Schertz style class invariants for quartic CM fields

Andreas Enge, Marco Streng

Schertz style class invariants for higher degree CM fields

Andreas Enge[1] and Marco Streng[2]

28 May 2021

Abstract

Values of Siegel modular functions for $\mathrm{Sp}_4(\mathbf{Z})$ in CM period matrices generate certain unramified abelian class fields of quartic CM fields, and they yield invariants of principally polarised abelian surfaces with a known endomorphism ring. Smaller alternative class invariants, values of modular functions for subgroups generating the same class fields, thus help to speed up constructions in explicit class field theory and public-key cryptography.

Generalising results due to Schertz from elliptic curves to abelian surfaces and from classical modular functions to Siegel modular functions, we show that modular functions for the congruence subgroup $\Gamma^0(N)$ yield class invariants under some splitting conditions on N. We show how to obtain all Galois conjugates of a class invariant by evaluating the same modular function in CM period matrices derived from an N-system. Such a system consists of binary quadratic forms with coefficients in the real-quadratic subfield satisfying certain congruence conditions modulo N. We examine conditions under which the minimal polynomial of a class invariant is real.

Examples show that we may obtain class invariants that are much smaller than in previous constructions.

2010 Mathematics Subject Classification: 11G15, 14K22
Keywords: complex multiplication, abelian surfaces, class invariants

Contents

[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
http://www.math.leidenuniv.nl/~streng/
streng@math.leidenuniv.nl

Acknowledgements. We thank Damien Robert for useful discussions. This research was partially funded by ERC Starting Grant ANTICS 278537, and by the Netherlands Organization for Scientific Research (NWO) Vernieuwingsimpuls.

1 Introduction

Starting from a *CM field* of degree $2g$, that is, an imaginary-quadratic extension K of a totally real number field K_0 of degree g, CM theory allows to characterise principally polarised abelian varieties of dimension g with endomorphism ring an order $\mathcal{O}$ of K. Invariants of such varieties are algebraic and lie in the *Shimura class field* of another CM field, known as the *reflex field* K^r and contained in the Galois closure of K. This class field is contained in the Hilbert class field, the maximal unramified abelian extension, of K^r. So computing these algebraic invariants, that is, computing their minimal polynomials, also called *class polynomials*, has the two-fold application of constructing abelian varieties with properties known in advance, and of explicitly constructing class fields as a first step towards the Hilbert class field of CM fields.

Concretely, the algebraic numbers are obtained as values of a *Siegel modular function* f in a CM period matrix τ in the *Siegel half space* $\mathbf{H}_g$, a subspace of the symmetric $g \times g$-matrices with complex coefficients.

In the case of $g = 1$, corresponding to elliptic curves, the field of Siegel modular functions is generated by the j-function; in the case of $g = 2$, corresponding to abelian surfaces and the topic of this article, it is generated by the absolute Igusa invariants i_1, i_2, i_3 of [21]. It is well-known that the values $f(\tau)$ of any of these functions f in a CM period matrix τ generate the Shimura class field, and algorithms

as well as implementations yielding the associated class polynomials are available [8, 9, 31, 33, 15].

However, the algebraic numbers thus obtained have a rather large height, that is, lead to class polynomials with large coefficients, which require a proportionally large precision and (over-)proportionally much running time for their construction. An approach pursued with success for $g = 1$ is to consider other functions in place of those modular for the full symplectic group $\mathrm{Sp}_{2g}(\mathbf{Z})$, in particular functions f modular for congruence subgroups $\Gamma^0(N)$ of some integer level N. The value $f(\tau)$ then lies in an abelian class field that is generally larger than the Shimura class field (since it is related not to the Hilbert class field of K^r, but to its ray class field of conductor N). However, under certain conditions, $f(\tau)$ lies in the Shimura class field; we then call it a *class invariant*. Compared to the j- or Igusa invariants, these class invariants have a height that is generally smaller by an asymptotically constant factor, which can be as big as 72 [11, Table 7.1], and which significantly increases the range of feasible fields for CM constructions.

The main tool for proving class invariants when $g = 1$ in articles such as [18, 19, 28, 12, 11] is an explicit version of Shimura's reciprocity law, which expresses the action of the absolute Galois group of $\mathbf{Q}$ on $f(\tau)$ via matrix actions on the function f and the argument τ. While mathematically satisfying, these approaches pose difficulties from an algorithmic and implementational point of view. They require a good understanding of Shimura reciprocity, which in general needs to be applied twice: First one shows that the action of the Galois group of the ray class field, where $f(\tau)$ lies *a priori*, over the Shimura class field is trivial on $f(\tau)$, establishing that $f(\tau)$ is a class invariant, essentially by proving a new mathematical theorem every time. In a second step, the action of the Galois group of the Shimura class field over the field K^r is made explicit to obtain the Galois conjugates $f_i(\tau_i)$ of $f(\tau)$ and ultimately the class polynomial, of which they are the roots. It is not straightforward to distill an algorithm that given K returns an integer N, a modular function f of level N, a period matrix τ and a polynomial $H(X) \in K^r[X]$ such that $f(\tau)$ is a class invariant and a root of $H(X)$.

In [28] Schertz uses Shimura reciprocity for $g = 1$ to derive a rather general criterion for proving class invariants: Roughly speaking, when the primes dividing N split or ramify in K, there is a binary quadratic form with coefficients in $\mathbf{Z}$ and with the same discriminant as K that represents N, and for τ a root of this form and f a function for $\Gamma^0(N)$ with rational q-expansion coefficients, the value $f(\tau)$ is a class invariant. In a sense, Schertz applies Shimura reciprocity once and for all; the result can then be used, without recourse to Shimura reciprocity, as a sufficient condition to determine integers N and class invariants $f(\tau)$ where f is a modular function of level N. His criterion has been applied subsequently to prove the existance of families of class invariants [12, 13, 11], which were instrumental in certifying primes of record size with elliptic curve primality proofs [10, 16, 25].

Another important contribution of Schertz's in [28] is to show that all the Galois conjugates of a class invariant $f(\tau)$, with τ derived from a quadratic form as sketched above, can be obtained as $f(\tau_i)$ for the same f, which makes it easier to write optimised implementations. Moreover, all the τ_i are derived from a system of quadratic forms satisfying certain congruence conditions modulo $2N$, a so-called *N-system*, which may easily be obtained algorithmically. Altogether, these advances provide a comprehensive algorithmic treatment of the problem to compute class polynomials attached to class invariants, and have enabled push-button implementations written

in C on top of standard multiprecision floating-point libraries [9].

The present article is a step in the endeavour of generalising this comprehensive algorithmic approach from $g = 1$ to $g = 2$, that is, from elliptic curves to abelian surfaces. From Shimura's adelic formulation of reciprocity theory, the second author has recently obtained an explicit description of the corresponding matrix actions on modular functions and period matrices, which has enabled him to obtain examples of class invariants leading to smaller class polynomials [32]. We use this as a starting point to derive analogues of Schertz's results of [28] in the case of $g = 2$.

First of all, we show how to obtain a class invariant from a quadratic form satisfying a congruence condition modulo an integer N and a Siegel modular function of level N. More precisely, given a quadratic form $AX^2 + BX + C$ with coefficients in the maximal order $\mathcal{O}_{K_0}$ of the real-quadratic subfield K_0 of K, with A coprime to N and C divisible by N, and a function f modular under $\Gamma^0(N)$ and with rational expansion coefficients, we construct in Theorem 3.10 (under some additional technical assumptions) a period matrix τ such that $f(\tau)$ is a class invariant for $(\mathcal{O}, \Phi)$, where $\mathcal{O}$ is an order (not necessarily maximal) of K and Φ a CM type. (The order $\mathcal{O}$ is the ring of endomorphisms of the abelian surface corresponding to the class invariant, and the CM type Φ is an additional complication related to the complex embeddings of K and the polarisation of the abelian surface that is trivial for $g = 1$; more precise definitions are given in §2.2.)

This result provides a sufficient criterion for obtaining a class invariant from a modular function of level N, albeit conditional to the existence of a quadratic form satisfying the congruence conditions modulo N, which is analysed in §3.3. Again, existence of such a form depends on the splitting behaviour of the primes dividing N in K. More precisely, Theorem 3.14 shows that a suitable form exists if and only if the prime ideals dividing $N\mathcal{O}_{K_0}$ either split in $\mathcal{O}_K$, or ramify and occur in $N\mathcal{O}_{K_0}$ with multiplicity 1, and the proof of the theorem provides an explicit algorithm for obtaining such a form.

