Modular polynomials on Hilbert surfaces

Enea Milio, Damien Robert

Contents

Abstract

We describe an evaluation/interpolation approach to compute modular polynomials on a Hilbert surface, which parametrizes abelian surfaces with maximal real multiplication. Under some heuristics we obtain a quasi-linear algorithm. The corresponding modular polynomials are much smaller than the ones on the Siegel threefold. We explain how to compute even smaller polynomials by using pullbacks of theta functions to the Hilbert surface.

1 Introduction

1.1 Context

Isogenies play an important role in elliptic curve cryptography. They allow to transfer the discrete logarithm problem from one curve to a possibly weaker one [25, 70]; they are used by the Schoof–Elkies–Atkin (SEA) point counting algorithm [67, 57, 18], and also by the CRT algorithms to compute class polynomials [73, 21] and modular polynomials [7]. Splitting the multiplication using isogenies can improve the efficiency of the arithmetic [13, 28], taking isogenies to mask the points reduces the impact of side channel attacks [69], and isogenies are used to construct a normal basis of a finite field [11]. They have also been used to construct hash functions [10] and to build cryptosystems [75, 65], in particular quantum-resistant cryptosystems [12].

In dimension 1, the ℓ-modular polynomials ϕ_ℓ parametrize pairs of elliptic curves E_1 and E_2 that are ℓ-isogenous over the algebraic closure. They can be computed in quasi-linear time [20] by the evaluation/interpolation method. More precisely the classical modular polynomials parametrize the elliptic curves from their j-invariants, so that E_1 and E_2 are ℓ-isogenous whenever $\phi_\ell(j(E_1), j(E_2)) = 0$. Other modular invariants have been proposed which yield smaller polynomials [23].

Principally polarized complex abelian surfaces (which are generically Jacobians of hyperelliptic curves) are parametrized by the Siegel threefold $\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathcal{H}_g$ (with $g = 2$) where $\mathcal{H}_g$ is the Siegel space of symmetric $g \times g$ complex matrices with totally positive definite imaginary part. The Siegel threefold is an algebraic variety birationally equivalent to three dimensional projective space, and is parametrized by the three Igusa invariants [40, 41]. One can then generalize modular polynomials to this setting: the ℓ-modular polynomials classify pairs of principally polarized abelian surfaces (A, B) which admit an ℓ-isogeny $A \to B$[1]. More precisely the ℓ-modular polynomials evaluated on the three Igusa invariants of A describe a dimension 0 subvariety of the Siegel threefold of degree $\ell^3 + \ell^2 + \ell + 1$ whose geometric points correspond to the triples of Igusa invariants of the ℓ-isogenous abelian surfaces B. Alternatively, these modular polynomials describe the image of $X_0(\ell)$ inside $X_0(1) \times X_0(1)$ where $X_0(\ell) = \Gamma^0(\ell)\backslash\mathcal{H}_g$ and $\Gamma^0(\ell) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z}) : \ell | b\}$. These polynomials have been studied in [27, 5] and computed for $\ell = 2$ in [16]. Generalizations of these modular polynomials using smaller Siegel modular invariants have more recently been computed in [55].

Unfortunately even using a quasi-linear algorithm, computing them is hard due to their size. Indeed compared to dimension 1 where modular polynomials describe a curve $X_0^1(\ell)$ inside the plane $X_0^1(1) \times X_0^1(1)$, and where the degree of the projection is $\ell + 1$, in dimension 2 they describe the threefold $X_0(\ell)$ inside a dimension six space and the degree of the projection

[1] An ℓ-isogeny is an isogeny $f : (A, \mathcal{L}) \to (B, \mathcal{M})$ between principally polarized abelian varieties such that $f^*\mathcal{M} = \mathcal{L}^\ell$.

is $\ell^3 + \ell^2 + \ell + 1$. Already these polynomials for $\ell = 7$ take 29 GB of memory just to write down the result (even using the most memory efficient choice of invariant). So it seems hard to go much further. But having them only up to $\ell = 7$ is not enough for most of the applications mentioned.

Another problem is that restricting to ℓ-isogenies does not allow one to explore the full isogeny graph of principally polarized abelian surfaces. In the CRT method to compute class polynomials, one key step of the algorithm is to take an abelian surface in the right isogeny graph, and then use isogenies to find an abelian surface with maximal complex multiplication [6, 50]. But this is not always possible using only ℓ-isogenies [8, Theorem 9.4].

We recall that an ℓ-isogeny f corresponds to a kernel $V = \operatorname{Ker} f$ which is maximal isotropic for the Weil pairing e_ℓ on the ℓ-torsion $A[\ell]$. The kernel of an ℓ-isogeny is then an abelian group of type (ℓ, ℓ). One can also consider cyclic isogenies, where the kernel is a cyclic subgroup of the ℓ-torsion. However, if A is principally polarized and V is cyclic in $A[\ell]$, then A/V is not principally polarizable in general. Indeed, the isogenous abelian surface admits a principal polarization if and only if there exists $\beta \in \operatorname{End}^{s,++}(A)$ a totally positive symmetric element of norm ℓ in the ring $\operatorname{End}^s(A)$ of symmetric endomorphisms of A such that $V \subset \operatorname{Ker} \beta$ (since V is cyclic it is automatically isotropic for the β-Weil pairing). We call such an isogeny a β-isogeny, and one is naturally led to try to define β-modular polynomials parametrizing pairs of β-isogenous abelian surfaces (A, B). Generically, a complex abelian surface A has no (non trivial) symmetric endomorphisms, so to define β-modular polynomials we need to restrict to a sublocus of the moduli space of abelian surfaces with specific real multiplication.

Let $\mathcal{O}_K$ be a maximal real quadratic order of discriminant Δ_K. The Hilbert moduli space is a surface parametrizing isomorphism[2] classes of principally polarized abelian surfaces A together with an embedding $\mathcal{O}_K \to \operatorname{End}^s(A)$. Let $\beta \in \mathcal{O}_K$ be a totally positive element of norm ℓ. In this article, we define β-modular polynomials on this Hilbert modular surface and we explain how to compute them by evaluation/interpolation. We use the forgetful map from the Hilbert modular surface to the Siegel space, or more precisely, to a Humbert surface, and use the tools already known there, especially those described in [16, 55] for the computation of ℓ-modular polynomials.

1.2 Results

We study several parametrizations of Humbert surfaces. The Siegel moduli threefold is parametrized by the three Igusa functions, and in [55] a cover of the Siegel space given by level 2 theta constant is also used to give smaller modular polynomials.

Now we fix the real multiplication, and we explain how to parametrize covers of the corresponding Humbert surface. Pulling back the Igusa functions to the Humbert surface gives rational[3] coordinates which can be used to define modular polynomials. Likewise pulling back theta functions give coordinates on a cover of the Humbert surface. Some Humbert surfaces are rational and can be parametrized by two invariants instead of the three defined above. In this paper we look in particular at the case of Humbert surfaces of discriminant 5 and 8 which can be parametrized by two Gundlach invariants.

For the modular polynomial computations, we need an algorithm for the evaluation step and one for the interpolation step. The first algorithm computes, given a period matrix $\tau \in \mathcal{H}_1^2$, the

[2] respecting the polarization

[3] in the sense that the coordinates have a denominator so are not defined everywhere

above invariants at some precision N in quasi-linear time in the precision N. The second one, given the value of the above invariants, computes a corresponding period matrix $\tau \in \mathcal{H}_1^2$ in time quasi-linear in the requested precision. Instead of computing on Humbert surfaces, our idea is to translate back and forth between the Hilbert moduli space and the Siegel moduli space where in the latter space both algorithms have been developed by Dupont in [16]. The translation is based on the work of Igusa [40, 41], Gundlach [34, 35], Resnikoff [63], Lauter-Yang [49], Runge [66] and Birkenhake-Wilhelm [4]. In the case of Humbert surfaces of discriminant 5, we have inverted the formulas of [49, Proposition 4.5] expressing the pullback of the Igusa invariants as a function of the Gundlach invariants (see Appendix B.1). In the case of Humbert surfaces of discriminant 8, we link in Theorem A.14 and Corollary A.15 the Gundlach invariants with the pullback of the Igusa invariants, as was done by Resnikoff for discriminant 5. These algorithms are described in Section 3.2 (see also Theorem 3.4).

The main result of this paper is the computation of modular polynomials on the Hilbert (or Humbert) surface. When $\beta \in \mathcal{O}_K$ is a totally positive prime element, we define β-isogenies and β-modular polynomials in Section 4. In particular β-modular polynomials parametrize isogenies corresponding to maximal isotropic (for the β-pairing) kernels $K \subset A[\beta]$ stable by real multiplication.

Suppose that β is a prime above ℓ. It turns out that for abelian surfaces there is a natural case distinction between ℓ inert, split, and ramified.

- If ℓ is split or ramified (so the norm of β is ℓ), then the β-isogenies correspond to isogenies with cyclic kernel $V \subset A[\beta] \subset A[\ell]$. All β-isogenies then preserve real multiplication (see Section 4.1 for the definition) and the β-modular polynomials parametrize all pairs of principally polarized abelian surfaces with maximal real multiplication and admitting a cyclic isogeny of degree ℓ;

- If ℓ is inert in $\mathcal{O}_K$ then $\beta = \ell$ is of norm ℓ^2. In this case the β-modular polynomials (on the Hilbert moduli space) parametrize β-isogenies between abelian surfaces with maximal real multiplication. By contrast to the Siegel ℓ-modular polynomials which given A parametrize all $\ell^3 + \ell^2 + \ell + 1$ abelian surfaces $B = A/V$ where $V \subset A[\ell]$ is maximal isotropic for the Weil pairing, the Hilbert β-modular polynomials parametrize all $\ell^2 + 1$ abelian surfaces $B = A/V$ where V is furthermore stable under the action of the real multiplication. In order to not induce confusion between Siegel ℓ-modular polynomials and Hilbert β-modular polynomials, we will always use the term ℓ-isogeny in the first case and β-isogeny in the second case.

We give in Theorem 4.15 a quasi-linear algorithm for computing β-modular polynomials for a large class of invariants, like Gundlach invariants (for $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$), pullbacks of Igusa invariants and pullbacks of theta constants (for all real quadratic fields). In the latter two cases we have three invariants for a moduli space of dimension 2 so we need to adapt the evaluation/interpolation algorithm to handle the fact that these three invariants have to satisfy a relation.

Theorem 4.15 is itself a particular case of Theorem 3.11 which gives an evaluation/interpolation algorithm to compute covers of Hilbert surfaces. Adapting this theorem to the cover parametrizing β-isogenies then yields Theorem 4.15.

The corresponding algorithms have been implemented in Pari/GP, and we give some examples of β-modular polynomials. We mainly give examples in the case where $K = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{5})$ since this allows us to compare different kinds of invariants.

Finally Martindale and Streng [53, 54] have also independently described an algorithm to compute modular polynomials on Hilbert moduli space. While we use evaluation/interpolation, they use linear algebra on the Fourier coefficients of the Hilbert modular form. The advantage of their method is that it works in any dimension and for any modular invariant (provided one can compute its Fourier coefficients). By contrast our evaluation/interpolation approach needs fast evaluation of modular invariants (for the complexity) and for the interpolation we need to be able to recover the period matrix from the values of the modular coefficients. We only know how to do that efficiently in dimension 2 (and 1) when the invariants are derived from theta constants (as mentioned by translating back and forth to the Siegel space and using [16]). In particular our algorithm can not be extended to higher dimension as long as the work of Dupont on the generalization of the AGM is not extended to dimension greater than 2. Work in this direction has been done by Labrande and Thomé in [45, 47]. However in dimension 2, we do obtain a quasi-linear algorithm, while there is no complexity analysis in [53], and our algorithm is practical since we have computed large polynomials. Our main limitation was the intrinsic size of the modular polynomials (see Tables 1,2,3) and not the speed of the computations.

1.3 Outline

The remainder of this article is organized as follows. In Section 2, we define the Siegel (in Section 2.1) and the Hilbert spaces (in Section 2.2) and describe the corresponding moduli data. We also give generators for the fields of modular functions on these spaces. Then in Section 2.3, we analyze the forgetful map from the Hilbert modular surface to the Siegel space. In Section 2.4, we focus on the Humbert surfaces. A Humbert surface is the image of a given Hilbert modular surface by the previous map. We conclude this Section by looking at covers of a Humbert surface in Section 2.5.

Section 3 is concerned with invariants of Hilbert surfaces. In Section 3.2 we explain how to efficiently evaluate a large class of Hilbert invariants. In Section 3.3 we give an interpolation algorithm, which will work even when we have relations between our invariants. Lastly we conclude the Section by giving in Section 3.4 an algorithm to compute covers of Hilbert surface.

Section 4 is concerned with modular polynomials on Hilbert surfaces. First in Section 4.1, we define isogenies preserving real multiplication. Then in Section 4.2, we introduce modular functions for β-isogenies and in Section 4.3, we define the modular polynomials depending on these isogenies and give an algorithm to compute them in quasi-linear time.

Finally in Section 5, we describe some polynomials we have computed.

While the algorithms presented in this paper are very general, to compute modular polynomials we need to make a choice of invariants. This is described in Appendix A. Appendix A.1 describes the pullback of Siegel invariants, giving (symmetric) invariants on any Hilbert modular surface. Of notable interest are the pullback of Igusa invariants and the pullback of theta functions. Gundlach invariants for $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ are described in Appendix A.2 and their relationship with the pullback of Igusa invariants in Appendix A.3. Other invariants are described in Appendix A.4. Further informations about covers of Humbert surfaces of level 2 and $(2, 4)$ is given in Appendix A.5.

Further details related to the computations of the modular polynomials from Section 5 are given in Appendix B. Appendix B.1 is concerned with modular polynomials expressed in term of Gundlach invariants and B.2 in terms of the pullback of theta functions.

Thanks We thank Pierre-Jean Spaenlehauer who successfully computed the Gröbner basis expressing the Gundlach invariants in term of the Igusa invariants for $D = 2$. We thank David Kohel who suggested us to look at the work of Elkies and Kumar [19] to get invariants for more Humbert or Hilbert surfaces (see Appendix A.4). We thank the anonymous reviewer for his careful reading and his many comments and suggestions.

2 Hilbert and Siegel modular spaces

2.1 Siegel modular space

The Siegel upper half-space in dimension 2 is the set $\mathcal{H}_2 = \{\Omega \in M_2(\mathbb{C}) \mid \Omega$ is symmetric and $\Im(\Omega) > 0\}$ ($\Im$ stands for the imaginary part). It is a moduli space for principally polarized complex abelian surfaces with symplectic basis: such a surface is a torus $\mathbb{C}^2/(\mathbb{Z}^2 + \Omega\mathbb{Z}^2)$ for some $\Omega \in \mathcal{H}_2$, and the canonical principal polarization is induced by the Hermitian form given by $\Im(\Omega)^{-1}$ (see [3, Section 8.1]).

We define the symplectic group $\mathrm{Sp}_4(\mathbb{Z})$ as $\{\gamma \in \mathrm{GL}_4(\mathbb{Z}) \mid {}^t\gamma J \gamma = J\}$ where $J = \left(\begin{smallmatrix} 0 & I_2 \\ -I_2 & 0 \end{smallmatrix}\right)$ and I_n is the identity matrix of size n. It acts on $\mathcal{H}_2$ by $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \cdot \Omega = (A\Omega + B)(C\Omega + D)^{-1}$ (it is a left action). The Siegel modular threefold is the Baily-Borel compactification [1] of the quotient space $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$ and this quotient space is a moduli space for isomorphism classes of principally polarized abelian surfaces. See [3, Section 8.2].

Let Γ be a subgroup of $\mathrm{Sp}_4(\mathbb{Z})$ of finite index and $k \in \mathbb{Z}$. A *Siegel modular form of weight k for Γ* is a holomorphic function $f : \mathcal{H}_2 \to \mathbb{C}$ such that for all $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma$ and $\Omega \in \mathcal{H}_2$, $f(\gamma\Omega) = \det(C\Omega + D)^k f(\Omega)$. The quotient of two Siegel modular forms for the same weight and group Γ is called a *Siegel modular function* for Γ. Note that if f is a Siegel modular function for Γ, and $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$, then $f(\gamma\Omega) = f(\Gamma\gamma\Omega)$ so that we can consider the set of right cosets $\Gamma\backslash\mathrm{Sp}_4(\mathbb{Z})$. More generally, in the rest of the paper, we will always consider sets of right cosets for a similar reason.

Let $a, b \in \{0, \frac{1}{2}\}^2$. The classical *theta constant with characteristic* (a, b) is

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](\Omega) = \sum_{n \in \mathbb{Z}^g} \exp(i\pi\, {}^t(n+a)\Omega(n+a) + 2i\pi\, {}^t(n+a)b).$$

To simplify the notation we define for all $a = \left(\begin{smallmatrix} a_0 \\ a_1 \end{smallmatrix}\right)$ and $b = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}$ in $\{0,1\}^2$

$$\theta_{b_0+2b_1+4a_0+8a_1}(\Omega) := \theta\begin{bmatrix} a/2 \\ b/2 \end{bmatrix}(\Omega).$$

Of the 16 theta constants, 6 are identically zero and we denote by $\mathcal{P} = \{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}$ the subscripts of the even theta constants (the non-zero ones). The following functions h_i are Siegel modular forms of weight i for the symplectic group $\mathrm{Sp}_4(\mathbb{Z})$

$$h_4 = \sum_{i \in \mathcal{P}} \theta_i^8, \quad h_6 = \sum_{\text{60 triples } (i,j,k) \in \mathcal{P}^3} \pm(\theta_i\theta_j\theta_k)^4,$$

$$h_{10} = \prod_{i \in \mathcal{P}} \theta_i^2, \quad h_{12} = \sum_{\text{15 tuples } (i,j,k,l,m,n) \in \mathcal{P}^6} (\theta_i\theta_j\theta_k\theta_l\theta_m\theta_n)^4$$

(see for example [42, Page 848], [16, Section 6.3.3] or [71, Section 7.1] for the exact definition).

We define the Siegel Eisenstein series ψ_k of even weight $k \geq 4$ by

$$\psi_k(\Omega) = \sum_{C,D} \det{(C\Omega + D)^{-k}},$$

where the sum is taken over the set of bottom halves (C, D) of elements $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ of $\mathrm{Sp}_4(\mathbb{Z})$ up to left multiplication by $\mathrm{SL}_2(\mathbb{Z})$. Let

$$\chi_{10} = -2^{-12}3^{-5}5^{-2}7^{-1}53^{-1}43867(\psi_4\psi_6 - \psi_{10}) \qquad \text{and}$$

$$\chi_{12} = 2^{-13}3^{-7}5^{-3}7^{-2}337^{-1}131 \cdot 593(3^27^2\psi_4^3 + 2 \cdot 5^3\psi_6^2 - 691\psi_{12})$$

are two Siegel modular cusp form of weights 10 and 12 respectively. These series can be written in terms of theta constants. Indeed we have by Igusa [42, Page 848] that $\psi_4 = 2^{-2}h_4$, $\psi_6 = 2^{-2}h_6$, $\chi_{10} = -2^{-14}h_{10}$ and $\chi_{12} = 2^{-17}3^{-1}h_{12}$. The graded ring of Siegel modular forms for $\mathrm{Sp}_4(\mathbb{Z})$ is the polynomial ring of ψ_4, ψ_6, χ_{10} and χ_{12}. We define the Igusa invariants from these last modular forms:

$$\mathrm{j}_1 = 2 \cdot 3^5 \frac{\chi_{12}^5}{\chi_{10}^6}, \qquad \mathrm{j}_2 = 2^{-3}3^3\frac{\psi_4\chi_{12}^3}{\chi_{10}^4} \qquad \text{and} \qquad \mathrm{j}_3 = 2^{-5}3\left(\frac{\psi_6\chi_{12}^2}{\chi_{10}^3} + 2^23\frac{\psi_4\chi_{12}^3}{\chi_{10}^4}\right). \tag{1}$$

The field of Siegel modular functions for $\mathrm{Sp}_4(\mathbb{Z})$ is $\mathbb{C}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$. Generically, two principally polarized abelian surfaces are isomorphic if and only if they have the same three Igusa invariants. (In [40, 41], Igusa has defined 10 absolute invariants, which allows to characterize all abelian surfaces up to isomorphisms over the algebraic closure of the base field.)

Let $\Gamma(2) = \{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z}) : \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \equiv I_4 \bmod 2\}$. It is a normal subgroup of $\mathrm{Sp}_4(\mathbb{Z})$ of index 720. The three following functions

$$r_1 = \frac{\theta_0^2\theta_1^2}{\theta_3^2\theta_2^2}, \qquad r_2 = \frac{\theta_1^2\theta_{12}^2}{\theta_2^2\theta_{15}^2} \qquad \text{and} \qquad r_3 = \frac{\theta_0^2\theta_{12}^2}{\theta_3^2\theta_{15}^2} \tag{2}$$

are Siegel modular functions for $\Gamma(2)$ called the *Rosenhain invariants*. They are generators for the field of modular functions belonging to $\Gamma(2)$ (see Mumford [60, Section 8]).

Let $\Gamma(2, 4) = \{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z}) : \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \equiv I_4 \bmod 2 \text{ and } B_0 \equiv C_0 \equiv 0 \bmod 4\}$, where X_0 denotes the vector composed of the diagonal elements of X. It is a normal subgroup of $\mathrm{Sp}_4(\mathbb{Z})$ of index 11520. The quotients of theta functions

$$b_i(\Omega) = \theta_i(\Omega/2)/\theta_0(\Omega/2) \tag{3}$$

for $i = 1, 2, 3$ are Siegel modular functions for $\Gamma(2, 4)$ and they are generators for the field of modular functions belonging to $\Gamma(2, 4)$ (see Manni [52, Theorem 1]).

2.2 Hilbert modular space

We refer to [31, 9, 32, 24, 61] for more details on Hilbert modular forms and Hilbert surfaces.

Let $D > 0$ be a square-free integer and $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field. Its discriminant Δ_K is D if $D \equiv 1 \bmod 4$ and $4D$ if $D \equiv 2, 3 \bmod 4$. Consider $\mathcal{O}_K$ to be the ring of integers of K. We have that $\mathcal{O}_K = \mathbb{Z} + \omega\mathbb{Z}$ where $\omega = \frac{1+\sqrt{D}}{2}$ if $D \equiv 1 \bmod 4$ and $\omega = \sqrt{D}$ otherwise. Denote by $\overline{a}$ the Galois conjugate of a in $\mathcal{O}_K$; that is, for $K \subset \mathbb{R}$ and $\sqrt{D} > 0$, we have $\overline{\alpha + \beta\sqrt{D}} = \alpha - \beta\sqrt{D}$.

The set $\mathcal{H}_1^+ = \{z \in \mathbb{C} : \Im(z) > 0\}$ is the *Poincaré half-plane.* We will often denote it as $\mathcal{H}_1$ to not surcharge the notations. Let $\mathcal{H}_1^- = -\mathcal{H}_1^+$. The group $\mathrm{SL}_2(\mathcal{O}_K)$ acts on the left on $\mathcal{H}_1^+ \times \mathcal{H}_1^-$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot (\tau_1, \tau_2) = (\frac{a\tau_1+b}{c\tau_1+d}, \frac{\overline{a}\tau_2+\overline{b}}{\overline{c}\tau_2+\overline{d}})$. The Baily-Borel compactification of the quotient space $\mathrm{SL}_2(\mathcal{O}_K)\backslash\mathcal{H}_1^+ \times \mathcal{H}_1^-$ is the *Hilbert modular surface* (see for example [31, Section 7]). It parametrizes principally polarized abelian surfaces (A, θ) with real multiplication by the maximal order $\mathcal{O}_K$, with an explicit embedding $\mu : \mathcal{O}_K \to \mathrm{End}(A)$ (see [3, Chapter 9]).

For computations, it can be convenient to work over another model, which we describe here. Let $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(K) : a, d \in \mathcal{O}_K, b \in \partial_K^{-1} \text{ and } c \in \partial_K\}$, where ∂_K is the different ideal of K. As $K = \mathbb{Q}(\sqrt{D})$, we have that $\partial_K = \sqrt{\Delta_K}\mathcal{O}_K$ and $\partial_K^{-1} = \frac{1}{\sqrt{\Delta_K}}\mathcal{O}_K$. We have group isomorphisms

$$\begin{array}{rrcl} \phi_\pm : & \mathrm{SL}_2(\mathcal{O}_K) & \to & \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \\ & \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) & \mapsto & \begin{pmatrix} a & b/\sqrt{\Delta_K} \\ c\sqrt{\Delta_K} & d \end{pmatrix} \end{array} \qquad \begin{array}{rrcc} \phi_\pm : & \mathcal{H}_1^+ \times \mathcal{H}_1^- & \to & \mathcal{H}_1^2 \\ & (\tau_1, \tau_2) & \mapsto & (\tau_1\sqrt{\Delta_K}, -\tau_2\sqrt{\Delta_K}) \end{array} \tag{4}$$

and the following diagram is commutative

$$\begin{tikzcd} \mathrm{SL}_2(\mathcal{O}_K) \times \mathcal{H}_1^+ \times \mathcal{H}_1^- \arrow[r] \arrow[d] & \mathcal{H}_1^+ \times \mathcal{H}_1^- \arrow[d] \\ \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \times \mathcal{H}_1^2 \arrow[r] & \mathcal{H}_1^2 \end{tikzcd} \tag{5}$$

(see [19, Section 3]). If $\tau = (\tau_1, \tau_2) \in \mathcal{H}_1^2$, the corresponding abelian surface is given by the torus $\mathbb{C}^2/(\mathbf{\Phi}(\mathcal{O}_K) \oplus \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix}\mathbf{\Phi}(\partial_K^{-1}))$ where $\mathbf{\Phi} : K \to \mathbb{C}^2$ is given by the two real embeddings induced by the CM type, and the polarization is induced by the symplectic form E on the lattice: $E(x_1 + x_2\tau, y_1 + y_2\tau) = \mathrm{tr}_{K/\mathbb{Q}}(x_1y_2 - x_2y_1)$. From the definition of ∂_K^{-1} we get indeed that E induces a principal polarization.

Since $\mathrm{SL}_2(\mathcal{O}_K)$ is generated by the matrices $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & \omega \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, the group $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ is generated by the matrices $\begin{pmatrix} 1 & 1/\sqrt{\Delta_K} \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & \omega/\sqrt{\Delta_K} \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1/\sqrt{\Delta_K} \\ \sqrt{\Delta_K} & 0 \end{pmatrix}$.

