An explicit version of Shimura's reciprocity law for Siegel modular functions

Marco Streng*

29th December 2011

Abstract

We give an explicit version of Shimura's reciprocity law for singular values of Siegel modular functions. We use this to construct examples of class invariants of quartic CM fields that are smaller than Igusa invariants.

1 Introduction

The values $f(\tau)$ of classical modular functions at CM points generate abelian extensions of $K = \mathbf{Q}(\tau)$, hence are acted on by ideals and idèles of K via the Artin isomorphism. Shimura's reciprocity law expresses these actions in terms of a GL_2-action on the modular functions f themselves.

An explicit version of this action allows one to search for *class invariants* of imaginary quadratic fields in a more systematic way [5], i.e., for modular function values $f(\tau)$ that generate the ring class field $K(j(\tau))$ over K. 'Small' class invariants can then replace $j(\tau)$ in applications such as the construction of (cryptographic) elliptic curves over finite fields, and finding defining equations of class fields.

Complex multiplication of higher-dimensional abelian varieties also generates class fields [19] and enables the construction of cryptographic curves [3,20]. A big speedup would be obtained if one would replace for example Igusa invariants in [20] by smaller class invariants.

Shimura gave various higher-dimensional analogues of his reciprocity law [12–17], and our main result (Theorems 2.2–2.4 below) is a sufficiently explicit version for finding class invariants of orders in *CM-fields*, i.e., orders in $K = \mathbf{Q}(\sqrt{d})$ with d a totally negative algebraic number. It takes the following form.

Fix a CM point $\tau \in \mathcal{H}_g$ in the Siegel upper half space, and let N be a positive integer. Assume that the CM-type Φ of τ is primitive, and let Φ^{r} be its reflex. Let $\mathcal{F}_N$ be the field of Siegel modular functions of level N with q-expansion coefficients in $\mathbf{Q}(\zeta_N)$. Assume for the sake of this introduction that τ has CM by a maximal order $\mathcal{O}_K \subset K$. Then given an ideal $\mathfrak{a}$ of K^{r} coprime to N, Theorem 2.4 (our main result) gives explicit $U \in \mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ and $M \in \mathrm{GSp}_{2g}(\mathbf{Q})^+$ with

$$f(\tau)^{\mathfrak{a}} = f^U(M\tau). \tag{1.1}$$

*Supported by EPSRC grant number EP/G004870/1. The author would like to thank Gaetan Bisson and Jean-Pierre Flori for many useful comments for the improvement of the exposition.

Here $\mathfrak{a}$ acts on $f(\tau)$ via the Artin map, and the actions of U and M on $\mathcal{F}_N$ and $\mathcal{H}_g$ are given in Section 2.

We use the reciprocity law to determine the ideal group corresponding to the field

$$\mathcal{H}(N) = K^{\mathrm{r}}(f(\tau) : f \in \mathcal{F}_N).$$

In the case of maximal orders, it is be

$$H(N) = \left\{\mathfrak{a} : N_{\Phi^{\mathrm{r}}}(\mathfrak{a}) = \mu\mathcal{O}_K, \mu\overline{\mu} \in \mathbf{Q}, \mu \equiv 1 \bmod^{\times} N\right\}.$$

Theorem 2.2 gives the general case, where the CM order of τ is not necessarily maximal.

If one considers only the Galois group $\mathrm{Gal}(\mathcal{H}(N)/\mathcal{H}(1))$, then U and M of (1.1) become particularly simple to express. Given $\mathfrak{a}$, let μ be as in the definition of $H(1)$, and let U be the transpose of the matrix of multiplication by μ with respect to the symplectic basis corresponding to τ. Theorem 2.3 then states

$$f(\tau)^{\mathfrak{a}} = f^{U}(\tau). \tag{1.2}$$

We have programmed the actions (1.1) and (1.2) into Sage [11] and will make the program available online at [21]. Via Sage, these programs use PARI [25] for most of the number field functionality, such as computation of ray class groups.

The action (1.2) allows us to show that $f(\tau)$ is in $\mathcal{H}(1)$ by considering only the action of some matrices U on $\mathcal{F}_N$. If $f(\tau)$ is in $\mathcal{H}(1)$, then the main theorems (more precisely, Theorems 2.2 and 2.4) allow us to verify $K^{\mathrm{r}}(f(\tau)) = \mathcal{H}(1)$, i.e., that $f(\tau)$ is a *class invariant*, and to compute the minimal polynomial H_f of $f(\tau)$ over K^{r} numerically.

The polynomial H_f becomes simpler to express and compute if its coefficients are in the maximal totally real subfield $K_0^{\mathrm{r}} \subset K^{\mathrm{r}}$. Proposition 2.7 gives a sufficient condition for this to happen. We give a detailed example in Section 6.

Rather than reproving the reciprocity law in our setting, we will quote a version proven by Shimura in the language of idèles (Section 3) and rework it into a version with ideals and a more explicit group action (Section 4).

The action of U becomes most explicit when expressing f in terms of theta constants. This is Section 5 and will be used for our examples in Section 6. Finally, Section 7 treats the applications mentioned in the introduction in more detail. These final three sections can be read independently of Section 4.

2 Definitions and statement of the main results

2.1 The upper half space

Fix a positive integer g. The *Siegel upper half space* $\mathcal{H} = \mathcal{H}_g$ is the set of $g \times g$ symmetric complex matrices with positive definite imaginary part. It parametrizes g-dimensional principally polarized abelian varieties A over $\mathbf{C}$ together with a *symplectic* basis $b_1, \ldots, b_{2g}$ of their first homology.

In more detail, an abelian variety over $\mathbf{C}$ is always of the form $A = \mathbf{C}^g/\Lambda$ for a lattice Λ of rank $2g$. A polarization is given by a Riemann form, i.e., an $\mathbf{R}$-bilinear form E on $\mathbf{C}^g$ that restricts to a bilinear form $\Lambda \times \Lambda \to \mathbf{Z}$ and such that $(u, v) \mapsto E(iu, v)$ is symmetric and positive definite. Given a basis of Λ, there is a matrix, which by abuse of notation we also denote by E, such

that $E(u,v) = u^{\mathrm{t}} E v$. We say that E is *principally polarized* if E has determinant 1. In that case, there exists a *symplectic basis*, i.e., a basis such that E is given in terms of (2×2)-blocks as

$$\Omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

To a point $\tau \in \mathcal{H}_g$, we associate the principally polarized abelian variety with $\Lambda = \tau \mathbf{Z}^g + \mathbf{Z}^g$ and symplectic basis $\tau e_1, \ldots, \tau e_g, e_1, \ldots, e_g$, where e_i is the i-th basis element of $\mathbf{Z}^g$. Conversely, given a principally polarized abelian variety and a symplectic basis, we can apply a $\mathbf{C}$-linear transformation of $\mathbf{C}^g$ to write it in this form.

2.2 The algebraic groups

Given a commutative ring R, let

$$\mathrm{GSp}_{2g}(R) = \{A \in \mathrm{Mat}_{2g}(R) : A^{\mathrm{t}} \Omega A = \nu \Omega \text{ with } \nu \in R^\times\}.$$

Note that ν defines a homomorphism of algebraic groups $\mathrm{GSp}_{2g} \to \mathbf{G}_{\mathrm{m}}$, and denote its kernel by Sp_{2g}. for $g = 1$, we have simply $\mathrm{GSp}_{2g}(R) = \mathrm{GL}_2(R)$, $\nu = \det$, $\mathrm{Sp}_{2g}(R) = \mathrm{SL}_2(R)$.

The homomorphism ν has a section $\iota^{-1} : t \mapsto \iota(t)^{-1}$, where

$$\iota(t) = \begin{pmatrix} 1 & 0 \\ 0 & t^{-1} \end{pmatrix}.$$

For any ring R for which this makes sense, we also define

$$\mathrm{GSp}_{2g}(R)^+ = \{A \in \mathrm{GSp}_{2g}(R) : \nu(A) > 0\}.$$

The group $\mathrm{GSp}_{2g}(\mathbf{Q})^+$ acts on $\mathcal{H}_g$ by

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

where a, b, c, d are $(g \times g)$-blocks. Changes of symplectic bases correspond to the action of $\mathrm{Sp}_{2g}(\mathbf{Z}) \subset \mathrm{GSp}_{2g}(\mathbf{Q})^+$ (see Lemma 4.6 below). It follows that $\mathrm{Sp}_{2g}(\mathbf{Z}) \backslash \mathcal{H}$ parametrizes the isomorphism classes of principally polarized abelian varieties of dimension g.

It is known that the natural map $\mathrm{Sp}_{2g}(\mathbf{Z}) \to \mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ is surjective [10, Thm. VII.21], and we denote its kernel by Γ_N.

2.3 Modular forms and group actions

A *Siegel modular form* of weight k and level N is a function $f : \mathcal{H} \to \mathbf{C}$ such that for all $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_N$, we have $f(A\tau) = \det(c\tau + d)^k f(\tau)$, and which is "holomorphic at the cusps". We will not define holomorphicity at the cusps, as it is automatically satisfied for $g > 1$ by the Koecher principle [6], and is a standard (textbook) condition for $g = 1$.

Any modular form f has a *Fourier expansion* or *q-expansion*

$$f(\tau) = \sum_{\xi} a_\xi q^\xi, \quad a_\xi \in \mathbf{C}, \quad q^\xi := \exp(2\pi i \mathrm{Tr}(\xi\tau)/N),$$

where ξ runs over the symmetric matrices in $\mathrm{Mat}_g(\frac{1}{2}\mathbf{Z})$ with integral diagonal entries. The numbers a_ξ are the *coefficients* of the q-expansion.

Let $\mathcal{F}_N$ and $\mathcal{F}_\infty$ be the fields

$$\mathcal{F}_N = \left\{ \frac{g_1}{g_2} : \begin{array}{l} g_i \text{ are Siegel modular forms of equal weight and level N,} \\ \text{with } q\text{-expansion coefficients in } \mathbf{Q}(\zeta_N), \text{ and } g_2 \neq 0 \end{array} \right\}$$

and $\mathcal{F}_\infty = \cup_N \mathcal{F}_N$.

