique polynomial $s(x) \in \mathbb{F}[x]$ such that $s(x)$ is either 0 or of degree less than k over $\mathbb{F}$ and $q(\mathbf{A}^{-1}) = s(\mathbf{A})$.

PROOF

(i) By Definition 1, $\mathbf{A}$ satisfies its minimum polynomial $\mu(x)$, which has leading coefficient 1. Then the proofs of parts (i) and (ii) of Proposition 3 of Chapter 8 with $\chi(\mathbf{A})$ replaced by $\mu(\mathbf{A})$, n replaced by k and the leading coefficient $c_n = (-1)^n$ replaced by 1

prove that $f(\mathbf{A}) = g(\mathbf{A})$, where $g(x) \in \mathbb{F}[x]$ is either 0 or of degree less than k. Suppose that $h(x) \neq g(x)$ is a polynomial which is either 0 or of degree less than k such that $f(\mathbf{A}) = h(\mathbf{A})$. Then $g(\mathbf{A}) - h(\mathbf{A}) = f(\mathbf{A}) - f(\mathbf{A}) = \mathbf{0}$ and $g(x) - h(x)$ is of degree less than k over $\mathbb{F}$ because both of $g(x)$ and $h(x)$ are either 0 or of degree less than k. Therefore, if $g(x) - h(x)$ is not the zero polynomial, $g(x) - h(x)$ is a polynomial of degree less than $k = \deg \mu(x)$ which is satisfied by $\mathbf{A}$. This is contrary to Definition 1, which asserts that $\mu(x)$ is of least degree among the polynomials which are satisfied by $\mathbf{A}$. Consequently $h(x) = g(x)$, and therefore $g(x)$ is the unique polynomial which is either 0 or of degree less than k over $\mathbb{F}$ such that $f(\mathbf{A}) = g(\mathbf{A})$.

(ii) Let us assume that $\mathbf{A}$ is non-singular. By Definition 1, $\mu(x)$ has leading coefficient 1 and we have denoted the degree of $\mu(x)$ by k. Therefore we can write

$$\mu(x) \equiv b_0 + b_1 x + b_2 x^2 + \ldots + b_{k-1} x^{k-1} + x^k.$$

By Definition 1, $\mathbf{A}$ satisfies $\mu(x)$, therefore

$$\mu(\mathbf{A}) = b_0 \mathbf{I} + b_1 \mathbf{A} + b_2 \mathbf{A}^2 + \ldots + b_{k-1} \mathbf{A}^{k-1} + \mathbf{A}^k = \mathbf{0}.$$

If $b_0 = 0$, then $\mathbf{A}h(\mathbf{A}) = \mathbf{0}$ where $h(\mathbf{A}) = b_1 \mathbf{I} + b_2 \mathbf{A} + \ldots + b_{k-1} \mathbf{A}^{k-2} + \mathbf{A}^{k-1}$ is a polynomial of degree $k-1$ in $\mathbf{A}$ over $\mathbb{F}$. As the degree of $h(x)$ is less than that of $\mu(x)$, $\mathbf{A}$ cannot satisfy $h(x)$ by Definition 1. It follows that either $\mathbf{A} = \mathbf{0}$ or there exists a matrix $\mathbf{B} \neq \mathbf{0}$ such that $\mathbf{AB} = \mathbf{0}$, which are both incompatible with $\mathbf{A}$ being non-singular. Therefore $b_0 \neq 0$, and by multiplying $\mu(\mathbf{A})$ by $\mathbf{A}^{-1}$ we obtain

$$b_0 \mathbf{A}^{-1} + b_1 \mathbf{I} + b_2 \mathbf{A} + \ldots + b_{k-1} \mathbf{A}^{k-2} + \mathbf{A}^{k-1} = \mathbf{0},$$

and therefore the polynomial $p(x)$ over $\mathbb{F}$ given by

$$p(x) = (b_1/b_0) + (b_2/b_0)x + \ldots + (b_{k-1}/b_0)x^{k-2} + (1/b_0)x^{k-1}$$

is a polynomial of degree less than k such that $\mathbf{A}^{-1} = p(\mathbf{A})$. By (i), $p(x)$ is the only polynomial with this property.

(iii) From (ii) it follows that for $q(x) \in \mathbb{F}[x]$ we have $q(\mathbf{A}^{-1}) = q(p(\mathbf{A}))$. The existence of the unique polynomial $s(x) \in \mathbb{F}[x]$ such that $q(\mathbf{A}^{-1}) = s(\mathbf{A})$, where $s(x)$ is either 0 or of degree less than k, then follows by applying (i) to the polynomial $q(p(x))$ over $\mathbb{F}$. ●

To illustrate the use of Theorem 3, we find the minimum polynomial $\mu_{\mathbf{A}}(x)$ of a matrix $\mathbf{A}$ and deduce from it the unique polynomial in $\mathbf{A}$ of least degree which is equal to a given polynomial in $\mathbf{A}$.

○ *Example 4*

Let us find the minimum polynomial $\mu(x)$ of the matrix $\mathbf{A} = \begin{pmatrix} 2 & 3 & 1 \\ -2 & -5 & -2 \\ 4 & 12 & 5 \end{pmatrix}$ over $\mathbb{Q}$ and deduce from it the unique polynomial in $\mathbf{A}$ of least degree over $\mathbb{Q}$ which is equal to $f(\mathbf{A}) = \mathbf{A}^4 + 3\mathbf{A}^2 + 2\mathbf{I}$.

We start our search for $\mu(x)$ by finding the characteristic polynomial $\chi(\lambda)$ of $\mathbf{A}$, where $\chi(\lambda) \equiv \det(\mathbf{A} - \lambda \mathbf{I})$. By using the first row, we obtain

$$\chi(\lambda)=\begin{vmatrix}2-\lambda & 3 & 1\\ -2 & -5-\lambda & -2\\ 4 & 12 & 5-\lambda\end{vmatrix}\equiv\begin{vmatrix}2-\lambda & 3 & 1\\ -\lambda & -2-\lambda & -1\\ 2\lambda & 6 & 3-\lambda\end{vmatrix}$$

and therefore, by adding three times the second row to the third, we obtain

$$\chi(\lambda)\equiv\begin{vmatrix}2-\lambda & 3 & 1\\ -\lambda & -2-\lambda & -1\\ -\lambda & -3\lambda & -\lambda\end{vmatrix}\equiv(-\lambda)\begin{vmatrix}2-\lambda & 3 & 1\\ -\lambda & -2-\lambda & -1\\ 1 & 3 & 1\end{vmatrix}.$$

We now subtract the third row from the first and evaluate the determinant by an expansion of the first row to obtain

$$\chi(\lambda)\equiv(-\lambda)\begin{vmatrix}1-\lambda & 0 & 0\\ -\lambda & -2-\lambda & -1\\ 1 & 3 & 1\end{vmatrix}\equiv-\lambda(1-\lambda)^2.$$

By Proposition 1, $\mu(x)$ divides $\chi(x)$ and, by Theorem 2, the eigenvalues 0 and 1 are roots of $\mu(x)$. As the leading coefficient of $\mu(x)$ is 1, this means that $\mu(x)$ is $x(x-1)$ if $\mathbf{A}$ satisfies it, and otherwise it is $-\chi(x)$. However,

$$\mathbf{A}(\mathbf{A}-\mathbf{I})=\begin{pmatrix}2 & 3 & 1\\ -2 & -5 & -2\\ 4 & 12 & 5\end{pmatrix}\begin{pmatrix}1 & 3 & 1\\ -2 & -6 & -2\\ 4 & 12 & 4\end{pmatrix}=\mathbf{0},$$

therefore $\mu(x)\equiv x(x-1)\equiv x^2-x$. Because $\mathbf{A}$ satisfies $\mu(x)$, $\mathbf{A}^2=\mathbf{A}$, consequently $\mathbf{A}=\mathbf{A}^2=\mathbf{A}^3=\mathbf{A}^4$. Therefore $f(\mathbf{A})=\mathbf{A}^4+3\mathbf{A}^2+2\mathbf{I}=4\mathbf{A}+2\mathbf{I}$. Because $4\mathbf{A}+2\mathbf{I}$ is of degree in $\mathbf{A}$ less than 2, which is the degree of $\mu(x)$, the expression $f(\mathbf{A})=4\mathbf{A}+2\mathbf{I}$ is unique by Theorem 3.

Now that the main properties of the minimum polynomial of a matrix have been found, we can use it to give an answer to Question 2 of Chapter 7. That is, we can obtain a more practical necessary and sufficient condition for a square matrix to be diagonalizable. We start by gaining some insight into whether the minimum polynomial has any influence over the matrix being diagonalizable. We do this by looking at two examples of matrices with different forms of minimum polynomial.

○ *Example 5*

In Example 3 it was shown that the matrix $\mathbf{A}=\begin{pmatrix}1 & 1 & 1\\ 0 & 2 & 0\\ 1 & 1 & 1\end{pmatrix}$ has the characteristic polynomial $\chi(x)\equiv-x(x-2)^2$ and minimum polynomial $\mu(x)\equiv x(x-2)^2$. The matrix has the three eigenvalues 0, 2, 2 in $\mathbb{R}$, therefore if $\mathbf{A}$ is diagonalizable at all it is diagonalizable over $\mathbb{R}$, by Theorem 3 of Chapter 6. According to Theorem 3 of Chapter 7, $\mathbf{A}$ is diagonalizable over $\mathbb{R}$ if and only if $\mathbf{A}$ has a one-dimensional vector space of eigenvectors associated with 0 and a two-dimensional vector space of eigenvectors associated with 2. The first of these conditions holds by Proposition 1 of Chapter 7, therefore we only need to test the second condition. The matrix of coefficients $\mathbf{A}-2\mathbf{I}$ of the system

of equations $(\mathbf{A} - 2\mathbf{I})\mathbf{x} = \mathbf{0}$ for the eigenvectors associated with the eigenvalue 2 is reducible to echelon form as follows:

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

which is of rank 2. By Theorem 2 of Chapter 4, the rank of the vector space of solutions of $(\mathbf{A} - 2\mathbf{I})\mathbf{x} = \mathbf{0}$ is 1, therefore $\mathbf{A}$ is not diagonalizable over $\mathbb{R}$.

○ *Example 6*

In Example 4 it was shown that the matrix $\mathbf{A} = \begin{pmatrix} 2 & 3 & 1 \\ -2 & -5 & -2 \\ 4 & 12 & 5 \end{pmatrix}$ has characteristic polynomial $\chi(x) = -x(x-1)^2$ and minimum polynomial $\mu(x) = x(x-1)$. To test whether $\mathbf{A}$ is diagonalizable, we again find the dimensions of the vector spaces of eigenvectors for $\mathbf{A}$. For the eigenvalue 0, the vector space of eigenvectors is of dimension 1 by Proposition 1 of Chapter 7. For the eigenvalue 1, the matrix of coefficients of the system of equations $(\mathbf{A} - \mathbf{I})\mathbf{x} = \mathbf{0}$ is

$$\mathbf{A} - \mathbf{I} = \begin{pmatrix} 1 & 3 & 1 \\ -2 & -6 & -2 \\ 4 & 12 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

which is of rank 1. By Theorem 2 of Chapter 4, the vector space of solutions of $(\mathbf{A} - \mathbf{I})\mathbf{x} = \mathbf{0}$ has dimension 2 over $\mathbb{R}$. Therefore the vector spaces of eigenvectors over $\mathbb{R}$ have dimensions equal to their multiplicities and consequently $\mathbf{A}$ is diagonalizable over $\mathbb{R}$, by Theorem 3 of Chapter 7.

In Example 6, where the minimum polynomial factorizes into distinct linear factors, we found that the matrix was diagonalizable, but in Example 5, where the minimum polynomial has a repeated root, we found that the matrix was not diagonalizable. This distinction suggests the following necessary and sufficient condition for a square matrix to be diagonalizable, which also excludes non-linear factors of the minimum polynomial.

• *Theorem 4*

Let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$ with a minimum polynomial $\mu(x)$. Then $\mathbf{A}$ is diagonalizable over $\mathbb{F}$ if and only if $\mu(x)$ is the product of distinct linear factors over $\mathbb{F}$.

PROOF

Let $\mathbf{A}$ be diagonalizable over $\mathbb{F}$ and let the eigenvalues of $\mathbf{A}$ be the distinct d_j of multiplicity $m(j)$, for $j = 1, 2, 3, \ldots, k \leq n$. Then there exist a non-singular matrix $\mathbf{P}$ over $\mathbb{F}$ and a diagonal matrix $\mathbf{D}$ over $\mathbb{F}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$. By Theorem 2 of Chapter 6, the diagonal elements of $\mathbf{D}$ are (in some order) $d_1, \ldots, d_1, d_2, \ldots, d_2, \ldots, d_k, \ldots, d_k \in \mathbb{F}$ and each eigenvalue d_j occurs according to its multiplicity $m(j)$, for $j = 1, 2, \ldots, k$. By transforming $\mathbf{D}$ by the elementary matrix $\mathbf{E}$ which exchanges the ith and jth rows, we obtain $\mathbf{E}^{-1}\mathbf{D}\mathbf{E} = \mathbf{D}_1$, where $\mathbf{D}_1$ is $\mathbf{D}$ with the ith and jth diagonal elements exchanged. By

a chain of such transformations, $\mathbf{D}$ can be transformed into $\mathbf{D}_2$ in which the diagonal elements occur in the order $d_1, \ldots, d_1, d_2, \ldots, d_2, \ldots, d_k, \ldots, d_k$. By Proposition 1 of Chapter 6, $\mathbf{A}$ is similar to $\mathbf{D}_2$, so we may assume without loss of generality that $\mathbf{D}$ is the matrix $\mathbf{D}_2$. Then we may write $\mathbf{D}$ as a partitioned matrix with all submatrices zero except for the diagonal submatrices, which are $d_1\mathbf{I}_{m(1)}, d_2\mathbf{I}_{m(2)}, \ldots, d_k\mathbf{I}_{m(k)}$, where $\mathbf{I}_{m(j)}$ is the $m(j) \times m(j)$ identity matrix, for $j = 1, 2, \ldots, k$. Then $\mathbf{D} - d_j\mathbf{I}_n$ is a diagonal partitioned matrix with a zero submatrix in the jth row and jth column, for $j = 1, 2, \ldots, k$. This allows the induction proof of Proposition 1 of Chapter 8 to be applied to the partitioned matrix $\mathbf{D}$ to show that $(\mathbf{D} - d_1\mathbf{I}_n)(\mathbf{D} - d_2\mathbf{I}_n) \ldots (\mathbf{D} - d_k\mathbf{I}_n) = \mathbf{0}$. By Theorem 2, the polynomial $p(x) \equiv (x - d_1)(x - d_2) \ldots (x - d_k) \in \mathbb{F}[x]$ has distinct roots which are roots of the minimum polynomial $\mu(x)$ of $\mathbf{A}$, and therefore $p(x)$ divides $\mu(x)$. By the argument used in Proposition 1 of Chapter 8, because $\mathbf{D}$ satisfies $p(x)$ so does $\mathbf{A}$. Therefore $\mu(x)$ divides $p(x)$, by Theorem 1. Consequently, there exists $0 \neq f \in \mathbb{F}$ such that $p(x) = f\mu(x)$ and, because $p(x)$ and $\mu(x)$ both have leading coefficient 1, $f = 1$ and $\mu(x) = p(x)$. Therefore the minimum polynomial $\mu(x)$ is the product of distinct linear factors over $\mathbb{F}$.

Conversely, let us assume that the $n \times n$ matrix $\mathbf{B}$ over $\mathbb{F}$ has a minimum polynomial $\mu(x)$ which is the product of distinct linear factors over $\mathbb{F}$, $\mu(x) \equiv (x - c_1)(x - c_2)(x - c_k)$. By Proposition 1, $\mu(x)$ divides the characteristic polynomial $\chi(x)$ of $\mathbf{B}$, therefore the linear factors $x - c_j$ of $\mu(x)$ divide $\chi(x)$, $j = 1, 2, \ldots, k$. Consequently, $c_1, c_2, \ldots, c_k$ are roots of $\chi(x)$ and therefore are eigenvalues of $\mathbf{B}$, by Theorem 1 of Chapter 6. Indeed, by Theorem 2 of the present chapter, all the eigenvalues of $\mathbf{A}$ are roots of $\mu(x)$, so $c_1, c_2, \ldots, c_k \in \mathbb{F}$ is the list of distinct eigenvalues of $\mathbf{B}$. Let the multiplicity of c_j as an eigenvalue of $\mathbf{B}$ be m_j, $j = 1, 2, \ldots, k$. Then, as $\mathbf{B}$ satisfies $\mu(x)$, $(\mathbf{B} - c_1\mathbf{I})(\mathbf{B} - c_2\mathbf{I}) \ldots (\mathbf{B} - c_k\mathbf{I}) = \mathbf{0}$.

According to Theorem 4 of Chapter 4, for $n \times n$ matrices $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_k$ over $\mathbb{F}$, $\operatorname{rank} \mathbf{A}_1\mathbf{A}_2 \geq \operatorname{rank} \mathbf{A}_1 + \operatorname{rank} \mathbf{A}_2 - n$, so a proof by induction shows that

$$\operatorname{rank} \mathbf{A}_1\mathbf{A}_2 \ldots \mathbf{A}_k \geq \operatorname{rank} \mathbf{A}_1 + \operatorname{rank} \mathbf{A}_2 + \ldots + \operatorname{rank} \mathbf{A}_k - (k-1)n.$$

Let us substitute $\mathbf{A}_j = \mathbf{B} - c_j\mathbf{I}$, $j = 1, 2, \ldots, k$, in this formula. Because $(\mathbf{B} - c_1\mathbf{I})(\mathbf{B} - c_2\mathbf{I}) \ldots (\mathbf{B} - c_k\mathbf{I}) = \mathbf{0}$, we obtain

$$R = \operatorname{rank}(\mathbf{B} - c_1\mathbf{I}) + \operatorname{rank}(\mathbf{B} - c_2\mathbf{I}) + \ldots + \operatorname{rank}(\mathbf{B} - c_k\mathbf{I}) \leq (k-1)n.$$

Let us now suppose that $\mathbf{B}$ is not diagonalizable over $\mathbb{F}$. Then, by Theorem 3 of Chapter 7, there is at least one eigenvalue c_q of $\mathbf{B}$ such that the dimension d_q of the vector space of eigenvectors of $\mathbf{B}$ associated with c_q is not equal to the multiplicity m_q of c_q. By the eigenvalue multiplicity theorem, for $j = 1, 2, \ldots, k$, the dimension of the vector space of eigenvectors of $\mathbf{B}$ associated with c_j is $d_j = n - \operatorname{rank}(\mathbf{B} - c_j\mathbf{I}) \leq m_j$ and therefore $\operatorname{rank}(\mathbf{B} - c_j\mathbf{I}) \geq n - m_j$. It follows that because $d_q \neq m_q$, we have $d_q = n - \operatorname{rank}(\mathbf{B} - c_q\mathbf{I}) < m_q$ and therefore $\operatorname{rank}(\mathbf{B} - c_q\mathbf{I}) > n - m_q$. On adding these inequalities, we obtain

$$R = \operatorname{rank}(\mathbf{B} - c_1\mathbf{I}) + \operatorname{rank}(\mathbf{B} - c_2\mathbf{I}) + \ldots + \operatorname{rank}(\mathbf{B} - c_k\mathbf{I}) > nk - s,$$

where $s = m_1 + m_2 + \ldots + m_k$. But s is the total number of (not necessarily distinct) eigenvalues of $\mathbf{B}$, which is an $n \times n$ matrix, and therefore $s = n$ because the eigenvalues are the roots of a polynomial of degree n by Theorem 1 of Chapter 6. This shows that $R > n(k-1)$, whereas we had already shown that $R \leq n(k-1)$. This contradiction shows that the matrix $\mathbf{B}$ is diagonalizable over $\mathbb{F}$. ●

TUTORIAL PROBLEM 9.3

Give a full proof by induction that $(\mathbf{D} - c_1\mathbf{I})(\mathbf{D} - c_2\mathbf{I}) \ldots (\mathbf{D} - c_k\mathbf{I}) = \mathbf{0}$ in the proof of Theorem 4.

When the field $\mathbb{F} = \mathbb{C}$, the condition in Theorem 4 reduces to the condition that all the factors of the minimum polynomial of the matrix are distinct, because the fundamental theorem of algebra ensures that all the factors are linear. This makes the difference in Exercise 9 between the matrix $\mathbf{A}$ when the field is $\mathbb{R}$ and the same matrix $\mathbf{A}$ when it is considered as a matrix over $\mathbb{C}$. However, Theorem 4 answers Question 2 of Chapter 7 for all square matrices and all fields.

Summary

The **minimum polynomial** $\mu(x) \in \mathbb{F}[x]$ of an $n \times n$ matrix $\mathbf{A}$ over a field $\mathbb{F}$ is the polynomial over $\mathbb{F}$ with leading coefficient 1 which is of least degree among the polynomials satisfied by $\mathbf{A}$. Then $\mu(x)$ is uniquely determined by $\mathbf{A}$ and $\mu(x)$ divides every $f(x) \in \mathbb{F}[x]$ such that $f(\mathbf{A}) = \mathbf{0}$. The polynomial $\mu(x)$ can be found for $\mathbf{A}$ because $\mu(x)$ divides the characteristic polynomial $\chi(x)$ of $\mathbf{A}$ and each root of $\chi(x)$ is a root of $\mu(x)$. These conditions determine a finite list L of polynomials over $\mathbb{F}$ with leading coefficients 1, and $\mu(x)$ is the unique $p(x) \in \mathbb{F}[x]$ which is of least degree in L such that $p(\mathbf{A}) = \mathbf{0}$. It also follows that if all the eigenvalues of $\mathbf{A}$ are distinct then $\mu(x) = (-1)^n\chi(x)$. The minimum polynomial $\mu(x)$ of $\mathbf{A}$ has the advantage over $\chi(x)$ that $\mu(x)$ has degree $m \leq n$ and that any polynomial in $\mathbf{A}$ is either $\mathbf{0}$ or equal to a unique polynomial of degree less than m in $\mathbf{A}$ over $\mathbb{F}$. Finally, we proved the criterion that the matrix $\mathbf{A}$ is diagonalizable over $\mathbb{F}$ if and only if its minimum polynomial $\mu(x)$ is the product of distinct linear factors over $\mathbb{F}$.

EXERCISES ON CHAPTER 9

1. Find the minimum polynomials of the matrices over $\mathbb{Q}$ in Exercise 1 of Chapter 8.
2. Find the minimum polynomials of the matrices over $\mathbb{R}$ in Exercise 2 of Chapter 8.
3. Find the minimum polynomials of the matrices in Exercise 3 of Chapter 8.
4. Find the characteristic polynomial $\chi(x)$ of the matrix $\mathbf{A} = \begin{pmatrix} 1 & -1 & 1 \\ 4 & 0 & -1 \\ 4 & -2 & 1 \end{pmatrix}$ over $\mathbb{Q}$.

   Deduce the minimum polynomial $\mu(x)$ of $\mathbf{A}$.
5. Let $\mathbf{D}$ be a diagonal matrix with the diagonal elements 1, 1, 0 in the first, second and third rows, respectively, and let $\mathbf{E}$ be the diagonal matrix with diagonal elements 1, 0, 0, respectively, in those rows. Show that $\mu_{\mathbf{D}}(x) = \mu_{\mathbf{E}}(x)$ although $\chi_{\mathbf{D}}(x) \neq \chi_{\mathbf{E}}(x)$.

6. Let $\mathbf{A}$ be the 3×3 matrix $5\mathbf{I}$, let $\mathbf{B} = \begin{pmatrix} 5 & 1 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{pmatrix}$ and let $\mathbf{C} = \begin{pmatrix} 5 & 1 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 5 \end{pmatrix}$. Show that $\chi_{\mathbf{A}}(x) = \chi_{\mathbf{B}}(x) = \chi_{\mathbf{C}}(x)$ but that $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ have three different minimum polynomials.

7. Let $\mathbf{A}$ be an $n \times n$ matrix over a field $\mathbb{F}$. By using the Cayley–Hamilton theorem, or otherwise, show that the following three statements are equivalent:

(i) $\mathbf{A}^n = \mathbf{0}$.

(ii) There exists a positive integer k such that $\mathbf{A}^k = \mathbf{0}$.

(iii) All n eigenvalues of $\mathbf{A}$ are 0.

8. For each matrix $\mathbf{M}$ of Exercise 3 express the polynomial $\mathbf{P(M)} = \mathbf{M}^4 + 2\mathbf{M}^3 - \mathbf{I}$ as a unique polynomial which is either $\mathbf{0}$ or of the lowest possible degree in $\mathbf{M}$.

9. Let $\mathbf{A} = \begin{pmatrix} \mathbf{B} & \mathbf{0} \\ \mathbf{0} & \mathbf{C} \end{pmatrix}$, where $\mathbf{B} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\mathbf{C} = \begin{pmatrix} 1 & -2 \\ 4 & 7 \end{pmatrix}$. Find the minimum polynomial of $\mathbf{A}$. Is the matrix $\mathbf{A}$ diagonalizable over $\mathbb{R}$? Is the matrix $\mathbf{A}$ diagonalizable over $\mathbb{C}$?

10. For each matrix $\mathbf{M}$ of Exercise 6 of Chapter 6, find the minimum polynomial $\mu(x)$ and decide whether $\mathbf{M}$ is diagonalizable over $\mathbb{R}$.

11. For each matrix $\mathbf{M}$ in Exercise 3 of Chapter 8, decide whether $\mathbf{M}$ is diagonalizable over $\mathbb{R}$. (The minimum polynomial of $\mathbf{M}$ was found in Exercise 3.)

10 · Euclidean Vector Spaces

Outline

In this chapter the scalar product of vector analysis is extended to $\mathbb{R}^n$ for any positive integer n by means of the formula $\mathbf{x}.\mathbf{y} = \mathbf{x}^T\mathbf{y}$, for column vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. With the extra operation of scalar multiplication, $\mathbb{R}^n$ is called a 'Euclidean vector space'. The concept of a Euclidean vector space is generalized to abstract vector spaces by means of an 'inner product'. In a Euclidean vector space the length of a vector is defined and so is the angle between a pair of vectors. In particular, in a Euclidean vector space two vectors are said to be 'orthogonal' if the angle between them is a right angle. Because the values of the scalar product are not preserved when the product is defined in terms of a different basis of the vector space, the principal problem for Euclidean vector spaces is to find the transition matrices of the changes of bases which preserve the values of the scalar product. These matrices are those called 'orthogonal matrices', a name which is somewhat misleading.

Introduction

The outstanding feature of the vector space V of vector analysis is the **vector** (or **cross**) **product** $\mathbf{v} \times \mathbf{w}$ of $\mathbf{v}, \mathbf{w} \in V$. By choosing a set of coordinate axes, the vectors of V can be taken to be those of $\mathbb{R}^3$, and therefore a natural question is whether this product can be defined similarly for $\mathbb{R}^2$ and $\mathbb{R}^n$, where n is an integer greater than 3. For the vectors $\mathbf{v} = (x, y, z)$ and $\mathbf{w} = (p, q, r) \in \mathbb{R}^3$ the product is defined as the vector $\mathbf{v} \times \mathbf{w} = (yr - zq, zp - xr, xq - yp)$. In fact, generalizations of either this definition or the original definition for V of $\mathbf{v} \times \mathbf{w}$ for $\mathbb{R}^2$ or $\mathbb{R}^n$ do not give vectors in the same vector space. Consequently, the use of the vector product of vector analysis is restricted to three dimensions, for which it was designed.

However, the other product of vector analysis, the **scalar product**, can be regarded as a standard feature of certain vector spaces. If $\mathbb{R}^3$ is regarded as consisting of column vectors then the scalar product of vector analysis can be evaluated as $\mathbf{v}.\mathbf{w} = \mathbf{v}^T\mathbf{w}$. The same product is also natural if we regard $\mathbb{R}^3$ as the position vectors in a system of Cartesian coordinates in Euclidean space because the length of such a position vector $\mathbf{v}$ is $\sqrt{\mathbf{v}.\mathbf{v}}$ and the angle θ between the unit vectors $\mathbf{t}$ and $\mathbf{u}$ is given by $\cos\theta = \mathbf{t}.\mathbf{u}$. This definition can be generalized to $\mathbb{R}^n$, where n is any positive integer, but it would not be worth doing unless there were some important applications. The value of this generalization is that it carries ideas such as length into $\mathbb{R}^n$ and also introduces the matrices

which change the bases of $\mathbb{R}^n$ without altering the scalar product. These matrices have many applications, including the rotation of Cartesian axes in euclidean geometry. However, these definitions are not effective if the vector space is over $\mathbb{Q}$ or $\mathbb{C}$, as is shown by the following examples.

○ Example 1

Suppose that the **scalar product** is defined in $\mathbb{Q}^2$ as $\mathbf{v}.\mathbf{w} = \mathbf{v}^T\mathbf{w}$ for $\mathbf{v}, \mathbf{w} \in \mathbb{Q}^2$, just as in vector analysis. Then, as in vector analysis, we define the **length** of the vector $\mathbf{v} \in \mathbb{Q}^2$ as $\|\mathbf{v}\| = \sqrt{\mathbf{v}.\mathbf{v}}$. For $\mathbf{v} = (1, 1)$ we obtain $\mathbf{v}.\mathbf{v} = 2$ and therefore $\|\mathbf{v}\| = \sqrt{2} \notin \mathbb{Q}$. Because the scalars for $\mathbb{Q}^2$ need to be in $\mathbb{Q}$, the idea of the length of a vector cannot be applied to $\mathbb{Q}^2$ in this way. However, this is a slight difficulty because the vectors in $\mathbb{Q}^2$ also belong to $\mathbb{R}^2$, therefore we can work in $\mathbb{R}^2$ instead.

○ Example 2

Suppose that in $\mathbb{C}^2$ the scalar product $\mathbf{v}.\mathbf{w}$ and the length of the vector are defined as in Example 1. Then the length of the vector $\mathbf{u} = (1, i)$ is the square root of $\mathbf{u}^2 = 1^2 + i^2 = 0$, which is unacceptable because $\mathbf{u} \neq \mathbf{0}$. Although the formula for the cosine of the angle between two vectors may define a complex angle, it still follows that $\mathbf{v}, \mathbf{w} \in \mathbb{C}^2$ are at right angles provided that $\mathbf{v}.\mathbf{w} = 0$. Unfortunately, because $\mathbf{u}.\mathbf{u} = 0$, it follows that the vector $\mathbf{u}$ is at right angles to itself, an intolerable phenomenon. Unlike in Example 1, these difficulties concerning $\mathbb{C}^2$ cannot be avoided by using a different field. However, we shall show in Chapter 14 that sensible and useful results can be obtained for $\mathbb{C}^2$ by using a different kind of product.

We shall now define the scalar product for $\mathbb{R}^n$ for any positive integer n, and later we shall extend this definition to other finite-dimensional vector spaces over $\mathbb{R}$, but Examples 1 and 2 show that we cannot use the same definitions for $\mathbb{Q}^n$ or $\mathbb{C}^n$.

• Definition 1

Let n be a positive integer. The **scalar product** on $\mathbb{R}^n$ (also called the **dot product** or the **standard inner product**) is the operation $\mathbf{v}.\mathbf{w} = \mathbf{v}^T\mathbf{w}$, where $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ are regarded as column vectors. The set $\mathbb{R}^n$ with the three operations of addition, multiplication by scalars and the scalar (dot) product is called a **Euclidean vector space**.

Notice that the dot product $\mathbf{v}.\mathbf{w}$ for $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ does not belong to $\mathbb{R}^n$ but is an element of $\mathbb{R}$. Consequently, the dot product cannot be repeated to produce, for example, $\mathbf{u}.(\mathbf{v}.\mathbf{w})$. Instead, for $\mathbf{u} \in V$, there exists the product $(\mathbf{v}.\mathbf{w})\mathbf{u} \in \mathbb{R}^n$ of the vector $\mathbf{u}$ by the scalar $\mathbf{v}.\mathbf{w} \in \mathbb{R}$. The basic properties of the scalar or dot product are given in the following proposition. This is easy to prove, as in the parts which are given.

• Proposition 1

Let $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ and $a \in \mathbb{R}$. Then the following are true:

(i) $\mathbf{v}.\mathbf{w} = \mathbf{w}.\mathbf{v}$;

(ii) $\mathbf{u}.(\mathbf{v} + \mathbf{w}) = \mathbf{u}.\mathbf{v} + \mathbf{u}.\mathbf{w}$;

(iii) $a(\mathbf{v}.\mathbf{w}) = (a\mathbf{v}).\mathbf{w} = \mathbf{v}.(a\mathbf{w})$;

(iv) $\mathbf{v}.\mathbf{v} \geq 0$;
(v) $\mathbf{v}.\mathbf{v} = 0 \Leftrightarrow \mathbf{v} = \mathbf{0}$.

PROOF of (iv) and (v)
(iv) For $\mathbf{v} \in \mathbb{R}^n$, there exist $v_1, v_2, v_3, \ldots, v_n \in \mathbb{R}$ such that $\mathbf{v} = (v_1 \quad v_2 \quad v_3 \quad \ldots \quad v_n)^T$ and therefore $\mathbf{v}.\mathbf{v} = \sum_{j=1}^{n} v_j^2 \geq 0 \in \mathbb{R}$.