For $\lambda \in K$ and $\tau = (\tau_1, \tau_2) \in \mathcal{H}_1^2$, we denote

$$\lambda\tau = (\lambda\tau_1, \overline{\lambda}\tau_2), \qquad N(\tau) = \tau_1\tau_2 \qquad \text{and} \qquad \mathrm{tr}(\tau) = \tau_1 + \tau_2.$$

We define σ to be the involution $\sigma : (\tau_1, \tau_2) \in \mathcal{H}_1^2 \mapsto (\tau_2, \tau_1) \in \mathcal{H}_1^2$. We let σ act by conjugation on $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ via $\sigma\gamma\sigma = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$. It is straightforward to check that this is compatible with the action on $\mathcal{H}_1^2$. We call the group $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \rtimes \langle\sigma\rangle$ the symmetric Hilbert modular group. For a function $f : \mathcal{H}_1^2 \to \mathbb{C}$ and $\gamma \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \rtimes \langle\sigma\rangle$ we denote $f^\gamma(\tau) = f(\gamma.\tau)$.

Definition 2.1. Let Γ be a subgroup of $\mathrm{SL}_2(K)$ commensurable with $\mathrm{SL}_2(\mathcal{O}_K)$. A holomorphic function f on $\mathcal{H}_1^2$ is called a *Hilbert modular form of weight k for the subgroup* Γ if it satisfies for any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $\tau = (\tau_1, \tau_2) \in \mathcal{H}_1^2$ the condition $f(\gamma\tau) = N(c\tau+d)^k f(\tau)$. If moreover it satisfies $f(\sigma(\tau)) = f(\tau)$ for all $\tau \in \mathcal{H}_1^2$, then we say that this form is *symmetric.* A *Hilbert modular function* is the quotient of Hilbert modular forms of the same weight and for the same group. We say that this function is symmetric when the forms are, for some choice of forms.

Remark 2.2. A Hilbert modular form f is holomorphic at the set of cusps $\mathrm{SL}_2(\mathcal{O}_K)\backslash\mathbb{P}^1(K) \simeq \mathrm{Cl}(\mathcal{O}_K)$ (see for example [9, Section 1.3] for more details).

For the study of Humbert surfaces in Section 2.4 we will also be interested in symmetric Hilbert modular forms and functions.

2.3 From Hilbert to Siegel

Let $\tau = (\tau_1, \tau_2) \in \mathcal{H}_1^2$, $x \in K$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$. We denote $\tau^* = \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix}$, $x^* = \left(\begin{smallmatrix} x & 0 \\ 0 & \overline{x} \end{smallmatrix}\right)$ and $\gamma^* = \left(\begin{smallmatrix} a^* & b^* \\ c^* & d^* \end{smallmatrix}\right)$. Fix $\{e_1, e_2\}$ a $\mathbb{Z}$-basis of $\mathcal{O}_K = \mathbb{Z} + \omega\mathbb{Z}$ (ω is defined in the beginning of the previous section) and define the matrices $R = \left(\begin{smallmatrix} e_1 & e_2 \\ f_1 & f_2 \end{smallmatrix}\right)$, with $f_i = \overline{e_i}$, and $S = \begin{pmatrix} {}^tR & 0 \\ 0 & R^{-1} \end{pmatrix}$ and the maps

(6)
$$\begin{array}{rccc} \phi_{e_1,e_2}: & \mathcal{H}_1^2 & \rightarrow & \mathcal{H}_2 \\ & \tau & \mapsto & {}^tR\tau^*R \end{array} \quad \text{and} \quad \begin{array}{rccc} \phi_{e_1,e_2}: & \mathrm{SL}_2(K) & \rightarrow & \mathrm{Sp}_4(\mathbb{Q}) \\ & \gamma & \mapsto & S\gamma^*S^{-1}. \end{array}$$

Recall that $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(K) : a, d \in \mathcal{O}_K, b \in 1/\sqrt{\Delta_K}\mathcal{O}_K \text{ and } c \in \sqrt{\Delta_K}\mathcal{O}_K\}$.

Proposition 2.3. *The map ϕ_{e_1,e_2} satisfies:*

- $\phi_{e_1,e_2}^{-1}(\mathrm{Sp}_4(\mathbb{Z})) = \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$*;*
- $\phi_{e_1,e_2}(\gamma \cdot \tau) = \phi_{e_1,e_2}(\gamma) \cdot \phi_{e_1,e_2}(\tau)$ *for all* $\gamma \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ *and* $\tau \in \mathcal{H}_1^2$*;*
- *If f_1, f_2 is another $\mathbb{Z}$-basis of $\mathcal{O}_K$, then there exists some $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ such that for all $\tau \in \mathcal{H}_1^2$, $\phi_{e_1,e_2}(\tau) = \gamma \cdot \phi_{f_1,f_2}(\tau)$;*
- *There exists some $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ such that $\phi_{e_1,e_2}(\sigma(\tau)) = \gamma \cdot \phi_{e_1,e_2}(\tau)$. We denote this γ by M_σ, and this allows us to extend ϕ_{e_1,e_2} to $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \rtimes \langle\sigma\rangle$.*

Proof. See for example [49, Proposition 3.1]. □

Thus, the map ϕ_{e_1,e_2} gives a map from $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)\backslash\mathcal{H}_1^2$ to $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$ which is independent of the choice of the basis of $\mathcal{O}_K$. It also sends τ and $\sigma(\tau)$ to the same point of $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$. Since ϕ_{e_1,e_2} allows us to identify $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ and $\langle\sigma\rangle$ as subgroups of $\mathrm{Sp}_4(\mathbb{Z})$, we will note $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)\sigma$ the group $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \rtimes \langle\sigma\rangle$.

We will often work with the basis $e_1 = 1$ and $e_2 = \omega$. We have $\phi_{1,\omega}(\tau) = \begin{pmatrix} \tau_1+\tau_2 & \tau_1\omega+\tau_2\overline{\omega} \\ \tau_1\omega+\tau_2\overline{\omega} & \tau_1\omega^2+\tau_2\overline{\omega}^2 \end{pmatrix} = \begin{pmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{pmatrix} \in \mathcal{H}_2$ and it satisfies

(7)
$$\begin{array}{rll} \frac{D-1}{4}\Omega_1 + \Omega_2 - \Omega_3 & = 0, & \text{if } D \equiv 1 \bmod 4; \\ D\Omega_1 - \Omega_3 & = 0, & \text{if } D \equiv 2, 3 \bmod 4. \end{array}$$

Moreover, set

(8)
$$M_\sigma = \begin{cases} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix} & \text{if } D \equiv 1 \bmod 4; \\ \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} & \text{if } D \equiv 2, 3 \bmod 4. \end{cases}$$

We have found that the matrix M_σ satisfies

(9)
$$\phi_{1,\omega}(\sigma(\tau)) = M_\sigma \cdot \phi_{1,\omega}(\tau).$$

Consider now $\gamma = \left(\begin{smallmatrix} a+a'\omega & (b+b'\omega)/\sqrt{\Delta_K} \\ \sqrt{\Delta_K}(c+c'\omega) & d+d'\omega \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$. Then

$$\phi_{1,\omega}(\gamma) = \begin{cases} \left(\begin{smallmatrix} a & a' & b' & b+b' \\ (\frac{D-1}{4})a' & a+a' & b+b' & b+(\frac{D+3}{4})b' \\ (\frac{D-1}{4})c'-c & c & d & (\frac{D-1}{4})d' \\ c & c' & d' & d+d' \end{smallmatrix}\right) & \text{if } D \equiv 1 \bmod 4; \\ \\ \left(\begin{smallmatrix} a & a' & b' & b \\ Da' & a & b & Db' \\ Dc' & c & d & Dd' \\ c & c' & d' & d \end{smallmatrix}\right) & \text{if } D \equiv 2, 3 \bmod 4. \end{cases} \tag{10}$$

2.4 Humbert surfaces

Humbert surfaces were first studied by Humbert in [37, 38, 39]. Let $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \mathcal{H}_2$ and $a, b, c, d, e \in \mathbb{Z}$. We call an equation of the form:

$$a\Omega_1 + b\Omega_2 + c\Omega_3 + d(\Omega_2^2 - \Omega_1\Omega_3) + e = 0$$

a *singular relation*. If $\gcd(a, b, c, d, e) = 1$, we say that this relation is *primitive*. Moreover, we define the *discriminant* of a singular relation to be $\Delta = b^2 - 4ac - 4de$.

Theorem 2.4 (Humbert's Lemma). *Let $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right)$ satisfy the singular relation:*

$$a\Omega_1 + b\Omega_2 + c\Omega_3 + d(\Omega_2^2 - \Omega_1\Omega_3) + e = 0$$

of discriminant $\Delta = b^2 - 4ac - 4de$. Then there exists a matrix $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ such that $\gamma \cdot \Omega = \left(\begin{smallmatrix} \Omega'_1 & \Omega'_2 \\ \Omega'_2 & \Omega'_3 \end{smallmatrix}\right)$ satisfies a normalized singular relation of the form:

$$k\Omega'_1 + \ell\Omega'_2 - \Omega'_3 = 0 \tag{11}$$

where k and ℓ are determined uniquely by $\Delta = 4k + \ell$ and $\ell \in \{0, 1\}$.

Proof. See [37, 38, 39] or for example Birkenhake-Wilhelm [4, Proposition 4.5] or Runge [66, Theorem 2]. □

Remark 2.5. Let $\Omega \in \mathcal{H}_2$. It can satisfy many singular relations of different discriminants. If it satisfies a singular relation of discriminant Δ, a constructive algorithm to find γ as in Humbert's Lemma can be found in [4, 66]. Conversely, let $\Omega \in \mathcal{H}_2$ be a matrix equivalent modulo $\mathrm{Sp}_4(\mathbb{Z})$ to a matrix satisfying (11). Then Ω satisfies necessarily a singular relation of discriminant Δ. Note that by Equation (7) a period matrix of the form $\Omega = \phi_{1,\omega}(\tau)$ satisfies a normalized singular relation (11) of discriminant Δ.

Proposition 2.6. *For any $\Delta \equiv 0$ or $1 \bmod 4$, $\Delta > 0$, the set $H_\Delta := \{\{\Omega\} \in \mathrm{Sp}_4(\mathbb{Z}) \backslash \mathcal{H}_2 : \Omega$ satisfies a primitive singular relation of discriminant $\Delta\}$ is a surface which we call the* Humbert surface of discriminant Δ.

Proof. See [4, Corollary 4.6 and Proposition 4.7] or [33, Proposition 2.11]. □

Proposition 2.7. *Let A_Ω be the principally polarized abelian surface associated to $\Omega \in \mathcal{H}_2$. Let also $\Delta \neq \Delta'$ be non-square discriminants. Then:*

- *A_Ω is simple if and only if $\Omega \notin \bigcup_{m>0} H_{m^2}$;*

- *If $\Omega \in H_\Delta$, then* $\mathrm{End}(A_\Omega)$ *contains the order of* $\mathbb{Q}(\sqrt{\Delta})$ *of discriminant* Δ*, i.e., equivalently, there exists a symmetric endomorphism of discriminant* Δ *on* A_Ω*;*
- *if* $\Omega \in H_\Delta \cap H_{\Delta'}$*, then either* A_Ω *is simple and* $\mathrm{End}(A_\Omega) \otimes \mathbb{Q}$ *is a totally indefinite quaternion algebra over* $\mathbb{Q}$*, or* A_Ω *is isogenous to* $E \times E$*, where* E *is an elliptic curve.*

Proof. See [4, Proposition 4.9] or [33, Corollary 2.10, Proposition 2.15]. □

We denote now $\tilde{\Gamma}(1) = \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$. Proposition 2.3 and Equations (7), (8) and (9) say that the images by $\phi_{1,\omega}$ of $\mathcal{H}_1^2$ and of $(\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma)\backslash\mathcal{H}_1^2$ are in the Humbert surface of discriminant Δ_K. This is also true for any ϕ_{e_1,e_2} because the images of τ by $\phi_{1,\omega}$ and by ϕ_{e_1,e_2} are equivalent modulo the action of $\mathrm{Sp}_4(\mathbb{Z})$ (which means that these maps send τ to the same point of the Humbert surface). More precisely, the Hilbert surface maps onto the Humbert surface:

Proposition 2.8. *The maps* ϕ_{e_1,e_2} *of Equation (6) give rise to the following commutative diagram :*

$$\begin{tikzcd}
\tilde{\Gamma}(1)\backslash\mathcal{H}_1^2 \arrow[rd, "\pi"] & \mathcal{H}_1^2 \arrow[l] \arrow[r, "\phi_{e_1,e_2}"] \arrow[d] & \mathcal{H}_2 \arrow[d] \\
 & (\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma)\backslash\mathcal{H}_1^2 \arrow[r, "\rho"] & \mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2
\end{tikzcd}$$

where π *is a map of degree* 2 *and* ρ *is a map generically of degree* 1 *onto the Humbert surface* H_{Δ_K}*.*

Proof. See van der Geer [30, Page 328] for the map ρ and the commutativity of the rectangular part of the diagram. The fact that π is of degree 2 is obvious. It remains to see that $\rho \circ \pi$ is generically of degree 2. But H_{Δ_K} is the locus of principally polarized abelian surfaces (A, θ) with real multiplication by $\mathcal{O}_K$, and the preimages correspond to explicit embeddings $\mu : \mathcal{O}_K \to \mathrm{End}(A)$. Generically there are only two such embeddings which differ by the real conjugation, which corresponds to the action of σ. □

The analytic quotient space $(\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma)\backslash\mathcal{H}_1^2$ is called a *symmetric Hilbert modular surface*; it is birational to the Humbert surface.

Lemma 2.9. *The pullbacks by* ρ *of the Igusa invariants to the symmetric Hilbert modular surface* $(\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma)\backslash\mathcal{H}_1^2$ *generate the function field of symmetric Hilbert modular functions. (These pullbacks can also be seen as the restriction of the Igusa invariants to the Humbert surface).*

Proof. This is a well-known result. We give the proof in Appendix A.1. □

2.5 Symmetric and non symmetric covers of the Humbert surface

We study here the covers of the Hilbert modular surface $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)\backslash\mathcal{H}_1^2$ given by a subgroup $\tilde{\Gamma}$ of finite index in $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$.

When $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, the subgroups $\Gamma(n)$, $\Gamma^0(\ell)$ and $\Gamma(2, 4)$ are standard, and of main interest for modular polynomials of elliptic curves. We want to generalize these notations to the Hilbert modular group. It is easier to define them first in the model of $\mathrm{SL}_2(\mathcal{O}_K)$ acting on $\mathcal{H}^+ \times \mathcal{H}^-$ and then transport them to the model of $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ action on $\mathcal{H}^2$ via the automorphism $\phi_\pm$ of Equation (4).

Definition 2.10. Let

$$\tilde{\Gamma}(n) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K) : a \equiv d \equiv 1 \bmod n,\ b \equiv c \equiv 0 \bmod n \right\}. \tag{12}$$

Define then for $D \equiv 1 \bmod 4$ and $D \equiv 2, 3 \bmod 4$

$$\tilde{\Gamma}(2,4) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \tilde{\Gamma}(2) : b \equiv c \equiv 0 \bmod 4 \right\}, \tag{13}$$

$$\tilde{\Gamma}(2,4) = \left\{ \left(\begin{smallmatrix} a & (b_1+b_2\omega) \\ (c_1+c_2\omega) & d \end{smallmatrix}\right) \in \tilde{\Gamma}(2) : b_2 \equiv c_2 \equiv 0 \bmod 4 \right\} \tag{14}$$

respectively.

By abuse of notation, we use the same notation for their image by $\phi_\pm$:

$$\tilde{\Gamma}(n) = \left\{ \left(\begin{smallmatrix} a & b/\sqrt{\Delta_K} \\ \sqrt{\Delta_K}c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) : a \equiv d \equiv 1 \bmod n,\ b \equiv c \equiv 0 \bmod n \right\}. \tag{15}$$

Define then for $D \equiv 1 \bmod 4$ and $D \equiv 2, 3 \bmod 4$

$$\tilde{\Gamma}(2,4) = \left\{ \left(\begin{smallmatrix} a & b/\sqrt{\Delta_K} \\ \sqrt{\Delta_K}c & d \end{smallmatrix}\right) \in \tilde{\Gamma}(2) : b \equiv c \equiv 0 \bmod 4 \right\}, \tag{16}$$

$$\tilde{\Gamma}(2,4) = \left\{ \left(\begin{smallmatrix} a & (b_1+b_2\omega)/\sqrt{\Delta_K} \\ \sqrt{\Delta_K}(c_1+c_2\omega) & d \end{smallmatrix}\right) \in \tilde{\Gamma}(2) : b_2 \equiv c_2 \equiv 0 \bmod 4 \right\} \tag{17}$$

respectively. Note the subtlety in the definition of $\tilde{\Gamma}(2,4)$ for $D \equiv 2, 3 \bmod 4$.

Remark 2.11. By Serre [68] a group $\tilde{\Gamma}$ of finite index in $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ is necessarily a congruence subgroup, meaning that it contains the congruence subgroup $\tilde{\Gamma}(n)$ for some positive integer n.

Lemma 2.12. *Let $\mathcal{G}$ be a subgroup of $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \rtimes \langle\sigma\rangle$ of finite index. If $\sigma \notin \mathcal{G}$ then $\mathcal{G} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$. Otherwise $\mathcal{G} = \tilde{\Gamma} \rtimes \langle\sigma\rangle$ for a subgroup $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ of finite index and normalized by σ (meaning that $\tilde{\Gamma}$ is stable under the real conjugation). In the latter case we say that $\mathcal{G}$ is symmetric.*

Proof. Indeed as a set it is easy to see that if $\sigma \in \mathcal{G}$, then $\mathcal{G} = \tilde{\Gamma} \cup \tilde{\Gamma}\sigma$ for a subgroup $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$. It remains to check that σ normalizes $\tilde{\Gamma}$. But since $\mathcal{G}$ is a group, $\overline{\tilde{\Gamma}} = \sigma\tilde{\Gamma}\sigma^{-1} \subset \mathcal{G}$, so $\overline{\tilde{\Gamma}} = \tilde{\Gamma}$. □

Definition 2.13. We denote by $\mathbb{C}_{\mathcal{G}}$ the field of meromorphic functions of $\mathcal{H}_1^2$ invariant under the action of $\mathcal{G}$. It is the function field of the Hilbert surface $H_{\mathcal{G}} = \mathcal{G}\backslash\mathcal{H}_1^2$.

Remark 2.14. $H_{\mathcal{G}}$ admits a Baily-Borel compactification [1], which in turn admits a smooth birational model. In this article we only work with functions of the Hilbert modular function field, so only up to birational equivalence, so we do not distinguish between these models.

Consider now Γ a subgroup of $\mathrm{Sp}_4(\mathbb{Z})$ of finite index. The projection $\pi : \Gamma\backslash\mathcal{H}_2 \to \mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$ is a finite map. Recall that if Δ_K is the discriminant of $\mathcal{O}_K$, we denote by H_{Δ_K} the Humbert surface of discriminant Δ_K. An irreducible component of $H_{\Delta_K}^{\Gamma} = \pi^{-1}(H_{\Delta_K})$ in $\Gamma\backslash\mathcal{H}_2$ is called a *Humbert surface component.*

Let $\mathcal{G} = \phi_{1,\omega}^{-1}(\Gamma)$ and $\tilde{\Gamma} = \mathcal{G} \cap \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$. If the matrix M_σ of Equation (8) is not in Γ, then $\mathcal{G} = \tilde{\Gamma}$, otherwise $\mathcal{G} = \tilde{\Gamma} \cup \tilde{\Gamma}\sigma$. By Proposition 2.8 we get that the following diagram is commutative:

$$\begin{tikzcd}
\mathcal{H}_1^2 \arrow[r, "\phi_{1,\omega}"] \arrow[d] & \mathcal{H}_2 \arrow[d] \\
\mathcal{G}\backslash\mathcal{H}_1^2 \arrow[r, "\rho"] & \Gamma\backslash\mathcal{H}_2
\end{tikzcd}$$

where ρ is a map generically of degree 1 onto its image, which is a Humbert surface component $H_{\Delta_K}^{\mathcal{G}}$.

Proposition 2.15. *Suppose that $i_1, \ldots, i_k$ are modular functions for Γ which generate the function field $\mathbb{C}(\Gamma)$. And suppose that the restrictions of $i_1, \ldots, i_k$ do not have poles at the generic points of the component $H_{\Delta_K}^{\mathcal{G}}$ so they are well defined on an open subset of $H_{\Delta_K}^{\mathcal{G}}$. Then $\rho^* i_1, \ldots, \rho^* i_k$ generate the function field $\mathbb{C}_{\mathcal{G}}$ of Hilbert modular functions.*

In particular if $M_\sigma \in \Gamma$, the pullbacks generate the symmetric Hilbert modular functions for $\tilde{\Gamma}$; while if $M_\sigma \notin \Gamma$ the pullbacks generate the full function field $\mathbb{C}_{\tilde{\Gamma}}$ of Hilbert modular functions for $\tilde{\Gamma}$.

Proof. This is identical to the proof of Lemma 2.9 (see Lemma A.1 in Appendix A.1). □

We have seen that by Lemma 2.9 we can take $\tilde{\mathfrak{j}}_k = \phi_{1,\omega}^* \mathfrak{j}_k$, for $k = 1, 2, 3$, as invariants on a symmetric Hilbert modular surface. These functions are algebraically dependent. Similarly, we will apply Proposition 2.15 to the functions $\tilde{b}_k = \phi_{1,\omega}^* b_k$ and $\tilde{r}_k = \phi_{1,\omega}^* r_k$ for $k = 1, 2, 3$. Recall Equations (1), (2) and (3) for the definitions of these invariants.

Theorem 2.16. *The functions $\tilde{r}_k$ and $\tilde{b}_k$ for $k = 1, 2, 3$ are generators for the field of Hilbert modular functions invariants by $\tilde{\Gamma}(2)$ and $\tilde{\Gamma}(2,4)$, if $D \equiv 1 \bmod 4$, and by $\tilde{\Gamma}(2) \cup \tilde{\Gamma}(2)\sigma$ and $\tilde{\Gamma}(2,4) \cup \tilde{\Gamma}(2,4)\sigma$, if $D \equiv 2, 3 \bmod 4$, respectively.*

Proof. By Equation (10), we have that $\phi_{1,\omega}^{-1}(\Gamma(2,4)) \cap \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) = \tilde{\Gamma}(2,4)$. Thus, the functions $\tilde{b}_k$ are modular for $\tilde{\Gamma}(2,4)$. Moreover, if $D \equiv 2, 3 \bmod 4$, then these functions are also modular for $\tilde{\Gamma}(2,4)\sigma$, as the matrix M_σ of Equation (8) belongs to $\Gamma(2,4)$. Similarly, $\phi_{1,\omega}^{-1}(\Gamma(2)) \cap \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) = \tilde{\Gamma}(2)$ and the $\tilde{r}_k$ are modular for $\tilde{\Gamma}(2)$ and also by $\tilde{\Gamma}(2)\sigma$ when $D \equiv 2, 3 \bmod 4$. We conclude using Proposition 2.15 and the fact that the b_i (resp. r_i) are generators for the field of Siegel modular functions invariants by $\Gamma(2,4)$ (resp. $\Gamma(2)$). The pullbacks are indeed well defined because the denominators of these invariants divide χ_{10}, so the locus of the denominators are components above the Humbert surface H_1. □

We refer to Appendix A.5 for the index of the subgroups $\tilde{\Gamma}(2)$ and $\tilde{\Gamma}(2,4)$ of $\tilde{\Gamma}(1)$, the number of Humbert surface components for $\Gamma(2)$ and for $\Gamma(2,4)$ and equations of the Humbert component corresponding to the image of $\phi_{1,\omega}$ for $\Gamma(2,4)$, $\Gamma(2)$ and $D \in \{2, 3, 5\}$.

3 Equations for Hilbert surfaces

3.1 Generators of the field of Hilbert modular functions

Let $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ be a subgroup of finite index. We denote by $H_{\tilde{\Gamma}} = \tilde{\Gamma}\backslash\mathcal{H}_1^2$ the corresponding Hilbert modular surface, and $H_{\tilde{\Gamma},\sigma} = (\tilde{\Gamma} \cup \tilde{\Gamma}\sigma)\backslash\mathcal{H}_1^2$ the corresponding symmetric

Hilbert modular surface. We let $\mathcal{G} = \tilde{\Gamma}$ in the first case, and $\mathcal{G} = \tilde{\Gamma} \cup \tilde{\Gamma}\sigma$ in the second one. Recall that $\mathbb{C}_{\mathcal{G}}$ is defined in Definition 2.13.

Proposition 3.1. *Let $H_{\mathcal{G}}$ be a Hilbert surface as above. Then $\mathbb{C}_{\mathcal{G}} = \mathbb{C}(i_1, i_2, i_3)$ where i_1 and i_2 are symmetric Hilbert modular functions for $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ and i_3 is algebraic over $\mathbb{C}(i_1, i_2)$. Moreover i_3 is symmetric if and only if $H_{\mathcal{G}}$ is symmetric.*

Proof. Since $H_{\mathcal{G}}$ is a surface, the field of Hilbert modular functions $\mathbb{C}_{\mathcal{G}}$ is of transcendence degree 2. By the primitive element theorem, $\mathbb{C}_{\mathcal{G}}$ is generated by two transcendental functions i_1, i_2 (called primary invariants) and a third one i_3 algebraic over $\mathbb{C}(i_1, i_2)$ (called a secondary invariant). Since $\mathbb{C}_{\mathcal{G}}$ is algebraic over $\mathbb{C}_{\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)\sigma}$, we can take $i_1, i_2 \in \mathbb{C}_{\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)\sigma}$. They are then symmetric, so $H_{\mathcal{G}}$ is symmetric if and only if i_3 is symmetric. □

Usually working with symmetric Hilbert modular surfaces yields invariants easier to compute than with non-symmetric surfaces. For instance while $H_{\tilde{\Gamma}(1)}$ is not often a rational surface according to Theorem A.16, from Elkies and Kumar [19] we have that $H_{\tilde{\Gamma}(1),\sigma}$ is a rational surface for every fundamental discriminant $\Delta_K < 100$. Hence for these surfaces we need only two birational primary invariants to define the modular polynomials. The drawback of symmetric modular surfaces is that they can not be used for all the applications of isogenies as we will see in Example 4.17.

Note that by the general theory of Shimura varieties [56] $H_{\mathcal{G}}$ has a (birational) model defined over an algebraic number field F. In fact by van der Geer [31, Section X.4], the Hilbert surface can be defined over $\mathbb{Q}$, and its connected components over an abelian extension of $\mathbb{Q}$. In particular if the invariants i_1, i_2, i_3 come from this model defined over F, the equation $E(i_1, i_2, i_3) = 0$ can be written as $E = \sum c_k(i_1, i_2) i_3^k$, where $c_k \in F(i_1, i_2)$.

The lemma below show that if the Hilbert invariants have their Fourier coefficients in a number field F then they are defined over F. In practice the invariants we use for computation (pullbacks of Igusa invariants, pullbacks of theta functions, Gundlach invariants) even have Fourier coefficients in $\mathbb{Q}$.

