Contents

1 **Roots of Polynomials** 1
1.1 Inequalities for roots 1
1.1.1 The Fundamental Theorem of Algebra 1
1.1.2 Cauchy's theorem 2
1.1.3 Laguerre's theorem 5
1.1.4 Apolar polynomials 7
1.1.5 The Routh-Hurwitz problem 11
1.2 The roots of a given polynomial and of its derivative 12
1.2.1 The Gauss-Lucas theorem 12
1.2.2 The roots of the derivative and the focal points of an ellipse 14
1.2.3 Localization of the roots of the derivative 15
1.2.4 The Sendov-Ilieff conjecture 18
1.2.5 Polynomials whose roots coincide with the roots of their derivatives 20
1.3 The resultant and the discriminant 20
1.3.1 The resultant 20
1.3.2 The discriminant 23
1.3.3 Computing certain resultants and discriminants 25
1.4 Separation of roots 27
1.4.1 The Fourier–Budan theorem 27
1.4.2 Sturm's Theorem 30
1.4.3 Sylvester's theorem 31
1.4.4 Separation of complex roots 35
1.5 Lagrange's series and estimates of the roots of a given polynomial 37
1.5.1 The Lagrange-Bürmann series 37
1.5.2 Lagrange's series and estimation of roots 40
1.6 Problems to Chapter 1 41
1.7 Solutions of selected problems 42

Bibliografische Informationen
http://d-nb.info/996064540

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

2 Irreducible Polynomials 47
2.1 Main properties of irreducible polynomials 47
2.1.1 Factorization of polynomials into irreducible factors 47
2.1.2 Eisenstein's criterion 50
2.1.3 Irreducibility modulo p 51
2.2 Irreducibility criteria 52
2.2.1 Dumas's criterion 52
2.2.2 Polynomials with a dominant coefficient 56
2.2.3 Irreducibility of polynomials attaining small values 58
2.3 Irreducibility of trinomials and fournomials 59
2.3.1 Irreducibility of polynomials of the form $x^n \pm x^m \pm x^p \pm 1$ 59
2.3.2 Irreducibility of certain trinomials 63
2.4 Hilbert's irreducibility theorem 65
2.5 Algorithms for factorization into irreducible factors 68
2.5.1 Berlekamp's algorithm 68
2.5.2 Factorization with the help of Hensel's lemma 71
2.6 Problems to Chapter 2 73
2.7 Solutions of selected problems 74

3 Polynomials of a Particular Form 77
3.1 Symmetric polynomials 77
3.1.1 Examples of symmetric polynomials 77
3.1.2 Main theorem on symmetric polynomials 79
3.1.3 Muirhead's inequalities 81
3.1.4 The Schur functions 83
3.2 Integer-valued polynomials 85
3.2.1 A basis in the space of integer-valued polynomials 85
3.2.2 Integer-valued polynomials in several variables 87
3.2.3 The q-analogue of integer-valued polynomials 88
3.3 The cyclotomic polynomials 89
3.3.1 Main properties of the cyclotomic polynomials 89
3.3.2 The Möbius inversion formula 90
3.3.3 Irreducibility of cyclotomic polynomials 91
3.3.4 The expression for Φ_{mn} in terms of Φ_n 93
3.3.5 The discriminant of a cyclotomic polynomial 94
3.3.6 The resultant of a pair of cyclotomic polynomials 95
3.3.7 Coefficients of the cyclotomic polynomials 96
3.3.8 Wedderburn's theorem 97
3.3.9 Polynomials irreducible modulo p 99
3.4 Chebyshev polynomials 100
3.4.1 Definition and main properties of Chebyshev polynomials 100
3.4.2 Orthogonal polynomials 105
3.4.3 Inequalities for Chebyshev polynomials 107
3.4.4 Generating functions 109

3.5 Bernoulli polynomials 112
3.5.1 Definition of Bernoulli polynomials 112
3.5.2 Theorems of complement, addition of arguments and multiplication 115
3.5.3 Euler's formula 116
3.5.4 The Faulhaber-Jacobi theorem 117
3.5.5 Arithmetic properties of Bernoulli numbers and Bernoulli polynomials 120
3.6 Problems to Chapter 3 125
3.6.1 Symmetric polynomials 125
3.6.2 Integer-valued polynomials 126
3.6.3 Chebyshev polynomials 126
3.7 Solution of selected problems 127