(v) If $\mathbf{v} = \mathbf{0}$ then $v_1 = v_2 = v_3 = \ldots = v_n = 0$ therefore $\mathbf{v}.\mathbf{v} = 0$. Conversely, if $\mathbf{v} \neq \mathbf{0}$ then there is at least one element $v_k \neq 0$, consequently $v_k^2 > 0$. Therefore, as $v_j^2 \geq 0$ for $j = 1, 2, 3, \ldots, n$, we deduce that $\mathbf{v}.\mathbf{v} > 0$. ●

Definition 1 cannot be used to define a scalar product for an arbitrary vector space of finite dimension over $\mathbb{R}$, but such a product can be defined by way of its properties. This was the way that linear transformations were defined by the properties of matrix linear transformations in Chapter 4. The precise definition is as follows.

• Definition 2

Let V be a vector space over $\mathbb{R}$. Then an **inner product** on V is a mapping of the set of ordered pair of vectors in V into $\mathbb{R}$ such that the pair $\mathbf{v}, \mathbf{w} \in V$ is mapped onto $\langle \mathbf{v}, \mathbf{w} \rangle \in \mathbb{R}$ and the following conditions hold for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and $a \in \mathbb{R}$:

(i) $\langle \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{w}, \mathbf{v} \rangle$;
(ii) $\langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle$;
(iii) $a\langle \mathbf{v}, \mathbf{w} \rangle = \langle a\mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{v}, a\mathbf{w} \rangle$;
(iv) $\langle \mathbf{v}, \mathbf{v} \rangle \geq 0$;
(v) $\langle \mathbf{v}, \mathbf{v} \rangle = 0 \Leftrightarrow \mathbf{v} = \mathbf{0}$.

If an inner product is defined on V, then V is a **vector space with an inner product.**

By Proposition 1, the Euclidean vector space $\mathbb{R}^n$ is a vector space with an inner product, which we write informally as $\mathbf{v}.\mathbf{w}$. (To be strictly correct, we should denote the mapping, not the result of the mapping.) The inner product can also be defined on infinite-dimensional vector spaces, as is shown by the following example.

○ Example 3

Let V be the vector space over $\mathbb{R}$ of all real-valued functions of a real variable x which are continuous for all x such that $0 \leq x \leq 1$. For all $f(x)$ and $g(x) \in V$, the integral $\int_0^1 f(x)g(x)\,dx$ is defined because the functions are continuous, therefore we can define

$$\langle f(x), g(x) \rangle = \int_0^1 f(x)g(x)\,dx \in \mathbb{R}.$$

It is immediately obvious that

$$\langle g(x), f(x) \rangle = \langle f(x), g(x) \rangle.$$

Let $h(x) \in V$ and let $a \in \mathbb{R}$. Then

$$\begin{aligned}\langle f(x), [g(x)+h(x)]\rangle &= \int_0^1 f(x)[g(x)+h(x)]\,dx \\ &= \int_0^1 f(x)g(x)\,dx + \int_0^1 f(x)h(x)\,dx \\ &= \langle f(x), g(x)\rangle + \langle f(x), h(x)\rangle,\end{aligned}$$

$$\begin{aligned}\langle af(x), g(x)\rangle &= \int_0^1 [af(x)]g(x)\,dx \\ &= a\int_0^1 f(x)g(x)\,dx \\ &= a\langle f(x), g(x)\rangle\end{aligned}$$

and similarly,

$$\langle f(x), ag(x)\rangle = a\langle f(x), g(x)\rangle.$$

Also

$$\langle f(x), f(x)\rangle = \int_0^1 [f(x)]^2\,dx,$$

which is non-negative because it is the integral of a non-negative function. Obviously, if $f(x)$ is the zero function then $\langle f(x), f(x)\rangle = 0$. Finally, $\langle f(x), f(x)\rangle$ can only be 0 for a continuous non-negative function $[f(x)]^2$ if $f(x)$ is the zero function, therefore $\langle f(x), g(x)\rangle$ is an inner product on V according to Definition 2.

Inner products can exist for finite-dimensional vector spaces, and even $\mathbb{R}^2$ can have inner products which are not the scalar product. Consider the following example.

Example 4

For $\mathbf{v}, \mathbf{w} \in \mathbb{R}^2$ we regard the vectors as column vectors and define $\langle \mathbf{v}, \mathbf{w}\rangle = \mathbf{v}^T\mathbf{A}\mathbf{w}$ where $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. We first show that $\langle \mathbf{v}, \mathbf{w}\rangle$ is an inner product for $\mathbb{R}^2$. Because $\langle \mathbf{v}, \mathbf{w}\rangle \in \mathbb{R}$, it is a 1×1 matrix and so equal to its own transpose, and therefore, because $\mathbf{A}^T = \mathbf{A}$, $\langle \mathbf{v}, \mathbf{w}\rangle = (\mathbf{v}^T\mathbf{A}\mathbf{w})^T = \mathbf{w}^T\mathbf{A}^T\mathbf{v} = \mathbf{w}^T\mathbf{A}\mathbf{v} = \langle \mathbf{w}, \mathbf{v}\rangle$. For $\mathbf{x} \in \mathbb{R}^2$, $\langle \mathbf{v}, \mathbf{w} + \mathbf{x}\rangle = \mathbf{v}^T\mathbf{A}(\mathbf{w} + \mathbf{x}) = \mathbf{v}^T\mathbf{A}\mathbf{w} + \mathbf{v}^T\mathbf{A}\mathbf{x} = \langle \mathbf{v}, \mathbf{w}\rangle + \langle \mathbf{v}, \mathbf{x}\rangle$. For $b \in \mathbb{R}$ we have $b(\mathbf{v}^T\mathbf{A}\mathbf{w}) = (b\mathbf{v})^T\mathbf{A}\mathbf{w} = \mathbf{v}^T\mathbf{A}(b\mathbf{w})$, and therefore $b\langle \mathbf{v}, \mathbf{w}\rangle = \langle b\mathbf{v}, \mathbf{w}\rangle = \langle \mathbf{v}, b\mathbf{w}\rangle$. Finally, let $\mathbf{v} = (x \;\; y)^T$. Then $\langle \mathbf{v}, \mathbf{v}\rangle = x^2 + 2xy + 2y^2$, and therefore $\langle \mathbf{v}, \mathbf{v}\rangle = (x + y)^2 + y^2 \geq 0$. Therefore $\langle \mathbf{v}, \mathbf{v}\rangle = 0$ if and only if $x + y = 0$ and $y = 0$, and this is equivalent to $\mathbf{v} = \mathbf{0}$. Therefore $\langle \mathbf{v}, \mathbf{w}\rangle$ is an inner product defined on $\mathbb{R}^2$. However, this inner product can be interpreted in a different way by representing $\mathbb{R}^2$ as $\mathbb{R}^2\sigma$ by the change of basis defined by the transition matrix $\mathbf{P} = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$. The representation is also $\mathbb{R}^2$ but, by Theorem 5 of Chapter 4, the vectors are $\mathbf{v}\sigma = \mathbf{P}^{-1}\mathbf{v}$, where $\mathbf{P}^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. Consequently, the inner product $\langle \mathbf{v}, \mathbf{w}\rangle$ is given by

$$\begin{aligned}\langle \mathbf{v}, \mathbf{w} \rangle &= \langle \mathbf{P}^{-1}\mathbf{v}\sigma, \mathbf{P}^{-1}\mathbf{w}\sigma \rangle \\ &= (\mathbf{P}^{-1}\mathbf{v}\sigma)^{\mathrm{T}}\mathbf{A}(\mathbf{P}^{-1}\mathbf{w}\sigma) \\ &= (\mathbf{v}\sigma)^{\mathrm{T}}\mathbf{B}(\mathbf{w}\sigma),\end{aligned}$$

where

$$\begin{aligned}\mathbf{B} = (\mathbf{P}^{-1})^{\mathrm{T}}\mathbf{A}\mathbf{P}^{-1} &= \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ &= \mathbf{I}.\end{aligned}$$

Therefore the inner product $\langle \mathbf{v}, \mathbf{w} \rangle = \mathbf{v}\sigma.\mathbf{w}\sigma$, which is the dot product.

Although $\mathbb{R}^n$ can have inner products other than the scalar or dot product $\mathbf{v}.\mathbf{w}$, it is assumed that whenever $\mathbb{R}^n$ is considered in a context which requires an inner product, then the product is the dot product unless the contrary is stated. This is similar to the assumption that if the set of vectors is $\mathbb{R}^n$ then the operations of addition and multiplication by scalars are the usual componentwise operations. However, other inner products are needed for $\mathbb{R}^n$ as follows. Let V be a vector space of dimension n over $\mathbb{R}$ with an inner product $\langle \mathbf{v}, \mathbf{w} \rangle$. Let V have the representation ρ with respect to the ordered basis B, as in Proposition 8 of Chapter 4. Then $V\rho = \mathbb{R}^n$ has the inner product $\langle \mathbf{v}\rho, \mathbf{w}\rho \rangle = \langle \mathbf{v}, \mathbf{w} \rangle$. Then the vectors can be regarded as column vectors and an $n \times n$ matrix $\mathbf{C}$ over $\mathbb{R}$ can be found such that $\langle \mathbf{v}\rho, \mathbf{w}\rho \rangle = (\mathbf{v}\rho)^{\mathrm{T}}\mathbf{C}(\mathbf{w}\rho)$.

TUTORIAL PROBLEM 10.1

Consider the vector space $P = \mathrm{P}_2(\mathbb{R})$ which consists of 0 and all polynomials over $\mathbb{R}$ in the indeterminate x which are of degree less than 3. The vector space P has the inner product $\langle f(x), g(x) \rangle = \int_0^1 f(x)g(x)\,dx$, where $f(x), g(x) \in P$, as was shown in Example 3. Find the representation ρ of P with respect to the ordered basis $B = \{1, x, x^2\}$ and find the matrix $\mathbf{C}$ such that $\langle f(x)\rho, g(x)\rho \rangle = [f(x)\rho]^{\mathrm{T}}\mathbf{C}[g(x)\rho]$.

The inner product can be used to define an analogue of the length of a vector $\mathbf{v}$ in a Euclidean vector space $\mathbb{R}^n$, which is given by $\|\mathbf{v}\| = \sqrt{\mathbf{v}.\mathbf{v}}$.

• Definition 3

Let V be a vector space with an inner product. The **length** of $\mathbf{v} \in V$, denoted by $\|\mathbf{v}\|$, is $\|\mathbf{v}\| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$ and $\mathbf{u} \in \mathbb{R}^n$ is a **unit vector** if $\|\mathbf{u}\| = 1$.

Definition 3 defines a length function or **metric** on a vector space V over $\mathbb{R}$ with an inner product. However, it can be shown that all the metrics for a finite-dimensional vector space V which can be defined by means of inner products can be represented by the metric of a Euclidean vector space via representation of V with respect to a suitable ordered basis. On the other hand, there are other metrics which can be defined for V

which are not related to inner products. These metrics are of considerable interest, but they need to be studied by means of topology or analysis rather than linear algebra. So instead, we move on to the problem of converting $\mathbf{v} \in V$ into a unit vector as defined by an inner product. It seems obvious that we should divide $\mathbf{v}$ by its length, and the following proposition proves that this method is effective.

• *Proposition 2*

Let V be a vector space over $\mathbb{R}$ with an inner product. Let $\mathbf{v} \in V$ and $a \in \mathbb{R}$. Then

(i) $\|a\mathbf{v}\| = |a|\|\mathbf{v}\|$;

(ii) if $\mathbf{v} \neq \mathbf{0}$ then $\|(\mathbf{v}/\|\mathbf{v}\|)\| = 1$.

PROOF

(i) By Definition 2(iii), $\langle a\mathbf{v}, a\mathbf{v}\rangle = a^2\langle \mathbf{v}, \mathbf{v}\rangle$, where $\langle \mathbf{v}, \mathbf{v}\rangle \geq 0$ by Definition 2(iv). Therefore $\|a\mathbf{v}\| = \sqrt{a^2}\sqrt{\langle \mathbf{v}, \mathbf{v}\rangle} = |a|\|\mathbf{v}\|$, by Definition 3.

(ii) For $\mathbf{v} \neq \mathbf{0}$, $\|\mathbf{v}\| \neq 0$ by Definition 2(v), therefore, by (i), $\|(\mathbf{v}/\|\mathbf{v}\|)\| = \|\mathbf{v}\|/\|\mathbf{v}\| = 1$. ●

The next two theorems prove inequalities which generalize results concerning the modulus in $\mathbb{R}$ to the lengths of vectors in $\mathbb{R}^n$. The idea behind the first theorem is illustrated by the following example.

○ *Example 5*

Let $\mathbf{v}, \mathbf{w} \in \mathbb{R}^2$ and let $\mathbf{v}$ and $\mathbf{w}$ represent the position vectors of points P and Q in a plane with Cartesian coordinates. Let the angle between the lines OP and OQ be θ. Then, by the formula of vector analysis, $\mathbf{v}.\mathbf{w} = \|\mathbf{v}\|\|\mathbf{w}\|\cos\theta$ and consequently the modulus $|\mathbf{v}.\mathbf{w}| \leq \|\mathbf{v}\|\|\mathbf{w}\|$. Conversely, this inequality allows the angle θ to be defined by $\cos\theta = \mathbf{v}.\mathbf{w}/\|\mathbf{v}\|\|\mathbf{w}\|$.

The following inequality relating the scalar product in $\mathbb{R}^n$ and the product in $\mathbb{R}$ was originally proved by A.-L. Cauchy (1789–1857). More abstract forms were proved by other mathematicians, including H.A. Schwarz (1843–1921), whose proof we use.

• *Theorem 1* The Cauchy–Schwarz inequality

Let $\mathbf{v}, \mathbf{w} \in V$, where V is a vector space V over $\mathbb{R}$ with the inner product $\langle \mathbf{v}, \mathbf{w}\rangle$. Then $|\langle \mathbf{v}, \mathbf{w}\rangle| \leq \|\mathbf{v}\|\|\mathbf{w}\|$.

PROOF

By Definition 3 and Definition 2(iv), for all $a, b \in \mathbb{R}$, $\|a\mathbf{v} + b\mathbf{w}\|^2 = \langle a\mathbf{v} + b\mathbf{w}, a\mathbf{v} + b\mathbf{w}\rangle \geq 0$. Therefore, by Definition 2(ii), $\langle a\mathbf{v}, a\mathbf{v}\rangle + \langle b\mathbf{w}, a\mathbf{v}\rangle + \langle a\mathbf{v}, b\mathbf{w}\rangle + \langle b\mathbf{w}, b\mathbf{w}\rangle \geq 0$ and thence, by Definition 2(i), $\langle a\mathbf{v}, a\mathbf{v}\rangle + 2\langle a\mathbf{v}, b\mathbf{w}\rangle + \langle b\mathbf{w}, b\mathbf{w}\rangle \geq 0$. Therefore, by Definition 2(iii), $a^2\langle \mathbf{v}, \mathbf{v}\rangle + 2ab\langle \mathbf{v}, \mathbf{w}\rangle + b^2\langle \mathbf{w}, \mathbf{w}\rangle \geq 0$. In order to obtain the final inequality, we intend to substitute inner products for a and b. If this is done, the expression in the inequality is of degree 3 in inner products, whereas the required inequality is essentially of degree 2. In order to achieve this we let $a = \langle \mathbf{w}, \mathbf{w}\rangle$. We shall

assume that $\mathbf{w} \neq \mathbf{0}$, because if $\mathbf{w} = \mathbf{0}$ then $\langle \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{v}, \mathbf{0} \rangle = 0\langle \mathbf{v}, \mathbf{v} \rangle = 0$ and therefore the theorem is equivalent to $0 \leq 0$. For all $b \in \mathbb{R}$, we isolate the common factor $\langle \mathbf{w}, \mathbf{w} \rangle$ to obtain $\langle \mathbf{w}, \mathbf{w} \rangle [\langle \mathbf{w}, \mathbf{w} \rangle \langle \mathbf{v}, \mathbf{v} \rangle + 2b\langle \mathbf{v}, \mathbf{w} \rangle + b^2] \geq 0$. But as $\mathbf{w} \neq \mathbf{0}$, Definition 2(v) implies that $\langle \mathbf{w}, \mathbf{w} \rangle \neq 0$. Therefore, for all $b \in \mathbb{R}$, $\langle \mathbf{w}, \mathbf{w} \rangle \langle \mathbf{v}, \mathbf{v} \rangle + 2b\langle \mathbf{v}, \mathbf{w} \rangle + b^2 \geq 0$. In order to convert the inequality into one concerning $\langle \mathbf{w}, \mathbf{w} \rangle \langle \mathbf{v}, \mathbf{v} \rangle$ and $\langle \mathbf{v}, \mathbf{w} \rangle$, we now let $b = -\langle \mathbf{v}, \mathbf{w} \rangle$ and obtain $\langle \mathbf{w}, \mathbf{w} \rangle \langle \mathbf{v}, \mathbf{v} \rangle - \langle \mathbf{v}, \mathbf{w} \rangle^2 \geq 0$. By Definition 3, this is $\langle \mathbf{v}, \mathbf{w} \rangle^2 \leq \|\mathbf{v}\|^2 \|\mathbf{w}\|^2$ and therefore, on taking square roots, $0 \leq |\mathbf{v}.\mathbf{w}| \leq \|\mathbf{v}\| \|\mathbf{w}\|$, because $\|\mathbf{v}\| \geq 0$ and $\|\mathbf{w}\| \geq 0$ by Definition 2(iv). ●

The second inequality gives the relation between the metric and addition in $\mathbb{R}^n$ and is named from its application in the following example.

◎ *Example 6*

Let $\mathbf{v}$, $\mathbf{w}$ be distinct, non-zero vectors in $\mathbb{R}^2$ such that $\mathbf{v} + \mathbf{w} \neq \mathbf{0}$. In a plane in which there are Cartesian coordinates with origin O, let $\mathbf{v}$ and $\mathbf{v} + \mathbf{w}$ be the position vectors of the points P and R. Then the position vector of R relative to P is $\mathbf{w}$. Consequently, the lengths of the sides of the triangle OPR are $\|\mathbf{v}\|$, $\|\mathbf{w}\|$ and $\|\mathbf{v} + \mathbf{w}\|$. Because none of $\mathbf{v}$ or $\mathbf{w}$ or $\mathbf{v} + \mathbf{w}$ is $\mathbf{0}$, the three points O, P and R are distinct. Therefore OPR is a proper triangle and the sum of the lengths of any two sides is greater than the length of the third. Therefore, in this case, $\|\mathbf{v} + \mathbf{w}\| < \|\mathbf{v}\| + \|\mathbf{w}\|$, which we call the **triangle inequality**.

• *Theorem 2* **The triangle inequality**

Let V be a vector space over $\mathbb{R}$ with the inner product $\langle \mathbf{v}, \mathbf{w} \rangle$, where $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$. Then $\|\mathbf{v} + \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|$.

PROOF

By Definition 3, $\|\mathbf{v} + \mathbf{w}\|^2 = \langle \mathbf{v} + \mathbf{w}, \mathbf{v} + \mathbf{w} \rangle$, so, applying first Definition 2(ii) and then Definition 2(i),

$$\begin{aligned} \|\mathbf{v} + \mathbf{w}\|^2 &= \langle \mathbf{v}, \mathbf{v} \rangle + \langle \mathbf{w}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle + \langle \mathbf{w}, \mathbf{w} \rangle \\ &= \langle \mathbf{v}, \mathbf{v} \rangle + 2\langle \mathbf{v}, \mathbf{w} \rangle + \langle \mathbf{w}, \mathbf{w} \rangle. \end{aligned}$$

For any $a \in \mathbb{R}$ it is true that $a \leq |a|$, consequently,

$$\begin{aligned} \|\mathbf{v} + \mathbf{w}\|^2 &\leq \langle \mathbf{v}, \mathbf{v} \rangle + 2|\langle \mathbf{v}, \mathbf{w} \rangle| + \langle \mathbf{w}, \mathbf{w} \rangle \\ &\leq \langle \mathbf{v}, \mathbf{v} \rangle + 2\|\mathbf{v}\| \|\mathbf{w}\| + \langle \mathbf{w}, \mathbf{w} \rangle \end{aligned}$$

by the Cauchy–Schwarz inequality. But, by Definition 3,

$$\|\mathbf{v}\|^2 = \langle \mathbf{v}, \mathbf{v} \rangle$$

and

$$\|\mathbf{w}\|^2 = \langle \mathbf{w}, \mathbf{w} \rangle,$$

therefore

$$\|\mathbf{v} + \mathbf{w}\|^2 \leq \|\mathbf{v}\|^2 + 2\|\mathbf{v}\| \|\mathbf{w}\| + \|\mathbf{w}\|^2 = (\|\mathbf{v}\| + \|\mathbf{w}\|)^2.$$

By Definition 3, $\|\mathbf{x}\| \geq 0$ for all $\mathbf{x} \in \mathbb{R}^n$, therefore, on taking square roots,

$$\|\mathbf{v}+\mathbf{w}\| \leq \|\mathbf{v}\|+\|\mathbf{w}\|. \quad \bullet$$

The Cauchy–Schwarz inequality allows the following definition, as suggested in Example 5.

• Definition 4

The **angle** θ between the vectors $\mathbf{v}$ and $\mathbf{w}$ in the vector space V over $\mathbb{R}$ with inner product $\langle \mathbf{v}, \mathbf{w} \rangle$ is given by $\cos\theta = \langle \mathbf{v}, \mathbf{w} \rangle / \|\mathbf{v}\| \|\mathbf{w}\|$.

It follows from Definition 4 that if $\mathbf{u}$ is a unit vector in a vector space V over $\mathbb{R}$ with an inner product and $\mathbf{v} \in V$ then $\langle \mathbf{v}, \mathbf{u} \rangle$ is the component of $\mathbf{v}$ parallel to $\mathbf{u}$. Definition 4 also gives a criterion for vectors to be perpendicular, which we call **orthogonal** for $\mathbf{v}, \mathbf{w} \in V$.

• Proposition 3

Let $\mathbf{v}, \mathbf{w} \in V$, where V is a vector space of finite dimension n over $\mathbb{R}$ with inner product $\langle \mathbf{v}, \mathbf{w} \rangle$. Then $\mathbf{v}$ and $\mathbf{w}$ are orthogonal if and only if $\langle \mathbf{v}, \mathbf{w} \rangle = 0$.

PROOF

Let the angle between $\mathbf{v}$ and $\mathbf{w}$ be θ. Then $\mathbf{v}$ and $\mathbf{w}$ are orthogonal if and only if $\theta = (2k+1)\pi/2$, where $k \in \mathbb{Z}$. This holds if and only if $\cos\theta = 0$, therefore, by Definition 4, $\mathbf{v}$ and $\mathbf{w}$ are orthogonal if and only if $\langle \mathbf{v}, \mathbf{w} \rangle = 0$. $\bullet$

The following definition extends the idea of orthogonality to vector spaces of dimension n over $\mathbb{R}$ with inner products, including Euclidean vectors spaces $\mathbb{R}^n$ with the dot product. In these vector spaces there are sets of n vectors which are orthogonal to each other.

• Definition 5

Let $S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_k\}$ be a set of non-zero vectors in the vector space V of dimension n over $\mathbb{R}$ with an inner product. Then S is **orthogonal** if every pair of vectors in S is orthogonal. If S is an orthogonal set of unit vectors then S is **orthonormal**.

Care should be taken to observe the important difference between 'orthogonal' and 'orthonormal', particularly as these terms have already become thoroughly confused in important terminology!

The following property of orthogonal sets of vectors is often useful.

• Proposition 4

Any orthogonal set of vectors in a vector space V of finite dimension over $\mathbb{R}$ is linearly independent over $\mathbb{R}$.

PROOF

Let $S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_k\}$ be an orthogonal set of vectors in V and let $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + a_3\mathbf{v}_3 + \ldots + a_k\mathbf{v}_k = \mathbf{0}$, where $a_1, a_2, a_3, \ldots, a_k \in \mathbb{R}$. Then, for $j = 1, 2, 3, \ldots, k$,

$$\begin{aligned}\langle \mathbf{v}_j, a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + a_3\mathbf{v}_3 + \ldots + a_k\mathbf{v}_k \rangle &= \langle \mathbf{v}_j, \mathbf{0} \rangle \\ &= \langle \mathbf{v}_j, 0\mathbf{v}_j \rangle \\ &= 0\langle \mathbf{v}_j, \mathbf{v}_j \rangle \\ &= 0\end{aligned}$$

and therefore

$$a_1\langle \mathbf{v}_j, \mathbf{v}_1 \rangle + a_2\langle \mathbf{v}_j, \mathbf{v}_2 \rangle + a_3\langle \mathbf{v}_j, \mathbf{v}_3 \rangle + \ldots + a_k\langle \mathbf{v}_j, \mathbf{v}_k \rangle = 0$$

by Definitions 2(ii) and 2(iii). As the set S is orthogonal, by Definition 4 and Proposition 3, $\langle \mathbf{v}_j, \mathbf{v}_i \rangle = 0$ for i j, therefore $a_j\langle \mathbf{v}_j, \mathbf{v}_j \rangle = 0$. By Definition 4, $\mathbf{v}_j$ $\mathbf{0}$, therefore $\langle \mathbf{v}_j, \mathbf{v}_j \rangle$ 0 by Definition 2(v) and hence $a_j = 0$. This holds for $j = 1, 2, 3, \ldots, k$, therefore S is linearly independent over $\mathbb{R}$. ●

By Proposition 4, any orthogonal set S of vectors in a finite-dimensional vector space V with an inner product is linearly independent, and therefore S is a subset of a basis B of $\mathbb{R}^n$ by Proposition 5 of Chapter 3. This result has added significance when suitable transition matrices are sought for vector spaces with inner products. In Example 4 the vector space with an inner product was represented with respect to an ordered basis which changed the formula for the inner product to that for the dot product. Clearly, if we already have the dot product (the scalar product) for $\mathbb{R}^n$, we would wish to keep it when we represent the vector space with respect to a different ordered basis for the benefit of some application. Theorem 3 of Chapter 6 associates the changes of basis for $\mathbb{R}^n$ with non-singular transformation matrices, therefore the question we need to ask is the following. What are the transformation matrices of changes of basis which preserve the scalar product? We now answer this question, but we first give a name to a type of matrix which appears in the proof.

• *Definition 6*

A square matrix $\mathbf{A}$ over $\mathbb{R}$ is **orthogonal** if it satisfies $\mathbf{A}^T\mathbf{A} = \mathbf{I}$.

• *Theorem 3*

Let $\mathbb{R}^n$ be a Euclidean vector space with the standard scalar product. Then the scalar product is preserved in the representation defined by the transition matrix $\mathbf{P}$ if and only if $\mathbf{P}$ is orthogonal.

PROOF

By Theorem 5 of Chapter 4, the vectors $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ correspond to the vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ in the representation where $\mathbf{x} = \mathbf{P}\mathbf{v}$ and $\mathbf{y} = \mathbf{P}\mathbf{w}$. The scalar product is preserved if and only if, for all $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$, $\mathbf{x}.\mathbf{y} = \mathbf{v}.\mathbf{w}$. Let us regard the vectors as column vectors over $\mathbb{R}$.

By Definition 1, this is equivalent to $(\mathbf{Pv})^{\mathrm{T}}(\mathbf{Pw}) = \mathbf{v}^{\mathrm{T}}\mathbf{w}$. If $\mathbf{P}$ is orthogonal, then, by Definition 6, $(\mathbf{Pv})^{\mathrm{T}}(\mathbf{Pw}) = \mathbf{v}^{\mathrm{T}}(\mathbf{P}^{\mathrm{T}}\mathbf{P})\mathbf{w} = \mathbf{v}^{\mathrm{T}}\mathbf{w}$, and we deduce that the scalar product is preserved.

Conversely, if the scalar product is preserved then $(\mathbf{Pv})^{\mathrm{T}}(\mathbf{Pw}) = \mathbf{v}^{\mathrm{T}}\mathbf{w}$ for all $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$. In particular, it holds for $\mathbf{v} = \mathbf{e}_i$ and $\mathbf{w} = \mathbf{e}_j$ for $i, j = 1, 2, 3, \ldots, n$, where $\mathbf{e}_i$ is a zero vector except for 1 in the ith place. Then $\mathbf{Pe}_i = \mathbf{c}_i$, the ith column of $\mathbf{P}$, for $i = 1, 2, 3, \ldots, n$. Therefore $(\mathbf{Pe}_i).(\mathbf{Pe}_j) = \mathbf{c}_i^{\mathrm{T}}\mathbf{c}_j = \mathbf{e}_i^{\mathrm{T}}\mathbf{e}_j = \delta_{ij}$ for $i, j = 1, 2, 3, \ldots, n$. Therefore $\mathbf{P}^{\mathrm{T}}\mathbf{P} = (\mathbf{c}_i^{\mathrm{T}}\mathbf{c}_j) = (\delta_{ij}) = \mathbf{I}$. We conclude that preservation of the scalar product implies that $\mathbf{P}$ is orthogonal. ●

In fact, an even stronger result than Theorem 4 is true: the metric of Definition 3 is preserved in the representation with transition matrix $\mathbf{P}$ if and only if $\mathbf{P}$ is orthogonal. This is one further reason for finding the basic properties of orthogonal matrices in the next chapter.

Summary

A **Euclidean vector space** is a total vector space $\mathbb{R}^n$ over $\mathbb{R}$ with the **scalar product** $\mathbf{v}.\mathbf{w} \in \mathbb{R}$ defined for every pair of vectors $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$. Alternatively, the constructions for a Euclidean vector space can be defined in a vector space V of finite dimension n over $\mathbb{R}$ with an **inner product** $\langle \mathbf{v}, \mathbf{w} \rangle \in \mathbb{R}$ which is defined by axioms which are elementary properties of $\mathbf{v}.\mathbf{w}$ for $\mathbb{R}^n$. The **Cauchy–Schwarz** and **triangle inequalities** were proved, and these justify the definition of the **angle** between two vectors and the length $\|\mathbf{v}\|$ of a vector in V. A consequence is that non-zero vectors $\mathbf{v}, \mathbf{w} \in V$ are perpendicular or **orthogonal** in V if and only if $\langle \mathbf{v}, \mathbf{w} \rangle = 0$. An orthogonal set of vectors is called **orthonormal** if every vector in the set has length 1. These terms are somewhat in conflict with the definition that a matrix $\mathbf{A}$ is **orthogonal** if it satisfies the equation $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \mathbf{I}$. Orthogonal matrices are important because they are the transition matrices for changes of bases which preserve the values of the dot product.

EXERCISES ON CHAPTER 10

1. Let $S = \{\mathbf{t} = (-1, 2, 1),\ \mathbf{u} = (0, 0, 1),\ \mathbf{v} = (2, -1, 4),\ \mathbf{w} = (1, 1, 0)\}$ in the Euclidean vector space $\mathbb{R}^3$. Let a change of basis of $\mathbb{R}^3$ correspond to the equation $\mathbf{y} = \mathbf{Px}$, where $\mathbf{P}$ is the transition matrix and the representations of the vectors are regarded as column vectors. Consider three changes of basis with $\mathbf{P} = \mathbf{A}, \mathbf{B}, \mathbf{C}$, where

$$\mathbf{A} = \begin{pmatrix} 1 & -2 & 4 \\ -1 & 1 & 7 \\ 3 & 1 & 1 \end{pmatrix}, \qquad \mathbf{B} = \frac{1}{5}\begin{pmatrix} 4 & 0 & -3 \\ 3 & 0 & 4 \\ 0 & 5 & 0 \end{pmatrix}$$

and

$$\mathbf{C} = \begin{pmatrix} 1 & 2 & -1 \\ 2 & -1 & 2 \\ -1 & 2 & 1 \end{pmatrix}.$$

(i) Calculate the scalar product for the pairs of distinct vectors in S. Are these values altered by the changes of basis?

(ii) What are the lengths of the vectors in S? Are these lengths altered by the changes in basis?

(iii) Which pairs of vectors in S are orthogonal? Are these pairs still orthogonal after the changes of basis?

(iv) Which of the matrices **A**, **B**, **C** are orthogonal?

2. Let the 3×3 matrices $\mathbf{A}_i$ be given by

$$\mathbf{A}_1 = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 2 & -1 & 1 \end{pmatrix}, \qquad \mathbf{A}_2 = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 3 & 0 \\ -1 & 0 & 1 \end{pmatrix}, \qquad \mathbf{A}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\mathbf{A}_4 = \mathbf{I}, \qquad \mathbf{A}_5 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Let the vectors in $\mathbb{R}^3$ be regarded as column vectors. For which matrices $\mathbf{A}_i$, $i = 1, 2, 3, 4, 5$, does the formula $\langle \mathbf{v}, \mathbf{w} \rangle = \mathbf{v}^{\mathrm{T}} \mathbf{A}_i \mathbf{w}$, for all $\mathbf{v}, \mathbf{w} \in \mathbb{R}^3$, define an inner product for $\mathbb{R}^3$?

3. Which of the following formulae define inner products for the stated vector spaces V over $\mathbb{R}$?

(i) $\langle \mathbf{A}, \mathbf{B} \rangle = \det \mathbf{AB}$, where V is the vector space of 2×2 matrices over $\mathbb{R}$.

(ii) $\langle \mathbf{C}, \mathbf{D} \rangle$ is the sum of the diagonal elements of **CD**, where V is the vector space of 4×4 diagonal matrices over $\mathbb{R}$.

(iii) $\langle f(x), g(x) \rangle = \mathfrak{D}[f(x)\, g(x)]$, where V is the vector space over $\mathbb{R}$ of differentiable real functions over $\mathbb{R}$.

