GRADUATE STUDIES IN MATHEMATICS 190

Lectures on Finite Fields

Xiang-dong Hou

American Mathematical Society

10.1090/gsm/190

GRADUATE STUDIES IN MATHEMATICS 190

Lectures on Finite Fields

Xiang-dong Hou

AMERICAN MATHEMATICAL SOCIETY
Providence, Rhode Island

2010 *Mathematics Subject Classification*. Primary 11-01, 11Exx, 11Rxx, 11Txx.

For additional information and updates on this book, visit
www.ams.org/bookpages/gsm-190

Library of Congress Cataloging-in-Publication Data

Names: Hou, Xiang-dong, 1962- author.
Title: Lectures on finite fields / Xiang-dong Hou.
Description: Providence, Rhode Island : American Mathematical Society, [2018] | Series: Graduate studies in mathematics ; volume 190 | Includes bibliographical references and index.
Identifiers: LCCN 2017049952 | ISBN 9781470442897 (alk. paper)
Subjects: LCSH: Finite fields (Algebra) | AMS: Number theory – Instructional exposition (textbooks, tutorial papers, etc.). msc | Number theory – Forms and linear algebraic groups – Forms and linear algebraic groups. msc | Number theory – Algebraic number theory: global fields – Algebraic number theory: global fields. msc | Number theory – Finite fields and commutative rings (number-theoretic aspects) – Finite fields and commutative rings (number-theoretic aspects). msc
Classification: LCC QA247.3 .H68 2018 | DDC 512/.3–dc23
LC record available at https://lccn.loc.gov/2017049952

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at `http://www.ams.org/`

10 9 8 7 6 5 4 3 2 1   23 22 21 20 19 18

To Dong-lin, Wendy, and Elaine

Contents

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

Bibliography

[1] E. Artin, *Geometric Algebra* (reprint of the 1957 original), John Wiley & Sons, New York, 1988.

[2] J. Ax, *Zeros of polynomials over finite fields*, Amer. J. Math. **86** (1964), 255–261.

[3] E. A. Bender and J. R. Goldman, *On the applications of Möbius inversion in combinatorial analysis*, Amer. Math. Monthly **82** (1975), 789–803.

[4] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

[5] B. C. Berndt and R. J. Evans, *The determination of Gauss sums*, Bull. Amer. Math. Soc. (NS) **5** (1981), 107–129.

[6] A. Cafure and G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. **12** (2006), 155–185.

[7] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 73–75.

[8] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, Mathematical Surveys, Vol. 6. American Mathematical Society, Providence, RI, 1951.

[9] P. Delsarte, J. M. Goethals, F. J. MacWilliams, *On generalized Reed-Muller codes and their relatives*, Inform. Control **16** (1970), 403–442.

[10] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.

[11] C. F. Gauss, *Summatio quarumdam serierum singularium*, Comment. Soc. Reg. Sci. Gottingensis **1** (1811); *Werke*, vol. 2, pp. 11–45, Königl. Gesellschaft der Wissenschaften, Göttingen, 1876; *Untersuchungen über Höhere Arithmetik* (H. Maser ed.), pp. 463–495, Springer, Berlin, 1889.

[12] D. Gorenstein, *Finite Simple Groups: An Introduction to Their Classification*, Plenum Press, New York, 1982.

[13] D. Gorenstein, R. Lyons, R. Solomon. *The Classification of the Finite Simple Groups*, American Mathematical Society, Providence, RI, 1994.

[14] L. C. Grove, *Classical Groups and Geometric Algebra*, Graduate Studies in Mathematics, Vol. 39, American Mathematical Society, Providence, RI, 2002.

[15] X. Hou, *Solution to a problem of S. Payne*, Proc. Amer. Math. Soc. **132** (2004), 1–6.

[16] X. Hou, *A note on the proof of a theorem of Katz*, Finite Fields Appl. **11** (2005) 316–319.

[17] X. Hou, *Permutation polynomials over finite fields — a survey of recent advances*, Finite Fields Appl. **32** (2015), 82–119.

[18] T. W. Hungerford, *Algebra*, Springer-Verlag, New York–Berlin, 1980.

[19] A. Hurwitz, *Mathematische Werke*, Band II, Birkhäuser Verlag, Basel–Stuttgart, 1963.

[20] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1990.

[21] N. Jacobson, *Basic Algebra I*, Freeman, New York, 1985.

[22] N. M. Katz, *On a theorem of Ax*, Amer. J. Math. **93** (1971), 485–499.

[23] S. Lang, *Algebraic Number Theory*, Springer-Verlag, New York, 1994.

[24] S. Lang, *Algebra*, Springer-Verlag, New York, 2002.

