Journal de Théorie des Nombres
de Bordeaux **14** (2002), 325–343

Weber's class invariants revisited

par Reinhard SCHERTZ

Résumé. Soit K un corps quadratique imaginaire de discriminant d et $\mathfrak{O}_t$ l'ordre à conducteur $t \in \mathbb{N}$ dans K. L'invariant modulaire $j(\mathfrak{O}_t)$ est un nombre algébrique qui génère sur K le corps de classes d'anneau modulo t. Les coefficients du polynôme minimal de $j(\mathfrak{O}_t)$ étant assez large, Weber considère dans [We] les fonctions $f, f_1, f_2, \gamma_2, \gamma_3$ définies plus bas, par lesquelles il construit des générateurs plus simples pour les corps de classes d'anneau.

Plus tard les valeurs singulières de ces fonctions ont joué un rôle central dans la solution de Heegner [He] du célèbre problème de déterminer tous les corps quadratiques imaginaires dont le nombre de classes est égal à 1 [He,Me2,St]. Actuellement on s'en sert en cryptographie pour trouver des courbes elliptiques sur des corps finis avec certaines jolies propriétés.

Le but de cet article est i) d'énoncer certains résultats déjà connus de [We,Bi,Me2,Sch1] cf. Théorèmes 1,2 et 3, concernant les valeurs singulières des fonctions $f, f_1, f_2, \gamma_2, \gamma_3$, et ii) de développer une preuve courte de ces résultats.

Cette méthode s'applique aussi à d'autres fonctions cf. Théorème 4 et le tableau précédent celui-ci. Les preuves des théorèmes 1 à 4 sont données en fin d'article.

Ces démonstrations résultent de la loi de réciprocité de Shimura (cf. théorème 5, ainsi que théorèmes 6 et 7), du calcul de la racine 24-ième de l'unité de $\eta = \sqrt[24]{\Delta}$ lors des transformations unimodulaires (cf. proposition 2, tirée de [Me1] formules (4.21) à (4.23) p.162), et donnent aussi via la proposition 3 des formules explicites pour les conjugués des valeurs singulières, qui sont très utiles pour des calculs numériques.

Certains de ceux-ci sont donnés comme exemples juste avant la Bibliograpie.

Abstract. Let K be a quadratic imaginary number field of discriminant d. For $t \in \mathbb{N}$ let $\mathfrak{O}_t$ denote the order of conductor t in K and $j(\mathfrak{O}_t)$ its modular invariant which is known to generate the ring class field modulo t over K. The coefficients of the minimal equation of $j(\mathfrak{O}_t)$ being quite large Weber considered in [We]

Manuscrit reçu le 20 juillet 2000.

the functions $f, f_1, f_2, \gamma_2, \gamma_3$ defined below and thereby obtained simpler generators of the ring class fields.

Later on the singular values of these functions played a crucial role in Heegner's solution [He] of the class number one problem for quadratic imaginary number fields [He,Me2,St]. Actually these numbers are used in cryptography to find elliptic curves over finite fields with nice properties.

It is the aim of this paper i) to enunciate some known results of [We,Bi,Me2,Sch1] cf. Theorem 1, 2 and 3, concerning singular values of the functions $f, f_1, f_2, \gamma_2, \gamma_3$, and ii) to give a short and easy proof of these results.

That method also applies to other functions, such as those in the table preceding Theorem 4. The proofs of Theorems 1 to 4 are given at the end of our article.

Our proofs rely on the reciprocity law of Shimura (cf. Theorem 5, and also Theorem 6 and 7), and on the knowledge of the 24-th root of unity that acquires $\eta = \sqrt[24]{\Delta}$ by unimodular substitution (cf. Proposition 2, and [Me1] p.162); they also give via Proposition 3 explicit formulas for the conjugates of the singular values (of the above functions), that are quite useful for numerical calculations.

Examples of such calculations are to be found immediately before the References.

Weber's Class Invariants

The Schläfli functions Weber used in [We] are defined by

$$f(z) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{z+1}{2}\right)}{\eta(z)}, \; f_1(z) = \frac{\eta\left(\frac{z}{2}\right)}{\eta(z)}, \; f_2(z) = \sqrt{2}\frac{\eta(2z)}{\eta(z)}, \; \Im(z) > 0$$

where

$$\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n), \quad q = e^{2\pi i z},$$

denotes the Dedekind η-function. They are related by the identity

$$f(z) f_1(z) f_2(z) = \sqrt{2}.$$

Further Weber considers the functions

$$\gamma_2(z) = \sqrt[3]{j(z)} := 12 \frac{g_2(z)}{(2\pi)^4 \eta(z)^8},$$

$$\gamma_3(z) = \sqrt{j(z) - 12^3} := 6^3 \frac{g_3(z)}{(2\pi)^6 \eta(z)^{12}}.$$

Herein j is the modular invariant and g_2, g_3 are the Eisenstein series

$$g_2(z) = 60 \sum_{\substack{w \in L_z \\ w \neq 0}} \frac{1}{w^4}, \quad g_3(z) = 140 \sum_{\substack{w \in L_z \\ w \neq 0}} \frac{1}{w^6}, \quad L_z = \mathbb{Z}z + \mathbb{Z}.$$

They have the $q-$expansions

$$g_2(\omega) = \frac{(2\pi i)^4}{2^2 3}\left[1 + 240 T_3\right], g_3(\omega) \qquad = \frac{(2\pi i)^6}{2^3 3^3}\left[-1 + 504 T_5\right]$$

with

$$T_k := \sum_{n=1}^{\infty} \sigma_k(n) q^n, \quad \sigma_k(n) := \sum_{0<d|n} d^k.$$

The Schläfli functions f, f_2 and the modular invariant j are related by the formulas

$$\gamma_2 = \frac{f^{24} - 16}{f^8} = \frac{f_1^{24} + 16}{f_1^8} = \frac{f_2^{24} + 16}{f_2^8}.$$

Some basic results (cf. [De] or [La]). In what follows let K be a quadratic imaginary number field of discriminant d and for some integer t we let $\mathfrak{O}_t$ denote the order of conductor t in K. Using the notation $[\omega_1, \omega_2] := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ the order $\mathfrak{O}_t$ is explicitly given by

$$\mathfrak{O}_t = \left[t\frac{d + \sqrt{d}}{2}, 1\right].$$

A $\mathbb{Z}$-module $\mathfrak{a}$ of rank 2 in K is called a proper ideal of $\mathfrak{O}_t$, if

$$\mathfrak{O}_t = \{\xi \in K \mid \xi\mathfrak{a} \subseteq \mathfrak{a}\}.$$

The set $\mathfrak{I}_t$ of proper $\mathfrak{O}_t$-ideals is a group under multiplication and the quotient

$$\mathfrak{R}_t := \mathfrak{I}_t / \mathfrak{H}_t$$

is called the ideal class group of $\mathfrak{O}_t$. For

$$[\alpha_1, \alpha_2] = \mathfrak{a} \in \mathfrak{k} \in \mathfrak{R}_t \quad \text{with } \Im(\frac{\alpha_1}{\alpha_2}) > 0$$

we set

$$j(\mathfrak{k}) := j(\mathfrak{a}) := j(\frac{\alpha_1}{\alpha_2})$$

which is well defined, because j is invariant under all unimodular transformations of $\mathbb{H}$. $j(\mathfrak{k})$ is called the **modular invariant of** $\mathfrak{k}$ or the **modular invariant of** $\mathfrak{a}$. For any class $\mathfrak{k} \in \mathfrak{R}_t$ the value $j(\mathfrak{k})$ is an algebraic number that generates the ring class field modulo t over K