Proposition 2.1. There are well-defined right group actions given by

$\mathcal{F}_\infty \circlearrowleft \mathrm{GSp}_{2g}(\mathbf{Q})^+$	$f^A(\tau) = f(A\tau)$,
$\mathcal{F}_N \circlearrowleft \mathrm{Sp}_{2g}(\mathbf{Z})$	$f^A(\tau) = f(A\tau)$,
$\mathcal{F}_N \circlearrowleft \mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$	$f^{(A \bmod N)} = f^A$ if $A \in \mathrm{Sp}_{2g}(\mathbf{Z})$,
$\mathcal{F}_N \circlearrowleft \iota((\mathbf{Z}/N\mathbf{Z})^\times)$	the inverse of the natural Galois action of $(\mathbf{Z}/N\mathbf{Z})^\times$ on the Fourier coefficients, i.e., if $f = \sum_\xi a_\xi q^\xi$, then $f^{\iota(t)} = \sum_\xi a_\xi^{t^{-1}} q^\xi$,
$\mathcal{F}_N \circlearrowleft \mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$	extending the actions of both $\iota((\mathbf{Z}/N\mathbf{Z})^\times)$ and $\mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ simultaneously.

We will give a proof in Section 3.

Given $A \in \mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ and $f \in \mathcal{F}_N$, how would one compute f^A? First, take $t = \nu(A)$, and notice $A = \iota(t)^{-1}B$ with $B = \iota(t)A \in \mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$. Next, lift B to $B_0 \in \mathrm{Sp}_{2g}(\mathbf{Z})$, and note $f^A = (f^{\iota(t^{-1})})^{B_0}$. The only part that is not completely explicit is the lifting from $\mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ to $\mathrm{Sp}_{2g}(\mathbf{Z})$. However, when $f \in \mathcal{F}_N$ is expressed in terms of *theta constants*, we will give a formula for the action of $\mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ on f (Section 5) that does not require finding a lift.

2.4 Complex multiplication

Suppose A is a g-dimensional polarized abelian variety over $\mathbf{C}$ with *complex multiplication*, i.e., such that $\mathrm{End}(A) \otimes \mathbf{Q}$ contains a CM-field K of degree $2g$.

It is known that any such A can be obtained as follows. Let $\Phi = \{\phi_1, \ldots, \phi_g\}$ be a *CM-type*, i.e., a set of g embeddings $K \to \mathbf{C}$ such that no two are complex conjugate. By abuse of notation, write $\Phi(x) = (\phi_1(x), \ldots, \phi_g(x)) \in \mathbf{C}^g$ for $x \in K$. Let $\mathfrak{b}$ be a lattice in K, i.e., a non-zero fractional ideal of an order of K. Let $\xi \in K$ be such that for all $\phi \in \Phi$, the complex number $\phi(\xi)$ lies on the positive imaginary axis, and such that the bilinear form $E_\xi : K \times K \to \mathbf{Q} : (x, y) \mapsto \mathrm{Tr}(\overline{x}y\xi)$ maps $\mathfrak{b} \times \mathfrak{b}$ to $\mathbf{Z}$. Let $A = \mathbf{C}^g/\Phi(\mathfrak{b})$ and let a polarization on A be given by E_ξ extended $\mathbf{R}$-linearly from $\mathfrak{b}$ to $\mathbf{C}^g$. Finally, let $\mathcal{O} = \{x \in K : x\mathfrak{b} \subset \mathfrak{b}\}$ be the multiplier ring of $\mathfrak{b}$, and embed it into $\mathrm{End}(A)$ by taking $x\Phi(u) = \Phi(xu)$ and extending this linearly.

Any CM-point τ thus corresponds to a quadruple $(\Phi, \mathfrak{b}, \xi, B)$ with Φ, $\mathfrak{b}$ and ξ as above and $B = (b_1, \ldots, b_{2g})$ a symplectic basis of $\mathfrak{b}$ for the pairing E_ξ. We will make the reciprocity law explicit in terms of such quadruples, and note that one obtains τ with the formula

$$\tau = (\Phi(b_{g+1})| \cdots |\Phi(b_{2g}))^{-1}(\Phi(b_1)| \cdots |\Phi(b_g)).$$

We will assume that Φ is a *primitive* CM-type, or, equivalently, $K = \mathrm{End}(A) \otimes \mathbf{Q}$ ([7, Thms. 1.3.3 and 1.3.5]). We then have $\mathcal{O} = \mathrm{End}(A)$.

2.5 The type norm

The type norm $N_\Phi : K \to \mathbf{C}$ is the map

$$N_\Phi : x \mapsto \prod_{\phi\in\Phi} \phi(x).$$

Its image generates the *reflex field* K^{r} of Φ, and there is a reflex type norm map

$$N_{\Phi^{\mathrm{r}}} : K^{\mathrm{r}} \to K : x \mapsto \prod_{\psi\in\Psi} \psi(x),$$

where the product is taken over the reflex type, i.e., those embeddings $\psi : K^{\mathrm{r}} \to \overline{K}$ such that there is a map $\phi : \overline{K} \to \mathbf{C}$ with $\phi\circ\psi = \mathrm{id}_{K^{\mathrm{r}}}$ and $\phi_{|K} \in \Phi$.

Recall that $\mathcal{O}$ is an order in K and let F be the smallest positive integer such that $F\mathcal{O}_K \subset \mathcal{O}$. For any positive integer N, let $I(NF)$ be the group of fractional ideals of $\mathcal{O}_{K^{\mathrm{r}}}$ coprime to NF. Let $N_{\Phi^{\mathrm{r}},\mathcal{O}}$ be the *type norm* homomorphism from $I(NF)$ to the group of invertible fractional $\mathcal{O}$-ideals coprime to NF defined by

$$N_{\Phi^{\mathrm{r}},\mathcal{O}}(\mathfrak{a})\mathcal{O}_L = \prod_{\psi\in\Psi} \psi(\mathfrak{a})\mathcal{O}_L,$$

where L is the normal closure of K. The existence and uniqueness of this map for $\mathcal{O} = \mathcal{O}_K$ is [19, Proposition 29 in § 8.3], and the general case then follows from the fact that the set of invertible fractional $\mathcal{O}$-ideals coprime to NF is naturally in bijection with the same set for $\mathcal{O}_K$.

2.6 The class fields generated by complex multiplication

Fix a CM-point τ and let the notation be as above. We will study the field $\mathcal{H}(N)$ generated over K^{r} by the values of $f(\tau)$ as f ranges over the elements of $\mathcal{F}_N$ that do not have a pole at τ. It is an abelian extension of K^{r}, and our first theorem gives the corresponding ideal group. To state it, we need some additional definitions.

For $x \in K$, we write $x \equiv 1 \bmod^\times N\mathcal{O}$ if we have $(x-1)/N \in \mathcal{O}\otimes\mathbf{Z}_p$ for all primes p dividing N. In other words, we have $x \equiv 1 \bmod^\times N\mathcal{O}$ if and only if there exist $a, b \in \mathcal{O}$ with $x = (1+Na)/(1+Nb)$. Note that $x \equiv 1 \bmod^\times 1\mathcal{O}$ holds for all elements of K.

The following theorem is analogous to [19, Main Theorem 3 in §17]. We will prove it using the reciprocity law. Recall that F is the smallest positive integer satisfying $F\mathcal{O}_K \subset \mathcal{O}$.

Theorem 2.2. *The extension $\mathcal{H}(N)/K^{\mathrm{r}}$ is abelian and of conductor dividing NF. Its Galois group is isomorphic via the Artin isomorphism to the group $I(NF)/H_{\Phi,\mathcal{O}}(N)$, where $I(NF)$ is the group of fractional $\mathcal{O}_{K^{\mathrm{r}}}$-ideals coprime to NF, and*

$$H_{\Phi,\mathcal{O}}(N) = \left\{ \mathfrak{a} \in I(NF) : \exists \mu \in K \text{ with } \begin{array}{c} N_{\Phi^{\mathrm{r}},\mathcal{O}}(\mathfrak{a}) = \mu\mathcal{O} \\ \mu\overline{\mu} = N(\mathfrak{a}) \in \mathbf{Q} \\ \mu \equiv 1 \bmod^\times N\mathcal{O} \end{array} \right\}.$$

Note that $\mathcal{H}(N)$ depends only on $\mathcal{O}$ and Φ.

2.7 The explicit reciprocity laws

The previous section stated $\mathrm{Gal}(\mathcal{H}_N/\mathcal{H}_1) = (I(NF) \cap H_{\Phi,\mathcal{O}}(1))/H_{\Phi,\mathcal{O}}(N)$ for certain ideal groups $H_{\Phi,\mathcal{O}}(1)$ and $H_{\Phi,\mathcal{O}}(N)$. The following reciprocity law makes the Galois action of $I(NF) \cap H_{\Phi,\mathcal{O}}(1)$ explicit.

Theorem 2.3. *Given a CM point $\tau \in \mathcal{H}$ and a positive integer N, let the notation be as above. For any $\mathfrak{a} \in I(NF) \cap H_{\Phi,\mathcal{O}}(1)$, let $[\mathfrak{a}]$ be its class modulo $H_{\Phi,\mathcal{O}}(N)$, and let μ be as in the definition of $H_{\Phi,\mathcal{O}}(1)$. Then the action of $[\mathfrak{a}]$ on $f(\tau)$ for any $f \in \mathcal{F}_N$ is given by*

$$f(\tau)^{[\mathfrak{a}]} = f^{\epsilon(\mu)}(\tau),$$

where $\epsilon(\mu)$ is the transpose of the matrix of multiplication by μ with respect to the basis $b_1, \ldots, b_{2g}$ of Section 2.4.

This defines a reciprocity map g as follows. Let S be the image in the group $\mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ of the stabilizer $\mathrm{Stab}_\tau \subset \mathrm{Sp}_{2g}(\mathbf{Z})$ of τ. Then we get a homomorphism

$$\begin{aligned} g : \frac{I(N) \cap H_{\Phi,\mathcal{O}}(1)}{H_{\Phi,\mathcal{O}}(N)} &\longrightarrow \mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})/S \\ [\mathfrak{a}] &\longmapsto \epsilon(\mu) \end{aligned}$$

such that

$$f(\tau)^{\mathfrak{a}} = f^{g(\mathfrak{a})}(\tau) \quad \text{and} \quad g((\alpha)) = \epsilon(N_{\Phi^{\mathrm{r}}}(\alpha)) \quad \text{for} \quad \alpha \in K^{\mathrm{r}}.$$

The following more general version of the reciprocity law gives the action of any $\mathfrak{a} \in I(NF)$.