[25] S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827.

[26] E. Leducq, *A new proof of Delsarte, Goethals and MacWilliams theorem on minimal weight codewords of generalized Reed-Muller codes*, Finite Fields Appl. **18** (2012), 581–586.

[27] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[28] G. L. Mullen and D. Panario (eds), *Handbook of Finite Fields*, Discrete Mathematics and Its Applications, CRC Press, Boca Raton, FL, 2013.

[29] S. E. Payne, *A complete determination of translation ovoids in finite Desarguian planes*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat Natur. (8) **51** (1971), 328–331.

[30] D. Robinson, *A Course in the Theory of Groups*, Springer, New York, 1995.

[31] J-P. Serre, *A Course in Arithmetic*, Springer, New York, 1973.

[32] W. M. Schmidt, *Equations over Finite Fields, An Elementary Approach*, Springer-Verlag, Berlin–Heidelberg–New York, 1976.

[33] C. L. Siegel, *Über das quadratische Reziprozitätsgesetz in algebraischen Zahlkörpern*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1960), 1–16.

[34] S. A. Stepanov, *Arithmetic of Algebraic Curves*, Plenum Publishing, New York, 1994.

[35] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[36] B. L. Van der Waerden, *Algebra II*, Springer-Verlag, Berlin, 1959.

[37] D. Wan, *An elementary proof of a theorem of Katz*, Amer. J. Math. **111** (1989), 1–8.

[38] D. Wan, *A Chevalley-Warning approach to p-adic estimates of character sums*, Proc. Amer. Math. Soc. **123** (1995), 45–54.

[39] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 76–83.

[40] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1997.

[41] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann et Cie., Paris, 1948.

List of Notation

$\mathbb{N}$	set of natural numbers $0, 1, 2, \ldots$
$\mathbb{Z}$	set of integers
$\mathbb{Z}^+$	set of positive integers
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	fields of rational, real, and complex numbers
$\mathbb{F}_q$	finite field with q elements
$[K : F]$	degree of field extension
$\overline{F}$	algebraic closure of F
F^*	multiplicative group of field F
$R^\times$	multiplicative group of ring R
$\mathtt{t}, \mathtt{T}, \mathtt{X}, \mathtt{Y}, \mathtt{Z}$	indeterminates
$\gcd(f, g)$	greatest common divisor of f and g
$\operatorname{lcm}(f, g)$	least common multiple of f and g
$\mathrm{M}_{m\times n}(R)$	set of $m \times n$ matrices over R
$F[\mathtt{X}]$	polynomial ring
$F(\mathtt{X})$	field of rational functions
$\|X\|$	cardinality of X
$\emptyset$	empty set
$\cong$	isomorphism, equivalence
$\subset$	subset
$\subsetneq$	proper subset
$\operatorname{char} F$	characteristic of F, 1
(f)	ideal generated by f, 3
$o(\alpha)$	order of α, 5
$\langle\ \rangle$	cyclic group generated by an element, 5
$\operatorname{Aut}(K/F)$	Galois group of K over F, 5
$\operatorname{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$, $\operatorname{Tr}_{q^n/q}$	trace from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, 7

$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$, $\mathrm{N}_{q^n/q}$	norm from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, 7
$\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^n}, \mathbb{F}_q)$	set of $\mathbb{F}_q$-maps from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, 7
$\tau\vert_K$	restriction of τ on K, 8
id	identity map, 9
μ	Möbius function, 12
$\delta(x, y)$	Kronecker symbol, 12
$\mathcal{P}(X)$	set of subsets of X, 15
$F[\mathtt{X}]_{\mathrm{m}}$	set of monic polynomials in $F[\mathtt{X}]$, 16
$\varprojlim \mathbb{Z}/i\mathbb{Z}$	inverse limit, 20
$F[[\mathtt{X}]]$	ring of formal power series, 21
$\zeta(s)$	Riemann zeta function, 21
$\mathcal{I}_q(n)$	set of monic irreducible polynomials of degree n, 23
null	nullity of a square matrix, 28
ϕ	Euler function, 31
$\mathcal{F}(X, Y)$	set of functions from X to Y, 32
$\mathcal{P}_{q,n}$	33
$R_q(r, n)$	Reed-Muller code, 34
$D_n(\mathtt{X}, \mathtt{Y})$	43
$D_n(\mathtt{X}, a)$	Dickson polynomial, 44
$\mathcal{L}(q, n)$	set of q-polynomials in $\mathbb{F}_{q^n}[\mathtt{X}]$, 46
$\mathcal{L}_k(q, n)$	set of q-polynomials in $\mathbb{F}_{q^n}[\mathtt{X}]$ of degree $\le q^k$, 46
$A(f)$	47
$F[\mathtt{X}; \sigma]$	skew polynomial ring, 48
$\Delta(\mathtt{X}_1, \ldots, \mathtt{X}_n)$	Moore determinant, 56
$\widehat{A}$	character group of A, 57
1^A	principal character of A, 57
$\langle \cdot, \cdot \rangle$	pairing between A and $\widehat{A}$, 58
$\mathcal{S}(A)$, $\mathcal{S}(\widehat{A})$	sets of subgroups of A and $\widehat{A}$, 58
$\widetilde{f}$	Fourier transform of f, 61
$f * g$	convolution, 61
$\mathbb{C}^A$	set of functions from A to $\mathbb{C}$, 63
$e_a(x)$	$\zeta_p^{\mathrm{Tr}_{q/p}(ax)}$, 63
$g_a(\chi)$	Gauss sum, 64
$g(\chi)$	$g_1(\chi)$, 65
$J(\chi_1, \ldots, \chi_k)$	Jacobi sum, 65
η	quadratic character of $\mathbb{F}_q^*$, 70
$K(\chi; a, b)$	Kloosterman sum, 74
$\overline{R}$	integral closure of R, 78
$\mathfrak{o}_F$	ring of integers of F, 79
$[K : F]_s$, $[K : F]_i$	separable and inseparable degree of K over F, 79
$\mathrm{Tr}_{K/F}$, $\mathrm{N}_{K/F}$	trace and norm from K to F, 79