$$K(j(\mathfrak{k})) = \Omega_t.$$

Ω_t is the abelian extension of K belonging to the subgroup $\mathfrak{U}_t$ of the ideal group of K that is generated by all ideals of the form (λ), λ integral, prime to t and $\lambda \equiv r \bmod t$ for some $r \in \mathbb{Z}$. For $\mathfrak{k}, \mathfrak{k}' \in \mathfrak{R}_t$ we have

$$j(\mathfrak{k}) \neq j(\mathfrak{k}') \text{ if } \mathfrak{k} \neq \mathfrak{k}'$$

and the values $j(\mathfrak{k}), \mathfrak{k} \in \mathfrak{R}_t$, form a complete system of conjugate numbers over K. It is even a complete system of conjugates over $\mathbb{Q}$. In particular this implies

$$\mathbb{Q}(j(\mathfrak{e})) = \mathbb{R} \cap \Omega_t$$

and

$$[\mathbb{Q}(j(\mathfrak{k})) : \mathbb{Q}] = [K(j(\mathfrak{k})) : K] = |\mathfrak{R}_t|.$$

We have the explicit formula

$$h_t := |\mathfrak{R}_t| = h_K \frac{t}{e} \prod_{p|t} \left(1 - \frac{1}{p}\left(\frac{d}{p}\right)\right),$$

where the product is over all primes p dividing t, and $\left(\frac{d}{p}\right)$ is the Legendre symbol (with d the discriminant of K). Here $h_K := |\mathfrak{R}_1|$ is the class number of K, and e the index of the group of all roots of unity in K, that are congruent to 1 mod t, in the group of all roots of unity in K.

More precisely there is an isomorphism

$$\sigma : \mathfrak{R}_t \to G(\Omega_t/K)$$

where $G(\Omega_t/K)$ denotes the Galois group of Ω_t/K such that the action on the j-invariants is

$$j(\mathfrak{k})^{\sigma(\mathfrak{h})} = j(\mathfrak{k}\mathfrak{h}^{-1}) \text{ for all } \mathfrak{k}, \mathfrak{h} \in \mathfrak{R}_t.$$

This isomorphism is in close connection to the description of $G(\Omega_t/K)$ given by class field theory. Let $\mathfrak{c}$ be an integral ideal of $\mathfrak{O}_1$, prime to t. Then $\mathfrak{c}_t := \mathfrak{c} \cap \mathfrak{O}_t$ is a proper $\mathfrak{O}_t$-ideal and

$$\sigma(\mathfrak{c}) = \sigma(\mathfrak{c}_t),$$

where in abuse of notation $\sigma(\mathfrak{c}) = \sigma(\mathfrak{c}\mathfrak{U}_t)$ denotes the Frobenius map associated to $\mathfrak{c}\mathfrak{U}_t$ by class field theory and on the right side $\sigma(\mathfrak{c}_t) = \sigma(\mathfrak{c}_t\mathfrak{H}_t)$.

In what follows $\mathbb{H}$ will denote the upper half plane. A quadratic imaginary number $\alpha \in \mathbb{H} \cap K$ is the root of a quadratic equation $AX^2 + BX + C = 0$ which is uniquely determined by α if normalized by

$$A, B, C \in \mathbb{Z}, \quad \gcd(A, B, C) = 1, A > 0.$$

We call such an equation **primitive**. The discriminant

$$D(\alpha) = B^2 - 4AC$$

is related to the discriminant d of K by

$$D(\alpha) = t^2 d$$

for some $t \in \mathbb{N}$. This implies $[\alpha, 1] \in \mathfrak{I}_t$, and, conversely, if $[\alpha_1, \alpha_2]$ is in $\mathfrak{I}_t$ then the quotient $\alpha = \frac{\alpha_1}{\alpha_2}$ is the root of some primitive equation of discriminant $t^2 d$. So for $\alpha \in \mathbb{H}$ with this property the field $\mathbb{Q}(j(\alpha))$ is conjugate to the maximal real subfield of Ω_t.

If g is one of the functions $f, f_1, f_2, \gamma_2, \gamma_3$ the above formulas tell us that

$$\mathbb{Q}(g(\alpha)) \supseteq \mathbb{Q}(j(\alpha)).$$

And following Weber we call $g(\alpha)$ a **class invariant** if

$$\mathbb{Q}(g(\alpha)) = \mathbb{Q}(j(\alpha)).$$

To describe the conjugates of $g(\alpha)$ we make the following definition.

Definition. *Let N be a natural number and $\alpha_1, \dots, \alpha_{h_t} \in \mathbb{H}$ such that*

$$[\alpha_1, 1], \dots, [\alpha_{h_t}, 1]$$

is a system of representatives for $\mathfrak{R}_t$ and that further the primitive equations $A_i X^2 + B_i X + C_i = 0$ of the α_i satisfy

$$\gcd(A_i, N) = 1 \text{ and } B_i \equiv B_j \bmod 2N,\ 1 \le i, j \le h_t.$$

Then we call $\alpha_1, \dots, \alpha_{h_t}$ a N**-system mod** t.

As we shall prove later in Proposition 3, there always exists a N-system mod t for every natural number N.

The following Theorem contains Weber's results on f and f_1 and also includes the assertions conjectured by Weber, and proved in the meantime in [Bi,Me2,Sch1].

Theorem 1. *Let $\alpha \in \mathbb{H}$ be the root of the primitive equation*

$$AX^2 + BX + C = 0 \quad \text{with } 2 \nmid A,\ B \equiv 0 \bmod 32$$

of discriminant $D(\alpha) = B^2 - 4AC = -4m = t^2 d$.

Then the following numbers $g(\alpha)$ are class invariants:

$$\left(\left(\frac{2}{A}\right)\frac{1}{\sqrt{2}} f(\alpha)^2\right)^3, \text{ if } m \equiv 1 \bmod 8,$$

$$f(\alpha)^3, \text{ if } m \equiv 3 \bmod 8,$$

$$\left(\frac{1}{2} f(\alpha)^4\right)^3, \text{ if } m \equiv 5 \bmod 8,$$

$$\left(\left(\frac{2}{A}\right)\frac{1}{\sqrt{2}} f(\alpha)\right)^3, \text{ if } m \equiv 7 \bmod 8,$$

$$\left(\left(\frac{2}{A}\right)\frac{1}{\sqrt{2}} f_1(\alpha)^2\right)^3, \text{ if } m \equiv 2 \bmod 4,$$

$$\left(\left(\frac{2}{A}\right)\frac{1}{2\sqrt{2}} f_1(\alpha)^4\right)^3, \text{ if } m \equiv 4 \bmod 8.$$

Herein the factor $\left(\frac{2}{A}\right)$ *denotes the Legendre symbol which is necessary for the following to hold.*
If $\alpha = \alpha_1, \ldots, \alpha_{h_t}$ *is a 16-system mod* t *the above singular values* $g(\alpha_i)$ *form a complete set of conjugates over* $\mathbb{Q}$*. Thus the minimal equation over* $\mathbb{Q}$ *is given by*

$$\prod_i (X - g(\alpha_i))$$

and has coefficients in $\mathbb{Z}$*, because from* [De] *we know that* $g(\alpha)$ *is integral.*