(iv) $\langle f(x), g(x) \rangle = \int_0^{\pi} f(x) g(x) \sin x \, dx$, where V is the vector space over $\mathbb{R}$ of real functions of a real variable x which are continuous for $0 \leq x \leq$.

(v) $\langle \mathbf{v}, \mathbf{w} \rangle = \| \mathbf{v} \times \mathbf{w} \|$ (the length of the vector product), where $V = \mathbb{R}^3$.

4. Use Example 3 and the Cauchy–Schwarz inequality to prove that

$$\int_0^1 \mathrm{e}^x \sin \pi x \, dx \leq 2(\mathrm{e} - 1)/\pi.$$

5. Let $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$. Use the triangle inequality to prove that

$$\| \mathbf{v} - \mathbf{w} \| \geq \| \mathbf{v} \| - \| \mathbf{w} \|.$$

6. Show that the subset S of $\mathbf{R}^4$ is orthogonal, where

$$S = \{\mathbf{u} = (1, -1, 1, 1),\ \mathbf{v} = (1, 1, -1, 1),\ \mathbf{w} = (1, 1, 1, -1)\}.$$

Verify that S is linearly independent over $\mathbb{R}$ and find a vector $\mathbf{x} \in \mathbb{R}^4$ such that $T = \{\mathbf{u}, \mathbf{v}, \mathbf{w}, \mathbf{x}\}$ is a basis of $\mathbb{R}^4$.

7. Let $\{\mathbf{v}, \mathbf{w}\}$ be an orthogonal pair of vectors in the Euclidean vector space $\mathbb{R}^n$. Prove that $\| \mathbf{v} + \mathbf{w} \|^2 = \| \mathbf{v} \|^2 + \| \mathbf{w} \|^2$.

8. Let $\theta \in \mathbb{R}$. Show that the matrix $\mathbf{A} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is orthogonal and $\det \mathbf{A} = 1$.

Show that for a rotation of Cartesian axes in the plane there exists $\theta \in \mathbb{R}$ such that the new and old coordinates $\mathbf{w}$ and $\mathbf{v}$ of a general point in the plane are related by $\mathbf{w} = \mathbf{A}\mathbf{v}$.

11 · Orthogonal Matrices

Outline

In Chapter 10 a matrix **A** was called 'orthogonal' if $\mathbf{A}^T\mathbf{A} = \mathbf{I}$. In this chapter it will be shown that orthogonal matrices represent rotations of axes in Cartesian geometry, and the main properties of orthogonal matrices will be found. The construction of orthogonal matrices with certain properties then motivates the 'Gram–Schmidt process', which provides a formula for the construction of an orthogonal basis from a given basis. Also the simple method of constructing an orthonormal basis from an orthogonal basis is given. These processes applied to the columns of a non-singular matrix then provide a construction for an orthogonal matrix with the same column space.

Introduction

We start this chapter by obtaining the basic properties of orthogonal matrices.

• Proposition 1

Let **A** and **B** be orthogonal $n \times n$ matrices and let **P** be an $n \times n$ matrix over $\mathbb{R}$. Then:

(i) the value of the determinant of **A**, det **A**, is either 1 or –1;
(ii) $\mathbf{A}^{-1} = \mathbf{A}^T$ is orthogonal;
(iii) **AB** is orthogonal;
(iv) **P** is orthogonal if and only if the columns of **P** are orthonormal;
(v) **P** is orthogonal if and only if the rows of **P** are orthonormal.

PROOF

(i) By Definition 6 of Chapter 10, $\mathbf{A}^T\mathbf{A} = \mathbf{I}$ and therefore $\det(\mathbf{A}^T\mathbf{A}) = \det \mathbf{I}$, where $\det \mathbf{I} = 1$. But the determinant of a product of matrices is the product of the determinants, therefore $(\det \mathbf{A}^T)(\det \mathbf{A}) = 1$. Because $\det \mathbf{A}^T = \det \mathbf{A}$, we have $(\det \mathbf{A})^2 = 1$ and therefore $\det \mathbf{A} = 1$ or -1.

(ii) By (i), $\mathbf{A}^{-1}$ is defined and hence $\mathbf{A}^{-1} = (\mathbf{A}^T\mathbf{A})\mathbf{A}^{-1} = \mathbf{A}^T(\mathbf{A}\mathbf{A}^{-1}) = \mathbf{A}^T$. Then, because $\mathbf{A}\mathbf{A}^{-1} = \mathbf{I}$, we have $(\mathbf{A}^T)^T\mathbf{A}^T = \mathbf{I}$ and therefore $\mathbf{A}^{-1} = \mathbf{A}^T$ is orthogonal, by Definition 6 of Chapter 10.

(iii) Because **A** is orthogonal, $(\mathbf{AB})^T\mathbf{AB} = \mathbf{B}^T\mathbf{A}^T\mathbf{AB} = \mathbf{B}^T\mathbf{B}$. Therefore $(\mathbf{AB})^T\mathbf{AB} = \mathbf{I}$, because **B** is orthogonal. Consequently **AB** is orthogonal.

(iv) Let **P** be partitioned into its columns as $\mathbf{P} = (\mathbf{c}_1 \ \mathbf{c}_2 \ \mathbf{c}_3 \ \dots \ \mathbf{c}_n)$. Then, by Theorem 4 of Chapter 2, $\mathbf{P}^T$ is the partitioned matrix which consists of a single column in which the submatrices are the row vectors $\mathbf{c}_j^T$, for $j = 1, 2, 3, \dots, n$. Therefore, by the use of Theorem 2 of Chapter 2, $\mathbf{P}^T\mathbf{P}$ is the matrix $(\mathbf{c}_i^T\mathbf{c}_j)$. But, by Definition 6 of Chapter 10, **P** is orthogonal if and only if $\mathbf{P}^T\mathbf{P} = \mathbf{I}$, which is equivalent to $(\mathbf{c}_i^T\mathbf{c}_j) = (\delta_{ij})$, that is, $\mathbf{c}_i \cdot \mathbf{c}_j = \delta_{ij}$ for $i, j = 1, 2, 3, \dots, n$. Consequently, by Definition 3 and Proposition 3 of Chapter 10, this is equivalent to the condition that the set of columns of **P** is orthonormal.

(v) By (ii), **P** is orthogonal if and only if $\mathbf{P}^T$ is orthogonal, which is equivalent to the columns of $\mathbf{P}^T$ forming an orthonormal set, by part (iv). Consequently, **P** is orthogonal if and only if the rows of **P** form an orthonormal set. ●

Those who have studied group theory will recognize that Proposition 1 implies that the set of $n \times n$ orthogonal matrices is a group under matrix multiplication. Parts (iv) and (v) of Proposition 1 also reveal the confusing fact that the rows (or columns) of an **orthogonal** matrix form an **orthonormal** set of vectors. Matrices with *orthogonal* sets of rows (or columns) have few uses and have no special name, whereas the following indicates the importance of orthogonal matrices.

• Theorem 1

The transformation $\mathbf{y} = \mathbf{P}\mathbf{x}$ of the vectors in $\mathbb{R}^n$, for $n = 2$ or 3, represents a rotation of axes if and only if **P** is an orthogonal matrix with $\det \mathbf{P} = 1$.

PROOF

That $\mathbf{y} = \mathbf{P}\mathbf{x}$ is a change of axes for Cartesian coordinates with fixed origin if and only if **P** is orthogonal and follows from Theorem 3 of Chapter 10, because both length and angle are preserved if and only if the dot product is preserved. But, by Proposition 1(i), $\det \mathbf{P} = 1$ or -1. For a rotation of axes about the origin, $\det \mathbf{P}$ is a continuous function of the elements of **P** regarded as real variables, consequently $\det \mathbf{P}$ cannot jump between 1 and –1. Consequently, $\det \mathbf{P}$ is always 1 or always –1. However, if we take the original axes in the usual order as *Oxyz*, the matrix of unit vectors in the direction of the axes is $\mathbf{U} = (\mathbf{e}_1 \ \mathbf{e}_2 \ \mathbf{e}_3)$. Because $\det \mathbf{U} = 1$, the sets of axes (called **right-handed**) to which *Oxyz* can be reached by rotation also have determinant 1. ●

Some formulae for three-dimensional Cartesian geometry are different if the axes are left-handed, but there is no such difference in the plane. In both cases, the change from right-handed to left-handed axes can be achieved by the equivalent of reflecting the space in a mirror. The following example shows the uses of a vector space basis which is orthogonal, which we call an **orthogonal basis**.

○ Example 1

A plane P in three-dimensional space is defined by two distinct lines L and M lying in it. If we wish to study some figure in P, we need Cartesian coordinates for P, and we need to derive these from information about L and M. In order to confine our calculations to Euclidean vector spaces, instead of using Cartesian coordinates, let us assume that the lines L and M pass through the origin. Then the lines L and M are defined by the vectors **r** and **s** and the points in P are those with position vectors in the subspace V of $\mathbb{R}^3$ which is spanned by $B = \{\mathbf{r}, \mathbf{s}\}$. In setting up coordinate axes for P or for finding a basis which allows the scalar product to be used (as given in Definition 1 of Chapter 10), we need an orthogonal basis of V. The spanning set B is a basis of V because otherwise B would be linearly dependent over $\mathbb{R}$, therefore **r** and **s** would be proportional, contrary to $L \neq M$.

Let us start the new basis with the vector **r**. Then we want to construct a basis $C = \{\mathbf{r}, \mathbf{t}\}$ such that $\mathbf{r}.\mathbf{t} = 0$. To take a particular example, let $\mathbf{r} = (1, 0, 7)$ and $\mathbf{s} = (2, 1, -1)$. Then, because B is a basis of V, there exist unique $a, b \in \mathbb{R}$ such that $\mathbf{t} = a\mathbf{r} + b\mathbf{s}$. Then we have the equation $\mathbf{r}.\mathbf{t} = 0$, which leads to $a(1, 0, 7) \cdot (1, 0, 7) + b(1, 0, 7) \cdot (2, 1, -1) = 0$. By calculating the scalar products we obtain $50a - 5b = 0$, therefore we can choose $a = 1$ and find that $b = 10$. Therefore $\mathbf{t} = (1, 0, 7) + 10(2, 1, -1) = (21, 10, -3)$ and $C = \{(1, 0, 7), (21, 10, -3)\}$ is an orthogonal set of vectors. Hence C is linearly independent over $\mathbb{R}$, by Proposition 4 of Chapter 10. Therefore C is a linearly independent set of two vectors in V, which is of dimension 2 and, by Proposition 4 of Chapter 3, C is a basis of V. Consequently, C is the required orthogonal basis of V. However, a set of **unit** vectors parallel to **r** and **t** would be better for geometrical purposes, and, by Proposition 2(ii) of Chapter 10, this can be obtained by dividing each vector by its length. For example, $\mathbf{r}.\mathbf{r} = 1^2 + 7^2 = 50$, therefore $\|(1, 0, 7)\| = \sqrt{50}$. Applying the same process to **t**, we form the basis D of V, where $D = \{(1,0,7)/\sqrt{50}, (21,10,-3)/\sqrt{550}\}$, which is an orthonormal set.

We call a basis of a vector space which is an orthonormal set an **orthonormal basis**. Therefore, because an orthonormal set is linearly independent by Proposition 4 of Chapter 10, part (iv) of Proposition 1 shows that we can construct an $n \times n$ orthogonal matrix by using an orthonormal basis of $\mathbb{R}^n$ as the columns. Unfortunately, the process for finding an orthogonal basis of a vector space V which we used in Example 1 lengthens rapidly as the dimension of V increases, because each additional basis element must be chosen to be orthogonal with each of the vectors that have already been constructed. Consequently, it is much quicker to use the following process, because it provides formulae for the elements of the orthogonal basis. It is called the **Gram–Schmidt process**, even though it would not be recognized in this form by its inventors J.P. Gram (1850–1916) and E. Schmidt (1876–1959), because they used the process for sets of continuous functions.

• *Theorem 2* The Gram–Schmidt process

Let V be a vector space of dimension m over $\mathbb{R}$ with inner product $\langle \mathbf{v}, \mathbf{w} \rangle$ and let $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_m\}$ be a basis of V. For $j = 2, 3, \ldots, m$ and $i = 1, 2, 3, \ldots, j-1$, let $\mathbf{c}_1 = \mathbf{b}_1$ and

$$\mathbf{c}_j = \mathbf{b}_j - p_{1j}\mathbf{c}_1 - p_{2j}\mathbf{c}_2 - p_{3j}\mathbf{c}_3 - \ldots - p_{j-1,j}\mathbf{c}_{j-1},$$

where $p_{ij} = \langle \mathbf{c}_i, \mathbf{b}_j \rangle / \langle \mathbf{c}_i, \mathbf{c}_i \rangle$. Then $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \ldots, \mathbf{c}_m\}$ is an orthogonal basis of V.

PROOF

Because B is a basis of V, $\mathbf{b}_1 \neq \mathbf{0}$ and therefore $\mathbf{c}_1 = \mathbf{b}_1$ is an orthogonal basis of $V_1 = \langle \mathbf{b}_1 \rangle$, the vector space spanned by $\mathbf{b}_1$.

Let us assume inductively that we have already constructed $C_{j-1} = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \ldots, \mathbf{c}_{j-1}\}$, which is an orthogonal basis of the vector space $V_{j-1} = \langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_{j-1} \rangle$. Because C_{j-1} is a basis, $\mathbf{c}_i \neq \mathbf{0}$ for $i = 1, 2, 3, \ldots, j-1$, therefore $\langle \mathbf{c}_i, \mathbf{c}_i \rangle \neq 0$ by Definition 2(v) of Chapter 10. In consequence, p_{ij} is defined for $i = 1, 2, 3, \ldots, j-1$. Therefore we can define

$$\mathbf{c}_j = \mathbf{b}_j - p_{1j}\mathbf{c}_1 - p_{2j}\mathbf{c}_2 - p_{3j}\mathbf{c}_3 - \ldots - p_{j-1,j}\mathbf{c}_{j-1}.$$

Because C_{j-1} spans V_{j-1} and $\mathbf{c}_j = \mathbf{b}_j + \mathbf{v}$, where $\mathbf{v} \in V_{j-1}$, the set $C_j = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \ldots, \mathbf{c}_j\}$ spans $V_j = \langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_j \rangle = \langle V_{j-1}, \mathbf{b}_j \rangle$. Also, for $i = 1, 2, 3, \ldots, j-1$,

$$\begin{aligned}\langle \mathbf{c}_i, \mathbf{c}_j \rangle &= \langle \mathbf{c}_i, \mathbf{b}_j \rangle - p_{1j}\langle \mathbf{c}_i, \mathbf{c}_1 \rangle - \ldots - p_{ij}\langle \mathbf{c}_i, \mathbf{c}_i \rangle - \ldots - p_{j-1,j}\langle \mathbf{c}_i, \mathbf{c}_{j-1} \rangle \\ &= \langle \mathbf{c}_i, \mathbf{b}_j \rangle - p_{ij}\langle \mathbf{c}_i, \mathbf{b}_i \rangle\end{aligned}$$

by Definition 5 of Chapter 10, as C_{j-1} is an orthogonal set by the induction hypothesis. Therefore the product

$$\begin{aligned}\langle \mathbf{c}_i, \mathbf{c}_j \rangle &= \langle \mathbf{c}_i, \mathbf{b}_j \rangle - \left[\langle \mathbf{c}_i, \mathbf{b}_j \rangle / \langle \mathbf{c}_i, \mathbf{c}_i \rangle\right]\langle \mathbf{c}_i, \mathbf{c}_i \rangle \\ &= \langle \mathbf{c}_i, \mathbf{b}_j \rangle - \langle \mathbf{c}_i, \mathbf{b}_j \rangle \\ &= 0,\end{aligned}$$

by the formula for p_{ji}. As C_{j-1} is orthogonal, it follows from Definition 5 of Chapter 10 that $C_j = C_{j-1} \cup \{\mathbf{c}_j\}$ is an orthogonal set. Therefore C_j is linearly independent by Proposition 4 of Chapter 10 and, because C_j spans V_j, it follows that C_j is an orthogonal basis of V_j. By the principle of induction, C_m is an orthogonal basis of $V_m = V$. ●

In Theorem 1, the elements in the bases B and C are only numbered to give a convenient notation, not in order to define ordered bases. Because of this, any vector in B can be chosen as $\mathbf{b}_1$ and therefore be included in C as $\mathbf{c}_1$. We now state the most frequently used form of the Gram–Schmidt process before we show how easy it is to use.

• *Proposition 2* Gram–Schmidt process for $\mathbb{R}^n$

Let V be a subspace of $\mathbb{R}^n$ and let $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_m\}$ be a basis of V. For $j = 2, 3, \ldots, m$ and $i = 1, 2, 3, \ldots, j-1$, let $\mathbf{c}_1 = \mathbf{b}_1$ and

$$\mathbf{c}_j = \mathbf{b}_j - p_{1j}\mathbf{c}_1 - p_{2j}\mathbf{c}_2 - p_{3j}\mathbf{c}_3 - \ldots - p_{j-1,j}\mathbf{c}_{j-1},$$

where $p_{ij} = (\mathbf{c}_i \cdot \mathbf{b}_j)/(\mathbf{c}_i \cdot \mathbf{c}_i)$. Then $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \ldots, \mathbf{c}_m\}$ is an orthogonal basis of V.

○ *Example 2*

Find an orthogonal basis of the vector space V of degree 4 over $\mathbb{R}$ given by

$$V = \langle \mathbf{b}_1 = (0, 1, 1, 1), \quad \mathbf{b}_2 = (1, 0, 1, 1), \quad \mathbf{b}_3 = (1, 1, 0, 1) \rangle.$$

We use the Gram–Schmidt process and start by defining $\mathbf{c}_1 = \mathbf{b}_1$. Then we have $\mathbf{c}_1 \cdot \mathbf{c}_1 = 3$. Therefore

$$p_{12} = (\mathbf{c}_1 \cdot \mathbf{b}_2)/(\mathbf{c}_1 \cdot \mathbf{c}_1) = (0, 1, 1, 1).(1, 0, 1, 1)/3 = \frac{2}{3},$$

and we define

$$\begin{aligned}\mathbf{c}_2 &= \mathbf{b}_2 - \frac{2}{3}\mathbf{c}_1 = (1, 0, 1, 1) - \frac{2}{3}(0, 1, 1, 1) \\ &= \frac{1}{3}(3, -2, 1, 1).\end{aligned}$$

We then have

$$\mathbf{c}_2 \cdot \mathbf{c}_2 = \frac{1}{9}(3, -2, 1, 1).(3, -2, 1, 1) = \frac{5}{3}.$$

Therefore

$$p_{13} = (1, 1, 0, 1).(0, 1, 1, 1)/3 = \frac{2}{3}$$

and

$$p_{23} = \frac{1}{3}(3, -2, 1, 1).(1, 1, 0, 1)/(5/3) = \frac{1}{5}(3, -2, 1, 1).(1, 1, 0, 1) = \frac{2}{5}$$

and we define

$$\begin{aligned}\mathbf{c}_3 &= \mathbf{b}_3 - \frac{2}{3}\mathbf{c}_1 - \frac{2}{5}\mathbf{c}_2 \\ &= (1, 1, 0, 1) - \frac{2}{3}(0, 1, 1, 1) - \frac{2}{15}(3, -2, 1, 1) \\ &= \frac{1}{5}(3, 3, -4, 1).\end{aligned}$$

Then, by Proposition 2, $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$ is an orthogonal basis of V.

Because the formula for each vector in the Gram–Schmidt process only uses the finite number of vectors already defined, the process also works for vector spaces spanned by infinite sequences. At the end of Chapter 10 it was shown that every orthogonal set in $\mathbb{R}^n$ is part of a basis B of $\mathbb{R}^n$. Can B be chosen to be orthogonal? Here is an example.

○ *Example 3*

The set of vectors $S = \{\mathbf{b}_1 = (1, 1, 1), \mathbf{b}_2 = (1, 0, -1)\}$ is orthogonal in $\mathbb{R}^3$ because $(1, 1, 1) \cdot (1, 0, -1) = 0$. Then the subspace $V = \langle S \rangle$ is the set of vectors $\{(a + b, a, a - b) : a, b \in \mathbb{R}\}$ in which any vector with second element 0 is of the form $(b, 0, -b)$, therefore $\mathbf{b}_3 = (0, 0, 1) \notin V$. Therefore $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$ is linearly independent and consequently is a basis of $\mathbb{R}^3$, because $\dim \mathbb{R}^3 = 3$. Can we find an orthogonal basis of $\mathbb{R}^3$ which contains S?

Let us start by finding an orthogonal basis of $\mathbb{R}^3$ by the Gram–Schmidt process. Then let $\mathbf{c}_1 = \mathbf{b}_1$ and therefore $\mathbf{c}_1 \cdot \mathbf{c}_1 = 3$. Then

$$\mathbf{c}_2 = \mathbf{b}_2 - [(\mathbf{c}_1 \cdot \mathbf{b}_2)/(\mathbf{c}_1 \cdot \mathbf{c}_1)]\mathbf{c}_1 = \mathbf{b}_2$$

because $\mathbf{c}_1 \cdot \mathbf{b}_2 = \mathbf{b}_1 \cdot \mathbf{b}_2 = 0$. Therefore $\mathbf{c}_2 \cdot \mathbf{c}_2 = 2$. For the last step in the process, we take

$$\begin{aligned}\mathbf{c}_3 &= \mathbf{b}_3 - [(\mathbf{c}_1 \cdot \mathbf{b}_3)/(\mathbf{c}_1 \cdot \mathbf{c}_1)]\mathbf{c}_1 - [(\mathbf{c}_2 \cdot \mathbf{b}_3)/(\mathbf{c}_2 \cdot \mathbf{c}_2)] \\ &= \mathbf{b}_3 - \frac{1}{3}\mathbf{c}_1 + \frac{1}{2}\mathbf{c}_2 \\ &= (0, 0, 1) - \frac{1}{3}(1, 1, 1) + \frac{1}{2}(1, 0, -1) \\ &= \frac{1}{6}(1, -2, 1).\end{aligned}$$

By Proposition 2, $C = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$ is an orthogonal basis of $\mathbb{R}^3$ which contains S.

In fact, the application of the Gram–Schmidt process as in Example 3 always gives the required orthogonal basis, as we now show.

• *Proposition 3*

Let S be an orthogonal subset of a vector space V with inner product of dimension n over $\mathbb{R}$. Then there exists a set T of vectors in V that is disjoint from S and such that $C = S \cup T$ is an orthogonal basis of V.

PROOF

Because S is orthogonal, S is linearly independent over $\mathbb{R}$ by Proposition 4 of Chapter 10. Therefore, by Proposition 5 of Chapter 3, there exists $T \subseteq V$ such that $S \cap T = \varnothing$ and $B = S \cup T$ is a basis for V. Because $\dim V = n$, B contains n vectors. Unless $B = S$, when there is nothing to prove, there exists k such that we can write $S = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_k\}$ and $T = \{\mathbf{b}_{k+1}, \mathbf{b}_{k+2}, \ldots, \mathbf{b}_m\}$. We apply the Gram–Schmidt process to B, obtaining the orthogonal basis $C = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \ldots, \mathbf{c}_m\}$ of V, where $\mathbf{c}_1 = \mathbf{b}_1$, and for $j = 1, 2, 3, \ldots, m$, and $i = 1, 2, 3, \ldots, j-1$, $\mathbf{c}_j = \mathbf{b}_j - p_{1j}\mathbf{c}_1 - p_{2j}\mathbf{c}_2 - p_{3j}\mathbf{c}_3 - \ldots - p_{j-1,j}\mathbf{c}_{j-1}$ and $p_{ij} = \langle \mathbf{c}_i, \mathbf{b}_j \rangle / \langle \mathbf{c}_i, \mathbf{c}_i \rangle$. We have $\mathbf{c}_1 = \mathbf{b}_1$ so we assume inductively that, for $j \leq k$, $\mathbf{c}_i = \mathbf{b}_i$ for all $i = 1, 2, 3, \ldots, j-1$. Then $p_{ij} = \langle \mathbf{c}_i, \mathbf{b}_j \rangle / \langle \mathbf{c}_i, \mathbf{c}_i \rangle = \langle \mathbf{b}_i, \mathbf{b}_j \rangle / \langle \mathbf{b}_i, \mathbf{b}_i \rangle$ by the induction hypothesis and therefore $p_{ij} = 0$ because $\mathbf{b}_i, \mathbf{b}_j \in S$, which is orthogonal. Therefore $\mathbf{c}_j = \mathbf{b}_j$ and we deduce from the principle of induction that $\mathbf{c}_j = \mathbf{b}_j$ for $j = 1, 2, 3, \ldots, k$. We conclude that $S \subseteq C$ and C is an orthogonal basis of V. ●

For the construction of both Cartesian coordinates and orthogonal matrices, we require orthogonal sets of unit vectors. However, by Proposition 2(ii) of Chapter 10, dividing any vector by its length produces a unit vector, therefore we only need to make sure that applying this operation to the vectors of an orthogonal basis does not destroy the other properties of the basis.

• *Proposition 4*

Let V be a vector space with inner product of finite dimension over $\mathbb{R}$, let $a_1, a_2, a_3, \ldots, a_m$ be non-zero real numbers and let $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_m\}$ be an orthogonal basis of V. Then

(i) $C = \{a_1\mathbf{b}_1, a_2\mathbf{b}_2, a_3\mathbf{b}_3, \ldots, a_m\mathbf{b}_m\}$ is an orthogonal basis of V;
(ii) $D = \{\mathbf{b}_1/\|\mathbf{b}_1\|, \mathbf{b}_2/\|\mathbf{b}_2\|, \mathbf{b}_3/\|\mathbf{b}_3\|, \ldots, \mathbf{b}_m/\|\mathbf{b}_m\|\}$ is an orthonormal basis of V.

PROOF

(i) Suppose that there exist $r_i \in \mathbb{R}$, for $i = 1, 2, 3, \ldots, m$, such that $r_1a_1\mathbf{b}_1 + r_2a_2\mathbf{b}_2 + r_3a_3\mathbf{b}_3 + \ldots + r_ma_m\mathbf{b}_m = \mathbf{0}$. Then, because B is a basis of V and therefore is linearly independent over $\mathbb{R}$, the coefficients $r_ia_i = 0$, for $i = 1, 2, 3, \ldots, m$. Because $a_i \neq 0$ it follows that $r_i = 0$, for $i = 1, 2, 3, \ldots, m$ and therefore C is linearly independent over $\mathbb{R}$. Because B is a basis of V and contains m vectors, $\dim V = m$. Because C is a linearly independent set of m elements in V, C is a basis of V by Proposition 4 of Chapter 3. For $i \neq j$ and $i, j = 1, 2, 3, \ldots, m$, the inner product $\langle a_i\mathbf{b}_i, a_j\mathbf{b}_j \rangle = a_ia_j\langle \mathbf{b}_i, \mathbf{b}_j \rangle$ by Definition 2(iii) of Chapter 10 and therefore $\langle a_i\mathbf{b}_i, a_j\mathbf{b}_j \rangle = 0$ because $\langle \mathbf{b}_i, \mathbf{b}_j \rangle = 0$ for the orthogonal set B

by Definition 5 and Proposition 3 of Chapter 10. Therefore C is an orthogonal set, and consequently C is an orthogonal basis of V.

(ii) Because B is a basis of V, $\mathbf{b}_i \neq \mathbf{0}$ for $i = 1, 2, 3, \ldots, m$, and therefore $\langle \mathbf{b}_i, \mathbf{b}_i \rangle \neq 0$ by Definition 2(v) of Chapter 10. Consequently, by Definition 3 and Proposition 2(ii) of Chapter 10, $\|\mathbf{b}_i\| \neq 0$ and therefore $\mathbf{b}_i / \|\mathbf{b}_i\|$ is a unit vector. It follows from (i) that D is an orthonormal basis of V. ●

The following example brings out some practical consequences of the Gram–Schmidt process (Proposition 2).

○ *Example 4*

Let us complete Example 2 by finding an orthonormal basis of the vector space V of degree 4 over $\mathbb{R}$. Then V has the orthogonal basis C, where

$$C = \left\{ \mathbf{c}_1 = (0, 1, 1, 1), \quad \mathbf{c}_2 = \frac{1}{3}(3, -2, 1, 1), \quad \mathbf{c}_3 = \frac{1}{5}(3, 3, -4, 1) \right\}.$$

The rational factors of two of these vectors make calculation of lengths awkward, so let us use Proposition 4(i) to replace C by the orthogonal basis D of V, where

$$\begin{aligned} D &= \{\mathbf{d}_1 = \mathbf{c}_1, \ \mathbf{d}_2 = 3\mathbf{c}_2, \ \mathbf{d}_3 = 5\mathbf{c}_3\} \\ &= \{\mathbf{d}_1 = (0, 1, 1, 1), \ \mathbf{d}_2 = (3, -2, 1, 1), \ \mathbf{d}_3 = (3, 3, -4, 1)\}. \end{aligned}$$

The lengths of the elements of D are then: $\|\mathbf{d}_1\| = \sqrt{3}$, $\|\mathbf{d}_2\| = \sqrt{15}$ and $\|\mathbf{d}_3\| = \sqrt{35}$. Therefore, by Proposition 2(ii), E is an orthonormal basis of V, where

$$E = \{\mathbf{e}_1 = (0, 1, 1, 1)/\sqrt{3}, \quad \mathbf{e}_2 = (3, -2, 1, 1)/\sqrt{15}, \quad \mathbf{e}_3 = (3, 3, -4, 1)/\sqrt{35}\}.$$

In Theorem 1, the Gram–Schmidt process is applied to a linearly independent set to produce an orthogonal set, which is linearly independent by Proposition 4 of Chapter 10. Now let us see what happens when we apply the process to a linearly dependent set of vectors.

○ *Example 5*

We apply the Gram–Schmidt process to the set of vectors S in $\mathbb{R}^4$, where

$$S = \{\mathbf{v}_1 = (1, 0, 0, 1), \quad \mathbf{v}_2 = (0, 1, 2, -1), \quad \mathbf{v}_3 = (2, 1, 2, 1), \quad \mathbf{v}_4 = (0, 1, 1, 2)\}.$$

We start by taking $\mathbf{w}_1 = \mathbf{v}_1$ and finding $\mathbf{w}_1 \cdot \mathbf{w}_1 = 2$. Then we construct

$$\begin{aligned} \mathbf{w}_2 &= \mathbf{v}_2 - [(\mathbf{w}_1 \cdot \mathbf{v}_2)/(\mathbf{w}_1 \cdot \mathbf{w}_1)]\mathbf{w}_1 \\ &= (0, 1, 2, -1) - \left(-\frac{1}{2}\right)(1, 0, 0, 1) \\ &= \frac{1}{2}(1, 2, 4, -1) \end{aligned}$$

and we find $\mathbf{w}_2 \cdot \mathbf{w}_2 = \frac{11}{2}$. So now we construct

$$\mathbf{w}_3 = \mathbf{v}_3 - [(\mathbf{w}_1 \cdot \mathbf{v}_3)/(\mathbf{w}_1 \cdot \mathbf{w}_1)]\mathbf{w}_1 - [(\mathbf{w}_2 \cdot \mathbf{v}_3)/(\mathbf{w}_2 \cdot \mathbf{w}_2)]\mathbf{w}_2$$
$$= (2, 1, 2, 1) - \frac{3}{2}(1, 0, 0, 1) - \frac{1}{2}(1, 2, 4, -1) = (0, 0, 0, 0) = \mathbf{0},$$

which cannot be used in the Gram–Schmidt process and cannot contribute to a spanning set, so let us ignore it. Instead, we calculate

$$\mathbf{w}_4 = \mathbf{v}_4 - [(\mathbf{w}_1 \cdot \mathbf{v}_4)/(\mathbf{w}_1 \cdot \mathbf{w}_1)]\mathbf{w}_1 - [(\mathbf{w}_2 \cdot \mathbf{v}_4)/(\mathbf{w}_2 \cdot \mathbf{w}_2)]\mathbf{w}_2$$
$$= (0, 1, 1, 2) - 1(1, 0, 0, 1) - \frac{2}{11}(1, 2, 4, -1)$$
$$= \frac{1}{11}(-13, 7, -3, 13).$$

Therefore $T = \{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_4\}$ is an orthogonal basis for the vector space V spanned by S. However, by Proposition 4(i), we can replace T by the more convenient orthogonal basis $U = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3\}$ of V, where $\mathbf{x}_1 = (1, 0, 0, 1)$, $\mathbf{x}_2 = (1, 2, 4, -1)$ and $\mathbf{x}_3 = (-13, 7, -3, 13)$.

TUTORIAL PROBLEM 11.1

Let $S = \{\mathbf{u}, \mathbf{v}\}$ in $\mathbb{R}^n$ be a set of vectors which is linearly independent over $\mathbb{R}$ and let $T = \{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ in $\mathbb{R}^n$ be linearly dependent over $\mathbb{R}$. Find the set of vectors which is obtained by applying the Gram–Schmidt process to T.

