Preface

In 1990 we introduced a one-semester applications of algebra course at North Carolina State University for students who had successfully completed semesters of linear and abstract algebra. We intended for the course to give students more exposure to basic algebraic concepts, and to show students some practical uses of these concepts. The course was received enthusiastically by both students and faculty and has become one of the most popular mathematics electives at NC State.

When we were originally deciding on material for the course, we knew that we wanted to include several topics from coding theory, cryptography, and counting (what we call *Polya* theory). With this in mind, at the suggestion of Michael Singer, we used George Mackiw's book *Applications of Abstract Algebra* for the first few years, and supplemented as we saw fit. After several years, Mackiw's book went out of print temporarily. Rather than search for a new book for the course, we decided to write our own notes and teach the course from a coursepack. About the same time, NC State incorporated the mathematics software package Maple V$^{TM\,1}$ into its calculus sequence, and we decided to incorporate it into our course as well. The use of Maple played a central role in the recent development of the course because it provides a way for students to see realistic examples of the topics discussed without having to struggle with extensive computations. With additional notes regarding the use of Maple in the course, our coursepack evolved into this book. In addition to the topics discussed in this book, we have included a number of other topics in the course. However, the present material has become the constant core for the course.

Our philosophy concerning the use of technology in the course is that it be a useful tool and not present new problems or frustrations. Consequently, we have included very detailed instructions regarding the use of

[1]Maple V is a registered trademark of Waterloo Maple, Inc., 57 Erb St. W, Waterloo, Canada N2L6C2, www.maplesoft.com.

Maple in this book. It is our hope that the Maple discussions are thorough enough to allow it to be used without much alternative aid. As alternative aids, we have included a basic Maple tutorial in Appendix A, and an introduction to some of Maple's linear algebra commands in Appendix B. Although we do not require students to produce the Maple code used in the course, we do require that they obtain a level of proficiency such that they can make basic changes to provided worksheets to complete numerous Maple exercises. So that this book can be used for applications of algebra courses in which Maple is not incorporated, we have separated all Maple material into sections that are clearly labeled, and separated all Maple and non-Maple exercises.

When teaching the course, we discuss the material in Chapter 1 as needed rather than review it all at once. More specifically, we discuss the material in Chapter 1 through examples the first time it is needed in the applications that follow. Some of the material in Chapter 1 is review material that does not apply specifically to the applications that follow. However, for students with weak backgrounds, Chapter 1 provides a comprehensive review of all necessary prerequisite mathematics.

Chapter 2 is a short chapter on block designs. In Chapters 3, 4, and 5 we discuss some topics from coding theory. In Chapter 3 we introduce error-correcting codes, and present Hadamard, Reed-Muller, and Hamming codes. In Chapters 4 and 5, we present BCH codes and Reed-Solomon codes. Each of these chapters are dependent in part on the preceding chapters. The dependency of Chapter 3 on Chapter 2 can be avoided by omitting Sections 3.2, 3.3, and 3.4 on Hadamard and Reed-Muller codes. In Chapters 6, 7, and 8 we discuss some topics from cryptography. In Chapter 6 we introduce algebraic cryptography, and present several variations of the Hill cryptosystem. In Chapter 7 we present the RSA cryptosystem and discuss some related topics, including the Diffie-Hellman key exchange. In Chapter 8 we present the ElGamal cryptosystem, and describe how elliptic curves can be incorporated into the system naturally. There is a slight dependency of Chapters 7 and 8 on Chapter 6, and of Chapter 8 on Chapter 7. Chapter 9 is a stand-alone chapter in which we discuss the Polya counting techniques, including Burnside's Theorem and the Polya Enumeration Theorem.

We wish to thank all those who have been involved in the development of this course and book. Pete Hardy taught from the coursepack and improved it with his suggestions. Also, Michael Singer suggested various topics and wrote notes on some of them. Many students have written on this material for various projects. Of these, the recent master's project by Karen Klein on elliptic curves was especially interesting. Finally, we wish to

thank our mentor, Jack Levine, for his interest in our projects, his guidance as we learned about applications of algebra, and his many contributions to the subject, especially in cryptography.