For discriminants not divisible by 3 the result of Theorem 1 can be improved using the above relation between f and γ_2 together with the following Theorem. It then turns out that the assertions of Theorem 1 even hold without the outer exponent 3 if the primitive equation of α also satisfies the conditions $3 \nmid A$ and $3|B$. The conjugates are then described by a $3 \cdot 16$-system modulo t. Indeed, we have for γ_2:

Theorem 2. *Let* $\alpha \in \mathbb{H}$ *be the root of the primitive equation*

$$AX^2 + BX + C = 0 \quad \text{with } 3 \nmid A,\ B \equiv 0 \ mod\ 3$$

of discriminant $D(\alpha) = B^2 - 4AC = t^2 d$.
Then

$$\mathbb{Q}(\gamma_2(\alpha)) = \begin{cases} \mathbb{Q}(j(\alpha)) & \text{if } 3 \nmid D(\alpha), \\ \mathbb{Q}(j(3\alpha)) & \text{if } 3|D(\alpha). \end{cases}$$

Herein $\mathbb{Q}(j(3\alpha))$ *is conjugate to the maximal real subfield of* Ω_{3t} *which is of degree 3 over* $\mathbb{Q}(j(\alpha))$ *when* $3|D(\alpha)$ *and* $D(\alpha) \neq -3$.
Moreover, in the case $3 \nmid t^2 d$ *, if* $\alpha = \alpha_1, \ldots, \alpha_{h_t}$ *is a 3-system mod* t*, then the singular values* $\gamma_2(\alpha_i)$ *form a complete set of conjugates over* $\mathbb{Q}$*. Thus the minimal equation over* $\mathbb{Q}$ *is given by*

$$\prod_i (X - \gamma_2(\alpha_i)).$$

and has coefficients in $\mathbb{Z}$*.*

A similar result holds for γ_3:

Theorem 3. *Let* $\alpha \in \mathbb{H}$ *be the root of the primitive equation*

$$AX^2 + BX + C = 0 \quad \text{with } 2 \nmid A$$

of discriminant $D(\alpha) = B^2 - 4AC = t^2 d$ *and we assume*

$$B \equiv \begin{cases} 0 \ mod\ 4 & \text{if } 2|D(\alpha), \\ 1 \ mod\ 4 & \text{if } 2 \nmid D(\alpha). \end{cases}$$

Then

$$\mathbb{Q}(\sqrt{d}\gamma_3(\alpha)) = \mathbb{Q}(j(\alpha)) \text{ if } 2 \nmid D(\alpha),$$
$$\mathbb{Q}(\gamma_3(\alpha)) = \mathbb{Q}(j(2\alpha)) \text{ if } 2|D(\alpha).$$

Herein $\mathbb{Q}(j(2\alpha))$ is conjugate to the maximal real subfield of Ω_{2t} which is of degree 2 over $\mathbb{Q}(j(\alpha))$ when $2|D(\alpha)$, $D(\alpha) \neq -4$.
Moreover, in the case $2 \nmid t^2 d$, if $\alpha = \alpha_1, \ldots, \alpha_{h_t}$ is a 2-system mod t, the above singular values $\gamma_3(\alpha_i)$ form a complete set of conjugates over K. Thus the minimal equation over K is given by

$$\prod_i (X - \gamma_3(\alpha_i))$$

and has coefficients in $\mathfrak{O}_1$.

The method of proof described in the next section also applies to other functions $g(\omega)$, as for example

Table 1

$$\left(\frac{\eta(\frac{\omega}{N})}{\eta(\omega)}\right)^8 \gamma_2(\omega)^{N-1}, \quad \text{if } 3 \nmid N,$$
$$\left(\frac{\eta(\frac{\omega}{N})}{\eta(\omega)}\right)^6 \gamma_3(\omega)^{\frac{N-1}{2}}, \quad \text{if } 2 \nmid N,$$
$$\left(\frac{\eta(\frac{\omega}{N})}{\eta(\omega)}\right)^m, \; m = \gcd(3, N), \quad \text{if } N = s^2, \; s \in \mathbb{N} \text{ and } 2 \nmid N,$$
$$\left(\frac{\eta(\frac{\omega}{p})\eta(\frac{\omega}{q})}{\eta(\frac{\omega}{pq})\eta(\omega)}\right) (\gamma_2(\omega)\gamma_3(\omega))^{\frac{p-1}{2}\frac{q-1}{2}}, \quad \text{if } N = pq, \; p, q \in \mathbb{N}, \; \gcd(6, N) = 1.$$

From [Sch4], Theorem 5, we know that the last function without the γ_2- and γ_3-factors is very useful for the numerical construction of ring class fields. They lead to generating equations for all ring class fields, whereas the Schläfli functions only apply to the cases when $t^2 d$ is even. Other useful functions for the construction of ring class fields have been defined in [Mo].

In fact, by Proposition 2 below, it is easy to show that the functions (of the above Table 1) all do satisfy the hypothesis of the following Theorem. It refers to the field F_N of modular functions of level N, $N \in \mathbb{N}$, whose q-expansion at every cusp has coefficients in the N-th cyclotomic field.

Theorem 4. *Let $g \in F_N$. We assume $g(z)$ and $g(\frac{-1}{z})$ to have a rational q-expansion and to be invariant under all unimodular transformations $M \equiv \binom{*\ 0}{*\ *}$ mod N. Let $\alpha \in \mathbb{H}$ be the root of a primitive equation $AX^2 + BX + C = 0$ of discriminant $B^2 - 4AC = t^2 d$ with $\gcd(A, N) = 1$ and $N|C$.*

Then, if $g(\alpha) \neq \infty$, *we have*

$$g(\alpha) \in \Omega_t.$$

Moreover, if $\alpha = \alpha_1, \ldots, \alpha_{h_t}$ *is a* N*-system mod* t, *then the numbers* $g(\alpha_i)$ *run through the images of* $g(\alpha)$ *under the different automorphisms of* Ω_t/K.

Proofs

First we state Shimura's Theorem (see [Sh,La]). The extension $F_N/\mathbb{Q}(j)$ is Galois and there is a natural isomorphism between

$$\mathrm{Gal}(F_N/\mathbb{Q}(j)) \quad \text{and} \quad \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$$

via the following action of integral 2×2 matrices B over $\mathbb{Z}$ having determinant prime to N on functions $g \in F_N$:

$$[g \circ B](z) = g(B(z)) \text{ for } B \in SL_2(\mathbb{Z}),$$

$$[g \circ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}]$$

with b prime to N is obtained from g by applying the isomorphism $(\zeta_N \mapsto \zeta_N^b)$ of the N-th cyclotomic field to the coefficients of the q-expansion of g. An arbitrary integral matrix B of determinant prime to N has a decomposition of the form

$$B \equiv M_1 \left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right) M_2 \bmod N$$

with b prime to N and unimodular matrices M_1, M_2. The action of B on g is then given according to the above rules by

$$g \circ B = \Big[[g \circ M_1] \circ \left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right)\Big] \circ M_2.$$

We recall that for an integral ideal $\mathfrak{b}$ of $\mathfrak{O}_1$ prime to t the intersection $\mathfrak{b}_t := \mathfrak{b} \cap \mathfrak{O}_t$ is a proper $\mathfrak{O}_t$-ideal. We can now state the

