

# Contents

<i>Preface</i>	<i>page xi</i>
<b>Part one: The Kronecker – Duval Philosophy</b>	<b>1</b>
<b>1 Euclid</b>	<b>3</b>
1.1 The Division Algorithm	4
1.2 Euclidean Algorithm	6
1.3 Bezout’s Identity and Extended Euclidean Algorithm	8
1.4 Roots of Polynomials	9
1.5 Factorization of Polynomials	10
1.6* <i>Computing a gcd</i>	12
1.6.1* <i>Coefficient explosion</i>	12
1.6.2* <i>Modular Algorithm</i>	16
1.6.3* <i>Hensel Lifting Algorithm</i>	16
1.6.4* <i>Heuristic gcd</i>	18
<b>2 Intermezzo: Chinese Remainder Theorems</b>	<b>23</b>
2.1 Chinese Remainder Theorems	24
2.2 Chinese Remainder Theorem for a Principal Ideal Domain	26
2.3 A Structure Theorem (1)	29
2.4 Nilpotents	32
2.5 Idempotents	35
2.6 A Structure Theorem (2)	39
2.7 Lagrange Formula	41
<b>3 Cardano</b>	<b>47</b>
3.1 A Tautology?	47
3.2 The Imaginary Number	48
3.3 An Impasse	51
3.4 A Tautology!	52

viii	<i>Contents</i>	
<b>4</b>	<b>Intermezzo: Multiplicity of Roots</b>	53
	4.1 Characteristic of a Field	54
	4.2 Finite Fields	55
	4.3 Derivatives	57
	4.4 Multiplicity	58
	4.5 Separability	62
	4.6 Perfect Fields	64
	4.7 Squarefree Decomposition	68
<b>5</b>	<b>Kronecker I: Kronecker's Philosophy</b>	74
	5.1 Quotients of Polynomial Rings	75
	5.2 The Invention of the Roots	76
	5.3 Transcendental and Algebraic Field Extensions	81
	5.4 Finite Algebraic Extensions	84
	5.5 Splitting Fields	86
<b>6</b>	<b>Intermezzo: Sylvester</b>	91
	6.1 Gauss Lemma	92
	6.2 Symmetric Functions	96
	6.3* Newton's Theorem	100
	6.4 The Method of Indeterminate Coefficients	106
	6.5 Discriminant	108
	6.6 Resultants	112
	6.7 Resultants and Roots	115
<b>7</b>	<b>Galois I: Finite Fields</b>	119
	7.1 Galois Fields	120
	7.2 Roots of Polynomials over Finite Fields	123
	7.3 Distinct Degree Factorization	125
	7.4 Roots of Unity and Primitive Roots	127
	7.5 Representation and Arithmetics of Finite Fields	133
	7.6* Cyclotomic Polynomials	135
	7.7* Cycles, Roots and Idempotents	141
	7.8 Deterministic Polynomial-time Primality Test	148
<b>8</b>	<b>Kronecker II: Kronecker's Model</b>	156
	8.1 Kronecker's Philosophy	156
	8.2 Explicitly Given Fields	159
	8.3 Representation and Arithmetics	164
	8.3.1 <i>Representation</i>	164
	8.3.2 <i>Vector space arithmetics</i>	165
	8.3.3 <i>Canonical representation</i>	165
	8.3.4 <i>Multiplication</i>	167
	8.3.5 <i>Inverse and division</i>	167

<i>Contents</i>		ix
	8.3.6 <i>Polynomial factorization</i>	168
	8.3.7 <i>Solving polynomial equations</i>	169
	8.3.8 <i>Monic polynomials</i>	169
	8.4 Primitive Element Theorems	170
<b>9</b>	<b>Steinitz</b>	175
	9.1 Algebraic Closure	176
	9.2 Algebraic Dependence and Transcendence Degree	180
	9.3 The Structure of Field Extensions	184
	9.4 Universal Field	186
	9.5* Lüroth's Theorem	187
<b>10</b>	<b>Lagrange</b>	191
	10.1 Conjugates	192
	10.2 Normal Extension Fields	193
	10.3 Isomorphisms	196
	10.4 Splitting Fields	203
	10.5 Trace and Norm	206
	10.6 Discriminant	212
	10.7* Normal Bases	216
<b>11</b>	<b>Duval</b>	221
	11.1 Explicit Representation of Rings	221
	11.2 Ring Operations in a Non-unique Representation	223
	11.3 Duval Representation	224
	11.4 Duval's Model	228
<b>12</b>	<b>Gauss</b>	232
	12.1 The Fundamental Theorem of Algebra	232
	12.2 Cyclotomic Equations	237
<b>13</b>	<b>Sturm</b>	263
	13.1* Real Closed Fields	264
	13.2 Definitions	272
	13.3 Sturm	275
	13.4 Sturm Representation of Algebraic Reals	280
	13.5 Hermite's Method	284
	13.6 Thom Codification of Algebraic Reals (1)	288
	13.7 Ben-Or, Kozen and Reif Algorithm	290
	13.8 Thom Codification of Algebraic Reals (2)	294
<b>14</b>	<b>Galois II</b>	297
	14.1 Galois Extension	298
	14.2 Galois Correspondence	300
	14.3 Solvability by Radicals	305
	14.4 Abel–Ruffini Theorem	314

x	<i>Contents</i>	
	14.5* Constructions with Ruler and Compass	318
	<b>Part two: Factorization</b>	327
<b>15</b>	<b>Prelude</b>	329
	15.1 A Computation	329
	15.2 An Exercise	338
<b>16</b>	<b>Kronecker III: factorization</b>	346
	16.1 Von Schubert Factorization Algorithm over the Integers	347
	16.2 Factorization of Multivariate Polynomials	350
	16.3 Factorization over a Simple Algebraic Extension	352
<b>17</b>	<b>Berlekamp</b>	361
	17.1 Berlekamp's Algorithm	361
	17.2 The Cantor–Zassenhaus Algorithm	369
<b>18</b>	<b>Zassenhaus</b>	380
	18.1 Hensel's Lemma	381
	18.2 The Zassenhaus Algorithm	389
	18.3 Factorization Over a Simple Transcendental Extension	391
	18.4 Cauchy Bounds	395
	18.5 Factorization over the Rationals	398
	18.6 Swinnerton-Dyer Polynomials	402
	18.7 $L^3$ Algorithm	405
<b>19</b>	<b>Finale</b>	415
	19.1 Kronecker's Dream	415
	19.2 Van der Waerden's Example	415
	<i>Bibliography</i>	420
	<i>Index</i>	422