Theorem 2.4. *Given a CM point $\tau \in \mathcal{H}$ and a positive integer N, let the notation be as above. For any $\mathfrak{a} \in I(NF)$, choose a symplectic basis C of $N_{\Phi^{\mathrm{r}},\mathcal{O}}(\mathfrak{a})^{-1}\mathfrak{b}$ with respect to $E_{N(\mathfrak{a})\xi}$.*

Let M^{t} be the basis transformation from B to C. In other words, if B and C are matrices with the elements of B and C as columns, written in terms of some $\mathbf{Q}$-basis of K, then $C = BM^{\mathrm{t}}$.

Then M is in $\mathrm{GSp}_{2g}(\mathbf{Q})^+$ and is N-integral and invertible mod N. Moreover, its inverse U is in $\mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$, and for any $f \in \mathcal{F}_N$, we have

$$f(\tau)^{[\mathfrak{a}]} = f^{UM}(\tau) = f^U(M\tau). \tag{2.1}$$

Remark 2.5. Computing symplectic bases is easy. Use the `symplectic_form` command on integer matrices in Sage [11] or `FrobeniusFormAlternating` in Magma [2], or see [22, Algorithm 4.2].

2.8 Complex conjugation

Now assume $f(\tau)$ is a class invariant, i.e., a generator of $\mathcal{H}(1)/K^{\mathrm{r}}$ with $f \in \mathcal{F}_N$. A priori, the coefficients of its minimal polynomial H_f over K^{r} are elements of K^{r}. But in many cases there is a way to make sure they are elements of the smaller field K_0^{r}.

Let $\mathcal{M} := \mathbf{Q}(f(\tau) : f \in \mathcal{F}_1)$ be the *field of moduli* of the principally polarized abelian variety corresponding to τ, and let $\mathcal{M}_0 = \mathcal{M}K_0^{\mathrm{r}}$. Then by definition, we have $\mathcal{H}(1) = \mathcal{M}_0 K^{\mathrm{r}}$, and $\mathcal{H}(1)/\mathcal{M}_0$ is an extension of degree at most 2.

We will concern ourselves with the case where this degree is exactly 2.

Lemma 2.6. Suppose τ corresponds to a pair $(\mathfrak{b}, \xi)$.

1. The degree of $\mathcal{H}(1)/\mathcal{M}_0$ is 2 if and only if there is an ideal $\mathfrak{a} \in I(F)$ and an element $\mu \in K^\times$ such that $N_{\Phi^{\mathrm{r}},\mathcal{O}}(\mathfrak{a})\overline{\mathfrak{b}} = \mu\mathfrak{b}$ and $\mu\overline{\mu} \in \mathbf{Q}$.
2. If $g \leq 2$ and $\mathcal{O} = \mathcal{O}_K$, then the conditions in part 1 are satisfied and we can take
   (a) $g = 1$, $\mathfrak{a} = N_\Phi(\mathfrak{b}/\overline{\mathfrak{b}})$ and $\mu = 1$; or
   (b) $g = 2$, $\mathfrak{a} = N_\Phi(\mathfrak{b})$ and $\mu = N_{K/\mathbf{Q}}(\mathfrak{b})$.
3. If $\mathfrak{b} = \mathcal{O}$, then the conditions in part 1 are satisfied and we can take $\mathfrak{a} = \mathcal{O}_{K^{\mathrm{r}}}$ and $\mu = 1$.

Proposition 2.7. Assume $\deg \mathcal{H}(1)/\mathcal{M}_0 = 2$ and suppose $f(\tau)$ is a class invariant with $f \in \mathcal{F}_N$.

Let $(\mathfrak{a}, \mu)$ be as in Lemma 2.6.1 and assume without loss of generality that $\mathfrak{a}$ is coprime to N. Let $M \in \mathrm{Mat}_{2g}(\mathbf{Q})$ be such that M^{t} transforms the symplectic basis $b_1, \ldots, b_g, b_{g+1}, \ldots, b_{2g}$ of $\mathfrak{b}$ corresponding to τ into the basis $\mu^{-1}\overline{b_1}, \ldots, \mu^{-1}\overline{b_g}, -\mu^{-1}\overline{b_{g+1}}, \ldots, -\mu^{-1}\overline{b_{2g}}$ of $\mu^{-1}\overline{\mathfrak{b}} = N_{\Phi^{\mathrm{r}},\mathcal{O}}(\mathfrak{a})^{-1}\mathfrak{b}$. Then M is finite and invertible modulo N. Let $U \in \mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ be its inverse and $U' = U\iota(-1)$. Then the following are equivalent:

1. $f(\tau) \in \mathcal{M}_0$
2. $f^{U'}(\tau) = f(\tau)$

If these conditions are satisfied, then the minimal polynomial of $f(\tau)$ over K^{r} has coefficients in K_0^{r}.

So to ensure that the minimal polynomial of $f(\tau)$ over K^{r} is defined over K_0^{r}, we can restrict to f that satisfy $f^{U'} = f$.

3 The adèlic version

Shimura developed his reciprocity laws for various types of multivariate modular functions, modular forms, and theta functions in a series of papers [12–17]. See also the textbook [18, 26.10]. We choose not to reprove the reciprocity law in the language of ideal groups, but instead to take a streamlined version proven by Shimura in the adèlic langage, and to work out exactly what it means in our situation in terms of ideal groups.

We start by citing Shimura's adèlic action of GSp_{2g}, and linking it to the actions of Proposition 2.1. In particular, this will prove Proposition 2.1, albeit in a rather indirect way.

Let $\mathbf{A}$ be the ring of adèles of $\mathbf{Q}$ and call an element of its unit group *positive* if its $\mathbf{R}$-component is positive. Let $\widehat{\mathbf{Z}} = \lim_{\leftarrow} \mathbf{Z}/N\mathbf{Z}$ be the ring of finite integral adéles, so $\mathbf{A} = (\widehat{\mathbf{Z}} \otimes \mathbf{Q}) \times \mathbf{R}$.

Proposition 3.1. Let $\mathrm{Aut}(\mathcal{F}_\infty)$ be the automorphism group of the field $\mathcal{F}_\infty$. There is a unique homomorphism $\mathrm{GSp}_{2g}(\mathbf{A})^+ \to \mathrm{Aut}(\mathcal{F}_\infty)$ satisfying

1. for $x \in \mathbf{A}^\times$ and $f \in \mathcal{F}_\infty$, we define $f^{\iota(x)}$ as f where x^{-1} acts on its Fourier coefficients,

2. for $A \in \mathrm{GSp}_{2g}(\mathbf{Q})^+$, $f \in \mathcal{F}_\infty$, $\tau \in \mathcal{H}$, we have $f^A(\tau) = f(A\tau)$,

3. for any N, the group $S = \{A \in \mathrm{GSp}_{2g}(\widehat{\mathbf{Z}}) : A \equiv 1 \bmod^\times N\} \cdot \mathrm{GSp}_{2g}(\mathbf{R})^+$ acts trivially on any $f \in \mathcal{F}_N$, where we write $A \equiv 1 \bmod^\times N$ if $A_p \equiv 1 \bmod N\mathrm{Mat}_{2g}(\mathbf{Z}_p)$ for all $p|N$.

Proof. Existence is a special case of [15, Thm. 5(v,vi,vii)]. Uniqueness follows from the proof of [17, Proposition 1.3]. □

Remark 3.2. Our reference for existence in Proposition 3.1, though directly applicable to our situation, may not be satisfactory to some readers, as it does not contain the proof. The action is constructed in [12, Section 2.7] for a field $k_S(V_S)$. The field $k_S(V_S)$ is defined without q-expansions, hence that reference only contains a weak version of 1, but 2 is [12, (2.7.2)] and 3 follows immediately from [12, $(2.5.3_\mathrm{a})$].

Our stronger version of 1, as well as the link between $\mathcal{F}_\infty$ and $k_S(V_S)$, is given in [15]. Both that reference and [14, § 6] claim that the proof is exactly the same as in the Hilbert modular case, which is [14].

Next, we make the action of $\mathrm{GSp}_{2g}(\widehat{\mathbf{Z}})$ on $\mathcal{F}_N$ explicit as a first step towards making the reciprocity law more explicit.

Proposition 3.3. The action of Proposition 3.1 has the following property:

4. For any positive integer N, any $f \in \mathcal{F}_N$, and any

$$A = (A_\mathrm{f}, A_\infty) \in \mathrm{GSp}_{2g}(\widehat{\mathbf{Z}}) \times \mathrm{GSp}_{2g}(\mathbf{R})^+ \subset \mathrm{GSp}_{2g}(\mathbf{A})^+,$$

   we have $f^A \in \mathcal{F}_N$, and f^A depends only on $(A_\mathrm{f} \bmod N) \in \mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$. Moreover, the induced action of $\mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ on $\mathcal{F}_N$ is exactly as in Proposition 2.1.

Proof. The fact $f^A \in \mathcal{F}_N$ follows from the construction of the action (see [12, 2.7 and (2.5.3)] and Remark 3.2 above). That f^A depends only on $(A_\mathrm{f} \bmod N)$ is Proposition 3.1.3. It follows that the action induces an action of $\mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ on $\mathcal{F}_N$. To prove that this action is as in Proposition 2.1, it remains only to compute this action for $B \in \mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ and for $B = \iota(t)$ with $t \in (\mathbf{Z}/N\mathbf{Z})^\times$.

In case of $B \in \mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$, we lift B to $A \in \mathrm{Sp}_{2g}(\mathbf{Z})$ (possible by [10]). As we have

$$\mathrm{Sp}_{2g}(\mathbf{Z}) = \mathrm{GSp}_{2g}(\mathbf{Q})^+ \cap (\mathrm{GSp}_{2g}(\widehat{\mathbf{Z}}) \times \mathrm{GSp}_{2g}(\mathbf{R})^+),$$

we can then apply Proposition 3.1.2 to find that the action of B is as in Proposition 2.1. In case of $B = \iota(t)$ with $t \in (\mathbf{Z}/N\mathbf{Z})^\times$, we lift t to $\widehat{\mathbf{Z}}^\times$ and apply Proposition 3.1.1. □

Proposition 2.1 now follows without having to do any work.