Theorem 5 (Reciprocity law of Shimura). *Let* g *be in* F_N *and* $\mathfrak{a} \in \mathfrak{I}_t$ *with* $\mathbb{Z}$*-basis* α_1, α_2 *and* $\alpha = \frac{\alpha_1}{\alpha_2} \in \mathbb{H}$, $g(\alpha) \neq \infty$. *Let* $\mathfrak{b}$ *be an integral ideal of* $\mathfrak{O}_1$ *of norm* b *prime to* tN *and let* B *be an integral matrix of determinant* b *such that*

$$B\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \text{ is a basis of } \mathfrak{a}\overline{\mathfrak{b}}_t.$$

Then

1) $g(\alpha)$ *is in* K_{tN}, *the ray class field modulo* tN *over* K,
2) *the action of the Frobenius map* $\sigma(\mathfrak{b})$ *belonging to* $\mathfrak{b}$ *is given by*

$$g(\alpha)^{\sigma(\mathfrak{b})} = [g \circ bB^{-1}](B(\alpha)).$$

For many functions occurring in complex multiplication the singular value in Theorem 5 in fact is contained in a much smaller field. We observe that by class field theory K_{tN} contains Ω_t and prove

Theorem 6. *Let $g \in F_N$ have a q-expansion with rational coefficients and we assume that $g \circ M = g$ for all unimodular matrices $M \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)$ mod N and let α be as in Theorem 5 with $g(\alpha) \neq \infty$.*

Then $g(\alpha) \in \Omega_{Nt}$.

Proof. The Galois group of the extension K_{tN}/Ω_t (i.e ray class/ring class field modulo tN) is the set of Frobenius maps $\sigma(r)$ belonging to integral ideals $\mathfrak{b} = (r)$ generated by natural numbers r prime to tN. The matrix B in Theorem 5 is then $B = \left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$ and one can find a unimodular matrix M satisfying

$$r^2 B^{-1} \equiv \begin{pmatrix} 1 & 0 \\ 0 & r^2 \end{pmatrix} M \bmod N,$$

$$\text{and } M \equiv \begin{pmatrix} r & 0 \\ 0 & r' \end{pmatrix} \bmod N$$

with a natural number r', $rr' \equiv 1 \bmod N$. Theorem 5 now implies $g(\alpha)^{\sigma(r)} = g(\alpha)$. Hence $g(\alpha) \in \Omega_{tN}$. □

For the computation of the conjugates of the numbers $g(\alpha)$ in Theorem 6 we derive from the reciprocity law

Theorem 7. *Let $\alpha_1, \ldots, \alpha_{h_t} \in \mathbb{H}$ be a N-system modulo t with primitive equations $A_i X^2 + B_i X + C_i = 0$.*
For $g \in F_N$ we set

$$g_i := g \circ \begin{pmatrix} A_i & 0 \\ 0 & 1 \end{pmatrix},$$

and we assume $g(A_1\alpha_1) \neq \infty$.

Then

$$g_i(\alpha_i) \in K_{tN}, \quad i = 1, \ldots, h_t,$$

and there exist automorphisms $\sigma_1, \ldots, \sigma_{h_t}$ of K_{tN}/K with

$$g_1(\alpha_1)^{\sigma_1^{-1}\sigma_i} = g_i(\alpha_i), \quad i = 1, \ldots, h_t,$$

such that the restrictions of the σ_i on Ω_t are

$$\sigma_i | \Omega_t = \sigma([\alpha_i, 1]^{-1})$$

which constitute the different automorphisms of Ω_t/K. In particular, if $g_1(\alpha_1) \in \Omega_t$, then

$$\prod_{i=1}^{h_t} (X - g_i(\alpha_i)) \in K[X].$$

Proof. By Proposition 3 which will be proved later, there exist unimodular transformations $M_i \in \Gamma(N)$, so that the $\alpha_i' := M_i(\alpha_i)$ have primitive equations

$$A_i' X^2 + B_i' X + C_i' = 0$$

satisfying

$$\gcd(A_i', tN) = 1, A_i' > 0 \text{ and } B_i' \equiv B_i \bmod N.$$

As $g(\alpha_i) = g(\alpha_i')$ and $\sigma([\alpha_i', 1]) = \sigma([\alpha_i, 1])$ it suffices to consider the case when the A_i are prime to tN. (Note that $g(A_1'\alpha_1') = g(A_1\alpha_1) \neq \infty$ because $A_1'\alpha_i' \equiv A_1\alpha_1 \bmod N\mathbb{Z}$.) Then the proper $\mathfrak{O}_t$-ideals

$$\mathfrak{a}_i := \overline{[A_i\alpha_i, A_i]}$$

are contained in $\mathfrak{O}_t$ and prime to tN and so for

$$\mathfrak{c}_i := \mathfrak{O}_1\mathfrak{a}_i$$

we have

$$\mathfrak{a}_i = \mathfrak{c}_i \cap \mathfrak{O}_t.$$

Now let $\sigma_i := \sigma(\mathfrak{c}_i)$ be the corresponding Frobenius maps of K_{tN}/K. Then their restrictions to Ω_t are

$$\sigma_i|\Omega_t = \sigma(\mathfrak{a}_i) = \sigma([\alpha_i, 1]^{-1})$$

which constitute the different automorphisms of Ω_t/K. We set

$$\alpha_0 := A_1\alpha_1 = \frac{-B_1 + t\sqrt{d}}{2}.$$

This is a quotient of a basis of $\mathfrak{O}_t$, and as by assumption $g(\alpha_0) \neq \infty$, the reciprocity law implies

$$g(\alpha_0) \in K_{tN}.$$

Using $B_1 \equiv B_i \bmod 2N$ we can write

$$g(\alpha_0) = g\left(\frac{-B_i + t\sqrt{d}}{2}\right), \quad i = 1, \ldots, h_t,$$

so by the reciprocity law we obtain

$$g(\alpha_0)^{\sigma_i} = \left[g \circ \begin{pmatrix} A_i & 0 \\ 0 & 1 \end{pmatrix}\right]\left(\frac{-B_i + t\sqrt{d}}{2A_i}\right) = g_i(\alpha_i).$$

This implies the assertion of the Theorem. □

We now consider a more special situation.

Proposition 1. *Let g be as in Theorem 6 and $\mathfrak{O}_t = [\beta, 1]$ with β prime to Nt and $\Im(\beta) > 0$. Let $A \in \mathbb{N}$ be prime to Nt with the property that A is the norm of a primitive ideal $\mathfrak{a}$ of $\mathfrak{O}_1$ and that $\overline{\mathfrak{a}}_t = [\beta, A]$.*

Then, if $g(\beta) \neq \infty$, we have

1) $g(\beta) \in \Omega_{tN}$,
2) $g(\beta)^{\sigma(\overline{\beta})} = g\left(\frac{1}{\beta}\right)$,
3) $g(\beta)^{\sigma(\mathfrak{a})} = g(\frac{\beta}{A})$.

Proof. Keeping in mind that g has rational q-expansion coefficients the first and third assertion follow directly from Theorem 5 and 6. To prove the second assertion we first observe that $\mathfrak{O}_t = [\beta, 1] = [\bar{\beta}, 1]$, whence $\beta\mathfrak{O}_t = [\beta, b]$ with $b = \beta\bar{\beta}$. Theorem 5 now implies $g(\beta)^{\sigma(\bar{\beta})} = g(\frac{\beta}{b}) = g(\frac{1}{\beta})$ which completes the proof. □

To apply Proposition 1 to the Schläfli functions we quote from [Me1], p. 162 formulas (4.21), (4.22) and (4.23):

Proposition 2. *Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be a unimodular matrix which we assume to be normalized by*

$$c \geq 0 \quad \textit{and} \quad d > 0 \textit{ if } c = 0.$$

We define c_1 and λ in $\mathbb{Z}$ by

$$c = c_1 2^\lambda \textit{ with } c_1 \equiv 1 \textit{ mod } 2 \textit{ if } c \neq 0,$$
$$c_1 = \lambda = 1 \textit{ if } c = 0.$$

Then we have the transformation formula

$$\eta(Mz) = \epsilon(M)\sqrt{cz + d}\ \eta(z) \qquad \textit{with } \Re(\sqrt{cz+d}) > 0$$

and

$$\epsilon(M) = (\frac{a}{c_1})\zeta_{24}^{ba + c(d(1-a^2)-a) + 3(a-1)c_1 + \lambda\frac{3}{2}(a^2-1)}.$$

Herein $(\frac{a}{c_1})$ is the Legendre symbol and $\zeta_{24} = e^{\frac{2\pi i}{24}}$.

