Schertz style class invariants for quartic CM fields

Andreas Enge, Marco Streng

Schertz style class invariants for quartic CM fields

Andreas Enge[1] and Marco Streng[2]

6 October 2016

Abstract

A *class invariant* is a CM value of a modular function that lies in a certain unramified class field. We show that Siegel modular functions over $\mathbf{Q}$ for $\Gamma^0(N) \subseteq \mathrm{Sp}_4(\mathbf{Z})$ yield class invariants under some splitting conditions on N. Small class invariants speed up constructions in explicit class field theory and public-key cryptography. Our results generalise results of Schertz's from elliptic curves to abelian varieties and from classical modular functions to Siegel modular functions.

1 Introduction

The values of Siegel modular functions in a CM period matrix $\tau \in \mathbf{H}_g$ lie in an abelian extension of the *reflex field* K^r. Of special interest is the extension $H_{\mathcal{O},\Phi}(1)$ generated by τ-values of modular functions of level 1. For a Siegel modular function f of any level, the value $f(\tau)$ is called a *class invariant* if it satisfies $f(\tau) \in H_{\mathcal{O},\Phi}(1)$.

In the case of dimension $g \leqslant 2$, the field of Siegel modular functions for $\mathrm{Sp}_{2g}(\mathbf{Z})$ on $\mathbf{H}_g$ is generated by the j-invariant ($g = 1$) or absolute Igusa invariants i_1, i_2, i_3 ($g = 2$), whose values are essential to CM constructions in cryptography and explicit class field theory. If f is a function such that for many τ the value $f(\tau)$ is a class invariant of smaller height than $j(\tau)$ or $i_k(\tau)$, then f can replace j or i_k in applications, which significantly increases the range of feasible fields for CM constructions.

Schertz [22] shows in the case $g = 1$ that modular functions for $\Gamma^0(N)$ often give class invariants when the primes dividing N split or ramify in $\mathbf{Q}(\tau)$. We generalise Schertz's results as follows, relying on CM theory and the explicit version of Shimura's reciprocity law of [26] as recalled in §2.

Let f be a Siegel modular function for $\Gamma^0(N)$ defined over $\mathbf{Q}$ in the sense that it is a quotient of Siegel modular forms with Fourier expansion coefficients in $\mathbf{Q}$.

[1]INRIA, LFANT, F-33400 Talence, France
CNRS, IMB, UMR 5251, F-33400 Talence, France
Univ. Bordeaux, IMB, UMR 5251, F-33400 Talence, France
https://www.math.u-bordeaux.fr/~aenge/
andreas.enge@inria.fr

[2]Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands
supported by NWO Vernieuwingsimpuls
http://www.math.leidenuniv.nl/~streng/
marco.streng@gmail.com

Our first main result, Theorem 3.15, states that if τ is a period matrix of a certain special form, then $f(\tau)$ is a class invariant.

The special form is given in §3, where the following existence statement is proved. In the case $g \leqslant 2$, let $\mathcal{O} \subseteq K$ be an order containing the maximal order $\mathcal{O}_{K_0}$ of the maximal totally real subfield $K_0 \subseteq K$ and such that the conductor of $\mathcal{O}$ is coprime to N, and suppose that a principally polarised abelian variety with CM by $\mathcal{O}$ exists. Then Theorem 3.18 shows that a period matrix of the special form with CM by $\mathcal{O}$ exists if and only if all primes dividing $N\mathcal{O}_{K_0}$ are either split in K/K_0 or are ramified in K/K_0 and divide N exactly once.

Next, §4 shows how to express the Galois conjugates of $f(\tau)$ in terms of *N-systems* in Theorems 4.5 and 4.6. Complex conjugation is studied in §5, and conditions for the minimal polynomial of $f(\tau)$ over K^r to have coefficients in the smaller, totally real field K_0^r are given in Theorems 5.1 and 5.2.

Finally, §6 is concerned with giving some functions for $\Gamma^0(N)$, which are used to derive explicit examples in §7.

Future work of the authors will provide analogous results for Hilbert modular forms, the grounds for which are already laid in the present article.

2 Explicit Shimura reciprocity

2.1 CM theory

We use the notations and definitions of [26]. Let $K/\mathbf{Q}$ be a CM field of degree $2g$, K_0 its totally real subfield, $\Phi = (\varphi_1, \ldots, \varphi_g) : K \to \mathbf{C}^g$ a CM type, $K^r \subseteq \mathbf{C}$ the reflex field associated to Φ and K_0^r its totally real subfield. Denote by Δ_0 the discriminant of K_0 and by $\Delta = \Delta_1\Delta_0^2$ the discriminant of K.

Definition 2.1. Let $\mathcal{O}$ be an order of K containing $\mathcal{O}_{K_0}$ and closed under complex conjugation, and let Φ be a primitive CM type. Let $\mathfrak{b}$ be a non-zero proper ideal of $\mathcal{O}$, that is, an ideal with $\mathcal{O}$ as its exact ring of multipliers. Suppose that there exists a $\xi \in K$ with $\Phi(\xi) \in \left(i\mathbf{R}^{>0}\right)^g$ such that $\xi\mathfrak{b}$ is the trace dual of the complex conjugate $\overline{\mathfrak{b}}$. (If $\mathcal{O} = \mathcal{O}_K$, then this condition is equivalent to $(\mathfrak{b}\overline{\mathfrak{b}}\mathcal{D}_K)^{-1} = \xi\mathcal{O}_K$, where $\mathcal{D}_K$ is the different of K.) Then $(\mathfrak{b}, \xi)$ is called a *principally polarised ideal* for $(\mathcal{O}, \Phi)$. Two such ideals $(\mathfrak{b}, \xi)$ and $(\mathfrak{b}', \xi')$ are called *equivalent* if there is a $\mu \in K^\times$ such that $\mathfrak{b}' = \mu\mathfrak{b}$ and $\xi' = (\mu\overline{\mu})^{-1}\xi$.

In the situation of the definition, the bilinear form $E_\xi : K \times K \to \mathbf{Q}$, $(x, y) \mapsto \mathrm{Tr}(\xi\overline{x}y)$ satisfies $E_\xi(\mathfrak{b}, \mathfrak{b}) = \mathbf{Z}$. Identifying $\mathfrak{b}$ via Φ with a $2g$-dimensional lattice in $\mathbf{C}^g$ and extending E_ξ to an $\mathbf{R}$-bilinear form on $\mathbf{C}^g \times \mathbf{C}^g$ gives a principal polarisation on the complex torus $\mathbf{C}^g/\Phi(\mathfrak{b})$, which has endomorphism ring $\mathcal{O}$. We say that the resulting principally polarised abelian variety has *CM by* $(\mathcal{O}, \Phi)$. If Φ is a *primitive* CM type, then it turns out that such polarised abelian varieties are isomorphic if and only if the associated principally polarised ideals are equivalent.

For any $n \in \mathbf{Z}^{>0}$, the CM type Φ induces a $\mathbf{Q}$-linear map $\Phi : K^n \to \mathrm{Mat}_{g\times n}(\mathbf{C})$, given by

$$\Phi : (x_1, \ldots, x_n) \mapsto \begin{pmatrix} \varphi_1(x_1) & \cdots & \varphi_1(x_n) \\ \vdots & & \vdots \\ \varphi_g(x_1) & \cdots & \varphi_g(x_n) \end{pmatrix}.$$

One may choose a symplectic $\mathbf{Z}$-basis $\mathcal{B} = (b_1, \ldots, b_{2g})$ of $\mathfrak{b}$, such that the matrix of E_ξ is

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \mathrm{id}_g \\ -\mathrm{id}_g & 0 \end{pmatrix}.$$

Let $B_1 = (b_1, \ldots, b_g)$ and $B_2 = (b_{g+1}, \ldots, b_{2g})$. Then

$$\tau = \Phi(B_2)^{-1}\Phi(B_1) = \big(\Phi(b_{g+1})|\cdots|\Phi(b_{2g})\big)^{-1}\big(\Phi(b_1)|\cdots|\Phi(b_g)\big) \tag{2.1}$$

is called a *CM point* in the *Siegel space* $\mathbf{H}_g$, the set of symmetric complex $g \times g$ matrices with positive definite imaginary part.

2.2 Modular functions and matrix actions

For a commutative ring R, let

$$\mathrm{GSp}_{2g}(R) = \left\{M \in \mathrm{Mat}_{2g}(R) : M^T J M = tJ \text{ with } t \in R^\times\right\}, \tag{2.2}$$

let $\mathrm{Sp}_{2g}(R)$ be the subgroup of such matrices with $t = 1$ and $\mathrm{GSp}^+_{2g}(R)$ the subgroup with $t > 0$ (where this definition makes sense). Notice that any matrix in $\mathrm{GSp}_{2g}(R)$ can be written as $\begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix} V$ with $V \in \mathrm{Sp}_{2g}(R)$.

Then $\mathrm{GSp}_{2g}(\mathbf{Q})$ and its subgroup $\Gamma = \mathrm{Sp}_{2g}(\mathbf{Z})$ act on $\mathbf{H}_g$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = (a\tau + b)(c\tau + d)^{-1},$$

where a, b, c, $d \in \mathrm{Mat}_g(\mathbf{Q})$.

For a positive integer N, let $\Gamma(N)$ be the kernel of the surjective reduction map $\mathrm{Sp}_{2g}(\mathbf{Z}) \to \mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$. A *Siegel modular function* of level N is a meromorphic function on $\Gamma(N)\backslash\mathbf{H}_g$. It can be written as a quotient of modular forms that have *q-expansions*

$$\sum_T a_T q_T, \quad a_T \in \mathbf{C}, \quad q_T = e^{2\pi i \,\mathrm{Tr}(T\tau)/N},$$

where T runs over the symmetric matrices in $\mathrm{Mat}_g\left(\frac{1}{2}\mathbf{Z}\right)$ with integral diagonal entries.

Denote by $\mathcal{F}_N$ the set of Siegel modular functions of level N that can be written as quotients of modular forms with q-coefficients $a_T \in \mathbf{Q}(\zeta_N)$. Then $M \in \mathrm{GSp}^+_{2g}(\mathbf{Q})$ acts on $\cup_N \mathcal{F}_N$ by $f^M(z) = f(Mz)$. We define an action of $\mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ on $\mathcal{F}_N$ as follows:

- The action of a matrix in $\mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ is given by that of an arbitrary lift to $\mathrm{Sp}_{2g}(\mathbf{Z})$.
- For $t \in (\mathbf{Z}/N\mathbf{Z})^\times$, the matrix $\begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix}$ acts on the q-coefficients of f as the Galois group element of $\mathbf{Q}(\zeta_N)/\mathbf{Q}$ sending ζ_N to ζ_N^t.

2.3 Class fields and class invariants

Dealing with non-maximal orders requires a few precautions, but in a class field theoretic context, we may avoid the finitely many prime ideals that pose problems. The *conductor* of $\mathcal{O}$ is the $\mathcal{O}$- and $\mathcal{O}_K$-ideal $\mathfrak{f} = \mathfrak{f}_\mathcal{O} = \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}\} \subseteq \mathcal{O}$. Let $F \in \mathbf{Z}^{>0}$ be such that $\mathfrak{f} \cap \mathbf{Z} = F\mathbf{Z}$.

The monoid of integral ideals of $\mathcal{O}$ coprime to $\mathfrak{f}$ is isomorphic to the monoid of integral ideals of $\mathcal{O}_K$ coprime to $\mathfrak{f}$ via the map $\mathfrak{a} \mapsto \mathfrak{a}_K := \mathfrak{a}\mathcal{O}_K$ and its inverse $\mathfrak{a}_K \mapsto \mathfrak{a} = \mathfrak{a}_K \cap \mathcal{O}$, see the proof of [6, Proposition 7.22], which is formulated for imaginary-quadratic fields, but carries over immediately to arbitrary number fields. An integral ideal $\mathfrak{a}$ of $\mathcal{O}$ coprime to $\mathfrak{f}$ is invertible, cf. [20, Propositions (12.4) and (12.10)].

Definition 2.2. Let $\mathcal{O}$ be an arbitrary order in an arbitrary number field K, and let $\mathfrak{m} \subseteq \mathfrak{f}_\mathcal{O}$ be an ideal of $\mathcal{O}$. We say that a fractional $\mathcal{O}$-ideal $\mathfrak{c}$ is *coprime* to $\mathfrak{m}$ if it can be written as $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$, where $\mathfrak{a}$, $\mathfrak{b}$ are integral ideals of $\mathcal{O}$ coprime to $\mathfrak{m}$.

Note that if $\mathcal{O}$ is the maximal order, then $\mathfrak{c}$ is coprime to $\mathfrak{m}$ if and only if for all primes $\mathfrak{p} \supseteq \mathfrak{m}$, we have $v_\mathfrak{p}(\mathfrak{c}) = 0$.

Definition and Proposition 2.3. Let $\mathcal{O}$, K and $\mathfrak{m}$ be as in Definition 2.2. An element $x \in K^\times$ is a *unit* $\bmod^\times(\mathfrak{m}, \mathcal{O})$ if it satisfies the following equivalent conditions:

(1) The principal fractional ideal $x\mathcal{O}$ is coprime to $\mathfrak{m}$ in the sense of Definition 2.2.

(2) $x = x_0/x_\infty$ with $x_0 \in \mathcal{O}$ coprime to $\mathfrak{m}$ and $x_\infty \in \mathcal{O}$ such that $x_\infty \equiv 1 \pmod{\mathfrak{m}}$, that is, such that $x_\infty - 1 \in \mathfrak{m}$.

If $\mathfrak{m} = m\mathcal{O}$ with $m \in \mathbf{Z}$, then we may furthermore assume $x_\infty \in \mathbf{Z}$ in (2).

Let $\mathfrak{n}$ be an integral ideal of $\mathcal{O}$ containing $\mathfrak{m}$. Then we write

$$x \equiv 1 \bmod^\times(\mathfrak{n}, \mathfrak{m}, \mathcal{O})$$

if x is a unit $\bmod^\times(\mathfrak{m}, \mathcal{O})$ and $x_0 \equiv 1 \pmod{\mathfrak{n}}$ in (2); note that we also have $x_\infty \equiv 1 \pmod{\mathfrak{n}}$ as $\mathfrak{n} \supseteq \mathfrak{m}$.

We use shorthand notation $\bmod^\times(\alpha, \beta, \mathcal{O})$ for $\bmod^\times(\alpha\mathcal{O}, \beta\mathcal{O}, \mathcal{O})$, $\bmod^\times(\mathfrak{m}, \mathcal{O})$ for $\bmod^\times(\mathfrak{m}, \mathfrak{m}, \mathcal{O})$, and $\bmod^\times \alpha\mathcal{O}$ for $\bmod^\times(\alpha\mathcal{O}, \alpha\mathcal{O}, \mathcal{O})$.

In what follows, we will mainly be interested in the case $\mathfrak{n} = N\mathcal{O}$ and $\mathfrak{m} = NF\mathcal{O}$ for some $N \in \mathbf{Z}$.

Proof. It is evident that (2) implies (1) with $\mathfrak{a} = x_0\mathcal{O}$ and $\mathfrak{b} = x_\infty\mathcal{O}$.

Now assume that (1) holds. Then $x\mathfrak{b} = \mathfrak{a}$ since $\mathfrak{b}$ is coprime to $\mathfrak{f}$ and thus invertible. Choose some $x_\infty \in \mathfrak{b} \subseteq \mathcal{O}$ with $\mu := x_\infty - 1 \in \mathfrak{m}$, which is possible by the Chinese remainder theorem (valid in any commutative ring) since $\mathfrak{b}$ and $\mathfrak{m}$ are coprime. Let $x_0 = xx_\infty \in \mathfrak{a} \subseteq \mathcal{O}$. Then by definition of μ and x_0 and using $\mathfrak{b}^{-1} \supseteq \mathcal{O}$, we get

$$x_0\mathcal{O} + \mathfrak{m} = x_\infty x\mathcal{O} + \mathfrak{m} = (1+\mu)\mathfrak{a}\mathfrak{b}^{-1} + \mathfrak{m} \supseteq (1+\mu)\mathfrak{a} + \mathfrak{m} = \mathfrak{a} + \mathfrak{m} = \mathcal{O}.$$

So x_0 is also coprime to $\mathfrak{m}$. This shows that (2) follows from (1).