Proof of Proposition 2.1. Restricting the action of Proposition 3.1 to elements $A \in \mathrm{GSp}_{2g}(\mathbf{Q})^+$ gives the action of that group according to part 2 of Proposition 3.1. Restricting the action instead to $A_\mathrm{f} \in \mathrm{GSp}_{2g}(\widehat{\mathbf{Z}})$ and $f \in \mathcal{F}_N$ yields the actions of $\mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ and its subgroups by Proposition 3.3. □

Let $\tau \in \mathcal{H}$ correspond to a simple principally polarized abelian variety $\mathbf{C}^g/\tau\mathbf{Z}^g + \mathbf{Z}^g$ with *complex multiplication* by K. Let $\epsilon : K \to \mathrm{Mat}_{2g}(\mathbf{Q})$ be the ring homomorphism sending $x \in K$ to the matrix of multiplication by x with respect to the symplectic basis corresponding to τ.

The type norm $N_{\Phi^{\mathrm{r}}}$ and the map ϵ induce adèlic maps $N_{\Phi^{\mathrm{r}}} : K_{\mathbf{A}}^{\mathrm{r}\times} \to K_{\mathbf{A}}^{\times}$ and $\epsilon : K_{\mathbf{A}}^{\times} \to \mathrm{GSp}_{2g}(\mathbf{A})^+$.

Shimura gives the following reciprocity law, stated in a very sleek manner using the action of Proposition 3.1.

Theorem 3.4 (Shimura's reciprocity law for Siegel modular functions)**.** *Let $\tau \in \mathcal{H}_n$ and the notation be as above and let $g = \epsilon \circ N_\Psi$. Then for any $f \in \mathcal{F}_\infty$ such that $f(\tau)$ is finite and any $x \in K_{\mathbf{A}}^{\mathrm{r}\times}$, we have*

$$f(\tau) \in K_{\mathrm{ab}}^{\mathrm{r}} \quad \textit{and} \quad f(\tau)^x = f^{g(x)^{-1}}(\tau).$$

Proof. This is exactly equation (3.43) of [17, p. 57]. (Actually, that reference works with the abelian variety $A = \mathbf{C}^2/(\tau\mathbf{Z}^n + \delta\mathbf{Z}^n)$ for an integer $\delta \geq 3$, but that variety has CM by K if and only if ours has, so that the result for $\delta = 1$ follows.) The matrix $\epsilon(x) \in \mathrm{Mat}_{2g}(\mathbf{Q})$ is defined differently and less explicitly in [17], namely by $\rho(x)(\tau, 1) = (\tau, 1)\epsilon(x)$ where $\rho(x) \in \mathrm{Mat}_g(\mathbf{C})$ is the matrix of multiplication by x with respect to the standard basis of $\mathbf{C}^g$. But since $(\tau, 1)$ is exactly what maps the standard basis of $\mathbf{Z}^{2g}$ to $\mathbf{C}^g$, our matrix $\epsilon(x)$ satisfies the definition of [17]. □

Remark 3.5. As in Remark 3.2, a more original reference is [12, (2.7.3)] (equivalently [13, (6.2.3)]).

See also [18, 26.8(4)] for a textbook version.

4 Proof of the main result

Our main result is an explicit version of Shimura's reciprocity law. In other words, given $f \in \mathcal{F}_N$ and the image $[\mathfrak{a}]$ of the idèle x in a ray class group of K^{r}, we would like to give $f^{g(x)^{-1}}$ in terms of the actions of Proposition 2.1. First of all, we need to determine an appropriate modulus for our ray class group groups. This is done in Section 4.1.

Next, we will write $g(x) = SUM$ with $M \in \mathrm{GSp}_{2g}(\mathbf{Q})^+$, $U \in \mathrm{GSp}_{2g}(\widehat{\mathbf{Z}})$, $S \in \mathrm{Stab}_f$, and both M and $(U \bmod N)$ explicit in terms of $\mathfrak{a}$. Then we can conclude $f^{\mathfrak{a}}(\tau) = f^{g(x)^{-1}}(\tau) = f^{(U \bmod N)}(M\tau)$.

Remark 4.1. The strong approximation theorem for $\mathrm{GSp}_{2g}(\mathbf{A})$ in fact tells us ([17, Lemma 1.1]) that such a decomposition always exists, even with $U \in \iota(\widehat{\mathbf{Z}}^\times)$. However, we will be satisfied with having only $U \in \mathrm{GSp}_{2g}(\widehat{\mathbf{Z}})$.

4.1 The conductor

Let the notation be as above and recall $\mathrm{End}(A) = \mathcal{O}$, and $F\mathcal{O}_K \subset \mathcal{O}$.

Lemma 4.2. For $a \in K$, we have $a \in \mathcal{O}$ if and only if $\epsilon(a) \in \mathrm{Mat}_{2g}(\mathbf{Z})$.

Proof. We have $a \in \mathcal{O}$ if and only if $a\mathfrak{b} \subset \mathfrak{b}$, which is equivalent to $\epsilon(a) \in \mathrm{Mat}_{2g}(\mathbf{Z})$. □

Corollary 4.3. For $a \in K$, we have $a \equiv 1 \bmod^\times N\mathcal{O}$ if and only if $\epsilon(a) \equiv 1 \bmod^\times N$.

Proof. Lemma 4.2 stays valid when considered locally at a prime number p, i.e., replacing $\mathcal{O}$ by $\mathcal{O} \otimes \mathbf{Z}_p$ and $\mathbf{Z}$ by $\mathbf{Z}_p$ for a prime p. We have $a \equiv 1 \bmod^\times N\mathcal{O}$ if and only if $(a-1)/N \in \mathcal{O} \otimes \mathbf{Z}_p$ for all $p|N$. The corollary follows if we apply the lemma to $(a-1)/N$ locally at all primes dividing N. □

Recall the abelian extension $\mathcal{H}(N) = K^{\mathrm{r}}(f(\tau) : f \in \mathcal{F}_N)$ of K^{r}.

Proposition 4.4. The conductor of $\mathcal{H}(N)$ divides NF.

Proof. What we need to prove is equivalent to the statement that W_{NF} acts trivially on $\mathcal{F}_N$ for $W_{NF} = \{x \in K_{\mathbf{A}}^{\mathrm{r}\times} : x \equiv 1 \bmod^\times NF\}$. So take any $x \in W_{NF}$, and let $y = \epsilon(N_{\Phi^{\mathrm{r}}}(x))^{-1}$. Then Theorem 3.4 tells us that for all $f \in \mathcal{F}_N$, we have $f(\tau)^x = f^y(\tau)$.

We have $N_{\Phi^{\mathrm{r}}}(x) \equiv 1 \bmod^\times NF$, hence $N_{\Phi^{\mathrm{r}}}(x) \equiv 1 \bmod^\times N\mathcal{O}$. By Corollary 4.3, we find that y is in the set S of Proposition 3.1. It follows from that proposition that $f^y = f$, hence x acts trivially on $f(\tau)$ for all $f \in \mathcal{F}_N$. □

Before we compute the actual ideal group corresponding to the field $\mathcal{H}(N)$ (i.e., prove Theorem 2.2), we first determine the action of $I(NF)$ (i.e., prove Theorems 2.4 and 2.3).

4.2 The mundane properties of M

Theorem 2.4 starts by stating that the matrix M of that theorem is in the group $\mathrm{GSp}_{2g}(\mathbf{Q})^+$. The purpose of the current section is to prove this.

Recall that $M \in \mathrm{GL}_{2g}(\mathbf{Q})$ is defined by $C = BM^{\mathrm{t}}$ where the columns of B and C are symplectic bases of the lattices $\mathfrak{b}$ and $N_{\Phi^{\mathrm{r}},\mathcal{O}}(\mathfrak{a})^{-1}\mathfrak{b}$ with respect to polarizations E_ξ and $E_{N(\mathfrak{a})\xi}$.

Lemma 4.5. Let M be as above. Then we have $M \in \mathrm{GSp}_{2g}(\mathbf{Q})^+$.

Proof. This follows by taking $y = N(\mathfrak{a})^{-1}$ in the following lemma. □

Lemma 4.6. Let $(\mathbf{C}^g/\Lambda, E)$ be a principally polarized abelian variety, and B a $(g \times 2g)$ complex matrix whose columns form a symplectic basis of Λ. Given $M \in \mathrm{GL}_{2g}(\mathbf{Q})$, let Λ' be the lattice in $\mathbf{C}^g$ generated by the columns of BM^{t}. Then the following are equivalent:

1. there exists $y \in \mathbf{Q}^\times$ such that yE is a principal polarization for $\mathbf{C}^g/\Lambda'$ and the columns of BM^{t} form a symplectic basis,
2. $M \in \mathrm{GSp}_{2g}(\mathbf{Q})^+$.

Moreover, if this is the case, then the point in $\mathcal{H}$ corresponding to C is $\tau' = M\tau$, and we have $y = \nu(M)^{-1}$.

Proof. Interpret B as a $(2g \times 2g)$ real matrix by identifying $\mathbf{C}$ with $\mathbf{R} + i\mathbf{R}$. Let F be the matrix of E with respect to the standard basis of $\mathbf{R}^{2g}$. Then we have $B^{\mathrm{t}}FB = \Omega$.

Note that yE satisfies all properties in the definition of a principal polarization, except possibly that $yE : (u, v) \mapsto yE(iu, v)$ is positive definite, and that

E maps $\Lambda' \times \Lambda'$ to $\mathbf{Z}$ with determinant 1. The first property is equivalent to $y > 0$, while the second follows from symplecticity of C. In particular, part 1 is equivalent to the existence of $y > 0$ in $\mathbf{Q}$ with $y(BM)^{\mathrm{t}} F B M = \Omega$. In other words, part 1 is equivalent to the existence of $y > 0$ in $\mathbf{Q}$ with $M^{\mathrm{t}} \Omega M = y^{-1}\Omega$, i.e., to $M \in \mathrm{GSp}_{2g}(\mathbf{Q})^+$. This also shows $\nu(M) = y^{-1}$.