Proof. The formula is easily derived from [Me1]. In fact there are two formulas in [Me1], one in the case $2 \nmid c$ and another in the case $2 \nmid a$. The above formula is obtained by applying the quadratic reciprocity law to the Legendre symbol $(\frac{c}{a})$ in front of the second formula in [Me1] which then in the case $2 \nmid c$ coincides with the first formula. □

Remark. A multiplicative interpretation of the above values $\epsilon(M)$, with M unimodular, can be found in the paper of Farshid Hajir [Ha].

Proposition 3. *Let N be a natural number, $\alpha_0 \in \mathbb{H}$ the quotient of a basis of an ideal $\mathfrak{a}_0$ from $\mathfrak{I}_t$ and $A_0X^2 + B_0X + C_0 = 0$ its primitive equation. We assume that* $\gcd(A_0, N) = 1$*. (this last exigency puts no restriction on the above ideal $\mathfrak{a}_0$). Then in any class of $\mathfrak{R}_t$ there exists an ideal $\mathfrak{a}$ and a $\mathbb{Z}$-basis of $\mathfrak{a}$ such that its quotient $\alpha \in \mathbb{H}$ has a primitive equation $AX^2 + BX + C = 0$ satisfying*

$$\gcd(A, N) = 1 \textit{ and } B \equiv B_0 \textit{ mod } 2N.$$

For any such α *there exists a unimodular transformation* $M \equiv \pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ *mod* N *such that the coefficients of the primitive equation* $A'X^2 + B'X + C' = 0$ *of* $M(\alpha)$ *satisfy*

$$\gcd(A', tN) = 1 \text{ and } B' \equiv B \text{ mod } 2N.$$

Proof. Let $\alpha \in \mathbb{H}$ be the quotient of a basis of an ideal $\mathfrak{a} \in \mathfrak{I}_t$. Then $\alpha' \in \mathbb{H}$ is the quotient of a basis of an ideal from the same class as $\mathfrak{a}$ if and only if $\alpha' = M(\alpha)$ with a unimodular transformation M. So we must show that there exists a unimodular transformation M such that the primitive equation of $M(\alpha)$ has the desired properties. We do this by induction on the number of primes dividing N. For $N = 1$ there is nothing to be shown. Note that $B^2 \equiv t^2 d$ mod 4 which implies the desired congruence for B in the case $N = 1$. So we assume the assertion to be shown for some $N \in \mathbb{N}$ and we contend that it is also true for $N' = Np^s, s \in \mathbb{N}$, with a prime p not dividing N. To construct the unimodular transformation needed, we define

$$M_\mu := \begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix}, \quad N_\mu := \begin{pmatrix} 1 & 0 \\ -\mu & 1 \end{pmatrix}, \quad \mu \in \mathbb{Z}.$$

If $\omega \in \mathbb{H}$ is a root of the primitive equation

$$AX^2 + BX + C = 0,$$

then $M_\mu(\omega)$ resp. $N_\mu(\omega)$ are roots of the equations

$$AX^2 + (B + 2\mu A)X + (C + \mu B + \mu^2 A) = 0$$
$$\text{resp. } (A + \mu B + \mu^2 C)X^2 + (B + 2\mu C)X + C = 0,$$

where the gcd of the coefficients is again equal to 1. Now we assume that α is a root of the primitive quadratic equation

$$AX^2 + BX + C = 0 \text{ with } \gcd(A, N) = 1, A > 0 \text{ and } B \equiv B_0 \text{ mod } N.$$

If α is transformed by some M_μ or N_μ with μ divisible by N, these conditions are conserved for μ sufficiently large. Note that $B^2 - 4AC < 0$ and $A > 0$ implies $C > 0$. Further by applying a product of M_μ's and N_μ's we can achieve that A becomes prime to p. For $p \neq 2$ or ($p = 2$ and $2|B$) this becomes clear by writing $A + \mu B + \mu^2 C = A + \mu(B + \mu C)$. If ($p = 2$ and $2 \nmid B$) we must first achieve that $2|C$ by applying some M_μ and then we get $\gcd(A, 2) = 1$ by applying some N_μ. In this way we end up with an equation where A is prime to N'. In order to get an equation in which B is congruent to B_0 mod N' we apply again some M_μ. Then B is transformed to $B' = B + 2\mu A$. Writing

$$B' - B_0 = 2\Big(\frac{B - B_0}{2} + \mu A\Big),$$

and keeping in mind that $B \equiv B_0 \bmod 2$, we then see that by a suitable choice of a number $\mu \equiv 0 \bmod N$ the congruence $B \equiv B_0 \bmod 2N'$ can be satisfied.

To prove the second assertion of Proposition 3 we continue applying this construction to the primes p dividing t and not dividing N. Then the parameters μ are divisible by N. So the unimodular transformation M satisfies $M \equiv \pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \bmod N$ because it is a product of M_μ's and N_μ's with $\mu \equiv 0 \bmod N$. $\square$

Proof of Theorem 1. Using Proposition 2 and the relation $f = \frac{\sqrt{2}}{f_1 f_2}$, we find that f^3 is invariant under unimodular Transformations $M \equiv \left(\begin{smallmatrix}*&0\\0&*\end{smallmatrix}\right) \bmod 16$. Further we can see from the definition that f^3 has rational q-expansion coefficients and by Proposition 2 it follows that f^3 is in F_{16}. Let m be the natural number from Theorem 1 and t be the conductor of the order $[\sqrt{-m}, 1]$. For $\mu \in \mathbb{Z}$ we set

$$\beta_\mu = \begin{cases} \sqrt{-m} + 2\mu, & \text{if } m \equiv 1 \bmod 2, \\ \sqrt{-m} + 1 + 2\mu, & \text{if } m \equiv 0 \bmod 2. \end{cases}$$

Then by Theorem 6 we have

$$f^3(\beta_\mu) \in \Omega_{16t}.$$

Here $[\Omega_{16t} : \Omega_t] = 16$ for $t^2 d \neq -4$ and $[\Omega_{16t} : \Omega_t] = 8$ for $t^2 d = -4$. Choosing the numbers $\mu \bmod 8$ with the property that the β_μ are prime to t we find that

$$\mathrm{Gal}(\Omega_{16t}/\Omega_t) = < \{\sigma(\overline{\beta_\mu}) \ : \ \mu \bmod 8\} > .$$

