

Contents

<i>Preface</i>	<i>page</i>	xi
1	Elliptic functions	1
1.1	Values of elliptic functions	1
1.2	The functions $\sigma(z \mathfrak{L})$, $\zeta(z \mathfrak{L})$ and $\wp(z \mathfrak{L})$	3
1.3	Construction of elliptic functions	7
1.4	Algebraic and geometric properties of elliptic functions	9
1.5	Division polynomials	13
1.6	Weierstrass functions	16
	1.6.1 Expansions at zero	18
	1.6.2 p -adic limits	23
1.7	Elliptic resolvents	27
1.8	q -expansions	32
1.9	Dedekind's η function and σ -product formula	35
1.10	The transformation formula of the Dedekind η function	38
2	Modular functions	41
2.1	The modular group	42
2.2	Congruence subgroups	45
2.3	Definition of modular forms	48
2.4	Examples of modular forms and modular functions	50
	2.4.1 The functions g_2, g_3 and Δ	50
	2.4.2 The functions $j, \sqrt[3]{j}, \sqrt[2]{j-12^3}, j_R, \varphi_R$	50
	2.4.3 η -quotients	51
	2.4.4 Weber's τ function	52
	2.4.5 The natural normalisation of the \wp function	53
	2.4.6 Klein's normalisation of the σ function	53
	2.4.7 Transformation of $\tau^{(e)}, p, \varphi$	53

viii	<i>Contents</i>	
2.5	Modular functions for Γ	54
2.5.1	Construction of modular functions for Γ	54
2.5.2	The q -expansion principle	59
2.6	Modular functions for subgroups of Γ	61
2.6.1	The isomorphisms of $\mathbb{C}_U/\mathbb{C}_\Gamma$	61
2.6.2	The extended q -expansion principle	62
2.7	Modular functions for Γ_R	63
2.8	Modular functions for $\Gamma(N)$	69
2.9	The field $\mathbb{Q}(\gamma_2, \gamma_3)$	72
2.10	Lower powers of η -quotients	74
3	Basic facts from number theory	82
3.1	Ideal theory of suborders in a quadratic number field	82
3.1.1	Fractional ideals, integral ideals, proper ideals, regular ideals	82
3.1.2	Ideal groups	86
3.1.3	Primitive matrices and bases of ideals	94
3.1.4	Integral ideals that are not regular	98
3.2	Density theorems	100
3.3	Class field theory	103
4	Factorisation of singular values	111
4.1	Singular values	111
4.2	Factorisation of $\varphi_A(\alpha)$	114
4.3	Factorisation of $\varphi(\xi \mid \mathfrak{L})$	118
4.4	A result of Dorman, Gross and Zagier	121
5	The Reciprocity Law	122
5.1	The Reciprocity Law of Weber, Hasse, Söhngen, Shimura	122
5.2	Applications of the Reciprocity Law	128
6	Generation of ring class fields and ray class fields	138
6.1	Generation of ring class fields by singular values of j	138
6.2	Generation of ray class fields by τ and j	141
6.3	The singular values of γ_2 and γ_3	144
6.4	The singular values of Schläfli's functions	148
6.5	Heegner's solution of the class number one problem	151
6.6	Generation of ring class fields by η -quotients	154
6.7	Double η -quotients in the ramified case	165
6.8	Generation of ray class fields by $\varphi(z \mid \frac{\omega_1}{\omega_2})$	169
6.9	Generalised principal ideal theorem	183

<i>Contents</i>		ix
7	Integral basis in ray class fields	190
	7.1 A normalisation of the Weierstrass \wp function	191
	7.2 The discriminant of $\mathcal{P}(\delta)$	193
	7.3 The denominator of $\mathcal{P}(\delta)$	197
	7.4 Construction of relative integral basis	201
	7.4.1 Analogy to cyclotomic fields	203
	7.5 Relative integral power basis	205
	7.6 Bley's generalisation for $K_{t,f}/\Omega_t$ with $t > 1$	210
8	Galois module structure	213
	8.1 Torsion points and good reduction	214
	8.2 Kummer theory of E	215
	8.3 Integral objects	217
	8.4 Global construction of $\tilde{\mathfrak{D}}_P$ and \mathfrak{A} as \mathfrak{D}_L -algebras	220
	8.5 Construction of a generating element for $\tilde{\mathfrak{D}}_P$ over \mathfrak{A}	221
	8.6 Galois module structure of ray class fields	224
	8.7 Models of elliptic curves	228
	8.7.1 The Weierstrass model	228
	8.7.2 The Fueter model	229
	8.7.3 The Deuring model	231
	8.7.4 Singular values of the Weierstrass, Fueter and Deuring functions	232
	8.7.5 Singular values of Weierstrass functions	234
	8.8 Proofs of Theorems 8.3.1 and 8.5.1	238
	8.9 Proofs of Theorems 8.4.1, 8.4.2 and 8.5.2	245
	8.10 Proofs of Theorems 8.9.2 and 8.6.2	250
	8.11 Analogy to the cyclotomic case	253
	8.12 Generalisation to ring classes by Bettner and Bley	256
9	Berwick's congruences	261
	9.1 Bettner's results	261
	9.2 Method of proof	263
10	Cryptographically relevant elliptic curves	266
	10.1 Reduction of the Weierstrass model	266
	10.2 Computation of $j(\mathfrak{D})$ modulo \mathfrak{P}	273
	10.2.1 Schläfli–Weber functions	275
	10.2.2 Double η -quotients	276
	10.2.3 Application of η -quotients in the ramified case	278
	10.3 Reduction of the Fueter and Deuring models	282
	10.3.1 Reduction of the Fueter model	282
	10.3.2 Reduction of the Deuring model	285

x	<i>Contents</i>	
11	The class number formulae of Curt Meyer	288
11.1	L -Functions of ring class characters	289
11.2	L -function s of ray class characters χ with $\mathfrak{f}_\chi \neq (1)$.	291
11.3	Class number formulae	293
12	Arithmetic interpretation of class number formulae	295
12.1	Group-theoretical lemmas for the case $L \supseteq K$	295
12.2	Applications of Theorems 12.1.1, 12.1.2	301
12.2.1	Application of Theorem 12.1.1	302
12.2.2	Application of Theorem 12.1.2	303
12.3	Class number formulae for $\Omega \supseteq L \supseteq K$	304
12.4	Class number formulae for $K_{\mathfrak{f}} \supseteq L \supseteq K$	309
12.4.1	Application of the formulae from 12.4	317
12.5	Group-theoretical lemmas for $M \not\supseteq K$	323
12.6	The Galois group of MK/K	336
12.7	Class number formulae for $\Omega \supset M \not\supseteq K$	338
12.8	Class number formulae for $K_{\mathfrak{f}} \supset M \not\supseteq K$	341
12.8.1	Applications of the class number formulae in 12.8	346
	<i>References</i>	351
	<i>Index of Notation</i>	356
	<i>Index</i>	360