Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 161–176

# Hilbert's 12th Problem, Complex Multiplication and Shimura Reciprocity

**Peter Stevenhagen**

**Abstract.**

We indicate the place of Shimura's reciprocity law in class field theory and give a formulation of the law that reduces the technical prerequisites to a minimum. We then illustrate its practical use by dealing with a number of classical problems from the theory of complex multiplication that have been the subject of recent research. Among them are the construction of class invariants and the explicit generation of ring class fields.

## §1. Hilbert's 12th problem

All variants of class field theory can be said to 'classify' in some way the abelian extensions of a given field $K$. The classical examples are those where $K$ is a number field, a function field in one variable over a finite field, or a local field, but the second half of this century has seen the birth of higher dimensional analogues as well [12].

In the classical cases, the main theorem of class field theory provides an anti-equivalence

$$\psi : \mathbf{Ab}_K \longrightarrow \mathbf{Sub}_X$$

between the category $\mathbf{Ab}_K$ of finite abelian extensions of $K$ (inside some algebraic closure $\overline{K}$ of $K$) and the category $\mathbf{Sub}_X$ of open subgroups of a locally compact abelian group $X = X(K)$, which is entirely defined 'in terms of $K$'. Here the morphisms in both categories are simply the inclusions between fields and subgroups, respectively. In the three standard examples mentioned above, $X(K)$ can be taken to be equal to the idèle class group of $K$ in the first two cases, which constitute the global case, and to the multiplicative group $K^*$ in the local case.

---

Acknowledgement: I thank N. Schappacher for drawing my attention to Söhngen's paper [15] during the conference.

Received October 7, 1998

Revised November 30, 1998

The definition of the anti-equivalence $\psi$ is entirely explicit: it maps a finite abelian extension $L$ of $K$ to the norm image $N_{L/K}X(L)$. The 'surjectivity on objects' of $\psi$ is the *existence theorem* of class field theory, which guarantees that every open subgroup $H \subset X_K$ is of the form $N_{L/K}X(L)$ for some finite abelian extension $L$ of $K$, the *class field* of $H$. The problem of finding a 'direct description' of the extension $L = \psi^{-1}[H]$ in terms of $H$ is known as *Hilbert's 12th problem*. Hilbert originally posed the problem for number fields, but it occurs in the other variants of class field theory as well.

Already for number fields, Hilbert's problem is not entirely well-posed, as one cannot say that the construction of class fields in the proof of the existence theorem is not 'explicit' or 'constructive'. However, the proof is not 'direct' in the sense that it does not generate the class fields over $K$ itself, but over large auxiliary extensions of $K$. What Hilbert had in mind was an analogue for arbitrary number fields of the following theorem over $\mathbf{Q}$.

**1.1. Kronecker-Weber theorem.** *The abelian extensions of* $\mathbf{Q}$ *are generated by the values of the exponential function* $\exp : \tau \mapsto e^{2\pi i\tau}$ *at rational arguments* $\tau$.

Even though the theorem exhibits the generators of the abelian extensions as values of a transcendental function, it is relatively easy to find the corresponding algebraic data, i.e., the irreducible polynomials in $\mathbf{Z}[X]$ corresponding to these generators. As $\exp[\mathbf{Q}] \cong \mathbf{Q}/\mathbf{Z}$ is the subgroup of roots of unity in $\mathbf{C}^*$, these are the *cyclotomic polynomials*. Moreover, the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the roots of unity generating the maximal abelian extension $\mathbf{Q}_{\mathrm{ab}}$ of $\mathbf{Q}$ yields an isomorphism

$$\mathrm{Gal}(\mathbf{Q}_{\mathrm{ab}}/\mathbf{Q}) \cong \mathrm{Aut}(\mathbf{Q}/\mathbf{Z}) = \widehat{\mathbf{Z}}^*.$$

For local fields and for function fields over finite fields, there is an analogue of the statement in 1.1 that there is a module $\mathbf{C}^*$ over the ring of integers $\mathbf{Z}$ of $\mathbf{Q}$ with the property that the torsion points of the $\mathbf{Z}$-action on $\mathbf{C}^*$ generate the abelian extensions of $\mathbf{Q}$. In both cases, the abelian extensions are generated by the torsion points of a suitable module over a 'ring of integers' $A \subset K$. In the local case, $A$ is the valuation ring and the module is provided by the Lubin-Tate theory of formal groups [10]. In the function field case, there is some choice for $A$ which has to be taken care of, and the modules one needs are rank-one Drinfeld $A$-modules [8].

As far as finding an analogue of the Kronecker-Weber theorem for number fields $K \neq \mathbf{Q}$ is concerned, Hilbert's problem is outstanding in

all but the special case of imaginary quadratic $K$. It is one of the main open problems in class field theory.

## §2. Complex multiplication

The theory that generalizes 1.1 for imaginary quadratic fields goes under the name of *complex multiplication*. We let $K$ further be imaginary quadratic, and use the unique infinite prime of $K$ to view $\mathbf{C}$ as the archimedean completion of $K$. This enables us to evaluate complex analytic functions in the '$K$-valued points' of either $\mathbf{C}$ itself or the complex upper half plane $\mathbf{H} = \{\tau \in \mathbf{C} : \mathrm{Im}(\tau) > 0\}$. It is our aim to generate the maximal abelian extension $K_{\mathrm{ab}}$ of $K$ using such values.

The maximal abelian extension $\mathbf{Q}_{\mathrm{ab}}$ of $\mathbf{Q}$, which contains $K$, is clearly a subfield of $K_{\mathrm{ab}}$. Weber tried to generate $K_{\mathrm{ab}}$ over $\mathbf{Q}_{\mathrm{ab}}$ using the values of the modular function $j : \mathbf{H} \to \mathbf{C}$. This is the unique holomorphic function on $\mathbf{H}$ that is invariant under the action of the modular group $\mathrm{SL}_2(\mathbf{Z})$ and has a Fourier expansion of the form $j(q) = q^{-1} + 744 + O(q)$ for $q = e^{2\pi i\tau}$ tending to 0. Weber thought incorrectly [18, §169] that $K_{\mathrm{ab}}$ is the compositum of $\mathbf{Q}_{\mathrm{ab}}$ and the field $K_j$ obtained by adjoining to $K$ the values $j(\tau)$ of the $j$-function at $\tau \in K \cap \mathbf{H}$. One does however come close.