By Proposition 1 we obtain the Galois action

$$f^3(\beta_0)^{\sigma(\overline{\beta_\mu})} = \left(f^3(\beta_\mu)\zeta_8^\mu\right)^{\sigma(\overline{\beta_\mu})} = f^3\Big(\frac{1}{\overline{\overline{\beta_\mu}}}\Big)\zeta_8^{\mu\sigma(\overline{\beta_\mu})},$$

keeping in mind that by class field theory ζ_8 is in Ω_{16t} (or by concluding $\zeta_8 = f(\beta_0)^3 f(\beta_1)^{-3} \in \Omega_{16t}$). Herein we have $\zeta_8^{\sigma(\overline{\beta_\mu})} = \zeta_8^{n_\mu}$ with the complex norm n_μ of $\overline{\beta_\mu}$. Further from Proposition 2 we get the identity $f(\frac{-1}{z}) = f(z)$. Whence our Galois action becomes

$$f^3(\sqrt{-m})^{\sigma(\overline{\beta_\mu})-1} = \zeta_8^{\mu(m+1+4\mu^2)} \qquad \text{if } 2 \nmid m.$$

Using the relation $f_1^3(z) = \zeta_{16} f^3(z+1)$ we further obtain

$$f_1^6(\sqrt{-m})^{\sigma(\overline{\beta_\mu})-1} = \zeta_8^{(m+2)(2\mu+1)}, \qquad \text{if } 2|m.$$

From the Frobenius congruence we deduce

$$\sqrt{2}^{\sigma(\overline{\beta_\mu})-1} = \Big(\frac{2}{n_\mu}\Big).$$

Discussing cases we now obtain that for the special arguments $\alpha = \sqrt{-m}$ the numbers of Theorem 1 are in Ω_t. Moreover these numbers are real as can be seen from the q-expansions. So we can conclude that they are contained in $\Omega_t \cap \mathbb{R} = \mathbb{Q}(j(\sqrt{-m}))$. They are even generators for this field, because of the relation $j = \frac{(f^{24}-16)^3}{f^{24}} = \frac{(f_1^{24}+16)^3}{f_1^{24}}$.

The assertions of Theorem 1 now follow from Theorem 7 keeping in mind that the action of the automorphism σ_i in Theorem 7 on $\sqrt{2}$ is given by $\sqrt{2}^{\sigma_i} = (\frac{2}{A_i})\sqrt{2}$. □

Proof of Theorem 2. Using Proposition 2 it can be seen that γ_2 is invariant under unimodular Transformations $M \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)$ mod 3. Further γ_2 has rational q-expansion coefficients. As in the proof of Theorem 1 we first assume α to be of the form

$$\alpha = \begin{cases} \sqrt{-m} & \text{or} \\ \frac{3m+\sqrt{-m}}{2}, & -m \equiv 1 \bmod 4, \end{cases}$$

with a natural number m and conclude by Theorem 6

$$\gamma_2(\alpha) \in \Omega_{3t},$$

where t denotes the conductor of the order $\mathfrak{O}_t = [\alpha, 1]$. For $\alpha = \frac{9+\sqrt{-3}}{2}$ the assertion is trivial because $\gamma_2(\alpha) = 0$. Otherwise we find

$$[\Omega_{3t} : \Omega_t] = \begin{cases} 3, & \text{if } m \equiv 0 \bmod 3, \\ 2, & \text{if } m \equiv -1 \bmod 3, \\ 4, & \text{if } m \equiv 1 \bmod 3. \end{cases}$$

and

$$\mathrm{Gal}(\Omega_{3t}/\Omega_t) = \begin{cases} < \sigma(\overline{\alpha+1}) >, & \text{if } m \equiv 0 \bmod 3, \\ < \sigma(\overline{\alpha+3}) >, & \text{if } m \equiv -1 \bmod 3, \\ < \sigma(\overline{\alpha \pm 1}) >, & \text{if } m \equiv 1 \bmod 3. \end{cases}$$

We compute the Galois action on $\gamma_2(\alpha)$ by Proposition 1:

$$\gamma_2(\alpha)^{\sigma(\overline{\alpha+\mu})} = (\gamma_2(\alpha+\mu)\zeta_3^{\mu})^{\sigma(\overline{\alpha+\mu})} = \gamma_2(\frac{1}{\overline{\alpha+\mu}})\zeta_3^{\mu n_\mu}.$$

Here n_μ is the norm of $\overline{\alpha+\mu}$ which is congruent to $m+\mu^2$ modulo 3. Using further the transformation formula $\gamma_2(\frac{-1}{z}) = \gamma_2(z)$ the Galois action becomes

$$\gamma_2(\alpha)^{\sigma(\overline{\alpha+\mu})} = \gamma_2(-\overline{\alpha})\zeta_3^{\mu(1+m+\mu^2)} = \gamma_2(\alpha)\zeta_3^{\mu(2+m)}.$$

Observing that $\gamma_2(\alpha)$ is real, we can conclude as in the proof of Theorem 1:

$$\mathbb{Q}(\gamma_2(\alpha)) = \begin{cases} \Omega_t \cap \mathbb{R} = \mathbb{Q}(j(\alpha)) & \text{if } 3 \nmid m, \\ \Omega_{3t} \cap \mathbb{R} = \mathbb{Q}(j(3\alpha)) & \text{if } 3 | m. \end{cases}$$

The rest of the proof now follows again from Theorem 7. $\square$

Proof of Theorem 3. As in the preceding proofs it suffices to consider the case when α is of the form

$$\alpha = \begin{cases} \frac{-m+\sqrt{-m}}{2}, & -m \equiv 1 \bmod 4, \text{ or} \\ & \sqrt{-m} \end{cases}$$

with a natural number m. As γ_3 satisfies the hypothesis of Proposition 1 with $N = 2$ we have

$$\gamma_3(\alpha) \in \Omega_{2t},$$

where t is the conductor of $\mathfrak{O}_t = [\alpha, 1]$. Here $D(\alpha) = -m$, and

$$[\Omega_{2t} : \Omega_t] = \begin{cases} 1 \text{ or } 3 & \text{if } 2 \nmid D(\alpha), \\ 2 \text{ if } 2|D(\alpha). \end{cases}$$

In the case $2 \nmid D(\alpha)$ this implies $\gamma_3(\alpha) \in \Omega_t$, because the square of $\gamma_3(\alpha)$ is in Ω_t. Here $\sqrt{d}\gamma_3(\alpha)$ is real and by the usual arguments it follows

$$\mathbb{Q}(\sqrt{d}\gamma_3(\alpha)) = \mathbb{Q}(j(\alpha)), \text{ if } 2 \nmid D(\alpha).$$

In the case $2|D(\alpha)$ the Galois group of Ω_{2t}/Ω_t is generated by $\sigma(\overline{\alpha + 1})$ and, using the identities $\gamma_3(z+1) = -\gamma_3(z)$ and $\gamma_3(\frac{-1}{z}) = -\gamma_3(z)$, we get $\gamma_3(\alpha)^{\sigma(\overline{\alpha+1})} = -\gamma_3(\alpha)$. This implies $\mathbb{Q}(\gamma_3(\alpha)) = \Omega_{2t} \cap \mathbb{R} = \mathbb{Q}(j(2\alpha))$ because in this case $\gamma_3(\alpha)$ is real. The last assertion of Theorem 3 follows again from Theorem 7. $\square$

Proof of Theorem 4. From Theorem 5 we know that $g(\alpha)$ is in K_{tN}. So we are left with the proof of $g(\alpha)$ being invariant under the automorphisms of K_{tN}/Ω_t. These are all Frobenius maps $\sigma(\mathfrak{c})$ belonging to some principal primitive prime ideal $\mathfrak{c} = \lambda\mathfrak{O}_1$ of norm c prime to tN with $\lambda \in \mathfrak{O}_t$. To compute $g(\alpha)^{\sigma(\mathfrak{c})}$ we observe that

$$\mathfrak{a} := [A\alpha, A] \in \mathfrak{I}_t \text{ and } \mathfrak{O}_t = [A\alpha, 1].$$