If $\mathfrak{m} = m\mathcal{O}$ with $m \in \mathbf{Z}$, then we multiply x_0 and x_∞ by $\mathrm{N}(x_\infty)/x_\infty$. Now it remains to show that $\mathrm{N}(x_\infty)/x_\infty \in \mathcal{O}$ and that $\mathrm{N}(x_\infty) \equiv 1 \pmod{m}$. For the first

property, let n be the degree of K and let χ be $(-1)^{[K:\mathbf{Q}]}$ times the characteristic polynomial of x_∞ with respect to the field extension $K/\mathbf{Q}$. Then

$$\mathrm{N}(x_\infty) = \chi(0) = \chi(0) - \chi(x_\infty) \in x_\infty \mathbf{Z}[x_\infty] \subseteq x_\infty \mathcal{O}.$$

Concerning the second property, choose a $\mathbf{Z}$-basis of $\mathcal{O}$, and for a non-zero $\alpha \in \mathcal{O}$, let $M_\alpha \in \mathrm{GL}_n(\mathbf{Z})$ denote the matrix of multiplication by α with respect to this basis. Write $x_\infty = 1 + m\alpha$ for some $\alpha \in \mathcal{O}$. Then

$$\mathrm{N}(x_\infty) = \det(M_{x_\infty}) = \det(\mathrm{id}_n + mM_\alpha) \equiv 1 \pmod{m\mathbf{Z}}. \qquad \square$$

Definition 2.4. Let $\mathfrak{m} \subseteq \mathfrak{n} \subseteq \mathcal{O}$ be as in Definition 2.3. For $x \in K$, we write $x \equiv 0 \bmod^\times (\mathfrak{n}, \mathfrak{m}, \mathcal{O})$ if x can be written as $x = x_0/x_\infty$ with $x_\infty \in \mathcal{O}$ coprime to $\mathfrak{m}$ and $x_0 \in \mathfrak{n}$.

Now let us return to our specific situation of a quartic CM-field K and an order $\mathcal{O}$ of K with $\overline{\mathcal{O}} = \mathcal{O}$ and such that $\mathcal{O}$ contains $\mathcal{O}_{K_0}$. Denote by $\mathcal{I}(NF)$ the group of fractional ideals of $\mathcal{O}_{K^r}$ that are coprime to $NF\mathcal{O}_{K^r}$. To a CM type Φ of K one may associate a *reflex CM type* Φ^r of K^r. Then the reflex type norm is the multiplicative map $K^r \to K$ given by $\mathrm{N}_{\Phi^r}(\alpha) = \prod_{\varphi^r \in \Phi^r} \varphi^r(\alpha)$. It extends naturally to a map on ideals, which sends ideals of $\mathcal{O}_{K^r}$ that are coprime to NF to ideals of $\mathcal{O}_K$ that are coprime to NF. Intersecting with $\mathcal{O}$ leads to ideals of $\mathcal{O}$ coprime to F, and we denote the resulting map by $\mathrm{N}_{\Phi^r,\mathcal{O}}$. Extending multiplicatively, we get a homomorphism $\mathrm{N}_{\Phi^r,\mathcal{O}}$ from the group $\mathcal{I}(NF)$ of fractional $\mathcal{O}_{K^r}$-ideals coprime to NF to the group of fractional $\mathcal{O}$-ideals coprime to NF.

For a fixed CM point τ with respect to the order $\mathcal{O}$ and CM type Φ, let $H_{\mathcal{O},\Phi}(N) \subseteq \mathbf{C}$ be the field generated over K^r by all values $f(\tau)$ for the $f \in \mathcal{F}_N$ that are regular at τ. Let

$$\begin{aligned} S_{\mathcal{O},\Phi}(N) = \{\mathfrak{a} \in \mathcal{I}(NF) : &\exists \mu \in K \text{ with } \mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a}) = \mu\mathcal{O}, \mu\overline{\mu} \in \mathbf{Q}, \\ &\mu \equiv 1 \bmod^\times (N, NF, \mathcal{O})\}, \end{aligned} \tag{2.3}$$

and let

$$\mathfrak{C}_{\mathcal{O},\Phi}(N) = \mathcal{I}(NF)/S_{\mathcal{O},\Phi}(N).$$

Then $H_{\mathcal{O},\Phi}(N)$ is, independently of τ, the abelian class field of K^r with Galois group $\mathfrak{C}_{\mathcal{O},\Phi}(N)$, see [26, Theorem 2.2] or [23, Main theorem 3 on page 142]. We denote the *Artin map*, which realises the isomorphism between the class group and the Galois group, by

$$\sigma = \sigma_N : \mathfrak{C}_{\mathcal{O},\Phi}(N) \xrightarrow{\sim} \mathrm{Gal}(H_{\mathcal{O},\Phi}(N)/K^r).$$

As $S_{\mathcal{O},\Phi}(N)$ contains the principal ray of modulus NF, the field $H_{\mathcal{O},\Phi}(N)$ is a subfield of the ray class field of modulus NF of K^r.

Of special interest are values of functions in $\mathcal{F}_N$ that lie in $H_{\mathcal{O},\Phi}(1)$, which in the case $g = 1$ is the ring class field of $\mathcal{O}$, generated over $K^r \cong K$ by the j-invariant of an elliptic curve with CM by $\mathcal{O}$. In the case $g = 2$, the field $H_{\mathcal{O},\Phi}(1)$ is generated over K^r by the Igusa invariants of principally polarised abelian varieties of dimension 2 with CM by $(\mathcal{O}, \Phi)$ (here one can take "the Igusa invariants" to mean either the complete set of eight invariants on page 642 of Igusa [16] or the set of three invariants j_1, j_2, j_3 of Cardona-Quer [4]). For $\mathcal{O} = \mathcal{O}_K$ the field $H_{\mathcal{O},\Phi}(1)$ is a subfield of the Hilbert class field of K^r.

Definition 2.5. Let $f \in \mathcal{F}_N$, and let τ be a CM point for $(\mathcal{O}, \Phi)$. We call $f(\tau)$ a *CM value* of f. If $f(\tau) \in H_{\mathcal{O},\Phi}(1)$, then we call it a *class invariant*, and by its *class polynomial* we mean its characteristic polynomial

$$\prod_{\mathfrak{a} \in \mathfrak{C}_{\mathcal{O},\Phi}(1)} \left(X - f(\tau)^{\sigma(\mathfrak{a})} \right).$$

for the field extension $H_{\mathcal{O},\Phi}(1)/K^r$.

2.4 Shimura reciprocity

The main tool in the study of which functions yield class invariants is Shimura's reciprocity law, which describes the action of the Galois group of $H_{\mathcal{O},\Phi}(N)/K^r$ on CM values $f(\tau)$ by matrix actions on the function f. The following explicit result is Theorem 2.4 of [26].

Theorem 2.6. *Let τ be a CM point coming from a symplectic basis $\mathcal{B} = (b_1 | \cdots | b_{2g})$ of a principally polarised ideal $(\mathfrak{b}, \xi)$ for $(\mathcal{O}, \Phi)$, where $\mathcal{O}$ is an order of a CM-field K. Let F be a positive integer with $F\mathcal{O}_K \subseteq \mathcal{O}$. Let $\sigma : \mathfrak{C}_{\mathcal{O},\Phi}(N) \to \mathrm{Gal}(H_{\mathcal{O},\Phi}(N)/K^r)$ be the Artin map.*

For any $\mathfrak{a} \in \mathcal{I}(NF)$ representing an element of $\mathfrak{C}_{\mathcal{O},\Phi}(N)$, let $\mathcal{C}$ be a symplectic basis of $\mathfrak{c} = \mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a})^{-1}\mathfrak{b}$ with respect to $E_{\mathrm{N}(\mathfrak{a})\xi}$. Let M^T be the basis transformation satisfying $\mathcal{C} = \mathcal{B}M^T$. Then we have $M \in \mathrm{GSp}_{2g}^+(\mathbf{Q})$ with $t = \mathrm{N}(\mathfrak{a})^{-1}$, and the reduction $M_{\bmod N}$ exists and satisfies $M_{\bmod N} \in \mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$. Write

$$(M_{\bmod N})^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{N}(\mathfrak{a}) \end{pmatrix} (V_{\bmod N})$$

with $V_{\bmod N} \in \mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$, and let V be an arbitrary lift of $V_{\bmod N}$ to $\mathrm{Sp}_{2g}(\mathbf{Z})$.

Then for any $f \in \mathcal{F}_N$, we have

$$f(\tau)^{\sigma(\mathfrak{a})} = \left(f^{(M_{\bmod N})^{-1}} \right)^M (\tau) = f^{\begin{pmatrix} 1 & 0 \\ 0 & \mathrm{N}(\mathfrak{a}) \end{pmatrix}} (VM\tau).$$

3 Class invariants from functions for $\Gamma^0(N)$

The aim of this section is to obtain an easily applicable sufficient criterion for functions for $\Gamma^0(N)$ to yield class invariants, by applying Shimura reciprocity "once and for all". Here $\Gamma^0(N)$ for $N \in \mathbf{Z}^{>0}$ is the subgroup of $\Gamma = \mathrm{Sp}_{2g}(\mathbf{Z})$ of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

such that all entries of the $g \times g$ block b are divisible by N.

3.1 Ideal bases and quadratic polynomials

To get an explicit handle on ideals and polarised ideal classes, we would like to mimick the situation for $g = 1$, where ideals are represented as $z\mathbf{Z} + \mathbf{Z}$ with $z \in K$ a root of a quadratic polynomial with coefficients in $\mathbf{Z}$ and of discriminant Δ. Such

a representation is not possible in arbitrary CM fields, where ideals are projective modules over the Dedekind ring $\mathcal{O}_{K_0}$, which leads to the notion of pseudo-bases, see [5, §1]. But if the different $\mathcal{D}_{K_0}$ is principal, generated by some $\lambda \in K_0$, which we will assume from now on, then it turns out that the existence of a principal polarisation forces all principally polarised ideals to actually be free $\mathcal{O}_{K_0}$-modules. This condition holds, for instance, when $g = 1$ with $\lambda = 1$ and when $g = 2$ with $\lambda = \sqrt{\Delta_0}$.

Let $\mathcal{O}$ be an order in a CM field K such that $\mathcal{O} \supseteq \mathcal{O}_{K_0}$ and $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$.

Proposition 3.1. *Given $z \in K$ such that $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ is a proper fractional ideal of $\mathcal{O}$, let $\xi = \xi(z) = ((z - \overline{z})\lambda)^{-1}$, and let Φ be the CM type such that $\Phi(\xi) \in \left(i\mathbf{R}^{>0}\right)^g$. Then $(\mathfrak{b}, \xi)$ is a principally polarised ideal for $(\mathcal{O}, \Phi)$.*

Conversely, up to equivalence, every principally polarised ideal occurs in this way.

Moreover, two such pairs $(\mathfrak{b}, \xi)$ and $(\mathfrak{b}', \xi')$ with $\mathfrak{b}' = z'\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ and $\xi' = \left((z' - \overline{z'})\lambda\right)^{-1}$ have the same CM type and are equivalent (cf. Definition 2.1) if and only if there is a matrix

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_{K_0})$$

such that $z' = Mz := \frac{\alpha z + \beta}{\gamma z + \delta}$. In that case, we have $\xi' = (\gamma z + \delta)(\gamma \overline{z} + \delta)\xi$.

Proof. The first two assertions are [25, Theorems I.5.9 and I.5.8], after correcting a sign in the proof and extending it to non-maximal orders.

It remains to prove the final statement about equivalence. Given any

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{K_0}),$$

one easily computes

$$\frac{z - \overline{z}}{Mz - \overline{Mz}} = (\gamma z + \delta)(\gamma \overline{z} + \delta)(\det M)^{-1}. \tag{3.1}$$

Now suppose we have two pairs $(\mathfrak{b}, \xi)$ and $(\mathfrak{b}', \xi')$ associated to z and z'.

Assume first that there exists $M \in \mathrm{SL}_2(\mathcal{O}_{K_0})$ with $z' = Mz$. Then one has $\mathfrak{b} = (\alpha z + \beta)\mathcal{O}_{K_0} + (\gamma z + \delta)\mathcal{O}_{K_0}$ and $\mathfrak{b}' = z'\mathcal{O}_{K_0} + \mathcal{O}_{K_0} = \mu\mathfrak{b}$ with $\mu = (\gamma z + \delta)^{-1}$. By (3.1) one sees $\xi' = \xi(\gamma z + \delta)(\gamma \overline{z} + \delta) = \xi(\mu\overline{\mu})^{-1}$. So $(\mathfrak{b}, \xi)$ and $(\mathfrak{b}', \xi')$ are indeed equivalent, and ξ' belongs to the same CM type Φ as ξ since $\mu\overline{\mu}$ is totally positive.

Conversely, if the two pairs are equivalent for the same Φ, then $\mathfrak{b}' = \mu\mathfrak{b}$ and $\xi' = (\mu\overline{\mu})^{-1}\xi$ for some $\mu \in K^\times$, which implies $z' = \mu(\alpha z + \beta)$ and $1 = \mu(\gamma z + \delta)$ for some α, β, γ, $\delta \in \mathcal{O}_{K_0}$, so that $z' = Mz$ with

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{K_0})$$

as the transformation is invertible. Now the definition of ξ and $\overline{\xi}$ and (3.1) yield $1 = \xi/(\xi'\mu\overline{\mu}) = \det M$, so $M \in \mathrm{SL}_2(\mathcal{O}_{K_0})$. □

We may then write down an explicit symplectic basis and period matrix.

Proposition 3.2. *Suppose $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$ and let z, $\mathfrak{b}$, ξ, Φ be as in Proposition 3.1. Let $\mathcal{B}_1 = (b_{1,1}, \dots, b_{1,g})$ be any $\mathbf{Z}$-basis of $\mathcal{O}_{K_0}$. Write its trace-dual $\mathbf{Q}$-basis of K_0 as $-\lambda^{-1}\mathcal{B}_2 = (-\lambda^{-1}b_{2,1}, \dots, -\lambda^{-1}b_{2,g})$. Then a symplectic basis of $(\mathfrak{b}, \xi)$ is given by*

$$\mathcal{B} = (zb_{1,1}, \dots, zb_{1,g}, b_{2,1}, \dots, b_{2,g}) = (z\mathcal{B}_1|\mathcal{B}_2)$$

and a period matrix by $\tau = \Phi(\mathcal{B}_2)^{-1}\Phi(z\mathcal{B}_1)$.

Proof. Note first that the trace-dual is a $\mathbf{Z}$-basis of $\mathcal{D}_{K_0}^{-1}$, so $\mathcal{B}$ is indeed a basis of $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$.

Next note that since ξ is purely imaginary, that is, $\overline{\xi} = -\xi$, we have $\mathrm{Tr}(\xi\alpha) = \mathrm{Tr}_{K_0/\mathbf{Q}}\left(\xi(\alpha - \overline{\alpha})\right)$ for any $\alpha \in K$. Since for $(u, v) = (zb_{1,i}, zb_{1,j})$ and for $(u, v) = (b_{2,i}, b_{2,j})$ we have $\overline{u}v \in K_0$, this implies $E_\xi(u, v) = \mathrm{Tr}(\xi\overline{u}v) = 0$. Finally,

$$\begin{aligned} E_\xi(zb_{1,i}, b_{2,j}) &= \mathrm{Tr}_{K_0/\mathbf{Q}}\left((z - \overline{z})^{-1}\lambda^{-1}(\overline{z}b_{1,i}b_{2,j} - zb_{1,i}b_{2,j})\right) \\ &= \mathrm{Tr}_{K_0/\mathbf{Q}}(-\lambda^{-1}b_{2,j}b_{1,i}) = \delta_{ij}, \end{aligned}$$

hence the basis is symplectic. The formula for the period matrix is (2.1). □

Corollary 3.3. Let $g = 2$ and $\lambda = \sqrt{\Delta_0}$. In the situation of Proposition 3.1, let the CM type be $\Phi = (\varphi_1, \varphi_2)$, and to simplify the notation, write $z_i = \varphi_i(z)$, $\lambda_i = \varphi_i(\lambda)$ and $\omega_i = \varphi_i(\omega)$ for ω defined below. A symplectic basis $\mathcal{B}$ of $\mathfrak{b}$ with respect to E_ξ and an associated period matrix τ are given as follows:

If Δ_0 is odd, let $\omega = \frac{1+\lambda}{2}$; then $\mathcal{B} = (z\omega, z, -1, 1 - \omega)$. If Δ_0 is even, let $\omega = \frac{\lambda}{2}$; then $\mathcal{B} = (z\omega, z, -1, -\omega)$. In both cases,

$$\tau = \frac{1}{-\lambda_1}\begin{pmatrix} z_1\omega_1^2 - z_2\omega_2^2 & z_1\omega_1 - z_2\omega_2 \\ z_1\omega_1 - z_2\omega_2 & z_1 - z_2 \end{pmatrix}.$$

Proof. Take $\mathcal{B}_1 = (\omega, 1)$, $b_{2,1} = -1$ and $b_{2,2} = -\omega$ if Δ_0 is even and $b_{2,2} = 1 - \omega$ if Δ_0 is odd. It is easy to check that $(-\lambda^{-1}b_{2,1}, -\lambda^{-1}b_{2,2})$ is the trace dual basis of $\mathcal{B}_1$, so the result follows from Proposition 3.2 using $\lambda_2 = -\lambda_1$. □

It will be convenient to represent the generator z occurring in Proposition 3.1 as the root of a quadratic polynomial over K_0 with integral coefficients. For $g = 1$, one usually assumes the polynomial to be primitive, that is, with coprime integral coefficients and $A > 0$. Unless the narrow class number of K_0 is 1, we cannot hope to achieve this in general, so we need to adopt a weaker convention, allowing us at least to avoid any finite set of primes.