**2.1. Theorem.** *The maximal abelian extension $K_{\mathrm{ab}}$ of $K$ is an infinite abelian extension of $K_j\mathbf{Q}_{\mathrm{ab}}$ with Galois group of exponent 2.*

Other functions are needed if one wants the full extension $K_{\mathrm{ab}}$ rather than the approximation 'up to quadratic extensions' from 1.2. There are two ways to proceed, and they appear to be rather different at first sight.

The first method goes back to Fueter, Takagi and Hasse. Fueter, who discovered the need of additional quadratic extensions, showed [4, Hauptsatz, p. 253] that $K_{\mathrm{ab}}$ is contained in the extension of $K_j\mathbf{Q}_{\mathrm{ab}}$ generated by the division values ('Teilwerte') of the *Weber function* $h_K$ associated to $K$. This function, which is not a modular but an elliptic function, is the 'normalized' $x$-coordinate on a Weierstrass model of the elliptic curve $E = \mathbf{C}/\mathcal{O}_K$ associated to the ring of integers $\mathcal{O}_K$ of $K$. It can be viewed as a meromorphic function on $\mathbf{C}$ with period lattice $\mathcal{O}_K$. The precise definition, which depends on the number of roots of unity in $K$, can be found in [18, §153], [9, Ch. 1, §5] or [3, §6].

Incomplete knowledge of the arithmetic nature of the division values of the Weber functions prevented Weber himself [18, §155] from making extensive use of $h_K$ in the theory of complex multiplication, and he uses Jacobi's elliptic function $\mathrm{sn}(z)$ as a substitute. Takagi, who devotes the final sections of his famous article on general class field theory to the

special case of imaginary quadratic $K$, follows this detour and provides explicit generators for $K_{\mathrm{ab}}$ using Jacobi functions [17, Satz 37]. A complete description of $K_{\mathrm{ab}}$ using Weber functions is finally obtained by Hasse [7]. It reads as follows.

**2.2. Theorem.** *Let $K$ be imaginary quadratic with ring of integers $\mathcal{O}_K = \mathbf{Z}[\tau_0]$. Then $K_{\mathrm{ab}}$ is generated over $K(j(\tau_0))$ by the values $h_K(\tau)$ of the Weber function $h_K$ at $\tau \in K \setminus \mathcal{O}_K$.*

The second method, which plays a central role in Shimura's version of complex multiplication, sticks to modular functions, but uses infinitely many of them. More precisely, one needs modular functions of higher level as defined in [9, Ch. 6, §3]. These functions form a field $F$, the *modular function field* over $\mathbf{Q}$. The algebraic closure of $\mathbf{Q}$ in $F$ is the maximal cyclotomic extension $\mathbf{Q}_{\mathrm{ab}}$ of $\mathbf{Q}$.

**2.3. Theorem.** *Let $K$ be imaginary quadratic, and pick $\tau \in K \cap \mathbf{H}$. Then $K_{\mathrm{ab}}$ is generated by the finite function values $f(\tau)$, with $f$ ranging over the modular function field $F$.*

Theorems 2.2 and 2.3 are not as different as they may look. One can use *Fricke functions* to generate $F$ over $\mathbf{Q}$ as in [9, Ch. 9, §3], and take $\tau$ in 2.3 equal to the value $\tau_0$ from 2.2. Then the values of the various Fricke functions evaluated at $\tau_0$ coincide with the values of the Weber function $h_K$ on $K \setminus \mathcal{O}_K$.

When comparing theorem 2.3, which fixes the argument but not the function, to the Kronecker-Weber theorem 1.1, one may wonder naively whether it is possible to replace the $j$-function in 2.1 by some other modular function $f \in F$ such that the simplicity of 1.1 is regained. Heinz Söhngen, a student of Emil Artin, showed in his thesis [15, Satz IV] that this is not possible.

**2.4. Theorem.** *Let $f \in F$ be any modular function, and let $K_f$ be the extension of $K$ that is obtained by adjoining the finite function values $f(\tau)$ for $\tau \in K \cap \mathbf{H}$ to $K$. Then $K_{\mathrm{ab}}$ has infinite degree over the compositum $K_f\mathbf{Q}_{\mathrm{ab}}$.*

In order to be useful in practice, the theorems 2.2 and 2.3 need to be complemented by a description of the Galois theoretic properties of the generators of $K_{\mathrm{ab}}$. We will focus on Shimura's formulation [14], which has a reputation of being the most 'abstract' approach to complex multiplication. This is partly due to the heavy notation in which it is often couched. In addition, most expositions first go through a somewhat cumbersome description of the multiplication of complex lattices by idèles.

In the next section, we furnish a concise description of Shimura's main results. It reduces notation to a minimum and avoids the usual 'componentwise' operations on idèles by a systematic use of profinite completions. The final three sections of the paper illustrate that this 'abstract' version is both an ideal instrument to obtain smooth conceptual proofs and a powerful algorithmic tool. In section 4, we prove a general result (4.4) that readily implies theorems 2.1 and 2.4. It encompasses most of Söhngen's results [15] on ray class fields for orders in a rather painless way. Sections 5 and 6, which extend the recent work of Alice Gee and the author [5, 6] to arbitrary orders, deal with the construction of class invariants and the explicit generation of ring class fields. They show that Shimura reciprocity not only completely removes the mystery that long surrounded Weber's claims on class invariants, but also yields the Galois theoretic properties of such invariants that are needed for their use in computational settings.

## §3. Shimura reciprocity

*Shimura's reciprocity law* for $K$ gives the action of the absolute abelian Galois group $\mathrm{Gal}(K_{\mathrm{ab}}/K)$ of $K$ on the 'singular value' $f(\tau)$ of a modular function $f \in F$ at $\tau \in K \cap \mathbf{H}$. It combines *Artin's reciprocity law* from class field theory, which describes $\mathrm{Gal}(K_{\mathrm{ab}}/K)$ as a quotient of the idèle group of $K$, with the Galois theory of the field $F$ of modular functions. It defines, for a *fixed* singular modulus $\tau \in K \cap \mathbf{H}$, an action of the idèle group of $K$ on the modular function field $F$ such that we have for every idèle $x$ the innocuously looking identity

$$(f(\tau))^x = (f^x)(\tau). \tag{3.1}$$

In this 'minimal notation version' of Shimura's reciprocity law the action of $x$ on the value $f(\tau)$ is via its Artin symbol, and the action of $x$ on $f \in F$ is explained in this section. We avoid explicit multiplication of lattices by idèles by defining the action first for suitable subgroups.

