Complex Multiplication

REINHARD SCHERTZ
Universität Augsburg
Contents

Preface

1 Elliptic functions
1.1 Values of elliptic functions 1
1.2 The functions \( \sigma(z|\mathcal{L}) \), \( \zeta(z|\mathcal{L}) \) and \( \wp(z|\mathcal{L}) \) 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 \( \eta \) function and \( \sigma \)-product formula 35
1.10 The transformation formula of the Dedekind \( \eta \) function 38

2 Modular functions
2.1 The modular group 41
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 \( \Delta \) 50
2.4.2 The functions \( j, \sqrt[3]{j}, \sqrt[3]{j - 123}, j_R, \varphi_R \) 50
2.4.3 \( \eta \)-quotients 51
2.4.4 Weber's \( \tau \) function 52
2.4.5 The natural normalisation of the \( \varphi \) function 53
2.4.6 Klein's normalisation of the \( \sigma \) function 53
2.4.7 Transformation of \( \tau^{(\infty)}, p, \varphi \) 53
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5</td>
<td>Modular functions for $\Gamma$</td>
<td>54</td>
</tr>
<tr>
<td>2.5.1</td>
<td>Construction of modular functions for $\Gamma$</td>
<td>54</td>
</tr>
<tr>
<td>2.5.2</td>
<td>The $q$-expansion principle</td>
<td>59</td>
</tr>
<tr>
<td>2.6</td>
<td>Modular functions for subgroups of $\Gamma$</td>
<td>61</td>
</tr>
<tr>
<td>2.6.1</td>
<td>The isomorphisms of $\mathbb{C}<em>U/\mathbb{C}</em>\Gamma$</td>
<td>61</td>
</tr>
<tr>
<td>2.6.2</td>
<td>The extended $q$-expansion principle</td>
<td>62</td>
</tr>
<tr>
<td>2.7</td>
<td>Modular functions for $\Gamma_R$</td>
<td>63</td>
</tr>
<tr>
<td>2.8</td>
<td>Modular functions for $\Gamma(N)$</td>
<td>69</td>
</tr>
<tr>
<td>2.9</td>
<td>The field $\mathbb{Q}(\gamma_2, \gamma_3)$</td>
<td>72</td>
</tr>
<tr>
<td>2.10</td>
<td>Lower powers of $\eta$-quotients</td>
<td>74</td>
</tr>
<tr>
<td>3</td>
<td><strong>Basic facts from number theory</strong></td>
<td>82</td>
</tr>
<tr>
<td>3.1</td>
<td>Ideal theory of suborders in a quadratic number field</td>
<td>82</td>
</tr>
<tr>
<td>3.1.1</td>
<td>Fractional ideals, integral ideals, proper ideals, regular ideals</td>
<td>82</td>
</tr>
<tr>
<td>3.1.2</td>
<td>Ideal groups</td>
<td>86</td>
</tr>
<tr>
<td>3.1.3</td>
<td>Primitive matrices and bases of ideals</td>
<td>94</td>
</tr>
<tr>
<td>3.1.4</td>
<td>Integral ideals that are not regular</td>
<td>98</td>
</tr>
<tr>
<td>3.2</td>
<td>Density theorems</td>
<td>100</td>
</tr>
<tr>
<td>3.3</td>
<td>Class field theory</td>
<td>103</td>
</tr>
<tr>
<td>4</td>
<td><strong>Factorisation of singular values</strong></td>
<td>111</td>
</tr>
<tr>
<td>4.1</td>
<td>Singular values</td>
<td>111</td>
</tr>
<tr>
<td>4.2</td>
<td>Factorisation of $\varphi_A(\alpha)$</td>
<td>114</td>
</tr>
<tr>
<td>4.3</td>
<td>Factorisation of $\varphi(\xi \mid \mathcal{L})$</td>
<td>118</td>
</tr>
<tr>
<td>4.4</td>
<td>A result of Dorman, Gross and Zagier</td>
<td>121</td>
</tr>
<tr>
<td>5</td>
<td><strong>The Reciprocity Law</strong></td>
<td>122</td>
</tr>
<tr>
<td>5.1</td>
<td>The Reciprocity Law of Weber, Hasse, Söhngen, Shimura</td>
<td>122</td>
</tr>
<tr>
<td>5.2</td>
<td>Applications of the Reciprocity Law</td>
<td>128</td>
</tr>
<tr>
<td>6</td>
<td><strong>Generation of ring class fields and ray class fields</strong></td>
<td>138</td>
</tr>
<tr>
<td>6.1</td>
<td>Generation of ring class fields by singular values of $j$</td>
<td>138</td>
</tr>
<tr>
<td>6.2</td>
<td>Generation of ray class fields by $\tau$ and $j$</td>
<td>141</td>
</tr>
<tr>
<td>6.3</td>
<td>The singular values of $\gamma_2$ and $\gamma_3$</td>
<td>144</td>
</tr>
<tr>
<td>6.4</td>
<td>The singular values of Schläfli's functions</td>
<td>148</td>
</tr>
<tr>
<td>6.5</td>
<td>Heegner's solution of the class number one problem</td>
<td>151</td>
</tr>
<tr>
<td>6.6</td>
<td>Generation of ring class fields by $\eta$-quotients</td>
<td>154</td>
</tr>
<tr>
<td>6.7</td>
<td>Double $\eta$-quotients in the ramified case</td>
<td>165</td>
</tr>
<tr>
<td>6.8</td>
<td>Generation of ray class fields by $\varphi(z \mid \omega_1 \omega_2)$</td>
<td>169</td>
</tr>
<tr>
<td>6.9</td>
<td>Generalised principal ideal theorem</td>
<td>183</td>
</tr>
</tbody>
</table>
# Contents

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 $\mathcal{O}_P$ and $\mathfrak{A}$ as $\mathcal{O}_L$-algebras 220  
8.5 Construction of a generating element for $\mathcal{O}_P$ 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 $j(\mathcal{O})$ modulo $\mathfrak{P}$ 273  
10.2.1 Schl"afli-Weber functions 275  
10.2.2 Double $\eta$-quotients 276  
10.2.3 Application of $\eta$-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
## Contents

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 fχ ≠ (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 ⊇ 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 Ω ⊇ L ⊇ K 304
  12.4 Class number formulae for Kf ⊇ L ⊇ K 309
    12.4.1 Application of the formulae from 12.4 317
  12.5 Group-theoretical lemmas for M ⊄ K 323
  12.6 The Galois group of MK/K 336
  12.7 Class number formulae for Ω ⊇ M ⊄ K 338
  12.8 Class number formulae for Kf ⊇ M ⊄ K 341
    12.8.1 Applications of the class number formulae in 12.8 346

References 351
Index of Notation 356
Index 360