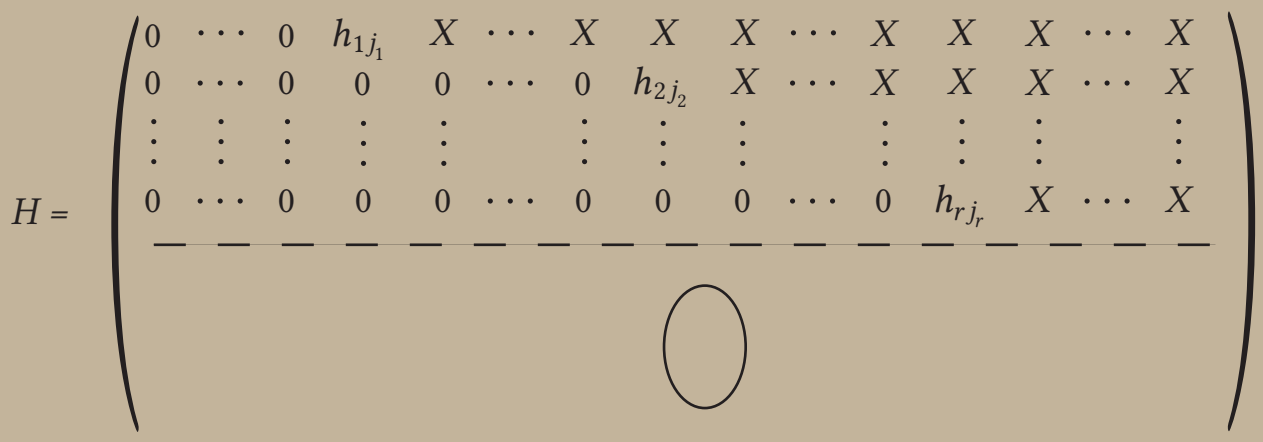
Comprehensive Introduction to Linear Algebra

PART II - POLYNOMIALS and CANONICAL FORMS

Joel G. Broida

S. Gill Williamson



Comprehensive Introduction to Linear Algebra

PART II - POLYNOMIALS AND CANONICAL FORMS

Joel G. Broida
S. Gill Williamson

Preface (Part II)

This book, Part 2 - Polynomials and Canonical Forms, covers Chapters 6 through 8 of the book *A Comprehensive Introduction to Linear Algebra* (Addison-Wesley, 1986), by Joel G. Broida and S. Gill Williamson. Chapter 6, Polynomials, will be review to some readers and new to others. Chapters 7 and 8 supplement and extend ideas developed in Part I, Basic Linear Algebra, and introduce the very powerful method of canonical forms. The original Preface, Contents and Index are included.

Preface (Parts I, II, III)

As a text, this book is intended for upper division undergraduate and beginning graduate students in mathematics, applied mathematics, and fields of science and engineering that rely heavily on mathematical methods. However, it has been organized with particular concern for workers in these diverse fields who want to review the subject of linear algebra. In other words, we have written a book which we hope will still be referred to long after any final exam is over. As a result, we have included far more material than can possibly be covered in a single semester or quarter. This accomplishes at least two things. First, it provides the basis for a wide range of possible courses that can be tailored to the needs of the student or the desire of the instructor. And second, it becomes much easier for the student to later learn the basics of several more advanced topics such as tensors and infinite-dimensional vector spaces from a point of view coherent with elementary linear algebra. Indeed, we hope that this text will be quite useful for self-study. Because of this, our proofs are extremely detailed and should allow the instructor extra time to work out exercises and provide additional examples if desired.

A major concern in writing this book has been to develop a text that addresses the exceptional diversity of the audience that needs to know something about the subject of linear algebra. Although seldom explicitly acknowledged, one of the central difficulties in teaching a linear algebra course to advanced students is that they have been exposed to the basic background material from many different sources and points of view. An experienced mathematician will see the essential equivalence of these points of view, but these same differences seem large and very formidable to the students. An engineering student for example, can waste an inordinate amount of time because of some trivial mathematical concept missing from their background. A mathematics student might have had a concept from a different point of view and not realize the equivalence of that point of view to the one currently required. Although such problems can arise in any advanced mathematics course, they seem to be particularly acute in linear algebra.

To address this problem of student diversity, we have written a very self-contained text by including a large amount of background material necessary for a more advanced understanding of linear algebra. The most elementary of this material constitutes Chapter 0, and some basic analysis is presented in three appendices. In addition, we present a thorough introduction to those aspects of abstract algebra, including groups, rings, fields and polynomials over fields, that relate directly to linear algebra. This material includes both points that may seem "trivial" as well as more advanced background material. While trivial points can be quickly skipped by the reader who knows them already, they can cause discouraging delays for some students if omitted. It is for this reason that we have tried to err on the side of over-explaining concepts, especially when these concepts appear in slightly altered forms. The more advanced reader can gloss over these details, but they are there for those who need them. We hope that more experienced mathematicians will forgive our repetitive justification of numerous facts throughout the text.

A glance at the Contents shows that we have covered those topics normally included in any linear algebra text although, as explained above, to a greater level of detail than other books. Where we differ significantly in content from most linear algebra texts however, is in our treatment of canonical forms (Chapter 8), tensors (Chapter 11), and infinite-dimensional vector spaces (Chapter 12). In particular, our treatment of the Jordan and rational canonical forms in Chapter 8 is based entirely on invariant factors and the

Smith normal form of a matrix. We feel this approach is well worth the effort required to learn it since the result is, at least conceptually, a constructive algorithm for computing the Jordan and rational forms of a matrix. However, later sections of the chapter tie together this approach with the more standard treatment in terms of cyclic subspaces. Chapter 11 presents the basic formalism of tensors as they are most commonly used by applied mathematicians, physicists and engineers. While most students first learn this material in a course on differential geometry, it is clear that virtually all the theory can be easily presented at this level, and the extension to differentiable manifolds then becomes only a technical exercise. Since this approach is all that most scientists ever need, we leave more general treatments to advanced courses on abstract algebra. Finally, Chapter 12 serves as an introduction to the theory of infinite-dimensional vector spaces. We felt it is desirable to give the student some idea of the problems associated with infinite-dimensional spaces and how they are to be handled. And in addition, physics students and others studying quantum mechanics should have some understanding of how linear operators and their adjoints are properly defined in a Hilbert space.

One major topic we have not treated at all is that of numerical methods. The main reason for this (other than that the book would have become too unwieldy) is that we feel at this level, the student who needs to know such techniques usually takes a separate course devoted entirely to the subject of numerical analysis. However, as a natural supplement to the present text, we suggest the very readable "Numerical Analysis" by I. Jacques and C. Judd (Chapman and Hall, 1987).

The problems in this text have been accumulated over 25 years of teaching the subject of linear algebra. The more of these problems that the students work the better. Be particularly wary of the attitude that assumes that some of these problems are "obvious" and need not be written out or precisely articulated. There are many surprises in the problems that will be missed from this approach! While these exercises are of varying degrees of difficulty, we have not distinguished any as being particularly difficult. However, the level of difficulty ranges from routine calculations that everyone reading this book should be able to complete, to some that will require a fair amount of thought from most students.

Because of the wide range of backgrounds, interests and goals of both students and instructors, there is little point in our recommending a particular

course outline based on this book. We prefer instead to leave it up to each teacher individually to decide exactly what material should be covered to meet the needs of the students. While at least portions of the first seven chapters should be read in order, the remaining chapters are essentially independent of each other. Those sections that are essentially applications of previous concepts, or else are not necessary for the rest of the book are denoted by an asterisk (*).

Now for one last comment on our notation. We use the symbol ∎ to denote the end of a proof, and /// to denote the end of an example. Sections are labeled in the format "Chapter.Section," and exercises are labeled in the format "Chapter.Section.Exercise." For example, Exercise 2.3.4 refers to Exercise 4 of Section 2.3, i.e., Section 3 of Chapter 2. Books listed in the bibliography are referred to by author and copyright date.

Contents (Part I, II#, III)

0	**Foundations**		**1**
	0.1	Sets	2
	0.2	Mappings	4
	0.3	Orderings and Equivalence Relations	7
	0.4	Cardinality and the Real Number System	11
	0.5	Induction	17
	0.6	Complex Numbers	19
	0.7	Additional Properties of the Integers	25
1	**An Introduction to Groups**		**30**
	1.1	Definitions	30
	1.2	Permutation Groups	35
	1.3	Homomorphisms of Groups	49
	1.4	Rings and Fields	53
	1.5	More on Groups and Rings	56

2 Vector Spaces **68**
2.1 Definitions 68
2.2 Linear Independence and Bases 75
2.3 Direct Sums 85
2.4 Inner Product Spaces 94
2.5 Orthogonal Sets 104

3 Linear Equations and Matrices **115**
3.1 Systems of Linear Equations 115
3.2 Elementary Row Operations 121
3.3 Row and Column Spaces 127
3.4 The Rank of a Matrix 135
3.5 Solutions to Systems of Linear Equations 138
3.6 Matrix Algebra 147
3.7 Invertible Matrices 157
3.8 Elementary Matrices 163

4 Determinants **170**
4.1 Definitions and Elementary Properties 171
4.2 Additional Properties of Determinants 176
4.3 Expansion by Minors 186
4.4 Determinants and Linear Equations 199
4.5 Block Matrices 204
4.6 The Cauchy-Binet Theorem 208

5 Linear Transformations and Matrices **215**
5.1 Linear Transformations 215
5.2 Further Properties of Linear Transformations 224
5.3 Matrix Representations 233
5.4 Change of Basis 243

6 # Polynomials **252**
6.1 Definitions 252
6.2 Factorization of Polynomials 261
6.3 Polynomial Ideals 269
6.4 Polynomials Over Algebraically Closed Fields 276
6.5 The Field of Quotients 281
6.6 Polynomials Over Finite Fields * 285

7 # Linear Transformations and Polynomials **296**
7.1 Minimal Polynomials 297
7.2 Eigenvalues and Eigenvectors 302
7.3 Characteristic Polynomials 308

7.4 Annihilators 322
7.5 Invariant Subspaces 329
7.6 The Primary Decomposition Theorem 337
7.7 More on Diagonalization 344
7.8 Projections 352
7.9 Quotient Spaces 360
7.10 The Triangular Form Theorem * 365
7.11 Nilpotent Transformations * 369
7.12 The Triangular Form Theorem Again * 376

8 # Canonical Forms 382
8.1 Elementary Canonical Forms 382
8.2 Matrices Over the Ring of Polynomials 389
8.3 The Smith Canonical Form 397
8.4 Similarity Invariants 406
8.5 The Rational Canonical Form 412
8.6 The Jordan Canonical Form 420
8.7 Cyclic Subspaces * 432
8.8 The Elementary Divisor Theorem * 439

9 Linear Forms 446
9.1 Bilinear Functionals 446
9.2 Double Duals and Annihilators 450
9.3 The Transpose of a Linear Transformation 458
9.4 Bilinear Forms 461
9.5 Symmetric and Antisymmetric Bilinear Forms 467
9.6 Diagonalization of Symmetric Bilinear Forms 474
9.7 Hermitian Forms 481
9.8 Simultaneous Diagonalization * 485

10 Linear Operators 490
10.1 Linear Functionals and Adjoints 490
10.2 Isometric and Unitary Operators 498
10.3 Normal Operators 508
10.4 Diagonalization of Normal Operators 514
10.5 The Spectral Theorem 523
10.6 The Matrix Exponential Series 528
10.7 Positive Operators 537

11 Multilinear Mappings and Tensors 543
11.1 Definitions 544
11.2 Special Types of Tensors 553
11.3 The Exterior Product 563

11.4 Tensor Algebras 574
11.5 The Tensor Product of Vector Spaces 577
11.6 Volumes in $\mathbb{R}^3$ 584
11.7 Volumes in $\mathbb{R}^n$ 589
11.8 Linear Transformations and Volumes 593
11.9 Orientations and Volumes 603
11.10 The Metric Tensor and Volume Forms 609

12 Hilbert Spaces 619
12.1 Mathematical Preliminaries 619
12.2 Operator Norms 635
12.3 Hilbert Spaces 640
12.4 Closed Subspaces 649
12.5 Hilbert Bases 655
12.6 Bounded Operators on a Hilbert Space 665
12.7 Hermitian, Normal and Unitary Operators 676

Appendices 680
A Metric Spaces 680
B Sequences and Series 696
C Path Connectedness 720

Bibliography 723

Index 727

CHAPTER 6

Polynomials

Before continuing with our treatment of linear operators and transformations, we must make a digression and consider the theory of polynomials in some detail. The subject matter of this chapter will be quite important throughout much of the remainder of this text. Our basic goal is to discuss the factorization of polynomials in detail, including many of the elementary properties that we all learned in high school.

6.1 DEFINITIONS

Let $\mathcal{F}$ be a field. In high school (or earlier), we all learned that a polynomial $p(x)$ in the indeterminate (or variable) x is basically an expression of the form

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

where n is any nonnegative integer and $a_0, \ldots, a_n$ are all elements of $\mathcal{F}$. Note that our elementary experience with polynomials tells us that if

$$q(x) = b_0 + b_1x + \cdots + b_mx^m$$

is another polynomial in x then, assuming without loss of generality that $n \geq m$, we have (where we define $a_j = 0$ for $j > n$ and $b_j = 0$ for $j > m$)

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

and

$$\begin{aligned} p(x)q(x) = {} & (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 \\ & + \cdots + (a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0)x^k \\ & + \cdots + a_nb_mx^{n+m} \ . \end{aligned}$$

While this has a definite intuitive appeal (to previous experience), the term "expression" in the above definition of polynomial is rather nebulous, and it is worth making this definition somewhat more precise. To accomplish this, we focus our attention on the coefficients a_i.

We define a **polynomial** over $\mathcal{F}$ to be an (infinite) sequence of scalars

$$p = \{a_0, a_1, a_2, \ldots\}$$

such that $a_n = 0$ for all but finitely many n. The scalars a_i are called the **coefficients** of the polynomial. If

$$q = \{b_0, b_1, b_2, \ldots\}$$

is another polynomial in $\mathcal{F}$, then p = q if and only if $a_i = b_i$ for every i. As we did for vector n-tuples, we define the addition of two polynomials p and q by

$$p + q = \{a_0 + b_0, a_1 + b_1, \ldots\} \ .$$

Furthermore, we now also define the multiplication of p and q by

$$pq = \{c_0, c_1, c_2, \ldots\}$$

where

$$c_k = \sum_{i+j=k} a_ib_j = \sum_{t=0}^{k} a_tb_{k-t} = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0 \ .$$

Since p and q have a finite number of nonzero terms, so do both p + q and pq, and hence both p + q and pq are also polynomials.

We claim that the set of all polynomials over $\mathcal{F}$ forms a ring. Indeed, if we define the zero polynomial to be the sequence {0, 0, . . . }, and the negative of any polynomial $\{a_0, a_1, \ldots\}$ to be the polynomial $\{-a_0, -a_1, \ldots\}$, then axioms (R1) – (R6) for a ring given in Section 1.4 are clearly satisfied. As to axiom (R7), let $p = \{a_0, a_1, \ldots\}$, $q = \{b_0, b_1, \ldots\}$ and $r = \{c_0, c_1, \ldots\}$. Then the k*th* coefficient of (pq)r is the sum (using the associative property of $\mathcal{F}$)

$$\sum_{i+j=k}\left(\sum_{m+n=i} a_m b_n\right)c_j = \sum_{m+n+j=k}(a_m b_n)c_j = \sum_{m+n+j=k} a_m(b_n c_j)$$
$$= \sum_{m+i=k} a_m\left(\sum_{n+j=i} b_n c_j\right) .$$

But this last expression is just the k*th* coefficient of p(qr). Finally, to prove axiom (R8), we use the distributive property of $\mathcal{F}$ to see that the k*th* coefficient of p(q + r) is

$$\sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j \quad .$$

Again we see that this last expression is just the k*th* coefficient of pq + pr. Similarly, it is easy to see that (p + q)r = pr + qr.

It should be clear that the ring of polynomials is commutative, and that if 1 is the unit element of $\mathcal{F}$, then {1, 0, 0, . . . } is a unit element for the ring of polynomials. However, since an arbitrary polynomial does not have a multiplicative inverse, the ring of polynomials does not form a field (see Theorem 6.2, Corollary 3 below).

Example 6.1 Consider the polynomials

$$\begin{aligned} p &= \{0, 1, 0, 0, \ldots\} \\ q &= \{1, 2, -1, 0, \ldots\} . \end{aligned}$$

Then

$$p + q = \{1, 3, -1, 0, \ldots\}$$

and

$$\begin{aligned} pq = \{&0(1), 0(2) + 1(1), 0(-1) + 1(2) + 0(1), \\ &0(0) + 1(-1) + 0(2) + 0(1), \ldots\} \end{aligned}$$

$$= \{0, 1, 2, -1, 0, \ldots\} \ . \ /\!/$$

Since the reader probably thought he (or she) already knew what a polynomial was, and since our definition may not be what it was he (or she) had in mind, what we will do now is relate our formal definition to our earlier elementary experience with polynomials. We will explain shortly why we are going through all of this apparently complicated formalism.

Given any element $a \in \mathcal{F}$, we associate a polynomial a′ defined by

$$a' = \{a, 0, 0, \ldots\} .$$

This is clearly a one-to-one mapping of $\mathcal{F}$ into the set of all polynomials with coefficients in $\mathcal{F}$. We also note that if $a, b \in \mathcal{F}$, then $a' = \{a, 0, \ldots\}$ and $b' = \{b, 0, \ldots\}$ so that

$$(a + b)' = \{a + b, 0, \ldots\} = a' + b'$$

and

$$(ab)' = \{ab, 0, \ldots\} = a'\ b' .$$

If $\mathcal{F}'$ denotes the set of all polynomials a' obtained in this manner, then $\mathcal{F}'$ is a field isomorphic to $\mathcal{F}$. Because of this isomorphism, we shall identify the elements of $\mathcal{F}$ with their corresponding polynomials, and write $a = \{a, 0, \ldots\}$.

Now let the symbol x denote the polynomial $\{0, 1, 0, 0, \ldots\}$. We call the symbol x an **indeterminate**. Applying our definition of polynomial multiplication, we see that $x^2 = \{0, 0, 1, 0, \ldots\}$ and, in general,

$$x^n = \{0, \ldots, 0, 1, 0, \ldots\}$$

where the 1 is in the n*th* position (remember that we start our numbering with 0). We also see that for any $a \in \mathcal{F}$ we have (applying our multiplication rule)

$$ax^n = \{a, 0, \ldots\}\{0, \ldots, 1, 0, \ldots\} = \{0, \ldots, a, 0, \ldots\} .$$

This means that an arbitrary polynomial $p = \{a_0, a_1, \ldots, a_n, 0, \ldots\}$ can be uniquely expressed in the familiar form

$$p = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n .$$

This discussion has now established a precise meaning to the term "expression" used at the beginning of this chapter. We will denote the commutative ring of all polynomials over $\mathcal{F}$ by $\mathcal{F}[x]$. In summary, we see that that while a polynomial was actually defined as a sequence, we showed that any polynomial $p = \{a_0, a_1, \ldots\} \in \mathcal{F}[x]$ could be uniquely expressed in terms of the indeterminate x as

$$p = a_0 + a_1x + \cdots + a_nx^n = \sum_{i=1}^{n} a_ix^i \quad .$$

Now suppose we are given both a polynomial $p = \sum a_ix^i \in \mathcal{F}[x]$ and any element $c \in \mathcal{F}$. We define the element $p(c) \in \mathcal{F}$ by $p(c) = \sum a_ic^i$. In other words, given a polynomial $p \in \mathcal{F}[x]$, the **polynomial function** p(x) is the mapping from $\mathcal{F}$ to $\mathcal{F}$ that takes $c \in \mathcal{F}$ into the element $p(c) \in \mathcal{F}$. We call p(c)

the **value** of the polynomial p when c is **substituted** for x. Because of this, a polynomial $p \in \mathcal{F}[x]$ is frequently denoted by p(x).

The reason for this apparently complicated technical definition is that it is possible for two different polynomials in $\mathcal{F}[x]$ to result in the same polynomial function (see Exercise 6.1.1).

Theorem 6.1 Suppose $p, q \in \mathcal{F}[x]$ and $c \in \mathcal{F}$. Then

(a) $(p \pm q)(c) = p(c) \pm q(c)$.

(b) $(pq)(c) = p(c)q(c)$.

Proof (a) Writing $p = a_0 + a_1x + \cdots + a_mx^m$ and $q = b_0 + b_1x + \cdots + b_nx^n$ we have

$$\begin{aligned}(p \pm q)(c) &= (a_0 \pm b_0) + (a_1 \pm b_1)c + (a_2 \pm b_2)c^2 + \cdots \\ &= (a_0 + a_1c + a_2c^2 + \cdots) \pm (b_0 + b_1c + b_2c^2 + \cdots) \\ &= p(c) \pm q(c) \ .\end{aligned}$$

(b) Using p and q from part (a) and the definition of pq, we have

$$\begin{aligned}(pq)(c) &= a_0b_0 + (a_0b_1 + a_1b_0)c + (a_0b_2 + a_1b_1 + a_2b_0)c^2 + \cdots \\ &= (a_0 + a_1c + a_2c^2 + \cdots)(b_0 + b_1c + b_2c^2 + \cdots) \\ &= p(c)q(c) \ . \ \blacksquare\end{aligned}$$

It should now be clear that the definitions given above for the algebraic properties of polynomials in terms of sequences are just those that we all learned in high school for adding and multiplying polynomials together. It should be easy for the reader to show that Example 6.1 may be repeated in terms of our elementary notion of polynomial addition and multiplication.

If $p = a_0 + a_1x + \cdots + a_nx^n \neq 0$ and $a_n \neq 0$, then we say that the **degree** of the polynomial p is n, and write we write deg p = n. The term a_n is called the **leading** coefficient of the polynomial, and if $a_n = 1$, then the polynomial is said to be **monic**. If deg p = 0, then p is said to be **constant**. By convention, the degree of the zero polynomial is not defined.

Theorem 6.2 Suppose $p, q \in \mathcal{F}[x]$ are nonzero. Then

(a) $\deg(p + q) \leq \max\{\deg p, \deg q\}$ (where $p + q \neq 0$).

(b) $\deg(pq) = \deg p + \deg q$.

Proof (a) Let $p = a_0 + a_1x + \cdots + a_mx^m$ and $q = b_0 + b_1x + \cdots + b_nx^n$ where $a_m, b_n \neq 0$. Then

$$p + q = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k$$

where $k = \max\{m, n\}$. Therefore $\deg(p + q) \leq \max\{\deg p, \deg q\}$ where the inequality follows since $a_k + b_k$ could equal 0.

(b) From the definition of pq, we see that (using the same p and q from part (a)) the k*th* term is $c_k x^k$ where $c_k = \sum_{i+j=k} a_i b_j$. But if $k > m + n$, then necessarily either a_i or b_j is zero, and therefore $c_k = 0$ for $k > m + n$. Since $\mathcal{F}$ is a field and therefore also a division ring, it follows that $a_m, b_n \neq 0$ implies $a_m b_n \neq 0$ (if $a_m b_n = 0$, then multiplying from the left by a_m^{-1} says that $b_n = 0$, a contradiction). Thus $\deg pq = m + n = \deg p + \deg q$. ∎

Corollary 1 If $p, q \in \mathcal{F}[x]$ are both nonzero, then $\deg p \leq \deg pq$.

Proof Since p and q are nonzero, $\deg p \geq 0$ and $\deg q \geq 0$, and hence $\deg p \leq \deg p + \deg q = \deg pq$. ∎

Corollary 2 If $p, q, r \in \mathcal{F}[x]$, then

(a) $pq = 0$ implies that either $p = 0$ or $q = 0$.

(b) If $pq = rq$ where $q \neq 0$, then $p = r$.

Proof (a) If $p \neq 0$ and $q \neq 0$, then $\deg pq \geq 0$ implies that $pq \neq 0$.

(b) Since $\mathcal{F}[x]$ is a ring, we see that if $pq = rq$, then $(p - r)q = 0$. But $q \neq 0$, so that by (a) we must have $p - r = 0$, or $p = r$. ∎

We note that part (a) of this corollary shows that $\mathcal{F}[x]$ has no zero divisors, and hence $\mathcal{F}[x]$ forms an integral domain (see Section 1.5).

Corollary 3 Let $p \neq 0$ be an element of $\mathcal{F}[x]$. Then there exists $q \in \mathcal{F}[x]$ such that $pq = 1$ if and only if $\deg p = 0$, and hence $\mathcal{F}[x]$ is not a field.

Proof If $\deg p = 0$ then $p = a \in \mathcal{F}$ with $a \neq 0$, and thus there exists $q = a^{-1} \in \mathcal{F}$ (hence $q = a^{-1} \in \mathcal{F}[x]$) such that $pq = aa^{-1} = 1$. On the other hand, if $pq = 1$ we have

$$0 = \deg 1 = \deg pq = \deg p + \deg q \ .$$

But $p \neq 0$ implies that $\deg p \geq 0$, and if $q \neq 0$, we must also have $\deg q \geq 0$. It then follows that $\deg p = 0$. ∎

We now prove a very useful and fundamental result known as the division algorithm. Essentially, we will show the existence of the polynomial quotient f/g (although technically this symbol as of yet has no meaning). The polyno-

mials q and r defined in the following theorem are called the **quotient** and **remainder** respectively. After the proof, we will give an example which shows that this is just the "long division" we all learned in elementary school.

Theorem 6.3 (**Division Algorithm**) Given f, g $\in \mathcal{F}$[x] with g $\neq$ 0, there exist unique polynomials q, r $\in \mathcal{F}$[x] such that

$$f = qg + r$$

where either r = 0 or deg r < deg g.

Proof The basic idea of the proof is to consider all possible degrees for the polynomials f and g, and show that the theorem can be satisfied in each case. After proving the existence of the polynomials q and r, we shall prove their uniqueness.

If f = 0 we simply choose q = r = 0. Now suppose that

$$f = a_0 + a_1x + \cdots + a_mx^m$$
$$g = b_0 + b_1x + \cdots + b_nx^n$$

where a_m, $b_n \neq 0$. If m = n = 0, then by Corollary 3 of Theorem 6.2, there exists $g^{-1} \in \mathcal{F}$[x] such that $g^{-1}g = 1$, and therefore $f = f(g^{-1}g) = (fg^{-1})g + 0$ satisfies our requirements. Next, if m = 0 and n > 0, then we may write f = 0g + f with deg r = deg f < deg g.

We now assume that m > 0 and proceed by induction on m. In other words, we assume that q and r can be found for all polynomials f with deg f $\leq$ m − 1 and proceed to construct new polynomials q and r for deg f = m. First note that if n > m we may again take f = 0g + f to satisfy the theorem. Thus we need only consider the case of n $\leq$ m.

Define the polynomial

$$f_1 = f - (a_m/b_n)x^{m-n}g \ .$$

Then the coefficient of the x^m term in f_1 is 0 (it cancels out on the right hand side), and hence deg $f_1 \leq$ m − 1. Therefore, by our induction hypothesis, there exist polynomials q_1 and r_1 in $\mathcal{F}$[x] with either $r_1 = 0$ or deg r_1 < deg g such that $f_1 = q_1g + r_1$. Substituting the definition of f_1 in this equation yields

$$f = [(a_m/b_n)x^{m-n} + q_1]g + r_1 \ .$$

If we define $r = r_1$ and $q = (a_m/b_n)x^{m-n} + q_1$, we see that $f = qg + r$ where either $r = 0$ or $\deg r < \deg g$. This proves the existence of the polynomials q and r, and all that remains is to prove their uniqueness.

Suppose that

$$f = qg + r = q'g + r'$$

where both r and r' satisfy the theorem, and assume that $r \neq r'$. Then

$$r - r' = (q' - q)g \neq 0$$

where

$$\deg(r - r') < \deg g$$

by Theorem 6.2(a). On the other hand, from Theorem 6.2(b) we see that

$$\deg(r - r') = \deg[(q' - q)g] = \deg(q' - q) + \deg g \geq \deg g \ .$$

This contradiction shows that in fact $r' = r$. We now have $(q' - q)g = 0$ with $g \neq 0$, and hence by Corollary 2(a) of Theorem 6.2, we have $q' - q = 0$, and therefore $q' = q$. ∎

Let us give an example of the division algorithm that should clarify what was done in the theorem.

Example 6.2 Consider the polynomials

$$f = 2x^4 + x^2 - x + 1$$
$$g = 2x - 1 \ .$$

Following the proof of Theorem 6.3 we have

$$f_1 = f - x^3 g = x^3 + x^2 - x + 1 \ .$$

Now let

$$f_2 = f_1 - (1/2)x^2 g = (3/2)x^2 - x + 1 \ .$$

Again, we let

$$f_3 = f_2 - (3/4)xg = (-1/4)x + 1$$

so that

$$f_4 = f_3 + (1/8)g = 7/8 \ .$$

Since deg(7/8) < deg g, we are finished with the division. Combining the above polynomials we see that

$$f = [x^3 + (1/2)x^2 + (3/4)x - (1/8)]g + f_4$$

and therefore

$$q = x^3 + (1/2)x^2 + (3/4)x - (1/8)$$
$$r = 7/8 \ .$$

This may also be written out in a more familiar form as

$$\begin{array}{r} x^3 + (1/2)x^2 + (3/4)x - (1/8) \\ 2x-1\overline{)\,2x^4 + x^2 - x + 1} \\ \underline{2x^4 - x^3} \\ x^3 + x^2 - x + 1 \\ \underline{x^3 - (1/2)x^2} \\ (3/2)x^2 - x + 1 \\ \underline{(3/2)x^2 - (3/4)x} \\ -(1/4)x + 1 \\ \underline{-(1/4)x + (1/8)} \\ 7/8 \end{array}$$

It should be noted that at each step in the division, we eliminated the highest remaining power of f by subtracting the appropriate multiple of g. //

Exercises

1. Let $\mathcal{F} = \{0, 1\}$ be the field consisting of only two elements, and define addition and multiplication on these elements in the obvious way (see Exercise 1.5.17). Show that the distinct polynomials $x^2 - x$ and 0 define the same polynomial function.

2. Use the division algorithm to find the quotient and remainder when $f = 2x^4 - x^3 + x - 1 \in \mathbb{R}[x]$ is divided by $g = 3x^3 - x^2 + 3 \in \mathbb{R}[x]$.

3. Consider the polynomials p = {2, 0, 1, 1} and q = {1, 1, −1} over $\mathbb{R}$. Evaluate the product pq by applying the definition. Show that this yields the same result as directly multiplying together the polynomial functions p and q.

4. Given a polynomial $p = a_n x^n + \cdots + a_1 x + a_0$, we define its **formal derivative** to be the polynomial $Dp = na_n x^{n-1} + \cdots + 2a_2 x + a_1$. In other words, $D: \mathcal{F}[x] \to \mathcal{F}[x]$ is a **differentiation operator**. Prove $D(p + q) = Dp + Dq$ and $D(pq) = p(Dq) + (Dp)q$.

5. Find the remainder when $ix^9 + 3x^7 + x^6 - 2ix + 1 \in \mathbb{C}[x]$ is divided by $x + i \in \mathbb{C}[x]$.

6.2 FACTORIZATION OF POLYNOMIALS

If f(x) is a polynomial in $\mathcal{F}[x]$, then $c \in \mathcal{F}$ is said to be a **zero** (or **root**) of f if f(c) = 0. We shall also sometimes say that c is a **solution** of the polynomial equation f(x) = 0. We will see that information about the roots of a polynomial plays an extremely important role throughout much of the remainder of this text.

If $f, g \in \mathcal{F}[x]$ and $g \neq 0$, then we say that f is **divisible** by g (or g **divides** f) over $\mathcal{F}$ if f = qg for some $q \in \mathcal{F}[x]$. In other words, f is divisible by g if the remainder in the division of f by g is zero. In this case we also say that g is a **factor** of f (over $\mathcal{F}$). It is standard notation to write g|f when we wish to say that g divides f, or to write $g \nmid f$ when g does not divide f.

The next theorem is known as the remainder theorem, and its corollary is known as the factor theorem.

Theorem 6.4 (**Remainder Theorem**) Suppose $f \in \mathcal{F}[x]$ and $c \in \mathcal{F}$. Then the remainder in the division of f by x − c is f(c). In other words,

$$f(x) = (x - c)q + f(c) \ .$$

Proof We see from the division algorithm that f = (x − c)q + r where either r = 0 or deg r < deg (x − c) = 1, and hence either r = 0 or deg r = 0 (in which case $r \in \mathcal{F}$). In either case, we may substitute c for x to obtain

$$f(c) = (c - c)q(c) + r = r \ . \ \blacksquare$$

Corollary (**Factor Theorem**) If $f \in \mathcal{F}[x]$ and $c \in \mathcal{F}$, then $x - c$ is a factor of f if and only if $f(c) = 0$.

Proof Rephrasing the statement of the corollary as $f = q(x - c)$ if and only if $f(c) = 0$, it is clear that this follows directly from the theorem. ∎

Example 6.3 If we divide $f = x^3 - 5x^2 + 7x$ by $g = x - 2$, we obtain $q = x^2 - 3x + 1$ and $r = 2$. It is also easy see that $f(2) = 8 - 5(4) + 7(2) = 2$ as it should according to Theorem 6.4. //

Let R be a commutative ring with unit element. An element $u \in R$ is called a **unit** (*not* a unit element) if there exists $r \in R$ such that $ur = 1$. Other ways to say this are that u divides 1, or that a unit is an element whose inverse is also in the ring. We leave it to the reader to show that $u \in R$ is a unit if and only if it is a factor of every element of R (see Exercise 6.2.1). An element $p \in R$ that is neither zero nor a unit is said to be **prime** if $p = ab$ implies that either a or b is a unit. Thus a prime element is one that can not be factored in a nontrivial way.

Example 6.4 Since for any integer $n \neq \pm 1$ the number $1/n$ is not an integer, it should be clear that the ring of integers $\mathbb{Z}$ has only the units 1 and -1. On the other hand, if $\mathcal{F}$ is any field and $a \in \mathcal{F}$, then a^{-1} is also a member of $\mathcal{F}$, and hence any nonzero element of a field is a unit. In particular, the units of the ring $\mathcal{F}[x]$ are just the polynomials of degree zero (i.e., the nonzero constant polynomials).

If we consider the ring of integers $\mathbb{Z}$, then a number $p \in \mathbb{Z}$ with $p \neq \pm 1$ or 0 will be prime if the only divisors of p are ± 1 and $\pm p$. However, if we consider the field $\mathbb{R}$, then any nonzero element of $\mathbb{R}$ (i.e., any nonzero real number) is a unit, and hence the notion of a prime real number is not very useful. //

In the particular case of $R = \mathcal{F}[x]$, a prime polynomial is frequently called an **irreducible** polynomial. A polynomial that is not irreducible is said to be **reducible**. Two polynomials $f, g \in \mathcal{F}[x]$ are said to be **associates** if $f = cg$ for some nonzero $c \in \mathcal{F}$, and in general, two elements $a, b \in R$ are said to be **associates** if $a = ub$ where u is a unit of R. We leave it to the reader to show that this defines an equivalence relation on a commutative ring with unit element (Exercise 6.2.3).

It should be clear that any nonzero polynomial has exactly one monic polynomial as an associate since we can always write

$$a_0 + a_1x + \cdots + a_nx^n = a_n(a_0a_n^{-1} + a_1a_n^{-1}x + \cdots + x^n) .$$

It should also be clear that any polynomial f with deg f ≥ 1 has its associates and the set of nonzero constant polynomials as divisors. Thus we see that a nonzero polynomial f is prime if and only if f = gh implies that either g or h is of degree zero, and hence the other is an associate of f.

It is important to realize that whether or not a polynomial is prime depends on the particular field $\mathcal{F}$. For example, since $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$, we see that $x^2 - 2$ is prime over $\mathbb{Q}$, but is not prime over $\mathbb{R}$.

Returning to our commutative ring R with unit element, we say that an element $d \in R$ is a **greatest common divisor** (frequently denoted simply by gcd) of the elements $a_1, \ldots, a_n \in R$ if

(1) $d|a_i$ for every $i = 1, \ldots, n$ (i.e., d is a **common divisor** of the a_i);
(2) If $c \in R$ is such that $c|a_i$ for every $i = 1, \ldots, n$, then $c|d$.

Two distinct elements $a, b \in R$ are said to be **relatively prime** if their greatest common divisor is a unit of R. Note that we have referred to *a* greatest common divisor, implying that there may be more than one. This is only true in a certain sense as the next theorem shows.

Theorem 6.5 Let $f_1, \ldots, f_n$ be nonzero polynomials in $\mathcal{F}[x]$. Then there exists at least one greatest common divisor d of the set $\{f_1, \ldots, f_n\}$. Moreover, this greatest common divisor is unique up to a unit factor, and can be expressed in the form $d = \sum_{i=1}^{n} h_i f_i$ for some set of polynomials $h_i \in \mathcal{F}[x]$.

Proof Consider the set S of all polynomials in $\mathcal{F}[x]$ of the form $g_1 f_1 + \cdots + g_n f_n$ where each g_i is an *arbitrary* element of $\mathcal{F}[x]$. Then in particular, each f_i is an element of S, and in addition, if $p \in S$ and $q \in \mathcal{F}[x]$, then $pq \in S$. Let D be the set of degrees of all nonzero polynomials in S. Then D is just a collection of nonnegative integers, and hence by the well-ordering principle (Section 0.5), D has a least element α. This means that there exists a nonzero polynomial $d = h_1 f_1 + \cdots + h_n f_n \in S$ such that $\alpha = \deg d \leq \deg c$ for all nonzero polynomials $c \in S$. We first show that $d|f_i$ for every $i = 1, \ldots, n$.

By the division algorithm, for each $i = 1, \ldots, n$ we have $f_i = q_i d + r_i$ where either $r_i = 0$ or $\deg r_i < \deg d$. But $r_i = f_i - q_i d \in S$ so that if $r_i \neq 0$, we would have $\deg r_i < \deg d$ which contradicts the definition of d. Therefore we must have $r_i = 0$ and hence $f_i = q_i d$ so that $d|f_i$ for every $i = 1, \ldots, n$. While this shows that d is a common divisor of $\{f_i\}$, we must show that it is in fact a greatest common divisor.

If c is any other common divisor of $\{f_1, \ldots, f_n\}$, then by definition there exist polynomials g_i such that $f_i = g_i c$ for each $i = 1, \ldots, n$. But then

$$d = \sum h_i f_i = \sum h_i(g_i c) = (\sum h_i g_i)c$$

so that $c|d$. This proves that d is a greatest common divisor.

Now suppose d' is another greatest common divisor of the set $\{f_1, \ldots, f_n\}$. Then by definition of greatest common divisor we must have both $d|d'$ and $d'|d$, so that $d' = ud$ and $d = vd'$ for some polynomials $u, v \in \mathcal{F}[x]$. Multiplying the second of these equations by u, we see that $uvd' = ud = d'$, and therefore $d'(1 - uv) = 0$. By Corollary 2(a) of Theorem 6.2, we then have $1 - uv = 0$ so that $uv = 1$ and hence u and v are units. (Alternatively, the fact that $\deg d = \deg d'$ implies that u and v must be of degree zero, and hence are units.) ∎

What we have shown is that a gcd exists, and is unique up to its associates. Therefore, if we restrict ourselves to *monic* greatest common divisors, then we have proved the existence of a unique gcd.

Corollary 1 Let $q_1, \ldots, q_n \in \mathcal{F}[x]$ be relatively prime (i.e., they have no common divisors other than units). Then there exist elements $h_1, \ldots, h_n \in \mathcal{F}[x]$ such that $h_1q_1 + \cdots + h_nq_n = 1$.

Proof This is an obvious special case of Theorem 6.5. ∎

Corollary 2 Suppose $f, g, p \in \mathcal{F}[x]$ where p is prime and $p|fg$. Then either $p|f$ or $p|g$.

Proof Since p is prime, its only divisors are units and its associates. Therefore, if we assume that $p \nmid f$, then the only greatest common divisor of p and f is a unit, and thus p and f are relatively prime. Applying Theorem 6.5, we may write $up + vf = 1$ for some $u, v \in \mathcal{F}[x]$, and hence multiplying by g yields $pug + fgv = g$. But $p|fg$ so that $fg = qp$ for some $q \in \mathcal{F}[x]$, and thus we have $p(ug + qv) = g$ so that $p|g$. It is obvious that had we started with the assumption that $p \nmid g$, we would have found that $p|f$. ∎

By choosing $f = f_1$ and $g = f_2 \cdots f_n$ in Corollary 2 we have the following obvious generalization.

Corollary 2′ If $p, f_1, f_2, \ldots, f_n \in \mathcal{F}[x]$ where p is prime and $p|f_1f_2 \cdots f_n$, then $p|f_i$ for some $i = 1, \ldots, n$.

While Theorem 6.5 proves the existence of a greatest common divisor, it is not of any help in actually computing one. Given two polynomials, we can find their gcd by a procedure known as the Euclidean algorithm (compare

Section 0.7). This approach, illustrated in the next example, is also an alternative proof of Theorem 6.5, the general case as stated in the theorem following by induction.

Example 6.5 (**Euclidean algorithm**) Suppose f, g $\in \mathcal{F}[x]$ and f $\neq$ 0. We show the existence of a unique monic polynomial d $\in \mathcal{F}[x]$ such that

(1) d|f and d|g.

(2) If c $\in \mathcal{F}[x]$ is such that c|f and c|g, then c|d.

First note that if g = 0 and a_m is the leading coefficient of f, then the monic polynomial $d = a_m^{-1}f$ satisfies both requirements (1) and (2). Now assume that g $\neq$ 0 also. By the division algorithm, there exist *unique* polynomials q_1 and r_1 such that

$$f = gq_1 + r_1$$

with either $r_1 = 0$ or deg r_1 < deg g. If $r_1 = 0$, then g|f and d = g satisfies (1) and (2). If $r_1 \neq 0$, then we apply the division algorithm again to obtain polynomials q_2 and r_2 such that

$$g = r_1q_2 + r_2 \ .$$

If $r_2 = 0$, then $r_1|g$ which implies that $r_1|f$, and thus $d = r_1$ is a common divisor. (It still remains to be shown that this d is a *greatest* common divisor.) If $r_2 \neq 0$, then we continue the process, thus obtaining the following progression:

$$\begin{aligned}
f &= gq_1 + r_1 && \deg r_1 < \deg g \\
g &= r_1q_2 + r_2 && \deg r_2 < \deg r_1 \\
r_1 &= r_2q_3 + r_3 && \deg r_3 < \deg r_2 \\
&\vdots && \vdots \\
r_{k-2} &= r_{k-1}q_k + r_k && \deg r_k < \deg r_{k-1} \\
r_{k-1} &= r_kq_{k+1}
\end{aligned}$$

This progression must terminate as shown since the degree of any polynomial is a positive integer and deg r_1 > deg r_2 > · · · > deg $r_k \geq 0$. Letting r_k be the last nonzero remainder, we claim that $r_k = d$.

To see this, first note that $r_k|r_{k-1}$ since $r_{k-1} = r_kq_{k+1}$. Next, we see that

$$r_{k-2} = r_{k-1}\, q_k + r_k = r_k\ q_{k+1}\, q_k + r_k$$

and therefore $r_k|r_{k-2}$. Continuing this procedure, we find that $r_k|r_{k-1}$, $r_k|r_{k-2}$, . . . , $r_k|r_1$, $r_k|g$ and finally $r_k|f$. This shows that $d = r_k$ satisfies (1). Now suppose that c|f and c|g. Then, since $r_1 = f - gq_1$ we must have $c|r_1$. Similarly $r_2 = g - r_1q_2$ so that $c|r_2$. Continuing this process, it is clear that we eventually

arrive at the conclusion that $c|r_k$, thus proving (2) for the choice $d = r_k$. Finally, if r is the leading coefficient of r_k, then $r^{-1}r_k$ is a monic polynomial satisfying (1) and (2), and its uniqueness follows exactly as in the proof of Theorem 6.5. //

Example 6.6 As a specific illustration of the preceding example, consider the polynomials $f = x^4 - x^3 - x^2 + 1$ and $g = x^3 - 1$ over the field $\mathbb{Q}$. Dividing f by g we obtain

$$x^4 - x^3 - x^2 + 1 = (x^3 - 1)(x - 1) + (-x^2 + x) .$$

Now divide g by $r_1 = -x^2 + x$ to obtain

$$x^3 - 1 = (-x^2 + x)(-x - 1) + (x - 1) .$$

Lastly, we divide r_1 by $r_2 = x - 1$ to find

$$-x^2 + x = (x - 1)(-x)$$

and therefore the gcd of f and g is $x - 1$. //

Our next very important result is known as the unique factorization theorem. Recall that by definition, a prime polynomial is not a unit, and thus has positive degree.

Theorem 6.6 (**Unique Factorization Theorem**) Every nonzero element $f \in \mathcal{F}[x]$ is either a unit, or is expressible as a unique (up to associates) finite product of prime elements.

Proof We first show that $f \in \mathcal{F}[x]$ is expressible as a product of prime polynomials. Afterwards we will prove uniqueness. Our approach is by induction on deg f; in other words, we assume that deg $f > 1$ (if deg $f = 0$ then f is a unit, and if deg $f = 1$ the theorem is obvious), and suppose that the theorem is true for all $g \in \mathcal{F}[x]$ with deg $g <$ deg f. We will show that the theorem is true for f.

Assume f is reducible (or else there is nothing to prove) so that $f = pq$ where neither p nor q is a unit. By Theorem 6.2(b) we have deg $p <$ deg $p +$ deg $q =$ deg f, and similarly deg $q <$ deg f. Therefore, by our induction hypothesis, both p and q can be written as a finite product of prime elements in $\mathcal{F}[x]$, and hence the same is true of $f = pq$.

To prove the uniqueness of the product, assume that

$$f = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

where each of the p_i and q_j are prime. Since $p_1 | p_1 p_2 \cdots p_n$, it follows that $p_1 | q_1 q_2 \cdots q_m$. By Corollary 2′ of Theorem 6.5, it then follows that $p_1 | q_j$ for some $j = 1, \ldots, m$. But since both p_1 and q_j are prime and $p_1 | q_j$, they must be associates, and hence $q_j = u_1 p_1$ where u_1 is a unit in $\mathcal{F}[x]$. This means that

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m = q_1 q_2 \cdots q_{j-1} u_1 p_1 q_{j+1} \cdots q_m .$$

Cancelling p_1 from both sides of this equation (using Theorem 6.2, Corollary 2) results in

$$p_2 \cdots p_n = u_1 q_1 \cdots q_{j-1} q_{j+1} \cdots q_m .$$

Repeating this argument, we next eliminate p_2 and one of the remaining factors on the right. Continuing in this manner, we pairwise eliminate one of the p_i and one of the q_k with each operation, always replacing a q_k with a corresponding u_k. But the primes on one side of this equation can not be eliminated before those on the other side because this would imply that a product of prime polynomials was equal to 1 which is impossible. Therefore $n = m$, and the expansion of f as a product of prime elements must be unique up to an associate. ∎

Note that the expansion proved in this theorem for $f \in \mathcal{F}[x]$ is completely unique (except for order) if we require that the prime polynomials be monic.

Example 6.7 Consider the polynomial $p = 3x^4 - 3x^2 - 6 \in \mathcal{F}[x]$. Using the fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ we can factor p three different ways depending on $\mathcal{F}$:

$$\begin{aligned} 3(x^2 - 2)(x^2 + 1) &\quad \text{in } \mathbb{Q}[x] \\ 3(x + \sqrt{2})(x - \sqrt{2})(x^2 + 1) &\quad \text{in } \mathbb{R}[x] \\ 3(x + \sqrt{2})(x - \sqrt{2})(x + i)(x - i) &\quad \text{in } \mathbb{C}[x] \end{aligned}$$

In each case, p is a product of prime polynomials relative to the appropriate field. //

Exercises

1. Let R be a commutative ring with unit element. Show that $u \in R$ is a unit of R if and only if u is a factor of every element of R.

2. Let R be an integral domain with unit element and suppose it is true that $a|b$ and $b|a$ for some $a, b \in R$. Show that $a = ub$ where u is a unit in R.

3. Show that the property of being associates defines an equivalence relation on a commutative ring with unit element.

4. Let $\mathcal{F}$ be an arbitrary field, and suppose $p \in \mathcal{F}[x]$ is of degree ≤ 3. Prove that p is prime in $\mathcal{F}[x]$ if and only if p is either of degree 1, or has no zeros in $\mathcal{F}$. Give an example to show that this result is not true if $\deg p > 3$.

5. Factor the following polynomials into their prime factors in both $\mathbb{R}[x]$ and $\mathbb{Q}[x]$:
   (a) $2x^3 - x^2 + x + 1$.
   (b) $3x^3 + 2x^2 - 4x + 1$.
   (c) $x^6 + 1$.
   (d) $x^4 + 16$.

6. Let $\mathcal{F} = \{0, 1\}$ be the field consisting of only two elements, and define addition and multiplication on $\mathcal{F}$ in the obvious way. Factor the following polynomials into primes in $\mathcal{F}[x]$:
   (a) $x^2 + x + 1$.
   (b) $x^3 + 1$.
   (c) $x^4 + x^2 + 1$.
   (d) $x^4 + 1$.

7. Let $\mathcal{F}$ be as in the previous problem. Find the greatest common divisor of $x^3 + x^2 + x + 1$ and $x^5 + x^4 + x^3 + x^2 + x + 1$ over $\mathcal{F}[x]$.

8. Find the greatest common divisor of the following pairs of polynomials over $\mathbb{R}[x]$. Express your result in the form defined in Theorem 6.5.
   (a) $4x^3 + 2x^2 - 2x - 1$ and $2x^3 - x^2 + x + 1$.
   (b) $x^3 - x + 1$ and $2x^4 + x^2 + x - 5$.
   (c) $x^4 + 3x^2 + 2$ and $x^5 - x$.
   (d) $x^3 + x^2 - 2x - 2$ and $x^4 - 2x^3 + 3x^2 - 6x$.

9. Use the remainder theorem to find the remainder when $2x^5 - 3x^3 + 2x + 1 \in \mathbb{R}[x]$ is divided by:
   (a) $x - 2 \in \mathbb{R}[x]$.
   (b) $x + 3 \in \mathbb{R}[x]$.

10. (a) Is $x - 3$ a factor of $3x^3 - 9x^2 - 7x + 21$ over $\mathbb{Q}[x]$?
    (b) Is $x + 2$ a factor of $x^3 + 8x^2 + 6x - 8$ over $\mathbb{R}[x]$?
    (c) For which $k \in \mathbb{Q}$ is $x - 1$ a factor of $x^3 + 2x^2 + x + k$ over $\mathbb{Q}[x]$?
    (d) For which $k \in \mathbb{C}$ is $x + i$ a factor of $ix^9 + 3x^7 + x^6 - 2ix + k$ over $\mathbb{C}[x]$?

11. (a) Construct an example to show that the division algorithm is not true if $\mathcal{F}$ is replaced by the integral domain $\mathbb{Z}$.
    (b) Prove that if the division algorithm is true for polynomials over an integral domain D, then D must be a field.

12. Determine the monic associate of:
    (a) $2x^3 - x + 1 \in \mathbb{Q}[x]$.
    (b) $-ix^2 + x + 1 \in \mathbb{C}[x]$.

13. Let $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ be a polynomial with integer coefficients, and suppose $r/s \in \mathbb{Q}$ is a rational root of f. Assume that r and s are relatively prime. Prove that $r|a_0$ and $s|a_n$.

6.3 POLYNOMIAL IDEALS

We now apply the formalism of Section 1.5 to polynomials. If the reader has not yet studied that section (or does not remember it), now is the time to go back and do so (again if necessary).

Example 6.8 Let A and B be ideals of $\mathcal{F}[x]$. We show that

$$A \cap B = \{f \in \mathcal{F}[x]: f \in A \text{ and } f \in B\}$$

and

$$A + B = \{f + g \in \mathcal{F}[x]: f \in A \text{ and } g \in B\}$$

are both ideals of $\mathcal{F}[x]$. Indeed, if $f, g \in A \cap B$, then $f \pm g \in A$ and $f \pm g \in B$ since A and B are ideals. Therefore $f \pm g \in A \cap B$ so that $A \cap B$ is a subgroup of $\mathcal{F}[x]$ under addition. Similarly, if $f \in A \cap B$ and $g \in \mathcal{F}[x]$, then $fg \in A$ and $fg \in B$ so that $fg \in A \cap B$, and hence $A \cap B$ is an ideal. Now suppose $f_1 + g_1, f_2 + g_2 \in A + B$. Then

$$(f_1 + g_1) \pm (f_2 + g_2) = (f_1 \pm f_2) + (g_1 \pm g_2) \in A + B$$

so that A + B is also a subgroup of $\mathcal{F}[x]$ under addition. Finally, suppose that $f_1 + g_1 \in A + B$ and $h \in \mathcal{F}[x]$. Then

$$(f_1 + g_1)h = f_1h + g_1h \in A + B$$

so that A + B is an ideal also. //

Recall that $\mathcal{F}[x]$ is not only a ring, it is in fact an integral domain (Corollary 2 of Theorem 6.2). Since $\mathcal{F}[x]$ is a ring, we see that if $p \in \mathcal{F}[x]$, then p can be used to generate the principal ideal (p) of $\mathcal{F}[x]$. Note that by construction, the ideal (p) can not contain any prime polynomials (other than associates of p) even if p itself is prime. This is because any $q \in (p)$ can be written in the form q = pr for some $r \in \mathcal{F}[x]$, and hence p|q. We will also write the principal ideal (p) in the form

$$(p) = p\mathcal{F}[x] = \{pf: f \in \mathcal{F}[x]\} .$$

Our next theorem is frequently useful when working with quotient rings (see Theorem 1.13) of the general form $\mathcal{F}[x]/(p)$.

Theorem 6.7 Suppose $p = a_0 + a_1x + \cdots + a_nx^n \in \mathcal{F}[x]$, $a_n \neq 0$, and let I = (p). Then every element of $\mathcal{F}[x]/I$ can be uniquely expressed in the form

$$I + (b_0 + b_1x + \cdots + b_{n-1}x^{n-1})$$

where $b_0, \ldots, b_{n-1} \in \mathcal{F}$.

Proof Choose any $I + f \in \mathcal{F}[x]/I$. By the division algorithm (Theorem 6.3) we can write f = pq + r for some $q, r \in \mathcal{F}[x]$ with either r = 0 or deg r < deg p. But by definition of I, we have $pq \in I$ so that

$$I + f = I + (pq + r) = I + r .$$

This shows that I + f has the form desired.

To prove the uniqueness of this representation, suppose that

$$I + (b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}) = I + (c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}) .$$

Then (by adding $I + (-c_0 - c_1x - \cdots - c_{n-1}x^{n-1})$ to both sides) we see that

$$(b_0 - c_0) + (b_1 - c_1)x + \cdots + (b_{n-1} - c_{n-1})x^{n-1} \in I .$$

But the degree of any nonzero polynomial in I must be greater than or equal to n = deg p (by definition of I and Theorem 6.2(b)), and therefore it follows that

$$(b_0 - c_0) + (b_1 - c_1)x + \cdots + (b_{n-1} - c_{n-1})x^{n-1} = 0 \ .$$

Since two polynomials are equal if and only if their coefficients are equal, this means that $b_i = c_i$ for every $i = 0, \ldots, n - 1$. ∎

It is an interesting fact that every ideal of $\mathcal{F}[x]$ is actually a principal ideal. We prove this in our next theorem.

Theorem 6.8 Every ideal of the ring $\mathcal{F}[x]$ is a principal ideal.

Proof Let I be any ideal of $\mathcal{F}[x]$. If $I = \{0\}$, then I is just the principal ideal (0). Now assume that $I \neq \{0\}$ and let g be any nonzero polynomial of least degree in I. (That g exists follows from the well-ordering principle. In other words, if S is the set of degrees of all polynomials in $\mathcal{F}[x]$, then S has a least element.) From the definitions it is clear that $(g) \subset I$. We now show that $I \subset (g)$ which will then prove that $I = (g)$.

By the division algorithm, for any $f \in I$ there exist polynomials $q, r \in \mathcal{F}[x]$ such that $f = gq + r$ where either $r = 0$ or $\deg r < \deg g$. Since $f \in I$ and $gq \in I$, it follows that $r = f - gq \in I$. But if $r \neq 0$ we have $\deg r < \deg g$ which contradicts the definition of g as the polynomial of least degree in I. Therefore $r = 0$ so that $f = gq \in (g)$, and hence $I \subset (g)$. ∎

Corollary Every ideal of $\mathcal{F}[x]$ is generated by a unique monic polynomial.

Proof Since every ideal of $\mathcal{F}[x]$ is principal, suppose that $(p) = (q)$ or, equivalently, $p\,\mathcal{F}[x] = q\,\mathcal{F}[x]$. Then clearly $p \in p\,\mathcal{F}[x]$ so that $p = qf_1$ for some $f_1 \in \mathcal{F}[x]$. Similarly, we see that $q = pf_2$ for some $f_2 \in \mathcal{F}[x]$ and hence

$$p = qf_1 = pf_2f_1 \ .$$

Since $\mathcal{F}[x]$ is an integral domain it follows that $f_1f_2 = 1$. But this means that f_1 and f_2 are units (i.e., constant polynomials), and hence $q = cp$ for some $c \in \mathcal{F}$. Noting that $cp\,\mathcal{F}[x]$ is the same as $p\,\mathcal{F}[x]$, we see that any ideal $p\,\mathcal{F}[x]$ may be written in the form $cp\,\mathcal{F}[x]$ for arbitrary $c \in \mathcal{F}$. By choosing c to be the inverse of the leading coefficient of p, we have shown that any ideal of $\mathcal{F}[x]$ has a unique monic generator. ∎

In Section 6.2 we discussed the greatest common divisor of a collection of polynomials. We now treat a related concept that the reader may be wondering about. If f, g $\in \mathcal{F}[x]$ then, by the **least common multiple** (or simply lcm) of f and g, we mean the polynomial m $\in \mathcal{F}[x]$ such that f|m and g|m, and if m′ $\in \mathcal{F}[x]$ is another polynomial that satisfies f|m′ and g|m′, then m|m′.

As a useful observation, note that if f, g $\in \mathcal{F}[x]$ and f|g, then g = fq for some q $\in \mathcal{F}[x]$. But (f) = f $\mathcal{F}[x]$ and hence

$$(g) = g\mathcal{F}[x] = fq\mathcal{F}[x] \subset (f) .$$

In other words, f|g implies that (g) $\subset$ (f).

Example 6.9 Let A and B be ideals of $\mathcal{F}[x]$. By Theorem 6.8 and Example 6.8 we may write A = h $\mathcal{F}[x]$ and B = k $\mathcal{F}[x]$, and also A $\cap$ B = m $\mathcal{F}[x]$ and A + B = d $\mathcal{F}[x]$. We claim that d is a greatest common divisor of h and k, and that m is a least common multiple of h and k.

To see this, first note that since h $\in$ h $\mathcal{F}[x]$ = A, it follows that h = h + 0 $\in$ A + B, and hence h = dh_1 for some $h_1 \in \mathcal{F}[x]$. Similarly, we must have k = dk_1 for some $k_1 \in \mathcal{F}[x]$. Therefore d|h and d|k so that d is a common divisor of h and k. We must show that if d′|h and d′|k, then d′|d. Now, if d′|h and d′|k, then A = (h) $\subset$ (d′) and B = (k) $\subset$ (d′). But then A + B $\subset$ (d′) because for any f + g $\in$ A + B we have f $\in$ A $\subset$ (d′) and g $\in$ B $\subset$ (d′), and therefore f + g $\in$ (d′) since (d′) is an ideal. This means that d $\in$ A + B $\subset$ (d′) so that d = d′p for some p $\in \mathcal{F}[x]$, and hence d′|d.