A large subgroup of $\mathrm{Aut}(F)$ is obtained by considering $F$ as an extension of the field $F_1 = \mathbf{Q}(j)$ of modular functions of level 1 over $\mathbf{Q}$. One has $F = \bigcup_{N \geq 1} F_N$, where $F_N$ is the field of modular functions of level $N$ over $\mathbf{Q}$. One can view $F_N$ as the function field of the modular curve $X(N)$ over the cyclotomic field $\mathbf{Q}(\zeta_N)$. Over the complex numbers, the curve $X(N)$ is a Galois cover with group $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})/\pm 1$ of the $j$-line $X(1) = \mathbf{P}^1$. When working over $\mathbf{Q}$, one has an isomorphism $\mathrm{Gal}(F_N/F_1) \cong \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})/\pm 1$. It may be obtained by combining the 'geometric action' of the subgroup $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})/\pm 1$ with the 'arithmetic

action' via the determinant map on the $N$-th roots of unity, cf. [9, Ch. 6, §3]. The restriction maps between the fields $F_N$ correspond to the natural maps between the groups $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})/\pm 1$, and one finds the subgroup

$$\mathrm{Gal}(F/\mathbf{Q}(j)) = \mathrm{GL}_2(\widehat{\mathbf{Z}})/\pm 1$$

of $\mathrm{Aut}(F)$ by taking the projective limit.

We now pick an element $\tau \in K \cap \mathbf{H}$, and write $AX^2 + BX + C$ with $A \in \mathbf{Z}_{>0}$ for the irreducible polynomial of $\tau$ in $\mathbf{Z}[X]$. Clearly, we have $K = \mathbf{Q}(\sqrt{D})$ with $D = B^2 - 4AC$. One easily checks that the lattice $L_\tau = \mathbf{Z} \cdot \tau + \mathbf{Z}$ corresponding to $\tau$ is an invertible $\mathcal{O}$-ideal for the quadratic order $\mathcal{O} = \mathbf{Z}[A\tau]$ of discriminant $D$.

Corresponding to the subgroup $\mathrm{Gal}(F/\mathbf{Q}(j)) \subset \mathrm{Aut}(F)$, there is the subgroup $\mathrm{Gal}(K_{\mathrm{ab}}/K(j(\tau)) \subset \mathrm{Gal}(K_{\mathrm{ab}}/K)$. It is well-known that $H_{\mathcal{O}} = K(j(\tau))$ is the *ring class field* of $K$ corresponding to the order $\mathcal{O}$. It is a finite abelian extension of $K$ whose Galois group over $K$ is isomorphic to the class group of the order $\mathcal{O}$. If $\tau$ generates the ring of integers $\mathcal{O}_K$ of $K$ over $\mathbf{Z}$, then $K(j(\tau))$ is the *Hilbert class field* $H = K(j(\tau_0))$ of $K$ occurring in theorem 2.2.

It follows from class field theory that we may describe $\mathrm{Gal}(K_{\mathrm{ab}}/K)$ by an exact sequence

$$1 \longrightarrow K^* \longrightarrow \widehat{K}^* \xrightarrow{\Psi} \mathrm{Gal}(K_{\mathrm{ab}}/K) \longrightarrow 1.$$

Here $\Psi$ denotes the Artin map on the group of *finite* $K$-idèles $\widehat{K}^* = (K \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}})^*$. Note that $\widehat{K} = K \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$ is the ring of finite adèles of $K$, and that $\widehat{K}^*$ is the quotient of the full idèle group of $K$ obtained by 'forgetting' the infinite component $\mathbf{C}^*$. For imaginary quadratic $K$, this amounts to dividing out the connected component of the identity element. Inside $\widehat{K}$ we have the profinite completion

$$\widehat{\mathcal{O}} = \varprojlim_N (\mathcal{O}/N\mathcal{O}) = \mathcal{O} \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}} = \widehat{\mathbf{Z}} + \widehat{\mathbf{Z}} \cdot A\tau$$

of the order $\mathcal{O}$. Its unit group $\widehat{\mathcal{O}}^* \subset \widehat{K}^*$ maps under the Artin map unto $\mathrm{Gal}(K_{\mathrm{ab}}/H_{\mathcal{O}})$, so we have a diagram with exact rows

(3.2)

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & \widehat{\mathcal{O}}^* & \xrightarrow{\Psi} & \mathrm{Gal}(K_{\mathrm{ab}}/H_{\mathcal{O}}) & \longrightarrow & 1 \\ & & & & \downarrow g_\tau & & & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathrm{GL}_2(\widehat{\mathbf{Z}}) & \longrightarrow & \mathrm{Gal}(F/\mathbf{Q}(j)) & \longrightarrow & 1. \end{array}$$

The connecting homomorphism $g_\tau : \widehat{\mathcal{O}}^* \to \mathrm{GL}_2(\widehat{\mathbf{Z}})$ sends the idèle $x \in \widehat{\mathcal{O}}^*$ to the *transpose* of the matrix representing the multiplication by

$x$ on the free $\widehat{\mathbf{Z}}$-module $\widehat{\mathbf{Z}} \cdot \tau + \widehat{\mathbf{Z}}$ with respect to the basis $[\tau, 1]$. The defining identity for $g_\tau(x)$, which is often written as $g_\tau(x)\binom{\tau}{1} = \binom{x\tau}{x}$, may be expanded into the explicit formula

$$g_\tau : \quad x = sA\tau + t \longmapsto \begin{pmatrix} t - Bs & -Cs \\ sA & t \end{pmatrix}. \tag{3.3}$$

The map $g = g_\tau$ yields an action of $\widehat{\mathcal{O}}^*$ on $F$, and the Galois conjugate $(f(\tau))^x$ of $f(\tau)$ under the Artin symbol $\Psi(x) \in \mathrm{Gal}(K_{\mathrm{ab}}/H_{\mathcal{O}})$ of $x \in \widehat{\mathcal{O}}^*$ can be computed from the reciprocity relation

$$(f(\tau))^x = (f^{g(x^{-1})})(\tau). \tag{3.4}$$

Whenever $F$ is Galois over $\mathbf{Q}(f)$, we have the fundamental equivalence

$$(f(\tau))^x = f(\tau) \quad \Longleftrightarrow \quad f^{g(x)} = f. \tag{3.5}$$

Note that only the implication $\Leftarrow$ is immediate from (3.4), the implication $\Rightarrow$ requires an additional argument [14, prop. 6.33].

