Preface

This little book began as a set of course notes for an unusual but very attractive freshman course in algebra for math majors. The course introduces students to the notions of rigorous mathematics in the familiar settings of the integers and polynomials. This is worthwhile because of the strong parallels between the two theories. Indeed, one can argue that it is these parallels that led to the theory of commutative algebra as a unifying force.

The current book is an expanded version of those notes. Some material has been added, and many more exercises are included. Historical notes are given at the end of each chapter with references to a few sources for the material.

These topics have the advantage of being somewhat familiar to a good high school graduate, yet harbour many interesting unforeseen results. The number of different proof techniques in the book makes this a good introduction to a wide variety of new ideas. In particular, special emphasis has been paid to the role of algorithms in mathematics. Due to the increased use of symbolic computing, and especially because of the availability of MAPLE here at Waterloo, it has been natural to investigate the theory behind many of these computations. It also provides an opportunity to have student work out problems with much larger numbers. Many other symbolic computation programs, such as MATHEMATICA, are equally good for use in this course.

This course has been taught at the University of Waterloo for over thirty years. Until about a decade ago, roughly 800–1200 first year students in the mathematical sciences took a course using the textbook *Classical Algebra* by W.J. Gilbert, now in a revised edition [**13**] co-authored by S.A. Vanstone. About 5% of these students took the 'advanced' version using these notes.

These notes were used for a one semester course. We would cover much of the material in this book, but not all. In writing this book, it has seemed advisable to expand on certain connections beyond the scope of the course. It is hoped that this will provide greater flexibility for the instructor and additional reading for the interested student.

Students entering university to study mathematics have probably encountered prime numbers. Chances are great that they believe every integer factors uniquely into a product of primes, but have not seen a proof. This important fact, known as the Fundamental Theorem of Arithmetic, is of crucial importance in the theory of numbers. It is not easy to prove. More importantly, it is not *intuitively obvious*. Indeed, its significance is only realized with very large numbers beyond our real experience. The crucial fact that enables us to prove this with relative ease is the Euclidean Algorithm for finding greatest common divisors. Chapters 1 and 2 deal with these basic properties of the integers and modular arithmetic. After giving the proof of the Fundamental Theorem of Arithmetic, we show that, in fact, the proof technique applies in much greater generality. In Section 1.8, we define Euclidean Domains and prove that all such rings have unique factorization. Throughout the book, we see applications of this general theorem in a large variety of setting, such as the Gaussian integers and polynomial rings over a field.

It is worth noting that there are number systems not very much different from the integers in which unique factorization into primes fails. Far from being a disaster, this is an opportunity to investigate why this phenomena occurs. It shows us which properties of the integers themselves are crucial to make the theory work. That is why we make a foray into quadratic number domains in Chapter 3. Already the material covered in Chapters 1–3 allow us to prove Quadratic Reciprocity, one of the crowning achievements of elementary number theory.

A nice application of modular arithmetic is the Rivest-Shamir-Adelman public key cryptography scheme. This code, which is covered in Chapter 4, allows the author to publish the method of *encoding* a message in a public place, while keeping the method of *decoding* the message secret. This is a rather different idea in coding, as for all previously known codes, the method of decoding merely reversed the encoding method. The secret here is that it is very easy (with a computer) to find large primes (say 200–300 digits) but very difficult to factor the product of two large primes. When one first encounters the problem of determining if a given number is prime, it is natural to try the brute force method of dividing by all numbers up to the square root. However, it turns out there are beautiful and clever methods to test for primality without finding any factors at all. We delve more deeply into this subject, briefly discussing the Agrawal-Kayal-Saxena algorithm and its connection to the topics we have seen thus far. We also discuss the probabilistic test due to Miller-Rabin.

In Chapter 5, we introduce the complex numbers. There is a tacit assumption that the student is already reasonably familiar with the real numbers from studying calculus. However, a section is devoted to a brief discussion of how the real numbers are developed. The main result of this chapter is the Fundamental Theorem of Algebra, which states that every complex

polynomial factors into a product of linear terms. We emphasize how *analytic* techniques play a key role in the proof of this cornerstone *algebraic* result. The proof we give is one of the simplest, and relies on the Extreme Value Theorem. We also develop the complex exponential function, which plays a vital role in applications of the complex numbers.

In Chapter 6, we show that the same theory developed for the integers applies to the algebra of polynomials. In particular, there is a Euclidean Algorithm and unique factorization into irreducible polynomials. We examine various tests for irreducibility, and study connections with irrationality of the roots. We then follow up with special topics about real and complex polynomials such as Sturm's Theorem for counting real roots, and the formula for solving cubics. In Chapter 7, we study finite fields in some detail. We draw parallels between modular arithmetic for the integers and arithmetic modulo an irreducible polynomial. Many of the results we have seen for $\mathbb{Z}_p$ in earlier chapters carry over to all finite fields. A rather beautiful application of these ideas is an algorithm for factoring polynomials over the rationals. This algorithm is based on a method for factoring polynomials modulo a prime integer p. It turns out that factoring a polynomial of degree d mod p is much easier than factoring a d digit base p number.

We would like to take this opportunity to thank the people who have helped with this endeavour. In particular, the first author thanks Stanley Burris with whom he has had many enjoyable conversations about this material. The first author also thanks Keith Geddes for some conversations on the algorithms used by MAPLE. The second author would like to thank David Jao and Stephen New for answering questions about the practical aspects of RSA. It is a pleasure to thank Anton Mosunov for a careful reading of an early draft of the new version of this book and for sending us detailed comments and corrections. We thank the referees and editors at AMS/MAA for their helpful comments. Lastly, we thank the many students in Math 145 classes who suffered through various versions of these notes and offered many helpful suggestions and corrections.

Kenneth R. Davidson
Matthew Satriano
Waterloo, January, 2023