Definition 3.4. Let $\mathfrak{m} \subseteq \mathcal{O}_{K_0}$ be a non-zero ideal. A quadratic polynomial $AX^2 + BX + C \in \mathcal{O}_{K_0}[X]$ is *semiprimitive modulo* $\mathfrak{m}$ if A is totally positive and furthemore $\gcd(A, B, C, \mathfrak{m}) = 1$, that is,

$$\gcd(A\mathcal{O}_{K_0}, B\mathcal{O}_{K_0}, C\mathcal{O}_{K_0}, \mathfrak{m}) := A\mathcal{O}_{K_0} + B\mathcal{O}_{K_0} + C\mathcal{O}_{K_0} + \mathfrak{m} = \mathcal{O}_{K_0}.$$

Proposition 3.5. *Let $\mathfrak{m} \subseteq \mathcal{O}_{K_0}$ be a non-zero ideal. Every element z of $K\backslash K_0$ is a root of a quadratic polynomial $AX^2 + BX + C \in \mathcal{O}_{K_0}[X]$ that is semiprimitive modulo $\mathfrak{m}$. This polynomial is unique up to multiplication by a totally positive $u \in K_0^\times$ that is a unit $\mathrm{mod}^\times(\mathfrak{m}, \mathcal{O}_{K_0})$. Moreover, its discriminant $B^2 - 4AC$ is totally negative.*

Proof. As $K = K_0(z) \supseteq K_0$ is a quadratic extension, there is a non-zero polynomial $AX^2 + BX + C \in K_0[X]$ with z as a root. After scaling, we get $A, B, C \in \mathcal{O}_{K_0}$. Write $\mathfrak{d} = \gcd(A, B, C)$. By the strong approximation theorem, for instance [5, Corollary 1.2.9], there is an element $d \in K_0$ such that $v_\mathfrak{p}(d) = -v_\mathfrak{p}(\mathfrak{d})$ for each prime ideal $\mathfrak{p}$ dividing $\mathfrak{m}$, $v_\mathfrak{p}(d) \geqslant 0$ for all other prime ideals, and the signs of d under the two real embeddings of K_0 coincide with those of A. Then we may multiply A, B and C by d to obtain new coefficients with $\gcd(A, B, C)$ coprime to $\mathfrak{m}$ and A totally positive. The discriminant is totally negative as $K = K_0(z) \supseteq K_0$ is totally imaginary quadratic.

If $A'X^2 + B'X + C'$ is another such polynomial, then it equals $u(AX^2 + BX + C)$ with the scaling factor $u = A'/A$ totally positive in $K_0^\times$ due to the positivity of A and A'. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{K_0}$ dividing $\mathfrak{m}$, then at least one of A, B and C has valuation 0 in $\mathfrak{p}$, which shows that $v_\mathfrak{p}(u) \geqslant 0$; the symmetric argument for A', B' and C' shows that $v_\mathfrak{p}(u) \leqslant 0$, so that $v_\mathfrak{p}(u) = 0$. This means that u is a unit $\bmod^\times(\mathfrak{m}, \mathcal{O}_{K_0})$. □

Now for any $z \in K \backslash K_0$, the elements z and 1 generate an $\mathcal{O}_{K_0}$-submodule of K of rank 2. This module is a fractional ideal for an order in K that can easily be derived from the coefficients of the polynomial as follows.

Proposition 3.6. *Let $z \in K \setminus K_0$ be a root of a quadratic polynomial as in Proposition 3.5. Then $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ is a subgroup of K with ring of multipliers*

$$\mathcal{O} = \mathfrak{d}^{-1}Az + \mathcal{O}_{K_0}, \text{ where } \mathfrak{d} = \gcd(A, B, C) \text{ and } \mathfrak{d}^{-1} = \{x \in K_0 : x\mathfrak{d} \subset \mathcal{O}_{K_0}\}.$$

In other words, $\mathfrak{b}$ is a proper fractional $\mathcal{O}$-ideal.

Proof. Given any $\mu \in K$, we write $\mu = xAz + y$ with $x, y \in K_0$. By definition of the ring of multipliers, we have $\mu \in \mathcal{O}$ if and only if $xAz+y$ and $(xAz+y)z = (y-xB)z - xC$ are both in $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$. But this is equivalent to $xA, y, y-xB, -xC \in \mathcal{O}_{K_0}$, i.e., to $y \in \mathcal{O}_{K_0}$ and $x\mathfrak{d} \subseteq \mathcal{O}_{K_0}$. □

Conversely, for a fixed order $\mathcal{O}$ and given CM type Φ, Proposition 3.1 implies that any polarised ideal class in the sense of Definition 2.1 may be represented as a root of a quadratic form that is semiprimitive modulo an arbitrarily fixed ideal $\mathfrak{m}$ of $\mathcal{O}_{K_0}$.

Definition 3.7. Let $\mathfrak{m} \subseteq \mathcal{O}_{K_0}$ be a non-zero ideal, and assume that $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$. Let $\mathcal{O}$ be an order of a CM-field K and let Φ be a CM-type. By Propositions 3.1 and 3.5, every principally polarised ideal class T for $(\mathcal{O}, \Phi)$ in the sense of Definition 2.1 admits a representative $(\mathfrak{b}, \xi)$ as in Proposition 3.1, where z is the root of a polynomial $AX^2 + BX + C$ that is semiprimitive modulo $\mathfrak{m}$. We then say that the quadratic polynomial *represents* T.

Notice that the quadratic polynomial and Φ define z, and thus $(\mathfrak{b}, \xi)$, uniquely since only one choice of root leads to a ξ as in Proposition 3.1 that is totally positive imaginary under Φ. This root is meant when in the following we speak of "the root" of a quadratic polynomial, and often the CM type Φ will be tacitly understood.

Propositions 3.1 also shows that there is an additional degree of freedom via the action of unimodular matrices over $\mathcal{O}_{K_0}$; we will use it to obtain a bit more than just $\gcd(A, B, C, \mathfrak{m}) = 1$, namely, $\gcd(A, \mathfrak{m}) = 1$.

Proposition 3.8. *Suppose $z' = Mz$ with $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_{K_0})$. Then z' is a root of $A'X^2 + B'X + C' \in \mathcal{O}_{K_0}[X]$ with*

$$\begin{aligned} A' &= A\delta^2 - B\gamma\delta + C\gamma^2, \\ B' &= -2A\beta\delta + B(1 + 2\beta\gamma) - 2C\alpha\gamma, \\ C' &= A\beta^2 - B\alpha\beta + C\alpha^2, \end{aligned} \tag{3.2}$$

where $\gcd(A', B', C') = \gcd(A, B, C)$.

If ξ and ξ' are obtained from z and z' as in Proposition 3.1, then

$$\xi' = \frac{A'}{A}\,\xi. \tag{3.3}$$

Proof. The shape of A', B' and C' follows from a direct computation using also $\det M = 1$. By Proposition 3.1 we have

$$\frac{\xi'}{\xi} = (\gamma z + \delta)(\gamma \overline{z} + \delta) = \frac{A'}{A},$$

using $z\overline{z} = \frac{C}{A}$ and $z + \overline{z} = -\frac{B}{A}$. □

Proposition 3.9. *Let $\mathfrak{m} \subseteq \mathcal{O}_{K_0}$ be a non-zero ideal, and assume that $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$. Then every principally polarised ideal class is represented by a quadratic form with A totally positive and* $\gcd(A, \mathfrak{m}) = \mathcal{O}_{K_0}$.

Proof. Using Propositions 3.1 and 3.5, we find a semiprimitive quadratic polynomial $AX^2 + BX + C$ modulo $\mathfrak{m}$ representing T. It remains to apply a suitable matrix M' as in Proposition 3.8 such that the resulting A' is totally positive and coprime to $\mathfrak{m}$. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{K_0}$ dividing $\mathfrak{m}$, we consider the homogeneous form $A' := A\delta^2 - B\gamma\delta + C\gamma^2$ in δ and γ of Proposition 3.8. Let

$$\begin{aligned} &M_{\bmod \mathfrak{p}} = \mathrm{id}, && A' = A && \text{if } \mathfrak{p} \nmid A, \\ &M_{\bmod \mathfrak{p}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, && A' = C && \text{if } \mathfrak{p} \nmid C, \mathfrak{p} \mid A, \\ &M_{\bmod \mathfrak{p}} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, && A' = A + C - B && \text{otherwise (in which case } \mathfrak{p} \nmid B). \end{aligned}$$

In all cases, we have $\mathfrak{p} \nmid A'$.

By Chinese remaindering, we obtain a matrix $M_{\bmod \mathrm{rad}\,\mathfrak{m}} \in \mathrm{SL}_2(\mathcal{O}_{K_0}/\mathrm{rad}(\mathfrak{m}))$, which can be lifted to a matrix $M \in \mathrm{SL}_2(\mathcal{O}_{K_0})$, e.g. by strong approximation [14, Appendix A.3]. Replace z by Mz, so A gets replaced by A', which is coprime to $\mathfrak{m}$.

If in the process we lost the total positivity of A, we may use strong approximation again as in the proof of Proposition 3.5 and multiply A, B and C by an element coprime to $\mathfrak{m}$ and with the same signs of embeddings as A without modifying z. □

Permitting unimodular transformations of the quadratic forms, we also need to examine how they act on our standard choice of symplectic bases. Fix $\mathcal{B}_i = (b_{i,1}, \ldots, b_{i,g})$ as in Proposition 3.2. For $\eta \in K_0$ and $i, j \in \{1, 2\}$ denote by $[\eta]_j^i \in \mathrm{Mat}_g(\mathbf{Q})$ the matrix of multiplication by η from K_0 with $\mathbf{Q}$-basis $\mathcal{B}_i$ to K_0 with $\mathbf{Q}$-basis $\mathcal{B}_j$, that is,

$$\eta\mathcal{B}_i = \mathcal{B}_j[\eta]_j^i, \tag{3.4}$$

where $\mathcal{B}_1$ and $\mathcal{B}_2$ are seen as $1 \times g$ matrices.

Proposition 3.10. *Under the hypotheses of Proposition 3.8, let τ and τ' be obtained from z and z' by taking the symplectic bases of Proposition 3.2. Then*

$$\tau' = M'\tau, \text{ where } M' = \begin{pmatrix} [\alpha]_1^1 & [\gamma]_1^2 \\ [\beta]_2^1 & [\delta]_2^2 \end{pmatrix}^T. \tag{3.5}$$

Proof. Let $\mathcal{B}$ and $\mathcal{B}'$ be the symplectic bases of Proposition 3.2. Then we have

$$\begin{aligned} \mathcal{B}' &= (z', 1) \begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} = (\gamma z + \delta)^{-1}(z, 1) M^T \begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} \\ &= (\gamma z + \delta)^{-1}(z, 1) \begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} \begin{pmatrix} [\alpha]_1^1 & [\gamma]_1^2 \\ [\beta]_2^1 & [\delta]_2^2 \end{pmatrix}. \end{aligned} \tag{3.6}$$

It follows that we have

$$\begin{aligned} \tau' &= \Phi(\mathcal{B}_2)^{-1}\Phi(z'\mathcal{B}_1) = \Phi\left(z\mathcal{B}_1[\gamma]_1^2 + \mathcal{B}_2[\delta]_2^2\right)^{-1} \Phi\left(z\mathcal{B}_1[\alpha]_1^1 + \mathcal{B}_2[\beta]_2^1\right) \\ &= (\Phi(z\mathcal{B}_1)[\gamma]_1^2 + \Phi(\mathcal{B}_2)[\delta]_2^2)^{-1}(\Phi(z\mathcal{B}_1)[\alpha]_1^1 + \Phi(\mathcal{B}_2)[\beta]_2^1) \\ &= \left(\tau[\gamma]_1^2 + [\delta]_2^2\right)^{-1} \left(\tau[\alpha]_1^1 + [\beta]_2^1\right). \end{aligned}$$

As $\tau' = (\tau')^T$ and $\tau = \tau^T$, we get

$$\tau' = \left(([\alpha]_1^1)^T\tau + ([\beta]_2^1)^T\right) \left(([\gamma]_1^2)^T\tau + ([\delta]_2^2)^T\right)^{-1} = M'\tau.$$

□

Corollary 3.11. The matrix $S := [1]_1^2 \in \mathrm{GL}_g(\mathbf{Z})$ is symmetric. If $\alpha, \beta, \gamma, \delta \in \mathbf{Q}$ in the situation of Proposition 3.10, then we have

$$M' = \begin{pmatrix} \alpha \,\mathrm{id}_g & \beta S^{-1} \\ \gamma S & \delta \,\mathrm{id}_g \end{pmatrix} \text{ and } \tau' = \left(\alpha\tau + \beta S^{-1}\right)(\gamma S\tau + \delta)^{-1}.$$

Proof. Notice that S is the base change matrix between the bases $\mathcal{B}_1$ and $\mathcal{B}_2$ of $\mathcal{O}_{K_0}$ and as such an element of $\mathrm{GL}_g(\mathbf{Z})$. We next prove that it is symmetric. Let $T : K_0 \times K_0 \to \mathbf{Q}$ be the bilinear form $T : (x, y) \mapsto \mathrm{Tr}_{K_0/\mathbf{Q}}(-\lambda^{-1}xy)$, which is obviously symmetric. Note that $\mathcal{B}_1$ and $\mathcal{B}_2$ are dual bases for T. In particular, the matrix $S = [1]_1^2 = \left([1]_2^1\right)^{-1}$ is the matrix of T with respect to the basis $\mathcal{B}_2$, hence it is symmetric.

Using $S = S^T$, the formulæ for M' and τ' follow from Propositions 3.8 and 3.10. □

Example 3.12. For $g = 2$ and $\lambda = \sqrt{\Delta_0}$ let $\mathcal{B}_1$ and $\mathcal{B}_2$ be as in the proof of Corollary 3.3. Then $S = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$ if Δ_0 is even, and $S = \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}$ if Δ_0 is odd.

The period matrix corresponding to $-z^{-1}$ is not always $-\tau^{-1}$, but it is close. Indeed, taking $\alpha = \delta = 0$, $\beta = -1$ and $\gamma = 1$ in Corollary 3.11 shows the following.

Example 3.13. If the period matrix corresponding to z is τ, then the period matrix corresponding to $-1/z$ is

$$\begin{pmatrix} 0 & -S^{-1} \\ S & 0 \end{pmatrix} \tau = -(S\tau S)^{-1} = \begin{pmatrix} S^{-1} & 0 \\ 0 & S \end{pmatrix} \left(-\tau^{-1}\right) \in \Gamma^0(N) \cdot \left(-\tau^{-1}\right)$$

for every $N \in \mathbf{Z}$, where S is as in Corollary 3.11.

Proposition 3.14. *In the situation of Proposition 3.1 and Proposition 3.5, consider the root $z' = -\overline{z}$ of the quadratic polynomial $AX^2 - BX + C$. With $\overline{\mathfrak{b}} = z'\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$, we have $\xi = \xi(z) = \xi(z')$, so ξ also defines a principal polarisation on $\overline{\mathfrak{b}}$, and the (as in Proposition 3.2) associated period matrix is $\tau' = -\overline{\tau}$.*

Proof. The assertion on the polarisation defined by ξ is clear, and the expression for τ' is a consequence of the shape of the symplectic basis given in Proposition 3.2. □

3.2 Class invariants

From now on, we assume $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$, which, as said before, is automatic for $g \leqslant 2$. We first provide a sufficient criterion for a CM value to be a class invariant. The criterion is a generalisation of the first statement in [22, Theorem 4 on p. 331] to higher dimension. For a generalisation of the remainder of [22, Theorem 4], see Theorem 4.6 below.

Theorem 3.15. *Let $N \in \mathbf{Z}^{>0}$ and assume $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$. Let $f \in \mathcal{F}_N$ be a quotient of modular forms with rational q-expansions, and suppose that f is invariant under $\Gamma^0(N)$. Let τ be a CM point for $(\mathcal{O}, \Phi)$ coming as in Propositions 3.2 and 3.5 from a proper ideal $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ with z a root of $AX^2 + BX + C$, where A and N are coprime and $N \mid C$.*

If τ is not a pole of f, then $f(\tau)$ is a class invariant.

We will use the following lemmata in the proof.

Lemma 3.16. With f and τ as in Theorem 3.15, let $\mu \in K^\times$. By Proposition 3.6 we can write $\mu = \frac{\alpha A z + \beta}{d}$ with $\alpha \in \mathfrak{d}^{-1}$ for $\mathfrak{d} = \gcd(A, B, C)$, $\beta \in \mathcal{O}_{K_0}$ and $d \in \mathbf{Z}^{>0}$.