By adding to α a suitable number from $N\mathbb{Z}$ we can further achieve that

$$\overline{\mathfrak{c}_t} = \mathfrak{O}_t\overline{\lambda} = [A\alpha, c] \text{ and } \mathfrak{a}\overline{\mathfrak{c}}_t = [A\alpha, Ac].$$

Under this change of α the value $g(\alpha)$ remains the same because g has the period N and also the assumptions about the coefficients of the primitive equation remain valid. The reciprocity law now implies

$$g(\alpha)^{\sigma(\mathfrak{c})} = g\Big(\frac{\alpha}{c}\Big).$$

To show that $g(\frac{\alpha}{c}) = g(\alpha)$ we observe that

$$\overline{\lambda}\begin{pmatrix} A\alpha \\ A \end{pmatrix} = \begin{pmatrix} u & vC \\ -vA & u - vB \end{pmatrix}\begin{pmatrix} A\alpha \\ A \end{pmatrix}$$

where $u, v \in \mathbb{Z}$ come from the representation $\lambda = u + vA\alpha \in \mathfrak{O}_t = [A\alpha, 1]$. Further we have

$$[A\alpha, Ac] = \mathfrak{a}\bar{\mathfrak{c}}_t = \overline{\lambda}[A\alpha, A].$$

So there is a unimodular matrix M satisfying

$$(+) \qquad \begin{pmatrix} A\alpha \\ Ac \end{pmatrix} = M\left(\overline{\lambda}\begin{pmatrix} A\alpha \\ A \end{pmatrix}\right) = M\begin{pmatrix} u & vC \\ -vA & u - vB \end{pmatrix}\begin{pmatrix} A\alpha \\ A \end{pmatrix}.$$

Comparing coefficients, we now get the identity

$$\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} = M\begin{pmatrix} u & vC \\ -vA & u - vB \end{pmatrix},$$

which tells us that

$$M \equiv \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \bmod N,$$

because by assumption we have $N|C$ and $\gcd(N, c) = 1$. From (+) we now conclude that $\frac{\alpha}{c} = M(\alpha)$ and the Galois action therefore becomes

$$g(\alpha)^{\sigma(\mathfrak{c})} = g(\frac{\alpha}{c}) = g(M(\alpha)) = g(\alpha).$$

This invariance implies $g(\alpha) \in \Omega_t$. □

Examples.

The polynomials in the following examples are the minimal polynomials of the numbers Θ from Theorem 1.

1) $m = 17, \Theta = \frac{1}{\sqrt{2}} f(\sqrt{-m})^2$

$$X^4 - X^3 - 2X^2 - X + 1$$

2) $m = 11, \Theta = f(\sqrt{-m})$

$$X^3 - 2X^2 + 2X - 2$$

3)$m = 13, \Theta = \frac{1}{2} f(\sqrt{-m})^4$

$$X^2 - 3X - 1$$

4) m=23 , $\Theta = \frac{1}{\sqrt{2}} f(\sqrt{-m})$

$$X^3 - X - 1$$

5) m=22, $\Theta = \frac{1}{\sqrt{2}} f_1(\sqrt{-m})^2$

$$X^2 - 2X - 1$$

6) m=28, $\Theta = \frac{1}{2\sqrt{2}} f_1(\sqrt{-m})^4$

$$X^2 - 6X + 2$$

7) m=1001, $\Theta = \frac{1}{\sqrt{2}} f(\sqrt{-m})^2$

$$X^{40} - 2824\,X^{39} + 75112\,X^{38} - 718892\,X^{37} + 2617834\,X^{36} - 3040200\,X^{35} - 5787096\,X^{34} + 11053184\,X^{33} - 12333429\,X^{32} + 12040916\,X^{31} + 9400544\,X^{30} + 582996\,X^{29} + 148470680\,X^{28} + 146227624\,X^{27} + 239284416\,X^{26} + 287353308\,X^{25} + 122239373\,X^{24} + 350484164\,X^{23} + 497832264\,X^{22} + 657032444\,X^{21} + 977531386\,X^{20} + 657032444\,X^{19} + 497832264\,X^{18} + 350484164\,X^{17} + 122239373\,X^{16} + 287353308\,X^{15} + 239284416\,X^{14} + 146227624\,X^{13} + 148470680\,X^{12} + 582996\,X^{11} + 9400544\,X^{10} + 12040916\,X^{9} - 12333429\,X^{8} + 11053184\,X^{7} - 5787096\,X^{6} - 3040200\,X^{5} + 2617834\,X^{4} - 718892\,X^{3} + 75112\,X^{2} - 2824\,X + 1$$

8) m=2003, $\Theta = f(\sqrt{-m})$

$$X^{27} - 360\,X^{26} + 3488\,X^{25} - 15310\,X^{24} - 752\,X^{23} - 69104\,X^{22} - 24664\,X^{21} - 91520\,X^{20} - 189088\,X^{19} - 175504\,X^{18} - 129792\,X^{17} - 118848\,X^{16} + 52160\,X^{15} - 122240\,X^{14} - 271744\,X^{13} + 161152\,X^{12} + 665344\,X^{11} + 314624\,X^{10} + 336512\,X^{9} + 522240\,X^{8} + 1093120\,X^{7} + 706304\,X^{6} - 737280\,X^{5} - 1262592\,X^{4} - 688384\,X^{3} - 163840\,X^{2} - 14336\,X - 512$$

9) m=1013, $\Theta = \frac{1}{2} f(\sqrt{-m})^4$

$$X^{26} - 8638585\,X^{25} - 2071370697\,X^{24} - 138021080344\,X^{23} + 383664717488\,X^{22} - 4702813029912\,X^{21} + 19839877238724\,X^{20} - 72973630222172\,X^{19} + 109241003683084\,X^{18} - 133315578757800\,X^{17} + 159614389643888\,X^{16} - 241116348297768\,X^{15} + 107250978902142\,X^{14} - 285857666066774\,X^{13} - 107250978902142\,X^{12} - 241116348297768\,X^{11} - 159614389643888\,X^{10} - 133315578757800\,X^{9} - 109241003683084\,X^{8} - 72973630222172\,X^{7} - 19839877238724\,X^{6} - 4702813029912\,X^{5} - 383664717488\,X^{4} - 138021080344\,X^{3} + 2071370697\,X^{2} - 8638585\,X - 1$$

10) m=1007, $\Theta = \frac{1}{\sqrt{2}} f(\sqrt{-m})$

$$X^{30} - 50\,X^{29} + 228\,X^{28} - 171\,X^{27} - 739\,X^{26} + 1063\,X^{25} + 642\,X^{24} - 2904\,X^{23} + 468\,X^{22} + 3816\,X^{21} - 2916\,X^{20} - 2965\,X^{19} + 4638\,X^{18} + 738\,X^{17} - 3948\,X^{16} + 1488\,X^{15} + 2069\,X^{14} - 1844\,X^{13} - 303\,X^{12} + 972\,X^{11} - 465\,X^{10} - 198\,X^{9} + 349\,X^{8} - 122\,X^{7} - 111\,X^{6} + 110\,X^{5} + 13\,X^{4} - 34\,X^{3} + 3\,X^{2} + 4\,X - 1$$