Now note that m $\in$ A $\cap$ B so that m $\in$ A implies m = hm_1 and m $\in$ B implies m = km_2 for some polynomials m_1, $m_2 \in \mathcal{F}[x]$. This means that h|m and k|m so that m is a common multiple of h and k. Next, note that if h|m′ then (m′) $\subset$ (h) = A, and if k|m′ then (m′) $\subset$ (k) = B. Therefore we see that m′ $\in$ (m′) $\subset$ A $\cap$ B = (m) so that m′ = mq for q $\in \mathcal{F}[x]$. Hence m|m′ and m is a least common multiple of h and k. //

Greatest common divisors and least common multiples will be of considerable use to us in the next chapter. The following important theorem relates least common multiples and greatest common divisors. Rather than prove it directly, we simply note that it follows easily from Theorem 6.10 below.

Theorem 6.9 Suppose h, k $\in \mathcal{F}[x]$ and let d and m be the greatest common divisor and least common multiple respectively of h and k. Then hk = dm.

Recall from Theorem 6.6 that any polynomial $h \in \mathcal{F}[x]$ is expressible as a unique product of prime polynomials. If h contains the prime factor $g_i \in \mathcal{F}[x]$ repeated r_i times, then we write $g_i^{r_i}$ as one of the factors of h. Therefore we may write the decomposition of h in the form $h = \prod_i g_i^{r_i}$. If $k \in \mathcal{F}[x]$ is another polynomial, then it may also be factored in the same manner as $k = \prod_j q_j^{s_j}$. In fact, we may write both h and k as a product of the *same* factors if we allow the exponent to be zero for any factor that does not appear in that expansion. In other words, we may write $h = \prod_{i=1}^{n} p_i^{r_i}$ and $k = \prod_{i=1}^{n} p_i^{s_i}$ where $r_i \geq 0$ and $s_i \geq 0$ for each $i = 1, \ldots, n$.

The next theorem contains Theorem 6.9 as an immediate and obvious corollary.

Theorem 6.10 Suppose that $h, k \in \mathcal{F}[x]$ and write

$$h = \prod_{i=1}^{n} p_i^{r_i} \qquad k = \prod_{i=1}^{n} p_i^{s_i}$$

where each $r_i \geq 0$ and each $s_i \geq 0$. For the given r_i and s_i, define the polynomials

$$\alpha = \prod_{r_i > s_i} p_i^{r_i} \qquad \beta = \prod_{r_i \leq s_i} p_i^{r_i} \qquad \gamma = \prod_{s_i < r_i} p_i^{s_i} \qquad \delta = \prod_{s_i \geq r_i} p_i^{s_i}$$

so that $h = \alpha\beta$ and $k = \gamma\delta$. Then the least common multiple m of h and k is given by

$$m = \alpha\delta = \prod_{i=1}^{n} p_i^{\max(r_i,\, s_i)}$$

and the greatest common divisor d is given by

$$d = \beta\gamma = \prod_{i=1}^{n} p_i^{\min(r_i,\, s_i)} \quad .$$

Proof Since the expressions for h and k are given in terms of the same set of prime polynomials p_i, a moment's thought should make it clear that the least common multiple is given by

$$m = \prod_{i=1}^{n} p_i^{\max(r_i,\, s_i)}$$

Formally, we see that $h|m$ and $k|m$, and if m' is another polynomial such that $h|m'$ and $k|m'$, then by Theorem 6.6 again we can write $m' = \prod_{i=1}^{n} p_i^{t_i}$ where we must have $t_i \geq r_i$ and $t_i \geq s_i$ for each $i = 1, \ldots, n$ in order that m' be a common multiple of h and k. But this means that $m|m'$ so that m is the least common multiple of h and k. In any case, m is exactly the same as the product $\alpha\delta$.

That the greatest common divisor is given by $\prod_{i=1}^{n} p_i^{\min(r_i, s_i)} = \beta\gamma$ follows from a similar argument. ∎

By Theorem 1.13, the quotient structure $\mathcal{F}[x]/(p)$ is a ring for any p, and we now show that it is actually a field for appropriate p.

Theorem 6.11 Suppose $p \in \mathcal{F}[x]$, and let $I = (p)$. Then $\mathcal{F}[x]/I$ is a field if and only if p is prime over $\mathcal{F}$.

Proof We first show that if p is reducible over $\mathcal{F}$, then $\mathcal{F}[x]/I$ is not a field. (This is the contrapositive to the statement that if $\mathcal{F}[x]/I$ is a field, then p must be prime.) To see this, assume that $p = ab$ where neither a nor b is a unit, and each is of degree less than that of p. From the definition of a principal ideal, we see that the degree of any polynomial in I must be greater than or equal to deg p, and hence neither a nor b can be an element of I. Since I is the zero element of $\mathcal{F}[x]/I$, we see that $I + a \neq I$ and $I + b \neq I$ must both be nonzero elements of $\mathcal{F}[x]/I$. But then

$$(I + a)(I + b) = I + ab = I + p = I$$

where we used the fact that $p \in I$. This shows that the product of two nonzero elements of $\mathcal{F}[x]/I$ yields the zero element of $\mathcal{F}[x]/I$, and thus the set of nonzero elements of $\mathcal{F}[x]/I$ is not closed under multiplication. Hence $\mathcal{F}[x]/I$ is neither a division ring nor an integral domain, so it certainly is not a field.

Conversely, suppose that p is prime. Since $\mathcal{F}[x]$ is a commutative ring, it follows that for any $a, b \in \mathcal{F}[x]$ we have that $\mathcal{F}[x]/I$ is also a commutative ring. The identity element in $\mathcal{F}[x]/I$ is easily seen to be $I + 1$ where 1 is the unit element for the field $\mathcal{F}$. Therefore, all that remains is to show the existence of a multiplicative inverse for each nonzero element in $\mathcal{F}[x]/I$.

If $I + f$ is any nonzero element in $\mathcal{F}[x]/I$, then $f \notin I$ so that $p \nmid f$. Since p is prime, its only divisors are units and its associates, and therefore the greatest common divisor of p and f is a unit (i.e., p and f are relatively prime). Applying Corollary 1 of Theorem 6.5 we see there exist $u, v \in \mathcal{F}[x]$ such that $up + vf = 1$. Then $1 - vf = up \in I$ and hence

$$I + 1 = I + up + vf = I + vf = (I + v)(I + f) .$$

This shows that $I + v$ is a multiplicative inverse of $I + f$. ∎

Exercises

1. Referring to Theorem 6.7, show that $\{I + c: c \in \mathcal{F}\}$ is a subfield of $\mathcal{F}[x]/I$ isomorphic to $\mathcal{F}$.

2. Let $p = 1 + x^2 \in \mathbb{R}[x]$ and let $I = (p)$.
   (a) Show $\mathbb{R}[x]/I$ is a field.
   (b) Show $\mathbb{R}[x]/I$ is isomorphic to $\mathbb{C}$. [*Hint*: Justify defining the mapping θ: $\mathbb{R}[x]/I \to \mathbb{C}$ by $\theta(I + (a + bx)) = a + ib$. Show that θ is bijective and preserves addition. To show that θ preserves multiplication, note that

$$(I + (a + bx))(I + (c + dx)) = I + (ac + (ad + bc)x + bdx^2) .$$

   Write this in the form $I + (u + vx)$ by following the first part of the proof of Theorem 6.7. Now show that

$$\theta[(I + (a + bx))(I + (c + dx))] = \theta(I + (a + bx))\theta(I + (c + dx)) .]$$

3. Suppose $f, g \in \mathcal{F}[x]$. Prove that $(f) = (g)$ if and only if f and g are associates.

4. Suppose $f, g \in \mathcal{F}[x]$. Prove or disprove the following:
   (a) If $(f) = (g)$, then $\deg f = \deg g$.
   (b) If $\deg f = \deg g$, then $(f) = (g)$.
   (c) If $f \in (g)$ and $\deg f = \deg g$, then $(f) = (g)$.

5. Find the greatest common divisor and least common multiple of the following pairs of polynomials:
   (a) $(x - 1)(x + 2)^2$ and $(x + 2)(x - 4)$.
   (b) $(x - 2)^2(x - 3)^4(x - i)$ and $(x - 1)(x - 2)(x - 3)^3$.
   (c) $(x^2 + 1)(x^2 - 1)$ and $(x + i)^3(x^3 - 1)$.

6. (a) Suppose $f_1, \ldots, f_n \in \mathcal{F}[x]$, and let $I = f_1\mathcal{F} + \cdots + f_n\mathcal{F}$ be the set of all polynomials of the form $g = f_1g_1 + \cdots + f_ng_n$ where $g_i \in \mathcal{F}[x]$. Show that I is an ideal. This is called the ideal **generated** by $\{f_1, \ldots, f_n\}$.
   (b) Show, in particular, that $\mathcal{F}[x]$ is an ideal generated by $\{1\}$. This is called the **unit** ideal.
   (c) Let d be the unique monic generator of I. Show that d divides each of the f_i.
   (d) If $c \in \mathcal{F}[x]$ divides each of the f_i, show that $c|d$.

(e) Suppose $\{f_1, f_2, f_3\}$ generates the unit ideal. Show that we can always find polynomials $f_{ij} \in \mathcal{F}[x]$ such that

$$\begin{vmatrix} f_1 & f_2 & f_3 \\ f_{21} & f_{22} & f_{23} \\ f_{31} & f_{32} & f_{33} \end{vmatrix} = 1 \ .$$

[*Hint*: Show there exists $g_1, g_2, g_3 \in \mathcal{F}[x]$ such that $\sum g_i f_i = 1$, and let $\alpha = \gcd\{g_1, g_2\}$. Next, show there exists $h_1, h_2 \in \mathcal{F}[x]$ such that $(g_1/\alpha)h_1 + (g_2/\alpha)h_2 = 1$. Now use the polynomials g_i, h_i and α to form the f_{ij}.]

6.4 POLYNOMIALS OVER ALGEBRAICALLY CLOSED FIELDS

We now turn to a discussion of polynomials over the fields $\mathbb{R}$ and $\mathbb{C}$. These are well worth considering in more detail since most practical applications in mathematics and physics deal with these two special cases. By way of terminology, a field $\mathcal{F}$ is said to be **algebraically closed** if every polynomial $f \in \mathcal{F}[x]$ with $\deg f > 0$ has at least one zero (or root) in $\mathcal{F}$.

Our next theorem is called the Fundamental Theorem of Algebra. While most proofs of this theorem involve the theory of complex variables, this result is so fundamental to our work that we present a proof in Appendix A that depends only on some relatively elementary properties of metric spaces. Basically, if the reader knows that a continuous function defined on a compact space takes its maximum and minimum values on the space, then there should be no problem understanding the proof. However, if the reader does not even know what a compact space is, then Appendix A presents all of the necessary formalism for a reasonably complete understanding of the concepts involved.

Theorem 6.12 (**Fundamental Theorem of Algebra**) The complex number field $\mathbb{C}$ is algebraically closed.

Proof See Appendix A. ∎

Let $p = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial of degree $n \geq 1$ over an algebraically closed field $\mathcal{F}$. Then there exists an element $\alpha_1 \in \mathcal{F}$ such that $p(\alpha_1) = 0$. Hence applying the factor theorem (Corollary to Theorem 6.4) we have

$$p = (x - \alpha_1)q$$

where q is a polynomial of degree n − 1. Again, if n − 1 > 0, we see that q has a zero α_2 in $\mathcal{F}$, and continuing this process we obtain

$$p = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where c is a unit of $\mathcal{F}$. We thus see that any polynomial of degree n ≥ 1 over an algebraically closed field has exactly n roots (although they need not be distinct). We repeat this statement as part of the next theorem.

Theorem 6.13 Let $\mathcal{F}$ be an algebraically closed field. Then every prime polynomial $p \in \mathcal{F}[x]$ has (up to a unit factor) the form x − a where $a \in \mathcal{F}$. Moreover, every monic polynomial $f \in \mathcal{F}[x]$ can be factored into the form

$$f = \prod_{i=1}^{n} (x - a_i)$$

where each $a_i \in \mathcal{F}$.

Proof Let $p \in \mathcal{F}[x]$ be prime. Since $\mathcal{F}$ is algebraically closed, there exists $a \in \mathcal{F}$ such that p(a) = 0. By the factor theorem, x − a must be a factor of p. But p is prime so its only factors are its associates and units. This proves the first part of the theorem.

Now let $f \in \mathcal{F}[x]$ be of degree n ≥ 1. The second part of the theorem is essentially obvious from the first part and Theorem 6.6. However, we may proceed as follows. Since $\mathcal{F}$ is algebraically closed there exists $a_1 \in \mathcal{F}$ such that $f(a_1) = 0$, and hence by the factor theorem,

$$f = (x - a_1)q_1$$

where $q_1 \in \mathcal{F}[x]$ and deg $q_1 = n - 1$ (Theorem 6.2(b)). Now, by the algebraic closure of $\mathcal{F}$ there exists $a_2 \in \mathcal{F}$ such that $q_1(a_2) = 0$, and therefore

$$q_1 = (x - a_2)q_2$$

where deg $q_2 = n - 2$. It is clear that we can continue this process a total of n times, finally arriving at

$$f = c(x - a_1)(x - a_2) \cdots (x - a_n)$$

where $c \in \mathcal{F}$ is a unit. In particular, c = 1 if q_{n-1} is monic. ∎

While Theorem 6.13 shows that any polynomial of degree n over an algebraically closed field has exactly n (not necessarily distinct) roots, a more general result is the following.

Theorem 6.14 Any polynomial $p \in \mathcal{F}[x]$ of degree $n \geq 1$ over $\mathcal{F}$ has at most n roots in $\mathcal{F}$.

Proof We proceed by induction on the degree n of p. If $n = 1$, then $p = a_0 + a_1x$ so that $-a_1/a_0$ is the unique root of p, and the theorem thus holds in this case. Now assume that $n > 1$ and that the theorem holds for all polynomials of degree less than n. If p has no roots, then the conclusion of the theorem is valid, so we assume that p has at least one root c. Then $(x - c)|p$ so that $p = (x - c)\,q$ for some $q \in \mathcal{F}[x]$ with $\deg q = n - 1$ (Theorem 6.2(b)). By our induction hypothesis, q has at most $n - 1$ roots in $\mathcal{F}$, so the proof will be finished if we can show that p has no roots in $\mathcal{F}$ other than c and the roots of q. Suppose that $b \in \mathcal{F}$ is such that $p(b) = (b - c)q(b) = 0$. Since the field $\mathcal{F}$ can have no zero divisors (Exercise 1.5.12), it must be true that either $b - c = 0$ or $q(b) = 0$. In other words, if $p(b) = 0$, then either $b = c$ or else b is a root of q. ∎

Corollary Every polynomial p of degree $n \geq 1$ over an algebraically closed field $\mathcal{F}$ has n roots in $\mathcal{F}$.

Proof While this was proved in Theorem 6.13, we repeat it here in a slightly different manner. As was done in the proof of Theorem 6.14, we proceed by induction on the degree of p. The case $n = 1$ is true as above, so we assume that $n > 1$. Since $\mathcal{F}$ is algebraically closed, there exists at least one root $c \in \mathcal{F}$ such that $p = (x - c)q$ where $\deg q = n - 1$. By our induction hypothesis, q has $n - 1$ roots in $\mathcal{F}$ which are also clearly roots of p. It therefore follows that p has at least $n - 1 + 1 = n$ roots in $\mathcal{F}$, while Theorem 6.14 shows that p has at most n roots in $\mathcal{F}$. Therefore p must have exactly n roots in $\mathcal{F}$. ∎

While we proved in Theorem 6.12 that the field $\mathbb{C}$ is algebraically closed, it is not true that $\mathbb{R}$ is algebraically closed. This should be obvious because any quadratic equation of the form $ax^2 + bx + c = 0$ has solutions given by the quadratic formula

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

and if $b^2 - 4ac < 0$, then there is no solution for x in the real number system. (Recall that the quadratic formula follows by writing

$$0 = x^2 + bx/a + c/a = (x + b/2a)^2 - b^2/4a^2 + c/a$$

and solving for x.) However, in the case of $\mathbb{R}[x]$, we do have the following result.

Theorem 6.15 Suppose $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{R}[x]$. If $\alpha \in \mathbb{C}$ is a root of f, then so is α^*. Furthermore, if $\alpha \neq \alpha^*$, then $(x - \alpha)(x - \alpha^*)$ is a factor of f.

Proof If $\alpha \in \mathbb{C}$ is a root of f, then $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Taking the complex conjugate of this equation and remembering that each $a_i \in \mathbb{R}$, we obtain $a_0 + a_1\alpha^* + \cdots + a_n\alpha^{*n} = 0$ so that α^* is also a root of f. The second part of the theorem now follows directly from the factor theorem. ∎

Corollary Every prime polynomial in $\mathbb{R}[x]$ is (up to a unit factor) either of the form $x - a$ or $x^2 + ax + b$ where $a, b \in \mathbb{R}$ and $a^2 - 4b < 0$.

Proof Let $f \in \mathbb{R}[x]$ be prime, and let $\alpha \in \mathbb{C}$ be a root of f (that α exists follows from Theorem 6.13). Then $x - \alpha$ is a factor of f so that if $\alpha \in \mathbb{R}$, then $f = c(x - \alpha)$ where $c \in \mathbb{R}$ (since f is prime). But if $\alpha \notin \mathbb{R}$, then $\alpha \in \mathbb{C}$ and $\alpha^* \neq \alpha$ so that by Theorem 6.15, f has the factor

$$(x - \alpha)(x - \alpha^*) = x^2 - (\alpha + \alpha^*)x + \alpha\alpha^* \ .$$

Writing $\alpha = u + iv$ we see that

$$-a = \alpha + \alpha^* = 2u \in \mathbb{R}$$

and

$$b = \alpha\alpha^* = u^2 + v^2 \in \mathbb{R}$$

so that f has the form (up to a unit factor) $x^2 + ax + b$. Finally, note that

$$a^2 - 4b = 4u^2 - 4(u^2 + v^2) = -4v^2 < 0 \ . \ ∎$$

Exercises

1. Suppose $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{C}[x]$ has zeros $\alpha_1, \ldots, \alpha_n$. Prove that $a_0 = \pm\alpha_1 \cdots \alpha_n$ and $a_{n-1} = -(\alpha_1 + \cdots + \alpha_n)$.

2. Let $V_n \subset \mathcal{F}[x]$ denote the set of all polynomials of degree $\leq n$, and let $a_0, a_1, \ldots, a_n \in \mathcal{F}$ be distinct.

(a) Show that V_n is a vector space over $\mathcal{F}$ with basis $\{1, x, x^2, \ldots, x^n\}$, and hence that dim $V_n = n + 1$.
(b) For each $i = 0, \ldots, n$, define the mapping $T_i: V_n \to \mathcal{F}$ by $T_i(f) = f(a_i)$. Show that the T_i are linear functionals on V_n, i.e., that $T_i \in V_n^*$.
(c) For each $k = 0, \ldots, n$ define the polynomial

$$p_k(x) = \frac{(x-a_0)\cdots(x-a_{k-1})(x-a_{k+1})\cdots(x-a_n)}{(a_k-a_0)\cdots(a_k-a_{k-1})(a_k-a_{k+1})\cdots(a_k-a_n)}$$
$$= \prod_{i\neq k}\left(\frac{x-a_i}{a_k-a_i}\right) \in V_n \quad .$$

Show that $T_i(p_j) = \delta_{ij}$.
(d) Show that $p_0, \ldots, p_n$ forms a basis for V_n, and hence that any $f \in V_n$ may be written as

$$f = \sum_{i=0}^{n} f(a_i)p_i \quad .$$

(e) Now let $b_0, b_1, \ldots, b_n \in \mathcal{F}$ be arbitrary, and define $f = \sum b_i p_i$. Show that $f(a_j) = b_j$ for $0 \leq j \leq n$. Thus there exists a polynomial of degree $\leq n$ that takes on given values at $n + 1$ distinct points.
(f) Now assume that $f, g \in \mathcal{F}[x]$ are of degree $\leq n$ and satisfy $f(a_j) = b_j = g(a_j)$ for $0 \leq j \leq n$. Prove that $f = g$, and hence that the polynomial defined in part (e) is unique. This is called the **Lagrange interpolation formula**.

3. Suppose $Q \subset M_2(\mathbb{C})$ is the set of all complex matrices of the form

$$\begin{pmatrix} z & w \\ -w^* & z^* \end{pmatrix} .$$

(a) Prove that Q is a division ring (i.e., that the nonzero elements of Q form a multiplicative group). Q is called the ring of **quaternions**.
(b) Prove that Q is not a field.
(c) Prove that $x^2 + 1 \in Q[x]$ has infinitely many roots in Q (where 1 denotes the unit element of Q, i.e., the 2 x 2 identity matrix).

4. Prove that $f, g \in \mathbb{C}[x]$ are relatively prime if and only if they have no root in common.

5. Let D be the differentiation operator defined in Problem 6.1.4, and suppose $f \in \mathbb{C}[x]$ is a monic polynomial. Prove that $f = (x - \alpha_1) \cdots (x - \alpha_n)$

where $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ are distinct if and only if f and Df are relatively prime.

6. If $f \in \mathcal{F}[x]$ has a root α, and $f = (x - \alpha)^m g$ where $g(\alpha) \neq 0$, then α is said to be a root of **multiplicity** m. In other words, m is the largest integer such that $(x - \alpha)^m | f$. Let α be a root of $f \in \mathcal{F}[x]$ and assume that $\deg f \geq 1$. Show that the multiplicity of f is > 1 if and only if $Df(\alpha) = 0$, and hence that the multiplicity of α is 1 if $Df(\alpha) \neq 0$. (See Problem 6.1.4 for the definition of Df.)

7. Show that the following polynomials have no multiple roots in $\mathbb{C}$ (see the previous problem for the definition of multiplicity):
   (a) $x^4 + x$.
   (b) $x^5 - 5x + 1$.
   (c) $x^2 + bx + c$ where $b, c \in \mathbb{C}$ and $b^2 - 4c \neq 0$.

6.5 THE FIELD OF QUOTIENTS

What we will do in this section is show how to construct a field out of the ring $\mathcal{F}[x]$. Rather than talk about polynomials specifically, we use the fact that $\mathcal{F}[x]$ is an integral domain and treat the problem on a more general footing.

Notice that the set $\mathbb{Z}$ of all integers has the property that if $ab = 0$ for some $a, b \in \mathbb{Z}$, then either a or b must equal 0. Since $\mathbb{Z}$ is a ring, this shows that $\mathbb{Z}$ is in fact an integral domain. Also note though, for any $a \in \mathbb{Z}$, $a \neq 1$, we have $a^{-1} = 1/a \notin \mathbb{Z}$, so that $\mathbb{Z}$ is not a field. However, if we enlarge the set $\mathbb{Z}$ to include all of the rational numbers, then we do indeed obtain a field. What this really entails is taking all pairs $a, b \in \mathbb{Z}$ and forming the object a/b with the appropriate algebraic operations defined on it. In this particular case, we say that $a/b = c/d$ if and only if $ad = bc$, and we define the operations of addition and multiplication by

$$a/b + c/d = (ad + bc)/bd$$

and

$$(a/b)(c/d) = (ac)/(bd) \ .$$

In order to generalize this result, we make the following definition. Let D be an integral domain (i.e., a commutative ring with no zero divisors), let D' denote the set of all *nonzero* elements of D, and let Q be the set of all ordered pairs

$$Q = \{(a, b) \in D \times D'\} \ .$$

(You may think of (a, b) as the quotient a/b.) We define a relation ~ on Q by (a, b) ~ (c, d) if ad = bc, and we claim that this is an equivalence relation (for example, 2/3 is "equivalent" to 8/12). To prove this, we must verify the three requirements given in Section 0.3. First, for any (a, b) $\in Q$ we have (a, b) ~ (a, b) since ab = ba. Next, for any (a, b), (c, d) $\in Q$ we see that (a, b) ~ (c, d) implies ad = bc, and hence cb = da which thus implies (c, d) ~ (a, b). Finally, suppose (a, b), (c, d), (e, f) $\in Q$ where (a, b) ~ (c, d) and (c, d) ~ (e, f). Then ad = bc and cf = de, and therefore bde = bcf = adf. But D is commutative, and hence this is just afd = bed. By assumption $d \neq 0$ so that, since D is an integral domain, we must have af = be and thus (a, b) ~ (e, f).

We are now in a position to show that any integral domain can be enlarged in a similar manner to form a field. By way of terminology, if there is a one-to-one homomorphism (i.e., an isomorphism) of a ring R into a ring R′, then we say that R can be **embedded** in R′. Furthermore, if R and R′ are both rings with unit elements 1 and 1′ respectively, then we require that the embedding take 1 into 1′. The ring R′ is also called an **extension** of R.

The proof of the next theorem appears to be quite involved, but it is actually nothing more than a long series of simple steps.

Theorem 6.16 Every integral domain D can be embedded in a field.

Proof Let D′ be the nonzero elements of D, and let Q be the set of all ordered pairs (a, b) $\in$ D × D′ as defined above. We let [a, b] denote the equivalence class in Q of (a, b) as constructed above. In other words,

$$[a, b] = \{(x, y) \in D \times D' : (a, b) \sim (x, y)\} .$$

We claim that the set $\mathcal{F}_D$ of all such equivalence classes forms a field. To prove this, we must first define addition and multiplication in $\mathcal{F}_D$.

Guided by the properties of $\mathbb{Z}$, we define addition in $\mathcal{F}_D$ by the rule

$$[a, b] + [c, d] = [ad + bc, bd] .$$

Since D is an integral domain, we know that $bd \neq 0$ for any nonzero b, d $\in$ D, and hence [ad + bc, bd] $\in \mathcal{F}_D$. We still must show that this addition is well-defined, i.e., if [a, b] = [a′, b′] and [c, d] = [c′, d′], then

$$[a, b] + [c, d] = [a', b'] + [c', d'] .$$

This is equivalent to showing that

$$[ad + bc, bd] = [a'd' + b'c', b'd']$$

or, alternatively, that

$$(ad + bc)b'd' = bd(a'd' + b'c') \ .$$

From $[a, b] = [a', b']$ we have $ab' = ba'$, and similarly $cd' = dc'$. Therefore we indeed have

$$\begin{aligned}(ad + bc)b'd' &= adb'd' + bcb'd' = ab'dd' + bb'cd' = ba'dd' + bb'dc' \\ &= bda'd' + bdb'c' = bd(a'd' + b'c') \ .\end{aligned}$$

Since D is commutative, it should be clear that if $c \neq 0$ then

$$[a, b] = [ac, bc] = [ca, cb] \ .$$

Therefore

$$[a, b] + [0, c] = [ac + b0, bc] = [ac, bc] = [a, b]$$

so that $[0, c]$ is a zero element for addition. We now see that

$$[a, b] + [-a, b] = [ab - ba, bb] = [0, b]$$

and hence $[-a, b]$ is the negative of $[a, b]$. The reader should now have no trouble showing that $\mathcal{F}_D$ is an abelian group under addition.

To complete our ring structure, we define multiplication in $\mathcal{F}_D$ by the rule

$$[a, b][c, d] = [ac, bd] \ .$$

As was the case with addition, the fact that $b, d \neq 0$ means that $bd \neq 0$, and hence the product is an element of $\mathcal{F}_D$. We leave it to the reader to show that the product is well-defined (see Exercise 6.5.1). It is also easy to see that $[x, x]$ is a unit element in $\mathcal{F}_D$ for any nonzero $x \in D$, and that the nonzero elements of $\mathcal{F}_D$ (i.e., those of the form $[a, b]$ with $a \neq 0$) form an abelian group under multiplication with the inverse of an element $[a, b]$ given by $[a, b]^{-1} = [b, a]$ (where $[b, a] \in \mathcal{F}_D$ since $a \neq 0$).

As to the ring axioms, we show only one of the distributive laws, and leave the others to the reader. This will complete the proof that $\mathcal{F}_D$ forms a field. If $[a, b], [c, d], [e, f] \in \mathcal{F}_D$, then

$$[a, b]([c, d]+[e, f]) = [a, b][cf + de, df] = [acf + ade, bdf]$$
$$= [b(acf + ade), bbdf] = [(ac)(bf) + (bd)(ae), (bd)(bf)]$$
$$= [ac, bd] + [ae, bf] = [a, b][c, d] + [a, b][e, f]$$

What we have accomplished up to this point is the construction of a field $\mathcal{F}_D$ from an arbitrary integral domain D. It still must be shown that D can be embedded in $\mathcal{F}_D$. As was noted above, for any nonzero x, y $\in$ D we have [ax, x] = [ay, y] because (ax)y = x(ay). This means that we can denote the element [ax, x] $\in \mathcal{F}_D$ by [a, 1]. (It is important to realize that the ring D does not necessarily contain a unit element, so that there need not exist a unit element $1 \in D$. What we have just done is *define* the element [a, 1] $\in \mathcal{F}_D$. Everything that follows in the remainder of this proof holds if we replace the symbol 1 by an arbitrary nonzero element $x \in D$.)

We now define the mapping ϕ: D $\to \mathcal{F}_D$ by $\phi(a) = [a, 1]$ for all $a \in D$. If $\phi(a) = \phi(a')$, then [a, 1] = [a′, 1] so that a1 = 1a′ and hence a = a′, thus proving that ϕ is one-to-one. (As we just mentioned, the symbol 1 could actually be replaced by any $x \neq 0$ since the fact that D is an integral domain then says that if ax = xa′, then x(a − a′) = 0 which also implies that a = a′.) To finish the proof, we need only show that ϕ is a homomorphism. But for any a, b $\in$ D we have

$$\phi(a + b) = [a + b, 1] = [a1 + b1, 1\cdot 1] = [a, 1] + [b, 1] = \phi(a) + \phi(b)$$

and

$$\phi(ab) = [ab, 1] = [ab, 1\cdot 1] = [a, 1][b, 1] = \phi(a)\phi(b) \ . \ \blacksquare$$

The field $\mathcal{F}_D$ constructed in this theorem is usually called the **field of quotients** of D. If we start with the ring of integers $\mathbb{Z}$, then this construction yields the rational field $\mathbb{Q}$. While we have shown that any integral domain D can be embedded in its field of quotients, there can be other fields in which D can also be embedded. However, it can be shown that $\mathcal{F}_D$ is the "smallest" field in which D can be embedded (see Exercise 6.5.2).

Exercises

1. Referring to the proof of Theorem 6.16, show that the product in $\mathcal{F}_D$ is well-defined.

2. Show that $\mathcal{F}_D$ is the smallest field in which an integral domain D can be embedded. In other words, show that if $\mathcal{K}$ is any field containing an integral domain isomorphic to D, then $\mathcal{K}$ contains a field isomorphic to $\mathcal{F}_D$.

[*Hint*: For simplicity, assume that D is actually a subring of $\mathcal{K}$. Now, for any a, b ∈ D show that the map $\phi: \mathcal{F}_D \to \mathcal{K}$ defined by $\phi([a, b]) = ab^{-1}$ is one-to-one and preserves addition and multiplication. Thus ϕ is an isomorphism of $\mathcal{F}_D$ onto a subfield of $\mathcal{K}$.]

3. Show that $\mathcal{F}_D$ obeys all of the axioms for a ring.

6.6 POLYNOMIALS OVER FINITE FIELDS *

With very few exceptions (e.g., Exercise 1.5.15), the fields we have been using (such as $\mathbb{R}$ and $\mathbb{C}$) contain an infinite number of elements. However, it is also possible to construct many fields that contain only a finite number of elements. This section is meant to be only an introduction to the theory of finite fields.

Recall from Example 1.11 that two integers a, b ∈ $\mathbb{Z}$ are said to be **congruent modulo n** (where $n \in \mathbb{Z}^+$) if $n|(a - b)$, and we write this as

$$a \equiv b \pmod{n} \ .$$

We also saw in Exercise 1.5.2 that for each $n \in \mathbb{Z}^+$, this defines an equivalence relation on $\mathbb{Z}$ that decomposes $\mathbb{Z}$ into n distinct congruence classes. We shall denote the congruence class (for a fixed n) of an integer $k \in \mathbb{Z}$ by [k]. If there is any possible ambiguity as to the value of n under discussion, we will write $[k]_n$. For example, if n = 5 we have

$$[2] = [7] = [-33] = \{\ldots, -8, -3, 2, 7, 12, \ldots\} \ .$$

We also refer to any of the integers in [k] as a representative of [k]. For example, 2 is the smallest positive representative of the class [7] (or the class [−33] etc.). We emphasize that [k] is a *subset* of $\mathbb{Z}$ for each k.

From Example 1.11, we say that the collection

$$\{[0], [1], [2], \ldots, [n - 1]\}$$

forms a **complete set** of congruence classes modulo n, and we denote this collection by $\mathbb{Z}_n$. We first show that $\mathbb{Z}_n$ can be made into an abelian group. For any [a], [b] ∈ $\mathbb{Z}_n$ we define a group "addition" operation $[a] \oplus [b] \in \mathbb{Z}_n$ by

$$[a] \oplus [b] = [a + b] \ .$$

(Note that the symbol $\oplus$ is used in an entirely different context when we talk about direct sums.) It should be obvious that [0] will serve as the additive identity element since [a] $\oplus$ [0] = [a + 0] = [a] and [0] $\oplus$ [a] = [0 + a] = [a]. Noting that, for example with n = 5 again, we have [3] = [18] and [4] = [−1], we must be sure that [3] $\oplus$ [4] = [18] $\oplus$ [−1]. Clearly this is true because [3] $\oplus$ [4] = [7] = [2] and [18] $\oplus$ [−1] = [17] = [2]. In other words, we must be sure that this addition operation is well-defined. That this is in fact the case is included in the next theorem.

Theorem 6.17 The set $\mathbb{Z}_n$ is an abelian group with respect to the operation $\oplus$ defined above.

Proof We leave it to the reader to show that $\oplus$ is indeed well-defined (see Exercise 6.6.1). As to the group properties, we prove associativity, leaving the rest of the proof to the reader (see Exercise 6.6.2). We have

$$[a]\oplus([b]\oplus[c]) = [a]\oplus[b+c] = [a+(b+c)] = [(a+b)+c]$$
$$= [a+b]\oplus[c] = ([a]\oplus[b])\oplus[c] \ . \ \blacksquare$$

By virtue of this theorem, $\mathbb{Z}_n$ is called the **group of integers modulo n** (or simply mod n). We can also define another operation on $\mathbb{Z}_n$ that is analogous to multiplication. Thus, we define the "multiplication" operation $\otimes$ on $\mathbb{Z}_n$ by

$$[a] \otimes [b] = [ab] \ .$$

(Again, this symbol should not be confused with the tensor product to be introduced in Chapter 11.) For example, if n = 6 we have [2] $\otimes$ [5] = [10] = [4] and [3] $\otimes$ [−4] = [−12] = [0]. The closest analogue to Theorem 6.17 that we have for $\otimes$ is the following.

Theorem 6.18 The operation $\otimes$ defined above on $\mathbb{Z}_n$ is well-defined, obeys the associative and commutative laws, and has [1] as the identity element.

Proof See Exercise 6.6.3. $\blacksquare$

Since [1] is the identity element for $\otimes$, it is easy to see that [0] has no multiplicative inverse in $\mathbb{Z}_n$, and hence $\mathbb{Z}_n$ can not possibly form a group under $\otimes$. Let us denote the set $\mathbb{Z}_n - [0] = \{[1], [2], \ldots, [n-1]\}$ by $\mathbb{Z}_n{}^+$. It turns out that for some (but not all) values of n, $\mathbb{Z}_n{}^+$ will in fact form a group with respect to $\otimes$. We will leave specific examples of this to the exercises at the end of this section.

With the operations $\oplus$ and $\otimes$ defined, it is now easy to see that $\mathbb{Z}_n$ actually forms a commutative ring. All we must do is verify the axioms given in Section 1.4. We will show that the first half of axiom (R8) is obeyed, and leave it to the reader to verify the rest of the ring axioms (see Exercise 6.6.4). We therefore have

$$\begin{aligned}[a]\otimes([b]\oplus[c]) &= [a]\otimes[b+c] = [a(b+c)] = [ab+ac] \\ &= [ab]\oplus[ac] = ([a]\otimes[b])\oplus([a]\otimes[c]) \ .\end{aligned}$$

Now consider the ring $\mathbb{Z}_n$ and assume that n is not prime. Then we may write n = rs where r, s > 1. But then [r] $\otimes$ [s] = [rs] = [n] = [0] where [r], [s] $\neq$ [0]. Since [0] is the zero element of $\mathbb{Z}_n$, this shows that $\mathbb{Z}_n$ is not an integral domain if n is not prime. On the other hand, suppose that n = p is prime. We claim that $\mathbb{Z}_p$ is an integral domain. For, suppose [a] $\in \mathbb{Z}_p$ and [a] $\neq$ [0]. We may assume that a is the smallest positive representative of the equivalence class [a], and hence a < p. Now assume that [b] $\in \mathbb{Z}_p$ is such that [a] $\otimes$ [b] = [ab] = [0] (where we again choose b < p to be the smallest positive representative of the class [b]). Then by definition we have p|ab. But p is prime so (by Theorem 0.9) this implies that either p|a or p|b. Since a < p, it is impossible for p to divide a, and therefore p|b. Since $0 \leq b < p$, we must have b = 0, and thus $\mathbb{Z}_p$ is an integral domain. This proves the next result.

Theorem 6.19 The ring $\mathbb{Z}_n$ is an integral domain if and only if n is prime.

Noting that $\mathbb{Z}_n$ consists of n equivalence classes, we now claim that $\mathbb{Z}_n$ is in fact a field if n is prime. This is an immediate consequence of the following general result. Recall that a field is a commutative ring with identity element in which the nonzero elements form a multiplicative group (i.e., a commutative division ring). Furthermore, any field is necessarily an integral domain (see Exercise 1.5.6 or 1.5.12).

Theorem 6.20 Every finite integral domain is a field.

Proof Let D be a finite integral domain (which is commutative by definition). We must show that $1 \in D$, and that every nonzero $a \in D$ has a multiplicative inverse that is also in D. In other words, we must show that for every nonzero $a \in D$ there exists $b \in D$ such that $ab = 1 \in D$. Let $\{x_1, \ldots, x_n\}$ denote all the elements of D, and consider the set $\{ax_1, \ldots, ax_n\}$ where $a \in D$ and $a \neq 0$. If $ax_i = ax_j$ for $i \neq j$, then $a(x_i - x_j) = 0$ which (since D has no zero divisors) implies that $x_i = x_j$, contradicting the assumption that $i \neq j$. Thus

$ax_1, \ldots, ax_n$ are all distinct. Since D contains n elements, it follows that in fact we have $D = \{ax_1, \ldots, ax_n\}$. In other words, every $y \in D$ can be written in the form $ax_i = x_i a$ for some $i = 1, \ldots, n$. In particular, we must have $a = ax_{i_0}$ for some $i_0 = 1, \ldots, n$. Then for any $y = x_i a \in D$ we have

$$yx_{i_0} = (x_i a)x_{i_0} = x_i(ax_{i_0}) = x_i a = y$$

so that x_{i_0} may be taken as the identity element 1 in D. Finally, since we have now shown that $1 \in D$, it follows that $1 = ax_j$ for some particular $j = 1, \ldots, n$. Defining $b = x_j$ yields $1 = ab$ and completes the proof. ∎

Corollary $\mathbb{Z}_n$ is a field if and only if n is prime.

We now turn our attention to the question of whether there exist any finite fields that do not contain a prime number of elements. As with groups, we refer to the number of elements in a finite field as its **order**. This is not surprising since any field is a ring, and any ring is an additive group. We will frequently denote a finite field by F rather than by $\mathcal{F}$.

Example 6.10 Let $S_2(\mathcal{F}) \subset M_2(\mathcal{F})$ denote the set of all matrices of the form

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}.$$

We will show that $S_2(\mathcal{F})$ is a field when $\mathcal{F} = \mathbb{Z}_3$ but not when $\mathcal{F} = \mathbb{Z}_5$.

We leave it as a simple exercise for the reader to show that if $A, B \in S_2(\mathcal{F})$, then $A + B$ and AB are also in $S_2(\mathcal{F})$. Furthermore, $AB = BA$ so that $S_2(\mathcal{F})$ is commutative. Note that $S_2(\mathcal{F})$ also contains the zero and identity matrices, and if $A \in S_2(\mathcal{F})$, then so is $-A$. Thus $S_2(\mathcal{F})$ is easily seen to be a subring of $M_2(\mathcal{F})$. We now consider the problem of inverses. If

$$A = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

has inverse

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

then $AA^{-1} = I$ yields the two simultaneous equations

$$ax - by = 1$$
$$ay + bx = 0 \quad .$$

Since x, y, a, b $\in \mathcal{F}$ we can (formally) solve these for a and b to obtain

$$a = \ x(x^2 + y^2)^{-1}$$
$$b = -y(x^2 + y^2)^{-1} \quad .$$

The element $(x^2 + y^2)^{-1}$ will exist as long as $x^2 + y^2 \neq 0$.

In $\mathbb{Z}_3$ we have x, y = {0, 1, 2} and it is easy to see by direct calculation that $x^2 + y^2 \neq 0$ as long as (x, y) ≠ (0, 0). For example, if x = 1 and y = 2 we have $x^2 + y^2 = 1 + 1 = 2$. Thus every nonzero matrix in $S_2(\mathbb{Z}_3)$ is invertible, and hence $S_2(\mathbb{Z}_3)$ is a field with 9 elements.

On the other hand, in $\mathbb{Z}_5$ we see that $1^2 + 2^2 = 0$ so that the matrix with x = 1 and y = 2 is not invertible, and hence $S_2(\mathbb{Z}_5)$ is not a field. //

Example 6.11 Since $\mathbb{Z}_3$ is a field, we can consider polynomials in $\mathbb{Z}_3[x]$. These may be used to generate a field of order 9 as follows. We define the set $F_9 \subset \mathbb{Z}_3[x]$ consisting of the nine polynomials of degree ≤ 1 with coefficients in $\mathbb{Z}_3$:

$$F_9 \ = \ \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\} \quad .$$

It is easy to see that this set is closed under ordinary polynomial addition. For example, remembering that our scalars lie in $\mathbb{Z}_3$ we have (x + 1) + (2x + 1) = 2. However, we must be careful in defining multiplication. This is because, for example, $(x + 1)(2x + 1) = 2x^2 + 1 \notin F_9$ even though it is in $\mathbb{Z}_3[x]$. To ensure that multiplication is closed, we multiply as usual in $\mathbb{Z}_3[x]$ and then **reduce modulo** $x^2 + 1$. In other words, we subtract off multiples of $x^2 + 1$. For example, we have

$$\begin{aligned} (x+1)(2x+1) &= 2x^2 + 1 && (\text{in } \mathbb{Z}_3[x]) \\ &= 2(x^2+1) + 2 \\ &= 2 && (\text{in } F_9) \quad . \end{aligned}$$

As another example,

$$\begin{aligned} (2x+1)(x) &= 2x^2 + x && (\text{in } \mathbb{Z}_3[x]) \\ &= 2(x^2+1) + (x+1) \\ &= x + 1 && (\text{in } F_9) \quad . \end{aligned}$$

Using the constant polynomials 0 and 1 as the 0 and 1 elements of a ring, it is easy to show that F_9 forms a commutative ring. That F_9 in fact is a field follows from the observation that each nonzero element of F_9 has the inverse shown below:

Element:	1	2	x	x+1	x+2	2x	2x+1	2x+2
Inverse:	1	2	2x	x+2	x+1	x	2x+2	2x+1

We leave verification of these facts to the reader. //

Let G be any group, and let e be the identity element of G. If there exists an element $x \in G$ such that every element in G is a power of x, then G is said to be a **cyclic** group **generated** by x. The cyclic group generated by x is usually denoted by $\langle x \rangle$. If we consider the set of all powers of the generator x, then this set will consist of either all distinct elements, or else some elements will be repeated. In the case of repeated elements, there will exist a positive integer $m > 0$ such that $x^m = e$ while no smaller nonzero power of x is also equal to e. For example, if $i \leq j$ and $x^i = x^j$, we have $e = x^j(x^i)^{-1} = x^j\, x^{-i} = x^{j-i}$. Then let m be the smallest nonzero value of all such differences $j - i$.

We say that $G = \{e, x, x^2, \ldots, x^{m-1}\}$ is a cyclic group of **order** m, and we denote this group by C_m. We are using the letter e to denote the identity element of a general group so that we may distinguish between the multiplicative identity (usually written as 1) of some groups and the additive identity (usually written as 0) of other groups. Note that given any $k \in \mathbb{Z}$ we may write $k = qm + r$ (where $0 \leq r < m$), and hence

$$x^k = (x^m)^q\, x^r = e^q\, x^r = x^r \ .$$

Thus all powers of x can indeed be written in terms of the first m powers of x.

In the case that *all* powers of x are distinct, then the group

$$G = \{ \ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots \}$$

contains an infinite number of elements. We denote such an infinite cyclic group by C_∞. Of importance to us is the fact that many apparently diverse groups are isomorphic to cyclic groups (either finite or infinite). We will see a simple example of this below.

If $x \in G$ and $m > 0$ is the smallest integer such that $x^m = 1$, then m is called the **order** of x, and will also be denoted by o(x). (This should not be confused with the order of G which is the number of elements in G. It is for this reason that o(G) is frequently denoted by |G|.) If $o(x) \leq o(G)$, then it is

easy to see that $\langle x \rangle$ is simply a subgroup of G, and furthermore that $o(x) = o(\langle x \rangle)$ (see Exercise 6.6.9).

Example 6.12 Let us show that the set of integers $\mathbb{Z}$ under addition is isomorphic to $C_\infty = \langle x \rangle$. We define the mapping $\phi: \mathbb{Z} \to C_\infty$ by $\phi(n) = x^n$. Clearly ϕ is a homomorphism of groups since

$$\phi(n + m) = x^{n+m} = x^n x^m = \phi(n)\phi(m) \ .$$

(Note that $n + m$ in $\phi(n + m)$ denotes the "product" of two group elements in $\mathbb{Z}$ while $\phi(n)\phi(m)$ denotes the product of two elements in C_∞.) It should also be obvious that ϕ is surjective because every $x^k \in C_\infty$ is just the image of $k \in \mathbb{Z}$. Finally, ϕ is injective since $\text{Ker } \phi = \{0\}$. We have thus constructed an isomorphism of $\mathbb{Z}$ onto C_∞.

We leave it to the reader to show that $\mathbb{Z}_m$ is isomorphic to C_m (see Exercise 6.6.7). //

Let $\mathcal{F}$ be any field. Since $\mathcal{F}$ is closed under addition and contains the multiplicative identity element 1, we see that for any $n \in \mathbb{Z}^+$, the sum $1 + \cdots + 1$ of n 1's is also in $\mathcal{F}$. For example, $2 = 1 + 1 \in \mathcal{F}$ as is $3 = 1 + 1 + 1$ and so on. (However, it is important to stress that in an arbitrary field these elements need not be distinct.) Therefore the positive integers form a (not necessarily infinite) cyclic subgroup $\langle 1 \rangle$ of the *additive* group of $\mathcal{F}$. In other words

$$\langle 1 \rangle = \{0, 1, 2, \ldots\}$$

where each $n \in \langle 1 \rangle$ denotes $1 + \cdots + 1$ (n times) in $\mathcal{F}$.

Now consider the special case where F is a finite field. Note that since $\langle 1 \rangle$ is a subgroup of F, Theorem 1.9 tells us that $o(\langle 1 \rangle) | o(F)$. The number $o(\langle 1 \rangle)$ is called the **characteristic** of F (see Section 1.5). For example, if $F = \mathbb{Z}_p$, then $\langle 1 \rangle = \{0, 1, 2, \ldots, p - 1\} = \mathbb{Z}_p$ and hence the characteristic of $\mathbb{Z}_p$ is $o(\langle 1 \rangle) = p = o(F)$. The characteristic of an infinite field may or may not be finite.

Example 6.13 Let us show that the characteristic of any finite field must be a prime number (if it is nonzero). By definition, the characteristic of F is the smallest $m \in \mathbb{Z}^+$ such that $m \cdot 1 = 1 + \cdots + 1 = 0$. If $m \neq 0$ is not prime, then we may write $m = rs$ for some integers $0 < r < m$ and $0 < s < m$. But then we have $rs = 0$ which implies (since we are in a field) that either $r = 0$ or $s = 0$. In either case this contradicts the definition of m as the least positive integer such that $m = 0$. Thus m must be prime. Note that this proof actually applies to any finite integral domain with an identity element. //

We now wish to prove that if a finite field exists, then its order must be a prime power. For example, we have seen that $\mathbb{Z}_n$ is a field if and only if n is prime, and the field F_9 discussed above is of order $9 = 3^2$. Our claim will follow as an immediate corollary of the next theorem. The reader should recall that the direct product of two groups was defined in Exercise 1.1.5. The direct product of a finite number of groups follows by an obvious induction argument.

Example 6.14 Consider the cyclic groups $C_2 = \langle x \rangle = \{1, x\}$ and $C_3 = \langle y \rangle = \{1, y, y^2\}$. Then the product $C_2 \times C_3$ consists of the six elements

$$C_2 \times C_3 = \{(1, 1), (1, y), (1, y^2), (x, 1), (x, y), (x, y^2)\} .$$

To show that this product group is isomorphic to C_6, let $z = (x, y) \in C_2 \times C_3$. Then by definition of the group product in $C_2 \times C_3$ we have $z^2 = (1, y^2)$, $z^3 = (x, 1)$, $z^4 = (1, y)$, $z^5 = (x, y^2)$, $z^6 = (1, 1)$. Therefore $C_2 \times C_3 = \{z, z^2, \ldots, z^6\}$ which is just a cyclic group of order 6. ∥

Theorem 6.21 If F is a finite field of characteristic p, then for some $r \geq 1$, the additive group of F is isomorphic to the r-fold direct product $(C_p)^r$. Thus $o(F) = p^r$.

Proof We leave it to the reader to show that $\mathbb{Z}_p$ is isomorphic to a subfield of F, and hence that F may be considered to be a vector space V over the field $\mathbb{Z}_p$. Since F is finite, $r = \dim V$ must also be finite. By the corollary to Theorem 2.8, V is isomorphic to $(\mathbb{Z}_p)^r = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$. Noting that $\mathbb{Z}_p = \{0, 1, \ldots, p - 1\} = \langle 1 \rangle$ is isomorphic to the (additive) cyclic group C_p, it follows that V is isomorphic to $(C_p)^r$ (i.e., the set of all r-tuples of field elements). Thus V has p^r elements. ∎

Corollary The order of a finite field must be a prime power.

Proof This follows from Example 6.13 and Theorem 6.21. ∎

We now comment briefly on the construction of finite fields. What we shall do is generalize the procedure demonstrated in Example 6.11 where we constructed the field F_9. Recall that the problem came in defining a closed multiplication in $\mathbb{Z}_3[x]$. A more general way to view the solution to this problem is to define an equivalence relation $\approx$ on $\mathbb{Z}_3[x]$ by the requirement that $a \approx b$ if $(x^2 + 1) | (a - b)$. Note that $x^2 + 1$ is prime in $\mathbb{Z}_3[x]$. We may now

take the elements of F_9 to be the equivalence classes of the nine polynomials that were previously used in Example 6.11 to define F_9. Another way to say this is that these nine polynomials of degree ≤ 1 form a complete set of representatives of the classes. In this case, addition and multiplication are defined as expected by

$$[a] + [b] = [a + b]$$

and

$$[a][b] = [ab] .$$

Note that if $(x^2 + 1)|(a - b)$, then the remainder of a divided by $x^2 + 1$ must be the same as the remainder of b divided by $x^2 + 1$. Since there are only a finite number of polynomials in $\mathbb{Z}_3[x]$, there can be only a finite number of distinct remainders, and the degree of each remainder must be less than that of $x^2 + 1$. Referring to Theorem 6.7 and its proof, a moments thought should convince you that all we are doing is considering the cosets $\mathbb{Z}_3[x]/(x^2 + 1)$ where $(x^2 + 1)$ denotes the principal ideal generated by $k = x^2 + 1 \in \mathbb{Z}_3[x]$. This is because any $p \in \mathbb{Z}_3[x]/(k) = \mathbb{Z}_3[x]/I$ is of the form $I + h$ where $h \in \mathbb{Z}_3[x]$. But $h = qk + r$ for some $q \in \mathbb{Z}_3[x]$ and where deg $r <$ deg k, and hence $qk \in I$. Therefore p must actually be of the form $I + r$, and thus there can be only as many distinct such p as there are distinct r.

The next theorem shows that this approach works in general.

Theorem 6.22 Let $k \in \mathbb{Z}_p[x]$ be a prime polynomial of degree r, and define an equivalence relation on $\mathbb{Z}_p[x]$ by $a \approx b$ if and only if $k|(a - b)$. Then the corresponding set of equivalence classes in $\mathbb{Z}_p[x]$ is a field of order p^r.

Proof First note that if $a_i \in \mathbb{Z}_p[x]$, then there are p^r distinct polynomials of the form $a_0 + a_1x + \cdots + a_{r-1}x^{r-1}$. This set of p^r polynomials (which consists of all distinct polynomials of degrees $0, 1, 2, \ldots, r - 1$) forms a complete set of representatives of the classes, and hence there are p^r classes in all. Since these equivalence classes are just the cosets $\mathbb{Z}_p[x]/(k)$ where k is prime, it follows from Theorem 6.11 that $\mathbb{Z}_p[x]/(k)$ is a field. ∎

One consequence of this theorem is that to construct a field of order p^r we need only find a prime polynomial of degree r in $\mathbb{Z}_p[x]$. While this is easy enough to do in most common cases, it is fairly hard to prove that there exists at least one prime polynomial for every choice of p and r. We refer the interested reader to e.g., the very readable book by Biggs (1985).

Exercises

1. Show that the operation $\oplus$ defined on $\mathbb{Z}_n$ is well-defined. In other words, show that if $[a_1] = [a_2]$ and $[b_1] = [b_2]$ then $[a_1 + b_1] = [a_2 + b_2]$.

2. Finish the proof that $\mathbb{Z}_n$ forms an additive group.

3. Prove Theorem 6.18.

4. Finish the proof that $\mathbb{Z}_n$ forms a ring.

5. Finish the details in Example 6.10.

6. Finish the details in Example 6.11.

7. Prove that $\mathbb{Z}_m$ is isomorphic to C_m.

8. If m and n are relatively prime positive integers, prove that $C_m \times C_n$ is isomorphic to C_{mn}. [*Hint*: Suppose $C_m = \langle x \rangle$ and $C_n = \langle y \rangle$. Let $z = (x, y) \in C_m \times C_n$ have order r. Show that $r = mn$ and then conclude that $C_m \times C_n$ must be a cyclic group.]

9. Let G be a group, and suppose $\langle x \rangle \subset G$. If $o(x) \leq o(G)$, show that $\langle x \rangle$ is a subgroup of G and that $o(x) = o(\langle x \rangle)$.

10. Fill in the details in the proof of Theorem 6.22.

11. For each of the following expressions in $\mathbb{Z}_5$, write the answer as [0], [1], [2], [3] or [4]:
    (a) $[3] \oplus [4]$
    (b) $[2] \oplus [-7]$
    (c) $[17] \oplus [76]$
    (d) $[3] \otimes [4]$
    (e) $[2] \otimes [-7]$
    (f) $[17] \otimes [76]$
    (g) $[3] \otimes ([2] \oplus [4])$
    (h) $([3] \otimes [2]) \oplus ([3] \otimes [4])$

12. Repeat the previous problem in $\mathbb{Z}_6$.

13. (a) Which elements of $\mathbb{Z}_4$ are zero divisors?
    (b) Which elements of $\mathbb{Z}_{10}$ are zero divisors?

14. Show that ([2], [0]) is a zero divisor in $\mathbb{Z}_3 \times \mathbb{Z}_3$.

15. (a) Show that $1 + x + x^2 \in \mathbb{Z}_2[x]$ is prime over $\mathbb{Z}_2$.
    (b) Show that $1 + x^2 \in \mathbb{Z}_3[x]$ is prime over $\mathbb{Z}_3$.
    [*Hint*: Use the factor theorem.]

16. (a) Show that $1 + x^2 + x^3 \in \mathbb{Z}_2[x]$ is prime over $\mathbb{Z}_2$, and use this to construct a field of order 8.
    (b) What is the order of its multiplicative group?

17. Prove that for every prime number p there exist fields of order p^2 and p^3.

18. For which of the following primes p can we construct a field of order p^2 by using the polynomial $1 + x^2$?

$$p = 3, 5, 7, 11, 13, 19, 23 \ .$$

    Describe the multiplicative group for the first two cases in which the field can be constructed.

CHAPTER 7

Linear Transformations and Polynomials

We now turn our attention to the problem of finding the basis in which a given linear transformation has the simplest possible representation. Such a representation is frequently called a **canonical form**. Although we would almost always like to find a basis in which the matrix representation of an operator is diagonal, this is in general impossible to do. Basically, in this chapter as well as in Chapters 8 and 10, we will try and find the general conditions that determine exactly what form it is possible for a representation to take.

In the present chapter, we focus our attention on eigenvalues and eigenvectors, which is probably the most important characterization of a linear operator that is available to us. We also treat the triangular form theorem from two distinct viewpoints. Our reason for this is that in this chapter we discuss both quotient spaces and nilpotent transformations, and the triangular form theorem is a good application of these ideas. However, since we also treat this theorem from an entirely different (and much simpler) point of view in the next chapter, the reader should feel free to skip Sections 7.10 to 7.12 if desired. (We also point out that Section 7.9 on quotient spaces is completely independent of the rest of this chapter, and may in fact be read immediately after Chapter 2.)

In Chapter 8 we give a complete discussion of canonical forms of matrices under similarity. All of the results that we prove in the present chapter for canonical forms of operators also follow from the development in Chapter 8. The reason for treating the "operator point of view" as well as the "matrix

point of view" is that the proof techniques and way of thinking can be quite different. The matrix point of view leads to more constructive and insightful proofs, while the operator point of view leads to techniques that are more likely to extend to infinite-dimensional analogs (although there is no complete extension to the infinite-dimensional version).

7.1 MINIMAL POLYNOMIALS

Let $f = a_0 + a_1x + \cdots + a_nx^n \in \mathcal{F}[x]$ be any polynomial in the indeterminate x. Then, given any linear operator $T \in L(V)$, we define the linear operator $f(T) \in L(V)$ as the polynomial in the operator T defined by substitution as

$$f(T) = a_0 1 + a_1 T + \cdots + a_n T^n$$

where 1 is the identity transformation on V. Similarly, given any matrix $A \in M_m(\mathcal{F})$, we define the matrix polynomial f(A) by

$$f(A) = a_0 I + a_1 A + \cdots + a_n A^n$$

where now I is the m x m identity matrix. If T is such that $f(T) = 0$, then we say that T is a **root** or **zero** of the polynomial f. This terminology also applies to a matrix A such that $f(A) = 0$.

If $A \in M_m(\mathcal{F})$ is the representation of $T \in L(V)$ relative to some (ordered) basis for V, then (in view of Theorem 5.13) we expect that f(A) is the representation of f(T). This is indeed the case.

Theorem 7.1 Let A be the matrix representation of an operator $T \in L(V)$. Then f(A) is the representation of f(T) for any polynomial $f \in \mathcal{F}[x]$.