Let M'_μ be the matrix of multiplication by μ with respect to the K_0-basis $(z, 1)$ of K, that is, $\mu(z, 1) = (z, 1)M'_\mu$. Then

$$M'_\mu = \frac{1}{d}\begin{pmatrix} \beta - \alpha B & \alpha A \\ -\alpha C & \beta \end{pmatrix} \in \mathrm{Mat}_2\left(\frac{1}{d}\,\mathcal{O}_{K_0}\right). \tag{3.7}$$

Let $\mathcal{B}$ be the symplectic basis of Proposition 3.2, and let $M_\mu \in \mathrm{Mat}_{2g}(\mathbf{Q})$ be the matrix of multiplication by μ with respect to the $\mathbf{Q}$-basis $\mathcal{B}$ of K, that is, $\mu\mathcal{B} = \mathcal{B}M_\mu$. Then

$$M_\mu = \frac{1}{d}\begin{pmatrix} [\beta - \alpha B]_1^1 & [\alpha A]_1^2 \\ [-\alpha C]_2^1 & [\beta]_2^2 \end{pmatrix} \in \mathrm{Mat}_{2g}\left(\frac{1}{d}\,\mathbf{Z}\right), \tag{3.8}$$

using the notation (3.4) after Proposition 3.5.

Proof. The entries of M'_μ are computed directly using the minimal polynomial of z; they are elements of $\frac{1}{d}\mathcal{O}_{K_0}$ since $\alpha \in \mathfrak{d}^{-1}$.

Next, we need to deal with the bases $\mathcal{B}_i = (b_{i,1}, \ldots, b_{i,g})$ of K_0 as a $\mathbf{Q}$-vector space that play a role in the symplectic basis $\mathcal{B} = (z\mathcal{B}_1 | \mathcal{B}_2)$ of Proposition 3.2. We compute, using also (3.4):

$$\begin{aligned}\mu\mathcal{B} = \mu(z\mathcal{B}_1 \mid \mathcal{B}_2) = (\mu z\mathcal{B}_1 \mid \mu\mathcal{B}_2) &= \frac{1}{d}\left((z(\beta - \alpha B) - \alpha C)\mathcal{B}_1 \mid (z(\alpha A) + \beta)\mathcal{B}_2\right) \\ &= \frac{1}{d}(z\mathcal{B}_1[\beta - \alpha B]_1^1 + \mathcal{B}_2[-\alpha C]_2^1 \mid z\mathcal{B}_1[\alpha A]_1^2 + \mathcal{B}_2[\beta]_2^2) = (z\mathcal{B}_1 \mid \mathcal{B}_2)M''_\mu\end{aligned}$$

with M''_μ equal to the right hand side of (3.8), hence $M_\mu = M''_\mu$. □

Lemma 3.17. With f and τ as in Theorem 3.15, let $\mu \in K$ be a unit $\bmod^\times(NF, \mathcal{O})$ (cf. Definition 2.3) with $\mu\overline{\mu} \in \mathbf{Q}$, and let M_μ be as in Lemma 3.16. Then its reduction $(M_\mu)_{\bmod N}$ modulo N exists and is an element of $\mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$, and $f^{(M_\mu)^T_{\bmod N}} = f$.

Proof. The matrix of E_ξ with respect to the basis $\mathcal{B}$ is $\mathrm{Tr}_{K/\mathbf{Q}}(\xi\overline{\mathcal{B}}^T\mathcal{B})$, where $\mathrm{Tr}_{K/\mathbf{Q}}$ is applied entry-wise to the matrix. Since $\mathcal{B}$ is a symplectic basis, we get

$$\mathrm{Tr}_{K/\mathbf{Q}}(\xi\overline{\mathcal{B}}^T\mathcal{B}) = J.$$

Using $\mu\overline{\mu} \in \mathbf{Q}$, we get

$$\begin{aligned} M_\mu^T J M_\mu &= \mathrm{Tr}_{K/\mathbf{Q}}(\xi\overline{M_\mu}^T\overline{\mathcal{B}}^T\mathcal{B}M_\mu) \\ &= \mathrm{Tr}_{K/\mathbf{Q}}(\xi\overline{\mathcal{B}}^T\overline{\mu}\mu\mathcal{B}) \\ &= \mu\overline{\mu}\,\mathrm{Tr}_{K/\mathbf{Q}}(\xi\overline{\mathcal{B}}^T\mathcal{B}) = \mu\overline{\mu}J. \end{aligned}$$

In particular, M_μ is an element of $\mathrm{GSp}_{2g}(\mathbf{Q})$ with the t of (2.2) equal to $\mu\overline{\mu}$. We write $\mu = \frac{\alpha Az+\beta}{d}$ as in Lemma 3.16 with furthermore d coprime to NF since μ is a unit $\bmod^\times(NF, \mathcal{O})$. Then M_μ is given by (3.8). Since both d and $\alpha Az + \beta$ are coprime to N and $M_\mu \in \mathrm{GSp}_{2g}(\mathbf{Q})$, its reduction $(M_\mu)_{\bmod N}$ is defined and an element of $\mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$.

Since $\alpha A \in \mathcal{O}_{K_0}$ and A is coprime to N, the element α has non-negative valuation in all primes of K_0 dividing N, so that $N \mid C$ implies $\alpha C \in N\mathcal{O}_{K_0}$.

This shows that all entries in the top right $g \times g$-block of M_μ^T are divisible by N, hence $(M_\mu)^T_{\bmod N}$ is the product of (the reduction modulo N of) an element of $\Gamma^0(N)$ with the block matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & \mu\overline{\mu} \bmod N \end{pmatrix}.$$

The assumptions on f guarantee that both these types of matrices fix f. □

Proof of Theorem 3.15. We use Theorem 2.6 to show that $f(\tau)$ is invariant under

$$\mathrm{Gal}\left(H_{\mathcal{O},\Phi}(N)/H_{\mathcal{O},\Phi}(1)\right) = \sigma\left(\frac{\mathcal{I}(NF) \cap S_{\mathcal{O},\Phi}(1)}{S_{\mathcal{O},\Phi}(N)}\right).$$

Let $\mathfrak{a} \in \mathcal{I}(NF) \cap S_{\mathcal{O},\Phi(1)}$. By the definition (2.3) of $S_{\mathcal{O},\Phi}(1)$, there is some $\mu \in K$ such that $\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a}) = \mu\mathcal{O}$ and $\mathrm{N}(\mathfrak{a}) = \mu\overline{\mu}$. As we took $\mathfrak{a}$ coprime to NF, we have that $N_{\Phi^r,\mathcal{O}}(\mathfrak{a})$ is a fractional $\mathcal{O}$-ideal coprime to NF. So μ is a unit $\bmod^\times(NF, \mathcal{O})$ in the sense of Definition 2.3. Let $M = M^T_{\mu^{-1}}$ in the notation of Lemma 3.17. Using Theorem 2.6 and Lemma 3.17, we get

$$f(\tau)^{\sigma(\mathfrak{a})} = f^{(M_\mu)^T_{\bmod N}}(M\tau) = f(M\tau).$$

To finish the proof, it suffices to show that $M\tau = \tau$. Lemma 4.6 of [26] states that if τ' is the period matrix associated to $\mathcal{B}M^T$, then $\tau' = M\tau$ holds. In our case, we have $\mathcal{B}M^T = \mu^{-1}\mathcal{B}$, and the period matrix τ' associated to $\mu^{-1}\mathcal{B}$ equals the period matrix τ associated to $\mathcal{B}$, which completes the proof.

To make the argument self-contained, we give the proof of Lemma 4.6 of [26]. Letting $\mathcal{B} = (B_1|B_2)$ and $\Omega_i = \Phi(B_i)$, we have $\tau = (\Omega_2)^{-1}\Omega_1$. Writing

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with a, b, c, $d \in \mathrm{Mat}_g(\mathbf{Z})$, we obtain

$$\mathcal{B}M^T = (B_1|B_2)\begin{pmatrix} a^T & c^T \\ b^T & d^T \end{pmatrix} = \left(B_1a^T + B_2b^T \,\middle|\, B_1c^T + B_2d^T\right)$$

and

$$\tau' = \left(\Omega_1c^T + \Omega_2d^T\right)^{-1}\left(\Omega_1a^T + \Omega_2b^T\right) = \left(\tau c^T + d^T\right)^{-1}\left(\tau a^T + b^T\right) = M\tau,$$

where we have used the $\mathbf{Z}$-linearity of Φ and the well-known (but not obvious from the above) symmetry of τ and τ'. □

3.3 Existence of quadratic polynomials with $\mathfrak{n} \mid C$

We would like to apply Theorem 3.15 to arbitrary orders $\mathcal{O}$ and moduli $\mathfrak{n}$. The requirements of the theorem are twofold: On the one hand, the function needs to be invariant under some $\Gamma^0(N)$. Such functions are plentyful, and we provide some interesting examples in §6. On the other hand, we need the existence of a suitable quadratic polynomial; using the terminology of Definitions 2.1 and 3.7, we need the existence of a polarised ideal class T for $(\mathcal{O}, \Phi)$ that is represented by a quadratic polynomial $AX^2 + BX + C$ satisfying

$$\mathfrak{n} \mid C \text{ and furthermore } \gcd(A, \mathfrak{n}) = 1 \text{ and } A \gg 0. \tag{3.9}$$

The following theorem gives a necessary and sufficient criterion for the existence of such a polynomial in the case that $\mathfrak{n}$ is prime to the conductor, which includes the particularly important case $\mathcal{O} = \mathcal{O}_K$. The result assumes the technical condition that a polarised ideal class exists for $(\mathcal{O}, \Phi)$, without which the question of computing a class polynomial is moot.

Theorem 3.18. *Let $\mathfrak{n}$ be an integral ideal of $\mathcal{O}_{K_0}$, let $\mathcal{O} \subseteq K$ be an order of conductor $\mathfrak{f}$ coprime to $\mathfrak{n}$ and containing $\mathcal{O}_{K_0}$, and let $F\mathbf{Z} = \mathfrak{f} \cap \mathbf{Z}$. Suppose that there exists a principally polarised ideal class for $(\mathcal{O}, \Phi)$. Then the following are equivalent.*

(1) Every prime ideal of $\mathcal{O}_{K_0}$ dividing $\mathfrak{n}$ is either split in $\mathcal{O}_K$, or it is ramified and divides $\mathfrak{n}$ with multiplicity 1.

(2) Every principally polarised ideal class for $(\mathcal{O}, \Phi)$ is represented by a polynomial satisfying (3.9) with $\gcd(\mathfrak{n}, \mathfrak{n}^{-1}C) = 1$.

(3) There exists a principally polarised ideal class for $(\mathcal{O}, \Phi)$ that is represented by a polynomial satisfying (3.9).

Furthermore, if (3) holds and $\mathcal{O}_{K_0}$ has narrow class number 1, then

3') the assertion of (3) holds with $A = 1$;

3") the assertion of (3) holds with $C = \nu$, where $\mathfrak{n} = \nu\mathcal{O}_{K_0}$.

We will use the following special case of the Kummer-Dedekind theorem in the proof.

Lemma 3.19. Let $\mathcal{O} \subseteq K$ be an order of conductor $\mathfrak{f}$ and containing $\mathcal{O}_{K_0}$, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{K_0}$ not dividing $\mathfrak{f}$, and let $z \in K$ be a root of a quadratic polynomial $AX^2 + BX + C$ as in Proposition 3.5 with $\mathfrak{p} \nmid \mathfrak{d} = \gcd(A, B, C)$ and such

that $z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ has multiplier ring $\mathcal{O}$. Write $U(X) = X^2 + BX + AC \in \mathcal{O}_{K_0}[X]$ with root $\vartheta = Az$, and let $\widetilde{U}$ be the reduction of U modulo $\mathfrak{p}$.

Then the splitting behaviour of $\mathfrak{p}$ in $\mathcal{O}$ is governed by the factorisation of $\widetilde{U}$ in $(\mathcal{O}_{K_0}/\mathfrak{p})[X]$ as follows. If $\widetilde{U} = \prod_i \widetilde{U_i}^{e_i}$ with monic $\widetilde{U_i}$ and U_i is an arbitrary monic lift of $\widetilde{U_i}$ to $\mathcal{O}_{K_0}[X]$, then the ideals above $\mathfrak{p}$ are given by the $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_K + U_i(\vartheta)\mathcal{O}_K$ of residue field degree $f_i = \deg \widetilde{U_i}$ and ramification index e_i.

Moreover, if $e_1 = 2$, then the remainder of U upon division by U_1, which is an element of $\mathcal{O}_{K_0}$, is not divisible by $\mathfrak{p}^2$. In particular, U has no root modulo $\mathfrak{p}^2$.

Proof. Notice that since $\mathfrak{p}$ is coprime to $\mathfrak{f}$, its splitting in $\mathcal{O}$ is the same as in $\mathcal{O}_K$. By Proposition 3.6, we have $\vartheta = Az \in \mathcal{O}$ and

$$\mathcal{O} = \mathfrak{d}^{-1}\vartheta + \mathcal{O}_{K_0},$$

which implies that the conductor of $\mathcal{O}_{K_0}[\vartheta]$ divides $\mathfrak{f}\mathfrak{d}$. As $\mathfrak{p} \nmid \mathfrak{f}\mathfrak{d}$, the Kummer-Dedekind criterion for relative number field extensions gives the statements of the lemma; see [5, Proposition 2.3.9] and [24, Theorem 8.2].

As the first reference does not include the final statement and the second reference states the results only for $\mathcal{O}_{K_0} = \mathbf{Z}$, we carry out the proof of the final statement. Write $U(X) = q(X)U_1(X) + r$ with $q \in \mathcal{O}_{K_0}[X]$ monic and linear and $r \in \mathcal{O}_{K_0}$. From $v_{\mathfrak{P}_1}(U_1(\vartheta)) = 1$ and $U(\vartheta) = 0$ we deduce $\mathfrak{P}_1 \mid r$, which is equivalent to $\mathfrak{p} \mid r$ since $r \in \mathcal{O}_{K_0}$. This implies $\widetilde{q} = \widetilde{U_1}$, so that $v_{\mathfrak{P}_1}(q(\vartheta)) = 1$ and $v_{\mathfrak{p}}(r) = \frac{1}{2}v_{\mathfrak{P}_1}(r) = \frac{1}{2}v_{\mathfrak{P}_1}(q(\vartheta)U_1(\vartheta)) = 1$. If U had a root modulo $\mathfrak{p}^2$, then we could choose without loss of generality U_1 such that it would have this root modulo $\mathfrak{p}^2$, which would imply the contradiction $\mathfrak{p}^2 \mid r$. □

Proof of Theorem 3.18. The implication (2)⇒(3) is trivial under the assumption that some polarised ideal class exists for $(\mathcal{O}, \Phi)$.

We start with (3)⇒(1). Assume that z is the root of a polynomial satisfying (3.9) and that $(\mathfrak{b}, \xi)$ is the associated principally polarised ideal as in Proposition 3.1. Every prime $\mathfrak{p} \mid \mathfrak{n}$ satisfies $\mathfrak{p} \mid C$. In particular, using the notation of Lemma 3.19, $\widetilde{U}$ is reducible, so the prime $\mathfrak{p}$ is not inert. If $\mathfrak{p}$ is ramified, then we have $\mathfrak{P}_1 = \mathfrak{p}\mathcal{O}_K + \vartheta\mathcal{O}_K$ with $v_{\mathfrak{P}_1}(\mathfrak{p}\mathcal{O}_K) = 2$, hence $v_{\mathfrak{P}_1}(\vartheta) = 1$ and $v_{\mathfrak{p}}(\mathfrak{n}) \leqslant v_{\mathfrak{p}}(C) = v_{\mathfrak{p}}(AC) = v_{\mathfrak{p}}(\mathrm{N}_{K/K_0}(\vartheta)) = 1$.

Now we prove (1)⇒(2). Let T be a principally polarised ideal class for $(\mathcal{O}, \Phi)$; by Proposition 3.9, it can be represented by a quadratic polynomial $AX^2 + BX + C$ with $A \gg 0$ and $\gcd(A, \mathfrak{n}) = 1$. We show how to modify z such that furthermore $\mathfrak{n} \mid C$. Let $\mathfrak{p}$ be a prime dividing $\mathfrak{n}$. As it is coprime to $\mathfrak{f}\mathfrak{d}$ with $\mathfrak{d} = \gcd(A, B, C)$ and split or ramified, the polynomial $\widetilde{U}$ of Lemma 3.19 has a root in $\mathcal{O}_{K_0}/\mathfrak{p}$. If $\mathfrak{p}$ is split, this root is simple, so we may Hensel lift it to a root modulo an arbitrary power of $\mathfrak{p}$. The Chinese remainder theorem allows us to combine the roots into a root $\beta \in \mathcal{O}_{K_0}$ modulo $\mathfrak{n}$. As A is coprime to $\mathfrak{n}$, we may furthermore assume that $A \mid \beta$. Let $\vartheta' = \vartheta - \beta$; its minimal polynomial is $U' = U(X + \beta) = X^2 + B'X + C'$ with $\mathfrak{n} \mid C'$. By (3.2) of Proposition 3.8 we have $B' = 2\beta + B$ and $C' = \beta^2 + B\beta + AC$, which is divisible by A. So $z' = \frac{\vartheta'}{A}$ is a root of the polynomial $AX^2 + B'X + \frac{C'}{A} \in \mathcal{O}_{K_0}$ and is obtained by the $\mathrm{SL}_2(\mathcal{O}_{K_0})$-transformation $z' = z - \beta/A$, where $A \mid \beta$. This shows that (3.9) holds.

