CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Table of Contents
More information

Contents

Preface *page* xi
Acknowledgements xiv
1 Numbers 1
1.1 The natural numbers and the integers 3
1.1.1 Well ordering and mathematical induction 3
1.2 Division with remainder 4
1.3 Congruences 5
1.3.1 Repeated squaring – an example 7
1.4 Greatest common divisor 8
1.5 The Euclidean algorithm 9
1.6 The Chinese remainder theorem 14
1.7 Euler's theorem 17
1.8 Prime numbers 19
1.8.1 There are infinitely many prime numbers 20
1.8.2 Unique factorization 22
1.8.3 How to compute $\varphi(n)$ 24
1.9 RSA explained 24
1.9.1 Encryption and decryption exponents 25
1.9.2 Finding astronomical prime numbers 26
1.10 Algorithms for prime factorization 30
1.10.1 The birthday problem 30
1.10.2 Pollard's ρ-algorithm 31
1.10.3 Pollard's $(p-1)$-algorithm 33
1.10.4 The Fermat–Kraitchik algorithm 34
1.11 Quadratic residues 36
1.12 Exercises 41

2 Groups 50
2.1 Definition 50
2.1.1 Groups and congruences 51
2.1.2 The composition table 53
2.1.3 Associativity 54
2.1.4 The first non-abelian group 54
2.1.5 Uniqueness of neutral and inverse elements 55
2.1.6 Multiplication by $g \in G$ is bijective 56
2.1.7 More examples of groups 57
2.2 Subgroups and cosets 60
2.2.1 Subgroups of $\mathbb{Z}$ 61
2.2.2 Cosets 61
2.3 Normal subgroups 64
2.3.1 Quotient groups of the integers 66
2.3.2 The multiplicative group of prime residue classes 66
2.4 Group homomorphisms 68
2.5 The isomorphism theorem 71
2.6 Order of a group element 72
2.7 Cyclic groups 74
2.8 Groups and numbers 76
2.8.1 Euler's theorem 76
2.8.2 Product groups 76
2.8.3 The Chinese remainder theorem 77
2.9 Symmetric and alternating groups 78
2.9.1 Cycles 79
2.9.2 Simple transpositions and "bubble" sort 82
2.9.3 The alternating group 85
2.9.4 Simple groups 86
2.9.5 The 15-puzzle 88
2.10 Actions of groups 92
2.10.1 Conjugacy classes 98
2.10.2 Conjugacy classes in the symmetric group 98
2.10.3 Groups of order p^r 100
2.10.4 The Sylow theorems 101
2.11 Exercises 104
3 Rings 111
3.1 Definition 112
3.1.1 Ideals 115
3.2 Quotient rings 116
3.2.1 Quotient rings of $\mathbb{Z}$ 117

CAMBRIDGE

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Table of Contents
More information

3.2.2 Prime ideals 118
3.2.3 Maximal ideals 118
3.3 Ring homomorphisms 119
3.3.1 The unique ring homomorphism from $\mathbb{Z}$ 120
3.3.2 Freshman's Dream 121
3.4 Fields of fractions 123
3.5 Unique factorization 125
3.5.1 Divisibility and greatest common divisor 126
3.5.2 Irreducible elements 126
3.5.3 Prime elements 127
3.5.4 Euclidean domains 130
3.5.5 Fermat's two-square theorem 132
3.5.6 The Euclidean algorithm strikes again 134
3.5.7 Prime numbers congruent to 1 modulo 4 135
3.5.8 Fermat's last theorem 137
3.6 Exercises 138
4 Polynomials 143
4.1 Polynomial rings 144
4.1.1 Binomial coefficients modulo a prime number 146
4.2 Division of polynomials 147
4.3 Roots of polynomials 150
4.3.1 Differentiation of polynomials 153
4.4 Cyclotomic polynomials 154
4.5 Primitive roots 157
4.5.1 Decimal expansions and primitive roots 159
4.5.2 Primitive roots and public key cryptography 160
4.5.3 Yet another application of cyclotomic polynomials 160
4.6 Ideals in polynomial rings 161
4.6.1 Polynomial rings modulo ideals 164
4.7 Theorema Aureum: the law of quadratic reciprocity 167
4.8 Finite fields 170
4.8.1 Existence of finite fields 172
4.8.2 Uniqueness of finite fields 172
4.8.3 A beautiful identity 173
4.9 Berlekamp's algorithm 176
4.10 Exercises 179
5 Gröbner bases 186
5.1 Polynomials in several variables 187
5.1.1 Term orderings 189

Cambridge University Press
978-0-521-82679-2 - Concrete Abstract Algebra: From Numbers to Grobner Bases
Niels Lauritzen
Table of Contents
More information

5.2 The initial term of a polynomial 193
5.3 The division algorithm 194
5.4 Gröbner bases 196
5.4.1 Hilbert’s basis theorem 198
5.5 Newton revisited 200
5.6 Buchberger’s S-criterion 203
5.6.1 The S-polynomials 204
5.6.2 The S-criterion 208
5.7 Buchberger’s algorithm 208
5.8 The reduced Gröbner basis 212
5.9 Solving equations using Gröbner bases 214
5.10 Exercises 217
Appendix A Relations 223
A.1 Basic definitions and properties 223
A.2 Equivalence relations 224
A.2.1 Construction of the integers $\mathbb{Z}$ 226
A.2.2 Construction of the rational numbers $\mathbb{Q}$ 227
A.3 Partial orderings 228
Appendix B Linear algebra 230
B.1 Linear independence 231
B.2 Dimension 232

References 234
Index 236