

# Contents

<i>Preface</i>	ix
----------------	----

<b>1</b>	<b>Finite Fields and Function Fields</b>	<b>1</b>
	1.1 Structure of Finite Fields	1
	1.2 Algebraic Closure of Finite Fields	4
	1.3 Irreducible Polynomials	7
	1.4 Trace and Norm	9
	1.5 Function Fields of One Variable	12
	1.6 Extensions of Valuations	25
	1.7 Constant Field Extensions	27
<b>2</b>	<b>Algebraic Varieties</b>	<b>30</b>
	2.1 Affine and Projective Spaces	30
	2.2 Algebraic Sets	37
	2.3 Varieties	44
	2.4 Function Fields of Varieties	50
	2.5 Morphisms and Rational Maps	56
<b>3</b>	<b>Algebraic Curves</b>	<b>68</b>
	3.1 Nonsingular Curves	68
	3.2 Maps Between Curves	76
	3.3 Divisors	80
	3.4 Riemann-Roch Spaces	84
	3.5 Riemann's Theorem and Genus	87
	3.6 The Riemann-Roch Theorem	89
	3.7 Elliptic Curves	95
	3.8 Summary: Curves and Function Fields	104
<b>4</b>	<b>Rational Places</b>	<b>105</b>
	4.1 Zeta Functions	105
	4.2 The Hasse-Weil Theorem	115
	4.3 Further Bounds and Asymptotic Results	122
	4.4 Character Sums	127

<b>5</b>	<b>Applications to Coding Theory</b>	147
	5.1 Background on Codes	147
	5.2 Algebraic-Geometry Codes	151
	5.3 Asymptotic Results	155
	5.4 NXL and XNL Codes	174
	5.5 Function-Field Codes	181
	5.6 Applications of Character Sums	187
	5.7 Digital Nets	192
<b>6</b>	<b>Applications to Cryptography</b>	206
	6.1 Background on Cryptography	206
	6.2 Elliptic-Curve Cryptosystems	210
	6.3 Hyperelliptic-Curve Cryptography	214
	6.4 Code-Based Public-Key Cryptosystems	218
	6.5 Frameproof Codes	223
	6.6 Fast Arithmetic in Finite Fields	233
<b>A</b>	<b>Appendix</b>	241
	A.1 Topological Spaces	241
	A.2 Krull Dimension	244
	A.3 Discrete Valuation Rings	245
	<i>Bibliography</i>	249
	<i>Index</i>	257