Lemma 3.2. *Let $i_1, \dots, i_n$ be Hilbert modular functions generating the Hilbert modular field $\mathbb{C}_{\mathcal{G}}$, and let $\mathcal{E}$ be the ideal of equations between the i_k and $H_{\mathcal{E}}$ the corresponding birational model of $H_{\mathcal{G}}$. If the Fourier coefficients of each i_k are in F, then the ideal $\mathcal{E}$ is generated by equations with coefficients in F, so $H_{\mathcal{E}}$ has a model over F.*

Proof. The proof uses a similar argument to Bröker and Lauter in [5, Theorem 5.2]. If we fix a monomial ordering, the generators of $\mathcal{E}$ are uniquely determined when they form a Gröbner basis. This Gröbner basis induces a set of linear relations on the Fourier coefficients of the i_k from which its coefficients (as unknowns) are the unique solution. But since the Fourier coefficients lie in F, this linear system is defined over F, so the solution is defined over F. □

Remark 3.3. The condition on the Fourier coefficients is a sufficient condition, but far from a necessary condition. In general the field of definition of the cusps will be larger than the field of definition of the Hilbert surface, so to know if the equations between the Hilbert functions i_k as in Lemma 3.2 will lie in a polynomial ring over a proper subfield of F, one needs to look at the Galois action on the Fourier coefficients (which lie in F by hypothesis).

3.2 Fast evaluation of Hilbert modular functions

We will compute modular polynomials using an evaluation/interpolation approach. To be able to compute these polynomials in time quasi linear in their size, we need two properties for the invariants used:

- For the evaluation, given $\tau = (\tau_1, \tau_2) \in \mathcal{G}\backslash\mathcal{H}_1^2$ we need to be able to compute the invariants $(i_1(\tau), i_2(\tau), i_3(\tau)) \in \mathbb{C}^3$ in time quasi-linear in the required precision;
- Given the value of $(i_1(\tau), i_2(\tau), i_3(\tau)) \in \mathbb{C}^3$ we need to be able to recover the matrix $\tau \in \mathcal{G}\backslash\mathcal{H}_1^2$ in time quasi-linear in the required precision. This allows us to have well-chosen evaluation points so that we can do the interpolation of trivariate rational fractions.

Recall that the notation $\tilde{O}(N)$ means $O(N)$ ignoring logarithmic factors. By quasi-linear complexity in N, we mean a complexity in $\tilde{O}(N)$.

Recall that by Theorem 2.16, the functions $\tilde{b}_k$, for $k = 1, 2, 3$, generate $\mathbb{C}_{\tilde{\Gamma}(2,4)}$ when $D \equiv 1 \bmod 4$ and $\mathbb{C}_{\tilde{\Gamma}(2,4)\cup\tilde{\Gamma}(2,4)\sigma}$ when $D \equiv 2, 3 \bmod 4$. Let $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ be a subgroup of finite index such that $\tilde{\Gamma} \supset \tilde{\Gamma}(2,4)$. Let $\mathcal{G} = \tilde{\Gamma}$ or $\mathcal{G} = \tilde{\Gamma}\cup\tilde{\Gamma}\sigma$, and i_1, i_2, i_3 be as in Proposition 3.1 and such that $F(H_\mathcal{G}) = F(i_1, i_2, i_3)$, where F is the field of definition of $H_\mathcal{G}$.

Then i_1 and i_2 can be expressed as rational functions in the $\tilde{b}_k$: $i_k = R_k(\tilde{b}_1, \tilde{b}_2, \tilde{b}_3)$. This is also true for i_3 unless $\mathcal{G} = \tilde{\Gamma}$ and $D \equiv 2, 3 \bmod 4$ because then the $\tilde{b}_k$ are symmetric while i_3 is not, and thus cannot be expressed as a rational function in the $\tilde{b}_k$. But in this case, $i_3 + \sigma(i_3)$ and $i_3\sigma(i_3)$ are symmetric, and can be expressed as rational functions $R_{3,1}$ and $R_{3,2}$ in the $\tilde{b}_k$.

Similarly, by Lemma 2.9, the pullbacks of the Igusa invariants generate the function field of symmetric Hilbert modular functions. Thus there are rational fractions in i_1, i_2, i_3 giving the pullbacks of the Igusa invariants.

Theorem 3.4. *Let $\tilde{\Gamma}$, $\mathcal{G}$ and i_1, i_2, i_3 be as above. Assume that we know R_1, R_2, and R_3 or $R_{3,1}$ and $R_{3,2}$ according to the cases discussed above, and the rational fractions giving the pullbacks of the Igusa invariants from i_1, i_2, i_3. Assume that in the case $\mathcal{G} = \tilde{\Gamma}$ and $D \equiv 2, 3 \bmod 4$, we are able to evaluate i_3 at small precision (knowing the first Fourier coefficients for example). Then, not taking rounding errors into account, both the evaluation map $\mathcal{G}\backslash\mathcal{H}_1^2 \to \mathbb{C}^3, \tau \mapsto (i_1(\tau), i_2(\tau), i_3(\tau))$ and the inversion map (the computation of a preimage of a point of the image of the evaluation map) can be computed in time quasi-linear in the precision.*

Proof. We first do the symmetric case.

By Enge and Thomé in [22, Theorem 5.8, Remark 5.9], given a Siegel matrix $\Omega \in \mathcal{H}_2$, evaluating the $b_k(\Omega)$ can be done in time quasi-linear in the precision (see also [16, 45, 47] on this subject), if we neglect the loss of precision. Given a period matrix $\tau \in \mathcal{H}_1^2$, one can use the map $\phi_{1,\omega}$ from Section 2.3 to get $\Omega = \phi_{1,\omega}(\tau) \in \mathcal{H}_2$, and then compute the values of $\tilde{b}_k(\tau) = b_k(\phi_{1,\omega}(\tau))$ in time quasi-linear, and finally deduce the values of $i_k(\tau) = R_k(\tilde{b}_1(\tau), \tilde{b}_2(\tau), \tilde{b}_3(\tau))$.

For the inverse, the (restriction of the) Igusa invariants $\tilde{\mathfrak{j}}_1, \tilde{\mathfrak{j}}_2, \tilde{\mathfrak{j}}_3$ can also be expressed as rational functions in the invariants i_1, i_2, i_3. From the values $(i_1(\tau), i_2(\tau), i_3(\tau))$, one can then compute $(\tilde{\mathfrak{j}}_1(\tau), \tilde{\mathfrak{j}}_2(\tau), \tilde{\mathfrak{j}}_3(\tau))$. Using [16] (in particular [16, Théorème 9.3] and [16, Pages 200 and 223] of Dupont), we compute in time quasi-linear in N an approximation to precision N of a matrix $\Omega \in \mathcal{H}_2$ which is equivalent modulo $\mathrm{Sp}_4(\mathbb{Z})$ to $\phi_{1,\omega}(\tau)$. The matrix Ω lies in the Humbert surface of discriminant Δ_K, so it satisfies a singular relation. By Section 2.4 there is a constructive algorithm to find $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ such that $\gamma.\Omega$ satisfies a normalized singular relation. By Section 2.3, $\gamma.\Omega$ is in the image of $\phi_{1,\omega}$, so one can compute $\tau' = \phi_{1,\omega}^{-1}(\gamma.\Omega) \in \mathcal{H}_1^2$. It then only remains to compute all classes of τ' under the action of the finite group $\mathcal{G}\backslash\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ to find a τ'' in the same class as τ modulo $\mathcal{G}$.

For the non symmetric case, recovering τ modulo $\mathcal{G}$ from the values of the invariants uses the same algorithm. The only difficulty is for the evaluation in the case $D \equiv 2, 3 \bmod 4$ because in this case the $\tilde{b}_k$ are symmetric while i_3 is not. However, since $t = i_3 + \sigma(i_3)$ and $n = i_3\sigma(i_3)$ are symmetric, one can evaluate $t(\tau)$ and $n(\tau)$ in time quasi-linear using the techniques above for the symmetric case. Thus $i_3(\tau)$ is a root of $X^2 - t(\tau)X + n(\tau)$. The two roots can be computed in quasi-linear time in the precision, and choosing the correct one only requires an evaluation with small precision of i_3. □

Remark 3.5. Computing the rational functions is just a precomputation step and this computation does not affect the asymptotic complexity. They can be computed by linear algebra on the Fourier coefficients, or by linear algebra on the evaluation of these modular functions at several period matrices τ (where the evaluation uses the slow summation series given by the Fourier coefficients).

In practice, it is important to optimize the speed of the computation of the invariants i_k as rational functions of the $\tilde{b}_k$ to be able to do concrete computations. Rather than using linear algebra, one can use an interpolation approach. This approach requires to be able to obtain, from the values $(b_1(\Omega), b_2(\Omega), b_3(\Omega))$, a period matrix Ω' equivalent to Ω modulo $\Gamma(2,4)$, at some given precision. We know how to do it by [55, 16]. It also requires the equation $P(\tilde{b}_1, \tilde{b}_2, \tilde{b}_3) = 0$ of the Humbert component described by the $\tilde{b}_k$. We refer to Section 3.3 for more details about the interpolation.

Likewise, to recover τ, rather than expressing the Igusa invariants j_k in terms of the Hilbert invariants i_k, one could simply use Newton's method to invert the equations $i_k = R_k(\tilde{b}_1, \tilde{b}_2, \tilde{b}_3), P(\tilde{b}_1, \tilde{b}_2, \tilde{b}_3) = 0$ for $k = 1, 2, 3$ to recover the values of the $\tilde{b}_k$ hence the matrix Ω, hence the matrix τ.

Remark 3.6. In the first paragraph of the second page of [47] about the computation of theta functions in genus $g > 1$ in quasi-linear time, Labrande and Thomé explain that they deliberately omit dealing with the precision losses because they expect that the loss of precision is not significant asymptotically. Indeed, this is what the analysis done by Labrande in genus $g = 1$ in [46] concludes.

3.3 Interpolation by Hilbert modular functions

Let $H_{\mathcal{G}}$ be a Hilbert surface defined over F of level $\mathcal{G} = \tilde{\Gamma}$ or $\mathcal{G} = \tilde{\Gamma} \cup \tilde{\Gamma}\sigma$, and c a Hilbert modular function in $F(H_{\mathcal{G}})$. We assume that the invariants i_1, i_2, i_3 are such that the map $\tau \in \mathcal{G}\backslash\mathcal{H}_1^2 \to (i_1(\tau), i_2(\tau), i_3(\tau))$ can be inverted in time quasi-linear (see Theorem 3.4) at the working precision. We explain how to get a fast interpolation algorithm to express c as a rational function in i_1, i_2, i_3. (Without the above property, one can still do linear algebra on the Fourier coefficients or the evaluations, which gives a slow interpolation algorithm). We assume that we have a quasi-linear time algorithm in the precision of the computations to evaluate c.

This interpolation algorithm will be used to compute the modular polynomials. Indeed, we will see that to compute them, we will have to interpolate bivariate or trivariate rational functions, that we can evaluate at any point (see the proof of Theorem 3.11 for the evaluation).

Case where $H_{\mathcal{G}}$ is a rational surface. In this case, $F(H_{\mathcal{G}})$ can be written as $F(J_1, J_2)$, using only two primary invariants. Thus c is a bivariate rational function in J_1 and J_2. The interpolation of c is explained in [55, Section 2], where a complexity analysis is given. We explain it briefly. We compute $c(J_1, J_2)$ by computing first by interpolation $c(J_1, J_1J_2)$ and then by substituting J_2 with J_2/J_1. Assume that we can write

$$c(J_1, J_1J_2) = \frac{A(J_1, J_2)}{B(J_1, J_2)} = \frac{\sum_{m=0}^{d^A_{J_1}} \sum_{n=0}^{d^A_{J_2}} a_{m,n} J_1^m J_2^n}{\sum_{m=0}^{d^B_{J_1}} \sum_{n=0}^{d^B_{J_2}} b_{m,n} J_1^m J_2^n} = \frac{\sum_{m=0}^{d^A_{J_1}} a_m(J_2) J_1^m}{\sum_{m=0}^{d^B_{J_1}} b_m(J_2) J_1^m},$$

such that $b_0(J_2) = 1$ (this is always possible because we consider $c(J_1, J_1J_2)$ and not $c(J_1, J_2)$ except when $b_0(J_2) = 0$ in which case we interpolate $c(J_1 + t_0, J_1J_2 + t_1)$ instead, for some integers t_0, t_1). Denote by d^A_T the total degree of the numerator of $c(J_1, J_2)$, i.e. $d^A_{J_1}$, and similarly for B. Find points $z_m \in \mathcal{H}_1^2$ for $m = 1, \dots, d^A_T + d^B_T + 2$ such that $(J_1(z_m), J_2(z_m))$ is of the form (u_m, vu_m) for $u_m \in \mathbb{C}$ and for a fixed $v \in \mathbb{C}$ (this is where we need the inversion map). Interpolate to find the univariate rational fraction $c(J_1, vJ_1)$ and write this fraction such that the coefficient of degree 0 of the denominator is 1. Thus we know the values $a_m(v)$ and $b_m(v)$ (this would not have been possible if we had considered $c(J_1, J_2)$ directly). Compute in this way the fractions $c(J_1, v_nJ_1)$ for $n = 1, \dots, \max(d^A_{J_2}, d^B_{J_2}) + 1$. Interpolate by Lagrange's or Newton's method the univariate polynomials a_m and b_m to obtain $c(J_1, J_1J_2)$.

In practice for the modular polynomials the coefficients of the bivariate rational fractions will be defined over $\mathbb{Q}$. So the computations are done at precision N which has to be large enough so that we can recognize the coefficients of the bivariate rational fractions as algebraic numbers in $\mathbb{Q}$ using a continuous fraction algorithm. We do not usually know any bounds for the precision so that in practice we double the precision until we manage to find a sufficient precision to compute the modular polynomials. The complexity of the interpolation of a bivariate rational fraction is $\tilde{O}(d_T d_{J_2} N)$, where $d_T = \max(d^A_T, d^B_T)$ and $d_{J_2} = \max(d^A_{J_2}, d^B_{J_2})$.

General case. Here, we have three invariants i_1, i_2, i_3 where i_1 and i_2 are primary, and i_3 is a secondary invariant, so there is an equation $E(i_1, i_2, i_3) = 0$ describing the surface $H_{\mathcal{G}}$.

Like in the previous case and as in [55, Section 2], we would like to work with points $z_j \in \mathcal{H}_1^2$ with the property that $(i_1(z_j), i_2(z_j), i_3(z_j))$ is of the form (u_m, v_nu_m, w_ru_m), where u_m, v_n, $w_r \in \mathbb{C}$ and the subscripts m, n and r vary from 1 to the maximal degree the variables i_1, i_2 and i_3 appear. But this is not possible because of the equation E that i_1, i_2, i_3 have to satisfy. Indeed, for fixed values (u_m, v_nu_m) such that $u_m = i_1(z)$, $v_nu_m = i_2(z)$ for some $z \in \mathcal{H}_1^2$, the values that $i_3(z)$ can take are determined (moreover, they will not be of the form w_ru_m and the number of values will be less than the degree in i_3). A solution to this problem consists in remarking that $F(i_1, i_2, i_3) = F(i_1, i_2)[X_3]/(E(i_1, i_2, X_3))$. Thus the modular function c can be written as $c(i_1, i_2, i_3) = \sum_{i=0}^{d-1} c_i(i_1, i_2) i_3^i$, where d is the degree in which the variable i_3 appears in E and $c_i \in F(i_1, i_2)$.

Assume as in the previous case that we have an algorithm to evaluate c at points in $\mathcal{H}_1^2$. The interpolation is done as follows. For sufficiently many values u_m and v_n, compute the d roots w_r of $E(u_m, v_nu_m, X_3)$. For $r = 1, \dots, d$, find $z_r \in \mathcal{H}_1^2$ such that $(i_1(z_r), i_2(z_r), i_3(z_r)) = (u_m, v_nu_m, w_r)$ and evaluate c at z_r to obtain $c(z_r) = \sum_{i=0}^{d-1} c_i(u_m, v_nu_m) w_r^i$. Since $w_r = i_3(z_r)$, we first interpolate c as a univariate polynomial in i_3 by interpolating on the d values w_r to recover the d coefficients $c_i(u_m, v_nu_m)$. This allows us to evaluate the bivariate rational functions $c_i(i_1, i_2)$ at a given point z_r. It remains to do the interpolation of the coefficients c_i

to recover them as rational functions in i_1, i_2 as was done in the previous case, where $H_{\mathcal{G}}$ was a rational surface. We summarize this discussion by the following theorem.

Theorem 3.7. *Let $\mathcal{G}$ be a subgroup of finite index in $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)\sigma$. Let N be a precision for the computations. Let i_1, i_2, i_3 generating $\mathbb{C}_{\mathcal{G}}$ be such that a preimage at precision N of the image of a point by the evaluation map $\tau \in \mathcal{G}\backslash\mathcal{H}_1^2 \to (i_1(\tau), i_2(\tau), i_3(\tau))$ can be found in time quasi-linear in N. Let $E(i_1, i_2, i_3)$ be the equation describing the Hilbert surface $H_{\mathcal{G}}$, and let d_E be the degree $\deg_{i_3}(E)$ of i_3 in E.*

Let c be a Hilbert modular function in $\mathbb{C}_{\mathcal{G}}$. We represent it in the form $c(i_1, i_2, i_3) = \sum_{k=0}^{d_E-1} c_k(i_1, i_2) i_3^k$, where $c_k(i_1, i_2) \in \mathbb{C}(i_1, i_2)$ are bivariate rational functions. We let d_T be the maximal total degree of all the coefficients c_k (where the degree of a rational function is the maximum of the degree of its numerator and denominator), and d_{i_2} the maximal degree in i_2 of the coefficients c_k.

Assume that we have a quasi-linear time algorithm in the precision N taking $\tau \in \mathcal{H}_1^2$ and N as inputs and returning the evaluation of c at τ with precision N. Assume we know d_T and d_{i_2} and N is large enough so that the interpolations give the correct coefficients $c_k(i_1, i_2)$ up to the precision. Then, not taking rounding errors into account, the coefficients c_k can be computed in precision N in time $\tilde{O}(d_E d_T d_{i_2} N)$.

Assume furthermore that the c_k lie in $F(i_1, i_2)$ for some number field F. Then the coefficients c_k can be recovered exactly in time $\tilde{O}(d_E d_T d_{i_2} N)$ if N is large enough for the coefficients to be recovered exactly using the Lenstra-Lenstra-Lovász (LLL) algorithm.

Proof. Indeed the evaluation of c will be executed $O(d_E d_T d_{i_2})$ times and we will interpolate $O(d_E)$ bivariate rational functions and do $O(d_T d_{i_2})$ interpolations of a univariate polynomial. The complexity is then

$$O(d_E d_T d_{i_2}) + O(d_E)\tilde{O}(d_T d_{i_2} N) + O(d_T d_{i_2})\tilde{O}(d_E N) \subset \tilde{O}(d_E d_T d_{i_2} N). \tag{18}$$

Given a coefficient $c_k \in \mathbb{C}$ computed at precision N, if the c_k lie in $F(i_1, i_2)$, where $F \subset \mathbb{C}$ is a number field, then one can use the LLL algorithm [51] to recover $c_k \in F$. More precisely, if h is the maximal (logarithmic) height of the coefficients c_k seen in $\mathbb{C}$, then N can be bounded by a term in $O(h)$. Using fast versions of LLL this reconstruction step can be done in time $\tilde{O}(N)$ (according to Novocin, Stehlé and Villard [62]).

□

Remark 3.8. In practice, the computation of d_T, d_{i_2} and N is a precomputation step. We fix values for them and try to do the computations. If it fails, we double each value and try again. The exact values of d_T and d_{i_2} can be found in this way.

More generally a similar technique could be used if we had several secondary invariants $i_3, i_4, \ldots i_\ell$. There is no unique expression of c in terms of the i_k due to the equations between the invariants i_k. But for the interpolation to work we need to interpolate the same rational function expression. A solution is to fix a monomial ordering, since this defines a unique rational function expressing c modulo the corresponding Gröbner basis. As long as the partial evaluation of the Gröbner basis corresponds to the Gröbner basis of the partial evaluation of the equation (see [2, 43]), the interpolation step will interpolate the correct expression of the rational function.

3.4 Equations for covers of Hilbert surfaces

Let $\mathcal{G}_2 \subset \mathcal{G}_1 \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)\sigma$ be congruence subgroups. Then $\mathcal{H}_{\mathcal{G}_2} \to \mathcal{H}_{\mathcal{G}_1}$ is a covering. Let i_1, i_2, i_3 be Hilbert modular functions such that $\mathbb{C}_{\mathcal{G}_1} = \mathbb{C}(i_1, i_2, i_3)$ and j_1, j_2, j_3 be Hilbert modular functions such that $\mathbb{C}_{\mathcal{G}_2} = \mathbb{C}(j_1, j_2, j_3)$.

To describe the cover $\mathcal{H}_{\mathcal{G}_2} \to \mathcal{H}_{\mathcal{G}_1}$ we need to give the full set of relations between $i_1, i_2, i_3, j_1, j_2, j_3$. To be more precise, as always in this text we work up to birational equivalence, and i_1, i_2, i_3 only give an embedding of an open subset of $\mathcal{H}_{\mathcal{G}_1}$, and similarly for j_1, j_2, j_3. To describe the full cover we would potentially need to give the relations between more modular functions invariant by $\mathcal{G}_1$ (respectively $\mathcal{G}_2$), but these relations can be computed with the same tool as for the relations between $i_1, i_2, i_3, j_1, j_2, j_3$.

Let i_1, i_2, i_3 be generators of the Hilbert modular field $\mathbb{C}_{\mathcal{G}_1}$ such that the evaluation and its inverse can be computed in time quasi-linear (see for instance Theorem 3.4).

Let j be a generator of the field extension $\mathbb{C}_{\mathcal{G}_2}/\mathbb{C}_{\mathcal{G}_1}$. Such a generator always exists by the primitive element theorem. The cover $\mathcal{H}_{\mathcal{G}_2} \to \mathcal{H}_{\mathcal{G}_1}$ is then (up to birationality) uniquely described by

- the minimal polynomial $\Phi_j \in \mathbb{C}_{\mathcal{G}_1}[X]$ of j over $\mathbb{C}_{\mathcal{G}_1}$;
- and polynomials $Q_k \in \mathbb{C}_{\mathcal{G}_1}[X]$ such that $j_k = Q_k(j)$.

In practice it is more convenient to use the polynomial $\Psi_k \in \mathbb{C}_{\mathcal{G}_1}[X]$ of minimal degree such that $j_k \Phi_j'(j) = \Psi_k(j)$ than the polynomials Q_k. The polynomial Ψ_k is called the Hecke representation of j_k and is more convenient for computations than Q_k because it has smaller coefficients [29, Section 3].

Lemma 3.9. *The polynomial Ψ_k is $\Psi_k(X) = \sum_{\gamma \in \mathcal{G}_2 \backslash \mathcal{G}_1} j_k^\gamma \Phi_j(X)/(X - j^\gamma)$.*

Proof. Let M/K be a finite Galois extension with Galois group G, and for $f \in M$ and $\gamma \in G$ denote by f^γ the action $\gamma.f$ of γ on f. Let $G_2 \subset G_1 \subset G$ and let $K_2 = M^{G_2}$, $K_1 = M^{G_1}$. Let j be a generator of K_2/K_1; then its minimal polynomial is $\Phi(X) = \prod_{\gamma \in G_2 \backslash G_1}(X - j^\gamma)$. Let $J \in K_2$ and let $Q \in K_1[X]$ be the polynomial of minimal degree such that $J = Q(j)$. Since $J^\gamma = Q(j^\gamma)$, we can use Lagrange interpolation to find Q.

Indeed, evaluating $\sum_{\delta \in G_2 \backslash G_1} J^\delta \prod_{\delta' \neq \delta}(X - j^{\delta'})/(j^\delta - j^{\delta'})$ at j^γ gives J^γ. Now, this expression is equal to $\sum_{\delta \in G_2 \backslash G_1} J^\delta \prod_{\delta' \neq \delta}(X - j^{\delta'})/\Phi'(j^\delta) = \sum_{\delta \in G_2 \backslash G_1} J^\delta \Phi(X)/((X - j^\delta)\Phi'(j^\delta))$ and we deduce that taking $\Psi(X) = \sum_{\delta \in G_2 \backslash G_1} J^\delta \Phi(X)/(X - j^\delta)$, we have the property $J^\gamma \Phi'(j^\gamma) = \Psi(j^\gamma)$.

We apply this to the extension $\mathbb{C}_{\tilde{\Gamma}(n)}/\mathbb{C}_{\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)\sigma}$ where $\tilde{\Gamma}(n)$ is a congruence subgroup included in $\mathcal{G}_2$. Indeed this is a Galois extension of Galois group $\tilde{\Gamma}(n) \backslash (\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)\sigma)$, and we apply the result above to $G_1 = \tilde{\Gamma}(n) \backslash \mathcal{G}_1$ and $G_2 = \tilde{\Gamma}(n) \backslash \mathcal{G}_2$ with the notations of the Lemma. □

Theorem 3.10. *Let $i_1, i_2, i_3, j, j_1, j_2, j_3$ be Hilbert modular functions such that $\mathbb{C}_{\mathcal{G}_1} = \mathbb{C}(i_1, i_2, i_3)$ and $\mathbb{C}_{\mathcal{G}_2} = \mathbb{C}_{\mathcal{G}_1}(j) = \mathbb{C}(j_1, j_2, j_3)$. Let E be the equation $E(i_1, i_2, i_3) = 0$ of the surface birational to $\mathcal{H}_{G_1}$ described by i_1, i_2, i_3, and let d be the degree $\deg_{i_3}(E)$ of i_3 in E. Assume that all these modular functions have Fourier coefficients in an algebraic number field $F \subset \mathbb{C}$.*

Let $\Phi(X, i_1, i_2, i_3) = \prod_{\gamma \in \mathcal{G}_2 \backslash \mathcal{G}_1}(X - j^\gamma) = X^L + \sum_{m=0}^{L-1} c_m(i_1, i_2, i_3) X^m$ be the minimal polynomial of j over $\mathbb{C}_{\mathcal{G}_1}$, where $L = \#\mathcal{G}_2 \backslash \mathcal{G}_1$. Let $\Psi_k \in \mathbb{C}_{\mathcal{G}_1}[X]$ be the polynomial given in

Lemma 3.9 for j_k. A birational model of the cover $\mathcal{H}_{\mathcal{G}_2} \to \mathcal{H}_{\mathcal{G}_1}$ is described by the equations

$$\Phi(j) = 0, \quad j_1\Phi'(j) = \Psi_1(j), \quad j_2\Phi'(j) = \Psi_2(j), \quad j_3\Phi'(j) = \Psi_3(j). \tag{19}$$

The coefficients c_m of the polynomial Φ can be written as $c_m = \sum_{n=0}^{d-1} c_{mn}(i_1, i_2)i_3^n$, and similarly for Ψ_k. We have $c_{mn} \in F(i_1, i_2)$.