We may refine this argument so as to obtain $\gcd(\mathfrak{n}, \mathfrak{n}^{-1}C) = 1$, that is, all primes $\mathfrak{p}$ dividing $\mathfrak{n}$ satisfy $v_{\mathfrak{p}}(\mathfrak{n}) = v_{\mathfrak{p}}(C)$. Given a prime $\mathfrak{p} \mid \mathfrak{n}$, let $e = v_{\mathfrak{p}}(\mathfrak{n})$. If $\mathfrak{p}$ splits, then

there are *unique* Hensel lifts of each of the two distinct roots of $\widetilde{U}$ modulo $\mathfrak{p}$ to a root modulo $\mathfrak{p}^e$ and a root modulo $\mathfrak{p}^{e+1}$. As each element of $\mathcal{O}_{K_0}/\mathfrak{p}^e$ has $\mathrm{N}_{K_0/\mathbf{Q}}(\mathfrak{p}) \geqslant 2$ different lifts to an element of $\mathcal{O}_{K_0}/\mathfrak{p}^{e+1}$, we may choose a root modulo $\mathfrak{p}^e$ that is not a root modulo $\mathfrak{p}^{e+1}$. In this way, the final $\frac{C'}{A}$ is divisible by $\mathfrak{p}^e$, but not by $\mathfrak{p}^{e+1}$. If $\mathfrak{p}$ ramifies in K/K_0, then $e = 1$ and by Lemma 3.19 the quadratic polynomial has no root modulo $\mathfrak{p}^2$, so that $v_\mathfrak{p}(\mathfrak{n}) = v_\mathfrak{p}(C)$ is automatically true.

Assume now that K_0 has narrow class number 1 and that (3) holds. It remains to prove that (3') and (3") hold. We start with the proof of (3"). Write $\mathfrak{n} = \nu\mathcal{O}_{K_0}$ with C/ν totally positive. We have already reached $\nu \mid C$ and $\gcd(A, \nu) = \gcd(C/\nu, \nu) = 1$. Also without loss of generality we can assume $\mathfrak{d} = \gcd(A, B, C) = 1$, even with $A \gg 0$, by the requirement on the narrow class number and $\gcd(\mathfrak{d}, \mathfrak{n}) = 1$.

Then let $z' = z\nu/C$, $A' = A\frac{C}{\nu} \gg 0$, $C' = \nu$ and $B' = B$. We still have $\gcd(A', \nu) = 1$ and hence $\mathfrak{d}' = \gcd(A', B', C') = 1 = \mathfrak{d}$. As we also have $A'z' = Az$, we find that $z'\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ has the same endomorphism ring $\mathcal{O}$ as $z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ by Proposition 3.6, and since $\nu/C \gg 0$ we find that it has the same CM-type. This finishes the proof of (3").

The proof of (3') is exactly the same, but with $z' = Az$, $A' = 1$ and $C' = AC$. □

4 N-systems

Next, we wish to explicitly describe the Galois conjugates of $f(\tau)$ in Theorem 3.15.

Let $\mathcal{T}_{\mathcal{O},\Phi}$ be the set of principally polarised ideal classes for $(\mathcal{O}, \Phi)$ as given in Definition 2.1. The group $\mathfrak{C}_{\mathcal{O},\Phi}(1)$ acts freely on $\mathcal{T}_{\mathcal{O},\Phi}$ via

$$\mathfrak{a}(\mathfrak{b}, \xi) = \left(\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a})^{-1}\mathfrak{b}, \mathrm{N}(\mathfrak{a})\xi\right) \tag{4.1}$$

for $\mathfrak{a} \in \mathcal{I}(F)$. Let $\mathcal{T} = \{T_1, \ldots, T_h\} \subseteq \mathcal{T}_{\mathcal{O},\Phi}$ with $h = |\mathfrak{C}_{\mathcal{O},\Phi}(1)|$ be one orbit under this action. For each T_i, we choose a representative $(\mathfrak{b}_i, \xi_i)$ with $\mathfrak{b}_i = z_i\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ and $\xi_i = \xi(z_i)$, and let τ_i be the period matrix associated to z_i as derived in §3.1. Letting $N = 1$ in Theorem 2.6 shows that if f is a Siegel modular function for the full modular group Γ and a quotient of modular forms with rational q-expansions, then the images of $f(\tau_1)$ under $\mathrm{Gal}(H_{\mathcal{O},\Phi}(1)/K^r)$ are exactly the $f(\tau_i)$.

For larger N, more care needs to be taken. Even if f is a modular function for $\Gamma^0(N)$ such that $f(\tau_1)$ lies in $H_{\mathcal{O},\Phi}(1)$ (for instance under the conditions of Theorem 3.15), then still each element of $\mathcal{T}_{\mathcal{O},\Phi}$ can be given by $[S_{\mathcal{O},\Phi}(1) : S_{\mathcal{O},\Phi}(N)]$ representatives that are pairwise inequivalent modulo $S_{\mathcal{O},\Phi}(N)$, and which may yield different values of f. Our aim in this section is to single out a consistent set of representatives z_i such that the $f(\tau_i)$ are conjugates under $\mathrm{Gal}(H_{\mathcal{O},\Phi}(1)/K^r)$.

We state everything in terms of an arbitrary non-zero ideal $\mathfrak{n} \subseteq \mathcal{O}_{K_0}$ because this will be useful in future work using Hilbert modular forms, while presently we only use the case $\mathfrak{n} = N\mathcal{O}_{K_0}$ with $N \in \mathbf{Z}^{>0}$.

Given z as above, take a quadratic polynomial $AX^2 + BX + C \in \mathcal{O}_{K_0}[X]$ of which it is the root. In the case $g = 1$, there is a unique *primitive* choice, that is, a choice with $A > 0$ and $\gcd(A, B, C) = 1$. For $g \geqslant 2$, the real subfield K_0 may have narrow class number larger than 1 and a primitive quadratic polynomial with root z may not exist. Instead, we used the weaker notion of semiprimitivity modulo an ideal $\mathfrak{m}$ so far, see Definition 3.4 and Proposition 3.5. It turns out that even this

is not enough for our purposes and that we need a stronger notion of compatibility between quadratic polynomials.

Definition 4.1. Let $\mathfrak{m}$ be an integral ideal of $\mathcal{O}_{K_0}$. A pair of quadratic polynomials $A_1X^2 + B_1X + C_1$ and $A_2X^2 + B_2X + C_2 \in \mathcal{O}_{K_0}[X]$ is *equiprimitive modulo* $\mathfrak{m}$ if both are semiprimitive modulo $\mathfrak{m}$ and their discriminants $D_1 = B_1^2 - 4A_1C_1$ and $D_2 = B_2^2 - 4A_2C_2$ are equal.

The following lemma measures, in a sense, how far two semiprimitive polynomials are from being equiprimitive.

Lemma 4.2. Let z_1 and z_2 as in Proposition 3.1 correspond to principally polarised ideals for the same $(\mathcal{O}, \Phi)$. Let z_i be a root of the quadratic polynomial $A_iX^2 + B_iX + C_i \in \mathcal{O}_{K_0}[X]$. Write $\mathfrak{d}_i = \gcd(A_i, B_i, C_i)$, $\delta_i = 2A_iz_i + B_i$ and $\varepsilon = \frac{\delta_1}{\delta_2}$. Then

$$\varepsilon\mathcal{O}_{K_0} = \mathfrak{d}_1\mathfrak{d}_2^{-1}. \tag{4.2}$$

If the two quadratic polynomials are semiprimitive modulo $\mathfrak{m}$, then ε is coprime to $\mathfrak{m}$ in the sense of Definition 2.2 and totally positive.

If the two quadratic polynomials are equiprimitive modulo $\mathfrak{m}$, then $\varepsilon = 1$, that is, $\delta_1 = \delta_2$, and $\mathfrak{d}_1 = \mathfrak{d}_2$.

Proof. Notice that $\delta_i^2 = D_i = B_i^2 - 4A_iC_i$, so that δ_i is a square root of the discriminant D_i. Notice also that $\varepsilon = \frac{A_1\xi_2}{A_2\xi_1}$ for $\xi_i = ((z_i - \overline{z}_i)\lambda)^{-1}$, which are purely imaginary; so ε is an element of K_0.

From Proposition 3.6 we have the two expressions for $\mathcal{O}$ as $\mathcal{O} = \mathfrak{d}_i^{-1}A_iz_i + \mathcal{O}_{K_0}$, leading to

$$2\mathcal{O} + \mathcal{O}_{K_0} = \mathfrak{d}_i^{-1}2A_iz_i + \mathcal{O}_{K_0} = \mathfrak{d}_i^{-1}(2A_iz_i + B_i) + \mathcal{O}_{K_0} = \mathfrak{d}_i^{-1}\delta_i + \mathcal{O}_{K_0},$$

so that

$$\mathfrak{d}_1^{-1}\delta_1 + \mathcal{O}_{K_0} = \mathfrak{d}_2^{-1}\delta_2 + \mathcal{O}_{K_0}.$$

Since $\mathcal{O}_{K_0}$ and the $\mathfrak{d}_i$ are real and the δ_i are purely imaginary, we may "compare real and imaginary parts" and find the desired equality (4.2).

In the semiprimitive case, by definition the $\mathfrak{d}_i$ are coprime to $\mathfrak{m}$ and the A_i are totally positive. So $\varepsilon\mathcal{O}_{K_0} = \mathfrak{d}_1\mathfrak{d}_2^{-1}$ is also coprime to $\mathfrak{m}$. Moreover, the signs of the two real embeddings of ε are those of the embeddings of $\xi_2\xi_1^{-1}$ under the CM type, and since the ξ_i have positive purely imaginary embeddings, their quotient is totally positive.

In the equiprimitive case, the element ε is a totally positive square root of $D_1/D_2 = 1$, so $\varepsilon = 1$, which means $\delta_1 = \delta_2$, so that also $\mathfrak{d}_1 = \mathfrak{d}_2$. □

If the $\mathfrak{d}_i$ were principal, then the quadratic polynomials could be scaled to become primitive. The previous lemma states that even if this is not the case, then at least the ideal $\mathfrak{d}_1\mathfrak{d}_2^{-1}$ is principal and generated (in the case $\Phi_1 = \Phi_2$ we are interested in) by the totally positive ε. So the "measure of nonprimitivity" $\mathfrak{d}_i$, while it cannot necessarily be eleminated, can be made the same for all polynomials. Moreover, the effect of scaling by units of $\mathcal{O}_{K_0}$ is eliminated by the notion of equiprimitivity.

Lemma 4.3. Let $A_iX^2 + B_iX + C_i \in \mathcal{O}_{K_0}[X]$ be semiprimitive quadratic polynomials modulo some ideal $\mathfrak{m}$ of $\mathcal{O}_{K_0}$, with respective roots z_i corresponding to principally polarised ideals for the same $(\mathcal{O}, \Phi)$. Then there is a (unique) $\varepsilon \in K_0^\times$

such that $A_1X^2 + B_1X + C_1$ and $A_2'X^2 + B_2'X + C_2' = \varepsilon(A_2X^2 + B_2X + C_2)$ are equiprimitive modulo $\mathfrak{m}$.

Moreover, if A_2 is coprime to some ideal $\mathfrak{n} \supseteq \mathfrak{m}$ of $\mathcal{O}_{K_0}$, then so is A_2'.

Proof. With the notation of Lemma 4.2, let $\varepsilon = \delta_1\delta_2^{-1}$; then the second polynomial, scaled by ε, has the same discriminant as the first polynomial. But ε is in general not an algebraic integer, so it is a priori not clear that the scaled polynomial still has integral coefficients. However, we have $\mathfrak{d}_2' = \gcd(A_2', B_2', C_2') = \varepsilon\mathfrak{d}_2 = \mathfrak{d}_1$, which is an integral ideal, so A_2', B_2' and C_2' are all integral. Since ε is totally positive and coprime to $\mathfrak{m}$ by Lemma 4.2, semiprimitivity is preserved, and A_2' remains coprime to any divisor $\mathfrak{n}$ of $\mathfrak{m}$ to which A_2 is coprime. Unicity of ε is clear. □

Definition 4.4. Let $\mathfrak{n} \subseteq \mathcal{O}_{K_0}$ be a non-zero ideal. Given quadratic polynomials $Q_i = A_iX^2 + B_iX + C_i$ with root z_i for $i = 1, \ldots, h$, let $\mathfrak{b}_i = z_i\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$, $\xi_i = ((z_i - \overline{z_i})\lambda)^{-1}$ and $T_i = (\mathfrak{b}_i, \xi_i)$.

We call the set $\{Q_1, \ldots Q_h\}$ an $\mathfrak{n}$-*system for* $(\mathcal{O}, \Phi)$ if $\{T_1, \ldots, T_h\}$ is an orbit in $\mathcal{T}_{\mathcal{O},\Phi}$ under the action of $\mathfrak{C}_{\mathcal{O},\Phi}(1)$ and the set consists of equiprimitive polynomials modulo $2F\mathfrak{n}$ that satisfy

(1) $\gcd(A_i, \mathfrak{n}) = 1$,

(2) $B_i \equiv B_j \mod 2\mathfrak{n}$ for all i and j.

If $\mathfrak{n} = N\mathcal{O}_{K_0}$ for some $N \in \mathbf{Z}_{>0}$, then we call $\{Q_1, \ldots, Q_h\}$ an N-*system*.

In the case $g = 1$, the action is transitive and every N-system as in [22, p. 329] is also an N-system in our definition.

We first show that an $\mathfrak{n}$-system always exists; in fact, we give an algorithm to transform any system of representatives into an $\mathfrak{n}$-system. The following is a generalisation of Schertz [22, Proposition 3 on pp. 335–336].

Theorem 4.5. *Let $\mathfrak{n}$ be a non-zero integral ideal of $\mathcal{O}_{K_0}$, and suppose that there is a principally polarised ideal class T_1 for $(\mathcal{O}, \Phi)$. By Proposition 3.9 we may assume that it is represented by a quadratic polynomial $Q_1 = A_1X^2 + B_1X + C_1$ with $A_1, B_1, C_1 \in \mathcal{O}_{K_0}$, $\gcd(A_1, \mathfrak{n}) = 1$ and A_1 totally positive. Then an $\mathfrak{n}$-system $\{Q_1, \ldots, Q_h\}$ for $(\mathcal{O}, \Phi)$ (containing the given Q_1) exists.*

Moreover, for each i the following holds. Let $z = z_i$ be the root of Q_i. Then there exists a transformation $M \in \mathrm{SL}_2(\mathcal{O}_{K_0})$ with $M \equiv 1 \pmod{\mathfrak{n}}$ such that $z' = Mz$ is a root of an equation $A'X^2 + B'X + C'$ with additionally $\gcd(A', F) = 1$, while the $\mathfrak{n}$-system conditions still hold.

Proof. Start with any set of representatives $z_1, \ldots, z_h$ of the orbit containing $(\mathfrak{b}_1, \xi_1)$ for the given z_1. Let $z = z_i$ be any other element of this set; by Proposition 3.9 it can be chosen as a root of $AX^2 + BX + C$ with $\gcd(A, 2F\mathfrak{n}) = 1$ and $A \gg 0$. We scale the quadratic polynomial using Lemma 4.3 to make it equiprimitive modulo $2F\mathfrak{n}$, while preserving the other properties of A.

Now (1) is satisfied, and we look for $\beta \in \mathcal{O}_{K_0}$ such that $z' = z + \beta$ satisfies (2). Note that we then have $A' = A$, $B' = B - 2A\beta$ and $2A'z' + B' = 2Az + B$, so the system remains equiprimitive and (1) remains satisfied.

Since by equiprimitivity the discriminants satisfy $B^2 - 4AC = B_1^2 - 4A_1C_1$, we have $4 \mid B^2 - B_1^2 = (B - B_1)(B + B_1)$. From $B - B_1 \equiv B + B_1 \pmod 2$ we deduce $2 \mid B - B_1$. For (2), it suffices to take β such that $A\beta \equiv \frac{B-B_1}{2} \pmod{\mathfrak{n}}$, which is possible since $\gcd(A, \mathfrak{n}) = 1$. This proves the first paragraph of the theorem.

