Preface

This book is partially based on the lecture notes of several graduate courses that I taught at the University of South Florida since 2005. The first draft was written in 2006. The manuscript went through a thorough revision between 2015 and 2016 and finally evolved into the present form.

The subject of finite fields is at the intersection of algebra, combinatorics, and number theory, and is a source of widespread applications in information theory and computer science; as such, its boundary is not always easy to define. The following is a partial list of some areas that are traditionally considered important in the subject: (i) algebraic structures of and related to finite fields; (ii) number theory of finite fields and function fields over finite fields; (iii) finite geometry and combinatorics of finite fields; (iv) applications of finite fields in coding theory and cryptography. The standard references for finite fields are *Finite Fields* [**27**] by R. Lidl and H. Niederreiter and *Handbook of Finite Fields* [**28**] edited by G. Mullen and D. Panario. The former is a treatise on the theory and applications of finite fields with a comprehensive bibliography up to the early 1980s. The latter is the first handbook of finite fields and contains significant results from all areas of finite fields up to the early 2010s.

The present book is intended to be an exposition of selected topics in the theory of finite fields that can be used as a textbook for a graduate course. More precisely, my expectation of the finished work is a volume with a limited scope that covers the fundamentals of finite fields and explores additional selected topics without excessive overlap with other existing books on finite fields. Material gathering for the book was guided by these objectives. Inevitably, the topics selected reflect my own perspectives on the subject. To limit the scope of the book, I have resisted the temptation to

include other topics that are arguably both important and interesting, and the temptation to expand on some topics that are already in the book. In particular, applications of finite fields are not explored except for the Reed-Muller codes, which are treated in Chapters 2 and 5 under the guise of polynomials over finite fields. I hope this shortcoming is remedied by the fact that there are many excellent books devoted to applications of finite fields. I wish to mention a few unique features of the book. It contains some nontrivial results that are not so well known but are quite useful (e.g., the formula for the cardinalities of the conjugacy classes of the affine linear group $\mathrm{AGL}(n, \mathbb{F}_q)$); it also contains simplified proofs of several important theorems (e.g., the author's proof of the Katz theorem and Leducq's proof of the Delsarte-Goethals-MacWilliams theorem).

Here are the outlines of the chapters:

Chapter 1: The first section provides the preliminaries for the rest of the book. All basic facts about finite fields are proved there. Section 1.2 is devoted to partially ordered sets and the Möbius function, which are used later to count the number of irreducible polynomials over finite fields.

Chapter 2: We address a number of issues related to the algebra and combinatorics of polynomials over finite fields, except for questions concerning zeros of polynomials over finite fields, which are discussed later in Chapter 5. The topics include Berlekamp's factorization algorithm, counting for irreducible polynomials and irreducible factors, polynomial representation of functions, permutation polynomials, Dickson polynomials, linearized polynomials, and a generalization of a theorem by S. Payne on linearized polynomials. I have resisted the temptation to expand the coverage of permutation polynomials, which constitute an active research area of finite fields; interested readers are referred to a recent survey [**17**] on permutation polynomials. The last section on Payne's theorem is rather technical; the reader may choose to skip it at first reading.

Chapter 3: After a discussion of characters of finite abelian groups, Gauss sums are introduced. The highlights of the chapter are the Davenport-Hasse theorem on the Gauss sum of a lifted character and the calculation of the Gauss quadratic sum.

Chapter 4: This chapter is essentially a tailored introduction to algebraic number theory. No prerequisites other than graduate algebra and elementary number theory are required. Basic properties of number fields are proved and prime factorization in an arbitrary number field is discussed. In section 4.5, we focus on cyclotomic fields and determine how primes factor in such fields. In the last section, the results on cyclotomic fields are used to prove the Stickelberger congruence for Gauss sums.

Chapter 5: Zeros of polynomials over finite fields are an area where sophisticated methods are developed and profound results are proved. In this chapter, we introduce several theorems on zeros of polynomials over finite fields that are of fundamental importance. The theorems of Ax and Katz give sharp lower bounds for the p-adic order of the number of zeros of one or several polynomials over a finite field of characteristic p. The proof of Ax's theorem relies on Stickelberger's congruence for Gauss sums. The proof of Katz's theorem adopted here, found by the author, is much simpler than the original. Theorem 5.9 is a sharp lower bound for the number of common zeros of several polynomials, and Theorem 5.11 is a sharp upper bound for the number of zeros of one polynomial. The Delsarte-Goethals-MacWilliams theorem completely determines the polynomials meeting the upper bound in Theorem 5.11. The Delsarte-Goethals-MacWilliams theorem originally appeared as a characterization of minimal-weight codewords in the q-ary Reed-Muller code [**9**]; unfortunately, this strong result does not seem to be well known outside the coding theory community. The proof of the Delsarte-Goethals-MacWilliams theorem included here, recently discovered by Leducq, is also much simpler than the original. The last major theorem of the chapter is the Hasse-Weil bound on the number of zeros of an absolutely irreducible polynomial over a finite field. The result is easily stated, but its proof is beyond the scope of the present book. We attempt to alleviate the predicament by including a sketchy and informal introduction to function fields; section 5.4 is devoted to outlining the components of function fields that lead to the Hasse-Weil bound. Along the theme-line "places – the Riemann-Roch theorem – extensions – the zeta function – Riemann's hypothesis for function fields – the Hasse-Weil bound", notions and concepts are defined and theorems are stated without proof. For readers with some knowledge of function fields, section 5.4 serves as a review; for those without such knowledge, the section serves as a preview.

Chapter 6: The last chapter is an introduction to classical groups over finite fields. For a considerable part of this chapter, the field F is assumed to be more general than finite. We prove the simplicity of $\mathrm{PSL}(n, F)$ and derive formulas for the cardinalities of the conjugacy classes of the general linear group $\mathrm{GL}(n, \mathbb{F}_q)$ and the affine linear group $\mathrm{AGL}(n, \mathbb{F}_q)$. The formula for $\mathrm{AGL}(n, \mathbb{F}_q)$, which is useful for studying $\mathrm{AGL}(n, \mathbb{F}_q)$-actions on sets, does not seem to have appeared in any book. The last two sections are devoted to bilinear forms, unitary forms, quadratic forms, and the classical groups associated to such forms. When the field is finite, the forms are classified and the orders of the associated classical groups are determined.

Each chapter contains a set of exercises ranging from easy to challenging. The book is mostly self-contained. Except for section 5.4, almost all results in the book are proved in detail. The reader is assumed to have a basic

knowledge of graduate algebra. Throughout the book, all rings are with identity, all modules are unitary, a subring has the same identity as the ambient ring, and a ring homomorphism maps identity to identity.

Clarity through conciseness is a mantra that I aspired to throughout the preparation of this book. I would be gratified if a fraction of this goal is achieved.

I owe my special thanks to Professor Gary Mullen; without his encouragement and mentorship, this project would not have come to fruition. I am grateful to the anonymous referees for their careful reading of the manuscript and for their insightful comments and valuable suggestions. I also wish to express my gratitude to the AMS editors and staff members for their patience during my preparation and revision of the manuscript and for their assistance at various stages of the project. Finally, I would like to thank my students for their stimulating input and supportive feedback.

XDH

Tampa, FL 2017