11) m=1006, $\Theta = \frac{1}{\sqrt{2}} f_1(\sqrt{-m})^2$

$$
\begin{aligned}
&X^{20} - 2862\,X^{19} + 18195\,X^{18} - 48762\,X^{17} + 11084\,X^{16} + 60534\,X^{15} - 174675\,X^{14} \\
&- 201690\,X^{13} - 351665\,X^{12} - 324756\,X^{11} - 32904\,X^{10} - 324756\,X^{9} \\
&- 351665\,X^{8} - 201690\,X^{7} - 174675\,X^{6} + 60534\,X^{5} + 11084\,X^{4} - 48762\,X^{3} \\
&+ 18195\,X^{2} - 2862\,X + 1
\end{aligned}
$$

12) m=1004, $\Theta = \frac{1}{2\sqrt{2}} f_1(\sqrt{-m})^4$

$$
\begin{aligned}
&X^{42} - 5671948\,X^{41} + 1112926984\,X^{40} - 74506711266\,X^{39} + 1675441064140\,X^{38} \\
&- 20345997579492\,X^{37} + 150351443028134\,X^{36} - 762529752723792\,X^{35} \\
&+ 2798004552329936\,X^{34} - 7787328942670784\,X^{33} + 16996307948907776\,X^{32} \\
&- 30010334766581376\,X^{31} + 44569850359633884\,X^{30} \\
&- 57942714536638960\,X^{29} + 67539174378820096\,X^{28} - 70938998122923512\,X^{27} \\
&+ 67381814594465424\,X^{26} - 58822250908214576\,X^{25} + 48241450095048360\,X^{24} \\
&- 37726219762705792\,X^{23} + 28473140297449600\,X^{22} \\
&- 21313830576800768\,X^{21} + 16561288807726592\,X^{20} - 13724502533179904\,X^{19} \\
&+ 11721800154235312\,X^{18} - 9568457484683072\,X^{17} + 6990811806670464\,X^{16} \\
&- 4392860511123296\,X^{15} + 2315747367256640\,X^{14} - 1000014874461888\,X^{13} \\
&+ 342306261424160\,X^{12} - 88137409618176\,X^{11} + 15377464747264\,X^{10} \\
&- 1245547475968\,X^{9} - 148822030336\,X^{8} + 50249859072\,X^{7} + 152754496\,X^{6} \\
&- 2497642752\,X^{5} + 580336640\,X^{4} - 81811072\,X^{3} + 5100288\,X^{2} - 360704\,X \\
&- 128
\end{aligned}
$$

A slightly simpler generating element for the same field is obtained by the singular value

$$\tilde{\Theta} = \frac{\eta\left(\frac{\alpha}{5}\right)\eta\left(\frac{\alpha}{5}\right)}{\eta\left(\frac{\alpha}{25}\right)\eta\left(\alpha\right)}, \quad \alpha = 186 + \sqrt{-m},$$

which is a quotient of the form α_1^2/α_2, for the ideal $\mathfrak{a} = [\alpha, 5]$, in the sense of [Ha-Vi] pp.518-519. For the above α the values $\gamma_2(\alpha)$ and $\gamma_3(\alpha)$ are class invariants. So Theorem 4 implies that $\tilde{\Theta}$ is in $K(j(\alpha)) = \Omega_4$ and from [Sch2, Sch3], we know that $\tilde{\Theta}$ is a generator of Ω_4/K. It also is a generator of $\mathbb{Q}(j(\alpha))/\mathbb{Q}$ because $\tilde{\Theta}$ has a real conjugate. Computing its minimal equation over $\mathbb{Q}$ by Theorem 4 we find

$$\begin{aligned}
&X^{42} - 388\,X^{41} + 39454\,X^{40} + 152772\,X^{39} - 1151521\,X^{38} - 1808750\,X^{37}\\
&+ 37261677\,X^{36} + 123881082\,X^{35} + 624595534\,X^{34} + 1415717296\,X^{33}\\
&+ 4094968517\,X^{32} - 11236196284\,X^{31} - 9140592356\,X^{30} + 19698906464\,X^{29}\\
&- 35151306728\,X^{28} - 76440167784\,X^{27} + 16320199943\,X^{26} + 4808571960\,X^{25}\\
&+ 21934161066\,X^{24} - 70262876284\,X^{23} + 549244154775\,X^{22}\\
&+ 172140515694\,X^{21} + 734171360591\,X^{20} + 439699716458\,X^{19}\\
&+ 1522058484380\,X^{18} + 339554800476\,X^{17} + 1544651311977\,X^{16}\\
&+ 525923997560\,X^{15} + 1338600826888\,X^{14} + 148663740988\,X^{13}\\
&+ 1025057142710\,X^{12} - 4796740960\,X^{11} + 445539315907\,X^{10}\\
&+ 7421360504\,X^{9} + 166511416826\,X^{8} - 70875911504\,X^{7} + 69044405135\,X^{6}\\
&- 18623298898\,X^{5} + 6114740239\,X^{4} - 639708518\,X^{3} + 22031834\,X^{2}\\
&- 259936\,X + 1.
\end{aligned}$$

References

[Bi] B. J. Birch, *Weber's Class Invariants.* Mathematika **16** (1969), 283–294.

[De] M. Deuring, *Die Klassenkörper der komplexen Multiplikation.* Enzykl. d. math. Wiss. I/2, 2.Auflage, Heft 10, Stuttgart, 1958.

[Ha-Vi] F. Hajir, F. R. Villegas, *Explicit elliptic units*, I. Duke Math. J. **90** (1997), 495–521.

[He] K. Heegner, *Diophantische Analysis und Modulfunktionen.* Math. Zeitschrift **56** (1952), 227–253.

[La] S. Lang, *Elliptic functions.* Addison Wesley, 1973.

[Me1] C. Meyer, *Über einige Anwendungen Dedekindscher Summen.* J. Reine Angew. Math. **198** (1957), 143–203.

[Me2] C. Meyer, *Bemerkungen zum Satz von Heegner-Stark über die imaginär-quadratischen Zahlkörper mit der Klassenzahl Eins.* J. Reine Angew. Math. **242** (1970), 179–214.

[Mo] F. Morain, *Modular Curves, Class Invariants and Applications*, preprint.

[Sch1] R. Schertz, *Die singulären Werte der Weberschen Funktionen* $f, f_1, f_2, \gamma_2, \gamma_3$. J. Reine Angew. Math. **286/287** (1976), 46–74.

[Sch2] R. Schertz, *Zur Theorie der Ringklassenkörper über imaginär-quadratischen Zahlkörpern.* J. Number Theory **10** (1978), 70–82.

[Sch3] R. Schertz, *Zur expliziten Berechnung von Ganzheitsbasen in Strahlklassenkörpern über einem imaginär-quadratischen Zahlkörper.* J. Number Theory **34** (1990), 41–53.

[Sch4] R. Schertz, *Construction of Ray Class Fields by Elliptic Units.* J. Théor. Nombres Bordeaux **9** (1997), 383–394.

[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.

[St] H. Stark, *On the "Gap" in a Theorem of Heegner.* J. Number Theory **1** (1969), 16–27.

[We] H. Weber, *Lehrbuch der Algebra*, Bd 3, 2.Aufl. Braunschweig, 1908; Neudruck, New York, 1962.

Reinhard Schertz
Institut für Mathematik der Universität Augsburg
Universitätsstraße 8
86159 Augsburg, Germany
E-mail : `Reinhard.Schertz@Math.Uni-Augsburg.DE`