Preface

Who is this book for? The target reader will already have experienced *a first course in linear algebra* covering matrix manipulation, determinants, linear mappings, eigenvectors and diagonalisation of matrices. Ideally the reader will have met bases of finite-dimensional vector spaces, the axioms for groups, rings and fields as well as some set theory including equivalence relations. Some familiarity with elementary number theory is also assumed, such as the Euclidean algorithm for the greatest common divisor of two integers, the Chinese remainder theorem and the fundamental theorem of arithmetic. In the proof of Lemma 6.35 it is assumed that the reader knows how to resolve a permutation into cycles. With these provisos the subject matter is virtually self-contained. Indeed many of the standard facts of linear algebra, such as the multiplicative property of determinants and the dimension theorem (any two bases of the same finite-dimensional vector space have the same number of vectors), are proved in a more general context. Nevertheless from a didactic point of view it is highly desirable, if not essential, for the reader to be already familiar with these facts.

What does the book do? The book is in two analogous parts and is designed to be *a second course in linear algebra* suitable for second/third year mathematics undergraduates, or postgraduates. The first part deals with the theory of finitely generated (f.g.) abelian groups: the emerging homology theory of topological spaces was built on such groups during the 1870s and more recently the classification of elliptic curves has made use of them. The starting point of the abstract theory couldn't be more concrete if it tried! Row and column operations are applied to an arbitrary matrix having integer entries with the aim of obtaining a diagonal matrix with non-negative entries such that the $(1, 1)$-entry is a divisor of the $(2, 2)$-entry, the $(2, 2)$-entry is a divisor of the (3, 3)-entry, and so on; a diagonal matrix of this type is said to be in *Smith normal form* (*Snf*) after the 19th century mathematician HJS Smith. Using an extension of the Euclidean algorithm it is shown in Chapter 1 that the Snf can be obtained without resort to prime factorisation. In fact the existence of the Snf is the cornerstone of the decomposition theory.

Free abelian groups of finite rank have $\mathbb{Z}$-bases and behave in many ways like finite-dimensional vector spaces. Each f.g. abelian group is best described as a quotient group of such a free abelian group by a subgroup which is necessarily also free. In Chapter 2 some time is spent on the concept of quotient groups which no student initially finds easy, but luckily in this context turns out to be little more than working modulo a given integer. The quotient groups arising in this way are specified by matrices over $\mathbb{Z}$ and the theory of the Snf is exactly what is needed to analyse their structure. Putting the pieces together in Chapter 3 each f.g. abelian group is seen to correspond to a sequence of non-negative integers (its *invariant factors*) in which each integer is a divisor of the next. The sequence of invariant factors of an f.g. abelian group encapsulates its properties: two f.g. abelian groups are isomorphic (abstractly identical) if and only if their sequences of invariant factors are equal. So broadly, apart from important side-issues such as specifying the automorphisms of a given group G, this is the end of the story as far as f.g. abelian groups are concerned! Nevertheless these side-issues are thoroughly discussed in the text and through numerous exercises; complete solutions to all exercises are on the associated website.

In the second part of the book the ring $\mathbb{Z}$ of integers is replaced by the ring $F[x]$ of polynomials over a field F. Such polynomials behave in the same way as integers and in particular the Euclidean algorithm can be used to find the gcd of each pair of them. In Chapter 4 the theory of the Smith normal form is shown to extend, almost effortlessly, to matrices over $F[x]$, the non-zero entries in the Snf here being *monic* (leading coefficient 1) polynomials. To what end? A question which occupies centre stage in linear algebra concerns $t \times t$ matrices A and B over a field F: is there a systematic method of finding, where it exists, an *invertible* $t \times t$ matrix X over F with $XA = BX$? Should X exist then A and $B = XAX^{-1}$ are called *similar*. The answer to the question posed above is a resounding YES! The systematic method amounts to reducing the matrices $xI - A$ and $xI - B$, which are $t \times t$ matrices over $F[x]$, to their Smith normal forms; if these forms are equal then A and B are similar and X can be found by referring back to the elementary operations used in the reduction processes; if these forms are different then A and B are not similar and X doesn't exist. The matrix $xI - A$ should be familiar to the reader as $\det(xI - A)$ is the characteristic polynomial of A. The non-constant diagonal entries in the Snf of $xI - A$ are called the *invariant factors* of A. It is proved in Chapter 6 that A and B are similar if and only if their sequences of invariant factors are equal. The theory culminates in the rational canonical form (rcf) of A which is the simplest matrix having the same invariant factors as A. It's significant that the rcf is obtained in a constructive way; in particular there is no reliance on factorisation into irreducible polynomials.

The analogy between the two parts is established using *R-modules* where R is a commutative ring. Abelian groups are renamed $\mathbb{Z}$-modules and structure-preserving mappings (*homomorphisms*) of abelian groups are $\mathbb{Z}$-linear mappings. The terminology helps the theory along: for instance the reader comfortable with 1-dimensional subspaces should have little difficulty with *cyclic* submodules. Each $t \times t$ matrix A over a field F gives rise to an associated $F[x]$-module $M(A)$. The relationship between A and $M(A)$ is explained in Chapter 5 where *companion* matrices are introduced. Just as each finite abelian group G is a direct sum of cyclic groups, so each matrix A, as above, is similar to a direct sum of companion matrices; the polynomial analogue of the order $|G|$ of G is the characteristic polynomial $\det(xI - A)$ of A.

The theory of the two parts can be conflated using the overarching concept of a finitely generated module over a principal ideal domain, which is the stance taken by several textbooks. An exception is *Rings*, *Modules and Linear Algebra* by B. Hartley and T.O. Hawkes, Chapman and Hall (1970) which opened my eyes to the beauty of the analogy explained above. I willingly acknowledge the debt I owe to this classic exposition. The two strands are sufficiently important to merit individual attention; nevertheless I have adopted proofs which generalise without material change, that of *the invariance theorem* 3.7 being a case in point.

Mathematically there is nothing new here: it is a rehash of 19th and early 20th century matrix theory from Smith to Frobenius, ending with the work of Shoda on automorphisms. However I have not seen elsewhere the step-by-step method of calculating the matrix Q described in Chapter 1 though it is easy enough once one has stumbled on the basic idea. The book is an expansion of material from a lecture course I gave in the University of London, off and on, over a 30 year period to undergraduates first at Westfield College and latterly at Royal Holloway. Lively students forced me to rethink both theory and presentation and I am grateful, in retrospect, to them. Dr. W.A. Sutherland read and commented on the text and Dr. E.J. Scourfield helped with the number theory in Chapter 3; I thank both. Any errors which remain are my own.

Finally I hope the book will attract mathematics students to what is undoubtedly an important and beautiful theory.

London, UK Christopher Norman