Proof. The birational model comes from the definition of the polynomials Ψ_k. As i_1, i_2, i_3, j have Fourier coefficients in F, the same argument as in Lemma 3.2 or [5, Theorem 5.2] shows that $c_m \in F(i_1, i_2, i_3)$. Moreover by the same argument the equation E is defined over F, and using that $F(i_1, i_2, i_3) = F(i_1, i_2)[X_3]/(E(i_1, i_2, X_3))$, we can also write $c_m = \sum_{n=0}^{d-1} c_{mn}(i_1, i_2)i_3^n$ and $c_{mn} \in F(i_1, i_2)$. □

Theorem 3.11. *With the conditions of Theorem 3.10, assume moreover that*

- *there is a fast evaluation algorithm in the precision to evaluate j, j_1, j_2, j_3.*
- *a preimage of the evaluation of (i_1, i_2, i_3) at some point can be computed in time quasi-linear in the precision;*

We let d_T be the maximal total degree of all the coefficients c_{mn} (where the degree of a rational function is the maximal of the degree of its numerator and denominator), and d_{i_2} be the degree in i_2 of the coefficients c_{mn}. Let N be the maximal height (over F) of the coefficients of each rational function $c_{mn} \in F(i_1, i_2)$. Then Φ and the Ψ_k can be computed in time $\tilde{O}(dd_T d_{i_2} LN)$.

Proof. We compute Φ by computing the coefficients $c_m \in F(i_1, i_2, i_3)$ by evaluation/interpolation. The evaluation of c_m at some $\tau \in \mathcal{H}_1^2$ is done as follows.

- Compute each value $j(\gamma.\tau)$ in precision N. It can be done with a complexity in $L\tilde{O}(N)$ time;
- Evaluate $\Phi(j(\tau)) = \prod_{\gamma \in \mathcal{G}_2 \backslash \mathcal{G}_1}(X - j(\gamma.\tau))$ using a subproduct tree (see [26, Section 10.1]). The polynomial $\Phi(j(\tau))$ can be obtained in $\tilde{O}(LN)$ time.
- Separating the coefficients according to powers of X gives the values $c_m(i_1(\tau), i_2(\tau), i_3(\tau))$.

By Section 3.3 and Theorem 3.7, to recover Φ, the evaluation step will be executed $O(dd_T d_{i_2})$ times and we will interpolate $O(dL)$ bivariate rational fractions and do $O(Ld_T d_{i_2})$ interpolations of a univariate polynomial. Recall that given the coefficient $c_{mn} \in \mathbb{C}$ computed at precision $O(N)$, using the LLL algorithm to recover $c_{mn} \in F$ can be done in time $\tilde{O}(N)$ ([62]). The final complexity is then

$$O(dd_T d_{i_2})\tilde{O}(LN) + O(dL)\tilde{O}(d_T d_{i_2} N) + O(Ld_T d_{i_2})\tilde{O}(dN) \subset \tilde{O}(dd_T d_{i_2} LN). \tag{20}$$

The same algorithm works for the Ψ_k, where at the evaluation step, $\Psi_k(j(\tau))$ is computed via a double subproduct tree on Ψ_k and Φ.

□

4 Modular polynomials

4.1 Isogenies preserving real multiplication

We want now to define modular polynomials, which parametrize isogenies between principally polarized abelian surfaces with real multiplication by $\mathcal{O}_K$. To achieve this, we need the following subgroups of $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$

$$\begin{aligned} \tilde{\Gamma}^0(\beta) &= \left\{ \left(\begin{smallmatrix} a & b/\sqrt{\Delta_K} \\ \sqrt{\Delta_K} c & d \end{smallmatrix} \right) \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) : b \in \beta\mathcal{O}_K \right\}, \\ \tilde{\Gamma}(\beta) &= \left\{ \left(\begin{smallmatrix} a & b/\sqrt{\Delta_K} \\ \sqrt{\Delta_K} c & d \end{smallmatrix} \right) \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) : a-1, d-1, b, c \in \beta\mathcal{O}_K \right\} \end{aligned} \tag{21}$$

where $\beta \in \mathcal{O}_K$ is a totally positive prime number. By abuse of notation, we use the same notation for their preimage by the isomorphism $\phi_\pm$ of Equation (4). Then the Hilbert cover $\tilde{\Gamma}^0(\beta)\backslash\mathcal{H}_1^2$ parametrizes pairs (A, B) of (principally polarized) abelian surfaces with real multiplication by $\mathcal{O}_K$ together with a β-isogeny $A \to B$, or equivalently pairs (A, K) where A has real multiplication by $\mathcal{O}_K$ and $K \subset A[\beta]$ is a kernel stable by $\mathcal{O}_K$ and maximally isotropic for the β-Weil pairing.

We now explain those terms and give more details on isogenies preserving the real multiplication. Let (A, θ_A) be a principally polarized abelian surface over a field k, with real multiplication given by $\mu : \mathcal{O}_K \to \mathrm{End}(A)$. Let $f : A \to B$ be an isogeny with kernel V. Then it is easy to see that B has real multiplication by $\mathcal{O}_K$ compatible with f if and only if V is stable under the action of $\mu(\mathcal{O}_K)$.

It remains to see when B admits a principal polarization. If θ_B is such a principal polarization, then $\theta = f^*\theta_B$ is a polarization on A. Denote by $\mathrm{End}^s(A)$ the subring of endomorphisms of A commuting with the Rosati involution induced by θ_A. By [3, Proposition 5.2.1 and Theorem 5.2.4], the group isomorphism between the Néron-Severi group of A and $\mathrm{End}^s(A)$ induces a bijection between the polarizations of some degree L of A and the set $\mathrm{End}^{s,++}(A)$ of totally positive symmetric endomorphisms of A with analytic norm L. When $\mathrm{End}^s(A) = \mathcal{O}_K$ (which is the case generically for an element of the Hilbert surface), then θ comes from a totally positive element $\beta \in \mathcal{O}_K^{++}$. Furthermore it is easy to check that V is a totally isotropic subgroup for the Weil pairing e_β on $A[\beta] = \{P \in A(\overline{k}) \mid \beta P = 0\}$. Looking at degrees, we also get that $\#V = N_{K/\mathbb{Q}}(\beta)$.

Conversely, let $\beta \in \mathcal{O}_K^{++}$ and denote by θ^β the polarization on A induced from θ_A by β (the polarization which arises from the composition of the polarization isogeny of θ_A with β), and $V \subset A[\beta]$ a maximal isotropic subgroup for the Weil pairing e_β. Then by descent theory, θ^β descends to a polarization θ_B on $B = A/V$, and since V is maximal, θ_B is principal. To emphasize the role of β, we call the isogeny f induced by V a β-isogeny.

Remark 4.1. The notation θ^β comes from the fact that if θ is induced by a symmetric line bundle $\mathcal{L}$ and $\beta = \ell \in \mathbb{N}$, then θ^ℓ is induced by the symmetric line bundle $\mathcal{L}^\ell$.

For more details we refer to [64, 14, 15] and in particular in [15, Theorem 1.1] of Dudeanu, Jetchev, Robert, and Vuille. We are mainly interested with cyclic isogenies of prime degree ℓ, these are induced by β of norm ℓ. We apply the discussion above to this special case by the following

Proposition 4.2. *Let (A, θ) be a principally polarized abelian surface lying on the Humbert surface H_{Δ_K}. Then there exist cyclic isogenies preserving real multiplication of degree ℓ (possibly defined over an extension of the field of definition of (A, θ)) from A to a principally polarized* *abelian surface if there exists a totally positive element $\beta \in \mathcal{O}_K^{++}$ of norm ℓ. And conversely if the principally polarised abelian surfaces lying on the Humbert surface admit cyclic isogenies preserving real multiplication of degree ℓ generically, then there exists such a β.*

Let β be a totally positive prime element above $\ell \in \mathbb{Z}$. The degree of the modular polynomial will differ according to whether $\ell \in \mathbb{Z}$ is an inert, split, or ramified prime number. These degrees will be given by the degree of the cover $\tilde{\Gamma}^0(\beta)\backslash\mathcal{H}_1^2 \to \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)\backslash\mathcal{H}_1^2$.

We first recall how to compute the number of ℓ-isogenies in the Siegel case, since we will adapt the proof to count number of β-isogenies. The ℓ-Weil pairing is the usual pairing e_ℓ on $A[\ell]$, and the corresponding ℓ-isogenies come from isotropic kernels of degree ℓ^2 (these are the same as maximal isotropic kernels when ℓ is prime). Over the splitting field of $A[\ell]$ over the field of definition of A, it is easy to see that there are $\ell^3+\ell^2+\ell+1$ such isogenies (this is the size of the quotient $\Gamma^0(\ell)\backslash\mathrm{Sp}_4(\mathbb{Z})$). The computation of the corresponding modular polynomials is described in [16, 5, 55].

On the Hilbert side of things, kernels of β-isogenies also corresponds to maximal isotropic kernels K for the β-Weil pairing on $A[\beta]$ with the further condition that K is stable under the real multiplication. Moreover, since the Weil pairing is compatible with endomorphisms, $A[\beta]$, as a $\mathcal{O}_K$-module, is given by a symplectic basis e_1, e_2. To such a basis one can associate the subgroup $V = \mathcal{O}_K e_1$ which is maximal isotropic for the Weil pairing and stable under the real multiplication by $\mathcal{O}_K$. All other such kernels are obtained in a similar way via the action of $\tilde{\Gamma}^0(\beta)\backslash\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ on the symplectic basis (e_1, e_2).

In particular, even if $\beta = \ell$ is inert, not all ℓ-isogenies are β-isogenies.

Proposition 4.3. *Let β be a totally positive prime element above $\ell \in \mathbb{Z}$.*

If ℓ is inert, the number of β-isogenies (over the algebraic closure) is the number of ℓ-isogenies whose kernel is stable under the real multiplication, and is given by ℓ^2+1.

If ℓ is split, the number of β-isogenies (over the algebraic closure) is $\ell+1$. They correspond to cyclic kernels of size ℓ in $A[\beta]$, which are all stable by $\mathcal{O}_K$.

Proof. First assume that $\beta = \ell$ is inert. Using $\phi_\pm$ (Equation (4)), we have to find the cardinality of $\tilde{\Gamma}^0(\ell)\backslash\mathrm{SL}_2(\mathcal{O}_K)$. We compute it as the quotient of $\#\tilde{\Gamma}(\ell)\backslash\mathrm{SL}_2(\mathcal{O}_K)$ by $\#\tilde{\Gamma}(\ell)\backslash\tilde{\Gamma}^0(\ell)$. We use the group isomorphism $\psi : \tilde{\Gamma}(\ell)\backslash\mathrm{SL}_2(\mathcal{O}_K) \simeq \mathrm{SL}_2(\ell\mathcal{O}_K\backslash\mathcal{O}_K)$ and we compute the cardinality of $\tilde{\Gamma}(\ell)\backslash\tilde{\Gamma}^0(\ell)$ looking at its image by ψ. Moreover we use that $\ell\mathcal{O}_K\backslash\mathcal{O}_K$ is isomorphic to $\mathbb{F}_{\ell^2}$ since ℓ is inert. So $\#\mathrm{SL}_2(\mathbb{F}_{\ell^2}) = \ell^2(\ell^4-1)$ and $\#\tilde{\Gamma}(\ell)\backslash\tilde{\Gamma}^0(\ell) = \ell^2(\ell^2-1)$.

Now assume that ℓ is ramified or split, so that β is of norm ℓ. We have seen that β-isogenies correspond to maximally isotropic kernels of size ℓ in $A[\beta]$. Since $A[\beta]$ is of size ℓ^2, such kernels are exactly the cyclic kernels of size ℓ. Since $\beta\mathcal{O}_K\backslash\mathcal{O}_K \simeq \mathbb{F}_\ell$, the elements of $\mathcal{O}_K$ act by scalar multiplication on $A[\beta]$ so they stabilize all the cyclic subgroups. And indeed since $\tilde{\Gamma}(\beta)\backslash\mathrm{SL}_2(\mathcal{O}_K) \simeq \mathrm{SL}_2(\mathbb{F}_\ell)$ it is easy to check that $\tilde{\Gamma}^0(\beta)\backslash\mathrm{SL}_2(\mathcal{O}_K)$ is of size $\ell+1$ and a set of representatives is given by the matrices $\left(\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right)$ for $x \in \{0,\dots,\ell-1\}$ and $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$. (since $\beta\mathcal{O}_K\backslash\mathcal{O}_K \simeq \ell\mathbb{Z}\backslash\mathbb{Z}$, we have that $\tilde{\Gamma}^0(\beta)\backslash\mathrm{SL}_2(\mathcal{O}_K) \simeq \Gamma^0(\ell)\backslash\mathrm{SL}_2(\mathbb{Z})$ whose set of representatives is well known). □

Remark 4.4. suppose that we have $\beta \in \mathcal{O}_K^{++}$ totally positive of norm ℓ. In this case either ℓ is ramified in $\mathcal{O}_K$ and there is only one kind of cyclic isogenies of degree ℓ, the β-isogenies, or ℓ splits as $\ell = \beta\overline{\beta}$ and $A[\ell] = A[\beta] \oplus A[\overline{\beta}]$ and there are two kind of cyclic isogenies: the β-isogenies and the $\overline{\beta}$-isogenies.

Furthermore it is easy to see that the composition of a β-isogeny and a $\overline{\beta}$-isogeny is an ℓ-isogeny (preserving real multiplication). Conversely a counting argument shows that any ℓ-isogeny preserving real multiplication splits as a β-isogeny and a $\overline{\beta}$-isogeny (which may be defined over an extension of greater degree). So when ℓ splits as $\beta\overline{\beta}$, $\beta \in \mathcal{O}_K^{++}$, we only need to compute β and $\overline{\beta}$ Hilbert modular polynomials.

If $\ell \in \mathbb{Z}$ is a prime number, we can also count the number of ℓ-isogenies preserving real multiplication, following the proof of Proposition 4.3. Indeed we use that $\ell\mathcal{O}_K \backslash \mathcal{O}_K$ is isomorphic to $\mathbb{F}_\ell^2$ if ℓ is split, to $\mathbb{F}_{\ell^2}$ if ℓ is inert and to $\mathbb{F}_\ell[X]/(X^2)$ if ℓ is ramified.

If ℓ is inert, $\#\mathrm{SL}_2(\mathbb{F}_{\ell^2}) = \ell^2(\ell^4-1)$ and $\#\tilde{\Gamma}(\ell)\backslash\tilde{\Gamma}^0(\ell) = \ell^2(\ell^2-1)$. If ℓ is split, $\#\mathrm{SL}_2(\mathbb{F}_\ell^2) = \ell^2(\ell^2-1)^2$ and $\#\tilde{\Gamma}(\ell)\backslash\tilde{\Gamma}^0(\ell) = \ell^2(\ell-1)^2$. If ℓ is ramified, $\#\mathrm{SL}_2(\mathbb{F}_\ell[X]/(X^2)) = \ell^6 - \ell^4$ and $\#\tilde{\Gamma}(\ell)\backslash\tilde{\Gamma}^0(\ell) = \ell^2(\ell^2-\ell)$.

So the number of ℓ-isogenies whose kernel is stable under the real multiplication is given by

- ℓ^2+1, if ℓ is inert in $\mathcal{O}_K$;
- $(\ell+1)^2$, if ℓ is split in $\mathcal{O}_K$;
- $\ell^2+\ell$, if ℓ is ramified in $\mathcal{O}_K$.

When ℓ is inert, we can always take $\beta = \ell$. However when ℓ is split (or ramified), there is no canonical β above ℓ; all splitting $\ell = \beta\overline{\beta}$ into totally positive elements yield a new modular polynomial. The next lemma clarify the dependency of the modular polynomial on the choice of β above ℓ.

Lemma 4.5. *Let $\ell = \beta\overline{\beta}$ be a splitting of ℓ into totally positive elements of $\mathcal{O}_K^{++}$. Let $V \subset A[\beta]$ be the kernel of a β-isogeny. Let $\epsilon \in \mathcal{O}_K^\times$ be a unit, so that ϵ^2 is totally positive and we have another splitting of ℓ as $\ell = (\epsilon^2\beta)(\overline{\epsilon^2\beta})$.*

Then $\epsilon^{-1}(V) = V$ is the kernel of an $\epsilon^2\beta$-isogeny, and the isogenous variety $A/\epsilon^{-1}(V)$ is isomorphic to A/V (as principally polarized abelian varieties).

Proof. Let ϵ be any endomorphism of A and θ a principal polarization. Then the pullback $\epsilon^*\theta$ is induced by the symmetric endomorphism $\hat{\epsilon}\epsilon$ where $\hat{\cdot}$ denote the Rosati involution. More generally, if β is totally positive, then $\epsilon^*\theta^\beta = \theta^{\hat{\epsilon}\beta\epsilon}$.

In particular, if $f : A \to B$ is a β-isogeny, then $f \circ \epsilon$ is a $\hat{\epsilon}\beta\epsilon$-isogeny. It suffices to apply this to $\epsilon \in \mathcal{O}_K^\times$ (so that $\hat{\epsilon} = \epsilon$) and $f : A \to B$ the isogeny with kernel V. If θ_B is the principal polarization induced by the descent of θ^β, then the descent of (A, θ^β) induced by $\epsilon^{-1}(V)$ is $(B, \theta_B^{\epsilon^{-2}})$ and $\epsilon^{-1} : B = A/V \to A/\epsilon^{-1}(V)$ induces the required isomorphism of principally polarized abelian varieties. □

From this lemma we deduce that the $\epsilon^2\beta$-modular polynomial will be the same as the β-modular polynomial.

Remark 4.6. For simplicity of the exposition we work with the maximal real order $\mathcal{O}_K$. However everything outlined above still work with a real order O that is only locally maximal at ℓ. It is also straightforward to adapt the results of Section 3 for computing invariants on the Hilbert surfaces of abelian surfaces with real multiplication by $\mathcal{O}$, and also to compute modular polynomials for such an $\mathcal{O}$.

4.2 Modular functions for β-isogenies

We let $\beta \in \mathcal{O}_K^{++}$ be a prime element of norm L. So $L = \ell$ if $\ell \in \mathbb{Z}$ is a prime number which splits or ramifies in $\mathcal{O}_K$, and $L = \ell^2$ if ℓ stays inert. Generalizing a bit the preceding section, we let $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ be a congruence subgroup containing $\tilde{\Gamma}(n)$. We want to apply the results of Section 3.4 to the extension $\mathbb{C}_{\tilde{\Gamma}^0(\beta)\cap\tilde{\Gamma}}/\mathbb{C}_{\tilde{\Gamma}}$. This cover corresponds to pairs of (principally polarized) abelian surfaces (A, B) with real multiplication together with a β-isogeny $A \to B$ as in Section 4.1, which is furthermore compatible with the level structure induced by $\tilde{\Gamma}$ on A and B.

For simplicity, we now assume that n is coprime to L. We first want to give an explicit set of representatives of $\tilde{\Gamma}^0(\beta) \cap \tilde{\Gamma}\backslash\tilde{\Gamma}$. Recall that there is an isomorphism $\phi_\pm : \mathrm{SL}_2(\mathcal{O}_K) \to \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ defined in Equation (4), so that by looking at the preimage by $\phi_\pm$ we can assume here that $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K)$. Recall that in this model, $\tilde{\Gamma}^0(\beta) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K) : \beta | b\}$.

Lemma 4.7. *Let N be an integer. Then the map $SL_2(\mathcal{O}_K) \to SL_2(\mathcal{O}_K/N\mathcal{O}_K)$ is surjective.*

Proof. This is an application of Strong approximation theory. In this case an elementary proof is also given in Bourbaki, Algebre Commutative, VII, §2, n.4: since $\mathrm{SL}_n(\mathcal{O}_K/N\mathcal{O}_K)$ is a product of local rings, it is generated by elementary matrices, so it suffices to lift these matrices. □

Lemma 4.8. *The quotient $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}$ is of cardinality $L + 1$.*

Proof. The sets $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}$ and $\tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}^0(\beta)\tilde{\Gamma}$ are in bijection so by Proposition 4.3.it suffices to prove that $\tilde{\Gamma}^0(\beta)\tilde{\Gamma} = \tilde{\Gamma}(1)$. So it suffices to prove that $\tilde{\Gamma}(L)\tilde{\Gamma}(n) = \tilde{\Gamma}(1)$, which is obvious by the Chinese Reminder Theorem.

Indeed by Lemma 4.7 it suffices to check that $\pi : \mathrm{SL}_2(\mathcal{O}_K) \to \mathrm{SL}_2(\mathcal{O}_K/Ln\mathcal{O}_K)$ is surjective on $\tilde{\Gamma}(L)\tilde{\Gamma}(n)$ (since this group contains the kernel). But since n is coprime to L, $\mathrm{SL}_2(\mathcal{O}_K/Ln\mathcal{O}_K) \simeq \mathrm{SL}_2(\mathcal{O}_K/L\mathcal{O}_K) \times \mathrm{SL}_2(\mathcal{O}_K/n\mathcal{O}_K)$ and $\pi(\tilde{\Gamma}(n))$ contains the left factor while $\pi(\tilde{\Gamma}(L))$ contains the right factor. □

Example 4.9. We describe in more detail the important case $\tilde{\Gamma} = \mathrm{SL}_2(\mathcal{O}_K)$. The group $\tilde{\Gamma}$ is generated by the three matrices $M_1 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $M_2 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $M_3 = \left(\begin{smallmatrix} 1 & \omega \\ 0 & 1 \end{smallmatrix}\right)$ (see Section 2.2 for the definition of ω). Note that $M_2\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)M_2 = -M_1$ so that it will be sometimes more convenient to use the matrix $\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$ instead of M_1.

By Lemma 4.8, the subgroup $\tilde{\Gamma}^0(\beta)$ of $\tilde{\Gamma}$ is of index $L + 1$ and the set of matrices $C_\beta = \{M_1, M_2^i, i \in \{0, \dots, L-1\}\}$ is a set of representatives of the classes of $\tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}$.

We can give a different proof using the matrices M_1, M_2 and M_3: the $L{+}1$ matrices of C_β are clearly in different classes of the quotient $\tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}$. Remark that ${}^tM_2 = M_1 M_2^{-1} M_1^{-1} \in \tilde{\Gamma}^0(\beta)$ and ${}^tM_3 = M_1 M_3^{-1} M_1^{-1} \in \tilde{\Gamma}^0(\beta)$ and that $\tilde{\Gamma}$ is generated by M_1, ${}^tM_2$ and ${}^tM_3$. For all $i \in \{0, \dots, L\}$, ${}^tM_2 M_2^i$ and ${}^tM_3 M_2^i$ are in the class of M_2^i while ${}^tM_2 M_1$ and ${}^tM_3 M_1$ are in the class of M_1. Moreover, $M_1 M_2^i$ is in the class of M_1 and $M_1 M_1 = -I_2$ which shows that there can not be more than the $L + 1$ classes that we already know.

Example 4.10. Another important example is the case $\tilde{\Gamma} = \tilde{\Gamma}(2, 4)$. By the above Lemma, the subgroup $\tilde{\Gamma}(2, 4) \cap \tilde{\Gamma}^0(\beta)$ of $\tilde{\Gamma}(2, 4)$ is of index $L + 1$.

If $\gamma \in \tilde{\Gamma}^0(\beta)\backslash\mathrm{SL}_2(\mathcal{O}_K)$ then there exists an element $\gamma' \in \tilde{\Gamma}^0(\beta)$ such that $\gamma'\gamma \in \tilde{\Gamma}(2, 4)$. For applications it is useful to have a constructive definition of γ'.

We look at γ' such that $\gamma'\gamma \equiv 0 \bmod 4$, namely such that $\gamma' \equiv \gamma^{-1} \bmod 4$, and such that $\gamma' \equiv \left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right) \bmod \ell$. By the Chinese Remainder Theorem, these conditions modulo 4 and ℓ give a matrix γ'' which must satisfy conditions modulo 4ℓ and by Lemma 4.7, γ'' can be lifted to a matrix in $\tilde{\Gamma}$.

Now we go back to the usual model $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$. Let $\mathcal{G}$ be either $\tilde{\Gamma}$ or $\tilde{\Gamma} \cup \tilde{\Gamma}\sigma$. We have $\mathcal{G} \cap \tilde{\Gamma}^0(\beta) = \tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$. In the case that $\sigma \in \mathcal{G}$, we recall that by Lemma 2.12 we can assume that the group $\tilde{\Gamma}$ is stable under real conjugation.

Let i_1, i_2, i_3 be generators of the Hilbert modular field $\mathbb{C}_{\mathcal{G}}$. Recall that $\mathbb{C}_{\mathcal{G}}$ is defined in Definition 2.13. (Later we will assume that they are chosen such that the evaluation and its inverse can be computed in time quasi-linear, like in Theorem 3.4.)

Let j be a generator of the field extension $\mathbb{C}_{\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)}/\mathbb{C}_{\mathcal{G}}$. Such a generator always exists by the primitive element theorem. In fact it is easy to find such a generator:

Proposition 4.11. *Let i_1, i_2, i_3 be generators of the Hilbert modular field $\mathbb{C}_{\tilde{\Gamma}}$. Let j be a Hilbert modular function invariant by $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$ but not by $\tilde{\Gamma}$. Then $\mathbb{C}_{\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)} = \mathbb{C}(i_1, i_2, i_3, j)$.*

Let $\mathcal{G} = \tilde{\Gamma} \cup \tilde{\Gamma}\sigma$. Let i_1, i_2, i_3 be generators of the symmetric Hilbert modular field $\mathbb{C}_{\mathcal{G}}$. Let j be a Hilbert modular function invariant by $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$ but not by $\tilde{\Gamma}$. If j is symmetric, $\mathbb{C}_{(\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta))\rtimes\langle\sigma\rangle} = \mathbb{C}(i_1, i_2, i_3, j)$, otherwise $\mathbb{C}_{\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)} = \mathbb{C}(i_1, i_2, i_3, j)$.

Proof. Since the symmetric case is easily deduced from the non symmetric one, we only do the case $\mathcal{G} = \tilde{\Gamma}$. We have seen in the proof of Lemma 3.9 that the extension $\mathbb{C}_{\tilde{\Gamma}(Ln)}/\mathbb{C}_{\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma}$ is Galois with Galois group $\tilde{\Gamma}(Ln)\backslash(\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma)$. Let $K_1 = \mathbb{C}_{\tilde{\Gamma}}(j) = \mathbb{C}(i_1, i_2, i_3, j)$ and $K_2 = \mathbb{C}_{\tilde{\Gamma}(Ln)}^{\tilde{\Gamma}(Ln)\backslash(\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta))} = \mathbb{C}_{\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)}$. Then $K_1 \subseteq K_2$ and we want to prove equality. By Galois theory, the subfields between K_1 and K_2 correspond to subgroups of $\tilde{\Gamma}$ containing $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$. If we show that the group $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$ is maximal in $\tilde{\Gamma}$, then we can deduce that $K_1 = \mathbb{C}_{\tilde{\Gamma}}$ or $K_1 = K_2$. By assumption, only the last possibility can be true. Looking at the image of $\tilde{\Gamma}^0(\beta) \cap \tilde{\Gamma}$ by the isomorphism $\tilde{\Gamma}(\beta) \cap \tilde{\Gamma}\backslash\tilde{\Gamma} \simeq \tilde{\Gamma}(\beta)\backslash\tilde{\Gamma}(\beta)\tilde{\Gamma} = \tilde{\Gamma}(\beta)\backslash\tilde{\Gamma}(1)$, we can see that is is enough to prove that $\tilde{\Gamma}^0(\beta)$ is maximal in $\tilde{\Gamma}(1)$.