In a second step we generalise the notion of an N-system, a system of quadratic forms representing a certain class group and satisfying congruence conditions modulo $2N$, in Definition 4.3, and show in Theorem 4.4 that if an N-system exists, it describes all the Galois conjugates of a class invariant obtained from Theorem 3.10. Again, there is a constructive proof for the existence of an N-system, which we pursue in §4.2.

Together these results can be summarised as follows (with some of the notions and notations made precise in later sections):

Theorem 1.1. *Let $\mathcal{O}$ be an order in a CM field K of degree $2g$ that is closed under complex conjugation and contains $\mathcal{O}_{K_0}$, and assume that the different of K_0 is principal. Let Φ be a primitive CM type such that there exists a polarised ideal class for $(\mathcal{O}, \Phi)$. Let N be a positive integer, coprime to the conductor of $\mathcal{O}$, and let f be a Siegel modular function of level N that is the quotient of two modular forms with rational q-expansions and invariant under $\Gamma^0(N)$. Assume that every prime ideal of $\mathcal{O}_{K_0}$ dividing $N\mathcal{O}_{K_0}$ is either split in $\mathcal{O}_K$ or it is ramified and occurs with multiplicity 1 in $N\mathcal{O}_{K_0}$.*

Then there exists a quadratic form $Q = AX^2 + BX + C \in \mathcal{O}_{K_0}[X]$ satisfying $N \mid C$, $\gcd(A, N) = 1$ and $A \gg 0$ giving rise to a period matrix τ with CM by $(\mathcal{O}, \Phi)$ (Theorem 3.14, Proposition 3.2). If τ is not a pole of f, then $f(\tau)$ is a class invariant (Theorem 3.10).

Let $\mathcal{Q} = \{Q_1, \dots, Q_h\}$ be an N-system with $Q_1 = Q$ as in Definition 4.3, which exists according to Theorem 4.7 and which can be computed by Algorithm 4.9. Then the Galois conjugates of the class invariant $f(\tau)$ are exactly the $f(\tau_i)$, where τ_i is the period matrix obtained from the quadratic form $Q_i \in \mathcal{Q}$ (Theorem 4.4).

Unlike some previous work, we do not require that $\mathcal{O}$ be the maximal order $\mathcal{O}_K$ or that $\mathcal{O}_{K_0}$ have (narrow) class number 1. Instead we make the milder assumptions, satisfied by $\mathcal{O}_K$, that the order $\mathcal{O}$ is closed under complex conjugation (which is classical in CM theory, cf. Definition 2.2), and that it contains the maximal order $\mathcal{O}_{K_0}$ of the real subfield (which ensures that the quadratic forms under consideration have coefficients in a Dedekind ring). The only restrictive condition is that the different of K_0 is principal, but it is always satisfied for $g \leqslant 2$ (see the discussion at the beginning of §3.1).

The next step is to exhibit families of modular functions of level N as in Theorem 1.1 leading to interesting families of class invariants. We describe a few constructions in §6. While they yield class invariants with smaller heights than the Igusa invariants, as can be seen from the examples in §7, the gain is not as spectacular as in the case of $g = 1$. This may be due to the absence of a function that could play the role of the Dedekind η-function and requires further work.

As an interlude, one may notice that while the j- and Igusa invariants define class fields over K^r, their class polynomials are actually defined over the smaller field K_0^r. We relate this property to N-systems in §5 and generalise to $g = 2$ criteria under which class invariants for $g = 1$ have been shown to yield real class polynomials in [11, 12]. These are also illustrated by 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 The notion of a class invariant

The aim of this section is to collect the well-known definitions and results on Siegel modular functions, complex multiplication and class field theory to give a precise sense to the following definition.

Definition 2.1. Let on one hand be $f \in \mathcal{F}_N$, the field of Siegel modular functions of level N and dimension g with q-expansion coefficients in the cyclotomic field $\mathbf{Q}(\zeta_N)$; and let on the other hand τ be a CM point for $(\mathcal{O}, \Phi)$, where $\mathcal{O}$ is an order in a CM field K of degree $2g$ and Φ a CM type. Then we call $f(\tau)$ a *CM value* of f.

Generically, $f(\tau)$ is then an element of $H_{\mathcal{O},\Phi}(N)$, the Shimura class field of level N associated to $\mathcal{O}$ and Φ over the reflex field K^r; if $\mathcal{O}$ is the maximal order of K, this is a subfield of the ray class field of conductor N of K^r.

If moreover $f(\tau) \in H_{\mathcal{O},\Phi}(1)$, then we call it a *class invariant*, and by its *class polynomial* we mean its characteristic polynomial

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

where $\mathfrak{C}_{\mathcal{O},\Phi}(1)$ is the Galois group of the abelian extension $H_{\mathcal{O},\Phi}(1)/K^r$.

So CM values of Siegel modular functions of level 1 are trivially class invariants; the interest of the definition stems from the fact that sometimes, under conditions

studied in later chapters of this article, CM values of higher level functions, which are more plentiful, lie in a class field of smaller conductor than expected (and then generically, they generate this class field).

2.1 Siegel modular functions

For a commutative ring R, let the *symplectic group* be

$$\mathrm{Sp}_{2g}(R) = \left\{ M \in \mathrm{Mat}_{2g}(R) : M^T J M = J \right\}, \tag{2.1}$$

where

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \mathrm{id}_g \\ -\mathrm{id}_g & 0 \end{pmatrix}. \tag{2.2}$$

The group $\Gamma = \mathrm{Sp}_{2g}(\mathbf{Z})$ acts on the *Siegel space* $\mathbf{H}_g$, the set of symmetric complex $g \times g$ matrices with positive definite imaginary part, by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = (a\tau + b)(c\tau + d)^{-1} \tag{2.3}$$

for $\tau \in \mathbf{H}_g$, where a, b, c, $d \in \mathrm{Mat}_g(\mathbf{Z})$.

For a positive integer N, let $\Gamma(N)$ be the kernel of the surjective reduction map $\mathrm{Sp}_{2g}(\mathbf{Z}) \to \mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$. Assuming $g > 1$, a *Siegel modular function* of level N is a meromorphic function on $\Gamma(N)\backslash\mathbf{H}_g$; for $g = 1$ the additional condition of the function being meromorphic at the cusps is needed. 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. Of special interest in the following is the space of functions $\mathcal{F}_N$ that can be written as quotients of forms with $a_T \in \mathbf{Q}(\zeta_N)$.

The field $\mathcal{F}_1$ of rational Siegel modular functions of level 1 is well-known for $g \leqslant 2$. If $g = 1$, it is the one-dimensional rational function field over $\mathbf{Q}$ generated by the modular j-invariant. If $g = 2$, then it is the rational function field of dimension 3 over $\mathbf{Q}$ generated, for instance, by the first three of the eight displayed quotients on page 642 of Igusa [21]. An alternative set of generators for $\mathcal{F}_1$ in case $g = 2$ is the set of three invariants i_1, i_2, i_3 of [33], which are more efficient to use in computations.

2.2 CM theory

Throughout the remainder of this article, we use the notations and definitions of [32]. Let $K/\mathbf{Q}$ be a CM field of degree $2g$, that is, an imaginary-quadratic extension of a totally real number field K_0 of degree g. Denote by Δ_0 the discriminant of K_0. By a *CM type* we understand a vector $\Phi = (\varphi_1, \ldots, \varphi_g) : K \to \mathbf{C}^g$ representing the complex embeddings of K up to complex conjugation, and we denote by K^r the associated reflex field, another CM field of degree $2g$ associated to Φ and living in the Galois closure of K, and by K_0^r the totally real subfield of K^r. A CM type is *primitive* if it is not induced by a CM type of a subfield of K; for details, see [31, §I.3]. Either all or no CM types of a given quartic CM field are primitive, so in the case $g = 2$ we may also use the adjective to characterise the field.

Definition 2.2. Let $\mathcal{O}$ be an order of K containing $\mathcal{O}_{K_0}$ that is 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 $\xi' = (\mu\overline{\mu})^{-1}\xi$; the equivalence classes under this relation are called *principally polarised ideal classes*.

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* $(\mathcal{O}, \Phi)$. Since Φ is a primitive CM type, 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 $\mathfrak{b}$, that is, a basis such that the matrix of E_ξ is J as in (2.2). Let $B_1 = (b_1, \ldots, b_g)$ and $B_2 = (b_{g+1}, \ldots, b_{2g})$. Then

$$\tau = \Phi(B_2)^{-1}\Phi(B_1) = \big(\Phi(b_{g+1})|\cdots|\Phi(b_{2g})\big)^{-1}\big(\Phi(b_1)|\cdots|\Phi(b_g)\big) \tag{2.4}$$

is called a *CM point*; it is an element of the Siegel space $\mathbf{H}_g$ defined in §2.1. For a Siegel modular function $f \in \mathcal{F}_N$, it therefore makes sense to consider its *CM value* $f(\tau)$.