Proof This is Exercise 7.1.1. ∎

The basic algebraic properties of polynomials in either operators or matrices are given by the following theorem.

Theorem 7.2 Suppose $T \in L(V)$ and let $f, g \in \mathcal{F}[x]$. Then

(a) $f(T)T = Tf(T)$.
(b) $(f \pm g)(T) = f(T) \pm g(T)$.
(c) $(fg)(T) = f(T)g(T)$.
(d) $(cf)(T) = cf(T)$ for any $c \in \mathcal{F}$.

Furthermore, these same results also hold for any matrix representation $A \in M_n(\mathcal{F})$.

Proof In view of Theorem 6.1, we leave this as an easy exercise for the reader (see Exercise 7.1.2). ∎

From this theorem and the fact that the ring of polynomials is commutative, it should be clear that any two polynomials in the operator T (or matrix A) also commute.

This discussion is easily generalized as follows. Let $\mathcal{A}$ be any algebra over $\mathcal{F}$ with unit element e, and let $f = a_0 + a_1x + \cdots + a_nx^n$ be any polynomial in $\mathcal{F}[x]$. Then for any $\alpha \in \mathcal{A}$ we define

$$f(\alpha) = a_0e + a_1\alpha + \cdots + a_n\alpha^n \in \mathcal{A} \ .$$

If $f(\alpha) = 0$, then α is a root of f and we say that α **satisfies** f. We now show that in fact every $\alpha \in \mathcal{A}$ satisfies some nontrivial polynomial in $\mathcal{F}[x]$. Recall that by definition, an algebra $\mathcal{A}$ is automatically a vector space over $\mathcal{F}$.

Theorem 7.3 Let $\mathcal{A}$ be an algebra (with unit element e) of dimension m over $\mathcal{F}$. Then every element $\alpha \in \mathcal{A}$ satisfies some nontrivial polynomial in $\mathcal{F}[x]$ of degree at most m.

Proof Since $\dim \mathcal{A} = m$, it follows that for any $\alpha \in \mathcal{A}$, the $m + 1$ elements $e, \alpha, \alpha^2, \ldots, \alpha^m \in \mathcal{A}$ must be linearly dependent (Theorem 2.6). This means there exist scalars $a_0, a_1, \ldots, a_m \in \mathcal{F}$ not all equal to zero such that

$$a_0e + a_1\alpha + \cdots + a_m\alpha^m = 0 \ .$$

But then α satisfies the nontrivial polynomial

$$f = a_0 + a_1x + \cdots + a_mx^m \in \mathcal{F}[x]$$

which is of degree at most m. ∎

Corollary Let V be a finite-dimensional vector space over $\mathcal{F}$, and suppose $\dim V = n$. Then any $T \in L(V)$ satisfies some nontrivial polynomial $g \in \mathcal{F}[x]$ of degree at most n^2.

Proof By Theorem 5.8, L(V) is an algebra over $\mathcal{F}$, and by Theorem 5.4 we have dim L(V) = dim L(V, V) = n^2. The corollary now follows by direct application of Theorem 7.3. ∎

While this corollary asserts that any $T \in L(V)$ always satisfies some polynomial $g \in \mathcal{F}[x]$ of degree at most n^2, we shall see a little later on that g can be chosen to have degree at most n (this is the famous Cayley-Hamilton theorem).

Now, for a given $T \in L(V)$, consider the set of all $f \in \mathcal{F}[x]$ with the property that f(T) = 0. This set is not empty by virtue of the previous corollary. Hence (by well-ordering) we may choose a polynomial $p \in \mathcal{F}[x]$ of least degree with the property that p(T) = 0. Such a polynomial is called a **minimal polynomial** for T over $\mathcal{F}$. (We will present an alternative definition in terms of ideals in Section 7.4.)

Theorem 7.4 Let V be finite-dimensional and suppose $T \in L(V)$. Then there exists a unique monic polynomial $m \in \mathcal{F}[x]$ such that m(T) = 0 and, in addition, if $q \in \mathcal{F}[x]$ is any other polynomial such that q(T) = 0, then m|q.

Proof The existence of a minimal polynomial $p \in \mathcal{F}[x]$ was shown in the previous paragraph, so all that remains is to prove the uniqueness of a particular (i.e., monic) minimal polynomial. Suppose

$$p = a_0 + a_1x + \cdots + a_nx^n$$

so that deg p = n. Multiplying p by a_n^{-1} we obtain a monic polynomial $m \in \mathcal{F}[x]$ with the property that m(T) = 0. If m' is another distinct monic polynomial of degree n with the property that $m'(T) = 0$, then $m - m'$ is a nonzero polynomial of degree less than n (since the leading terms cancel) that is satisfied by T, thus contradicting the definition of n. This proves the existence of a unique monic minimal polynomial.

Now let q be another polynomial satisfied by T. Applying the division algorithm we have q = mg + r where either r = 0 or deg r < deg m. Substituting T into this equation and using the fact that q(T) = 0 and m(T) = 0 we find that r(T) = 0. But if $r \neq 0$, then we would have a polynomial r with deg r < deg m such that r(T) = 0, contradicting the definition of m. We must therefore have r = 0 so that q = mg, and hence m|q. ∎

From now on, all minimal polynomials will be assumed to be monic unless otherwise noted. Furthermore, in Section 7.3 we will show (as a consequence of the Cayley-Hamilton theorem) the existence of a minimal polynomial for matrices. It then follows as a consequence of Theorem 7.1 that

any $T \in L(V)$ and its corresponding matrix representation A both have the same minimal polynomial (since $m(T) = 0$ if and only if $m(A) = 0$).

Recall that $T \in L(V)$ is invertible if there exists an element $T^{-1} \in L(V)$ such that $TT^{-1} = T^{-1}T = 1$ (where 1 is the identity element of $L(V)$). It is interesting to note that for any invertible $T \in L(V)$, its inverse T^{-1} is actually a polynomial in T. This fact is essentially shown in the proof of the next theorem.

Theorem 7.5 Let V be finite-dimensional over $\mathcal{F}$. Then $T \in L(V)$ is invertible if and only if the constant term in the minimal polynomial for T is not equal to zero.

Proof Let the minimal polynomial for T over $\mathcal{F}$ be

$$m = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n .$$

We first assume that $a_0 \neq 0$. Since m is the minimal polynomial for T, we have

$$m(T) = a_0 1 + a_1 T + \cdots + a_{n-1}T^{n-1} + T^n = 0$$

and hence multiplying by a_0^{-1} and using Theorem 7.2 yields

$$0 = 1 + a_0^{-1}T(a_1 1 + a_2 T + \cdots + a_{n-1}T^{n-2} + T^{n-1})$$

or

$$\begin{aligned} 1 &= T[-a_0^{-1}(a_1 1 + a_2 T + \cdots + a_{n-1}T^{n-2} + T^{n-1})] \\ &= [-a_0^{-1}(a_1 1 + a_2 T + \cdots + a_{n-1}T^{n-2} + T^{n-1})]T \quad . \end{aligned}$$

This shows that $T^{-1} = -a_0^{-1}(a_1 1 + a_2 T + \cdots + a_{n-1}T^{n-2} + T^{n-1})$, and hence T is invertible.

Now suppose T is invertible, but that $a_0 = 0$. Then we have

$$\begin{aligned} 0 &= a_1 T + a_2 T^2 + \cdots + a_{n-1}T^{n-1} + T^n \\ &= (a_1 1 + a_2 T + \cdots + a_{n-1}T^{n-2} + T^{n-1})T \quad . \end{aligned}$$

Multiplying from the right by T^{-1} yields

$$0 = a_1 1 + a_2 T + \cdots + a_{n-1}T^{n-2} + T^{n-1}$$

and hence T satisfies the polynomial $p = a_1 + a_2 x + \cdots + a_{n-1}x^{n-2} + x^{n-1} \in \mathcal{F}[x]$. But $\deg p = n - 1 < n$ which contradicts the definition of m as the minimal polynomial. Therefore we must have $a_0 \neq 0$. ∎

Corollary Let V be finite-dimensional over $\mathcal{F}$, and assume that $T \in L(V)$ is invertible. Then T^{-1} is a polynomial in T over $\mathcal{F}$.

Proof If T is invertible, then $m(T) = a_0 1 + a_1 T + \cdots + a_{n-1}T^{n-1} + T^n = 0$ with $a_0 \neq 0$. Multiplying by a_0^{-1} then shows that

$$T^{-1} = -a_0^{-1}(a_1 1 + a_2 T + \cdots + a_{n-1}T^{n-2} + T^{n-1}) \ . \ \blacksquare$$

While we have so far shown the existence of minimal polynomials, most readers would be hard-pressed at this point to actually find one given any particular linear operator. Fortunately, we will discover a fairly general method for finding the minimal polynomial of a matrix in Chapter 8 (see Theorem 8.10).

As we stated earlier, V will always denote a finite-dimensional vector space over a field $\mathcal{F}$. In addition, we will let $1 \in L(V)$ denote the identity transformation on V (i.e., the unit element of L(V)), and we let $I \in M_n(\mathcal{F})$ be the identity matrix.

Exercises

1. Prove Theorem 7.1.

2. Prove Theorem 7.2.

3. Let V be finite-dimensional over $\mathcal{F}$, and suppose $T \in L(V)$ is singular. Prove there exists a nonzero $S \in L(V)$ such that $ST = TS = 0$.

4. Suppose V has a basis $\{e_1, e_2\}$. If $T \in L(V)$, then $Te_i = \sum_j e_j a_{ji}$ for some $(a_{ij}) \in M_2(\mathcal{F})$. Find a nonzero polynomial of degree 2 in $\mathcal{F}[x]$ satisfied by T.

5. Repeat the previous problem, but let dim V = 3 and find a polynomial of degree 3.

6. Let $\alpha \in \mathcal{F}$ be fixed, and define the linear transformation $T \in L(V)$ by $T(v) = \alpha v$. This is called the **scalar mapping** belonging to α. Show that T is the scalar mapping belonging to α if and only if the minimal polynomial for T is $m(x) = x - \alpha$.

7.2 EIGENVALUES AND EIGENVECTORS

We now make a very important definition. If $T \in L(V)$, then an element $\lambda \in \mathcal{F}$ is called an **eigenvalue** (also called a **characteristic value** or **characteristic root**) of T if there exists a nonzero vector $v \in V$ such that $T(v) = \lambda v$. In this case, we call the vector v an **eigenvector** (or **characteristic vector**) belonging to the eigenvalue λ. Note that while an eigenvector is nonzero by definition, an eigenvalue may very well be zero.

Throughout the remainder of this chapter we will frequently leave off the parentheses around vector operands. In other words, we sometimes write Tv rather than T(v). This simply serves to keep our notation as uncluttered as possible.

An important criterion for the existence of an eigenvalue of T is the following.

Theorem 7.6 A linear operator $T \in L(V)$ has eigenvalue $\lambda \in \mathcal{F}$ if and only if $\lambda 1 - T$ is singular.

Proof Suppose $\lambda 1 - T$ is singular. By definition, this means there exists a nonzero $v \in V$ such that $(\lambda 1 - T)v = 0$. But this is just $Tv = \lambda v$. The converse should be quite obvious. ∎

Note, in particular, that 0 is an eigenvalue of T if and only if T is singular. In an exactly analogous manner, we say that an element $\lambda \in \mathcal{F}$ is an **eigenvalue** of a matrix $A \in M_n(\mathcal{F})$ if there exists a nonzero (column) vector $v \in \mathcal{F}^n$ such that $Av = \lambda v$, and we call v an **eigenvector** of A belonging to the eigenvalue λ. Given a basis $\{e_i\}$ for $\mathcal{F}^n$, we can write this matrix eigenvalue equation in terms of components as

$$\sum_{j=1}^{n} a_{ij} v_j = \lambda v_i \ , \qquad i = 1, \ldots , n \ .$$

Now suppose $T \in L(V)$ and $v \in V$. If $\{e_1, \ldots , e_n\}$ is a basis for V, then $v = \sum_i v_i e_i$ and hence

$$T(v) = T(\textstyle\sum_i v_i e_i) = \sum_i v_i T(e_i) = \sum_{i,j} e_j a_{ji} v_i$$

where $A = (a_{ij})$ is the matrix representation of T relative to the basis $\{e_i\}$. Using this result, we see that if $T(v) = \lambda v$, then

$$\textstyle\sum_{i,j} e_j a_{ji} v_i = \lambda \sum_j v_j e_j$$

and hence equating components shows that $\sum_i a_{ji} v_i = \lambda v_j$. We thus see that (as expected) the isomorphism between L(V) and $M_n(\mathcal{F})$ (see Theorem 5.13) shows that λ is an eigenvalue of the linear transformation T if and only if λ is also an eigenvalue of the corresponding matrix representation A. Using the notation of Chapter 5, we can say that $T(v) = \lambda v$ if and only if $[T]_e[v]_e = \lambda[v]_e$.

Example 7.1 Let us find all of the eigenvectors and associated eigenvalues of the matrix

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

This means that we must find a vector $v = (x, y)$ such that $Av = \lambda v$. In matrix notation, this equation takes the form

$$\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix}$$

or

$$\begin{pmatrix} 1-\lambda & 2 \\ 3 & 2-\lambda \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 0 \quad .$$

This is equivalent to the system

$$\begin{aligned} (1-\lambda)x + 2y &= 0 \\ 3x + (2-\lambda)y &= 0 \end{aligned} \qquad (*)$$

Since this homogeneous system of equations has a nontrivial solution if and only if the determinant of the coefficient matrix is nonzero (Corollary to Theorem 4.13), we must have

$$\begin{vmatrix} 1-\lambda & 2 \\ 3 & 2-\lambda \end{vmatrix} = \lambda^2 - 3\lambda - 4 = (\lambda - 4)(\lambda + 1) = 0 \quad .$$

We thus see that the eigenvalues are $\lambda = 4$ and $\lambda = -1$. (The roots of this polynomial are found either by inspection, or by applying the quadratic formula proved following Theorem 6.14.)

Substituting $\lambda = 4$ into (*) yields

$$\begin{aligned} -3x + 2y &= 0 \\ 3x - 2y &= 0 \end{aligned}$$

or y = (3/2)x. This means that every eigenvector corresponding to the eigenvalue $\lambda = 4$ has the form v = (x, 3x/2). In other words, every multiple of the vector v = (2, 3) is also an eigenvector with eigenvalue equal to 4. If we substitute $\lambda = -1$ in (*), then we similarly find y = −x, and hence every multiple of the vector v = (1, −1) is an eigenvector with eigenvalue equal to −1. //

We will generalize this approach in the next section. However, let us first take a brief look at some of the relationships between the eigenvalues of an operator and the roots of its minimal polynomial.

Theorem 7.7 Let λ be an eigenvalue of $T \in L(V)$. Then $p(\lambda)$ is an eigenvalue of $p(T)$ for any $p \in \mathcal{F}[x]$.

Proof If λ is an eigenvalue of T, then there exists a nonzero $v \in V$ such that $Tv = \lambda v$. But then

$$T^2(v) = T(Tv) = T(\lambda v) = \lambda T(v) = \lambda^2 v$$

and by induction, it is clear that $T^k(v) = \lambda^k v$ for any k = 1, 2, ... If we define $p = a_0 + a_1 x + \cdots + a_m x^m$, then we have

$$p(T) = a_0 1 + a_1 T + \cdots + a_m T^m$$

and hence

$$\begin{aligned} p(T)v &= a_0 v + a_1 \lambda v + \cdots + a_m \lambda^m v \\ &= (a_0 + a_1 \lambda + \cdots + a_m \lambda^m)v \\ &= p(\lambda)v \quad . \ \blacksquare \end{aligned}$$

Corollary Let λ be an eigenvalue of $T \in L(V)$. Then λ is a root of the minimal polynomial for T.

Proof If m(x) is the minimal polynomial for T, then m(T) = 0 by definition. From Theorem 7.7, we have $m(\lambda)v = m(T)v = 0$ where $v \neq 0$ is an eigenvector corresponding to λ. But then $m(\lambda) = 0$ (see Theorem 2.1(b)) so that λ is a root of m(x). ∎

Since any eigenvalue of T is a root of the minimal polynomial for T, it is natural to ask about the number of eigenvalues that exist for a given $T \in L(V)$. Recall from the corollary to Theorem 6.4 that if $c \in \mathcal{F}$ is a root of $f \in \mathcal{F}[x]$, then $(x - c) | f$. If c is such that $(x - c)^m | f$ but no higher power of $x - c$ divides f, then we say that c is a root of **multiplicity** m. (The context should make it

clear whether we mean the multiplicity m or the minimal polynomial m(x).) In counting the number of roots that a polynomial has, we shall always count a root of multiplicity m as m roots. A root of multiplicity 1 is frequently called a **simple** root.

If dim V = n then, since the minimal polynomial m for $T \in L(V)$ is of degree at most n^2 (Corollary to Theorem 7.3), there can be at most n^2 roots of m (Theorem 6.14). In particular, we see that any $T \in L(V)$ has a finite number of distinct eigenvalues. Moreover, if the field over which V is defined is algebraically closed, then T will in fact have at least as many (not necessarily distinct) eigenvalues as is the degree of its minimal polynomial.

Theorem 7.8 If $v_1, \ldots, v_r$ are eigenvectors belonging to the distinct eigenvalues $\lambda_1, \ldots, \lambda_r$ of $T \in L(V)$, then the set $\{v_1, \ldots, v_r\}$ is linearly independent.

Proof If r = 1 there is nothing to prove, so we proceed by induction on r. In other words, we assume that the theorem is valid for sets of less than r eigenvectors and show that in fact it is valid for sets of size r. Suppose that

$$a_1 v_1 + \cdots + a_r v_r = 0 \tag{1}$$

for some set of scalars $a_i \in \mathcal{F}$. We apply T to this relation to obtain

$$a_1 T(v_1) + \cdots + a_r T(v_r) = a_1 \lambda_1 v_1 + \cdots + a_r \lambda_r v_r = 0 \ . \tag{2}$$

On the other hand, if we multiply (1) by λ_r and subtract this from (2), we find (since $Tv_i = \lambda_i v_i$)

$$a_1(\lambda_1 - \lambda_r)v_1 + \cdots + a_{r-1}(\lambda_{r-1} - \lambda_r)v_{r-1} = 0 \ .$$

By our induction hypothesis, the set $\{v_1, \ldots, v_{r-1}\}$ is linearly independent, and hence $a_i(\lambda_i - \lambda_r) = 0$ for each $i = 1, \ldots, r-1$. But the λ_i are distinct so that $\lambda_i - \lambda_r \neq 0$ for $i \neq r$, and therefore $a_i = 0$ for each $i = 1, \ldots, r-1$. Using this result in (1) shows that $a_r = 0$ (since $v_r \neq 0$ by definition), and therefore $a_1 = \cdots = a_r = 0$. This shows that the entire collection $\{v_1, \ldots, v_r\}$ is independent. ∎

Corollary 1 Suppose $T \in L(V)$ and dim V = n. Then T can have at most n distinct eigenvalues in $\mathcal{F}$.

Proof Since dim V = n, there can be at most n independent vectors in V. Since n distinct eigenvalues result in n independent eigenvectors, this corollary follows directly from Theorem 7.8. ∎

Corollary 2 Suppose $T \in L(V)$ and dim V = n. If T has n distinct eigenvalues, then there exists a basis for V which consists of eigenvectors of T.

Proof If T has n distinct eigenvalues, then (by Theorem 7.8) T must have n linearly independent eigenvectors. But n is the number of elements in any basis for V, and hence these n linearly independent eigenvectors in fact form a basis for V. ∎

It should be remarked that one eigenvalue can belong to more than one linearly independent eigenvector. In fact, if $T \in L(V)$ and λ is an eigenvalue of T, then the set V_λ of all eigenvectors of T belonging to λ is a subspace of V called the **eigenspace** of λ. It is also easy to see that $V_\lambda = \text{Ker}(\lambda 1 - T)$ (see Exercise 7.2.1).

Exercises

1. (a) If $T \in L(V)$ and λ is an eigenvalue of T, show that the set V_λ of all eigenvectors of T belonging to λ is a T-invariant subspace of V (i.e., a subspace with the property that $T(v) \in V_\lambda$ for all $v \in V_\lambda$).
   (b) Show that $V_\lambda = \text{Ker}(\lambda 1 - T)$.

2. An operator $T \in L(V)$ with the property that $T^n = 0$ for some $n \in \mathbb{Z}^+$ is said to be **nilpotent**. Show that the only eigenvalue of a nilpotent operator is 0.

3. If $S, T \in L(V)$, show that ST and TS have the same eigenvalues. [*Hint*: First use Theorems 5.16 and 7.6 to show that 0 is an eigenvalue of ST if and only if 0 is an eigenvalue of TS. Now assume $\lambda \neq 0$, and let $ST(v) = \lambda v$. Show that Tv is an eigenvector of TS.]

4. (a) Consider the rotation operator $R(\alpha) \in L(\mathbb{R}^2)$ defined in Example 1.2. Does $R(\alpha)$ have any eigenvectors? Explain.
   (b) Repeat part (a) but now consider rotations in $\mathbb{R}^3$.

5. For each of the following matrices, find all eigenvalues and linearly independent eigenvectors:

(*a*) $\begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$ (*b*) $\begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}$ (*c*) $\begin{pmatrix} 5 & -1 \\ 1 & 3 \end{pmatrix}$

6. Consider the spaces $D[\mathbb{R}]$ and $F[\mathbb{R}]$ defined in Exercise 2.1.6, and let $d: D[\mathbb{R}] \to F[\mathbb{R}]$ be the usual derivative operator.
(a) Show that the eigenfunctions (i.e., eigenvectors) of d are of the form $\exp(\lambda x)$ where λ is the corresponding eigenvalue.
(b) Suppose $\lambda_1, \ldots, \lambda_r \in \mathbb{R}$ are distinct. Show that the set

$$S = \{\exp(\lambda_1 x), \ldots, \exp(\lambda_r x)\}$$

is linearly independent. [*Hint*: Consider the linear span of S.]

7. Suppose $T \in L(V)$ is invertible. Show that λ is an eigenvalue of T if and only if $\lambda \neq 0$ and λ^{-1} is an eigenvalue of T^{-1}.

8. Suppose $T \in L(V)$ and $\dim V = n$. If T has n linearly independent eigenvectors, what can you say about the matrix representation of T?

9. Let V be a two-dimensional space over $\mathbb{R}$, and let $\{e_1, e_2\}$ be a basis for V. Find the eigenvalues and eigenvectors of the operator $T \in L(V)$ defined by:
(a) $Te_1 = e_1 + e_2$ $\quad Te_2 = e_1 - e_2$.
(b) $Te_1 = 5e_1 + 6e_2$ $\quad Te_2 = -7e_2$.
(c) $Te_1 = e_1 + 2e_2$ $\quad Te_2 = 3e_1 + 6e_2$.

10. Suppose $A \in M_n(\mathbb{C})$ and define $R_i = \sum_{j=1}^{n} |a_{ij}|$ and $P_i = R_i - |a_{ii}|$.
(a) Show that if $Ax = 0$ for some nonzero $x = (x_1, \ldots, x_n)$, then for any r such that $x_r \neq 0$ we have

$$|a_{rr}||x_r| = \left| \sum_{j \neq r} a_{rj} x_j \right| .$$

(b) Show that part (a) implies that for some r we have $|a_{rr}| \leq P_r$.
(c) Prove that if $|a_{ii}| > P_i$ for all $i = 1, \ldots, n$, then all eigenvalues of A are nonzero (or, equivalently, that $\det A \neq 0$).

11. (a) Suppose $A \in M_n(\mathbb{C})$ and let λ be an eigenvalue of A. Using the previous exercise prove **Gershgorin's Theorem**: $|\lambda - a_{rr}| \leq P_r$ for some r with $1 \leq r \leq n$.
(b) Use this result to show that every eigenvalue λ of the matrix

$$A = \begin{pmatrix} 4 & 1 & 1 & 0 & 1 \\ 1 & 3 & 1 & 0 & 0 \\ 1 & 2 & 3 & 1 & 0 \\ 1 & 1 & -1 & 4 & 0 \\ 1 & 1 & 1 & 1 & 5 \end{pmatrix}$$

satisfies $1 \leq |\lambda| \leq 9$.

7.3 CHARACTERISTIC POLYNOMIALS

So far our discussion has dealt only theoretically with the existence of eigenvalues of an operator $T \in L(V)$. From a practical standpoint (as we saw in Example 7.1), it is much more convenient to deal with the matrix representation of an operator. Recall that the definition of an eigenvalue $\lambda \in \mathcal{F}$ and eigenvector $v = \sum v_i e_i$ of a matrix $A = (a_{ij}) \in M_n(\mathcal{F})$ is given in terms of components by $\sum_j a_{ij} v_j = \lambda v_i$ for each $i = 1, \ldots, n$. This may be written in the form

$$\sum_{j=1}^{n} a_{ij} v_j = \lambda \sum_{j=1}^{n} \delta_{ij} v_j$$

or, alternatively, as

$$\sum_{j=1}^{n} (\lambda \delta_{ij} - a_{ij}) v_j = 0 \quad .$$

In matrix notation, this is

$$(\lambda I - A)v = 0 \quad .$$

By the corollary to Theorem 4.13, this set of homogeneous equations has a nontrivial solution if and only if $\det(\lambda I - A) = 0$.

Another way to see this is to note that by Theorem 7.6, λ is an eigenvalue of the operator $T \in L(V)$ if and only if $\lambda 1 - T$ is singular. But according to Theorem 5.16, this means that $\det(\lambda 1 - T) = 0$ (recall that the determinant of a linear transformation T is defined to be the determinant of any matrix representation of T). In other words, λ is an eigenvalue of T if and only if $\det(\lambda 1 - T) = 0$. This proves the following important result.

Theorem 7.9 Suppose $T \in L(V)$ and $\lambda \in \mathcal{F}$. Then λ is an eigenvalue of T if and only if $\det(\lambda 1 - T) = 0$.

Let [T] be a matrix representation of T. The matrix xI − [T] is called the **characteristic matrix** of [T], and the expression det(x1 − T) = 0 is called the **characteristic** (or **secular**) **equation** of T. The determinant det(x1 − T) is frequently denoted by $\Delta_T(x)$. Writing out the determinant in a particular basis, we see that det(x1 − T) is of the form

$$\Delta_T(x) = \begin{vmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{vmatrix}$$

where $A = (a_{ij})$ is the matrix representation of T in the chosen basis. Since the expansion of a determinant contains exactly one element from each row and each column, we see that (see Exercise 7.3.1)

$$\begin{aligned} \det(x1 - T) &= (x - a_{11})(x - a_{22})\cdots(x - a_{nn}) \\ &\quad + \text{ terms containing } n-1 \text{ factors of the form } x - a_{ii} \\ &\quad + \cdots + \text{ terms with no factors containing } x \\ &= x^n - (\operatorname{Tr} A)x^{n-1} + \text{ terms of lower degree in } x + (-1)^n \det A \ . \end{aligned}$$

This polynomial is called the **characteristic polynomial** of T.

From the discussion following Theorem 5.18, we see that if $A' = P^{-1}AP$ is similar to A, then

$$\det(xI - A') = \det(xI - P^{-1}AP) = \det[P^{-1}(xI - A)P] = \det(xI - A)$$

(since $\det P^{-1} = (\det P)^{-1}$). We thus see that similar matrices have the same characteristic polynomial (the converse of this statement is *not* true), and hence also the same eigenvalues. Therefore the eigenvalues (*not* eigenvectors) of an operator $T \in L(V)$ do not depend on the basis chosen for V. Note also that according to Exercise 4.2.14, we may as well write Tr T and det T (rather than Tr A and det A) since these are independent of the particular basis chosen. Using this terminology, we may rephrase Theorem 7.9 as follows.

Theorem 7.9′ A scalar $\lambda \in \mathcal{F}$ is an eigenvalue of $T \in L(V)$ if and only if λ is a root of the characteristic polynomial $\Delta_T(x)$.

Since the characteristic polynomial is of degree n in x, the corollary to Theorem 6.14 tells us that if we are in an algebraically closed field (such as

$\mathbb{C}$), then there must exist n roots. In this case, the characteristic polynomial may be factored into the form

$$\det(x1 - T) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n)$$

where the eigenvalues λ_i are not necessarily distinct. Expanding this expression we have

$$\det(x1 - T) = x^n - (\sum\lambda_i)x^{n-1} + \cdots + (-1)^n \lambda_1\lambda_2 \cdots \lambda_n \ .$$

Comparing this with the above general expression for the characteristic polynomial, we see that

$$\mathrm{Tr}\, T = \sum_{i=1}^{n} \lambda_i$$

and

$$\det T = \prod_{i=1}^{n} \lambda_i \ .$$

It should be remembered that this result only applies to an algebraically closed field (or to any other field $\mathcal{F}$ as long as all n roots of the characteristic polynomial lie in $\mathcal{F}$).

Example 7.2 Let us find the eigenvalues and eigenvectors of the matrix

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

The characteristic polynomial of A is given by

$$\Delta_A(x) = \begin{vmatrix} x-1 & -4 \\ -2 & x-3 \end{vmatrix} = x^2 - 4x - 5 = (x-5)(x+1)$$

and hence the eigenvalues of A are $\lambda = 5, -1$. To find the eigenvectors corresponding to each eigenvalue, we must solve $Av = \lambda v$ or $(\lambda I - A)v = 0$. Written out for $\lambda = 5$ this is

$$\begin{pmatrix} 4 & -4 \\ -2 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} .$$

We must therefore solve the set of homogeneous linear equations

$$4x - 4y = 0$$
$$-2x + 2y = 0$$

which is clearly equivalent to the single equation x − y = 0, or x = y. This means that every eigenvector corresponding to the eigenvalue λ = 5 is a multiple of the vector (1, 1), and thus the corresponding eigenspace is one-dimensional.

For λ = −1 we have

$$\begin{pmatrix} -2 & -4 \\ -2 & -4 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

and the equation to be solved is (since both are the same) −2x − 4y = 0. The solution is thus −x = 2y so that the eigenvector is a multiple of (2, −1).

We now note that

$$\text{Tr } A = 1 + 3 = 4 = \sum \lambda_i$$

and

$$\det A = 3 - 8 = -5 = \prod \lambda_i \quad .$$

It is also easy to see that these relationships hold for the matrix given in Example 7.1. //

It is worth remarking that the existence of eigenvalues of a given operator (or matrix) depends on the particular field we are working with. For example, the matrix

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

has characteristic polynomial $x^2 + 1$ which has no real roots, but does have the complex roots $\pm i$. In other words, A has no eigenvalues in $\mathbb{R}$, but does have the eigenvalues $\pm i$ in $\mathbb{C}$ (see Exercise 7.3.6).

Returning to the general case of an arbitrary field, it is clear that letting λ = 0 in $\Delta_T(\lambda) = \det(\lambda 1 - T) = 0$ shows that the constant term in the characteristic polynomial of A is given by $\Delta_T(0) = (-1)^n \det A$. In view of Theorems 4.6, 7.5 and the corollary to Theorem 7.7, we wonder if there are any relationships between the characteristic and minimal polynomials of T. There are indeed, and the first step in showing some of these relationships is to prove that every $A \in M_n(\mathcal{F})$ satisfies some nontrivial polynomial. This is the essential content of our next result, the famous Cayley-Hamilton theorem.

Before we prove this theorem, we should point out that we will be dealing with matrices that have polynomial entries, rather than entries that are simply elements of the field $\mathcal{F}$. However, if we regard the polynomials as elements of

the field of quotients (see Section 6.5), then all of our previous results (for example, those dealing with determinants) remain valid. We shall elaborate on this problem in detail in the next chapter. Furthermore, the proof we are about to give is the standard one at this level. We shall find several other methods of proof throughout this text, including a remarkably simple one in the next chapter (see the discussion of matrices over the ring of polynomials).

Theorem 7.10 (**Cayley-Hamilton Theorem**) Every matrix $A \in M_n(\mathcal{F})$ satisfies its characteristic polynomial.

Proof First recall from Theorem 4.11 that any matrix $A \in M_n(\mathcal{F})$ obeys the relation

$$A(\text{adj } A) = (\det A)I_n$$

where adj A is the matrix whose elements are the determinants of the minor matrices of A. In particular, the characteristic matrix xI – A obeys

$$(xI - A)B(x) = \det(xI - A)I$$

where we let

$$B(x) = \text{adj}(xI - A) \ .$$

Thus the entries of the n x n matrix B(x) are polynomials in x of degree ≤ n – 1. For example, if

$$B(x) = \begin{pmatrix} x^2 + 2 & x & 3 \\ -x + 1 & 1 & 0 \\ 0 & 4 & x^2 \end{pmatrix}$$

then

$$B(x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} x^2 + \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} x + \begin{pmatrix} 2 & 0 & 3 \\ 1 & 1 & 0 \\ 0 & 4 & 0 \end{pmatrix} .$$

Hence in general, we may write B(x) in the form

$$B(x) = B_0 + B_1x + \cdots + B_{n-1}x^{n-1}$$

where each $B_i \in M_n(\mathcal{F})$.

Now write

$$\Delta_A(x) = \det(xI - A) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \ .$$

Then Theorem 4.11 becomes

$$(xI - A)(B_0 + B_1x + \cdots + B_{n-1}x^{n-1}) = (a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n)I \ .$$

Equating powers of x in this equation yields

$$\begin{aligned} -AB_0 &= a_0I \\ B_0 - AB_1 &= a_1I \\ B_1 - AB_2 &= a_2I \\ &\vdots \\ B_{n-2} - AB_{n-1} &= a_{n-1}I \\ B_{n-1} &= I \end{aligned}$$

We now multiply the first of these equations by $A^0 = I$, the second by $A^1 = A$, the third by $A^2, \ldots$, the n*th* by A^{n-1}, and the last by A^n to obtain

$$\begin{aligned} -AB_0 &= a_0I \\ AB_0 - A^2B_1 &= a_1A \\ A^2B_1 - A^3B_2 &= a_2A^2 \\ &\vdots \\ A^{n-1}B_{n-2} - A^nB_{n-1} &= a_{n-1}A^{n-1} \\ A^nB_{n-1} &= A^n \end{aligned}$$

Adding this last group of matrix equations, we see that the left side cancels out and we are left with

$$0 = a_0I + a_1A + a_2A^2 + \cdots + a_{n-1}A^{n-1} + A^n \ .$$

This shows that A satisfies its characteristic polynomial. ∎

In view of this theorem, we see that there exists a nonempty set of nonzero polynomials $p(x) \in \mathcal{F}[x]$ such that $p(A) = 0$ for any $A \in M_n(\mathcal{F})$. (Alternatively, Theorem 7.3 and its corollary apply equally well to the algebra of matrices, although the degree is bounded by n^2 rather than by n.) As we did for linear transformations, we may define the **minimal polynomial** for A as that polynomial p(x) of least degree for which $p(A) = 0$. We also noted following Theorem 7.4 that any $T \in L(V)$ and its corresponding representation $A \in M_n(\mathcal{F})$ satisfy the same minimal polynomial. Theorem 7.4 thus applies equally well to matrices, and hence there exists a unique monic

minimal polynomial m(x) for A such that m(A) = 0. In addition, m(x) divides every other polynomial which has A as a zero. In particular, since A satisfies $\Delta_A(x)$, we must have $m(x)|\Delta_A(x)$.

Theorem 7.11 Suppose $A \in M_n(\mathcal{F})$ and m(x) is the minimal polynomial for A. Then $m(x)|\Delta_A(x)$ and $\Delta_A(x)|[m(x)]^n$.

Proof That $m(x)|\Delta_A(x)$ was proved in the previous paragraph. Let $m(x) = x^k + m_1x^{k-1} + \cdots + m_{k-1}x + m_k$. We define the matrices $B_i \in M_n(\mathcal{F})$ by

$$\begin{aligned} B_0 &= I \\ B_1 &= A + m_1 I \\ B_2 &= A^2 + m_1 A + m_2 I \\ &\vdots \\ B_{k-1} &= A^{k-1} + m_1 A^{k-2} + \cdots + m_{k-1} I \end{aligned}$$

where $I = I_n$. Working our way successively down this set of equations, we may rewrite them in the form

$$\begin{aligned} B_0 &= I \\ B_1 - AB_0 &= m_1 I \\ B_2 - AB_1 &= m_2 I \\ &\vdots \\ B_{k-1} - AB_{k-2} &= m_{k-1} I \end{aligned}$$

From the previous expression for B_{k-1}, we multiply by $-A$ and then add and subtract m_kI to obtain (using m(A) = 0)

$$\begin{aligned} -AB_{k-1} &= m_k I - (A^k + m_1 A^{k-1} + \cdots + m_{k-1} A + m_k I) \\ &= m_k I - m(A) \\ &= m_k I \quad . \end{aligned}$$

Now define $B(x) = x^{k-1}B_0 + x^{k-2}B_1 + \cdots + xB_{k-2} + B_{k-1}$ (which may be viewed either as a polynomial with matrix coefficients or as a matrix with polynomial entries). Then, using our previous results, we find that

$$\begin{aligned}(xI - A)B(x) &= xB(x) - AB(x) \\ &= (x^k B_0 + x^{k-1}B_1 + \cdots + x^2 B_{k-2} + xB_{k-1}) \\ &\qquad - (x^{k-1}AB_0 + x^{k-2}AB_1 + \cdots + xAB_{k-2} + AB_{k-1}) \\ &= x^k B_0 + x^{k-1}(B_1 - AB_0) + x^{k-2}(B_2 - AB_1) \\ &\qquad + \cdots + x(B_{k-1} - AB_{k-2}) - AB_{k-1} \\ &= x^k I + m_1 x^{k-1} I + m_2 x^{k-2} I + \cdots + m_{k-1} xI + m_k I \\ &= m(x)I \quad . \end{aligned} \tag{*}$$

Since the determinant of a diagonal matrix is the product of its (diagonal) elements (see the corollary to Theorem 4.5), we see that

$$\det[m(x)I] = [m(x)]^n .$$

Therefore, taking the determinant of both sides of (*) and using Theorem 4.8 we find that

$$[\det(xI - A)]\,[\det B(x)] = \det[m(x)I] = [m(x)]^n .$$

But det B(x) is just some polynomial in x, so this equation shows that $[m(x)]^n$ is some multiple of $\Delta_A(x) = \det(xI - A)$. In other words, $\Delta_A(x) \mid [m(x)]^n$. ∎

Theorem 7.12 The characteristic polynomial $\Delta_A(x)$ and minimal polynomial m(x) of a matrix $A \in M_n(\mathcal{F})$ have the same prime factors.

Proof Let m(x) have the prime factor f(x) so that f(x)|m(x). Since we showed in the above discussion that $m(x) \mid \Delta_A(x)$, it follows that $f(x) \mid \Delta_A(x)$ and hence f(x) is a factor of $\Delta_A(x)$ also. Now suppose that $f(x) \mid \Delta_A(x)$. Theorem 7.11 shows that $\Delta_A(x) \mid [m(x)]^n$, and therefore $f(x) \mid [m(x)]^n$. However, since f(x) is prime, Corollary 2′ of Theorem 6.5 tells us that f(x)|m(x). ∎

It is important to realize that this theorem does *not* say that $\Delta_A(x) = m(x)$, but only that $\Delta_A(x)$ and m(x) have the same prime factors. However, each factor can be of a different multiplicity in m(x) from what it is in $\Delta_A(x)$. In particular, since $m(x) \mid \Delta_A(x)$, the multiplicity of any factor in $\Delta_A(x)$ must be greater than or equal to the multiplicity of the same factor in m(x). Since a linear factor (i.e., a factor of the form $x - \lambda$) is prime, it then follows that $\Delta_A(x)$ and m(x) have the same roots (although of different multiplicities).

Theorem 7.13 Suppose $A \in M_n(\mathcal{F})$ and $\lambda \in \mathcal{F}$. Then λ is an eigenvalue of A if and only if λ is a root of the minimal polynomial for A.

Proof By Theorem 7.9, λ is an eigenvalue of A if and only if $\Delta_A(\lambda) = 0$. But from the above remarks, λ is a root of $\Delta_A(x)$ if and only if λ is a root of the minimal polynomial for A. ∎

An alternative proof of Theorem 7.13 is to note that since $m(x)|\Delta_A(x)$, we may write $\Delta_A(x) = m(x)p(x)$ for some polynomial $p(x)$. If λ is a root of $m(x)$, then $\Delta_A(\lambda) = m(\lambda)p(\lambda) = 0$ so that λ is also a root of $\Delta_A(x)$. In other words, λ is an eigenvalue of A. The converse is just the corollary to Theorem 7.7. If we use this proof, then Theorem 7.12 is essentially just a corollary of Theorem 7.13.

Using Theorem 7.13, we can give another proof of Theorem 7.5 which also applies to the characteristic polynomial of any $T \in L(V)$. In particular, from Theorem 5.10 we see that T is invertible if and only if T is nonsingular if and only if 0 is not an eigenvalue of T (because this would mean that $Tv = 0v = 0$ for some $v \neq 0$). But from Theorem 7.13, this is true if and only if 0 is not a root of the minimal polynomial for T. Writing the minimal polynomial as $m(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + x^k$, we then see that $a_0 = m(0) \neq 0$ as claimed.

Example 7.3 Consider the matrix A given by

$$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}.$$

The characteristic polynomial is given by

$$\Delta_A(x) = \det(xI - A) = (x - 2)^3(x - 5)$$

and hence Theorem 7.12 tells us that both $x - 2$ and $x - 5$ must be factors of $m(x)$. Furthermore, it follows from Theorems 7.4 and 7.10 that $m(x)|\Delta_A(x)$, and thus the minimal polynomial must be either $m_1(x)$, $m_2(x)$ or $m_3(x)$ where

$$m_j(x) = (x - 2)^j(x - 5) \ .$$

From the Cayley-Hamilton theorem we know that $m_3(A) = \Delta_A(A) = 0$, and it is easy to show that $m_2(A) = 0$ also while $m_1(A) \neq 0$. Therefore the minimal polynomial for A must be $m_2(x)$. //

We now turn our attention to one of the most important aspects of the existence of eigenvalues. Suppose that $T \in L(V)$ with $\dim V = n$. If V has a basis $\{v_1, \ldots, v_n\}$ that consists entirely of eigenvectors of T, then the matrix representation of T in this basis is defined by

$$T(v_i) = \sum_{j=1}^{n} v_j a_{ji} = \lambda_i v_i = \sum_{j=1}^{n} \delta_{ji} \lambda_j v_j$$

and therefore $a_{ji} = \delta_{ji}\lambda_j$. In other words, T is represented by a diagonal matrix in a basis of eigenvectors. Conversely, if T is represented by a diagonal matrix $a_{ji} = \delta_{ji}\lambda_j$ relative to some basis $\{v_i\}$, then reversing the argument shows that each v_i is an eigenvector of T. This proves the following theorem.

Theorem 7.14 A linear operator $T \in L(V)$ can be represented by a diagonal matrix if and only if V has a basis consisting of eigenvectors of T. If this is the case, then the diagonal elements of the matrix representation are precisely the eigenvalues of T. (Note however, that the eigenvalues need not necessarily be distinct.)

If $T \in L(V)$ is represented in some basis $\{e_i\}$ by a matrix A, and in the basis of eigenvectors v_i by a diagonal matrix D, then Theorem 5.18 tells us that A and D must be similar matrices. This proves the following version of Theorem 7.14, which we state as a corollary.

Corollary 1 A matrix $A \in M_n(\mathcal{F})$ is similar to a diagonal matrix D if and only if A has n linearly independent eigenvectors.

Corollary 2 A linear operator $T \in L(V)$ can be represented by a diagonal matrix if T has $n = \dim V$ distinct eigenvalues.

Proof This follows from Corollary 2 of Theorem 7.8. ∎

Note that the existence of $n = \dim V$ distinct eigenvalues of $T \in L(V)$ is a sufficient but not necessary condition for T to have a diagonal representation. For example, the identity operator has the usual diagonal representation, but its only eigenvalues are $\lambda = 1$. In general, if any eigenvalue has multiplicity greater than 1, then there will be fewer distinct eigenvalues than the dimension of V. However, in this case we *may* be able to choose an appropriate linear combination of eigenvectors in each eigenspace so that the matrix of T will still be diagonal. We shall have more to say about this in Section 7.7.

We say that a matrix A is **diagonalizable** if it is similar to a diagonal matrix D. If P is a nonsingular matrix such that $D = P^{-1}AP$, then we say that P

diagonalizes A. It should be noted that if λ is an eigenvalue of a matrix A with eigenvector v (i.e., $Av = \lambda v$), then for any nonsingular matrix P we have

$$(P^{-1}AP)(P^{-1}v) = P^{-1}Av = P^{-1}\lambda v = \lambda(P^{-1}v) \ .$$

In other words, $P^{-1}v$ is an eigenvector of $P^{-1}AP$. Similarly, we say that $T \in L(V)$ is **diagonalizable** if there exists a basis for V that consists entirely of eigenvectors of T.

While all of this sounds well and good, the reader might wonder exactly how the transition matrix P is to be constructed. Actually, the method has already been given in Section 5.4. If $T \in L(V)$ and A is the matrix representation of T in a basis $\{e_i\}$, then P is defined to be the transformation that takes the basis $\{e_i\}$ into the basis $\{v_i\}$ of eigenvectors. In other words, $v_i = Pe_i = \sum_j e_j p_{ji}$. This means that the i*th* column of (p_{ij}) is just the i*th* eigenvector of A. The fact that P must be nonsingular coincides with the requirement that T (or A) have n linearly independent eigenvectors v_i.

Example 7.4 Referring to Example 7.2, we found the eigenvectors $v_1 = (1, 1)$ and $v_2 = (2, -1)$ belonging to the matrix

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

Then P and P^{-1} are given by

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

and

$$P^{-1} = \frac{\operatorname{adj} P}{\det P} = \begin{pmatrix} 1/3 & 2/3 \\ 1/3 & -1/3 \end{pmatrix}$$

and therefore

$$D = P^{-1}AP = \begin{pmatrix} 1/3 & 2/3 \\ 1/3 & -1/3 \end{pmatrix}\begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & -1 \end{pmatrix} \ .$$

We see that D is a diagonal matrix, and that the diagonal elements are just the eigenvalues of A. Note also that

$$D(P^{-1}v_1) = \begin{pmatrix} 5 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1/3 & 2/3 \\ 1/3 & -1/3 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 5 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 5\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$
$$= \lambda_1(P^{-1}v_1)$$

with a similar result holding for $P^{-1}v_2$. ∥

Example 7.5 Let us show that the matrix

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

is not diagonalizable. The characteristic equation is $(x - 1)^2 = 0$, and hence there are two identical roots $\lambda = 1$. If there existed an eigenvector $v = (x, y)$, it would have to satisfy the equation $(\lambda I - A)v = 0$ or

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

Since this yields $-2y = 0$, the eigenvectors must be of the form $(x, 0)$, and hence it is impossible to find two linearly independent such eigenvectors.

Note that the minimal polynomial for A is either $x - 1$ or $(x - 1)^2$. But since $A - 1I \neq 0$, $m(x)$ must be $(x - 1)^2$. We will see later (Theorem 7.24) that a matrix is diagonalizable if and only if its minimal polynomial is a product of distinct linear factors. ∥

Exercises

1. Suppose $T \in L(V)$ has matrix representation $A = (a_{ij})$, and $\dim V = n$. Prove that

$$\det(x1 - T) = x^n - (\text{Tr } A)x^{n-1} + \text{terms of lower degree in } x + (-1)^n \det A.$$

[*Hint*: Use the definition of determinant.]

2. Suppose $T \in L(V)$ is diagonalizable. Show that the minimal polynomial $m(x)$ for T must consist of distinct linear factors. [*Hint*: Let T have distinct eigenvalues $\lambda_1, \ldots, \lambda_r$ and consider the polynomial

$$f(x) = (x - \lambda_1) \cdots (x - \lambda_r) \ .$$

Show that $m(x) = f(x)$.]

3. Prove by direct substitution that $\Delta_A(A) = 0$ if $A \in M_n(\mathcal{F})$ is diagonal.

4. Find, in the form $a_0 + a_1x + a_2x^2 + a_3x^3$, the characteristic polynomial of

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

Show by direct substitution that A satisfies its characteristic polynomial.

5. If $T \in L(V)$ and $\Delta_T(x)$ is a product of distinct linear factors, prove that T is diagonalizable.

6. Consider the following matrices:

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 4 \end{pmatrix} \qquad B = \begin{pmatrix} 3 & -1 \\ 13 & -3 \end{pmatrix}$$

(a) Find all eigenvalues and linearly independent eigenvectors over $\mathbb{R}$.
(b) Find all eigenvalues and linearly independent eigenvectors over $\mathbb{C}$.

7. For each of the following matrices, find all eigenvalues, a basis for each eigenspace, and determine whether or not the matrix is diagonalizable:

$$(a) \begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix} \qquad (b) \begin{pmatrix} -3 & 1 & -1 \\ -7 & 5 & -1 \\ -6 & 6 & -2 \end{pmatrix}$$

8. Consider the operator $T \in L(\mathbb{R}^3)$ defined by

$$T(x, y, z) = (2x + y, y - z, 2y + 4z) \ .$$

Find all eigenvalues and a basis for each eigenspace.

9. Let $A = (a_{ij})$ be a triangular matrix, and assume that all of the diagonal entries of A are distinct. Is A diagonalizable? Explain.

10. Suppose $A \in M_3(\mathbb{R})$. Show that A can not be a zero of the polynomial $f = x^2 + 1$.

11. If $A \in M_n(\mathcal{F})$, show that A and A^T have the same eigenvalues.

12. Suppose A is a block triangular matrix with square matrices A_{ii} on the diagonal. Show that the characteristic polynomial of A is the product of the characteristic polynomials of the A_{ii}.

13. Find the minimal polynomial of

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

14. For each of the following matrices A, find a nonsingular matrix P (if it exists) such that $P^{-1}AP$ is diagonal:

$$(a)\ A = \begin{pmatrix} 3 & 1 & 1 \\ 2 & 4 & 2 \\ 1 & 1 & 3 \end{pmatrix} \qquad (b)\ \begin{pmatrix} 1 & 2 & 2 \\ 1 & 2 & -1 \\ -1 & 1 & 4 \end{pmatrix} \qquad (c)\ \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

15. Consider the following real matrix:

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

Find necessary and sufficient conditions on a, b, c and d so that A is diagonalizable.

16. Let A be an idempotent matrix (i.e., $A^2 = A$) of rank r. Show that A is similar to the matrix

$$B = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

17. Let V be the space of all real polynomials $f \in \mathbb{R}[x]$ of degree at most 2, and define $T \in L(V)$ by $Tf = f + f' + xf'$ where f' denotes the usual derivative with respect to x.

(a) Write down the most obvious basis $\{e_1, e_2, e_3\}$ for V you can think of, and then write down $[T]_e$.
(b) Find all eigenvalues of T, and then find a nonsingular matrix P such that $P^{-1}[T]_e P$ is diagonal.

18. Prove that any real symmetric 2 x 2 matrix is diagonalizable.

19. (a) Let $C \in M_2(\mathbb{C})$ be such that $C^2 = 0$. Prove that either $C = 0$, or else C is similar over $\mathbb{C}$ to the matrix

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

(b) Prove that $A \in M_2(\mathbb{C})$ is similar over $\mathbb{C}$ to one of the following two types of matrices:

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} a & 0 \\ 1 & a \end{pmatrix} .$$

20. Find a matrix $A \in M_3(\mathbb{R})$ that has the eigenvalues 3, 2 and 2 with corresponding eigenvectors (2, 1, 1), (1, 0, 1) and (0, 0, 4).

21. Is it possible for the matrix

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

to have the eigenvalues −1, 2, 3 and 5?

7.4 ANNIHILATORS

The purpose of this section is to repeat our description of minimal polynomials using the formalism of ideals developed in the previous chapter. Our reasons for this are twofold. First, we will gain additional insight into the meaning and action of minimal polynomials. And second, these results will be of use in the next chapter when we discuss cyclic subspaces.

If V is a vector space of dimension n over $\mathcal{F}$, then for any $v \in V$ and any $T \in L(V)$, the $n + 1$ vectors $v, T(v), T^2(v), \ldots, T^n(v)$ must be linearly

dependent. This means there exist scalars $a_0, \ldots, a_n \in \mathcal{F}$ not all equal to zero, such that

$$\sum_{i=1}^{n} a_i T^i(v) = 0 \quad .$$

If we define the polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathcal{F}[x]$, we see that our relation may be written as $f(T)(v) = 0$. In other words, given any (fixed) $v \in V$ and $T \in L(V)$, then there exists a polynomial f of degree $\leq n$ such that $f(T)(v) = 0$.

Now, for any fixed $v \in V$ and $T \in L(V)$, we define the set $N_T(v)$ by

$$N_T(v) = \{f(x) \in \mathcal{F}[x]: f(T)(v) = 0\} \quad .$$

This set is called the **T-annihilator** of v. If $f_1, f_2 \in N_T(v)$, then we have

$$[f_1(T) \pm f_2(T)](v) = f_1(T)(v) \pm f_2(T)(v) = 0$$

and for any $g(x) \in \mathcal{F}[x]$, we also have

$$[g(T)f_1(T)](v) = g(T)[f_1(T)(v)] = 0 \quad .$$

This shows that $N_T(v)$ is actually an ideal of $\mathcal{F}[x]$. Moreover, from Theorem 6.8 and its corollary, we see that $N_T(v)$ is a principal ideal, and hence has a unique monic generator, which we denote by $m_v(x)$. By definition, this means that $N_T(v) = m_v(x)\mathcal{F}[x]$, and since we showed above that $N_T(v)$ contains at least one polynomial of degree less than or equal to n, it follows from Theorem 6.2(b) that $\deg m_v(x) \leq n$. We call $m_v(x)$ the **minimal polynomial of the vector v** corresponding to the given transformation T. (Many authors also refer to $m_v(x)$ as the **T-annihilator** of v, or the **order** of v.) It is thus the unique monic polynomial of least degree such that $m(T)(v) = 0$.

Theorem 7.15 Suppose $T \in L(V)$, and let $v \in V$ have minimal polynomial $m_v(x)$. Assume $m_v(x)$ is reducible so that $m_v(x) = m_1(x)m_2(x)$ where $m_1(x)$ and $m_2(x)$ are both monic polynomials of degree ≥ 1. Then the vector $w = m_1(T)(v) \in V$ has minimal polynomial $m_2(x)$. In other words, every factor of the minimal polynomial of a vector is also the minimal polynomial of some other vector.

Proof First note that

$$m_2(T)(w) = m_2(T)[m_1(T)(v)] = m_v(T)(v) = 0$$

and thus $m_2(x) \in N_T(w)$. Then for any nonzero polynomial $f(x) \in \mathcal{F}[x]$ with $f(T)(w) = 0$, we have $f(T)[m_1(T)(v)] = 0$, and hence $f(x)m_1(x) \in N_T(v) = m_v(x)\,\mathcal{F}[x]$. Using this result along with Theorem 6.2(b), we see that

$$\deg m_1 + \deg f = \deg m_1 f \geq \deg m_v = \deg m_1 + \deg m_2$$

and therefore $\deg m_2 \leq \deg f$. This shows that $m_2(x)$ is the monic polynomial of least degree such that $m_2(T)(w) = 0$. ∎

Theorem 7.16 Suppose $T \in L(V)$, and let $m_u(x)$ and $m_v(x)$ be the minimal polynomials of $u \in V$ and $v \in V$ respectively. Then the least common multiple $m(x)$ of $m_u(x)$ and $m_v(x)$ is the minimal polynomial of some vector in V.

Proof We first assume that $m_u(x)$ and $m_v(x)$ are relatively prime so that their greatest common divisor is 1. By Theorem 6.9 we then have $m_u(x)m_v(x) = m(x)$. From Theorem 6.5 we may write $m_u(x)k(x) + m_v(x)h(x) = 1$ for some polynomials $h, k \in \mathcal{F}[x]$, and therefore

$$m_u(T)k(T) + m_v(T)h(T) = 1 \ .$$

Now define the vector $w \in V$ by

$$w = h(T)(u) + k(T)(v) \ .$$

Then, using $m_u(T)(u) = 0 = m_v(T)(v)$ we have

$$\begin{aligned} m_u(T)(w) &= m_u(T)h(T)(u) + m_u(T)k(T)(v) \\ &= m_u(T)k(T)(v) \\ &= [1 - m_v(T)h(T)](v) \\ &= v \end{aligned}$$

and similarly, we find that $m_v(T)(w) = u$. This means $m_u(T)m_v(T)(w) = 0$ so that $m_u(x)m_v(x) \in N_T(w)$.

Now observe that $N_T(w) = m_w(x)\mathcal{F}[x]$ where $m_w(x)$ is the minimal polynomial of w. Then

$$m_w(T)(u) = m_w(T)m_v(T)(w) = 0$$

and

$$m_w(T)(v) = m_w(T)m_u(T)(w) = 0$$

so that $m_w(x) \in N_T(u) \cap N_T(v)$. Since $N_T(u) = m_u(x)\mathcal{F}[x]$ and $N_T(v) = m_v(x)\mathcal{F}[x]$, we see from Example 6.9 (along with the fact that $m_u(x)$ and $m_v(x)$ are relatively prime) that

$$m_w(x) \in m(x)\mathcal{F}[x] = m_u(x)m_v(x)\mathcal{F}[x]$$

and hence $m_u(x)m_v(x)|m_w(x)$. On the other hand, since

$$m_u(x)m_v(x) \in N_T(w) = m_w(x)\mathcal{F}[x]$$

we have $m_w(x)|m_u(x)m_v(x)$. Since $m_w(x)$, $m_u(x)$ and $m_v(x)$ are monic, it follows that $m_w(x) = m_u(x)m_v(x) = m(x)$. This shows that in the case where $m_u(x)$ and $m_v(x)$ are relatively prime, then $m(x) = m_u(x)m_v(x)$ is the minimal polynomial of w.

Now let $d(x)$ be the greatest common divisor of $m_u(x)$ and $m_v(x)$, and consider the general case where (see Theorem 6.9) $m_u(x)m_v(x) = m(x)d(x)$. Using the notation of Theorem 6.10, we write $m_u = \alpha\beta$ and $m_v = \gamma\delta$. Since m_u and m_v are minimal polynomials by hypothesis, Theorem 7.15 tells us that α and δ are each also the minimal polynomial of some vector. However, by their construction, α and δ are relatively prime since they have no factors in common. This means that we may apply the first part of this proof to conclude that $\alpha\delta$ is the minimal polynomial of some vector. To finish the proof, we simply note that (according to Theorem 6.10) $\alpha\delta$ is just $m(x)$. ∎

A straightforward induction argument gives the following result.

Corollary For each $i = 1, \ldots, k$ let $m_{v_i}(x)$ be the minimal polynomial of a vector $v_i \in V$. Then there exists a vector $w \in V$ whose minimal polynomial $m(x)$ is the least common multiple of the $m_{v_i}(x)$.

Now suppose that $T \in L(V)$ and V has a basis $\{v_1, \ldots, v_n\}$. If $m_{v_i}(x)$ is the minimal polynomial of v_i, then by the corollary to Theorem 7.16, the least common multiple $m(x)$ of the $m_{v_i}(x)$ is the minimal polynomial of some vector $w \in V$, and therefore $\deg m(x) \leq \dim V = n$. But $m(x)$ is the least common multiple, so that for each $i = 1, \ldots, n$ we have $m(x) = f_i(x)m_{v_i}(x)$ for some $f_i(x) \in \mathcal{F}[x]$. This means that

$$m(T)(v_i) = [f_i(T)m_{v_i}(T)](v_i) = f_i(T)[m_{v_i}(T)(v_i)] = 0$$

for each v_i, and hence $m(T) = 0$. In other words, every $T \in L(V)$ satisfies some monic polynomial $m(x)$ with $\deg m(x) \leq \dim V = n$.

