Contents

Introduction v

1 An Introduction to Polynomials **1**

1.1 Construction and Representation of Polynomials 1

1.1.1 Construction of polynomials 1

1.1.2 Representation of polynomials 4

1.2 Complexity and Cost 6

1.2.1 Complexity 6

1.2.2 Cost of polynomial operations 7

1.3 Polynomial Division 13

1.3.1 Divisibility 13

1.3.2 Unique factorization domains 14

1.3.3 The Euclidean division algorithm 16

1.3.4 Existence of gcd 17

1.3.5 Construction of gcd 18

1.3.6 Pseudo–division and polynomial remainder sequences . . 19

1.4 Polynomial Factorization 25

1.4.1 Polynomials over factorial rings 26

1.5 Polynomial Roots. Elimination. Resultants 29

1.5.1 Polynomial roots 29

1.5.2 Elimination theory. Resultants 33

1.5.3 The abridged method of Bézout 34

1.5.4 Jacobi's version 36

1.5.5 Cauchy's contribution 37

1.5.6 The companion matrix 39

1.6 Symmetric Functions 42

1.7 Polynomial Interpolation 48

1.7.1 Lagrange interpolation 49

1.7.2 Lagrange–Hermite interpolation 49

1.7.3 Newton interpolation 50

1.7.4 Taylor interpolation 51

1.7.5 Newton–Hermite interpolation 52

1.7.6 Finite differences 53

1.7.7 Chinese remainder theorem 54

1.8 Irreducibility Criteria 58
1.8.1 Irreducible polynomials in one variable 58
1.8.2 Irreducible polynomials in many variables 63
1.8.3 Generalized difference polynomials 66

2 Complex Polynomials **77**
2.1 Polynomial Size 77
2.1.1 Norm 77
2.1.2 Measure 79
2.1.3 Length and height of a polynomial 83
2.1.4 Upper bounds for factors 85
2.2 Geometry of Polynomials 92
2.2.1 Location of polynomial roots 93
2.2.2 Apolar polynomials 95
2.3 Stable Polynomials 101
2.4 Polynomial Roots Inside the Unit Disk 108
2.5 Bounds for the Roots 113
2.5.1 Inclusion radii 113
2.5.2 Disks containing no roots 120
2.5.3 Disks containing at least one root 121
2.5.4 Disks containing at least a prescribed number of roots . . 123
2.6 Applications to Integer Polynomials 132
2.6.1 An irreducibility test 133
2.6.2 Primes and polynomial irreducibility 134
2.7 Separation of Roots 137

3 Polynomials with Coefficients in a Finite Field **141**
3.1 Finite Fields 141
3.1.1 Construction of finite fields 142
3.1.2 Representation of elements of finite fields 148
3.2 Cyclotomic Polynomials 154
3.2.1 Definition of cyclotomic polynomials 154
3.2.2 Möbius inversion formula 156
3.2.3 Factorization of cyclotomic polynomials 157
3.3 Fast Fourier Transform 162
3.3.1 Discrete Fourier transform 162
3.3.2 Discrete fast Fourier transform 166
3.3.3 Fast multiplication of polynomials 169
3.4 Number of Irreducible Polynomials over a Finite Field 180
3.5 Construction of Irreducible Polynomials Over a Finite Field . . . 186
3.5.1 Exponents of polynomials over a finite field 186
3.5.2 Irreducibility of binomials 192
3.5.3 Artin–Schreier polynomials 193
3.6 Roots of Polynomials Over Finite Fields 196
3.7 Squarefree Polynomials 200
3.7.1 Definition of squarefree polynomials 200

3.7.2 Factorization into a product of squarefree polynomials . . 200
3.7.3 The number of squarefree polynomials 202
3.8 Berlekamp's Algorithm 204
3.8.1 Factorization of polynomials over finite fields 204
3.8.2 Polynomial factorization over $\mathbb{F}_p$ 205
3.8.3 Polynomial factorization over $\mathbb{F}_q$ 207
3.8.4 Description of the algorithm 211
3.8.5 Berlekamp's method over large fields 214
3.9 Niederreiter's Algorithm 221
3.9.1 Factorization of squarefree polynomials 222
3.9.2 Factorization of nonsquarefree polynomials 225
3.9.3 Factorization over $\mathbb{F}_2$ 228
3.9.4 The refinement by Göttfert 230
3.9.5 Hasse–Teichmüller derivatives method 233

4 Integer Polynomials 241

4.1 Kronecker's Factorization Method 241
4.1.1 Kronecker's algorithm 241
4.1.2 Kronecker–Hausmann algorithm 243
4.1.3 A bound for factors 248
4.2 The Berlekamp–Zassenhaus Algorithm 249
4.2.1 Modern methods of factorization in $\mathbb{Z}[X]$ 250
4.2.2 Size of factors 251
4.2.3 Hensel's lemma 252
4.2.4 Reconstruction of factors over the integers 256
4.3 The LLL Factorization Algorithm 261
4.3.1 Reduced bases for lattices 261
4.3.2 Reduced lattices 262
4.3.3 Basis reduction algorithm 265
4.3.4 Polynomial factorization and lattices 271
4.3.5 The factorization algorithm 276
4.3.6 Cost of the algorithm 280

Bibliography 285

Notation 295

List of Algorithms 299

Name Index 301

Subject Index 303