Contents

1 Endomorphisms 1
- 1.1 Generalized Eigenspaces 2
  - 1.1.A Big Kernels and Small Images 3
  - 1.1.B Minimal Polynomials and Eigenspaces 6
- 1.2 Minimal and Characteristic Polynomials 12
- 1.3 Nilpotent Endomorphisms and Multiplicities 17
- 1.4 The Module Structure Given by an Endomorphism 24
- 1.5 Commendable Endomorphisms 34
- 1.6 Other Special Endomorphisms 40

2 Families of Commuting Endomorphisms 47
- 2.1 Commuting Families 49
- 2.2 Kernels and Big Kernels of Ideals 54
  - 2.2.A Properties of Zero-Dimensional Rings 55
  - 2.2.B Properties of Kernels and Big Kernels of Ideals 59
- 2.3 Eigenfactors 64
- 2.4 Joint Eigenspaces 69
- 2.5 Splitting Endomorphisms 77
- 2.6 Simultaneous Diagonalization and Triangularization 89

3 Special Families of Endomorphisms 95
- 3.1 $\mathscr{F}$-Cyclic Vector Spaces 96
- 3.2 Unigenerated Families 101
- 3.3 Commendable Families 110
- 3.4 Local Families 113
- 3.5 Dual Families 119
- 3.6 Extended Families 126

4 Zero-Dimensional Affine Algebras 131
- 4.1 Multiplication Endomorphisms 134
- 4.2 Primary Decomposition and Separators 139
- 4.3 Commendable and Splitting Multiplication Endomorphisms . . . 145

4.4 Local Multiplication Families 153
4.5 Dual Multiplication Families 161
4.6 Hilbert Functions and the Cayley-Bacharach Property 175

5 Computing Primary and Maximal Components 185
5.1 Computing Primary Decompositions 188
5.1.A Using the Generically Extended Linear Form 189
5.1.B Using Linear Forms and Idempotents 194
5.1.C Computing Joint Eigenspaces 200
5.2 Primary Decomposition over Finite Fields 203
5.3 Computing Maximal Components via Factorization 213
5.3.A Minimal Polynomials and Finite Field Extensions 213
5.3.B Factorizing over Extension Fields 218
5.3.C Using Factorizations to Compute Maximal Components . 223
5.4 Primary Decompositions Using Radical Ideals 226
5.4.A Maximal Components via Radical Ideals 227
5.4.B Primary Components from Maximal Components 233
5.5 The Separable Subalgebra 237

6 Solving Zero-Dimensional Polynomial Systems 243
6.1 Rational Zeros via Commuting Families 245
6.1.A Computing One-Dimensional Joint Eigenspaces 246
6.1.B Computing Linear Maximal Ideals 252
6.2 Rational Zeros via Eigenvalues and Eigenvectors 255
6.2.A The Eigenvalue Method 256
6.2.B The Eigenvector Method 264
6.3 Solving Polynomial Systems over Finite Fields 269
6.3.A Computing Isomorphisms of Finite Fields 271
6.3.B Solving over Finite Fields via Cloning 279
6.3.C Solving over Finite Fields via Univariate Representations 285
6.3.D Solving over Finite Fields via Recursion 290
6.4 Solving Polynomial Systems over the Rationals 295
6.4.A Splitting Fields in Characteristic Zero 297
6.4.B Solving over the Rational Numbers via Cloning 302

Notation 311

References 315

Index 317