Finally, write $B = (B_1|B_2)$ and note $\tau = B_2^{-1}B_1$. We get $BM^{\mathrm{t}} = (B_1 a^{\mathrm{t}} + B_2 b^{\mathrm{t}} | B_1 c^{\mathrm{t}} + B_2 d^{\mathrm{t}})$, hence $\tau' = (B_1 c^{\mathrm{t}} + B_2 d^{\mathrm{t}})^{-1}(B_1 a^{\mathrm{t}} + B_2 b^{\mathrm{t}})$. Cancelling $B_2^{-1}B_2$ on the right hand side, we find $\tau' = (\tau c^{\mathrm{t}} + d^{\mathrm{t}})^{-1}(\tau a^{\mathrm{t}} + c^{\mathrm{t}})$. The fact that τ and τ' are symmetric matrices yields $\tau' = (a\tau + b)(c\tau + d)^{-1} = M^{\mathrm{t}}\tau$. □

4.3 Decomposing $g(x)$ modulo the stabilizer

The bridge between adèlic and ideal theoretic class field theory is the surjection

$$K_{\mathbf{A}}^{\mathrm{r}\times}/K^{\mathrm{r}\times} \to I(NF)/P(NF)$$

that maps the class of an idèle $x \equiv 1 \bmod^{\times} NF$ to the class of the ideal $\mathfrak{a}$ with $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = \mathrm{ord}_{\mathfrak{p}}(x_{\mathfrak{p}})$ modulo the ray $P(NF) = \{(\alpha) : \alpha \equiv 1 \bmod^{\times} NF\}$.

Let $\mathfrak{a}$ be a fractional $\mathcal{O}_{K^{\mathrm{r}}}$-ideal coprime to NF. Let the notation be as in Theorem 2.4, and pick any idèle $x = (x_v)_v \in K_{\mathbf{A}}^{\mathrm{r}\times}$ such that

1. for any finite prime $\mathfrak{p}$ of K^{r}, we have $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = \mathrm{ord}_{\mathfrak{p}}(x_{\mathfrak{p}})$, and
2. for any valuation v of K^{r} with $v(NF) > 0$, we have $x_v = 1$.

Then we immediately have

$$g(x) \equiv 1_{2g} \bmod^{\times} NF, \tag{4.1}$$

where $g = \epsilon \circ N_\Phi$ is as in Theorem 3.4.

At the same time, we also have the following.

Lemma 4.7. Let $g(x)$ be as above and M as in Theorem 2.4. Then the matrix $A = g(x)M^{-1}$ lies in $\mathrm{GSp}_{2g}(\widehat{\mathbf{Z}}) \times \mathrm{GSp}_{2g}(\mathbf{R})^+$.

Proof. Let's recall the situation of Theorem 2.4: we have a symplectic basis $B = (b_1|\dots|b_g)$ of $\mathfrak{b}$ with respect to E_ξ and a symplectic basis $C = (c_1|\dots|c_g) = BM^{\mathrm{t}}$ of $N_{\Phi^{\mathrm{r}},\mathcal{O}}(\mathfrak{a})^{-1}\mathfrak{b}$ with respect to $E_{N(\mathfrak{a})\xi}$.

Note $\nu \circ g = N_{K^{\mathrm{r}}/\mathbf{Q}}$, so the fact that K^{r} has no real embeddings implies $\nu(g(x))_\infty > 0$, i.e., $g(x)_\infty \in \mathrm{GSp}_{2g}(\mathbf{R})^+$. We also have $M \in \mathrm{GSp}_{2g}(\mathbf{Q})^+$ by Lemma 4.5, hence $A_\infty \in \mathrm{GSp}_{2g}(\mathbf{R})^+$. It now suffices to prove for every prime number p that A_p is in $\mathrm{GSp}_{2g}(\mathbf{Z}_p)$. for $x \in K_{\mathbf{A}}^{\mathrm{r}\times}$, write $x_p \in K^{\mathrm{r}} \otimes \mathbf{Z}_p$ for the part corresponding to primes over p.

We have the following identity of $\mathbf{Z}_p$-submodules of $K \otimes \mathbf{Z}_p$ of rank $2g$:

$$(N_{\Phi^{\mathrm{r}}}(\mathfrak{a})^{-1}\mathfrak{b}) \otimes \mathbf{Z}_p = N_{\Phi^{\mathrm{r}}}(x)_p^{-1}(\mathfrak{b} \otimes \mathbf{Z}_p),$$

and we have already chosen a basis $c_1, \dots, c_{2g}$ of the left hand side, and by definition of M, it consists of the columns of $(b_1|\cdots|b_{2g})M^{\mathrm{t}}$. We take the $\mathbf{Z}_p$-basis $N_{\Phi^{\mathrm{r}}}(x)_p^{-1}b_1, \dots, N_{\Phi^{\mathrm{r}}}(x)_p^{-1}b_{2g}$ of the right hand side and notice that A_p^{t} is the matrix that transforms one basis to the other. In particular, we have $A_p \in \mathrm{GL}_{2g}(\mathbf{Z}_p)$. As the basis on the left is symplectic for $N(\mathfrak{a})\xi$ and the one on the right is symplectic for $N(x)_p\xi$, we apply the proof of Lemma 4.6 and find $A_p \in \mathrm{GSp}_{2g}(\mathbf{Q}_p)$. As we already had $A_p \in \mathrm{GL}_{2g}(\mathbf{Z}_p)$, we conclude $A_p \in \mathrm{GSp}_{2g}(\mathbf{Z}_p)$. □

Proof of Theorem 2.4. We already know $M \in \mathrm{GSp}_{2g}(\mathbf{Q})^+$ by Lemma 4.5, which is the first statement in Theorem 2.4.

Next, we have $g(x) = AM$ with $A \in \mathrm{GSp}_{2g}(\widehat{\mathbf{Z}}) \times \mathrm{GSp}_{2g}(\mathbf{R})^+$ by Lemma 4.7. The reciprocity law (Thm. 3.4) now tells us $f(\tau)^x = f^{AM}(\tau)$. By Proposition 3.3, we find that A acts as $(A \bmod N)$ does on f. Moreover, we have $A \equiv M^{-1} \bmod^\times NF$ by (4.1), so the definition of U in Theorem 2.4 is equivalent to $U = (A \bmod N)$. Conclusion: $f(\tau)^x = f^U(M\tau)$. □

Proof of Theorem 2.3. Theorem 2.3 is a special case of Theorem 2.4 as follows. Pick $c_i = \mu^{-1} b_i$. Then $M\tau = \tau$ since multiplication by $\Phi(\mu)$ is a $\mathbf{C}$-linear isomorphism that transforms one symplectic basis into the other. At the same time, the matrix M is the transpose of the matrix of multiplication by μ^{-1}, hence U is the transpose of the matrix of multiplication by μ. □

4.4 Determining the ideal group

Next, we prove Theorem 2.2. A similar result exists in terms of fields of moduli of torsion points (Main Theorem 3 in §17 of [19]), but we give a proof directly in the language of our fields $\mathcal{F}_N$ using the reciprocity laws.

Proof of Theorem 2.2. Note that Theorem 2.3 already implies that $H_{\Phi,\mathcal{O}}(N)$ acts trivially on $\mathcal{H}(N)$, so that it remains to prove only the converse, and without loss of generality only for integral ideals $\mathfrak{a}$.

Let $\mathfrak{a} \in I(NF)$ be an integral ideal with $f(\tau)^{\mathfrak{a}} = f(\tau)$ for all $f \in \mathcal{F}_N$. Let U and M be as in Theorem 2.4, so that for all $f \in \mathcal{F}_N$, we get $f(\tau) = f(\tau)^{\mathfrak{a}} = f^U(M\tau)$ with $U \in \mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ and $M \in \mathrm{GSp}_{2g}(\mathbf{Q})^+$ such that $(M \bmod NF)$ is defined and invertible with inverse U. We claim that without loss of generality, we have $U = 1$, $M \equiv 1 \bmod^\times N$ and $M\tau = \tau$.

Proof of the claim: By taking $f = \zeta_N$, we find $\zeta_N^{\nu(U)} = \zeta_N$, hence $U \in \mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$. Then lift U to $\mathrm{Sp}_{2g}(\mathbf{Z})$, and use the lift to change the chosen basis $c_1, \ldots, c_g$ of Theorem 2.3. We find that without loss of generality, we have $U = 1$, which implies $M \equiv 1 \bmod^\times N$. We now have $f(\tau) = f(M\tau)$ for all $f \in \mathcal{F}_N$, and by [12, (2.5.1)], this implies $\tau \in \Gamma_N M\tau$, i.e., $\tau = \gamma M\tau$ for some $\gamma \in \Gamma_N$. We use γ to change the basis $c_1, \ldots, c_g$ again, and conclude also $M\tau = \tau$. This proves the claim.

Let $X = M^{-1}$, so $X \equiv 1 \bmod^\times N$ and $X\tau = \tau$. Let $\mathfrak{c} = N_{\Phi^{\mathrm{r}},\mathcal{O}}(\mathfrak{a})$. We have $\mathfrak{c} \subset \mathcal{O}$ and X sends a basis $c_1, \ldots, c_{2g}$ of $\mathfrak{c}^{-1}\mathfrak{b}$ to a basis $b_1, \ldots, b_{2g}$ of $\mathfrak{b} \subset \mathfrak{c}^{-1}\mathfrak{b}$, hence $X \in \mathrm{Mat}_{2g}(\mathbf{Z})$. The congruences on M now tell us $X \in \Gamma_N$.

The fact $X\tau = \tau$ shows that there is an isomorphism $h : \mathbf{C}^g/\Phi(\mathfrak{c}^{-1}\mathfrak{b}) \to \mathbf{C}^g/\Phi(\mathfrak{b}) = A$ preserving symplectic bases. The identity map on $\mathbf{C}^g$ induces an isogeny the other way around, which scales the polarization by $N(\mathfrak{a})$. Their composite is an $\mu \in \mathrm{End}(A) = \mathcal{O}$, which therefore satisfies $\mu^{-1}\mathfrak{b} = \mathfrak{c}^{-1}\mathfrak{b}$ and $\mu\overline{\mu} = N(\mathfrak{a}) \in \mathbf{Q}$. This last identity shows that ν is coprime to F, so if we look at the coprime-to-F part of $\mu^{-1}\mathfrak{b} = \mathfrak{c}^{-1}\mathfrak{b}$ and use that the coprime-to-F part of $\mathfrak{b}$ is invertible, then we find $\mu\mathcal{O} = \mathfrak{c}$.

