Schertz style class invariants for higher degree CM fields

Andreas Enge, Marco Streng

Schertz style class invariants for higher degree CM fields

Andreas Enge[1] and Marco Streng[2]

June 10, 2024

Abstract

Special values of Siegel modular functions for $\mathrm{Sp}_{2g}(\mathbf{Z})$ generate class fields of CM fields. They also yield abelian varieties with a known endomorphism ring. Smaller alternative values of modular functions that lie in the same class fields (class invariants) thus help to speed up the computation of those mathematical objects.

We show that modular functions for the subgroup $\Gamma^0(N) \subseteq \mathrm{Sp}_{2g}(\mathbf{Z})$ yield class invariants under some splitting conditions on N, generalising results due to Schertz from classical modular functions to Siegel modular functions. 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 quadratic polynomials with coefficients in the real-quadratic subfield satisfying certain congruence conditions modulo N. We also 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

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, the theory of *complex multiplication (CM)* characterises 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. This class field is contained in the Hilbert class field of K^r, its maximal unramified abelian extension. So computing these algebraic invariants has the two-fold application of

[1]INRIA, Université de Bordeaux, CNRS, CANARI, 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.

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. We compute the minimal polynomials of these values, called *class polynomials*.

In the case of $g = 1$, corresponding to elliptic curves, the field of Siegel modular functions of level 1 is generated by the j-function. In the case of $g = 2$, corresponding to abelian surfaces and the main focus of this article, it is generated by the absolute Igusa invariants i_1, i_2, i_3 of [30]. It is well-known that the values $f(\tau)$ 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 for $g = 1$ [10, 17, 49, 9] and $g = 2$ [43, 50, 8, 20, 47, 48, 19].

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 f which are 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 [13, 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 [23, 24, 39, 14, 13] 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 [39] 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 quadratic polynomial with coefficients in $\mathbf{Z}$ and with the same discriminant as K that represents N, and for τ a root of this polynomial 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 an integer N and a modular function f of level N such that $f(\tau)$ is a class invariant. His criterion has been applied subsequently to prove

the existence of families of class invariants [14, 15, 13], which were instrumental in certifying primes of record size with elliptic curve primality proofs [12, 21, 36].

Another important contribution of Schertz's in [39] is to show that all the Galois conjugates of a class invariant $f(\tau)$, with τ derived from a quadratic polynomial 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 polynomials 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 $g \geqslant 2$, that is, from elliptic curves to abelian surfaces and higher dimensional abelian varieties. From Shimura's adelic formulation of reciprocity theory, the second author has 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 [45]. We use this as a starting point to derive analogues of Schertz's results of [39] in the case of $g \geqslant 2$.

First of all, we show how to obtain a class invariant from a Siegel modular function of level N and a quadratic polynomial that satisfies a congruence condition modulo N. More precisely, given a function f modular under $\Gamma^0(N)$ and with rational q-expansion coefficients, and a quadratic polynomial $AX^2 + BX + C$ 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, we construct in Theorem 3.9 a period matrix τ such that $f(\tau)$ is a class invariant.

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 polynomial satisfying the congruence conditions modulo N, which is analysed in §3.4. Again, existence of such a polynomial depends on the splitting behaviour of the primes dividing N in K. More precisely, Theorem 3.17 shows that a suitable polynomial 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 polynomial.

In a second step we generalise the notion of an N-system, a system of quadratic polynomials 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 3.9. 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 polynomial $Q = AX^2+BX+C \in \mathcal{O}_{K_0}[X]$ satisfying $N \mid C$, $\gcd(A, N) = 1$ and $A \gg 0$, which gives rise to a period matrix τ with CM by $(\mathcal{O}, \Phi)$ (Theorem 3.17, Proposition 3.2). If τ is not a pole of f, then $f(\tau)$ is a class invariant (Theorem 3.9).

Let $\mathcal{Q} = \{Q_1, \ldots, Q_h\}$ be an N-system with $Q_1 = Q$ as in Definition 4.3, which exists according to Theorem 4.5 and which can be computed by Algorithm 4.7. 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 polynomial $Q_i \in \mathcal{Q}$ (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 necessary for the existence of principal polarisations, cf. Definition 2.3), and that it contains the maximal order $\mathcal{O}_{K_0}$ of the real subfield (which ensures that the quadratic polynomials under consideration have coefficients in a Dedekind ring). The only restrictive condition is that the different of K_0 is principal, but this 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 totally real field K_0^r. We relate this property to N-systems in §5 and generalise to $g \geqslant 2$ criteria under which class invariants for $g = 1$ have been shown to yield real class polynomials in [14, 13]. 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 needed 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* or *special value* of f.

Generically, the value $f(\tau)$ is then an element of $H_{\mathcal{O},\Phi}(N)$, the *Shimura ray class field of level N* associated to $\mathcal{O}$ and Φ over the reflex field K^r of K (see Section 2.3); if $\mathcal{O}$ is the maximal order of K, this class field 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

$$\prod_{[\mathfrak{a}]\in\mathfrak{C}_{\mathcal{O},\Phi}(1)} \left(X - f(\tau)^{\sigma([\mathfrak{a}])}\right). \tag{2.1}$$

where $\mathfrak{C}_{\mathcal{O},\Phi}(1)$ is the CM class group of (2.6) and σ is the Artin map realising its isomorphism with 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

$$\mathrm{Sp}_{2g}(R) = \left\{\mathbb{M} \in \mathrm{Mat}_{2g}(R) : \mathbb{M}^T\mathbb{J}\mathbb{M} = \mathbb{J}\right\}, \tag{2.2}$$

where

$$\mathbb{J} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \mathrm{id}_g \\ -\mathrm{id}_g & 0 \end{pmatrix}. \tag{2.3}$$

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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = (a\tau + b)(c\tau + d)^{-1} \tag{2.4}$$

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 $\mathcal{F}_N$ of functions 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 1-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 [30], or alternatively by the three invariants i_1, i_2, i_3 of [47], 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 [45]. 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.

Definition 2.2. Let $\mathcal{O}$ be an order of K. By a *fractional $\mathcal{O}$-ideal* we understand a non-zero, finitely generated $\mathcal{O}$-submodule of K. We call it a *proper fractional $\mathcal{O}$-ideal* if $\mathcal{O}$ is its exact ring of multipliers in K.

By a *CM type* we understand a vector $\Phi = (\varphi_1, \dots, \varphi_g) : K \to \mathbf{C}^g$ 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. 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 itself.

Definition 2.3. Let $\mathcal{O}$ be an order of K containing $\mathcal{O}_{K_0}$, and let Φ be a primitive CM type of K. Let $\mathfrak{b}$ be a proper fractional $\mathcal{O}$-ideal in the sense of Definition 2.2. 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 last 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 the pair $(\mathfrak{b}, \xi)$ is called a *principally polarised ideal* for $(\mathcal{O}, \Phi)$.

Two such pairs $(\mathfrak{b}, \xi)$ and $(\mathfrak{b}', \xi')$ are called *equivalent* if there is a $\mu \in K^\times$ such that $\mathfrak{b}' = \mu\mathfrak{b}$ and $\xi' = (\mu\overline{\mu})^{-1}\xi$. There are finitely many equivalence classes under this relation; we call them *principally polarised ideal classes* of $(\mathcal{O}, \Phi)$, and denote the class of $(\mathfrak{b}, \xi)$ by $[(\mathfrak{b}, \xi)]$ and the set of all classes by $\mathcal{T}_{\mathcal{O},\Phi}$.

Note that the existence of a principally polarised ideal class implies that $\mathcal{O}$ is closed under complex conjugation, as it is the ring of multipliers of both $\mathfrak{b}$ and $\overline{\mathfrak{b}}$.

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

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

One may choose a symplectic $\mathbf{Z}$-basis $\mathcal{S} = (b_1, \dots, b_{2g})$ of $\mathfrak{b}$, that is, a basis such that the matrix of E_ξ is $\mathbb{J}$ as in (2.3). Let $\mathcal{S}_1 = (b_1, \dots, b_g)$ and $\mathcal{S}_2 = (b_{g+1}, \dots, b_{2g})$. Then

$$\tau = \Phi(\mathcal{S}_2)^{-1}\Phi(\mathcal{S}_1) = \big(\Phi(b_{g+1})|\cdots|\Phi(b_{2g})\big)^{-1}\big(\Phi(b_1)|\cdots|\Phi(b_g)\big) \tag{2.5}$$

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 [7, Proposition 7.20], 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. [37, 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 $\mathcal{O}_K$: A non-zero integral ideal $\mathfrak{a}$ of $\mathcal{O}$ is coprime to NF if and only if $\mathfrak{a} = \mathfrak{a}_K \cap \mathcal{O}$ for an integral ideal $\mathfrak{a}_K$ of $\mathcal{O}_K$ such that $v_{\mathfrak{p}}(\mathfrak{a}_K) = 0$ for all primes $\mathfrak{p} \mid NF$, and a fractional $\mathcal{O}$-ideal $\mathfrak{c}$ is coprime to NF if and only if it can be written as $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$ with non-zero integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}$ that are coprime to NF.

We define coprimality and congruences for elements of $K^\times$ as in [45, Definition 4.2].

Definition 2.4. 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 $a \in \mathcal{O}$ and $b \in \mathbf{Z}\backslash\{0\}$ with $a' \in (\mathcal{O}/NF\mathcal{O})^\times$ and $b \in 1+NF\mathbf{Z}$;

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

We write $x \equiv 1 \bmod^\times N\mathcal{O}$ to mean that the following condition holds:

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

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 fractional $\mathcal{O}_{K^r}$-ideals coprime to NF to the group of fractional $\mathcal{O}$-ideals coprime to NF.

Let the *CM class group* for $(\mathcal{O}, \Phi)$ of level N be defined by

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

where

$$\begin{aligned} S_{\mathcal{O},\Phi}(N) = \{\mathfrak{a} \in \mathcal{I}(NF) \ : \ & \exists \mu \in K^\times \text{ with } \mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a}) = \mu\mathcal{O},\ \mu\overline{\mu} \in \mathbf{Q}, \\ & \mu \equiv 1 \bmod^\times N\mathcal{O}\}. \end{aligned} \tag{2.7}$$

The CM class group of level 1, $\mathfrak{C}_{\mathcal{O},\Phi}(1)$, acts freely on the set $\mathcal{T}_{\mathcal{O},\Phi}$ of principally polarised ideal classes as given in Definition 2.3, via

$$[\mathfrak{a}] \cdot [(\mathfrak{b}, \xi)] = \left[(\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a})^{-1}\mathfrak{b}, \mathrm{N}(\mathfrak{a})\xi)\right], \tag{2.8}$$

where $[\mathfrak{a}]$ denotes the class of $\mathfrak{a} \in \mathcal{I}(F)$. So the role of the type norm map is to connect the realms of CM class groups of K^r and of principally polarised ideal classes of K.

For a fixed CM point τ derived from a principally polarised ideal class in $\mathcal{T}_{\mathcal{O},\Phi}$, 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. Then $H_{\mathcal{O},\Phi}(N)$ is, independently of τ, the abelian class field of K^r with Galois group isomorphic to $\mathfrak{C}_{\mathcal{O},\Phi}(N)$, see [45, Theorem 2.5] or [41, Main theorem 3, p. 142]. We call $H_{\mathcal{O},\Phi}(N)$ the *Shimura ray class field of level* N, or if $N = 1$ simply the *Shimura class field*. We denote the *Artin map*, which realises the isomorphism between the class group and the Galois group, by

$$\sigma = \sigma_N : \mathfrak{C}_{\mathcal{O},\Phi}(N) \xrightarrow{\sim} \mathrm{Gal}(H_{\mathcal{O},\Phi}(N)/K^r). \tag{2.9}$$

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, the field $H_{\mathcal{O}_K,\Phi}(1)$ 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 and symplectic bases

To get an explicit handle on ideals and polarised ideal classes, we would like to mimic the situation for $g = 1$, where ideals are represented as $z\mathbf{Z} + \mathbf{Z}$ with $z \in K$. 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 $\lambda \in K_0$, where $\mathcal{D}_{K0}$ is the different of 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 K be a CM field such that $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$ for some $\lambda \in K_0$.*

To $z \in K \setminus K_0$ associate $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ and $\xi = ((z - \overline{z})\lambda)^{-1}$. Then $\mathcal{O} = \{x \in K : x\mathfrak{b} \subseteq \mathfrak{b}\}$ is an order in K that is stable under complex conjugation and contains $\mathcal{O}_{K_0}$, the set $\Phi = \{\varphi : K \to \mathbf{C} \mid \varphi(\xi) \in i\mathbf{R}^{>0}\}$ is a CM type of K, and the pair $(\mathfrak{b}, \xi)$ is a principally polarised ideal for $(\mathcal{O}, \Phi)$.

Conversely, every principally polarised ideal class for any CM type Φ of K and any order $\mathcal{O}$ of K that is stable under complex conjugation and contains $\mathcal{O}_{K_0}$ has such a representative.

Proof. The results are [46, Theorems I.5.8–9], where they are stated for maximal orders $\mathcal{O}$, but the proof only uses that $\mathcal{O}_{K_0}$ is maximal. □

We may then write down an explicit symplectic basis and period matrix for such a polarised ideal.

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

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

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 $\mathcal{S}$ 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 (2.5). □

Corollary 3.3. Let $g = 2$ and $\lambda = \sqrt{\Delta_0}$. In the situation of Proposition 3.1, let $(\varphi_1, \varphi_2) = \Phi$, and to simplify the notation, write $\alpha_i = \varphi_i(\alpha)$ for any $\alpha \in K$. A symplectic basis $\mathcal{S}$ 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 $\mathcal{S} = (z\omega, z, -1, 1 - \omega)$. If Δ_0 is even, let $\omega = \frac{\lambda}{2}$; then $\mathcal{S} = (z\omega, z, -1, -\omega)$. 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 or $b_{2,2} = 1 - \omega$ 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 $\lambda_2 = -\lambda_1$. □

3.2 Quadratic polynomials and polarised ideal classes

We have seen in Proposition 3.1 that a polarised ideal class can be represented by a pair $(\mathfrak{b}, \xi)$, in which the fractional ideal $\mathfrak{b}$ satisfies $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ for some $z \in K$, and $\xi \in K$ is also computed as a function of z. So ultimately z determines the class. It is conveniently given as the root of a quadratic polynomial $AX^2 + BX + C$ with coefficients $A, B, C \in \mathcal{O}_{K_0}$.

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

Note that if Q 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 $\overline{\xi} = -\xi$, which is purely negative imaginary under the embeddings in Φ instead of purely positive imaginary. So when the context is clear, we call this z *the* root of Q. (Another way to look at this is to notice that $\overline{z}$ leads by Proposition 3.1 to the same order $\overline{\mathcal{O}} = \mathcal{O}$ and to the CM type $\overline{\Phi}$, which is equivalent to Φ by CM theory; or without recourse to theory, one notices that replacing z by $\overline{z}$ and Φ by $\overline{\Phi}$ in Proposition 3.2 and Corollary 3.3 leads to the same value of τ.)

For $g = 1$, one usually assumes Q to be primitive, that is, with coprime coefficients in $\mathbf{Z}$ and $A > 0$; this choice makes the polynomial unique. 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 3.8). We are mainly interested in congruences of the quadratic polynomial modulo rational integers; but 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 a rational integer N.

In a first step, let us consider a notion weaker than primitivity, which can be made to hold for arbitrary $z \in K \setminus K_0$.

Definition 3.5. 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 furthermore $\gcd(A, B, C, \mathfrak{n}) = 1$.