We now define the (nonempty) set

$$N_T = \{f(x) \in \mathcal{F}[x]: f(T) = 0\} \ .$$

As was the case with the T-annihilator, it is easy to prove that N_T is an ideal of $\mathcal{F}[x]$. Since N_T consists of those polynomials in T that annihilate every vector in V, it must be the same as the intersection of all T-annihilators $N_T(v)$ in V, i.e.,

$$N_T = \cap_{v \in V} N_T(v) \ .$$

By Theorem 6.8 the ideal N_T is principal, and we define the **minimal polynomial** for $T \in L(V)$ to be the unique monic generator of N_T. We claim that the minimal polynomial for T is precisely the polynomial m(x) defined in the previous paragraph.

To see this, note first that deg m(x) ≤ dim V = n, and since m(x) is the minimal polynomial of some $w \in V$, it follows directly from the definition of the minimal polynomial of w as the unique monic generator of $N_T(w)$ that $N_T(w) = m(x)\mathcal{F}[x]$. Next, the fact that m(T) = 0 means that m(T)(v) = 0 for every $v \in V$, and therefore $m(x) \in \cap_{v \in V} N_T(v) = N_T$. Since any polynomial in $N_T(w)$ is a multiple of m(x) and hence annihilates every $v \in V$, we see that $N_T(w) \subset N_T$. Conversely, any element of N_T is automatically an element of $N_T(w)$, and thus $N_T = N_T(w) = m(x)\mathcal{F}[x]$. This shows that m(x) is the minimal polynomial for T, and since m(x) generates N_T, it is the polynomial of least degree such that m(T) = 0.

Example 7.6 Let $V = \mathbb{R}^4$ have basis $\{e_1, e_2, e_3, e_4\}$ and define the operator $T \in L(V)$ by

$$T(e_1) = e_1 + e_3 \qquad T(e_2) = 3e_2 - e_4$$
$$T(e_3) = 3e_1 - e_3 \qquad T(e_4) = 3e_2 - e_4$$

Note that since $T(e_2) = T(e_4)$, the matrix representation of T has zero determinant, and hence T is singular (either by Theorem 5.9 or Theorem 5.16). Alternatively, we have $T(e_2 - e_4) = 0$ so that T must be singular since $e_2 - e_4 \neq 0$. In any case, we now have

$$T^2(e_1) = T(e_1 + e_3) = T(e_1) + T(e_3) = 4e_1$$

so that

$$(T^2 - 4)(e_1) = (T - 2)(T + 2) = 0 \ .$$

Similarly

$$T^2(e_2) = T(3e_2 - e_4) = 3T(e_2) - T(e_4) = 6e_2 - 2e_4 = 2T(e_2)$$

so that

$$(T^2 - 2T)(e_2) = T(T - 2)(e_2) = 0 .$$

Thus the minimal polynomial of e_1 is given by

$$m_1(x) = x^2 - 4 = (x - 2)(x + 2)$$

and the minimal polynomial of e_2 is given by

$$m_2(x) = x(x - 2) .$$

That these are indeed minimal polynomials is clear if we note that in neither case will a linear expression in T annihilate either e_1 or e_2 (just look at the definition of T).

It should be obvious that the least common multiple of m_1 and m_2 is

$$x(x - 2)(x + 2) = x(x^2 - 4)$$

and hence (by Theorem 7.16) this is the minimal polynomial of some vector $w \in \mathbb{R}^4$ which we now try to find. We know that $m_1(x) = x^2 - 4$ is the minimal polynomial of e_1, but is x the minimal polynomial of some vector u? Since $m_2(x) = x(x - 2)$ is the minimal polynomial of e_2, we see from Theorem 7.15 that the vector $u = (T - 2)(e_2) = e_2 - e_4$ has minimal polynomial x. Now, x and $x^2 - 4$ are relatively prime so, as was done in the first part of the proof of Theorem 7.16, we define the polynomials $h_1(x) = x/4$ and $k_1(x) = -1/4$ by the requirement that $xh_1 + (x^2 - 4)k_1 = 1$. Hence

$$w = (T/4)(e_1) + (-1/4)(u) = (1/4)(e_1 - e_2 + e_3 + e_4)$$

is the vector with minimal polynomial $x(x^2 - 4)$.

We leave it to the reader to show that $T^2(e_3) = 4e_3$ and $T^2(e_4) = 2T(e_4)$, and thus e_3 has minimal polynomial $m_3(x) = x^2 - 4$ and e_4 has minimal polynomial $m_4(x) = x(x - 2)$. It is now easy to see that $m(x) = x(x^2 - 4)$ is the minimal polynomial for T since m(x) has the property that $m(T)(e_i) = 0$ for each $i = 1, \ldots, 4$ and it is the least common multiple of the $m_i(x)$. We also note that the constant term in m(x) is zero, and hence T is singular by Theorem 7.5. //

Example 7.7 Relative to the standard basis for $\mathbb{R}^3$, the matrix

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

represents the operator $T \in L(\mathbb{R}^3)$ defined by $Te_1 = 2e_1 + e_2$, $Te_2 = -e_1 + e_3$ and $Te_3 = -2e_2 + e_3$. It is easy to see that $T^2e_1 = 3e_1 + 2e_2 + e_3$ and $T^3e_1 = 4e_1 + e_2 + 3e_3$, and hence the set $\{e_1, Te_1, T^2e_1\}$ is linearly independent, while the four vectors $\{e_1, Te_1, T^2e_1, T^3e_1\}$ must be linearly dependent. This means there exists $a, b, c, d \in \mathbb{R}$ such that

$$ae_1 + bTe_2 + cT^2 e_1 + dT^3 e_1 = 0 \ .$$

This is equivalent to the system

$$\begin{aligned} a + 2b + 3c + 4d &= 0 \\ b + 2c + \ d &= 0 \\ c + 3d &= 0 \end{aligned}$$

Since there is one free variable, choosing $d = 1$ we find $a = -5$, $b = 5$ and $c = -3$. Therefore the minimal polynomial of e_1 is $m_1(x) = x^3 - 3x^2 + 5x - 5$. Since the lcm of the minimal polynomials of e_1, e_2 and e_3 must be of degree ≤ 3, it follows that $m_1(x)$ is in fact the minimal polynomial $m(x)$ of T (and hence also of A). Note that by Theorem 7.5 we have $A(A^2 - 3A + 5I) = 5I$, and hence $A^{-1} = (1/5)(A^2 - 3A + 5I)$ or

$$A^{-1} = \frac{1}{5}\begin{pmatrix} 2 & 1 & 2 \\ -1 & 2 & 4 \\ 1 & -2 & 1 \end{pmatrix} \ . \ \textit{//}$$

Exercises

1. Show that N_T is an ideal of $\mathcal{F}[x]$.

2. For each of the following linear operators $T \in L(V)$, find the minimal polynomial of each of the (standard) basis vectors for V, find the minimal polynomial of T, and find a vector whose minimal polynomial is the same as that of T:
   (a) $V = \mathbb{R}^2$: $Te_1 = e_2$, $Te_2 = e_1 + e_2$.

(b) $V = \mathbb{R}^2$: $Te_1 = 2e_1 - 3e_2$, $Te_2 = e_1 + 5e_2$.

(c) $V = \mathbb{R}^3$: $Te_1 = e_1 - e_2 + e_3$, $Te_2 = -2e_2 + 5e_3$, $Te_3 = 2e_1 + 3e_2$.

(d) $V = \mathbb{R}^3$: $Te_1 = 2e_2$, $Te_2 = 2e_1$, $Te_3 = 2e_3$.

(e) $V = \mathbb{R}^4$: $Te_1 = e_1 + e_3$, $Te_2 = 3e_4$, $Te_3 = e_1 - e_3$, $Te_4 = e_2$.

(f) $V = \mathbb{R}^4$: $Te_1 = e_1 + e_2$, $Te_2 = e_2 - e_3$, $Te_3 = e_3 + e_4$, $Te_4 = e_1 - e_4$.

3. For each of the following matrices, find its minimal polynomial over $\mathbb{R}$, and then find its inverse if it exists:

$$(a)\ \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix} \qquad (b)\ \begin{pmatrix} 4 & -1 \\ -4 & 1 \end{pmatrix}$$

$$(c)\ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix} \qquad (d)\ \begin{pmatrix} 2 & 0 & 0 \\ -1 & 3 & 0 \\ 5 & 2 & 1 \end{pmatrix}$$

$$(d)\ \begin{pmatrix} 1 & 1 & 0 & 0 \\ 4 & 1 & 0 & 0 \\ 0 & 0 & 0 & -3 \\ 0 & 0 & 1 & 4 \end{pmatrix} \qquad (e)\ \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

7.5 INVARIANT SUBSPACES

Recall that two matrices $A, B \in M_n(\mathcal{F})$ are said to be similar if there exists a nonsingular matrix $P \in M_n(\mathcal{F})$ such that $B = P^{-1}AP$. As was shown in Exercise 5.4.1, this defines an equivalence relation on $M_n(\mathcal{F})$. Since $L(V)$ and $M_n(\mathcal{F})$ are isomorphic (Theorem 5.13), this definition applies equally well to linear operators. We call the equivalence class of a matrix (or linear operator) defined by this similarity relation its **similarity class**. While Theorem 7.14 gave us a condition under which a matrix may be diagonalized, this form is not possible to achieve in general. The approach we shall now take is to look for a basis in which the matrix of some linear operator in a given similarity class has a particularly simple standard form. As mentioned at the beginning of this chapter, these representations are called canonical forms. Of the many possible canonical forms, we shall consider only several of the more useful and important forms in this book. We begin with a discussion of some additional types of subspaces. A complete discussion of canonical forms under similarity is given in Chapter 8.

Suppose $T \in L(V)$ and let W be a subspace of V. Then W is said to be **invariant under T** (or simply **T-invariant**) if $T(w) \in W$ for every $w \in W$. For example, if $V = \mathbb{R}^3$ then the xy-plane is invariant under the linear transformation that rotates every vector in $\mathbb{R}^3$ about the z-axis. As another example, note that if $v \in V$ is an eigenvector of T, then $T(v) = \lambda v$ for some $\lambda \in \mathcal{F}$, and hence v generates a one-dimensional subspace of V that is invariant under T (this is *not* necessarily the same as the eigenspace of λ).

Another way to describe the invariance of W under T is to say that $T(W) \subset W$. Then clearly $T^2(W) = T(T(W)) \subset W$, and in general $T^n(W) \subset W$ for every $n = 1, 2, \ldots$. Since W is a subspace of V, this means that $f(T)(W) \subset W$ for any $f(x) \in \mathcal{F}[x]$. In other words, if W is invariant under T, then W is also invariant under any polynomial in T (over the same field as W).

If $W \subset V$ is T-invariant, we may define the **restriction** of T to W in the usual way as that operator $T|W: W \to W$ defined by $(T|W)(w) = T(w)$ for every $w \in W$. We will frequently write T_W instead of $T|W$.

Theorem 7.17 Suppose $T \in L(V)$ and let W be a T-invariant subspace of V. Then

(a) $f(T_W)(w) = f(T)(w)$ for any $f(x) \in \mathcal{F}[x]$ and $w \in W$.

(b) The minimal polynomial $m'(x)$ for T_W divides the minimal polynomial $m(x)$ for T.

Proof This is Exercise 7.5.2. ∎

If $T \in L(V)$ and $f(x) \in \mathcal{F}[x]$, then $f(T)$ is also a linear operator on V, and hence we may define the kernel (or null space) of $f(T)$ in the usual way by

$$\text{Ker } f(T) = \{v \in V: f(T)(v) = 0\} .$$

Theorem 7.18 If $T \in L(V)$ and $f(x) \in \mathcal{F}[x]$, then Ker $f(T)$ is a T-invariant subspace of V.

Proof Recall from Section 5.2 that Ker $f(T)$ is a subspace of V. To show that Ker $f(T)$ is T-invariant, we must show that $Tv \in \text{Ker } f(T)$ for any $v \in \text{Ker } f(T)$, i.e., $f(T)(Tv) = 0$. But using Theorem 7.2(a) we see that

$$f(T)(Tv) = T(f(T)(v)) = T(0) = 0$$

as desired. ∎

Now suppose $T \in L(V)$ and let $W \subset V$ be a T-invariant subspace. Furthermore let $\{v_1, v_2, \ldots, v_n\}$ be a basis for V, where the first $m < n$ vectors form a basis for W. If $A = (a_{ij})$ is the matrix representation of T relative to

this basis for V, then a little thought should convince you that A must be of the block matrix form

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

where $a_{ij} = 0$ for $j \leq m$ and $i > m$. This is because $T(w) \in W$ and any $w \in W$ has components $(w_1, \ldots, w_m, 0, \ldots, 0)$ relative to the above basis for V. The formal proof of this fact is given in the following theorem.

Theorem 7.19 Let W be a subspace of V and suppose $T \in L(V)$. Then W is T-invariant if and only if T can be represented in the block matrix form

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

where B is a matrix representation of T_W.

Proof First suppose that W is T-invariant. Choose a basis $\{v_1, \ldots, v_m\}$ for W, and extend this to a basis $\{v_1, \ldots, v_m, v_{m+1}, \ldots, v_n\}$ for V (see Theorem 2.10). Then, since $T(v_i) \in W$ for each $i = 1, \ldots, m$, there exist scalars b_{ij} such that

$$T_W(v_i) = T(v_i) = v_1 b_{1i} + \cdots + v_m b_{mi}$$

for each $i = 1, \ldots, m$. In addition, since $T(v_i) \in V$ for each $i = m + 1, \ldots, n$, there also exist scalars c_{ij} and d_{ij} such that

$$T(v_i) = v_1 c_{1i} + \cdots + v_m c_{mi} + v_{m+1} d_{m+1\,i} + \cdots + v_n d_{ni}$$

for each $i = m + 1, \ldots, n$.

From Theorem 5.11, we see that the matrix representation of T is given by an n x n matrix A of the form

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

where B is an m x m matrix that represents T_W, C is an m x (n − m) matrix, and D is an (n − m) x (n − m) matrix.

Conversely, if A has the stated form and $\{v_1, \ldots, v_n\}$ is a basis for V, then the subspace W of V defined by vectors of the form

$$w = \sum_{i=1}^{m} \alpha_i v_i$$

where each $\alpha_i \in \mathcal{F}$ will be invariant under T. Indeed, for each i = 1, . . . , m we have

$$T(v_i) = \sum_{j=1}^{n} v_j a_{ji} = v_1 b_{1i} + \cdots + v_m b_{mi} \in W$$

and hence T(w) ∈ W. ∎

Corollary Suppose T ∈ L(V) and W is a T-invariant subspace of V. Then the characteristic polynomial of T_W divides the characteristic polynomial of T.

Proof See Exercise 7.5.3. ∎

Recall from Theorem 2.18 that the orthogonal complement $W^\perp$ of a set W ⊂ V is a subspace of V. If W is a subspace of V and both W and $W^\perp$ are T-invariant, then since V = W ⊕ $W^\perp$ (Theorem 2.22), a little more thought should convince you that the matrix representation of T will now be of the block diagonal form

$$A = \begin{pmatrix} B & 0 \\ 0 & D \end{pmatrix} .$$

We now proceed to discuss a variation of Theorem 7.19 in which we take into account the case where V can be decomposed into a direct sum of subspaces.

Let us assume that V = $W_1 \oplus \cdots \oplus W_r$ where each W_i is a T-invariant subspace of V. Then we define the restriction of T to W_i to be the operator $T_i = T_{W_i} = T|W_i$. In other words, $T_i(w_i) = T(w_i) \in W_i$ for any $w_i \in W_i$. Given any v ∈ V we have v = $v_1 + \cdots + v_r$ where $v_i \in W_i$ for each i = 1, . . . , r, and hence

$$T(v) = \sum_{i=1}^{r} T(v_i) = \sum_{i=1}^{r} T_i(v_i) \quad .$$

This shows that T is completely determined by the effect of each T_i on W_i. In this case we call T the **direct sum** of the T_i and we write

$$T = T_1 \oplus \cdots \oplus T_r \quad .$$

We also say that T is **reducible** (or **decomposable**) into the operators T_i, and the spaces W_i are said to **reduce** T, or to form a **T-invariant direct sum decomposition** of V. In other words, T is reducible if there exists a basis for V such that V = $W_1 \oplus \cdots \oplus W_r$ and each W_i is T-invariant.

For each i = 1, . . . , r we let $B_i = \{w_{i1}, \ldots, w_{in_i}\}$ be a basis for W_i so that B = ∪B_i is a basis for V = $W_1 \oplus \cdots \oplus W_r$ (Theorem 2.15). We also let $A_i = (a_{i,\,kj})$ be the matrix representation of T_i with respect to the basis B_i (where k

and j label the rows and columns respectively of the matrix A_i). Therefore we see that

$$T(w_{ij}) = T_i(w_{ij}) = \sum_{k=1}^{n_i} w_{ik} a_{i,\,kj}$$

where i = 1, . . . , r and j = 1, . . . , n_i . If A is the matrix representation of T with respect to the basis B = $\{w_{11}, \ldots, w_{1n_1}, \ldots, w_{r1}, \ldots, w_{rn_r}\}$ for V, then since the i*th* column of A is just the image of the i*th* basis vector under T, we see that A must be of the block diagonal form

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & A_r \end{pmatrix}.$$

If this is not immediately clear, then a minute's thought should help, keeping in mind that each A_i is an n_i x n_i matrix, and A is an n x n matrix where $n = \sum_{i=1}^{r} n_i$. It is also helpful to think of the elements of B as being numbered from 1 to n rather than by the confusing double subscripts (also refer to the proof of Theorem 7.19).

The matrix A is called the **direct sum** of the matrices $A_1, \ldots, A_r$ and we write

$$A = A_1 \oplus \cdots \oplus A_r .$$

In this case we also say that the matrix A is **reducible**. Thus a representation [T] of T is reducible if there exists a basis for V in which [T] is block diagonal. (Some authors say that a representation is **reducible** if there exists a basis for V in which the matrix of T is triangular. In this case, if there exists a basis for V in which the matrix is block diagonal, then the representation is said to be **completely reducible**. We shall not follow this convention.) This discussion proves the following theorem.

Theorem 7.20 Suppose $T \in L(V)$ and assume that $V = W_1 \oplus \cdots \oplus W_r$ where each W_i is T-invariant. If A_i is the matrix representation of $T_i = T|W_i$, then the matrix representation of T is given by the matrix $A = A_1 \oplus \cdots \oplus A_r$.

Corollary Suppose $T \in L(V)$ and $V = W_1 \oplus \cdots \oplus W_r$ where each W_i is T-invariant. If $\Delta_T(x)$ is the characteristic polynomial for T and $\Delta_i(x)$ is the characteristic polynomial for $T_i = T|W_i$, then $\Delta_T(x) = \Delta_1(x) \cdots \Delta_r(x)$.

Proof See Exercise 7.5.4. ∎

Example 7.8 Referring to Example 2.8, consider the space $V = \mathbb{R}^3$. We write $V = W_1 \oplus W_2$ where $W_1 = \mathbb{R}^2$ (the xy-plane) and $W_2 = \mathbb{R}^1$ (the z-axis). Note that W_1 has basis vectors $w_{11} = (1, 0, 0)$ and $w_{12} = (0, 1, 0)$, and W_2 has basis vector $w_{21} = (0, 0, 1)$.

Now let $T \in L(V)$ be the linear operator that rotates any $v \in V$ counterclockwise by an angle θ about the z-axis. Then clearly both W_1 and W_2 are T-invariant. Letting $\{e_i\}$ be the standard basis for $\mathbb{R}^3$, we have $T_i = T|W_i$ and consequently (see Example 1.2),

$$\begin{aligned} T_1(e_1) &= T(e_1) = (\cos\theta)e_1 + (\sin\theta)e_2 \\ T_1(e_2) &= T(e_2) = (-\sin\theta)e_1 + (\cos\theta)e_2 \\ T_2(e_3) &= T(e_3) = e_3 \end{aligned}$$

Thus $V = W_1 \oplus W_2$ is a T-invariant direct sum decomposition of V, and T is the direct sum of T_1 and T_2. It should be clear that the matrix representation of T is given by

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which is just the direct sum of the matrix representations of T_1 and T_2. ∥

Exercises

1. Suppose $V = W_1 \oplus W_2$ and let $T_1: W_1 \to V$ and $T_2: W_2 \to V$ be linear. Show that $T = T_1 \oplus T_2$ is linear.

2. Prove Theorem 7.17.

3. Prove the corollary to Theorem 7.19.

4. Prove the corollary to Theorem 7.20.

5. Let V be a finite-dimensional inner product space over $\mathbb{C}$, and let G be a finite group. If for each $g \in G$ there is a $U(g) \in L(V)$ such that

   $$U(g_1)U(g_2) = U(g_1g_2)$$

   then the collection $U(G) = \{U(g)\}$ is said to form a **representation** of G. If W is a subspace of V with the property that $U(g)(W) \subset W$ for all $g \in$

G, then we will say that W is U(G)-**invariant** (or simply **invariant**). Furthermore, we say that U(G) is **irreducible** if there is no nontrivial U(G)-invariant subspace (i.e., the only invariant subspaces are {0} and V itself).

(a) Prove **Schur's lemma 1**: Let U(G) be an irreducible representation of G on V. If $A \in L(V)$ is such that $AU(g) = U(g)A$ for all $g \in G$, then $A = \lambda 1$ where $\lambda \in \mathbb{C}$. [*Hint*: Let λ be an eigenvalue of A with corresponding eigenspace V_λ. Show that V_λ is U(G)-invariant.]

(b) If $S \in L(V)$ is nonsingular, show that $U'(G) = SU(G)S^{-1}$ is also a representation of G on V. (Two representations of G related by such a similarity transformation are said to be **equivalent**.)

(c) Prove **Schur's lemma 2**: Let U(G) and U′(G) be two irreducible representations of G on V and V′ respectively, and suppose $A \in L(V', V)$ is such that $AU'(g) = U(g)A$ for all $g \in G$. Then either $A = 0$, or else A is an isomorphism of V′ onto V so that A^{-1} exists and U(G) is equivalent to U′(G). [*Hint*: Show that Im A is invariant under U(G), and that Ker A is invariant under U′(G).]

6. Suppose $A \in M_n(\mathcal{F})$ has minimal polynomial m_A and $B \in M_m(\mathcal{F})$ has minimal polynomial m_B. Let $m_{A\oplus B}$ be the minimal polynomial for $A \oplus B$ and let $p = \text{lcm}\{m_A, m_B\}$. Prove $m_{A\oplus B} = p$.

7. Let W be a T-invariant subspace of a finite-dimensional vector space V over $\mathcal{F}$, and suppose $v \in V$. Define the set

$$N_T(v, W) = \{f \in \mathcal{F}[x]: f(T)v \in W\} .$$

(a) Show that $N_T(v, W)$ is an ideal of $\mathcal{F}[x]$. This means that $N_T(v, W)$ has a unique monic generator $c_v(x)$ which is called the **T-conductor of** v **into** W.

(b) Show that every T-conductor divides the minimal polynomial m(x) for T.

(c) Now suppose the minimal polynomial for T is of the form

$$m(x) = (x - \lambda_1)^{n_1} \cdots (x - \lambda_r)^{n_r}$$

and let W be a proper T-invariant subspace of V. Prove there exists a vector $v \in V$ with $v \notin W$ such that $(T - \lambda 1)v \in W$ where λ is an eigenvalue of T. [*Hint*: Suppose $v_1 \in V$ with $v_1 \notin W$. Show that the T-conductor c_{v_1} of v_1 into W is of the form $c_{v_1}(x) = (x - \lambda)d(x)$. Now consider the vector $v = d(T)v_1$.]

8. Let V be finite-dimensional over $\mathcal{F}$ and suppose $T \in L(V)$. Prove there exists a basis for V in which the matrix representation A of T is upper-triangular if and only if the minimal polynomial for T is of the form $m(x) = (x - \lambda_1)^{n_1} \cdot \cdots \cdot (x - \lambda_r)^{n_r}$ where each $n_i \in \mathbb{Z}^+$ and the λ_i are the eigenvalues of T. [*Hint*: Apply part (c) of the previous problem to the basis $v_1, \ldots, v_n$ in which A is upper-triangular. Start with $W = \{0\}$ to get v_1, then consider the span of v_1 to get v_2, and continue this process.]

9. Relative to the standard basis for $\mathbb{R}^2$, let $T \in L(\mathbb{R}^2)$ be represented by

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

(a) Prove that the only T-invariant subspaces of $\mathbb{R}^2$ are $\{0\}$ and $\mathbb{R}^2$ itself.
(b) Suppose $U \in L(\mathbb{C}^2)$ is also represented by A. Show that there exist one-dimensional U-invariant subspaces.

10. Find all invariant subspaces over $\mathbb{R}$ of the operator represented by

$$A = \begin{pmatrix} 2 & -5 \\ 1 & -2 \end{pmatrix} .$$

11. (a) Suppose $T \in L(V)$, and let $v \in V$ be arbitrary. Define the set of vectors

$$Z(v, T) = \{f(T)(v): f \in \mathcal{F}[x]\} .$$

Show that Z(v, T) is a T-invariant subspace of V. (This is called the **T-cyclic subspace generated** by v.)
(b) Let v have minimal polynomial $m_v(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_r x + a_0$. Prove that Z(v, T) has a basis $\{v, Tv, \ldots, T^{r-1}v\}$, and hence also that $\dim Z(v, T) = \deg m_v(x)$. [*Hint*: Show that $T^k v$ is a linear combination of $\{v, Tv, \ldots, T^{r-1}v\}$ for every integer $k \geq r$.]
(c) Let $T \in L(\mathbb{R}^3)$ be represented in the standard basis by

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

If $v = e_1 - e_2$, find the minimal polynomial of v and a basis for Z(v, T). Extend this to a basis for $\mathbb{R}^3$, and show that the matrix of T relative to this basis is block triangular.

7.6 THE PRIMARY DECOMPOSITION THEOREM

We now proceed to show that there exists an important relationship between the minimal polynomial of a linear operator $T \in L(V)$ and the conditions under which V can be written as a direct sum of T-invariant subspaces of V. In the present context, this theorem (the primary decomposition theorem) is best obtained by first proving two relatively simple preliminary results.

Theorem 7.21 Suppose $T \in L(V)$ and assume that $f \in \mathcal{F}[x]$ is a polynomial such that $f(T) = 0$ and $f = h_1h_2$ where h_1 and h_2 are relatively prime. Define $W_1 = \text{Ker } h_1(T)$ and $W_2 = \text{Ker } h_2(T)$. Then W_1 and W_2 are T-invariant subspaces, and $V = W_1 \oplus W_2$.

Proof We first note that W_1 and W_2 are T-invariant subspaces according to Theorem 7.18. Next, since h_1 and h_2 are relatively prime, there exist polynomials g_1 and g_2 such that $g_1h_1 + g_2h_2 = 1$ (Theorem 6.5), and hence

$$g_1(T)h_1(T) + g_2(T)h_2(T) = 1 \quad . \tag{*}$$

Then for any $v \in V$ we have

$$g_1(T)h_1(T)(v) + g_2(T)h_2(T)(v) = v \quad .$$

However

$$\begin{aligned} h_2(T)g_1(T)h_1(T)(v) &= g_1(T)h_1(T)h_2(T)(v) \\ &= g_1(T)f(T)(v) \\ &= g_1(T)0(v) \\ &= 0 \end{aligned}$$

so that $g_1(T)h_1(T)(v) \in \text{Ker } h_2(T) = W_2$. Similarly, it is easy to see that $g_2(T)h_2(T)(v) \in W_1$, and hence $v \in W_1 + W_2$. This shows that $V = W_1 + W_2$, and it remains to be shown that this sum is direct.

To show that this sum is direct we use Theorem 2.14. In other words, if $v = w_1 + w_2$ where $w_i \in W_i$, then we must show that each w_i is uniquely determined by v. Applying $g_1(T)h_1(T)$ to $v = w_1 + w_2$ and using the fact that $h_1(T)(w_1) = 0$ we obtain

$$g_1(T)h_1(T)(v) = g_1(T)h_1(T)(w_2) .$$

Next, we apply (*) to w_2 and use the fact that $h_2(T)(w_2) = 0$ to obtain

$$g_1(T)h_1(T)(w_2) = w_2 .$$

Combining these last two equations shows that $w_2 = g_1(T)h_1(T)(v)$, and thus w_2 is uniquely determined by v (through the action of $g_1(T)h_1(T)$). We leave it to the reader to show in a similar manner that $w_1 = g_2(T)h_2(T)(v)$. Therefore $v = w_1 + w_2$ is a unique decomposition, and hence $V = W_1 \oplus W_2$. ∎

Theorem 7.22 Suppose $T \in L(V)$, and let $f = h_1h_2 \in \mathcal{F}[x]$ be the (monic) minimal polynomial for T, where h_1 and h_2 are relatively prime. If $W_i = \text{Ker } h_i(T)$, then h_i is the (monic) minimal polynomial for $T_i = T|W_i$.

Proof For each i = 1, 2 let m_i be the (monic) minimal polynomial for T_i. Since $W_i = \text{Ker } h_i(T)$, Theorem 7.17(a) tells us that $h_i(T_i) = 0$, and therefore (by Theorem 7.4) we must have $m_i|h_i$. This means that $m_i|f$ (since $f = h_1h_2$), and hence f is a multiple of m_1 and m_2. From the definition of least common multiple, it follows that the lcm of m_1 and m_2 must divide f. Since h_1 and h_2 are relatively prime, m_1 and m_2 must also be relatively prime (because if m_1 and m_2 had a common factor, then h_1 and h_2 would each also have this same common factor since $m_i|h_i$). But m_1 and m_2 are monic, and hence their greatest common divisor is 1. Therefore the lcm of m_1 and m_2 is just m_1m_2 (Theorem 6.9). This shows that $m_1m_2|f$.

On the other hand, since $V = W_1 \oplus W_2$ (Theorem 7.21), we see that for any $v \in V$

$$\begin{aligned}[m_1(T)m_2(T)](v) &= [m_1(T)m_2(T)](w_1 + w_2) \\ &= m_2(T)[m_1(T)(w_1)] + m_1(T)[m_2(T)(w_2)] \\ &= m_2(T)[m_1(T_1)(w_1)] + m_1(T)[m_2(T_2)(w_2)] \\ &= 0\end{aligned}$$

because m_i is the minimal polynomial for T_i. Therefore $(m_1m_2)(T) = 0$, and hence $f|m_1m_2$ (from Theorem 7.4 since, by hypothesis, f is the minimal polynomial for T). Combined with the fact that $m_1m_2|f$, this shows that $f = m_1m_2$ (since m_1, m_2 and f are monic). This result, along with the definition $f = h_1h_2$, the fact that h_1 and h_2 are monic, and the fact that $m_i|h_i$ shows that $m_i = h_i$. ∎

We are now in a position to prove the main result of this section.

Theorem 7.23 (**Primary Decomposition Theorem**) Suppose $T \in L(V)$ has minimal polynomial

$$m(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_r(x)^{n_r}$$

where each $f_i(x)$ is a distinct monic prime polynomial and each n_i is a positive integer. Let $W_i = \text{Ker } f_i(T)^{n_i}$, and define $T_i = T|W_i$. Then V is the direct sum of the T-invariant subspaces W_i, and $f_i(x)^{n_i}$ is the minimal polynomial for T_i.

Proof If $r = 1$ the theorem is trivial since $W_1 = \text{Ker } f_1(T)^{n_1} = \text{Ker } m(T) = V$. We now assume that the theorem has been proved for some $r - 1 \geq 1$, and proceed by induction to show that it is true for r. We first remark that the W_i are T-invariant subspaces by Theorem 7.18. Define the T-invariant subspace

$$U = \text{Ker}[f_2(T)^{n_2} \cdots f_r(T)^{n_r}] \ .$$

Because the $f_i(x)^{n_i}$ are relatively prime (by Corollary 2 of Theorem 6.5, since the $f_i(x)$ are all distinct primes), we can apply Theorem 7.21 to write $V = W_1 \oplus U$. In addition, since m(x) is the mini-mal polynomial for T, Theorem 7.22 tells us that $f_1(x)^{n_1}$ is the minimal polynomial for T_1, and $[f_2(x)^{n_2} \cdots f_r(x)^{n_r}]$ is the minimal polynomial for $T_U = T|U$.

Applying our induction hypothesis, we find that $U = W_2 \oplus \cdots \oplus W_r$ where for each $i = 2, \ldots, r$ we have $W_i = \text{Ker } f_i(T_U)^{n_i}$, and $f_i(x)^{n_i}$ is the minimal polynomial for $T_i = T_U|W_i$. However, it is obvious that $f_i(x)^{n_i}$ divides $[f_2(x)^{n_2} \cdots f_r(x)^{n_r}]$ for each $i = 2, \ldots, r$ and hence $\text{Ker } f_i(T)^{n_i} \subset U$. Specifically, this means that the set of all vectors $v \in V$ with the property that $f_i(T)^{n_i}(v) = 0$ are also in U, and therefore $\text{Ker } f_i(T)^{n_i} = \text{Ker } f_i(T_U)^{n_i} = W_i$. Furthermore, $T|W_i = T_U|W_i = T_i$ and thus $f_i(x)^{n_i}$ is also the minimal polynomial for $T|W_i$.

Summarizing, we have shown that $V = W_1 \oplus U = W_1 \oplus W_2 \oplus \cdots \oplus W_r$ where $W_i = \text{Ker } f_i(T)^{n_i}$ for each $i = 1, \ldots, r$ and $f_i(x)^{n_i}$ is the minimal polynomial for $T|W_i = T_i$. This completes the induction procedure and proves the theorem. ∎

In order to make this result somewhat more transparent, as well as in aiding actual calculations, we go back and look carefully at what we have done in defining the spaces $W_i = \text{Ker } f_i(T)^{n_i}$. For each $i = 1, \ldots, r$ we define the polynomials $g_i(x)$ by

$$m(x) = f_i(x)^{n_i} g_i(x) \ .$$

In other words, $g_i(x)$ is a product of the $r - 1$ factors $f_j(x)^{n_j}$ with $j \neq i$. We claim that in fact

$$W_i = g_i(T)(V) \ .$$

It is easy to see that $g_i(T)(V) \subset W_i$ because

$$f_i(T)^{n_i}[g_i(T)(v)] = [f_i(T)^{n_i}g_i(T)](v) = m(T)(v) = 0$$

for every $v \in V$. On the other hand, $f_i(x)^{n_i}$ and $g_i(x)$ are monic relative primes, and hence (by Theorem 6.5) there exist polynomials $a(x), b(x) \in \mathcal{F}[x]$ such that $a(x)f_i(x)^{n_i} + b(x)g_i(x) = 1$. Then for any $v_i \in W_i = \operatorname{Ker} f_i(T)^{n_i}$ we have $f_i(T)^{n_i}(v_i) = 0$, and hence

$$v_i = a(T)[f_i(T)^{n_i}(v_i)] + g_i(T)[b(T)(v_i)] = 0 + g_i(T)[b(T)(v_i)] \in g_i(T)(V) \ .$$

Hence $W_i \subset g_i(T)(V)$, and therefore $W_i = g_i(T)(V)$ as claimed. This gives us, at least conceptually, a practical method for computing the matrix of a linear transformation T with respect to the bases of the T-invariant subspaces.

As a final remark, note that for any $j \neq i$ we have $g_i(T)(W_j) = 0$ because $g_i(T)$ contains $f_j(T)^{n_j}$ and $W_j = \operatorname{Ker} f_j(T)^{n_j}$. In addition, since W_i is T-invariant we see that $g_i(T)(W_i) \subset W_i$. But we also have

$$\begin{aligned} W_i &= a(T)[f_i(T)^{n_i}(W_i)] + g_i(T)[b(T)(W_i)] \\ &= 0 + g_i(T)[b(T)(W_i)] \\ &\subset g_i(T)(W_i) \end{aligned}$$

and hence $g_i(T)(W_i) = W_i$. This should not be surprising for the following reason. If we write

$$V_i = W_1 \oplus \cdots \oplus W_{i-1} \oplus W_{i+1} \oplus \cdots \oplus W_r$$

then $g_i(T)(V_i) = 0$, and therefore

$$W_i = g_i(T)(V) = g_i(T)(W_i \oplus V_i) = g_i(T)(W_i) \ .$$

Example 7.9 Consider the space $V = \mathbb{R}^3$ with basis $\{u_1, u_2, u_3\}$ and define the linear transformation $T \in L(V)$ by

$$T(u_1) = u_2$$
$$T(u_2) = u_3$$
$$T(u_3) = -2u_1 + 3u_2 \ .$$

Then

$$T^2(u_1) = T(u_2) = u_3$$

and hence

$$T^3(u_1) = T(u_3) = -2u_1 + 3u_2 = -2u_1 + 3T(u_1) \ .$$

Therefore $T^3(u_1) - 3T(u_1) + 2u_1 = 0$ so that the minimal polynomial of u_1 is given by

$$m_1(x) = x^3 - 3x + 2 = (x - 1)^2(x + 2) \ .$$

Now recall that the minimal polynomial m(x) for T is just the least common multiple of the minimal polynomials $m_i(x)$ of the basis vectors for V, and deg $m(x) \leq \dim V = n$ (see the discussion prior to Example 7.6). Since $m_1(x)$ is written as a product of prime polynomials with deg $m_1 = 3 = \dim V$, it follows that $m(x) = m_1(x)$. We thus have $f_1(x)^{n_1} = (x - 1)^2$ and $f_2(x)^{n_2} = (x + 2)$.

We now define

$$W_1 = g_1(T)(V) = (T + 2)(V)$$

and

$$W_2 = g_2(T)(V) = (T - 1)^2(V) \ .$$

A simple calculation shows that

$$(T + 2)u_1 = 2u_1 + u_2$$
$$(T + 2)u_2 = 2u_2 + u_3$$
$$(T + 2)u_3 = -2u_1 + 3u_2 + 2u_3 = (T + 2)(-u_1 + 2u_2) \ .$$

Therefore W_1 is spanned by the basis vectors $\{2u_1 + u_2, 2u_2 + u_3\}$. Similarly, it is easy to show that $(T - 1)^2u_1 = u_1 - 2u_2 + u_3$ and that both $(T - 1)^2u_2$ and $(T - 1)^2 u_3$ are multiples of this. Hence $\{u_1 - 2u_2 + u_3\}$ is the basis vector for W_2.

We now see that $T_1 = T|W_1$ and $T_2 = T|W_2$ yield the transformations

$$T_1(2u_1 + u_2) = 2u_2 + u_3$$
$$T_1(2u_2 + u_3) = -2u_1 + 3u_2 + 2u_3 = -(2u_1 + u_2) + 2(2u_2 + u_3)$$
$$T_2(u_1 - 2u_2 + u_3) = -2(u_1 - 2u_2 + u_3)$$

and hence T_1 and T_2 are represented by the matrices A_1 and A_2, respectively, given by

$$A_1 = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} \qquad A_2 = (-2) \ .$$

Therefore $T = T_1 \oplus T_2$ is represented by the matrix $A = A_1 \oplus A_2$ where

$$A = \begin{pmatrix} \boxed{\begin{matrix} 0 & -1 \\ 1 & 2 \end{matrix}} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \end{matrix} & \boxed{-2} \end{pmatrix} . \ \textit{//}$$

From Corollary 1 of Theorem 7.14 we know that a matrix $A \in M_n(\mathcal{F})$ is diagonalizable if and only if A has n linearly independent eigenvectors, and from Theorem 7.13, the corresponding *distinct* eigenvalues $\lambda_1, \ldots, \lambda_r$ (where $r \leq n$) must be roots of the minimal polynomial for A. The factor theorem (corollary to Theorem 6.4) then says that $x - \lambda_i$ is a factor of the minimal polynomial for A, and hence the minimal polynomial for A must contain at least r distinct linear factors if A is to be diagonalizable.

We now show that the minimal polynomial of a diagonalizable linear transformation consists precisely of distinct linear factors.

Theorem 7.24 A linear transformation $T \in L(V)$ is diagonalizable if and only if the minimal polynomial m(x) for T is of the form

$$m(x) = (x - \lambda_1) \cdots (x - \lambda_r)$$

where $\lambda_1, \ldots, \lambda_r$ are the distinct eigenvalues of T.

Proof Suppose that $m(x) = (x - \lambda_1) \cdots (x - \lambda_r)$ where $\lambda_1, \ldots, \lambda_r \in \mathcal{F}$ are distinct. Then, according to Theorem 7.23, $V = W_1 \oplus \cdots \oplus W_r$ where $W_i = \text{Ker}(T - \lambda_i 1)$. But then for any $w \in W_i$ we have

$$0 = (T - \lambda_i 1)(w) = T(w) - \lambda_i w$$

and hence any $w \in W_i$ is an eigenvector of T with eigenvalue λ_i. It should be clear that any eigenvector of T with eigenvalue λ_i is also in W_i. In particular, this means that any basis vector of W_i is also an eigenvector of T. By Theorem 2.15, the union of the bases of all the W_i is a basis for V, and hence V has a basis consisting entirely of eigenvectors. This means that T is diagonalizable (Theorem 7.14).

On the other hand, assume that T is diagonalizable, and hence V has a basis $\{v_1, \ldots, v_n\}$ of eigenvectors of T that correspond to the (not necessarily

distinct) eigenvalues $\lambda_1, \ldots, \lambda_n$. If the v_i are numbered so that $\lambda_1, \ldots, \lambda_r$ are the *distinct* eigenvalues of T, then the operator

$$f(T) = (T - \lambda_1 1) \cdots (T - \lambda_r 1)$$

has the property that $f(T)(v_i) = 0$ for each of the basis eigenvectors $v_1, \ldots, v_n$. Thus $f(T) = 0$ and the minimal polynomial $m(x)$ for T must divide $f(x)$ (Theorem 7.4). While this shows that $m(x)$ must consist of linear factors, it is in fact also true that $f(x) = m(x)$. To see this, suppose that we delete any factor $T - \lambda_\alpha 1$ from $f(T)$ to obtain a new linear operator $f'(T)$. But the λ_i are all distinct so that $f'(T)(v_\alpha) \neq 0$, and hence $f'(T) \neq 0$. Therefore $f'(x)$ cannot be the minimal polynomial for T, and we must have $f(x) = m(x)$. ∎

In a manner similar to that used in Corollary 1 of Theorem 7.14, we can rephrase Theorem 7.24 in terms of matrices as follows.

Corollary 1 A matrix $A \in M_n(\mathcal{F})$ is similar to a diagonal matrix D if and only if the minimal polynomial for A has the form

$$m(x) = (x - \lambda_1) \cdots (x - \lambda_r)$$

where $\lambda_1, \ldots, \lambda_r \in \mathcal{F}$ are all distinct. If this is the case, then $D = P^{-1}AP$ where P is the invertible matrix whose columns are any set of n linearly independent eigenvectors $v_1, \ldots, v_n$ of A corresponding to the eigenvalues $\lambda_1, \ldots, \lambda_n$. (If $r < n$, then some of the eigenvalues will be repeated.) In addition, the diagonal elements of D are just the eigenvalues $\lambda_1, \ldots, \lambda_n$.

Corollary 2 A linear transformation $T \in L(V)$ is diagonalizable if and only if $V = W_1 \oplus \cdots \oplus W_r$ where $W_i = \text{Ker}(T - \lambda_i 1) = V_{\lambda_i}$.

Proof Recall that V_{λ_i} is the eigenspace corresponding to the eigenvalue λ_i, and the fact that $V_{\lambda_i} = \text{Ker}(T - \lambda_i 1)$ was shown in the proof of Theorem 7.24. If T is diagonalizable, then the conclusion that $V = W_1 \oplus \cdots \oplus W_r$ follows directly from Theorems 7.24 and 7.23. On the other hand, if $V = W_1 \oplus \cdots \oplus W_r$ then each W_i has a basis of eigenvectors and hence so does V (Theorem 2.15). ∎

It is important to realize that one eigenvalue can correspond to more than one linearly independent eigenvector (recall the comment following Theorem 7.8). This is why the spaces W_i in the first part of the proof of Theorem 7.24 can have bases consisting of more than one eigenvector. In particular, any eigenvalue of multiplicity greater than one can result in an eigenspace of

dimension greater than one, a result that we treat in more detail in the next section.

Exercises

1. Write each of the following linear transformations $T \in L(V)$ as a direct sum of linear transformations whose minimal polynomials are powers of prime polynomials:
   (a) $V = \mathbb{R}^2$: $Te_1 = e_2$, $Te_2 = 3e_1 + 2e_2$.
   (b) $V = \mathbb{R}^2$: $Te_1 = -4e_1 + 4e_2$, $Te_2 = e_2$.
   (c) $V = \mathbb{R}^3$: $Te_1 = e_2$, $Te_2 = e_3$, $Te_3 = 2e_1 - e_2 + 2e_3$.
   (d) $V = \mathbb{R}^3$: $Te_1 = 3e_1$, $Te_2 = e_2 - e_3$, $Te_3 = e_1 + 3e_2$.
   (e) $V = \mathbb{R}^3$: $Te_1 = 3e_1 + e_2$, $Te_2 = e_2 - 5e_3$, $Te_3 = 2e_1 + 2e_2 + 2e_3$.

2. Let V be finite-dimensional and suppose $T \in L(V)$ has minimal polynomial $m(x) = f_1(x)^{n_1} \cdots f_r(x)^{n_r}$ where the $f_i(x)$ are distinct monic primes and each $n_i \in \mathbb{Z}^+$. Show that the characteristic polynomial is of the form

$$\Delta(x) = f_1(x)^{d_1} \cdots f_r(x)^{d_r}$$

   where

$$d_i = \dim(\operatorname{Ker} f_i(T)^{n_i})/\deg f_i \ .$$

3. Let $\mathcal{D} = \{T_i\}$ be a collection of mutually commuting (i.e., $T_iT_j = T_jT_i$ for all i, j) diagonalizable linear operators on a finite-dimensional space V. Prove that there exists a basis for V relative to which the matrix representation of each T_i is diagonal. [*Hint*: Proceed by induction on dim V. Let $T \in \mathcal{D}$ ($T \neq c1$) have distinct eigenvalues $\lambda_1, \ldots, \lambda_r$ and for each i define $W_i = \operatorname{Ker}(T - \lambda_i 1)$. Show that W_i is invariant under each operator that commutes with T. Define $\mathcal{D}_i = \{T_j|W_i: T_j \in \mathcal{D}\}$ and show that every member of $\mathcal{D}_i$ is diagonalizable.]

7.7 MORE ON DIAGONALIZATION

If an operator $T \in L(V)$ is diagonalizable, then in a (suitably numbered) basis of eigenvectors, its matrix representation A will take the form

$$A = \begin{pmatrix} \lambda_1 I_{m_1} & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2 I_{m_2} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \lambda_r I_{m_r} \end{pmatrix}$$

where each λ_i is repeated m_i times and I_{m_i} is the m_i x m_i identity matrix. Note that $m_1 + \cdots + m_r$ must be equal to dim V. Thus the characteristic polynomial for T has the form

$$\Delta_T(x) = \det(xI - A) = (x - \lambda_1)^{m_1} \cdots (x - \lambda_r)^{m_r}$$

which is a product of (possibly repeated) *linear* factors. That the characteristic polynomial of a diagonalizable operator is of this form also follows directly from Theorems 7.24 and 7.12. However, we stress that just because the characteristic polynomial factors into a product of linear terms does not mean that the operator is diagonalizable. We now investigate the conditions that determine just when an operator will be diagonalizable.

Let us assume that T is diagonalizable, and hence that the characteristic polynomial factors into linear terms. For each distinct eigenvalue λ_i, we have seen that the corresponding eigenspace V_{λ_i} is just $\mathrm{Ker}(T - \lambda_i 1)$. Relative to a basis of eigenvectors, the matrix $[T - \lambda_i 1]$ is diagonal with precisely m_i zeros along its main diagonal (just look at the matrix A shown above and subtract off $\lambda_i I$). From Theorem 5.15 we know that the rank of a linear transformation is the same as the rank of its matrix representation, and hence $r(T - \lambda_i 1)$ is just the number of remaining nonzero rows in $[T - \lambda_i 1]$ which is dim V – m_i (see Theorem 3.9). But from Theorem 5.6 we then see that

$$\begin{aligned} \dim V_{\lambda_i} &= \dim \mathrm{Ker}(t - \lambda_i 1) = \mathrm{nul}(T - \lambda_i 1) = \dim V - \mathrm{r}(T - \lambda_i 1) \\ &= m_i \quad . \end{aligned}$$

In other words, if T is diagonalizable, then the dimension of each eigenspace V_{λ_i} is just the multiplicity of the eigenvalue λ_i. Let us clarify this in terms of some common terminology. In so doing, we will also repeat this conclusion from a slightly different viewpoint.

Given a linear operator $T \in L(V)$, what we have called the multiplicity of an eigenvalue λ is the largest positive integer m such that $(x - \lambda)^m$ divides the characteristic polynomial $\Delta_T(x)$. This is properly called the **algebraic multiplicity** of λ, in contrast to the **geometric multiplicity** which is the number of linearly independent eigenvectors belonging to that eigenvalue. In other words, the geometric multiplicity of λ is the dimension of V_λ . In general, we will use the word "multiplicity" to mean the algebraic multiplicity. The set of

all eigenvalues of a linear operator $T \in L(V)$ is called the **spectrum** of T. If some eigenvalue in the spectrum of T is of algebraic multiplicity > 1, then the spectrum is said to be **degenerate**.

If $T \in L(V)$ has an eigenvalue λ of algebraic multiplicity m, then it is not hard for us to show that the dimension of the eigenspace V_λ must be less than or equal to m. Note that since every element of V_λ is an eigenvector of T with eigenvalue λ, the space V_λ must be a T-invariant subspace of V. Furthermore, every basis for V_λ will obviously consist of eigenvectors corresponding to λ.

Theorem 7.25 Let $T \in L(V)$ have eigenvalue λ. Then the geometric multiplicity of λ is always less than or equal to its algebraic multiplicity. In other words, if λ has algebraic multiplicity m, then $\dim V_\lambda \leq m$.

Proof Suppose $\dim V_\lambda = r$ and let $\{v_1, \ldots, v_r\}$ be a basis for V_λ. By Theorem 2.10, we extend this to a basis $\{v_1, \ldots, v_n\}$ for V. Relative to this basis, T must have the matrix representation (see Theorem 7.19)

$$\begin{pmatrix} \lambda I_r & C \\ 0 & D \end{pmatrix}.$$

Applying Theorem 4.14 and the fact that the determinant of a diagonal matrix is just the product of its (diagonal) elements, we see that the characteristic polynomial $\Delta_T(x)$ of T is given by

$$\begin{aligned} \Delta_T(x) &= \begin{vmatrix} (x-\lambda)I_r & -C \\ 0 & xI_{n-r} - D \end{vmatrix} \\ &= \det[(x-\lambda)I_r]\det(xI_{n-r} - D) \\ &= (x-\lambda)^r \det(xI_{n-r} - D) \end{aligned}$$

which shows that $(x - \lambda)^r$ divides $\Delta_T(x)$. Since by definition m is the largest positive integer such that $(x - \lambda)^m | \Delta_T(x)$, it follows that $r \leq m$. ∎

Note that a special case of this theorem arises when an eigenvalue is of (algebraic) multiplicity 1. In this case, it then follows that the geometric and algebraic multiplicities are necessarily equal. We now proceed to show just when this will be true in general. Recall that any polynomial over an algebraically closed field will factor into linear terms (Theorem 6.13).

Theorem 7.26 Assume that $T \in L(V)$ has a characteristic polynomial that factors into (not necessarily distinct) linear terms. Let T have distinct eigenvalues $\lambda_1, \ldots, \lambda_r$ with (algebraic) multiplicities $m_1, \ldots, m_r$ respectively, and let dim $V_{\lambda_i} = d_i$. Then T is diagonalizable if and only if $m_i = d_i$ for each $i = 1, \ldots, r$.

Proof Let dim V = n. We note that since the characteristic polynomial of T is of degree n and factors into linear terms, it follows that $m_1 + \cdots + m_r = n$. We first assume that T is diagonalizable. By definition, this means that V has a basis consisting of n linearly independent eigenvectors of T. Since each of these basis eigenvectors must belong to at least one of the eigenspaces V_{λ_i}, it follows that $V = V_{\lambda_1} + \cdots + V_{\lambda_r}$ and consequently $n \leq d_1 + \cdots + d_r$. From Theorem 7.25 we know that $d_i \leq m_i$ for each $i = 1, \ldots, r$ and hence

$$n \leq d_1 + \cdots + d_r \leq m_1 + \cdots + m_r = n$$

which implies that $d_1 + \cdots + d_r = m_1 + \cdots + m_r$ or

$$(m_1 - d_1) + \cdots + (m_r - d_r) = 0 \ .$$

But each term in this equation is nonnegative (by Theorem 7.25), and hence we must have $m_i = d_i$ for each i.

Conversely, suppose that $d_i = m_i$ for each $i = 1, \ldots, r$. For each i, we know that any basis for V_{λ_i} consists of linearly independent eigenvectors corresponding to the eigenvalue λ_i, while by Theorem 7.8, we know that eigenvectors corresponding to distinct eigenvalues are linearly independent. Therefore the union $\mathcal{B}$ of the bases of $\{V_{\lambda_i}\}$ forms a linearly independent set of $d_1 + \cdots + d_r = m_1 + \cdots + m_r$ vectors. But $m_1 + \cdots + m_r = n = \dim V$, and hence $\mathcal{B}$ forms a basis for V. Since this shows that V has a basis of eigenvectors of T, it follows by definition that T must be diagonalizable. ∎

The following corollary is a repeat of Corollary 2 of Theorem 7.24. Its (very easy) proof may be based entirely on the material of this section.

Corollary 1 An operator $T \in L(V)$ is diagonalizable if and only if

$$V = W_1 \oplus \cdots \oplus W_r$$

where $W_1, \ldots, W_r$ are the eigenspaces corresponding to the distinct eigenvalues of T.

Proof This is Exercise 7.7.1. ∎

Using Theorem 5.6, we see that the geometric multiplicity of an eigenvalue λ is given by

$$\dim V_\lambda = \dim(\mathrm{Ker}(T - \lambda 1)) = \mathrm{nul}(T - \lambda 1) = \dim V - r(T - \lambda 1) .$$

This observation together with Theorem 7.26 proves the next corollary.

Corollary 2 An operator $T \in L(V)$ whose characteristic polynomial factors into linear terms is diagonalizable if and only if the algebraic multiplicity of λ is equal to $\dim V - r(T - \lambda 1)$ for each eigenvalue λ.

Example 7.10 Consider the operator $T \in L(\mathbb{R}^3)$ defined by

$$T(x, y, z) = (9x + y, 9y, 7z) .$$

Relative to the standard basis for $\mathbb{R}^3$, the matrix representation of T is given by

$$A = \begin{pmatrix} 9 & 1 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & 7 \end{pmatrix}$$

and hence the characteristic polynomial is

$$\Delta_A(x) = \det(A - \lambda I) = (9 - \lambda)^2(7 - \lambda)$$

which is a product of linear factors. However,

$$A - 9I = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

which clearly has rank 2, and hence $\mathrm{nul}(T - 9) = 3 - 2 = 1$ which is not the same as the algebraic multiplicity of $\lambda = 9$. Thus T is not diagonalizable. //

Example 7.11 Consider the operator on $\mathbb{R}^3$ defined by the following matrix:

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

In order to avoid factoring a cubic polynomial, we compute the characteristic polynomial $\Delta_A(x) = \det(xI - A)$ by applying Theorem 4.4 as follows (the reader should be able to see exactly what elementary row operations were performed in each step).

$$\begin{vmatrix} x-5 & 6 & 6 \\ 1 & x-4 & -2 \\ -3 & 6 & x+4 \end{vmatrix} = \begin{vmatrix} x-2 & 0 & -x+2 \\ 1 & x-4 & -2 \\ -3 & 6 & x+4 \end{vmatrix}$$

$$= (x-2)\begin{vmatrix} 1 & 0 & -1 \\ 1 & x-4 & -2 \\ -3 & 6 & x+4 \end{vmatrix}$$

$$= (x-2)\begin{vmatrix} 1 & 0 & -1 \\ 0 & x-4 & -1 \\ 0 & 6 & x+1 \end{vmatrix}$$

$$= (x-2)\begin{vmatrix} x-4 & -1 \\ 6 & x+1 \end{vmatrix}$$

$$= (x-2)^2(x-1) \ .$$

We now see that A has eigenvalue $\lambda_1 = 1$ with (algebraic) multiplicity 1, and eigenvalue $\lambda_2 = 2$ with (algebraic) multiplicity 2. From Theorem 7.25 we know that the algebraic and geometric multiplicities of λ_1 are necessarily the same and equal to 1, so we need only consider λ_2. Observing that

$$A - 2I = \begin{pmatrix} 3 & -6 & -6 \\ -1 & 2 & 2 \\ 3 & -6 & -6 \end{pmatrix}$$

it is obvious that $r(A - 2I) = 1$, and hence $\text{nul}(A - 2I) = 3 - 1 = 2$. This shows that A is indeed diagonalizable.

Let us now construct bases for the eigenspaces $W_i = V_{\lambda_i}$. This means that we seek vectors $v = (x, y, z) \in \mathbb{R}^3$ such that $(A - \lambda_i I)v = 0$. This is easily solved by the usual row reduction techniques as follows. For $\lambda_1 = 1$ we have

$$A - I = \begin{pmatrix} 4 & -6 & -6 \\ -1 & 3 & 2 \\ 3 & -6 & -5 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & -1 \\ -1 & 3 & 2 \\ 3 & -6 & -5 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & -1 \\ 0 & 3 & 1 \\ 0 & -6 & -2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & -1 \\ 0 & 3 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

which has the solutions x = z and y = −z/3 = −x/3. Therefore W_1 is spanned by the single eigenvector $v_1 = (3, -1, 3)$. As to $\lambda_2 = 2$, we proceed in a similar manner to obtain

$$A - 2I = \begin{pmatrix} 3 & -6 & -6 \\ -1 & 2 & 2 \\ 3 & -6 & -6 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -2 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

which implies that any vector (x, y, z) with x = 2y + 2z will work. For example, we can let x = 0 and y = 1 to obtain z = −1, and hence one basis vector for W_2 is given by $v_2 = (0, 1, -1)$. If we let x = 1 and y = 0, then we have z = 1/2 so that another independent basis vector for W_2 is given by $v_3 = (2, 0, 1)$. In terms of these eigenvectors, the transformation matrix P that diagonalizes A is given by

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

and we leave it to the reader to verify that AP = PD (i.e., $P^{-1}AP = D$) where D is the diagonal matrix with diagonal elements $d_{11} = 1$ and $d_{22} = d_{33} = 2$.

Finally, we note that since A is diagonalizable, Theorems 7.12 and 7.24 show that the minimal polynomial for A must be (x − 1)(x − 2). //

Exercises

1. Prove Corollary 1 of Theorem 7.26.

2. Show that two similar matrices A and B have the same eigenvalues, and these eigenvalues have the same geometric multiplicities.

3. Let $\lambda_1, \ldots, \lambda_r \in \mathcal{F}$ be distinct, and let $D \in M_n(\mathcal{F})$ be diagonal with a characteristic polynomial of the form

$$\Delta_D(x) = (x - \lambda_1)^{d_1} \cdots (x - \lambda_r)^{d_r} .$$

   Let V be the space of all n x n matrices B that commute with D, i.e., the set of all B such that BD = DB. Prove that $\dim V = d_1^2 + \cdots + d_r^2$.