By definition of μ, h, and X, the endomorphism μ acts as M^{t} on the chosen symplectic bases (i.e., $\epsilon(\mu) = M$). Corollary 4.3 therefore shows $\mu \equiv 1 \bmod^\times N\mathcal{O}$. □

4.5 Complex conjugation

Next, we prove the results in Section 2.8.

Proof of Lemma 2.6. Recall $\mathcal{M}_0 = K_0^{\mathrm{r}}(f(\tau) : f \in \mathcal{F}_1)$, and consider the extension $\mathcal{H}(1) = \mathcal{M}_0 K^{\mathrm{r}}/\mathcal{M}_0$. Part 1 is to prove that this extension has degree 2 if and only if there exist $\mathfrak{a} \in I(F)$ and $\mu \in K^\times$ such that $N_{\Phi^{\mathrm{r}},\mathcal{O}}(\mathfrak{a})\overline{\mathfrak{b}} = \mu\mathfrak{b}$ and $\mu\overline{\mu} \in \mathbf{Q}$.

Any non-trivial automorphism γ_0 of this extension restricts to complex conjugation on K^{r}, so $\gamma : x \mapsto \overline{x^{\gamma_0}}$ is an element of $\mathrm{Gal}(\mathcal{H}(1)/K^{\mathrm{r}})$. Note that γ and complex conjugation are equal on $\mathcal{M}_0$.

Next, suppose τ corresponds to $(\mathfrak{b}, \xi)$, and let A be the corresponding principally polarized abelian variety. Then by [7, Prop. 3.5.5], the abelian variety $\overline{A}$ corresponds to $(\overline{\mathfrak{b}}, \xi)$. The automorphism γ then corresponds to the class of an ideal $\mathfrak{a}$ of K^{r} such that $N_{\Phi^{\mathrm{r}}}(\mathfrak{a})\overline{\mathfrak{b}} = \mu\mathfrak{b}$ and $N(\mathfrak{a}) = \mu\overline{\mu}$ for some $\mu \in K^\times$. This proves one implication of part 1; the other follows by reading our argument backwards.

In case $g = 1$ and $\mathcal{O} = \mathcal{O}_K$, we can simply take $\mathfrak{a} = N_\Phi(\mathfrak{b}/\overline{\mathfrak{b}})$ and $\mu = 1$. If $g = 2$ and $\mathcal{O} = \mathcal{O}_K$, take $\mathfrak{a} = N_\Phi(\mathfrak{b})$ and $\mu = N(\mathfrak{b})$ (see the proof of [22, Corollary I.9.3] for details). This shows part 2.

Finally, if $\mathfrak{b} = \mathcal{O}$, then $\overline{\mathfrak{b}} = \overline{\mathcal{O}} = \mathcal{O}$, so $\mathfrak{a} = 1$ and $\mu = 1$ suffice. □

Proof of Proposition 2.7. Assume that $\mathcal{H}(1)/\mathcal{M}_0$ is an extension of degree 2, so $\mathfrak{a}$, μ and γ_0 as in the proof of Lemma 2.6 exist. By scaling $\mathfrak{a}$ (and scaling μ accordingly), we can assume $\mathfrak{a}$ to be coprime to NF.

Let $f(\tau)$ be any class invariant with $f \in \mathcal{F}_N$. Now $f(\tau)$ is in $\mathcal{M}_0$ if and only if $f(\tau)^{\gamma_0} = f(\tau)$, i.e., if and only if $\overline{f(\tau)^{[\mathfrak{a}]}} = f(\tau)$.

The action of complex conjugation on $f(\tau)$ is easy to describe. Note that $f^{\iota(-1 \bmod N)}$ is f with its Fourier coefficients replaced by their complex conjugates. Since complex conjugation is continuous, we get

$$\overline{f(\tau)} = f^{\iota(-1 \bmod N)}(-\overline{\tau}). \tag{4.2}$$

Let's look at the action of $[\mathfrak{a}]$ via the reciprocity law Theorem 2.4. Let $b_1, \ldots, b_{2g}$ be the symplectic basis of $\mathfrak{b}$ corresponding to τ. Then

$$\mu^{-1}\overline{b_1}, \ldots, \mu^{-1}\overline{b_g}, -\mu^{-1}\overline{b_{g+1}}, \ldots, -\mu^{-1}\overline{b_{2g}}$$

is a symplectic basis of $\mu^{-1}\overline{\mathfrak{b}} = N_{\Phi^{\mathrm{r}},\mathcal{O}}(\mathfrak{a})^{-1}\mathfrak{b}$ w.r.t. $\mu\overline{\mu}\xi = N(\mathfrak{a})\xi$, and the period matrix corresponding to this symplectic basis is $-\overline{\tau}$.

In particular, the transformation M^{t} between these bases (as in Proposition 2.7) satisfies the conditions of Theorem 2.4, so that we get $M \in \mathrm{GSp}_{2g}(\mathbf{Q})^+$ and M is finite and invertible modulo M. Let $U \in \mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ be its inverse, so we get $f(\tau)^{[\mathfrak{a}]} = f^U(M\tau) = f^U(-\overline{\tau})$.

Combining this with (4.2), we find $\overline{f(\tau)^{[\mathfrak{a}]}} = f^{U'}(\tau)$ with $U' = U\iota(-1)$. We conclude that indeed $f^{U'}(\tau) = f(\tau)$ if and only if $f(\tau) \in \mathcal{M}_0$.

Finally, if $f(\tau)$ is in $\mathcal{M}_0$ and generates $\mathcal{H}(1)$ over K^{r}, then we get

$$[K_0^{\mathrm{r}}(f(\tau)) : K_0^{\mathrm{r}}] \leq [\mathcal{M}_0 : K_0^{\mathrm{r}}] = [\mathcal{H}(1) : K^{\mathrm{r}}] = [K^{\mathrm{r}}(f(\tau)) : K^{\mathrm{r}}],$$

so the minimal polynomial of $f(\tau)$ over K^{r} is also the minimal polynomial over K_0^{r}. This finishes the proof of Proposition 2.7. □

5 Theta constants

For $c_1, c_2 \in \mathbf{Q}^g$, the *theta constant* with characteristic c_1, c_2 is

$$\theta[c_1, c_2](\tau) = \sum_{v \in \mathbf{Z}^g} \exp(\pi i (v + c_1)\tau (v + c_1)^{\mathrm{t}} + 2\pi i (v + c_1) c_2^{\mathrm{t}}).$$

Its quotients come with an explicit action of $\mathrm{Sp}_{2g}(\mathbf{Z})$.

Lemma 5.1. Given $A \in \mathrm{Sp}_{2g}(\mathbf{Z})$, there is a holomorphic $\rho = \rho_A : \mathcal{H}_g \to \mathbf{C}^*$ such that for all $c_1, c_2 \in \mathbf{Q}^g$, we have

$$\theta[c_1, c_2](A\tau) = \rho(\tau) \exp(2\pi i r) \theta[d_1, d_2](\tau),$$

where

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

$$\begin{pmatrix} d_1 \\ d_2 \end{pmatrix} = A^{\mathrm{t}} \begin{pmatrix} c_1 - \frac{1}{2}\mathrm{diag}(cd^{\mathrm{t}}) \\ c_2 - \frac{1}{2}\mathrm{diag}(ab^{\mathrm{t}}) \end{pmatrix}, \quad \text{and}$$

$$r = \frac{1}{2}((dd_1 - cd_2)^{\mathrm{t}}(-bd_1 + ad_2 + \mathrm{diag}(ab^{\mathrm{t}})) - d_1^{\mathrm{t}} d_2).$$

Proof. This is Formula 8.6.1 and Lemma 8.4.1(b) of [1]. □

For quotients of theta constants, this implies the following:

Proposition 5.2. Given $D \in 2\mathbf{Z}$ and $c_1, c_2, c_1', c_2' \in D^{-1}\mathbf{Z}^g$, we have

$$\frac{\theta[c_1, c_2]}{\theta[c_1', c_2']} \in \mathcal{F}_{2D^2},$$

where $A \in \mathrm{Sp}_{2g}(\mathbf{Z}/2D^2\mathbf{Z})$ acts by

$$\frac{\theta[c_1, c_2]}{\theta[c_1', c_2']}(A\tau) = \frac{\exp(2\pi i r)}{\exp(2\pi i r')} \frac{\theta[d_1, d_2]}{\theta[d_1', d_2']}(\tau),$$

with d_1, d_2 and r, as in Lemma 5.1 and d_1', d_2', r' analogously.

Proof. The action of $A \in \mathrm{Sp}_{2g}(\mathbf{Z})$ is implied by Lemma 5.1, as the factors ρ cancel. The theta constants themselves depend only on c_1, c_2 modulo $2\mathbf{Z}^g$, which proves that the action of A is trivial if $A \equiv 1 \bmod 2D^2$. Multiplying the numerator and denominator by $\theta[0, 0]^7$ and using $\rho_A(\tau)^8 = (\det c\tau + d)^4$ ([1, Exercise 8.11(9)]), we find that the function is a quotient of modular forms of equal weight with Fourier coefficients in $\mathbf{Q}(\zeta_{2D^2})$. □

It is known that the field generated by all quotients f as in Proposition 5.2 equals the field $\mathcal{F}_\infty$ (see e.g. [18, 27.15]). In particular, every element of $\mathcal{F}_\infty$ is a rational functions in theta functions. We can evaluate the action of $\mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ on such a rational function via Proposition 5.2 without the need of lifting to $\mathrm{Sp}_{2g}(\mathbf{Z})$.

The action of $\iota((\mathbf{Z}/N\mathbf{Z})^\times)$ on quotients of theta constants is even more explicit. Indeed, we have the following.

Lemma 5.3. Let D be an even positive integer and $c_1, c_2 \in D^{-1}\mathbf{Z}^g$. Let $N = 2D^2$. The action of $t \in (\mathbf{Z}/N\mathbf{Z})^\times$ on $\mathcal{F}_N$ is given by $\theta[c_1, c_2]^t = \theta[c_1, tc_2]$.