2.3 Class fields

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 $\mathfrak{f} = \mathfrak{f}_\mathcal{O} = \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}\} \subseteq \mathcal{O}$.

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 [5, 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 $\mathfrak{f}$, by which we mean that $\mathfrak{a}+\mathfrak{f} = \mathcal{O}$, is invertible, cf. [26, Propositions (12.4) and (12.10)].

Let F be the positive integer such that $\mathfrak{f} \cap \mathbf{Z} = F\mathbf{Z}$. To simplify, from now on we will assume that all integral or fractional ideals are coprime to F. Then additional coprimality conditions in $\mathcal{O}$ can be expressed in terms of the Dedekind ring $\mathcal{O}_K$: An integral ideal $\mathfrak{a}$ of $\mathcal{O}$ is coprime to N if and only if $v_\mathfrak{p}(\mathfrak{a}) = 0$ for all primes $\mathfrak{p} \mid N$, and a fractional $\mathcal{O}$-ideal $\mathfrak{c}$ is coprime to N if and only if it can be written as $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$ with integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}$ that are coprime to N.

We define coprimality and congruences for elements of $K^\times$ as in [32, Definition 4.2].

Definition 2.3. For a positive integer N and for $x \in K^\times$, we say that x is *coprime to NF with respect to $\mathcal{O}$* if one of the following equivalent conditions holds, where $a \mapsto a'$ denotes reduction modulo NF in $\mathcal{O}$.

(1) $x = a/b$ for some $a, b \in \mathcal{O}$ with $a', b' \in (\mathcal{O}/NF\mathcal{O})^\times$ and $b \neq 0$;

(2) $x = a/b$ for some $a \in \mathcal{O}$ and $b \in \mathbf{Z}\backslash\{0\}$ with $a' \in (\mathcal{O}/NF\mathcal{O})^\times$ and $b \in 1+NF\mathbf{Z}$;

(3) for all prime numbers $p \mid NF$, we have $x \in \mathcal{O}_{(p)}^\times$, where

$$\mathcal{O}_{(p)} = \{a/b \in K : a \in \mathcal{O}, b \in \mathbf{Z} \setminus p\mathbf{Z}\};$$

(4) $x\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1}$ for non-zero $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ that are coprime to $NF\mathcal{O}$.

We write $x \equiv 1 \bmod^\times N\mathcal{O}$ to mean that one of the following equivalent conditions holds, which are stronger than the conditions above:

(1') as in (1) above, with additionally $a - b \in N\mathcal{O}$;

(2') as in (2) above, with additionally $a - 1 \in N\mathcal{O}$.

(3') as in (3) above, with additionally $x - 1 \in N\mathcal{O}_{(p)}$ for all prime numbers $p \mid N$.

Now let us return to our specific situation of a 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. 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 NF, 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 non-zero fractional $\mathcal{O}_{K^r}$-ideals coprime to NF to the group of non-zero 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

$$\begin{aligned} S_{\mathcal{O},\Phi}(N) = \{\mathfrak{a} \in \mathcal{I}(NF) \ : \ & \exists \mu \in K \text{ with } N_{\Phi^r}(\mathfrak{a}) = \mu\mathcal{O}_K, \mu\overline{\mu} \in \mathbf{Q}, \\ & \mu \equiv 1 \bmod^\times N\mathcal{O}\}. \end{aligned} \tag{2.5}$$

Let

$$\mathfrak{C}_{\mathcal{O},\Phi}(N) = \mathcal{I}(NF)/S_{\mathcal{O},\Phi}(N). \tag{2.6}$$

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 [32, Theorem 2.5] or [29, Main theorem 3, p. 142]. We denote the *Artin map*, which realises the isomorphism between the class group and the Galois group, by

$$\sigma = \sigma_N : \mathfrak{C}_{\mathcal{O},\Phi}(N) \xrightarrow{\sim} \mathrm{Gal}(H_{\mathcal{O},\Phi}(N)/K^r). \tag{2.7}$$

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. In particular, if $\mathcal{O} = \mathcal{O}_K$, then the field $H_{\mathcal{O}_K,\Phi}(1)$, generated by CM values of Igusa invariants as mentioned at the end of §2.1, is a subfield of the Hilbert class field of K^r.

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

3.1 Polarised ideal classes, symplectic 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 $z \in K$ and z is the root of a quadratic polynomial with coefficients in $\mathbf{Z}$. In higher degree CM fields, one would hope for an analogous representation with $\mathcal{O}_{K_0}$ in the place of $\mathbf{Z}$. While such a representation need not exist in general, it does in a more special situation we assume from now on: Let $\mathcal{O}$ be an order in a CM field K such that $\mathcal{O} \supseteq \mathcal{O}_{K_0}$ and $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$ for some $\lambda \in K_0$. Such a λ exists, for instance, when $g = 1$ (with $\lambda = 1$) and when $g = 2$ (with $\lambda = \sqrt{\Delta_0}$, the square root of the discriminant of K_0).

We then get the following classification of principally polarised ideal classes.

Proposition 3.1. *Let $\mathcal{O}$ be an order in a CM field K such that $\mathcal{O}$ is closed under complex conjugation and contains $\mathcal{O}_{K_0}$. Assume $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$ for some $\lambda \in K_0$.*

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

Conversely, for every CM type Φ of K, every principally polarised ideal class for $(\mathcal{O}, \Phi)$ (cf. Definition 2.2) has such a representative.

Moreover, given $z' \in K$, taking $\mathfrak{b}'$, ξ', and Φ' defined in the same way and assuming that $\mathfrak{b}'$ is a proper fractional $\mathcal{O}$-ideal, the following are equivalent.

(1) we have $\Phi' = \Phi$ and $(\mathfrak{b}', \xi')$ is equivalent to $(\mathfrak{b}, \xi)$,

(2) 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 [31, Theorems I.5.8–9], which are stated there for maximal orders $\mathcal{O}$, but the proof only uses that $\mathcal{O}_{K_0}$ is maximal.

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 for such a polarised ideal.

Proposition 3.2. *Suppose $\mathcal{O} \subseteq \mathcal{O}_{K_0}$ and $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$, 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 (2.4). □

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 take 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: We may at least

avoid any finite set of primes in the greatest common divisor; and, more strongly, we will see that each polarised ideal class has a representative in which the coefficient A is not divisible by any of these primes (Proposition 3.5).

Definition 3.4. Let T be a principally polarised ideal class for $(\mathcal{O}, \Phi)$ and let $P = AX^2 + BX + C \in \mathcal{O}_{K_0}[X]$. Then we say that P *represents* T if there is a root z of P such that the principally polarised ideal $(\mathfrak{b}, \xi)$ obtained from z by Proposition 3.1 is in the class T.

Note that if P represents T, then only one root z of the two roots of T leads to a principally polarised ideal for $(\mathcal{O}, \Phi)$: The other one, $\overline{z}$, leads to $-\xi$, which is purely negative imaginary under the embeddings in Φ instead of purely positive imaginary. Since no confusion is possible, we call this z *the* root of P.

We are interested in polynomials representing polarised ideal classes and satisfying certain congruence conditions modulo integers N; since the proofs are identical, we formulate generalisations modulo ideals $\mathfrak{n}$ of $\mathcal{O}_{K_0}$, which most of the time will be $\mathfrak{n} = N\mathcal{O}_{K_0}$ for the concrete applications.

Proposition 3.5. *Let $\mathfrak{n}$ be a non-zero ideal of $\mathcal{O}_{K_0}$, and assume that $\mathcal{O} \supseteq \mathcal{O}_{K_0}$ and $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$. Then every principally polarised ideal class for $(\mathcal{O}, \Phi)$ is represented by a polynomial $AX^2+BX+C \in \mathcal{O}_{K_0}[X]$ with A totally positive and $\gcd(A\mathcal{O}_{K_0}, \mathfrak{n}) = \mathcal{O}_{K_0}$.*

We prove this proposition in two steps: In a first step, we show that *any* element $z \in K$ is the root of a polynomial satisfying weaker conditions, which we call *semiprimitivity*; in a second step, we use the equivalence relation of polarised ideals to satisfy the stronger condition.