Proposition 3.6. *Let $\mathfrak{n}$ be a non-zero ideal of $\mathcal{O}_{K_0}$. Every element z of $K\setminus K_0$ 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. The $\mathcal{O}_{K_0}$-module $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ is an invertible (hence proper) fractional ideal of the order*

$$\mathcal{O} = \mathfrak{d}^{-1}Az + \mathcal{O}_{K_0}, \tag{3.1}$$

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

Proof. 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. By the strong approximation theorem, for instance [5, Corollary 1.2.9], there is an element $d \in K_0$ such that $v_{\mathfrak{p}}(d) = -v_{\mathfrak{p}}(\mathfrak{d})$ for each prime ideal $\mathfrak{p}$ dividing $\mathfrak{n}$, such that $v_{\mathfrak{p}}(d) \geqslant 0$ for all other prime ideals, and such that the signs of d under the real embeddings of K_0 coincide with those of A. Then we may multiply A, B and C by d to obtain new coefficients in $\mathcal{O}_{K_0}$ 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.

The set $\mathcal{O}$ is a ring as $A^2z^2 = -ABz - AC \in \mathfrak{d}^2\mathcal{O}$. The $\mathcal{O}_{K_0}$-module $\mathfrak{b}$ is a fractional $\mathcal{O}$-ideal as both Az and $Az^2 = -Bz - C$ lie in $\mathfrak{d}\mathfrak{b}$. Moreover, we have $\mathfrak{b}\overline{\mathfrak{b}} = z\overline{z}\mathcal{O}_{K_0}+z\mathcal{O}_{K_0}+\overline{z}\mathcal{O}_{K_0}+\mathcal{O}_{K_0} = (C/A)\mathcal{O}_{K_0}+z\mathcal{O}_{K_0}+(B/A)\mathcal{O}_{K_0}+\mathcal{O}_{K_0} = \mathfrak{d}\mathcal{O}/A$, so $\mathfrak{b}$ is an invertible fractional $\mathcal{O}$-ideal with inverse $\mathfrak{d}^{-1}A\overline{\mathfrak{b}}$. □

To go further, we can use the leeway provided by the possibility of changing the representative of a polarised ideal class. So we need to consider under which conditions two numbers $z, z' \in K\setminus K_0$ represent the same polarised ideal class.

Proposition 3.7. *In the situation that $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$, associate to $z, z' \in K\setminus K_0$ the principally polarised ideals $(\mathfrak{b}, \xi)$ for $(\mathcal{O}, \Phi)$ and $(\mathfrak{b}', \xi')$ for $(\mathcal{O}', \Phi')$ as in Proposition 3.1. Then the following assertions are equivalent:*

(1) We have $(\mathcal{O}', \Phi') = (\mathcal{O}, \Phi)$ and $[(\mathfrak{b}', \xi')] = [(\mathfrak{b}, \xi)]$.

(2) There is a matrix

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

such that $z' = Mz := \frac{\alpha z+\beta}{\gamma z+\delta}$.

If the equivalent assertions hold, then we have $\xi' = (\gamma z+\delta)(\gamma\overline{z}+\delta)\xi$. *If furthermore* z *is a root of* $AX^2+BX+C \in \mathcal{O}_{K_0}[X]$, *then* z' *is a root of* $A'X^2+B'X+C' \in \mathcal{O}_{K_0}[X]$ *with*

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

and

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

Finally, we have $\gcd(A', B', C') = \gcd(A, B, C)$, *and* A' *is totally positive if* A *is, so that semiprimitivity of the polynomial for* z *carries over to the polynomial for* z'.

Proof. Given any

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

one easily computes

$$\frac{z-\overline{z}}{Mz-\overline{Mz}} = (\gamma z+\delta)(\gamma\overline{z}+\delta)(\det M)^{-1}. \tag{3.4}$$

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 $\mu = (\gamma z+\delta)^{-1}$. This implies $\mathcal{O}' = \mathcal{O}$. By (3.4) one sees that $\xi' = \xi(\gamma z+\delta)(\gamma\overline{z}+\delta) = \xi(\mu\overline{\mu})^{-1}$. 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 $(\mathcal{O}, \Phi)$, 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 (3.4) yield $1 = \xi/(\xi'\mu\overline{\mu}) = \det M$, so $M \in \mathrm{SL}_2(\mathcal{O}_{K_0})$.

Now define A', B', and C' by (3.2). A direct verification shows that $z' = Mz$ is a root of $A'X^2 + B'X + C$ (in fact, we have $A'X^2 + B'XZ + C'Z^2 = (AX^2 + BXZ + CZ^2) \circ M^{-1}$). We also have

$$\frac{\xi'}{\xi} = (\gamma z+\delta)(\gamma\overline{z}+\delta) = \gamma^2\frac{C}{A} + \gamma\delta\frac{-B}{A} + \delta^2 = \frac{A'}{A},$$

which is (3.3) and proves that A' is totally positive if A is.

From (3.2) one reads off that $\gcd(A, B, C) \mid \gcd(A', B', C')$; noticing that the inverse matrix M^{-1} leads to similar formulæ to express (A', B', C') in terms of (A, B, C) shows the converse. □

Now we have all ingredients to formulate and prove the main result of Section 3.2.

Proposition 3.8. *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 $\gcd(A\mathcal{O}_{K_0}, \mathfrak{n}) = \mathcal{O}_{K_0}$.*

Proof. Using Propositions 3.1 and 3.6, we find a semiprimitive quadratic polynomial AX^2+BX+C modulo $\mathfrak{n}$ representing the principally polarised ideal class. It remains to apply a suitable matrix M as in Proposition 3.7 such that the resulting A' is totally positive and coprime to $\mathfrak{n}$. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{K_0}$ dividing $\mathfrak{n}$, we consider the homogeneous form $A' := A\delta^2 - B\gamma\delta + C\gamma^2$ in δ and γ of (3.2). Let

$$\begin{aligned} &M_\mathfrak{p} = \mathrm{id}, && A' = A && \text{if } \mathfrak{p} \nmid A, \\ &M_\mathfrak{p} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, && A' = C && \text{if } \mathfrak{p} \nmid C, \mathfrak{p} \mid A, \\ &M_\mathfrak{p} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, && A' = A + C - B && \text{otherwise (in which case } \mathfrak{p} \nmid B). \end{aligned} \tag{3.5}$$

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

By Chinese remaindering, we obtain a matrix $M_\mathfrak{n} \in \mathrm{SL}_2(\mathcal{O}_{K_0}/\operatorname{rad}(\mathfrak{n}))$, which can be lifted to a matrix $M \in \mathrm{SL}_2(\mathcal{O}_{K_0})$, e.g. by strong approximation [22, Appendix A.3]. Replace z by Mz, so that A gets replaced by A', which is coprime to $\mathfrak{n}$; and by Proposition 3.7 the total positivity of A carries over to A'. □

3.3 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 [39, Theorem 4, p. 331] to CM fields of higher degree. For a generalisation of the remainder of [39, 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 first 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 3.9. *Suppose that $f \in \mathcal{F}_N$ is the quotient of two modular forms with rational q-expansions and that it is invariant under $\Gamma^0(N)$ for some positive $N \in \mathbf{Z}$.*

Let K_0 be a totally real number field such that $\mathcal{D}_{K_0}$ is principal. Consider a polynomial $AX^2+BX+C \in \mathcal{O}_{K_0}[X]$ of totally negative discriminant B^2-4AC that is semiprimitive modulo N and such that $N \mid C$. Let z be a root of the polynomial and let $K = K_0(z)$ be the CM field generated by z over K_0. Let τ be obtained from z as in Propositions 3.1 and 3.2.

If τ is not a pole of f, then $f(\tau)$ is a class invariant. In other words, the value $f(\tau)$ lies in the Shimura class field of the order and CM type corresponding to z as in Proposition 3.1.

The remainder of Section 3.3 is devoted to the proof of Theorem 3.9. The main tool 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

$$\mathrm{GSp}_{2g}(R) = \left\{ \mathbb{M} \in \mathrm{Mat}_{2g}(R) : \mathbb{M}^T \mathbb{J} \mathbb{M} = t\mathbb{J} \text{ for some } t \in R^\times \right\} \tag{3.6}$$

with $\mathbb{J}$ as in (2.3). For $\mathbb{M} \in \mathrm{GSp}_{2g}(R)$, write

$$\mathbb{M}^T \mathbb{J} \mathbb{M} = t(\mathbb{M})\mathbb{J} \qquad \text{with} \qquad t(\mathbb{M}) \in R^\times. \tag{3.7}$$

Lemma 3.10. For $\mathbb{M} \in \mathrm{GSp}_{2g}(R)$, both $\mathbb{M}^T$ and $\mathbb{M}^{-1}$ lie in $\mathrm{GSp}_{2g}(R)$ as well. We have $t(\mathbb{M}^T) = t(\mathbb{M})$ and $t(\mathbb{M}^{-1}) = t(\mathbb{M})^{-1}$.

Proof. Moving $\mathbb{M}^T$ and $\mathbb{M}$ to the other side of the equality symbol in (3.7) yields $\mathbb{J} = t(\mathbb{M})(\mathbb{M}^{-1})^T \mathbb{J} \mathbb{M}^{-1}$, hence $\mathbb{M}^{-1} \in \mathrm{GSp}_{2g}(R)$ with $t(\mathbb{M}^{-1}) = t(\mathbb{M})^{-1}$. Subsequently inverting (and observing $\mathbb{J}^{-1} = -\mathbb{J}$) gives $\mathbb{J} = t(\mathbb{M})^{-1}\mathbb{M}\mathbb{J}\mathbb{M}^T$, hence $\mathbb{M}^T \in \mathrm{GSp}_{2g}(R)$ with $t(\mathbb{M}^T) = t(\mathbb{M})$. □

It follows that $\mathrm{GSp}_{2g}(R)$ is a subgroup of $\mathrm{GL}_{2g}(R)$. Let $\mathrm{Sp}_{2g}(R) \subseteq \mathrm{GSp}_{2g}(R)$ be the subgroup 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

$$\begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix} \mathbb{V} \qquad \text{with} \qquad \mathbb{V} \in \mathrm{Sp}_{2g}(R).$$

The action of $\Gamma = \mathrm{Sp}_{2g}(\mathbf{Z})$ on the Siegel space $\mathbf{H}_g$ as given in (2.4) 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 $f^{\mathbb{M}}(\tau) = f(\mathbb{M}\tau)$ for $\mathbb{M} \in \mathrm{GSp}^+_{2g}(\mathbf{Q})$. There is also a well-known 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 that of an arbitrary lift to $\mathrm{Sp}_{2g}(\mathbf{Z})$.
- For $t \in (\mathbf{Z}/N\mathbf{Z})^\times$, the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & t \end{smallmatrix}\right)$ 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 as given in [45, 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 2.3). Let $\mathcal{S}$ 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. (2.9)*. The Galois action on $f(\tau)$ is described as follows.*

Let F be the least positive integer such that $F\mathcal{O}_K \subset \mathcal{O}$. For any $[\mathfrak{a}] \in \mathfrak{C}_{\mathcal{O},\Phi}(N)$ with $\mathfrak{a} \in \mathcal{I}(NF)$, 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 $\mathbb{M} \in \mathrm{GL}_{2g}(\mathbf{Q})$ be given by $\mathcal{C} = \mathcal{S}\mathbb{M}^T$. Then we have $\mathbb{M} \in \mathrm{GSp}^+_{2g}(\mathbf{Q})$ with $t = \mathrm{N}(\mathfrak{a})^{-1}$, and the reduction $\mathbb{M}_{\bmod N}$ exists and satisfies $\mathbb{M}_{\bmod N} \in \mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$. Then

$$f(\tau)^{\sigma([\mathfrak{a}])} = f^{(\mathbb{M}_{\bmod N})^{-1}}(\mathbb{M}\tau) = f^{(\mathbb{M}_{\bmod N})^{-1}}(\tau'),$$

where τ' is obtained from $\mathcal{C}$

Shimura reciprocity links Galois actions to matrix actions on modular functions and period matrices. In our setting the period matrices are obtained from symplectic bases of ideals as in (2.5), written in terms of roots z of quadratic polynomials. We need to bring together the action of symplectic matrices of dimension $2g \times 2g$ on period matrices with the action of matrices of dimension 2×2 on elements $z \in K$ as described in Proposition 3.7. This can be done explicitly using the two bases

$\mathcal{B}_1 = (b_{1,1}, \ldots, b_{1,g})$ and $\mathcal{B}_2 = (b_{2,1}, \ldots, b_{2,g})$ of K_0 over $\mathbf{Q}$, which we will interpret as matrices of dimension $1 \times g$ with entries in K_0, occurring in our choice of the symplectic basis $\mathcal{S}$ in Proposition 3.2. The important property of these bases is that they are dual with respect to the symmetric $\mathbf{Q}$-bilinear form

$$K_0 \times K_0 \to \mathbf{Q}, \quad (x, y) \mapsto L(xy)$$

with L a $\mathbf{Q}$-linear map, precisely,

$$L : K_0 \to \mathbf{Q}, \quad x \mapsto \mathrm{Tr}_{K_0/\mathbf{Q}}\left(-\lambda^{-1}x\right);$$

that is, $L(b_{1,i}b_{2,j}) = \delta_{i,j}$. Given $\alpha \in K_0$ and $i, j \in \{1, 2\}$, denote by $[\alpha]_j^i \in \mathrm{Mat}_g(\mathbf{Q})$ the transposed matrix of multiplication by α from K_0 with $\mathbf{Q}$-basis $\mathcal{B}_i$ to K_0 with $\mathbf{Q}$-basis $\mathcal{B}_j$, that is,

$$\alpha\mathcal{B}_i^T = [\alpha]_j^i \mathcal{B}_j^T. \tag{3.8}$$

We obtain the following map from $\mathrm{Mat}_2(K_0)$ to $\mathrm{Mat}_{2g}(\mathbf{Q})$.

Lemma 3.12. Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Mat}_2(K_0)$. Then

$$M^T \begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} = \begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} [M]^T \tag{3.9}$$

with

$$[M] = \begin{pmatrix} [\alpha]_1^1 & [\beta]_2^1 \\ [\gamma]_1^2 & [\delta]_2^2 \end{pmatrix} \in \mathrm{Mat}_{2g}(\mathbf{Q}). \tag{3.10}$$

If $M \in \mathrm{GL}_2(K_0)$ with $\det M \in \mathbf{Q}$, then $[M] \in \mathrm{GSp}_{2g}(\mathbf{Q})$ with $t([M]) = \det M$. In particular, if $M \in \mathrm{SL}_2(\mathcal{O}_{K_0})$, then $[M] \in \mathrm{Sp}_{2g}(\mathbf{Z})$.

Proof. Formula (3.9) follows by a direct computation from the definition of $[\cdot]_j^i$:

$$\begin{pmatrix} \mathcal{B}_1^T & 0 \\ 0 & \mathcal{B}_2^T \end{pmatrix} M = \begin{pmatrix} \alpha\mathcal{B}_1^T & \beta\mathcal{B}_1^T \\ \gamma\mathcal{B}_2^T & \delta\mathcal{B}_2^T \end{pmatrix} = \begin{pmatrix} [\alpha]_1^1\mathcal{B}_1^T & [\beta]_2^1\mathcal{B}_2^T \\ [\gamma]_1^2\mathcal{B}_1^T & [\delta]_2^2\mathcal{B}_2^T \end{pmatrix} = \mathbb{M} \begin{pmatrix} \mathcal{B}_1^T & 0 \\ 0 & \mathcal{B}_2^T \end{pmatrix}$$

with $\mathbb{M} = [M]$. Concerning symplecticity of $\mathbb{M}$, we use the map L and the two bases $\mathcal{B}_1$ and $\mathcal{B}_2$ to define a bilinear form $E : \mathbf{Q}^{2g} \times \mathbf{Q}^{2g} \to \mathbf{Q}$,

$$\begin{aligned} E : (u, v) \ &\longmapsto L\left(u^T \begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix}^T \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} v\right) \\ &= L\left(u^T \begin{pmatrix} 0 & \mathcal{B}_1^T\mathcal{B}_2 \\ -\mathcal{B}_2^T\mathcal{B}_1 & 0 \end{pmatrix} v\right), \end{aligned} \tag{3.11}$$

in which the matrix between u^T and v is an element of $\mathrm{Mat}_{2g}(K_0)$. Plugging in the unit vectors for u and v and using that $\mathcal{B}_1$ and $\mathcal{B}_2$ are dual shows that E is a symplectic form with the unit vectors as symplectic basis, so that in fact $E(u, v) = u^T\mathbb{J}v$. Plugging in $\mathbb{M}^T v$ for v and $\mathbb{M}^T u$ for u and using (3.9) changes the factor

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ into } M \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} M^T = \det(M) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Since $\det(M) \in \mathbf{Q}$ can be taken outside the $\mathbf{Q}$-linear L, we get $E(\mathbb{M}^T u, \mathbb{M}^T v) = \det(M)E(u, v)$. In other words, we have $\mathbb{M}\mathbb{J}\mathbb{M}^T = \det(M)\mathbb{J}$. By Lemma 3.10, we get that $\mathbb{M}$ is symplectic with $t(\mathbb{M}) = \det(M)$. □

Lemma 3.13. With $\tau(z)$ obtained from z as in Proposition 3.2, we have

$$\tau(Mz) = [M]\,\tau(z), \tag{3.12}$$

where $[M]$ is as in Lemma 3.12.