Proof. The Fourier coefficients correspond to the factors $\exp(2\pi i(v + c_1)c_2^{\mathrm{t}})$ in the definition of $\theta[c_1, c_2]$. These factors are N-th roots of unity, so the action is simply raising them to the power t, i.e., multiplying c_2 by t. □

We actually restrict to theta constants with $c_i \in [0, 1)^g$, because we have

$$\theta[c_1 + n_1, c_2 + n_2] = \exp(2\pi i c_1 n_2^{\mathrm{t}})\theta[c_1, c_2] \qquad \text{for} \quad n_1, n_2 \in \mathbf{Z}^g. \tag{5.1}$$

In particular, we only need to consider finitely many theta constants for any given D.

6 Class invariants

Given an order $\mathcal{O}$ in a CM-field K and Φ a CM-type of K, a *class invariant* is a value $f(\tau)$ with $f \in \mathcal{F}_\infty$ that generates the class field $\mathcal{H}(1)$ over K^{r}.

For example, if K is quadratic and $\mathcal{O} = \mathbf{Z} + \tau\mathbf{Z}$, then $j(\tau)$ is a class invariant, and its minimal polynomial over K is called the *Hilbert class polynomial* $H_{\mathcal{O}} \in \mathbf{Z}[X]$. Weber [26] gave class invariants of imaginary quadratic orders with minimal polynomial that are much smaller than $H_{\mathcal{O}}$.

As mentioned in the introduction, we would like to have smaller class invariants than the values of j (for $g = 1$) or of Igusa invariants (for $g = 2$). For any $f \in \mathcal{F}_N$, we can check the inclusion $K^{\mathrm{r}}(f(\tau)) \subset \mathcal{H}(1)$, i.e., $f(\tau) \in \mathcal{H}(1)$, using Theorem 2.3. If f is sufficiently general, then the inclusion of fields is a bijection, which can be verified using (2.1). Equation (2.1) also allows us to numerically approximate the minimal polynomial of $f(\tau)$ over K^{r}.

6.1 A detailed example

As an example, we will look for small f that are quotients of products of theta constants with $c_1, c_2 \in \{0, \frac{1}{2}\}^2$, i.e., $g = 2$, $D = 2$, $N = 8$. The ones for which $4c_1c_2^{\mathrm{t}}$ is odd are identically zero, and we are left with 10 theta constants, called the *even theta constants*, which happen to have Fourier coefficients in $\mathbf{Z}$. Following [4], we use the notation $\theta[(a, b), (c, d)] = \theta_{16b+8a+4d+2c}$, so the even theta constants are θ_k for $k \in \{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}$.

Let $K = \mathbf{Q}(\alpha) = \mathbf{Q}[X]/(X^4 + 27X^2 + 52)$ be a quartic CM-field with real quadratic subfield $K_0 = \mathbf{Q}(\sqrt{521})$. This is the field K from [22, Example III.3.2]. Take the CM-type Φ of K consisting of the two embeddings $K \to \mathbf{C}$ that map α to the positive imaginary axis. Let w be the (positive) square root of 13. The real quadratic subfield of the reflex field K^{r} is $\mathbf{Q}(w)$.

We start by finding one pair $(\mathfrak{b}, \xi)$ and the corresponding τ as in [23]. In our case, this is $\mathfrak{b} = \mathcal{O}$, $\xi = 2(-5882941509\alpha^3 - 146560028765\alpha)^{-1}$, and τ corresponding to the symplectic basis

$$\begin{aligned}
&\tfrac{1}{4}(-12075\alpha^3 + 5774\alpha^2 - 300821\alpha + 143846,\\
&\quad 27037\alpha^3 - 9188\alpha^2 + 673565\alpha - 228898,\\
&\quad 12075\alpha^3 - 24150\alpha^2 + 300821\alpha - 601642,\\
&\quad 29924\alpha^2 + 745488)
\end{aligned}$$

of $\mathfrak{b}$.

Next, we compute the image of the map

$$g : \frac{I(N) \cap H_{\Phi,\mathcal{O}}(1)}{H_{\Phi,\mathcal{O}}(N)} \longrightarrow \mathrm{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})/S$$

from Section 2.7. When listing the elements of $H_{\Phi,\mathcal{O}}(1)$, the following lemma seriously limits the elements of the class group to be checked.

Lemma 6.1. In the case $g = 2$, the square of every element $\mathfrak{a}$ of $H_{\Phi,\mathcal{O}}(1)$ is an ideal from K_0^{r} times a principal ideal.

Proof. One can check that if r is the non-trivial automorphism of K_0^{r}, then $\mathfrak{a}^2 = r(N_{K^{\mathrm{r}}/K_0^{\mathrm{r}}}(\mathfrak{a}))^{-1} N_\Phi(\mu)\mathcal{O}_{K^{\mathrm{r}}}$. See also [22, Proof of Lemma I.8.4]. □

In the specific example we are treating right now, the class group of K^{r} has odd order and the class number of K_0^{r} is one, so that actually $H_{\Phi,\mathcal{O}}(1)$ is the group of principal ideals. So we restrict to principal ideals (α) and have $g((\alpha)) = \epsilon(N_{\Phi^{\mathrm{r}}}(\alpha))$. We only need (α) up to $H_{\Phi,\mathcal{O}}(N)$, i.e., we only need α modulo 8. So we compute a set of 6 generators of the group $(\mathcal{O}_{K^{\mathrm{r}}}/(8))^\times \cong C_{12}^2 \times C_2^4$ and compute $N_{\Phi^{\mathrm{r}}}$ and ϵ with respect to the chosen symplectic basis of $\mathfrak{b}$.

The generators map to 6 matrices in $\mathrm{GSp}_{2g}(\mathbf{Z}/8\mathbf{Z})$, and the 8th powers of the theta constants fall into 4 orbits for these matrices: $\{\theta_0^8, \theta_6^8, \theta_1^8\}$, $\{\theta_2^8, \theta_4^8, \theta_3^8\}$, $\{\theta_8^8, \theta_9^8, \theta_{15}^8\}$, and the fixed point $\{\theta_{12}^8\}$. The first two orbits are identified under the action of U' from Proposition 2.7, so we choose

$$f = \zeta_8^k \left(\frac{\theta_{12}^3}{\theta_8\theta_9\theta_{15}} \right)^l,$$

and note that if 8 divides both k and l, then we have $f(\tau) \in \mathcal{H}(1)$. We minimize l and find that in fact $k = l = 2$ already gives a function that is invariant under U' and the image of g, i.e., such that $f \in \mathcal{H}(1)$.

Finally, for each of the 7 ideal classes of K^{r}, we compute U and M as in Theorem 2.4. We make sure that the basis $C = BM^{\mathrm{t}}$ is such that $M\tau$ is *reduced* for the action of $\mathrm{GSp}_{2g}(\mathbf{Z})$ (see e.g., [22, II.5]), so that the theta constants can be numerically evaluated most efficiently.

Then we compute f^U and evaluate it numerically in $M\tau$ to get a root of the minimal polynomial of $f(\tau)$ over K^{r}. This gives us a numerical approximation of the minimal polynomial

$$H_f = \prod (X - f^U(M\tau)) \in K_0^{\mathrm{r}}[X],$$

and we recognize its coefficients as elements of $K_0^{\mathrm{r}} \subset \mathbf{C}$ with the LLL-algorithm as in [8, Section 7].

We find that numerically with high precision, we have

$$\begin{aligned} 3^8 101^2 H_f = {} & 66928761X^7 + (21911488848w - 76603728240)X^6 \\ & + (-203318356742784w + 733099844294784)X^5 \\ & + (-280722122877358080w + 1012158088965439488)X^4 \\ & + (-234912038356251443 2w + 846987458815862 3744)X^3 \\ & + (-785912031217487708 16w + 283364613421131104256)X^2 \\ & + (250917334141632512w - 904696010264018944)X \\ & - 364471595827200w + 1312782658043904, \end{aligned}$$

which is significantly smaller than the smallest minimal polynomial obtained when using Igusa class polynomials, even with the small Igusa invariants from [23]:

$$\begin{aligned}
101^2 H_1 = {} & 10201X^7 \\
& + (1552051621163586477 55w + 559600170220938887110)X^6 \\
& + (1524076876974601951759207505355941525 50w \\
& \quad + 549513732768094956258970636118192859400)X^5 \\
& + \tfrac{1}{2}(2201909580030523730272623848434538048317834513875w \\
& \quad + 7939097894735431844153019089320973153011210882125)X^4 \\
& + (1047175262927393182849164587480891367594710449395570625w \\
& \quad + 377564410488220083286572934642975206938020009784573 6875)X^3 \\
& + \tfrac{1}{2}(9073929148004948551367529911060413111164047132473806072343 75w \\
& \quad + 3271651681305911192688931423723753094763461200379169938284375)X^2 \\
& + (1501416604965651986004588022297124411339065052590506998745406250 0w \\
& \quad + 5413434555036719078560598444558693989308353185140536597841106250 0)X \\
& + \tfrac{1}{2}(3208541702911513221287770105217518905131207705054905377776763289843 75w \\
& \quad + 1156856162931200670387093211443242850125709667683265459917987279296875)
\end{aligned}$$

6.2 More examples

We searched for class invariants with $D = g = 2$ for a few more fields. For each field we tried, the results were similar to Section 6.1.

Recently, Andreas Enge and Emmanuel Thomé computed the Igusa class polynomials of the maximal order $\mathcal{O}_K$ of the field $K = Q[X]/(X^4 + 310X^2 + 17644)$ of class number 3948.

It turns out that the functions

$$t = \frac{\theta_0\theta_8}{\theta_4\theta_{12}} \in \mathcal{F}_8, \quad u = \left(\frac{\theta_2\theta_8}{\theta_6\theta_{12}}\right)^2 \in \mathcal{F}_2, \quad v = \left(\frac{\theta_0\theta_2}{\theta_4\theta_6}\right)^2 \in \mathcal{F}_2$$

are class invariants for a certain τ with CM by $\mathcal{O}_K$. We have yet to find out how much these class invariants would speed up their computation.