Definition 3.6. Let $\mathfrak{n}$ be a non-zero ideal of $\mathcal{O}_{K_0}$. A quadratic polynomial $AX^2 + BX + C \in \mathcal{O}_{K_0}[X]$ is *semiprimitive modulo* $\mathfrak{n}$ if A is totally positive and furthemore $\gcd(A, B, C, \mathfrak{n}) = 1$, that is,

$$A\mathcal{O}_{K_0} + B\mathcal{O}_{K_0} + C\mathcal{O}_{K_0} + \mathfrak{n} = \mathcal{O}_{K_0}.$$

Proposition 3.7. *Let $\mathfrak{n}$ be a non-zero ideal of $\mathcal{O}_{K_0}$. 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 $\mathfrak{n}$. The discriminant $B^2 - 4AC$ of the polynomial 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 $\mathfrak{d} = A\mathcal{O}_{K_0} + B\mathcal{O}_{K_0} + C\mathcal{O}_{K_0}$. By the strong approximation theorem, for instance [4, 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 $\mathfrak{n}$, $v_\mathfrak{p}(d) \geqslant 0$ 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 $\mathfrak{n}$ and A totally positive.

The discriminant is totally negative as $K = K_0(z) \supsetneq K_0$ is totally imaginary-quadratic. □

According to Proposition 3.1, equivalence of principally polarised ideal classes is related to the action of unimodular matrices over $\mathcal{O}_{K_0}$; it remains to see how this action on the roots z connects with a corresponding action on polynomials.

Proposition 3.8. *Let z be a root of $AX^2+BX+C \in \mathcal{O}_{K_0}[X]$, and 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 $z + \overline{z} = -\frac{B}{A}$. □

Proof of Proposition 3.5. Using Propositions 3.1 and 3.7, we find a semiprimitive quadratic polynomial $AX^2 + BX + C$ modulo N 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 N. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{K_0}$ dividing N, we consider the homogeneous form $A' := A\delta^2 - B\gamma\delta + C\gamma^2$ in δ and γ of Proposition 3.8. Let

$$\begin{aligned} &M_{\mathfrak{p}} = \mathrm{id}, && A' = A && \text{if } \mathfrak{p} \nmid A, \\ &M_{\mathfrak{p}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, && A' = C && \text{if } \mathfrak{p} \nmid C, \mathfrak{p} \mid A, \\ &M_{\mathfrak{p}} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, && A' = A + C - B && \text{otherwise (in which case } \mathfrak{p} \nmid B). \end{aligned} \tag{3.4}$$

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

By Chinese remaindering, we obtain a matrix $M_N \in \mathrm{Sl}_2\left(\mathcal{O}_{K_0}/\operatorname{rad}(N\mathcal{O}_{K_0})\right)$, which can be lifted to a matrix $M \in \mathrm{Sl}_2(\mathcal{O}_{K_0})$, e.g. by strong approximation [17, Appendix A.3]. Replace z by Mz, so A gets replaced by A', which is coprime to N.

Moreover, A' is totally positive, since the total positivity of A and of $4AC - B^2$ (see Proposition 3.7) implies that the quadratic form $AX^2 - BXY + CY^2$, of which A' is a value, is positive definite. □

In what follows, it will also be useful to write the order $\mathcal{O}$ in terms of the coefficients of the quadratic polynomial.

Proposition 3.9. *Under the conditions of Proposition 3.5 we have*

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

where $\mathfrak{d} = A\mathcal{O}_{K_0} + B\mathcal{O}_{K_0} + C\mathcal{O}_{K_0}$ *and* $\mathfrak{d}^{-1} = \{x \in K_0 : x\mathfrak{d} \subseteq \mathcal{O}_{K_0}\}$.

Proof. We first show that under the weaker conditions of Proposition 3.7, the fractional ideal $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ is proper for the order $\mathcal{O}' = \mathfrak{d}^{-1}Az + \mathcal{O}_{K_0}$, that is, it has exactly $\mathcal{O}'$ as its ring of multipliers. To see this, write any $\mu \in K$ as $\mu = xAz+y$ with $x, y \in K_0$. By definition, μ is an element of the ring of multipliers 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 $x\mathfrak{d} \subseteq \mathcal{O}_{K_0}$.

Now under the stronger conditions of Proposition 3.5, the ideal $\mathfrak{b}$ is proper for $\mathcal{O}$, so $\mathcal{O} = \mathcal{O}'$. □

3.2 Class invariants

We now have all ingredients at our disposal to state the first main result of this article, which generalises the first statement in [28, Theorem 4, p. 331] to CM fields of higher degree. For a generalisation of the remainder of [28, Theorem 4], see Theorem 4.4 below. Let

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbf{Z}) : N \mid b \right\}.$$

The main theorem provides a sufficient criterion for a CM value of a function invariant under $\Gamma^0(N)$ to yield a class invariant, cf. Definition 2.1.

Theorem 3.10. *Let $\mathcal{O}$ be an order in a CM field K that is closed under complex conjugation and contains $\mathcal{O}_{K_0}$, assume that $\mathcal{D}_{K_0}$ is principal. Let Φ be a primitive CM type of K, and let N be a positive integer. Suppose that $f \in \mathcal{F}_N$ is the quotient of two modular forms with rational q-expansions and that it is invariant under $\Gamma^0(N)$. Let τ be a CM point obtained as in Proposition 3.2 from a polynomial $AX^2 + BX + C \in \mathcal{O}_{K_0}[X]$ representing a principally polarised ideal class $(\mathfrak{b}, \xi)$ for $(\mathcal{O}, \Phi)$ as in Proposition 3.5, where A and N are coprime, A is totally positive and additionally $N \mid C$.*

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

The main tool in the proof of Theorem 3.10 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. For a commutative ring R, let

$$\mathrm{GSp}_{2g}(R) = \left\{ M \in \mathrm{Mat}_{2g}(R) : M^T J M = tJ \text{ for some } t \in R^\times \right\} \tag{3.5}$$

with J as in (2.2). Let $\mathrm{Sp}_{2g}(R)$ be the subgroup of such matrices with $t = 1$ and $\mathrm{GSp}^+_{2g}(R)$ the subgroup with $t > 0$ for rings R 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 $V \in \mathrm{Sp}_{2g}(R)$.

The action of $\Gamma = \mathrm{Sp}_{2g}(\mathbf{Z})$ on the Siegel space $\mathbf{H}_g$ as given in (2.3) extends to the action $\tau \mapsto (a\tau+b)(c\tau+d)^{-1}$ of the full group $\mathrm{GSp}^+_{2g}(\mathbf{Q})$. and induces an action on Siegel modular functions by $f^M(\tau) = f(M\tau)$ for $M \in \mathrm{GSp}^+_{2g}(\mathbf{Q})$. We also 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.

We use the following explicit formulation of Shimura reciprocity in terms of matrix actions as given in [32, Theorems 2.4 and 2.5].

Theorem 3.11 (Shimura's reciprocity law)**.** *Let $\mathcal{O}$ be an order of K and Φ a primitive CM type. Let $(\mathfrak{b}, \xi)$ be a principally polarised ideal for $(\mathcal{O}, \Phi)$ (cf. Definition 2.2). Let $\mathcal{B}$ be an E_ξ-symplectic basis of $\mathfrak{b}$ and let τ be the corresponding period matrix. Then for any $f \in \mathcal{F}_N$ without a pole in τ, we have $f(\tau) \in H_{\mathcal{O},\Phi}(N)$.*

Let $\sigma : \mathfrak{C}_{\mathcal{O},\Phi}(N) \to \mathrm{Gal}(H_{\mathcal{O},\Phi}(N)/K^r)$ be the Artin map, cf. (2.7)*. The Galois action on $f(\tau)$ is described as follows.*

Let $\mathfrak{f}$ be the conductor of $\mathcal{O}$ and F the positive integer such that $\mathfrak{f} \cap \mathbf{Z} = F\mathbf{Z}$. 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 $M^T \in \mathrm{GL}_{2g}(\mathbf{Q})$ 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

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

The following lemma, used for the proof of Theorem 3.10, describes the multiplication by constants $\mu \in K^\times$ explicitly with respect to different bases. On one hand, let $M'_\mu \in \mathrm{Mat}_2(K_0)$ be the matrix of multiplication by μ with respect to the K_0-basis $(z, 1)$ of K, that is, $\mu(z, 1) = (z, 1)M'_\mu$. On the other hand, 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, $\mu\mathcal{B} = \mathcal{B}M_\mu$. This in turn is related to multiplication in K_0 with respect to the two different bases $\mathcal{B}_1$ and $\mathcal{B}_2$ of $K_0/\mathbf{Q}$ occurring in our choice of symplectic basis $\mathcal{B}$ of Proposition 3.2. So 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,

$$\eta\mathcal{B}_i = \mathcal{B}_j[\eta]_j^i, \tag{3.6}$$

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

Lemma 3.12. With A, B, C, and τ as in Theorem 3.10, let $\mu \in K^\times$. 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 $d \in \mathbf{Z}^{>0}$. Then

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

and

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

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 $\alpha \in \mathfrak{d}^{-1}$. Then we compute

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

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

Under some conditions on μ, the matrix M_μ can be reduced modulo N, and its action on modular functions can be computed explicitly.