The content of Shimura's reciprocity law is that the natural $\mathbf{Q}$-linear extension of the map $g_\tau$ in (3.3), which is a homomorphism

$$g_\tau : \widehat{K}^* = (\widehat{\mathcal{O}} \otimes_{\mathbf{Z}} \mathbf{Q})^* \longrightarrow \mathrm{GL}_2(\widehat{\mathbf{Q}}),$$

connects the exact rows in the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^* & \longrightarrow & \widehat{K}^* & \xrightarrow{\Psi} & \mathrm{Gal}(K_{\mathrm{ab}}/K) & \longrightarrow & 1 \\ & & & & \downarrow g_\tau & & & & \\ 1 & \longrightarrow & \mathbf{Q}^* & \longrightarrow & \mathrm{GL}_2(\widehat{\mathbf{Q}}) & \longrightarrow & \mathrm{Aut}(F) & \longrightarrow & 1 \end{array} \tag{3.6}$$

extending (3.2) in such a way that (3.4) and (3.5) hold unchanged for this map.

The statement above is not complete without a description of the action of the group $\mathrm{GL}_2(\widehat{\mathbf{Q}})$ of of invertible $2 \times 2$-matrices over the finite adèle ring $\widehat{\mathbf{Q}} = \mathbf{Q} \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$ of $\mathbf{Q}$ on $F$. It is obtained as in [9, Ch. 7] by writing the elements of this group in the form $u \cdot \alpha$, with $u \in \mathrm{GL}_2(\widehat{\mathbf{Z}})$ in the subgroup for which we know already how it acts, and $\alpha \in \mathrm{GL}_2(\mathbf{Q})^+$ a rational $2 \times 2$-matrix of positive determinant. Note that $u$ and $\alpha$ are not uniquely determined by the product $u \cdot \alpha$, since we have

$$\mathrm{GL}_2(\widehat{\mathbf{Z}}) \cap \mathrm{GL}_2(\mathbf{Q})^+ = \mathrm{SL}_2(\mathbf{Z}) \subset \mathrm{GL}_2(\widehat{\mathbf{Q}}).$$

Nevertheless, the natural action of $\mathrm{GL}_2(\mathbf{Q})^+$ on $\mathbf{H}$ via fractional linear transformations induces a right action of $\mathrm{GL}_2(\mathbf{Q})^+$ on $F$ that can be

combined with the action of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ on $F$. A well-defined action of $\mathrm{GL}_2(\widehat{\mathbf{Q}})$ on $F$ is obtained by putting

$$f^{u\cdot\alpha} = (f^u)^\alpha. \tag{3.7}$$

## §4. Ray class fields for orders

As our presentation in the previous section indicates, one can generate $K_{\mathrm{ab}}$ over $K$ in two steps. One first picks a quadratic order $\mathcal{O} \subset K$, and considers the ring class field $H_{\mathcal{O}}$ of $\mathcal{O}$. This is the finite abelian extension of $K$ generated by the $j$-invariant $j(\mathcal{O})$ of the order. The Galois group $\mathrm{Gal}(H_{\mathcal{O}}/K)$ is isomorphic to the class group $Cl(\mathcal{O})$ of the order $\mathcal{O}$, with the ideal class $[\mathfrak{a}] \in Cl(\mathcal{O})$ acting on $j(\mathcal{O})$ by

$$j(\mathcal{O})^{[\mathfrak{a}]} = j(\mathfrak{a}^{-1}). \tag{4.1}$$

The top row of (3.2) shows that the Galois group of $K_{\mathrm{ab}}$ over $H_{\mathcal{O}}$ has a rather uncomplicated structure: as $\mathcal{O}^*$ is a finite group consisting of the roots of unity in $\mathcal{O}$, the group $\mathrm{Gal}(K_{\mathrm{ab}}/H_{\mathcal{O}})$ is essentially the unit group of the profinite completion $\widehat{\mathcal{O}}$ of $\mathcal{O}$. This means that $K_{\mathrm{ab}}$ can be obtained as the union of the finite extensions $H_{N,\mathcal{O}}$ of $H_{\mathcal{O}}$ corresponding to the finite quotients

$$\widehat{\mathcal{O}}^* \twoheadrightarrow (\widehat{\mathcal{O}}/N\widehat{\mathcal{O}})^* = (\mathcal{O}/N\mathcal{O})^* \tag{4.2}$$

of $\widehat{\mathcal{O}}^*$ for $N \in \mathbf{Z}_{\geq 1}$. We call $H_{N,\mathcal{O}}$ the *ray class field* of conductor $N$ for the order $\mathcal{O}$. Its Galois group over $H_{\mathcal{O}}$ is isomorphic to $(\mathcal{O}/N\mathcal{O})^*/\mathrm{im}[\mathcal{O}^*]$. If $\mathcal{O}$ is the maximal order of $K$, then $H_{N,\mathcal{O}}$ is the ray class field of conductor $N$ of $K$. We clearly have $H_{1,\mathcal{O}} = H_{\mathcal{O}}$.