4. Relative to the standard basis, let $T \in L(\mathbb{R}^4)$ be represented by

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \end{pmatrix}.$$

Find conditions on a, b and c such that T is diagonalizable.

5. Determine whether or not each of the following matrices is diagonalizable. If it is, find a nonsingular matrix P and a diagonal matrix D such that $P^{-1}AP = D$.

$$(a)\ \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{pmatrix} \qquad (b)\ \begin{pmatrix} 3 & -1 & -2 \\ 2 & 0 & -2 \\ 2 & -1 & -1 \end{pmatrix} \qquad (c)\ \begin{pmatrix} -1 & 1 & 0 \\ 0 & 5 & 0 \\ 4 & -2 & 5 \end{pmatrix}$$

$$(d)\ \begin{pmatrix} -1 & -3 & -9 \\ 0 & 5 & 18 \\ 0 & -2 & -7 \end{pmatrix} \qquad (e)\ \begin{pmatrix} 7 & -4 & 0 \\ 8 & -5 & 0 \\ 6 & -6 & 3 \end{pmatrix} \qquad (f)\ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$(g)\ \begin{pmatrix} 3 & 1 & 1 \\ 2 & 4 & 2 \\ -1 & -1 & 1 \end{pmatrix}$$

6. Determine whether or not each of the following operators $T \in L(\mathbb{R}^3)$ is diagonalizable. If it is, find an eigenvector basis for $\mathbb{R}^3$ such that [T] is diagonal.
   (a) T(x, y, z) = (−y, x, 3z).
   (b) T(x, y, z) = (8x + 2y − 2z, 3x + 3y − z, 24x + 8y − 6z).
   (c) T(x, y, z) = (4x + z, 2x + 3y + 2z, x + 4z).
   (d) T(x, y, z) = (−2y − 3z, x + 3y + 3z, z).

7. Suppose a matrix A is diagonalizable. Prove that A^m is diagonalizable for any positive integer m.

8. Summarize several of our results by proving the following theorem:

Let V be finite-dimensional, suppose $T \in L(V)$ has distinct eigenvalues $\lambda_1, \ldots, \lambda_r$, and let $W_i = \mathrm{Ker}(T - \lambda_i 1)$. Then the following are equivalent:
(a) T is diagonalizable.
(b) $\Delta_T(x) = (x - \lambda_1)^{m_1} \cdots (x - \lambda_r)^{m_r}$ and W_i is of dimension m_i for each $i = 1, \ldots, r$.
(c) $\dim W_1 + \cdots + \dim W_r = \dim V$.

9. Let V_3 be the space of real polynomials of degree at most 3, and let f' and f'' denote the first and second derivatives of $f \in V$. Define $T \in L(V_3)$ by $T(f) = f' + f''$. Decide whether or not T is diagonalizable, and if it is, find a basis for V_3 such that [T] is diagonal.

10. (a) Let V_2 be the space of real polynomials of degree at most 2, and define $T \in L(V_2)$ by $T(ax^2 + bx + c) = cx^2 + bx + a$. Decide whether or not T is diagonalizable, and if it is, find a basis for V_2 such that [T] is diagonal.
(b) Repeat part (a) with $T = (x + 1)(d/dx)$. (See Exercise 7.3.17.)

7.8 PROJECTIONS

In this section we introduce the concept of projection operators and show how they may be related to direct sum decompositions where each of the subspaces in the direct sum is invariant under some linear operator.

Suppose that U and W are subspaces of a vector space V with the property that $V = U \oplus W$. Then every $v \in V$ has a unique representation of the form $v = u + w$ where $u \in U$ and $w \in W$ (Theorem 2.14). We now define the mapping $E: V \to V$ by $Ev = u$. Note that E is well-defined since the direct sum decomposition is unique. Moreover, given any other $v' \in V = U \oplus W$ with $v' = u' + w'$, we know that $v + v' = (u + u') + (w + w')$ and $kv = ku + kw$, and hence it is easy to see that E is in fact linear because

$$E(v + v') = u + u' = Ev + Ev'$$

and

$$E(kv) = ku = k(Ev) .$$

The linear operator $E \in L(V)$ is called the **projection of** V **on** U **in the direction of** W. Furthermore, since any $u \in U \subset V$ may be written in the form $u = u + 0$, we also see that $Eu = u$ and therefore

$$E^2 v = E(Ev) = Eu = u = Ev .$$

In other words, a projection operator E has the property that $E^2 = E$. By way of terminology, any operator $T \in L(V)$ with the property that $T^2 = T$ is said to be **idempotent**.

On the other hand, given a vector space V, suppose we have an operator $E \in L(V)$ with the property that $E^2 = E$. We claim that $V = \text{Im } E \oplus \text{Ker } E$. Indeed, first note that if $u \in \text{Im } E$, then by definition this means there exists $v \in V$ with the property that $Ev = u$. It therefore follows that

$$Eu = E(Ev) = E^2v = Ev = u$$

and thus $Eu = u$ for any $u \in \text{Im } E$. Conversely, the equation $Eu = u$ obviously says that $u \in \text{Im } E$, and hence we see that $u \in \text{Im } E$ if and only if $Eu = u$.

Next, note that given any $v \in V$ we may clearly write

$$v = Ev + v - Ev = Ev + (1 - E)v$$

where by definition, $Ev \in \text{Im } E$. Since

$$E[(1 - E)v] = (E - E^2)v = (E - E)v = 0$$

we see that $(1 - E)v \in \text{Ker } E$, and hence $V = \text{Im } E + \text{Ker } E$. We claim that this sum is in fact direct. To see this, let $w \in \text{Im } E \cap \text{Ker } E$. Since $w \in \text{Im } E$ and $E^2 = E$, we have seen that $Ew = w$, while the fact that $w \in \text{Ker } E$ means that $Ew = 0$. Therefore $w = 0$ so that $\text{Im } E \cap \text{Ker } E = \{0\}$, and hence

$$V = \text{Im } E \oplus \text{Ker } E \ .$$

Since we have now shown that any $v \in V$ may be written in the unique form $v = u + w$ with $u \in \text{Im } E$ and $w \in \text{Ker } E$, it follows that $Ev = Eu + Ew = u + 0 = u$ so that E is the projection of V on Im E in the direction of Ker E.

It is also of use to note that

$$\text{Ker } E = \text{Im}(1 - E)$$

and

$$\text{Ker}(1 - E) = \text{Im } E \ .$$

To see this, suppose $w \in \text{Ker } E$. Then

$$w = Ew + (1 - E)w = (1 - E)w$$

which implies that $w \in \text{Im}(1 - E)$, and hence $\text{Ker } E \subset \text{Im}(1 - E)$. On the other hand, if $w \in \text{Im}(1 - E)$ then there exists $w' \in V$ such that $w = (1 - E)w'$ and hence

$$Ew = (E - E^2)w' = (E - E)w' = 0$$

so that $w \in \text{Ker } E$. This shows that $\text{Im}(1 - E) \subset \text{Ker } E$, and therefore $\text{Ker } E = \text{Im}(1 - E)$. The similar proof that $\text{Ker}(1 - E) = \text{Im } E$ is left as an exercise for the reader (Exercise 7.8.1).

Theorem 7.27 Let V be a vector space with $\dim V = n$, and suppose $E \in L(V)$ has rank $k = \dim(\text{Im } E)$. Then E is idempotent (i.e., $E^2 = E$) if and only if any one of the following statements is true:
(a) If $v \in \text{Im } E$, then $Ev = v$.
(b) $V = \text{Im } E \oplus \text{Ker } E$ and E is the projection of V on $\text{Im } E$ in the direction of $\text{Ker } E$.
(c) $\text{Im } E = \text{Ker}(1 - E)$ and $\text{Ker } E = \text{Im}(1 - E)$.
(d) It is possible to choose a basis for V such that $[E] = I_k \oplus 0_{n-k}$.

Proof Suppose $E^2 = E$. In view of the above discussion, all that remains is to prove part (d). Applying part (b), we let $\{e_1, \ldots, e_k\}$ be a basis for $\text{Im } E$ and $\{e_{k+1}, \ldots, e_n\}$ be a basis for $\text{Ker } E$. By part (a), we know that $Ee_i = e_i$ for $i = 1, \ldots, k$, and by definition of $\text{Ker } E$, we have $Ee_i = 0$ for $i = k + 1, \ldots, n$. But then $[E]$ has the desired form since the i*th* column of $[E]$ is just Ee_i.

Conversely, suppose (a) is true and $v \in V$ is arbitrary. Then $E^2v = E(Ev) = Ev$ implies that $E^2 = E$. Now suppose that (b) is true and $v \in V$. Then $v = u + w$ where $u \in \text{Im } E$ and $w \in \text{Ker } E$. Therefore $Ev = Eu + Ew = Eu = u$ (by definition of projection) and $E^2v = E^2u = Eu = u$ so that $E^2v = Ev$ for all $v \in V$, and hence $E^2 = E$. If (c) holds and $v \in V$, then $Ev \in \text{Im } E = \text{Ker}(1 - E)$ so that $0 = (1 - E)Ev = Ev - E^2v$ and hence $E^2v = Ev$ again. Similarly, $(1 - E)v \in \text{Im}(1 - E) = \text{Ker } E$ so that $0 = E(1 - E)v = Ev - E^2v$ and hence $E^2v = Ev$. In either case, we have $E^2 = E$. Finally, from the form of $[E]$ given in (d), it is obvious that $E^2 = E$. ∎

It is also worth making the following observation. If we are given a vector space V and a subspace $W \subset V$, then there may be many subspaces $U \subset V$ with the property that $V = U \oplus W$. For example, the space $\mathbb{R}^3$ is not necessarily represented by the usual orthogonal Cartesian coordinate system. Rather, it may be viewed as consisting of a line plus any (oblique) plane not containing the given line. However, in the particular case that $V = W \oplus W^\perp$, then $W^\perp$ is uniquely specified by W (see Section 2.5). In this case, the projection $E \in L(V)$ defined by $Ev = w$ with $w \in W$ is called the **orthogonal projection** of V

on W. In other words, E is an orthogonal projection if $(\text{Im } E)^\perp = \text{Ker } E$. By the corollary to Theorem 2.22, this is equivalent to the requirement that $(\text{Ker } E)^\perp = \text{Im } E$.

It is not hard to generalize these results to the direct sum of more than two subspaces. Indeed, suppose that we have a vector space V such that $V = W_1 \oplus \cdots \oplus W_r$. Since any $v \in V$ has the unique representation as $v = w_1 + \cdots + w_r$ with $w_i \in W_i$, we may define for each $j = 1, \ldots, r$ the operator $E_j \in L(V)$ by $E_j v = w_j$. That each E_j is in fact linear is easily shown exactly as above for the simpler case. It should also be clear that $\text{Im } E_j = W_j$ (see Exercise 7.8.2). If we write

$$w_j = 0 + \cdots + 0 + w_j + 0 + \cdots + 0$$

as the unique expression for $w_j \in W_j \subset V$, then we see that $E_j w_j = w_j$, and hence for any $v \in V$ we have

$$E_j^2 v = E_j(E_j v) = E_j w_j = w_j = E_j v$$

so that $E_j^2 = E_j$.

The representation of each w_j as $E_j v$ is very useful because we may write any $v \in V$ as

$$v = w_1 + \cdots + w_r = E_1 v + \cdots + E_r v = (E_1 + \cdots + E_r)v$$

and thus we see that $E_1 + \cdots + E_r = 1$. Furthermore, since the image of E_j is W_j, it follows that if $E_j v = 0$ then $w_j = 0$, and hence

$$\text{Ker } E_j = W_1 \oplus \cdots \oplus W_{j-1} \oplus W_{j+1} \oplus \cdots \oplus W_r \ .$$

We then see that for any $j = 1, \ldots, r$ we have $V = \text{Im } E_j \oplus \text{Ker } E_j$ exactly as before. It is also easy to see that $E_i E_j = 0$ if $i \neq j$ because $\text{Im } E_j = W_j \subset \text{Ker } E_i$.

Theorem 7.28 Let V be a vector space, and suppose that $V = W_1 \oplus \cdots \oplus W_r$. Then for each $j = 1, \ldots, r$ there exists a linear operator $E_j \in L(V)$ with the following properties:

(a) $1 = E_1 + \cdots + E_r$.

(b) $E_i E_j = 0$ if $i \neq j$.

(c) $E_j^2 = E_j$.

(d) $\text{Im } E_j = W_j$.

Conversely, if $\{E_1, \ldots, E_r\}$ are linear operators on V that obey properties (a) and (b), then each E_j is idempotent and $V = W_1 \oplus \cdots \oplus W_r$ where $W_j = \text{Im } E_j$.

Proof In view of the previous discussion, we only need to prove the converse statement. From (a) and (b) we see that

$$E_j = E_j 1 = E_j(E_1 + \cdots + E_r) = E_j^2 + \Sigma_{i \neq j} E_j E_i = E_j^2$$

which shows that each E_j is idempotent. Next, property (a) shows us that for any $v \in V$ we have

$$v = 1v = E_1 v + \cdots + E_r v$$

and hence $V = W_1 + \cdots + W_r$ where we have defined $W_j = \text{Im } E_j$. Now suppose that $0 = w_1 + \cdots + w_r$ where each $w_j \in W_j$. If we can show that this implies $w_1 = \cdots = w_r = 0$, then any $v \in V$ will have a unique representation $v = v_1 + \cdots + v_r$ with $v_i \in W_i$. This is because if

$$v = v_1 + \cdots + v_r = v_1' + \cdots + v_r'$$

then

$$(v_1 - v_1') + \cdots + (v_r - v_r') = 0$$

would imply that $v_i - v_i' = 0$ for each i, and thus $v_i = v_i'$. Hence it will follow that $V = W_1 \oplus \cdots \oplus W_r$ (Theorem 2.14).

Since $w_1 + \cdots + w_r = 0$, it is obvious that $E_j(w_1 + \cdots + w_r) = 0$. However, note that $E_j w_i = 0$ if $i \neq j$ (because $w_i \in \text{Im } E_i$ and $E_j E_i = 0$), while $E_j w_j = w_j$ (since $w_j = E_j w'$ for some $w' \in V$ and hence $E_j w_j = E_j^2 w' = E_j w' = w_j$). This shows that $w_1 = \cdots = w_r = 0$ as desired. ∎

We now turn our attention to invariant direct sum decompositions, referring to Section 7.5 for notation. We saw in Corollary 1 of Theorem 7.26 that a diagonalizable operator $T \in L(V)$ leads to a direct sum decomposition of V in terms of the eigenspaces of T. However, Theorem 7.28 shows us that such a decomposition should lead to a collection of projections on these eigenspaces. Our next theorem elaborates on this observation in detail. Before stating and proving this result however, let us take another look at a matrix that has been diagonalized. We observe that a diagonal matrix of the form

$$A = \begin{pmatrix} \lambda_1 I_{m_1} & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2 I_{m_2} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \lambda_r I_{m_r} \end{pmatrix}$$

can also be written as

$$A = \lambda_1 \begin{pmatrix} I_{m_1} & & & \\ & 0_{m_2} & & \\ & & \ddots & \\ & & & 0_{m_r} \end{pmatrix} + \lambda_2 \begin{pmatrix} 0_{m_1} & & & \\ & I_{m_2} & & \\ & & \ddots & \\ & & & 0_{m_r} \end{pmatrix} + \cdots + \lambda_r \begin{pmatrix} 0_{m_1} & & & \\ & 0_{m_2} & & \\ & & \ddots & \\ & & & I_{m_r} \end{pmatrix} .$$

If we define E_i to be the matrix obtained from A by setting $\lambda_i = 1$ and $\lambda_j = 0$ for each $j \neq i$ (i.e., the i*th* matrix in the above expression), then this may be written in the simple form

$$A = \lambda_1 E_1 + \lambda_2 E_2 + \cdots + \lambda_r E_r$$

where clearly

$$I = E_1 + E_2 + \cdots + E_r \quad .$$

Furthermore, it is easy to see that the matrices E_i have the property that

$$E_i E_j = 0 \text{ if } i \neq j$$

and

$$E_i^2 = E_i \neq 0 \quad .$$

With these observations in mind, we now prove this result in general.

Theorem 7.29 If $T \in L(V)$ is a diagonalizable operator with distinct eigenvalues $\lambda_1, \ldots, \lambda_r$, then there exist linear operators $E_1, \ldots, E_r$ in L(V) such that:

(a) $1 = E_1 + \cdots + E_r$.
(b) $E_i E_j = 0$ if $i \neq j$.
(c) $T = \lambda_1 E_1 + \cdots + \lambda_r E_r$.
(d) $E_j^2 = E_j$.
(e) $\operatorname{Im} E_j = W_j$ where $W_j = \operatorname{Ker}(T - \lambda_j 1)$ is the eigenspace corresponding to λ_j.

Conversely, if there exist distinct scalars $\lambda_1, \ldots, \lambda_r$ and distinct nonzero linear operators $E_1, \ldots, E_r$ satisfying properties (a), (b) and (c), then properties (d) and (e) are also satisfied, and T is diagonalizable with $\lambda_1, \ldots, \lambda_r$ as its distinct eigenvalues.

Proof First assume T is diagonalizable with distinct eigenvalues $\lambda_1, \ldots, \lambda_r$ and let $W_1, \ldots, W_r$ be the corresponding eigenspaces. By Corollary 1 of Theorem 7.26 we know that $V = W_1 \oplus \cdots \oplus W_r$. (Note that we do not base this result on Theorem 7.24, and hence the present theorem does not depend in any way on the primary decomposition theorem.) Then Theorem 7.28 shows the existence of the projection operators $E_1, \ldots, E_r$ satisfying properties (a),

(b), (d) and (e). As to property (c), we see (by property (a)) that for any $v \in V$ we have $v = E_1 v + \cdots + E_r v$. Since $E_j v \in W_j$, we know from the definition of eigenspace that $T(E_j v) = \lambda_j(E_j v)$, and therefore

$$\begin{aligned} Tv &= T(E_1 v) + \cdots + T(E_r v) \\ &= \lambda_1(E_1 v) + \cdots + \lambda_r(E_r v) \\ &= (\lambda_1 E_1 + \cdots + \lambda_r E_r)v \end{aligned}$$

which verifies property (c).

Now suppose that we are given a linear operator $T \in L(V)$ together with distinct scalars $\lambda_1, \ldots, \lambda_r$ and (nonzero) linear operators $E_1, \ldots, E_r$ that obey properties (a), (b) and (c). Multiplying (a) by E_i and using (b) proves (d). Now multiply (c) from the right by E_i and use property (b) to obtain $TE_i = \lambda_i E_i$ or $(T - \lambda_i 1)E_i = 0$. If $w_i \in \operatorname{Im} E_i$ is arbitrary, then $w_i = E_i w_i'$ for some $w_i' \in V$ and hence $(T - \lambda_i 1)w_i = (T - \lambda_i 1)E_i w_i' = 0$ which shows that $w_i \in \operatorname{Ker}(T - \lambda_i 1)$. Since $E_i \neq 0$, this shows the existence of a nonzero vector $w_i \in \operatorname{Ker}(T - \lambda_i 1)$ with the property that $Tw_i = \lambda_i w_i$. This proves that each λ_i is an eigenvalue of T. We claim that there are no other eigenvalues of T other than $\{\lambda_i\}$. To see this, let α be any scalar and assume that $(T - \alpha 1)v = 0$ for some nonzero $v \in V$. Using properties (a) and (c), we see that

$$T - \alpha 1 = (\lambda_1 - \alpha)E_1 + \cdots + (\lambda_r - \alpha)E_r$$

and hence letting both sides of this equation act on v yields

$$0 = (\lambda_1 - \alpha)E_1 v + \cdots + (\lambda_r - \alpha)E_r v \ .$$

Multiplying this last equation from the left by E_i and using properties (b) and (d), we then see that $(\lambda_i - \alpha)E_i v = 0$ for every $i = 1, \ldots, r$. Since $v \neq 0$ may be written as $v = E_1 v + \cdots + E_r v$, it must be true that $E_j v \neq 0$ for some j, and hence in this case we have $\lambda_j - \alpha = 0$ or $\alpha = \lambda_j$.

We must still show that T is diagonalizable, and that $\operatorname{Im} E_i = \operatorname{Ker}(T - \lambda_i 1)$. It was shown in the previous paragraph that any nonzero $w_j \in \operatorname{Im} E_j$ satisfies $Tw_j = \lambda_j w_j$, and hence any nonzero vector in the image of any E_i is an eigenvector of E_i. Note this says that $\operatorname{Im} E_i \subset \operatorname{Ker}(T - \lambda_i 1)$. Using property (a), we see that any $w \in V$ may be written as $w = E_1 w + \cdots + E_r w$ which shows that V is spanned by eigenvectors of T. But this is just what we mean when we say that T is diagonalizable. Finally, suppose $w_i \in \operatorname{Ker}(T - \lambda_i 1)$ is arbitrary. Then $(T - \lambda_i 1)w_i = 0$ and hence (exactly as we showed above)

$$0 = (\lambda_1 - \lambda_i)E_1 w_i + \cdots + (\lambda_r - \lambda_i)E_r w_i \ .$$

Thus for each $j = 1, \ldots, r$ we have

$$0 = (\lambda_j - \lambda_i)E_j w_i$$

which implies $E_j w_i = 0$ for $j \neq i$. Since $w_i = E_1 w_i + \cdots + E_r w_i$ while $E_j w_i = 0$ for $j \neq i$, we conclude that $w_i = E_i w_i$ which shows that $w_i \in \operatorname{Im} E_i$. In other words, we have also shown that $\operatorname{Ker}(T - \lambda_i 1) \subset \operatorname{Im} E_i$. Together with our earlier result, this proves that $\operatorname{Im} E_i = \operatorname{Ker}(T - \lambda_i 1)$. ∎

Exercises

1. (a) Let E be an idempotent linear operator. Show that $\operatorname{Ker}(1 - E) = \operatorname{Im} E$.
   (b) If $E^2 = E$, show that $(1 - E)^2 = 1 - E$.

2. Let $V = W_1 \oplus \cdots \oplus W_r$ and suppose $v = w_1 + \cdots + w_r \in V$. For each $j = 1, \ldots, r$ we define the operator E_j on V by $E_j v = w_j$.
   (a) Show that $E_j \in L(V)$.
   (b) Show that $\operatorname{Im} E_j = W_j$.

3. Give a completely independent proof of Theorem 7.24 as follows:
   (a) Let $T \in L(V)$ be diagonalizable with decomposition $T = \lambda_1 E_1 + \cdots + \lambda_r E_r$. Show that $f(T) = f(\lambda_1)E_1 + \cdots + f(\lambda_r)E_r$ for any $f(x) \in \mathcal{F}[x]$.
   (b) Use part (a) to conclude that the minimal polynomial for T must be of the form $m(x) = (x - \lambda_1) \cdots (x - \lambda_r)$.
   (c) Now suppose $T \in L(V)$ has minimal polynomial

   $$m(x) = (x - \lambda_1) \cdots (x - \lambda_r)$$

   where $\lambda_1, \ldots, \lambda_r \in \mathcal{F}$ are distinct. Define the polynomials

   $$p_j(x) = \prod_{i \neq j} \left(\frac{x - \lambda_i}{\lambda_j - \lambda_i} \right) .$$

   Note that $\deg p_j = r - 1 < \deg m$. By Exercise 6.4.2, any polynomial f of degree $\leq r - 1$ can be written as $f = \sum_j f(\lambda_j)p_j$. Defining $E_j = p_j(T)$, show that $E_j \neq 0$ and that

   $$1 = E_1 + \cdots + E_r$$

   and

   $$T = \lambda_1 E_1 + \cdots + \lambda_r E_r \ .$$

(d) Show that $m|p_i p_j$ for $i \neq j$, and hence show that $E_i E_j = 0$ for $i \neq j$.
(e) Conclude that T is diagonalizable.

4. Let $E_1, \ldots, E_r$ and $W_1, \ldots, W_r$ be as defined in Theorem 7.28, and suppose $T \in L(V)$.
(a) If $TE_i = E_i T$ for every E_i, prove that every $W_j = \text{Im } E_j$ is T-invariant.
(b) If every W_j is T-invariant, prove that $TE_i = E_i T$ for every E_i. [*Hint*: Let $v \in V$ be arbitrary. Show that property (a) of Theorem 7.28 implies $T(E_i v) = w_i$ for some $w_i \in W_i = \text{Im } E_i$. Now show that $E_j(TE_i)v = (E_i w_i)\delta_{ij}$, and hence that $E_j(Tv) = T(E_j v)$.]

5. Prove that property (e) in Theorem 7.29 holds for the matrices E_i given prior to the theorem.

6. Let W be a finite-dimensional subspace of an inner product space V.
(a) Show that there exists precisely one orthogonal projection on W.
(b) Let E be the orthogonal projection on W. Show that for any $v \in V$ we have $\|v - Ev\| \leq \|v - w\|$ for every $w \in W$. In other words, show that Ev is the unique element of W that is "closest" to v.

7.9 QUOTIENT SPACES

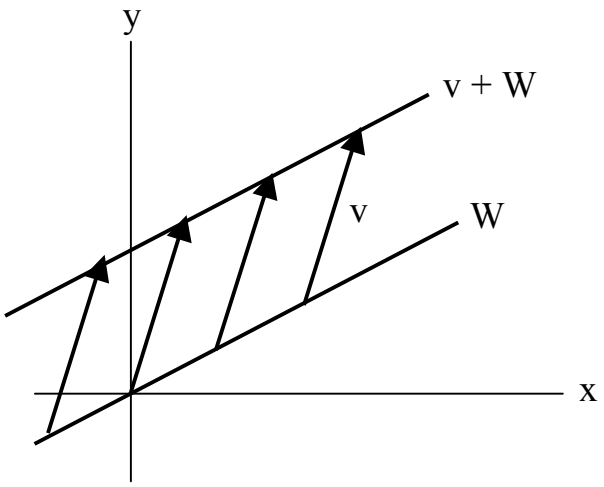
Recall that in Section 1.5 we gave a brief description of normal subgroups and quotient groups (see Theorem 1.12). In this section we elaborate on and apply this concept to vector spaces, which are themselves abelian groups. In the next section we will apply this formalism to proving the triangular form theorem for linear operators.

Let V be a vector space and W a subspace of V. Since W is an abelian subgroup of V, it is easy to see that W is just a normal subgroup since for any $w \in W$ and $v \in V$ we have $v + w + (-v) = w \in W$ (remember that group multiplication in an abelian group is frequently denoted by the usual addition sign, and the inverse of an element v is just $-v$). We may therefore define the quotient group V/W whose elements, $v + W$ for any $v \in V$, are just the cosets of W in V. It should be obvious that V/W is also an abelian group. In fact, we will show below that V/W can easily be made into a vector space.

Example 7.12 Let $V = \mathbb{R}^2$ and suppose

$$W = \{(x, y) \in \mathbb{R}^2 : y = mx \text{ for some fixed scalar } m\} .$$

In other words, W is just a line through the origin in the plane $\mathbb{R}^2$. The elements of V/W are the cosets $v + W = \{v + w: w \in W\}$ where v is any vector in V.



Therefore, the set V/W consists of all lines in $\mathbb{R}^2$ that are parallel to W (i.e., that are displaced from W by the vector v). //

While we proved in Section 1.5 that cosets partition a group into disjoint subsets, let us repeat this proof in a different manner that should help familiarize us with some of the properties of V/W. We begin with several simple properties that are grouped together as a theorem for the sake of reference.

Theorem 7.30 Let W be a subspace of a vector space V. Then the following properties are equivalent:

(a) $u \in v + W$;
(b) $u - v \in W$;
(c) $v \in u + W$;
(d) $u + W = v + W$.

Proof (a) $\Rightarrow$ (b): If $u \in v + W$, then there exists $w \in W$ such that $u = v + w$. But then $u - v = w \in W$.

(b) $\Rightarrow$ (c): $u - v \in W$ implies $v - u = -(u - v) \in W$, and hence there exists $w \in W$ such that $v - u = w$. But then $v = u + w \in u + W$.

(c) $\Rightarrow$ (d): If $v \in u + W$, then there exists $w \in W$ such that $v = u + w$. But then $v + W = u + w + W = u + W$.

(d) $\Rightarrow$ (a): $0 \in W$ implies $u = u + 0 \in u + W = v + W$. ∎

Theorem 7.31 Let W be a subspace of a vector space V. Then the cosets of W in V are distinct, and every element of V lies in some coset of W.

Proof It is easy to see that any $v \in V$ lies in V/W since $v = v + 0 \in v + W$. Now suppose that $v_1 \neq v_2$ and that the cosets $v_1 + W$ and $v_2 + W$ have some element u in common. Then $u \in v_1 + W$ and $u \in v_2 + W$, and hence by Theorem 7.30 we have $v_1 + W = u + W = v_2 + W$. ∎

Let V be a vector space over $\mathcal{F}$, and let W be a subspace of V. We propose to make V/W into a vector space. If $\alpha \in \mathcal{F}$ and $u + W, v + W \in V/W$, we define

$$(u + W) + (v + W) = (u + v) + W$$

and

$$\alpha(u + W) = \alpha u + W \ .$$

The first thing to do is show that these operations are well-defined. In other words, if we suppose that $u + W = u' + W$ and $v + W = v' + W$, then we must show that $(u + v) + W = (u' + v') + W$ and $\alpha(u + W) = \alpha(u' + W)$. Using $u + W = u' + W$ and $v + W = v' + W$, Theorem 7.30 tells us that $u - u' \in W$ and $v - v' \in W$. But then

$$(u + v) - (u' + v') = (u - u') + (v - v') \in W$$

and hence $(u + v) + W = (u' + v') + W$. Next, we see that $u - u' \in W$ implies $\alpha(u - u') \in W$ since W is a subspace. Then $\alpha u - \alpha u' \in W$ implies $\alpha u + W = \alpha u' + W$, or $\alpha(u + W) = \alpha(u' + W)$.

Theorem 7.32 Let V be a vector space over $\mathcal{F}$ and W a subspace of V. For any $u + W, v + W \in V/W$ and $\alpha \in \mathcal{F}$, we define the operations

(1) $(u + W) + (v + W) = (u + v) + W$

(2) $\alpha(u + W) = \alpha u + W$.

Then, with these operations, V/W becomes a vector space over $\mathcal{F}$.

Proof Since $(0 + W) + (u + W) = (0 + u) + W = u + W$, we see that W is the zero element of V/W. Similarly, we see that $-(u + W) = -u + W$. In view of the above discussion, all that remains is to verify axioms (V1) – (V8) for a vector space given at the beginning of Section 2.1. We leave this as an exercise for the reader (see Exercise 7.9.1). ∎

The vector space V/W defined in this theorem is called the **quotient space** of V by W. If V is finite-dimensional, then any subspace $W \subset V$ is also finite-

dimensional, where in fact dim W ≤ dim V (Theorem 2.9). It is then natural to ask about the dimension of V/W.

Theorem 7.33 Let V be finite-dimensional over $\mathcal{F}$ and W be a subspace of V. Then

$$\dim V/W = \dim V - \dim W .$$

Proof Suppose $\{w_1, \ldots, w_m\}$ is a basis for W. By Theorem 2.10 we can extend this to a basis $\{w_1, \ldots, w_m, v_1, \ldots, v_r\}$ for V, where dim V = m + r = dim W + r. Then any $v \in V$ may be written as

$$v = \alpha_1 w_1 + \cdots + \alpha_m w_m + \beta_1 v_1 + \cdots + \beta_r v_r$$

where $\{\alpha_i\}, \{\beta_j\} \in \mathcal{F}$. For ease of notation, let us define $\bar{V} = V/W$ and, for any $v \in V$, we let $\bar{v} = v + W \in \bar{V}$. Note that this association is linear because (by Theorem 7.32)

$$\overline{v + v'} = v + v' + W = v + W + v' + W = \bar{v} + \bar{v}'$$

and

$$\overline{kv} = kv + W = k(v + W) = k\bar{v} .$$

Since $w_i \in W$, we see that $\bar{w}_i = w_i + W = W$, and hence $\bar{v} = \beta_1 \bar{v}_1 + \cdots + \beta_r \bar{v}_r$. Alternatively, any $\bar{v} \in \bar{V}$ may be written as

$$\bar{v} = v + W = \sum_i \alpha_i w_i + \sum_j \beta_j v_j + W = \sum_j \beta_j v_j + W = \sum_j \beta_j \bar{v}_j$$

since $\sum \alpha_i w_i \in W$. In any case, this shows that the $\bar{v}_i$ span $\bar{V}$. Now suppose that $\sum_i \gamma_i v_i = 0$ for some scalars $\gamma_i \in \mathcal{F}$. Then

$$\gamma_1 \bar{v}_1 + \cdots + \gamma_r \bar{v}_r = \bar{0} = W .$$

Using $\bar{v}_i = v_i + W$, we then see that $\gamma_1 v_1 + \cdots + \gamma_r v_r + W = W$ which implies that $\sum_i \gamma_i v_i \in W$. But $\{w_i\}$ forms a basis for W, and hence there exist $\delta_1, \ldots, \delta_m \in \mathcal{F}$ such that

$$\gamma_1 v_1 + \cdots + \gamma_r v_r = \delta_1 w_1 + \cdots + \delta_m w_m .$$

However, $\{w_1, \ldots, w_m, v_1, \ldots, v_r\}$ is a basis for V and hence is linearly independent. This means that $\gamma_i = 0$ for each i = 1, . . . , r and that $\delta_j = 0$ for each j = 1, . . . , m. Thus $\{\bar{v}_i\}$ is linearly independent and forms a basis for $\bar{V} = V/W$, and dim V/W = r = dim V − dim W. ∎

There is a slightly different way of looking at this result that will be of use to us later.

Theorem 7.34 Let V be finite-dimensional over $\mathcal{F}$ and W be a subspace of V. Suppose that W has basis $w_1, \ldots, w_m$ and $\bar{V} = V/W$ has basis $\bar{v}_1, \ldots, \bar{v}_r$ where $\bar{v}_i = v_i + W$ for some $v_i \in V$. Then $\{w_1, \ldots, w_m, v_1, \ldots, v_r\}$ is a basis for V.

Proof Let $u \in V$ be arbitrary. Then $\bar{u} = u + W \in \bar{V}$, and hence there exists $\{\alpha_i\} \in \mathcal{F}$ such that

$$u + W = \bar{u} = \alpha_1\bar{v}_1 + \cdots + \alpha_r\bar{v}_r = \alpha_1 v_1 + \cdots + \alpha_r v_r + W \ .$$

By Theorem 7.30 there exists $w = \beta_1 w_1 + \cdots + \beta_m w_m \in W$ such that

$$u = \alpha_1 v_1 + \cdots + \alpha_r v_r + w = \alpha_1 v_1 + \cdots + \alpha_r v_r + \beta_1 w_1 + \cdots + \beta_m w_m \ .$$

This shows that $\{w_1, \ldots, w_m, v_1, \ldots, v_r\}$ spans V.

To show that these vectors are linearly independent, we suppose that

$$\gamma_1 w_1 + \cdots + \gamma_m w_m + \delta_1 v_1 + \cdots + \delta_r v_r = 0 \ .$$

Since the association between V and $\bar{V}$ is linear (see the proof of Theorem 7.33) and $\bar{w}_i = w_i + W = W$, we see that

$$\delta_1\bar{v}_1 + \cdots + \delta_r\bar{v}_r = \bar{0} = W \ .$$

But the $\bar{v}_i$ are linearly independent (since they are a basis for $\bar{V}$), and hence $\delta_1 = \cdots = \delta_r = 0$. (This is just the definition of linear independence if we recall that W is the zero vector in $\bar{V} = V/W$.) This leaves us with $\gamma_1 w_1 + \cdots + \gamma_m w_m = 0$. But again, the w_i are linearly independent, and therefore $\gamma_1 = \cdots = \gamma_m = 0$. This shows that $\{w_1, \ldots, w_m, v_1, \ldots, v_r\}$ is a basis for V, and hence dim V = dim W + dim V/W. ∎

Exercises

1. Finish the proof of Theorem 7.32.

2. Let U and V be finite-dimensional, and suppose T is a linear transformation of U onto V. If W = Ker T, prove that V is isomorphic to U/W. [*Hint*: See Exercise 1.5.11.]

3. Let V be a vector space over $\mathcal{F}$, and let W be a subspace of V. Define a relation R on the set V by xRy if $x - y \in W$.
   (a) Show that R defines an equivalence relation on V.
   (b) Let the equivalence class of $x \in V$ be denoted by [x], and define the quotient set V/R to be the set of all such equivalence classes. For all $x, y \in V$ and $a \in \mathcal{F}$ we define addition and scalar multiplication in V/R by

$$[x] + [y] = [x + y]$$

   and

$$a[x] = [ax] \ .$$

   Show that these operation are well-defined, and that V/R is a vector space over $\mathcal{F}$.
   (c) Now assume that V is finite-dimensional, and define the mapping $T: V \to V/R$ by Tx = [x]. Show that this defines a linear transformation.
   (d) Using Theorem 5.6, prove that dim V/R + dim W = dim V.

7.10 THE TRIANGULAR FORM THEOREM *

Now that we know something about quotient spaces, let us look at the effect of a linear transformation on such a space. Unless otherwise noted, we restrict our discussion to finite-dimensional vector spaces. In particular, suppose that $T \in L(V)$ and W is a T-invariant subspace of V. We first show that T induces a natural linear transformation on the space V/W. (The reader should be careful to note that $\overline{0}$ in Theorem 7.33 is the zero vector in $\overline{V} = V/W$, while in the theorem below, $\overline{0}$ is the zero transformation on $\overline{V}$.)

Theorem 7.35 Suppose $T \in L(V)$ and let W be a T-invariant subspace of V. Then T induces a linear transformation $\overline{T} \in L(V/W)$ defined by

$$\overline{T}(v + W) = T(v) + W \ .$$

Furthermore, if T satisfies any polynomial $p(x) \in \mathcal{F}[x]$, then so does $\overline{T}$. In particular, the minimal polynomial $\overline{m}(x)$ for $\overline{T}$ divides the minimal polynomial m(x) for T.

Proof Our first task is to show that $\overline{T}$ is well-defined and linear. Thus, suppose $v + W = v' + W$. Then $v - v' \in W$ so that $T(v - v') = T(v) - T(v') \in W$ since W is T-invariant. Therefore, using Theorem 7.30, we see that

$$\overline{T}(v + W) = T(v) + W = T(v') + W = \overline{T}(v' + W)$$

and hence $\overline{T}$ is well-defined. To show that $\overline{T}$ is a linear transformation, we simply calculate

$$\begin{aligned}\overline{T}[(v_1 + W) + (v_2 + W)] &= \overline{T}(v_1 + v_2 + W) = T(v_1 + v_2) + W \\ &= T(v_1) + T(v_2) + W = T(v_1) + W + T(v_2) + W \\ &= \overline{T}(v_1 + W) + \overline{T}(v_2 + W)\end{aligned}$$

and

$$\begin{aligned}\overline{T}[\alpha(v + W)] &= \overline{T}(\alpha v + W) = T(\alpha v) + W = \alpha T(v) + W \\ &= \alpha[T(v) + W] = \alpha\overline{T}(v + W) \ .\end{aligned}$$

This proves that $\overline{T}$ is indeed a linear transformation.

Next we observe that for any $T \in L(V)$, T^2 is a linear transformation and W is also invariant under T^2. This means that we can calculate the effect of $\overline{T^2}$ on any $v + W \in V/W$:

$$\begin{aligned}\overline{T^2}(v + W) &= T^2(v) + W = T[T(v)] + W = \overline{T}[T(v) + W] \\ &= \overline{T}[\overline{T}(v + W)] = \overline{T}^2(v + W) \ .\end{aligned}$$

This shows that $\overline{T^2} = \overline{T}^2$, and it is easy to see that in general $\overline{T}^{\overline{m}} = \overline{T}^m$ for any $m \geq 0$. Then for any $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathcal{F}[x]$, we have

$$\begin{aligned}\overline{p(T)}(v + W) &= p(T)(v) + W = \Sigma a_m T^m(v) + W = \Sigma a_m[T^m(v) + W] \\ &= \Sigma a_m \overline{T^m}(v + W) = \Sigma a_m \overline{T}^m(v + W) = p(\overline{T})(v + W)\end{aligned}$$

so that $\overline{p(T)} = p(\overline{T})$.

Now note that for any $v + W \in V/W$ we have $\overline{0}(v + W) = 0(v) + W = W$, and hence $\overline{0}$ is the zero transformation on V/W (since W is the zero vector in V/W). Therefore, if $p(T) = 0$ for some $p(x) \in \mathcal{F}[x]$, we see that $\overline{0} = \overline{p(T)} = p(\overline{T})$ and hence $\overline{T}$ satisfies p(x) also.

Finally, let $\overline{m}(x)$ be the minimal polynomial for $\overline{T}$. If p(x) is such that $p(\overline{T}) = \overline{0}$, then we know that $\overline{m}|p$ (Theorem 7.4). If m(x) is the minimal polynomial for T, then $m(T) = 0$, and therefore $m(\overline{T}) = \overline{0}$ by what we just proved. Hence $\overline{m}|m$. ∎

We now come to the main result of this section. By way of motivation, we saw in Theorem 7.24 that a linear transformation $T \in L(V)$ is diagonalizable if and only if the minimal polynomial for T can be written as the product of distinct linear factors. What we wish to do now is take into account the more general case where all of the *distinct* factors of the minimal polynomial are linear, but possibly with a multiplicity greater than one. We shall see that this leads to a triangular form for the matrix representation of T.

For definiteness we consider upper-triangular matrices, so what we are looking for is a basis $\{v_i\}$ for V in which the action of T takes the form

$$\begin{aligned} T(v_1) &= v_1 a_{11} \\ T(v_2) &= v_1 a_{12} + v_2 a_{22} \\ &\vdots \\ T(v_n) &= v_1 a_{1n} + \cdots + v_n a_{nn} \quad . \end{aligned}$$

We present two versions of this theorem in the present chapter. The first is more intuitive, while the second requires the development of some additional material that is also of use in other applications. Because of this, we postpone the second version until after we have discussed nilpotent transformations in the next section. (Actually, Exercises 7.5.7 and 7.5.8 outlined another way to prove the first version that used the formalism of ideals and annihilators, and made no reference whatsoever to quotient spaces.) Furthermore, in Section 8.1 we give a completely independent proof for the special case of matrices over an algebraically closed field.

Recall from Theorem 7.9 that an element $\lambda \in \mathcal{F}$ is an eigenvalue of T if and only if λ is a root of the characteristic polynomial of T. Thus all the eigenvalues of T lie in $\mathcal{F}$ if and only if the characteristic polynomial factors into linear terms.

Theorem 7.36 (**Triangular Form Theorem**) Suppose $T \in L(V)$ has a characteristic polynomial that factors into (not necessarily distinct) linear terms. Then V has a basis in which the matrix of T is triangular.

Proof If $\dim V = 1$, then T is represented by a 1 x 1 matrix which is certainly triangular. Now suppose that $\dim V = n > 1$. We assume the theorem is true for $\dim V = n - 1$, and proceed by induction to prove the result for $\dim V = n$. Since the characteristic polynomial of T factors into linear polynomials, there exists at least one nonzero eigenvalue λ_1 and corresponding eigenvector v_1 such that $T(v_1) = \lambda_1 v_1 \equiv a_{11} v_1$. Let W be the one-dimensional T-invariant subspace spanned by v_1, and define $\bar{V} = V/W$ so that (by Theorem 7.33) $\dim \bar{V} = \dim V - \dim W = n - 1$.

According to Theorem 7.35, T induces a linear transformation $\overline{T}$ on $\overline{V}$ such that the minimal polynomial $\overline{m}(x)$ for $\overline{T}$ divides the minimal polynomial m(x) for T. But this means that any root of $\overline{m}(x)$ is also a root of m(x). Since the characteristic polynomial of T factors into linear polynomials by hypothesis, so does m(x) (see Theorem 7.12). Therefore $\overline{m}(x)$ must also factor into linear polynomials, and hence so does the characteristic polynomial of T. This shows that $\overline{T}$ and $\overline{V}$ satisfy the hypotheses of the theorem, and hence there exists a basis $\{\bar{v}_2, \ldots, \bar{v}_n\}$ for $\overline{V} = V/W$ such that

$$\begin{aligned}\overline{T}(\overline{v}_2) &= \overline{v}_2 a_{22}\\ \overline{T}(\overline{v}_3) &= \overline{v}_2 a_{23} + \overline{v}_3 a_{33}\\ &\vdots\\ \overline{T}(\overline{v}_n) &= \overline{v}_2 a_{2n} + \cdots + \overline{v}_n a_{nn} \quad .\end{aligned}$$

We now let $v_2, \ldots, v_n$ be elements of V such that $\bar{v}_i = v_i + W$ for each $i = 2, \ldots, n$. Since W has basis $\{v_1\}$, Theorem 7.35 tells us that $\{v_1, v_2, \ldots, v_n\}$ is a basis for V. According to our above result, we have $\overline{T}(\bar{v}_2) = \bar{v}_2 a_{22}$ which is equivalent to $\overline{T}(\bar{v}_2) - \bar{v}_2 a_{22} = \overline{0}$, and hence the definition of $\overline{T}$ (see Theorem 7.35) along with Theorem 7.30 tells us that $T(v_2) - v_2 a_{22} \in W$. Since W is spanned by v_1, this says there exists $a_{12} \in \mathcal{F}$ such that $T(v_2) - v_2 a_{22} = v_1 a_{12}$, i.e., $T(v_2) = v_1 a_{12} + v_2 a_{22}$. Clearly, an identical argument holds for any of the $\overline{T}(\bar{v}_i)$, and thus for each $i = 2, \ldots, n$ there exists $a_{1i} \in \mathcal{F}$ such that $T(v_i) - v_2 a_{2i} - \cdots - v_i a_{ii} \in W$ implies

$$T(v_i) = v_1 a_{1i} + v_2 a_{2i} + \cdots + v_i a_{ii} \quad .$$

Written out, this is just

$$\begin{aligned}T(v_1) &= v_1 a_{11}\\ T(v_2) &= v_1 a_{12} + v_2 a_{22}\\ &\vdots\\ T(v_n) &= v_1 a_{1n} + \cdots + v_n a_{nn} \quad .\end{aligned}$$

In other words, the elements $v_1, \ldots, v_n \in V$ are a basis for V in which every $T(v_i)$ is a linear combination of v_j for $j \leq i$. This is precisely the definition of triangular form. ∎

We now give a restatement of this theorem in terms of matrices. For ease of reference, this version is presented as a corollary.

Corollary Let $A \in M_n(\mathcal{F})$ be a matrix whose characteristic polynomial factors into linear polynomials. Then A is similar to a triangular matrix.

Proof The matrix $A = (a_{ij})$ defines a linear transformation T on the space $\mathcal{F}^n$ by $T(v_i) = \sum_{j=1}^{n} v_j a_{ji}$ where $\{v_i\}$ is a basis for $\mathcal{F}^n$. In particular, relative to the basis $\{v_i\}$, the matrix representation of T is precisely the matrix A (since T takes the i*th* basis vector into the i*th* column of the matrix representing T). Since the characteristic polynomial of T is independent of the basis used in the matrix representation of T, and the characteristic polynomial of A factors into linear polynomials, we see that Theorem 7.36 applies to T. Thus there is a basis for $\mathcal{F}^n$ in which the matrix of T (i.e., the matrix A) is triangular. By Theorem 5.18 we then see that A must be similar to a triangular matrix. ∎

If a linear transformation T can be represented by a triangular matrix, then we say that T can be **brought into triangular form**. Since λ is an eigenvalue of T if and only if $\det(\lambda I - T) = 0$ (Theorem 7.9), Theorem 4.5 tells us that the eigenvalues of a triangular matrix are precisely the diagonal elements of the matrix (this was also discussed in the previous section).

7.11 NILPOTENT TRANSFORMATIONS *

An operator $T \in L(V)$ is said to be **nilpotent** if $T^n = 0$ for some positive integer n. If $T^k = 0$ but $T^{k-1} \neq 0$, then k is called the **index of nilpotency** of T (note that $T^{k-1} \neq 0$ implies that $T^j \neq 0$ for all $j \leq k - 1$). This same terminology applies to any square matrix A with the property that $A^n = 0$. Some elementary facts about nilpotent transformations are contained in the following theorem. Note Theorem 7.1 implies that if A is the matrix representation of T and T is nilpotent with index k, then A is also nilpotent with index k.

Theorem 7.37 Suppose $T \in L(V)$, and assume that for some $v \in V$ we have $T^k(v) = 0$ but $T^{k-1}(v) \neq 0$. Define the set

$$S = \{v, T(v), T^2(v), \ldots, T^{k-1}(v)\} .$$

Then S has the following properties:

(a) The elements of S are linearly independent.

(b) The linear span W of S is a T-invariant subspace of V.

(c) The operator $T_W = T|W$ is nilpotent with index k.

(d) With respect to the ordered basis $\{T^{k-1}(v), \ldots, T(v), v\}$ for W, the matrix of T_W has the form

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Thus the matrix of T_W has all zero entries except on the **superdiagonal** where they are all equal to one. This shows that the matrix representation of T_W is a nilpotent matrix with index k.

Proof (a) Suppose that

$$\alpha_0 v + \alpha_1 T(v) + \cdots + \alpha_{k-1} T^{k-1}(v) = 0$$

for some set of scalars $\alpha_i \in \mathcal{F}$. Applying T^{k-1} to this equation results in $\alpha_0 T^{k-1}(v) = 0$. Since $T^{k-1}(v) \neq 0$, this implies that $\alpha_0 = 0$. Using this result, apply T^{k-2} to the above equation to obtain $\alpha_1 = 0$. Continuing this procedure, we eventually arrive at $\alpha_i = 0$ for each $i = 0, 1, \ldots, k - 1$ and hence the elements of S are linearly independent.

(b) Since any $w \in W$ may be written in the form

$$w = \beta_0 v + \beta_1 T(v) + \cdots + \beta_{k-1} T^{k-1}(v)$$

we see that $T(w) = \beta_0 T(v) + \cdots + \beta_{k-2} T^{k-1}(v) \in W$, and hence $T(W) \subset W$.

(c) Using $T^k(v) = 0$, it follows that $T_W{}^k(T^i(v)) = T^{k+i}(v) = 0$ for each $i = 0, \ldots, k - 1$. This shows that $T_W{}^k$ applied to each element of S (i.e., each of the basis vectors for W) is zero, and thus $T_W{}^k = 0$. In addition, since $v \in W$ we see that $T_W{}^{k-1}(v) = T^{k-1}(v) \neq 0$, and therefore T_W is nilpotent with index k.

(d) Using $T_W(T^i(v)) = T^{i+1}(v)$ along with the fact that the i*th* column of $[T_W]$ is the image of the i*th* basis vector for W, it is easy to see that $[T_W]$ has the desired form. ∎

One must be careful to understand exactly what Theorem 7.37 says and what it does not say. In particular, if T is nilpotent with index k, then $T^k(u) = 0$ for *all* $u \in V$, while $T^{k-1}(v) \neq 0$ for *some* $v \in V$. This is because if $w = T(v)$, then $T^{k-1}(w) = T^{k-1}(T(v)) = T^k(v) = 0$. Hence it is impossible for $T^{k-1}(v)$ to be nonzero for all $v \in V$.

It is also interesting to note that according to Theorem 7.37(b), the subspace W is T-invariant, and hence by Theorem 7.19, the matrix of T must be of the block form

$$\begin{pmatrix} M_k & B \\ 0 & C \end{pmatrix}$$

where M_k is the k x k matrix of $T_W = T|W$ defined in part (d) of Theorem 7.37. If we can find another T-invariant subspace U of V such that $V = W \oplus U$, then the matrix representation of T will be in block diagonal form (Theorem 7.20). We now proceed to show that this can in fact be done. Let us first prove two more easy results.

Theorem 7.38 Let $T \in L(V)$ be nilpotent, and let $S = \alpha_1 T + \cdots + \alpha_m T^m$ where each $\alpha_i \in \mathcal{F}$. Then $\alpha_0 1 + S$ is invertible for any nonzero $\alpha_0 \in \mathcal{F}$.

Proof Suppose the index of T is k. Then $T^k = 0$, and therefore $S^k = 0$ also since the lowest power of T in the expansion of S^k is k. If $\alpha_0 \neq 0$, we leave it as a trivial exercise for the reader to show that

$$(\alpha_0 1 + S)(1/\alpha_0 - S/\alpha_0^2 + S^2/\alpha_0^3 + \cdots + (-1)^{k-1} S^{k-1}/\alpha_0^k) = 1 .$$

This shows that $\alpha_0 1 + S$ is invertible, and that its inverse is given by the above polynomial in S. ∎

Theorem 7.39 Let $T \in L(V)$ be nilpotent with index n, and let W be the T-invariant subspace spanned by $\{T^{n-1}(v), \ldots, T(v), v\}$ where $v \in V$ is such that $T^{n-1}(v) \neq 0$. If $w \in W$ is such that $T^{n-k}(w) = 0$ for some $0 < k \leq n$, then there exists $w_0 \in W$ such that $T^k(w_0) = w$.

Proof Since $w \in W$, we have

$$w = \alpha_n T^{n-1}(v) + \cdots + \alpha_{k+1} T^k(v) + \alpha_k T^{k-1}(v) + \cdots + \alpha_2 T(v) + \alpha_1 v$$

and therefore (since $T^n = 0$)

$$0 = T^{n-k}(w) = \alpha_k T^{n-1}(v) + \cdots + \alpha_1 T^{n-k}(v) .$$

But $\{T^{n-1}(v), \ldots, T^{n-k}(v)\}$ is linearly independent (Theorem 7.37), and thus $\alpha_k = \cdots = \alpha_1 = 0$. This means that

$$w = \alpha_n T^{n-1}(v) + \cdots + \alpha_{k+1} T^k(v) = T^k(w_0)$$

where $w_0 = \alpha_n T^{n-k-1}(v) + \cdots + \alpha_{k+1} v \in W$. ∎

We are now in a position to prove our above assertion on the decomposition of V. This (by no means trivial) result will form the basis of the principle theorem dealing with nilpotent transformations (Theorem 7.41 below). It is worth pointing out that while the following theorem will be quite useful to us, its proof is not very constructive.

Theorem 7.40 Let T and W be as defined in the previous theorem. Then there exists a T-invariant subspace U of V such that $V = W \oplus U$.

Proof Let $U \subset V$ be a T-invariant subspace of largest dimension with the property that $W \cap U = \{0\}$. (Such a space exists since even $\{0\}$ is T-invariant, and $W \cap \{0\} = \{0\}$.) We first show that $V = W + U$. If this is not the case, then there exists $z \in V$ such that $z \notin W + U$. Since $T^0(z) = z \notin W + U$ while $T^n(z) = 0 \in W + U$, it follows that there must exist an integer k with $0 < k \leq n$ such that $T^k(z) \in W + U$ and $T^j(z) \notin W + U$ for $j < k$. We write $T^k(z) = w + u$ where $w \in W$ and $u \in U$, and therefore

$$0 = T^n(z) = T^{n-k}(T^k(z)) = T^{n-k}(w) + T^{n-k}(u) .$$

Since both W and U are T-invariant, we have $T^{n-k}(w) \in W$ and $T^{n-k}(u) \in U$. But $W \cap U = \{0\}$ so that

$$T^{n-k}(w) = -T^{n-k}(u) \in W \cap U = 0 .$$

(Remember that W and U are subspaces so $x \in U$ implies that $-x \in U$ also.) We now apply Theorem 7.39 to conclude that there exists $w_0 \in W$ such that $T^k(w_0) = w$, and hence $T^k(z) = w + u = T^k(w_0) + u$. Defining $x = z - w_0$, we then have

$$T^k(x) = T^k(z) - T^k(w_0) = u \in U .$$

But U is T-invariant, and hence it follows that $T^m(x) \in U$ for any $m \geq k$. Considering lower powers of T, let us assume that $j < k$. Then the T-invariance of W implies $T^j(w_0) \in W$, while we saw above that $T^j(z) \notin W + U$. This means that

$$T^j(x) = T^j(z) - T^j(w_0) \notin U$$

(because if $T^j(x) \in U$, then $T^j(z) = T^j(w_0) + T^j(x) \in W + U$, a contradiction)

Now let U_x be that subspace of V spanned by U together with the set $\{T^{k-1}(x), \ldots, T(x), x\}$. Since U is T-invariant and $T^j(x) \notin U$, it must be true that $x \notin U$. Together with $U \subset U_x$, this means $\dim U_x > \dim U$. Applying T to $\{T^{k-1}(x), \ldots, T(x), x\}$ we obtain the set $\{T^k(x), T^{k-1}(x), \ldots, T^2(x), T(x)\}$. Since $T^k(x) \in U$ and the rest of the vectors in this set are included in the set that spans U_x, it follows that U_x is also T-invariant.

By assumption, U is the subspace of largest dimension that is both T-invariant *and* satisfies $W \cap U = \{0\}$. Since $\dim U_x > \dim U$ and U_x is T-invariant, we must have $W \cap U_x \neq \{0\}$. Therefore there exists a nonzero element in $W \cap U_x$ of the form $u_0 + \alpha_k T^{k-1}(x) + \cdots + \alpha_2 T(x) + \alpha_1 x$ where $u_0 \in U$. We can not have $\alpha_i = 0$ for every $i = 1, \ldots, k$ because this would imply that $0 \neq u_0 \in W \cap U = \{0\}$, a contradiction. If we let $\alpha_r \neq 0$ be the first nonzero α_i , then we have

$$u_0 + (\alpha_k T^{k-r} + \cdots + \alpha_{r+1} T + \alpha_r) T^{r-1}(x) \in W \quad . \qquad (*)$$

From Theorem 7.38 we see that $\alpha_k T^{k-r} + \cdots + \alpha_{r+1} T + \alpha_r$ is invertible, and its inverse is given by some polynomial p(T). Since W and U are T-invariant, they are also invariant under p(T).

Applying p(T) to (*), we see that

$$p(T)(u_0) + T^{r-1}(x) \in p(T)(W) \subset W \quad .$$

This means that $T^{r-1}(x) \in W + p(T)(U) \subset W + U$. But $r - 1 < r < k$, and hence this result contradicts the earlier conclusion that $T^j(x) \notin U$ for $j < k$. Since this contradiction arose from the assumed existence of an element $z \in V$ with $z \notin W + U$, we conclude that $V = W + U$. Finally, since $W \cap U = \{0\}$ by hypothesis, we have $V = W \oplus U$. ∎

Combining several previous results, the next major theorem follows quite easily.

Theorem 7.41(a) Let $T \in L(V)$ be nilpotent with index of nilpotence n_1, and let M_k be the k x k matrix containing all 0's except for 1's on the superdiagonal (see Theorem 7.37). Then there exists a basis for V in which the matrix of T has the block diagonal form

$$\begin{pmatrix} M_{n_1} & 0 & \cdots & 0 \\ 0 & M_{n_2} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & M_{n_r} \end{pmatrix}$$

where $n_1 \geq \cdots \geq n_r$ and $n_1 + \cdots + n_r = \dim V$.

Proof Since $T^{n_1} = 0$ but $T^{n_1-1} \neq 0$, there exists $v \in V$ such that $T^{n_1-1}(v) \neq 0$. Applying Theorem 7.37, we see that the vectors $v_1 = T^{n_1-1}(v), \ldots, v_{n_1-1} = T(v), v_{n_1} = v$ are linearly independent and form the basis for a T-invariant subspace W_1 of V. Moreover, the matrix of $T_1 = T|W_1$ in this basis is just M_{n_1}.