Summary

A set of vectors of length 1 is **orthonormal** if every pair of vectors in the set is orthogonal. It was first proved that a matrix $\mathbf{A}$ is **orthogonal** if its set of columns is orthonormal. Because mutually orthogonal sets of vectors are always linearly independent, orthogonal matrices are always non-singular. In fact, it was proved that the determinant of an orthogonal matrix is either 1 or –1. Furthermore, only orthogonal matrices with determinant 1 determine rotations of axes in Cartesian geometry. This is a motive for constructing orthogonal matrices, which can therefore be assembled from orthonormal sets of vectors. The main result in this chapter is the **Gram–Schmidt process**, which gives a sequence of formulae by which a basis B of a subspace V of $\mathbb{R}^n$ is replaced by an **orthogonal basis** C of V, that is, a basis that is an orthogonal set of vectors. Dividing each vector in C by its own length then produces an **orthonormal basis** D of V, that is, an orthogonal basis of unit vectors. Also, if an orthogonal set of vectors S in V is extended to make a basis B of V, the Gram–Schmidt process constructs an orthogonal basis C of V which includes the vectors of S. Furthermore, the Gram–Schmidt process also works with a linearly dependent set to produce an orthogonal set of vectors provided that every zero vector that is produced during the process is immediately rejected.

EXERCISES ON CHAPTER 11

1. Show that the columns of the matrix $\mathbf{A} = \begin{pmatrix} 2 & 1 \\ 2 & -1 \end{pmatrix}$ form an orthogonal set but the

rows of **A** do not. Let **B** be an $n \times n$ matrix over $\mathbb{R}$ in which the columns form an orthonormal set. Prove that the rows of **B** also form an orthonormal set.

2. Show that the set S of vectors given by

$$\left\{\mathbf{v} = (1 \quad 0 \quad 1)^{\mathrm{T}},\ \mathbf{w} = (1 \quad 1 \quad -1)^{\mathrm{T}},\ \mathbf{x} = (-1 \quad 2 \quad 1)^{\mathrm{T}}\right\}$$

is orthogonal. Find an orthogonal matrix **A** such that the columns of **A** are parallel to the vectors **v**, **w**, **x**, respectively.

3. Let $\lambda \in \mathbb{R}$ be an eigenvalue of the orthogonal matrix **A**. Show that $\lambda = \pm 1$. Show that

$\mathbf{B} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is an orthogonal matrix and the eigenvalues of **B** are i and –i.

4. Let **E** be an elementary $n \times n$ matrix which exchanges rows, that is, such that the product **EA** is the matrix **A** with two rows exchanged for every $n \times n$ matrix **A** over $\mathbb{R}$. Prove that **E** is an orthogonal matrix.

Let **P** be an $n \times n$ **permutation matrix**, that is, a matrix such that the product **PA** is the matrix **A** with the order of the rows permuted. Prove that **P** is an orthogonal matrix.

5. Let V be the subspace of $\mathbb{R}^4$ with basis B, where $B = \{(1, 1, 0, 0), (2, 0, 1, -1), (0, -1, 2, 1)\}$. By a direct calculation, find an orthogonal basis C of V such that C contains $(1, 1, 0, 0)$. Use the Gram–Schmidt process to find an orthogonal basis D (possibly equal to C) of V such that D contains $(1, 1, 0, 0)$.

6. Use the Gram–Schmidt process to find an orthogonal basis containing the first vector in the list for each of the following Euclidean vector spaces:

(i) $\langle (1, 1, 1), (2, 1, 1), (1, 3, 5) \rangle$,
(ii) $\langle (1, 2, 2, -1), (0, 1, -1, 2), (0, 0, 1, 3) \rangle$,
(iii) $\langle (0, 0, 2, -1), (3, 1, 0, 0), (0, 1, -1, 0) \rangle$.

7. Find an orthogonal basis of the vector space V of solutions over $\mathbb{R}$ of the linear equation $w - x + y - z = 0$.

8. Use the Gram-Schmidt process to find an orthogonal basis of the vector space over $\mathbb{R}$ spanned by the set S, where

$$S = \{(0, 1, 1, 1), (1, 0, 1, 1), (1, 1, 2, 2), (1, 1, 0, 1), (1, -1, 0, 0)\}.$$

9. Find a vector $\mathbf{y} \in \mathbb{R}^4$ such that $\{\mathbf{u}, \mathbf{v}, \mathbf{w}, \mathbf{y}\}$ is an orthogonal basis of $\mathbb{R}^4$, where **u**, **v**, **w** are the vectors defined in Exercise 6 of Chapter 10.

10. Find an orthonormal basis for each vector space in Exercise 6.

12 · Quadratic Forms and Symmetric Matrices

Outline

This chapter introduces the concept of a 'quadratic form' over a field $\mathbb{F}$ as a homogeneous polynomial of degree 2 over $\mathbb{F}$ and defines its 'associated matrix', which is 'symmetric' in that it is equal to its transpose. The transformation of quadratic forms over $\mathbb{R}$ which are associated with geometrical figures by changes of coordinates is shown to be equivalent to 'orthogonal similarity' of the forms and their associated matrices. The main result is that every quadratic form over $\mathbb{R}$ is orthogonally similar to a quadratic form which is a sum of multiples of squares of the indeterminates.

Introduction

Quadratic forms were introduced briefly in Example 4 of Chapter 1 in a problem concerning Euclidean geometry. In this chapter we shall solve the part of this problem that concerns quadratic forms. However, in the next chapter we shall introduce further problems concerning quadratic forms which require a different approach. We now start by introducing quadratic forms in greater detail in order to define each quadratic form by means of a matrix.

For $i = 1, 2, 3, \ldots, n$, let x_i be an indeterminate over the field $\mathbb{F}$, that is, a symbol which can be replaced by an element of $\mathbb{F}$. The set of polynomials in $x_1, x_2, x_3, \ldots, x_n$ is defined step by step by means of the definition of the set $S[y]$ of polynomials in one indeterminate y over a suitable set of coefficients S. We start with $\mathbb{F}[x_1]$, and if we have already defined $\mathbb{F}[x_1, x_2, x_3, \ldots, x_k]$ then we define $\mathbb{F}[x_1, x_2, x_3, \ldots, x_{k+1}]$ to be $\mathbb{F}[x_1, x_2, x_3, \ldots, x_k][x_{k+1}]$. Because the indeterminate y in $S[y]$ has the property that $sy = ys$ for all $s \in S$, it follows from this definition that $x_i x_{k+1} = x_{k+1} x_i$ for all $i = 1, 2, 3, \ldots, k$. By means of a simple proof by mathematical induction, we deduce from this that in $\mathbb{F}[x_1, x_2, x_3, \ldots, x_n]$ we have $x_i x_j = x_j x_i$ for all $i, j = 1, 2, 3, \ldots, n$. For a polynomial in $\mathbb{F}[x_1, x_2, x_3, \ldots, x_n]$, the degree of a (non-zero) term is the sum of the exponents of the indeterminates occurring in the term. For example, the degree of $10x_2^2 x_5 x_8^3$ is the sum of the three exponents, $2 + 1 + 3 = 6$. The degree of any polynomial in $\mathbb{F}[x_1, x_2, x_3, \ldots, x_n]$ other than the polynomial 0 is the largest degree of any of its terms. A polynomial in $\mathbb{F}[x_1, x_2, x_3, \ldots, x_n]$ is **homogeneous** if every term of the polynomial has the same degree. For example, the polynomial $x_1^3 + 2x_2^2 x_4$ is homogeneous of degree 3. We can now define a quadratic form.

• Definition 1

A **quadratic form** over a field $\mathbb{F}$ in indeterminates $x_1, x_2, x_3, \ldots, x_n$ is a homogeneous polynomial of degree 2 in $\mathbb{F}[x_1, x_2, x_3, \ldots, x_n]$.

A quadratic form, for example $x^2 + 2yz$, can be written as $Q(x, y, z)$. Then the value of $Q(x, y, z)$ for given values of the indeterminates can be written as, for example, $Q(2, 1, 1) = 4$. Also, as for other polynomials, we use the congruence symbol, $\equiv$, to indicate that two quadratic forms are identically equal and we use the equality symbol, $=$, for values of the quadratic form and also to indicate that two quadratic forms in different sets of indeterminates (related by a transformation) are always equal. The notation $Q(x, y, z) = Q(x_1, y_1, z_1)$ can be used to indicate this relationship, but it is often simpler to write $Q = Q_1$, where $Q_1 = Q(x_1, y_1, z_1)$. This is more precise because Q and Q_1 have different coefficients.

⊙ Example 1

Consider the quadratic form Q over $\mathbb{R}$ in the indeterminates x, y, z given by

$$Q \equiv x^2 + 2y^2 + 4z^2 + 6yz + zx + 10xy.$$

The usual method of extracting information from polynomials is to transform the indeterminates in order to incorporate an expression (usually linear) which is important in a practical problem, such as $x + y + 2z$. Also the linear transformation substitution should be non-singular in order to preserve the set of values of the polynomial. For example, if we used the obviously singular transformation $x = x_1$, $y = y_1$, $z = y_1$, then Q would become $Q_1 \equiv x_1^2 + 12y_1^2 + 11x_1y_1$. Then for $x = y = 0$ and $z = 1$ we would have $Q = 4$ but $Q_1 = 0$ (as well as the contradiction that $1 = z = y_1 = 0$).

To include $X = x + y + 2z$ in a transformation we might choose the transformation $X = x + y + 2z$, $Y = y$, $Z = z$ which can be written as

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \mathbf{P}\begin{pmatrix} x \\ y \\ z \end{pmatrix}, \qquad \text{where } \mathbf{P} = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The matrix $\mathbf{P}$ is obviously non-singular, therefore the transformation has the inverse transformation which is $x = X - Y - 2Z$, $y = Y$ and $z = Z$. Therefore,

$$\begin{aligned} Q &= (X - Y - 2Z)^2 + 2Y^2 + 4Z^2 + 6YZ + Z(X - Y - 2Z) + 10Y(X - Y - 2Z) \\ &= X^2 - 7Y^2 + 6Z^2 - 11YZ - 3ZX + 8XY. \end{aligned}$$

We shall consider transformations of quadratic forms of this kind in the next chapter, but here we consider geometrical applications of quadratic forms which require rotation of axes of the form $(X \;\; Y \;\; Z)^{\mathrm{T}} = \mathbf{R}(x \;\; y \;\; z)^{\mathrm{T}}$, where $\mathbf{R}$ is an orthogonal matrix, according to Theorem 1 of Chapter 11.

The way that a singular transformation of variables can give false information is illustrated by the following tutorial problem.

TUTORIAL PROBLEM 12.1

Let the quadratic form Q over $\mathbb{R}$ in the indeterminates x, y, z be given by

$$Q \equiv x^2 + 4y^2 + z^2 - 2yz - 2zx + 4xy.$$

(i) Transform Q by the transformation $x = 2x_1 - y_1$, $y = -x_1 + y_1$, $z = x_1 - z_1$ into the quadratic form $Q_1(x_1, y_1, z_1)$. Show that if $x_1 = 0$ then $Q_1 > 0$ unless $y_1 = z_1 = 0$.

(ii) Transform Q by the transformation $x = -x_2 + 3y_2 - 3z_2$, $y = x_2 - 2y_2 + 2z_2$, $z = y_2 - z_2$ into the quadratic form Q_2 in the indeterminates x_2, y_2, z_2. Show that $Q_2 = 0$ if $x_2 - 2y_2 + 2z_2 = 0$.

(iii) By evaluating $Q(0, 0, 1)$ by using the transformations, or otherwise, show that (i) and (ii) give inconsistent results. Determine which of the transformations is singular.

The discussion in Example 1 leads to the following question.

QUESTION 1

Let Q be a quadratic form over $\mathbb{R}$. Does there exist an orthogonal matrix $\mathbf{P}$ such that transformation of the indeterminates by means of $\mathbf{P}$ transforms Q into a sum of multiples of squares of the new indeterminates?

Question 1 resembles Question 2 of Chapter 6, which asks if every square matrix is diagonalizable. In order to use the work on that question, we now try to determine each quadratic form by a suitable matrix.

○ *Example 2*

Because $Q \equiv x^2 + 2y^2 + 4z^2 + 6yz + zx + 10xy$ is quadratic, to obtain a matrix expression, we need to multiply a suitable matrix $\mathbf{A}$ twice by column vectors like $\mathbf{v} = (x \quad y \quad z)^{\mathrm{T}}$. To do this we multiply $\mathbf{A}$ on the right by $\mathbf{v}$ and then on the left by $\mathbf{v}^{\mathrm{T}}$. We start by isolating the factor $\mathbf{v}^{\mathrm{T}}$ on the left, which gives us

$$\begin{aligned} Q &\equiv x(x + ay + bz) + y(cx + 2y + dz) + z(ex + fy + 4z) \\ &\equiv \mathbf{v}^{\mathrm{T}}(x + ay + bz \quad cx + 2y + dz \quad ex + fy + 4z)^{\mathrm{T}} \\ &\equiv \mathbf{v}^{\mathrm{T}}\mathbf{A}\mathbf{v}, \end{aligned}$$

where $d + f = 6$, $b + e = 1$ and $a + c = 10$ and

$$\mathbf{A} = \begin{pmatrix} 1 & a & b \\ c & 2 & d \\ e & f & 4 \end{pmatrix}.$$

This construction has given us too wide a choice of matrices $\mathbf{A}$ such that $Q \equiv \mathbf{v}^{\mathrm{T}}\mathbf{A}\mathbf{v}$, so we choose a matrix $\mathbf{A}$ which is determined by Q and is easy to work with. We know from Example 5 of Chapter 6 that triangular matrices cannot always be diagonalized, so such a matrix would be a poor choice. The other simple choice is to make the two coefficients in each sum equal, that is: $d = f = 3$, $b = e = \frac{1}{2}$ and $a = c = 5$. This is unique for the choice of $\mathbf{v}$ and has the advantage of giving symmetry to the expressions in (for example) xy and yx. This leads to the choice of

$$\mathbf{A} = \begin{pmatrix} 1 & 5 & \frac{1}{2} \\ 5 & 2 & 3 \\ \frac{1}{2} & 3 & 4 \end{pmatrix}.$$

The matrix **A** also has the property that $\mathbf{A}^T = \mathbf{A}$, which is an advantage when applying orthogonal matrices, as in Question 1. We give a name to this property.

• Definition 2

Let **A** be a square matrix over a field $\mathbb{F}$. Then **A** is **symmetric** if $\mathbf{A}^T = \mathbf{A}$, or **A** is **skew-symmetric** if $\mathbf{A}^T = -\mathbf{A}$.

Although skew-symmetric matrices are important in some applications, they appear only in exercises in this book.

Note that the construction of the symmetric matrix **A** in Example 2 required division by 2. As we have all used division by 2 since the age of 5 without ever having been struck by lightning or engulfed by earthquakes, an example is needed to explain why this creates a difficulty.

○ Example 3

Digital computers check their calculations by keeping track of whether integers in them are odd or even. The methods of doing this are based on the use of the field $\mathbb{Z}_2$ of **integers modulo 2**, which has two elements 'even', written 0, and 'odd', written 1. The rule that 'even times odd is even' is then written as $0 \times 1 = 0$, and the rule that 'odd plus odd is even' is written $1 + 1 = 0$. The second equation creates the problem. $\mathbb{Z}_2$ is a field which can be incorporated in larger fields which are used in computing and elsewhere, such as the field $\mathbb{Z}_2(x)$ of rational functions in the indeterminate x over $\mathbb{Z}_2$. To avoid such fields, we insist that all quadratic forms be over fields which satisfy the following condition.

• Definition 3

A field $\mathbb{F}$ is **not of characteristic 2** if $1 + 1 \neq 0$ in $\mathbb{F}$.

Of course, the fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are not of characteristic 2, consequently we can continue to regard them as the principal examples.

• Proposition 1

Let $\mathbb{F}$ be a field which is not of characteristic 2 and let Q be a quadratic form in the n indeterminates $x_1, x_2, x_3, \ldots, x_n$ over $\mathbb{F}$. Then there exists a symmetric $n \times n$ matrix **A** over $\mathbb{F}$, called the **matrix associated with** Q, such that $Q \equiv \mathbf{x}^T\mathbf{A}\mathbf{x}$, where $\mathbf{x} = (x_1 \ x_2 \ \ldots \ x_n)^T$.

PROOF

By Definition 1, Q is a homogeneous polynomial of degree 2 over $\mathbb{F}$, therefore there exist the elements $b_{jk} \in \mathbb{F}$, for $j, k = 1, 2, 3, \ldots, n$ such that $Q \equiv \sum_{j=1}^{n} \sum_{k=1}^{n} b_{jk} x_j x_k$.

We can rearrange these sums as $Q \equiv \sum_{j=1}^{n} b_{jj}x_j^2 + \sum_{j=1}^{n}\sum_{k=1}^{j-1}(b_{jk} + b_{kj})x_j x_k$. We define $a_{jk} \in \mathbb{F}$ by $a_{jj} = b_{jj}$ and $a_{jk} = a_{kj} = (b_{jk} + b_{kj})/2$, for $j, k = 1, 2, 3, \ldots, n$ and $k \neq j$, where division by 2 is possible because $\mathbb{F}$ is not of characteristic 2. Let us define $\mathbf{A} = (a_{jk})$. Then

$$\begin{aligned} Q &\equiv +\sum_{j=1}^{n} a_{jj}x_j^2 \sum_{j=1}^{n}\sum_{k=1}^{j-1}(a_{jk} + a_{kj})x_j x_k \\ &\equiv \sum_{j=1}^{n}\sum_{k=1}^{n} a_{jk}x_j x_k \\ &\equiv \sum_{j=1}^{n}\left[x_j \sum_{k=1}^{n} a_{jk}x_k\right] \\ &\equiv (x_1 \quad x_2 \quad x_3 \quad \ldots \quad x_n)\left(\sum_{k=1}^{n} a_{jk}x_k\right) \\ &\equiv \mathbf{x}^{\mathrm{T}}(a_{jk})(x_1 \quad x_2 \quad x_3 \quad \ldots \quad x_n)^{\mathrm{T}} \\ &\equiv \mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x}. \end{aligned}$$

●

Because the associated matrix **A** is unique for the quadratic form Q (for a given ordering of the indeterminates), the properties of **A** can be ascribed to Q. For example, the **rank** of Q is the rank of **A**. In this way we can call a sum of multiples of squares of indeterminates a **diagonal (quadratic) form** because it is associated with a diagonal matrix. For example,

$$Q_1 \equiv ax^2 + by^2 + cz^2 \equiv \mathbf{x}^{\mathrm{T}}\mathbf{D}\mathbf{x} \qquad \text{where } \mathbf{D} = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}.$$

Of particular interest are those properties of a quadratic form Q which are the same for all the quadratic forms into which Q can be transformed by non-singular transformations. Another consequence of Proposition 1 is that the problems about quadratic forms in this chapter can be regarded as problems concerning symmetric matrices over $\mathbb{R}$.

TUTORIAL PROBLEM 12.2

Find all possible symmetric matrices associated with the quadratic form $Q \equiv x^2 + 3xy + 5y^2 - 2yz - z^2$ in x, y, z over $\mathbb{R}$.

In order to be able to study quadratic forms by means of their associated symmetric matrices, we need to know the effect of non-singular transformation of indeterminates on the matrices.

• Proposition 2

Let Q be a quadratic form $\mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x}$ with associated symmetric matrix **A** of rank r and column vector **x** of indeterminates over the field $\mathbb{F}$, which is not of characteristic 2. Let Q_1 be the form in indeterminates which are elements of the column vector **y** into which Q is transformed by a non-singular transformation over $\mathbb{F}$. Then there exists a

non-singular matrix $\mathbf{P}$ over $\mathbb{F}$ such that Q_1 has associated matrix $\mathbf{P}^T\mathbf{AP}$, the **conjugate** of $\mathbf{A}$ by $\mathbf{P}$, and rank $\mathbf{P}^T\mathbf{AP} = r$.

PROOF

Because the transformation of indeterminates over $\mathbb{F}$ is non-singular, there exists a non-singular matrix over $\mathbb{F}$ which we write as $\mathbf{P}^{-1}$ such that $\mathbf{y} = \mathbf{P}^{-1}\mathbf{x}$. Therefore $\mathbf{x} = \mathbf{Py}$ and $Q \equiv \mathbf{x}^T\mathbf{Ax} \equiv (\mathbf{Py})^T\mathbf{A}(\mathbf{Py}) \equiv \mathbf{y}^T\mathbf{P}^T\mathbf{APy} \equiv \mathbf{y}^T(\mathbf{P}^T\mathbf{AP})\mathbf{y} \equiv Q_1$. Because $\mathbf{A}$ is symmetric, $(\mathbf{P}^T\mathbf{AP})^T = \mathbf{P}^T\mathbf{A}^T\mathbf{P} = \mathbf{P}^T\mathbf{AP}$ therefore $\mathbf{P}^T\mathbf{AP}$ is symmetric over $\mathbb{F}$. Consequently, by Proposition 1, Q_1 is a quadratic form over $\mathbb{F}$ with associated matrix $\mathbf{P}^T\mathbf{AP}$. It follows from Theorem 6 of Chapter 4 that the rank of a product of a matrix $\mathbf{M}$ with a non-singular matrix is the rank of $\mathbf{M}$, therefore rank $\mathbf{P}^T\mathbf{AP}$ = rank $\mathbf{A} = r$. ●

Proposition 2 converts the operation of transforming the indeterminates of a quadratic form Q into the operation of replacing the associated matrix $\mathbf{A}$ of Q by its conjugate $\mathbf{P}^T\mathbf{AP}$ by a non-singular matrix $\mathbf{P}$. However, the main question of this chapter concerns transforming Q by an orthogonal matrix $\mathbf{P}$, when $\mathbf{P}^T = \mathbf{P}^{-1}$, by Proposition 1(ii) of Chapter 11. Therefore the conjugate $\mathbf{P}^T\mathbf{AP}$ is the matrix $\mathbf{P}^{-1}\mathbf{AP}$, which is similar to $\mathbf{A}$. We give a name to this relationship.

• Definition 4

Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times n$ matrices over $\mathbb{R}$. Then $\mathbf{B}$ is **orthogonally similar** to $\mathbf{A}$ if there exists an orthogonal $n \times n$ matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{B}$.

Proposition 2 and Definition 4 allow us to translate Question 1 into the following question about matrices.

QUESTION 2

Let $\mathbf{A}$ be a symmetric matrix over $\mathbb{R}$. Is $\mathbf{A}$ orthogonally similar to a diagonal matrix over $\mathbb{R}$?

The Gram–Schmidt process can be used to replace a linearly independent set of vectors by an orthonormal set of vectors, which suggests that we can try to answer Question 2 for a symmetric matrix $\mathbf{A}$ over $\mathbb{R}$ by modifying the construction of a non-singular matrix $\mathbf{P}$ over $\mathbb{R}$ such that $\mathbf{P}^{-1}\mathbf{AP}$ is diagonal. However, this raises three questions about symmetric matrices over $\mathbb{R}$, which we shall answer in turn. The first question is this: do the eigenvalues of a symmetric matrix $\mathbf{A}$ over $\mathbb{R}$ belong to $\mathbb{R}$? If not, $\mathbf{A}$ cannot be similar to a diagonal matrix $\mathbf{D}$ over $\mathbb{R}$, because the diagonal elements are the eigenvalues of $\mathbf{A}$ by Theorem 3 of Chapter 6.

• Theorem 1

Every eigenvalue of a symmetric matrix over $\mathbb{R}$ belongs to $\mathbb{R}$.

PROOF

Let $\mathbf{A}$ be an $n \times n$ symmetric matrix over $\mathbb{R}$. The characteristic polynomial $\chi(\lambda)$ of $\mathbf{A}$ is over $\mathbb{R}$, therefore its eigenvalues belong to $\mathbb{C}$, by the fundamental theorem of algebra. We shall use complex conjugates of the eigenvalues to show that their imaginary parts are zero.

Let $\lambda \in \mathbb{C}$ be an eigenvalue of $\mathbf{A}$. Then, by Definition 2 of Chapter 6, there exists $\mathbf{0} \neq \mathbf{u} \in \mathbb{C}^n$ such that $\mathbf{Au} = \lambda\mathbf{u}$. Then $\overline{\mathbf{Au}} = \overline{\lambda\mathbf{u}}$, by which we mean that the complex conjugate is taken for each element in $\mathbf{Au}$ and $\lambda\mathbf{u}$. Because $\overline{wz} = \overline{w}\,\overline{z}$ for all $w, z \in \mathbb{C}$, this equation implies that $\overline{\mathbf{A}}\,\overline{\mathbf{u}} = \overline{\lambda}\,\overline{\mathbf{u}}$ and therefore, because $\mathbf{A}$ is over $\mathbb{R}$, that $\mathbf{A}\overline{\mathbf{u}} = \overline{\lambda}\overline{\mathbf{u}}$. By the rules for forming the transposition of products, we deduce that $\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}} = \overline{\lambda}\,\overline{\mathbf{u}}^{\mathrm{T}}$ and thence $\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{A} = \overline{\lambda}\,\overline{\mathbf{u}}^{\mathrm{T}}$, by Definition 2, because $\mathbf{A}$ is symmetric. Now we multiply $\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{A}$ on the right by $\mathbf{u}$ and obtain $\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{Au} = \overline{\lambda}\,\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{u}$. However, we can also obtain $\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{Au}$, by multiplying $\mathbf{Au} = \lambda\mathbf{u}$ on the left by $\overline{\mathbf{u}}^{\mathrm{T}}$. This gives us $\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{Au} = \lambda\,\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{u}$ and therefore the two equations give us $\overline{\lambda}\,\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{u} = \lambda\,\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{u}$. Therefore $(\lambda - \overline{\lambda})\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{u} = 0$, so we wish to show that $\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{u} \neq 0$. Because $\mathbf{u} = (u_1 \;\; u_2 \;\; u_3 \;\; \ldots \;\; u_n)^{\mathrm{T}} \neq \mathbf{0}$, at least one $u_j \neq 0$ for $j = 1, 2, 3, \ldots, n$. Also $\overline{\mathbf{u}}^{\mathrm{T}} = (\overline{u}_1 \;\; \overline{u}_2 \;\; \overline{u}_3 \;\; \ldots \;\; \overline{u}_n)$ and therefore we have

$$\begin{aligned}\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{u} &= \overline{u}_1u_1 + \overline{u}_2u_2 + \overline{u}_3u_3 + \ldots + \overline{u}_nu_n \\ &= |u_1|^2 + |u_2|^2 + |u_3|^2 + \ldots + |u_n|^2,\end{aligned}$$

for which each term is non-negative and $|u_j|^2 > 0$. Therefore $\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{u} \neq 0$ and consequently $\lambda - \overline{\lambda} = 0$. We conclude that $\lambda \in \mathbb{R}$, so every eigenvalue of $\mathbf{A}$ is in $\mathbb{R}$. ●

In our attempt to answer Question 2, we shall use the Gram–Schmidt process to construct orthogonal sets of eigenvectors associated with a given eigenvalue. As we are seeking an orthonormal set of columns for an orthogonal matrix, we require the eigenvectors associated with different eigenvalues to be orthogonal. Consequently, our second question is this: do two eigenvectors which are associated with different eigenvalues of a symmetric matrix over $\mathbb{R}$ form an orthogonal pair? This question can easily be answered directly.

• *Proposition 3*

Let $\mathbf{A}$ be a symmetric matrix over $\mathbb{R}$, let λ and μ be distinct eigenvalues of $\mathbf{A}$, let $\mathbf{u}$ be an eigenvector associated with λ and $\mathbf{v}$ be an eigenvector associated with μ. Then $\{\mathbf{u}, \mathbf{v}\}$ is orthogonal.

PROOF

Because $\mathbf{v}$ is an eigenvector of $\mathbf{A}$ associated with μ, by Definition 2 of Chapter 6, $\mathbf{Av} = \mu\mathbf{v}$ therefore $\mathbf{u}^{\mathrm{T}}\mathbf{Av} = \mu\mathbf{u}^{\mathrm{T}}\mathbf{v}$. By taking the transpose, $(\mathbf{u}^{\mathrm{T}}\mathbf{Av})^{\mathrm{T}} = \mu(\mathbf{u}^{\mathrm{T}}\mathbf{v})^{\mathrm{T}}$ therefore $\mathbf{v}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}\mathbf{u} = \mathbf{v}^{\mathrm{T}}\mathbf{Au} = \mu\mathbf{v}^{\mathrm{T}}\mathbf{u}$, as $\mathbf{A}$ is symmetric. Also $\mathbf{u}$ is an eigenvector of $\mathbf{A}$ associated with the eigenvalue λ, therefore $\mathbf{Au} = \lambda\mathbf{u}$ and thence $\mathbf{v}^{\mathrm{T}}\mathbf{Au} = \lambda\mathbf{v}^{\mathrm{T}}\mathbf{u}$. It follows that $\lambda\mathbf{v}^{\mathrm{T}}\mathbf{u} = \mu\mathbf{v}^{\mathrm{T}}\mathbf{u}$ and $(\lambda - \mu)\mathbf{v}^{\mathrm{T}}\mathbf{u} = 0$. Then $\mathbf{v}^{\mathrm{T}}\mathbf{u} = 0$ because $\lambda \neq \mu$, and therefore the pair of eigenvectors $\mathbf{u}$ and $\mathbf{v}$ are orthogonal by Proposition 3 of Chapter 10. ●

The final problem concerning Question 2 is whether, for a symmetric matrix **A** over $\mathbb{R}$, every k times repeated eigenvalue of **A** has a subspace of associated eigenvectors of dimension k over $\mathbb{R}$. By Theorem 3 of Chapter 7, this is necessary for **A** to be diagonalizable. Although Theorem 2, which gives a positive answer to Question 2, uses neither the answer to this problem nor Proposition 3, these are both needed for the method of construction which is given later. We now answer Question 2 by means of a proof by mathematical induction which hides the details of the construction of the orthogonal matrix.

• *Theorem 2*

Every symmetric matrix over $\mathbb{R}$ is orthogonally similar to a diagonal matrix over $\mathbb{R}$.

PROOF

The theorem is trivially true for all 1×1 symmetric matrices over $\mathbb{R}$. Let us assume inductively that the theorem holds for all $(n-1) \times (n-1)$ symmetric matrices over $\mathbb{R}$.

Let **A** be an $n \times n$ symmetric matrix over $\mathbb{R}$ and let λ be an eigenvalue of **A**. Then $\lambda \in \mathbb{R}$ by Theorem 1 therefore **A** has an eigenvector $\mathbf{f}_1 \in \mathbb{R}^n$, where $\mathbf{f}_1 \neq \mathbf{0}$ by Definition 2 of Chapter 6. It follows that $\{\mathbf{f}_1\}$ is a linearly independent subset of $\mathbb{R}^n$ and therefore there exists a basis $F = \{\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \ldots, \mathbf{f}_n\}$ of $\mathbb{R}^n$ which contains $\{\mathbf{f}_1\}$, by Proposition 5 of Chapter 3. By Proposition 2 of Chapter 11, the Gram–Schmidt process changes F into an orthogonal basis $G = \{\mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3, \ldots, \mathbf{g}_n\}$ of $\mathbb{R}^n$ for which $\mathbf{g}_1 = \mathbf{f}_1$ and so $\mathbf{g}_1$ is an eigenvector of **A** associated with λ. Now define $\mathbf{h}_j = \mathbf{g}_j / \sqrt{\mathbf{g}_j \cdot \mathbf{g}_j}$, for $j = 1, 2, 3, \ldots, n$ to construct an orthonormal basis $H = \{\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3, \ldots, \mathbf{h}_n\}$ of $\mathbb{R}^n$, by Proposition 4(ii) of Chapter 11. Also $\mathbf{h}_1$ is an eigenvector of **A** associated with λ because it is a non-zero multiple of an eigenvector. Let us regard the vectors in H as column vectors and construct $\mathbf{S} = (\mathbf{h}_j)$ as the $n \times n$ matrix with columns $\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3, \ldots, \mathbf{h}_n$. By Proposition 1(iv) of Chapter 11, **S** is an orthogonal matrix. Hence, by Proposition 1(ii) of Chapter 11, $\mathbf{S}^{-1} = \mathbf{S}^{\mathrm{T}}$.