4 Certain Properties of Polynomials 133
4.1 Polynomials with prescribed values 133
4.1.1 Lagrange's interpolation polynomial 133
4.1.2 Hermite's interpolation polynomial 136
4.1.3 The polynomial with prescribed values at the zeros of its derivative 137
4.2 The height of a polynomial and other norms 139
4.2.1 Gauss's lemma 139
4.2.2 Polynomials in one variable 141
4.2.3 The maximum of the absolute value and S. Bernstein's inequality 145
4.2.4 Polynomials in several variables 148
4.2.5 An inequality for a pair of relatively prime polynomials 151
4.2.6 Mignotte's inequality 152
4.3 Equations for polynomials 154
4.3.1 Diophantine equations for polynomials 154
4.3.2 Functional equations for polynomials 162
4.4 Transformations of polynomials 166
4.4.1 Tchirnhaus's transformation 166
4.4.2 5th degree equation in Bring's form 168
4.4.3 Representation of polynomials as sums of powers of linear functions 169
4.5 Algebraic numbers 173
4.5.1 Definition and main properties of algebraic numbers ... 173
4.5.2 Kronecker's theorem 175
4.5.3 Liouville's theorem 176
4.6 Problems to Chapter 4 179

5 Galois Theory 181
5.1 Lagrange's theorem and the Galois resolvent 181
5.1.1 Lagrange's theorem 181
5.1.2 The Galois resolvent 185
5.1.3 Theorem on a primitive element 189
5.2 Basic Galois theory 191
5.2.1 The Galois correspondence 191
5.2.2 A polynomial with the Galois group S_5 195
5.2.3 Simple radical extensions 196
5.2.4 The cyclic extensions 197
5.3 How to solve equations by radicals 199
5.3.1 Solvable groups 199
5.3.2 Equations with solvable Galois group 200
5.3.3 Equations solvable by radicals 201
5.3.4 Abelian equations 204
5.3.5 The Abel-Galois criterion for solvability of equations of prime degree 208
5.4 Calculation of the Galois groups 212
5.4.1 The discriminant and the Galois group 212
5.4.2 Resolvent polynomials 213
5.4.3 The Galois group modulo p 216

6 Ideals in Polynomial Rings 219
6.1 Hilbert's basis theorem and Hilbert's theorem on zeros 219
6.1.1 Hilbert's basis theorem 219
6.1.2 Hilbert's theorem on zeros 221
6.1.3 Hilbert's polynomial 224
6.1.4 The homogeneous Hilbert's Nullstellensatz for p-fields 231
6.2 Gröbner bases 233
6.2.1 Polynomials in one variable 234
6.2.2 Division of polynomials in several variables 235
6.2.3 Definition of Gröbner bases 235
6.2.4 Buchberger's algorithm 237
6.2.5 A reduced Gröbner basis 239

7 Hilbert's Seventeenth Problem 243
7.1 The sums of squares: introduction 243
7.1.1 Several examples 243
7.1.2 Artin-Cassels-Pfister theorem 248
7.1.3 The inequality between the arithmetic and geometric means 251
7.1.4 Hilbert's theorem on non-negative polynomials $p_4(x, y)$ 253
7.2 Artin's theory 259
7.2.1 Real fields 259
7.2.2 Sylvester's theorem for real closed fields 263

7.2.3 Hilbert's seventeenth problem 266
7.3 Pfister's theory 270
7.3.1 The multiplicative quadratic forms 270
7.3.2 C_i-fields 273
7.3.3 Pfister's theorem on the sums of squares of rational functions 274

8 Appendix 279
8.1 The Lenstra-Lenstra-Lovász algorithm 279
8.1.1 The general description of the algorithm 279
8.1.2 A reduced basis of the lattice 280
8.1.3 The lattices and factorization of polynomials 283

References 289

Index 297