

Contents

Preface — V

1	The natural, integral and rational numbers — 1
1.1	Number theory and axiomatic systems — 1
1.2	The natural numbers and induction — 1
1.3	The integers $\mathbb{Z}$ — 10
1.4	The rational numbers $\mathbb{Q}$ — 13
1.5	The absolute value in $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ — 15
2	Division and factorization in the integers — 19
2.1	The Fundamental Theorem of Arithmetic — 19
2.2	The division algorithm and the greatest common divisor — 23
2.3	The Euclidean algorithm — 26
2.4	Least common multiples — 30
2.5	General gcd's and lcm's — 33
3	Modular arithmetic — 39
3.1	The ring of integers modulo n — 39
3.2	Units and the Euler φ -function — 43
3.3	RSA cryptosystem — 46
3.4	The Chinese Remainder Theorem — 47
3.5	Quadratic residues — 54
4	Exceptional numbers — 61
4.1	The Fibonacci numbers — 61
4.1.1	The golden rectangle — 67
4.1.2	Squares in semicircles — 68
4.1.3	Side length of a regular 10-gon — 69
4.1.4	Construction of the golden section α with compass and straightedge from a given $a \in \mathbb{R}$, $a > 0$ — 70
4.2	Perfect numbers and Mersenne numbers — 71
4.3	Fermat numbers — 78
5	Pythagorean triples and sums of squares — 83
5.1	The Pythagorean Theorem — 83
5.2	Classification of the Pythagorean triples — 85
5.3	Sum of squares — 89

6	Polynomials and unique factorization — 95
6.1	Polynomials over a ring — 95
6.2	Divisibility in rings — 98
6.3	The ring of polynomials over a field K — 100
6.3.1	The division algorithm for polynomials — 101
6.3.2	Zeros of polynomials — 103
6.4	Horner-Scheme — 108
6.5	The Euclidean algorithm and greatest common divisor of polynomials over fields — 112
6.5.1	The Euclidean algorithm for $K[x]$ — 114
6.5.2	Unique factorization of polynomials in $K[x]$ — 115
6.5.3	General unique factorization domains — 116
6.6	Polynomial interpolation and the Shamir secret sharing scheme — 117
6.6.1	Secret sharing — 117
6.6.2	Polynomial interpolation over a field K — 117
6.6.3	The Shamir secret sharing scheme — 121
7	Field extensions and splitting fields — 125
7.1	Fields, subfield and characteristic — 125
7.2	Field extensions — 126
7.3	Finite and algebraic field extensions — 131
7.3.1	Finite fields — 134
7.4	Splitting fields — 135
8	Permutations and symmetric polynomials — 141
8.1	Permutations — 141
8.2	Cycle decomposition of a permutation — 144
8.2.1	Conjugate elements in S_n — 147
8.2.2	Marshall Hall's Theorem — 148
8.3	Symmetric polynomials — 151
9	Real numbers — 157
9.1	The real number system — 157
9.2	Decimal representation of real numbers — 168
9.3	Periodic decimal numbers and the rational number — 172
9.4	The uncountability of $\mathbb{R}$ — 173
9.5	Continued fraction representation of real numbers — 175
9.6	Theorem of Dirichlet and Cauchy's Inequality — 176
9.7	p -adic numbers — 178
9.7.1	Normed fields and Cauchy completions — 179
9.7.2	The p -adic fields — 180
9.7.3	The p -adic norm — 183

9.7.4	The construction of $\mathbb{Q}_p$ —	184
9.7.5	Ostrowski's theorem —	185
10	The complex numbers, the Fundamental Theorem of Algebra and polynomial equations —	189
10.1	The field $\mathbb{C}$ of complex numbers —	189
10.2	The complex plane —	193
10.2.1	Geometric interpretation of complex operations —	196
10.2.2	Polar form and Euler's identity —	197
10.2.3	Other constructions of $\mathbb{C}$ —	201
10.2.4	The Gaussian integers —	201
10.3	The Fundamental Theorem of Algebra —	202
10.3.1	First proof of the Fundamental Theorem of Algebra —	204
10.3.2	Second proof of the Fundamental Theorem of Algebra —	207
10.4	Solving polynomial equations in terms of radicals —	209
10.5	Skew field extensions of $\mathbb{C}$ and Frobenius's Theorem —	220
11	Quadratic number fields and Pell's equation —	227
11.1	Algebraic extensions of $\mathbb{Q}$ —	227
11.2	Algebraic and transcendental numbers —	228
11.3	Discriminant and norm —	230
11.4	Algebraic integers —	235
11.4.1	The ring of algebraic integers —	236
11.5	Integral bases —	238
11.6	Quadratic fields and quadratic integers —	240
12	Transcendental numbers and the numbers e and π —	249
12.1	The numbers e and π —	249
12.1.1	Calculation of π —	251
12.2	The irrationality of e and π —	256
12.3	e and π throughout mathematics —	263
12.3.1	The normal distribution —	263
12.3.2	The Gamma Function and Stirling's approximation —	264
12.3.3	The Wallis Product Formula —	266
12.4	Existence of a transcendental number —	270
12.5	The transcendence of e and π —	273
12.6	An amazing property of π and a connection to prime numbers —	282
13	Compass and straightedge constructions and the classical problems —	289
13.1	Historical remarks —	289
13.2	Geometric constructions —	289

13.3	Four classical construction problems — 296
13.3.1	Squaring the circle (problem of Anaxagoras 500–428 BC) — 296
13.3.2	The doubling of the cube or the problem from Delos — 296
13.3.3	The trisection of an angle — 297
13.3.4	Construction of a regular n-gon — 298

14 Euclidean vector spaces — 303

14.1	Length and angle — 303
14.2	Orthogonality and Applications in $\mathbb{R}^2$ and $\mathbb{R}^3$ — 309
14.3	Orthonormalization and closest vector — 317
14.4	Polynomial approximation — 321
14.5	Secret sharing scheme using the closest vector theorem — 323

Bibliography — 327

Index — 329