Therefore $\mathbf{S}^{-1}$ is the matrix of which the rows are $\mathbf{h}_j^{\mathrm{T}}$ for $j = 1, 2, 3, \ldots, n$, and consequently

$$\mathbf{S}^{-1}\mathbf{A}\mathbf{S} = (\mathbf{h}_j^{\mathrm{T}})\mathbf{A}(\mathbf{h}_k) = (\mathbf{h}_j^{\mathrm{T}})(\mathbf{A}\mathbf{h}_k) = (\mathbf{h}_j^{\mathrm{T}}\mathbf{A}\mathbf{h}_k).$$

Here the formula gives the term in the jth row and kth column of $\mathbf{S}^{-1}\mathbf{A}\mathbf{S}$. Because $\mathbf{h}_1$ is an eigenvector of **A** associated with λ, $\mathbf{A}\mathbf{h}_1 = \lambda\mathbf{h}_1$, therefore, for $j = 1, 2, 3, \ldots, n$, $\mathbf{h}_j^{\mathrm{T}}\mathbf{A}\mathbf{h}_1 = \lambda\mathbf{h}_j^{\mathrm{T}}\mathbf{h}_1 = \lambda\delta_{j1}$ by Definition 5 of Chapter 10. Therefore $\mathbf{S}^{-1}\mathbf{A}\mathbf{S} = \begin{pmatrix} \lambda & \mathbf{r}^{\mathrm{T}} \\ \mathbf{0} & \mathbf{B} \end{pmatrix}$, where **B** is an $(n-1) \times (n-1)$ matrix over $\mathbb{R}$ and the elements of $\mathbf{r}^{\mathrm{T}}$ are $r_j = \mathbf{h}_1^{\mathrm{T}}\mathbf{A}\mathbf{h}_j$ for $j = 2, 3, \ldots, n$. But r_j is a 1×1 matrix, therefore $r_j = r_j^{\mathrm{T}} = (\mathbf{h}_1^{\mathrm{T}}\mathbf{A}\mathbf{h}_j)^{\mathrm{T}} = \mathbf{h}_j^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}\mathbf{h}_1$ $= \mathbf{h}_j^{\mathrm{T}}\mathbf{A}\mathbf{h}_1$ because **A** is symmetric. The previous calculation then gives $r_j = \lambda\delta_{j1} = 0$ for $j = 2, 3, \ldots, n$, therefore $\mathbf{S}^{-1}\mathbf{A}\mathbf{S} = \begin{pmatrix} \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix}$. Because $\mathbf{S}^{-1} = \mathbf{S}^{\mathrm{T}}$ and $\mathbf{A}^{\mathrm{T}} = \mathbf{A}$, $(\mathbf{S}^{-1}\mathbf{A}\mathbf{S})^{\mathrm{T}} = (\mathbf{S}^{\mathrm{T}}\mathbf{A}\mathbf{S})^{\mathrm{T}} = \mathbf{S}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}\mathbf{S} = \mathbf{S}^{-1}\mathbf{A}\mathbf{S}$. Also, by Theorem 4 of Chapter 2,

$(\mathbf{S}^{-1}\mathbf{AS})^{\mathrm{T}} = \begin{pmatrix} \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^{\mathrm{T}} \end{pmatrix}$ and consequently $\begin{pmatrix} \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^{\mathrm{T}} \end{pmatrix} = \begin{pmatrix} \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix}$. We conclude that $\mathbf{B}^{\mathrm{T}} = \mathbf{B}$. Therefore $\mathbf{B}$ is an $(n-1) \times (n-1)$ symmetric matrix over $\mathbb{R}$.

By the induction hypothesis, there exists an $(n-1) \times (n-1)$ orthogonal matrix $\mathbf{R}$ such that $\mathbf{R}^{-1}\mathbf{BR} = \mathbf{R}^{\mathrm{T}}\mathbf{BR} = \mathbf{D}$, where $\mathbf{D}$ is a diagonal matrix over $\mathbb{R}$.

Let $\mathbf{P} = \mathbf{S}\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}$. Then

$$\mathbf{P}^{\mathrm{T}}\mathbf{P} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}^{\mathrm{T}} \mathbf{S}^{\mathrm{T}}\mathbf{S} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}^{\mathrm{T}} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}$$

because $\mathbf{S}^{\mathrm{T}} = \mathbf{S}^{-1}$. Therefore, by Theorem 4 of Chapter 2,

$$\mathbf{P}^{\mathrm{T}}\mathbf{P} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R}^{\mathrm{T}} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R}^{\mathrm{T}}\mathbf{R} \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} = \mathbf{I},$$

as $\mathbf{R}$ is orthogonal. We conclude that $\mathbf{P}$ is an orthogonal $n \times n$ matrix and $\mathbf{P}^{-1} = \mathbf{P}^{\mathrm{T}}$.

Therefore

$$\mathbf{P}^{-1}\mathbf{AP} = \mathbf{P}^{\mathrm{T}}\mathbf{AP} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R}^{\mathrm{T}} \end{pmatrix} \mathbf{S}^{\mathrm{T}}\mathbf{AS} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}.$$

Thence,

$$\mathbf{P}^{-1}\mathbf{AP} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R}^{\mathrm{T}} \end{pmatrix} \begin{pmatrix} \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix} = \begin{pmatrix} \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{R}^{\mathrm{T}}\mathbf{BR} \end{pmatrix} = \begin{pmatrix} \lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{D} \end{pmatrix},$$

by earlier working. Because the final matrix is a diagonal matrix over $\mathbb{R}$, the $n \times n$ matrix $\mathbf{A}$ is orthogonally similar to a diagonal matrix over $\mathbb{R}$. The truth of the theorem then follows by the principle of mathematical induction. ●

There is no need to find the orthogonal matrix $\mathbf{P}$ which transforms a quadratic form over $\mathbb{R}$ (or its associated symmetric matrix) into diagonal form when the diagonal form is all that is required because the diagonal elements are determined by the following result.

• Proposition 4

Let Q be a quadratic form in n indeterminates over $\mathbb{R}$. Then there exists an orthogonal transformation of the indeterminates such that $Q = \lambda_1 y_1^2 + \lambda_2 y_2^2 + \lambda_3 y_3^2 + \ldots + \lambda_n y_n^2$, where $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n$ are the eigenvalues of the symmetric matrix associated with Q.

PROOF

Let the n indeterminates be the elements of the column vector $\mathbf{x}$. Then, by Proposition 1, there exists a symmetric matrix $\mathbf{A}$ over $\mathbb{R}$ such that $Q \equiv \mathbf{x}^{\mathrm{T}}\mathbf{Ax}$. By Theorem 2, there exists an orthogonal matrix $\mathbf{P}$ such that $\mathbf{P}^{\mathrm{T}}\mathbf{AP} = \mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$, where $\mathbf{D}$ is a diagonal matrix over $\mathbb{R}$. By Theorem 3 of Chapter 6, the diagonal elements of $\mathbf{D}$ are the eigen-

values of **A**. We write the transformation of indeterminates in the form $\mathbf{x} = \mathbf{Py}$, where the column vector $\mathbf{y} = (y_1 \quad y_2 \quad y_3 \quad \ldots \quad y_n)^T$. Then we obtain

$$Q \equiv \mathbf{x}^T\mathbf{Ax} = \mathbf{y}^T\mathbf{P}^T\mathbf{APy} = \mathbf{y}^T\mathbf{Dy} = \mathbf{y}^T(\lambda_1 y_1 \quad \lambda_2 y_2 \quad \lambda_3 y_3 \quad \ldots \quad \lambda_n y_n)^T$$
$$= \lambda_1 y_1^2 + \lambda_2 y_2^2 + \lambda_3 y_3^2 + \ldots + \lambda_n y_n^2. \quad \bullet$$

If the problem in which a quadratic form Q occurs requires a knowledge of the transformation which converts Q into a diagonal form, the proof of Theorem 2 provides a method which is too long and indirect. The following more direct construction is used instead. However, as the construction is unrelated to the proof, the description includes references which justify some of its steps.

• Construction 1

The following procedure constructs an orthogonal transformation of indeterminates which transforms a quadratic form Q in n indeterminates over $\mathbb{R}$ into a diagonal form over $\mathbb{R}$.

(1) Choose an order for the indeterminates, which we write here as $x_1, x_2, x_3, \ldots, x_n$, and form the column vector $\mathbf{x} = (x_1 \quad x_2 \quad x_3 \quad \ldots \quad x_n)^T$.

(2) Find the unique symmetric $n \times n$ matrix **A** over $\mathbb{R}$ such that $Q = \mathbf{x}^T\mathbf{Ax}$ by the method in the proof of Proposition 1, as in Example 2.

(3) Find the eigenvalues of **A**, which are in $\mathbb{R}$ by Theorem 1.

(4) For each unrepeated eigenvalue μ of **A**, find a real eigenvector $\mathbf{b}_\mu$ to form a basis of the vector space of eigenvectors associated with μ by Proposition 1 of Chapter 7. Then, by Proposition 3, $\mathbf{b}_\mu$ is orthogonal to all eigenvectors associated with other eigenvalues.

(5) For each repeated eigenvalue ν of **A**, which we assume is repeated k_ν times, find a basis B_ν of the vector space V_ν of eigenvectors associated with ν. Then by Theorem 3 of Chapter 7, $\dim V_\nu = k_\nu$ because **A** is diagonalizable over $\mathbb{R}$ by Theorem 2.

(6) Apply the Gram–Schmidt process to B_ν to construct a basis C_ν of V_ν; C_ν is an orthogonal basis of V_ν by Proposition 2 of Chapter 11.

(7) Let $D = \{\mathbf{b}_\mu, C_\nu : \chi(\mu) = 0, \chi(\nu) = 0\}$, where $\chi(\lambda)$ is the characteristic polynomial of **A**. D is orthogonal by construction, hence D is linearly independent over $\mathbb{R}$ by Proposition 4 of Chapter 10. The number of vectors in D is n, the total number of roots of $\chi(\lambda)$, therefore D is an orthogonal basis of $\mathbb{R}^n$, by Proposition 3 of Chapter 3.

(8) Divide each vector in D by its length to construct the orthonormal basis E of $\mathbb{R}^n$, by Proposition 4(ii) of Chapter 11.

(9) Define $\mathbf{P} = (\mathbf{e}_1 \quad \mathbf{e}_2 \quad \mathbf{e}_3 \quad \ldots \quad \mathbf{e}_n)$, where $E = \{\mathbf{e}_j : j = 1, 2, 3, \ldots, n\}$. Then **P** is orthogonal by Proposition 1(iv) of Chapter 11 and $\mathbf{P}^T\mathbf{AP} = \mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$ is a diagonal matrix over $\mathbb{R}$ by Theorem 3 of Chapter 7. Also $\mathbf{x} = \mathbf{Py}$ transforms $\mathbf{x}^T\mathbf{Ax}$ into the diagonal form $\mathbf{y}^T\mathbf{Dy}$, by Proposition 2.

Even without the references which form the proofs that the steps are effective, Construction 1 looks very long. However, the only difficult step is the finding of the eigenvalues

of the symmetric matrix **A**. It is true that the large number of steps gradually complicates the arithmetic, but the construction is not too difficult in practice.

○ Example 4

Let us find an orthogonal transformation of indeterminates which transforms the quadratic form

$$Q \equiv -x^2 + 2y^2 - z^2 + 4xy + 8zx - 4yz.$$

into a diagonal form.

(1) Let us choose alphabetical order for the indeterminates, and therefore write $\mathbf{x} = (x \;\; y \;\; z)^{\mathrm{T}}$.

(2) After finding a few symmetric matrices associated with quadratic forms by the method of Example 2, the pattern of the matrix becomes clear and the matrix can be written down immediately. With x as chosen in (1), the coefficients of x^2, y^2 and z^2 are the diagonal elements of the associated symmetric matrix **A** while half the coefficients of xy and xz are the elements in the first row and first column of **A**, and so on. Then $Q \equiv \mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x}$, where $\mathbf{A} = \begin{pmatrix} -1 & 2 & 4 \\ 2 & 2 & -2 \\ 4 & -2 & -1 \end{pmatrix}$. (After calculating a few of them, the associated matrix for a given quadratic can be written down immediately.)

(3) The roots of the characteristic polynomial of **A** satisfy

$$\chi(\lambda) = \det(\mathbf{A} - \lambda\mathbf{I}) = \begin{vmatrix} -1-\lambda & 2 & 4 \\ 2 & 2-\lambda & -2 \\ 4 & -2 & -1-\lambda \end{vmatrix} = 0.$$

By adding row 1 to row 3 of the determinant then dividing the new row 3 by $3 - \lambda$, we obtain

$$\chi(\lambda) = \begin{vmatrix} -1-\lambda & 2 & 4 \\ 2 & 2-\lambda & -2 \\ 3-\lambda & 0 & 3-\lambda \end{vmatrix} = (3-\lambda)\begin{vmatrix} -1-\lambda & 2 & 4 \\ 2 & 2-\lambda & -2 \\ 1 & 0 & 1 \end{vmatrix}.$$

Evaluating the last determinant by row 3 then gives

$$\chi(\lambda) = (3-\lambda)\left[1\begin{vmatrix} 2 & 4 \\ 2-\lambda & -2 \end{vmatrix} + 1\begin{vmatrix} -1-\lambda & 2 \\ 2 & 2-\lambda \end{vmatrix}\right]$$

$$= (3-\lambda)(\lambda^2 + 3\lambda - 18) = (3-\lambda)(\lambda-3)(\lambda+6).$$

Therefore the eigenvalues of **A** are –6, 3, 3.

(4) The only unrepeated eigenvalue of **A** is –6, so we require an eigenvector associated with –6. This is a solution of the system of linear equations with matrix of coefficients

$$\mathbf{A}+6\mathbf{I}=\begin{pmatrix}5&2&4\\2&8&-2\\4&-2&5\end{pmatrix}\sim\begin{pmatrix}5&2&4\\1&4&-1\\4&-2&5\end{pmatrix}\sim\begin{pmatrix}1&4&-1\\5&2&4\\4&-2&5\end{pmatrix}$$
$$\sim\begin{pmatrix}1&4&-1\\0&-18&9\\0&-18&9\end{pmatrix}\sim\begin{pmatrix}1&4&-1\\0&-18&9\\0&0&0\end{pmatrix}\sim\begin{pmatrix}1&4&-1\\0&-2&1\\0&0&0\end{pmatrix}.$$

The third unknown is disposable, therefore it is the parameter $0\neq\theta\in\mathbb{R}$, which gives the solutions $\theta(-1\quad\frac{1}{2}\quad 1)^{\mathrm{T}}$. We choose the convenient value $\theta=2$ and therefore find the eigenvector $\mathbf{b}_{-6}=(-2\quad 1\quad 2)^{\mathrm{T}}$.

(5) The only repeated eigenvalue of $\mathbf{A}$ is the double eigenvalue 3. The vector space V_3 of eigenvectors associated with 3 is the solution space of the system of linear equations with matrix of coefficients

$$\mathbf{A}-3\mathbf{I}=\begin{pmatrix}-4&2&4\\2&-1&-2\\4&-2&-4\end{pmatrix}\sim\begin{pmatrix}2&-1&-2\\-4&2&4\\4&-2&-4\end{pmatrix}\sim\begin{pmatrix}2&-1&-2\\0&0&0\\0&0&0\end{pmatrix}.$$

Here the second and third unknowns are disposable, therefore they are the parameters ϕ and ψ in $\mathbb{R}$ where ϕ and ψ are not both 0. The first unknown is then $\phi/2+\psi$. We choose pairs of parameters $\phi=2$, $\psi=0$ and $\phi=0$, $\psi=1$ to obtain the basis $B_3=\{(1\quad 2\quad 0)^{\mathrm{T}},(1\quad 0\quad 1)^{\mathrm{T}}\}$ of V_3.

(6) By the formulae for the Gram–Schmidt process in Proposition 2 of Chapter 11, the first vector in the orthogonal basis is $(1\quad 2\quad 0)^{\mathrm{T}}$ and the second is

$$(1\quad 0\quad 1)^{\mathrm{T}}-\tfrac{1}{5}(1\quad 2\quad 0)^{\mathrm{T}}=\tfrac{1}{5}(4\quad -2\quad 5)^{\mathrm{T}}.$$

Therefore we can choose the orthogonal basis C_3 of V_3 to be $C_3=\{(1\quad 2\quad 0)^{\mathrm{T}},(4\quad -2\quad 5)^{\mathrm{T}}\}$, by Proposition 4(i) of Chapter 11.

(7) We define an orthogonal basis D of $\mathbb{R}^3$ by

$$D=\{\mathbf{b}_{-6}\}\cup C_3=\left\{(-2\quad 1\quad 2)^{\mathrm{T}},(1\quad 2\quad 0)^{\mathrm{T}},(4\quad -2\quad 5)^{\mathrm{T}}\right\}.$$

(8) Because $\mathbf{b}_{-6}.\mathbf{b}_{-6}=9$, we have $\mathbf{e}_1=\mathbf{b}_{-6}/\|\mathbf{b}_{-6}\|=\mathbf{b}_{-6}/3=\frac{1}{3}(-2\quad 1\quad 2)^{\mathrm{T}}$. Similarly, $\mathbf{e}_2=\dfrac{1}{\sqrt{5}}(1\quad 2\quad 0)^{\mathrm{T}}$ and $\mathbf{e}_3=\dfrac{1}{3\sqrt{5}}(4\quad -2\quad 5)^{\mathrm{T}}$.

(9) Let the column vector of transformed indeterminates be $\mathbf{y}=(X\quad Y\quad Z)^{\mathrm{T}}$. Then the required orthogonal transformation is $\mathbf{x}=\mathbf{P}\mathbf{y}$, where

$$\mathbf{P}=\frac{1}{3\sqrt{5}}\begin{pmatrix}-2\sqrt{5}&3&4\\\sqrt{5}&6&-2\\2\sqrt{5}&0&5\end{pmatrix}.$$

As the columns of $\mathbf{P}$ are, respectively, eigenvectors associated with –6, 3, 3, the quadratic form $Q=-6X^2+3Y^2+3Z^2$ by Proposition 4.

Summary

A **quadratic form** in a finite set of indeterminates over a field $\mathbb{F}$ is a homogeneous quadratic polynomial in the indeterminates with coefficients in $\mathbb{F}$. Quadratic forms can be studied by means of matrices because for all fields $\mathbb{F}$ which are **not of characteristic 2** a quadratic form Q can be expressed as $\mathbf{x}^T\mathbf{A}\mathbf{x}$, where $\mathbf{x}$ is a column vector with the indeterminates as elements and $\mathbf{A}$ is a matrix over $\mathbb{F}$. The matrix $\mathbf{A}$ is called the **matrix associated with** Q provided that $\mathbf{A}$ is **symmetric**, that is, $\mathbf{A}^T = \mathbf{A}$. A change of indeterminates for a quadratic form Q over $\mathbb{F}$ is made by an equation $\mathbf{x} = \mathbf{P}\mathbf{y}$, where the column vector $\mathbf{x}$ contains the original indeterminates, the column vector $\mathbf{y}$ contains the new indeterminates and $\mathbf{P}$ is a non-singular matrix over $\mathbb{F}$. Under the transformation $\mathbf{x} = \mathbf{P}\mathbf{y}$, the associated matrix $\mathbf{A}$ is transformed into $\mathbf{P}^T\mathbf{A}\mathbf{P}$, which is the **conjugate** of $\mathbf{A}$ by $\mathbf{P}$. Consequently, the study of all quadratic forms over a field $\mathbb{F}$ which is not of characteristic 2 can be conducted as a study of the symmetric matrices over $\mathbb{F}$.

The applications of quadratic forms that are studied in this chapter are to problems concerning quadratic forms over $\mathbb{R}$ in Euclidean geometry and Newtonian mechanics, and these require the changes of the indeterminates to be caused by changes of Cartesian axes. Consequently, the changes of indeterminates considered have equations of the form $\mathbf{x} = \mathbf{P}\mathbf{y}$, where $\mathbf{P}$ is an orthogonal matrix. Under such a transformation, the associated matrix $\mathbf{A}$ is transformed into $\mathbf{P}^T\mathbf{A}\mathbf{P} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$, which is **orthogonally similar** to $\mathbf{A}$. The methods of Chapters 6–11 are all available for use in discussing the orthogonal similarity of a matrix and orthogonal transformation of a quadratic form over $\mathbb{R}$. The main result proved is that for every quadratic form Q over $\mathbb{R}$ there is an orthogonal transformation into a quadratic form associated with a diagonal matrix over $\mathbb{R}$, that is, a **diagonal form**. A key result in this proof is that all the eigenvalues of a symmetric matrix over $\mathbb{R}$ belong to $\mathbb{R}$. The chapter ends with a construction which, given a symmetric matrix $\mathbf{A}$ over $\mathbb{R}$, determines an orthogonal matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$, where $\mathbf{D}$ is a diagonal matrix over $\mathbb{R}$. Whatever orthogonal matrices $\mathbf{P}$ are used, the diagonal elements of the diagonal matrix $\mathbf{D}$ are always the eigenvalues of $\mathbf{A}$ in various orders.

EXERCISES ON CHAPTER 12

1. Find all the 2×2 symmetric matrices over $\mathbb{R}$ which are orthogonal.
2. Let $\mathbf{A}$ be a square matrix over $\mathbb{R}$. Show that any two of the following conditions implies the third:
   (i) $\mathbf{A}$ is symmetric.
   (ii) $\mathbf{A}$ is orthogonal.
   (iii) $\mathbf{A}^2 = \mathbf{I}$.
3. Let $\mathbf{A}$ be a square matrix over a field $\mathbb{F}$ which is not of characteristic 2. Prove that $\mathbf{S} = \frac{1}{2}(\mathbf{A} + \mathbf{A}^T)$ is a symmetric matrix. Deduce that $\mathbf{A}$ is the sum of $\mathbf{S}$ and a skew-symmetric matrix $\mathbf{K}$ over $\mathbb{F}$. Prove that the expression $\mathbf{A} = \mathbf{S} + \mathbf{K}$ as a sum of a symmetric matrix over $\mathbb{F}$ and a skew-symmetric matrix over $\mathbb{F}$ is unique. Explain the reason for including the condition that the field $\mathbb{F}$ is not of characteristic 2 in this exercise.

4. Find symmetric matrices associated with the following quadratic forms over $\mathbb{R}$:
   (i) $Q_1 \equiv x^2 + xy + 3y^2 + 3yx$,
   (ii) $Q_2 \equiv 2xy + z^2$,
   (iii) $Q_3 \equiv x^2 + 4xy - 2y^2 + z^2$,
   (iv) $Q_4 \equiv x^2 + y^2 + z^2 + 2xy$,
   (v) $Q_5 \equiv (x + 2y - z)(3x - y)$.

5. Find the symmetric matrices associated with the quadratic forms R_2, R_3, R_4 over $\mathbb{R}$ into which the quadratic forms Q_2, Q_3, Q_4 of Exercise 4 are transformed by the non-singular transformation $x = X - 2Y + 4Z$, $y = -X + Y$, $z = 3X + Y + Z$.

6. Let $\mathbf{A}$ be a skew-symmetric matrix over $\mathbb{R}$. Prove that the real part of every eigenvalue of $\mathbf{A}$ is 0.

7. Let $\mathbf{A}$ be a skew-symmetric matrix over $\mathbb{R}$, let $\mathbf{u}$ be an eigenvector of $\mathbf{A}$ associated with the eigenvalue $i\rho$ and let $\mathbf{v}$ be an eigenvector of $\mathbf{A}$ associated with the eigenvalue $i\sigma$, where $\rho, \sigma \in \mathbb{R}$ and $\rho \neq \sigma$. Prove that $\overline{\mathbf{u}}^{\mathrm{T}}\mathbf{v} = 0$.

8. Find diagonal forms over $\mathbb{R}$ to which the quadratic forms Q_1, Q_3 and Q_4 in Exercise 4 can be transformed by orthogonal transformations of the indeterminates.

9. Find orthogonal matrices $\mathbf{P}$ so that $\mathbf{P}^{-1}\mathbf{AP}$ is a diagonal matrix for the following two matrices:

   (i) $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 2 & -2 \end{pmatrix}$, (ii) $\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

10. Find an orthogonal transformation of the indeterminates which transforms the quadratic form Q into a diagonal form $aX^2 + bY^2$, where $Q = 5x^2 + 4xy + 8y^2$.

11. Find an orthogonal transformation of the indeterminates which transforms the quadratic form

    $$Q = 2wx + 2wy - 2wz - 2xy + 2xz + 2yz.$$

    into a diagonal form.

13 · Positive Definite Quadratic Forms

Outline

This chapter studies non-singular transformations of quadratic forms into diagonal forms. In particular, it uses them to decide whether a quadratic form is positive or negative definite. We start by showing that whether a certain quadratic form is positive or negative definite is a criterion for a stationary point of a function of several variables to be a minimum or maximum point. It is first shown that these criteria can be expressed in terms of the eigenvalues of the associated matrix. Alternatively, 'Lagrange's process' can be used to transform the quadratic form into diagonal form. Then 'Sylvester's law of inertia' shows that the signs of the coefficients in the diagonal form are invariant, and this provides a different criterion for a quadratic form to be positive or negative definite. Finally, it is proved that two quadratic forms can be diagonalized simultaneously provided that one of them is positive definite.

Introduction

A simple method of transforming quadratic forms into diagonal forms will be given in this chapter, but it does not lead to an orthogonal transformation. Although this more general kind of transformation has uses in both mechanics and geometry, they occur in rather abstract contexts that are impossible to describe briefly. However, the following example introduces a familiar problem.

○ Example 1

Let x and y be real variables and $f(x, y) = (x^2 - 3xy + 3y^2)e^x$. What are the maximum and minimum points of the function f?

To find these, we start by finding the stationary points, those points (a, b) where the partial differential coefficients of $f(x, y)$ with respect to x and y equal 0. Because $\partial f(x,y)/\partial x = f_x(x,y) = (2x-3y)e^x + (x^2 - 3xy + 3y^2)e^x$ and $f_y(x, y) = (6y - 3x)e^x$, this happens if and only if $x = 2y$ and $y(1 + y) = 0$. Therefore $f(x, y)$ has stationary points at $(0, 0)$ and $(2, 1)$. Let us consider what we must do to find out whether $(0, 0)$ is a maximum or a minimum or something else.

Because $f(x, y)$ has second- and third-order partial differential coefficients, Taylor's theorem applied to f at $(0, 0)$ gives us

$$f(x,y) - f(0,0) = \frac{1}{2}x^2 f_{xx}(0,0) + xyf_{xy}(0,0) + \frac{1}{2}y^2 f_{yy}(0,0) + R_2$$

where f_{xx}, f_{xy} and f_{yy} are the second-order partial differential coefficients and the terms of R_2 are of degree 3 in x and y. But $f_{xx}(x, y) = 2e^x + 2(2x - 3y)e^x + (x^2 - 3xy + 3y^2)e^x$, $f_{yy} = 6e^x$ and $f_{xy} = -3e^x + (-3x + 6y)e^x$, therefore $f_{xx}(0, 0) = 2$, $f_{yy}(0, 0) = 6$ and $f_{xy}(0, 0) = -3$. Therefore $f(x, y) - f(0, 0) = x^2 - 3xy + 3y^2 + R_2$. Because the terms of R_2 are of degree 3 in x and y, when x and y are sufficiently small $f(x, y) - f(0, 0)$ has the same sign as the quadratic form $Q \equiv x^2 - 3xy + 3y^2$. If $Q > 0$ unless $x = y = 0$, then $f(x, y) - f(0, 0) > 0$ for small x and y, therefore $(0, 0)$ is a minimum point for $f(x, y)$. Similarly, $(0, 0)$ is a maximum point for $f(x, y)$ if $Q < 0$ unless $x = y = 0$. Finally, if Q takes both positive and negative values, $(0, 0)$ is neither a maximum nor a minimum point for $f(x, y)$.

The distinctions concerning quadratic forms over $\mathbb{R}$ that are used in Example 1 are conveyed by the following definition.

• Definition 1

The quadratic form $Q \equiv \mathbf{x}^T\mathbf{A}\mathbf{x}$ over $\mathbb{R}$ belongs to one of the following **value classes**:

(i) Q is **positive definite** if $Q \geq 0$ and $Q = 0$ if and only if $\mathbf{x} = \mathbf{0}$;
(ii) Q is **negative definite** if $Q \leq 0$ and $Q = 0$ if and only if $\mathbf{x} = \mathbf{0}$;
(iii) Q is **positive (negative) semi-definite** if $Q \geq 0$ ($Q \leq 0$);
(iv) Q is **indefinite** otherwise.

○ Example 2

To solve the problem concerning the function in Example 1, we find the value class of the quadratic form $Q \equiv x^2 - 3xy + 3y^2$ in two indeterminates over $\mathbb{R}$. A simple approach is to complete the square containing x^2 to obtain a positive term. Then $Q \equiv (x^2 - 3xy + \frac{9}{4}y^2) + y^2$ therefore $Q \equiv (x - \frac{3}{2}y)^2 + \frac{3}{4}y^2$. Consequently Q is a sum of two positive terms. Therefore Q is positive definite and the point is a minimum.

The technique we used to find the value class of the quadratic form Q in Example 2 was to transform Q into a diagonal form $D = u^2 + \frac{3}{4}v^2$ by means of the obviously non-singular transformation of indeterminates $u = x - \frac{3}{2}y$ and $v = y$. We then used the signs of the diagonal coefficients to decide the value class. We shall use this as our general method for deciding the value class of a quadratic form, although there are two methods for calculating the coefficients. Both methods are based on finding quadratic forms equivalent to the given form, according to the following definition.

• Definition 2

Let Q and R be quadratic forms over a field $\mathbb{F}$ which is not of characteristic 2. R is **equivalent over $\mathbb{F}$ to** Q if R can be transformed into Q by a non-singular transformation of indeterminates.

Proposition 2 of Chapter 12 determines the relationship between the associated matrices of Q and R in Definition 2.

• Proposition 1

Let $\mathbb{F}$ be a field which is not of characteristic 2. Then equivalence over $\mathbb{F}$ of quadratic forms is an equivalence relation.

TUTORIAL PROBLEM 13.1

Prove Proposition 1.

One method of deciding the value class of a quadratic form $Q \equiv \mathbf{x}^T\mathbf{A}\mathbf{x}$ over $\mathbb{R}$ is to use Proposition 4 and Theorem 2 of Chapter 12. These prove that Q is equivalent to a diagonal form of which the diagonal elements are the eigenvalues of $\mathbf{A}$ by the transformation determined in Theorem 2.

• Theorem 1

Let Q be a quadratic form over $\mathbb{R}$ with associated matrix $\mathbf{A} \neq \mathbf{O}$. Then:

(i) Q is positive (negative) definite if and only if all the eigenvalues of $\mathbf{A}$ are positive (negative);

(ii) Q is positive (negative) semi-definite if and only if the eigenvalues of $\mathbf{A}$ are non-negative (non-positive);

(iii) otherwise Q is indefinite.

PROOF

Let Q be a quadratic form in n indeterminates over $\mathbb{R}$. Then, by Proposition 4 of Chapter 12, there exists an orthogonal transformation $\mathbf{x} = \mathbf{P}\mathbf{y}$ of the indeterminates such that $Q = \lambda_1 y_1^2 + \lambda_2 y_2^2 + \ldots + \lambda_n y_n^2$, where $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the eigenvalues of the symmetric matrix associated with Q. The proof is easy except for two parts. To prove that $Q = 0$ if and only if $\mathbf{x} = \mathbf{0}$ in (i) we note that $Q = 0$ if and only if $\mathbf{y} = \mathbf{0}$. But $\mathbf{P}$ is non-singular, therefore $\mathbf{x} = \mathbf{P}\mathbf{y}$ and $\mathbf{y} = \mathbf{P}^{-1}\mathbf{x}$ imply that $\mathbf{y} = \mathbf{0}$ if and only if $\mathbf{x} = \mathbf{0}$. The other part that requires care is to show that the condition in (iii) implies that Q is indefinite. The condition holds if at least one eigenvalue $\lambda_p > 0$ and at least one $\lambda_q < 0$. Then $Q > 0$ for $y_p > 0$ and all other indeterminates equal to 0 and $Q < 0$ for $y_q > 0$ and all other indeterminates 0. Consequently, Q is indefinite. ●

The following example reveals that there may be factors that make it difficult to find the value class of a quadratic form.

○ Example 3

Let us find the value class of the quadratic form

$$Q \equiv w^2 + 9x^2 + 25z^2 - 6wx + 10wz + 4xy - 10xz + 4yz.$$

over $\mathbb{R}$. First we try to use Theorem 1, so we write the characteristic polynomial of the associated matrix $\mathbf{A}$ of Q as

$$\chi(\lambda) = \det(\mathbf{A} - \lambda\mathbf{I}) = \begin{vmatrix} 1-\lambda & -3 & 0 & 5 \\ -3 & 9-\lambda & 2 & -5 \\ 0 & 2 & -\lambda & 2 \\ 5 & -5 & 2 & 25-\lambda \end{vmatrix}.$$

Unfortunately, the symmetry of the matrix prevents the reduction of the matrix to a 3×3 matrix. Alternatively, perhaps $\chi(\lambda)$ has an integer root k. If so, k divides the constant term of the polynomial $\det \mathbf{A} = 80$ of $\chi(\lambda)$, hence there are only a finite number of possible values of k. In fact, $\chi(\lambda)$ does not have an integer root, therefore the only course left is to solve $\chi(\lambda) = 0$ by a standard method for solving equations of degree 4. However, if Q had contained five or more indeterminates, the equation $\chi(\lambda) = 0$ would have been of degree 5 or above. Because it has been proved that there are no general algebraic solutions of such equations, this could be an insuperable difficulty in those cases. Finally, we can try to complete the squares for the indeterminates, as in Example 2. We start by completing the square in Q which starts with w^2 and obtain

$$\begin{aligned} Q &\equiv (w^2 - 6wx + 10wz - 30xz + 9x^2 + 25z^2) + 4xy - 10xz + 4yz + 30xz \\ &\equiv (w^2 - 3x + 5z)^2 + 4xy + 20xz + 4yz. \end{aligned}$$

As there is now no further square to complete, we cannot proceed.

The way out of the difficulties revealed in Example 4 was found by J.L. Lagrange (1736–1813), who needed a solution of this problem for use in dynamics problems. He completed the method of Example 2 as follows.

• *Construction I* Lagrange's process

Let Q be a non-zero quadratic form in the indeterminates $x_1, x_2, x_3, \ldots, x_n$ with associated matrix symmetric $\mathbf{A}$ over a field $\mathbb{F}$ which is not of characteristic 2.