Proof. Take $z' = Mz$ and observe that Lemma 3.12 gives

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

The period matrix for the left hand side is $\tau(Mz)$. The period matrix for the right hand side is the same as the period matrix for $\mathcal{S}\,[M]^T$, which is $[M]\,\tau(z)$ by [45, Lemma 4.7(b)]. □

Remark 3.14. Lemma 3.13 tells us that $z \mapsto \tau(z)$ gives a well-defined map from the set of z-values up to $\mathrm{SL}_2(\mathcal{O}_{K_0})$ to the set $\mathrm{Sp}_{2g}(\mathbf{Z})\backslash\mathbf{H}_g$. In fact, this is exactly the natural map from the Hilbert moduli space to the Siegel moduli space restricted to our values z, which are CM points of the Hilbert moduli space.

To treat polarised ideals only up to equivalence, we need to consider multiplications by constants $\mu \in K^\times$; the following lemma describes them explicitly as linear maps $K \to K$ with respect to different bases.

Lemma 3.15. Let A, B, $C \in K_0$ and $z \in K$ be as in Theorem 3.9, and let $\mu \in K^\times$. Following (3.1) 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 the matrices

$$M_\mu = \frac{1}{d}\begin{pmatrix}\beta-\alpha B & -\alpha C\\ \alpha A & \beta\end{pmatrix} \in \mathrm{Mat}_2\left(\frac{1}{d}\,\mathcal{O}_{K_0}\right) \tag{3.13}$$

and

$$\mathbb{M}_\mu = [M_\mu] = \frac{1}{d}\begin{pmatrix}[\beta-\alpha B]_1^1 & [-\alpha C]_2^1\\ [\alpha A]_1^2 & [\beta]_2^2\end{pmatrix} \in \mathrm{Mat}_{2g}\left(\frac{1}{d}\,\mathbf{Z}\right). \tag{3.14}$$

satisfy $\mu(z,1) = (z,1)M_\mu^T$ and $\mu\mathcal{S} = \mathcal{S}\mathbb{M}_\mu^T$, where $\mathcal{S}$ is the $\mathbf{Q}$-basis of K of Proposition 3.2. Furthermore $\mathbb{M}_\mu^{-1} = \mathbb{M}_{\mu^{-1}}$, where $\mathbb{M}_{\mu^{-1}}$ is obtained from μ^{-1} in a manner analogous to (3.14).

Proof. The identity $\mu(z,1) = (z,1)M_\mu^T$ is obtained by direct computation using $Az^2+Bz+C=0$. Combining this with Lemma 3.12, we get

$$\begin{aligned}\mu\mathcal{S} = \mu(z,1)\begin{pmatrix}\mathcal{B}_1 & 0\\ 0 & \mathcal{B}_2\end{pmatrix} &= (z,1)M_\mu^T\begin{pmatrix}\mathcal{B}_1 & 0\\ 0 & \mathcal{B}_2\end{pmatrix}\\ &= (z,1)\begin{pmatrix}\mathcal{B}_1 & 0\\ 0 & \mathcal{B}_2\end{pmatrix}\mathbb{M}_\mu^T = \mathcal{S}\mathbb{M}_\mu^T.\end{aligned}$$

So $\mathbb{M}_\mu$ and $\mathbb{M}_{\mu^{-1}}$ are the transposed matrices of multiplication in K by μ and μ^{-1} with respect to the same $\mathbf{Q}$-basis, which implies that they are inverses of each other. □

Proof of Theorem 3.9. 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 (2.7) of $S_{\mathcal{O},\Phi}(1)$, there is some $\mu\in K^\times$ 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 (2) of Definition 2.4.

Let $\mathcal{S}$ be the symplectic basis of $\mathfrak{b}$ that gave rise to τ. Then $\mathcal{C}=\mu^{-1}\mathcal{S}$ is a symplectic basis of $N_{\Phi^r,\mathcal{O}}(\mathfrak{a})^{-1}\mathfrak{b}$. We get $\mathcal{C}=\mathcal{S}\mathbb{M}_{\mu^{-1}}^T$ in the notation of Lemma 3.15. Using Shimura's reciprocity law Theorem 3.11 we obtain

$$f(\tau)^{\sigma([\mathfrak{a}])} = f^{\left(\left(\mathbb{M}_{\mu^{-1}}\right)_{\bmod N}\right)^{-1}}(\tau') = f^{\left(\mathbb{M}_{\mu}\right)_{\bmod N}}(\tau') = f^{\left(\mathbb{M}_{\mu}\right)_{\bmod N}}(\tau),$$

where we have used the last statement of Lemma 3.15 and that τ', the period matrix obtained from $\mathcal{C}=\mu^{-1}\mathcal{S}$, equals the period matrix obtained from $\mathcal{S}$, which is τ. It remains only to show that $f^{\left(\mathbb{M}_{\mu}\right)_{\bmod N}}=f$.

For this we write $\mu=\frac{\alpha Az+\beta}{d}$ as in Lemma 3.15 with furthermore d coprime to NF (using Definition 2.4(1) and Proposition 3.6). Then by Theorem 3.11, the matrix $\left(\mathbb{M}_{\mu}\right)_{\bmod N}$, as given by the four blocks of size $g\times g$ of (3.14), is an element of $\mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ with $t=\mathrm{N}(\mathfrak{a})=\mu\overline{\mu}\pmod N$ coprime to N. So $\left(\mathbb{M}_{\mu}\right)_{\bmod N}$ is the product of the matrix $\left(\begin{smallmatrix}1&0\\0&t\end{smallmatrix}\right)\in\mathrm{Mat}_{2g}(\mathbf{Z}/NZ)$, under which the function f is invariant as a quotient of forms with rational q-expansions, and a matrix in $\mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ for which the upper right block equals $[-\alpha C]_2^1 \bmod N$. Since $\alpha\in\mathfrak{d}^{-1}$ we have $\alpha C\in\mathcal{O}_{K_0}$. With $\mathfrak{d}=\gcd(A,B,C)$ coprime to N, the element $\alpha\in\mathfrak{d}^{-1}$ has non-negative valuation in all primes of K_0 dividing N, so that $N\mid C$ implies $\alpha C\in N\mathcal{O}_{K_0}$. Thus the upper right block vanishes modulo N, and the matrix in $\mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ can be lifted to a matrix in $\Gamma^0(N)$, under which the function f is also invariant by assumption. □

Remark 3.16. Our map $M\mapsto[M]$ generalises the map ϕ of [35, (3.4)]. They have $K_0=\mathbf{Q}(\sqrt{D})\subset\mathbf{R}$ with $D\equiv 1 \pmod 4$ prime and $\sqrt{D}>0$, let σ be the non-trivial automorphism of K_0, write $\mathcal{O}_{K_0}=\mathbf{Z}e_1+\mathbf{Z}e_2$ and take $\varepsilon\in\mathcal{O}_{K_0}^\times$ with $\varepsilon\sigma(\varepsilon)=-1$ and $\varepsilon>0$. Observe that $e_1\sigma(e_2)-e_2\sigma(e_1)=s\sqrt{D}$ for some $s\in\{\pm1\}$. Then loc. cit. defines $\phi(M)=SM^*S^{-1}$, where

$$M^*=\begin{pmatrix}\alpha&0&\beta&0\\0&\sigma(\alpha)&0&\sigma(\beta)\\\gamma&0&\delta&0\\0&\sigma(\gamma)&0&\sigma(\delta)\end{pmatrix}\quad\text{and}\quad S=\begin{pmatrix}e_1&\sigma(e_1)&0&0\\e_2&\sigma(e_2)&0&0\\0&0&\frac{s\sigma(e_2)}{\varepsilon}&\frac{se_2}{\sigma(\varepsilon)}\\0&0&\frac{-s\sigma(e_1)}{\varepsilon}&\frac{-se_1}{\sigma(\varepsilon)}\end{pmatrix}.$$

Now choose $\mathcal{B}_1=(e_1,e_2)$, which has trace dual $s\sqrt{D}^{-1}(\sigma(e_2),-\sigma(e_1))$. Choosing $\lambda=-\sqrt{D}/\varepsilon$ in Proposition 3.2, we obtain $\mathcal{B}_2$ as $-\lambda$ times the trace dual of $\mathcal{B}_1$, which is $\mathcal{B}_2=(\frac{s}{\varepsilon}\sigma(e_2),-\frac{s}{\varepsilon}\sigma(e_1))$. In particular, the first and third column of the matrix identity $SM^*=\phi(M)S$ read

$$S\begin{pmatrix}\alpha&\beta\\0&0\\\gamma&\delta\\0&0\end{pmatrix}=\phi(M)\begin{pmatrix}e_1&0\\e_2&0\\0&\frac{s\sigma(e_2)}{\varepsilon}\\0&\frac{-s\sigma(e_1)}{\varepsilon}\end{pmatrix},$$

which is exactly

$$\begin{pmatrix} \mathcal{B}_1^T & 0 \\ 0 & \mathcal{B}_2^T \end{pmatrix} M = \phi(M) \begin{pmatrix} \mathcal{B}_1^T & 0 \\ 0 & \mathcal{B}_2^T \end{pmatrix}.$$

As [35, (3.4)] gives that $\phi(M)$ has rational coefficients, this implies that it equals $[M]$, so that indeed the map $M \mapsto [M]$ generalises ϕ.

3.4 Existence of quadratic polynomials with $N \mid C$

We would like to apply Theorem 3.9 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 plentiful, 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 2.3 and 3.4, we need the existence of a polarised ideal class T for $(\mathcal{O}, \Phi)$ that is represented by a quadratic polynomial $Q = AX^2 + BX + C$ satisfying

$$Q \text{ is semiprimitive modulo } \mathfrak{n} \text{ and } \mathfrak{n} \mid C \tag{3.15}$$

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 for $(\mathcal{O}, \Phi)$ exists, but otherwise the question of computing a class polynomial would be moot.

Theorem 3.17. *Let $\mathfrak{n}$ be a non-zero ideal of $\mathcal{O}_{K_0}$, assume that $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$ 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 (3.15) with

$$\gcd(A, F\mathfrak{n}) = 1 \text{ and } \gcd(\mathfrak{n}, \mathfrak{n}^{-1}C) = 1.$$

(3) There exists a principally polarised ideal class for $(\mathcal{O}, \Phi)$ that is represented by a polynomial satisfying (3.15).

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 3.18. 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 3.6 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 $\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + U_i(\vartheta)\mathcal{O}$ 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 (3.1), we have $\vartheta = Az \in \mathcal{O}$ and

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

which implies that the conductor of $\mathcal{O}_{K_0}[\vartheta]$ divides $\mathfrak{f}\mathfrak{d}$. As $\mathfrak{p} \nmid \mathfrak{f}\mathfrak{d}$, the Kummer-Dedekind criterion for relative number field extensions gives the statements of the lemma; see [5, Proposition 2.3.9] and [44, 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 3.17. 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 (3.15) 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 3.18, $\widetilde{U}$ is reducible, so the prime $\mathfrak{p}$ is not inert. If $\mathfrak{p}$ is ramified, that is $\mathfrak{p} \mid B$, 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 3.8, it can be represented by a quadratic polynomial $AX^2 + BX + C$ with $A \gg 0$ and $\gcd(A, F\mathfrak{n}) = 1$. 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 $\mathfrak{f}$ and A and split or ramified, the polynomial $U(X) = X^2 + BX + AC$ of Lemma 3.18 has a root in $\mathcal{O}_{K_0}/\mathfrak{p}$. If $\mathfrak{p}$ is split, then 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 an element $r \in \mathcal{O}_{K_0}$ that is a root modulo $\mathfrak{n}$. As A is coprime to $\mathfrak{n}$, we may furthermore assume that $A \mid r$. Let $\vartheta' = \vartheta - r$; its minimal polynomial is $U' = U(X + r) = X^2 + B'X + AC'$ with $B' = B + 2r$ and $C' = U(r)/A \in \mathfrak{n}$. So $z' = \vartheta'/A$ is a root of the polynomial $AX^2 + B'X + C' \in \mathcal{O}_{K_0}$ satisfying (3.15). The polynomial is obtained by the $\mathrm{SL}_2(\mathcal{O}_{K_0})$-transformation $z' = z - r/A$, where $A \mid r$, so by Proposition 3.7 it represents the same principally polarised ideal class.

We now 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' 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 3.18 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 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 (3.1), 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 3.9 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 [39], are *N-systems*, consisting of quadratic polynomials representing (in the sense of Definition 3.4) the equivalence classes 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 show that N-systems always exist and provide an algorithm to compute them explicitly.

Throughout this section we assume as before that the order $\mathcal{O}$ of conductor $\mathfrak{f}$ is closed under complex conjugation and contains $\mathcal{O}_{K_0}$, that $\mathcal{D}_{K_0} = \lambda\mathcal{O}_{K_0}$ and that $F\mathbf{Z} = \mathfrak{f} \cap \mathbf{Z}$.

4.1 Galois conjugates from N-systems

As seen in §2.3, the CM class group of level 1, $\mathfrak{C}_{\mathcal{O},\Phi}(1)$, acts freely on the set $\mathcal{T}_{\mathcal{O},\Phi}$ of principally polarised ideal classes via (2.8). Let $\mathcal{T} = \{T_1, \ldots, T_h\} \subseteq \mathcal{T}_{\mathcal{O},\Phi}$ with $h = |\mathfrak{C}_{\mathcal{O},\Phi}(1)|$ be one orbit under this action. In the light of Proposition 3.8, the classes in $\mathcal{T}$ 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 period matrices τ_i as in Proposition 3.2 and Corollary 3.3.

If f is a Siegel modular function of level $N = 1$, then Shimura reciprocity implies that for any choice of quadratic polynomials, the $f(\tau_i)$ form a Galois orbit and are thus the roots of a class polynomial as in (2.1). For general N, each T_i can be given by $[S_{\mathcal{O},\Phi}(1) : S_{\mathcal{O},\Phi}(N)]$ representatives that are inequivalent under the action of $S_{\mathcal{O},\Phi}(N)$, and which in general yield different values of f; so some work is needed

to write down a consistent set of quadratic polynomials leading to a Galois invariant set of CM values. Before giving a solution by imposing congruence conditions modulo N, we address another problem arising for $g > 1$. When $g = 1$, it is natural to choose *primitive* representatives, satisfying $A_i > 0$ and $\gcd(A_i, B_i, C_i) = 1$. In the general case, this rigidity is not possible unless the narrow class number of $\mathcal{O}_{K_0}$ is 1. So far we worked around this by using the notion of semiprimitivity modulo the ideal $\mathfrak{n} = N\mathcal{O}_{K_0}$, see Definition 3.5 and Proposition 3.6, which imposes that the greatest common divisor of the coefficients is coprime to $\mathfrak{n}$. This is compatible with multiplying A_i, B_i and C_i by the same element of $\mathcal{O}_{K_0}$ coprime to $\mathfrak{n}$ without changing z_i and τ_i, which turns out to be undesirable. So we impose an additional notion of compatibility between the quadratic polynomials.