Lemma 3.13. With f and τ as in Theorem 3.10, let $\mu \in K^\times$ be coprime to NF with respect to $\mathcal{O}$ (cf. Definition 2.3) with $\mu\overline{\mu} \in \mathbf{Q}$. Then the reduction $(M_\mu)_{\bmod N}$ of M_μ 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 $\mathrm{Tr}_{K/\mathbf{Q}}\left(\xi\overline{\mathcal{B}}^T\mathcal{B}\right)$, where $\mathrm{Tr}_{K/\mathbf{Q}}$ is applied entry-wise to the matrix. Since $\mathcal{B}$ is a symplectic basis, we get

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

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

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

In particular, M_μ is an element of $\mathrm{GSp}_{2g}(\mathbf{Q})$ with the t of (3.5) equal to $\mu\overline{\mu}$. We write $\mu = \frac{\alpha Az+\beta}{d}$ as in Lemma 3.12 with furthermore d coprime to NF (using Definition 2.3(2) and Proposition 3.9). 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 3.10. We use Theorem 3.11 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 (2.5) 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 μ is coprime to NF with respect to $\mathcal{O}$ by condition (4) of Definition 2.3.

Let $\mathcal{B}$ be the symplectic basis of $\mathfrak{b}$ that gave rise to τ. Then $\mathcal{C} = \mu^{-1}\mathcal{B}$ is a symplectic basis of $N_{\Phi^r,\mathcal{O}}(\mathfrak{a})^{-1}\mathfrak{b}$. We get $\mathcal{C} = \mathcal{B}M^T$ with $M = M^T_{\mu^{-1}}$ in the notation of Lemma 3.13. Using Theorem 3.11 and Lemma 3.13, 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 4.7 of [32] states (among other things) 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 the relevant part of Lemma 4.7 of [32]. 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 $N \mid C$

We would like to apply Theorem 3.10 to arbitrary orders $\mathcal{O}$ and integers 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 families of examples in §6. On the other hand, we need the existence of a suitable quadratic polynomial; using the terminology of Definitions 2.2 and 3.4, 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

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

for $\mathfrak{n} = N\mathcal{O}_{K_0}$. 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 $\mathcal{O} = \mathcal{O}_K$. Since the proof is identical, we formulate it directly for the case of a general ideal $\mathfrak{n}$ of $\mathcal{O}_{K_0}$, although later applications will only need the case $\mathfrak{n} = N\mathcal{O}_{K_0}$. The result assumes the technical condition that a polarised ideal class exists for $(\mathcal{O}, \Phi)$, but otherwise the question of computing a class polynomial would be moot.

Theorem 3.14. *Let $\mathfrak{n}$ be a non-zero ideal of $\mathcal{O}_{K_0}$, assume $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$ and that $\mathcal{O} \subseteq K$ is 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 (as in Definition 3.4) 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 3.15. Let $\mathcal{O} \subseteq K$ be an order of conductor $\mathfrak{f}$ and containing $\mathcal{O}_{K_0}$, assume $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$, and 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 3.7 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 3.9, 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 [4, Proposition 2.3.9] and [30, 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 3.14. 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 3.15, $\widetilde{U}$ 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 3.5, 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 3.15 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 $z' = \vartheta'/A$ is a root of the polynomial $AX^2 + B'X + C'/A \in \mathcal{O}_{K_0}$ 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 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 3.15 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 3.9, 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

The main Theorem 3.10 of the preceding section provides a convenient and very generic way of obtaining class invariants in the sense of Definition 2.1. For computing them algebraically, we need a handle on their characteristic polynomials (see also Definition 2.1); otherwise said, we need to explicitly describe their Galois conjugates.

A tool for doing so, introduced for $g = 1$ in [28], are N-systems, quadratic polynomials representing (in the sense of Definition 3.4) the class group of principally polarised ideals and satisfying certain congruence conditions modulo N. We generalise this notion to arbitrary g in §4.1 and prove that an N-system describes a complete set of Galois conjugates of class invariants. Then in §4.2 we prove that N-systems always exist and provide an algorithm to compute them explicitly.

Throughout this section we assume as before that the order $\mathcal{O}$ is closed under complex conjugation and contains $\mathcal{O}_{K_0}$, and that $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$

4.1 Galois conjugates from N-systems

Let $\mathcal{T}_{\mathcal{O},\Phi}$ be the set of principally polarised ideal classes for $(\mathcal{O},\Phi)$ as given in Definition 2.2. The group $\mathfrak{C}_{\mathcal{O},\Phi}(1)$ of (2.6) acts freely on $\mathcal{T}_{\mathcal{O},\Phi}$ via

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

for $\mathfrak{a}\in\mathcal{I}(F)$. Let $\mathcal{T}=\{T_1,\dots,T_h\}\subseteq\mathcal{T}_{\mathcal{O},\Phi}$ with $h=|\mathfrak{C}_{\mathcal{O},\Phi}(1)|$ be one orbit under this action. We let τ_i be the period matrix associated to T_i as described in §3.1. Letting $N=1$ in Theorem 3.11 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 $f(\tau_1)$ is an element of $H_{\mathcal{O},\Phi}(1)$ and its images 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 $f(\tau_1)$ is a class invariant (for instance under the conditions of Theorem 3.10), 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 in general yield different values of f. Our aim in this section is to single out a consistent set of representatives such that the $f(\tau_i)$ are conjugates under $\mathrm{Gal}(H_{\mathcal{O},\Phi}(1)/K^r)$. Notice that Shimura's reciprocity Theorem 3.11 already provides a set of Galois conjugates $f_i(\tau_i)$, which has been used in [32] to compute class polynomials. In the N-system approach, all f_i are actually equal to the same f with which we started, so that only one function needs to be implemented. The corresponding τ_i are also easily computed.

In the light of Proposition 3.5, the classes may be represented by quadratic polynomials $A_iX^2+B_iX+C_i\in\mathcal{O}_{K_0}[X]$, the roots z_i of which determine the τ_i as in Proposition 3.1. If $g=1$, we may choose *primitive* representatives, satisfying $A_i>0$ and $\gcd(A_i,B_i,C_i)=1$. For $g\geqslant 2$, this is still possible if the real subfield K_0 has narrow class number 1, but not in general. Instead, we used the weaker notion of semiprimitivity modulo the ideal $\mathfrak{n}=N\mathcal{O}_{K_0}$ so far, see Definition 3.6 and Proposition 3.7. It turns out that even this is not enough for our purposes and that we need a stronger notion of compatibility between quadratic polynomials.

Again, we state results in terms of an arbitrary non-zero ideal $\mathfrak{n}\subseteq\mathcal{O}_{K_0}$ when their proofs are rigorously identical; this will be useful in future work using Hilbert modular forms. However, for the applications in the remainder of this article only the case that $\mathfrak{n}$ is generated by a rational integer will be needed.

Definition 4.1. Let $\mathfrak{n}$ 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* $\mathfrak{n}$ if both are semiprimitive modulo $\mathfrak{n}$ 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. Assume $\mathcal{O}\supseteq\mathcal{O}_{K_0}$ and $\mathcal{D}_{K_0}=\lambda\mathcal{O}_{K_0}$. Let $A_iX^2+B_iX+C_i\in\mathcal{O}_{K_0}[X]$ with roots z_i for $i\in\{1,2\}$ represent two classes of principally polarised ideals for $(\mathcal{O},\Phi)$. Write $\mathfrak{d}_i=\gcd(A_i,B_i,C_i)$, $\delta_i=2A_iz_i+B_i$ and $\varepsilon=\delta_1\delta_2^{-1}$. Then

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

If the two quadratic polynomials are semiprimitive modulo $\mathfrak{n}$, then ε is coprime to $\mathfrak{n}$ and totally positive.

If the two quadratic polynomials are equiprimitive modulo $\mathfrak{n}$, 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 3.9 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 $\mathfrak{n}$ and the A_i are totally positive. So $\varepsilon\mathcal{O}_{K_0} = \mathfrak{d}_1\mathfrak{d}_2^{-1}$ is also coprime to $\mathfrak{n}$. 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 $\mathfrak{d}_1 = \mathfrak{d}_2$. □

We postpone further discussion of the properties of equiprimitive polynomials to §4.2 in favour of stating the definition of N-systems and the main result on Galois conjugates.