Let $\pi : \tilde{\Gamma} \twoheadrightarrow \mathrm{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K)$. If β is split, then $\mathrm{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K) \simeq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^2$ and $\pi(\tilde{\Gamma}^0(\beta)) = \{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right) \times \left(\begin{smallmatrix} * & * \\ * & * \end{smallmatrix}\right)\}$. By King [44, Theorem 4.1], the set of triangular matrices of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is maximal and thus $\pi(\tilde{\Gamma}^0(\beta))$ is maximal in $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^2$. As π is surjective, we deduce that $\tilde{\Gamma}^0(\beta)$ is maximal in $\tilde{\Gamma}$.

If $\beta = \ell$ is inert, then the image of $\pi(\tilde{\Gamma}(\beta))$ is given by triangular matrices of $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$ so it is also maximal.

If ℓ is ramified, then $\mathrm{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K) \simeq \mathrm{SL}_2((\mathbb{Z}/\ell\mathbb{Z})[X]/(X^2))$ and $\pi(\tilde{\Gamma}^0(\beta))$ is the set of matrices of the form $\left(\begin{smallmatrix} * & xX \\ * & * \end{smallmatrix}\right)$ for any $x \in \mathbb{Z}/\ell\mathbb{Z}$. Let G be a group which contains strictly $\pi(\tilde{\Gamma}^0(\beta))$. Then there exists some matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in G$, with $B(0) \neq 0$. If A is invertible (namely $A(0) \neq 0$) then $\left(\begin{smallmatrix} 1 & 0 \\ -AC & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} A^{-1} & 0 \\ 0 & A \end{smallmatrix}\right)\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & A^{-1}B \\ 0 & 1 \end{smallmatrix}\right) \in G$ and $(A^{-1}B)(0) \neq 0$ so that $A^{-1}B = x_0 + x_1X$ with $x_0 \neq 0$. Finally we have $\left(\begin{smallmatrix} 1 & x_0+x_1X \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -x_1X \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & x_0 \\ 0 & 1 \end{smallmatrix}\right)$ from which we deduce that $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in G$. As this last matrix and the matrices $\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & X \\ 0 & 1 \end{smallmatrix}\right)$ are all in G and are generators for $\mathrm{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K)$, we deduce that G is $\pi(\tilde{\Gamma})$, that $\pi(\tilde{\Gamma}^0(\beta))$ is maximal and thus by surjectivity that $\tilde{\Gamma}^0(\beta)$ is also maximal. If A is not invertible but D is, the proof proceeds similarly. Otherwise, if both A and D are not invertible, then B and C are. Moreover, $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} A+B & B \\ C+D & D \end{smallmatrix}\right)$ and $(A+B)(0) \neq 0$, which ends the proof. □

4.3 Computing modular polynomials

Using the notation of Section 4.2, we want to compute modular polynomials classifying all β-isogenies from an abelian surface with real multiplication by $\mathcal{O}_K$.

First consider the case $\tilde{\Gamma} = \tilde{\Gamma}(1)$. Recall from Section 4.1 that geometrically, a point in $H_{\tilde{\Gamma}^0(\beta)}$ corresponds to a triple (A, θ, V) with a principally polarized abelian surface (A, θ) and V the kernel of a β-isogeny (equivalently V is maximally isotropic for the e_β Weil pairing on $A[\beta]$). We denote by $\pi : (A, \theta, V) \to (A, \theta) \times (A/V, \theta')$ where θ' is the polarization induced on A/V by θ^β. This defines an algebraic map (a modular correspondence) $H_{\tilde{\Gamma}^0(\beta)} \to H_{\tilde{\Gamma}(1)} \times H_{\tilde{\Gamma}(1)}$. The β-modular polynomials describe the algebraic relations giving the image of this map.

Concretely, if i_1, i_2, i_3 generate $\mathbb{C}(\tilde{\Gamma}(1))$, the β-modular polynomials for the invariants i_k describe the locus of the modular points $((i_1(z), i_2(z), i_3(z)), (i_1(z/\beta), i_2(z/\beta), i_3(z/\beta))$ for $z \in \mathcal{H}_1^2$. In particular the β-modular polynomials classify the β-isogenies. Indeed if $z \in \tilde{\Gamma}(1)\backslash\mathcal{H}_1^2$, the β-isogenous varieties are $\frac{1}{\beta}\gamma \cdot z$ for $\gamma \in \tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}(1)$. Furthermore since $\sigma\tilde{\Gamma}^0(\beta)\sigma = \tilde{\Gamma}^0(\overline{\beta})$, the $\overline{\beta}$-isogenous varieties are given by $\frac{1}{\overline{\beta}}\gamma \cdot z$, for $\gamma \in \tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}(1)$.

Furthermore, by Lemma 4.13, the modular function $i_1(z/\beta)$ is invariant by $\tilde{\Gamma}^0(\beta)$, so by Proposition 4.11 it is a generator of $\mathbb{C}(H_{\tilde{\Gamma}^0(\beta)})/\mathbb{C}(H_{\tilde{\Gamma}(1)})$. This implies that the modular correspondance $H_{\tilde{\Gamma}^0(\beta)} \to H_{\tilde{\Gamma}(1)} \times H_{\tilde{\Gamma}(1)}$ is an embedding (at least birationally), so that the β-modular polynomials do give equations for $H_{\tilde{\Gamma}^0(\beta)}$.

More generally, for a group $\tilde{\Gamma}$ containing a congruence subgroup $\tilde{\Gamma}(n)$ with n coprime to L, we would like to define β-modular polynomials describing the image of a map (a modular correspondence) $H_{\tilde{\Gamma}\cap\tilde{\Gamma}(\beta)} \to H_{\tilde{\Gamma}} \times H_{\tilde{\Gamma}}$. A point in $H_{\tilde{\Gamma}\cap\tilde{\Gamma}(\beta)}$ corresponds to a triple (A, θ, V) as above together with an extra level structure G defined by $\tilde{\Gamma}$. For the modular correspondence to give an embedding of $H_{\tilde{\Gamma}\cap\tilde{\Gamma}(\beta)}$ we need for G to induce a unique extra level structure G' on $(A/V, \theta')$.

Definition 4.12. Let $\gamma \in \tilde{\Gamma}^0(\beta) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. We denote $\gamma_\beta = \begin{pmatrix} a & b/\beta \\ c\beta & d \end{pmatrix} \in \tilde{\Gamma}(1)$.

Lemma 4.13. *Let i be a meromorphic function $\mathcal{H}_1^2 \to \mathbb{C}$, and define $i_\beta(z) = i(z/\beta)$. Recall that, for $\gamma \in \tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma$, $i^\gamma(z) = i(\gamma \cdot z)$ and define $i_\beta^\gamma(z) = i(\frac{1}{\beta}\gamma \cdot z)$. Then for $\gamma \in \tilde{\Gamma}^0(\beta)$,*

$$i_\beta^\gamma(z) = i(\frac{1}{\beta}\gamma \cdot z) = i(\gamma_\beta \cdot (\frac{1}{\beta}z)) = i^{\gamma_\beta}(\frac{1}{\beta}z)$$

$$i_\beta^\sigma(z) = i(\frac{1}{\beta}\sigma z) = i^\sigma(\frac{1}{\overline{\beta}}z))$$

$$i_\beta^{\gamma\sigma}(z) = i(\frac{1}{\beta}\gamma\sigma \cdot z) = i(\sigma\overline{\gamma}_{\overline{\beta}} \cdot (\frac{1}{\overline{\beta}}z)) = i^{\sigma\overline{\gamma}_{\overline{\beta}}}(\frac{1}{\overline{\beta}}z)$$

Corollary 4.14. *Let i be a Hilbert modular function for $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$. Let $\tilde{\Gamma}_\beta = \{\gamma \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \mid \gamma_\beta \in \tilde{\Gamma}\} \subset \tilde{\Gamma}^0(\beta)$. Then i_β is a modular Hilbert function for $\tilde{\Gamma}_\beta$. Furthermore if i is symmetric and $\overline{\beta} = \beta$, then i_β is symmetric.*

Assume that for every $\gamma \in \tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$, $\gamma_\beta \in \tilde{\Gamma}$, so

$$\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta) = \tilde{\Gamma} \cap \tilde{\Gamma}_\beta. \tag{22}$$

Then if i is a Hilbert modular function for $\tilde{\Gamma}$, then i_β is a Hilbert modular function for $\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)$.

If $\tilde{\Gamma}$ satisfies Equation (22) (such is the case when $\tilde{\Gamma} = \tilde{\Gamma}(n)$ is a congruence subgroup), one can then define the modular correspondence as $H_{\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)} \to H_{\tilde{\Gamma}} \times H_{\tilde{\Gamma}}, z \mapsto ((i_1(z),\, i_2(z),\, i_3(z)),\, (i_1(z/\beta),\, i_2(z/\beta),\, i_3(z/\beta)))$ for $z \in \mathcal{H}_1^2$ and i_1, i_2, i_3 generating $\mathbb{C}_{\tilde{\Gamma}}$.

Theorem 4.15. Non symmetric case: *let $\tilde{\Gamma}$ be a congruence subgroup such that $\tilde{\Gamma}(2,4) \subset \tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$. Let $\beta \in \mathcal{O}_K^{++}$ be a prime element of norm L, and assume that for every $\gamma \in \tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$, $\gamma_\beta \in \tilde{\Gamma}$.*

Let C_β be a set of representatives of $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}$.

Let i_1, i_2, i_3 be modular functions generating $\mathbb{C}_{\tilde{\Gamma}}$ and with Fourier coefficients in a number field F.

Define the modular polynomials:

$$\Phi_\beta(X, i_1, i_2, i_3) = \prod_{\gamma \in C_\beta} (X - i_{1,\beta}^{\gamma}), \quad \textit{and} \quad \Psi_{k,\beta}(X, i_1, i_2, i_3) = \sum_{\gamma \in C_\beta} i_{k,\beta}^{\gamma} \frac{\Phi_\beta(X, i_1, i_2, i_3)}{X - i_{1,\beta}^{\gamma}} \tag{23}$$

for $k = 2, 3$. They lie in $F(i_1, i_2, i_3)[X]$.

Then after a precomputation step described in Theorem 3.4 (which does not depend on β, only on i_1, i_2, i_3), and under the heuristics of [55, Theorem 34], the modular polynomials can be computed in time quasi-linear in their size.

Symmetric case: *Let $\mathcal{G} = \tilde{\Gamma} \cup \tilde{\Gamma}\sigma$. If $\overline{\beta} = \beta$ we let C_β be a set of representatives of $((\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)) \cup (\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta))\sigma)\backslash\mathcal{G} \simeq \tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}$, otherwise we let C_β be a set of representatives of $(\mathcal{G} \cap \tilde{\Gamma}^0(\beta))\backslash\mathcal{G} \simeq \left(\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}\right) \cup \left(\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}\right)\sigma$. Then the same definition as in Equation (23) applies and the corresponding modular polynomials can be computed in time quasi-linear in their size.*

Proof. This is Theorem 3.11, applied to (in the notation of the Theorem) $j_1 = i_{1,\beta}$, $j_2 = i_{2,\beta}$, $j_3 = i_{3,\beta}$. We only detail the non symmetric case, the adaptations to the symmetric case are obvious. Since $\tilde{\Gamma} \neq \tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$, one of the $i_{k,\beta}$ is not invariant by $\tilde{\Gamma}$ so, by Proposition 4.11, $i_{k,\beta}$ generates the field extension $\mathbb{C}_{\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)}/\mathbb{C}_{\tilde{\Gamma}}$. Then in the notation of Theorem 3.10 we can use $j = i_{k,\beta}$. (In Theorem 4.15 we assume $k = 1$).

It remains to check that the $i_{k,\beta}$ can be evaluated in time quasi-linear in the precision, but this is obvious from their definition and the fact that the i_k can due to Theorem 3.4. □

Definition 4.16. The polynomials $\Phi_\beta(X, i_1, i_2, i_3)$ and $\Psi_{k,\beta}(X, i_1, i_2, i_3)$ for $k = 2, 3$ defined in Theorem 4.15 are called the *β-modular polynomials* for i_1, i_2, i_3.

Example 4.17.

- If $\beta = \ell$ is an inert prime. Then Φ_ℓ has degree ℓ^2+1 and $\Psi_{k,\ell}$ has degree ℓ^2. If i_1, i_2, i_3 are symmetric, then $i_{1,\ell}, i_{2,\ell}, i_{3,\ell}$ also, hence they are invariant under $(\tilde{\Gamma}\cap\tilde{\Gamma}^0(\ell)) \cup (\tilde{\Gamma}\cap\tilde{\Gamma}^0(\ell))\sigma$.

- If β has norm ℓ, so $\ell = \beta\overline{\beta}$ is split or ramified. Then if $\mathcal{G} = \tilde{\Gamma}$ is not symmetric, Φ_β has degree $\ell + 1$ and $\Psi_{k,\beta}$ has degree ℓ.

  However if $\sigma \in \mathcal{G}$, so that $\mathcal{G} = \tilde{\Gamma} \rtimes \langle\sigma\rangle$, then in the split case since the $i_{k,\beta}$ are not symmetric, Φ_β has degree $2\ell + 2$ and $\Psi_{k,\beta}$ has degree $2\ell + 1$. Since $\tilde{\Gamma}$ is stable under the real conjugation, we can make explicit the action of σ as follows: if we let C_β be a set of representatives of $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}$ the modular polynomials are given by

$$\Phi_\beta(X, i_1, i_2, i_3) = \prod_{\gamma \in C_\beta} (X - i_{1,\beta}^{\gamma})(X - i_{1,\beta}^{\gamma\sigma}) = \prod_{\gamma \in C_\beta} (X - i_{1,\beta}^{\gamma})(X - i_{1,\overline{\beta}}^{\gamma}) \qquad \text{and}$$

$$\Psi_{k,\beta}(X, i_1, i_2, i_3) = \sum_{\gamma \in C_\beta} i_{k,\beta}^{\gamma} \frac{\Phi_\beta(X, i_1, i_2, i_3)}{X - i_{1,\beta}^{\gamma}} + \sum_{\gamma \in C_\beta} i_{k,\beta}^{\gamma\sigma} \frac{\Phi_\beta(X, i_1, i_2, i_3)}{X - i_{1,\overline{\beta}}^{\gamma}}.$$

In this case the β-modular polynomials parametrize both β and $\overline{\beta}$-isogenies (so they are equal to the $\overline{\beta}$-modular polynomials). This may be a drawback for some of the applications of isogenies , hence the interest to also have non symmetric invariants, even if they are harder to compute.

If ℓ is ramified, then the $i_{k,\beta}$ are symmetric, so in this case we don't need non symmetric invariants.

Remark 4.18 (Changing β when $\tilde{\Gamma} = \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$)**.** Let ϵ be a fundamental unit of $\mathcal{O}_K$. Let $\epsilon' \in \mathcal{O}_K^{\times,++}$, then there are also $\epsilon'\beta$-isogenies. (We only consider totally positive units ϵ' to guarantee the fact that $\epsilon' z \in \mathcal{H}_1^2$, for $z \in \mathcal{H}_1^2$).

If there exists $n \in \mathbb{Z}$ such that $\epsilon' = \epsilon^{2n}$, then the matrix $\gamma = \begin{pmatrix} \epsilon^n & 0 \\ 0 & \epsilon^{-n} \end{pmatrix}$ is in $\tilde{\Gamma}$ and $\gamma \cdot z = \epsilon' z$. Thus, in this case, $i_k(\epsilon' z) = i_k(z)$, and, in particular, a β-isogeny is also a $\epsilon'\beta$-isogeny. (For a more intrinsic proof see Lemma 4.5.)

When $D = 2$ or 5, a fundamental unit ϵ has norm -1 while $\epsilon' \in \mathcal{O}_K^{\times,+}$ has norm 1, so that the latter can always been written as an even power of ϵ. Thus, the choice of the splitting of ℓ does not matter.

Remark 4.19 (General modular polynomials)**.** Let $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$ that does not satisfy Equation (22). Then a level structure G associated to a triple (A, θ, V) corresponds to several level structures G' on $(A/V, \theta')$.

From Corollary 4.14 the modular functions $i_{k,\beta}$ are modular for the group $\tilde{\Gamma}_\beta = \{\gamma \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \mid \gamma_\beta \in \tilde{\Gamma}\} \subset \tilde{\Gamma}^0(\beta)$. So we can define modular polynomials in a similar way as in Theorem 4.15 except that we act by $\tilde{\Gamma} \cap \tilde{\Gamma}_\beta \backslash \tilde{\Gamma}$. The fibers correspond to β-isogenies together with an extra structure determined by the action of $\tilde{\Gamma} \cap \tilde{\Gamma}_\beta \backslash \tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$. So we lose the corresponding factor in the degree of the modular polynomials. A possible solution would be to replace $i_{1,\beta}$ by its trace under the action of $\tilde{\Gamma} \cap \tilde{\Gamma}_\beta \backslash \tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$ to get a modular function invariant by $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$.

Also, if $\tilde{\Gamma}$ does not contain a congruence subgroup $\tilde{\Gamma}(n)$ of level n coprime to ℓ, then $\tilde{\Gamma} \cap \tilde{\Gamma}(\beta) \backslash \tilde{\Gamma}$ may not be isomorphic to $\tilde{\Gamma}(\beta) \backslash \tilde{\Gamma}(1)$, but only isomorphic to a subgroup. We can still compute modular polynomials, but they will not parametrize all β-isogenies, only those which are compatible with the structure induced by $\tilde{\Gamma}$.

Finally if $\beta \in \mathcal{O}_K^{++}$ is totally positive but not prime, it is easy to adapt Theorem 4.15 (if we suppose that i_1 is still a generator of the rational function field of the corresponding cover, or in other words that i_1 is not invariant by subgroups of the form $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\mathfrak{I})$ for all strict divisors ideal $\mathfrak{I}$ of (β)). The only difference is on the degree of the polynomials, Φ_β will not be of degree the norm of $\beta + 1$. Rather the degree depends on the factorization of (β) into principal prime ideals.

Of course this whole discussion is easily extended to the symmetric case.

5 Results

The aim of this section is to present some polynomials we have computed and to compare the polynomials with the different invariants when this comparison makes sense. All the polynomials computed are accessible at `https://members.loria.fr/EMilio/` . In particular, we do not present here the polynomials computed when ℓ is inert or when $D = 3$.

The first invariants we used are the Gundlach invariants J_1, J_2, which are defined in Appendix A.2. They are defined for $D = 2, 5$ and are invariant by $\mathrm{SL}_2(\mathcal{O}_K)$. And we also used the pullbacks $\tilde{b}_i = \phi_{1,\omega}^* b_i$ of the b_i functions defined in Equation (3) by the map $\phi_{1,\omega}$ defined in Equation (6). They are defined for any D and are invariant by $\tilde{\Gamma}(2, 4)$ (see Definition 2.10). See also Appendix B.1 and B.2 about the modular polynomials with these invariants.

5.1 Case $D = 2$

We have computed the β-modular polynomials with the Gundlach invariants for $\ell = 2$, 7, 17, 23, 31, 41, 47 and 71. If we write, in the split case,

$$\Phi_\beta(X, J_1, J_2) = X^{2\ell+2} + \sum_{i=0}^{2\ell+1} c_i(J_1, J_2) X^i \qquad \text{and} \qquad \Psi_\beta(X, J_1, J_2) = \sum_{i=0}^{2\ell+1} d_i(J_1, J_2) X^i,$$

then we have seen that the denominator of c_i is of the form $P(J_1, J_2)^4$ unless $i = 2\ell + 1$ where it is $P(J_1, J_2)^2$, and that the denominator of d_i is of the form $P(J_1, J_2)^6$, unless $i = 2\ell + 1$ where it is $P(J_1, J_2)^4$. We have for example for $\ell = 7$

$$P(J_1, J_2) = J_1^2 - J_1 J_2^2 + 2J_1 J_2 - 81J_1 + 64J_2^2$$

and for $\ell = 17$

$$\begin{aligned} P(J_1, J_2) \quad = \quad & J_1^7 - J_1^6 J_2^3 - 6J_1^6 J_2^2 + J_1^6 J_2 - 414J_1^6 + 428J_1^5 J_2^3 + 2387J_1^5 J_2^2 - \\ & 17760J_1^5 J_2 + 431811J_1^5 + 17728J_1^4 J_2^4 - 331952J_1^4 J_2^3 - 2578856J_1^4 J_2^2 + \\ & 6229197J_1^4 J_2 - 80515134J_1^4 - 6145536J_1^3 J_2^4 + 52974272J_1^3 J_2^3 + \\ & 535037040J_1^3 J_2^2 + 6116816412J_1^3 J_2 + 37822859361J_1^3 - 91648000J_1^2 J_2^5 - \\ & 6502153216J_1^2 J_2^4 - 75793205760J_1^2 J_2^3 - 197144611776J_1^2 J_2^2 - \\ & 17565696000J_1 J_2^5 - 7812042752J_1 J_2^4 + 110592000000J_2^6. \end{aligned}$$

Table 1 contains some information about these polynomials. The first column is the prime number, the second the size of the β-modular polynomials, then we have put the total degree and the degree in J_1 and in J_2 of the denominator $P(J_1, J_2)$, and then similarly for the maximal degrees appearing in the numerators. The last column is the number of decimal digits of the largest coefficient appearing in the polynomials.

2	8.5 KB	3	0	3	4	4	2	8
7	172 KB	3	2	2	25	23	13	66
17	5.8 MB	9	7	6	65	61	36	196
23	21 MB	12	11	8	87	85	48	280
31	70 MB	17	14	10	117	111	61	401
41	225 MB	23	21	14	157	153	84	560
47	400 MB	26	25	16	179	177	96	665
71	2.2 GB	42	37	24	275	265	144	1078

Table 1: Information about the modular polynomials for $D = 2$ (Gundlach invariants)

We have computed the β-modular polynomials with theta invariants for $\ell = 17$, 41, 73, 89 and 97 (which are 1 modulo 4, see Proposition B.9). By Remark B.11, the β-modular polynomials are

$$\Phi_\beta(X, \tilde{b}_2, \tilde{b}_3) = X^{2\ell+2} + \sum_{i=0}^{2\ell+1} c_i(\tilde{b}_2, \tilde{b}_3) X^i \qquad \text{and} \qquad \Psi_\beta(X, \tilde{b}_2, \tilde{b}_3) = \sum_{i=0}^{2\ell+1} d_i(\tilde{b}_2, \tilde{b}_3) X^i.$$

We have seen that the denominators of c_i and d_i are of the form $P(\tilde{b}_2, \tilde{b}_3)^2$ unless $i = 2\ell + 1$ where it is $P(\tilde{b}_2, \tilde{b}_3)$. For example, we have for $\ell = 17$ and $\beta = 5 + 2\sqrt{2}$

$$\begin{aligned} P(\tilde{b}_2, \tilde{b}_3) \;=\; & \tilde{b}_3^6 \tilde{b}_2^{18} + (6\tilde{b}_3^8 - 6\tilde{b}_3^4 + 1)\tilde{b}_2^{16} + (15\tilde{b}_3^{10} - 24\tilde{b}_3^6 + 7\tilde{b}_3^2)\tilde{b}_2^{14} + (20\tilde{b}_3^{12} - 42\tilde{b}_3^8 + 9\tilde{b}_3^4 + \\ & 2)\tilde{b}_2^{12} + (15\tilde{b}_3^{14} - 48\tilde{b}_3^{10} + 37\tilde{b}_3^6 + 4\tilde{b}_3^2)\tilde{b}_2^{10} + (6\tilde{b}_3^{16} - 42\tilde{b}_3^{12} + 68\tilde{b}_3^8 - 26\tilde{b}_3^4 + 3)\tilde{b}_2^8 + \\ & (\tilde{b}_3^{18} - 24\tilde{b}_3^{14} + 37\tilde{b}_3^{10} + 8\tilde{b}_3^6 - \tilde{b}_3^2)\tilde{b}_2^6 + (-6\tilde{b}_3^{16} + 9\tilde{b}_3^{12} - 26\tilde{b}_3^8 - 24\tilde{b}_3^4 + 2)\tilde{b}_2^4 + \\ & (7\tilde{b}_3^{14} + 4\tilde{b}_3^{10} - \tilde{b}_3^6)\tilde{b}_2^2 + (\tilde{b}_3^{16} + 2\tilde{b}_3^{12} + 3\tilde{b}_3^8 + 2\tilde{b}_3^4 + 1). \end{aligned}$$

For $\ell = 17$ and 41, the degrees of the coefficients c_i and d_i in the variables $\tilde{b}_2$ and $\tilde{b}_3$ are close to the degrees in the variables J_1 and J_2. But with the $\tilde{b}_i$, some relations between the exponents occur. The numerator of c_i can be written as $\sum_m \sum_n c_{i,m,n} \tilde{b}_2^m \tilde{b}_3^n$ (and similarly for d_i). We have then for $\ell = 17$ and $\beta = 5 + 2\sqrt{2}$

$$\begin{array}{rcl} m & \equiv & 0 \bmod 2 \\ n+i & \equiv & 0 \bmod 2 \\ m+n & \equiv & i \bmod 4 \end{array} \qquad \text{and} \qquad \begin{array}{rcl} m & \equiv & 1 \bmod 2 \\ n+i & \equiv & 1 \bmod 2 \\ m+n & \equiv & i \bmod 4 \end{array} \tag{24}$$

for c_i and d_i respectively. In the case $\ell = 41$ and $\beta = 7 + 2\sqrt{2}$, these equations are the same except the last which is $m + n \equiv -i \bmod 4$ for c_i and d_i.

17	221 KB	24	18	18	57	53	50	13
41	7.2 MB	64	56	56	144	140	132	38
73	81 MB	120	112	112	264	260	246	79
89	188 MB	152	138	138	325	317	309	102
97	269 MB	168	154	154	357	345	341	112

Table 2: Information about the modular polynomials for $D = 2$ (theta invariants)

Comparing Tables 1 and 2, we can see that taking the invariants based on the theta functions give better results. But, here, this is the case only when $\ell \equiv 1 \bmod 4$.