Again we state results in terms of an arbitrary non-zero ideal $\mathfrak{n}$ of $\mathcal{O}_{K_0}$ 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 shows that equiprimitivity forces the greatest common divisors of the coefficients to all be the same over the set of quadratic polynomials.

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

$$\varepsilon\mathcal{O}_{K_0} = \mathfrak{d}_1\mathfrak{d}_2^{-1}. \tag{4.1}$$

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 (3.1) 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 imaginary parts" and find the desired equality (4.1).

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 $\delta_1 = \delta_2$ and $\mathfrak{d}_1 = \mathfrak{d}_2$. □

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 $\mathcal{Q} = \{Q_1, \dots, Q_h\}$ with $Q_i = A_i X^2 + B_i X + C_i \in \mathcal{O}_{K_0}[X]$ 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 $F\mathfrak{n}$ that satisfy

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

(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 [39, p. 329] is also an N-system in our sense. Compared to [39] we have added the condition that $\gcd(A, F) = 1$, which simplifies some proofs without having practical implications, as it is always possible by Theorem 4.5 and Algorithm 4.7 to satisfy the stricter condition. The following is a generalisation of Schertz [39, Theorem 4, pp. 331–332] from the case $g = 1$.

Theorem 4.4. *Under the hypotheses of Theorem 3.9, let $\tau_1, \dots, \tau_h$ be the period matrices obtained as in Proposition 3.2 and Corollary 3.3 from an N-system given as $\{Q_1, \dots, Q_h\}$ such that $N \mid C_1$ and τ_1 is not a pole of f.*

Then $f(\tau_1)$ is a class invariant, and the set of Galois conjugates of $f(\tau_1)$ over K^r is exactly $\{f(\tau_1), \dots, f(\tau_h)\}$.

More precisely, let $(\mathfrak{b}_i, \xi_i)$ be the polarised ideal associated to Q_i. Then there is $\mathfrak{a}_i \in \mathcal{I}(NF)$ and $\mu_i \in K^\times$ such that $\mathfrak{b}_i = \mu_i^{-1} \mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a}_i)^{-1}\mathfrak{b}_1$ and $\xi_i = \mu_i\overline{\mu_i}\,\mathrm{N}(\mathfrak{a}_i)\xi_1$. For any such $\mathfrak{a}_i$, we have

$$f(\tau_1)^{\sigma([\mathfrak{a}_i])} = f(\tau_i). \tag{4.2}$$

Proof. We know from Theorem 3.9 that $f(\tau_1)$ is a class invariant. Equiprimitivity and the other properties of an N-system imply that all the C_i are divisible by N; so actually all the $f(\tau_i)$ are class invariants. It remains to show that they are Galois conjugates as given by (4.2).

The $\mathfrak{a}_i$ and μ_i exist because by definition the polarised ideal classes derived from an N-system form an orbit under the action (2.8) of the CM class group $\mathfrak{C}_{\mathcal{O},\Phi}(1)$; here a priori $\mathfrak{a}_i \in \mathcal{I}(F)$, but (as usual in class field theory) we may take a representative satisfying the additional coprimality condition $\mathfrak{a}_i \in \mathcal{I}(NF)$.

The action of $\sigma([\mathfrak{a}_i])$ is computed using Theorem 3.11 as follows. With the notations of Theorem 3.11 and Proposition 3.2, we have $\mathfrak{c} = \mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{a}_i)^{-1}\mathfrak{b}_1 = \mu_i\mathfrak{b}_i$,

$$\mathcal{S} = (z_1, 1)\begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} \text{ and } \mathcal{C} = \mu_i(z_i, 1)\begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix}.$$

By equiprimitivity of an N-system and Lemma 4.2, we have

$$2A_i z_i + B_i = 2A_1 z_1 + B_1, \text{ so } (z_i, 1) = (z_1, 1)M^T \text{ with } M = \begin{pmatrix} \frac{A_1}{A_i} & \frac{B_1 - B_i}{2A_i} \\ 0 & 1 \end{pmatrix}.$$

Let M_{μ_i} be as in Lemma 3.15 for $z = z_1$, that is, such that $\mu_i(z_1, 1) = (z_1, 1)M_{\mu_i}^T$. Then

$$\begin{aligned}\mathcal{C} &= \mu_i(z_1,1)M^T \begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} = (z_1,1)M_{\mu_i}^T M^T \begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} \\ &= (z_1,1)(MM_{\mu_i})^T \begin{pmatrix} \mathcal{B}_1 & 0 \\ 0 & \mathcal{B}_2 \end{pmatrix} \\ &= \mathcal{S}\mathbb{M}^T \quad \text{with} \quad \mathbb{M} = [MM_{\mu_i}] \quad \text{as in Lemma 3.12.}\end{aligned}$$

By Shimura's reciprocity law (Theorem 3.11) we get

$$f(\tau_1)^{\sigma([\mathfrak{a}_i])} = f^{\mathbb{M}^{-1}_{\bmod N}}(\tau'), \tag{4.3}$$

where τ' is obtained from the basis $\mathcal{S}\mathbb{M}^T$, hence $\tau' = \tau_i$. As in the proof of Theorem 3.9, we will show $f^{\mathbb{M}^{-1}_{\bmod N}} = f$ by looking at the upper right entry of $\mathbb{M}$.

Write $\vartheta_i = A_i z_i \in \mathcal{O}$ and $\mathfrak{d}_i = \gcd(A_i, B_i, C_i)$ and notice that $A_i\mathfrak{b}_i = \vartheta_i\mathcal{O}_{K_0} + A_i\mathcal{O}_{K_0}$ is an integral ideal of $\mathcal{O}$ and that $A_i\overline{\mathfrak{b}}_i$ is an integral ideal of $\mathcal{O} = \overline{\mathcal{O}}$. Then

$$\begin{aligned}(A_i\mathfrak{b}_i)(A_i\overline{\mathfrak{b}}_i) &= A_i(A_i z_i\mathcal{O}_{K_0} + A_i\mathcal{O}_{K_0})(\overline{z}_i\mathcal{O}_{K_0} + \mathcal{O}_{K_0}) \\ &= A_i(A_i z_i\overline{z}_i\mathcal{O}_{K_0} + A_i(z_i + \overline{z}_i)\mathcal{O}_{K_0} + A_i\mathcal{O}_{K_0} + \vartheta_i\mathcal{O}_{K_0}) \\ &= A_i(\mathfrak{d}_i + \vartheta_i\mathcal{O}_{K_0}) = A_i\mathfrak{d}_i\mathcal{O} \text{ by (3.1).}\end{aligned} \tag{4.4}$$

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 2.4(2) that μ_i is coprime to NF with respect to $\mathcal{O}$. We may write it as in Lemma 3.15 as $\mu_i = \frac{\alpha_i A_1 z_1 + \beta_i}{d_i}$ with $\alpha_i \in \mathfrak{d}_1^{-1}$, $\beta_i \in \mathcal{O}_{K_0}$ and, by Definition 2.4(1), 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 (3.13) that the top right 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 top right entry of M is also divisible by N, and hence the same holds for the product of the NF-integral matrices M and M_{μ_i}.

The matrix $\mathbb{M} = [MM_{\mu_i}]$ is obtained from MM_{μ_i} as in (3.10) by replacing elements of K_0 by their $g \times g$-matrices with respect to $\mathbf{Z}$-bases of $\mathcal{O}_{K_0}$. In particular, if an element of K_0 is N-integral, 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 $\mathbb{M}$ is N-integral with upper right block divisible by N. We conclude $f^{\mathbb{M}^{-1}_{\bmod N}} = f$, which finishes the proof. □

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 [39, Proposition 3, pp. 335–336].

Theorem 4.5. *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 Proposition 3.8 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* $F\mathfrak{n}$ *with* $\gcd(A_1, F\mathfrak{n}) = 1$. *Then there is an* $\mathfrak{n}$*-system* $\mathcal{Q} = \{Q_1, \dots, Q_h\}$ *for* $(\mathcal{O}, \Phi)$ *containing the given* Q_1.

Proof. Start with an arbitrary set of polynomials $\{Q_1, \dots, Q_h\}$ 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 3.8, we may change Q and z such that they represent the same class, Q is still semiprimitive modulo $F\mathfrak{n}$ and $\gcd(A, F\mathfrak{n}) = 1$.

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

Lemma 4.6. 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 Q_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 $\mathfrak{m}$, then so is A_2'.

Proof of Lemma 4.6. 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 $\mathfrak{m}$ if A_2 is. 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 $D' = D$, so the system remains equiprimitive and (1) remains satisfied.

Since by equiprimitivity the discriminants satisfy $B^2 - 4AC = B_1^2 - 4A_1C_1$, we have $4 \mid B^2 - B_1^2 = (B - B_1)(B + B_1)$. From $B - B_1 \equiv B + B_1 \pmod 2$ we deduce $2 \mid B - B_1$. For (2), it suffices to take β such that $A\beta \equiv \frac{B-B_1}{2} \pmod{\mathfrak{n}}$, which is possible since $\gcd(A, \mathfrak{n}) = 1$. This finishes the proof of Theorem 4.5. □

For the reader's convenience, we summarise the constructive proof of Theorem 4.5 in the following algorithm, before discussing in more detail how single steps of it can be carried out.

Algorithm 4.7.
Input: *A quadratic polynomial* Q_1 *as in Theorem 4.5*
Output: *An* $\mathfrak{n}$*-system* $\mathcal{Q}$ *containing* Q_1

(1) Enumerate the orbit of the polarised ideal class represented by Q_1 *under the action of* $\mathfrak{C}_{\mathcal{O},\Phi}(1)$*, 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* $\gcd(A_i, B_i, C_i, F\mathfrak{n}) = 1$ *as in Proposition 3.6.*

(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* $\gcd(A_i, F\mathfrak{n}) = 1$*, while remaining semiprimitive modulo* $F\mathfrak{n}$*.*

(c) *As in Lemma 4.6, multiply* Q_i *by* $\varepsilon = \delta_1\delta_i^{-1}$ *with* $\delta_i = 2A_iz_i + B_i$*.*

(d) *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, [20, 3] for the computation of the CM class group and the orbits. An implementation is provided by `cmh` [19], to which we have added the remaining steps of Algorithm 4.7 as the function `nsystem`.

Step (2a) is an application of strong approximation as in [5, Corollary 1.2.9]: Given a finite set $\mathcal{P}_0$ of prime ideals of $\mathcal{O}_{K_0}$ (the primes dividing $\gcd(A_i, B_i, C_i, F\mathfrak{n})$), 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 [2], for instance, this can be implemented using the function `idealchinese`.

One way to do Step (2b) is to construct matrices $M_\mathfrak{p}$ as in (3.5) for every $\mathfrak{p} \mid F\mathfrak{n}$. Chinese remaindering (using again `idealchinese`) provides a matrix $M_{\bmod \mathfrak{m}} \in \mathrm{SL}_2(\mathcal{O}_{K_0}/\mathfrak{m})$, where $\mathfrak{m} = \mathrm{rad}(F\mathfrak{n})$, 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 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ 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 the Chinese remainder theorem, 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 u and v in $\mathcal{O}_{K_0}$ such that $au + vb = 1$ as follows: By the Chinese remainder theorem, 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 $m = ad - bc - 1 \in \mathfrak{m}$. Then

$$M = \begin{pmatrix} a & b \\ c + vm & d - um \end{pmatrix}$$

has determinant 1 and reduction $M_{\bmod \mathfrak{m}}$ modulo $\mathfrak{m}$. This process is deterministic, polynomial time if the factorisation of $F\mathfrak{n}$ 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 the Chinese remainder theorem.

5 Complex conjugation

Class invariants $f(\tau)$ with $f \in \mathcal{F}_N$ are roots of class polynomials of degree $h = |\mathfrak{C}_{\mathcal{O},\Phi}(1)|$ with coefficients that lie *a priori* in K^r. But it is well-known that the j-invariant for $g = 1$ and the Igusa invariants for $g = 2$, both of level $N = 1$, lead to class polynomials with coefficients in the real subfield K_0^r of K. In this section we examine criteria under which this happens for higher level modular functions and

arbitrary g 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.

As a preparatory step, we look at how complex conjugation acts on our different algebraic structures and complex values.

Lemma 5.1. Assume the familiar setting of this article, that is, $(\mathfrak{b}, \xi)$ and z, a root of the quadratic polynomial $AX^2 + BX + C$, are as in Propositions 3.1 and 3.6, the period matrix τ is computed as in Proposition 3.2, and f is a quotient of two Siegel modular forms with real q-expansions.

If $\mathcal{A} = \mathbf{C}^g/\Phi(\mathfrak{b})$ is the abelian variety associated to $(\mathfrak{b}, \xi)$, then its 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 $\xi' = \xi$. The value z' is a root of the quadratic polynomial $A'X^2 + B'X + C'$ with $A' = A$, $C' = C$ and $B' = -B$, and the associated period matrix is $\tau' = -\overline{\tau}$. Finally $f(\tau') = \overline{f(\tau)}$.

Proof. The assertion on $\overline{\mathcal{A}}$ follows from the fact that complex conjugation commutes with the embeddings forming the CM type Φ, see [33, Proposition 3.5.5]. The values of $\mathfrak{b}'$, z', A', B' and C' are clear by definition, that of τ' is computed by Proposition 3.2.

We now consider q-expansions. To $\tau = \left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{smallmatrix}\right)$ we associate the values $q_k = e^{2\pi i \tau_k}$, and similarly the q'_k are associated to τ'. Then $q'_k = \overline{q_k}$, and the q-expansions of the numerator and the denominator of f having real coefficients implies that $f(\tau') = \overline{f(\tau)}$. □

In the following two sections we transpose two theorems on class polynomials being defined over the real subfield from $g = 1$ to higher dimension. To do so, we explicitly identify pairs of quadratic polynomials that yield complex conjugate values. The main added difficulty is to examine under which conditions these pairs belong to the same orbit under $\mathfrak{C}_{\mathcal{O},\Phi}(1)$: If they belonged to different orbits, we would obtain not one real class polynomial, but two complex conjugate class polynomials, one for each orbit. We derive two separate, but related criteria for the favourable situation in Propositions 5.3 and 5.8.

5.1 Real class polynomials for ramified levels

The following result is the analogue of [13, 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 4.4, assume furthermore that F and N are coprime and that all primes dividing $N\mathcal{O}_{K_0}$ are ramified in $\mathcal{O}_K$. Suppose that the following holds for the ideal $\mathfrak{b} = \mathfrak{b}_1 = z_1\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$:*

$$\begin{aligned} &\text{There exist } \mathfrak{c} \in \mathcal{I}(F) \text{ and } \mu \in K^\times \\ &\text{such that } \mu^{-1}\,\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{c})^{-1}\mathfrak{b} = \overline{\mathfrak{b}} \text{ and } \mu\overline{\mu}\,\mathrm{N}(\mathfrak{c}) = 1. \end{aligned} \tag{5.1}$$

Then the class polynomial of Theorem 4.4 is an element of $K_0^r[X]$.

More precisely, let $\mathfrak{c}$ be as in (5.1), let (as in the theorem) $[\mathfrak{a}_i] \in \mathfrak{C}_{\mathcal{O},\Phi}(1)$ be such that $[\mathfrak{a}_i] \cdot [(\mathfrak{b}, \xi)] = [(\mathfrak{b}_i, \xi_i)]$, and let $c(i)$ be the index such that $[\mathfrak{a}_{c(i)}] = \left[\mathfrak{a}_i^{-1}\mathfrak{c}\right]$. Then

$$\overline{f(\tau_i)} = f(\tau_{c(i)}). \tag{5.2}$$

Remark that the condition $N \mid C_1$ of Theorem 4.4 and the ramification condition imply by Theorem 3.17, (3)⇒(1), that the ideal $N\mathcal{O}_{K_0}$ is square-free.