(1)First we assume that $a_{11} = a_{22} = a_{33} = \ldots = a_{nn} = 0$. Because Q is non-zero, there are non-zero coefficients and therefore there exist integers p and q which are minimal such that $p < q$ and $a_{pq} \neq 0$. Then $Q \equiv 2a_{pq}x_px_q + Q_1$, where Q_1 is a quadratic form over $\mathbb{F}$ in $x_1, x_2, x_3, \ldots, x_n$ with no diagonal terms. Let us apply to the indeterminates the transformation $x_p = y_p - y_q$, $x_q = y_p + y_q$ and $x_j = y_j$ for $j = 1, 2, \ldots, p-1, p+1, \ldots, q-1, q+1, \ldots, n$. This transformation has equation $\mathbf{x} = \mathbf{R}\mathbf{y}$, where $\mathbf{R}$ is an identity matrix except for a 2×2 submatrix $\mathbf{G} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$. Therefore $\det \mathbf{R} = \begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = 2$ and hence $\mathbf{x} = \mathbf{R}\mathbf{y}$ is non-singular. Then

$$2a_{pq}x_px_q = 2a_{pq}(y_p - y_q)(y_p + y_q) = 2a_{pq}y_p^2 - 2a_{pq}y_q^2$$

and the other terms in Q are of one of the following forms:

$$2a_{pk}x_px_k = 2a_{pk}(y_p - y_q)y_k = 2a_{pk}y_py_k - 2a_{pk}y_qy_k,$$

or

$$2a_{qk}x_qx_k = 2a_{qk}(y_p + y_q)y_k = 2a_{qk}y_py_k + 2a_{qk}y_qy_k,$$

or

$$2a_{jk}x_jx_k = 2a_{jk}y_jy_k,$$

where $j, k \neq p$ or q. Therefore $Q = 2a_{pq}y_p^2 - 2a_{pq}y_q^2 + Q_2$, where Q_2 is a quadratic form in $y_1, y_2, y_3, \ldots, y_n$ with no diagonal terms. We conclude that Q is equivalent to a quadratic form in the $y_1, y_2, \ldots, y_n$ in which y_p^2 has the non-zero coefficient $2a_{pq}$.

(2) Alternatively, suppose that Q has diagonal terms, that is, terms of the form ax^2. Then there exists a least integer p such that $a_{pp} \neq 0$. In the following the summation sign $\sum'^{n}_{j=1}$ denotes a sum in which $j \neq p$. Then

$$\begin{aligned} Q &\equiv a_{pp}x_p^2 + \sum_{j=1}^{n}{}' 2a_{pj}x_p x_j + \sum_{j=1}^{n}{}' \sum_{k=1}^{n}{}' a_{jk}x_j x_k \\ &\equiv a_{pp}\left[x_p^2 + \sum_{j=1}^{n}{}' b_{pj}x_p x_j\right] + Q_3, \end{aligned}$$

where $b_{pj} = a_{pj}/a_{pp}$ and Q_3 is a quadratic form over $\mathbb{F}$ in $x_1, x_2, \ldots, x_{p-1}, x_{p+1}, \ldots, x_n$. Therefore $Q \equiv a_{pp}\left(x_p + \sum'^{n}_{j=1} b_{pj}x_j\right)^2 + Q_4$, where $Q_4 \equiv Q_3 - a_{pp}\sum'^{n}_{j=1} b_{pj}x_j^2$ is a quadratic form over $\mathbb{F}$ in $x_1, x_2, \ldots, x_{p-1}, x_{p+1}, \ldots, x_n$. We then use the transformation $\mathbf{y} = \mathbf{Sx}$ given by $y_p = x_p + \sum'^{n}_{j=1} b_{pj}x_j$ and $y_j = x_j$, for $j = 1, 2, \ldots, p-1, p+1, \ldots, n$. By evaluating $\det \mathbf{S}$ by its pth row, we obtain $\det \mathbf{S} = 1$, consequently $\mathbf{y} = \mathbf{Sx}$ is a non-singular transformation. Therefore Q is equivalent to $a_{pp}y_p^2 + Q_5$, where $Q_5 = Q_4(y_1, \ldots, y_{p-1}, y_{p+1}, \ldots, y_n)$ by the non-singular transformation $\mathbf{x} = \mathbf{S}^{-1}\mathbf{y}$. Then, by Proposition 1, Q is equivalent over $\mathbb{R}$ by at most two non-singular transformations to $Q = ct_1^2 + Q_6$, where $c \in \mathbb{F}$ and Q_6 is a quadratic form over $\mathbb{F}$ in $t_2, t_3, \ldots, t_n$.

Lagrange's process supplies the device that is needed to continue the calculation in Example 3, so let us do so.

○ *Example 4*

In Example 3 we showed that the quadratic form

$$Q \equiv w^2 + 9x^2 + 25z^2 - 6wx + 10wz + 4xy - 10xz + 4yz$$

over $\mathbb{R}$ can be written as

$$Q \equiv (w^2 - 3x + 5z)^2 + 4xy + 20xz + 4yz.$$

Therefore $Q = w_1^2 + Q_1$, where $w_1 = w - 3x + 5z$ and $Q_1 \equiv 4xy + 20xz + 4yz$. By step 1 of Lagrange's process, we let $x = s - t$ and $y = s + t$, which gives

$$Q_1 = 4(s-t)(s+t) + 20(s-t)z + 4(s+t)z = 4s^2 - 4t^2 + 24sz - 16tz,$$

and we complete the square containing $4s^2$:

$$\begin{aligned} Q_1 &= 4[s^2 + 6sz] - 4t^2 - 16tz \\ &= 4[s^2 + 6sz + 9z^2] - 36z^2 - 4t^2 - 16tz \\ &= 4(s+3z)^2 - 36z^2 - 4t^2 - 16tz \\ &= 4s_1^2 + Q_2, \end{aligned}$$

where $s_1 = s + 3z$ and $Q_2 \equiv -4[t^2 + 4tz + 9z^2]$. But $Q_2 = -4[t^2 + 4tz + 4z^2] - 20z^2$,

therefore $Q_2 = -4t_1^2 - 20z^2$, where $t_1 = t + 2z$. On assembling these equations, we obtain $Q = w_1^2 + 4s_1^2 - 4t_1^2 - 20z_1^2$, where $w_1 = w - 3x + 5z$, $s_1 = s + 3z$, $t_1 = t + 2z$ and $z_1 = z$. Therefore Q is equivalent to the diagonal form $w_1^2 + 4s_1^2 - 4t_1^2 - 20z_1^2$ over $\mathbb{R}$. However, we have not completed the calculation because we still need to solve the linear equations to give the final indeterminates in terms of w, x, y and z.

In fact, for any quadratic form Q over a field which is not of characteristic 2, the use of Lagrange's process transforms Q into a diagonal form, as we now prove.

• *Theorem 2*

Let Q be a quadratic form in n indeterminates over a field $\mathbb{F}$ which is not of characteristic 2. Then there exists a non-singular transformation of indeterminates which is the composite of at most $2n - 2$ steps of Lagrange's process and transforms Q into a diagonal quadratic form equivalent to Q.

PROOF

Each application of at most two steps of Construction 1 transforms a quadratic form Q_1 into an equivalent quadratic form $at^2 + Q_2$, where the quadratic form Q_2 is in one fewer indeterminates than Q_1. Consequently, after at most $2n - 2$ steps of Construction 1 applied to the successive quadratic forms, the final form has only one indeterminate and therefore is of the form bu^2, where $b \in \mathbb{F}$ and u is an indeterminate. Therefore, by Proposition 1, Q is equivalent to the sum Q_3 of n multiples of squares of indeterminates. In consequence, Q_3 is a diagonal quadratic form over $\mathbb{F}$ which is equivalent to Q. ●

TUTORIAL PROBLEM 13.2

Use Lagrange's process to find a diagonal form into which the quadratic form $Q \equiv w^2 + 3x^2 + 2y^2 + 5z^2 - 4wx - 4yz$ over $\mathbb{R}$ can be transformed by a non-singular transformation of indeterminates. Repeat the calculation by using Theorem 1.

For a given quadratic form, Lagrange's process can be carried out in a number of different ways. For example, in Example 4 we could have taken

$$Q \equiv \left[(5z)^2 + 2w(5z) - 2x(5z) + 2\left(\frac{2}{5}\right)y(5z)\right] + w^2 + 9x^2 - 6wx + 4xy,$$

then completed the square in the brackets and obtained a final result which is very different from Example 4. We know from Proposition 2 of Chapter 12 that the ranks of quadratic forms that are equivalent over a field are the same, but what other properties do they have in common? J.J. Sylvester (1814–1897), who introduced the word 'matrix' to linear algebra, answered this question for quadratic forms over $\mathbb{R}$ by means of the following theorem.

• *Theorem 3* Sylvester's law of intertia

Let Q be a quadratic form over $\mathbb{R}$ and let the diagonal forms D and E be equivalent over $\mathbb{R}$ to Q. Then E has the same number of positive coefficients as D.

PROOF

Let r be the rank of Q. Then, by Proposition 2 of Chapter 12, the diagonal forms D and E are also of rank r. Therefore the number of non-zero diagonal coefficients of D or E is $r = \text{rank } D = \text{rank } E$. Let D have s positive coefficients and let E have t positive coefficients. Let us suppose that the theorem is false and $s > t$ (by exchanging the names of D and E if necessary). For both D and E we number the indeterminates in such an order that the positive coefficients occur first, then the negative coefficients and indeterminates numbered $r + 1$ to n have zero coefficients. Then we have

$$D = a_1y_1^2 + a_2y_2^2 + \ldots + a_sy_s^2 - a_{s+1}y_{s+1}^2 - a_{s+2}y_{s+2}^2 - \ldots - a_ry_r^2$$

and

$$E = b_1z_1^2 + b_2z_2^2 + \ldots + b_tz_t^2 - b_{t+1}z_{t+1}^2 - b_{t+2}z_{t+2}^2 - \ldots - b_rz_r^2,$$

where $0 < a_j \in \mathbb{R}$ and $0 < b_j \in \mathbb{R}$ for $j = 1, 2, 3, \ldots, r$. The indeterminates y_j and z_j, $j = 1, 2, 3, \ldots, r$, are linear combinations of the n indeterminates such that $Q \in \mathbb{R}[x_1, x_2, x_3, \ldots, x_n]$. Therefore the equations $y_{s+1} = 0$, $y_{s+2} = 0, \ldots, y_n = 0$, $z_1 = 0$, $z_2 = 0, \ldots, z_t = 0$ are a set of $n - s + t < n$ homogeneous linear equations in the n unknowns $x_1, x_2, x_3, \ldots, x_n$. Because there are fewer equations than unknowns, this system of equations has a non-trivial solution $x_i = c_i \in \mathbb{R}$ for $i = 1, 2, 3, \ldots, n$. We write $\mathbf{x} = (x_1 \;\; x_2 \;\; x_3 \;\ldots\; x_n)^T$ and $\mathbf{c} = (c_1 \;\; c_2 \;\; c_3 \;\ldots\; c_n)^T$ and $y_j(\mathbf{c})$ and $z_j(\mathbf{c})$ for y_j and z_j with $\mathbf{x} = \mathbf{c}$. Then, because D and E are obtained from Q by non-singular transformations, $Q = D = E$. Therefore $D = E$ for $\mathbf{x} = \mathbf{c}$, and, taking the linear equations into account,

$$a_1y_1^2(\mathbf{c}) + a_2y_2^2(\mathbf{c}) + \ldots + a_sy_s^2(\mathbf{c}) = -b_{t+1}z_{t+1}^2(\mathbf{c}) - b_{t+2}z_{t+2}^2(\mathbf{c}) - \ldots - b_rz_r^2(\mathbf{c}).$$

Because the left-hand side of this equation is non-negative and the right side is non-positive, we have $a_1y_1^2(\mathbf{c}) + a_2y_2^2(\mathbf{c}) + \ldots + a_sy_s^2(\mathbf{c}) = 0$. The coefficients in this equation are all positive, therefore $y_j(\mathbf{c}) = 0$ for $j = 1, 2, 3, \ldots, s$. But $y_j(\mathbf{c}) = 0$ for $j = s + 1$, $s + 2, \ldots, n$ from the system of homogeneous linear equations, therefore $y_j(\mathbf{c}) = 0$ for $j = 1, 2, 3, \ldots, n$. But $\mathbf{y} = (y_1 \;\; y_2 \;\; y_3 \;\ldots\; y_n)^T = \mathbf{Px}$, where $\mathbf{P}$ is a non-singular matrix over $\mathbb{R}$. Therefore for $\mathbf{c} \neq \mathbf{0}$ we have $\mathbf{c} = \mathbf{P}^{-1}\mathbf{0} = \mathbf{0}$, which is a contradiction that proves the theorem. ●

Sylvester's law of inertia determines a second invariant of a quadratic form Q over $\mathbb{R}$. Together with the rank, this invariant characterizes the quadratic forms equivalent to Q, as the following proposition shows.

• Proposition 2

Let Q be a quadratic form of rank r over $\mathbb{R}$, let D be a diagonal form which is equivalent over $\mathbb{R}$ to Q and let D have p positive and m negative coefficients. Then:

(i) $s = p - m$ is an invariant of Q, called the **signature** of Q and denoted by sig Q;

(ii) $p = (r + s)/2$ and $m = (r - s)/2$;

(iii) Q is equivalent over $\mathbb{R}$ to D^*, where

$$D^* = u_1^2 + u_2^2 + \ldots + u_p^2 - u_{p+1}^2 - u_{p+2}^2 - \ldots - u_r^2;$$

(iv) the quadratic form Q_1 over $\mathbb{R}$ is equivalent over $\mathbb{R}$ to Q if and only if rank $Q_1 = r$ and sig $Q_1 = s$.

PROOF

(i) By Proposition 2 of Chapter 12, rank $D = r$, therefore D has r non-zero coefficients. By Theorem 3, the number p of positive coefficients of D is an invariant of Q. The number of negative coefficients of D is $m = r - p$, therefore m is also an invariant of Q. It follows that the sig $Q = p - m$ is an invariant of Q.

(ii) As D has r non-zero coefficients, $p + m = r$ and, by definition, $p - m = s$. Therefore $p = (r + s)/2$ and $m = (r - s)/2$.

(iii) By Theorem 2, Q is equivalent over $\mathbb{R}$ to a diagonal form D_1 and, by (ii), D_1 has $p = (r + s)/2$ positive coefficients and $m = r - p$ negative coefficients. Therefore, by renumbering the indeterminates if necessary, there exist $0 < d_j \in \mathbb{R}$, for $j = 1, 2, 3, \ldots, r$, such that

$$D_1 = d_1y_1^2 + d_2y_2^2 + \ldots + d_py_p^2 - d_{p+1}y_{p+1}^2 - d_{p+2}y_{p+2}^2 - \ldots - d_ry_r^2.$$

We transform D_1 into D^* by the non-singular transformation $v_j = u_j/\sqrt{d_j}$, for $j = 1, 2, 3, \ldots, r$, and $y_j = u_j$, for $j = p + 1, p + 2, \ldots, n$, where n is the number of indeterminates for Q. This gives us

$$D^* = u_1^2 + u_2^2 + \ldots + u_p^2 - u_{p+1}^2 - u_{p+2}^2 - \ldots - u_r^2.$$

As D_1 is equivalent over $\mathbb{R}$ to Q and D^* is equivalent over $\mathbb{R}$ to D_1, then D^* is equivalent over $\mathbb{R}$ to Q, by Proposition 1.

(iv) Suppose that Q_1 is equivalent over $\mathbb{R}$ to Q. Then rank Q_1 = rank Q by Proposition 2 of Chapter 12. Also, by Proposition 1 of the present chapter, if Q is also equivalent over $\mathbb{R}$ to the diagonal form D, then Q_1 is also equivalent over $\mathbb{R}$ to D. Consequently, by (i), sig Q_1 = sig D = sig Q. Conversely, suppose that rank Q_1 = rank Q and sig Q_1 = sig Q. Then, by (iii), Q is equivalent over $\mathbb{R}$ to D^*. Therefore, by Proposition 1, D^* is equivalent over $\mathbb{R}$ to Q. Again by (iii), Q_1 is equivalent over $\mathbb{R}$ to D^*; therefore, by Proposition 1, Q_1 is equivalent over $\mathbb{R}$ to Q. ●

We can use Proposition 2 to give the following alternative set of criteria for the value class of a quadratic form over $\mathbb{R}$.

• *Theorem 4*

Let Q be a quadratic form of rank $r > 0$ and signature s in n indeterminates over $\mathbb{R}$. Let $u_1, u_2, u_3, \ldots, u_n$ be indeterminates and let $p = (r + s)/2$. Then

(i) Q is positive (or negative) definite $\Leftrightarrow r = s = n$ (or $r = -s = n$) $\Leftrightarrow$ Q is equivalent over $\mathbb{R}$ to $D = z_1^2 + z_2^2 + z_3^2 + \ldots + z_n^2$ (or $-D$);

(ii) Q is positive (or negative) semi-definite $\Leftrightarrow r = s$ (or $r = -s$) $\Leftrightarrow$ Q is equivalent over $\mathbb{R}$ to $E = u_1^2 + u_2^2 + u_3^2 + \ldots + u_r^2$ (or $-E$);

(iii) Q is indefinite $\Leftrightarrow s < r \Leftrightarrow$ Q is equivalent over $\mathbb{R}$ to

$$u_1^2 + u_2^2 + \ldots + u_p^2 - u_{p+1}^2 - u_{p+2}^2 - \ldots - u_r^2,$$

where $0 < p < r$.

PROOF

By Proposition 2(iii), Q is equivalent over $\mathbb{R}$ to

$$D^* = z_1^2 + z_2^2 + \ldots + z_p^2 - z_{p+1}^2 - z_{p+2}^2 - \ldots - z_r^2,$$

which becomes the five quadratic forms of the statement according to the values of r and s. Also, by Proposition 4 of Chapter 12, Q is equivalent over $\mathbb{R}$ to the diagonal form $L \equiv \lambda_1 y_1^2 + \lambda_2 y_2^2 + \lambda_3 y_3^2 + \ldots + \lambda_n y_n^2$, where $y_1, y_2, y_3, \ldots, y_n$ are indeterminates and $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n$ are the eigenvalues of the symmetric matrix $\mathbf{A}$ associated with Q. Therefore, by Proposition 2(iv), rank $L = r$ and sig $L = s$. Because $r > 0$, L is not a zero quadratic form but, by Proposition 2(ii), L has p positive coefficients and $m = (r - s)/2$ negative coefficients. Therefore the number of positive (negative) eigenvalues of $\mathbf{A}$ is $p(m)$ and the value class of Q can be determined from Theorem 1 to complete the proof. ●

In some applications of linear algebra it is desirable to transform two quadratic forms into diagonal forms by the same transformation of indeterminates. We shall now show that this is sometimes possible.

• Definition 3

Let $Q \equiv \mathbf{x}^T\mathbf{A}\mathbf{x}$ and $R \equiv \mathbf{x}^T\mathbf{B}\mathbf{x}$ be quadratic forms over $\mathbb{R}$. Then Q and R are **simultaneously reducible (by $\mathbf{x} = \mathbf{P}\mathbf{y}$ over $\mathbb{R}$)** if there is a non-singular transformation of indeterminates ($\mathbf{x} = \mathbf{P}\mathbf{y}$) over $\mathbf{R}$ which transforms both Q and R into diagonal forms.

Here are two quadratic forms which are not simultaneously reducible.

TUTORIAL PROBLEM 13.3

Show that $x^2 - 2xy$ and $2xy$ are not simultaneously reducible over $\mathbb{R}$.

When studying the mechanics of vibrating systems it is desirable to reduce two quadratic forms simultaneously to diagonal forms. One of the quadratic forms, K, represents the kinetic energy of the system and therefore is a sum of terms each of which is the product of a positive constant and the square of a speed. It follows that $K \geq 0$ and that $K = 0$ if and only if the system is at rest. Consequently, K is a positive definite quadratic form, by Definition 1. In order to cover mechanics problems like these, we shall discuss the **simultaneous reduction** of pairs of quadratic forms over $\mathbb{R}$ where at least one form is positive definite. In fact, simultaneous reduction is also possible for pairs of quadratic forms where one is of full rank, but the process is not certain to succeed, and even when successful it may construct a diagonal form over $\mathbb{C}$ instead of $\mathbb{R}$. Therefore we start by finding some properties of a positive definite quadratic form $\mathbf{x}^T\mathbf{B}\mathbf{x}$ and its associated matrix $\mathbf{B}$, and we call $\mathbf{B}$ a **positive definite matrix.**

• *Proposition 3*

Let $\mathbf{x}^T\mathbf{B}\mathbf{x}$ be a positive definite quadratic form in n indeterminates over $\mathbb{R}$, where $\mathbf{B}$ is a symmetric matrix. Then $\langle \mathbf{v}, \mathbf{w} \rangle = \mathbf{v}^T\mathbf{B}\mathbf{w}$ is an inner product on $\mathbb{R}^n$, the **B-product** on $\mathbb{R}^n$.

PROOF

Parts (i), (ii) and (iii) of Definition 2 of Chapter 10 were proved for a matrix $\mathbf{A}$ in Example 4 of Chapter 10 using only the fact that $\mathbf{A}$ was symmetric, therefore they hold for $\mathbf{v}^T\mathbf{B}\mathbf{w}$. Because $\mathbf{v}^T\mathbf{B}\mathbf{v}$ is positive definite, Definition 1(i) asserts that parts (iv) and (v) of Definition 2 of Chapter 10 hold, therefore $\langle \mathbf{v}, \mathbf{w} \rangle = \mathbf{v}^T\mathbf{B}\mathbf{w}$ is an inner product for $\mathbb{R}^n$. ●

We can now prove our main theorem.

• *Theorem 5*

Let $\mathbf{A}$ and $\mathbf{B}$ be symmetric $n \times n$ matrices over $\mathbb{R}$ and let $\mathbf{B}$ be positive definite. Then there exists a non-singular matrix $\mathbf{P}$ over $\mathbb{R}$ such that the transformation $\mathbf{x} = \mathbf{P}\mathbf{y}$ transforms the quadratic forms $\mathbf{x}^T\mathbf{A}\mathbf{x}$ and $\mathbf{x}^T\mathbf{B}\mathbf{x}$ into the diagonal forms

$$\mu_1 y_1^2 + \mu_2 y_2^2 + \mu_3 y_3^2 + \ldots + \mu_n y_n^2$$

and $y_1^2 + y_2^2 + y_3^2 + \ldots + y_n^2$, respectively, where $\mu_1, \mu_2, \mu_3, \ldots, \mu_n$ are the roots of the polynomial $\det(\mathbf{A} - \mu\mathbf{B})$.

PROOF

By Theorem 4(i), there exists a non-singular matrix $\mathbf{L}$ over $\mathbb{R}$ such that $\mathbf{x} = \mathbf{L}\mathbf{z}$ transforms $\mathbf{x}^T\mathbf{B}\mathbf{x}$ into $\mathbf{z}^T\mathbf{z}$. By Proposition 2 of Chapter 12, this implies that $\mathbf{L}^T\mathbf{B}\mathbf{L} = \mathbf{I}$ and therefore that $\mathbf{B} = (\mathbf{L}^T)^{-1}\mathbf{L}^{-1}$. However, $\mathbf{x} = \mathbf{L}\mathbf{z}$ also transforms $\mathbf{x}^T\mathbf{A}\mathbf{x}$ into $\mathbf{z}^T\mathbf{L}^T\mathbf{A}\mathbf{L}\mathbf{z}$. By Proposition 4 of Chapter 12 there exists an orthogonal matrix $\mathbf{K}$ such that $\mathbf{K}^{-1}(\mathbf{L}^T\mathbf{A}\mathbf{L})\mathbf{K} = \mathbf{D}$, where $\mathbf{D}$ is the diagonal matrix whose diagonal elements $\mu_1, \mu_2, \mu_3, \ldots, \mu_n$ are the eigenvalues of $\mathbf{L}^T\mathbf{A}\mathbf{L}$. By Theorem 1 of Chapter 6, this means that the diagonal elements are the roots of the polynomial equation $\det(\mathbf{L}^T\mathbf{A}\mathbf{L} - \mu\mathbf{I}) = 0$. Because $\mathbf{L}$ is non-singular, this is equivalent to $[\det(\mathbf{L}^T)^{-1}][\det(\mathbf{L}^T\mathbf{A}\mathbf{L} - \mu\mathbf{I})][\det \mathbf{L}^{-1}] = 0$. But for any matrices $\mathbf{M}$, $\mathbf{N}$ we have $(\det \mathbf{M})(\det \mathbf{N}) = \det(\mathbf{M}\mathbf{N})$, therefore $\det[(\mathbf{L}^T)^{-1}(\mathbf{L}^T\mathbf{A}\mathbf{L} - \mu\mathbf{I})\mathbf{L}^{-1}] = 0$ is equivalent to

$$\det[(\mathbf{L}^T)^{-1}\mathbf{L}^T\mathbf{A}\mathbf{L}\mathbf{L}^{-1} - \mu(\mathbf{L}^T)^{-1}\mathbf{I}\mathbf{L}^{-1}] = \det[\mathbf{A} - \mu(\mathbf{L}^T)^{-1}\mathbf{L}^{-1}] = \det(\mathbf{A} - \mu\mathbf{B}) = 0$$

because $(\mathbf{L}^T)^{-1}\mathbf{L}^{-1} = \mathbf{B}$. Because $\mathbf{K}$ is orthogonal, this implies that $\mathbf{K}^{-1}(\mathbf{L}^T\mathbf{A}\mathbf{L})\mathbf{K} = \mathbf{K}^T\mathbf{L}^T\mathbf{A}\mathbf{L}\mathbf{K} = (\mathbf{L}\mathbf{K})^T\mathbf{A}(\mathbf{L}\mathbf{K}) = \mathbf{D}$, where the diagonal elements of $\mathbf{D}$ are the roots of $\det(\mathbf{A} - \mu\mathbf{B})$. Therefore, by Proposition 2 of Chapter 12, the transformation $\mathbf{x} = \mathbf{L}\mathbf{K}\mathbf{y}$ transforms $\mathbf{x}^T\mathbf{A}\mathbf{x}$ into $\mathbf{y}^T\mathbf{D}\mathbf{y}$ and also transforms $\mathbf{x}^T\mathbf{B}\mathbf{x}$ into $S \equiv \mathbf{y}^T(\mathbf{L}\mathbf{K})^T\mathbf{B}(\mathbf{L}\mathbf{K})\mathbf{y}$. But $(\mathbf{L}\mathbf{K})^T\mathbf{B}(\mathbf{L}\mathbf{K}) = \mathbf{K}^T(\mathbf{L}^T\mathbf{B}\mathbf{L})\mathbf{K} = \mathbf{K}^T\mathbf{I}\mathbf{K} = \mathbf{K}^T\mathbf{K} = \mathbf{I}$ as $\mathbf{L}^T\mathbf{B}\mathbf{L} = \mathbf{I}$ and $\mathbf{K}$ is orthogonal. Therefore $S \equiv \mathbf{y}^T\mathbf{y}$. ●

Theorem 5 names the diagonal forms which are obtained by the simultaneous reduction, which is sufficient for some applications However, for other applications the matrix $\mathbf{P}$ of the transformation is also needed and this is not easily obtained from the

proof of Theorem 5. Instead we now give a shorter construction for **P** which uses the similarity of the polynomial $\det(\mathbf{A} - \mu\mathbf{B})$ to the characteristic polynomial of **A**. We start by proving results which resemble the preliminaries for Construction 1 in Chapter 12.

• Proposition 4

Let **A** and **B** be symmetric $n \times n$ matrices over $\mathbb{R}$ and let **B** be positive definite.

(i) The roots of the polynomial in μ, $\det(\mathbf{A} - \mu\mathbf{B}) = 0$, belong to $\mathbb{R}$.

(ii) Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ and ρ, σ be roots of $\det(\mathbf{A} - \mu\mathbf{B}) = 0$ such that $(\mathbf{A} - \rho\mathbf{B})\mathbf{u} = \mathbf{0}$ and $(\mathbf{A} - \sigma\mathbf{B})\mathbf{v} = \mathbf{0}$, where $\rho \neq \sigma$. Then $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^T\mathbf{B}\mathbf{v} = 0$ and we say that **u** and **v** are **B-orthogonal**.

(iii) Let σ be an m-times repeated root of $\det(\mathbf{A} - \mu\mathbf{B}) = 0$. Then the vector space V_σ of solutions of $(\mathbf{A} - \sigma\mathbf{B})\mathbf{x} = \mathbf{0}$ has a basis C_σ consisting of m vectors in which each pair is **B**-orthogonal.

PROOF

(i) By Theorem 5, there exists a non-singular matrix **P** over $\mathbb{R}$ such that $\mathbf{P}^T\mathbf{A}\mathbf{P} = \mathbf{D}$, where the diagonal elements of the diagonal matrix **D** are the roots of $\det(\mathbf{A} - \mu\mathbf{B})$. Because **A** and **P** are over $\mathbb{R}$, the matrix **D** is over $\mathbb{R}$. It follows that the roots of $\det(\mathbf{A} - \mu\mathbf{B})$ are in $\mathbb{R}$.

(ii) The proof of Proposition 3 of Chapter 12 with the equations $\mathbf{A}\mathbf{u} = \lambda\mathbf{u}$ and $\mathbf{A}\mathbf{v} = \mu\mathbf{v}$ replaced by $\mathbf{A}\mathbf{u} = \rho\mathbf{B}\mathbf{u}$ and $\mathbf{A}\mathbf{v} = \sigma\mathbf{B}\mathbf{v}$ leads to $(\rho - \sigma)\mathbf{v}^T\mathbf{B}\mathbf{u} = 0$. Consequently $\langle \mathbf{v}, \mathbf{u} \rangle = \mathbf{v}^T\mathbf{B}\mathbf{u} = 0$.

(iii) By Theorem 5, there exists a non-singular matrix **P** over $\mathbb{R}$ such that $\mathbf{P}^T\mathbf{A}\mathbf{P} = \mathbf{D}$ and $\mathbf{P}^T\mathbf{B}\mathbf{P} = \mathbf{I}$, with the matrix **D** defined in (i). Because σ is an m-times repeated root of $\det(\mathbf{A} - \sigma\mathbf{B})$, the number σ occurs m times in the main diagonal of **D** and therefore $\operatorname{rank}(\mathbf{D} - \sigma\mathbf{I}) = n - m$. Because multiplying by a non-zero matrix does not change the rank,

$$\begin{aligned}\operatorname{rank}(\mathbf{A} - \sigma\mathbf{B}) &= \operatorname{rank}\left[\mathbf{P}^T(\mathbf{A} - \sigma\mathbf{B})\mathbf{P}\right] \\ &= \operatorname{rank}\left[\mathbf{P}^T\mathbf{A}\mathbf{P} - \sigma\mathbf{P}^T\mathbf{B}\mathbf{P}\right] \\ &= \operatorname{rank}(\mathbf{D} - \sigma\mathbf{I}) = n - m.\end{aligned}$$

Consequently the nullity of $\mathbf{A} - \sigma\mathbf{B}$ is m and, by Theorem 2 of Chapter 4, $\dim V_\sigma = m$. Therefore V_σ has a basis B_σ containing m vectors over $\mathbb{R}$. We now apply the Gram–Schmidt process with respect to the inner product $\langle \mathbf{v}, \mathbf{u} \rangle$ to B_σ. Then, by Theorem 2 of Chapter 11 with respect to the inner product $\langle \mathbf{v}, \mathbf{u} \rangle$, C_σ is a basis of V_σ containing m vectors in which each pair of vectors is **B**-orthogonal. ●

We can now justify the following construction, which is very similar to Construction 1 of Chapter 12.

• Construction 2

Let Q be a quadratic form in n indeterminates $x_1, x_2, x_3, \ldots, x_n$ over $\mathbb{R}$ and let R be a positive definite quadratic form in $x_1, x_2, x_3, \ldots, x_n$ over $\mathbb{R}$. The following construction

gives a non-singular transformation over $\mathbb{R}$ which reduces Q and R simultaneously to diagonal form.

(1) Apply Lagrange's process (Construction 1) to R and evaluate the rank, r, and signature, s, of Q. If $r = s = n$, then, by Theorem 4, R is positive definite by Theorem 4, as required. Otherwise apply Lagrange's process to Q to prove that Q is positive definite and exchange the names Q and R.

(2) Choose an order for the indeterminates and form the column vector $\mathbf{x} = (x_1 \ x_2 \ x_3 \ \ldots \ x_n)^{\mathrm{T}}$.

(3) Find the unique symmetric $n \times n$ matrices $\mathbf{A}$ and $\mathbf{B}$ over $\mathbb{R}$ such that $Q \equiv \mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x}$ and $R \equiv \mathbf{x}^{\mathrm{T}}\mathbf{B}\mathbf{x}$ by the construction in Proposition 1 of Chapter 12.

(4) Find the roots of $\det(\mathbf{A} - \mu\mathbf{B}) = 0$, which are in $\mathbb{R}$ by Proposition 4(i).

(5) For each unrepeated root ρ of $\det(\mathbf{A} - \mu\mathbf{B}) = 0$, find a solution $\mathbf{b}_\rho$ of the equation $(\mathbf{A} - \rho\mathbf{B})\mathbf{x} = \mathbf{0}$ which then forms a basis of the vector space of solutions, as in Proposition 1 of Chapter 7. Then, by Proposition 4(ii), $\mathbf{b}_\rho$ is $\mathbf{B}$-orthogonal to all vectors associated with other roots of $\det(\mathbf{A} - \mu\mathbf{B})$.

(6) For each m_σ-times repeated root σ of $\det(\mathbf{A} - \mu\mathbf{B})$ we find a basis C_σ of m_σ vectors for the solution space of $(\mathbf{A} - \sigma\mathbf{B})\mathbf{x} = \mathbf{0}$ in which each pair is $\mathbf{B}$-orthogonal, as constructed in Proposition 4(iii).