For $\ell = 7$ ($\ell \equiv 3 \bmod 4$), we have done as explained at the end of Appendix B.2. On the one hand, we have computed the polynomials using the subgroup of index $4(\ell + 1)$ and on the other hand, we have computed the polynomials using the Rosenhain invariants. The first solution give better results in terms of degree, sparsity and the whole polynomials fill 930 KB in the first case while 70 MB in the second. In both cases, the polynomials are bigger than those using the Gundlach invariants. This is also true for $\ell = 23$, where using the first method, the polynomials fill 110 MB.

5.2 Case $D = 5$

We have computed the β-modular polynomials with the Gundlach invariants for $\ell = 5$, 11, 19, 29, 31, 41 and 59. If we write

$$\Phi_\beta(X, J_1, J_2) = X^{2\ell+2} + \sum_{i=0}^{2\ell+1} c_i(J_1, J_2)X^i \qquad \text{and} \qquad \Psi_\beta(X, J_1, J_2) = \sum_{i=0}^{2\ell+1} d_i(J_1, J_2)X^i,$$

when ℓ is split, then we have seen that the denominators of c_i and of d_i are of the form $P(J_1, J_2)^4$ except for $i = 2\ell + 1$ where it is $P(J_1, J_2)^2$. We have for example for $\ell = 11$

$$\begin{aligned} P(J_1, J_2) \;=\;& 4J_1^7 + (-12J_2^2 - 19236J_2 + 119497519)J_1^6 + (12J_2^4 + 56972J_2^3 - 387805052J_2^2 - \\ & 278163835056J_2 + 35953243171744)J_1^5 + (-4J_2^6 - 55980J_2^5 + 449730698J_2^4 + \\ & 943837290960J_2^3 - 133230692691392J_2^2 + 6651010132099840J_2 + \\ & 13001634695104256)J_1^4 + (18500J_2^7 - 215193500J_2^6 - 1170430882000J_2^5 + \\ & 388324233980000J_2^4 - 32395226716512000J_2^3)J_1^3 + (32609375J_2^8 + \\ & 635091750000J_2^7 - 718632513000000J_2^6 + 34620677424000000J_2^5)J_1^2 + \\ & (-124875000000J_2^9 + 601911000000000J_2^8)J_1 - 182250000000000J_2^{10}. \end{aligned}$$

We have computed the β-modular polynomials with theta invariants for $\ell = 5$, 11, 19, 29, 31, 41 and 59. These polynomials are

$$\Phi_\beta(X, \tilde{b}_1, \tilde{b}_2, \tilde{b}_3) = X^{\ell+1} + \sum_{i=0}^{\ell}(\sum_{j=0}^{4} c_{i,j}(\tilde{b}_1, \tilde{b}_2)\tilde{b}_3^j)X^i \qquad \text{and}$$

$$\Psi_{k,\beta}(X, \tilde{b}_1, \tilde{b}_2, \tilde{b}_3) = X^{\ell+1} + \sum_{i=0}^{\ell}(\sum_{j=0}^{4} d_{k,i,j}(\tilde{b}_1, \tilde{b}_2)\tilde{b}_3^j)X^i,$$

by Equation (28) and Appendix B.2. Table 3 contains the same information as Table 1, but the first part concerns the polynomials with the Gundlach invariants and the second the polynomials with the $\tilde{b}_i$ invariants.

We can see that there is a gain in terms of memory space, except for $\ell = 5$, which corresponds to the ramified case. The degrees are larger with the $\tilde{b}_i$ but there also are relations modulo 4 between the exponents.

5.3 Examples of isogenous curves

The modular polynomials allow one to compute hyperelliptic curves with isogenous Jacobians. In particular over finite field as the β-polynomials found can be reduced modulo a prime number $p \not| 6\beta\overline{\beta}$ without losing their meaning ([6, Section 6, page 511]).

We begin with examples of curves found when working on $\mathbb{Q}(\sqrt{2})$ and taking the Gundlach invariants. The Jacobians of the following curves are $(3 + \sqrt{2})$-isogenous over $\mathbb{F}_{2333}$:

$$\begin{aligned} Y^2 &= 356X^6 + 116X^5 + 1589X^4 + 986X^3 + 178X^2 + 1094X + 1229, \\ Y^2 &= 144X^6 + 2096X^5 + 387X^4 + 1562X^3 + 478X^2 + 486X + 1718 \end{aligned}$$

while the Jacobians of the following ones are $(5 + 2\sqrt{2})$-isogenous over $\mathbb{F}_{345267203}$:

5	22 KB	5	3	5	10	10	10	53
11	3.5 MB	10	7	10	40	40	40	252
19	33 MB	16	12	16	64	64	64	513
29	188 MB	25	20	25	100	100	100	830
31	248 MB	26	21	26	104	104	104	885
41	785 MB	35	29	35	140	140	140	1191
59	3.6 GB	50	43	50	200	200	200	1820
5	26 KB	16	8	8	31	19	22	5
11	308 KB	72	40	40	84	52	52	11
19	3.6 MB	128	96	96	132	103	108	25
29	21 MB	200	152	152	212	160	168	44
31	28 MB	216	160	160	224	173	172	47
41	115 MB	288	240	240	324	272	272	69
59	470 MB	424	352	352	440	373	370	109

Table 3: Information about the modular polynomials for $D = 5$

$$\begin{aligned} Y^2 &= 288618938X^5 + 208826828X^4 + 73681500X^3 + 329580565X^2 + \\ &\quad 193693317X + 328425210, \\ Y^2 &= 229859713X^5 + 180037958X^4 + 95105703X^3 + 68631100X^2 + \\ &\quad 32660205X + 107566399 \end{aligned}$$

and the Jacobians of the curves hereafter are $(7+\sqrt{2})$-isogenous over $\mathbb{F}_{3526982779}$:

$$\begin{aligned} Y^2 &= 3476666651X^5 + 2997006123X^4 + 2343918968X^3 + 1313289865X^2 + \\ &\quad 1251164949X + 1521154595, \\ Y^2 &= 2390845907X^6 + 2649299485X^5 + 3307186776X^4 + 2143442296X^3 + \\ &\quad 1448110737X^2 + 918458873X + 1476608496. \end{aligned}$$

We also give two examples of pairs of curves computed with the β-modular polynomials with the Gundlach invariants for $\mathbb{Q}(\sqrt{5})$. First example of curves for $(4-(1+\sqrt{5})/2)$-isogenies over $\mathbb{F}_{56311}$:

$$\begin{aligned} Y^2 &= 13477X^5 + 6136X^4 + 35146X^3 + 28148X^2 + 7150X + 19730, \\ Y^2 &= 2953X^5 + 26725X^4 + 14100X^3 + 6565X^2 + 22149X + 19740 \end{aligned}$$

and second example for $(5+2(1+\sqrt{5})/2)$-isogenies over $\mathbb{F}_{6728947}$:

$$\begin{aligned} Y^2 &= 3739712X^6 + 4881762X^5 + 6611129X^4 + 5775262X^3 + 521647X^2 + \\ &\quad 2066678X + 350732, \\ Y^2 &= 2707309X^6 + 1535264X^5 + 311501X^4 + 2965267X^3 + 3507011X^2 + \\ &\quad 101110X + 5795310. \end{aligned}$$

Finally, we give pairs of curves, whose Jacobians are $(7+2\sqrt{2})$-isogenous over $\mathbb{F}_{562789}$, computed using the β-modular polynomials with the $\tilde{b}_i$ for $\mathbb{Q}(\sqrt{2})$:

$$\begin{aligned} Y^2 &= 540913X^5 + 353915X^4 + 118050X^3 + 355166X^2 + 424096X + 379433, \\ Y^2 &= 231396X^5 + 474300X^4 + 200176X^3 + 335056X^2 + 345222X + 464702 \end{aligned}$$

and a pair for $(5-(1+\sqrt{5})/2)$-isogenies over $\mathbb{F}_{5362789}$, computed using the polynomials with the $\tilde{b}_i$ for $\mathbb{Q}(\sqrt{5})$:

$$\begin{aligned} Y^2 &= 2531476X^5 + 900554X^4 + 1248025X^3 + 440959X^2 + 912166X + \\ &\quad 4367293, \\ Y^2 &= 1772175X^5 + 3557482X^4 + 848889X^3 + 4562893X^2 + 146681X + \\ &\quad 475016. \end{aligned}$$

The motivated reader can check that the curves are indeed isogenous in verifying that the curves have the same zeta function (by a result of Tate [74, Theorem 1]). We have done the verification.

References

[1] W. L. Baily and A. Borel. "Compactification of Arithmetic Quotients of Bounded Symmetric Domains". In: *Annals of Mathematics* 84.3 (1966), pp. 442–528 (cit. on pp. 7, 13).

[2] T. Becker. "On Gröbner bases under specialization". In: *Applicable Algebra in Engineering, Communication and Computing* 5.1 (1994), pp. 1–8 (cit. on p. 19).

[3] C. Birkenhake and H. Lange. *Complex abelian varieties.* Vol. 302. Grundlehren der Mathematischen Wissenschaften. Springer, 2003 (cit. on pp. 7, 9, 22).

[4] C. Birkenhake and H. Wilhelm. "Humbert surfaces and the Kummer plane". In: *Transactions of the American Mathematical society* 355.5 (2003), pp. 1819–1841 (cit. on pp. 5, 11, 12).

[5] R. Bröker and K. Lauter. "Modular polynomials for genus 2". In: *LMS Journal of Computation and Mathematics* 12 (Jan. 2009), pp. 326–339. ISSN: 1461-1570 (cit. on pp. 3, 15, 21, 23, 49).

[6] R. Bröker, D. Gruenewald, and K. Lauter. "Explicit CM theory for level 2-structures on abelian surfaces". In: *Algebra & Number Theory* 5.4 (2011), pp. 495–528 (cit. on pp. 4, 32).

[7] R. Bröker, K. Lauter, and A. Sutherland. "Modular polynomials via isogeny volcanoes". In: *Mathematics of Computation* 81.278 (2012), pp. 1201–1231 (cit. on p. 3).

[8] E. H. Brooks, D. Jetchev, and B. Wesolowski. "Isogeny graphs of ordinary abelian varieties". In: *Research in Number Theory* 3.1 (2017), p. 28 (cit. on p. 4).

[9] J. H. Bruinier. "Hilbert modular forms and their applications". In: *The 1-2-3 of modular forms.* Springer, 2008, pp. 105–179 (cit. on pp. 8, 9, 40).

[10] D. Charles, K. Lauter, and E. Goren. "Cryptographic hash functions from expander graphs". In: *Journal of Cryptology* 22.1 (2009), pp. 93–113 (cit. on p. 3).

[11] J. Couveignes and R. Lercier. "Elliptic periods for finite fields". In: *Finite fields and their applications* 15.1 (2009), pp. 1–22 (cit. on p. 3).

[12] L. De Feo, D. Jao, and J. Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247 (cit. on p. 3).

[13] C. Doche, T. Icart, and D. Kohel. "Efficient scalar multiplication by isogeny decompositions". In: *Public Key Cryptography-PKC 2006* (2006), pp. 191–206 (cit. on p. 3).

[14] A. Dudeanu. “Computational Aspects of Jacobians of Hyperelliptic Curves”. PhD thesis. École Polytechnique Fédérale de Lausanne, 2016 (cit. on p. 22).

[15] A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille. “Cyclic Isogenies for Abelian Varieties with Real Multiplication” (cit. on p. 22).

[16] R. Dupont. “Moyenne arithmético-géométrique, suites de Borchardt et applications”. PhD thesis. École polytechnique, 2006 (cit. on pp. 3–7, 16, 17, 23, 47, 48, 53).

[17] R. Dupont. “Fast evaluation of modular functions using Newton iterations and the AGM”. In: *Mathematics of Computation* 80.275 (2011), pp. 1823–1847 (cit. on p. 47).

[18] N. Elkies. “Elliptic and modular curves over finite fields and related computational issues”. In: *Computational perspectives on number theory: Proceedings of the conference in honor of A.O.L. Atkin.* Vol. 7. AMS/IP Studies in Advanced Mathematics. AMS, 1998, pp. 21–76 (cit. on p. 3).

[19] N. Elkies and A. Kumar. “K3 surfaces and equations for Hilbert modular surfaces”. In: *Algebra and Number Theory* 8.10 (2014), pp. 2297–2411 (cit. on pp. 7, 9, 15, 44).

[20] A. Enge. “Computing modular polynomials in quasi-linear time”. In: *Math. Comp* 78.267 (2009), pp. 1809–1824 (cit. on p. 3).

[21] A. Enge and A. Sutherland. “Class invariants by the CRT method, ANTS IX: Proceedings of the Algorithmic Number Theory 9th International Symposium”. In: *Lecture Notes in Computer Science* 6197 (July 2010), pp. 142–156 (cit. on p. 3).

[22] A. Enge and E. Thomé. “Computing class polynomials for abelian surfaces”. In: *Experimental Mathematics* 23.2 (2014), pp. 129–145 (cit. on pp. 16, 48).

[23] A. Enge and F. Morain. “Comparing invariants for class fields of imaginary quadratic fields”. In: *Algorithmic number theory.* Springer, 2002, pp. 252–266 (cit. on p. 3).

[24] E. Freitag. “Hilbert modular forms”. In: *Hilbert Modular Forms.* Springer, 1990, pp. 5–71 (cit. on p. 8).

[25] S. Galbraith, F. Hess, and N. Smart. “Extending the GHS Weil descent attack”. In: *Advances in Cryptology—EUROCRYPT 2002.* Springer. 2002, pp. 29–44 (cit. on p. 3).

[26] J. von zur Gathen and G. Jürgen. *Modern Computer Algebra.* New York, NY, USA: Cambridge University Press, 1999. ISBN: 0-521-64176-4 (cit. on p. 21).

[27] P. Gaudry. “Algorithmique des courbes hyperelliptiques et applications à la cryptologie”. PhD thesis. École Polytechnique, 2000 (cit. on p. 3).

[28] P. Gaudry. “Fast genus 2 arithmetic based on Theta functions”. In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265 (cit. on p. 3).

[29] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. “The 2-adic CM method for genus 2 curves with application to cryptography”. In: *International Conference on the Theory and Application of Cryptology and Information Security.* Springer. 2006, pp. 114–129 (cit. on p. 20).

[30] G. van der Geer. “On the geometry of a Siegel modular threefold”. In: *Math. Ann.* 260.3 (1982), pp. 317–350 (cit. on p. 12).

[31] G. van der Geer. *Hilbert modular surfaces.* Vol. 16. Springer Science & Business Media, 2012 (cit. on pp. 8, 9, 15).

[32] E. Z. Goren. *Lectures on Hilbert modular varieties and modular forms.* American Mathematical Soc., 2002 (cit. on p. 8).

[33] D. Gruenewald. "Explicit algorithms for Humbert surfaces". http://www.maths.usyd.edu.au/u/davidg/thesis.html. PhD thesis. University of Sydney, 2008 (cit. on pp. 11, 12, 46, 50).

[34] K.-B. Gundlach. "Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers $\mathbb{Q}(\sqrt{5})$". In: *Math. Annalen* 152 (1963), pp. 226–256 (cit. on pp. 5, 40, 41).

[35] K.-B. Gundlach. "Die Bestimmung der Funktionen zu einigen Hilbertschen Modulgruppen". In: *Journal für die reine und angewandte Mathematik* 220 (1965) (cit. on pp. 5, 40, 41).

[36] F. Hirzebruch and D. Zagier. "Classification of Hilbert Modular Surfaces". In: *Complex Analysis and Algebraic Geometry.* Ed. by W. L. J. Baily and T. Shioda. Cambridge University Press, 1977, pp. 43–78 (cit. on p. 44).

[37] G. Humbert. "Sur les fonctions abéliennes singulières I". In: *Journal de Mathématiques Pures et Appliquées, serie 5* V (1899), pp. 233–350 (cit. on p. 11).

[38] G. Humbert. "Sur les fonctions abéliennes singulières II". In: *Journal de Mathématiques Pures et Appliquées, serie 5* VI (1900), pp. 279–386 (cit. on p. 11).

[39] G. Humbert. "Sur les fonctions abéliennes singulières III". In: *Journal de Mathématiques Pures et Appliquées, serie 5* VII (1901), pp. 97–124 (cit. on p. 11).

[40] J. Igusa. "Arithmetic variety of moduli for genus 2". In: *Annals of Mathematics* 72.3 (1960) (cit. on pp. 3, 5, 8).

[41] J. Igusa. "On Siegel modular forms of genus 2". In: *American Journal of Mathematics* 84.1 (1962) (cit. on pp. 3, 5, 8).

[42] J. Igusa. "Modular Forms and Projective Invariants". In: *American Journal of Mathematics* 89.3 (1967) (cit. on pp. 7, 8).

[43] M. Kalkbrener. "On the stability of Gröbner bases under specializations". In: *Journal of Symbolic Computation* 24.1 (1997), pp. 51–58 (cit. on p. 19).

[44] O. King. "The subgroup structure of finite classical groups in terms of geometric configurations". In: *Surveys in Combinatorics 2005.* Ed. by B. S. Webb. Cambridge University Press, 2005, pp. 29–56 (cit. on p. 26).

[45] H. Labrande. "Explicit computation of the Abel-Jacobi map and its inverse". PhD thesis. Université de Lorraine, 2016 (cit. on pp. 6, 16).

[46] H. Labrande. "Computing Jacobi's theta in quasi-linear time". In: *Math. Comp.* 87 (2018), pp. 1479–1508 (cit. on p. 17).

[47] H. Labrande and E. Thomé. "Computing theta functions in quasi-linear time in genus two and above". In: *LMS Journal of Computation and Mathematics* 19.A (2016), pp. 163–177 (cit. on pp. 6, 16, 17).

[48] K. Lauter, M. Naehrig, and T. Yang. "Hilbert theta series and invariants of genus 2 curves". In: *Journal of Number Theory* (2015) (cit. on p. 51).

[49] K. Lauter and T. Yang. "Computing genus 2 curves from invariants on the Hilbert moduli space". In: *Journal of Number Theory, Elliptic Curve Cryptography* 131, Issue 5 (2011) (cit. on pp. 5, 10, 40, 42, 43).

[50] K. E. Lauter and D. Robert. “Improved CRT Algorithm for Class Polynomials in Genus 2”. In: *ANTS X — Proceedings of the Tenth Algorithmic Number Theory Symposium.* Vol. 1. The Open Book Series. Mathematical Sciences Publisher, 2013, pp. 437–461 (cit. on p. 4).

[51] A. K. Lenstra, H. W. Lenstra, and L. Lovász. “Factoring polynomials with rational coefficients”. In: *Mathematische Annalen* 261.4 (1982), pp. 515–534 (cit. on p. 19).

[52] R. Manni. “Modular varieties with level 2 theta structure”. In: *American Journal of Mathematics* 116 (1994), pp. 1489–1511 (cit. on p. 8).

[53] C. Martindale. “Isogeny Graphs, Modular Polynomials, and Applications”. PhD thesis. Universiteit Leiden, 2018 (cit. on pp. 6, 43).

[54] C. Martindale. “Hilbert modular polynomials”. In: (2019). URL: `https://hal.inria.fr/hal-01990298/` (cit. on p. 6).

[55] E. Milio. “A quasi-linear time algorithm for computing modular polynomials in dimension 2”. In: *LMS Journal of Computation and Mathematics* 18.1 (2015). `https://members.loria.fr/EMilio/`, pp. 603–632 (cit. on pp. 3, 4, 17, 18, 23, 28, 47, 49, 52).

[56] J. S. Milne. “Introduction to Shimura varieties”. In: *Harmonic analysis, the trace formula, and Shimura varieties* 4 (2005), pp. 265–378 (cit. on p. 15).

[57] F. Morain. “Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques”. In: *Journal de théorie des nombres de Bordeaux* 7 (1995), pp. 255–282 (cit. on p. 3).

[58] R. Müller. “Hilbertsche modulformen und modulfunktionen zu $\mathbb{Q}(\sqrt{8})$”. In: *Mathematische Annalen* 266.1 (1983), pp. 83–103 (cit. on pp. 41, 43).

[59] R. Müller. “Hilbertsche Modulformen und Modulfunktionen zu $\mathbb{Q}(\sqrt{5})$”. In: *Archiv der Mathematik* 45.3 (1985), pp. 239–251 (cit. on pp. 41, 43).

[60] D. Mumford. *Tata lectures on theta II.* Vol. 43. Progress in Mathematics. Birkhäuser, 1984 (cit. on p. 8).

[61] S. Nagaoka. “On the ring of Hilbert modular forms over $\mathbb{Z}$”. In: *Journal Math. Soc. Japan* 35.4 (1983), pp. 589–608 (cit. on pp. 8, 40, 41).

[62] A. Novocin, D. Stehlé, and G. Villard. “An LLL-reduction algorithm with quasi-linear time complexity”. In: *Proceedings of the forty-third annual ACM symposium on Theory of computing.* ACM. 2011, pp. 403–412 (cit. on pp. 19, 21).

[63] H. Resnikoff. “On the Graded Ring of Hilbert Modular Forms Associated with $\mathbb{Q}(\sqrt{5})$”. In: *Math. Ann.* 208 (1974), pp. 161–170 (cit. on pp. 5, 42, 43).

[64] D. Robert. “Computing cyclic isogenies using real multiplication”. (Notes). ANR Peace meeting, Paris. Apr. 2013. URL: `http://www.normalesup.org/~robert/pro/publications/notes/2013-04-Peace-Paris-Cyclic-Isogenies.pdf` (cit. on p. 22).

[65] A. Rostovtsev and A. Stolbunov. “Public-key cryptosystem based on isogenies”. In: *International Association for Cryptologic Research. Cryptology ePrint Archive* (2006) (cit. on p. 3).

[66] B. Runge. “Endomorphism rings of abelian surfaces and projective models of their moduli spaces”. In: *Tohoku mathematical journal* 51.3 (1999), pp. 283–303 (cit. on pp. 5, 11, 45).

[67] R. Schoof. “Counting points on elliptic curves over finite fields”. In: *Journal de théorie des nombres de Bordeaux* 7.1 (1995), pp. 219–254 (cit. on p. 3).

[68] J.-P. Serre. “Le Problème des Groupes de Congruence Pour SL_2”. In: *Annals of Mathematics* 92.3 (1970), pp. 489–527 (cit. on p. 13).

[69] N. Smart. “An analysis of Goubin’s refined power analysis attack”. In: *Cryptographic Hardware and Embedded Systems-CHES 2003* (2003), pp. 281–290 (cit. on p. 3).

[70] B. Smith. “Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves,” in: *Journal of Cryptology* 22.4 (2009), pp. 505–529 (cit. on p. 3).

[71] M. Streng. “Complex multiplication of abelian surfaces”. PhD thesis. Universiteit Leiden, 2010 (cit. on pp. 7, 39).

[72] M. Streng. “Computing Igusa class polynomials”. In: *Mathematics of Computation* 83.285 (2014), pp. 275–309 (cit. on p. 39).

[73] A. Sutherland. “Computing Hilbert class polynomials with the Chinese remainder theorem”. In: *Mathematics of Computation* 80.273 (2011), pp. 501–538 (cit. on p. 3).

[74] J. Tate. “Endomorphisms of Abelian Varieties over Finite Fields”. In: *Inventiones mathematicae* 2 (1966), pp. 133–144 (cit. on p. 34).

[75] E. Teske. “An elliptic curve trapdoor system”. In: *Journal of cryptology* 19.1 (2006), pp. 115–133 (cit. on p. 3).

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex
Institut de Mathématiques de Bordeaux, 351 Cours de la Libération, 33400 Talence, France
E-mail adress: damien.robert@inria.fr

École Polytechnique Fédérale de Lausanne, EPFL SB MathGeom GR-JET, Switzerland
E-mail adress: enea.milio@epfl.ch

A Examples of invariants on Hilbert and Humbert surfaces

A.1 Pullback of Siegel invariants

We prove here Lemma 2.9 which states that we can always use the pullback of Igusa's invariants to get invariants for the Humbert surface.

Lemma A.1. *Let X be a subvariety of Y, with both X and Y irreducible and defined over a field F. Then the restriction map (which is not defined everywhere) on the function fields $F(Y) \dashrightarrow F(X)$ is surjective.*

Proof. This result is well-known. We give a proof for convenience. Since X is a subvariety of Y, it is a closed variety of an open locus U of Y. The inclusion $\iota : X \to U$ then yields an epimorphism of sheaves $\iota^* : O_U \to O_X$. Looking at the stalks of the generic points we deduce that the map $F(Y) \to F(X)$ (defined for functions $f \in F(Y)$ which are defined on the generic point of X) is surjective. □

Proof of Lemma 2.9. By the theory of Shimura varieties, both $(\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma) \backslash \mathcal{H}_1^2$ and $\mathrm{Sp}_4(\mathbb{Z}) \backslash \mathcal{H}_2$ are algebraic, and so is ρ, the map of Proposition 2.8. Proposition 2.8 says that the map from the symmetric Hilbert modular surface $(\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma) \backslash \mathcal{H}_1^2$ to the Siegel space is birational to its image, the Humbert surface H_{Δ_K}. Its field of functions are the symmetric Hilbert modular functions. So, by Lemma A.1, any symmetric Hilbert modular function (seen by birationality as a rational function on the Humbert surface) can be lifted to a Siegel modular function. Since the Igusa invariants generate the field of the Siegel modular functions, it suffices to check that the restriction of these invariants to H_{Δ_K} is well defined (on an open set). But the denominators of these functions is (up to a scalar multiple) χ_{10} (see Equation (1)) whose evaluation at $\Omega \in \mathcal{H}_2$ is zero when Ω is in H_1, the set of abelian surfaces isomorphic to a product of elliptic curves. By Proposition 2.7 the intersection of H_1 and H_{Δ_K} is a (union of) curves, so the Igusa invariants are well defined on $H_{\Delta_K} \setminus H_1$. □

As seen in Section 2.5, we can also always take pullbacks of theta functions (to get invariants in some level higher than one). These pullbacks will be studied further in Appendix A.5. By Theorem 2.16 these give non symmetric invariants when $D \equiv 1 \bmod 4$. More generally to get a non symmetric invariant of level 1 we could take traces of pullbacks of theta functions of higher levels.

In practice we used pullbacks of theta functions or Gundlach invariants to compute the (symmetric) Hilbert modular polynomials. The reader interested in computing them with pullbacks of Igusa invariants is advised to use a variant defined by Streng in [71, 72] to get smaller coefficients.

A.2 Gundlach invariants for $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$

When $K = \mathbb{Q}(\sqrt{2})$ or $K = \mathbb{Q}(\sqrt{5})$ there is a fundamental unit ϵ of norm -1 and such that $\epsilon > 0$ is a real number. Let $\alpha = \mathrm{diag}(1, \frac{\sqrt{\Delta_K}}{\epsilon})$. Then

$$(25) \qquad \begin{array}{cccc} \phi_0 : & \mathcal{H}_1^2 & \to & \mathcal{H}_1^2 \\ & \tau & \mapsto & \frac{\epsilon}{\sqrt{\Delta_K}}\tau \end{array} \quad \text{and} \quad \begin{array}{cccc} \phi_0 : & \mathrm{SL}_2(\mathcal{O}_K) & \to & \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \\ & \gamma & \mapsto & \alpha\gamma\alpha^{-1} \end{array}$$

are group isomorphisms which induce a commutative diagram similar to the one in Equation (5). Note that when $\epsilon > 0$ has norm -1, then $\overline{\epsilon} < 0$ so that $\frac{\epsilon}{\sqrt{\Delta_K}}$ is totally positive and $\phi_0(\tau) \in \mathcal{H}_1^2$.