Proof. Notice that it is sufficient to show (5.2), which implies that the roots of the class polynomial are permuted by complex conjugation and thus the coefficients are fixed by complex conjugation, so that the polynomial is indeed an element of $K_0^r[X]$.

Let $\mathcal{Q} = \{Q_1, \ldots, Q_h\}$ be the n-system, and let $Q_i = A_iX^2 + B_iX + C_i$ be one of its elements. We first prove that B_i is divisible by N. Let $\mathfrak{p}$ be a prime divisor of $N\mathcal{O}_{K_0}$. As F and A_i are coprime to N, while C_i is divisible by N and $\mathfrak{p}$ is ramified in K/K_0, Lemma 3.18 implies that $\tilde{U}(X) = X(X + B_i)$ is a square modulo $\mathfrak{p}$, which is only possible if $\mathfrak{p} \mid B_i$. Since $N\mathcal{O}_{K_0}$ is square-free, this shows that $N \mid B_i$.

Let $Q_i' = A_i'X^2 + B_i'X + C_i'$ with $A_i' = A_i$, $C_i' = C_i$, $B_i' = -B_i$, with root $z_i' = -\overline{z_i}$ and associated period matrix τ_i'. Then by Lemma 5.1 the left hand side of (5.2) equals $f(\tau_i')$, which to simplify we will call the value of f in Q_i'. The quadratic polynomial Q_i' represents the polarised ideal class

$$\begin{aligned}\left[\left(\overline{\mathfrak{b}}_i, \xi_i\right)\right] &= [\overline{\mathfrak{a}}_i][(\overline{\mathfrak{b}}, \xi)] \text{ since the CM class group action is compatible with complex conjugation} \\ &= [\overline{\mathfrak{a}}_i\mathfrak{c}][(\mathfrak{b}, \xi)] \text{ by (5.1).}\end{aligned}$$

The right hand side of (5.2) is the value of f in $Q_{c(i)}$, which represents the same polarised ideal class $\left[\mathfrak{a}_i^{-1}\mathfrak{c}\right][(\mathfrak{b}, \xi)] = [\overline{\mathfrak{a}}_i\mathfrak{c}][(\mathfrak{b}, \xi)]$, where we have used that $\overline{\mathfrak{a}}_i\mathfrak{a}_i$, as an element of $S_{\mathcal{O},\Phi}(1)$ with $\mu = \mathrm{N}(\mathfrak{a}_i)$ in (2.7), is the identity of the CM class group.

It is now readily verified that Q_i' satisfies the conditions of the N-system as imposed by Q_i: The two polynomials are equiprimitive and satisfy $\gcd(A_i', N) = \gcd(A_i, N) = \mathcal{O}_{K_0}$ as they have the same $A_i' = A_i$ and discriminant; furthermore $B_i - B_i' = 2B_i$ is divisible by $2N$.

So $\mathcal{Q}' = \mathcal{Q}\backslash\{Q_{c(i)}\} \cup \{Q_i'\}$ is an N-system. If $h = |\mathfrak{C}_{\mathcal{O},\Phi}(1)| > 1$, then the two N-systems share a common element and by Theorem 4.4 lead to the same values of f, the roots of the class polynomial; so the values of f in $Q_{c(i)}$ and Q' are the same, that is, (5.2) holds. If $h = 1$, the proof of Theorem 4.4 shows that f has the same value in the two quadratic polynomials representing the same polarised ideal class and satisfying the N-system congruences. □

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.

We need to examine more closely the validity of (5.1). It is easily shown to hold for one element of an orbit if and only if it holds for all elements of the orbit. In practice, we will mainly consider situations in which it is known to hold for all principally polarised ideals.

Proposition 5.3. *Let $\mathcal{O}$ be an order in a CM field K with $\mathcal{O} \supseteq \mathcal{O}_{K_0}$, and let Φ be a primitive CM type of K. Let $(\mathfrak{b}, \xi)$ be a principally polarised ideal of $(\mathcal{O}, \Phi)$ such that $\mathfrak{b}$ is coprime to F. Then* (5.1) *holds for $\mathfrak{b}$ in all of the following cases:*

(1) $g \leqslant 2$;

(2) $g = 3$ and K contains an imaginary-quadratic subfield;

(3) $g = 6$, $\zeta_5 \in \mathcal{O}$, the field K is Galois over $\mathbf{Q}$, and the CM type Φ is CPQ-compatible as in [42].

Proof. Suppose that (1) holds. If $g = 1$, then one verifies directly that $\mathfrak{c} = \mathfrak{b}/\overline{\mathfrak{b}}$ and $\mu = 1$ suffice. If $g = 2$, then take $\mathfrak{a} = \mathfrak{b}\mathcal{O}_K$, $\mathfrak{c} = N_\Phi(\mathfrak{a}) \in \mathcal{I}(F)$, and $\mu = \mathrm{N}(\mathfrak{a})^{-1}$. Lemma I.8.4 of [46] then gives

$$N_{\Phi^r}(\mathfrak{c}) = \mu^{-1}\mathfrak{a}\overline{\mathfrak{a}}^{-1}. \tag{5.3}$$

Via the isomorphism between the groups of fractional ideals coprime to F of $\mathcal{O}$ and $\mathcal{O}_K$, we get $\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{c}) = \mu^{-1}\mathfrak{b}\overline{\mathfrak{b}}^{-1}$, which is the first equality of (5.1). As we have $\mathrm{N}(\mathrm{N}_\Phi(\mathfrak{a})) = \mathrm{N}(\mathfrak{a})^g$ and thus $\mathrm{N}(\mathfrak{c}) = \mathrm{N}(\mathfrak{a})^2$, we get $\mu\overline{\mu}N(\mathfrak{c}) = 1$, which is the second equality of (5.1).

In case (2), we can embed K in such a way into $\mathbf{C}$ that $K = K^r$ (see e.g. [32, Propositions 3.3.2 and 3.4.2]). Then take $\mathfrak{a} = \mathfrak{b}\mathcal{O}_K$, $\mathfrak{c} = \mathfrak{a}^{-1}\mathrm{N}_\Phi(\mathfrak{a}) \in \mathcal{I}(F)$, and $\mu = \mathrm{N}(\mathfrak{a})^{-1}$. If K is not Galois over $\mathbf{Q}$, then (5.3) is exactly equation (3.4.2) of [32], which can be shown to also hold in the Galois case using the same argument. The proof is finished exactly as for $g = 2$. Alternatively in the Galois case the displayed equation in the proof of [32, Proposition 3.3.5] gives a $\mathfrak{c}$ that works with $\mu = 1$.

In case (3), there are two possibilities for the Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$ by [42, Proposition 4.3.4].

The first case is that G is cyclic and generated by s of order 12, and after choosing an appropriate embedding of K into $\mathbf{C}$ we have $K^r = K$, $\Phi^r = \{1, s^4, s^7, s^8, s^9, s^{11}\}$, the fixed field of s^4 is $\mathbf{Q}(\zeta_5)$ and complex conjugation is s^6 by [42, Proposition 4.3.11]. Take $\mathfrak{a} = \mathfrak{b}\mathcal{O}_K$ and $\alpha \in \mathbf{Q}(\zeta_5)$ such that $\alpha\mathbf{Z}[\zeta_5] = N_{K/\mathbf{Q}(\zeta_5)}(s(\mathfrak{a}))$ and let $\mu = \overline{\alpha}/\alpha \in \mathbf{Q}(\zeta_5)$. Let $\mathfrak{c} = (s(\mathfrak{a})s^5(\mathfrak{a}))/(\mathfrak{a}s^6(\mathfrak{a}))$. A direct computation (or the first displayed equation of the proof of [42, Proposition 4.3.13]) again gives (5.3). We also have $\mu\overline{\mu} = 1$ and $N(\mathfrak{c}) = 1$.

The final case is where $G = \langle s, t : ts = s^5t, t^2 = s^3, s^6 = 1\rangle$, the fixed field of s^2 is $\mathbf{Q}(\zeta_5)$, complex conjugation is s^3, and after choosing an appropriate embedding of K into $\mathbf{C}$ we have $K^r = K$ and $\Phi^r = \{1, s^2, s^4, s^3t, s^4t, s^5t\}$ by [42, Proposition 4.3.15]. Take $\mathfrak{a} = \mathfrak{b}\mathcal{O}_K$ and $\alpha \in \mathbf{Q}(\zeta_5)$ such that $\alpha\mathbf{Z}[\zeta_5] = N_{K/\mathbf{Q}(\zeta_5)}(t(\mathfrak{a}))$ and let $\mu = \overline{\alpha}/\alpha$. Let $\mathfrak{c} = t(\mathfrak{a})/s^5t(\mathfrak{a})$. A direct computation (or the displayed equation of the proof of [42, Proposition 4.3.16]) again gives (5.3). We also have $\mu\overline{\mu} = 1$ and $N(\mathfrak{c}) = 1$. □

Notice that by the discussion following (4.4) the fractional ideal $\mathfrak{b}_1$ occurring in Theorem 5.2 is coprime to F since it comes from a quadratic polynomial with $\gcd(A_1, F) = 1$, so Proposition 5.3 applies in this case.

5.2 Real class polynomials from the Fricke involution

The following result is a generalisation of [14, 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 5.4. *Under the conditions of Theorem 4.4, suppose furthermore that we have* $\gcd(N, C_i/N) = 1$ *for all elements* $Q_i = A_iX^2 + B_iX + C_i$ *of the* N*-system and that* f *is invariant under the Fricke involution* $\iota : \tau \mapsto -N\tau^{-1}$ *of* $\mathbf{H}_g$*. Denote by* z_i *the roots of the* N*-system and by* $[(\mathfrak{b}_i, \xi_i)]$ *the associated polarised ideal classes. Let* $\mathfrak{N} = N\mathcal{O} + A_1z_1\mathcal{O}$*. Assume that the following hypothesis is satisfied for*

$\mathfrak{b} = \mathfrak{b}_1 = z_1\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$:

$$\begin{aligned} &\text{There exist } \mathfrak{c} \in \mathcal{I}(F) \text{ and } \mu \in K^\times \\ &\text{such that } \mu^{-1}\,\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{c})^{-1}\mathfrak{b}\mathfrak{N} = \overline{\mathfrak{b}} \text{ and } \mu\overline{\mu}\,\mathrm{N}(\mathfrak{c}) = N. \end{aligned} \tag{5.4}$$

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

More precisely, let $[\mathfrak{a}_i] \in \mathfrak{C}_{\mathcal{O},\Phi}(1)$ be such that $[\mathfrak{a}_i]\cdot[(\mathfrak{b},\xi)] = [(\mathfrak{b}_i,\xi_i)]$, and let $c(i)$ be the index such that $[\mathfrak{a}_{c(i)}] = \left[\mathfrak{a}_i^{-1}\mathfrak{c}\right]$. Then

$$\overline{f(\tau_i)} = f(\tau_{c(i)}). \tag{5.5}$$

Before proving this theorem, we have a closer look at the different assumptions occurring in it, assessing how to verify them and whether they represent important limitations.

The congruence condition $\gcd(N, C_i/N) = 1$ is not essential: By Theorem 3.17(2) we may assume that it holds for $i = 1$, and then impose that $B_i = B_1$ modulo higher powers of prime ideals dividing $N\mathcal{O}_{K_0}$ (very crudely, switching to an N^2-system will work).

Condition (5.4) is a variation on (5.1). In fact, letting $N = 1$ and thus $\mathfrak{N} = \mathcal{O}$ in (5.4) retrieves (5.1) as a special case. Moreover, if (5.1) is valid (for instance under the conditions of Proposition 5.3), then (5.4) becomes equivalent to the following:

$$\begin{aligned} &\text{There exist } \mathfrak{c} \in \mathcal{I}(F) \text{ and } \mu \in K^\times \\ &\text{such that } \mathfrak{N} = \mu\,\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{c}) \text{ and } \mu\overline{\mu}\,\mathrm{N}(\mathfrak{c}) = N, \end{aligned} \tag{5.6}$$

which again shows that (5.4) is independent of the element in the orbit, at least under (5.1), and that in reality it is a statement about $\mathfrak{N}$. We will see in Proposition 5.8 that this condition often holds. The example in Section 7.5 shows that it is necessary in the sense that the theorem becomes false when replacing the condition with (5.1).

In order to 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 5.5. Let $\mathbf{Z}$-bases $\mathcal{B}_1$ and $\mathcal{B}_2$ of $\mathcal{O}_{K_0}$ be given as in Proposition 3.2, and let $S \in \mathrm{GL}_g(\mathbf{Z})$ be the matrix such that $\mathcal{B}_2^T = S\mathcal{B}_1^T$. Then S is symmetric.

If τ is the period matrix associated to z by Proposition 3.2, then the period matrix associated to $-1/z$ is

$$\tau' = \begin{pmatrix} 0 & -S^{-1} \\ S & 0 \end{pmatrix}\tau = -(S\tau S)^{-1}. \tag{5.7}$$

Proof. Notice that $S = [1]_1^2$ and $S^{-1} = [1]_2^1$ with the notation of (3.8). Then by Lemma 3.12, the matrix

$$\mathbb{M} = \left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right] = \begin{pmatrix} 0 & -S^{-1} \\ S & 0 \end{pmatrix}$$

satisfies $\mathbb{M} \in \mathrm{Sp}_{2g}(\mathbf{Z})$, which implies $S = S^T$.

It remains to show that $\tau' = \mathbb{M}\tau$, which is the special case $M = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ of Lemma 3.13. □

Example 5.6. 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

$$S = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \text{ if } \Delta_0 \text{ is even, and } S = \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix} \text{ if } \Delta_0 \text{ is odd.}$$

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 the Fricke involution $\iota : \tau \mapsto -N\tau^{-1}$ if and only if it is invariant under ι'.

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

Proof. Let $S = [1]_1^2$ be as in Lemma 5.5. 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 (5.7) in Lemma 5.5.

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 5.4. We follow the same approach as in the proof of Theorem 5.2.

By Lemma 5.1, we have $\overline{f(\tau_i)} = f(-\overline{\tau_i})$, with the latter period matrix corresponding to $-\overline{z}_i$. By Lemma 5.7(2) and invariance of f under the Fricke involution, $f(-\overline{\tau_i}) = f(\iota'(-\overline{\tau_i}))$, and by 5.7(1) the latter period matrix corresponds to $z_i' = N/\overline{z}_i$. This is a root of the polynomial $Q_i' = A_i'X^2 + B_i'X + C_i'$ with $A_i' = C_i/N$, $B_i' = B_i$ and $C_i' = A_iN$, which satisfies the N-system conditions as imposed by Q_i: The discriminant $B_i^2 - 4A_iC_i$ of Q_i is totally negative, so that with A_i totally positive also C_i is totally positive. Since $\gcd(N, C_i/N) = 1$ by assumption, the polynomial Q_i' is semiprimitive modulo N as in Definition 3.5. Moreover, the discriminants of Q_i' and Q_i are equal, which implies equiprimitivity modulo N as in Definition 4.1.

The left hand side of (5.5) is the value of f in Q_i', the right hand side is the value of f in $Q_{c(i)}$. If we can show that the two polynomials represent the same principally polarised ideal class, we conclude as in the proof of Theorem 5.2 that they lead to the same value and thus finish the proof of Theorem 5.4.