Definition 4.3. Let $\mathfrak{n}$ be a non-zero ideal of $\mathcal{O}_{K_0}$, and let $\mathcal{Q} = \{Q_1, \ldots, Q_h\}$ with $Q_i = A_iX^2 + B_iX + C_i \in \mathcal{O}_{K_0}[X]$ be a set of polynomials representing an orbit of principally polarised ideal classes under the action of $\mathfrak{C}_{\mathcal{O},\Phi}(1)$. We call $\mathcal{Q}$ an $\mathfrak{n}$-*system for* $(\mathcal{O}, \Phi)$ if it consists of equiprimitive polynomials modulo $2F\mathfrak{n}$ that satisfy

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

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

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

In the case $g = 1$, the action of the Galois group on the ideal class group is transitive, and every N-system as in [28, p. 329] is also an N-system in our sense. The following is a generalisation of Schertz [28, Theorem 4, pp. 331–332] from the case $g = 1$.

Theorem 4.4. *Under the hypotheses of Theorem 3.10, let $\tau_1, \ldots, \tau_h$ be the period matrices obtained from an N-system $\{Q_1, \ldots, Q_h\}$ 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 $\{f(\tau_1), \ldots, f(\tau_h)\}$.

For the proof of the theorem, we need to work with ideals coprime to F, or otherwise said, we need the A_i of the $\mathfrak{n}$-system to be coprime also to F. While we could have included this additional condition into Definition 4.3(1) without much loss of generality, we prefer to prove, as in [28], a more fine-grained result with a relaxed condition, which requires less work for Algorithm 4.9 of §4.2. On the other hand, it requires us to prove a few additional auxiliary results.

Lemma 4.5. Let $\mathcal{Q} = \{Q_1, \dots, Q_h\}$ with $Q_i = A_i X^2 + B_i X + C_i \in \mathcal{O}_{K_0}[X]$ and roots z_i be an $\mathfrak{n}$-system. Then for each i there exists a transformation $M_i \in \mathrm{Sl}_2(\mathcal{O}_{K_0})$ with $M_i \equiv 1 \pmod{\mathfrak{n}}$ such that $z_i' = M_i z_i$ is the root of a polynomial $Q_i' = A_i' X^2 + B_i' X + C_i'$ with additionally $\gcd(A_i', F) = 1$, while $\mathcal{Q}' = \{Q_1', \dots, Q_h'\}$ still satisfies the $\mathfrak{n}$-system conditions.

Proof. To lighten the notation, let $Q = AX^2 + BX + C$ be one of the Q_i. The matrix $M = M_i$ is constructed 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 3.5 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 [17, 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 $B \equiv B' \pmod{2\mathfrak{n}}$. As seen in the last paragraph of the proof of Proposition 3.5 on page 12, A' is totally positive since the quadratic form $AX^2 - BXY + CY^2$ 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 that the ε as defined in Lemma 4.2 satisfies $\varepsilon = \frac{A\xi'}{A'\xi} = 1$ by (3.3). □

We need that in this situation the values $f(\tau_i)$ and $f(\tau_i')$ are the same for a Siegel modular function $f \in \mathcal{F}_N$ invariant under $\Gamma^0(N)$; this follows from the way in which the period matrices τ_i and τ_i' derived from the quadratic polynomials are related.

Lemma 4.6. 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 using the notation (3.6),

$$\tau' = M'\tau, \text{ where } M' = \begin{pmatrix} [\alpha]_1^1 & [\gamma]_1^2 \\ [\beta]_2^1 & [\delta]_2^2 \end{pmatrix}^T. \tag{4.3}$$

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

$$\begin{aligned} \mathcal{B}' &= (z', 1)\begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} = (\gamma z + \delta)^{-1}(z, 1)M^T \begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} \\ &= (\gamma z + \delta)^{-1}(z, 1)\begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix}\begin{pmatrix} [\alpha]_1^1 & [\gamma]_1^2 \\ [\beta]_2^1 & [\delta]_2^2 \end{pmatrix}. \end{aligned} \tag{4.4}$$

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

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

□

Proof of Theorem 4.4. We know from Theorem 3.10 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 Lemma 4.5 with $\mathfrak{n} = N\mathcal{O}_{K_0}$, we have $z_i' = M_i z_i$ with $M_i \equiv 1 \pmod{N\mathcal{O}_{K_0}}$, and hence by (4.3) in Lemma 4.6 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 $\gcd(A_i, FN) = 1$.

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 $\mathfrak{a}_i \in \mathcal{I}(NF)$. Let $(\mathfrak{b}_i, \xi_i)$ be the polarised ideals associated to the z_i as in Proposition 3.1. Since these are representatives of an orbit under $\mathfrak{C}_{\mathcal{O},\Phi}(1)$, there are elements $\mu_i \in K^\times$ such that $\mathfrak{b}_i = \mu_i^{-1}\,\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a}_i)^{-1}\mathfrak{b}_1$ and $\xi_i = \mu_i\overline{\mu_i}\,\mathrm{N}(\mathfrak{a}_i)\xi_1$. It now suffices to prove

$$f(\tau_1)^{\sigma(\mathfrak{a}_i)} = f(\tau_i). \tag{4.5}$$

The action of $\sigma(\mathfrak{a}_i)$ is computed using Theorem 3.11. With the notations of Theorem 3.11 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 3.9 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

$$\begin{aligned}(A_i\mathfrak{b}_i)(A_i\overline{\mathfrak{b}}_i) &= A_i(A_i z_i\mathcal{O}_{K_0} + A_i\mathcal{O}_{K_0})(\overline{z}_i\mathcal{O}_{K_0} + \mathcal{O}_{K_0}) \\ &= A_i(A_i z_i\overline{z}_i\mathcal{O}_{K_0} + A_i(z_i + \overline{z}_i)\mathcal{O}_{K_0} + A_i\mathcal{O}_{K_0} + \vartheta_i\mathcal{O}_{K_0}) \\ &= A_i(\mathfrak{d}_i + \vartheta_i\mathcal{O}_{K_0}) = A_i\mathfrak{d}_i\mathcal{O} \supseteq A_i^2\mathcal{O}.\end{aligned} \tag{4.6}$$

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 by Definition 2.3(4) that μ_i is coprime to NF with respect to $\mathcal{O}$. We may write them as in Lemma 3.12 as $\mu_i = \frac{\alpha_i A_1 z_1 + \beta_i}{d_i}$ with $\alpha_i \in \gcd(A_1, B_1, C_1)^{-1}$, $\beta_i \in \mathcal{O}_{K_0}$ and, by Definition 2.3(2), with a denominator $d_i \in \mathbf{Z}$ 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 divisible by N (in the sense that its valuation in every prime ideal $\mathfrak{p} \mid N\mathcal{O}_{K_0}$ is at least $v_\mathfrak{p}(N\mathcal{O}_{K_0})$).

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

Now the matrix M^T of Theorem 3.11 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 3.11 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 3.10. □

4.2 Existence and computation of N-systems

We show that an $\mathfrak{n}$-system in the sense of Definition 4.3 always exists by describing an algorithm to transform any set of polynomials representing an orbit of principally polarised ideal classes into an $\mathfrak{n}$-system. The following is a generalisation of Schertz [28, Proposition 3, pp. 335–336].

Theorem 4.7. *Let $\mathcal{O}$ be an order in a CM field K that is closed under complex conjugation and contains $\mathcal{O}_{K_0}$, assume that $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$, and let $\mathfrak{n}$ be a non-zero integral ideal of $\mathcal{O}_{K_0}$. Suppose that there is a principally polarised ideal class T_1 for $(\mathcal{O}, \Phi)$. By Propositions 3.7 and 3.5 we may assume that it is represented by a quadratic polynomial $Q_1 = A_1X^2 + B_1X + C_1 \in \mathcal{O}_{K_0}[X]$ that is semiprimitive modulo $2FN$ and with $\gcd(A_1, \mathfrak{n}) = 1$ and A_1 totally positive. Then there is an $\mathfrak{n}$-system $\mathcal{Q} = \{Q_1, \ldots, Q_h\}$ for $(\mathcal{O}, \Phi)$ containing the given Q_1.*

Proof. Start with an arbitrary set of polynomials $\{Q_1, \ldots, Q_h\}$ representing an orbit of the principally polarised ideal classes under $\mathfrak{C}_{\mathcal{O},\Phi}(1)$. Let $Q = AX^2 + BX + C$ with root z be one of the Q_i for $i \geqslant 2$. Using Proposition 3.7, we may replace Q by a semiprimitive polynomial modulo $2F\mathfrak{n}$ that still has z as root, and we may change Q and z such that they represent the same class and satisfy $\gcd(A, \mathfrak{n}) = 1$ and Q is still semiprimitive modulo $2F\mathfrak{n}$ (either by simply enforcing $\gcd(A, 2F\mathfrak{n}) = 1$ and $A \gg 0$ by Proposition 3.5, or by a more fine-grained process to obtain $\gcd(A, \mathfrak{n}) = 1$ and $A \gg 0$ while keeping A unchanged modulo the prime ideals dividing $2F$, but not $\mathfrak{n}$, see the discussion after Algorithm 4.9).