Let $\{e_1, e_2\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$ and $q_j = e^{2i\pi(\epsilon e_j \tau_1 - \overline{\epsilon e_j}\tau_2)/\sqrt{\Delta_K}}$ for $j = 1, 2$ and $\tau = (\tau_1, \tau_2)$. The superscript $++$ stands for totally positive.

Proposition A.2. *Let $\mathfrak{a} \subset K$ be a fractional ideal and $\mathrm{SL}_2(\mathcal{O}_K \oplus \mathfrak{a}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(K) : a, d \in \mathcal{O}_K, b \in \mathfrak{a}^{-1}$ and $c \in \mathfrak{a}\}$. Let $\mathfrak{a}^* = \partial_K^{-1}\mathfrak{a}^{-1}$ be the dual of $\mathfrak{a}$ with respect to the trace, and $\mathfrak{a}^{*,++}$ the set of totally positive elements of $\mathfrak{a}^*$.*

Let g be a Hilbert modular form for $\mathrm{SL}_2(\mathcal{O}_K \oplus \mathfrak{a})$ of weight k. Then it has a Fourier expansion

$$g(\tau) = a_g(0) + \sum_{v \in \mathfrak{a}^{*,++}} a_g(v) e^{2\pi i \mathrm{tr}(v\tau)}.$$

Proof. See [9, Example 1.6 and Corollary 1.21]. □

Corollary A.3. *Let g be a Hilbert modular form for $\mathrm{SL}_2(\mathcal{O}_K)$ of weight k. Then it has a Fourier expansion*

$$g(\tau) = a_g(0) + \sum_{t = ae_1 + be_2 \in \mathcal{O}_K^{++}} a_g(t) q_1^a q_2^b.$$

Proof. See [49, Proposition 3.2]. By Proposition A.2 the Fourier coefficients are indexed by $\partial_K^{-1,++}$, but if $v \in \partial_K^{-1,++}$, then $v = \frac{\epsilon}{\sqrt{D}} t$ with $t = ae_1 + be_2 \in O_K^{++}$. □

We denote by $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))_k$ the $\mathbb{Z}$-module of symmetric Hilbert modular forms of even weight k with rational integral Fourier coefficients and put $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K)) = \bigoplus A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))_k$. Define the Hilbert Eisenstein series of even weight $k \geq 2$:

$$G_k(\tau) = 1 + \sum_{t = ae_1 + be_2 \in \mathcal{O}_K^{++}} b_k(t) q_1^a q_2^b,$$

where

$$b_k(t) = \kappa_k \sum_{\substack{\mu \in \mathcal{O}_K \text{ such that} \\ t\mathcal{O}_K \subset \mu\mathcal{O}_K}} |\,\mathcal{O}_K/\mu\mathcal{O}_K|^{k-1}$$

and $\kappa_k = \zeta_K(k)^{-1}(2\pi)^{2k}((k-1)!)^{-2}\Delta_K^{1/2-k}$ (by [61, Equation (1.5)]).

Lemma A.4 (Gundlach)**.**

- *If $K = \mathbb{Q}(\sqrt{2})$, let $\epsilon = 1 + \sqrt{2}$. Then $\kappa_2 = 2^4 \cdot 3$, $\kappa_4 = 2^5 \cdot 3 \cdot 5 \cdot 11^{-1}$ and $\kappa_6 = 2^4 \cdot 3^2 \cdot 7 \cdot 19^{-2}$;*
- *If $K = \mathbb{Q}(\sqrt{5})$, let $\epsilon = \frac{1+\sqrt{5}}{2}$. Then $\kappa_2 = 2^3 \cdot 3 \cdot 5$, $\kappa_4 = 2^4 \cdot 3 \cdot 5$, $\kappa_6 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 67^{-1}$ and $\kappa_{10} = 2^3 \cdot 3 \cdot 5^2 \cdot 11 \cdot 412751^{-1}$.*

Proof. See [34, 35]. See also [61, Lemma 1.1]. □

The Hilbert Eisenstein series are symmetric Hilbert modular forms for $\mathrm{SL}_2(\mathcal{O}_K)$ with coefficients in $\mathbb{Q}$. We focus now on the cases $D = 2, 5$ and we fix the basis $\{1, \overline{\epsilon}\}$, which gives a nice expression for q_1 and q_2. We have

Theorem A.5 (Nagaoka)**.** *In the case $K = \mathbb{Q}(\sqrt{2})$, we put*

$$F_4 = 2^{-6} \cdot 3^{-2} \cdot 11(G_2^2 - G_4) \quad \textit{and} \quad F_6 = \frac{-5 \cdot 7^2}{2^8 3^3 13} G_2^3 + \frac{11 \cdot 59}{2^8 3^2 5 \cdot 13} G_2 G_4 - \frac{19^2}{2^7 3^3 5 \cdot 13} G_6.$$

Then G_2, F_4 and F_6 are in $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))_k$ for $k = 2, 4, 6$ respectively. Furthermore, they form a minimal set of generators of $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))$ over $\mathbb{Z}$.

Proof. See [61, Theorem 1]. See also [35, Page 119]. □

Theorem A.6 (Gundlach)**.** *In the case $K = \mathbb{Q}(\sqrt{2})$, the field of symmetric meromorphic Hilbert modular functions for $\mathrm{SL}_2(\mathcal{O}_K)$ are rational functions of*

$$J_1 = \frac{G_2^2}{F_4} \quad \textit{and} \quad J_2 = \frac{G_2 F_6}{F_4^2}.$$

Proof. See [35, Page 119]. See also [58, Lemma 6] or Appendix A.3. □

Definition A.7. The functions J_1 and J_2 of Theorem A.6 are called the *Gundlach invariants* for $\mathbb{Q}(\sqrt{2})$.

Theorem A.8 (Nagaoka)**.** *In the case $K = \mathbb{Q}(\sqrt{5})$, we put*

$$F_6 = \frac{67}{2^5 3^3 5^2}(G_2^3 - G_6),$$

$$F_{10} = 2^{-10} 3^{-5} 5^{-5} 7^{-1} (412751 G_{10} - 5 \cdot 67 \cdot 2293 G_2^2 G_6 + 2^2 3 \cdot 7 \cdot 4231 G_2^5),$$

$$\textit{and} \qquad F_{12} = 2^{-2}(F_6^2 - G_2 F_{10}).$$

The four modular forms G_2, F_6, F_{10} and F_{12} are in $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))_k$ for $k = 2, 6, 10$ and 12 respectively. Furthermore, they form a minimal set of generators of $A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))$ over $\mathbb{Z}$.

Proof. See [61, Theorem 2]. See also [34, Satz 5]. □

Theorem A.9 (Gundlach)**.** *In the case $K = \mathbb{Q}(\sqrt{5})$, the field of symmetric meromorphic Hilbert modular functions for $\mathrm{SL}_2(\mathcal{O}_K)$ are rational functions of*

$$J_1 = \frac{G_2^5}{F_{10}} \quad \textit{and} \quad J_2 = \frac{F_6 G_2^2}{F_{10}}.$$

Proof. See [34, Satz 6]. See also [59, Page 249] or the proof in Appendix A.3. Note that it is usual to take the invariants $\frac{G_2^5}{F_{10}}$ and $\frac{F_6}{G_2^3}$. We have substituted the last one by the product of the two. As explained in Appendix B.1 these invariants will give smaller modular polynomials than with the usual ones. Indeed we will see that the denominators of the invariants determine the denominators of the modular polynomials so that it is better to have fewer factors. □

Definition A.10. The functions J_1 and J_2 of Theorem A.9 are called the *Gundlach invariants* for $\mathbb{Q}(\sqrt{5})$.

A.3 Gundlach and pullbacks of the Igusa invariants

For $D = 2, 5$, a fundamental unit has norm -1 and it will be more convenient to work with the basis $\{1, \bar{\epsilon}\}$, which was used to define the Fourier coefficients of the symmetric Hilbert modular forms in Appendix A.2. Let

$$\phi_1 := \phi_{1,\bar{\epsilon}} \qquad \text{and} \qquad \phi_\epsilon := \phi_1 \circ \phi_0, \tag{26}$$

where ϕ_0 denotes the isomorphisms of Equation (25). The map ϕ_ϵ satisfies similar equalities as in Proposition 2.3 between the action of $\mathrm{SL}_2(\mathcal{O}_K)$ on $\mathcal{H}_1^2$ and the action of $\mathrm{Sp}_4(\mathbb{Z})$ on $\mathcal{H}_2$. It also maps to the Humbert surface and Proposition 2.8 applies with ϕ_ϵ instead of ϕ_{e_1,e_2}.

For a basis $\{e_1, e_2\}$, we give in Proposition A.11 the relation between the Fourier coefficients of a Siegel modular form f and the coefficients of its pullback $\phi_{e_1,e_2}^* f$, which is a symmetric Hilbert modular form. Recall Equation (6) for the definition of ϕ_{e_1,e_2} and recall that q_1 and q_2 are defined just before Proposition A.2. The superscript $++$ stands for totally positive.

Proposition A.11. *Let*

$$Sym_2(\mathbb{Z})^\vee = \left\{ T = \begin{pmatrix} m_1 & \frac{1}{2}m \\ \frac{1}{2}m & m_2 \end{pmatrix} : m_i, m \in \mathbb{Z} \right\}$$

be the dual of $Sym_2(\mathbb{Z})$ and let $Q_T(x_1, x_2) = (x_1, x_2)T\binom{x_1}{x_2}$ be the positive definite quadratic form associated to T. Let

$$f(\Omega) = a_f(0) + \sum_{T \in Sym_2(\mathbb{Z})^{\vee,++}} a_f(T) q^T$$

be a Siegel modular form for $\mathrm{Sp}_4(\mathbb{Z})$ of weight k, where $q^T = e^{2i\pi \mathrm{tr}(T\Omega)}$. Then its pullback $g = \phi_{e_1,e_2}^* f$ is a symmetric Hilbert modular form with the following Fourier expansion:

$$g(\tau) = f(\phi_{e_1,e_2}(\tau)) = a_g(0) + \sum_{t = ae_1 + be_2 \in \mathcal{O}_K^{++}} a_g(t) q_1^a q_2^b,$$

with $a_g(0) = a_f(0)$ and

$$a_g(t) = \sum_{\substack{T \in Sym_2(\mathbb{Z})^{\vee,++} \\ Q_T(e_1,e_2) = t}} a_f(T).$$

Proof. See [49, Proposition 3.2]. □

We are interested in the pullbacks of the Igusa invariants (defined in Equation (1)). They are already known in the case $D = 5$.

Theorem A.12 (Resnikoff)**.** *For $K = \mathbb{Q}(\sqrt{5})$ we have*

$$\begin{array}{rcl} \phi_\epsilon^* \psi_4 & = & G_2^2; \\ \phi_\epsilon^* \psi_6 & = & -\frac{42}{25} G_2^3 + \frac{67}{25} G_6 = G_2^3 - 2^5 3^3 F_6; \\ -4\phi_\epsilon^* \chi_{10} & = & F_{10}; \\ 12\phi_\epsilon^* \chi_{12} & = & 3F_6^2 - 2G_2 F_{10}. \end{array}$$

Proof. See [63, Theorem 1]. □

Corollary A.13 (Lauter-Yang)**.** *One has*

$$\begin{array}{rcl} \phi_\epsilon^* \mathfrak{j}_1 & = & 8J_1(3J_2^2/J_1-2)^5; \\ \phi_\epsilon^* \mathfrak{j}_2 & = & \frac{1}{2}J_1(3J_2^2/J_1-2)^3; \\ \phi_\epsilon^* \mathfrak{j}_3 & = & 2^{-3}J_1(3J_2^2/J_1-2)^2(4J_2^2/J_1+2^5 3^2 J_2/J_1-3). \end{array}$$

Proof. See [49, Proposition 4.5]. □

We did not find in the literature a similar result as Theorem A.12 for $\mathbb{Q}(\sqrt{2})$. Using Proposition A.11 and comparing the different Fourier series (as done in [63] in the case $D=5$) we have found

Theorem A.14. *For $K=\mathbb{Q}(\sqrt{2})$ we have*

$$\begin{array}{rcl} \phi_\epsilon^* \psi_4 & = & G_2^2+144F_4; \\ \phi_\epsilon^* \psi_6 & = & G_2^3-648F_4G_2-1728F_6; \\ \phi_\epsilon^* \chi_{10} & = & -\frac{1}{4}F_4F_6; \\ \phi_\epsilon^* \chi_{12} & = & \frac{1}{12}G_2F_4F_6+F_4^3+F_6^2. \end{array}$$

Corollary A.15. *One has*

$$\begin{array}{rcl} \phi_\epsilon^* \mathfrak{j}_1 & = & 8J_1^3/J_2(1+12/J_2+12J_2/J_1)^5; \\ \phi_\epsilon^* \mathfrak{j}_2 & = & J_1^2/J_2/2(J_1+144)(1+12/J_2+12J_2/J_1)^3; \\ \phi_\epsilon^* \mathfrak{j}_3 & = & 1/8(1+12/J_2+12J_2/J_1)^2 \cdot \\ & & (J_1^3/J_2+16J_1^2+16J_1^3/J_2^2+2304J_1^2/J_2^2+408J_1^2/J_2+2880J_1). \end{array}$$

Proof of Theorems A.6 and A.9. By Lemma 2.9, any symmetric Hilbert modular function is a rational function with complex coefficients in the pullbacks of the Igusa invariants. By Corollaries A.15 and A.13, the pullbacks of the Igusa invariants can be expressed in terms of the Gundlach invariants for $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ respectively. Thus each symmetric Hilbert modular function can be expressed in terms of the Gundlach invariants. □

A.4 Other invariants

By Müller [59], non-symmetric Gundlach invariants for $\mathbb{Q}(\sqrt{5})$ can be obtained by considering the Hilbert modular forms

$$F_{15}^2 = 16(5^5F_{10}^3 - 5^3G_2^2F_6F_{10}^2/2 + G_2^5F_{10}^2/2^4 + 3^2 5^2 G_2F_6^3F_{10}/2 - G_2^4F_6^2F_{10}/2^3 - 2\cdot 3^3F_6^5 + G_2^3F_6^4/2^4),$$

$$F_5^2 = F_{10}$$

and by defining the modular function $J_3 = F_{15}/F_5^3$. To use interpolation to compute non-symmetric Hilbert modular polynomials for J_1, J_2 and J_3, we need the equation of the Hilbert modular surface, which is given by

$$J_3^2 = (J_1^3 + (-2J_2^2 - 1000J_2 + 50000)J_1^2 + (J_2^4 + 1800J_2^3)J_1 - 864J_2^5)/(16J_1^2).$$

Müller gives an expression of F_5 and of F_{15} in terms of theta constants so J_3 can be efficiently evaluated at $\tau \in \mathcal{H}_1^2$. The polynomials obtained are smaller than the symmetric ones with J_1 and J_2 only, as they are not symmetric and thus parameterize only β-isogenies. We refer to Martindale [53] for more details on the polynomials coming from these invariants.

Similarly for $\mathbb{Q}(\sqrt{2})$, see the work of Müller [58].

In fact in these two cases the Hilbert surface is rational (that is birational to $\mathbb{P}^2$):

Theorem A.16. *The Hilbert modular surface is rational for $D = 2, 3, 5, 13, 17$.*

Proof. See [36, Theorem 3]. □

The paper [19] of Elkies and Kumar allows to get the corresponding birational isomorphisms. For instance, for $\mathbb{Q}(\sqrt{5})$, they give an explicit birational isomorphism between the Humbert surface H_5 and $\mathbb{P}^2$ (different from the one induced by the Gundlach invariants), and show that a birational model over $\mathbb{Q}$ of the non symmetric Hilbert modular surface is given by the double cover of $\mathbb{P}^2$

$$z^2 = 2(6250h^2 - 4500g^2h - 1350gh - 108h - 972g^5 - 324g^4 - 27g^3).$$

As this surface is also rational by Theorem A.16, a parametrization is obtained, given by the modular functions m and n. We have by [19, Section 6]

$$m = -(5g^2 + 3g/2 - 125h/9 + 3/25)/(g^2 + 13g/30 + 1/25), \qquad n = z/(18(g^2 + 13g/30 + 1/25))$$

and

$$g = (m^2 - 5n^2 - 9)/30, \quad k = 3m(10g + 3)(15g + 2)/6250,$$
$$h = k + 9(250g^2 + 75g + 6)/6250, \quad z = 3n(10g + 3)(15g + 2)/25.$$

Using these equations, [19, Corollary 15] (linking the Igusa-Clebsh invariants with g and h) and Theorem A.12, we have found the relations

$$g = -J_1/(6J_2^2), \quad h = J_1^2/J_2^5 \quad \text{and} \quad z = -F_5^3F_{15}/(2F_6^5) \tag{27}$$

from which we can compute m, n explicitly. The functions g and h are easy to evaluate from the Gundlach invariants. For z, we use the expression of F_i in terms of theta constant or the equation of the double cover given above and the first coefficients of the Fourier series of z for the choice of the square root.

More generally, equations for Humbert and Hilbert surfaces are given in [19] for every quadratic field $\mathbb{Q}(\sqrt{\Delta})$ for all thirty fundamental discriminants Δ with $1 < \Delta < 100$. We can then use their results to get non symmetric invariants for all these fields. Furthermore, the equation of the Humbert surface for these fields is always rational, so we only need two symmetric invariants (like the Gundlach case for $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{2})$) and don't need to take the pullback of the Igusa invariants for these fields. The difficulty resides in the optimization of these invariants: for instance for computing modular polynomials it is better if they have the same denominator.

A.5 Components of Humbert surfaces of level 2 and $(2, 4)$

This is a complement to Section 2.5.

Proposition A.17. *The subgroups $\tilde{\Gamma}(2)$ and $\tilde{\Gamma}(2,4)$ of $\tilde{\Gamma}(1)$ are of index*

$$\begin{cases} 36 & \textit{and} & 576, & \textit{if } D \equiv 1 \bmod 8; \\ 60 & \textit{and} & 960, & \textit{if } D \equiv 5 \bmod 8; \\ 48 & \textit{and} & 192, & \textit{if } D \equiv 2, 3 \bmod 4. \end{cases}$$

Proof. We do the proof for $\tilde{\Gamma}(2,4)$ as the other one is similar. Note that $\tilde{\Gamma}(1)/\tilde{\Gamma}(4) \simeq \mathrm{SL}_2(\mathcal{O}_K/4\mathcal{O}_K)$. We have then that $\mathcal{O}_K/4\mathcal{O}_K$ is isomorphic to

- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ when 2 is split, namely when $D \equiv 1 \bmod 8$;
- $\mathbb{Z}/4\mathbb{Z}[X]/(X^2+X+1)$ when 2 is inert, namely when $D \equiv 5 \bmod 8$;
- $\mathbb{Z}/4\mathbb{Z}[X]/(X^2-D)$ when 2 is ramified, namely when $D \equiv 2,3 \bmod 4$.

The cardinality of $\mathrm{SL}_2(\mathcal{O}_K/4\mathcal{O}_K)$ is then 48^2, 3840 and 3072 respectively. Moreover, the index of the subgroup $\tilde{\Gamma}(4)$ of $\tilde{\Gamma}(2,4)$ is 4 when $D \equiv 1 \bmod 4$ and 16 when $D \equiv 2,3 \bmod 4$. As these two sets are normal subgroups of $\tilde{\Gamma}(1)$, the third isomorphism theorem of groups gives us the desired results. □

Proposition A.18 (Besser, Runge). *The number of Humbert surface components for* $\Gamma(2)$ *and for* $\Gamma(2,4)$ *is respectively*

$$\begin{cases} 10 & \textit{if } D \equiv 1 \bmod 8 \\ 6 & \textit{if } D \equiv 5 \bmod 8 \\ 15 & \textit{if } D \equiv 2,3 \bmod 4 \end{cases} \quad \textit{and} \quad \begin{cases} 10 & \textit{if } D \equiv 1 \bmod 8 \\ 6 & \textit{if } D \equiv 5 \bmod 8 \\ 60 & \textit{if } D \equiv 2,3 \bmod 4 \end{cases}$$

Proof. The numbers for $\Gamma(2)$ are due to Besser and the other ones to Runge. See [66, Page 293]. An heuristic argument for $\Gamma(2,4)$ is that given $P(b_1,b_2,b_3)$, the Humbert component $H^{\mathcal{G}}_{\Delta_K}$ which is the image of $\phi_{1,\omega}$ and $\Omega = \phi_{1,\omega}(\tau) \in \mathcal{H}_2$, then for any $\gamma \in \Gamma(2,4)\backslash\mathrm{Sp}_4(\mathbb{Z})$, we have that $P(b_i(\gamma\Omega)) = 0$ only for the matrices γ which come from the image of $\phi_{1,\omega}(\tilde{\Gamma}(2,4)\backslash\tilde{\Gamma}(1))$ and of $\phi_{1,\omega}(\tilde{\Gamma}(2,4)\sigma\backslash\tilde{\Gamma}(1))$ in $\Gamma(2,4)\backslash\mathrm{Sp}_4(\mathbb{Z})$. The number of components corresponds to the number

$$v(D) \cdot |\Gamma(2,4)\backslash\mathrm{Sp}_4(\mathbb{Z})|/|\tilde{\Gamma}(2,4)\backslash\tilde{\Gamma}(1)|,$$

where $v(D)$ is 1 if $D \equiv 2,3 \bmod 4$ and $\frac{1}{2}$ if $D \equiv 1 \bmod 4$. This argument works also for $\Gamma(2)$. (Recall that $|\Gamma(2,4)\backslash\mathrm{Sp}_4(\mathbb{Z})| = 11520$ and $|\Gamma(2)\backslash\mathrm{Sp}_4(\mathbb{Z})| = 720$.)

This is easier to see via the modular interpretation. Let $\Gamma = \Gamma(2)$ (respectively $\Gamma(2,4)$). Then an element of $\Gamma\backslash\mathcal{H}_2$ corresponds to a principally polarized abelian surface with a symplectic basis of the 2-torsion (resp. a symmetric theta structure of level 2). The cover $\Gamma\backslash\mathcal{H}_2 \to \mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$ corresponds to forgetting this extra structure, and the fibers form a torsor under the isomorphisms of this extra structure, which are equal to $\Gamma(2)\backslash\mathrm{Sp}_4(\mathbb{Z})$ (resp. $\Gamma(2,4)\backslash\mathrm{Sp}_4(\mathbb{Z})$).

The same is true for the map $H^{\mathcal{G}}_{\Delta_K} \simeq \mathcal{G}\backslash\mathcal{H}_1^2 \to H^{\Gamma}_{\Delta_K} \simeq \tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma\backslash\mathcal{H}_1^2$ and the action of $\mathcal{G}\backslash\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma$ on the fibers, where $\mathcal{G}$ is $\tilde{\Gamma}(2)$ (resp. $\tilde{\Gamma}(2,4)$) when $D \equiv 1 \bmod 4$ and $\tilde{\Gamma}(2)\cup\tilde{\Gamma}(2)\sigma$ (resp. $\tilde{\Gamma}(2,4) \cup \tilde{\Gamma}(2,4)\sigma$) when $D \equiv 2,3 \bmod 4$. Except that here the extra structure has to be compatible with the action of $\mathcal{O}_K$. (For instance a symmetric theta structure of level 2 is induced by a symplectic basis of the 2-torsion and a compatible symplectic decomposition of the 4-torsion into maximal isotropic subgroups. For this symmetric theta structure to be compatible with the action of $\mathcal{O}_K$, these maximal isotropic subgroups have to be stable under the action of $\mathcal{O}_K$).

In particular on the Humbert component $H^{\mathcal{G}}_{\Delta_K}$, then the action of $\mathcal{G}\backslash\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma$ permutes the fibers. Since this quotient is isomorphic to $\Gamma(2)\backslash\phi_{1,\omega}(\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma)\Gamma(2)$ (resp. to $\Gamma(2,4)\backslash\phi_{1,\omega}(\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma)\Gamma(2,4)$) this means that the action of $\left(\phi_{1,\omega}(\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma)\Gamma(2)\right)\backslash\mathrm{Sp}_4(\mathbb{Z})$ (resp. $\phi_{1,\omega}(\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma)\Gamma(2,4)\backslash\mathrm{Sp}_4(\mathbb{Z})$), which is not compatible with $\mathcal{O}_K$, permutes the components. □

We give the equations of the Humbert component corresponding to the image of $\phi_{1,\omega}$ for $\Gamma(2,4)$ and $D = 2,\ 3,\ 5$

$$\begin{gathered} b_1 - \tfrac{1}{2}(b_2^2 + b_3^2) = 0; \\ -b_1^4 - b_2^4 - 4b_3^2 - 2b_1^2b_2^2 + 4b_1b_2 + 4b_1b_2b_3^2 = 0; \\ \tfrac{-1}{2}(\textstyle\sum_i b_i^4 + \sum_i \sum_{j\neq i}(b_ib_j)^4) + b_1b_2b_3(1 + \sum_i b_i^4 - b_1b_2b_3) = 0 \end{gathered} \tag{28}$$

and similarly for $\Gamma(2)$ and $D = 2$ only, as for $D = 3$ the equations are too big to be put in the paper,

$$\begin{gathered} ((16r_3^2 - 16r_3)r_2^2 + (-16r_3^2 + 16r_3)r_2)r_1^4 + ((-16r_3^2 + 16r_3)r_2^3 + (-16r_3^3 + 16r_3^2)r_2^2 + \\ (16r_3^3 - 16r_3)r_2)r_1^3 + (-r_2^4 + (16r_3^3 - 16r_3 + 2)r_2^3 + (-14r_3^2 + 14r_3 - 1)r_2^2 + \\ (-16r_3^3 + 14r_3^2 + 2r_3)r_2 + (-r_3^4 + 2r_3^3 - r_3^2))r_1^2 + (2r_3r_2^4 + (-16r_3^3 + 14r_3^2 - 2r_3)r_2^3 + \\ (14r_3^3 - 12r_3^2)r_2^2 + (2r_3^4 - 2r_3^3)r_2)r_1 + (-r_3^2r_2^4 + 2r_3^3r_2^3 - r_3^4r_2^2) = 0. \end{gathered} \tag{29}$$

These equations were computed by Gruenewald in [33], where he gives equations for components of Humbert surfaces for many discriminants and many models.

B Examples of Hilbert modular polynomials

We apply now the results of the Sections 3 and 4 with Gundlach invariants for $D = 2, 5$ and with pullbacks of theta functions. We also propose non symmetric invariants.