Condition (5.4) and invertibility of $\mathfrak{b}$ (Proposition 3.6) imply that $\mathfrak{N}$ is invertible and $[\mathfrak{c}] \cdot [(\mathfrak{b}_1, \xi_1)] = \left[(\mathfrak{N}^{-1}\overline{\mathfrak{b}_1}, N\xi_1)\right]$, and this gives us a handle on $Q_{c(i)}$, which represents the polarised ideal class

$$\begin{aligned}
[\mathfrak{a}_{c(i)}][(\mathfrak{b}_1, \xi_1)] &= \left[\mathfrak{a}_i^{-1}\mathfrak{c}\right][(\mathfrak{b}_1, \xi_1)] \text{ by definition} \\
&= [\overline{\mathfrak{a}}_i]\left[(\mathfrak{N}^{-1}\overline{\mathfrak{b}}_1, N\xi_1)\right] \\
&\quad \text{from the action of } \mathfrak{c} \text{ and since } \left[\mathfrak{a}_i^{-1}\right] = [\overline{\mathfrak{a}}_i] \text{ as seen before} \\
&= \left[(\mathfrak{N}^{-1}\overline{\mathfrak{b}}_i, N\xi_i)\right] \\
&\quad \text{by compatibility of the type norm with complex conjugation.}
\end{aligned}$$

It remains to show that Q_i' represents the same polarised ideal class. By Proposition 3.1 it leads to the polarised ideal $(\mathfrak{b}_i', \xi_i')$ with $\mathfrak{b}_i' = (N/\overline{z}_i)\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ and

$$\xi_i' = ((N/\overline{z_i} - N/z_i)\lambda)^{-1} = N^{-1} z_i \overline{z}_i \left((z_i - \overline{z}_i)\lambda\right)^{-1},$$

which is equivalent to $\left(N^{-1}\overline{z}_i\mathfrak{b}_i', N^2/(z_i\overline{z_i})\xi_i'\right) = \left(N^{-1}\overline{z}_i\mathfrak{b}_i', N\xi_i\right)$.

The component $N\xi_i$ is already what we are looking for, and it remains to show that

$$\mathfrak{N}(N^{-1}\overline{z}_i\mathfrak{b}_i') = \overline{\mathfrak{b}}_i \tag{5.8}$$

on the ideal side. We first examine $\mathfrak{N}$ more closely. Let $\vartheta_1 = A_1 z_1$ and $\vartheta_i = A_i z_i$. Since by equiprimitivity the quadratic polynomials Q_1 and Q_i have the same discriminant, we obtain $\vartheta_1 - \vartheta_i = \frac{B_i - B_1}{2}$, and this difference is divisible by N from the N-system congruences. It follows that $\mathfrak{N} = N\mathcal{O} + \vartheta_1\mathcal{O} = N\mathcal{O} + \vartheta_i\mathcal{O}$. Using

$$\mathcal{O} = \mathcal{O}_{K_0} + \mathfrak{d}_i^{-1}\vartheta_i$$

of (3.1) we compute

$$\begin{aligned}
\mathfrak{N} &= N\mathcal{O}_{K_0} + N\mathfrak{d}_i^{-1}\vartheta_i + \mathcal{O}_{K_0}\vartheta_i + \mathfrak{d}_i^{-1}\vartheta_i^2 \\
&= N\mathcal{O}_{K_0} + N\mathfrak{d}_i^{-1}\vartheta_i + \mathcal{O}_{K_0}\vartheta_i + \mathfrak{d}_i^{-1}(B_i\vartheta_i + A_iC_i) \\
&= N\mathcal{O}_{K_0} + N\mathfrak{d}_i^{-1}\vartheta_i + \mathcal{O}_{K_0}\vartheta_i \text{ since } N|C_i,\ \mathfrak{d}_i|A_i \text{ and } \mathfrak{d}_i|B_i \\
&= N\mathcal{O}_{K_0} + \mathfrak{d}_i^{-1}\vartheta_i \text{ since } \gcd(\mathfrak{d}_i, N) = 1.
\end{aligned} \tag{5.9}$$

So the left hand side of (5.8) is computed as

$$\begin{aligned}
&(N\mathcal{O}_{K_0} + \mathfrak{d}_i^{-1}A_iz_i)(\mathcal{O}_{K_0} + N^{-1}\overline{z}_i\mathcal{O}_{K_0}) \\
&= N\mathcal{O}_{K_0} + \overline{z}_i\mathcal{O}_{K_0} + \mathfrak{d}_i^{-1}A_iz_i + \mathfrak{d}_i^{-1}C_i/N \\
&= N\mathcal{O}_{K_0} + \overline{z}_i\mathcal{O}_{K_0} + \mathfrak{d}_i^{-1}(B_i - A_i\overline{z}_i) + \mathfrak{d}_i^{-1}C_i/N \\
&= N\mathcal{O}_{K_0} + \overline{z}_i\mathcal{O}_{K_0} + \mathfrak{d}_i^{-1}B_i + \mathfrak{d}_i^{-1}C_i/N \\
&= \mathcal{O}_{K_0} + \overline{z}_i\mathcal{O}_{K_0} \\
&= \overline{\mathfrak{b}}_i,
\end{aligned}$$

which finishes the proof. □

Proposition 5.8. *Let K be a CM field with a primitive CM type Φ. Let $z \in K \setminus K_0$ be a root of a quadratic polynomial $Q = AX^2 + BX + C \in \mathcal{O}_{K_0}[X]$ and let $\mathcal{O}$ be the ring of multipliers of $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$. Suppose that $N \mid C$ and that all of A, $\gcd(B, C/N)$, and the conductor $\mathfrak{f}$ of $\mathcal{O}$ are coprime to N. In each of the following cases, the ideal $\mathfrak{N} = \mathcal{O} + Az\mathcal{O}$ satisfies* (5.6) *and* (5.4)*:*

(1) $g = 1$;

(2) $g = 2$ and N is coprime to the discriminant of K.

We have identified more cases in which (5.6) holds, with somewhat lengthy proofs relying only on Galois theory and unrelated to class invariants; to lighten the presentation, we delegate these results to another venue.

Proof. Since $g \leqslant 2$ the conclusion of Proposition 5.3 holds and (5.4) and (5.6) are equivalent; we proceed to prove the latter.

Letting $\vartheta = Az$ and $\mathfrak{d} = \gcd(A, B, C)$, we obtain by (5.9) that

$$\begin{aligned}\mathfrak{N}\overline{\mathfrak{N}} &= (N\mathcal{O}_{K_0} + \mathfrak{d}^{-1}\vartheta)(N\mathcal{O}_{K_0} + \mathfrak{d}^{-1}\overline{\vartheta}) \\ &= N\left(\mathfrak{d}^{-1}\vartheta + N\mathcal{O}_{K_0} + \mathfrak{d}^{-1}B + (\mathfrak{d}^{-1}A)(\mathfrak{d}^{-1}C/N)\right) \\ &= N(\mathfrak{d}^{-1}\vartheta + \mathcal{O}_{K_0}) \text{ because of the conditions of coprimality with } N \\ &= N\mathcal{O}. \end{aligned} \tag{5.10}$$

If $g = 1$, then without loss of generality N_{Φ^r} is the identity on $K = K^r$; we take $\mu = 1$ and $\mathfrak{c} = \mathfrak{N}\mathcal{O}_K$ and conclude by (5.10).

If $g = 2$ and N is coprime to the discriminant of K, then all primes $p \mid N$ are unramified in K. This and the assumption that N is coprime to $\mathfrak{f}$ imply that B is coprime to N by Lemma 3.18. Then

$$\mathfrak{N} + \overline{\mathfrak{N}} = N\mathcal{O}_{K_0} + \mathfrak{d}^{-1}\vartheta + \mathfrak{d}^{-1}B = \mathcal{O}_{K_0} + \mathfrak{d}^{-1}\vartheta = \mathcal{O}. \tag{5.11}$$

For every $p \mid N$, let $\mathfrak{N}_p = \mathfrak{N} + (p)$; then $\mathfrak{N}_p\overline{\mathfrak{N}_p} = (p)$, and by the multiplicativity of (5.6) it suffices to show the result for p and $\mathfrak{N}_p$ in the place of N and $\mathfrak{N}$. We choose $\mu = 1$; then it is enough to show the existence of an ideal $\mathfrak{c}$ such that $\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{c}) = \mathfrak{N}_p$, from which $\mathrm{N}(\mathfrak{c}) = \mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{c})\overline{\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{c})} = \mathfrak{N}_p\overline{\mathfrak{N}_p} = p\mathcal{O}_{K_0}$ follows.

Let $\mathfrak{p}$ be a prime ideal above p of $L = KK^r$, which is the Galois closure of K. Theorems 1 and 2 of [26] give all possible decomposition groups of $\mathfrak{p}$ when p is unramified in K. By (5.11) the primes of $\mathcal{O}_{K_0}$ above p split in K/K_0, hence only case (1) of Theorem 1 and cases (1), (3), and (5) of Theorem 2 occur.

Case (1) of Theorem 1 is the totally split case with $\mathrm{Gal}(K/\mathbf{Q}) = \langle y \rangle$ for an element y of order 4 such that $\Phi = \{1, y\}$, and y^2 is complex conjugation. We have $(p) = \mathfrak{p} \cdot y(\mathfrak{p}) \cdot y^2(\mathfrak{p}) \cdot y^3(\mathfrak{p})$ and $(p) = \mathfrak{N}_p \cdot y^2(\mathfrak{N}_p)$, so that $\mathfrak{N}_p = y^a(\mathfrak{p})y^{a-1}(\mathfrak{p})$ for some $a \in \{0, 1, 2, 3\}$. Without loss of generality, we may assume $a = 0$ (or, otherwise said, we may replace $\mathfrak{p}$ by $y^a(\mathfrak{p})$); then $\Phi^r = \{1, y^{-1}\}$ implies $\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{p}) = \mathfrak{N}_p$.

Case (1) of Theorem 2 is also totally split, but now $\mathrm{Gal}(L/\mathbf{Q}) = \langle x, y \rangle \cong D_4$ with $x^2 = y^4 = 1$ and $xyx = y^3$, $\mathrm{Gal}(L/K) = \langle x \rangle$, $\mathrm{Gal}(L/K^r) = \langle xy^3 \rangle$, and y^2 is complex conjugation. The eight prime ideals of L above p are the $g(\mathfrak{p})$ for $g \in D_4$ and the prime ideals of K above p are the $y^a(\mathfrak{p}) \cdot xy^a(\mathfrak{p})$ for $a = 0, 1, 2, 3$, so $\mathfrak{N}_p = y^a(\mathfrak{p}) \cdot xy^a(\mathfrak{p}) \cdot y^{a-1}(\mathfrak{p}) \cdot xy^{a-1}(\mathfrak{p})$ for some a. Without loss of generality (that is, after potentially choosing a different $\mathfrak{p}$), we can assume $a = 0$, and then $\mathfrak{N}_p$ is exactly what appears as the type norm $\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{p} \cap K^r) = (\mathfrak{p} \cdot x(\mathfrak{p}))(y^3(\mathfrak{p})xy^3(\mathfrak{p}))$ of Case (1) on page 38 of [26], just below Theorem 2.

Cases (3) and (5) of Theorem 2 are conjugate, so without loss of generality (choosing a different $\mathfrak{p}$ for the same p if needed) we are in Case (5). In that case, pages 38 and 39 of [26] give the decomposition of p in K as a product of two primes $(p) = (\mathfrak{p}y^3(\mathfrak{p}))(y(\mathfrak{p})y^2(\mathfrak{p}))$, and the type norm as $\mathrm{N}_{\Phi^r,\mathcal{O}}(\mathfrak{p} \cap K^r) = (\mathfrak{p}y^3(\mathfrak{p}))$. But then the prime $(\mathfrak{p}y^3(\mathfrak{p}))$ of K is $\mathfrak{N}_p$ or $\overline{\mathfrak{N}_p}$, so that taking $\mathfrak{c} = \mathfrak{p} \cap K^r$ or $\mathfrak{c} = \overline{\mathfrak{p} \cap K^r}$ gives the desired result. □

Remark 5.9. We now sketch a more geometric view of Theorems 5.2 and 5.4 and their proofs, giving an alternative explanation of where the involution and the complex conjugation hypotheses (5.1) and (5.4) come from.

The variety $\Gamma^0(N)\backslash\mathbf{H}_g$ is the coarse moduli space of N-isogenies, in the sense that its points correspond to triples $t = (A, A', \varphi)$, where A and A' are principally polarised abelian varieties of dimension g and $\varphi : A \to A'$ is an N-isogeny. Each

$z = z_i \in K \setminus K_0$ gives rise to such a triple $t = t_i$ as follows. With $\mathfrak{b} = z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ and ξ as in Proposition 3.1, we get a principally polarized abelian variety $A/\overline{\mathbf{Q}}$ with $A(\mathbf{C}) \cong \mathbf{C}^g/\Phi(\mathfrak{b})$, which has CM by $(\mathcal{O}, \Phi)$ via an isomorphism $\iota : \mathcal{O} \to \mathrm{End}(A)$. Similarly from $z' = N^{-1}z$ we get $\mathfrak{b}'$, ξ', A', and ι'. Moreover, we now have the N-isogeny $\varphi : A \to A'$ that is the identity on $\mathbf{C}^g$.

Let f be a function on $\Gamma^0(N)\backslash\mathbf{H}_g$ defined over $\mathbf{Q}$, as in our theorems. The values $f(\tau_i) = f(t_i)$ will depend only on the isomorphism classes of the corresponding triples t_i. Moreover, for any $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, including complex conjugation, we have $\sigma(f(t)) = f(\sigma(t))$.

To get a class polynomial with real coefficients, we want to have $\bar{t} \cong \sigma(t)$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/K^r)$. To see when this can and cannot happen we look more closely at the kernel of φ as follows.

Under some mild assumptions, we have (similarly to (5.8)) the equality $\mathfrak{b}' = \overline{\mathfrak{N}}^{-1}\mathfrak{b}$ for some ideal $\mathfrak{N}$ with $\mathfrak{N}\overline{\mathfrak{N}} = (N)$. It follows that φ is actually an $\overline{\mathfrak{N}}$-*multiplication* with respect to the CM type Φ, that is, an isogeny satisfying

$$\ker(\varphi) = A[\iota(\overline{\mathfrak{N}})] := \bigcap_{\beta \in \overline{\mathfrak{N}}} \ker(\iota(\beta)) \text{ and } \iota'(\alpha) \circ \varphi = \varphi \circ \iota(\alpha) \tag{5.12}$$

for all $\alpha \in \mathcal{O}$, where both ι and ι' have type Φ.

Complex conjugation turns $t = (A, A, \varphi)$ into $\bar{t} = (\overline{A}, \overline{A'}, \overline{\varphi})$. The complex conjugate abelian varieties $\overline{A}$ and $\overline{A'}$ again have CM type Φ once we adorn them with $\bar{\iota} : \alpha \mapsto \overline{\iota(\overline{\alpha})}$ and the similarly defined $\overline{\iota'}$. Then $\overline{\varphi}$ is an $\mathfrak{N}$-multiplication (with $\mathfrak{N}$, not $\overline{\mathfrak{N}}$) as can be seen by taking complex conjugates of (5.12).

On the other hand, all $\mathrm{Gal}(\overline{\mathbf{Q}}/K^r)$-conjugates of the $\overline{\mathfrak{N}}$-multiplication φ are again $\overline{\mathfrak{N}}$-multiplications with respect to the CM type Φ ([41, Proof of Prop. 11 in §14.7, see also §7.6 and Prop. 31 of §8.5]). So in order for $\bar{t}$ to be $\mathrm{Gal}(\overline{\mathbf{Q}}/K^r)$-conjugate to t, we need to have $\mathfrak{N} = \overline{\mathfrak{N}}$.

This explains why Theorem 5.2 assumes that all primes dividing N ramify in K: so that we have $\mathfrak{N} = \overline{\mathfrak{N}}$. As the $\mathrm{Gal}(\overline{\mathbf{Q}}/K^r)$-action is not always transitive, we need to supplement this assumption with the assumption that the first components $\overline{A}$ and A of $\bar{t}$ and t are in the same orbit, which is exactly (5.1).

However, if $\mathfrak{N} \neq \overline{\mathfrak{N}}$, then we need to somehow turn our $\mathfrak{N}$-multiplication $\overline{\varphi}$ back into an $\overline{\mathfrak{N}}$-multiplication. We can do so by taking its dual, see [41, §14.4, Prop. 6], which corresponds to taking the Fricke involution on the moduli space. This is why we assume that f is fixed under the Fricke involution in Theorem 5.4: so that f makes no distinction between $\bar{t}$ and its dual $(\overline{A'}, \overline{A}, \overline{\varphi}^\dagger)$. To get a class polynomial with real coefficients, we furthermore need $\overline{A'}$ and A to be in the same $\mathrm{Gal}(\overline{\mathbf{Q}}/K^r)$-orbit, which is exactly (5.4) in Theorem 5.4.