For the final statement, given $z = z_i$, construct M as follows. Write $F\mathcal{O}_{K_0} = \mathfrak{f}_1\mathfrak{f}_2$ with $\mathfrak{f}_1$ coprime to $\mathfrak{n}$ and $\mathfrak{f}_2$ dividing a power of $\mathfrak{n}$. As in the proof of Proposition 3.9 we can find a matrix $M_{\bmod \mathfrak{f}_1}$ such that, using the notation of (3.2), $\gcd(A', \mathfrak{f}_1) = 1$; and we let $M_{\bmod \mathfrak{n}}$ be the identity matrix. Again, strong approximation [14, Appendix A.3] allows us to lift to a matrix $M \in \mathrm{SL}_2(\mathcal{O}_{K_0})$ with the given reductions modulo $\mathfrak{f}_1$ and $\mathfrak{n}$. Then by (3.2) we have $\gcd(A', \mathfrak{f}_1\mathfrak{n}) = \gcd(A', F\mathfrak{n}) = 1$ and $B \equiv B' \pmod{2\mathfrak{n}}$. Moreover, A' is totally positive, since the total positivity of A and of $4AC - B^2$ (see Proposition 3.5) implies that the quadratic form $AX^2 - BXY + CY^2$, of which A' is a value, is positive definite. Then semiprimitivity is preserved since $\gcd(A', B', C') = \gcd(A, B, C)$ and equiprimitivity follows from a direct computation, or using $\varepsilon = \frac{A\xi'}{A'\xi} = 1$ by (3.3). □

The following is a generalisation of Schertz [22, Theorem 4 on pp. 331–332] from the case $g = 1$.

Theorem 4.6. *Let f satisfy the hypotheses of Theorem 3.15, and let $\tau_1, \dots, \tau_h$ be the period matrices obtained from an N-system $\{Q_1, \dots, Q_h\}$ as above.*

If $N \mid C_1$, then $f(\tau_1)$ is a class invariant; N divides all the C_i, and the set of Galois conjugates of $f(\tau_1)$ over K^r is exactly $\{f(\tau_1), \dots, f(\tau_h)\}$.

Proof. We know from Theorem 3.15 that $f(\tau_1)$ is a class invariant. Divisibility of all the C_i by N follows with a little computation from equiprimitivity and the other properties of an N-system. It remains to prove that the given values are the conjugates.

When taking z_i' and τ_i' as in the final statement of Theorem 4.5, we have $z_i' = M_i z_i$ with $M_i \equiv 1 \pmod{N\mathcal{O}_{K_0}}$, and hence by (3.5) in Proposition 3.10 we get $\tau_i' = M_i'\tau_i$ with $M_i' \equiv 1 \pmod{N}$, so $f(\tau_i) = f(\tau_i')$. In particular, we can assume without loss of generality $z_i = z_i'$ and hence $\gcd(A_i, FN\mathcal{O}_{K_0}) = 1$.

Let $\mathfrak{a}_i \in \mathcal{I}(F)$ be representatives of $\mathfrak{C}_{\mathcal{O},\Phi}(1)$; in fact, as usual in class field theory, we may even assume that $\mathfrak{a}_i \in \mathcal{I}(NF)$. Since the z_i are representatives of an orbit under $\mathfrak{C}_{\mathcal{O},\Phi}(1)$, there are elements $\mu_i \in K^\times$ such that (with the notations of Definition 4.4) $\mathfrak{b}_i = \mu_i^{-1} \mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a}_i)^{-1}\mathfrak{b}_1$ and $\xi_i = \mu_i\overline{\mu_i}\,\mathrm{N}(\mathfrak{a}_i)\xi_1$. It now suffices to prove

$$f(\tau_1)^{\sigma(\mathfrak{a}_i)} = f(\tau_i). \tag{4.3}$$

The action of $\sigma(\mathfrak{a}_i)$ is computed using Theorem 2.6. With the notations of Theorem 2.6 and Proposition 3.2, we have $\mathfrak{c} = \mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a}_i)^{-1}\mathfrak{b}_1 = \mu_i\mathfrak{b}_i$,

$$\mathcal{B} = (z_1 b_{1,1}, z_1 b_{1,2}, b_{2,1}, b_{2,2}) \text{ and } \mathcal{C} = \mu_i(z_i b_{1,1}, z_i b_{1,2}, b_{2,1}, b_{2,2}).$$

By equiprimitivity of an N-system and Lemma 4.2,

$$2A_i z_i + B_i = 2A_1 z_1 + B_1.$$

Let M'_{μ_i} be the matrix of multiplication by μ_i with respect to the K_0-basis $(z_1, 1)$ of K. Then

$$\mu_i(z_i, 1) = \mu_i(z_1, 1)M' = (z_1, 1)M'_{\mu_i}M' \text{ with } M' = \begin{pmatrix} \frac{A_1}{A_i} & 0 \\ \frac{B_1 - B_i}{2A_i} & 1 \end{pmatrix}.$$

Write $\vartheta_i = A_i z_i \in \mathcal{O}$ and $\mathfrak{d}_i = \gcd(A_i, B_i, C_i)$ and notice that by Proposition 3.6 the ideals $A_i\mathfrak{b}_i = \vartheta_i\mathcal{O}_{K_0} + A_i\mathcal{O}_{K_0}$ and $A_i\overline{\mathfrak{b}}_i$ are integral ideals of $\mathcal{O} = \overline{\mathcal{O}}$. Then

$$\begin{aligned}(A_i\mathfrak{b}_i)(A_i\overline{\mathfrak{b}}_i) &= A_i(A_i z_i\mathcal{O}_{K_0} + A_i\mathcal{O}_{K_0})(\overline{z}_i\mathcal{O}_{K_0} + \mathcal{O}_{K_0}) \\ &= A_i(A_i z_i\overline{z}_i\mathcal{O}_{K_0} + A_i(z_i + \overline{z}_i)\mathcal{O}_{K_0} + A_i\mathcal{O}_{K_0} + \vartheta_i\mathcal{O}_{K_0}) \qquad (4.4) \\ &= A_i(\mathfrak{d}_i + \vartheta_i\mathcal{O}_{K_0}) = A_i\mathfrak{d}_i\mathcal{O} \supseteq A_i^2\mathcal{O}.\end{aligned}$$

As A_i is coprime to $NF\mathcal{O}_{K_0}$, this shows that all the $\mathfrak{b}_i$ (including $\mathfrak{b}_1$) are coprime to $NF\mathcal{O}$; with $N_{\Phi^r,\mathcal{O}}(\mathfrak{a}_i)$ being coprime to $NF\mathcal{O}$, this implies, using the notation introduced in Definition 2.4, that μ_i is a unit $\bmod^\times(NF, \mathcal{O})$. We may write it as in Lemma 3.16 as $\mu = \frac{\alpha A_1 z + \beta}{d}$ with $\alpha \in \gcd(A_1, B_1, C_1)^{-1}$, $\beta \in \mathcal{O}_{K_0}$ and, by Proposition 2.3, with a denominator $d \in \mathbf{Z}$ that is coprime to NF. As $C_1 \in N\mathcal{O}_{K_0}$ by assumption, we then see from (3.7) that the bottom left entry of M'_{μ_i} is $0 \bmod^\times(N, NF, \mathcal{O}_{K_0})$.

By properties (1) and (2) of an N-system we find that the bottom left entry of M' is also $0 \bmod^\times(N, NF, \mathcal{O}_{K_0})$, and hence the same holds for the product of the NF-integral matrices $M'_{\mu_i}M'$.

Now the matrix M^T of Theorem 2.6 is obtained from $M'_{\mu_i}M'$ as in (3.8) by replacing elements of K_0 by their matrices with respect to $\mathbf{Z}$-bases of $\mathcal{O}_{K_0}$. In particular, if an element of K_0 is integral at N, then so are the entries of the corresponding $g \times g$ block. And if an element of K_0 is divisible by N, then so are the entries of the corresponding $g \times g$ block. So the transposed matrix M is N-integral with upper right block divisible by N. We conclude that $f^{M^{-1}_{\bmod N}} = f$, whence by Theorem 2.6 we get

$$f(\tau_1)^{\sigma(\mathfrak{a}_i)} = f^{M^{-1}_{\bmod N}}(M\tau_1) = f(M\tau_1).$$

Finally, we have $M\tau_1 = \tau_i$ because τ_1 is computed from the basis $\mathcal{B}$ and τ_i from the basis $\mathcal{C} = \mathcal{B}M^T$, see the last paragraph of the proof of Theorem 3.15. □

5 Complex conjugation

Next, we examine conditions under which class polynomials obtained from $f(\tau)$, which are *a priori* defined over K^r, are in fact invariant under complex conjugation and thus defined over K_0^r. Note that this happens if and only if the complex conjugate $\overline{f(\tau)}$ is a root of the same class polynomial; in the setting of Theorem 4.6, this is equivalent to $\overline{f(\tau)} = f(\tau')$ for some τ' obtained from the same N-system.

Given a principally polarised ideal $(\mathfrak{b}, \xi)$ with $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ and $\xi = \xi(z)$, consider its associated abelian variety $\mathcal{A} = \mathbf{C}^g/\Phi(\mathfrak{b})$. As complex conjugation commutes with the embeddings forming the CM type Φ, it is no surprise that the complex conjugate variety $\overline{\mathcal{A}}$ is induced by $(\mathfrak{b}', \xi')$, where $\mathfrak{b}' = \overline{\mathfrak{b}} = z'\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ with $z' = -\overline{z}$ and $\xi' = \xi$ [18, Proposition 3.5.5], see also Proposition 3.14. It becomes natural to determine conditions under which z and $-\overline{z}$ are roots of quadratic polynomials in a common N-system.

The following result is the analog of [9, Theorems 4.4 and 6.1]; it works for any function f, but imposes severe restrictions on N.

Theorem 5.1. *Under the conditions of Theorem 3.15, assume furthermore that F and N are coprime, and that all primes dividing $N\mathcal{O}_{K_0}$ are ramified in $\mathcal{O}_K$. Then the class polynomial of $f(\tau)$ is an element of $K_0^r[X]$.*

The hypotheses of the theorem include (via Theorem 3.15) that we have $N \mid C$, hence by Theorem 3.18 the ideal $N\mathcal{O}_{K_0}$ is square-free.

Proof. Let $Q = AX^2 + BX + C$ with root z be an element of an N-system for $(\mathcal{O}, \Phi)$ as in Theorem 4.6 such that $f(\tau)$ is not already real. Then $z' = -\overline{z}$ is a root of $Q' = AX^2 + B'X + C$ with $B' = -B$. By Proposition 3.14, one has $\tau' = -\overline{\tau}$ for the period matrices belonging to z and z', respectively. We now consider the q-expansion of f. To $\tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix}$ we associate the values $q_k = e^{2\pi i \tau_k}$. Then $q_k' = \overline{q_k}$. This shows that $\overline{f(\tau)} = f(\tau')$ since f is a quotient of modular forms with rational q-expansions by the hypothesis of Theorem 3.15.

We need to verify whether Q' can be assumed to belong to the same N-system as Q. Notice that the two polynomials are equiprimitive and satisfy $\gcd(A', N) = \gcd(A, N) = \mathcal{O}_{K_0}$ as they have the same A and discriminant. The condition $B \equiv B' = -B \pmod{2N\mathcal{O}_{K_0}}$ is equivalent to $N \mid B$, which follows from Lemma 3.19 since N is a product of distinct primes that ramify in K/K_0 and are coprime to the conductor.

The assertion follows if we can show that $(\mathfrak{b}, \xi)$ and $(\overline{\mathfrak{b}}, \xi)$ belong to the same orbit under $\mathfrak{C}_{\mathcal{O},\Phi}(1)$, that is, there is $\mu \in K^\times$ as in Definition 2.1 and an ideal $\mathfrak{a} \in \mathcal{I}(F)$ as in (4.1), such that $\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a}) = \mu\mathfrak{b}/\overline{\mathfrak{b}}$. This is the case by [25, Lemma I.8.4] with $\mu = \mathrm{N}(\mathfrak{b})$ and $\mathfrak{a}$ the image of $\mathfrak{b}$ under the type norm map from K to K^r. As in the proof of Theorem 4.6, using the last point of Theorem 4.5, we may assume without loss of generality that A is coprime to F. Then the discussion following (4.4) shows that the fractional ideal $\mathfrak{b}$ is coprime to F in the sense of Definition 2.2, so that indeed $\mathfrak{a} \in \mathcal{I}(F)$ as the image of $\mathfrak{b}$ under a type norm map. □

This proof is constructive in the sense that it allows to immediately identify pairs of elements of the N-system that yield complex conjugate values, which almost halves the time needed to compute floating point approximations of the values of f. This also holds for the following result, which is a generalisation of [10, Theorem 3.4]; it makes stronger assumptions on the function than Theorem 5.1, but does not require the primes dividing N to ramify.

Theorem 5.2. *Let f be a function satisfying the conditions of Theorem 3.15, and assume furthermore that f is invariant under the Fricke involution $\iota : \tau \mapsto -N\tau^{-1}$ of $\mathbf{H}_g$.*

Moreover, let $Q_1 = A_1X^2 + B_1X + C_1$ with root z_1 and $Q_2 = C_1/NX^2 + B_1X + A_1N$ with root $z_2 = \frac{A_1N}{C_1}z_1$ be elements of an N-system $\{Q_1, \ldots, Q_h\}$ satisfying $N \mid C_1$.

Then the class polynomial of $f(\tau_1)$ is an element of $K_0^r[X]$.

In fact, for any i, we obtain the complex conjugate of $f(\tau_i)$ as follows. Let $\mathcal{O}_{K^r} = \mathfrak{a}_1, \ldots, \mathfrak{a}_h \in \mathcal{I}(F)$ and $1 = \mu_1, \ldots, \mu_h \in K^\times$ be as in the proof of Theorem 4.6, that is, for all i we have $\mathfrak{b}_i = \mu_i^{-1}\,\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a}_i)^{-1}\mathfrak{b}_1$ and $\xi_i = \mu_i\overline{\mu_i}\,\mathrm{N}(\mathfrak{a}_i)\xi_1$. Let j be such that $\mathfrak{a}_j$ is in the class of $\mathfrak{a}_2\mathfrak{a}_i^{-1}$ in the group $\mathfrak{C}_{\mathcal{O},\Phi}(1)$. Then $\overline{f(\tau_i)} = f(\tau_j)$.

Before we prove the theorem, we have a look at the Fricke involution ι and its relation to the involution $z \mapsto -Nz^{-1}$.

Lemma 5.3. There is an involution $\iota' : \mathbf{H}_g \to \mathbf{H}_g$ with the following properties.

(1) If τ and τ' correspond to respectively z and $-Nz^{-1}$, then $\tau' = \iota'(\tau)$.

(2) Let f be a modular function for $\Gamma^0(N)$. Then f is invariant under ι if and only if it is invariant under ι'.

(3) If $g = 1$, then $\iota = \iota'$.

Proof of Lemma 5.3. Fix a basis $\mathcal{B}_1$ of $\mathcal{O}_{K_0}$ and let $\mathcal{B}_2$ and all period matrices be as in Proposition 3.2. Let $S = [1]_1^2$ be as in Proposition 3.10 and Corollary 3.11. Let $\iota' = \iota_S : \mathbf{H}_g \to \mathbf{H}_g$ be the involution given by $\tau \mapsto -N(S\tau S)^{-1}$. Note that for $g = 1$ we have $\mathcal{B}_1 = \mathcal{B}_2 = (1)$, hence $S = 1$ and $\iota' = \iota$, which proves the third statement.

The first statement is Example 3.13.

Finally, we have $\iota^2 = \mathrm{id}_{\mathbf{H}_g}$ and hence

$$\iota^{-1}\iota'\tau = \iota\iota'\tau = -N(-N(S\tau S)^{-1})^{-1} = S\tau S = \begin{pmatrix} S & 0 \\ 0 & S^{-1} \end{pmatrix} \tau.$$

As the latter matrix is in $\Gamma^0(N)$, we find that f is invariant under ι if and only if it is invariant under ι'. □

Proof of Theorem 5.2. We first consider the case $i = 1$ with $\mathfrak{a}_1 = \mathcal{O}_{K^r}$ and $j = 2$. As in the proof of Theorem 5.1 we have $\overline{f(\tau_1)} = f(-\overline{\tau_1})$ because f is a quotient of modular forms with rational q-expansions. By Proposition 3.14, $-\overline{\tau_1}$ corresponds to $-\overline{z_1}$.

We have $z_1\overline{z_1} = \mathrm{N}_{K/K_0}(z_1) = C_1/A_1$, hence by the hypothesis of the theorem $-\overline{z_1} = -N/z_2$, which by Lemma 5.3(1) corresponds to $\iota(\tau_2)$, so that $-\overline{\tau_1} = \iota(\tau_2)$. As f is invariant under the involution by Lemma 5.3(2), we find $f(-\overline{\tau_1}) = f(\tau_2)$.