Let $\tau \in K \cap \mathbf{H}$ be as in the previous section, and $\mathcal{O}$ the order corresponding to the lattice $[\tau, 1]$. For any $N \in \mathbf{Z}_{\geq 1}$, we obtain from (3.2) a diagram with exact rows

$$\begin{array}{ccccccccc} & \mathcal{O}^* & \longrightarrow & (\mathcal{O}/N\mathcal{O})^* & \longrightarrow & \mathrm{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}}) & \longrightarrow & 1 \\ & & & \downarrow \overline{g}_\tau & & & & \\ \{\pm 1\} & \longrightarrow & \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z}) & \longrightarrow & \mathrm{Gal}(F_N/\mathbf{Q}(j)) & \longrightarrow & 1 & & \end{array} \tag{4.3}$$

in which all groups are finite. Here $\overline{g}_\tau$ is the natural reduction modulo $N$ of the map $g_\tau$ in (3.2) and (3.3), and $F_N$ is the field of modular functions of level $N$.

It is clear from (3.4) that for every modular function $f \in F_N$ of level $N$, the value $f(\tau)$ is contained in the ray class field $H_{N,\mathcal{O}}$ of conductor $N$ for the order $\mathcal{O}$ corresponding to $\tau$. In fact, a standard argument as

in [9, p. 128] shows that the extension of $H_{\mathcal{O}}$ generated by the values $f(\tau)$ for all $f \in F_N$ is *equal* to $H_{N,\mathcal{O}}$. In fact, it suffices to adjoin the value of the Weber function for the elliptic curve $\mathbf{C}/L_\tau$ at a generator of the cyclic $\mathcal{O}$-module $\frac{1}{N}L_\tau/L_\tau$.

Let $L_N \subset K_{\mathrm{ab}}$ be the field obtained by adjoining to $K$ all the finite function values $f(\tau)$, with $f$ ranging over $F_N$ and $\tau$ ranging over $K \cap \mathbf{H}$. As all orders $\mathcal{O} \subset K$ occur as the multiplyer ring of a lattice $L_\tau$, we have

$$L_N = \varinjlim H_{N,\mathcal{O}} \subset K_{\mathrm{ab}},$$

where the injective limit is taken over all orders $\mathcal{O} \subset K$.

Writing $\mathcal{O}_p = \mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Z}_p$, we have $\widehat{\mathcal{O}}^* = \prod_p \mathcal{O}_p^* \subset \widehat{K}^*$. The kernel of the natural map $\widehat{\mathcal{O}}^* \twoheadrightarrow (\mathcal{O}/N\mathcal{O})^*$ in (4.2) equals

$$\widehat{\mathcal{O}}^*_{(N)} = \{x \in \widehat{\mathcal{O}}^* : x \equiv 1 \bmod^* N\} = \prod\nolimits_{p \nmid N} \mathcal{O}_p^* \times \prod\nolimits_{p \mid N} (1 + N\mathcal{O}_p),$$

so an inclusion of orders yields an inclusion of kernels and we find

$$\mathcal{O}_1 \subset \mathcal{O}_2 \Longrightarrow H_{N,\mathcal{O}_1} \supset H_{N,\mathcal{O}_2}.$$

For $N = 1$ this is the *Anordnungssatz* for ring class fields [3, §19].

The field $L_N$ is the infinite extension of $K$ corresponding to the subgroup

$$\bigcap_{\mathcal{O} \subset K} \widehat{\mathcal{O}}^*_{(N)} = \widehat{\mathbf{Z}}^*_{(N)} = \{x \in \widehat{\mathbf{Z}}^* : x \equiv 1 \bmod^* N\}$$
$$= \prod\nolimits_{p \nmid N} \mathbf{Z}_p^* \times \prod\nolimits_{p \mid N} (1 + N\mathbf{Z}_p).$$

By class field theory, the Artin symbol of an idèle $x \in \widehat{\mathcal{O}}^*$ acts trivially on the maximal cyclotomic extension $\mathbf{Q}_{\mathrm{ab}}$ of $\mathbf{Q}$ if and only if its image under the norm map $\widehat{\mathcal{O}}^* \to \widehat{\mathbf{Z}}^* \cong \mathrm{Gal}(\mathbf{Q}_{\mathrm{ab}}/\mathbf{Q})$ is trivial. As the norm of an element $x \in \widehat{\mathbf{Z}}^* \subset \widehat{\mathcal{O}}^*$ is simply its square, we find the following Galois theoretic description of the compositum $L_N\mathbf{Q}_{\mathrm{ab}} \subset K_{\mathrm{ab}}$.

**4.4. Theorem.** *Let $L_N \subset K_{\mathrm{ab}}$ be the field obtained by adjoining the finite values of the modular functions of level $N$ at the points $\tau \in K \cap \mathbf{H}$ to $K$. Then the restriction of the Artin map $\widehat{K}^* \xrightarrow{\Psi} \mathrm{Gal}(K_{\mathrm{ab}}/K)$ to the subgroup $\widehat{\mathbf{Z}}^* \subset \widehat{K}^*$ induces a surjection*

$$\widehat{\mathbf{Z}}^*_{(N)}[2] = \{x \in \widehat{\mathbf{Z}}^* : x \equiv 1 \bmod^* N \text{ and } x^2 = 1\} \longrightarrow \mathrm{Gal}(K_{\mathrm{ab}}/L_N\mathbf{Q}_{\mathrm{ab}})$$

*with kernel* $\widehat{\mathbf{Z}}^*_{(N)}[2] \cap \{\pm 1\}$. *In particular,* $K_{\mathrm{ab}}/L_N\mathbf{Q}_{\mathrm{ab}}$ *is an infinite abelian extension of exponent* 2.

The map in 4.4 is an isomorphism for $N \geq 3$ and has a kernel of order 2 for $N \leq 2$.

For $N = 1$ we have $F_N = \mathbf{Q}(j)$, so $L_1 = K_j$ is the field occurring in theorem 2.1. This yields the following precise version of theorem 2.1.

**4.5. Corollary.** *Let* $K_j$ *be as in* 2.1. *Then there is a natural exact sequence*

$$1 \longrightarrow \{\pm 1\} \longrightarrow \bigoplus_{p \text{ prime}} \{\pm 1\} \longrightarrow \mathrm{Gal}(K_{\mathrm{ab}}/K_j\mathbf{Q}_{\mathrm{ab}}) \longrightarrow 1.$$

It follows from 4.4 that theorem 2.1 cannot be improved in a substantial way by replacing $j$ by some other modular function $f \in F$. In fact, by employing finitely many modular functions one always generates a subfield of the field $L_N$ for some $N \in \mathbf{Z}_{\geq 1}$, and $L_N\mathbf{Q}_{\mathrm{ab}}$ is a finite extension of $K_j\mathbf{Q}_{\mathrm{ab}}$. In particular, we see that Söhngen's theorem 2.4 is an immediate corollary of 4.4.