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 3.9, i.e., functions that are invariant under $\Gamma^0(N)$ and quotients of modular forms with rational q-expansions. We will use them in Section 7 to provide numerical examples. These are just a few examples. We expect that many more good functions exist, and we leave a thorough search for future research.

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 $\mathrm{Sp}_4(\mathbf{Z})$ [31]; so for $\mathbb{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbf{Z})$ and $\mathbb{M}\tau = (a\tau + b)(c\tau + d)^{-1}$, one has $h_k(\mathbb{M}\tau) = \det(c\tau + d)^k h_k(\tau)$. Taking quotients of forms of the same weight yields modular functions for $\mathrm{Sp}_4(\mathbf{Z})$ such as

$$i_1 = \frac{h_4 h_6}{h_{10}}, \quad i_2 = \frac{h_4^2 h_{12}}{h_{10}^2}, \quad \text{and} \quad i_3 = \frac{h_4^5}{h_{10}^2}$$

known as *absolute Igusa invariants*. There are many possible choices of absolute Igusa invariants; the above functions correspond to [47]. Since these are modular functions for the full modular group, their CM values are automatically class invariants.

Alternatively, one may take *simple h_k-quotients*

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

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

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

stable under $\Gamma^0(N)$ for $N = N_1 N_2$. The latter function is also invariant under the Fricke involution $\iota : \tau \mapsto -N\tau^{-1}$ of Theorem 5.4:

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

where we have used $h_k(-\tau^{-1}) = h_k(\mathbb{J}\tau) = \det(-\tau)^k h_k(\tau)$ for $\mathbb{J}$ as in (2.3).

As for simple and double eta quotients in dimension 1, the process may be generalised to obtain multiple quotients of h_k, cf. [15].

For $k = 10$, similar functions and their square roots have also been studied by de Shalit and Goren [40].

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 abridged notation

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

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

Ibukiyama has shown in [29, 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 $2^{12}\,yk = h_{10}$.

Evaluating 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 X^2/Y, Z/Y and X^3/K.

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 $\Gamma^0(2N_1N_2)$. The form $F = X$ is promising in this context due to its low weight, as is the divisor $F = Y$ of h_{10}.

7 Numerical examples

7.1 Implementation and setup for reproducibility

We have implemented the algorithms described above in the PARI/GP system [1] at version 2.15.4; the code for reproducing our example class polynomials is made available as supplementary material to this article [16]. More precisely, we have added code for computing N-systems to the GP script `shimura.gp` in the latest release 1.1.1 of CMH [19], developed by the first author, Emmanuel Thomé and Régis Dupont and described in [20]. This N-system code is now also used in CMH for Igusa class polynomials with $N = 1$. The CMH library provides C code for asymptotically fast evaluations of Siegel modular forms using arbitrary precision floating point operations. It can be called from GP scripts using the PariTwine software [11] at version 0.2.0, which relies additionally on GNU MP at version 6.2.1 [27], GNU MPFR at version 4.2.0 [28] and GNU MPC at version 1.3.1 [18]. The GP script `common.gp` modifies the N-system computation of CMH to enforce the divisibility conditions of Theorems 3.9 and 5.4 of the values C_i using the algorithms of the proof of Theorem 3.17. It then calls CMH through PariTwine to compute the complex roots of the class polynomial and it guesses the correct algebraic class polynomial. It is called by the scripts `example1.gp`, `example2.gp` and `example3.gp`, which compute the Igusa class polynomials and our alternative class polynomials for the examples given in detail in the following three subsections.

Additionally, we have used the second author's RECIP [48] code at version 3.4.1, which is developed as a package for SageMath [38], to compute Igusa class polynomials; its `class_polynomial` command returns a result proved to be correct by the

approaches of Bouyer–Streng [4] and Lauter–Viray [34]. In all cases, these Igusa polynomials were identical to those computed using CMH and our GP scripts.

We followed the reproducibility approach described in [6] to easily make the results available to the reader through Guix [25]. For reproducing the computation of the first example, it is enough to run from the subdirectory `parigp` of [16] the command

```
guix time-machine -C channels.scm -- shell -C -m manifest.scm -- \
   gp < example1.gp
```

and analogously for the other examples, using the provided files `channels.scm` and `manifest.scm`, which record the computing environment with the exact dependencies of all required software.

Outside of Guix, the reader may install the software packages given above at their respective versions into the prefix `/usr/local`, say, and then call

```
export GUIX_ENVIRONMENT=/usr/local
gp < example1.gp
```

7.2 Detailed example for a Hilbert class field

To illustrate the approach, we provide an example of a class polynomial. We choose K primitive such that K^r has odd class number and K_0^r has class number 1, so that by [46, 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 $K_0 = \mathbf{Q}(y) \cong \mathbf{Q}(\sqrt{5})$ 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 $\omega_r = -\frac{1}{4}(t^2+55) = \frac{1+\sqrt{661}}{2}$, where the positive real square root has been taken. We find that the Igusa 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 3.17 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 $3 \mid C_1$. With the approach of Theorem 3.17 we find $[A_1, B_1, C_1] = [1, 1, 3\omega + 6]$.

This quadratic form has discriminant $D = -12\omega - 23$ and a 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 that is positive imaginary under the two embeddings φ_1 and φ_2. Following Corollary 3.3, we obtain for z_1 the period matrix

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

We compute

$$f_1 = I_4(\tau_1/3)/I_4(\tau_1) \approx 4.31041770567796242256320 - 1.05769871912283540433298i,$$

which is a class invariant by Theorem 3.9.

The CM class group $\mathfrak{C}_{\mathcal{O}_K,\Phi}(1)$ is isomorphic to the image $\mathfrak{D}$ of the homomorphism

$$\mathrm{Cl}(\mathcal{O}_{K^r}) \to \left\{ (\mathfrak{b}, \nu) : \begin{array}{l} \mathfrak{b} \text{ fractional ideal of } \mathcal{O}_K, \\ \nu \in K_0, \nu \gg 0, \mathrm{N}_{K/K_0}(\mathfrak{b}) = \nu\mathcal{O}_{K_0} \end{array} \right\} / \sim, \tag{7.1}$$

$$\mathfrak{a} \mapsto (N_{\Phi^r,\mathcal{O}_K}(\mathfrak{a}), N(\mathfrak{a})), \tag{7.2}$$

where the equivalence relation $\sim$ is given by the subgroup $\{(\mu\mathcal{O}_K, \mu\overline{\mu}) : \mu \in K^\times\}$; it can be computed as in [20] by the function `shimura_group_type_norm_subgroup` of CMH. In this particular example, the group $\mathfrak{D}$ is of order 3. We have implemented Algorithm 4.7 as the function `nsystem` in CMH; for $N = 3$, it outputs, besides the initial $[1, 1, 3\omega + 6]$, the polynomials

$$[7\omega + 24, 48\omega - 83, -72\omega + 117] \text{ and } [3\omega + 14, -12\omega + 49, -24\omega + 51].$$

As a quick check, one immediately sees that the A are coprime to 3 and that the B are congruent to 1 modulo 6; then it is readily verified that the discriminants are the same.

The three period matrices are computed by the functions `symplectic_basis` and `period_matrix` of CMH. They lead to the floating point polynomial

$$\begin{aligned} F(X) \approx X^3 &+ (-1520.818645778858227823 22 + 358.629756234205144714067i)X^2 \\ &+ (120340.426264405965468052 - 39203.237756783401358759 2i)X \\ &+ (-454033.008835683648854405 + 276194.792435730065214643i), \end{aligned}$$

the coefficients of which are (not necessarily integral) elements of the reflex field K^r. Using the command `recognize_polynomial` of recip (based on the LLL algorithm) on K^r and a more precise approximation of F we find conjecturally

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

with $d' = 2^3 \cdot 11^5 \cdot 31^2$. Alternatively, we can also obtain this polynomial as follows. Guessing the minimal polynomials of the coefficients (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 multiply F with $d' = 2^3 \cdot 11 \cdot d$. 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 above.

The height of this polynomial is a bit smaller than that of the classical polynomial obtained from Igusa invariants above, but only moderately so. Moreover since the polynomial has coefficients in the CM field K^r instead of its totally real subfield K_0^r, printing all coefficients actually takes more space. But maybe it is not very surprising that quotients of Igusa invariants do not result in a substantial gain in size: They are an analogue in dimension 2 of quotients of the elliptic modular form Δ, which in turn are the 24-th powers of η-quotients; only lower powers of such quotients are known to yield smaller class invariants [13].

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 given by

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

7.3 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 non-Galois quartic CM field with x a root of $X^4 + 18X^2 + 68$, which has real subfield $K_0 = \mathbf{Q}(\sqrt{13})$, where $\sqrt{13} = x^2 + 9$. Consider again the maximal order $\mathcal{O} = \mathcal{O}_K$. The hypothesis (5.1) in Theorem 5.2 holds by Proposition 5.3(1).

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 with the function i_1, we obtain the following Igusa class polynomial for K:

$$\begin{aligned} & 19^2 \cdot 59^2 \cdot X^4 + (13817456632163323131 30\omega_r - 3547293859211493542130)X^3 \\ & + (14847399540341502978206984 1975\omega_r - 3803219239613918225257814694 75)X^2 \\ & + (53446717303584740489076774954210 00\omega_r - 1369063916394900234276201766812 9000)X \\ & + (52888480565700710835194263641602550000\omega_r - 1354765672661534272258644627137882 70000). \end{aligned}$$

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

$$A_1 = 1, \quad B_1 = 0, \quad C_1 = 16\omega + 22,$$

where C_1 is divisible by $N = 2$. We will thus obtain a class polynomial defined over K_0^r by Theorem 5.2.

The group $\mathfrak{C}_{\mathcal{O}_K,\Phi}(1)$ is cyclic of order 4, and a 2-system is computed as

$$\begin{aligned} & A_2 = A_3 = 5\omega + 7, && B_2 = -B_3 = 8\omega + 8, && C_2 = C_3 = 2\omega + 8, \\ & A_4 = -\omega + 5, && B_4 = 0, && C_4 = 6\omega + 8, \end{aligned}$$

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 $f = i_1 = h_4h_6/h_{10}$, we get exactly the polynomial above. For the function $f = X^2/Y$ of §6.2, we obtain numerically the following class polynomial:

$$\begin{aligned} X^4 &- 19506.967024137696849928723905438692311 17X^3 \\ &+ 34104.710879805841997045921439355140420 24X^2 \\ &- 31621.315449235542959712862322005592043 41X \\ &+ 17775.001585130354576554260234894978533 78, \end{aligned}$$

which can be rewritten over K_0 as

$$\begin{aligned} 19^4 \cdot 59^2 \cdot X^4 &+ (41960216624328\omega_r - 116332595812008)X^3 \\ &+ (-924565238142480\omega_r + 2383794199841616)X^2 \\ &+ (8404908240715776\omega_r - 21543961272975360)X \\ &+ (-10331028745814016\omega_r + 26471539326320640), \end{aligned}$$

which is noticeably smaller than the Igusa class polynomial. As Y is the square of a modular form, the function f is the square of a modular function. Again it turns out that the zeroes of the previous polynomial are squares of the zeroes of an even smaller polynomial, namely of:

$$\begin{aligned} 19^2 \cdot 59 \cdot X^4 &+ (-2523732\omega_r + 9426660)X^3 + (17576244\omega_r - 46804644)X^2 \\ &+ (-15869952\omega_r + 38596608)X - 49372416\omega_r + 129309696. \end{aligned}$$

7.4 Real example with a double Igusa quotient

The following example illustrates Theorem 5.4. Let $\mathcal{O}$ be the maximal order of the non-Galois quartic CM field $K = \mathbf{Q}(x)$ with x a root of $X^4 + 53X^2 + 601$ and with real subfield $K_0 \cong \mathbf{Q}(\sqrt{5})$. 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. With CMH and RECIP and i_1 we obtain the following Igusa class polynomial for K:

$$\begin{aligned} &2^{40} \cdot 13^4 \cdot X^5 \\ &+ (-614058542222020444579430 4\omega_r - 322904904921695447307780096)X^4 \\ &+ (-966328840322764032741757419 52\omega_r - 413142774420346684276332088 5248)X^3 \\ &+ (-961856435411091691207536138780672\omega_r - 199224267525331686318496120732385 28)X^2 \\ &+ (-281087887503220694727970359035087641 6\omega_r - 325074516288879508580178801914290211 84)X \\ &+ (-394999172899294951535875785508015253080 1\omega_r - 591879683087731591574848056616335060746 74) \end{aligned}$$

We fix $N = 6$, the product of two primes that are inert in $K_0/\mathbf{Q}$ and split in K/K_0. The hypothesis (5.4) then follows from Proposition 5.8(2). Moreover, by Theorem 3.17, there is a quadratic polynomial $A_1X^2 + B_1X + C_1$ representing a polarised ideal class with $6 \mid C_1$ and $\gcd(C_1/6, 6) = 1$; for instance, $A_1 = 1$, $B_1 = \omega + 5$ and $C_1 = 6\omega + 12$, where $\omega = \frac{1}{9}(x^2 + 31)$. 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 3.9, the value $f(\tau_1)$ is a class invariant, and by Theorem 5.4, its minimal polynomial is real.

A 6-system containing this initial form $Q_1 = [A_1, B_1, C_1]$ is computed as

$$\begin{array}{lll} A_1 = 1, & B_1 = \omega + 5, & C_1 = 6\omega + 12; \\ A_2 = -3\omega + 7, & B_2 = 145\omega - 211, & C_2 = -1110\omega + 1866; \\ A_3 = 3\omega + 7, & B_3 = -143\omega + 5, & C_3 = 294\omega + 606; \\ A_4 = -34\omega + 157, & B_4 = -3959\omega + 2309, & C_4 = 4194\omega + 34356; \\ A_5 = \omega + 2, & B_5 = -71\omega + 5, & C_5 = 180\omega + 546. \end{array}$$

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 $f(\tau_3)$ and $f(\tau_5)$ on the other hand are complex conjugate pairs.

Numerically the class polynomial is approximated by

$$\begin{aligned} X^5 &- 277.27759072275568417X^4 + 3131337.2766719955916X^3 \\ &- 6196803.8120055534180X^2 - 2658.4275679312005124X - 1. \end{aligned}$$

Multiplying by the guessed denominator and identifying the resulting coefficients as elements of $\mathbf{Z}[\omega_r]$ leads to the class polynomial

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

which is already considerably smaller than the classical Igusa polynomial.

As h_{10} is the square of a modular form, the function f is the square of a modular function. It turns out that the zeroes of the previous polynomial are squares of the zeroes of the following even smaller polynomial:

$$\begin{aligned} 2^2 \cdot 13^2 X^5 &+ (1326\omega_r + 23894)X^4 + (8833\omega_r + 1025477)X^3 \\ &+ (-14003\omega_r - 1482307)X^2 + (-2040\omega_r - 6080)X - 2^2 \cdot 13^2. \end{aligned}$$

7.5 Necessity of the second complex conjugation hypothesis

We now give an example that does not satisfy (5.4), so Theorem 5.4 does not apply, and for which the associated class polynomial is defined over K^r, but not K_0^r.

Let $\mathcal{O} = \mathcal{O}_K$ be the maximal order of the non-Galois quartic CM field $K = \mathbf{Q}(x)$ with x a root of $x^4 + 11x^2 + 29$ and with real subfield $K_0 \cong \mathbf{Q}(\sqrt{5})$. The class group of K is of order 2 and generated by the ideal $\mathfrak{p}_2 = (2, x^2 + x + 5)$. For every CM type of K, the abelian varieties with CM by $\mathcal{O}_K$ of that type are, up to $\overline{\mathbf{Q}}$-isomorphism and the action of $\mathrm{Gal}(K_0^r/\mathbf{Q})$, the Jacobians of two curves over K_0^r given in [4, Table 2B]. In particular, the CM class group $\mathfrak{C}_{\mathcal{O}_K,\Phi}(1)$ is trivial.