Next, we consider $H_{\mathcal{O},\Phi}(1)$ as an extension of K_0^r. The Hilbert class field of $\mathcal{O}_{K^r}$ is an extension of K_0^r with Galois group $\mathcal{I}(F)/\mathcal{P}_{K^r}(F) \rtimes \langle\kappa\rangle$, where $\mathcal{P}_{K^r}(F)$ denotes principal ideals coprime to F, κ is complex conjugation and the multiplication in the semi-direct product is given by $\kappa\sigma(\mathfrak{a})\kappa = \sigma(\overline{\mathfrak{a}})$. In particular, the subextension $H_{\mathcal{O},\Phi}(1)/K_0^r$ is also Galois and has Galois group $\mathfrak{C}_{\mathcal{O},\Phi} \rtimes \langle\kappa\rangle$, where this time we even have $\kappa\sigma(\mathfrak{a})\kappa = \sigma(\overline{\mathfrak{a}}) = \sigma(\mathfrak{a}^{-1})$ since $\overline{\mathfrak{a}}\mathfrak{a} \in S_{\mathcal{O},\Phi}(1)$ with $\mu = \mathrm{N}_{\Phi^r,\mathcal{O}}(\overline{\mathfrak{a}}\mathfrak{a}) = \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{a}) \in \mathbf{Q}$. Using (4.3), we obtain

$$\begin{aligned} f(\tau_i)^\kappa &= f(\tau_1)^{\sigma(\mathfrak{a}_i)\kappa} = f(\tau_1)^{\kappa\sigma(\mathfrak{a}_i^{-1})} = f(\tau_2)^{\sigma(\mathfrak{a}_i^{-1})} = f(\tau_1)^{\sigma(\mathfrak{a}_2\mathfrak{a}_i^{-1})} \\ &= f(\tau_1)^{\sigma(\mathfrak{a}_j)} = f(\tau_j). \end{aligned}$$ □

Besides the condition on the invariance of f under the involution, Theorem 5.2 also adds a condition on the existence of the quadratic polynomial Q_2 in the same N-system, which needs not hold for arbitrary quartic CM fields. We will consider the setting of Theorem 3.18. Then Q_1 can be taken as a semiprimitive polynomial modulo N satisfying (3.9) and $\gcd(C_1/N, N) = \mathcal{O}_{K_0}$. Notice that C_1 is automatically totally positive, since A_1 is totally positive and the discriminant $B_1^2 - 4A_1C_1$ is totally negative by Proposition 3.5. Then we have $A_2 = \frac{C_1}{N}$, $B_2 = B_1$ and $C_2 = A_1N$, leading to a semiprimitive polynomial modulo N and an equiprimitive pair. The congruence conditions of an N-system are trivially verified. Notice that the ideals $\mathfrak{b}_2$ and $\mathfrak{b}_1$ have the same order $\mathcal{O}$ as multiplier rings by Proposition 3.6, since $\mathfrak{d}_1 = \gcd(A_1, B_1, C_1) = \gcd(A_2, B_2, C_2) = \mathfrak{d}_2$: Clearly $\mathfrak{d}_1$ and $\mathfrak{d}_2$ coincide outside N, and both are coprime to N from $\gcd(C_1/N, N) = \mathcal{O}_{K_0}$. The total positivity of A_1 and C_1 together with $\xi_2 = \frac{C_1}{A_1N}\xi_1$ imply that the associated abelian surfaces have complex multiplication by the same $(\mathcal{O}, \Phi)$.

The only non-trivial point to check is whether $(\mathfrak{b}_1, \xi_1)$ and $(\mathfrak{b}_2, \xi_2)$ belong to the same orbit under $\mathfrak{C}_{\mathcal{O},\Phi}(1)$. In dimension 1, there is only one orbit. In dimension 2 for a primitive CM field, the number of orbits is a power of 2 by [25, Theorem III.2.2]. If furthermore $\mathcal{O} = \mathcal{O}_K$, then [25, Lemmata I.3.4 and II.3.5] imply that the total number of isomorphism classes of abelian surfaces with complex multiplication by $(\mathcal{O}_K, \Phi)$ is h_1, the quotient of the ideal class numbers of $\mathcal{O}_K$ and $\mathcal{O}_{K_0}$. If then h_1 is odd, there is again only one orbit. If h_1 is even, the size of the orbit can be computed explicitly, either as the cardinality of $\mathfrak{C}_{\mathcal{O},\Phi}(1)$, computed as a quotient of the ideal class group of K^r, or as in [13, §4] as the cardinality of the image under the reflex type norm of the class group of K^r inside the Shimura class group of K. In many cases, it will equal h_1, and then Theorem 5.2 applies.

6 Suitable functions for $\Gamma^0(N)$

Let us first give some examples of modular functions that satisfy the hypotheses of Theorem 3.15, i.e., functions that are invariant under $\Gamma^0(N)$ and quotients of modular forms with rational q-expansions.

6.1 Functions obtained from Igusa invariants

Igusa defines modular forms h_4, h_6, h_{10} and h_{12} with rational q-expansions that generate the graded ring of modular forms for $\mathrm{Sp}_4(\mathbf{Z})$ [17]; so for $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_4(\mathbf{Z})$ and $M\tau = (a\tau + b)(c\tau + d)^{-1}$, one has $h_k(M\tau) = \det(c\tau + d)^k h_k(\tau)$. Taking quotients of forms of the same weight yields modular functions for $\mathrm{Sp}_4(\mathbf{Z})$ such as

$$j_1 = \frac{h_4 h_6}{h_{10}}, \quad j_2 = \frac{h_4^2 h_{12}}{h_{10}^2} \quad \text{and} \quad j_3 = \frac{h_4^5}{h_{10}^2}$$

known as *absolute Igusa invariants*. Since these are modular functions for the full modular group, their CM values are automatically class invariants.

Alternatively, one may take *simple h_k-quotients*

$$\frac{h_k(\tau/N)}{h_k(\tau)}$$

stable under $\Gamma^0(N)$ or *double h_k-quotients*

$$f = \frac{h_k(\tau/N_1) h_k(\tau/(N_2)}{h_k(\tau) h_k(\tau/(N_1 N_2))} \tag{6.1}$$

stable under $\Gamma^0(N)$ for $N = N_1 N_2$. The latter function is also invariant under the Fricke involution $\iota : \tau \mapsto -N\tau^{-1}$ of Theorem 5.2:

$$f(\iota(\tau)) = \frac{h_k(-N_1\tau^{-1}) h_k(-N_2\tau^{-1})}{h_k(-N_1 N_2 \tau^{-1}) h_k(-\tau^{-1})} = f(\tau),$$

where we have used $h_k(-\tau^{-1}) = h_k(J\tau) = \det(-\tau)^k h_k(\tau)$ for $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbf{Z})$.

As for simple and double eta quotients in dimension 1, the process may be generalized to obtain multiple quotients of h_k, cf. Enge and Schertz [11].

For $k = 10$, similar functions and their square roots have also been studied by de Shalit and Goren [7].

6.2 Theta products

The *theta constant* of characteristic $(\alpha, \beta) \in (\mathbf{Q}^g)^2$ is given by

$$\vartheta[\alpha,\beta](\tau) = \sum_{n \in \mathbf{Z}^g} \exp(\pi i (n+\alpha)^T \tau (n+\alpha) + 2\pi i (n+\alpha)^T \beta)$$

for $\tau \in \mathbf{H}_g$. For α, $\beta \in \{0, 1/2\}^g$, it is a modular form of weight $\frac{1}{2}$ for $\Gamma(8)$ with q-expansion coefficients in $\mathbf{Q}$.

From now on, we consider only the case $g = 2$, and we also use the abbreviated notation

$$\vartheta_{8a_1+4a_2+2b_1+b_2} = \vartheta \begin{pmatrix} a_1/2 \\ a_2/2 \end{pmatrix} \cdot \begin{pmatrix} b_1/2 \\ b_2/2 \end{pmatrix}$$

introduced in [8, §6.2] for a_1, a_2, b_1, $b_2 \in \{0, 1\}$.

Ibukiyama has shown in [15, Theorem A] that the graded ring of modular forms for $\Gamma_0(2)$ is generated by the four forms with rational q-expansions given by

$$\begin{aligned} x &= (\vartheta_0^4 + \vartheta_1^4 + \vartheta_2^4 + \vartheta_3^4)/4 \\ y &= (\vartheta_0\vartheta_1\vartheta_2\vartheta_3)^2 \\ z &= (\vartheta_4^4 - \vartheta_6^4)^2/2^{14} \\ k &= (\vartheta_4\vartheta_6\vartheta_8\vartheta_9\vartheta_{12}\vartheta_{15})^2/2^{12} \end{aligned}$$

of respective weights 2, 4, 4 and 6; notice that $2^{12}\, yk = h_{10}$.

Evalutating these forms in $\tau/2$, we obtain generators for the graded ring of modular forms for $\Gamma^0(2)$ as $X(\tau) = x(\tau/2)$, $Y(\tau) = y(\tau/2)$, $Z(\tau) = z(\tau/2)$ and $K(\tau) = k(\tau/2)$. The smallest weight for which the vector space of forms has dimension at least 2 is 4, with a basis given by X^2, Y and Z. By taking a quotient of two such forms, we obtain a function for $\Gamma^0(2)$, which we expect to yield small class invariants. In fact, the second part of the theorem by Ibukiyama shows that the field of Siegel modular functions for $\Gamma^0(2)$ is rational of transcendence degree 3 and generated by Y/X^2, Z/X^2 and K/X^3.

We may also fix F as one of X, Y, Z or K and consider simple quotients $\frac{F(\tau/N)}{F(\tau)}$, which are functions for $\Gamma^0(2N)$, and double quotients $\frac{F(\tau/N_1)F(\tau/N_2)}{F(\tau)F(\tau/(N_1N_2))}$, which are functions for $\Gamma^0(2N_1N_2)$. Due to its lowest possible weight of 2, the form $F = X$ is most promising in this context.

7 Numerical examples

7.1 Detailed example for a Hilbert class field

To illustrate the approach, we provide an example of a class polynomial where the underlying parameters have been chosen so as to simplify the computations, and

where the N-system can be obtained by hand instead of using the algorithm behind the proof of Theorem 4.5. In particular, we choose K primitive such that K^r has odd class number and K_0^r has class number 1, so that by [25, Theorem I.10.3] the constructed class field is the Hilbert class field of K^r.

Let $K = \mathbf{Q}(x)$ be the primitive non-cyclic CM field with x a root of X^4+57X^2+661 and let $\mathcal{O} = \mathcal{O}_K$ be the maximal order of K. We have $K_0 = \mathbf{Q}(y) = \mathbf{Q}(\sqrt{5})$ with $y = x^2$ a root of $Y^2 + 57Y + 661$, and $\mathcal{O}_{K_0} = \mathbf{Z}[\omega]$ has narrow class number 1, where $\omega = \frac{y+34}{11}$ satisfies $\omega^2 - \omega - 1 = 0$. A generator of the different is $\lambda = 2\omega - 1$, which satisfies $\lambda^2 = 5$.

We choose the CM type $\Phi = (\varphi_1, \varphi_2)$ as

$$\varphi_1(x) = i\sqrt{\frac{57 - 11\sqrt{5}}{2}}, \quad \varphi_2(x) = i\sqrt{\frac{57 + 11\sqrt{5}}{2}},$$

which implies

$$\varphi_1(\lambda) = -\varphi_2(\lambda) = \sqrt{5}, \quad \varphi_1(\omega) = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \varphi_2(\omega) = \frac{1-\sqrt{5}}{2},$$

where all square roots of real numbers are taken positive.

The reflex field of K is given by $K^r = \mathbf{Q}(t) \subseteq \mathbf{C}$ with $t \approx 10.41248483930371i$ a root of $X^4 + 114X^2 + 605$; it contains the real quadratic number $\omega_r = \frac{1+\sqrt{661}}{2}$, where the positive real square root has been taken. The class group $\mathfrak{C}_{\mathcal{O}_K,\Phi}(1)$ has order 3, which indeed equals the class number of K^r.

For reference, we computed the Igusa class polynomial associated to the invariant j_1 of §6 using two different implementations: On one hand, the software `cmh` [12] developed by the first author and Thomé, described in [13], which relies on PARI/GP [1] for the number theoretic computations and C code for multiprecision floating point operations, in particular asymptotically fast evaluations of Siegel modular forms. On the other hand, the second author's RECIP [27] code developed for SageMath [21]; the `class_polynomial` command of this package returns a result proved to be correct by the approaches of Bouyer–Streng [2] and Lauter–Viray [19]. We find that the class polynomial is

$$\begin{aligned} 841X^3 &+ (-5611098752\omega_r - 17741044214880)X^2 \\ &+ (3232391784287232\omega_r - 68899837678801920)X \\ &+ (7331944332391841792\omega_r - 131969791422849515520). \end{aligned}$$

The prime 3 is inert in K_0 and splits in K/K_0, so by Theorem 3.18 we may choose $N = 3$ and are assured of the existence of a $z_1 \in K \backslash K_0$ representing a principally polarised abelian surface, such that z_1 is the root of a quadratic polynomial $[A_1, B_1, C_1]$ (which we use from now on as a short-hand notation for $A_1X^2 + B_1X + C_1$) over $\mathcal{O}_{K_0}$ with $\gcd(A_1, 3) = 1$ and $3 \mid C_1$.

To construct an N-system, we use the class group $\mathrm{Cl}(\mathcal{O}_K)$ of K, which is justified by the following observations. Let

$$\mathfrak{D} = \{(\mathfrak{b}, \nu) : \mathfrak{b} \text{ fractional ideal of } \mathcal{O}_K, \nu \in K_0, \nu \gg 0, \mathrm{N}_{K/K_0}(\mathfrak{b}^{-1}) = \nu\mathcal{O}_{K_0}\}/\sim,$$

where the equivalence relation $\sim$ is given by the subgroup $\{(\mu^{-1}\mathcal{O}_K, \mu\overline{\mu}) : \mu \in K^*\}$. As our CM field K is quartic non-cyclic over $\mathbf{Q}$, the sequence

$$1 \to U_0^+ / \mathrm{N}_{K/K_0}(U) \xrightarrow{\nu \mapsto (\mathcal{O}_K, \nu)} \mathfrak{D} \xrightarrow{(\mathfrak{b},\nu)\mapsto\mathfrak{b}} \mathrm{Cl}(\mathcal{O}_K) \xrightarrow{\mathrm{N}_{K/K_0}} \mathrm{Cl}^+(\mathcal{O}_{K_0}) \to 1 \quad (7.1)$$

is exact, where U denotes the unit group of $\mathcal{O}_K$, U_0^+ the group of totally positive units of $\mathcal{O}_{K_0}$ and Cl^+ the narrow class group [3, Theorem 3.1]. If the fundamental unit of $\mathcal{O}_{K_0}$ has norm -1, then the quotient of unit groups on the left is trivial, see [25, Corollary II.3.4], and $\mathrm{Cl}^+(\mathcal{O}_{K_0}) = \mathrm{Cl}(\mathcal{O}_{K_0})$, which is also often trivial. In our example, both vanish, so $\mathfrak{D}$ is isomorphic to $\mathrm{Cl}(\mathcal{O}_K)$, which is of order 3. Moreover, the action (4.1) of $\mathfrak{C}_{\mathcal{O},\Phi}$ on principally polarised ideal classes suggests to define the following map, which can easily be shown to be a group monomorphism:

$$\mathfrak{C}_{\mathcal{O}_K,\Phi}(1) \to \mathfrak{D}, \quad \mathfrak{a} \mapsto \left(\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a})^{-1}, \mathrm{N}_{K^r/\mathbf{Q}}(\mathfrak{a})\right).$$

In our example, $\mathfrak{C}_{\mathcal{O}_K,\Phi}(1)$ and $\mathfrak{D}$ are both of order 3, so the groups are isomorphic, and the reflex type norm map defines an isomorphism between $\mathfrak{C}_{\mathcal{O}_K,\Phi}(1)$ and $\mathrm{Cl}(\mathcal{O}_K)$. So if we can choose $\mathfrak{b}_1$ as a principal fractional ideal, then the ideals $\mathfrak{b}_i$ derived from the N-system are a system of representatives of $\mathrm{Cl}(\mathcal{O}_K)$.

To do so, we let $A_1 = 1$ to obtain an algebraic integer z_1, let $B_1 = 1$ and, by trial and error, $C_1 = 3\omega + 6$, which is clearly divisible by $N = 3$. The discriminant of this quadratic form is $D = -12\omega - 23$, and it has the root $z_1 = \frac{-x^3-34x-11}{22}$, which can readily be verified to lead to a ξ_1 as in Proposition 3.1 which is positive imaginary under the two embeddings φ_1 and φ_2. Following Corollary 3.3, we obtain for z_1 the period matrix

$$\tau_1 \approx \begin{pmatrix} 0.5 + 4.1498183124610i & 0.5 + 1.8108031294328i \\ 0.5 + 1.8108031294328i & 2.3390151830282i \end{pmatrix}.$$

We compute

$$f_1 = I_4(\tau_1/3)/I_4(\tau_1) \approx 4.31041770567796242256320 - 1.05769871912283540433297i,$$

which is a class invariant by Theorem 3.15.