(7) Let $D = \{\mathbf{b}_\rho, C_\sigma : \det(\mathbf{A} - \rho\mathbf{B}) = 0, \det(\mathbf{A} - \sigma\mathbf{B}) = 0\}$. D is $\mathbf{B}$-orthogonal by construction, therefore D is linearly independent over $\mathbb{R}$ by Proposition 4 of Chapter 10. The number of vectors in D is n, the total number of roots of $\det(\mathbf{A} - \mu\mathbf{B})$, therefore D is a $\mathbf{B}$-orthogonal basis of $\mathbb{R}^n$, by Proposition 3 of Chapter 3.

(8) Divide each vector $\mathbf{d}$ in D by $\sqrt{\langle \mathbf{d}, \mathbf{d} \rangle}$, which is possible because $\langle \mathbf{d}, \mathbf{d} \rangle \neq 0$ by Proposition 3. This constructs a $\mathbf{B}$-orthogonal basis E of $\mathbb{R}^n$ which consists of vectors for which $\langle \mathbf{e}_i, \mathbf{e}_i \rangle = 1$ for $i = 1, 2, \ldots, n$, by Proposition 2(ii) of Chapter 11. Because each pair of vectors is $\mathbf{B}$-orthogonal, $\langle \mathbf{e}_i, \mathbf{e}_j \rangle = \delta_{ij}$ for $i, j = 1, 2, 3, \ldots, n$.

(9) Define $\mathbf{P} = (\mathbf{e}_1 \ \mathbf{e}_2 \ \mathbf{e}_3 \ \ldots \ \mathbf{e}_n)$, where $E = \{\mathbf{e}_j : j = 1, 2, 3, \ldots, n\}$. Then the element in the ith row and jth column of $\mathbf{P}^{\mathrm{T}}\mathbf{B}\mathbf{P}$ is $\mathbf{e}_i^{\mathrm{T}}\mathbf{B}\mathbf{e}_j = \langle \mathbf{e}_i, \mathbf{e}_j \rangle = \delta_{ij}$, by (8). Therefore $\mathbf{P}^{\mathrm{T}}\mathbf{B}\mathbf{P} = \mathbf{I}$. Also, by (5) and (6), there is a root τ of $\det(\mathbf{A} - \mu\mathbf{B})$ such that $(\mathbf{A} - \tau\mathbf{B})\mathbf{e}_j = \mathbf{0}$ and therefore $\mathbf{A}\mathbf{e}_j = \tau\mathbf{B}\mathbf{e}_j$. Consequently, $\mathbf{e}_i^{\mathrm{T}}\mathbf{A}\mathbf{e}_j = \tau\,\mathbf{e}_i^{\mathrm{T}}\mathbf{B}\mathbf{e}_j = \tau\delta_{ij}$. Because the element in the ith row and jth column of $\mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P}$ is $\mathbf{e}_i^{\mathrm{T}}\mathbf{A}\mathbf{e}_j$ and because (5) and (6) ensure that for each root of $\det(\mathbf{A} - \mu\mathbf{B})$ the number of vectors in E is equal to the number of repetitions as a root, we conclude that $\mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P} = \mathbf{D}$, where $\mathbf{D}$ is a diagonal matrix with the roots of $\det(\mathbf{A} - \mu\mathbf{B})$ as the diagonal elements. Therefore, by Proposition 2 of Chapter 12, the non-singular transformation $\mathbf{x} = \mathbf{P}\mathbf{y}$ over $\mathbb{R}$ transforms $Q \equiv \mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x}$ into $\mathbf{y}^{\mathrm{T}}\mathbf{D}\mathbf{y}$ and the positive definite quadratic form $R \equiv \mathbf{x}^{\mathrm{T}}\mathbf{B}\mathbf{x}$ into $\mathbf{y}^{\mathrm{T}}\mathbf{y}$.

Just like the construction for an orthogonal transformation of a quadratic form in Construction 1 of Chapter 12, the process of Construction 2 is simpler than the description suggests. In practice, the only difficulty is the solution of the equation $\det(\mathbf{A} - \mu\mathbf{B}) = 0$.

○ *Example 5*

Let us attempt the simultaneous reduction over $\mathbb{R}$ of the quadratic forms $Q \equiv 2yz - y^2 - 2z^2$ and $R \equiv x^2 + 5y^2 + 3z^2 + 4xy + 2xz + 2yz$ over $\mathbb{R}$.

(1) Because the rank of Q is obviously less than 3, we need R to be positive definite. Then

$$\begin{aligned} R &\equiv (x^2+4xy+2xz)+5y^2+3z^2+2yz \\ &\equiv (x^2+4y^2+z^2+4xy+2xz+4yz)+y^2+2z^2-2yz \\ &\equiv (x+2y+z)^2+(y-z)^2+z^2. \end{aligned}$$

Therefore R is a positive definite quadratic form by Theorem 4(i).

(2) We choose $\mathbf{x} = (x \quad y \quad z)^{\mathrm{T}}$.

(3) By inspection, $Q \equiv \mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x}$ and $R \equiv \mathbf{x}^{\mathrm{T}}\mathbf{B}\mathbf{x}$, where

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & -2 \end{pmatrix} \qquad \text{and} \qquad \mathbf{B} = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 5 & 1 \\ 1 & 1 & 3 \end{pmatrix}.$$

(4) We now solve the equation $\det(\mathbf{A} - \mu\mathbf{B}) = 0$: by subtracting multiples of the first row from the others, we obtain

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

Therefore the roots of $\det(\mathbf{A} - \mu\mathbf{B})$ are $\mu = 0, -1, -1$.

(5) For the unrepeated root $\mu = 0$, the system of equations is $\mathbf{A}\mathbf{x} = \mathbf{0}$. This is $-y + z = 0$, $y - 2z = 0$. The absent unknown x is therefore disposable and the solutions are $\mathbf{x} = (\psi \quad 0 \quad 0)^{\mathrm{T}}$ for all $0 \neq \psi \in \mathbb{R}$. We choose the solution $\mathbf{b} = (1 \quad 0 \quad 0)^{\mathrm{T}}$.

(6) For the twice repeated root $\mu = -1$, the system of equations $(\mathbf{A} + \mathbf{B})\mathbf{x} = \mathbf{0}$ reduces to the equation $x + 2y + z = 0$. Therefore the solution space is

$$V_{-1} = \{((-2\theta - \phi) \quad \theta \quad \phi)^{\mathrm{T}} : 0 \neq \theta, \phi \in \mathbb{R}\}.$$

A basis of V_{-1} is then $B_{-1} = \{\mathbf{s}_1 = (-2 \quad 1 \quad 0)^{\mathrm{T}}, \mathbf{s}_2 = (-1 \quad 0 \quad 1)^{\mathrm{T}}\}$. Then, by the Gram–Schmidt process for $\langle \mathbf{v}, \mathbf{u} \rangle$, we form the basis C_{-1} of V_{-1} where $C_{-1} = \{\mathbf{c}_1, \mathbf{c}_2\}$, $\mathbf{c}_1 = \mathbf{s}_1$, $\mathbf{c}_2 = \mathbf{s}_2 - p_{21}\mathbf{c}_1$ and, by the proof of Proposition 4(iii),

$$p_{21} = \langle \mathbf{c}_1, \mathbf{s}_2 \rangle / \langle \mathbf{c}_1, \mathbf{c}_1 \rangle = (\mathbf{c}_1^{\mathrm{T}}\mathbf{B}\mathbf{s}_2)/(\mathbf{c}_1^{\mathrm{T}}\mathbf{B}\mathbf{c}_1)$$

and this gives $p_{21} = 1$. Therefore $\mathbf{c}_2 = \mathbf{s}_2 + \mathbf{c}_1 = (-3 \quad 1 \quad 1)^{\mathrm{T}}$.

(7) Then $\mathbb{R}^3$ has the basis $D = \{\mathbf{b}, \mathbf{c}_1, \mathbf{c}_2\}$.

(8) We now divide each vector $\mathbf{d}_j$ in D by $\sqrt{\langle \mathbf{d}_j, \mathbf{d}_j \rangle} = \sqrt{(\mathbf{d}_j^{\mathrm{T}}\mathbf{B}\mathbf{d}_j)}$. However, in this case, $\langle \mathbf{b}, \mathbf{b} \rangle = \langle \mathbf{c}_1, \mathbf{c}_1 \rangle = \langle \mathbf{c}_2, \mathbf{c}_2 \rangle = 1$, therefore $E = D$.

(9) By taking the vectors of E as the columns of $\mathbf{P}$, we obtain the required matrix of the transformation as $\mathbf{P} = \begin{pmatrix} 1 & -2 & -3 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Summary

The identification of a turning point of a real function of several real variables leads to a need for a classification of quadratic forms over $\mathbb{R}$ into **value classes**. The most important value classes are the classes of **positive definite** forms, which are positive except at **0**, and **negative definite** forms, which are negative except at **0**. The value class of a quadratic form over $\mathbb{R}$ can be determined from the eigenvalues of the associated matrix, although finding the roots of the characteristic polynomial introduces difficulties. An easier alternative approach uses **Lagrange's process**, which constructs a non-singular transformation of any quadratic form Q over a field $\mathbb{F}$ which is not of characteristic 2 into a diagonal form D. In fact, for all such fields $\mathbb{F}$, rank D = rank Q. Moreover, for $\mathbb{F} = \mathbb{R}$, **Sylvester's law of inertia** asserts that the **signature**, s, of Q is an invariant, where s is the difference between the number of positive coefficients of D and the number of negative coefficients of D. The value class of Q can be deduced easily from the values of r and s. The rest of the chapter is devoted to **simultaneous reduction** of two quadratic forms Q and R over $\mathbb{R}$ to diagonal forms by means of a non-singular transformation of the indeterminates. It is proved that this is always possible when one of the quadratic forms is positive definite, and a construction for obtaining the transformation is found for this case.

EXERCISES ON CHAPTER 13

1. Determine the value class of each of the nine quadratic forms $Q(b, c)$ over $\mathbb{R}$ in the indeterminates x, y, z given by $Q(b, c) = x^2 + by^2 + cz^2$, where $b, c = -1, 0, 1$.

2. Determine the value class of each of the following three quadratic forms over $\mathbb{R}$ in the indeterminates x and y:
   (i) $Q_1 \equiv 4x^2 - 4xy + y^2$, (ii) $Q_2 \equiv 7xy$,
   (iii) $Q_3 \equiv 6xy - x^2 - 10y^2$.

3. Find the eigenvalues and determine the value classes of the following quadratic forms over $\mathbb{R}$ in the indeterminates x, y, z.
   (i) $Q_1 \equiv 2xy + z^2$,
   (ii) $Q_2 \equiv x^2 - 2y^2 + z^2 + 4xy$,
   (iii) $Q_3 \equiv x^2 + y^2 + z^2 + 2xy$,
   (iv) $Q_4 \equiv (x + 2y - z)(3x - y)$.

4. Use Lagrange's process to transform each of the following ten quadratic forms over $\mathbb{R}$ in the indeterminates x, y, z into diagonal forms.
   (i) $Q_1 \equiv 14xy - 7x^2 - 7y^2$,
   (ii) $Q_2 \equiv x^2 - 5z^2 - 6xy + 4xz + 6yz$,
   (iii) $Q_3 \equiv x^2 + 2y^2 + 2z^2 - 2xy - 2yz$,
   (iv) $Q_4 \equiv -4x^2 - 2y^2 - 2z^2 + 4xy + 2yz$,
   (v) $Q_5 \equiv 5x^2 + y^2 + 2z^2 + 4xy - 6xz - 2yz$,
   (vi) $Q_6 \equiv x^2 + 4y^2 + 9z^2 - 4xy - 6xz + 13yz$,
   (vii) $Q_7 \equiv 3x^2 + 27y^2 + 3z^2 + 18xy - 6xz - 18yz$,
   (viii) $Q_8 \equiv 3x^2 + 14y^2 + 26z^2 + 12xy - 6xz$,

(ix) $Q_9 \equiv -x^2 - 2y^2 - z^2 + 2xy + 2xz - 2yz$,
(x) $Q_{10} \equiv xy + yz + zx$.

5. Use Lagrange's process to transform each of the following three quadratic forms over $\mathbb{C}$ in the indeterminates x, y, z into diagonal forms:

(i) $x^2 - z^2 + 2ixy + 4xz$,
(ii) $(1 + i)x^2 + (5 + 3i)y^2 - iz^2 + (4 + 4i)xy - (2 - 2i)yz$,
(iii) $2ix^2 - (1 + 2i)y^2 - z^2 + 4xy + 2yz$.

6. Which of the following three quadratic forms over $\mathbb{Q}$ in the indeterminates x, y, z is equivalent over $\mathbb{Q}$ to $u^2 + v^2 + w^2$, where u, v, w are indeterminates?

(i) $x^2 + 2y^2 + z^2 - 2xy - 2xz$,
(ii) $4x^2 + 37y^2 + 14z^2 - 8xz - 20yz$,
(iii) $2x^2 + 3y^2 + 11z^2 - 4xy + 4xz$.

7. Find the ranks and signatures of the quadratic forms in Exercise 4.

8. Determine the value class of each quadratic form in Exercise 4.

9. Prove that two quadratic forms over $\mathbb{C}$ in the same indeterminates are equivalent if and only if they have the same rank.

10. Show that $Q \equiv x^2 + 6xy + 8y^2$ and $R \equiv x^2 + 2xy + 4y^2$ are not equivalent over $\mathbb{R}$.

11. Show that $Q \equiv x^2 + 13y^2 + 7z^2 + 6xy + 8yz$ is a positive definite quadratic form over $\mathbb{R}$ in x, y, z. Let $\mathbf{A}$ be the symmetric matrix associated with Q. Find a non-singular transformation $\mathbf{x} = \mathbf{Pu}$ over $\mathbb{R}$ which transforms Q into $\mathbf{u}^T\mathbf{u}$. Show that $\mathbf{x} = \mathbf{Pu}$ transforms the inner product $\langle \mathbf{x}_1, \mathbf{x}_2 \rangle = \mathbf{x}_1^T\mathbf{A}\mathbf{x}$ into the scalar product $\mathbf{u}_1 . \mathbf{u}_2$.

12. Reduce the quadratic forms $Q \equiv 2xy + 5y^2$ and $R \equiv 2x^2 + 10xy + 13y^2$ simultaneously to diagonal forms over $\mathbb{R}$.

13. Reduce the quadratic forms $Q \equiv x^2 - 4y^2 + 2xy - 4yz$ and $R \equiv x^2 + 2y^2 + 5z^2 + 2xy + 4yz$ simultaneously to diagonal forms over $\mathbb{R}$.

14. Reduce the quadratic forms $Q \equiv 4x^2 + y^2 + z^2 + 4xy - 4xz - 2yz$ and $R \equiv 13x^2 + 2y^2 + 3z^2 + 10xy - 10xz - 4yz$ simultaneously to diagonal forms over $\mathbb{R}$.

14 · Further Developments

Outline

The main results of this chapter modify for vector spaces over $\mathbb{C}$ the work of Chapters 10–13, which requires vector spaces to be over $\mathbb{R}$. The foundation for the extension of these results is the definition of an inner product, the 'Euclidean inner product' $\mathbf{v} \odot \mathbf{w}$ for vectors $\mathbf{v}, \mathbf{w} \in \mathbb{C}^n$. This leads to a satisfactory definition of length for a vector and for orthogonality of vectors, but not to a concept of angle between vectors in $\mathbb{C}^n$. Properties of Euclidean vector spaces over $\mathbb{R}$ were proved by using the transpose of a matrix, whose place in proofs concerning vector spaces over $\mathbb{C}$ is taken by the 'conjugate transpose' $\mathbf{A}^*$ of a matrix $\mathbf{A}$ over $\mathbb{C}$. The properties of orthogonal matrices over $\mathbb{R}$ hold for a matrix $\mathbf{U}$ over $\mathbb{C}$ if it is 'unitary', that is, if $\mathbf{U}^*\mathbf{U} = \mathbf{I}$. The places of quadratic forms and symmetric matrices for vector spaces over $\mathbb{C}$ are taken by 'Hermitian forms' and 'Hermitian matrices' for vector spaces over $\mathbb{C}$. The properties of Hermitian matrices over $\mathbb{C}$ strongly resemble those of symmetric matrices over $\mathbb{R}$.

Introduction

Some applications of linear algebra to physics require methods and results like those discussed in Chapters 10–13 but require the field of complex numbers instead of $\mathbb{R}$. Example 2 in Chapter 10 showed that the dot product for $\mathbb{R}^n$ gives unsatisfactory results when applied to $\mathbb{C}^n$. However, the **complex conjugate** $\overline{c} = a - ib$

• Definition 1

Let $\mathbf{A}$ be a matrix over $\mathbb{C}$. The **complex conjugate** $\overline{\mathbf{A}}$ of $\mathbf{A}$ is formed by replacing each element of $\mathbf{A}$ by its complex conjugate and the **conjugate transpose** $\mathbf{A}^*$ of $\mathbf{A}$ is the complex conjugate of $\mathbf{A}^T$.

The properties of the conjugate transposes of matrices are easy to prove, and we summarize those that we use in the following proposition.

• Proposition 1

Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times n$ matrices over $\mathbb{C}$ and let $c \in \mathbb{C}$. Then

(i) $(\mathbf{A}^*)^* = \mathbf{A}$;
(ii) $(\mathbf{A} + \mathbf{B})^* = \mathbf{A}^* + \mathbf{B}^*$;

(iii) $(\mathbf{cA})^* = \bar{c}\mathbf{A}^*$;
(iv) $(\mathbf{AB})^* = \mathbf{B}^*\mathbf{A}^*$.

We can now define the most commonly used inner product for $\mathbb{C}^n$.

• Definition 2

Let n be a positive integer and $\mathbf{v}, \mathbf{w} \in \mathbb{C}^n$. The **Euclidean inner product** $\mathbf{v}\odot\mathbf{w}$ of $\mathbf{v}$ and $\mathbf{w}$ is given by $\mathbf{v}\odot\mathbf{w} = \mathbf{v}^*\mathbf{w}$, where $\mathbf{v}$ and $\mathbf{w}$ are regarded as column vectors.

A vector space $\mathbb{C}^n$ with the Euclidean inner product is called a **unitary vector space**. The Euclidean inner product is usually a complex rather than a real number, as is clear from the following example.

⊙ Example 1

Consider $\mathbf{u} = (1 + \mathrm{i}, 7 + 5\mathrm{i}, 2 - 3\mathrm{i})$ and $\mathbf{v} = (2, \mathrm{i}, 2 - 3\mathrm{i}) \in \mathbb{C}^3$. Then

$$\begin{aligned}\mathbf{u}\odot\mathbf{v} &= \overline{(1+\mathrm{i})}2 + \overline{(7+5\mathrm{i})}\mathrm{i} + \overline{(2-3\mathrm{i})}(2-3\mathrm{i}) \\ &= (1-\mathrm{i})2 + (7-5\mathrm{i})\mathrm{i} + (2+3\mathrm{i})(2-3\mathrm{i}) \\ &= 2 - 2\mathrm{i} + 5 + 7\mathrm{i} + 13 \\ &= 20 + 5\mathrm{i}.\end{aligned}$$

Therefore $\mathbf{u}\odot\mathbf{v} \in \mathbb{C}$ is not a real number, and indeed

$$\begin{aligned}\mathbf{v}\odot\mathbf{u} &= \bar{2}(1+\mathrm{i}) + \bar{\mathrm{i}}(7+5\mathrm{i}) + \overline{(2-3\mathrm{i})}(2-3\mathrm{i}) \\ &= 2(1+\mathrm{i}) - \mathrm{i}(7+5\mathrm{i}) + (2+3\mathrm{i})(2-3\mathrm{i}) \\ &= 2 + 2\mathrm{i} + 5 - 7\mathrm{i} + 13 \\ &= 20 - 5\mathrm{i},\end{aligned}$$

therefore in this case $\mathbf{v}\odot\mathbf{u} = \overline{\mathbf{u}\odot\mathbf{v}}$. However,

$$\begin{aligned}\mathbf{u}\odot\mathbf{u} &= \overline{(1+\mathrm{i})}(1+\mathrm{i}) + \overline{(7+5\mathrm{i})}(7+5\mathrm{i}) + \overline{(2-3\mathrm{i})}(2-3\mathrm{i}) \\ &= (1-\mathrm{i})(1+\mathrm{i}) + (7-5\mathrm{i})(7+5\mathrm{i}) + (2+3\mathrm{i})(2-3\mathrm{i}) \\ &= (1^2 + 1^2) + (7^2 + 5^2) + (2^2 + 3^2) \\ &= 89 \in \mathbb{R}.\end{aligned}$$

In fact, Definition 2 suggests that $\mathbf{w}\odot\mathbf{w}$ may be real for all $\mathbf{w} \in \mathbb{C}^n$.

The following proposition can be proved in the same way as Proposition 1 of Chapter 10, but the results differ. The important difference is that, for $\mathbf{v}, \mathbf{w} \in \mathbb{C}^n$, $\mathbf{v}\odot\mathbf{w} \neq \mathbf{w}\odot\mathbf{v}$ unless $\mathbf{v}\odot\mathbf{w} \in \mathbb{R}$. Also there is a weaker result concerning $c(\mathbf{v}\odot\mathbf{w})$ for $c \in \mathbb{C}$.

• Proposition 2

Let $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{C}^n$ and let $c \in \mathbb{C}$. Then the following are true:

(i) $\mathbf{v}\odot\mathbf{w} = \overline{\mathbf{w}\odot\mathbf{v}}$;
(ii) $\mathbf{u}\odot(\mathbf{v} + \mathbf{w}) = \mathbf{u}\odot\mathbf{v} + \mathbf{u}\odot\mathbf{w}$;
(iii) $(c\mathbf{v})\odot\mathbf{w} = \bar{c}(\mathbf{v}\odot\mathbf{w})$ and $\mathbf{v}\odot(c\mathbf{w}) = c(\mathbf{v}\odot\mathbf{w})$;
(iv) $\mathbf{v}\odot\mathbf{v} \in \mathbb{R}$ and $\mathbf{v}\odot\mathbf{v} \geq 0$;
(v) $\mathbf{v}\odot\mathbf{v} = 0 \Leftrightarrow \mathbf{v} = \mathbf{0}$.

TUTORIAL PROBLEM 14.1

Prove Proposition 2.

Proposition 2 can be used to define an abstract 'inner product' for a vector space over $\mathbb{C}$ as in Definition 2 of Chapter 10, although, due to the differences in parts (i) and (iii), the resulting inner product over $\mathbb{C}$ differs from the inner product of Chapter 10. Parts (iv) and (v) of Proposition 2 enable us to ascribe a magnitude to $\mathbf{v} \in \mathbb{C}^n$. We can also define orthogonality for vectors in $\mathbb{C}^n$, although the fact that the Euclidean inner product of two vectors is usually complex prevents a definition of angle between two vectors.

• *Definition 3*

Let $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{C}^n$. The **length** of $\mathbf{v}$, denoted by $\|\mathbf{v}\|$, is $\|\mathbf{v}\| = \sqrt{\mathbf{v} \odot \mathbf{v}}$ and $\mathbf{u}$ is a **unit vector** if $\|\mathbf{u}\| = 1$. The vectors $\mathbf{v}$ and $\mathbf{w}$ are **orthogonal (with respect to the Euclidean inner product)** if $\mathbf{v} \odot \mathbf{w} = 0$.

Slight changes in the proofs for the real case prove the analogue of Proposition 2 of Chapter 10, the Cauchy–Schwarz inequality and the triangle inequality for the length function of Definition 3. The following example illustrates these results.

○ *Example 2*

Let $\mathbf{v} = (1 + \mathrm{i}, \mathrm{i}, -1)$ and $\mathbf{w} = (2 - \mathrm{i}, 3, 2\mathrm{i}) \in \mathbb{C}^3$. Let us verify the Cauchy–Schwarz inequality (Theorem 1 of Chapter 10) for the product $\mathbf{v} \odot \mathbf{w}$ of Definition 2. Then $\mathbf{v} \odot \mathbf{v} = \|\mathbf{v}\|^2 = |1+\mathrm{i}|^2 + |\mathrm{i}|^2 + |-1|^2 = 4$, by Definition 3, therefore the length (or magnitude) of $\mathbf{v}$ is $\|\mathbf{v}\| = 2$. Similarly, $\mathbf{w} \odot \mathbf{w} = \|\mathbf{w}\|^2 = 18$, therefore $\|\mathbf{w}\| = 3\sqrt{2}$. As $\overline{\mathbf{v}} = (1-\mathrm{i}, -\mathrm{i}, -1)$, by Definition 2, $\mathbf{v} \odot \mathbf{w} = (1 - \mathrm{i})(2 - \mathrm{i}) + (-\mathrm{i})3 + (-1)(2\mathrm{i}) = 1 - 8\mathrm{i}$. Therefore the square of the modulus of $\mathbf{v} \odot \mathbf{w}$ is $|\mathbf{v} \odot \mathbf{w}|^2 = 65$. Also the product of the squares of the lengths of $\mathbf{v}$ and $\mathbf{w}$ is $\|\mathbf{v}\|^2 \|\mathbf{w}\|^2 = 4 \times 18 = 72$. Because the modulus and the lengths are non-negative, it follows that $|\mathbf{v} \odot \mathbf{w}| \leq \|\mathbf{v}\| \|\mathbf{w}\|$ in this case. We have therefore verified the Cauchy–Schwarz inequality for $\mathbf{v}$ and $\mathbf{w}$ in $\mathbb{C}^3$.

Next, we try to find $\mathbf{x}$ in the vector space $\langle \mathbf{v}, \mathbf{w} \rangle$ such that $\{\mathbf{v}, \mathbf{x}\}$ is orthogonal according to Definition 3. To do this we let $\mathbf{x} = c\mathbf{v} + d\mathbf{w}$, where $c, d \in \mathbb{C}$. Then, by Definition 3, $\mathbf{v}$ and $\mathbf{x}$ are orthogonal if and only if $\mathbf{v} \odot \mathbf{x} = 0$. By Proposition 2, $\mathbf{v} \odot \mathbf{x} = \mathbf{v} \odot (c\mathbf{v} + d\mathbf{w}) = \mathbf{v} \odot (c\mathbf{v}) + \mathbf{v} \odot (d\mathbf{w}) = c(\mathbf{v} \odot \mathbf{v}) + d(\mathbf{v} \odot \mathbf{w}) = 4c + d(1 - 8\mathrm{i})$. Therefore $\mathbf{v}$ and $\mathbf{x}$ are orthogonal if and only if $4c + d(1 - 8\mathrm{i}) = 0$. Because we are only looking for one vector $\mathbf{x}$ which is orthogonal to $\mathbf{v}$, we can let $d = 4$ and obtain $c = -1 + 8i$. This gives us the vector $\mathbf{x} = (-1 + 3\mathrm{i}, 4 - \mathrm{i}, 1)$ for which we can confirm that $\mathbf{v} \odot \mathbf{x} = 0$.

In Theorem 3 of Chapter 10 we found that the dot product is preserved for Euclidean vector spaces over $\mathbb{R}$ if the transition matrix of the transformation is orthogonal. We give a similar definition to find transformations which preserve the Euclidean inner product.

• Definition 4

A square matrix $\mathbf{U}$ over $\mathbb{C}$ is **unitary** if it satisfies $\mathbf{U}^*\mathbf{U} = \mathbf{I}$.

The main properties of unitary matrices are summarized in the following two results, which can be proved by methods like those used in Theorem 3 of Chapter 10 and Proposition 1 of Chapter 11, although they are slightly weaker than the corresponding results for orthogonal matrices.

• Theorem 1

Let the Euclidean inner product be defined on $\mathbb{C}^n$. Then the Euclidean inner product is preserved in the representation defined by the transition matrix $\mathbf{P}$ if and only if $\mathbf{P}$ is unitary.

• Proposition 3

Let $\mathbf{A}$ and $\mathbf{B}$ be unitary $n \times n$ matrices over $\mathbb{C}$. Then:

(i) the modulus of the determinant of $\mathbf{A}$, $|\det \mathbf{A}| = 1$;
(ii) $\mathbf{A}^{-1} = \mathbf{A}^*$ is unitary;
(iii) $\mathbf{A}^T$, $\overline{\mathbf{A}}$ and $\mathbf{AB}$ are unitary;
(iv) $\mathbf{A}$ is unitary if and only if the columns (or rows) of $\mathbf{A}$ form an orthonormal set, that is, an orthogonal set of unit vectors;
(v) each eigenvalue of $\mathbf{A}$ has modulus 1.

PROOF OF (v)
Let λ be an eigenvalue of the unitary matrix $\mathbf{A}$ and let $\mathbf{v} \neq \mathbf{0}$ be an eigenvector associated with λ. Then $\mathbf{Av} = \lambda\mathbf{v}$ and, by Proposition 1, $\mathbf{v}^*\mathbf{A}^* = \bar{\lambda}\mathbf{v}^*$. By multiplying these two equations we obtain $\mathbf{v}^*\mathbf{A}^*\mathbf{Av} = \bar{\lambda}\mathbf{v}^*\lambda\mathbf{v}$ and therefore $\mathbf{v}^*\mathbf{v} = \bar{\lambda}\lambda\mathbf{v}^*\mathbf{v}$, by Definition 4. Consequently, by Definition 3, $\|\mathbf{v}\|^2(|\lambda|^2 - 1) = 0$ and it follows from Proposition 2(v) that $\|\mathbf{v}\|^2 \neq 0$ and therefore $|\lambda|^2 = 1$. ●

For any real matrix $\mathbf{B}$ the conjugate transpose $\mathbf{B}^* = \mathbf{B}^T$ and therefore any orthogonal matrix $\mathbf{A}$ over $\mathbb{R}$ is unitary because it satisfies $\mathbf{A}^T\mathbf{A} = \mathbf{I}$. Therefore Proposition 3(v) implies that an eigenvalue of $\mathbf{A}$ which is in $\mathbb{R}$ is either 1 or -1 and that complex eigenvalues of $\mathbf{A}$ have modulus 1 and occur in complex conjugate pairs. Proposition 3(iv) shows that unitary matrices can be constructed provided that orthogonal sets of vectors can be constructed. Fortunately, this is possible by the Gram–Schmidt process, although this process is slightly different over $\mathbb{C}$. The formulae of Theorem 2 in Chapter 11 still hold over $\mathbb{C}$ but, because $\mathbf{w}\odot\mathbf{v} \neq \mathbf{v}\odot\mathbf{w}$ the coefficient p_{ij} cannot be written in the alternative form $(\mathbf{b}_j\odot\mathbf{c}_i)/(\mathbf{c}_i\odot\mathbf{c}_i)$. The following example shows that, if the products are taken in the correct order, the process works just as well for $\mathbb{C}^n$.

○ Example 3

Let us find an orthonormal basis for the subspace V of $\mathbb{C}^3$ which has the basis $B = \{\mathbf{b}_1 = (1, i, i),\ \mathbf{b}_2 = (i, 0, i)\}$. Because $\mathbf{b}_1\odot\mathbf{b}_2 = 1 + i$, the basis B is not orthogonal but we can use the Gram–Schmidt process to find the orthogonal basis $C = \{\mathbf{c}_1, \mathbf{c}_2\}$ of V.

Then, we use Theorem 2 of Chapter 11 as follows. The element $\mathbf{c}_1 = \mathbf{b}_1 = (1, \mathrm{i}, \mathrm{i})$ therefore $\mathbf{c}_1 \odot \mathbf{c}_1 = |1|^2 + |\mathrm{i}|^2 + |\mathrm{i}|^2 = 3$ and $\mathbf{c}_1 \odot \mathbf{b}_2 = 1 + \mathrm{i}$. Then the coefficient $p_{12} = (1 + \mathrm{i})/3$, and consequently

$$\begin{aligned}\mathbf{c}_2 &= \mathbf{b}_2 - p_{12}\mathbf{c}_1 = (\mathrm{i}, 0, \mathrm{i}) - [(1+\mathrm{i})/3](1, \mathrm{i}, \mathrm{i}) \\ &= (-1+2\mathrm{i},\ 1-\mathrm{i},\ 1+2\mathrm{i})/3.\end{aligned}$$

By Definition 3, the length of a vector in $\mathbb{C}^3$ is real, therefore, by Proposition 2(iii), $\mathbf{d}_1 = \mathbf{c}_1/\|\mathbf{c}_1\|$ and $\mathbf{d}_2 = \mathbf{c}_2/\|\mathbf{c}_2\|$ are unit vectors. Therefore an orthonormal basis of V is $D = \{\mathbf{d}_1, \mathbf{d}_2\}$, where

$$\mathbf{d}_1 = \frac{1}{\sqrt{3}}(1, \mathrm{i}, \mathrm{i}), \qquad \mathbf{d}_2 = \frac{1}{2\sqrt{3}}(-1+2\mathrm{i},\ 1-\mathrm{i},\ 1+2\mathrm{i}).$$

In Chapter 12 we showed that symmetric matrices and quadratic forms over $\mathbb{R}$ are orthogonally similar to diagonal matrices and forms. The corresponding results over $\mathbb{C}$ were proved for applications to physics and show that the following forms and matrices are similar to diagonal forms and matrices by transformation by unitary matrices.