We fix $N = 14$, the product of the two primes 2 and 7 that are inert in $K_0/\mathbf{Q}$. The prime 2 ramifies as $(2) = \mathfrak{p}_2^2$ with $\mathfrak{p}_2$ as above, and 7 splits as $(7) = \mathfrak{p}_7\overline{\mathfrak{p}_7}$ with the principal ideal $\mathfrak{p}_7 = (x^2 + x + 6)$.

Let $\omega = x^2 + 6$ and consider the quadratic polynomial $AX^2 + BX + C$ with $A = 1$, $B = 12\omega - 2$, $C = 14(2\omega + 3)$. Let z be a root of this polynomial and choose

the CM type Φ in a compatible way. From z we compute $\mathfrak{b} = (1)$, $\xi = (2x^3+16x)^{-1}$, and $\mathfrak{N} = N\mathcal{O}_K + Az\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_7$, which is non-principal. As $\mathfrak{C}_{\mathcal{O}_K,\Phi}(1)$ is trivial, we get that $\mu N_{\Phi^r,\mathcal{O}_K}(\mathfrak{c})$ is principal in (5.6) and hence never equal to $\mathfrak{N}$. So we get that (5.6) does not hold, and hence by Proposition 5.3 neither does the second complex conjugation hypothesis (5.4).

Consider the simple I_4 quotient

$$h(\tau) = I_4(\tau/N)/I_4(\tau),$$

which has rational q-expansion coefficients and is modular for $\Gamma^0(N)$. The function $f = h + h \circ \iota$ is stable under the Fricke involution $\iota : \tau \mapsto -N/\tau^{-1}$.

We use interval arithmetic and [48] to evaluate f in the point τ obtained from z. This yields

$$f(\tau) \approx -65577.5 + 546773.0i,$$

with an error of absolute value less than 10^{-1}, which proves that $f(\tau)$ is non-real, and hence confirms that its (linear) class polynomial does not have coefficients in K_0^r. This proves that condition (5.4) is necessary in Theorem 5.4.

We used the complicated function f instead of a double Igusa quotient for the following reason. Let $z_7 = z/7$, which is a root of $(7A)X^2 + BX + (C/7)$ and gives rise to $\tau_7 = \tau/7$. Then the double Igusa quotient

$$\frac{h_k(\tau/2)h_k(\tau/7)}{h_k(\tau)h_k(\tau/14)} = \frac{h_k(\tau/2)}{h_k(\tau)} \cdot \left(\frac{h_k(\tau_7/2)}{h_k(\tau_7)}\right)^{-1}$$

is a quotient of simple Igusa quotients with ramified level 2, which for this example both lie in K_0^r by Theorem 5.2, hence do not illustrate the necessity of (5.4). In fact, as $\mathfrak{p}_7$ is principal, we find that both simple Igusa quotients take the same value and hence this double Igusa quotient is equal to 1.

References

[1] [SW Rel.] Bill Allombert and Karim Belabas, *PARI/GP* version 2.15.4, Feb. 2024. LIC: GPL-2.0-or-later. URL: `https://pari.math.u-bordeaux.fr/`, SWHID: ⟨`swh:1:dir:8e76e2daa122f03e6a9206e18a62aa7ab48efb93;origin=https://pari.math.u-bordeaux.fr/git/pari.git;visit=swh:1:snp:cd7a1ce7663980b27dfdfc3e96c97fb073271c02;anchor=swh:1:rel:68863db68dd3d346ce5685ad767360c01dfca26a`⟩.

[2] [SW] Bill Allombert and Karim Belabas, *PARI/GP*. LIC: GPL-2.0-or-later. URL: `https://pari.math.u-bordeaux.fr/`.

[3] Jared Asuncion. "Complex multiplication constructions of abelian extensions of quartic fields". PhD thesis. Université de Bordeaux and Universiteit Leiden, 2022.

[4] Florian Bouyer and Marco Streng. “Examples of CM curves of genus two defined over the reflex field”. In: *LMS J. Comput. Math.* 18.1 (2015). arXiv:1307.0486, pp. 507–538. ISSN: 1461-1570. DOI: 10.1112/S1461157015000121. URL: http://dx.doi.org/10.1112/S1461157015000121.

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

[6] Ludovic Courtès et al. *A guide to reproducible research papers*. June 2023. URL: https://hpc.guix.info/blog/2023/06/a-guide-to-reproducible-research-papers/.

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

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

[9] Andreas Enge. cm — *Complex multiplication of elliptic curves*. 0.4.0. Distributed under GPL v3+, https://www.multiprecision.org/cm/. INRIA. May 2022.

[10] Andreas Enge. “The complexity of class polynomial computation via floating point approximations”. In: *Mathematics of Computation* 78.266 (2009), pp. 1089–1107.

[11] [SW Rel.] Andreas Enge and Fredrik Johansson, *PariTwine* version 0.2.0, Feb. 2024. LIC: GPL-2.0-or-later. URL: https://www.multiprecision.org/paritwine/, SWHID: ⟨swh:1:dir:fd037e066d9e70bdb470d0fccc436c4abf6a5fc4;origin=https://gitlab.inria.fr/enge/paritwine;visit=swh:1:snp:df00e58f1e998be5919b0f0c8abca51ab73071ef;anchor=swh:1:rev:5daceec1db5b6fcba8358f01dfa14eb87d49a06f⟩.

[12] Andreas Enge and François Morain. “Comparing Invariants for Class Fields of Imaginary Quadratic Fields”. In: *Algorithmic Number Theory — ANTS-V*. Ed. by Claus Fieker and David R. Kohel. Vol. 2369. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2002, pp. 252–266. URL: papers/ants5.ps.gz.

[13] Andreas Enge and François Morain. “Generalised Weber Functions”. In: *Acta Arithmetica* 164.4 (2014), pp. 309–341.

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

[15] Andreas Enge and Reinhard Schertz. “Singular values of multiple eta-quotients for ramified primes”. In: *LMS Journal of Computation and Mathematics* 16 (2013), pp. 407–418.

[16] [SW Rel.] Andreas Enge and Marco Streng, *nsystem-cmh* version 0.2, June 2024. LIC: GPL-3.0-or-later. URL: `https://gitlab.inria.fr/enge/nsystem-cmh`, SWHID: ⟨`swh:1:dir:cb8b485fcebc16e01fb728348992bfcd44efc4a1;origin=https://gitlab.inria.fr/enge/nsystem-cmh.git;visit=swh:1:snp:97e5601fd87d6f82853cfc43515e39bfe0abd437;anchor=swh:1:rev:b714c397ca053fef1a9e98fbd5804798667e623a`⟩.

[17] Andreas Enge and Andrew V. Sutherland. “Class Invariants by the CRT Method”. In: *Algorithmic Number Theory — ANTS-IX*. Ed. by Guillaume Hanrot, François Morain, and Emmanuel Thomé. Vol. 6197. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2010, pp. 142–156.

[18] [SW Rel.] Andreas Enge, Philippe Théveny, and Paul Zimmermann, *GNU MPFR* version 1.3.1, Dec. 2022. LIC: LGPL-3.0-or-later. URL: `https://www.multiprecision.org/mpc/`, SWHID: ⟨`swh:1:dir:5236adaa0e5163b0621c0151919d879f4f86e1ff;origin=https://gitlab.inria.fr/mpc/mpc;visit=swh:1:snp:a9728932ea1e8286f2634cac6ba18a340a184977;anchor=swh:1:rev:9e125d9407a8230339cfbae0857d3ad61cd378ce`⟩.

[19] [SW Rel.] Andreas Enge and Emmanuel Thomé, *CMH* version 1.1.1, July 2022. LIC: GPL-3.0-or-later. URL: `https://www.multiprecision.org/cmh/`, SWHID: ⟨`swh:1:dir:fc590714b96e7f146e322c7719f4d0fb35b6c259;origin=https://gitlab.inria.fr/cmh/cmh;visit=swh:1:snp:b83dbb3aeafa040422a0428a5d967fbe5d0d7861;anchor=swh:1:rev:6043add6b10ea9b894963972b27249546a8638db`⟩.

[20] Andreas Enge and Emmanuel Thomé. “Computing class polynomials for abelian surfaces”. In: *Experimental Mathematics* 23.2 (2014), pp. 129–145.

[21] Jens Franke et al. “Proving the Primality of Very Large Numbers with fastECPP”. In: *Algorithmic Number Theory — ANTS-VI*. Ed. by Duncan Buell. Vol. 3076. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2004, pp. 194–207.

[22] Paul B. Garrett. *Holomorphic Hilbert modular forms*. The Wadsworth & Brooks/Cole Mathematics Series. Pacific Grove, CA: Wadsworth & Brooks/Cole Advanced Books & Software, 1990, pp. xvi+304. ISBN: 0-534-10344-8.

[23] Alice Gee. “Class Invariants by Shimura’s Reciprocity Law”. In: *Journal de Théorie des Nombres de Bordeaux* 11.1 (1999), pp. 45–72.

[24] Alice Gee and Peter Stevenhagen. “Generating Class Fields Using Shimura Reciprocity”. In: *Algorithmic Number Theory — ANTS-III*. Ed. by J. P. Buhler. Vol. 1423. Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1998, pp. 441–453.

[25] [SW Rel.] GNU Guix contributors, *GNU Guix* version commit bf17a01, Feb. 2024. LIC: GPL-3.0-or-later. URL: `https://guix.gnu.org/`, SWHID: ⟨`swh:1:rev:bf17a01e06abc100651ed643f2d5c7fea07d37ba;origin=https://git.savannah.gnu.org/git/guix.git;visit=swh:1:snp:2eafcb87f5ed2c6be3c4784658f8ed9147137241`⟩.

[26] Eyal Z. Goren. “On certain reduction problems concerning abelian surfaces”. In: *Manuscripta Math.* 94.1 (1997), pp. 33–43. ISSN: 0025-2611,1432-1785. DOI: `10.1007/BF02677837`. URL: `https://doi.org/10.1007/BF02677837`.

[27] [SW Rel.] Torbjörn Granlund et al., *GNU MP* version 6.2.1, Nov. 2020. LIC: LGPL-3.0-or-later. URL: `https://gmplib.org/`, SWHID: ⟨`swh:1:dir:31da2a73b2e10e765fb52996d15e6f5f453453a3;origin=https://gmplib.org/repo/gmp-6.2/;visit=swh:1:snp:f40ef7cd40cb4ccec48e3d4291d44ca8def8f592;anchor=swh:1:rel:acd9a44abc3f7a2a39ab039d3d4ac81eb57e5943`⟩.

[28] [SW Rel.] Guillaume Hanrot et al., *GNU MPFR* version 4.2.0, Jan. 2023. LIC: LGPL-3.0-or-later. URL: `https://www.mpfr.org/`, SWHID: ⟨`swh:1:dir:dd9133d55874f4fc39788797b217e6503f9e23ea;origin=https://gitlab.inria.fr/mpfr/mpfr;visit=swh:1:snp:7832a1dd4a2a06a21cf366267497bd5d64088ece;anchor=swh:1:rel:b5e308c5dd459a81d8523e1dcb84c19dbc47b51b`⟩.

[29] Tomoyoshi Ibukiyama. “On Siegel modular varieties of level 3”. In: *International Journal of Mathematics* 2.1 (1991), pp. 17–35.

[30] Jun-Ichi Igusa. “Arithmetic Variety of Moduli for Genus Two”. In: *Annals of Mathematics*. 2nd ser. 72.3 (1960), pp. 612–649.

[31] Jun-Ichi Igusa. “On Siegel Modular Forms of Genus Two”. In: *American Journal of Mathematics* 84.1 (1962), pp. 175–200.

[32] Pınar Kılıçer. “The CM class number one problem for curves”. `https://openaccess.leidenuniv.nl/handle/1887/41145`. PhD thesis. Université de Bordeaux and Universiteit Leiden, 2016.

[33] Serge Lang. *Complex Multiplication*. Vol. 255. Grundlehren der mathematischen Wissenschaften. Springer, 1983. ISBN: 978-0-387-90786-4.

[34] Kristin Lauter and Bianca Viray. “An arithmetic intersection formula for denominators of Igusa class polynomials”. In: *Amer. J. Math.* 137.2 (2015), pp. 497–533. ISSN: 0002-9327. DOI: `10.1353/ajm.2015.0010`. URL: `http://dx.doi.org/10.1353/ajm.2015.0010`.

[35] Kristin Lauter and Tonghai Yang. "Computing genus 2 curves from invariants on the Hilbert moduli space". In: *J. Number Theory* 131.5 (2011), pp. 936–958. ISSN: 0022-314X,1096-1658. DOI: 10.1016/j.jnt.2010.05.012. URL: https://doi.org/10.1016/j.jnt.2010.05.012.

[36] François Morain. "Implementing the asymptotically fast version of the elliptic curve primality proving algorithm". In: *Mathematics of Computation* 76.257 (2007), pp. 493–505.

[37] Jürgen Neukirch. *Algebraic Number Theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften. Berlin: Springer-Verlag, 1999.

[38] [SW Rel.] SageMath Community, *SageMath* version 10.2, Dec. 2023. LIC: GPL-3.0. URL: https://www.sagemath.org/, SWHID: ⟨swh:1:rel:9ae9c96b6ee5b53fa189662f5c2d6c426d221642;origin=https://github.com/sagemath/sage;visit=swh:1:snp:a53110fbb26bc97b816592acccf5fbb48751f9e9⟩.

[39] Reinhard Schertz. "Weber's Class Invariants Revisited". In: *Journal de Théorie des Nombres de Bordeaux* 14.1 (2002), pp. 325–343.

[40] Ehud de Shalit and Eyal Z. Goren. "On special values of theta functions of genus two". In: *Ann. Inst. Fourier (Grenoble)* 47.3 (1997), pp. 775–799. ISSN: 0373-0956. URL: http://www.numdam.org/item?id=AIF_1997__47_3_775_0.

[41] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*. Vol. 6. Publications of the Mathematical Society of Japan. The Mathematical Society of Japan, Tokyo, 1961, pp. xi+159.

[42] Anna Somoza. "Inverse Jacobian and related topics for certain superelliptic curves". https://scholarlypublications.universiteitleiden.nl/handle/1887/70564. PhD thesis. UPC Barcelona and Universiteit Leiden, 2019.

[43] Anne-Monika Spallek. "Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen". http://www.iem.uni-due.de/zahlentheorie/AES-KG2.pdf. Dissertation. Universität Gesamthochschule Essen, 1994.

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

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

[46] Marco Streng. “Complex multiplication of abelian surfaces”. PhD thesis. Universiteit Leiden, 2010.

[47] Marco Streng. “Computing Igusa class polynomials”. In: *Math. Comp.* 83.285 (2014). arXiv:0903.4766, pp. 275–309. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-2013-02712-3.

[48] [SW Rel.] Marco Streng, *RECIP – REpository of Complex multIPlication sage code* version 3.4.1, May 2024. URL: http://pub.math.leidenuniv.nl/~strengtc/recip/, SWHID: ⟨swh:1:dir:abb6d8c3dac5908cbea4a182ebba797e28e10410;origin=https://bitbucket.org/mstreng/recip;visit=swh:1:snp:94671b864585b53be47182ff7843a3e80eeff3e0;anchor=swh:1:rev:87b3dca8bf18e922147fe13aacdca1dc00ac5b12⟩.

[49] Andrew V. Sutherland. “Accelerating the CM method”. In: *LMS J. Comput. Math.* 15 (2012), pp. 172–204. DOI: 10.1112/S1461157012001015. URL: https://doi-org.ezproxy.leidenuniv.nl/10.1112/S1461157012001015.

[50] Paul van Wamelen. “Examples of genus two CM curves defined over the rationals”. In: *Math. Comp.* 68.225 (1999), pp. 307–320. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-99-01020-0. URL: http://dx.doi.org/10.1090/S0025-5718-99-01020-0.