$\Delta_{K/F}(\alpha_1, \ldots, \alpha_n)$	discriminant of $\alpha_1, \ldots, \alpha_n \in K$ over F, 81
δ_F	discriminant of F, 82
h_F	class number of number field F, 83
$\mathrm{Spec}^*(\mathfrak{o}_F)$	set of nonzero prime ideals of $\mathfrak{o}_F$, 85
$\mathrm{Cl}(F)$	ideal class group, 85
$\nu_{\mathfrak{p}}$	$\mathfrak{p}$-adic valuation, 86
$e(\mathfrak{P}\vert\mathfrak{p})$, $f(\mathfrak{P}\vert\mathfrak{p})$	ramification index and degree, 89
$D(\mathfrak{P}\vert\mathfrak{p})$	decomposition group of $\mathfrak{P}$ over $\mathfrak{p}$, 91
$E(\mathfrak{P}\vert\mathfrak{p})$	inertia group of $\mathfrak{P}$ over $\mathfrak{p}$, 91
$\mathbb{Q}(n)$	$\mathbb{Q}(e^{2\pi i/n})$, 96
$\chi_{\mathfrak{p}}$	103
$\wp$	103
$Z(f)$	set of zeros of f, 111
$\boldsymbol{x}^{\boldsymbol{u}}$	$x_1^{u_1} \cdots x_n^{u_n}$, 113
$\mathrm{supp}(f)$	support of f, 122
$\vert f\vert$	(Hamming) weight of f, 122
1_{H_i}	indicator function of H_i, 124
$\mathbb{P}_F$	set of places of function field F/K, 128
ν_P	valuation at place P, 128
$\mathcal{O}_P$	valuation ring of place P, 129
F_P	residue field of place P, 129
$\mathcal{D}_F$	divisor group of F, 129
$\deg A$	degree of divisor A, 129
$\mathcal{C}_F$	divisor class group of F, 129
$\mathcal{L}(A)$	130
$\dim A$	dimension of divisor A, 130
g	genus, 130
$\mathcal{A}_F$	set of adeles of F, 130
Ω_F	set of Weil differentials of F, 130
$e(P'\vert P)$, $f(P'\vert P)$	ramification index and relative degree, 132
h	class number of function field $F/\mathbb{F}_q$, 133
$Z_F(\mathtt{t})$	zeta function of F, 133
$L_F(\mathtt{t})$	L-polynomial of F, 134
$I(P, f \cap g)$	intersection number, 135
$\mathbb{P}^n(K)$	n-dimensional projective space over K, 136
$m_P(f)$	multiplicity of f at P, 136
$V_{\mathbb{P}^n(\mathbb{F}_q)}(f)$	137
$\mathrm{Z}(G)$	center of G, 143
G'	commutator subgroup of G, 143
$\mathrm{N}_G(H)$	normalizer of H in G, 143
$\mathrm{C}_G(X)$	centralizer of X in G, 143
$[a]_G$	conjugacy class of a in G, 143