In the next step, we scale Q to make it equiprimitive modulo $2F\mathfrak{n}$ with Q_1 while preserving the conditions on A; the following lemma (with $\mathfrak{m} = 2F\mathfrak{n}$) provides the required scaling factor ε.

Lemma 4.8. Let $Q_1 = A_1X^2 + B_1X + C_1$ and $Q = Q_2 = A_2X^2 + B_2X + C_2 \in \mathcal{O}_{K_0}[X]$ be semiprimitive quadratic polynomials modulo some ideal $\mathfrak{m}$ of $\mathcal{O}_{K_0}$, representing principally polarised ideal classes 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 $\mathfrak{n} \mid \mathfrak{m}$ of $\mathcal{O}_{K_0}$, then so is A_2'.

Proof of Lemma 4.8. 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. □

Now (1) of Definition 4.3 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 $\gcd(A, \mathfrak{n}) = 1$. □

For the reader's convenience, we summarise the constructive proof of Theorem 4.7 in the following algorithm, before discussing in more detail how single steps of it can be carried out.

Algorithm 4.9.
INPUT: *A quadratic polynomial Q_1 as in Theorem 4.7*
OUTPUT: *An $\mathfrak{n}$-system $\mathcal{Q}$ containing Q_1*

(1) Enumerate the orbit of the polarised ideal class represented by Q_1 under $\mathfrak{C}_{\mathcal{O},\Phi}(1)$, and let $Q_1, \dots, Q_h$ be the resulting polynomials in $\mathcal{O}_{K_0}[X]$.

(2) For $i = 2, \dots, h$, write $Q_i = A_iX^2 + B_iX + C_i$ and do the following:

(a) Multiply A_i, B_i and C_i by an element in K_0 such that they become elements of $\mathcal{O}_{K_0}$ with $A_i \gg 0$ and $\gcd(A_i, B_i, C_i, 2F\mathfrak{n}) = 1$ as in Proposition 3.7.

(b) Modify Q_i by a matrix in $\mathrm{Sl}_2(\mathcal{O}_{K_0})$ as in Proposition 3.8 such that the new Q_i satisfies $\gcd(A_i, \mathfrak{n}) = 1$, while remaining semiprimitive modulo $2F\mathfrak{n}$.

(c) As in Lemma 4.8, multiply Q_i by $\varepsilon = \delta_1\delta_i^{-1}$ with $\delta_i = 2A_iz_i + B_i$.

(d) As in the proof of Theorem 4.7, let $\beta \in \mathcal{O}_{K_0}$ be such that $A_i\beta \equiv \frac{B_i-B_1}{2} \pmod{\mathfrak{n}}$; replace C_i by $A_i\beta^2 - B_i\beta + C_i$ and B_i by $B_i - 2\beta A_i$.

The details of Step (1) of the algorithm are out of the scope of this article; see, for instance, [31, 15] for the computation of the Shimura class group and the orbits.

Step (2a) is an application of strong approximation as in [4, Corollary 1.2.9]: Given a finite set $\mathcal{P}_0$ of prime ideals of $\mathcal{O}_{K_0}$ (the primes dividing $\gcd(A_i, B_i, C_i, 2F\mathfrak{n})$), integers $e_\mathfrak{p}$ for $\mathfrak{p} \in \mathcal{P}_0$ (the negatives of the exponents of $\mathfrak{p}$ in the gcd), $\mathcal{P}_\infty$ the set of the real embeddings of K_0 and signs $e_v \in \{\pm 1\}$ for $v \in \mathcal{P}_\infty$ (the signs of A_i under v), we need to find an element $\alpha \in \mathcal{O}_{K_0}$ such that $v_\mathfrak{p}(\alpha) = e_\mathfrak{p}$ for $\mathfrak{p} \in \mathcal{P}_0$ and $\mathrm{sign}(v(\alpha)) = e_v$ for $v \in \mathcal{P}_\infty$. In the PARI/GP system for number theory [1], for instance, this is implemented by the command `idealchinese`.

For Step (2b) we construct matrices $M_\mathfrak{p}$ as in (3.4) for every $\mathfrak{p} \mid \mathfrak{n}$. For $\mathfrak{p}$ dividing $2F$, but not $\mathfrak{n}$, we may either also take the matrix of (3.4) (and end up with A_i coprime to $2F\mathfrak{n}$) or use $M_\mathfrak{p} = \mathrm{id}$ (and then not modify A_i modulo this $\mathfrak{p}$); the effort is the same, so in practice we may as well impose coprimality of A_i with $2F\mathfrak{n}$. Chinese remaindering (using again `idealchinese`) provides a matrix $M_{\bmod \mathfrak{m}} \in \mathrm{Sl}_2(\mathcal{O}_{K_0}/\mathfrak{m})$, where $\mathfrak{m} = \mathrm{rad}(2F\mathfrak{n})$, with $M_{\bmod \mathfrak{m}} \equiv M_\mathfrak{p} \pmod{\mathfrak{p}}$. The question is now how to lift this matrix to $\mathrm{Sl}_2(\mathcal{O}_{K_0})$. We may start with an arbitrary lift $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $\mathrm{Mat}_2(\mathcal{O}_{K_0}) \cap \mathrm{Gl}_2(K_0)$. If a and b are not coprime, then we may replace b, using weak

approximation, by a $b' \in \mathcal{O}_{K_0}$ satisfying $b' \equiv b \pmod{\mathfrak{m}}$ and $b' \equiv 1 \pmod{\gcd(a,b)}$; this is possible since $\mathfrak{m}$ and $\gcd(a,b)$ are coprime: Otherwise, the determinant of the matrix would have a non-trivial greatest common divisor with $\mathfrak{m}$. Then we compute Bézout coefficients u and v such that $au+vb=1$ as follows: By weak approximation let $t \in \mathcal{O}_{K_0}$ such that $t \in a\mathcal{O}_{K_0}$ and $t-1 \in b\mathcal{O}_{K_0}$, and let $u = t/a$ and $v = (1-t)/b$. Write $D = ad - bc - 1 \in \mathfrak{m}$. Then $M = \begin{pmatrix} a & b \\ c+vD & d-uD \end{pmatrix}$ has determinant 1 and reduction $M_{\bmod \mathfrak{m}}$ modulo $\mathfrak{m}$. This process is deterministic, polynomial time if the factorisation of $2F\mathfrak{n}$ is known, and produces matrices M with polynomial size coefficients. Alternatively, one may draw random matrices $M \in \mathrm{Sl}_2(\mathcal{O}_{K_0})$ until the resulting Q_i satisfies the desired coprimality conditions.

The value ε of Step (2c) is most conveniently computed as the totally positive square root of $(B_1^2 - 4A_1C_1)(B_i^2 - 4A_iC_i)^{-1}$.

Clearly Step (2d) amounts to yet another application of weak approximation.

5 Complex conjugation

The Igusa class invariants $f(\tau)$ with $f \in \mathcal{F}_1$, which are *a priori* defined over K^r, are in fact invariant under complex conjugation and thus defined over K_0^r. In this section we examine criteria under which this happens for higher level modular functions in our framework. This is not only of theoretical interest, but also leads to a considerable speed-up of algorithms computing class polynomials by floating point approximations.

5.1 Real class polynomials for ramified levels

The class invariant $f(\tau)$ is real if and only if its complex conjugate $\overline{f(\tau)}$ is a root of the same class polynomial; in the setting of Theorem 4.4, 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 $\xi' = \xi$ [23, Proposition 3.5.5]. It becomes natural to determine conditions under which z and $-\overline{z}$ are roots of quadratic polynomials in a common N-system, which is a motivation to have a closer look at $-\overline{z}$.

Lemma 5.1. In the situation of Propositions 3.1 and 3.7, 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 defines a principal polarisation also 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. □

The following result is the analog of [11, Theorems 4.4 and 6.1]; it works for any function f, but imposes severe restrictions on N.

Theorem 5.2. *Under the conditions of Theorem 3.10, 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 3.10) that we have $N \mid C$, hence by Theorem 3.14 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 4.4 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 Lemma 5.1, 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 3.10.