For the other two elements of $\mathrm{Cl}(K)$, of order 3 and inverses of each other, it is enough to choose a principal prime ideal of $\mathcal{O}_{K_0}$ that splits in $\mathcal{O}_K$ into two non-principal ideals, and set $A_2 = A_3$ as the generator of the ideal of $\mathcal{O}_{K_0}$. We use the ramified ideal of K_0 above 5, which is coprime to $FN = 3$, with generator $\lambda = \sqrt{5}$, twisted by a unit to make it totally positive. Suitable B_i are found by trial and error in the congruence class of B_1 modulo $2N$, and such that the resulting C_i for a quadratic form with discriminant D is integral:

$$\begin{aligned} &A_2 = A_3 = \lambda\omega \gg 0 \\ &B_2 = 1 = B_1 && C_2 = (B_2^2 - D)/(4A_2) = 3 \\ &B_3 = 19 \equiv B_1 \pmod 6 && C_3 = (B_3^2 - D)/(4A_3) = -18\omega + 57 \end{aligned}$$

The resulting floating point polynomial is given by

$$F(X) \approx X^3 + (-1520.8186457788582278232 + 358.629756234205144714067i)X^2 + \ldots;$$

its coefficients are non-integral elements of the reflex field K^r. Guessing their minimal polynomials (using the GP command `algdep (·, 4)`, for instance) reveals a common denominator of $d = 11^4 \cdot 31^2$; taking the index between the polynomial order $\mathbf{Z}[t]$ and its integral closure $\mathcal{O}_{K^r}$ into account, we use $d' = 2^3 \cdot 11 \cdot d$. Integral linear dependencies obtained by the GP command `lindep` between each coefficient

of F and 1, t, t^2 and t^3 yield the class polynomial conjecturally and to high precision as

$$\begin{aligned}
&d'F(X) = 2^3 \cdot 11^5 \cdot 31^2 \cdot X^3 \\
&+ (8560748430t^3 + 11670666480t^2 + 9708000405 30t - 617685149664)X^2 \\
&+ (4018507696 05t^3 - 3039243175155t^2 + 38906895998175t - 180513547604841)X \\
&+ (-2982488461975t^3 + 4298737055525t^2 - 2905182951980 65t - 96097164139933).
\end{aligned}$$

This is a bit larger than the classical polynomial obtained from Igusa invariants above. But maybe it is not very surprising that quotients of Igusa invariants do not result in a gain in size: They are an analogue in dimension 2 of quotients of the elliptic modular form Δ, which is the 24-th power of an η-quotient; only lower powers of such quotients are known to yield smaller class invariants [9].

In our case, it turns out that the $\sqrt{f_i}$ also lie in the Hilbert class field (and thus generate it). The "reason" for this is that h_4 is the square of a Hilbert modular form for $\mathcal{O}_{K_0}$, a situation that we will examine in a future article. The class polynomial with roots $\sqrt{f_1}$, $\sqrt{f_2}$ and $-\sqrt{f_3}$ (where all square roots are taken with positive real part) is conjecturally and to high precision given by

$$\begin{aligned}
F = 2^3 \cdot 11^3 \cdot 31 \cdot X^3 \\
+ (44850t^3 - 26268t^2 + 5007630t - 13168716)X^2 \\
+ (-639765t^3 + 657855t^2 - 68212395t - 21782871)X \\
+ (693935t^3 - 453871t^2 + 68999645t + 182497403).
\end{aligned}$$

7.2 Real example with a ramified level

The following example illustrates Theorem 5.1 for getting class invariants with real class polynomials. We will use the level $N = 2$. Let $K = \mathbf{Q}(x)$ be the primitive non-cyclic CM field with x a root of X^4+18X^2+68 over the real subfield $K_0 = \mathbf{Q}(\sqrt{13})$, and consider again the maximal order $\mathcal{O} = \mathcal{O}_K$. Then the left and right members in (7.1) are again trivial, the group $\mathfrak{D}$ is isomorphic to the class group of K and cyclic of order 8, whereas $\mathfrak{C}_{\mathcal{O}_K,\Phi}(1)$ is cyclic of order 4 according to `cmh`. So it is isomorphic to the subgroup of $\mathrm{Cl}(\mathcal{O}_K)$ generated by the class of $17\mathcal{O}_K + (x-4)\mathcal{O}_K$.

The real subfield of the reflex field is $K_0^r = \mathbf{Q}(\omega_r)$ with $\omega_r = \frac{1+\sqrt{17}}{2}$, with again the usual embedding taking a positive real square root. Using `cmh` and RECIP again, we show that we have the following Igusa class polynomial for K:

$$\begin{aligned}
&19^2 \cdot 59^2 \cdot X^4 + (-13817456632163323131 30\omega_r - 216554819599516122 9000)X^3 \\
&+ (-14847399540341502978206984 1975\omega_r - 23184792855797679274371162 7500)X^2 \\
&+ (-53446717303584740489076774 95421000\omega_r - 83459674335905282938543401 72708000)X \\
&+ (-52888480565700710835194263641602550000\omega_r - 82588086700452716390670199072185720000).
\end{aligned}$$

The prime 2 is inert in $K_0/\mathbf{Q}$ and ramified in K/K_0. Let $\omega = \frac{x^2+10}{2} = \frac{1+\sqrt{13}}{2} \in K$, which generates K_0. We fix the initial form as

$$A_1 = 1, \quad B_1 = 0, \quad C_1 = -2\omega + 10,$$

where C_1 is divisible by $N = 2$. We will thus obtain a class polynomial defined over K_0^r by Theorem 5.1. A 2-system is given by

$$A_2 = A_3 = -\omega - 4, \quad B_2 = -B_3 = 8, \quad C_2 = C_3 = 2\omega - 8,$$
$$A_4 = 9\omega + 19, \quad B_4 = 128, \quad C_4 = -128\omega + 398,$$

so that $f(\tau_1)$ and $f(\tau_4)$ are real and $f(\tau_2)$ and $f(\tau_3)$ are complex conjugates whenever f is a function for $\Gamma^0(2)$ obtained as a quotient of two forms with rational q-expansions. For $f = j_1 = h_4h_6/h_{10}$, we get exactly the polynomial above. For the function $f = X^2/Y$ of §6.2, we obtain to high precision the following class polynomial:

$$\begin{aligned} 19^4 \cdot 59^2 \cdot X^4 &+ (-41960216624328\omega_r - 74372379187680)X^3 \\ &+ (924565238142480\omega_r + 1459228961699136)X^2 \\ &+ (-8404908240715776\omega_r - 13139053032259584)X \\ &+ (10331028745814016\omega_r + 16140510580506624), \end{aligned}$$

which is noticeably smaller than the Igusa class polynomial. Its writing could be shortened further by factoring out a common rational numerator of 72 occurring in all coefficients except for the denominator in front of X^4.

7.3 Real example with a double Igusa quotient

The following example illustrates Theorem 5.2. Let $\mathcal{O}$ be the maximal order of $K = \mathbf{Q}(x)$, the primitive non-cyclic CM field with x a root of $X^4 + 53X^2 + 601$ over the real subfield $K_0 = \mathbf{Q}(\sqrt{5})$. The class group of $\mathcal{O}_K$ is cyclic of order 5 and isomorphic to $\mathfrak{C}_{\mathcal{O}_K,\Phi}(1)$. The real subfield of the reflex field is $K_0^r = \mathbf{Q}(\sqrt{601})$, and we identify the algebraic integer $\omega_r = \frac{1+\sqrt{601}}{2}$ with its positive real embedding. Using `cmh` and RECIP again, we show that we have the following Igusa class polynomial for K:

$$\begin{aligned} &2^{40} \cdot 13^4 \cdot X^5 \\ &+ (-614058542222020444579430 4\omega_r - 3229049049216954473077800 96)X^4 \\ &+ (-966328840322764032741757419 52\omega_r - 413142774420346684276332088 5248)X^3 \\ &+ (-961856435411091691207536138780672\omega_r - 199224267525331686318496120732385 28)X^2 \\ &+ (-281087887503220694727970359035087641 6\omega_r - 325074516288879508580178801914290211 84)X \\ &+ (-394999172899294951535875785508015253080 1\omega_r - 591879683087731591574848056616335060746 74) \end{aligned}$$

We fix $N = 6$, the product of two primes that are inert in $K_0/\mathbf{Q}$ and split in K/K_0. By Theorem 3.18, there is thus a quadratic polynomial $A_1X^2 + B_1X + C_1$ representing a polarised ideal class with $6 \mid C_1$; for instance, $A_1 = 1$, $B_1 = \omega - 7$ and $C_1 = 18$, where $\omega = \frac{1+\sqrt{5}}{2}$. Let z_1 be a root of this polynomial, and choose the CM type in a compatible way; finally let τ_1 be the associated period matrix as in Corollary 3.3. We consider the double Igusa quotient

$$f = \frac{h_{10}(\tau/2)h_{10}(\tau/3)}{h_{10}(\tau)h_{10}(\tau/6)}.$$

Then by Theorem 3.15, $f(\tau_1)$ is a class invariant, and by Theorem 5.2, its minimal polynomial is real.

To determine the class polynomial, we need a 6-system. In a first step, we compute an orbit of the polarised ideal class with which we started under the action of $\mathfrak{C}_{\mathcal{O}_K,\Phi}(1)$; by the above, this amounts to enumerating the class group of K. It turns out that the group, of order 5, admits as representatives $\mathcal{O}_K$ and the four ideals of $\mathcal{O}_K$ of relative norm 2 or 3, so that an orbit is given by the quadratic polynomials $A_iX^2 + B_iX + C_i$ with

$$\begin{aligned} &A_1 = 1, && B_1 = \omega - 7, && C_1 = 18;\\ &A_2 = A_3 = 2, && B_2 = -B_3 = B_1, && C_2 = C_2 = 9;\\ &A_4 = A_5 = 3, && B_4 = -B_5 = B_1, && C_4 = C_5 = 6. \end{aligned}$$

These polynomials trivially have the same discriminant and are thus equiprimitive in the sense of Definition 4.1, and their roots define polarised ideals for the same CM type.

Next, we need to modify the polynomials such that the A_i become coprime to 6. By applying suitable matrices $M_i \in \mathrm{SL}_2(\mathcal{O}_{K_0})$, we modify the ideals, while keeping their classes fixed; Proposition 3.9 suggests a systematic way of finding these matrices, but almost any matrix will work. We choose $M_i = \begin{pmatrix} 1 & 0 \\ -\gamma_i & 1 \end{pmatrix}$, which keeps the C_i, replaces B_i by $B_i + 2\gamma_i C_i$ and A_i by $A_i + \gamma_i B_i + \gamma_i^2 C_i$ by Proposition 3.8. Letting $\gamma_1 = 0$ and $\gamma_2 = \cdots = \gamma_5 = 1$, we obtain

$$\begin{aligned} &A_1 = 1, && B_1 = \omega - 7, && C_1 = 18;\\ &A_2 = \omega + 4, && B_2 = \omega + 11, && C_2 = 9;\\ &A_3 = -\omega + 18, && B_3 = -\omega + 25, && C_3 = 9;\\ &A_4 = \omega + 2, && B_4 = \omega + 5, && C_4 = 6;\\ &A_5 = -\omega + 16, && B_5 = -\omega + 19, && C_5 = 6. \end{aligned}$$

Finally, following the algorithm given in the proof of Theorem 4.5, we apply matrices $M_i = \begin{pmatrix} 1 & \beta_i \\ 0 & 1 \end{pmatrix}$, which by Proposition 3.8 leave the A_i unchanged, and replace B_i by $B_i - 2\beta_i A_i$ and C_i by $C_i - \beta_i B_i + \beta_i^2 A_i$, in order to obtain B_i which are congruent to B_1 modulo 12. We compute $\beta_1 = \beta_4 = 0$, $\beta_2 = 3\omega + 3$, $\beta_3 = 2\omega - 1$ and $\beta_5 = 3\omega - 2$, and obtain a 12-system with

$$\begin{aligned} &A_1 = 1, && B_1 = \omega - 7, && C_1 = 18;\\ &A_2 = \omega + 4, && B_2 = -35\omega - 19, && C_2 = 114\omega + 72;\\ &A_3 = -\omega + 18, && B_3 = -71\omega + 65, && C_3 = -54\omega + 126;\\ &A_4 = \omega + 2, && B_4 = \omega + 5, && C_4 = 6;\\ &A_5 = -\omega + 16, && B_5 = -95\omega + 89, && C_5 = -114\omega + 258. \end{aligned}$$

Letting τ_i denote the associated period matrices obtained by Corollary 3.3, the conjugate $f(\tau_2)$ of the class invariant is real, while $f(\tau_1)$ and $f(\tau_4)$ on one hand and $f(\tau_2)$ and $f(\tau_5)$ on the other hand are complex conjugate pairs. The final class polynomial is given by

$$2^4 \cdot 13^4 \cdot X^5 + (-53182948\omega_r + 551780268)X^4 + (22828729975\omega_r + 1139705021035)X^3$$
$$+ (-46035175179\omega_r - 2244489935231)X^2 + (10035944\omega_r - 1342872664)X - 2^4 \cdot 13^4,$$

which is considerably smaller than the classical Igusa polynomial.

Acknowledgements. We thank Damien Robert for useful discussions. This research was partially funded by ERC Starting Grant ANTICS 278537.

References

[1] Karim Belabas et al. PARI/GP. Bordeaux, 2.7.6 edition, June 2016. `http://pari.math.u-bordeaux.fr/`.

[2] Florian Bouyer and Marco Streng. Examples of CM curves of genus two defined over the reflex field. *LMS J. Comput. Math.*, 18(1):507–538, 2015. `https://arxiv.org/abs/1307.0486`.

[3] Reinier Bröker, David Gruenewald, and Kristin Lauter. Explicit CM theory for level 2-structures on abelian surfaces. *Algebra & Number Theory*, 5(4):495–528, 2011.

[4] Gabriel Cardona and Jordi Quer. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 71–83. World Scientific, 2005. arXiv:math/0207015v1.

[5] Henri Cohen. *Advanced Topics in Computational Number Theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[6] David A. Cox. *Primes of the Form $x^2 + ny^2$ — Fermat, Class Field Theory, and Complex Multiplication*. John Wiley & Sons, New York, 1989.

[7] E. de Shalit and E. Z. Goren. On special values of theta functions of genus two. *Ann. Inst. Fourier (Grenoble)*, 47(3):775–799, 1997.

[8] Régis Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications*. Thèse de doctorat, Ecole polytechnique, Palaiseau, 2006.

[9] Andreas Enge and François Morain. Generalised Weber functions. *Acta Arithmetica*, 164(4):309–341, 2014.

[10] Andreas Enge and Reinhard Schertz. Constructing elliptic curves over finite fields using double eta-quotients. *Journal de Théorie des Nombres de Bordeaux*, 16:555–568, 2004.

[11] Andreas Enge and Reinhard Schertz. Singular values of multiple eta-quotients for ramified primes. *LMS Journal of Computation and Mathematics*, 16:407–418, 2013.

[12] Andreas Enge and Emmanuel Thomé. `cmh` — *Complex multiplication of abelian surfaces*. INRIA, 1.0 edition, March 2014. Distributed under GPL v3+, `http://cmh.gforge.inria.fr/`.

[13] Andreas Enge and Emmanuel Thomé. Computing class polynomials for abelian surfaces. *Experimental Mathematics*, 23(2):129–145, 2014.

[14] Paul B. Garrett. *Holomorphic Hilbert modular forms*. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1990.

[15] Tomoyoshi Ibukiyama. On Siegel modular varieties of level 3. *International Journal of Mathematics*, 2(1):17–35, 1991.

[16] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, 72(3):612–649, 1960.

[17] Jun-Ichi Igusa. On Siegel modular forms of genus two. *American Journal of Mathematics*, 84(1):175–200, 1962.

[18] Serge Lang. *Complex Multiplication*, volume 255 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1983.

[19] Kristin Lauter and Bianca Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. *Amer. J. Math.*, 137(2):497–533, 2015.

[20] Jürgen Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1999.

[21] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.2)*, 2016. `http://www.sagemath.org`.

[22] Reinhard Schertz. Weber's class invariants revisited. *Journal de Théorie des Nombres de Bordeaux*, 14(1):325–343, 2002.

[23] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.

[24] Peter Stevenhagen. The arithmetic of number rings. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 209–266. Cambridge Univ. Press, Cambridge, 2008.

[25] Marco Streng. *Complex multiplication of abelian surfaces*. Phd thesis, Universiteit Leiden, 2010.

[26] Marco Streng. An explicit version of Shimura's reciprocity law for Siegel modular functions. Technical Report 1201.0020, ArXiv, 2012. `http://arxiv.org/abs/1201.0020/`.

[27] Marco Streng. RECIP – REpository of Complex multIPlication sage code. `http://pub.math.leidenuniv.nl/~strengtc/recip/`, 2015.