## §5. Class invariants

We have seen that the ring class field $H_{\mathcal{O}}$ corresponding to a quadratic order $\mathcal{O} \subset K$ is obtained by adjoining the value $j(\mathcal{O})$ to $K$. The irreducible polynomial $\phi_{\mathcal{O}}$ of $j(\mathcal{O})$ over $K$, which is known to be a polynomial in $\mathbf{Z}[X]$ with highest coefficient 1, is the *class polynomial* of the order $\mathcal{O}$. The zeroes of $\phi_{\mathcal{O}}$ are the $j$-values $j(\mathfrak{a})$ of the ideal classes $[\mathfrak{a}] \in Cl(\mathcal{O})$, and we can numerically determine $\phi_{\mathcal{O}}$ from the complex approximations of its zeroes. This is much faster than the algebraic determination of $\phi_{\mathcal{O}}$ as the divisor of some modular polynomial $\Phi_m(X, X) \in \mathbf{Z}[X]$ as in [2, p. 297], which is only computationally feasible for a few very small $\mathcal{O}$.

Weber noticed already that class polynomials have huge coefficients. In fact, they are so large that they are never useful in actually computing Hilbert class fields. For instance, for the quadratic field of discriminant

$-95$ the maximal order $\mathcal{O}$ has class polynomial

$$\begin{aligned}\phi_{\mathcal{O}} = X^8 &+ 19874477919500\,X^7 - 688170786018119250\,X^6 \\ &+ 39501357586714451925820312 5\,X^5 \\ &- 13089776536501963407329479984375\,X^4 \\ &+ 35216332285866472676272522829492 1875\,X^3 \\ &- 14374159398715735745728390109712480468 75\,X^2 \\ &+ 21106316391166752679539154247640568847656 25\,X \\ &+ 10778969457654001000297677199617714868164 0625.\end{aligned}$$

It was discovered by Weber that in some cases, 'small' elliptic functions $f$ of level $N > 1$ can be used to generate $H_{\mathcal{O}}$ as well. In the example above, one can take for $f$ the Weber function $\sqrt{2}\frac{\eta(2z)}{\eta(z)}$ of level 48 or the function $\frac{1}{\sqrt{5}}(\frac{\eta((z+3)/5)}{\eta(z)})^2$ of level 120. When evaluated at suitable $\tau \in K \cap \mathbf{H}$, these $f$ yield elements $f(\tau) \in H_{\mathcal{O}}$ with irreducible polynomials

$$X^8 - X^7 + X^5 - 2X^4 - X^3 + 2X^2 + 2X - 1$$
$$X^8 - 3X^7 + X^6 - 8X^5 - X^4 - 8X^3 + X^2 - 3X + 1$$

over $K$. In such cases $f(\tau)$ is said to be a *class invariant* of $\mathcal{O}$.

Weber used several modular functions of higher level in a rather ad hoc manner to compute by hand a number of class invariants. His computations of class invariants in [18] are a mix of theorems, tricks, numerical observations, conjectures and open questions. Among them is the famous *class number one problem*, which already goes back to Gauss. Heegner's 1954 solution of the problem, which proved the completeness of Gauss's list of class number one discriminants, was not accepted because it relied heavily on the observations of Weber, which were not in all cases theorems. Only when Baker and Stark gave independent proofs in 1968 of the same result, it was realized that Heegner's proof was essentially correct [16]. The renewed interest in Weber's class invariants resulting from this led to new proofs and additional results [1, 16], but not to a systematic way to deal with such questions.

Shimura reciprocity enables us to determine in a rather mechanical way, for any given modular function $f \in F$, the set of orders $\mathcal{O} = \mathbf{Z}[\tau]$ for which the value $f(\tau)$ lies in the ring class field $H_{\mathcal{O}}$. As $\mathcal{O}$ determines $\tau$ only up to an additive constant $k \in \mathbf{Z}$ and the value $f(\tau)$ may depend on $k$ for functions $f \in F$ of higher level, we fix $\tau$ to be the 'standard generator' of $\mathcal{O} \subset K$ having trace $\mathrm{Tr}_{K/\mathbf{Q}}(\tau) \in \{0, 1\}$. We will show that

with this normalization, the set of orders $\mathcal{O}$ for which $f(\tau)$ is a class invariant for $\mathcal{O}$ can be described in terms of congruence conditions on the discriminant $D = \mathrm{disc}(\mathcal{O})$ modulo some integer $n(f)$. In fact, $n(f)$ divides $4N$ if $f$ has level $N$.

Suppose we are given a modular function $f$ in the field $F_N$ of modular functions of level $N$, together with the explicit $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$-action on $f$. In practice, this means that we know the action of the standard generators $S, T \in \mathrm{SL}_2(\mathbf{Z})/\pm 1$ on $f$ and the action of the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}) = (\mathbf{Z}/N\mathbf{Z})^*$ on the Fourier coefficients of $f$. We let $\mathcal{O} = \mathbf{Z}[\tau]$ be the quadratic order of discriminant $D$, and $X^2 + BX + C \in \mathbf{Z}[X]$ the irreducible polynomial of $\tau$, and impose the mild restriction that $\mathbf{Q}(f) \subset F$ be Galois.

From the top row of (4.3) we see that the value $f(\tau)$, which a priori only is known to lie in the ray class field $H_{N,\mathcal{O}}$ of conductor $N$ for $\mathcal{O}$, is a class invariant for $\mathcal{O}$ if and only if the Artin symbols of all elements of $(\mathcal{O}/N\mathcal{O})^*$ leave $f(\tau)$ fixed. Shimura's equivalence (3.5) shows that this is equivalent to the requirement that $\overline{g}_\tau(x)$ fixes $f$ for all $x \in (\mathcal{O}/N\mathcal{O})^*$. Thus, we only need to compute a set of generators $x_i$ for the finite abelian group $(\mathcal{O}/N\mathcal{O})^*$, compute their $\overline{g}_\tau$-images

$$\overline{g}_\tau(x_i) \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$$

using (3.3), and check whether these elements of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ fix $f \in F_N$.

