

Contents

Forewordxi
Prefacexiii
Chapter 1 Algebraic Foundations	1
1 Groups	2
2 Rings and Fields	11
3 Polynomials	18
4 Field Extensions	30
Notes	37
Exercises	40
Chapter 2 Structure of Finite Fields	47
1 Characterization of Finite Fields	48
2 Roots of Irreducible Polynomials	51
3 Traces, Norms, and Bases	54
4 Roots of Unity and Cyclotomic Polynomials	63

5	Representation of Elements of Finite Fields	66
6	Wedderburn's Theorem	69
	Notes	73
	Exercises	78
Chapter 3	Polynomials over Finite Fields	83
1	Order of Polynomials and Primitive Polynomials	84
2	Irreducible Polynomials	91
3	Construction of Irreducible Polynomials	96
4	Linearized Polynomials	107
5	Binomials and Trinomials	124
	Notes	131
	Exercises	140
Chapter 4	Factorization of Polynomials	147
1	Factorization over Small Finite Fields	148
2	Factorization over Large Finite Fields	157
3	Calculation of Roots of Polynomials	168
	Notes	177
	Exercises	183
Chapter 5	Exponential Sums	186
1	Characters	187
2	Gaussian Sums	192
3	Jacobi Sums	205
4	Character Sums with Polynomial Arguments	217
5	Further Results on Character Sums	226
	Notes	240
	Exercises	257
Chapter 6	Equations over Finite Fields	268
1	Elementary Results on the Number of Solutions	269
2	Quadratic Forms	278
3	Diagonal Equations	289
4	The Stepanov-Schmidt Method	300
	Notes	317
	Exercises	339
Chapter 7	Permutation Polynomials	347
1	Criteria for Permutation Polynomials	348
2	Special Types of Permutation Polynomials	351

3	Groups of Permutation Polynomials	357
4	Exceptional Polynomials	362
5	Permutation Polynomials in Several Indeterminates	368
	Notes	377
	Exercises	389
Chapter 8	Linear Recurring Sequences	394
1	Feedback Shift Registers, Periodicity Properties	395
2	Impulse Response Sequences, Characteristic Polynomial	402
3	Generating Functions	411
4	The Minimal Polynomial	418
5	Families of Linear Recurring Sequences	423
6	Characterization of Linear Recurring Sequences	437
7	Distribution Properties of Linear Recurring Sequences	444
	Notes	453
	Exercises	464
Chapter 9	Applications of Finite Fields	470
1	Linear Codes	471
2	Cyclic Codes	482
3	Finite Geometries	496
4	Combinatorics	508
5	Linear Modular Systems	517
	Notes	528
	Exercises	533
Chapter 10	Tables	541
1	Computation in Finite Fields	541
2	Tables of Irreducible Polynomials	543
	Notes	544
	Tables	546
	Bibliography	567
	List of Symbols	727
	Author Index	731
	Subject Index	747