

# Introduction to Algebra

Peter J. Cameron  
Queen Mary, University of London

CLARENDON PRESS • OXFORD

2007



# Preface

---

This new edition of my algebra textbook has a number of changes.

The most significant is that the book now tries to live up to its title better than it did: the introductory chapter has more than doubled in length, including basic material on proofs, numbers, algebraic manipulations, sets, functions, relations, matrices, and permutations. I hope that it is now accessible to a first-year mathematics undergraduate, and suitable for use in a first-year mathematics course. Indeed, much of this material comes from a course (also with the title ‘Introduction to Algebra’) which I gave at Queen Mary, University of London, in spring 2007.

I have also revised and corrected the rest of the book, while keeping the structure intact. In particular, the pace of the first chapter is quite gentle; in Chapters 2 and 3 it picks up a bit, and in the later chapters it is a bit faster again. Once you are used to the way I write mathematics, you should be able to take this in your stride. Since the book is intended to be used in a variety of courses, there is a certain amount of repetition. For example, concepts or results introduced in exercises may be dealt with later in the main text. New material on the Axiom of Choice,  $p$ -groups and local rings has been added, and there are many new exercises.

I am grateful to many people who have helped me. First and foremost, Robin Chapman, for spotting many misprints and making many suggestions; and Csaba Szabó, who encouraged his students (named below) to proofread the book very thoroughly! Also, Gary McGuire spotted a gap in the proof of the Fundamental Theorem of Galois Theory, and R. A. Bailey suggested a different proof of Sylow’s Theorem. The people who notified me of errors in the book, or who suggested improvements (as well as the above) are Laura Alexander, Richard Anderson, M. Q. Baig, Steve DiMauro, Karl Fedje, Emily Ford, Roderick Foreman, Will Funk, Rippon Gupta, Matt Harvey, Jessica Hubbs, Young-Han Kim, Bill Martin, William H. Millerd, Ioannis Pantelidakis, Brandon Peden, Nayim Rashid, Elizabeth Rothwell, Ben Rubin, and Amjad Tuffaha; my thanks to all of you, and to anyone else whose name I have inadvertently omitted!

P.J.C.

*London*

*April 2007*

## **Preface to the first edition**

The axiomatic method is characteristic of modern mathematics. By making our assumptions explicit, we reduce the risk of making an error in our reasoning based

on false analogy; and our results have a clearly defined area of applicability which is as wide as possible (any situation in which the axioms hold).

However, switching quickly from the concrete to the abstract makes a heavy demand on students. The axiomatic style of mathematics is usually met first in a course with a title such as ‘Abstract Algebra’, ‘Algebraic Structures’, or ‘Groups, Rings and Fields’. Students who are used to factorising a particular integer or finding the stationary points of a particular curve find it hard to verify that a set whose elements are subsets of another set satisfies the axioms for a group, and even harder to get a feel for what such a group really looks like.

For this reason, among others, I have chosen to treat rings before groups, although they are logically more complicated. Everyone is familiar with the set of integers, and can see that it satisfies the axioms for a ring. In the early stages, when one depends on precedent, the integers form a fairly reliable guide. Also, the abstract factorisation theorems of ring theory lead to proofs of important and subtle properties of the integers, such as the Fundamental Theorem of Arithmetic. Finally, the path to non-trivial applications is shorter from ring theory than from group theory.

I have been teaching algebra for the whole of my professional career, and this book reflects that experience. Most immediately, it grew out of the Abstract Algebra course at Queen Mary and Westfield College. Chapters 2 and 3 are based fairly directly on the course content, and provide an introduction to rings (and fields) and to groups. The first chapter contains essential background material that every student of mathematics should know, and which can certainly stand repetition. (A great deal of algebra depends on the concept of an equivalence relation.)

Chapter 4, on vector spaces, doesn’t try to be a complete account, since most students will have met vector spaces before they reach this point. The purpose is twofold: to give an axiomatic approach; and to provide material in a form which generalises to modules over Euclidean rings, from where two very important applications (finitely generated abelian groups and canonical forms of matrices) come.

Chapter 7 carries further the material of Chapters 2 and 3, and also introduces some other types of algebra, chosen for their unifying features: universal algebra, lattices, and categories. This follows a chapter in which the number systems are defined (so that our earlier trust that the integers form a ring can be firmly founded), the distinction between algebraic and transcendental numbers is established, and certain ruler-and-compass construction problems are shown to be impossible. The final chapter treats two important applications, drawing on much of what has gone before: coding theory and Galois theory.

As mentioned earlier, Chapters 2 and 3 can form the basis of a first course on algebra, followed by a course based on Chapters 5 and 7. Alternatively, Chapter 3 and Sections 7.1–7.8 could form a group theory course, and Chapters 2 and 5 and Sections 7.9–7.14 a ring theory course. Sections 2.14–2.16, 6.6–6.8, 7.15–7.18 and 8.6–8.11 make up a Galois theory course. Sections 6.1–6.5 and 6.9–6.10 could

supplement a course on set theory, and Sections 2.14–2.16, 7.15–7.18 and 8.1–8.5 could be used in conjunction with some material on information theory for a coding theory course.

Some parts of the book (Sections 7.8, 7.13, and probably the last part of Chapter 7) are really too sketchy to be used for teaching a course; they are designed to tempt students into further exploration.

At the end, there is a list of books for further reading, and solutions to selected exercises from the first three chapters.

Asterisks denote harder exercises.

There is a World Wide Web site associated with this book. It contains solutions to the remaining exercises, further topics, problems, and links to other sites of interest to algebraists. The address is

<http://www.maths.qmul.ac.uk/~pjc/algebra/>

Thanks are due to many generations of students, whose questions and perplexities have helped me clarify my ideas and so resulted in a better book than I might otherwise have written.

P.J.C.

*London*

*December 1997*



# Contents

---

<b>1. Introduction</b>	<b>1</b>
What is mathematics?	1
Numbers	10
Elementary algebra	23
Sets	32
Modular arithmetic	48
Matrices	52
Appendix: Logic	58
<b>2. Rings</b>	<b>63</b>
Rings and subrings	63
Homomorphisms and ideals	74
Factorisation	87
Fields	99
Appendix: Miscellany	104
<b>3. Groups</b>	<b>110</b>
Groups and subgroups	110
Subgroups and cosets	118
Homomorphisms and normal subgroups	123
Some special groups	132
Appendix: How many groups?	146
<b>4. Vector spaces</b>	<b>150</b>
Vector spaces and subspaces	150
Linear transformations and matrices	161
<b>5. Modules</b>	<b>182</b>
Introduction	182
Modules over a Euclidean domain	190
Applications	196
<b>6. The number systems</b>	<b>208</b>
To the complex numbers	209
Algebraic and transcendental numbers	219
More about sets	229
<b>7. Further topics</b>	<b>235</b>
Further group theory	235
Further ring theory	254

Further field theory	266
Other structures	276
<b>8. Applications</b>	<b>297</b>
Coding theory	297
Galois theory	315
<b>Further reading</b>	<b>332</b>
<b>Index</b>	<b>336</b>