If one finds that $f$ is not left invariant by all $\overline{g}_\tau(x_i)$, a look at the $\overline{g}_\tau[(\mathcal{O}/N\mathcal{O})^*]$-orbit of $f$ often suffices to see which modification of $f$ does have this property. There are many examples in [5] where a small power of $f$, if necessary multiplied by a well chosen root of unity, turns out to have the desired property. We refer to [5] and [6] for a large number of examples.

The computation of generators $x_i$ of $(\mathcal{O}/N\mathcal{O})^*$ and their $\overline{g}_\tau$-images in the group $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ only depends on the residue class modulo $N$ of the coefficients of the irreducible polynomial $X^2+BX+C$ of $\tau$. Thus, if $\tau$ is the standard generator of $\mathcal{O}$ having $B = -\mathrm{Tr}_{K/\mathbf{Q}}(\tau_0) \in \{0, 1\}$, the pair $(B \bmod N, C \bmod N)$ only depends on the residue class of $D = B^2 - 4C$ modulo $4N$. This proves our claim for $n(f)$ made above.

There is a large supply of classical modular functions $f$ of higher level that are, in a sense that can be made precise, 'smaller' than the $j$-function, and to which the 'algorithm' above can be applied. The functions $\gamma_3 = \sqrt{j - 1728}$ and $\gamma_2 = \sqrt[3]{j}$ of level 2 and 3 are the simplest and most classical examples. The Weber functions $\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2$ of level 48 analyzed in [13] and, more generally, the normalized quotients of Dedekind $\eta$-functions in [5, 6], are other examples of small modular functions. They

give rise to integral class invariants for which the irreducible polynomials are much smaller than the class polynomials.

## §6. Computation of ring class fields

The method in the preceding section enables us to prove in a systematic way that certain singular values $f(\tau)$ lie in the ring class field $H_{\mathcal{O}}$ corresponding to the order $\mathcal{O} = \mathbf{Z}[\tau]$. It does not tell us how to find the conjugates of $f(\tau)$ over $K$. This is indispensable in *computational class field theory*, where one wants to compute the irreducible polynomial of $f(\tau)$ over $K$ in order to obtain an explicit generating polynomial for $H_{\mathcal{O}}$. The need for explicit conjugates also arises in other situations, e.g. in primality proving [11, p. 119].

By class field theory, the Galois group $\mathrm{Gal}(H_{\mathcal{O}}/K)$ is isomorphic to the class group $Cl(\mathcal{O})$ of $\mathcal{O}$, and the elements of this group can conveniently be listed as reduced primitive binary quadratic forms $[a, b, c]$ of discriminant $D = \mathrm{disc}(\mathcal{O})$. For our purposes, it suffices to know that these are triples $[a, b, c]$ of integers satisfying $\gcd(a, b, c) = 1$ and $b^2 - 4ac = D$. They are reduced if they satisfy the inequalities $|b| \leq a \leq c$ and, in case we have $|b| = a$ or $a = c$, also $b \geq 0$. For any given discriminant $D < 0$, there are only finitely many such triples, and they are easily enumerated if $D$ is not too large. The correspondence between reduced forms and elements of the class group is obtained by associating to $[a, b, c]$ the class of the ideal with $\mathbf{Z}$-basis $[\frac{-b+\sqrt{D}}{2}, a]$. Note that $[a, b, c]$ and $[a, -b, c]$ correspond to inverse ideal classes.

The classical formula (4.1) for the action of the class group of $\mathcal{O} = \mathbf{Z}[\tau]$ on the canonical generator $j(\tau)$ of $H_{\mathcal{O}}$ over $K$ can be rewritten as

$$j(\tau)^{[a,-b,c]} = j(\tfrac{-b+\sqrt{D}}{2a}).$$

For a general modular function $f \in F$ with $f(\tau) \in H_{\mathcal{O}}$, Shimura reciprocity enables us to determine the conjugate $\tilde{f}$ of $f$ over $\mathbf{Q}(j)$ for which we have

$$f(\tau)^{[a,-b,c]} = \tilde{f}(\tfrac{-b+\sqrt{D}}{2a}). \tag{6.1}$$

This is done by picking for every class $[\mathfrak{a}] \in Cl(\mathcal{O})$ an idèle $x \in \widehat{K}^*$ that generates the $\widehat{\mathcal{O}}$-ideal $\mathfrak{a} \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$. Such an element $x$ exists since every invertible $\mathcal{O}$-ideal is locally principal. It is only determined up to multiplication by elements of $\widehat{\mathcal{O}}^*$. As in the case of (3.3), this abstract description of $x$ may be translated into a simple explicit recipe. If $\mathfrak{a}$ is

the invertible $\mathcal{O}$-ideal with $\mathbf{Z}$-basis $[\frac{-b+\sqrt{D}}{2}, a]$ corresponding to $[a,b,c]$, one has $\widehat{\mathfrak{a}} = x\widehat{\mathcal{O}}$ for the idèle $x = (x_p)_p \in \widehat{K}^*$ with components

$$x_p = \begin{cases} a & \text{if } p \nmid a \\ \frac{-b+\sqrt{D}}{2} & \text{if } p \mid a \text{ and } p \nmid c \\ \frac{-b+\sqrt{D}}{2} - a & \text{if } p \mid a \text{ and } p \mid c \end{cases} \tag{6.2}$$

for each rational prime $p$. The Artin symbol of the idèle $x$ acts on $H_{\mathcal{O}}$ as the ideal class $[\mathfrak{a}] \in Cl(\mathcal{O})$, so we have $f(\tau)^{[a,b,c]} = f(\tau)^x$ for this $x$. Applying the reciprocity relation (3.4) for $x^{-1}$ and $g = g_\tau$, we find

$$f(\tau)^{[a,-b,c]} = (f^{g_\tau(x)})(\tau). \tag{6.3}$$

The element $g_\tau(x) \in \mathrm{GL}_2(\widehat{\mathbf{Q}})$ is only determined by $[a,-b,c]$ up to left multiplication by elements $u \in g_\tau[\widehat{\mathcal{O}}^*] \subset \mathrm{GL}_2(\widehat{\mathbf{Z}})$. However, the fact that $f(\tau)$ is a class invariant exactly means that we have $f^u = f$ for such $u$, so (3.7) shows that the right hand side of (6.3) does not depend on the choice of the generator $x$ of $\widehat{\mathfrak{a}}$.