By Theorem 7.40, there exists a T-invariant subspace $U \subset V$ such that $V = W_1 \oplus U$. Define a basis for V by taking the basis $\{v_1, \ldots, v_{n_1}\}$ for W_1 together with any basis for U. Then, according to Theorem 7.20, the matrix of T with respect to this basis is of the form

$$\begin{pmatrix} M_{n_1} & 0 \\ 0 & A_2 \end{pmatrix}$$

where A_2 is the matrix of $T_2 = T|U$. For any $u \in U$ and positive integer m we have $T_2^m(u) = T^m(u)$. Since $T^{n_1} = 0$, we see that $T_2^m = 0$ for all $m \geq n_1$, and thus there exists an integer $n_2 \leq n_1$ such that $T_2^{n_2} = 0$. This shows that T_2 is nilpotent with index n_2.

We now repeat the above argument using T_2 and U instead of T and V. This time we will decompose A_2 into

$$\begin{pmatrix} M_{n_2} & 0 \\ 0 & A_3 \end{pmatrix}$$

and therefore the representation of T becomes

$$\begin{pmatrix} M_{n_1} & 0 & 0 \\ 0 & M_{n_2} & 0 \\ 0 & 0 & A_3 \end{pmatrix}.$$

Continuing this process, it should be clear that we will eventually arrive at a basis for V in which the matrix of T has the desired form. It is also obvious that $\sum_{i=1}^{r} n_i = \dim V = n$ since the matrix of T must be of size n. ∎

Our next result is a rephrasing of Theorem 7.41(a).

Theorem 7.41(b) Let $T \in L(V)$ be nilpotent with index k. Then there exists a basis for V in which the matrix representation of T is block diagonal, and where each of these diagonal entries (i.e., square matrices) is of the super-diagonal form M given in Theorem 7.37. Moreover,

(a) There is at least one M matrix of size k, and every other M matrix is of size $\leq$ k.

(b) The total number of M matrices in the representation of T (i.e., the total number of blocks in the representation of T) is just nul T = dim(Ker T).

Proof See Exercise 7.11.1. ∎

Example 7.13 Consider the matrix

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

We leave it to the reader to show that A is nilpotent with index 3, i.e., $A^3 = 0$ but $A^2 \neq 0$. We seek the diagonal representation of A described in Theorem 7.41(b). It is obvious that r(A) = 2, and therefore (using Theorem 5.6) nul A = 5 − 2 = 3. Thus there are three M matrices in the diagonal representation of A, and one of them must be of size 3. This means that the only possibility for the remaining two matrices is that they both be of size 1. Thus the block diagonal form for A must be

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

It is easy to see that this matrix is also nilpotent with index 3. //

Exercises

1. Prove Theorem 7.41(b). [*Hint*: What is the rank of the matrix in Theorem 7.41(a)?]

2. Suppose S, T $\in$ L(V) are nilpotent with the property that ST = TS. Show that S + T and ST are also nilpotent.

3. Suppose A is a **supertriangular** matrix, i.e., all entries of A on or below the main diagonal are zero. Show that A is nilpotent.

4. Let V_n be the vector space of all polynomials of degree $\leq$ n, and let D $\in$ L(V_n) be the usual differentiation operator. Show that D is nilpotent with index n + 1.

5. Show that the following nilpotent matrices of size n are similar:

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

6. Show that two nilpotent 3 x 3 matrices are similar if and only if they have the same index of nilpotency. Give an example to show that this is not true for nilpotent 4 x 4 matrices.

7.12 THE TRIANGULAR FORM THEOREM AGAIN *

After all the discussion on nilpotent transformations in the previous section, let us return to our second version of the triangular form theorem which, as we shall see in the next chapter, is just the Jordan canonical form. While this theorem applies to a finite-dimensional vector space over an arbitrary field, the minimal polynomial m(x) for T must be factorable into linear polynomials. This means that all the roots of m(x) must lie in $\mathcal{F}$. Clearly, this will always be true if $\mathcal{F}$ is algebraically closed.

Theorem 7.42 (**Jordan Form**) Suppose T $\in$ L(V), and assume that the minimal polynomial m(x) for T can be written in the form

$$m(x) = (x - \lambda_1)^{n_1} \cdots (x - \lambda_r)^{n_r}$$

where each n_i is a positive integer, and the λ_i are distinct elements of $\mathcal{F}$. Then there exists a basis for V in which the matrix representation A of T has the block diagonal form $A = A_1 \oplus \cdots \oplus A_r$ where each $A_i \in M_{k_i}(\mathcal{F})$ for some integer $k_i \geq n_i$, and each A_i has the upper triangular form

$$\begin{pmatrix} \lambda_i & * & 0 & \cdots & 0 & 0 \\ 0 & \lambda_i & * & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_i & * \\ 0 & 0 & 0 & \cdots & 0 & \lambda_i \end{pmatrix}$$

where the *'s may be either 0 or 1.

Proof For each $i = 1, \ldots, r$ we define $W_i = \text{Ker}(T - \lambda_i 1)^{n_i}$ and $k_i = \dim W_i$. By the primary decomposition theorem (Theorem 7.23), we see that $V = W_1 \oplus \cdots \oplus W_r$ (where each W_i is T-invariant), and hence according to Theorem 2.15, V has a basis which is just the union of bases of the W_i. Letting the basis for V be the union of the bases for $W_1, \ldots, W_r$ taken in this order, it follows from Theorem 7.20 that $A = A_1 \oplus \cdots \oplus A_r$ where each A_i is the matrix representation of $T_i = T|W_i$. We must show that each A_i has the required form, and that $k_i \geq n_i$ for each $i = 1, \ldots, r$.

If we define $N_i = T - \lambda_i 1$, then $N_i \in L(W_i)$ since W_i is T-invariant. In other words, N_i is a linear operator defined on the space W_i, and hence so is $N_i^{n_i}$. However, since $W_i = \text{Ker } N_i^{n_i}$, it follows from the definition of kernel that $N_i^{n_i} = 0$ so that N_i is nilpotent. The result now follows by applying Theorem 7.41(a) to each N_i and writing $T = N_i + \lambda_i 1$. ∎

Note that each A_i in this theorem is a direct sum of matrices of the form

$$\begin{pmatrix} \lambda_i & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_i & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_i \end{pmatrix}$$

which are referred to as **basic Jordan blocks belonging** to λ_i. This theorem will be discussed in much more detail (and from an entirely different point of view) in Chapter 8.

Many of our earlier results follow in a natural manner as corollaries to Theorem 7.42. In particular, suppose that V is finite-dimensional over an algebraically closed field $\mathcal{F}$, and $T \in L(V)$ satisfies the hypotheses of Theorem 7.42. We wish to know the form of the characteristic polynomial $\Delta_T(x)$. Relative to the basis for V given by Theorem 7.42, we see that the characteristic matrix $xI - A$ is given by

$$\begin{array}{c} \uparrow \\ k_1 \\ \downarrow \\ \uparrow \\ k_2 \\ \downarrow \\ \vdots \end{array} \begin{pmatrix} \boxed{\begin{matrix} x-\lambda_1 & & * \\ & \ddots & \\ 0 & & x-\lambda_1 \end{matrix}} & & \\ & \boxed{\begin{matrix} x-\lambda_2 & & * \\ & \ddots & \\ 0 & & x-\lambda_2 \end{matrix}} & \\ & & \ddots \end{pmatrix}$$

and hence (using Theorem 4.5)

$$\Delta_T(x) = \det(xI - A) = \prod_{i=1}^{r} (x - \lambda_i)^{k_i} \quad .$$

On the other hand, since $m(x) = \prod_{i=1}^{r} (x - \lambda_i)^{n_i}$ and $k_i \geq n_i$, properties (a) and (b) in the following corollary should be clear, and property (c) follows from the proof of Theorem 7.42. Note that property (c) is just the Cayley-Hamilton theorem again.

Corollary Suppose $T \in L(V)$ where V is finite-dimensional over an algebraically closed field $\mathcal{F}$, and let the minimal and characteristic polynomials of T be $m(x)$ and $\Delta_T(x)$ respectively. Then

(a) $m(x) | \Delta_T(x)$.

(b) $m(x)$ and $\Delta_T(x)$ have the same roots (although they are not necessarily of the same algebraic multiplicity).

(c) $\Delta_T(T) = 0$.

Example 7.14 Let $V = \mathbb{C}^3$ have basis $\{v_1, v_2, v_3\}$ and define $T \in L(V)$ by

$$T(v_1) = -v_1 + 2v_3$$
$$T(v_2) = 3v_1 + 2v_2 + v_3$$
$$T(v_3) = -v_3 \quad .$$

Then the matrix representation of T in this basis is

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

We first find the minimal polynomial for T. Note that while we have given many theorems dealing with the minimal polynomial, there has as yet been no general method presented for actually finding it. (We shall see that such a method can be based on Theorem 8.8.) Since the minimal polynomial has the same irreducible factors as does the characteristic polynomial (Theorem 7.12), we begin by finding $\Delta_T(x) = \det(xI - A)$. A simple calculation yields

$$\Delta_T(x) = (x + 1)^2(x - 2)$$

and therefore the minimal polynomial must be either

$$(x + 1)^2(x - 2)$$

or

$$(x + 1)(x - 2) \quad .$$

To decide between these two possibilities, we could simply substitute A and multiply them out. However, it is worthwhile to instead apply Theorem 7.23. In other words, we find the subspaces $W_i = \text{Ker } f_i(x)^{n_i}$ and see which value of n_1 (i.e., either 1 or 2) results in $V = W_1 \oplus W_2$. We must therefore find the kernel (i.e., the null space) of $(T + 1)$, $(T + 1)^2$ and $(T - 2)$. Applying the operator $T + 1$ to each of the basis vectors yields

$$(T + 1)(v_1) = 2v_3$$
$$(T + 1)(v_2) = 3v_1 + 3v_2 + v_3$$
$$(T + 1)(v_3) = 0 \quad .$$

Since $\text{Im}(T + 1)$ is spanned by these three vectors, only two of which are obviously independent, we see that $r(T + 1) = 2$. Therefore, applying Theorem 5.6, we find that $\text{nul}(T + 1) = \dim V - r(T + 1) = 1$. Similarly, we have

$$(T+1)^2(v_1) = 0$$
$$(T+1)^2(v_2) = 9(v_1 + v_2 + v_3)$$
$$(T+1)^2(v_3) = 0$$

and so $r(T + 1)^2 = 1$ implies $nul(T + 1)^2 = 2$. It should also be clear that the space $Ker(T + 1)^2$ is spanned by the set $\{v_1, v_3\}$. Finally,

$$(T-2)(v_1) = -3v_1 + 2v_3$$
$$(T-2)(v_2) = 3v_1 + v_3$$
$$(T-2)(v_3) = -3v_3$$

so that $r(T - 2) = 2$ and hence $nul(T - 2) = 1$. We also note that since

$$(T - 2)(v_1 + v_2 + v_3) = 0$$

and $nul(T - 2) = 1$, it follows that the space $W_2 = Ker(T - 2)$ must be spanned by the vector $\{v_1 + v_2 + v_3\}$. Alternatively, we could assume that W_2 is spanned by some vector $u = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3$ and proceed to find α_1, α_2 and α_3 by requiring that $(T - 2)(u) = 0$. This results in

$$(T - 2)(u) = \alpha_1(-3v_1 + 2v_3) + \alpha_2(3v_1 + v_3) + \alpha_3(-3v_3) = 0$$

so that we have the simultaneous set of equations

$$-3\alpha_1 + 3\alpha_2 = 0$$
$$2\alpha_1 + \alpha_2 - 3\alpha_3 = 0 \ .$$

This yields $\alpha_1 = \alpha_2 = \alpha_3$ so that $u = v_1 + v_2 + v_3$ will span W_2 as we found by inspection.

From the corollary to Theorem 2.15 we have $\dim V = \dim W_1 + \dim W_2$, and since $\dim W_2 = nul(T - 2) = 1$, it follows that we must have $\dim W_1 = 2$, and hence $W_1 = Ker(T + 1)^2$. Thus the minimal polynomial for T must be given by

$$m(x) = (x + 1)^2(x - 2) \ .$$

Note that because of this form for m(x), Theorem 7.24 tells us that T is not diagonalizable.

According to Theorem 7.42, the matrix A_1 corresponding to $\lambda = -1$ must be at least a 2 x 2 matrix, and the matrix A_2 corresponding to $\lambda = 2$ must be at least a 1 x 1 matrix. However, since $\dim V = 3$, these are in fact the actual

sizes required. While A_2 is unambiguous, the matrix A_1 could be either a single 2 x 2 matrix, or it could be a direct sum of two 1 x 1 matrices. To resolve this we use Theorem 7.41(b) which tells us that the number of blocks in the representation of the nilpotent operator T + 1 is dim(Ker(T + 1)) = 1. This means that the Jordan form of T must be

$$\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix} . \quad /\!/$$

Exercises

1. Let $V = \mathbb{C}^4$ and suppose $T \in L(V)$. If T has only one eigenvalue λ of multiplicity 4, describe all possible Jordan forms of T.

2. Let $V = \mathbb{C}^4$ and suppose $m(x) = (x - \lambda_1)^{n_1} \cdots (x - \lambda_r)^{n_r}$ is the minimal polynomial for $T \in L(V)$. Let $A = A_1 \oplus \cdots \oplus A_r$ be the Jordan form of T. Prove directly from the structure of the A_i that the largest Jordan block belonging to λ_i has size n_i x n_i.

3. Let $V = \mathbb{C}^n$. If the Jordan form of $T \in L(V)$ consists of just one Jordan block (counting 1 x 1 blocks), what is the Jordan form of T^2? Explain.

4. Let $V = \mathbb{C}^n$, suppose $T \in L(V)$, and let λ be an eigenvalue of T. What is the relationship between the number of Jordan blocks belonging to λ and the rank of $T - \lambda I$? Explain.

5. Let $V = \mathbb{C}^n$, and suppose that each matrix below represents $T \in L(V)$ relative to the standard basis. Determine the Jordan form of T. [*Hint*: Use the previous exercise.]

(*a*) $\begin{pmatrix} 1 & -1 & -1 & -1 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 2 \end{pmatrix}$ (*b*) $\begin{pmatrix} 1 & -1 & -1 & -1 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$

(*c*) $\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 2 \end{pmatrix}$ (*d*) $\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$

CHAPTER 8

Canonical Forms

Recall that at the beginning of Section 7.5 we stated that a canonical form for $T \in L(V)$ is simply a representation in which the matrix takes on an especially simple form. For example, if there exists a basis of eigenvectors of T, then the matrix representation will be diagonal. In this case, it is then quite trivial to assess the various properties of T such as its rank, determinant and eigenvalues. Unfortunately, while this is generally the most desirable form for a matrix representation, it is also generally impossible to achieve.

We now wish to determine certain properties of T that will allow us to learn as much as we can about the possible forms its matrix representation can take. There are three major canonical forms that we will consider in this chapter : triangular, rational and Jordan. (This does not count the Smith form, which is really a tool, used to find the rational and Jordan forms.) As we have done before, our approach will be to study each of these forms in more than one way. By so doing, we shall gain much insight into their meaning, as well as learning additional techniques that are of great use in various branches of mathematics.

8.1 ELEMENTARY CANONICAL FORMS

In order to ease into the subject, this section presents a simple and direct method of treating two important results: the triangular form for complex matrices and the diagonalization of normal matrices. To begin with, suppose

that we have a matrix $A \in M_n(\mathbb{C})$. We define the **adjoint** (or **Hermitian adjoint**) of A to be the matrix $A^\dagger = A^{*T}$. In other words, the adjoint of A is its complex conjugate transpose. From Theorem 3.18(d), it is easy to see that

$$(AB)^\dagger = B^\dagger A^\dagger \ .$$

If it so happens that $A^\dagger = A$, then A is said to be a **Hermitian** matrix.

If a matrix $U \in M_n(\mathbb{C})$ has the property that $U^\dagger = U^{-1}$, then we say that U is **unitary**. Thus a matrix U is unitary if $UU^\dagger = U^\dagger U = I$. (Note that by Theorem 3.21, it is only necessary to require either $UU^\dagger = I$ or $U^\dagger U = I$.) We also see that the product of two unitary matrices U and V is unitary since $(UV)^\dagger UV = V^\dagger U^\dagger UV = V^\dagger IV = V^\dagger V = I$. If a matrix $N \in M_n(\mathbb{C})$ has the property that it commutes with its adjoint, i.e., $NN^\dagger = N^\dagger N$, then N is said to be a **normal** matrix. Note that Hermitian and unitary matrices are automatically normal.

Example 8.1 Consider the matrix $A \in M_2(\mathbb{C})$ given by

$$A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ i & i \end{pmatrix} \ .$$

Then the adjoint of A is given by

$$A^\dagger = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -1 & -i \end{pmatrix}$$

and we leave it to the reader to verify that $AA^\dagger = A^\dagger A = 1$, and hence show that A is unitary. //

We will devote considerable time in Chapter 10 to the study of these matrices. However, for our present purposes, we wish to point out one important property of unitary matrices. Note that since $U \in M_n(\mathbb{C})$, the rows U_i and columns U^i of U are just vectors in $\mathbb{C}^n$. This means that we can take their inner product relative to the standard inner product on $\mathbb{C}^n$ (see Example 2.9). Writing out the relation $UU^\dagger = I$ in terms of components, we have

$$(UU^\dagger)_{ij} = \sum_{k=1}^{n} u_{ik} u^\dagger{}_{kj} = \sum_{k=1}^{n} u_{ik} u_{jk}{}^* = \sum_{k=1}^{n} u_{jk}{}^* u_{ik} = \langle U_j, U_i \rangle = \delta_{ij}$$

and from $U^\dagger U = I$ we see that

$$(U^\dagger U)_{ij} = \sum_{k=1}^{n} u^\dagger{}_{ik} u_{kj} = \sum_{k=1}^{n} u_{ki}{}^* u_{kj} = \langle U^i, U^j \rangle = \delta_{ij} \ .$$

In other words, a matrix is unitary if and only if its rows (or columns) each form an orthonormal set. Note we have shown that if the rows (columns) of $U \in M_n(\mathbb{C})$ form an orthonormal set, then so do the columns (rows), and either of these is a sufficient condition for U to be unitary. For example, the reader can easily verify that the matrix A in Example 8.1 satisfies these conditions.

It is also worth pointing out that Hermitian and unitary matrices have important analogues over the real number system. If $A \in M_n(\mathbb{R})$ is Hermitian, then $A = A^\dagger = A^T$, and we say that A is **symmetric**. If $U \in M_n(\mathbb{R})$ is unitary, then $U^{-1} = U^\dagger = U^T$, and we say that U is **orthogonal**. Repeating the above calculations over $\mathbb{R}$, it is easy to see that a real matrix is orthogonal if and only if its rows (or columns) form an orthonormal set.

It will also be useful to recall from Section 3.6 that if A and B are two matrices for which the product AB is defined, then the i*th* row of AB is given by $(AB)_i = A_iB$ and the i*th* column of AB is given by $(AB)^i = AB^i$. We now prove yet another version of the triangular form theorem.

Theorem 8.1 (**Schur Canonical Form**) If $A \in M_n(\mathbb{C})$, then there exists a unitary matrix $U \in M_n(\mathbb{C})$ such that $U^\dagger AU$ is upper-triangular. Furthermore, the diagonal entries of $U^\dagger AU$ are just the eigenvalues of A.

Proof If n = 1 there is nothing to prove, so we assume that the theorem holds for any square matrix of size $n - 1 \geq 1$, and suppose A is of size n. Since we are dealing with the algebraically closed field $\mathbb{C}$, we know that A has n (not necessarily distinct) eigenvalues (see Section 7.3). Let λ be one of these eigenvalues, and denote the corresponding eigenvector by $\tilde{U}^1$. By Theorem 2.10 we extend $\tilde{U}^1$ to a basis for $\mathbb{C}^n$, and by the Gram-Schmidt process (Theorem 2.21) we assume that this basis is orthonormal. From our discussion above, we see that this basis may be used as the columns of a unitary matrix $\tilde{U}$ with $\tilde{U}^1$ as its first column. We then see that

$$\begin{aligned}(\tilde{U}^\dagger A\tilde{U})^1 &= \tilde{U}^\dagger(A\tilde{U})^1 = \tilde{U}^\dagger(A\tilde{U}^1) = \tilde{U}^\dagger(\lambda\tilde{U}^1) = \lambda(\tilde{U}^\dagger\tilde{U}^1) \\ &= \lambda(\tilde{U}^\dagger\tilde{U})^1 = \lambda I^1\end{aligned}$$

and hence $\tilde{U}^\dagger A\tilde{U}$ has the form

$$\tilde{U}^\dagger A\tilde{U} = \begin{pmatrix} \lambda & * & \cdots & * \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$$

where $B \in M_{n-1}(\mathbb{C})$ and the *'s are (in general) nonzero scalars. By our induction hypothesis, we may choose a unitary matrix $W \in M_{n-1}(\mathbb{C})$ such that $W^\dagger BW$ is upper-triangular. Let $V \in M_n(\mathbb{C})$ be a unitary matrix of the form

$$V = \begin{pmatrix} 1 & 0 \cdots 0 \\ 0 & \\ \vdots & \boxed{W} \\ 0 & \end{pmatrix}$$

and define the unitary matrix $U = \tilde{U}V \in M_n(\mathbb{C})$. Then

$$U^\dagger AU = (\tilde{U}V)^\dagger A(\tilde{U}V) = V^\dagger(\tilde{U}^\dagger A\tilde{U})V$$

is upper-triangular since (in an obvious shorthand notation)

$$V^\dagger(\tilde{U}^\dagger A\tilde{U})V = \begin{pmatrix} 1 & 0 \\ 0 & W^\dagger \end{pmatrix}\begin{pmatrix} \lambda & * \\ 0 & B \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & W \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & W^\dagger \end{pmatrix}\begin{pmatrix} \lambda & * \\ 0 & BW \end{pmatrix}$$
$$= \begin{pmatrix} \lambda & * \\ 0 & W^\dagger BW \end{pmatrix}$$

and $W^\dagger BW$ is upper-triangular by the induction hypothesis.

Noting that $\lambda I - U^\dagger AU$ is upper-triangular, it is easy to see (using Theorem 4.5) that the roots of $\det(\lambda I - U^\dagger AU)$ are just the diagonal entries of $U^\dagger AU$. But

$$\det(\lambda I - U^\dagger AU) = \det[U^\dagger(\lambda I - A)U] = \det(\lambda I - A)$$

so that A and $U^\dagger AU$ have the same eigenvalues. ∎

Corollary If $A \in M_n(\mathbb{R})$ has all its eigenvalues in $\mathbb{R}$, then the matrix U defined in Theorem 8.1 may be chosen to have all real entries.

Proof If $\lambda \in \mathbb{R}$ is an eigenvalue of A, then $A - \lambda I$ is a real matrix with determinant $\det(A - \lambda I) = 0$, and therefore the homogeneous system of equations $(A - \lambda I)X = 0$ has a real solution. Defining $\tilde{U}^1 = X$, we may now proceed as in Theorem 8.1. The details are left to the reader (see Exercise 8.8.1). ∎

We say that two matrices $A, B \in M_n(\mathbb{C})$ are **unitarily similar** (written $A \sim B$) if there exists a unitary matrix U such that $B = U^\dagger AU = U^{-1}AU$. Since this

defines an equivalence relation on the set of all matrices in $M_n(\mathbb{C})$, many authors say that A and B are **unitarily equivalent**. However, we will be using the term "equivalent" in a somewhat more general context later in this chapter, and the word "similar" is in accord with our earlier terminology.

We leave it to the reader to show that if A and B are unitarily similar and A is normal, then B is also normal (see Exercise 8.8.2). In particular, suppose that U is unitary and N is such that $U^\dagger NU = D$ is diagonal. Since any diagonal matrix is automatically normal, it follows that N must be normal also. We now show that the converse is also true, i.e., that any normal matrix is unitarily similar to a diagonal matrix.

To see this, suppose N is normal, and let $U^\dagger NU = D$ be the Schur canonical form of N. Then D is both upper-triangular and normal (since it is unitarily similar to a normal matrix). We claim that the only such matrices are diagonal. For, consider the (1, 1) elements of $DD^\dagger$ and $D^\dagger D$. From what we showed above, we have

$$(DD^\dagger)_{11} = \langle D_1, D_1 \rangle = |d_{11}|^2 + |d_{12}|^2 + \cdots + |d_{1n}|^2$$

and

$$(D^\dagger D)_{11} = \langle D^1, D^1 \rangle = |d_{11}|^2 + |d_{21}|^2 + \cdots + |d_{n1}|^2 \ .$$

But D is upper-triangular so that $d_{21} = \cdots = d_{n1} = 0$. By normality we must have $(DD^\dagger)_{11} = (D^\dagger D)_{11}$, and therefore $d_{12} = \cdots = d_{1n} = 0$ also. In other words, with the possible exception of the (1, 1) entry, all entries in the first row and column of D must be zero. In the same manner, we see that

$$(DD^\dagger)_{22} = \langle D_2, D_2 \rangle = |d_{21}|^2 + |d_{22}|^2 + \cdots + |d_{2n}|^2$$

and

$$(D^\dagger D)_{22} = \langle D^2, D^2 \rangle = |d_{12}|^2 + |d_{22}|^2 + \cdots + |d_{n2}| \ .$$

Since the fact that D is upper-triangular means $d_{32} = \cdots = d_{n2} = 0$ and we just showed that $d_{21} = d_{12} = 0$, it again follows by normality that $d_{23} = \cdots = d_{2n} = 0$. Thus all entries in the second row and column with the possible exception of the (2, 2) entry must be zero.

Continuing this procedure, it is clear that D must be diagonal as claimed. In other words, *an upper-triangular normal matrix is necessarily diagonal*. This discussion proves the following very important theorem.

Theorem 8.2 A matrix $N \in M_n(\mathbb{C})$ is normal if and only if there exists a unitary matrix U such that $U^\dagger NU$ is diagonal.

Corollary If $A = (a_{ij}) \in M_n(\mathbb{R})$ is symmetric, then there exists an orthogonal matrix S such that $S^T AS$ is diagonal.

Proof If we can show that a real symmetric matrix has all real eigenvalues, then this corollary will follow from the corollary to Theorem 8.1 and the real analogue of the proof of Theorem 8.2. Now suppose $A = A^T$ so that $a_{ij} = a_{ji}$. If λ is an eigenvalue of A, then there exists a (nonzero and not necessarily real) vector $x \in \mathbb{C}^n$ such that $Ax = \lambda x$ or

$$\sum_{j=1}^{n} a_{ij}x_j = \lambda x_i \quad . \tag{1}$$

Multiplying (1) by x_i^*, summing over i and using the standard inner product on $\mathbb{C}^n$ we obtain

$$\sum_{i,j=1}^{n} x_i^* a_{ij} x_j = \lambda \|x\|^2 \quad . \tag{2}$$

On the other hand, we may take the complex conjugate of (1), then multiply by x_i and sum over i to obtain (since each a_{ij} is real)

$$\sum_{i,j=1}^{n} x_i a_{ij} x_j^* = \lambda^* \|x\|^2 \quad . \tag{3}$$

But $a_{ij} = a_{ji}$ and therefore the left hand side of (3) becomes

$$\sum_{i,j=1}^{n} x_i a_{ij} x_j^* = \sum_{i,j=1}^{n} x_j^* a_{ji} x_i = \sum_{i,j=1}^{n} x_i^* a_{ij} x_j$$

where in the last step we relabelled the index i by j and the index j by i. Since this shows that the left hand sides of (2) and (3) are equal, it follows that $\lambda = \lambda^*$ as claimed. ∎

We will return to this theorem in Chapter 10 where it will be proved in an entirely different manner.

Exercises

1. Finish the proof of the corollary to Theorem 8.1.

2. Show that if $A, B \in M_n(\mathbb{C})$ are unitarily similar and A is normal, then B is also normal.

3. Suppose $A, B \in M_n(\mathbb{C})$ commute (i.e., $AB = BA$).
   (a) Prove there exists a unitary matrix U such that $U^\dagger AU$ and $U^\dagger BU$ are both upper-triangular. [*Hint*: Let $V_\lambda \subset \mathbb{C}^n$ be the eigenspace of B corresponding to the eigenvalue λ. Show that V_λ is invariant under A, and

hence show that A and B have a common eigenvector $\tilde{U}^1$. Now proceed as in the proof of Theorem 8.1.]
(b) Show that if A and B are also normal, then there exists a unitary matrix U such that $U^\dagger AU$ and $U^\dagger BU$ are diagonal.

4. Can every matrix $A \in M_n(\mathbb{C})$ be written as a product of two unitary matrices? Explain.

5. (a) Prove that if H is Hermitian, then det H is real.
(b) Is it the case that every square matrix A can be written as the product of finitely many Hermitian matrices? Explain.

6. A matrix M is **skew-Hermitian** if $M^\dagger = -M$.
(a) Show that skew-Hermitian matrices are normal.
(b) Show that any square matrix A can be written as a sum of a skew-Hermitian matrix and a Hermitian matrix.

7. Describe all diagonal unitary matrices. Prove that any n x n diagonal matrix can be written as a finite sum of unitary diagonal matrices. [*Hint*: Do the cases n = 1 and n = 2 to get the idea.]

8. Using the previous exercise, show that any n x n normal matrix can be written as the sum of finitely many unitary matrices.

9. If A is unitary, does this imply that $\det A^k = 1$ for some integer k? What if A is a real unitary matrix (i.e., orthogonal)?

10. (a) Is an n x n matrix A that is similar (but not necessarily *unitarily* similar) to a Hermitian matrix necessarily Hermitian?
(b) If A is similar to a normal matrix, is A necessarily normal?

11. If N is normal and $Nx = \lambda x$, prove that $N^\dagger x = \lambda^* x$. [*Hint*: First treat the case where N is diagonal.]

12. Does the fact that A is similar to a diagonal matrix imply that A is normal?

13. Discuss the following conjecture: If N_1 and N_2 are normal, then $N_1 + N_2$ is normal if and only if $N_1N_2^\dagger = N_2^\dagger N_1$.

14. (a) If $A \in M_n(\mathbb{R})$ is nonzero and skew-symmetric, show that A can not have any real eigenvalues.
(b) What can you say about the eigenvalues of such a matrix?
(c) What can you say about the rank of A?

15. Let $\sigma \in S_n$ be a permutation, and let f: {1, . . . , n} → {+1, −1}. Define the **signed permutation matrix** P_σ^f by

$$P_\sigma^f(i, j) = \begin{cases} f(j) & \text{if } \sigma(j) = i \\ 0 & \text{otherwise} \end{cases}.$$

Show that signed permutation matrices are orthogonal.

16. (a) Prove that a real n x n matrix A that commutes with all n-square real orthogonal matrices is a multiple of I_n. [*Hint*: Show that the matrices E_{ij} of Section 3.6 can be represented as sums of signed permutation matrices.]
(b) What is true for a complex matrix that commutes with all unitary matrices?

8.2 MATRICES OVER THE RING OF POLYNOMIALS

For the remainder of this chapter we will be discussing matrices with polynomial entries. Unfortunately, this requires some care since the ring of polynomials $\mathcal{F}[x]$ does not form a field (see Theorem 6.2, Corollary 3). However, the reader should recall that it is possible to embed $\mathcal{F}[x]$ (or any integral domain for that matter) in a field of quotients as we saw in Section 6.5 (see Theorem 6.16). This simply means that quotients (i.e., rational functions) such as f(x)/g(x) are defined (if $g \neq 0$), along with their inverses g(x)/f(x) (if $f \neq 0$).

First of all, we will generally restrict ourselves to only the real and complex number fields. In other words, $\mathcal{F}$ will be taken to mean either $\mathbb{R}$ or $\mathbb{C}$ unless otherwise stated. Next, we introduce some additional simplifying notation. We denote $\mathcal{F}[x]$ (the ring of polynomials) by $\mathcal{P}$, and the associated field of quotients by $\mathcal{R}$ (think of $\mathcal{P}$ as meaning polynomial and $\mathcal{R}$ as meaning ratio). Thus, an m x n matrix with polynomial entries is an element of $M_{mxn}(\mathcal{P})$, and an m x n matrix over the field of quotients is an element of $M_{m\ x\ n}(\mathcal{R})$. Note that $M_{mxn}(\mathcal{P})$ is actually a subset of $M_{mxn}(\mathcal{R})$ since any polynomial p(x) may be written as p(x)/1.

It is important to realize that since $\mathcal{R}$ is a field, all of our previous results apply to $M_{mxn}(\mathcal{R})$ just as they do to $M_{mxn}(\mathcal{F})$. However, we need to reformulate some of our definitions in order to handle $M_{mxn}(\mathcal{P})$. In other words, as

long as we allow all operations in $\mathcal{R}$ there is no problem. Where we must be careful is when we restrict ourselves to multiplication by polynomials only (rather than by rational functions). To begin with, we must modify the definition of elementary row and column operations that we gave in Section 3.2. In particular, we now define the **$\mathcal{P}$-elementary** row (column) operations as follows. The type α operation remains the same, the type β operation is multiplication by $c \in \mathcal{F}$, and the type γ operation is now taken to be the addition of a polynomial multiple of one row (column) to another. In other words, if A_i is the i*th* row of $A \in M_{m \times n}(\mathcal{P})$, then the $\mathcal{P}$-elementary operations are:

(α) Interchange A_i and A_j.
(β) $A_i \rightarrow cA_i$ where $c \in \mathcal{F}$.
(γ) $A_i \rightarrow A_i + pA_j$ where $p \in \mathcal{P}$.

With these modifications, it is easy to see that all of our discussion on the techniques of reduction to row-echelon form remains valid, although now the distinguished elements of the matrix (i.e., the first nonzero entry in each row) will in general be polynomials (which we will assume to be monic). In other words, the row-echelon form of a matrix $A \in M_n(\mathcal{P})$ will in general be an upper-triangular matrix in $M_n(\mathcal{P})$ (which may, however, have zeros on the main diagonal). However, if $A \in M_n(\mathcal{P})$ is nonsingular, then $r(A) = n$, and the row-echelon form of A will be upper-triangular with nonzero monic polynomials down the main diagonal. (This is true since $M_n(\mathcal{P}) \subset M_n(\mathcal{R})$, and hence all of our results dealing with the rank remain valid for elements of $M_n(\mathcal{P})$). In other words, the row-echelon form of $A \in M_n(\mathcal{P})$ will be

$$\begin{pmatrix} p_{11} & p_{12} & p_{13} & \cdots & p_{1n} \\ 0 & p_{22} & p_{23} & \cdots & p_{2n} \\ 0 & 0 & p_{33} & \cdots & p_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & p_{nn} \end{pmatrix}$$

where each $p_{ij} \in \mathcal{P}$.

Example 8.2 Let us illustrate the basic approach in applying $\mathcal{P}$-elementary operations. For notational simplicity we will consider only the first column of a matrix $A \in M_3(\mathcal{P})$. Thus, suppose we have

$$\begin{pmatrix} x^2 - 2x + 1 \\ x - 1 \\ x^2 + 2 \end{pmatrix}.$$

Multiplying the second row by −x and adding to the third yields

$$\begin{pmatrix} x^2 - 2x + 1 \\ x - 1 \\ x + 2 \end{pmatrix}.$$

Adding −1 times the second row to the third and then multiplying the third by 1/3 now yields

$$\begin{pmatrix} x^2 - 2x + 1 \\ x - 1 \\ 1 \end{pmatrix}.$$

Adding −(x − 1) times the third row to the second, and $-(x^2 - 2x + 1)$ times the third to the first gives us

$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Finally, interchanging rows 1 and 3 will put this into row-echelon form. Note that while we came up with a field element in this last form, we could have ended up with some other nonconstant polynomial.

We now repeat this procedure on column 2, but only on rows 2 and 3 since only these rows have zeros in the first column. This results in a matrix that will in general have nonzero elements in row 1 of column 1, in rows 1 and 2 of column 2, and in all three rows of column 3. It should now be clear that when applied to any $A \in M_n(\mathcal{P})$, this procedure will result in an upper-triangular matrix. //

A moments thought should convince the reader that it will not be possible in general to transform a matrix in $M_n(\mathcal{P})$ to reduced row-echelon form if we allow only $\mathcal{P}$-elementary operations. For example, if the row-echelon form of $A \in M_2(\mathcal{P})$ is

$$\begin{pmatrix} x^2 + 1 & 2x - 3 \\ 0 & x^2 \end{pmatrix}$$

then it is impossible to add any polynomial multiple of the second row to the first to eliminate the $2x - 3$ term. This is exactly the type of difference that occurs between operations in the ring $\mathcal{P}$ and those in the field $\mathcal{R}$.

It should also be clear that we can define $\mathcal{P}$-elementary matrices in the obvious way, and that each $\mathcal{P}$-elementary matrix is also in $M_n(\mathcal{P})$. Moreover, each $\mathcal{P}$-elementary matrix has an inverse which is also in $M_n(\mathcal{P})$, as is its transpose (see Theorem 3.23). In addition, Theorem 4.5 remains valid for matrices over $\mathcal{P}$, as does Theorem 4.4 since replacing row A_i by $A_i + pA_j$ where p is a polynomial also has no effect on det A. This shows that if we reduce a matrix $A \in M_n(\mathcal{P})$ to its row-echelon form $\tilde{A}$, then the fact that $\tilde{A}$ is upper-triangular means that

$$\det \tilde{A} = k \det A$$

where k is a unit in $\mathcal{P}$ (recall from Example 6.4 that the units of the ring $\mathcal{P} = \mathcal{F}[x]$ are just the elements of $\mathcal{F}$, i.e., the nonzero constant polynomials). We will refer to units of $\mathcal{P}$ as (nonzero) **scalars**.

We say that a matrix $A \in M_n(\mathcal{P})$ is a **unit matrix** if A^{-1} exists and is also an element of $M_n(\mathcal{P})$. (Do not confuse a unit matrix with the identity matrix.) Note this is more restrictive than to say that $A \in M_n(\mathcal{P})$ is merely invertible, because we now also require that A^{-1} have entries only in $\mathcal{P}$, whereas in general it could have entries in $\mathcal{R}$. From our discussion above, we see that $\mathcal{P}$-elementary matrices are also unit matrices. The main properties of unit matrices that we shall need are summarized in the following theorem.

Theorem 8.3 If $A \in M_n(\mathcal{P})$ and $\tilde{A} \in M_n(\mathcal{P})$ is the row-echelon form of A, then

(a) A is a unit matrix if and only if A can be row-reduced to $\tilde{A} = I$.
(b) A is a unit matrix if and only if det A is a nonzero scalar.
(c) A is a unit matrix if and only if A is a product of $\mathcal{P}$-elementary matrices.

Proof (a) If A is a unit matrix, then A^{-1} exists so that $r(A) = n$ (Theorem 3.21). This means that the row-echelon form of A is an upper-triangular matrix $\tilde{A} = (p_{ij}) \in M_n(\mathcal{P})$ with n nonzero diagonal entries. Since $AA^{-1} = I$, it follows that $(\det A)(\det A^{-1}) = 1$ (Theorem 4.8 is also still valid) and hence $\det A \neq 0$. Furthermore, since both det A and $\det A^{-1}$ are in $\mathcal{P}$, Theorem 6.2(b) shows us that $\deg(\det A) = \deg(\det A^{-1}) = 0$ and thus det A is a scalar. Our discussion above showed that

$$k \det A = \det \tilde{A} = \prod_{i=1}^{n} p_{ii}$$

where k is a scalar, and therefore each polynomial p_{ii} must also be of degree zero (i.e., a scalar). In this case we can apply $\mathcal{P}$-elementary row operations to further reduce $\tilde{A}$ to the identity matrix I.

Conversely, if A is row-equivalent to $\tilde{A} = I$, then we may write

$$E_1 \cdots E_r A = I$$

where each $E_i \in M_n(\mathcal{P})$ is an elementary matrix. It follows that A^{-1} exists and is given by $A^{-1} = E_1 \cdots E_r \in M_n(\mathcal{P})$. Thus A is a unit matrix.

(b) If A is a unit matrix, then the proof of part (a) showed that det A is a nonzero scalar. On the other hand, if det A is a nonzero scalar, then the proof of part (a) showed that $\tilde{A} = E_1 \cdots E_r A = I$, and hence $A^{-1} = E_1 \cdots E_r \in M_n(\mathcal{P})$ so that A is a unit matrix.

(c) If A is a unit matrix, then the proof of part (a) showed that A may be written as a product of $\mathcal{P}$-elementary matrices. Conversely, if A is the product of $\mathcal{P}$-elementary matrices, then we may write $A = E_r^{-1} \cdots E_1^{-1} \in M_n(\mathcal{P})$. Therefore $A^{-1} = E_1 \cdots E_r \in M_n(\mathcal{P})$ also and hence A is a unit matrix. ∎

Recall from Section 5.4 that two matrices A, $B \in M_n(\mathcal{F})$ are said to be similar if there exists a nonsingular matrix $S \in M_n(\mathcal{F})$ such that $A = S^{-1}BS$. In order to generalize this, we say that two matrices A, $B \in M_{m\times n}(\mathcal{P})$ are equivalent over $\mathcal{P}$ if there exist unit matrices $P \in M_m(\mathcal{P})$ and $Q \in M_n(\mathcal{P})$ such that A = PBQ. The reader should have no trouble showing that this defines an equivalence relation on the set of all m x n matrices over $\mathcal{P}$.

Note that since P and Q are unit matrices, they may be written as a product of $\mathcal{P}$-elementary matrices (Theorem 8.3). Now recall from our discussion at the end of Section 3.8 that multiplying B from the right by an elementary matrix E has the same effect on the columns of B as multiplying from the left by E^T does on the rows. We thus conclude that if A and B are equivalent over $\mathcal{P}$, then A is obtainable from B by a sequence of $\mathcal{P}$-elementary row and column operations. Conversely, if A is obtainable from B by a sequence of $\mathcal{P}$-elementary row and column operations, the fact that each $E_i \in M_n(\mathcal{P})$ is a unit matrix means that A and B are $\mathcal{P}$-equivalent.

Theorem 8.4 (a) Two matrices A, $B \in M_{m\times n}(\mathcal{P})$ are equivalent over $\mathcal{P}$ if and only if A can be obtained from B by a sequence of $\mathcal{P}$-elementary row and column operations.

(b) $\mathcal{P}$-equivalent matrices have the same rank.

Proof (a) This was proved in the preceding discussion.

(b) Suppose A, B $\in M_{m\times n}(\mathcal{P})$ and A = PBQ where P $\in M_m(\mathcal{P})$ and Q $\in M_n(\mathcal{P})$ are unit matrices and hence nonsingular. Then, applying the corollary to Theorem 3.20, we have

$$\begin{aligned} r(A) = r(PBQ) &\le \min\{r(P), r(BQ)\} = \min\{m, r(BQ)\} = r(BQ) \\ &\le \min\{r(B), r(Q)\} = r(B) \ . \end{aligned}$$

Similarly, we see that $r(B) = r(P^{-1}AQ^{-1}) \le r(A)$ and hence r(A) = r(B). ∎

Another point that should be clarified is the following computational technicality that we will need to apply several times in the remainder of this chapter. Referring to Section 6.1, we know that the product of two polynomials $p(x) = \sum_{i=0}^{m} a_i x^i$ and $q(x) = \sum_{j=0}^{n} b_j x^j$ is given by

$$p(x)q(x) = \sum_{k=0}^{m+n} \sum_{t=0}^{k} a_t x^t b_{k-t} x^{k-t}$$

where we have been careful to write everything in its original order. In the special case that x, a_i, $b_j \in \mathcal{F}$, this may be written in the more common and simpler form

$$p(x)q(x) = \sum_{k=0}^{m+n} c_k x^k$$

where $c_k = \sum_{t=0}^{k} a_t b_{k-t}$. However, we will need to evaluate the product of two polynomials when the coefficients as well as the indeterminate x are matrices. In this case, none of the terms in the general form for pq can be assumed to commute with each other, and we shall have to be very careful in evaluating such products. We do though, have the following useful special case.

Theorem 8.5 Let $p(x) = \sum_{i=0}^{m} a_i x^i$ and $q(x) = \sum_{j=0}^{n} b_j x^j$ be polynomials with (matrix) coefficients a_i, $b_j \in M_s(\mathcal{F})$, and let $r(x) = \sum_{k=0}^{m+n} c_k x^k$ where $c_k = \sum_{t=0}^{k} a_t b_{k-t}$. Then if A $\in M_s(\mathcal{F})$ commutes with all of the $b_j \in M_s(\mathcal{F})$, we have p(A)q(A) = r(A).

Proof We simply compute using $Ab_j = b_jA$:

$$\begin{aligned} p(A)q(A) &= \sum_{k=0}^{m+n} \sum_{t=0}^{k} a_t A^t b_{k-t} A^{k-t} = \sum_{k=0}^{m+n} \sum_{t=0}^{k} a_t b_{k-t} A^k \\ &= \sum_{k=0}^{m+n} c_k A^k = r(A) \ . \ ∎ \end{aligned}$$

What this theorem has shown us is that if A commutes with all of the b_j, then we may use the simpler form for the product of two polynomials. As an interesting application of this result, we now give yet another (very simple) proof of the **Cayley-Hamilton theorem**. Suppose $A \in M_n(\mathcal{F})$, and consider its characteristic matrix $xI - A$ along with the characteristic polynomial $\Delta_A(x) = \det(xI - A)$. Writing equation (1b) of Section 4.3 in matrix notation we obtain

$$[\text{adj}(xI - A)](xI - A) = \Delta_A(x)I \ .$$

Now notice that any matrix with polynomial entries may be written as a polynomial with (constant) matrix coefficients (see the proof of Theorem 7.10). Then $\text{adj}(xI - A)$ is just a polynomial in x of degree $n - 1$ with (constant) matrix coefficients, and $xI - A$ is similarly a polynomial in x of degree 1. Since A obviously commutes with I and A, we can apply Theorem 8.5 with $p(x) = \text{adj}(xI - A)$ and $q(x) = xI - A$ to obtain $p(A)q(A) = \Delta_A(A)$. But $q(A) = 0$, and hence we find that $\Delta_A(A) = 0$.

The last technical point that we wish to address is the possibility of dividing two polynomials with matrix coefficients. The reason that this is a problem is that all of our work in Chapter 6 was based on the assumption that we were dealing with polynomials over a field, and the set of all square matrices of any fixed size certainly does not in general form a field. Referring back to the proof of the division algorithm (Theorem 6.3), we see that the process of dividing $f(x) = a_m x^m + \cdots + a_1 x + a_0$ by $g(x) = b_n x^n + \cdots + b_1 x + b_0$ depends on the existence of b_n^{-1}. This then allows us to show that $x - c$ is a factor of f(x) if and only if c is a root of f(x) (Corollary to Theorem 6.4).

We would like to apply Theorem 6.4 to a special case of polynomials with matrix coefficients. Thus, consider the polynomials $f(x) = B_n x + \cdots + B_1 x + B_0$ and $g(x) = xI - A$ where $A, B_i \in M_n(\mathcal{F})$. In this case, I is obviously invertible and we may divide g(x) into f(x) in the usual manner. The first two terms of the quotient q(x) are then given by

$$\begin{array}{r} B_n x^{n-1} + (B_{n-1} + B_n A)x^{n-2} \\ \hline xI - A \,\big)\, B_n x^n + B_{n-1}x^{n-1} + \cdots + B_1 x + B_0 \\ \underline{B_n x^n - B_n A x^{n-1}} \\ (B_{n-1} + B_n A)x^{n-1} \end{array}$$

It should now be clear (using Theorem 8.5) that Theorem 6.4 applies in this special case, and if $f(A) = 0$, then we may write $f(x) = q(x)(xI - A)$. In other words, if A is a root of f(x), then $xI - A$ is a factor of f(x). Note that in order

to divide $f(x) = B_n x^n + \cdots + B_0$ by $g(x) = A_m x^m + \cdots + A_0$, only the leading coefficient A_m of $g(x)$ need be invertible.

Let us also point out that because matrix multiplication is not generally commutative, the order in which we multiply the divisor and quotient is important when dealing with matrix coefficients. We will adhere to the convention used in the above example.

Another point that we should take note of is the following. Two polynomials $p(x) = \sum_{k=0}^{m} A_k x^k$ and $q(x) = \sum_{k=0}^{m} B_k x^k$ with coefficients in $M_n(\mathcal{F})$ are defined to be equal if $A_k = B_k$ for every $k = 1, \ldots, m$. For example, recalling that x is just an indeterminate, we consider the polynomial $p(x) = A_0 + A_1 x = A_0 + xA_1$. If $C \in M_n(\mathcal{F})$ does not commute with A_1 (i.e., $CA_1 \neq A_1 C$), then $A_0 + A_1 C \neq A_0 + CA_1$. This means that going from an equality such as $p(x) = q(x)$ to $p(C) = q(C)$ must be done with care in that the same convention for placing the indeterminate be applied to both $p(x)$ and $q(x)$.

Exercise

Determine whether or not each of the following matrices is a unit matrix by verifying each of the properties listed in Theorem 8.3:

$$(a)\ \begin{pmatrix} x+2 & 1 & -3x^3-6x^2 \\ 2x+6 & 2 & -6x^3-18x^2 \\ x^2+2x & x^2+x+1 & -3x^4-6x^3-3 \end{pmatrix}$$

$$(b)\ \begin{pmatrix} x+1 & x^2 & -2 \\ x^2-1 & x^3-x^2 & x+7 \\ 3x^2+3x & 3 & 0 \end{pmatrix}$$

$$(c)\ \begin{pmatrix} x^2+3x+2 & 0 & x & x^3-3x^2 \\ 2x^2+4x & x^2 & 0 & x-3 \\ x+2 & -x^2 & 1 & x^2-3x \\ 3x+6 & -6x^2 & 3 & 3x^2-9x \end{pmatrix}$$

8.3 THE SMITH CANONICAL FORM

If the reader has not studied (or does not remember) the Cauchy-Binet theorem (Section 4.6), now is the time to go back and read it. We will need this result several times in what follows, as well as the notation defined in that section.

We know that the norm of any integer is just its absolute value, and the greatest common divisor of a set of nonzero integers is just the largest *positive* integer that divides them all. Similarly, we define the **norm** of any polynomial to be its degree, and the **greatest common divisor** (frequently denoted by gcd) of a set of nonzero polynomials is the polynomial of highest degree that divides all of them. By convention, we will assume that the gcd is monic (i.e., the leading coefficient is 1).

Suppose $A \in M_{mxn}(\mathcal{P})$, and assume that $1 \le k \le \min\{m, n\}$. If A has at least one nonzero k-square subdeterminant, then we define f_k to be the greatest common divisor of all k*th* order subdeterminants of A. In other words,

$$f_k = \gcd\{\det A[\alpha|\beta]: \alpha \in INC(k, m), \beta \in INC(k, n)\} .$$

If there is no nonzero k*th* order subdeterminant, then we define $f_k = 0$. Furthermore, for notational convenience we define $f_0 = 1$. The numbers f_k are called the **determinantal divisors** of A. We will sometimes write $f_k(A)$ if there is more than one matrix under consideration.

Example 8.3 Suppose

$$A = \begin{pmatrix} x & 2x^2 & 1 \\ x^3 & x+2 & x^2 \\ x+2 & x-1 & 0 \end{pmatrix} .$$

Then the sets of nonzero 1-, 2- and 3-square subdeterminants are, respectively,

$$\{x, 2x^2, 1, x^3, x + 2, x^2, x + 2, x - 1\}$$

$$\{-x(2x^4 - x - 2), 2x^4 - x - 2, x^4 - x^3 - x^2 - 4x - 4, -x^2(x + 2), -x^2(x - 1), -x(2x^2 + 3x + 1), -(x + 2), -(x - 1)\}$$

$$\{2x^5 + 4x^4 - x^2 - 4x - 4\}$$

and hence $f_1 = 1$, $f_2 = 1$ and $f_3 = x^5 + 2x^4 - (1/2)x^2 - 2x - 2$. //

Our next result contains two very simple but important properties of determinantal divisors. Recall that the notation p|q means p divides q.

Theorem 8.6 (a) If $f_k = 0$, then $f_{k+1} = 0$.
(b) If $f_k \neq 0$, then $f_k | f_{k+1}$.

Proof Using Theorem 6.6, it is easy to see that these are both immediate consequences of Theorem 4.10 since a $(k + 1)$*th* order subdeterminant may be written as a linear combination of k*th* order subdeterminants. ∎

If $A \in M_{mxn}(\mathcal{P})$ has rank r, then Theorem 4.12 tells us that $f_r \neq 0$ while $f_{r+1} = 0$. Hence, according to Theorem 8.6(b), we may define the quotients q_k by

$$f_k = q_k f_{k-1}$$

for each $k = 1, \ldots, r$. The polynomials q_k are called the **invariant factors** of A. Note that $f_0 = 1$ implies $f_1 = q_1$, and hence

$$f_k = q_k f_{k-1} = q_k q_{k-1} f_{k-2} = \cdots = q_k q_{k-1} \cdots q_1 .$$

Because each f_k is defined to be monic, it follows that each q_k is also monic. Moreover, the unique factorization theorem (Theorem 6.6) shows that each q_k $(k = 1, \ldots, r)$ can be factored uniquely (except for order) into products of powers of prime (i.e., irreducible) polynomials as

$$q_k = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$$

where $p_1, \ldots, p_s$ are *all* the distinct prime factors of the invariant factors, and each e_i is a nonnegative integer. Of course, since every q_k will not necessarily contain all of the p_i's as factors, some of the e_i's may be zero.

Each of the factors $p_i^{e_i}$ for which $e_i > 0$ is called an **elementary divisor** of A. We count an elementary divisor once for each time that it appears as a factor of an invariant factor. This is because a given elementary divisor can appear as a factor in more than one invariant factor. Note also that the elementary divisors clearly depend on the field under consideration (see Example 6.7). However, the elementary divisors of a matrix over $\mathbb{C}[x]$ are always powers of linear polynomials (Theorem 6.13). As we shall see following Theorem 8.8 below, the list of elementary divisors determines the list of invariant factors, and hence the determinantal divisors.

Example 8.4 Let A_1 be the 3 x 3 matrix

$$A_1 = \begin{pmatrix} x & -1 & 0 \\ 0 & x & -1 \\ -1 & 1 & x-1 \end{pmatrix}$$

and note that $\det A_1 = (x - 1)(x^2 + 1)$. Now consider the block diagonal matrix

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_1 \end{pmatrix} .$$

Using Theorem 4.14, we immediately find

$$f_6 = \det A = (x - 1)^2(x^2 + 1)^2 .$$

We now observe that every 5 x 5 submatrix of A is either block triangular with a 3 x 3 matrix on its diagonal that contains one zero row (so the determinant is zero), or else is block diagonal with A_1 as one of the blocks (you should try to write out some of these and see this for yourself). Therefore

$$f_5 = (x - 1)(x^2 + 1)$$

and hence

$$q_6 = f_6/f_5 = (x - 1)(x^2 + 1) .$$

As to f_4, we see that some of the 4 x 4 subdeterminants contain $\det A_1$ while others (such as the one obtained by deleting both rows and columns 3 and 4) do not contain any factors in common with this. Thus $f_4 = 1$ and we must have $q_5 = f_5$. Since $f_6 = q_1q_2 \cdots q_6$, it follows that $q_4 = q_3 = q_2 = q_1 = 1$.

If we regard A as a matrix over $\mathbb{R}[x]$, then the elementary divisors of A are $x - 1$, $x^2 + 1$, $x - 1$, $x^2 + 1$. However, if we regard A as a matrix over $\mathbb{C}[x]$, then its elementary divisors are $x - 1$, $x + i$, $x - i$, $x - 1$, $x + i$, $x - i$. //

Theorem 8.7 Equivalent matrices have the same determinantal divisors.

Proof Suppose that A = PBQ. Applying the Cauchy-Binet theorem (the corollary to Theorem 4.15), we see that any k*th* order subdeterminant of A is just a sum of multiples of k*th* order subdeterminants of B. But then the gcd of all k*th* order subdeterminants of B must divide all the k*th* order subdeterminants of A. In other words, $f_k(B)|f_k(A)$. Conversely, writing $B = P^{-1}AQ^{-1}$ we see that $f_k(A)|f_k(B)$, and therefore $f_k(A) = f_k(B)$. ∎

From Example 8.4 (which was based on a relatively simple block diagonal matrix), it should be obvious that a brute force approach to finding invariant factors leaves much to be desired. The proof of our next theorem is actually nothing more than an algorithm for finding the invariant factors of any matrix A. The matrix B defined in the theorem is called the **Smith canonical** (or **normal**) **form** of A. After the proof, we give an example that should clarify the various steps outlined in the algorithm.

Theorem 8.8 (**Smith Canonical Form**) Suppose $A \in M_{m \times n}(\mathcal{P})$ has rank r. Then A has precisely r + 1 nonzero determinantal divisors $f_0, f_1, \ldots, f_r$, and A is equivalent over $\mathcal{P}$ to a unique diagonal matrix $B = (b_{ij}) \in M_{m \times n}(\mathcal{P})$ with $b_{ii} = q_i = f_i/f_{i-1}$ for $i = 1, \ldots, r$ and $b_{ij} = 0$ otherwise. Moreover $q_i | q_{i+1}$ for each $i = 1, \ldots, r - 1$.

Proof While we have already seen that A has precisely r + 1 nonzero determinantal divisors, this will also fall out of the proof below. Furthermore, the uniqueness of B follows from the fact that equivalence classes are disjoint, along with Theorem 8.7 (because determinantal divisors are defined to be monic). As to existence, we assume that $A \neq 0$ or it is already in Smith form. Note in the following that all we will do is perform a sequence of $\mathcal{P}$-elementary row and column operations on A. Recall that if E is an elementary matrix, then EA represents the same elementary row operation applied to A, and AE^T is the same operation applied to the columns of A. Therefore, what we will finally arrive at is a matrix of the form B = PAQ where $P = E_{i_1} \cdots E_{i_r}$ and $Q = E_{j_1}{}^T \cdots E_{j_s}{}^T$. Recall also that the norm of a polynomial is defined to be its degree.

Step 1. Search A for a nonzero entry of least norm and bring it to the (1, 1) position by row and column interchanges. By subtracting the appropriate multiples of row 1 from rows 2, . . . , m, we obtain a matrix in which every element of column 1 below the (1, 1) entry is either 0 or of smaller norm than the (1, 1) entry. Now perform the appropriate column operations to make every element of row 1 to the right of the (1, 1) entry either 0 or of smaller norm than the (1, 1) entry. Denote this new matrix by $\tilde{A}$.

Step 2. Search the first row and column of $\tilde{A}$ for a nonzero entry of least norm and bring it to the (1, 1) position. Now repeat the procedure of Step 1 to decrease the norm of every element of the first row and column outside the (1, 1) position by at least 1. Repeating this step a finite number of times, we must eventually arrive at a matrix A_1 equivalent to A which is 0 everywhere in the first row and column outside the (1, 1) position. Let us denote the (1, 1) entry of A_1 by a.

Step 3. Suppose b is the (i, j) element of A_1 (where $i, j > 1$) and $a \nmid b$. If no such b exists, then go on to Step 4. Put b in the (1, j) position by adding row i

to row 1. Since $a \nmid b$, we may write $b = aq + r$ where $r \neq 0$ and $\deg r < \deg a$ (Theorem 6.3). We place r in the (1, j) position by subtracting q times column 1 from column j. This results in a matrix with an entry of smaller norm than that of a. Now repeat Steps 1 and 2 with this matrix to obtain a new matrix A_2 equivalent to A which is 0 everywhere in the first row and column outside the (1, 1) position.