7 Applications

7.1 Class fields

By definition of a class invariant, the minimal polynomial of any class invariant gives an equation defining $\mathcal{H}(1)$, and it is easy to compute numerically. However, with the j-invariant or Igusa invariants, this polynomial has coefficients that are too large to be practical. Smaller class invariants would reduce this size.

7.2 Curves of genus two with prescribed Frobenius

In this section, we sketch the CM method for constructing curves of genus two, and finish by showing how class invariants give a practical improvement.

7.2.1 The CM method

Suppose we want to construct a g-dimensional abelian variety over a finite field with a prescribed characteristic polynomial f of the Frobenius endomorphism. For simplicity, assume f is irreducible. The field $K = \mathbf{Q}[X]/(f)$ is a CM-field of degree $2g$ and the constant coefficient $f(0) = p^m$ is a prime power.

Now take any abelian variety A/k with $k \supset K^{\mathrm{r}}$ such that A has CM by $\mathcal{O}_K$. Let Φ be the CM-type of A and $\mathfrak{P}/p$ a prime of k. Suppose A has good reduction at $\mathfrak{P}$ and let $\widetilde{A}$ be the reduction. Let $\mathrm{Frob} \in \mathrm{End}(\widetilde{A})$ be the Frobenius endomorphism of $\widetilde{A}$. It is known that reduction modulo p gives an embedding $\mathcal{O}_K = \mathrm{End}(A) \subset \mathrm{End}(\widetilde{A})$. We then have the following result.

Theorem 7.1 (Shimura-Taniyama formula [19, Thm.1 in §13])**.** *The endomorphism* Frob *is an element of the ring* $\mathcal{O}_K \subset \mathrm{End}(\widetilde{A})$ *and generates the ideal* $N_{\Phi^{\mathrm{r}}}(N_{k/K^{\mathrm{r}}}(\mathfrak{P}))$ *of* $\mathcal{O}_K$*.*

This, together with the fact $\mathrm{Frob}\overline{\mathrm{Frob}} = \#(\mathcal{O}_k/\mathfrak{P})^g$ determines Frob up to roots of unity.

By choosing $\mathfrak{P}$ appropriately, we can thus construct an abelian variety corresponding to f if it exists [24]. By choosing f appropriately, this yields elliptic curves or curves of genus two that are suitable for cryptography [3].

In practice, one does this only for $g \leq 2$ and one does not write down defining equations for A, but only computes some elements of $\mathcal{F}_1$ evaluated at A. In case $g = 1$, it suffices to take the j-invariant, while in the case $g = 2$, one takes a triple of absolute Igusa invariants, i.e., generators of $\mathcal{F}_1$.

In the case $g = 1$, the elliptic curve $\widetilde{A}$ can be reconstructed from $j(A) \bmod \mathfrak{P}$ by a simple formula found in any textbook on elliptic curves. In the case $g = 2$, for generic values of the Igusa invariants modulo $\mathfrak{P}$, one can reconstruct $\widetilde{A}$ as the Jacobian of a hyperelliptic curve using Mestre's algorithm [9]. For $g \geq 3$, no sufficiently general analogue of Mestre's algorithm exists.

In the CM method for $g = 1$, the j-invariant is usually represented by its minimal polynomial, the Hilbert class polynomial. Reduction modulo a prime $\mathfrak{P}/p$ is done by taking the reduction modulo p of the class polynomial and taking a root of that in $\overline{\mathbf{F}_p}$.

In the case $g = 2$, one can take a minimal polynomial H_{i_1} of the first Igusa invariant, $i_1(A)$, over K^{r}, and let i_2 and i_3 be represented by polynomials

$$\widehat{H}_{i_1,i_n} = \sum_{\gamma} i_n(A)^{\gamma} \prod_{\sigma} (X - i_n(A)^{\sigma}) \in K_0^{\mathrm{r}}[X],$$

where sum and product range over $\mathrm{Gal}(\mathcal{H}(1)/K^{\mathrm{r}})$. Reducing H_1 modulo $\mathfrak{p}_0 = \mathfrak{P} \cap K_0^{\mathrm{r}}$ and taking any root is equivalent to reducing $i_n(A)$ modulo a prime over $\mathfrak{p}_0$. Changing $\mathfrak{P}$ without changing $\mathfrak{p}_0$ will change the ideal in Theorem 7.1 at most by complex conjugation, which will not affect the characteristic polynomial of Frobenius. We can then find $i_2(\widetilde{A})$ and $i_3(\widetilde{A})$ by computing

$$i_n(\widetilde{A}) = \frac{\widehat{H}_{i_1,i_n}(i_1(\widetilde{A}))}{H'_{i_1}(i_1(\widetilde{A}))}$$

if p is sufficiently large.

7.3 Class invariants for genus one

In the case $g = 1$, the use of class invariants in the CM method is standard. Let H_f be the minimal polynomial of a class invariant $f(\tau)$, and let $\Phi_{f,j}(X, Y) \in \mathbf{Q}(X)[Y]$ be such that $\Phi_{f,j}(j, Y) \in \mathbf{Q}(j)[Y]$ is the minimal polynomial of $f \in \mathcal{F}_N$ over $\mathcal{F}_1 = \mathbf{Q}(j)$. Then $\Phi_{f,j}(j(\tau), f(\tau)) = 0$, so we can find $j(\tau)$ by solving for X in $\Phi_{f,j}(X, f(\tau)) = 0$.

For the CM-method, we now only compute H_f and $\Phi_{f,j}$. Here $\Phi_{f,j}$ can be precomputed once for every function $f \in \mathcal{F}_N$ that we would like to use for class invariants, and H_f is much smaller, hence needs less precision, than the Hilbert class polynomial H_j. We compute $f(\tau)$ modulo a prime over $\mathfrak{P}$ by taking a root of H_f modulo p (and call it $\widetilde{f}$). Then we compute $j(\widetilde{A})$ by solving for X in $\Phi_{f,j}(X, \widetilde{f}) = 0$. There may be multiple solutions to try here.

7.4 Class invariants for genus two

For genus two, modular polynomials are much harder to compute, and the analogue of solving $\Phi_{f,j}(X, \widetilde{f}) = 0$ means finding a Groebner basis, which is hard as well.

Instead, we work with polynomials

$$\widehat{H}_{f,i_n} = \sum_{\gamma} i_n(A)^{\gamma} \prod_{\sigma} (X - f(A)^{\sigma}) \in K^{\mathrm{r}}[X].$$

In fact, if the conditions of Proposition 2.7 are satisfied, then these polynomials are in $K_0^{\mathrm{r}}[X]$. We find $\widetilde{f}$ as in the elliptic case, and compute $i_n(\widetilde{A})$ for $n = 1, 2, 3$ from it by the formula

$$i_n(\widetilde{A}) = \frac{\widehat{H}_{f,i_n}(f(\widetilde{A}))}{H_f'(\widetilde{f})}.$$

The downside of this is that we get four polynomials instead of the three polynomials that we had when not using class invariants. Still, all of these polynomials can be a lot smaller than the original polynomials, as the size of all four of them is dominated by the height of f, which is hopefully much smaller than the height of i_1.

For the example from Section 6.1, the four polynomials $H_f, \widehat{H}_{f,i_n}$ together take up 15% less space than the three polynomials $H_{i_1}, \widehat{H}_{i_1,i_n}$, and the largest coefficient (which determines the precision at which theta constants need to be evaluated, the dominant step) is 40% smaller. And this is just one easily found class invariant, for the first field that was tried.

References

[1] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der mathematischen Wissenschaften*. Springer, second edition, 2004.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[4] Régis Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications*. PhD thesis, École Polytechnique, 2006. `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/these_soutenance.pdf`.

[5] Alice Gee and Peter Stevenhagen. Generating class fields using Shimura reciprocity. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 441–453. Springer, Berlin, 1998.

[6] Max Koecher. Zur Theorie der Modulformen n-ten Grades. I. *Math. Z.*, 59:399–416, 1954.

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

[8] Hendrik W. Lenstra, Jr. Lattices. In J. Buhler and P. Stevenhagen, editors, *Surveys in Algorithmic Number Theory*, volume 44 of *MSRI Publications*, pages 127 – 181. Cambridge University Press, 2008.

[9] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334, Boston, MA, 1991. Birkhäuser Boston.

[10] Morris Newman. *Integral matrices*. Academic Press, New York, 1972. Pure and Applied Mathematics, Vol. 45.

[11] SAGE. SAGE Mathematics Software, version 4.7.1. `http://www.sagemath.org/`.

[12] Goro Shimura. On canonical models of bounded symmetric domains I. *Ann of Math*, 91:144–222, 1970.

[13] Goro Shimura. On canonical models of bounded symmetric domains II. *Ann of Math*, 92:528–549, 1970.

[14] Goro Shimura. On some arithmetic properties of modular forms of one and several variables. *Ann. of Math. (2)*, 102(3):491–515, 1975.

[15] Goro Shimura. On the Fourier coefficients of modular forms of several variables. *Göttingen Nachr. Akad. Wiss.*, pages 261–268, 1975.

[16] Goro Shimura. Theta functions with complex multiplication. *Duke Mathematical Journal*, (4):673–696, 1976.

[17] Goro Shimura. On certain reciprocity-laws for theta functions and modular forms. *Acta Math.*, 141(1-2):35–71, 1978.

[18] Goro Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998. Sections 1–16 essentially appeared before in [19].

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

[20] Anne-Monika Spallek. *Kurven vom Geschlecht* 2 *und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994. `http://www.uni-due.de/zahlentheorie/theses_de.shtml`.

[21] Marco Streng. Sage package for using Shimura's reciprocity law for Siegel modular funcions. `http://www.warwick.ac.uk/~masjap/recip`.

[22] Marco Streng. *Complex multiplication of abelian surfaces*. PhD thesis, Universiteit Leiden, 2010. `http://hdl.handle.net/1887/15572`.

[23] Marco Streng. Computing Igusa class polynomials. submitted, arXiv:0903.4766, 2011.

[24] John Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda). *Sémin. Bourbaki 1968/69, No.352*, pages 95–110, 1971.

[25] The PARI Group, Bordeaux. *PARI/GP, version* `2.4.3`, 2011. available from `http://pari.math.u-bordeaux.fr/`.

[26] Heinrich Weber. *Algebraische Zahlen*, volume 3 of *Lehrbuch der Algebra*. Braunschweig, Friedrich Vieweg, 1908.