Let $M \in \mathrm{GL}_2(\mathbf{Q})^+ \subset \mathrm{GL}_2(\widehat{\mathbf{Q}})$ be the transpose of the $\widehat{\mathbf{Q}}$-linear map on $\widehat{K} = \widehat{\mathbf{Q}} \cdot \tau + \widehat{\mathbf{Q}} \cdot 1$ that maps the basis $[\tau, 1]$ to $[\frac{-b+\sqrt{D}}{2}, a]$. Then the action of $M$ on $\mathbf{H}$ satisfies $M(\tau) = \frac{-b+\sqrt{D}}{2a}$. Putting $u_x = g_\tau(x) \cdot M^{-1} \in \mathrm{GL}_2(\widehat{\mathbf{Q}})$, we can rewrite (6.3) as

$$f(\tau)^{[a,-b,c]} = f^{g_\tau(x)\cdot M^{-1}}(\tfrac{-b+\sqrt{D}}{2a}) = f_\tau^{u_x}(\tfrac{-b+\sqrt{D}}{2a}). \tag{6.4}$$

Comparing the defining identity $M\binom{\tau}{1} = \binom{(-b+\sqrt{D})/2}{a}$ for $M$ to that for $g_\tau(x)$, we see that both elements are transposes of $\widehat{\mathbf{Q}}$-linear maps on $\widehat{K} = \widehat{\mathbf{Q}} \cdot \tau + \widehat{\mathbf{Q}} \cdot 1$ that map the $\widehat{\mathbf{Z}}$-lattice $\widehat{\mathcal{O}} = \widehat{\mathbf{Z}} \cdot \tau + \widehat{\mathbf{Z}} \cdot 1$ onto $\widehat{\mathfrak{a}} = x\widehat{\mathcal{O}}$. It follows that $u_x = g_\tau(x) \cdot M^{-1}$, being the transpose of an element that stabilizes the $\widehat{\mathbf{Z}}$-lattice $\widehat{\mathcal{O}} \subset \widehat{K}$ spanned by the basis $[\tau, 1]$, is actually in $\mathrm{GL}_2(\widehat{\mathbf{Z}})$. This means that $f^{u_x} = \tilde{f}$ is a conjugate of $f$ over $\mathbf{Q}(j)$. Thus (6.4) tells us which conjugate $\tilde{f}$ of $f$ we have to take in (6.1).

Computing the function $\tilde{f} = f^{u_x}$ from $f$ is another instance of the problem considered in the previous section. Choosing $x$ as in (6.2), it is straightforward to write down an explicit formula for the components of $u_x \in \mathrm{GL}_2(\widehat{\mathbf{Z}})$ at each $\mathbf{Z}_p$ as in [5]. As before, all we really need is the image of $u_x$ in the finite group $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, with $N$ the level of $f$.

## References


[1] B. Birch, Weber's class invariants, Mathematika, **16** (1969), 283–294.

[2] D. A. Cox, "Primes of the form $x^2 + ny^2$", Wiley-Interscience, 1989.

[3] M. Deuring, Die Klassenkörper der komplexen Multiplikation, in "Enzyklopädie der Math. Wiss., Band I, 2. Teil, Heft 10, Teil II", Teubner, 1958.

[4] R. Fueter, Abelsche Gleichungen in quadratisch-imaginären Zahlkörpern, Math. Annalen, **75** (1914), 177–255.

[5] A. C. P. Gee, Class fields by Shimura reciprocity, thesis, University of Amsterdam (2000).

[6] A. C. P. Gee and P. Stevenhagen, Generating class fields using Shimura reciprocity, in "Algorithmic Number Theory", (J. P. Buhler, ed.), Springer LNCS 1423, 1998, pp. 441–453.

[7] H. Hasse, Neue Begründung der komplexen Multiplikation. I, J. reine angew. Math., **157** (1927), 115–139; II, J. reine angew. Math., **165** (1931), 64–88.

[8] D. R. Hayes, A brief introduction to Drinfeld modules, in "The arithmetic of function fields", (D. Goss, D. R. Hayes, M. I. Rosen, eds.), de Gruyter, 1992.

[9] S. Lang, "Elliptic functions", 2nd edition, Springer Graduate Text in Mathematics 112, 1987.

[10] J. Lubin, J. T. Tate, Formal complex multiplication in local fields, Ann. of Math., **81** no.2 (1965), 380–387.

[11] F. Morain, Primality proving using elliptic curves: an update, in "Algorithmic Number Theory", (J. P. Buhler, ed.), Springer LNCS 1423, 1998, pp. 111–127.

[12] W. Raskind, Abelian class field theory of arithmetic schemes, in "$K$-theory and Algebraic Geometry": Connection with Quadratic Forms and Division Algebras, AMS Proc. of Symp. in Pure Math., **58** no.1 (1995), 85–187.

[13] R. Schertz, Die singulären Werte der Weberschen Funktionen $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$, $\gamma_2$, $\gamma_3$, J. Reine Angew. Math., **286/287** (1976), 46–74.

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

[15] H. Söhngen, Zur komplexen Multiplikation, Math. Annalen, **111** (1935), 302–328.

[16] H. M. Stark, On a "gap" in a theorem of Heegner, J. Number Theory, **1** (1969), 16–27.

[17] T. Takagi, Über eine Theorie des relativ Abel'schen Zahlkörpers, J. College of Science, **41** no.9 (1920), 1–133, Imperial Univ. of Tokyo; in "Collected Works", Iwanami Shoten, 1973, pp. 73–167.

[18] H. Weber, "Lehrbuch der Algebra, vol. III", Chelsea reprint, original edition 1908.

*Mathematisch Instituut*
*Universiteit Leiden*
*Postbus 9512*
*2300 RA Leiden, The Netherlands*
*E-mail address*: psh@math.leidenuniv.nl