This process is repeated with A_2 to obtain A_3 and so forth. We thus obtain a sequence $A_1, A_2, \ldots, A_s$ of matrices in which the norms of the (1, 1) entries are strictly decreasing, and in which all elements of row 1 and column 1 are 0 outside the (1, 1) position. Furthermore, we go on from A_p to obtain A_{p+1} only as long as there is an element of $A_p(1|1)$ that is not divisible by the (1, 1) element of A_p. Since the norms of the (1, 1) entries are strictly decreasing, this process must terminate with a matrix $C = (c_{ij}) \in M_{m\times n}(\mathcal{P})$ equivalent to A and having the following properties:

(i) $c_{11} | c_{ij}$ for every $i, j > 1$;
(ii) $c_{1j} = 0$ for every $j = 2, \ldots, n$;
(iii) $c_{i1} = 0$ for every $i = 2, \ldots, m$.

Step 4. Now repeat the entire procedure on the matrix C, except that this time apply the $\mathcal{P}$-elementary row and column operations to rows $2, \ldots, m$ and columns $2, \ldots, n$. This will result in a matrix $D = (d_{ij})$ that has all 0 entries in the first two rows and columns except for the (1, 1) and (2, 2) entries. Since $c_{11} | c_{ij}$ (for $i, j > 1$), it follows that $c_{11} | d_{ij}$ for all i, j. (This true because every element of D is just a linear combination of elements of C.) Thus the form of D is

$$D = \begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ 0 & d & \cdots & 0 \\ \vdots & \vdots & G & \\ 0 & 0 & & \end{pmatrix}$$

where $G = (g_{ij}) \in M_{(m-2)\times(n-2)}(\mathcal{P})$, $c_{11} | d$ and $c_{11} | g_{ij}$ for $i = 1, \ldots, m-2$ and $j = 1, \ldots, n-2$. It is clear that we can continue this process until we eventually obtain a diagonal matrix $H = (h_{ij}) \in M_{m\times n}(\mathcal{P})$ with the property that $h_{ii} | h_{i+1\, i+1}$ and $h_{i+1\, i+1} \neq 0$ for $i = 1, \ldots, p-1$ (where $p = \operatorname{rank} H$). But H is equivalent to A so that H and A have the same determinantal divisors (Theorem 8.7) and $p = r(H) = r(A) = r$ (Theorem 8.4(b)).

For each k with $1 \leq k \leq r$, we observe that the only nonzero k-square subdeterminants of H are of the form $\prod_{s=1}^{k} h_{i_s i_s}$, and the gcd of all such products is

$$f_k = \prod_{i=1}^{k} h_{ii}$$

(since $h_{ii}|h_{i+1\ i+1}$ for i = 1, . . . , r − 1). But then applying the definition of invariant factors, we see that

$$\prod_{i=1}^{k} h_{ii} = f_k = \prod_{i=1}^{k} q_i \quad .$$

In particular, this shows us that

$$\begin{aligned} h_{11} &= q_1 \\ h_{11}h_{22} &= q_1q_2 \\ &\vdots \\ h_{11}\cdots h_{rr} &= q_1\cdots q_r \end{aligned}$$

and hence $h_{22} = q_2$, . . . , $h_{rr} = q_r$ also. In other words, H is precisely the desired matrix B. Finally, note that $h_{ii}|h_{i+1\ i+1}$ is just the statement that $q_i|q_{i+1}$. ∎

Suppose $A \in M_{mxn}(\mathcal{P})$ has rank r, and suppose that we are given a list of all the elementary divisors of A. From Theorem 8.8, we know that $q_i|q_{i+1}$ for i = 1, . . . , r − 1. Therefore, to compute the invariant factors of A, we first multiply together the highest powers of all the *distinct* primes that appear in the list of elementary divisors. This gives us q_r. Next, we multiply together the highest powers of the remaining distinct primes to obtain q_{r-1} . Continuing this process until the list of elementary divisors is exhausted, suppose that q_k is the last invariant factor so obtained. If k > 1, we then set $q_1 = \cdots = q_{k-1} = 1$. The reader should try this on the list of elementary divisors given at the end of Example 8.4.

Corollary If $A, B \in M_{mxn}(\mathcal{P})$, then A is $\mathcal{P}$-equivalent to B if and only if A and B have the same invariant factors (or determinantal divisors or elementary divisors).

Proof Let A_S and B_S be the Smith forms for A and B. If A and B have the same invariant factors then they have the same Smith form. If we denote $\mathcal{P}$-equivalence by ≈ , then $A \approx A_S = B_S \approx B$ so that A ≈ B. Conversely, if A ≈ B then $A \approx B \approx B_S$ implies that $A \approx B_S$, and hence the uniqueness of A_S implies that $A_S = B_S$, and thus A and B have the same invariant factors.

If we recall Theorem 6.6, then the statement for elementary divisors follows immediately. Now note that $f_0 = 1$ so that $f_1 = q_1$, and in general we then have $f_k = q_kf_{k-1}$. This takes care of the statement for determinantal divisors. ∎

Example 8.5 Consider the matrix A given in Example 7.3. We shall compute the invariant factors of the associated characteristic matrix xI − A. The reason for using the characteristic matrix will become clear in a later section. According to Step 1, we obtain the following sequence of equivalent matrices. Start with

$$xI - A = \begin{pmatrix} x-2 & -1 & 0 & 0 \\ 0 & x-2 & 0 & 0 \\ 0 & 0 & x-2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

Put −1 in the (1, 1) position:

$$\begin{pmatrix} -1 & x-2 & 0 & 0 \\ x-2 & 0 & 0 & 0 \\ 0 & 0 & x-2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

Add x − 2 times row 1 to row 2, and x − 2 times column 1 to column 2:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & (x-2)^2 & 0 & 0 \\ 0 & 0 & x-2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

Since all entries in row 1 and column 1 are 0 except for the (1, 1) entry, this last matrix is A_1 and we have also finished Step 2. Furthermore, there is no element $b \in A_1$ that is not divisible by −1, so we go on to Step 4 applied to the 3 x 3 matrix in the lower right hand corner. In this case, we first apply Step 1 and then follow Step 3. We thus obtain the following sequence of matrices. Put x − 2 in the (2, 2) position:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & x-2 & 0 & 0 \\ 0 & 0 & (x-2)^2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

$(x-2) \nmid (x-5)$ so add row 4 to row 2:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & x-2 & 0 & x-5 \\ 0 & 0 & (x-2)^2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

Note $x - 5 = 1(x - 2) + (-3)$, so subtract 1 times column 2 from column 4:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & x-2 & 0 & -3 \\ 0 & 0 & (x-2)^2 & 0 \\ 0 & 0 & 0 & x-5 \end{pmatrix}.$$

Now put -3 in the (2, 2) position:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -3 & 0 & x-2 \\ 0 & 0 & (x-2)^2 & 0 \\ 0 & x-5 & 0 & 0 \end{pmatrix}.$$

Add $(x - 5)/3$ times row 2 to row 4, and then add $(x - 2)/3$ times column 2 to column 4 to obtain

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & (x-2)^2 & 0 \\ 0 & 0 & 0 & (x-2)(x-5)/3 \end{pmatrix}.$$

Elementary long division (see Example 6.2) shows that $(x - 2)(x - 5)/3$ divided by $(x - 2)^2$ equals $1/3$ with a remainder of $-x + 2$. Following Step 3, we add row 4 to row 3 and then subtract 1/3 times column 3 from column 4 to obtain

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & (x-2)^2 & -x+2 \\ 0 & 0 & 0 & (x-2)(x-5)/3 \end{pmatrix}.$$

Going back to Step 1, we first put $-x + 2 = -(x - 2)$ in the (3, 3) position. We then add $(x - 5)/3$ times row 3 to row 4 and $(x - 2)$ times column 3 to column 4 resulting in

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & -(x-2) & 0 \\ 0 & 0 & 0 & (x-2)^2(x-5)/3 \end{pmatrix}.$$

Lastly, multiplying each row by a suitable nonzero scalar we obtain the final (unique) Smith form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x-2 & 0 \\ 0 & 0 & 0 & (x-2)^2(x-5) \end{pmatrix}. \quad /\!/$$

Exercises

1. Find the invariant factors of the matrix A given in Example 8.4 by using the list of elementary divisors also given in that example.

2. For each of the following matrices A, find the invariant factors of the characteristic matrix xI – A:

(a) $\begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix}$ (b) $\begin{pmatrix} 0 & 1 & -1 \\ -4 & 4 & -2 \\ -2 & 1 & 1 \end{pmatrix}$

(c) $\begin{pmatrix} 2 & -4 & 2 & 2 \\ -2 & 0 & 1 & 3 \\ -2 & -2 & 3 & 3 \\ -2 & -6 & 3 & 7 \end{pmatrix}$ (d) $\begin{pmatrix} 0 & -3 & 1 & 2 \\ -2 & 1 & -1 & 2 \\ -2 & 1 & -1 & 2 \\ -2 & -3 & 1 & 4 \end{pmatrix}$

8.4 SIMILARITY INVARIANTS

Recall that A, B $\in M_n(\mathcal{F})$ are similar over $\mathcal{F}$ if there exists a nonsingular matrix S $\in M_n(\mathcal{F})$ such that $A = S^{-1}BS$. Note that similar matrices are therefore also equivalent, although the converse is certainly not true (since in general $P \neq Q^{-1}$ in our definition of equivalent matrices). For our present purposes however, the following theorem is quite useful.

Theorem 8.9 Two matrices A, B $\in M_n(\mathcal{F})$ are similar over $\mathcal{F}$ if and only if their characteristic matrices xI − A and xI − B are equivalent over $\mathcal{P} = \mathcal{F}[x]$. In particular, if xI − A = P(xI − B)Q where $Q^{-1} = R_m x^m + \cdots + R_1 x + R_0$, then $A = S^{-1}BS$ where $S^{-1} = R_m B^m + \cdots + R_1 B + R_0$.

Proof If A and B are similar, then there exists a nonsingular matrix S $\in M_n(\mathcal{F})$ for which $A = S^{-1}BS$, and hence

$$xI - A = xI - S^{-1}BS = S^{-1}(xI - B)S \ .$$

But S is a unit matrix in $M_n(\mathcal{P})$, and therefore xI − A and xI − B are $\mathcal{P}$-equivalent.

On the other hand, if xI − A and xI − B are $\mathcal{P}$-equivalent, then there exist unit matrices P, Q $\in M_n(\mathcal{P})$ such that

$$xI - A = P(xI - B)Q \ .$$

We wish to find a matrix S $\in M_n(\mathcal{F})$ for which $A = S^{-1}BS$. Since Q $\in M_n(\mathcal{P})$ is a unit matrix, we may apply Theorem 4.11 to find its inverse R $\in M_n(\mathcal{P})$ which is also a unit matrix and hence will also have polynomial entries. In fact, we may write (as in the proof of Theorem 7.10)

$$R = R_m x^m + R_{m-1} x^{m-1} + \cdots + R_1 x + R_0 \qquad (1)$$

where m is the highest degree of any polynomial entry of R and each $R_i \in M_n(\mathcal{F})$.

From xI − A = P(xI − B)Q and the fact that P and Q are unit matrices we have

$$P^{-1}(xI - A) = (xI - B)Q = Qx - BQ \ . \qquad (2)$$

Now recall Theorem 8.5 and the discussion following its proof. If we write both P^{-1} and Q $\in M_n(\mathcal{P})$ in the same form as we did in (1) for R, then we may replace x by A in the resulting polynomial expression for Q to obtain a matrix

$W \in M_n(\mathcal{F})$. Since A commutes with I and A, and $B \in M_n(\mathcal{F})$, we may apply Theorem 8.5 and replace x by A on both sides of (2), resulting in

$$0 = WA - BW \ .$$

Since R is the inverse of Q and $Qx^i = x^iQ$, we have RQ = I or (from (1))

$$R_mQx^m + R_{m-1}Qx^{m-1} + \cdots + R_1Qx + R_0Q = I \ .$$

Replacing x by A in this expression yields

$$\sum_{i=0}^{m} R_i W A^i = I \ . \tag{3}$$

But WA = BW so that $WA^2 = BWA = B^2W$ and, by induction, it follows that $WA^i = B^iW$. Using this in (3) we have

$$\left(\sum_{i=0}^{m} R_i B^i\right) W = I$$

so defining

$$S^{-1} = \sum_{i=0}^{m} R_i B^i \in M_n(\mathcal{F}) \tag{4}$$

we see that $S^{-1} = W^{-1}$ and hence W = S. Finally, noting that WA = BW implies $A = W^{-1}BW$, we arrive at $A = S^{-1}BS$ as desired. ∎

Corollary 1 Two matrices $A, B \in M_n(\mathcal{F})$ are similar if and only if their characteristic matrices have the same invariant factors (or elementary divisors).

Proof This follows directly from Theorem 8.9 and the corollary to Theorem 8.8. ∎

Corollary 2 If A and B are in $M_n(\mathbb{R})$, then A and B are similar over $\mathbb{C}$ if and only if they are similar over $\mathbb{R}$.

Proof Clearly, if A and B are similar over $\mathbb{R}$ then they are also similar over $\mathbb{C}$. On the other hand, suppose that A and B are similar over $\mathbb{C}$. We claim that the algorithm in the proof of Theorem 8.9 yields a real S if A and B are real. From the definition of S in the proof of Theorem 8.9 (equation (4)), we see that S will be real if all of the R_i are real (since each B^i is real by hypothesis), and this in turn requires that Q be real (since $R = Q^{-1}$). That P and Q can indeed be chosen to be real is left as an exercise for the reader (see Exercise 8.4.1). ∎

The invariant factors of the characteristic matrix of A are called the **similarity invariants** of A. We will soon show that the similarity invariant of highest degree is just the minimal polynomial for A.

Example 8.6 Let us show that the matrices

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$$

are similar over $\mathbb{R}$. We have the characteristic matrices

$$xI - A = \begin{pmatrix} x-1 & -1 \\ -1 & x-1 \end{pmatrix} \qquad \text{and} \qquad xI - B = \begin{pmatrix} x & 0 \\ 0 & x-2 \end{pmatrix}$$

and hence the determinantal divisors are easily seen to be $f_1(A) = 1$, $f_2(A) = x(x-2)$, $f_1(B) = 1$, $f_2(B) = x(x-2)$. Thus $f_1(A) = f_1(B)$ and $f_2(A) = f_2(B)$ so that A and B must be similar by the corollary to Theorem 8.9.

For the sake of illustration, we will show how to compute the matrix S^{-1} following the method used in the proof of Theorem 8.9 (see equation (4)). While there is no general method for finding the matrices P and Q, the reader can easily verify that if we choose

$$P = \begin{pmatrix} 1 & x^2 - x + 1 \\ -1 & -x^2 + x + 1 \end{pmatrix} \qquad Q = \frac{1}{2}\begin{pmatrix} -x^2 + 3x - 1 & -x^2 + 3x - 1 \\ 1 & 1 \end{pmatrix}$$

then $xI - A = P(xI - B)Q$. It is then easy to show that

$$\begin{aligned} R = Q^{-1} &= \begin{pmatrix} 1 & x^2 - 3x + 3 \\ -1 & -x^2 + 3x - 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}x^2 + \begin{pmatrix} 0 & -3 \\ 0 & -3 \end{pmatrix}x + \begin{pmatrix} 1 & 3 \\ -1 & -1 \end{pmatrix} \end{aligned}$$

and hence (from (4)) we have

$$S^{-1} = \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}^2 + \begin{pmatrix} 0 & -3 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 3 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} . \ \text{//}$$

Now recall the definition of minimal polynomial given in Section 7.3 (see the discussion following the proof of Theorem 7.10). We also recall that the minimal polynomial m(x) for $A \in M_n(\mathcal{F})$ divides the characteristic polynomial $\Delta_A(x)$. In the particular case that $m(x) = \Delta_A(x)$, the matrix A is called **nonderogatory**, and if $m(x) \neq \Delta_A(x)$, then (as you might have guessed) A is said to be **derogatory**. Our next theorem is of fundamental importance.

Theorem 8.10 The minimal polynomial m(x) for $A \in M_n(\mathcal{F})$ is equal to its similarity invariant of highest degree.

Proof Since $\Delta_A(x) = \det(xI - A)$ is just a (monic) polynomial of degree n in x, it is clearly nonzero, and hence $q_n(x)$, the similarity invariant of highest degree, is also nonzero. Now define the matrix $Q(x) = \text{adj}(xI - A)$, and note that the entries of Q(x) are precisely all the (n − 1)-square subdeterminants of xI − A. This means $f_{n-1}(x)$ (i.e., the $(n-1)$*th* determinantal divisor of xI − A) is just the monic gcd of all the entries of Q(x), and therefore we may write

$$Q(x) = f_{n-1}(x)D(x)$$

where the matrix D(x) has entries that are relatively prime. Noting that by definition we have $\Delta_A(x) = f_n(x) = q_n(x)f_{n-1}(x)$, it follows that

$$f_{n-1}(x)D(x)(xI - A) = Q(x)(xI - A) = \Delta_A(x)I = q_n(x)f_{n-1}(x)I \tag{1}$$

where we used equation (1b) of Section 4.3. Since $f_{n-1}(x) \neq 0$ (by Theorem 8.6(a) and the fact that $f_n(x) \neq 0$), we must have

$$D(x)(xI - A) = q_n(x)I \tag{2}$$

(this follows by equating the polynomial entries of the matrices on each side of (1) and then using Corollary 2(b) of Theorem 6.2).

By writing both sides of (2) as polynomials with matrix coefficients and then applying Theorem 8.5, it follows that $q_n(A) = 0$ and hence $m(x)|q_n(x)$ (Theorem 7.4). We may now define the polynomial p(x) by writing

$$q_n(x) = m)x)p(x) \ . \tag{3}$$

By definition, A is a root of m(x), and therefore our discussion at the end of Section 8.2 tells us that we may apply Theorem 6.4 to write

$$m(x)I = C(x)(xI - A)$$

where C(x) is a polynomial with matrix coefficients. Using this in (2) we have

$$D(x)(xI - A) = q_n(x)I = p(x)m(x)I = p(x)C(x)(xI - A) \tag{4}$$

where we used the fact that m(x) and p(x) are just polynomials with scalar coefficients so that m(x)p(x) = p(x)m(x).

Since $\det(xI - A) \neq 0$, we know that $(xI - A)^{-1}$ exists over $M_n(\mathcal{R})$, and thus (4) implies that

$$D(x) = p(x)C(x) \ .$$

Now regarding both D(x) and C(x) as matrices with polynomial entries, this equation shows that p(x) divides each of the entries of D(x). But the entries of D(x) are relatively prime, and hence p(x) must be a unit (i.e., a nonzero scalar). Since both m(x) and $q_n(x)$ are monic by convention, (3) implies that p(x) = 1, and therefore $q_n(x) = m(x)$. ∎

Corollary A matrix $A \in M_n(\mathcal{F})$ is nonderogatory if and only if its first n − 1 similarity invariants are equal to 1.

Proof Let A have characteristic polynomial $\Delta_A(x)$ and minimal polynomial m(x). Using the definition of invariant factors and Theorem 8.10 we have

$$\begin{aligned}\Delta_A(x) = \det(xI - A) = f_n(x) &= q_n(x)q_{n-1}(x)\cdots q_1(x) \\ &= m(x)q_{n-1}(x)\cdots q_1(x) \ .\end{aligned}$$

Clearly, if $q_{n-1}(x) = \cdots = q_1(x) = 1$ then $\Delta_A(x) = m(x)$. On the other hand, if $\Delta_A(x) = m(x)$, then $q_{n-1}(x) \cdots q_1(x) = 1$ (Theorem 6.2, Corollary 2(b)) and hence each $q_i(x)$ (i = 1, . . . , n − 1) is a nonzero scalar (Theorem 6.2, Corollary 3). Since each $q_k(x)$ is defined to be monic, it follows that $q_{n-1}(x) = \cdots = q_1(x) = 1$. ∎

Example 8.7 Comparison of Examples 7.3 and 8.8 shows that the minimal polynomial of the matrix A is indeed the same as its similarity invariant of highest degree. //

Exercises

1. Finish the proof of Corollary 2 to Theorem 8.9.

2. Show that the minimal polynomial for $A \in M_n(\mathcal{F})$ is the least common multiple of the elementary divisors of $xI - A$.

3. If $(x^2 - 4)^4$ is the minimal polynomial of an n-square matrix A, can $A^6 - A^4 + A^2 - I_n$ ever be zero? If $(x^2 - 4)^3$ is the minimal polynomial, can $A^8 - A^4 + A^2 - I_n = 0$? Explain.

4. Is the matrix
$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$
derogatory or nonderogatory? Explain.

5. Suppose A is an n-square matrix and p is a polynomial with complex coefficients. If $p(A) = 0$, show that $p(SAS^{-1}) = 0$ for any nonsingular n-square S. Is this true if p is a polynomial with n-square matrices as coefficients?

6. Prove or disprove:
(a) The elementary divisors of A are all linear if and only if the characteristic polynomial of A is a product of distinct linear factors.
(b) The elementary divisors of A are all linear if and only if the minimal polynomial of A is a product of distinct linear factors.

7. Prove or disprove:
(a) There exists a real nonsingular matrix S such that $SAS^{-1} = B$ where
$$A = \begin{pmatrix} 3 & 0 \\ -1 & 2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 4 & 2 \\ -1 & 1 \end{pmatrix}.$$
(b) There exists a complex nonsingular matrix S such that $SAS^{-1} = B$ where
$$A = \begin{pmatrix} 3 & 0 \\ -1 & 2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 4 & 2i \\ i & 1 \end{pmatrix}.$$

8.5 THE RATIONAL CANONICAL FORM

Given any monic polynomial $p(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0 \in \mathcal{F}[x]$, the matrix $C(p(x)) \in M_n(\mathcal{F})$ defined by

$$C(p(x)) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{n-1} \end{pmatrix}$$

is called the **companion matrix** of the polynomial p(x). If there is no possible ambiguity, we will denote the companion matrix simply by C. The companion matrix has several interesting properties that we will soon discover. We will also make use of the associated characteristic matrix $xI - C \in M_n(\mathcal{R})$ given by

$$xI - C = \begin{pmatrix} x & 0 & \cdots & 0 & 0 & -a_0 \\ -1 & x & \cdots & 0 & 0 & -a_1 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & x & -a_{n-2} \\ 0 & 0 & \cdots & 0 & -1 & x - a_{n-1} \end{pmatrix}.$$

Our next theorem is quite useful.

Theorem 8.11 Let $p(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0 \in \mathcal{F}[x]$ have companion matrix C. Then $\det(xI - C) = p(x)$.

Proof We proceed by induction on the degree of p(x). If n = 1, then $p(x) = x - a_0$, $C = (a_0)$ and $xI - C = (x - a_0)$ so that

$$\det(xI - C) = x - a_0 = p(x) .$$

Now assume that the theorem is true for all polynomials of degree less than n, and suppose deg p(x) = n > 1. If we expand det(xI – C) by minors of the first row, we obtain (see Theorem 4.10)

$$\det(xI - C) = x \det C_{11} + (-a_0)(-1)^{n+1} \det C_{1n}$$

where the minor matrices C_{11} and C_{1n} are given by

$$C_{11} = \begin{pmatrix} x & 0 & \cdots & 0 & 0 & -a_1 \\ -1 & x & \cdots & 0 & 0 & -a_2 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & x & -a_{n-2} \\ 0 & 0 & \cdots & 0 & -1 & x - a_{n-1} \end{pmatrix}$$

$$C_{1n} = \begin{pmatrix} -1 & x & 0 & \cdots & 0 & 0 \\ 0 & -1 & x & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & x \\ 0 & 0 & 0 & \cdots & 0 & -1 \end{pmatrix} .$$

Defining the polynomial $p'(x) = x^{n-1} - a_{n-1}x^{n-2} - \cdots - a_2x - a_1$ along with its companion matrix C', we see that $C_{11} = xI - C'$. By our induction hypothesis, it then follows that

$$\det C_{11} = \det(xI - C') = p'(x) .$$

Next we note that C_{1n} is an upper-triangular matrix, and hence (by Theorem 4.5) $\det C_{1n} = (-1)^{n-1}$. Putting all of this together we find that

$$\det(xI - C) = xp'(x) - a_0 = p(x) . \blacksquare$$

Recall that two matrix representations are similar if and only if they represent the same underlying operator in two different bases (see Theorem 5.18).

Theorem 8.12 (a) The companion matrix $C = C(p(x))$ of any monic polynomial $p(x) \in \mathcal{F}[x]$ has $p(x)$ as its minimal polynomial $m(x)$.

(b) If $\dim V = n$ and $T \in L(V)$ has minimal polynomial $m(x)$ of degree n, then $C(m(x))$ represents T relative to some basis for V.

Proof (a) From the preceding proof, we see that deleting the first row and n*th* column of $xI - C$ and taking the determinant yields $\det C_{1n} = (-1)^{n-1}$. Therefore $f_{n-1}(x) = 1$ so that $q_1(x) = q_2(x) = \cdots = q_{n-1}(x) = 1$. Hence C is nonderogatory (corollary to Theorem 8.10), so that by Theorem 8.11 we have $m(x) = q_n(x) = \det(xI - C) = p(x)$.

(b) Note $\dim V = \deg \Delta_T(x) = n = \deg m(x)$ so that any $[T]$ has similarity invariants $q_1(x) = \cdots = q_{n-1}(x) = 1$ and $q_n(x) = m(x)$ (see Theorem 8.10 and its corollary). Since the proof of part (a) showed that $C = C(m(x))$ has the

same similarity invariants as [T], it follows from Corollary 1 of Theorem 8.9 that C and [T] are similar. ∎

Note that Theorems 8.11 and 8.12(a) together show that the companion matrix is nonderogatory.

Given any $A \in M_n(\mathcal{F})$, we can interpret A as the matrix representation of a linear transformation T on an n-dimensional vector space V. If A has minimal polynomial m(x) with deg m(x) = n, then so does T (by Theorem 7.1). Hence the companion matrix C of m(x) represents T relative to some basis for V (Theorem 8.12(b)). This means that A is similar to C (Theorem 5.18), and therefore $C = P^{-1}AP$ for some nonsingular transition matrix $P \in M_n(\mathcal{F})$. But then

$$xI - C = xI - P^{-1}AP = P^{-1}(xI - A)P$$

and hence det(xI − C) = det(xI − A) by Theorem 4.8 and its corollary. Using Theorem 8.11, we then have the following result.

Theorem 8.13 Let $A \in M_n(\mathcal{F})$ have minimal polynomial m(x) of degree n. Then m(x) = det(xI − A).

Our next theorem is a useful restatement of what we have done so far in this section.

Theorem 8.14 Let $p(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0 \in \mathcal{F}[x]$. Then the companion matrix C(p(x)) is nonderogatory, and its characteristic polynomial $\Delta_C(x)$ and minimal polynomial m(x) both equal p(x). Moreover, xI − C is equivalent over $\mathcal{P}$ to the n x n matrix (the Smith canonical form of xI − C)

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & p(x) \end{pmatrix}.$$

For notational convenience, we sometimes write a diagonal matrix by listing its diagonal entries. For example, the matrix shown in the above theorem would be written as diag(1, . . . , 1, p(x)).

Theorem 8.15 If $A \in M_n(\mathcal{F})$, then A is similar over $\mathcal{F}$ to the direct sum of the companion matrices of its nonunit similarity invariants.

Proof The proof is an application of Theorem 8.9. Assume that $A \neq cI$ (where $c \in \mathcal{F}$) or there is nothing to prove. Hence $f_1(x)$, the first determinantal divisor of $xI - A$, must be 1. But $f_0(x) = 1$ by definition, and hence we have $f_1(x) = q_1(x)f_0(x) = q_1(x) = 1$. Since at least $q_1(x) = 1$, we now assume that in fact the first k similarity invariants of A are equal to 1. In other words, we assume that $q_1(x) = \cdots = q_k(x) = 1$, and then $\deg q_i(x) = d_i \geq 1$ for $i = k + 1, \ldots, n$.

Since $f_n(x) = q_1(x) \cdots q_n(x)$, Theorem 6.2(b) tells us that $\deg f_n(x) = \sum_{j=1}^{n} \deg q_j(x)$ and hence (using $\deg q_j = 0$ for $j = 1, \ldots, k$)

$$n = \deg \Delta_A(x) = \deg f_n(x) = \sum_{j=k+1}^{n} \deg q_j(x) = \sum_{j=k+1}^{n} d_j \quad .$$

Let $Q_i = C(q_i(x)) \in M_{d_i}(\mathcal{P})$ for $i = k + 1, \ldots, n$. We want to show that $xI - A$ is equivalent over $\mathcal{P}$ to

$$xI - (Q_{k+1} \oplus \cdots \oplus Q_n) = (xI - Q_{k+1}) \oplus \cdots \oplus (xI - Q_n) \quad .$$

(Note that each of the identity matrices in this equation may be of a different size.)

It should be clear that the Smith form of $xI - A$ is the diagonal $n \times n$ matrix

$$(xI - A)_S = \operatorname{diag}(q_1(x), \ldots, q_n(x)) = \operatorname{diag}(1, \ldots, 1, q_{k+1}(x), \ldots, q_n(x)) \quad .$$

From Theorem 8.14, we know that $(xI - Q_i)_S = \operatorname{diag}(1, \ldots, 1, q_i(x)) \in M_{d_i}(\mathcal{P})$. Since $\sum_{i=k+1}^{n} d_i = n$, we now see that by suitable row and column interchanges we have

$$xI - A \approx (xI - A)_S \approx (xI - Q_{k+1})_S \oplus \cdots \oplus (xI - Q_n)_S \qquad (*)$$

where $\approx$ denotes equivalence over $\mathcal{P}$.

If we write $(xI - Q_i)_S = E_i(xI - Q_i)F_i$ where E_i and F_i are unit matrices, then (by multiplying out the block diagonal matrices) it is easy to see that

$$\begin{aligned} &E_{k+1}(xI - Q_{k+1})F_{k+1} \oplus \cdots \oplus E_n(xI - Q_n)F_n \\ &\quad = [E_{k+1} \oplus \cdots \oplus E_n][(xI - Q_{k+1}) \oplus \cdots \oplus (xI - Q_n)][F_{k+1} \oplus \cdots \oplus F_n] \quad . \end{aligned}$$

Since the direct sum of unit matrices is clearly a unit matrix (so that both $E_{k+1} \oplus \cdots \oplus E_n$ and $F_{k+1} \oplus \cdots \oplus F_n$ are unit matrices), this shows that the right hand side of (*) is equivalent to $(xI - Q_{k+1}) \oplus \cdots \oplus (xI - Q_n)$. (Note we have shown that if $\{S_i\}$ and $\{T_i\}$ are finite collections of matrices such that $S_i \approx T_i$, then it follows that $S_1 \oplus \cdots \oplus S_n \approx T_1 \oplus \cdots \oplus T_n$.) Therefore $xI - A$

is equivalent to $xI - (Q_{k+1} \oplus \cdots \oplus Q_n)$ which is what we wanted to show. The theorem now follows directly from Theorem 8.9. ∎

We are now in a position to prove the **rational canonical form** theorem. Note that the name is derived from the fact that the rational form of a matrix is obtained by the application of a finite number of rational operations (which essentially constitute the Smith algorithm).

Theorem 8.16 (**Rational Canonical Form**) A matrix $A \in M_n(\mathcal{F})$ is similar over $\mathcal{F}$ to the direct sum of the companion matrices of the elementary divisors of $xI - A$.

Proof As in the proof of Theorem 8.15, we assume that the first k similarity invariants of A are $q_1(x) = \cdots = q_k(x) = 1$ and that $\deg q_i(x) = d_i \geq 1$ for $i = k + 1, \ldots, n$. Changing notation slightly from our first definition, we write each nonunit invariant factor as a product of powers of prime polynomials (i.e., as a product of elementary divisors): $q_i(x) = e_{i1}(x) \cdots e_{im_i}(x)$ for each $i = k + 1, \ldots, n$. From Theorem 8.14, we know that $xI - Q_i = xI - C(q_i(x))$ is $\mathcal{P}$-equivalent to the $d_i \times d_i$ matrix

$$B_i = \operatorname{diag}(1, \ldots, 1, q_i(x)) \ .$$

Similarly, if $c_{ij} = \deg e_{ij}(x)$, each $xI - C(e_{ij}(x))$ $(j = 1, \ldots, m_i)$ is $\mathcal{P}$-equivalent to a $c_{ij} \times c_{ij}$ matrix

$$D_{ij} = \operatorname{diag}(1, \ldots, 1, e_{ij}(x)) \ .$$

Since $\deg q_i(x) = \sum_j \deg e_{ij}(x)$, it follows that the block diagonal matrix

$$\begin{aligned} D_i &= D_{i1} \oplus \cdots \oplus D_{im_i} \\ &= \operatorname{diag}(1, \ldots, 1, e_{i1}(x)) \oplus \operatorname{diag}(1, \ldots, 1, e_{i2}(x)) \\ &\qquad \oplus \cdots \oplus \operatorname{diag}(1, \ldots, 1, e_{im_i}(x)) \end{aligned}$$

is also a $d_i \times d_i$ matrix. We first show that B_i (and hence also $xI - Q_i$) is $\mathcal{P}$-equivalent to D_i.

Consider the collection of all $(d_i - 1) \times (d_i - 1)$ subdeterminants of D_i. For each $r = 1, \ldots, m_i$, this collection will contain that subdeterminant obtained by deleting the row and column containing e_{ir}. In particular, this subdeterminant will be $\prod_{j \neq r} e_{ij}$. But the gcd of all such subdeterminants taken over r (for a fixed i of course) is just 1. (To see this, consider the product abcd. If we look at the collection of products obtained by deleting one of a, b, c or d we obtain {bcd, acd, abd, abc}. Since there is no factor in common with all four of these

products, it follows that the gcd of this collection is 1.) Therefore the $(d_i - 1)$*th* determinantal divisor $f_{d_i-1}(x)$ of D_i is 1, and hence the fact that $f_{k-1}(x)$ divides $f_k(x)$ means $f_1(x) = \cdots = f_{d_i-1}(x) = 1$ and $f_{d_i}(x) = \prod_j e_{ij}(x) = q_i(x)$. From the definition of determinantal divisor (or the definition of invariant factor along with the fact that B_i is in its Smith canonical form), it is clear that B_i has precisely these same determinantal divisors, and hence (by the corollary to Theorem 8.8) B_i must be $\mathcal{P}$-equivalent to D_i.

All that remains is to put this all together and apply Theorem 8.9 again. We now take the direct sum of each side of the equivalence relation $xI - Q_i \approx B_i \approx D_{i1} \oplus \cdots \oplus D_{im_i} = D_i$ using the fact that (as we saw in the proof of Theorem 8.15) $(xI - Q_{k+1}) \oplus \cdots \oplus (xI - Q_n) \approx D_{k+1} \oplus \cdots \oplus D_n$. It will be convenient to denote direct sums by $\Sigma\oplus$. For example, we have already seen it is true in general that

$$\sum_{i=k+1}^{n} \oplus (xI - Q_i) = xI - \sum_{i=k+1}^{n} \oplus Q_i$$

(where we again remark that the identity matrices in this equation may be of different dimensions). Therefore, we have shown that

$$\begin{aligned} xI - \sum_{i=k+1}^{n} \oplus Q_i &= \sum_{i=k+1}^{n} \oplus (xI - Q_i) \approx \sum_{i=k+1}^{n} \oplus (D_{i1} \oplus \cdots \oplus D_{im_i}) \\ &= \sum_{i=k+1}^{n} \oplus \left(\sum_{j=1}^{m_i} \oplus D_{ij} \right) \approx \sum_{i=k+1}^{n} \oplus \left(\sum_{j=1}^{m_i} \oplus [xI - C(e_{ij}(x))] \right) \\ &= xI - \sum_{i=k+1}^{n} \oplus \left(\sum_{j=1}^{m_i} \oplus C(e_{ij}(x)) \right) \end{aligned}$$

and hence $\Sigma_{i=k+1}^{n}\oplus Q_i$ is similar over $\mathcal{F}$ to $\Sigma_{i=k+1}^{n} \oplus [\Sigma_{j=1}^{m_i} \oplus C(e_{ij}(x))]$. But Theorem 8.15 tells us that A is similar over $\mathcal{F}$ to $\Sigma_{i=k+1}^{n}\oplus Q_i$, and therefore we have shown that A is similar over $\mathcal{F}$ to

$$\sum_{i=k+1}^{n} \oplus \left(\sum_{j=1}^{m_i} \oplus C(e_{ij}(x)) \right) . \quad \blacksquare$$

Example 8.8 Consider the polynomial

$$p(x) = (x - 1)^2(x^2 + 1)^2 = x^6 - 2x^5 + 3x^4 - 4x^3 + 3x^2 - 2x + 1 .$$

Its companion matrix is

$$C = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & -3 \\ 0 & 0 & 1 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & -3 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix} \in \mathrm{M}_6(\mathbb{R}) \ .$$

According to Theorem 8.14, C is nonderogatory and its minimal polynomial is p(x). Then by Theorem 8.10 and its corollary, the only nonunit similarity invariant of C is also p(x). This means that C is already in the form given by Theorem 8.15.

The elementary divisors (in $\mathbb{R}[x]$) of xI – C are

$$e_1(x) = (x - 1)^2 = x^2 - 2x + 1$$

and

$$e_2(x) = (x^2 + 1)^2 = x^4 + 2x^2 + 1 \ .$$

These have the companion matrices

$$C(e_1(x)) = \begin{pmatrix} 0 & -1 \\ 0 & 2 \end{pmatrix}$$

$$C(e_2(x)) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

and hence Theorem 8.16 tells us that C is similar over $\mathbb{R}$ to the direct sum $C(e_1(x)) \oplus C(e_2(x))$. We leave it to the reader to find the rational canonical form of C if we regard it as a matrix over $\mathbb{C}[x]$. //

Exercises

1. Prove Corollary 1 of Theorem 7.24 using the rational canonical form.

2. (a) Let V be a real 6-dimensional vector space, and suppose $T \in L(V)$ has minimal polynomial $m(x) = (x^2 - x + 3)(x - 2)^2$. Write down all possible rational canonical forms for T (except for the order of the blocks).
   (b) Let V be a real 7-dimensional vector space, and suppose $T \in L(V)$ has minimal polynomial $m(x) = (x^2 + 2)(x + 3)^3$. Write down all possible rational canonical forms for T (except for the order of the blocks).

3. Let A be a 4 x 4 matrix with minimal polynomial $m(x) = (x^2 + 1)(x^2 - 3)$. Find the rational canonical form if A is a matrix over:
   (a) The rational field $\mathbb{Q}$.
   (b) The real field $\mathbb{R}$.
   (c) The complex field $\mathbb{C}$.

4. Find the rational canonical form for the Jordan block

$$\begin{pmatrix} a & 1 & 0 & 0 \\ 0 & a & 1 & 0 \\ 0 & 0 & a & 1 \\ 0 & 0 & 0 & a \end{pmatrix}.$$

5. Find a 3 x 3 matrix A with integral entries such that $A^3 + 3A^2 + 2A + 2 = 0$. Prove that your matrix satisfies this identity.

6. Discuss the validity of each of the following assertions:
   (a) Two square matrices are similar if and only if they have the same eigenvalues (including multiplicities).
   (b) Two square matrices are similar if and only if they have the same minimal polynomial.
   (c) Two square matrices are similar if and only if they have the same elementary divisors.
   (d) Two square matrices are similar if and only if they have the same determinantal divisors.

7. Suppose $A = B \oplus C$ where B and C are square matrices. Is the list of elementary divisors of A equal to the list of elementary divisors of B concatenated with (i.e., "added on to") the list of elementary divisors of C? What if "elementary divisors" is replaced by "invariant factors" or "determinantal divisors" in this statement?

8.6 THE JORDAN CANONICAL FORM

We have defined a canonical form as that matrix representation A of a linear transformation $T \in L(V)$ that is of a particularly simple form in some basis for V. If all the eigenvalues of T lie in the base field $\mathcal{F}$, then the minimal polynomial m(x) for T will factor into a product of linear terms. In addition, if the eigenvalues are all distinct, then T will be diagonalizable (Theorem 7.24). But in the general case of repeated roots, we must (so far) fall back to the triangular form described in Chapter 7 and in Section 8.1. However, in this more general case there is another very important form that follows easily from what we have already done. If $A \in M_n(\mathbb{C})$, then (by Theorem 6.13) all the elementary divisors of $xI - A$ will be of the simple form $(x - a)^k$. We shall now investigate the "simplest" form that such an A can take.

To begin with, given a polynomial $p(x) = (x - a_0)^n \in \mathcal{F}[x]$, we define the **hypercompanion matrix** $H(p(x)) \in M_n(\mathcal{F})$ to be the upper-triangular matrix

$$\begin{pmatrix} a_0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & a_0 \end{pmatrix}.$$

A matrix of this form is also referred to as a **basic Jordan block** belonging to a_0. Now consider the characteristic matrix $xI - H(p(x))$. Note that if we delete the n*th* row and first column of this characteristic matrix, we obtain a lower-triangular matrix with all diagonal entries equal to -1, and hence its determinant is equal to $(-1)^{n-1}$. Thus the corresponding determinantal divisor $f_{n-1}(x)$ is equal to 1, and therefore $f_1(x) = \cdots = f_{n-1}(x) = 1$ (because $f_{k-1}(x) | f_k(x)$). Using $f_k(x) = q_k(x) f_{k-1}(x)$, it follows that $q_1(x) = \cdots = q_{n-1}(x) = 1$, and thus H is nonderogatory (corollary to Theorem 8.10). Since it is obvious that $\Delta_H(x) = (x - a_0)^n = p(x)$, we conclude that $\Delta_H(x) = m(x) = p(x)$. (Alternatively, by Theorem 8.10, we see that the minimal polynomial for H is $q_n(x) = f_n(x) = (x - a)^n$ which is also just the characteristic polynomial of H.) Along with the definition of the Smith canonical form, this proves the following result analogous to Theorem 8.14.

Theorem 8.17 The hypercompanion matrix $H(p(x))$ of the polynomial $p(x) = (x - a)^n \in \mathcal{F}[x]$ is nonderogatory, and its characteristic and minimal polynomials both equal p(x). Furthermore, the Smith form of $xI - H(p(x))$ is

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & p(x) \end{pmatrix}.$$

Theorems 8.14 and 8.17 show that given the polynomial $p(x) = (x - a)^n \in \mathbb{C}[x]$, both $C = C(p(x))$ and $H = H(p(x))$ have precisely the same similarity invariants. Using Theorem 8.16, we then see that C and H are similar over $\mathbb{C}$. Now, if $A \in M_n(\mathbb{C})$, we know that the elementary divisors of $xI - A$ will be of the form $(x - a)^k$. Furthermore, Theorem 8.16 shows us that A is similar over $\mathbb{C}$ to the direct sum of the companion matrices of these elementary divisors. But each companion matrix is similar over $\mathbb{C}$ to the corresponding hypercompanion matrix, and hence A is similar over $\mathbb{C}$ to the direct sum of the hypercompanion matrices of the elementary divisors of $xI - A$.

It may be worth briefly showing that the notions of similarity and direct sums may be treated in the manner just claimed. In other words, denoting similarity over $\mathbb{C}$ by $\sim$, we suppose that $A \sim C_1 \oplus C_2 = S^{-1}AS$ for some nonsingular matrix $S \in M_n(\mathbb{C})$. We now also assume that $C_i \sim H_i = T_i^{-1}C_iT_i$ for each $i = 1, 2$. Then we see that

$$\begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix} = \begin{pmatrix} T_1^{-1}C_1T_1 & 0 \\ 0 & T_2^{-1}C_2T_2 \end{pmatrix}$$

$$= \begin{pmatrix} T_1^{-1} & 0 \\ 0 & T_2^{-1} \end{pmatrix} \begin{pmatrix} C_1 & 0 \\ 0 & C_2 \end{pmatrix} \begin{pmatrix} T_1 & 0 \\ 0 & T_2 \end{pmatrix}$$

which (in an obvious shorthand notation) may be written in the form $H = T^{-1}CT$ if we note that

$$\begin{pmatrix} T_1^{-1} & 0 \\ 0 & T_2^{-1} \end{pmatrix} = \begin{pmatrix} T_1 & 0 \\ 0 & T_2 \end{pmatrix}^{-1}.$$

We therefore have $H = T^{-1}CT = T^{-1}S^{-1}AST = (ST)^{-1}A(ST)$ which shows that A is indeed similar to the direct sum of the hypercompanion matrices. In any case, we have proved the difficult part of the next very important theorem (see also Theorem 7.42).

Theorem 8.18 (**Jordan Canonical Form**) If $A \in M_n(\mathbb{C})$, then A is similar over $\mathbb{C}$ to the direct sum of the hypercompanion matrices of all the elementary divisors of $xI - A$, and this direct sum is unique except for the order of the blocks. Moreover, the numbers appearing on the main diagonal of the Jordan form are precisely the eigenvalues of A. (Note that the field $\mathbb{C}$ can be replaced by an arbitrary field $\mathcal{F}$ if all the eigenvalues of A lie in $\mathcal{F}$.)

Proof Existence was proved in the above discussion, so we now consider uniqueness. According to our general prescription, given a matrix $A \in M_n(\mathbb{C})$, we would go through the following procedure to find its Jordan form. First we reduce the characteristic matrix $xI - A$ to its *unique* Smith form, thus obtaining the similarity invariants of A. These similarity invariants are then factored (over $\mathbb{C}$) to obtain the elementary divisors of $xI - A$. Finally, the corresponding hypercompanion matrices are written down, and the Jordan form of A is just their direct sum.

All that remains is to prove the statement about the eigenvalues of A. To see this, recall that the eigenvalues of A are the roots of the characteristic polynomial $\det(xI - A)$. Suppose that $J = S^{-1}AS$ is the Jordan form of A. Then the eigenvalues of J are the roots of

$$\det(xI - J) = \det(xI - S^{-1}AS) = \det[S^{-1}(xI - A)S] = \det(xI - A)$$

so that A and J have the same eigenvalues. But J is an upper-triangular matrix, and hence the roots of $\det(xI - J)$ are precisely the diagonal entries of J. ∎

Example 8.9 Referring to Example 8.8, we regard C as a matrix over $M_6(\mathbb{C})$. Then its elementary divisors are $e_1(x) = (x - 1)^2$, $e_2(x) = (x + i)^2$ and $e_3(x) = (x - i)^2$. The corresponding hypercompanion matrices are

$$H_1 = H(e_1(x)) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$H_2 = H(e_2(x)) = \begin{pmatrix} -i & 1 \\ 0 & -i \end{pmatrix}$$

$$H_3 = H(e_3(x)) = \begin{pmatrix} i & 1 \\ 0 & i \end{pmatrix}$$

and therefore A is similar over $\mathbb{C}$ to its Jordan form $H_1 \oplus H_2 \oplus H_3$. //

Our next theorem is really a corollary to Theorem 8.18, but it is a sufficiently important result that we single it out by itself.

Theorem 8.19 The geometric multiplicity of an eigenvalue λ_i (i.e., $\dim V_{\lambda_i}$) belonging to a matrix $A \in M_n(\mathbb{C})$ is the number of elementary divisors of the characteristic matrix $xI - A$ that correspond to λ_i. In other words, the number of basic Jordan blocks (i.e., hypercompanion matrices) belonging to λ_i in the Jordan canonical form of A is the same as the geometric multiplicity of λ_i.

Proof Suppose that there are n_i elementary divisors belonging to λ_i, and let $\{H_{i1}, \ldots, H_{in_i}\}$ be the corresponding hypercompanion matrices. By suitably numbering the eigenvalues, we may write the Jordan form of A as

$$A = H_{11} \oplus \cdots \oplus H_{1n_1} \oplus \cdots \oplus H_{r1} \oplus \cdots \oplus H_{rn_r}$$

where we assume that there are r distinct eigenvalues of A. For definiteness, let us arbitrarily consider the eigenvalue λ_1 and look at the matrix $\lambda_1 I - A$. Since $\lambda_1 - \lambda_i \neq 0$ for $i \neq 1$, this matrix takes the form

$$\lambda_1 I - A = B_{11} \oplus \cdots \oplus B_{1n_1} \oplus J_{21} \oplus \cdots \oplus J_{2n_2} \oplus \cdots \oplus J_{r1} \oplus \cdots \oplus J_{rn_r}$$

where each B_{ij} is of the form

$$\begin{pmatrix} 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & -1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

and each J_{ij} looks like

$$\begin{pmatrix} \lambda_1 - \lambda_i & -1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_1 - \lambda_i & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_1 - \lambda_i & -1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_1 - \lambda_i \end{pmatrix}.$$

It should be clear that each J_{ij} is nonsingular (since they are all equivalent to the identity matrix of the appropriate size), and that each B_{ij} has rank equal to one less than its size. Since A is of size n, this means that the rank of $\lambda_1 I - A$

is $n - n_1$ (just look at the number of linearly independent rows in $\lambda_1 I - A$). But from Theorem 5.6 we have

$$\dim V_{\lambda_1} = \dim \mathrm{Ker}(\lambda_1 I - A) = \mathrm{nul}(\lambda_1 I - A) = n - r(\lambda_1 I - A) = n_1 .$$

In other words, the geometric multiplicity of λ_1 is equal to the number of hypercompanion matrices corresponding to λ_1 in the Jordan form of A. Since λ_1 could have been any of the eigenvalues, we are finished. ∎

Example 8.10 Suppose $A \in M_6(\mathbb{C})$ has characteristic polynomial

$$\Delta_A(x) = (x - 2)^4(x - 3)^2$$

and minimal polynomial

$$m(x) = (x - 2)^2(x - 3)^2 .$$

Then A has eigenvalue $\lambda_1 = 2$ with multiplicity 4, and $\lambda_2 = 3$ with multiplicity 2, and these must lie along the diagonal of the Jordan canonical form. We know that (see the proof of the corollary to Theorem 8.10)

$$\Delta_A(x) = m(x)q_{n-1}(x) \cdots q_1(x)$$

where $q_n(x) = m(x), \ldots, q_1(x)$ are the similarity invariants of A, and that the elementary divisors of $xI - A$ are the powers of the prime factors of the $q_i(x)$. What we do not know however, is whether the set of elementary divisors of $xI - A$ is $\{(x - 2)^2, (x - 3)^2, (x - 2)^2\}$ or $\{(x - 2)^2, (x - 3)^2, x - 2, x - 2\}$.

Using Theorem 8.18, we then see that the only possible Jordan canonical forms are (up to the order of the blocks)

$$\begin{pmatrix} \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & & \\ & \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & \\ & & \boxed{\begin{matrix} 3 & 1 \\ & 3 \end{matrix}} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & & & \\ & \boxed{2} & & \\ & & \boxed{2} & \\ & & & \boxed{\begin{matrix} 3 & 1 \\ & 3 \end{matrix}} \end{pmatrix}$$

Note that in the first case, the geometric multiplicity of $\lambda_1 = 2$ is two, while in the second case, the geometric multiplicity of $\lambda_1 = 2$ is three. In both cases, the eigenspace corresponding to $\lambda_2 = 3$ is of dimension 1. //

Example 8.11 Let us determine all possible Jordan canonical forms for the matrix $A \in \mathbb{C}(3)$ given by

$$\begin{pmatrix} 2 & a & b \\ 0 & 2 & c \\ 0 & 0 & -1 \end{pmatrix}.$$

The characteristic polynomial for A is easily seen to be

$$\Delta_A(x) = (x - 2)^2(x + 1)$$

and hence (by Theorem 7.12) the minimal polynomial is either the same as $\Delta_A(x)$, or is just $(x - 2)(x + 1)$. If $m(x) = \Delta(x)$, then (using Theorem 8.18 again) the Jordan form must be

$$\begin{pmatrix} \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & & \\ & & \\ & & \boxed{-1} \end{pmatrix}$$

while in the second case, it must be

$$\begin{pmatrix} \boxed{2} & & \\ & \boxed{2} & \\ & & \boxed{-1} \end{pmatrix}$$

If A is to be diagonalizable, then (either by Theorem 7.26 or the fact that the Jordan form in the second case is already diagonal) we must have the second case, and hence

$$0 = m(A) = (A - 2I)(A + I) = \begin{pmatrix} 0 & 3a & ac \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

so that A will be diagonalizable if and only if $a = 0$. //

As another application of Theorem 8.16 we have the following useful result. Note that here the field $\mathcal{F}$ can be either $\mathbb{R}$ or $\mathbb{C}$, and need not be algebraically closed in general.

Theorem 8.20 Suppose $B_i \in M_{n_i}(\mathcal{F})$ for $i = 1, \ldots, r$ and let $A = B_1 \oplus \cdots \oplus B_r \in M_n(\mathcal{F})$ (so that $n = \sum_{i=1}^{r} n_i$). Then the set of elementary divisors of $xI - A$ is the totality of elementary divisors of all the $xI - B_i$ taken together.

Proof We prove the theorem for the special case of $A = B_1 \oplus B_2$. The general case follows by an obvious induction argument. Let $S = \{e_1(x), \ldots, e_m(x)\}$ denote the totality of elementary divisors of $xI - B_1$ and $xI - B_2$ taken together. Thus, the elements of S are powers of prime polynomials. Following the method discussed at the end of Theorem 8.8, we multiply together the highest powers of all the distinct primes that appear in S to obtain a polynomial which we denote by $q_n(x)$. Deleting from S those $e_i(x)$ that we just used, we now multiply together the highest powers of all the remaining distinct primes to obtain $q_{n-1}(x)$. We continue this procedure until all the elements of S are exhausted, thereby obtaining the polynomials $q_{k+1}(x), \ldots, q_n(x)$. Note that our construction guarantees that $q_j(x) | q_{j+1}(x)$ for $j = k + 1, \ldots, n - 1$. Since $f_n(x) = q_1(x) \cdots q_n(x)$, it should also be clear that

$$\sum_{i=k+1}^{n} \deg q_j(x) = n_1 + n_2 = n \quad .$$

Denote the companion matrix $C(q_j(x))$ by simply C_j, and define the matrix

$$Q = C_{k+1} \oplus \cdots \oplus C_n \in M_n(\mathcal{F}) \quad .$$

Then

$$xI - Q = (xI - C_{k+1}) \oplus \cdots \oplus (xI - C_n) \quad .$$

But according to Theorem 8.14, $xI - C_j \approx \operatorname{diag}(1, \ldots, 1, q_j(x))$, and hence

$$xI - Q \approx \operatorname{diag}(1, \ldots, 1, q_{k+1}(x)) \oplus \cdots \oplus \operatorname{diag}(1, \ldots, 1, q_n(x)) \quad .$$

Then (since the Smith form is unique) the nonunit similarity invariants of Q are just the $q_j(x)$ (for $j = k + 1, \ldots, n$), and hence (by definition of elementary divisor) the elementary divisors of $xI - Q$ are exactly the polynomials in S. Then by Theorem 8.16, Q is similar to the direct sum of the companion matrices of all the polynomials in S.

On the other hand, Theorem 8.16 also tells us that B_1 and B_2 are each similar to the direct sum of the companion matrices of the elementary divisors of $xI - B_1$ and $xI - B_2$ respectively. Therefore $B_1 \oplus B_2 = A$ is similar to the direct sum of the companion matrices of all the polynomials in S. We now see that A is similar to Q, and hence (by Theorem 8.9, Corollary 1) $xI - A$ and $xI - Q$ have the same elementary divisors. Since the elementary divisors of $xI - Q$ are just the polynomials in S, and S was defined to be the totality of elementary divisors of $xI - B_1$ and $xI - B_2$, the proof is complete. ∎

The notion of "uniqueness" in Theorem 8.18 is an assertion that the Jordan form is "uniquely defined" or "well-defined." Suppose $A \in M_n(\mathbb{C})$ has Jordan form $H_1 \oplus \cdots \oplus H_p$ where each H_i is a basic Jordan block, and suppose that $G_1 \oplus \cdots \oplus G_q$ is any other matrix similar to A which is a direct sum of basic Jordan blocks. Then it follows from Theorem 8.20 that the G_i must, except for order, be exactly the same as the H_i (see Exercise 8.6.4). We state this in the following corollary to Theorem 8.20.

Corollary (**Uniqueness of the Jordan form**) Suppose $A \in M_n(\mathbb{C})$, and let both $G = G_1 \oplus \cdots \oplus G_p$ and $H = H_1 \oplus \cdots \oplus H_q$ be similar to A, where each G_i and H_i is a basic Jordan block. Then $p = q$ and, except for order, the G_i are the same as the H_i.

We saw in Section 7.5 that if a vector space V is the direct sum of T-invariant subspaces W_i (where $T \in L(V)$), then the matrix representation A of T is the direct sum of the matrix representations of $T_i = T|W_i$ (Theorem 7.20). Another common way of describing this decomposition of A is the following. We say that a matrix is **reducible** over $\mathcal{F}$ if it is similar to a block diagonal matrix with more than one block. In other words, $A \in M_n(\mathcal{F})$ is reducible if there exists a nonsingular matrix $S \in M_n(\mathcal{F})$ and matrices $B \in M_p(\mathcal{F})$ and $C \in M_q(\mathcal{F})$ with $p + q = n$ such that $S^{-1}AS = B \oplus C$. If A is not reducible, then we say that A is **irreducible**. A fundamental result is the following.

Theorem 8.21 A matrix $A \in M_n(\mathcal{F})$ is irreducible over $\mathcal{F}$ if and only if A is nonderogatory and the characteristic polynomial $\Delta_A(x)$ is a power of a prime polynomial. Alternatively, A is irreducible if and only if $xI - A$ has only one elementary divisor.

Proof If A is irreducible, then $xI - A$ can have only one elementary divisor (which is then necessarily a prime to some power) because (by Theorem 8.16) A is similar to the direct sum of the companion matrices of all the elementary divisors of $xI - A$. But these elementary divisors are the factors of the similarity invariants $q_k(x)$ where $q_k(x)|q_{k+1}(x)$, and therefore it follows that

$$q_1(x) = \cdots = q_{n-1}(x) = 1 \ .$$

Hence A is nonderogatory (corollary to Theorem 8.10).

Now assume that A is nonderogatory and that $\Delta_A(x)$ is a power of a prime polynomial. From Theorem 8.10 and its corollary we know that $q_1(x) = \cdots = q_{n-1}(x) = 1$, and hence $q_n(x) = m(x) = \Delta_A(x)$ is now the only elementary divisor of $xI - A$. If A were reducible, then (in the above notation) it would be similar over $\mathbb{F}$ to a matrix of the form $B \oplus C = S^{-1}AS$, and by Corollary 1 of Theorem 8.9, it would then follow that $xI - A$ has the same elementary divisors as $xI - (B \oplus C) = (xI - B) \oplus (xI - C)$. Note that by the corollary to Theorem 8.8, $xI - A$ and $S^{-1}(xI - A)S = xI - S^{-1}AS$ have the same elementary divisors. But $xI - B$ and $xI - C$ necessarily have at least one elementary divisor each (since their characteristic polynomials are nonzero), and (by Theorem 8.20) the elementary divisors of $xI - S^{-1}AS$ are the totality of the elementary divisors of $xI - B$ plus those of $xI - C$. This contradicts the fact that $xI - A$ has only one elementary divisor, and therefore A must be irreducible. ∎

For example, we see from Theorem 8.17 that the hypercompanion matrix $H((x - a)^k)$ is always irreducible. One consequence of this is that the Jordan canonical form of a matrix is the "simplest" in the sense that there is no similarity transformation that will further reduce any of the blocks on the diagonal. Similarly, since any elementary divisor is a power of a prime polynomial, we see from Theorem 8.14 that the companion matrix of an elementary divisor is always irreducible. Thus the rational canonical form can not be further reduced either. Note that the rational canonical form of a matrix $A \in M_n(\mathbb{C})$ will have the same "shape" as the Jordan form of A. In other words, both forms will consist of the same number of blocks of the same size on the diagonal.