Index

SELECTED PUBLISHED TITLES IN THIS SERIES

190 **Xiang-dong Hou,** Lectures on Finite Fields, 2018
187 **John Douglas Moore,** Introduction to Global Analysis, 2017
186 **Bjorn Poonen,** Rational Points on Varieties, 2017
185 **Douglas J. LaFountain and William W. Menasco,** Braid Foliations in Low-Dimensional Topology, 2017
184 **Harm Derksen and Jerzy Weyman,** An Introduction to Quiver Representations, 2017
183 **Timothy J. Ford,** Separable Algebras, 2017
182 **Guido Schneider and Hannes Uecker,** Nonlinear PDEs, 2017
181 **Giovanni Leoni,** A First Course in Sobolev Spaces, Second Edition, 2017
180 **Joseph J. Rotman,** Advanced Modern Algebra: Third Edition, Part 2, 2017
179 **Henri Cohen and Fredrik Strömberg,** Modular Forms, 2017
178 **Jeanne N. Clelland,** From Frenet to Cartan: The Method of Moving Frames, 2017
177 **Jacques Sauloy,** Differential Galois Theory through Riemann-Hilbert Correspondence, 2016
176 **Adam Clay and Dale Rolfsen,** Ordered Groups and Topology, 2016
175 **Thomas A. Ivey and Joseph M. Landsberg,** Cartan for Beginners: Differential Geometry via Moving Frames and Exterior Differential Systems, Second Edition, 2016
174 **Alexander Kirillov Jr.,** Quiver Representations and Quiver Varieties, 2016
173 **Lan Wen,** Differentiable Dynamical Systems, 2016
172 **Jinho Baik, Percy Deift, and Toufic Suidan,** Combinatorics and Random Matrix Theory, 2016
171 **Qing Han,** Nonlinear Elliptic Equations of the Second Order, 2016
170 **Donald Yau,** Colored Operads, 2016
169 **András Vasy,** Partial Differential Equations, 2015
168 **Michael Aizenman and Simone Warzel,** Random Operators, 2015
167 **John C. Neu,** Singular Perturbation in the Physical Sciences, 2015
166 **Alberto Torchinsky,** Problems in Real and Functional Analysis, 2015
165 **Joseph J. Rotman,** Advanced Modern Algebra: Third Edition, Part 1, 2015
164 **Terence Tao,** Expansion in Finite Simple Groups of Lie Type, 2015
163 **Gérald Tenenbaum,** Introduction to Analytic and Probabilistic Number Theory, Third Edition, 2015
162 **Firas Rassoul-Agha and Timo Seppäläinen,** A Course on Large Deviations with an Introduction to Gibbs Measures, 2015
161 **Diane Maclagan and Bernd Sturmfels,** Introduction to Tropical Geometry, 2015
160 **Marius Overholt,** A Course in Analytic Number Theory, 2014
159 **John R. Faulkner,** The Role of Nonassociative Algebra in Projective Geometry, 2014
158 **Fritz Colonius and Wolfgang Kliemann,** Dynamical Systems and Linear Algebra, 2014
157 **Gerald Teschl,** Mathematical Methods in Quantum Mechanics: With Applications to Schrödinger Operators, Second Edition, 2014
156 **Markus Haase,** Functional Analysis, 2014
155 **Emmanuel Kowalski,** An Introduction to the Representation Theory of Groups, 2014
154 **Wilhelm Schlag,** A Course in Complex Analysis and Riemann Surfaces, 2014
153 **Terence Tao,** Hilbert's Fifth Problem and Related Topics, 2014
152 **Gábor Székelyhidi,** An Introduction to Extremal Kähler Metrics, 2014
151 **Jennifer Schultens,** Introduction to 3-Manifolds, 2014
150 **Joe Diestel and Angela Spalsbury,** The Joys of Haar Measure, 2013
149 **Daniel W. Stroock,** Mathematics of Probability, 2013
148 **Luis Barreira and Yakov Pesin,** Introduction to Smooth Ergodic Theory, 2013
147 **Xingzhi Zhan,** Matrix Theory, 2013

The theory of finite fields encompasses algebra, combinatorics, and number theory and has furnished widespread applications in other areas of mathematics and computer science. This book is a collection of selected topics in the theory of finite fields and related areas. The topics include basic facts about finite fields, polynomials over finite fields, Gauss sums, algebraic number theory and cyclotomic fields, zeros of polynomials over finite fields, and classical groups over finite fields. The book is mostly self-contained, and the material covered is accessible to readers with the knowledge of graduate algebra; the only exception is a section on function fields. Each chapter is supplied with a set of exercises. The book can be adopted as a text for a second year graduate course or used as a reference by researchers.

ISBN 978-1-4704-3518-9

9 781470 435189

GSM/190

For additional information and updates on this book, visit

www.ams.org/bookpages/gsm-190

AMS
www.ams.org