• Definition 5

Let $\mathbf{H}$ and $\mathbf{S}$ be $n \times n$ matrices over $\mathbb{C}$ and let $\mathbf{x}$ be a column vector of which the elements are n indeterminates. Then $\mathbf{H}$ is **Hermitian** if $\mathbf{H}^* = \mathbf{H}$, $\mathbf{S}$ is **skew-Hermitian** if $\mathbf{S}^* = -\mathbf{S}$ and a **Hermitian form** is a polynomial in indeterminates and their complex conjugates given by $\mathbf{x}^*\mathbf{H}\mathbf{x}$. The matrix $\mathbf{B}$ over $\mathbb{C}$ is **unitarily similar** to matrix $\mathbf{A}$ over $\mathbb{C}$ if there exists a unitary matrix $\mathbf{U}$ such that $\mathbf{U}^*\mathbf{B}\mathbf{U} = \mathbf{A}$.

Because of the related definitions for forms and matrices over $\mathbb{R}$ and over $\mathbb{C}$, it is reasonable to expect results over $\mathbb{C}$ resembling those that we have already found over $\mathbb{R}$. Although this idea is broadly true, there are a few surprising differences. Let us look at some examples before obtaining the basic properties.

○ Example 4

Let $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in \mathbb{C}$. Then $\mathbf{A}$ is Hermitian if and only if $\mathbf{A} = \mathbf{A}^* = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$, which holds if and only if $\bar{a} = a$, $\bar{d} = d$, $\bar{c} = b$ and $\bar{b} = c$. Therefore A is Hermitian if and only if $a, d \in \mathbb{R}$ and $c = \bar{b}$. Therefore $\mathbf{B} = \begin{pmatrix} 2 & \mathrm{i} \\ -\mathrm{i} & 3 \end{pmatrix}$ is an example of a Hermitian matrix, and so is any 2×2 symmetric matrix over $\mathbb{R}$. Consequently, for $\mathbf{x} = (x \quad y)^{\mathrm{T}}$, $F = \mathbf{x}^*\mathbf{B}\mathbf{x} \equiv 2\bar{x}x + 3\bar{y}y + \mathrm{i}\bar{x}y - \mathrm{i}\bar{y}x$ is a Hermitian form. Let us substitute $x = g \in \mathbb{C}$ and $y = h \in \mathbb{C}$ into F. This gives us

$$\begin{aligned}F(g,h) &= 2|g|^2 + 3|h|^2 + \mathrm{i}\bar{g}h - \mathrm{i}\bar{h}g \\ &= 2|g|^2 + 3|h|^2 + s\end{aligned}$$

where $s = i\bar{g}h - i\bar{h}g$. But the conjugate of $i\bar{g}h$ *is* $i\bar{h}g$, therefore s is twice the real part of $i\bar{g}h$. Therefore $s \in \mathbb{R}$ and, because the other terms are obviously in $\mathbb{R}$, $F(g, h) \in \mathbb{R}$ for arbitary $g, h \in \mathbb{C}$.

Definition 1 of Chapter 12 defines a quadratic form as a special kind of polynomial, but there is no such definition for a Hermitian form, although there is a definition by means of axioms. We can illustrate the difficulties with the polynomials $i\bar{x}x$ and $2\bar{x}y$. The matrix of coefficients for $i\bar{x}x$ is the 1×1 matrix $\mathbf{A} = (i)$ for which $\mathbf{A}^* \neq \mathbf{A}$, therefore $\mathbf{A}$ is certainly not Hermitian. For $2\bar{x}y$ the matrix of coefficients is $\mathbf{B} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$ and this cannot be replaced by a Hermitian matrix such as $\mathbf{C} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ because that gives the Hermitian form $\bar{x}y + \bar{y}x$ which differs from $2\bar{x}y$ when, for example, $x = 1$ and $y = i$.

• Proposition 4

Let $\mathbf{H}$ be a Hermitian matrix of rank r over $\mathbb{C}$ and let F be the Hermitian form $F \equiv \mathbf{x}^*\mathbf{H}\mathbf{x}$. Then the following hold:

(i) The diagonal elements of $\mathbf{H}$ and the coefficients of terms of the form $\bar{x}x$ in F belong to $\mathbb{R}$.
(ii) For all values of $\mathbf{x}$ over $\mathbb{C}$, the value of F is real.
(iii) Let F_1 be the form in indeterminates which are elements of the column vector $\mathbf{y}$ into which F is transformed by a non-singular transformation. Then there exists a non-singular matrix $\mathbf{P}$ over $\mathbb{C}$ such that F_1 has associated Hermitian matrix $\mathbf{P}^*\mathbf{H}\mathbf{P}$, and rank $\mathbf{P}^*\mathbf{H}\mathbf{P} = r$.

PROOF

(i) For a diagonal element h_{jj} of $\mathbf{H}$, Definition 5 gives $\bar{h}_{jj} = h_{jj}$ and therefore $h_{jj} \in \mathbb{R}$.

(ii) Let $\mathbf{x} = \mathbf{v}$ over $\mathbb{C}$. Then the complex conjugate of $F(\mathbf{v})$ is given by

$$\overline{F(\mathbf{v})} = \overline{\mathbf{v}^*\mathbf{H}\mathbf{v}} = \mathbf{v}^{\mathrm{T}}\overline{\mathbf{H}}\,\overline{\mathbf{v}}$$

by Definition 3. Because any 1×1 matrix is its own transpose,

$$\overline{F(\mathbf{v})} = \left(\mathbf{v}^{\mathrm{T}}\overline{\mathbf{H}}\,\overline{\mathbf{v}}\right)^{\mathrm{T}} = \overline{\mathbf{v}}^{\mathrm{T}}\overline{\mathbf{H}}^{\mathrm{T}}\mathbf{v} = \mathbf{v}^*\mathbf{H}^*\mathbf{v} = \mathbf{v}^*\mathbf{H}\mathbf{v}$$

because $\mathbf{H}$ is Hermitian. Therefore $\overline{F(\mathbf{v})} = F(\mathbf{v})$, and consequently $F(\mathbf{v}) \in \mathbb{R}$.

(iii) This is proved like Proposition 2 of Chapter 12. •

Our first problem concerning Hermitian forms is related to Question 1 of Chapter 12, though it does not have the strong geometrical motivation of that question. However, Proposition 4(iii) and Definition 5 allow us to convert this problem into the following question about matrices.

QUESTION 1

Let $\mathbf{H}$ be a Hermitian matrix over $\mathbb{C}$. Is $\mathbf{H}$ unitarily similar to a diagonal matrix over $\mathbb{R}$?

The similar Question 2 of Chapter 12 about symmetric matrices over $\mathbb{R}$ was solved by obtaining the properties of their eigenvalues and eigenvectors. By replacing the dot product by the Euclidean scalar product, the transpose by the conjugate transpose, the symmetric matrix **A** by the Hermitian matrix **H** and the orthogonal matrix **P** by the unitary matrix **U**, we can prove the following theorem.

• *Theorem 2*

Let **H** be an $n \times n$ Hermitian matrix over $\mathbb{C}$. Then there exists a unitary matrix **U** such that $\mathbf{U^*HU = D}$, where **D** is a diagonal matrix over $\mathbb{R}$ of which the diagonal elements are the eigenvalues $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n$ of **H**.

The following example shows how a modification of Construction 1 of Chapter 12 can determine the unitary matrix **U** of Theorem 2.

○ *Example 5*

Let **H** be the Hermitian matrix $\mathbf{H} = \begin{pmatrix} 3 & -\mathrm{i} & 0 \\ \mathrm{i} & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. Let us find a diagonal matrix **D** over $\mathbb{R}$ and a unitary matrix **U** such that $\mathbf{U^*HU = D}$ by modifying the steps of Construction 1 of Chapter 12.

(3) The eigenvalues of **H** satisfy $\chi(\lambda) = \det(\mathbf{H} - \lambda\mathbf{I}) = 0$ and, by expanding the determinant by the last row, we obtain

$$0 = \begin{vmatrix} 3-\lambda & -\mathrm{i} & 0 \\ \mathrm{i} & 3-\lambda & 0 \\ 0 & 0 & 2-\lambda \end{vmatrix} = (2-\lambda)\begin{vmatrix} 3-\lambda & -\mathrm{i} \\ \mathrm{i} & 3-\lambda \end{vmatrix}$$

$$= (2-\lambda)\left[(3-\lambda)^2 - 1\right]$$

$$= (2-\lambda)(\lambda-2)(\lambda-4).$$

Therefore, the eigenvalues of **H** are 2, 2, 4.

(4) The only unrepeated eigenvalue of **H** is 4, and its eigenvectors are the solutions of the system of linear equations with matrix of coefficients

$$\mathbf{H} - 4\mathbf{I} = \begin{pmatrix} -1 & -\mathrm{i} & 0 \\ \mathrm{i} & -1 & 0 \\ 0 & 0 & -2 \end{pmatrix} \sim \begin{pmatrix} -1 & -\mathrm{i} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}.$$

The third unknown is 0, therefore if we take the disposable second unknown as i, we find the eigenvector $\mathbf{b}_4 = (1 \quad \mathrm{i} \quad 0)^{\mathrm{T}}$ of **H** associated with 4.

(5) The only repeated eigenvalue of **H** is the double eigenvalue 2. The vector space V_2 of eigenvectors associated with 2 is the solution space of the system of linear equations with matrix of coefficients

$$\mathbf{H}-2\mathbf{I}=\begin{pmatrix}1 & -\mathrm{i} & 0\\ \mathrm{i} & 1 & 0\\ 0 & 0 & 0\end{pmatrix}\sim\begin{pmatrix}1 & -\mathrm{i} & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}.$$

Here the second and third unknowns are disposable, therefore they are the parameters θ and ϕ in $\mathbb{C}$ where θ and ϕ are not both 0. The first unknown is then $\mathrm{i}\theta$. For pairs of parameters $\theta = 0$, $\phi = 1$, and $\theta = 1$, $\phi = 0$, we obtain the following basis of V_2:

$$B_2 = \left\{\mathbf{b}_{21} = (\mathrm{i} \quad 1 \quad 0)^{\mathrm{T}},\ \mathbf{b}_{22} = (0 \quad 0 \quad 1)^{\mathrm{T}}\right\}.$$

(6) For the elements of B_2, we have

$$\mathbf{b}_{21}\odot\mathbf{b}_{22} = \mathbf{b}_{21}^{*}\mathbf{b}_{22} = (-\mathrm{i} \quad 1 \quad 0)(0 \quad 0 \quad 1)^{\mathrm{T}} = 0.$$

Therefore B_2 is already orthogonal with respect to the Euclidean inner product and the Gram–Schmidt process in Theorem 2 is not needed. Choose

$$C_2 = \{(\mathrm{i} \quad 1 \quad 0)^{\mathrm{T}}, (0 \quad 0 \quad 1)^{\mathrm{T}}\}$$

as the orthogonal basis of V_2.

(7) Then $D = \{\mathbf{b}_4\} \cup C_2$ is an orthogonal basis of $\mathbb{C}^3$.

(8) Because $\mathbf{b}_4\odot\mathbf{b}_4 = \mathbf{b}_4^{*}\mathbf{b}_4 = (1 \quad -\mathrm{i} \quad 0)(1 \quad \mathrm{i} \quad 0)^{\mathrm{T}} = 2$, we have

$$\mathbf{e}_1 = \mathbf{b}_4/\|\mathbf{b}_4\| = \frac{1}{\sqrt{2}}(1 \quad \mathrm{i} \quad 0)^{\mathrm{T}}.$$

Similarly,

$$\mathbf{e}_2 = \frac{1}{\sqrt{2}}(\mathrm{i} \quad 1 \quad 0)^{\mathrm{T}}, \qquad \mathbf{e}_3 = (0 \quad 0 \quad 1)^{\mathrm{T}}.$$

(9) The required unitary matrix is

$$\mathbf{U} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & \mathrm{i} & 0\\ \mathrm{i} & 1 & 0\\ 0 & 0 & \sqrt{2}\end{pmatrix}.$$

Because the columns of $\mathbf{U}$ are, respectively, eigenvectors associated with the eigenvalues 4, 2, 2, the diagonal matrix $\mathbf{D}$ has diagonal elements 4, 2, 2 in that order, by Theorem 2.

By Proposition 4(ii), the values $F(\mathbf{v})$ of a Hermitian form F for all vectors $\mathbf{v}$ over $\mathbb{C}$ are real. Consequently, F can be classified as belonging to one of the value classes in Definition 1 of Chapter 13, just as if F were a quadratic form over $\mathbb{R}$. By Theorem 2, F is unitarily similar to a diagonal Hermitian form, which is the ingredient that is needed to prove Theorem 1 of Chapter 13 for Hermitian forms. Unfortunately, Lagrange's process as given in Chapter 13 may not be effective for Hermitian forms, as the following tutorial problem shows.

TUTORIAL PROBLEM 14.2

Show that Lagrange's process does not transform the Hermitian form $F \equiv \mathrm{i}\bar{x}y - \mathrm{i}\bar{y}x$ into a diagonal Hermitian form.

For Hermitian forms a different diagonalization process is needed.

• *Construction I*
Lagrange's process for Hermitian forms

Let F be a non-zero Hermitian form in the indeterminates $x_1, x_2, x_3, \ldots, x_n$ with associated Hermitian matrix $\mathbf{H}$ over $\mathbb{C}$.

(1) First we assume that $h_{11} = h_{22} = h_{33} = \ldots = h_{nn} = 0$ and for no coefficient h_{jk} is the real part $\mathrm{Re}(h_{jk}) \neq 0$. Therefore $h_{jk} = \mathrm{i}g_{jk}$, where $g_{jk} \in \mathbb{R}$ for all $j, k = 1, 2, 3, \ldots, n$. Because F is non-zero, there exist integers p and q such that $g_{pq} \neq 0$. We apply the non-singular transformation in which $x_p = \mathrm{i}w_p$ and let $x_j = w_j$ otherwise. Then F has the following pair of terms:

$$\begin{aligned} h_{pq}\bar{x}_p x_q + h_{qp}\bar{x}_q x_p &= \mathrm{i}g_{pq}(-\mathrm{i}\bar{w}_p)w_q - \mathrm{i}g_{pq}\bar{w}_q \mathrm{i}w_q \\ &= g_{pq}(\bar{w}_p w_q + \bar{w}_q w_p). \end{aligned}$$

Therefore, with these indeterminates, F has at least one term with a non-zero real part.

(2) Alternatively, $h_{11} = h_{22} = h_{33} = \ldots = h_{nn} = 0$ but there exist integers p and q such that $\mathrm{Re}(h_{pq}) \neq 0$. Then $F \equiv h_{pq}\bar{x}_p x_q + h_{qp}\bar{x}_q x_p + F_1$, where F_1 is a Hermitian form in $x_1, x_2, x_3, \ldots, x_n$ with no diagonal terms or terms in $\bar{x}_p x_q$ or $\bar{x}_q x_p$. Also $h_{qp} = \bar{h}_{pq}$ because $\mathbf{H}$ is Hermitian. Therefore,

$$F \equiv h_{pq}\bar{x}_p x_q + \bar{h}_{pq}\bar{x}_q x_p + F_1.$$

We apply the following non-singular transformation to the indeterminates: $x_p = y_p + \mathrm{i}y_q$, $x_q = y_p - \mathrm{i}y_q$ and $x_j = y_j$ for $j = 1, 2, \ldots, p-1, p+1, \ldots, q-1, q+1, \ldots, n$. Then

$$F = 2\,\mathrm{Re}(h_{pq})\bar{y}_p y_p - 2\,\mathrm{Re}(h_{pq})\bar{y}_q y_q + F_2,$$

where F_2 is a Hermitian form in $y_1, y_2, y_3, \ldots, y_n$ with no diagonal terms. We conclude that $\bar{y}_p y_p$ has the coefficient $2\mathrm{Re}(h_{pq}) \neq 0$ in F.

(3) Finally, we suppose that there exists an integer p such that $h_{pp} \neq 0$. In the following calculations the summation sign $\sum'^{n}_{j=1}$ denotes a sum in which $j \neq p$. Then

$$F \equiv h_{pp}\left[\overline{x_p}x_p + \sum_{j=1}^{n}{}'\left[f_{pj}\overline{x_p}x_j + \overline{f_{pj}}\,\overline{x_j}x_p\right]\right] + F_3,$$

where $f_{pj} = h_{pj}/h_{pp}$ and F_3 is a Hermitian form in $x_1, x_2, \ldots, x_{p-1}, x_{p+1}, \ldots, x_n$. Therefore,

$$F \equiv h_{pp}\left[\overline{x_p} + \sum_{j=1}^{n}{}'\overline{f_{pj}}\,\overline{x_j}\right]\left[x_p + \sum_{j=1}^{n}{}' f_{pj}x_j\right] + F_4,$$

where F_4 is a Hermitian form in $x_1, x_2, \ldots, x_{p-1}, x_{p+1}, \ldots, x_n$. Then, by the non-singular transformation in which $z_p = x_p + \sum'_{j=1}^{n} f_{pj}x_j$ and $z_j = x_j$ for every $j \neq p$, we obtain $F = h_{pp}\overline{z_p}z_p + F_5$, where F_5 is a Hermitian form in the $n-1$ indeterminates $z_1, \ldots, z_{p-1}, z_{p+1}, \ldots, z_n$. Thus, in at most three steps, the number of indeterminates which occur in non-diagonal terms is reduced by at least one, therefore repeated application of this process transforms any Hermitian form to a Hermitian form with a diagonal matrix over $\mathbb{R}$.

A Hermitian form G is **equivalent (over $\mathbb{C}$)** to the Hermitian form F if G can be transformed into F by a non-singular transformation of indeterminates. This is an equivalence relation on the set of Hermitian forms. Construction 1 provides an effective method for finding whether two Hermitian forms are equivalent. The proof of Theorem 3 of Chapter 13 is effective for Hermitian forms, therefore Sylvester's law of inertia holds for Hermitian forms just as for quadratic forms. Consequently, Proposition 2 and Theorem 4 of Chapter 13 are both true for Hermitian forms, and therefore the value class of a Hermitian form can be determined by its rank and signature. Let us apply Construction 1 to a suitably awkward Hermitian form in order to determine its value class.

○ *Example 6*

Let $F \equiv \mathrm{i}\bar{x}y - \mathrm{i}\bar{y}x - 2\mathrm{i}\bar{x}z + 2\mathrm{i}\bar{z}x + 4\mathrm{i}\bar{y}z - 4\mathrm{i}\bar{z}y$. Because F has no diagonal terms and all the coefficients of the cross terms have real part 0, we apply step (1) of Construction 1 and let $x = \mathrm{i}x_1$, $y = y_1$ and $z = z_1$. Then

$$\begin{aligned} F &= \mathrm{i}(\overline{\mathrm{i}x_1})y_1 - \mathrm{i}\bar{y}_1(\mathrm{i}x_1) - 2\mathrm{i}(\overline{\mathrm{i}x_1})z_1 + 2\mathrm{i}\bar{z}_1(\mathrm{i}x_1) + 4\mathrm{i}\bar{y}_1z_1 - 4\mathrm{i}\bar{z}_1y_1 \\ &= \bar{x}_1y_1 + \bar{y}_1x_1 - 2\bar{x}_1z_1 - 2\bar{z}_1x_1 + 4\mathrm{i}\bar{y}_1z_1 - 4\mathrm{i}\bar{z}_1y_1. \end{aligned}$$

As a Hermitian form in x_1, y_1, z_1, F has no diagonal terms but has the terms $\bar{x}_1y_1 + \bar{y}_1x_1$ for which the coefficients have non-zero real parts. Therefore, by step (2) of Construction 1, we let $x_1 = x_2 + \mathrm{i}y_2$, $y_1 = x_2 - \mathrm{i}y_2$ and $z_1 = z_2$ and so obtain

$$\begin{aligned} F &= (\bar{x}_2 - \mathrm{i}\bar{y}_2)(x_2 - \mathrm{i}y_2) + (\bar{x}_2 + \mathrm{i}\bar{y}_2)(x_2 + \mathrm{i}y_2) - 2(\bar{x}_2 - \mathrm{i}\bar{y}_2)z_2 \\ &\qquad - 2\bar{z}_2(x_2 + \mathrm{i}y_2) + 4\mathrm{i}(\bar{x}_2 + \mathrm{i}\bar{y}_2)z_2 - 4\mathrm{i}\bar{z}_2(x_2 - \mathrm{i}y_2) \\ &= 2\bar{x}_2x_2 - 2\bar{y}_2y_2 - 2\bar{x}_2z_2 - 2\bar{z}_2x_2 + 2\mathrm{i}\bar{y}_2z_2 - 2\mathrm{i}\bar{z}_2y_2 \\ &\qquad + 4\mathrm{i}\bar{x}_2z_2 - 4\mathrm{i}\bar{z}_2x_2 - 4\bar{y}_2z_2 - 4\bar{z}_2y_2 \\ &= 2\bar{x}_2x_2 - 2\bar{y}_2y_2 - (2 - 4\mathrm{i})\bar{x}_2z_2 - (2 + 4\mathrm{i})\bar{z}_2x_2 \\ &\qquad - (4 - 2\mathrm{i})\bar{y}_2z_2 - (4 + 2\mathrm{i})\bar{z}_2y_2. \end{aligned}$$

The Hermitian form F in x_2, y_2 and z_2 has a non-zero diagonal coefficient for $\bar{x}_2x_2$, therefore we can now apply step (3) of Construction 1 and write

$$\begin{aligned}F &= 2\left[\bar{x}_2x_2 - (1-2\mathrm{i})\bar{x}_2z_2 - (1+2\mathrm{i})\bar{z}_2x_2\right] \\ &\quad - 2\bar{y}_2y_2 - (4-2\mathrm{i})\bar{y}_2z_2 - (4+2\mathrm{i})\bar{z}_2y_2 \\ &= 2\left[\bar{x}_2x_2 - (1-2\mathrm{i})\bar{x}_2z_2 - (1+2\mathrm{i})\bar{z}_2x_2 + 5\bar{z}_2z_2\right] \\ &\quad - 2\bar{y}_2y_2 - 10\bar{z}_2z_2 - (4-2\mathrm{i})\bar{y}_2z_2 - (4+2\mathrm{i})\bar{z}_2y_2 \\ &= 2\left[\bar{x}_2 - (1+2\mathrm{i})\bar{z}_2\right]\left[x_2 - (1-2\mathrm{i})z_2\right] \\ &\quad - 2\left[\bar{y}_2y_2 + (2-\mathrm{i})\bar{y}_2z_2 + (2+\mathrm{i})\bar{z}_2y_2\right] - 10\bar{z}_2z_2 \\ &= 2\bar{x}_3x_3 - 2\left[\bar{y}_2y_2 + (2-\mathrm{i})\bar{y}_2z_2 + (2+\mathrm{i})\bar{z}_2y_2 + 5\bar{z}_2z_2\right],\end{aligned}$$

where $x_3 = x_2 - (1 + 2\mathrm{i})z_2$. The Hermitian form in y_2 and z_2 has non-zero diagonal coefficient -2 for $\bar{y}_2y_2$, therefore we apply step (3) to it and obtain

$$\begin{aligned}F &= 2\bar{x}_3x_3 - 2\left[\bar{y}_2 + (2+\mathrm{i})\bar{z}_2\right]\left[y_2 + (2-\mathrm{i})z_2\right] \\ &= 2\bar{x}_3x_3 - 2\bar{y}_3y_3,\end{aligned}$$

where $y_3 = y_2 + (2 - \mathrm{i})z_2$. From the last formula we deduce that F has rank 2 and signature 0, therefore by Theorem 4(iii) of Chapter 13, F is indefinite.

Summary

The previous four chapters were concerned with vector spaces over $\mathbb{R}$, and this chapter outlines the corresponding results for vector spaces over $\mathbb{C}$. The total vector space $\mathbb{C}^n$ is a **unitary vector space** if the **Euclidean inner product** $\mathbf{v}\odot\mathbf{w} \in \mathbb{C}$ is defined for every pair of vectors $\mathbf{v}, \mathbf{w} \in \mathbb{C}^n$. For column vectors $\mathbf{v}, \mathbf{w} \in \mathbb{C}^n$, $\mathbf{v}\odot\mathbf{w} = \mathbf{v}^*\mathbf{w}$, where $\mathbf{v}^*$ is the **conjugate transpose** of $\mathbf{v}$, that is, the transpose of the matrix of complex conjugates of the elements of $\mathbf{v}$. The **Cauchy–Schwarz** and **triangle inequalities** hold for $\mathbb{C}^n$, justifying the definition of the **length** $\|\mathbf{v}\|$ of a vector in $\mathbb{C}^n$. Because $\mathbf{v}\odot\mathbf{w} \in \mathbb{C}$ there is no definition of angle, but vectors $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ are defined to be **orthogonal** (with respect to the Euclidean inner product) if $\mathbf{v}\odot\mathbf{w} = 0$. A set of vectors of length 1 is **orthonormal** if every pair in the set is orthogonal, while a matrix $\mathbf{U}$ is **unitary** if its set of columns is orthonormal. It follows that $\mathbf{U}$ is unitary if and only if $\mathbf{U}^*\mathbf{U} = \mathbf{I}$. A unitary matrix is non-singular because the modulus of its determinant is 1. The **Gram–Schmidt process over** $\mathbb{C}$ gives a sequence of formulae by which a basis B of a subspace V of $\mathbb{C}^n$ is replaced by an **orthogonal basis** C of V with respect to the Euclidean inner product. Dividing each vector in C by its own length then produces an **orthonormal basis** D of V. A square matrix $\mathbf{H}$ over $\mathbb{C}$ is **Hermitian** if $\mathbf{H}^* = \mathbf{H}$, which is a generalization of 'symmetric' for a matrix over $\mathbb{R}$. This includes the definition of **Hermitian form** $F = \mathbf{x}^*\mathbf{H}\mathbf{x}$, in which $\mathbf{H}$ is Hermitian and $\mathbf{x}$ is a column vector of indeterminates. Every Hermitian form F is **unitarily similar** to a Hermitian form for which the matrix is diagonal, that is, there exists a unitary matrix $\mathbf{U}$ such that $\mathbf{U}^*\mathbf{H}\mathbf{U}$ is a diagonal matrix $\mathbf{D}$. However, the matrix $\mathbf{D}$ is over $\mathbb{R}$ and all values of a Hermitian form are in $\mathbb{R}$, which means that Hermitian forms resemble quadratic forms over $\mathbb{R}$ more than they resemble quadratic forms over $\mathbb{C}$. This allows Hermitian forms to be classified into the same value classes as for quadratic forms over $\mathbb{R}$. As in the real case, the value class of a Hermitian form over $\mathbb{C}$ can be determined from the eigenvalues, or by using **Lagrange's process for Hermitian**

forms. Also **Sylvester's law of inertia** holds for a Hermitian form F and the value class of F can be deduced easily from the rank and signature of F.

EXERCISES ON CHAPTER 14

1. Let S be the subset of the vector space $\mathbb{C}^3$ given by

$$S = \{(1, i, 0), (i, 1 - i, -1), (-i, 1, i), (3i, 3, 0), (-2, 2 + 2i, -2i)\}.$$

(i) For each pair of distinct vectors $\mathbf{v}, \mathbf{w} \in S$ calculate $\mathbf{v} \odot \mathbf{w}$ and $\mathbf{w} \odot \mathbf{v}$.
(ii) Find the length of each vector in S.
(iii) Which pairs of vectors in S are parallel?
(iv) Which pairs of vectors in S are orthogonal?

2. In each of the following cases, find a vector $\mathbf{w} \in \mathbb{C}^3$ which is orthogonal in $\mathbb{C}^3$ to each of the given vectors $\mathbf{u}$ and $\mathbf{v}$:

(i) $\mathbf{u} = (1, 0, 0)$, $\mathbf{v} = (0, 1, i)$,
(ii) $\mathbf{u} = (i, -i, i)$, $\mathbf{v} = (1, 1, 1)$,
(iii) $\mathbf{u} = (1, 1, i)$, $\mathbf{v} = (1, -i, 1)$.

3. Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times n$ matrices over $\mathbb{C}$ and let $c \in \mathbb{C}$. Prove that:

(i) $(c\mathbf{A})^* = \bar{c}\mathbf{A}^*$, (ii) $(\mathbf{AB})^* = \mathbf{B}^*\mathbf{A}^*$.

4. Let $\mathbf{A}$ and $\mathbf{B}$ be unitary $n \times n$ matrices over $\mathbb{C}$. Prove that:

(i) the modulus of $\det \mathbf{A}$ equals 1,
(ii) $\mathbf{A}^T$ is unitary;
(iii) $\overline{\mathbf{A}}$ is unitary;
(iv) $\mathbf{AB}$ is unitary.

5. Let $S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_k\}$ be an orthogonal set of vectors in $\mathbb{C}^n$. Prove that S is linearly independent over $\mathbb{C}$.

6. Use the Gram–Schmidt process for $\mathbb{C}$ to find an orthogonal basis containing the first vector in the list for each of the following unitary vector spaces:

(i) $\langle (1, 1, i), (2, i, 1), (1, 3, 5i) \rangle$,
(ii) $\langle (1, 2, 2, -i), (0, i, -1, 2), (0, 0, i, 3) \rangle$,
(iii) $\langle (0, 0, 2, -i), (3, i, 0, 0), (0, 1, -i, 0) \rangle$.

7. Let V be a subspace of $\mathbb{C}^n$, let $c_1, c_2, c_3, \ldots, c_m$ be non-zero complex numbers and let $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_m\}$ be a basis of V which is orthogonal (with respect to the Euclidean inner product). Prove that

(i) $C = \{c_1\mathbf{b}_1, c_2\mathbf{b}_2, c_3\mathbf{b}_3, \ldots, c_m\mathbf{b}_m\}$ is an orthogonal basis of V;
(ii) $D = \{\mathbf{b}_1/\|\mathbf{b}_1\|, \mathbf{b}_2/\|\mathbf{b}_2\|, \mathbf{b}_3/\|\mathbf{b}_3\|, \ldots, \mathbf{b}_m/\|\mathbf{b}_m\|\}$ is an orthonormal basis of V.

8. Let **S** be a skew-Hermitian matrix. Prove that:

(i) the diagonal elements of **S** have real part 0;
(ii) i**S** is Hermitian;
(iii) the real parts of the eigenvalues of **S** are 0.

9. Let **H** be a Hermitian matrix over $\mathbb{C}$, let λ and μ be distinct eigenvalues of **H**, let **u** be an eigenvector of **H** associated with λ and let **v** be an eigenvector of **H** associated with μ. Prove that **u** and **v** are orthogonal with respect to the Euclidean inner product.

10. Find a unitary matrix **U** such that **U***HU is a diagonal matrix, where **H** is the Hermitian matrix $\mathbf{H} = \begin{pmatrix} 1 & -2\mathrm{i} \\ 2\mathrm{i} & -2 \end{pmatrix}$.

11. Let **H** be the Hermitian matrix $\mathbf{H} = \begin{pmatrix} 2 & 0 & 4\mathrm{i} \\ 0 & 2 & 0 \\ -4\mathrm{i} & 0 & 2 \end{pmatrix}$. Find a unitary matrix **U** and a diagonal matrix **D** such that **U***HU = **D**.

12. Let **H** be the Hermitian matrix $\mathbf{H} = \begin{pmatrix} 0 & \mathrm{i}\sqrt{6} & \mathrm{i}\sqrt{3} \\ -\mathrm{i}\sqrt{6} & 1 & -\sqrt{2} \\ -\mathrm{i}\sqrt{3} & -\sqrt{2} & 2 \end{pmatrix}$. Find a unitary matrix **U** and a diagonal matrix **D** over $\mathbb{R}$ such that **U***HU = **D**. (3 is an eigenvalue of **H**.)

13. Find the eigenvalues of the following Hermitian matrices and determine the value classes of the Hermitian forms of which they are the associated matrices:

(i) $\mathbf{H}_1 = \begin{pmatrix} 0 & -\mathrm{i} & 0 \\ \mathrm{i} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$,

(ii) $\mathbf{H}_2 = \begin{pmatrix} 1 & -2\mathrm{i} & 0 \\ 2\mathrm{i} & -2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$,

(iii) $\mathbf{H}_3 = \begin{pmatrix} 5 & 0 & 2-2\mathrm{i} \\ 0 & 6 & 0 \\ 2+2\mathrm{i} & 0 & 7 \end{pmatrix}$.

14. Use Lagrange's process for Hermitian forms to transform each of the following five Hermitian forms in the indeterminates x, y, z into diagonal Hermitian forms:

(i) $F_1 \equiv \bar{x}x + 2\bar{y}y + 2\bar{z}z - \bar{x}y - \bar{y}x$,
(ii) $F_2 \equiv \bar{x}x - \bar{y}y + \mathrm{i}\bar{x}z - \mathrm{i}\bar{z}x - \bar{y}z - \bar{z}y$,
(iii) $F_3 \equiv \bar{x}x + \mathrm{i}\bar{x}y - \mathrm{i}\bar{y}x + \mathrm{i}\bar{y}z - \mathrm{i}\bar{z}y$,
(iv) $F_4 \equiv \bar{x}x + \bar{y}y + 5\bar{z}z - \mathrm{i}\bar{x}y + \mathrm{i}\bar{y}x + (2+\mathrm{i})\bar{x}z + (2-\mathrm{i})\bar{z}x - (1-3\mathrm{i})\bar{y}z - (1+3\mathrm{i})\bar{z}y$,
(v) $F_5 \equiv 2\bar{z}z - 2\bar{y}y - \bar{x}x - 2\mathrm{i}\bar{x}y + 2\mathrm{i}\bar{y}x + (1+\mathrm{i})\bar{y}z + (1-\mathrm{i})\bar{z}y$.

15. Determine the rank, the signature and the value class of each Hermitian form in Exercise 14.

Index