In Sections 7.2 and 7.7 we proved several theorems that showed some of the relationships between eigenvalues and diagonalizability. Let us now relate what we have covered in this chapter to the question of diagonalizability. It is easiest to do this in the form of two simple theorems. The reader should note that the companion matrix of a linear polynomial $x - a_0$ is just the 1 x 1 matrix (a_0).

Theorem 8.22 A matrix $A \in M_n(\mathcal{F})$ is similar over $\mathcal{F}$ to a diagonal matrix $D \in M_n(\mathcal{F})$ if and only if all the elementary divisors of $xI - A$ are linear.

Proof If the elementary divisors of $xI - A$ are linear, then each of the corresponding companion matrices consists of a single scalar, and hence the rational canonical form of A will be diagonal (Theorem 8.16). Conversely, if A is similar to a diagonal matrix D, then $xI - A$ and $xI - D$ will have the same elementary divisors (Theorem 8.9, Corollary 1). Writing $D = D_1 \oplus \cdots \oplus D_n$ where $D_i = (d_i)$ is just a 1 x 1 matrix, we see from Theorem 8.20 that the ele-

mentary divisors of $xI - D$ are the linear polynomials $\{x - d_1, \ldots, x - d_n\}$ (since the elementary divisor of $xI - D_i = (x - d_i)$ is just $x - d_i$). ∎

Theorem 8.23 A matrix $A \in M_n(\mathcal{F})$ is similar over $\mathcal{F}$ to a diagonal matrix $D \in M_n(\mathcal{F})$ if and only if the minimal polynomial for A has distinct linear factors in $\mathcal{P} = \mathcal{F}[x]$.

Proof Recall that the elementary divisors of a matrix in $M_n(\mathcal{P})$ are the powers of prime polynomials that factor the invariant factors $q_k(x)$, and furthermore, that $q_k(x) | q_{k+1}(x)$. Then all the elementary divisors of such a matrix will be linear if and only if its invariant factor of highest degree has distinct linear factors in $\mathcal{P}$. But by Theorem 8.10, the minimal polynomial for $A \in M_n(\mathcal{F})$ is just its similarity invariant of highest degree (i.e., the invariant factor of highest degree of $xI - A \in M_n(\mathcal{P})$). Then applying Theorem 8.22, we see that A will be diagonalizable if and only if the minimal polynomial for A has distinct linear factors in $\mathcal{P}$. ∎

While it is certainly not true that any $A \in M_n(\mathbb{C})$ is similar to a diagonal matrix, it is an interesting fact that A is similar to a matrix in which the off-diagonal entries are arbitrarily small. To see this, we first put A into its Jordan canonical form J. In other words, we have

$$J = S^{-1}AS = \begin{pmatrix} j_{11} & j_{12} & 0 & 0 & \cdots & 0 & 0 \\ 0 & j_{22} & j_{23} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & j_{n-1\,n-1} & j_{n-1\,n} \\ 0 & 0 & 0 & 0 & \cdots & 0 & j_{nn} \end{pmatrix}.$$

If we now define the matrix $T = \text{diag}(1, \delta, \delta^2, \ldots, \delta^{n-1})$, then we leave it to the reader to show that

$$T^{-1}JT = (ST)^{-1}A(ST)$$
$$= \begin{pmatrix} j_{11} & \delta j_{12} & 0 & 0 & \cdots & 0 & 0 \\ 0 & j_{22} & \delta j_{23} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & j_{n-1\,n-1} & \delta j_{n-1\,n} \\ 0 & 0 & 0 & 0 & \cdots & 0 & j_{nn} \end{pmatrix}.$$

By choosing δ as small as desired, we obtain the form claimed.

Exercises

1. If all the eigenvalues of $A \in M_n(\mathcal{F})$ lie in $\mathcal{F}$, show that the Jordan canonical form of A has the same "block structure" as its rational canonical form.

2. Prove Theorem 7.25 using the Jordan canonical form (Theorem 8.18).

3. Prove Theorem 7.26 using the Jordan canonical form.

4. Finish proving the corollary to Theorem 8.20.

5. State and prove a corollary to Theorem 8.16 that is the analogue of the corollary to Theorem 8.20.

6. (a) Suppose a matrix A has characteristic polynomial

$$\Delta_A(x) = (x-2)^4(x-3)^3$$

and minimal polynomial

$$m(x) = (x-2)^2(x-3)^2 \ .$$

What are the possible Jordan forms for A?
(b) Suppose A has characteristic polynomial $\Delta_A(x) = (x-2)^3(x-5)^2$. What are the possible Jordan forms?

7. Find all possible Jordan forms for those matrices with characteristic and minimal polynomials given by:
(a) $\Delta(x) = (x-2)^4(x-3)^2$ and $m(x) = (x-2)^2(x-3)^2$.
(b) $\Delta(x) = (x-7)^5$ and $m(x) = (x-7)^2$.
(c) $\Delta(x) = (x-2)^7$ and $m(x) = (x-2)^3$.
(d) $\Delta(x) = (x-3)^4(x-5)^4$ and $m(x) = (x-3)^2(x-5)^2$.

8. Show that every complex matrix is similar to its transpose.

9. Is it true that all complex matrices $A \in M_n(\mathbb{C})$ with the property that $A^n = I$ but $A^k \neq I$ for $k < n$ are similar? Explain.

10. (a) Is it true that an eigenvalue λ of a matrix $A \in M_n(\mathbb{C})$ has multiplicity 1 if and only if $\lambda I - A$ has rank $n - 1$?
(b) Suppose an eigenvalue λ of $A \in M_n(\mathbb{C})$ is such that $r(\lambda I - A) = n - 1$. Prove that either λ has multiplicity 1, or else $r(\lambda I - A)^2 = n - 2$.

11. Suppose $A \in M_n(\mathbb{C})$ is idempotent, i.e., $A^2 = A$. What is the Jordan form of A?

12. Suppose $A \in M_n(\mathbb{C})$ is such that $p(A) = 0$ where

$$p(x) = (x - 2)(x - 3)(x - 4) .$$

Prove or disprove the following statements:
(a) The minimal polynomial for A must be of degree 3.
(b) A must be of size $n \leq 3$.
(c) If $n > 3$, then the characteristic polynomial of A must have multiple roots.
(d) A is nonsingular.
(e) A must have 2, 3 and 4 as eigenvalues.
(f) If $n = 3$, then the minimal and characteristic polynomials of A must be the same.
(g) If $n = 3$ then, up to similarity, there are exactly 10 different choices for A.

13. Recall that $A \in M_n(\mathbb{C})$ is said to be nilpotent of index k if k is the smallest integer such that $A^k = 0$.
(a) Describe the Jordan form of A.
Prove or disprove each of the following statements about $A \in M_n(\mathbb{C})$:
(b) A is nilpotent if and only if every eigenvalue of A is zero.
(c) If A is nilpotent, then $r(A) - r(A^2)$ is the number of elementary divisors of A.
(d) If A is nilpotent, then $r(A) - r(A^2)$ is the number of p x p Jordan blocks of A with $p > 1$.
(e) If A is nilpotent, then the nul(A) is the number of Jordan blocks of A (counting 1 x 1 blocks).
(f) If A is nilpotent, then $\text{nul}(A^{k+1}) - \text{nul}(A^k)$ is the number of Jordan blocks of size greater than k.

14. Suppose $A \in M_n(\mathbb{C})$ has eigenvalue λ of multiplicity m. Prove that the elementary divisors of A corresponding to λ are all linear if and only if $r(\lambda I - A) = r((\lambda I - A)^2)$.

15. Prove or disprove the following statements about matrices $A, B \in M_n(\mathbb{C})$:
(a) If either A or B is nonsingular, then AB and BA have the same minimal polynomial.
(b) If both A and B are singular and $AB \neq BA$, then AB and BA are not similar.

16. Suppose $A \in M_n(\mathbb{C})$, and let adj A be as in Theorem 4.11. If A is nonsingular, then $(SAS^{-1})^{-1} = SA^{-1}S^{-1}$ implies that $\text{adj}(SAS^{-1}) = S(\text{adj } A)S^{-1}$ by Theorem 4.11. By using "continuity" arguments, it is easy to show that this identity is true even if A is singular. Using this fact and the Jordan form, prove:
(a) If $\det A = 0$ but $\text{Tr}(\text{adj } A) \neq 0$, then 0 is an eigenvalue of A with multiplicity 1.
(b) If $\det A = 0$ but $\text{Tr}(\text{adj } A) \neq 0$, then $r(A) = n - 1$.

8.7 CYCLIC SUBSPACES *

It is important to realize that the Jordan form can only be found in cases where the minimal polynomial is factorable into linear polynomials (for example, if the base field is algebraically closed). On the other hand, the rational canonical form is valid over non-algebraically closed fields. In order to properly present another way of looking at the rational canonical form, we first introduce cyclic subspaces. Again, we are seeking a criterion for deciding when two matrices are similar. The clue that we now follow up on was given earlier in Theorem 7.37.

Let $V \neq 0$ be a finite-dimensional vector space over an arbitrary field $\mathbb{F}$, and suppose $T \in L(V)$. We say that a nonzero T-invariant subspace Z of V is **T-cyclic** if there exists a nonzero $v \in Z$ and a positive integer $k \geq 0$ such that Z is spanned by the set $\{v, T(v), \ldots, T^k(v)\}$. An equivalent way of defining T-cyclic subspaces is given in the following theorem.

Theorem 8.24 Let V be finite-dimensional and suppose $T \in L(V)$. A subspace $Z \subset V$ is T-cyclic if and only if there exists a nonzero $v \in Z$ such that every vector in Z can be expressed in the form $f(T)(v)$ for some $f(x) \in \mathcal{F}[x]$.

Proof If Z is T-cyclic, then by definition, any $u \in Z$ may be written in terms of the set $\{v, T(v), \ldots, T^k(v)\}$ as

$$u = a_0v + a_1T(v) + \cdots + a_kT^k(v) = (a_0 + a_1T + \cdots + a_kT^k)(v) = f(T)(v)$$

where $f(x) = a_0 + a_1x + \cdots + a_kx^k \in \mathcal{F}[x]$. On the other hand, if every $u \in Z$ is of the form $f(T)(v)$, then Z must be spanned by the set $\{v, T(v), T^2(v), \ldots\}$. But Z is finite-dimensional (since it is a subset of the finite-dimensional space V), and hence there must exist a positive integer k such that Z is spanned by the set $\{v, T(v), \ldots, T^k(v)\}$. ∎

Generalizing these definitions slightly, let $v \in V$ be nonzero. Then the set of all vectors of the form $f(T)(v)$ where $f(x)$ varies over all polynomials in $\mathcal{F}[x]$ is a T-invariant subspace called the **T-cyclic subspace of** V **generated by** v. We denote this subspace by $Z(v, T)$. We also denote the restriction of T to $Z(v, T)$ by $T_v = T|Z(v, T)$. That $Z(v, T)$ is a subspace is easily seen since for any $f, g \in \mathcal{F}[x]$ and $a, b \in \mathcal{F}$ we have

$$af(T)(v) + bg(T)(v) = [af(T) + bg(T)](v) = h(T)(v) \in Z(v, T)$$

where $h(x) = af(x) + bg(x) \in \mathcal{F}[x]$ (by Theorem 7.2). It should be clear that $Z(v, T)$ is T-invariant since any element of $Z(v, T)$ is of the form $f(T)(v)$, and hence

$$T[f(T)(v)] = [Tf(T)](v) = g(T)(v)$$

where $g(x) = x\,f(x) \in \mathcal{F}[x]$. In addition, $Z(v, T)$ is T-cyclic by Theorem 8.24. In the particular case that $Z(v, T) = V$, then v is called a **cyclic vector** for T.

Let us briefly refer to Section 7.4 where we proved the existence of a unique monic polynomial $m_v(x)$ of least degree such that $m_v(T)(v) = 0$. This polynomial was called the minimal polynomial of the vector v. The existence of $m_v(x)$ was based on the fact that V was of dimension n, and hence for any $v \in V$, the $n + 1$ vectors $\{v, T(v), \ldots, T^n(v)\}$ must be linearly dependent. This showed that $\deg m_v(x) \leq n$. Since $m_v(x)$ generates the ideal $N_T(v)$, it follows that $m_v(x)|f(x)$ for any $f(x) \in N_T(v)$, i.e., where $f(x)$ is such that $f(T)(v) = 0$. Let us now show how this approach can be reformulated in terms of T-cyclic subspaces.

Using Theorem 8.24, we see that for any nonzero $v \in V$ we may define $Z(v, T)$ as that finite-dimensional T-invariant subspace of V spanned by the linearly independent set $\{v, T(v), \ldots, T^{d-1}(v)\}$, where the integer $d \geq 1$ is defined as the smallest integer such that the set $\{v, T(v), \ldots, T^d(v)\}$ is linearly

dependent. This means that $T^d(v)$ must be a linear combination of the vectors $v, T(v), \ldots, T^{d-1}(v)$, and hence is of the form

$$T^d(v) = a_0 v + \cdots + a_{d-1}T^{d-1}(v)$$

for some set of scalars $\{a_i\}$. Defining the polynomial

$$m_v(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0$$

we see that $m_v(T)(v) = 0$, where $\deg m_v(x) = d$. All that really remains is to show that if $f(x) \in \mathcal{F}[x]$ is such that $f(T)(v) = 0$, then $m_v(x)|f(x)$. This will prove that $m_v(x)$ is the polynomial of least degree with the property that $m_v(T)(v) = 0$.

From the division algorithm, there exists $g(x) \in \mathcal{F}[x]$ such that

$$f(x) = m_v(x)g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg m_v(x)$. Substituting T and applying this to v we have (using $m_v(T)(v) = 0$)

$$0 = f(T)(v) = g(T)m_v(T)(v) + r(T)(v) = r(T)(v) \ .$$

But if $r(x) \neq 0$ with $\deg r(x) < \deg m_v(x)$, then (since $Z(v, T)$ is T-invariant) $r(T)(v)$ is a linear combination of elements in the set $\{v, T(v), \ldots, T^{d-1}(v)\}$, and hence the equation $r(T)(v) = 0$ contradicts the assumed linear independence of this set. Therefore we must have $r(x) = 0$, and hence $m_v(x)|f(x)$.

Lastly, we note that $m_v(x)$ is in fact the *unique* monic polynomial of least degree such that $m_v(T)(v) = 0$. Indeed, if $m'(x)$ is also of least degree such that $m'(T)(v) = 0$, then the fact that $\deg m'(x) = \deg m_v(x)$ together with the result of the previous paragraph tells us that $m_v(x)|m'(x)$. Thus $m'(x) = \alpha m_v(x)$ for some $\alpha \in F$, and choosing $\alpha = 1$ shows that $m_v(x)$ is the unique *monic polynomial* of least degree such that $m_v(T)(v) = 0$.

We summarize this discussion in the following theorem.

Theorem 8.25 Let $v \in V$ be nonzero and suppose $T \in L(V)$. Then there exists a unique monic polynomial $m_v(x)$ of least degree such that $m_v(T)(v) = 0$. Moreover, for any polynomial $f(x) \in \mathcal{F}[x]$ with $f(T)(v) = 0$ we have $m_v(x)|f(x)$.

Corollary If $m(x)$ is the minimal polynomial for T on V, then $m_v(x)|m(x)$ for every nonzero $v \in V$.

Proof By definition of minimal polynomial we know that $m(T) = 0$ on V, so that in particular we have $m(T)(v) = 0$. But now Theorem 8.25 shows that $m_v(x)|m(x)$. ∎

For ease of reference, we bring together Theorems 8.24 and 8.25 in the next basic result.

Theorem 8.26 Let $v \in V$ be nonzero, suppose $T \in L(V)$, and let

$$m_v(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0$$

be the minimal polynomial of v. Then $\{v, T(v), \ldots, T^{d-1}(v)\}$ is a basis for the T-cyclic subspace $Z(v, T)$, and hence $\dim Z(v, T) = \deg m_v(x) = d$.

Proof From the way that $m_v(x)$ was constructed, the vector $T^d(v)$ is the first vector in the sequence $\{v, T(v), T^2(v), \ldots\}$ that is a linear combination of the preceding vectors. This means that the set $S = \{v, T(v), \ldots, T^{d-1}(v)\}$ is linearly independent. We must now show that $f(T)(v)$ is a linear combination of the elements of S for every $f(x) \in \mathcal{F}[x]$.

Since $m_v(T)(v) = 0$ we have $T^d(v) = \sum_{i=0}^{d-1} a_i T^i(v)$. Therefore

$$T^{d+1}(v) = \sum_{i=0}^{d-2} a_i T^{i+1}(v) + a_{d-1}T^d(v) = \sum_{i=0}^{d-2} a_i T^{i+1}(v) + a_{d-1}\sum_{i=0}^{d-2} a_i T^i(v) \quad .$$

This shows that $T^{d+1}(v)$ is a linear combination of the elements of S. We can clearly continue this process for any $T^k(v)$ with $k \geq d$, and therefore $f(T)(v)$ is a linear combination of $v, T(v), \ldots, T^{d-1}(v)$ for every $f(x) \in \mathcal{F}[x]$. Thus S is a basis for the T-cyclic subspace of V generated by v. ∎

The following example will be used in the proof of the elementary divisor theorem given in the next section.

Example 8.12 Suppose that the minimal polynomial of v is given by $m_v(x) = p(x)^n$ where $p(x)$ is a monic prime polynomial of degree d. Defining $W = Z(v, T)$, we will show that $p(T)^s(W)$ is a T-cyclic subspace generated by $p(T)(v)$, and is of dimension $d(n - s)$ if $s < n$, and dimension 0 if $s \geq n$. It should be clear that $p(T)^s(W)$ is a T-cyclic subspace since every element of W is of the form $f(T)(v)$ for some $f(x) \in \mathcal{F}[x]$ and W is T-invariant.

Since p(x) is of degree d, we see that deg $m_v(x)$ = deg $p(x)^n$ = dn (see Theorem 6.2(b)). From Theorem 8.26, we then follows that W has the basis $\{v, T(v), \ldots, T^{dn-1}(v)\}$. This means that any $w \in W$ may be written as

$$w = a_0 v + a_1 T(v) + \cdots + a_{dn-1} T^{dn-1}(v)$$

for some set of scalars a_i. Applying $p(T)^s$ to w we have

$$p(T)^s(w) = a_0 p(T)^s(v) + \cdots + a_i [T^i p(T)^s](v) + \cdots + a_{dn-1} [T^{dn-1} p(T)^s](v) \ .$$

But $m_v(T)(v) = p(T)^n(v) = 0$ where deg $m_v(x)$ = dn, and deg $p(x)^s$ = ds. Therefore, if $s \geq n$ we automatically have $p(T)^s(w) = 0$ so that $p(T)^s(W)$ is of dimension 0. If $s < n$, then the maximum value of i in the expression for $p(T)^s(w)$ comes from the requirement that $i + ds < dn$ which is equivalent to $i < d(n - s)$. This leaves us with

$$p(T)^s(w) = a_0 [p(T)^s(v)] + \cdots + a_{d(n-s)-1} T^{d(n-s)-1} [p(T)^s(v)]$$

and we now see that any element in $p(T)^s(W)$ is a linear combination of the terms $a_i T^i [p(T)^s(v)]$ for $i = 0, \ldots, d(n - s) - 1$. Therefore if $s < n$, this shows that $p(T)^s(W)$ is a T-cyclic subspace of dimension $d(n - s)$ generated by $p(T)^s(v)$. //

In Section 7.4 we showed that the minimal polynomial for T was the unique monic generator of the ideal $N_T = \cap_{v \in V} N_T(v)$. If we restrict ourselves to the subspace Z(v, T) of V then, as we now show, it is true that the minimal polynomial $m_v(x)$ of v is actually the minimal polynomial for $T_v = T|Z(v, T)$.

Theorem 8.27 Let Z(v, T) be the T-cyclic subspace of V generated by v. Then $m_v(x)$ is equal to the minimal polynomial for $T_v = T|Z(v, T)$.

Proof Since Z(v, T) is spanned by $\{v, T(v), T^2(v), \ldots, T^{d-1}(v)\}$, the fact that $m_v(T)(v) = 0$ means that $m_v(T) = 0$ on Z(v, T) (by Theorem 7.2). If p(x) is the minimal polynomial for T_v, then Theorem 7.4 tells us that $p(x) | m_v(x)$. On the other hand, from Theorem 7.17(a), we see that $p(T)(v) = p(T_v)(v) = 0$ since p(x) is the minimal polynomial for T_v. Therefore, Theorem 8.25 shows us that $m_v(x) | p(x)$. Since both $m_v(x)$ and p(x) are monic, this implies that $m_v(x) = p(x)$. ∎

Theorem 8.27 also gives us another proof of the corollary to Theorem 8.25. Thus, since $m_v(x) = p(x)$ (i.e., the minimal polynomial for T_v), Theorem 7.17(b) shows that $m_v(x)|m(x)$. Moreover, we have the next result that ties together these concepts with the structure of quotient spaces.

Theorem 8.28 Suppose $T \in L(V)$, let W be a T-invariant subspace of V and let $\bar{T} \in A(\bar{V})$ be the induced linear operator on $\bar{V} = V/W$ (see Theorem 7.35). Then the minimal polynomial $\bar{m}_v(x)$ for $\bar{v} \in V/W$ divides the minimal polynomial $m(x)$ for T.

Proof From the corollary to Theorem 8.25 we have $\bar{m}_v(x)|\bar{m}(x)$ where $\bar{m}(x)$ is the minimal polynomial for $\bar{T}$. But $\bar{m}(x)|m(x)$ by Theorem 7.35. ∎

Corollary Using the same notation as in Theorems 8.25 and 8.28, if the minimal polynomial for T is of the form $p(x)^n$ where $p(x)$ is a monic prime polynomial, then for any $v \in V$ we have $m_v(x) = p(x)^{n_1}$ and $\bar{m}_v(x) = p(x)^{n_2}$ for some $n_1, n_2 \leq n$.

Proof From the above results we know that $m_v(x)|p(x)^n$ and $\bar{m}_v(x)|p(x)^n$. The corollary then follows from this along with the unique factorization theorem (Theorem 6.6) and the fact that $p(x)$ is monic and prime. ∎

In the discussion that followed Theorem 7.16 we showed that the (unique) minimal polynomial $m(x)$ for $T \in L(V)$ is also the minimal polynomial $m_v(x)$ for some $v \in V$. (This is because each basis vector v_i for V has its own minimal polynomial $m_i(x)$, and the least common multiple of the $m_i(x)$ is both the minimal polynomial for some vector $v \in V$ and the minimal polynomial for T.) Now suppose that v also happens to be a cyclic vector for T, i.e., $Z(v, T) = V$. By Theorem 8.26 we know that

$$\dim V = \dim Z(v, T) = \deg m_v(x) = \deg m(x) .$$

However, the characteristic polynomial $\Delta_T(x)$ for T must always be of degree equal to $\dim V$, and hence the corollary to Theorem 7.42 (or Theorems 7.11 and 7.12) shows us that $m(x) = \Delta_T(x)$.

On the other hand, suppose that the characteristic polynomial $\Delta_T(x)$ of T is equal to the minimal polynomial $m(x)$ for T. Then if $v \in V$ is such that $m_v(x) = m(x)$ we have

$$\dim V = \deg \Delta_T(x) = \deg m(x) = \deg m_v(x) .$$

Applying Theorem 8.26 again, we see that dim Z(v, T) = deg $m_v(x)$ = dim V, and hence v is a cyclic vector for T. We have thus proven the following useful result.

Theorem 8.29 Let V be finite-dimensional and suppose $T \in L(V)$. Then T has a cyclic vector if and only if the characteristic and minimal polynomials for T are identical. Thus the matrix representation of T is nonderogatory.

In view of Theorem 8.12, our next result should have been expected.

Theorem 8.30 Let Z(v, T) be a T-cyclic subspace of V, let $T_v = T|Z(v, T)$ and suppose that the minimal polynomial for v is given by

$$m_v(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0 .$$

Then the matrix representation of T_v relative to the basis v, T(v), . . . , $T^{d-1}(v)$ for Z(v, T) is the companion matrix

$$C(m_v(x)) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & a_{d-2} \\ 0 & 0 & 0 & \cdots & 1 & a_{d-1} \end{pmatrix} .$$

Proof Simply look at T_v applied to each of the basis vectors of Z(v, T) and note that $m_v(T)(v) = 0$ implies that $T^d(v) = a_0v + \cdots + a_{d-1}T^{d-1}(v)$. This yields

$$\begin{aligned} T_v(v) &= 0v + T(v) \\ T_v(T(v)) &= 0v + 0T(v) + T^2(v) \\ &\vdots \\ T_v(T^{d-2}(v)) &= 0v + \cdots + T^{d-1}(v) \\ T_v(T^{d-1}(v)) &= T^d(v) = a_0v + \cdots + a_{d-1}T^{d-1}(v) \end{aligned}$$

As usual, the i*th* column of the matrix representation of T_v is just the image under T_v of the i*th* basis vector of Z(v, T) (see Theorem 5.11). ∎

Exercises

1. If $T \in L(V)$ and $v \in V$, prove that $Z(v, T)$ is the intersection of all T-invariant subspaces containing v.

2. Suppose $T \in L(V)$, and let $u, v \in V$ have relatively prime minimal polynomials $m_u(x)$ and $m_v(x)$. Show that $m_u(x)m_v(x)$ is the minimal polynomial of $u + v$.

3. Prove that $Z(u, T) = Z(v, T)$ if and only if $g(T)(u) = v$ where $g(x)$ is relatively prime to $m_u(x)$.

8.8 THE ELEMENTARY DIVISOR THEREOM *

The reader should recall from Section 7.5 that if the matrix representation A of an operator $T \in L(V)$ is the direct sum of smaller matrices (in the appropriate basis for V), then V is just the direct sum of T-invariant subspaces (see Theorem 7.20). If we translate Theorem 8.16 (the rational canonical form) into the corresponding result on the underlying space V, then we obtain the elementary divisor theorem.

Theorem 8.31 (**Elementary Divisor Theorem**) Let $V \neq \{0\}$ be finite-dimensional over an arbitrary field $\mathcal{F}$, and suppose $T \in L(V)$. Then there exist vectors $v_1, \ldots, v_r$ in V such that:

(a) $V = Z(v_1, T) \oplus \cdots \oplus Z(v_r, T)$.

(b) Each v_i has minimal polynomial $p_i(x)^{n_i}$ where $p_i(x) \in \mathcal{F}[x]$ is a monic prime.

(c) The number r of terms in the decomposition of V is uniquely determined, as is the set of minimal polynomials $p_i(x)^{n_i}$.

Proof This is easy to prove from Theorem 8.16 (the rational canonical form) and what we know about companion matrices and cyclic subspaces (particularly Theorem 8.30). The details are left to the reader. ∎

From Theorem 8.26 we see that $\dim Z(v_i, T) = \deg p_i(x)^{n_i}$, and hence from the corollary to Theorem 2.15 we have

$$\dim V = \sum_{i=1}^{r} \deg p_i(x)^{n_i} \quad .$$

The polynomials $p_i(x)^{n_i}$ defined in Theorem 8.31 are just the elementary divisors of $x1 - T$. For example, suppose that $T \in L(V)$ and $x1 - T$ has the ele-

mentary divisors $x + 1$, $(x - 1)^2$, $x + 1$, $x^2 + 1$ over the field $\mathbb{R}$. This means that V is a vector space over $\mathbb{R}$ with

$$V = Z(v_1, T) \oplus Z(v_2, T) \oplus Z(v_3, T) \oplus Z(v_4, T)$$

and the minimal polynomials of v_1, v_2, v_3, v_4 are $x + 1$, $(x - 1)^2$, $x + 1$, $x^2 + 1$ respectively. Furthermore, $T = T_1 \oplus T_2 \oplus T_3 \oplus T_4$ where $T_i = T|Z(v_i, T)$ and the minimal polynomial for T_i is just the corresponding minimal polynomial of v_i (Theorem 8.27). Note that if the field were $\mathbb{C}$ instead of $\mathbb{R}$, then $x^2 + 1$ would not be prime, and hence could not be an elementary divisor of $x1 - T$.

It is important to realize that Theorem 8.31 only claims the uniqueness of the set of elementary divisors of $x1 - T$. Thus the vectors $v_1, \ldots, v_r$ and corresponding subspaces $Z(v_1, T), \ldots, Z(v_r, T)$ are themselves not uniquely determined by T. In addition, we have seen that the elementary divisors are unique only up to a rearrangement.

It is also possible to prove Theorem 8.31 without using Theorem 8.16 or any of the formalism developed in Sections 8.2 – 8.7. We now present this alternative approach as a difficult but instructive application of quotient spaces, noting that it is not needed for anything else in this book. We begin with a special case that takes care of most of the proof. Afterwards, we will show how Theorem 8.31 follows from Theorem 8.32. It should also be pointed out that Theorem 8.32 also follows from the rational canonical form (Theorem 8.16).

Theorem 8.32 Let $T \in L(V)$ have minimal polynomial $p(x)^n$ where $p(x)$ is a monic prime polynomial. Then there exist vectors $v_1, \ldots, v_r \in V$ such that

$$V = Z(v_1, T) \oplus \cdots \oplus Z(v_r, T) \ .$$

In addition, each v_i has corresponding minimal polynomial (i.e., order) given by $p(x)^{n_i}$ where $n = n_1 \geq n_2 \geq \cdots \geq n_r$. Furthermore, any other decomposition of V into the direct sum of T-cyclic subspaces has the same number r of components and the same set of minimal polynomials (i.e., orders).

Proof Throughout this (quite long) proof, we will use the term "order" rather than "minimal polynomial" for the sake of clarity. Furthermore, we will refer to the **T-order** of a vector rather than simply the order when there is a possible ambiguity with respect to the operator being referred to.

We proceed by induction on the dimension of V. First, if $\dim V = 1$, then $T(V) = V$ and hence $f(T)(V) = V$ for any $f(x) \in \mathcal{F}[x]$. Therefore V is T-cyclic

and the theorem holds in this case. Now assume dim V > 1, and suppose that the theorem holds for all vector spaces of dimension less than that of V.

Since $p(x)^n$ is the minimal polynomial for T, we know that $p(T)^n(v) = 0$ for all $v \in V$. In particular, there must exist a $v_1 \in V$ such that $p(T)^n(v_1) = 0$ but $p(T)^{n-1}(v_1) \neq 0$ (or else $p(x)^{n-1}$ would be the minimal polynomial for T). This means that $p(x)^n$ must be the T-order of v_1 (since the minimal polynomial of v_1 is unique and monic). Now let $Z_1 = Z(v_1, T)$ be the T-invariant T-cyclic subspace of V generated by v_1. We also define $\bar{V} = V/Z_1$ along with the induced operator $\bar{T} \in A(\bar{V})$. Then by Theorem 7.35 we know that the minimal polynomial for $\bar{T}$ divides the minimal polynomial $p(x)^n$ for T, and hence the minimal polynomial for $\bar{T}$ is $p(x)^{n_2}$ where $n_2 \leq n$. This means that $\bar{V}$ and $\bar{T}$ satisfy the hypotheses of the theorem, and hence by our induction hypothesis (since dim $\bar{V}$ < dim V), $\bar{V}$ must be the direct sum of T-cyclic subspaces. We thus write

$$\bar{V} = Z(\bar{v}_2, \bar{T}) \oplus \cdots \oplus Z(\bar{v}_r, \bar{T})$$

where each $\bar{v}_i$ has corresponding $\bar{T}$-order $p(x)^{n_i}$ with $n \geq n_2 \geq \cdots \geq n_r$. It is important to remember that each of these $\bar{v}_i$ is a coset of Z_1 in V, and thus may be written as $\bar{v}_i = u_i + Z_1$ for some $u_i \in V$. This means that every element of $\bar{v}_i$ is of the form $u_i + z_i$ for some $z_i \in Z_1$.

We now claim that there exists a vector v_2 in the coset $\bar{v}_2$ such that the T-order of v_2 is just the $\bar{T}$-order $p(x)^{n_2}$ of $\bar{v}_2$. To see this, let $w \in \bar{v}_2$ be arbitrary so that we may write $w = u_2 + z_2$ for some $u_2 \in V$ and $z_2 \in Z_1 \subset V$. Since $p(\bar{T})^{n_2}(\bar{v}_2) = \bar{0} = Z_1$, we have (see Theorem 7.35)

$$Z_1 = p(\bar{T})^{n_2}(\bar{v}_2) = p(\bar{T})^{n_2}(u_2 + Z_1) = p(T)^{n_2}(u_2) + Z_1$$

and hence $p(T)^{n_2}(u_2) \in Z_1$. Using the fact that Z_1 is T-invariant, we see that

$$p(T)^{n_2}(w) = p(T)^{n_2}(u_2) + p(T)^{n_2}(z_2) \in Z_1 .$$

Using the definition of Z_1 as the T-cyclic subspace generated by v_1, this last result implies that there exists a polynomial $f(x) \in \mathcal{F}[x]$ such that

$$p(T)^{n_2}(w) = f(T)(v_1) . \tag{1}$$

But $p(x)^n$ is the minimal polynomial for T, and hence (1) implies that

$$0 = p(T)^n(w) = p(T)^{n-n_2}p(T)^{n_2}(w) = p(T)^{n-n_2}f(T)(v_1) .$$

Since we showed that $p(x)^n$ is also the T-order of v_1, Theorem 8.25 tells us that $p(x)^n$ divides $p(x)^{n-n_2}f(x)$, and hence there exists a polynomial $g(x) \in \mathcal{F}[x]$ such that $p(x)^{n-n_2} f(x) = p(x)^n g(x)$. Rearranging, this may be written as $p(x)^{n-n_2}[f(x) - p(x)^{n_2}g(x)] = 0$. Since $\mathcal{F}[x]$ is an integral domain, this implies (see Theorem 6.2, Corollary 2)

$$f(x) = p(x)^{n_2} g(x) \quad . \tag{2}$$

We now define

$$v_2 = w - g(T)(v_1) \quad . \tag{3}$$

By definition of Z_1 we see that $w - v_2 = g(T)(v_1) \in Z_1$, and therefore (see Theorem 7.30)

$$v_2 \in w + Z_1 = u_2 + z_2 + Z_1 = u_2 + Z_1 = \bar{v}_2 \quad .$$

Since $\bar{v}_2 = u_2 + Z_1$ and $v_2 \in \bar{v}_2$, it follows that $v_2 = u_2 + z$ for some $z \in Z_1$. Now suppose that $h(x)$ is any polynomial such that $h(T)(v_2) = 0$. Then

$$0 = h(T)(v_2) = h(T)(u_2 + z) = h(T)(u_2) + h(T)(z)$$

so that $h(T)(u_2) = -h(T)(z) \in Z_1$ (since Z_1 is T-invariant). We then have

$$h(\bar{T})(\bar{v}_2) = h(\bar{T})(u_2 + Z_1) = h(T)(u_2) + Z_1 = Z_1 = \bar{0} \quad .$$

According to Theorem 8.25, this then means that the $\bar{T}$-order of $\bar{v}_2$ divides $h(x)$. In particular, choosing $h(x)$ to be the T-order of v_2, we see that the T-order of v_2 is some multiple of the $\bar{T}$-order of $\bar{v}_2$. In other words, the T-order of v_2 must equal $p(x)^{n_2}q(x)$ for some polynomial $q(x) \in \mathcal{F}[x]$. However, from (3), (1) and (2) we have

$$\begin{aligned} p(T)^{n_2}(v_2) &= p(T)^{n_2}[w - g(T)(v_1)] \\ &= p(T)^{n_2}(w) - p(T)^{n_2} g(T)(v_1) \\ &= f(T)(v_1) - f(T)(v_1) \\ &= 0 \quad . \end{aligned}$$

This shows that in fact the T-order of v_2 is equal to $p(x)^{n_2}$ as claimed.

In an exactly analogous manner, we see that there exist vectors $v_3, \ldots, v_r$ in V with $v_i \in \bar{v}_i$ and such that the T-order of v_i is equal to the $\bar{T}$-order $p(x)^{n_i}$ of $\bar{v}_i$. For each $i = 1, \ldots, r$ we then define the T-cyclic subspaces $Z_i = Z(v_i, T)$

where Z_1 was defined near the beginning of the proof. We must show that $V = Z_1 \oplus \cdots \oplus Z_r$.

Let deg p(x) = d so that deg $p(x)^{n_i} = dn_i$ (see Theorem 6.2(b)). Since $p(x)^{n_i}$ is the T-order of v_i, Theorem 8.26 shows that $Z(v_i, T)$ has basis

$$\{v_i, T(v_i), \ldots, T^{dn_i-1}(v_i)\} .$$

Similarly, $p(x)^{n_i}$ is also the $\bar{T}$-order of $\bar{v}_i$ for i = 2, . . . , r and hence $Z(\bar{v}_i, \bar{T})$ has the basis

$$\{\bar{v}_i, \bar{T}(\bar{v}_i), \ldots, \bar{T}^{dn_i-1}(\bar{v}_i)\} .$$

Since $\bar{V} = Z(\bar{v}_2, \bar{T}) \oplus \cdots \oplus Z(\bar{v}_r, \bar{T})$, we see from Theorem 2.15 that $\bar{V}$ has basis

$$\{\bar{v}_2, \ldots, \bar{T}^{dn_2-1}(\bar{v}_2), \ldots, \bar{v}_r, \ldots, \bar{T}^{dn_r-1}(\bar{v}_r)\} .$$

Recall that $\bar{v}_i = u_i + Z_1$ and $v_i \in \bar{v}_i$. This means that $v_i = u_i + z_i$ for some $z_i \in Z_1$ so that

$$\bar{v}_i = v_i - z_i + Z_1 = v_i + Z_1$$

and hence (see the proof of Theorem 7.35)

$$\bar{T}^m(\bar{v}_i) = \bar{T}^m(v_i + Z_1) = \bar{T}^{\bar{m}}(v_i + Z_1) = T^m(v_i) + Z_1 .$$

Using this result in the terms for the basis of $\bar{V}$, Theorem 7.34 shows that V has the basis (where we recall that Z_1 is just $Z(v_1, T)$)

$$\{v_1, \ldots, T^{dn_1-1}(v_1), v_2, \ldots, T^{dn_2-1}(v_2), \ldots, v_r, \ldots, T^{dn_r-1}(v_r)\} .$$

Therefore, by Theorem 2.15, V must be the direct sum of the $Z_i = Z(v_i, T)$ for i = 1, . . . , r. This completes the first part of the proof.

We now turn to the uniqueness of the direct sum expansion of V. Note that we have just shown that $V = Z_1 \oplus \cdots \oplus Z_r$ where each $Z_i = Z(v_i, T)$ is a T-cyclic subspace of V. In addition, the minimal polynomial (i.e., order) of v_i is $p(x)^{n_i}$ where p(x) is a monic prime polynomial of degree d, and $p(x)^n$ is the minimal polynomial for T. Let us assume that we also have the decomposition $V = Z'_1 \oplus \cdots \oplus Z'_s$ where $Z'_i = Z(v'_i, T)$ is a T-cyclic subspace of V, and v'_i has minimal polynomial $p(x)^{m_i}$ with $m_1 \geq \cdots \geq m_s$. (Both v_i and v'_i have orders that are powers of the same polynomial p(x) by the corollary to Theorem 8.25.) We must show that s = r and that $m_i = n_i$ for i = 1, . . . , r.

Suppose that $n_i \neq m_i$ for at least one i, and let k be the first integer such that $n_k \neq m_k$ while $n_j = m_j$ for j = 1, . . . , k − 1. We may arbitrarily take $n_k >$

m_k. Since $V = Z'_1 \oplus \cdots \oplus Z'_s$, any $u \in V$ may be written in the form $u = u'_1 + \cdots + u'_s$ where $u'_i \in Z'_i$. Furthermore, since $p(T)^{m_i}$ is linear, we see that

$$p(T)^{m_i}(u) = p(T)^{m_i}(u'_1) + \cdots + p(T)^{m_i}(u'_s)$$

and hence we may write

$$p(T)^{m_i}(V) = p(T)^{m_i}(Z'_1) \oplus \cdots \oplus p(T)^{m_i}(Z'_s) \ .$$

Using the definition of the T-cyclic subspace Z'_k along with the fact that $p(T)^{m_k}(v'_k) = 0$, it is easy to see that $p(T)^{m_k}(Z'_k) = 0$. But the inequality $m_k \geq m_{k+1} \geq \cdots \geq m_s$ implies that $p(T)^{m_k}(Z'_i) = 0$ for $i = k, k + 1, \ldots, s$ and hence we have

$$p(T)^{m_k}(V) = p(T)^{m_k}(Z'_1) \oplus \cdots \oplus p(T)^{m_k}(Z'_{k-1}) \ .$$

From Example 8.12, we see that $p(T)^{m_i}(Z'_j)$ is of dimension $d(m_j - m_i)$ for $m_i \leq m_j$. This gives us (see the corollary to Theorem 2.15)

$$\dim p(T)^{m_k}(V) = d(m_1 - m_k) + \cdots + d(m_{k-1} - m_k) \ .$$

On the other hand, we have $V = Z_1 \oplus \cdots \oplus Z_r$, and since $k \leq r$ it follows that $Z_1 \oplus \cdots \oplus Z_k \subset V$. Therefore

$$p(T)^{m_k}(V) \supset p(T)^{m_k}(Z_1) \oplus \cdots \oplus p(T)^{m_k}(Z_k)$$

and hence, since $\dim p(T)^{m_i}(Z_j) = d(n_j - m_i)$ for $m_i \leq n_j$, we have

$$\dim p(T)^{m_k}(V) \geq d(n_1 - m_k) + \cdots + d(n_{k-1} - m_k) + d(n_k - m_k) \ .$$

However, $n_i = m_i$ for $i = 1, \ldots, k - 1$ and $n_k > m_k$. We thus have a contradiction in the value of $\dim p(T)^{m_k}(V)$, and hence $n_i = m_i$ for every $i = 1, \ldots, r$ (since if $r < s$ for example, then we would have $0 = n_s \neq m_s$ for every $s > r$). This completes the entire proof of Theorem 8.32. ∎

In order to prove Theorem 8.31 now, we must remove the requirement in Theorem 8.32 that $T \in L(V)$ have minimal polynomial $p(x)^n$. For any finite-dimensional $V \neq \{0\}$, we know that any $T \in L(V)$ has a minimal polynomial $m(x)$ (Theorem 7.4). From the unique factorization theorem (Theorem 6.6), we know that any polynomial can be factored into a product of prime polynomials. We can thus always write $m(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r}$ where each

$p_i(x)$ is prime. Hence, from the primary decomposition theorem (Theorem 7.23), we then see that V is the direct sum of T-invariant subspaces $W_i = \text{Ker } p_i(T)^{n_i}$ for $i = 1, \ldots, r$ such that minimal polynomial of $T_i = T|W_i$ is $p_i(x)^{n_i}$.

Applying Theorem 8.32 to each space W_i and operator $T_i \in L(W_i)$, we see that there exist vectors $w_{i_k} \in W_i$ for $k = 1, \ldots, r_i$ such that W_i is the direct sum of the $Z(w_{i_k}, T_i)$. Moreover, since each W_i is T-invariant, each of the T_i-cyclic subspaces $Z(w_{i_k}, T_i)$ is also T-cyclic, and the minimal polynomial of each generator w_{i_k} is a power of $p_i(x)$. This discussion completes the proof of Theorem 8.31.

Finally, we remark that it is possible to prove the rational form of a matrix from this version (i.e., proof) of the elementary divisor theorem. However, we feel that at this point it is not terribly instructive to do so, and hence the interested reader will have to find this approach in one of the books listed in the bibliography.

Exercise

Prove Theorem 8.31 using the rational canonical form.

Index

Absolute convergence 710
Absolute value 15, 20
Accumulation point 622, 690, 700
Adjoint
    classsical 192
    of a linear operator 493, 673
    of a matrix 183, 384
Algebra 227
Algebraic number 16
Algebraically closed field 276
Alternation mapping 556
Annihilator 323
    of a set of vectors 453
Anti-derivation 572
Antilinear mapping 452
Archimedean axiom 13
Archimedean property 13
Arcwise connected 720
Augmented matrix 117
Automorphism 50
Axiom of choice 9

Banach space 630
Basic Jordan block 378, 420
Basis 77
    dual 446
    g-orthonormal 613
    negatively oriented 608
    ordered 79
    positively oriented 608
    similarly oriented 606
Basis 1-forms 447, 554
Bessel's inequality 106, 657, 658
Bijective 5
Bilinear form 461
    alternating 467
    antisymmetric 467
    nonnegative 479
    polar form of 472
    positive definite 479
    positive semidefinite 479
    symmetric 469
Bilinear functional 448
Bilinear map 461
Binomial coefficient 18
Binomial theorem 18
Block matrix 204
Bolzano-Weierstrass theorem 691, 700
Boundary 703

Bounded 625
  mapping 692
  sequence 697
  set 691, 697
Bounded linear map 635

Cancellation law 31
Canonical form 296
Cardinality 11
Cartesian product 3
Cauchy criterion 708
Cauchy sequence 699
Cauchy-Binet theorem 214
Cauchy-Schwartz inequality 100, 621
Cauchy's inequality 643
Cayley transform 508
Cayley-Hamilton theorem 312, 378, 395
Cayley's theorem 52
Chain 8
Characteristic
  equation 309
  matrix 309
  of integral domain 58
  polynomial 309
  root 302
  value 302
  vector 302
Closed ball 683
Closed interval 14
Closed set 649, 683
Closure of a set 702
Cluster point 700
Cofactor 187
Column space 128
Compact space 686
Companion matrix 412
Comparable 8
Comparison test 715
Complete metric space 630, 699
Complete orthonormal set 660
Completely reducible 333
Completeness relation 113
Complex conjugate 20
Complex number 19
  imaginary part 19
  modulus 20
  nth root 24
  real part 19
Conductor 335
Congruent matrices 465
Conjugate exponents 641
Conjugate linear 452
Conjugate space 665
Continuous 623, 684
Continuous linear map 635
Contravariant vector 545
Convergent sequence of vectors 640
Convex set 650
Coordinate function 633
Coordinates 3, 79
Coprime 28
Coset 61
Covariant vector 545
Cramer's rule 200
Critical
  point 523
  value 523
Cyclic group 290
  order of 290
Cyclic subspace 336, 432
Cyclic vector 433

De Moivre's theorem 24
De Morgan formulas 3
Dense 13, 647, 706
  nowhere 706
  somewhere 706
Derived set 703
Determinant 171, 600
  of a linear operator 246
  order 171
Determinantal divisors 397
Diagonal subgroup 34
Diagonalizable 248, 317
Differential of a function 551
Direct sum 90
  external 89
  internal 88
  of matrices 333
  of operators 332
Division algorithm 26, 258
Division ring 54
Double dual 222, 452
Dual basis 222
Dual space 222, 446, 665

Eigenspace 306
Eigenvalue 302
  spectrum 346, 524
Eigenvector 302
Elementary divisor theorem 439
Elementary divisor 398
Elementary matrix 163
Elementary row operations 121
Empty set 2
Equivalence class 9
Equivalence relation 9
Equivalent norms 629
Equivalent representations 335

Euclidean algorithm 27, 265
Euclidean space 99, 508
Expansion by minors 189
    (see also Laplace expansion)
Extended real number system 14
Exterior of a set 703
Exterior algebra 574
Exterior product 563
Exterior r-forms 554

Factor group 64
Factor theorem 262
Factorial 18
Field 54
    characteristic of 58
Field of quotients 284
Finite field
    characteristic of 291
    order of 288
Finite-dimensional 77
Formal linear combinations 578
Fourier coefficients 106, 655
Free variables 142
Free vector space 579
Function 4
Functional 665
Fundamental Theorem of Algebra 276, 693
Fundamental Theorem of Arithmetic 29

Gaussian elimination 124
Generalized permutation symbol 565
Gershgorin's theorem 307
Graded associative algebra 575
Graded components 574
Gram-Schmidt process 109
Gramian 197
Grassmann algebra 574
Greatest common divisor 26, 263
Greatest lower bound 8
Group 30
    abelian 30
    center of 67
    class 35
    conjugate elements of 35
    cyclic 291
    direct product 34
    finite 31
    homomorphism 49
    infinite 31
    multiplication 30
    order of 31
    representation 33, 335
g-volume 615
Hausdorff property 687
Heine-Borel theorem 687, 691
Hermitian adjoint 383
Hermitian form 481
    associated quadratic form 482
    nonnegative semidefinite 482
    positive definite 482
Hermitian inner product 620
Hilbert basis 660
Hilbert space 630, 640
Homomorphic groups 49
Homomorphism 49
    kernel of 50
    vector space 79
Hölder's inequality 642
Hypercompanion matrix 420
Hyperplane 457
Hyperspace 457

Ideal 59
    generated by 275
    unit 275
Idempotent 157, 232, 353
Identity mapping 6, 227
Identity matrix 136
Indeterminate 115, 255
Index set 2
Induction 17
Infimum 8
Infinite series 708
Infinity symbols 14
Injective 5
Inner product 98
    Hermitian 98
    indefinite 609
    nondegenerate 451, 609
Inner product space 99
    complex 99
    real 99
Integers
    modulo n 57, 285
Integral domain 57
Interior of a set 702
Interior product 572
Invariant direct sum decomposition 332
Invariant factors 398
Invariant subspace 329
Invariant volume element 617
Irrational number 12
Irreducible representation 335
Isolated point 622
Isometry 113, 498
Isomorphic 59, 79
Isomorphic groups 50
Isomorphism 50, 79
    inner product space 501

Jacobian 599
Jointly continuous 648
Jordan form 376, 422
  uniqueness of 427

Kronecker delta 105
Kronecker product 581

Lagrange interpolation formula 280
Lagrange's theorem 61
Laplace expansion 573
Law of cosines 96
Law of inertia 478
Least common multiple 29, 272
Least upper bound 8
Least upper bound property 12
Left identity 31
Left inverse 31, 157
Left zero divisor 163
Levi-Civita
  symbol 560
  tensor 560
Limit 625
Limit inferior 713
Limit point 700
Limit superior 713
Linear extension theorem 639
Linear algebra 227
Linear combination 72
Linear equations 115
  coefficients of 115
  constant term 115
  solution vector 115
  system of 116
    equivalent 118
    homogeneous 138
    nonhomogeneous 138
    nontrivial solution 138
    trivial solution 138
Linear functional 221
Linear manifold 649
Linear operators 227
Linear span 72
Linear transformation 79, 215
  diagonalizable 318
  image 224
  inverse 228
  invertible 228
  kernel 225
  matrix representation of 235
  negative of 219
  nonsingular 229
  nullity 225
  orientation preserving 608
  range 225
  rank 225
  reducible 332
  restriction of 330
  singular 229
  volume preserving 608
Linearly dependent 75
Linearly independent 75
Lorentz frame 613
Lorentz transformation 616
Lower bound 8
Lower limit 713
Lowering the index 610

Mapping 4
  alternating 180
  associative 6
  bilinear 578
  commutative 6
  composite 6
  domain 4
  image 4
  inverse 5
  inverse image 4
  multilinear 180, 544
  one-to-one 5
  onto 5
  range 4
  restriction 4
Matrix 117
  adjoint 183, 383
  anticommutator 156, 184
  antisymmetric 156, 184, 469
  block 204
  canonical form 169
  classical adjoint 191
  column rank 128
  columns 117
  commutator 154, 156
  conjugate transpose 183
  derogatory 409
  diagonal 154, 165
  direct product 581
  distinguished elements 124
  equivalent 515
  equivalent over $\mathbb{P}$ 393
  Hermitian 383, 482
  Hermitian adjoint 482
  idempotent 157
  inverse 157
  invertible 157
  irreducible 427

lower-triangular 156, 162, 177
negative 148
nilpotent 184
nonderogatory 409
nonsingular 157
normal 383, 515
orthogonal 183, 249, 384, 502
product 148
rank 136
reduced row-echelon form 123
reducible 333, 427
row equivalent 123
row rank 128
row-echelon form 123
row-reduced form 125
rows 117
singular 157
size 117
skew-Hermitian 388
skewsymmetric 156
square 148
sum 147
supertriangular 376
symmetric 156, 184, 384, 470
tensor product 581
trace 155, 246
transpose 152
unit 392
unitarily similar 515
unitary 183, 383, 502
upper-triangular 156, 162, 177
Matrix exponential series 530
Matrix of coefficients 116
Maximal element 8
Metric 104, 680
Metric space 680
complete 699
Metric tensor 580
contravariant 611
covariant 610
index of 613
Lorentz 613
Riemannian 613
Metric volume form 615
Minimal element 9
Minimal polynomial 299, 313, 326
of a vector 323
Minkowski's inequality 643
Minor 188
Minor matrix 187
Module 69
Multilinear form 544
Multiplicity
algebraic 345
geometric 345

Natural mapping 453
Natural numbers 2
n-cell 689
Neighborhood 690
deleted 690
Nilpotent 233
index of nilpotency 369
operator 306, 369
Nondegenerate 462
Nonnegative 2
Norm 619
Normal coordinates 489
Normal matrix 515
Normed vector space 101, 620
Null space 154, 225

1-forms 447
Open
ball 681
cover 686
interval 14
set 681
subcover 686
Operator 490, 653
adjoint 673
anti-Hermitian 508
antisymmetric 511
Hermitian 495, 676
isometric 498, 499, 677
nonnegative 508
normal 509, 677
orthogonal 499, 501
positive 508
positive definite 508
positive semidefinite 508
self-adjoint 495, 676
skew-Hermitian 508
symmetric 511
unitary 499, 678
Operator norm 637
Order of a vector 440
Ordered by inclusion 8
Orientation 606, 608
negative 592, 608
positive 592, 608
Oriented vector space 606, 608
Oriented volume 592
Orthogonal 102
compliment 105, 620
projection 217, 354
set 105
Orthonormal set 105

Parallelogram law 103, 621
Parallelpiped
  base 589
  height 589
  r-dimensional 589
  r-volume 589
Parseval's equation 662
Partial isometry 507
Partial ordering 7
  bounded above 8
  induced 8
  largest element 8
  smallest element 8
  upper bound 8
Partially ordered set 7
Partition 9
  induced 10
Path 720
Path connected 720
Pauli spin matrices 156
$\mathcal{P}$-elementary operations 390
Permutation 35
  even 44
  odd 44
  one-line notation 36
  sign of 46
  two-line notation 35
Permutation group 40
  cycle 41
  degree of 40
  equivalent elements in 41
  orbit 41
Permutation symbol 560
Perpendicular 102
Polar decomposition 540
Polar form identities 103
Polygonally connected 721
Polynomial 253
  associates 262
  coefficients of 253
  constant 256
  degree of 256
  factor of 261
  greatest common divisor 397
  irreducible 262
  leading coefficient of 256
  minimal 300, 314, 327
  monic 256
  norm of 397
  reducible 262
  root 261, 297
  zero 261, 297
Polynomial equation 261
  solution 261
Polynomial function 255
Positive integers 2
Positive transformation 539
Power set 7
Preimage 4
Primary decomposition theorem 339
Prime number 25
Prime polynomial 262
Principal ideal 60
  generator of 60
Product 625
Projection 157, 232, 352, 654
Pull-back 595
Push-forward 602
Pythagorean theorem 95, 103, 622

Quadratic
  form 471
    diagonal representation 477
  polynomial 471
Quaternions 280
Quotient 25
Quotient group 64
Quotient ring 64
Quotient space 362

Raising an index 611
Rank
  of a bilinear form 465
  of a matrix 135
Ratio test 717
Rational canonical form 416
Rational numbers 2
Rayleigh quotient 513
Rearrangement lemma 34
Reducible representation 333
Reflexive space 671
Relation 7
Relatively prime 28, 263
Remainder 25
Remainder theorem 261
Resolution of the identity 524
r-forms 554
Riesz representation theorem 666
Riesz-Fischer theorem 663
Right identity 31
Right inverse 31, 157
Right zero divisor 163
Ring 53
  associates 262
  associative 53
  commutative 53
  embedded 282
  extension 282
  homomorphism 56

kernel of 59
isomorphism 59
with unit element 53
Ring of sets 4
r-linear form 544
Root 261
multiplicity of 281, 305
Root test 717
Row canonical form 125
Row space 128
Row-column-equivalent 169

Scalar 69
Scalar mapping 301
Scalar multiplication 68
Scalar product 94
Scalar triple product 588
Schur canonical form 384
Schur's lemma 335
Schwartz's inequality 20
generalized 649
Second dual 222, 452
Secular equation 309
Separable 647, 695
Sequence 696
Cauchy 699
decreasing 699
increasing 699
limit of 622, 696
monotonic 699
range 697
Series 708
rearrangement of 710
Sesquilinear form 620
Set 2
closed 683
complement of 2
countable 11
countably infinite 11
disjoint 3
family of 2
finite 11
infinite 11
intersection 3
open 681
symmetric difference 4
uncountable 11
union 2
Shuffle 563
Signature 477
Signed permutation matrix 389
Similar matrices 184, 245
Similarity class 329
Similarity invariants 408
Similarity transformation 184, 245
Simple root 305
Smith canonical form 400
Solution set 116
Space of linear functionals 222
Space of linear transformations 220
Spectral decomposition 524
Spectral theorem 525
Spectrum 346
degenerate 346
Square root 15
Standard basis 79
Standard inner product 99, 620
Standard orientation 608
Subdeterminant 185
Subgroup 33
index of 62
normal 62
Submatrix 185, 193, 209
Subsequence 707
Subsequential limit 707
Subset 2
proper 2
Subspace 72, 649
closed 649
generated by 72, 660
intersection of 86
invariant 243, 329
irreducible 518
null 618
of a metric space 684
proper 72
spacelike 618
spanned by 72
sum of 74, 86
timelike 618
trivial 72
Summation convention 545
Sup norm 625, 629, 633
Superdiagonal 155, 370
Superset 2
Supremum 8
Surjective 5
Sylvester's theorem 478
Symmetric group 37
Symmetrizing mapping 556

T-cyclic subspace 432
generated by 432
T-invariant subspace 243
Tensor 545
antisymmetric 553, 554
classical law of transformation 550
components 545, 547
contraction 552
contravariant order 545

covariant order 545
rank 545
skew-symmetric 553
symmetric 553, 554
trace 552
type 545
Tensor algebra 574
Tensor product 462, 464, 547, 580
Total 660
Total ordering 8
Trace 155
Transcendental number 17
Transition matrix 243
orthogonal 249
Transpose
of a linear transformation 459
of a matrix 153
Transpositions 44
Triangle inequality 101
Triangular form theorem 367, 376
Two-sided inverse 157

Uniformly continuous 623
Unique factorization theorem 266
Unit (of a ring) 262
Unit cube 593
Unit matrix 392
Unit vector 99
Unitarily similar 385, 515
Unitary 183, 383, 499, 502, 678
Unitary space 99, 508
Unknowns 115
Upper limit 713

Vandermonde matrix 195
Vector 69
length of 99
lightlike 614
norm of 99
spacelike 614
timelike 614
Vector multiplication 227
Vector space 68
complex 69
dimension of 77, 83
generated by 578
infinite-dimensional 640
isometric 113
normed 101
ordinary Euclidean 613
pseudo-Euclidean 613
real 69
singular 613
Vector space homomorphism 79
Volume forms 607
equivalent 607

Wedge product 462, 563
Well-defined 4
Well-ordered 17
Weyl's formula 536

Zero divisor 57
Zero mapping 219
Zero matrix 148
Zorn's lemma 9