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 3.15 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 2.2 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 [31, 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 4.4, using Lemma 4.5, we may assume without loss of generality that A is coprime to F. Then the discussion following (4.6) shows that the fractional ideal $\mathfrak{b}$ is coprime to F, 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.

5.2 Real class polynomials from the Fricke involution

The following result is a generalisation of [12, Theorem 3.4]; it makes stronger assumptions on the function than Theorem 5.2, but does not require the primes dividing N to ramify. Again, it provides an explicit criterion for pairing up elements of the N-system leading to complex conjugate roots of the class polynomial.

Theorem 5.3. *Let f be a function satisfying the conditions of Theorem 3.10, 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 $K_0^r[X]$.*

More precisely, 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 4.4, 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 several involutions occurring in our context, such as the Fricke involution ι and the involutions $z \mapsto -N/z$ and $z \mapsto -1/z$.

Lemma 5.4. Using the notation of (3.6), let $S = [1]_1^2$. This is a symmetric matrix in $\mathrm{Gl}_g(\mathbf{Z})$.

If $\alpha, \beta, \gamma, \delta \in \mathbf{Q}$ in the situation of Lemma 4.6, then we have

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

Proof. Notice that S is the basis 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 Proposition 3.8 and Lemma 4.6. □

Example 5.5. 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 Lemma 5.4 shows the following result.

Example 5.6. 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 Lemma 5.4.

Lemma 5.7. 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 $-N/z$, 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. 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 Lemma 5.4. 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 5.6.

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 5.3. We first consider the case $i = 1$ with $\mathfrak{a}_1 = \mathcal{O}_{K^r}$ and $j = 2$. As in the proof of Theorem 5.2 we have $\overline{f(\tau_1)} = f(-\overline{\tau_1})$ because f is a quotient of modular forms with rational q-expansions. By Lemma 5.1, $-\overline{\tau_1}$ 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 5.7(1) corresponds to $\iota(\tau_2)$, so that $-\overline{\tau_1} = \iota(\tau_2)$. As f is invariant under the involution by Lemma 5.7(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 (4.5), 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 5.3 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 3.14. 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 3.7. Then we have $A_2 = C_1/N$, $B_2 = B_1$ 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 3.9, 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 [31, Theorem III.2.2]. If furthermore $\mathcal{O} = \mathcal{O}_K$, then [31, 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 [15, §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 5.3 applies.

6 Families of functions for $\Gamma^0(N)$

In this section we provide a few examples of families of functions for $g = 2$ that can be used in the context of Theorem 3.10, 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 $\mathrm{Sp}_4(\mathbf{Z})$ [22]; 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*

$$f = \frac{h_k(\tau/N_1)h_k(\tau/(N_2)}{h_k(\tau)h_k(\tau/(N_1N_2))} \tag{6.1}$$

stable under $\Gamma^0(N)$ for $N = N_1N_2$. The latter function is also invariant under the Fricke involution $\iota : \tau \mapsto -N\tau^{-1}$ of Theorem 5.3:

$$f(\iota(\tau)) = \frac{h_k(-N_1\tau^{-1})h_k(-N_2\tau^{-1})}{h_k(-N_1N_2\tau^{-1})h_k(-\tau^{-1})} = f(\tau),$$

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 iterated to obtain multiple quotients of h_k, cf. [13].

For $k = 10$, similar functions and their square roots have also been studied by de Shalit and Goren [6].

6.2 Theta products

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

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

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

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

introduced in [7, §6.2] for a_1, a_2, b_1, $b_2 \in \{0, 1\}$.

Ibukiyama has shown in [20, 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 Algorithm 4.9. 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 [31, 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` [14] developed by the first author and Thomé, described in [15], 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 [34] code developed for SageMath [27]; the `class_polynomial` command of this package returns a result proved to be correct by the approaches of Bouyer–Streng [2] and Lauter–Viray [24]. 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 3.14 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

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

where the equivalence relation $\sim$ is given by the subgroup $\left\{(\mu^{-1}\mathcal{O}_K, \mu\overline{\mu}) : \mu \in K^\times\right\}$. 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 [33, Lemma 4.15], 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 $\mathfrak{C}_{\mathcal{O}_K,\Phi}(1)$ 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

$$\tau_1 \approx \begin{pmatrix} 0.5 + 4.14981831246 10i & 0.5 + 1.81080312943 28i \\ 0.5 + 1.81080312943 28i & 2.33901518302 82i \end{pmatrix}.$$

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 3.10.

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

$$F(X) \approx X^3 + (-1520.81864577885822782 32 + 358.62975623420514471 4067i)X^2 + ...;$$

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 $d'F$ and 1, t, t^2 and t^3 yield the class polynomial conjecturally and to high precision as

$$\begin{aligned} d'F(X) &= 2^3 \cdot 11^5 \cdot 31^2 \cdot X^3 \\ &+ (8560748430t^3 + 11670666480t^2 + 970800040530t - 617685149664)X^2 \\ &+ (401850769605t^3 - 3039243175155t^2 + 38906895998175t - 180513547604841)X \\ &+ (-2982488461975t^3 + 4298737055525t^2 - 290518295198065t - 96097164139933). \end{aligned}$$

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 [11].

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

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

7.2 Real example with a ramified level

The following example illustrates Theorem 5.2 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:

$$\begin{aligned}&19^2 \cdot 59^2 \cdot X^4 + (-1381745663216332313130\omega_r - 2165548195995161229000)X^3 \\ &+ (-1484739954034150297820698419 75\omega_r - 2318479285579767927437116 27500)X^2 \\ &+ (-5344671730358474048907677495421000\omega_r - 8345967433590528293854340172708000)X \\ &+ (-5288848056570071083519426364160255 0000\omega_r - 8258808670045271639067019907 2185720000).\end{aligned}$$

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 5.2. A 2-system is given by

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

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 5.3. 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:

$$
\begin{aligned}
&2^{40} \cdot 13^4 \cdot X^5 \\
&+ (-6140585422220204445794304\omega_r - 32290490492169544730778096)X^4 \\
&+ (-96632884032276403274175741952\omega_r - 413142774420346684276332088524 8)X^3 \\
&+ (-96185643541109169120753613878067 2\omega_r - 19922426752533168631849612073238528)X^2 \\
&+ (-28108788750322069472797035903508764 16\omega_r - 32507451628887950858017880191429021184)X \\
&+ (-39499917289929495153587578550801525308 01\omega_r - 59187968308773159157484805661633506074674)
\end{aligned}
$$

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 3.14, 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 3.10, $f(\tau_1)$ is a class invariant, and by Theorem 5.3, 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 3.5 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 4.7, 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

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

which is considerably smaller than the classical Igusa polynomial.

References

[1] Karim Belabas et al. PARI/GP. Bordeaux, 2.11.0 edition, July 2018. `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. arXiv: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] Henri Cohen. *Advanced Topics in Computational Number Theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

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

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

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

[8] Andreas Enge. The complexity of class polynomial computation via floating point approximations. *Mathematics of Computation*, 78(266):1089–1107, 2009.

[9] Andreas Enge. `cm` — *Complex multiplication of elliptic curves*. INRIA, 0.3.1 edition, September 2020. Distributed under GPL v3+, `http://cm.multiprecision.org/`.

[10] Andreas Enge and François Morain. Comparing invariants for class fields of imaginary quadratic fields. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory — ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, page 252–266, Berlin, 2002. Springer-Verlag.

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

[12] 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.

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

[14] 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/`.

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

[16] J. Franke, T. Kleinjung, F. Morain, and T. Wirth. Proving the primality of very large numbers with fastECPP. In Duncan Buell, editor, *Algorithmic Number Theory — ANTS-VI*, volume 3076 of *Lecture Notes in Computer Science*, pages 194–207, Berlin, 2004. Springer-Verlag.

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

[18] Alice Gee. Class invariants by Shimura's reciprocity law. *Journal de Théorie des Nombres de Bordeaux*, 11(1):45–72, 1999.

[19] Alice Gee and Peter Stevenhagen. Generating class fields using Shimura reciprocity. In J. P. Buhler, editor, *Algorithmic Number Theory — ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 441–453, Berlin, 1998. Springer-Verlag.

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

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

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

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

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

[25] F. Morain. Implementing the asymptotically fast version of the elliptic curve primality proving algorithm. *Mathematics of Computation*, 76(257):493–505, 2007.

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

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

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

[29] 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.

[30] 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.

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

[32] Marco Streng. An explicit version of Shimura's reciprocity law for Siegel modular functions. preprint, arXiv:1201.0020, 2012.

[33] Marco Streng. Computing Igusa class polynomials. *Math. Comp.*, 83(285):275–309, 2014. arXiv:0903.4766.

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