B.1 Modular polynomials with Gundlach invariants

Evaluation and inversion: We first illustrate Theorem 3.4 for the Gundlach invariants J_1, J_2 defined for $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ in Definition A.7 and A.10. The only small difference is that we use the map ϕ_ϵ defined in Equation (26) rather than the map $\phi_{1,\omega}$ (Equation (6)) to map Hilbert matrices $\tau \in \mathcal{H}_1^2$ to Siegel matrices $\Omega \in \mathcal{H}_2$.

In this case we have already seen how to express the pullbacks of the Igusa invariants in terms of the Gundlach invariants in Appendix A.3 (see Corollaries A.13 and A.15). The expression is easier than the method outlined in Theorem 3.4 because the Gundlach invariants are expressed in terms of symmetric Hilbert modular forms whose relation to the pullbacks of the Siegel modular forms defining the Igusa invariants are very simple (see Theorems A.12 and A.14).

We outline the algorithm (Algorithm B.1) to find $\tau \in (\mathrm{SL}_2(\mathcal{O}_K) \cup \mathrm{SL}_2(\mathcal{O}_K)\sigma)\backslash\mathcal{H}_1^2$ from the values $J_1(\tau)$ and $J_2(\tau)$ at some precision N.

Algorithm B.1: $\tau \in (\mathrm{SL}_2(\mathcal{O}_K) \cup \mathrm{SL}_2(\mathcal{O}_K)\sigma)\backslash\mathcal{H}_1^2$ from $(J_1(\tau), J_2(\tau))$ at precision N

```
Data: The values $J_1(\tau)$ and $J_2(\tau)$, the working precision $N$
Result: $\tau$ modulo $\mathrm{SL}_2(\mathcal{O}_K) \cup \mathrm{SL}_2(\mathcal{O}_K)\sigma$ at precision $N$
1 Deduce $\mathrm{j}_1(\Omega)$, $\mathrm{j}_2(\Omega)$, $\mathrm{j}_3(\Omega)$ from $J_1(\tau)$, $J_2(\tau)$, where $\Omega \in \mathcal{H}_2$ such that $\Omega = \phi_\epsilon(\tau)$;
2 Deduce a period matrix $\Omega'$ at precision $N$ equivalent to $\Omega$ modulo $\mathrm{Sp}_4(\mathbb{Z})$, up to the
    precision, from the three Igusa invariants;
3 Find some $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ such that $\gamma\Omega'$ satisfies Equation (11) and deduce $\tau$;
```

The first step can be done using Corollary A.13 or A.15. The second is explained in [16, 17, 55] and can be done in $\tilde{O}(N)$. For the third step, remark that for $D = 5$, if $\tau \in \mathcal{H}_1^2$, then $\phi_\epsilon(\tau) = \left(\begin{smallmatrix}\Omega_1 & \Omega_2\\ \Omega_2 & \Omega_3\end{smallmatrix}\right) \in \mathcal{H}_2$ satisfies by definition $\Omega_1 + \Omega_2 - \Omega_3 = 0$. The second step provides $\Omega' \in \mathcal{H}_2$ which is equivalent to a period matrix in the Humbert surface H_5. Thus by Humbert's Lemma we know there exists a matrix $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ such that $\Omega'' = \gamma\Omega' = \left(\begin{smallmatrix}\Omega''_1 & \Omega''_2\\ \Omega''_2 & \Omega''_3\end{smallmatrix}\right)$ satisfies $\Omega''_1 + \Omega''_2 - \Omega''_3 = 0$ (see Remark 2.5 for the computation of γ). We have then $\tau^* = ((\frac{\epsilon}{\sqrt{\Delta_K}})^*)^{-1}\,{}^t R^{-1}\Omega'' R^{-1}$ (see Section 2.3 for the notation). For $D = 2$, $\phi_\epsilon(\tau)$ satisfies $\Omega_1 + 2\Omega_2 - \Omega_3 = 0$ and we can adapt the algorithm to find the matrix γ. Thus

Corollary B.2. *Given $J_1(\tau)$ and $J_2(\tau)$, where J_1 and J_2 are the Gundlach invariants for $D = 2$ or 5 evaluated at some $\tau \in \mathcal{H}_1^2$, we can find an approximation of $\tau \in (\mathrm{SL}_2(\mathcal{O}_K) \cup \mathrm{SL}_2(\mathcal{O}_K)\sigma)\backslash\mathcal{H}_1^2$ at precision N in time $\tilde{O}(N)$.*

For the evaluation of the Gundlach invariants, using their definition as Fourier series would not give a good enough complexity. Instead Theorem 3.4 suggests to express J_1 and J_2 in term of the $\tilde{b}_k$. Here, since the Gundlach invariants are invariants for the full modular group $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$, we can also express them directly in terms of the (pullbacks of the) Igusa invariants $\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3$. Rather than doing an interpolation using Section 3.3, Corollaries A.13 and A.15 expressing the Igusa invariants in term of the Gundlach invariants are sufficiently simple to be inverted using a Gröbner basis.

In the case $D = 5$ we have found:

$$\begin{gathered}
J_2/J_1 = (1/6912\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2 - 1/2304\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_3 - 1/3359232\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^3 + 1/373248\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^2\phi_\epsilon^*\mathrm{j}_3 + \\
1/864\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^2 - 1/124416\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2\phi_\epsilon^*\mathrm{j}_3^2 + 1/124416\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_3^3 + 1/3359232\phi_\epsilon^*\mathrm{j}_2^4 - \\
1/1119744\phi_\epsilon^*\mathrm{j}_2^3\phi_\epsilon^*\mathrm{j}_3)/(\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^2 + 1/1944\phi_\epsilon^*\mathrm{j}_2^4 - 1/648\phi_\epsilon^*\mathrm{j}_2^3\phi_\epsilon^*\mathrm{j}_3);
\end{gathered}$$

$$\begin{gathered}
J_1 = -(45349632\phi_\epsilon^*\mathrm{j}_1^3\phi_\epsilon^*\mathrm{j}_2^4 - 2584929024/5\phi_\epsilon^*\mathrm{j}_1^3\phi_\epsilon^*\mathrm{j}_2^3\phi_\epsilon^*\mathrm{j}_3 - 499571546112/5\phi_\epsilon^*\mathrm{j}_1^3\phi_\epsilon^*\mathrm{j}_2^3 + \\
11019960576/5\phi_\epsilon^*\mathrm{j}_1^3\phi_\epsilon^*\mathrm{j}_2^2\phi_\epsilon^*\mathrm{j}_3^2 + 1410554953728/5\phi_\epsilon^*\mathrm{j}_1^3\phi_\epsilon^*\mathrm{j}_2^2\phi_\epsilon^*\mathrm{j}_3 - 20815481088/5\phi_\epsilon^*\mathrm{j}_1^3\phi_\epsilon^*\mathrm{j}_2\phi_\epsilon^*\mathrm{j}_3^3 + \\
14693280768/5\phi_\epsilon^*\mathrm{j}_1^3\phi_\epsilon^*\mathrm{j}_3^4 - 186624\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2^6 + 16236288/5\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2^5\phi_\epsilon^*\mathrm{j}_3 - 12380449536/5\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2^5 - \\
23514624\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2^4\phi_\epsilon^*\mathrm{j}_3^2 + 146887458048/5\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2^4\phi_\epsilon^*\mathrm{j}_3 + 31972578951168/5\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2^4 + \\
90699264\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2^3\phi_\epsilon^*\mathrm{j}_3^3 - 651402114048/5\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2^3\phi_\epsilon^*\mathrm{j}_3^2 - 90275517038592/5\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2^3\phi_\epsilon^*\mathrm{j}_3 - \\
196515072\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2^2\phi_\epsilon^*\mathrm{j}_3^4 + 1279948013568/5\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2^2\phi_\epsilon^*\mathrm{j}_3^3 + 226748160\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2\phi_\epsilon^*\mathrm{j}_3^5 - \\
940369969152/5\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_2\phi_\epsilon^*\mathrm{j}_3^4 - 544195584/5\phi_\epsilon^*\mathrm{j}_1^2\phi_\epsilon^*\mathrm{j}_3^6 + 192\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^8 - 22464/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^7\phi_\epsilon^*\mathrm{j}_3 - \\
18289152/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^7 + 229824/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^6\phi_\epsilon^*\mathrm{j}_3^2 + 260527104/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^6\phi_\epsilon^*\mathrm{j}_3 + 30051689472/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^6 - \\
1342656/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^5\phi_\epsilon^*\mathrm{j}_3^3 - 1482541056/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^5\phi_\epsilon^*\mathrm{j}_3^2 - 171240210432/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^5\phi_\epsilon^*\mathrm{j}_3 + \\
979776\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^4\phi_\epsilon^*\mathrm{j}_3^4 + 4212476928/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^4\phi_\epsilon^*\mathrm{j}_3^3 + 243799621632/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^4\phi_\epsilon^*\mathrm{j}_3^2 - \\
2286144\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^3\phi_\epsilon^*\mathrm{j}_3^5 - 5976073728/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^3\phi_\epsilon^*\mathrm{j}_3^4 + 16656192/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^2\phi_\epsilon^*\mathrm{j}_3^6 + \\
3386105856/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2^2\phi_\epsilon^*\mathrm{j}_3^5 - 13856832/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_2\phi_\epsilon^*\mathrm{j}_3^7 + 5038848/5\phi_\epsilon^*\mathrm{j}_1\phi_\epsilon^*\mathrm{j}_3^8 - 320\phi_\epsilon^*\mathrm{j}_2^9 + \\
5568\phi_\epsilon^*\mathrm{j}_2^8\phi_\epsilon^*\mathrm{j}_3 - 155520\phi_\epsilon^*\mathrm{j}_2^8 - 40320\phi_\epsilon^*\mathrm{j}_2^7\phi_\epsilon^*\mathrm{j}_3^2 + 4572288/5\phi_\epsilon^*\mathrm{j}_2^7\phi_\epsilon^*\mathrm{j}_3 + 3869835264/5\phi_\epsilon^*\mathrm{j}_2^7 +
\end{gathered}$$

$$155520\phi_\epsilon^*\mathrm{j}_2^6\phi_\epsilon^*\mathrm{j}_3^3 - 6718464/5\phi_\epsilon^*\mathrm{j}_2^6\phi_\epsilon^*\mathrm{j}_3^2 - 336960\phi_\epsilon^*\mathrm{j}_2^5\phi_\epsilon^*\mathrm{j}_3^4 + 388800\phi_\epsilon^*\mathrm{j}_2^4\phi_\epsilon^*\mathrm{j}_3^5 - 186624\phi_\epsilon^*\mathrm{j}_2^3\phi_\epsilon^*\mathrm{j}_3^6)/$$
$$(\phi_\epsilon^*\mathrm{j}_2^8 - 42/5\phi_\epsilon^*\mathrm{j}_2^7\phi_\epsilon^*\mathrm{j}_3 - 7776/5\phi_\epsilon^*\mathrm{j}_2^7 + 117/5\phi_\epsilon^*\mathrm{j}_2^6\phi_\epsilon^*\mathrm{j}_3^2 - 108/5\phi_\epsilon^*\mathrm{j}_2^5\phi_\epsilon^*\mathrm{j}_3^3);$$

In the case $D = 2$, the equations are too large to be included in the paper. But see `https://members.loria.fr/EMilio/` .

We then have the following algorithm:

Algorithm B.3: Evaluation of $J_1(\tau)$ and $J_2(\tau)$ at precision N, for $\tau \in \mathcal{H}_1^2$

```
Data: $\tau \in \mathcal{H}_1^2$ and a working precision $N$
Result: $J_1(\tau)$ and $J_2(\tau)$ at precision $N$
1 Compute $\Omega = \phi_\epsilon(\tau)$;
2 Compute $\mathrm{j}_1(\Omega)$, $\mathrm{j}_2(\Omega)$ and $\mathrm{j}_3(\Omega)$ at precision $N$;
3 Deduce $J_1(\tau)$ and $J_2(\tau)$ from the Igusa invariants;
```

For the first step we only have to use the definition of ϕ_ϵ. For the second, we refer to [16]. The evaluation of the Igusa invariants can be done in $\tilde{O}(N)$ by [22]. For the third, we use the equations above.

Corollary B.4. *We can evaluate the Gundlach invariants $J_1(\tau)$ and $J_2(\tau)$ at precision N for $D = 2$ or 5 at any point $\tau \in \mathcal{H}_1^2$ with a complexity in $\tilde{O}(N)$ time.*

Modular polynomials: Since we only have two invariants, this simplifies the definition of the modular polynomials:

Proposition B.5. *Let $D = 2$ or 5 and ℓ be a prime number. If $\beta := \ell \in \mathcal{O}_K^{++}$ is inert or if $\ell = \beta\overline{\beta}$ with $\beta \in \mathcal{O}_K^{++}$, then the polynomials*

$$\Phi_\beta(X, J_1, J_2) = \prod_{\gamma \in C_\beta} (X - J_{1,\beta}^\gamma) \qquad \text{and} \qquad \Psi_\beta(X, J_1, J_2) = \sum_{\gamma \in C_\beta} J_{2,\beta}^\gamma \frac{\Phi_\beta(X, J_1, J_2)}{X - J_{1,\beta}^\gamma}$$

lie in $\mathbb{Q}(J_1, J_2)[X]$. If $\ell = \beta\overline{\beta}$ is split with $\beta \in \mathcal{O}_K^{++}$, then the polynomials

$$\Phi_\beta(X, J_1, J_2) = \prod_{\gamma \in C_\beta} (X - J_{1,\beta}^\gamma)(X - J_{1,\overline{\beta}}^\gamma) \qquad \text{and}$$

$$\Psi_\beta(X, J_1, J_2) = \sum_{\gamma \in C_\beta} J_{2,\beta}^\gamma \frac{\Phi_\beta(X, J_1, J_2)}{X - J_{1,\beta}^\gamma} + \sum_{\gamma \in C_\beta} J_{2,\overline{\beta}}^\gamma \frac{\Phi_\beta(X, J_1, J_2)}{X - J_{1,\overline{\beta}}^\gamma}$$

lie in $\mathbb{Q}(J_1, J_2)[X]$. These polynomials depend only on ℓ and can be computed in time quasi-linear in their size.

Proof. This is a corollary of Theorem 4.15. These polynomials depend only on ℓ as $\mathbb{Q}(\sqrt{D})$ for $D = 2$ or 5 has a fundamental unit of norm -1 (see the discussion in Remark 4.18). □

By construction, for any $z \in \mathcal{H}_1^2$, the modular polynomials satisfy $\Phi_\beta(X, J_1(z), J_2(z)) = 0$ when X is the evaluation of J_1 in one of the β- or $\overline{\beta}$-isogenous points z'. Then $J_2(z') = \Psi_\beta(J_1(z'), J_1(z), J_2(z))/\Phi'_\beta(J_1(z'), J_1(z), J_2(z))$, where Φ'_β is the derivative of Φ_β with respect to the variable X. Thus, given $J_1(z)$ and $J_2(z)$, the β-modular polynomials allow one to compute all the Gundlach invariants at the points isogenous to z.

Let $\mathcal{L}_\ell$ be the locus of the principally polarized abelian surfaces with real multiplication by $\mathcal{O}_K$ which are β- or $\overline{\beta}$-isogenous to a product of elliptic curves (and which are not isomorphic to a product of elliptic curves as principally polarized surfaces because when this happens, the Gundlach invariants are not always defined).

Proposition B.6. *In the case where $D = 5$, the denominators of the modular polynomials Φ_β and Ψ_β are divisible by a polynomial L_ℓ in $\mathbb{Q}[J_1, J_2]$ describing $\mathcal{L}_\ell$.*

Proof. We adapt the proof of [5, Lemma 6.3]. Let $z \in \mathcal{H}_1^2$ be β- or $\overline{\beta}$-isogenous to a product of elliptic curves and let c_i be a coefficient of Φ_β. The cusp form χ_{10} vanishes exactly at products of elliptic curves and by Theorem A.12, we have $F_{10} = -4\phi_\epsilon^* \chi_{10}$ so that F_{10} also vanishes at a product of elliptic curves. Thus J_1 and J_2 have poles at these values and there exists some $\gamma \in \tilde{\Gamma}^0(\beta)\backslash\tilde{\Gamma}(1)$ such that $J_{1,\beta}^\gamma(z)$ or $J_{1,\overline{\beta}}^\gamma(z)$ is infinite. The evaluation of c_i at z is a symmetric expression in the $J_{1,\beta}^\gamma(z)$ and in the $J_{1,\overline{\beta}}^\gamma(z)$. Generically, there is no algebraic relation between these values and the evaluation of c_i at z is therefore infinite. Since $J_1(z)$ and $J_2(z)$ are finite, the numerator of c_i is finite. The denominator of c_i must vanish at z which means that c_i is divisible by L_ℓ. The proof for Ψ_β is similar. □

If $D = 2$, the Gundlach invariants J_1 and J_2 have poles when $F_4(z) = 0$. Since by Theorem A.14, we have that $\phi_\epsilon^* \chi_{10} = \frac{-1}{4} F_4 F_6$, hence the set of poles is a subset of the products of elliptic curves. We have thus to consider the subset $\mathcal{L}'_\ell$ of $\mathcal{L}_\ell$ of the surfaces z such that $F_4(\frac{1}{\beta}\gamma \cdot z) = 0$ or $F_4(\frac{1}{\overline{\beta}}\gamma \cdot z) = 0$ for some $\gamma \in C_\beta$.

Proposition B.7. *In the case where $D = 2$, the denominators of the modular polynomials Φ_β and Ψ_β are divisible by a polynomial L'_ℓ in $\mathbb{Q}[J_1, J_2]$ describing $\mathcal{L}'_\ell$.*

We have proved that we have in the denominators of the modular polynomials a subset of the set H_β of abelian surfaces which are β-isogenous to a product of elliptic curves (and which are not isomorphic to a product of elliptic curves).

B.2 Modular polynomials with theta invariants

In this section, we define modular polynomials for any D square-free by using theta constants. They illustrate nicely the different possibilities of Theorem 4.15. We use the action of $\tilde{\Gamma}(2,4)\backslash(\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)\sigma)$ to prove symmetries of these polynomials and accelerate their computations.

The invariants we use are the pullbacks $\tilde{b}_i = \phi_{1,\omega}^* b_i$ for $i = 1, 2, 3$, of the generators b_1, b_2, b_3 (defined in Equation (3)) for the group $\Gamma(2,4)$. They are modular functions for the group $\tilde{\Gamma}(2,4)$, which is defined in Equations (16) and (17) and are generators for a corresponding field of modular functions by Theorem 2.16. Recall that we define $\tilde{\Gamma}(1) = \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K)$.

Evaluation and inversion: We now outline efficient procedures for the computation of the values $\tilde{b}_i(\tau)$ of Hilbert modular functions at any $\tau \in \mathcal{H}_1^2$ and for finding some $\tau \in \mathcal{H}_1^2$ from the $\tilde{b}_i(\tau)$. The first one is similar to Algorithm B.3, the third step being trivial as $\tilde{b}_i = \phi_{1,\omega}^* b_i$, and has the same complexity. For the second procedure, we also proceed as in Algorithm B.1, the first step being also trivial. For the second, it is possible to find Ω modulo $\Gamma(2,4)$ in $\tilde{O}(N)$ time (see [55]). The difficulty is in the third step. Indeed, we are able to find γ such that $\phi_{1,\omega}(\tau) = \gamma\Omega$, but γ is not necessarily in $\Gamma(2,4)$ so that we only find τ modulo $\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma$

instead of τ modulo $\tilde{\Gamma}(2,4)$, if $D \equiv 1 \bmod 4$, or modulo $\tilde{\Gamma}(2,4) \cup \tilde{\Gamma}(2,4)\sigma$, if $D \equiv 2,3 \bmod 4$. One solution is to compute beforehand all the classes of the quotient $\tilde{\Gamma}(2,4)\backslash\tilde{\Gamma}(1)$ and of $\tilde{\Gamma}(2,4)\sigma\backslash\tilde{\Gamma}(1)$ and see how they are sent to the classes of $\Gamma(2,4)\backslash\mathrm{Sp}_4(\mathbb{Z})$. It suffices to find to which class of $\Gamma(2,4)\backslash\mathrm{Sp}_4(\mathbb{Z})$ the matrix γ belongs in order to find a corresponding matrix $\tilde{\gamma}$ in $\tilde{\Gamma}(2,4)\backslash\tilde{\Gamma}(1)$ or in $\tilde{\Gamma}(2,4)\sigma\backslash\tilde{\Gamma}(1)$. Then we have $\phi_{1,\omega}(\tilde{\gamma}^{-1}\tau) = \phi_{1,\omega}(\tilde{\gamma}^{-1})\phi_{1,\omega}(\tau) = \gamma^{-1}\gamma\Omega = \Omega$.

Corollary B.8. *We can evaluate the three $\tilde{b}_i(\tau)$ at precision N for $\tau \in \mathcal{H}_1^2$ in time $\tilde{O}(N)$ and we can find τ at precision N modulo $\tilde{\Gamma}(2,4)$ if $D \equiv 1 \bmod 4$, or modulo $\tilde{\Gamma}(2,4) \cup \tilde{\Gamma}(2,4)\sigma$ if $D \equiv 2,3 \bmod 4$, from the values $\tilde{b}_i(\tau)$ with this same complexity.*

Note that when we use the functions $\tilde{b}_i$ to define modular polynomials, for the interpolation step we need the equations of the Humbert component defined by the $\tilde{b}_i$, as explained in Section 3.3. We refer to Equation (28) for the equations for $D = 2,3,5$ and to [33] for larger discriminants.

Modular polynomials: Recall that we denote for $i = 1,2,3$, $\beta \in \mathcal{O}_K^{++}$ and $\gamma \in \tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma$:

$$\begin{array}{rccc} \tilde{b}_{i,\beta}: & \mathcal{H}_1^2 & \to & \mathbb{C} \\ & \tau & \mapsto & \tilde{b}_i(\frac{1}{\beta}\tau) \end{array} \quad \text{and} \quad \begin{array}{rccc} \tilde{b}_{i,\beta}^{\gamma}: & \mathcal{H}_1^2 & \to & \mathbb{C} \\ & \tau & \mapsto & \tilde{b}_i(\frac{1}{\beta}\gamma\cdot\tau). \end{array}$$

For a matrix $\gamma \in \tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta)$, we would like to write

$$\tilde{b}_{i,\beta}^{\gamma}(\tau) = \tilde{b}_i(\frac{1}{\beta}\gamma\cdot\tau) = \tilde{b}_i(\gamma_\beta\cdot(\frac{1}{\beta}\tau)) = \tilde{b}_i(\frac{1}{\beta}\tau) = \tilde{b}_{i,\beta}(\tau)$$

so that the functions $\tilde{b}_{i,\beta}$ for $i = 1,2,3$ would be modular for the group $\tilde{\Gamma}(2,4)\cap\tilde{\Gamma}^0(\beta)$. However the third equality is true only if the matrix γ_β is in $\tilde{\Gamma}(2,4)$ (see Corollary 4.14). A simple calculation shows that this is always the case when $D \equiv 1 \bmod 4$. When $D \equiv 2,3 \bmod 4$, this happens only when β is of the form $a + b\omega$ with b even. If $D \equiv 2 \bmod 4$, this is equivalent to asking that $\ell \equiv 1 \bmod 4$ and else if $D \equiv 3 \bmod 4$, ℓ must necessarily satisfy $\ell \equiv 1 \bmod 4$. In particular, in the last case, 0, 1 or 2 modular polynomials with $\tilde{\Gamma}(2,4)$ structure can exist for a given prime which splits in totally positive factors, according to the fundamental unit ϵ. Thus

Proposition B.9. *The functions $\tilde{b}_{i,\beta}$ for $i = 1,2,3$ are modular functions for $\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta)$ when*

- $D \equiv 1 \bmod 4$*;*
- $D \equiv 2 \bmod 4$ *and $\beta = a + b\omega$ with b even, or, equivalently, $\ell \equiv 1 \bmod 4$;*
- $D \equiv 3 \bmod 4$ *and $\beta = a + b\omega$ with b even; this implies that $\ell \equiv 1 \bmod 4$.*

Proposition B.10. *Let ℓ be a prime number. Write $\ell = \beta$ if ℓ is inert and $\ell = \beta\overline{\beta}$ if ℓ is split or ramified with $\beta \in \mathcal{O}_K^{++}$. Let C_β be a set of representatives of $(\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta))\backslash\tilde{\Gamma}(2,4)$. If $D \equiv 1 \bmod 4$, then the polynomials*

$$\Phi_\beta(X,\tilde{b}_1,\tilde{b}_2,\tilde{b}_3) = \prod_{\gamma\in C_\beta}(X - \tilde{b}_{1,\beta}^{\gamma}), \quad \textit{and} \quad \Psi_{k,\beta}(X,\tilde{b}_1,\tilde{b}_2,\tilde{b}_3) = \sum_{\gamma\in C_\beta}\tilde{b}_{k,\beta}^{\gamma}\frac{\Phi_\beta(X,\tilde{b}_1,\tilde{b}_2,\tilde{b}_3)}{X - \tilde{b}_{1,\beta}^{\gamma}}$$

for $k = 2,3$ lie in $\mathbb{Q}(\tilde{b}_1, \tilde{b}_2, \tilde{b}_3)[X]$. If $D \equiv 2,3 \bmod 4$ and $\beta = a + b\omega$ with b even, then

$$\Phi_\beta(X, \tilde{b}_1, \tilde{b}_2, \tilde{b}_3) = \prod_{\gamma \in C_\beta} (X - \tilde{b}_{1,\beta}^{\gamma})(X - \tilde{b}_{1,\beta}^{\gamma\sigma}), \qquad \textit{and}$$

$$\Psi_{k,\beta}(X, \tilde{b}_1, \tilde{b}_2, \tilde{b}_3) = \sum_{\gamma \in C_\beta} \tilde{b}_{k,\beta}^{\gamma} \frac{\Phi_\beta(X, \tilde{b}_1, \tilde{b}_2, \tilde{b}_3)}{X - \tilde{b}_{1,\beta}^{\gamma}} + \sum_{\gamma \in C_\beta} \tilde{b}_{k,\beta}^{\gamma\sigma} \frac{\Phi_\beta(X, \tilde{b}_1, \tilde{b}_2, \tilde{b}_3)}{X - \tilde{b}_{1,\beta}^{\gamma\sigma}}$$

for $k = 2,3$ lie in $\mathbb{Q}(\tilde{b}_1, \tilde{b}_2, \tilde{b}_3)[X]$. They can be computed in time quasi-linear in their size.

Proof. This is a corollary of Theorem 4.15. The difference between the cases $D \equiv 1 \bmod 4$ and $D \equiv 2,3 \bmod 4$ comes from Equations (8) and (9): in the first case, by Proposition 2.8, the map $\tilde{\Gamma}(2,4)\backslash\mathcal{H}_1^2 \to \mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$ is injective while in the second it is the map $(\tilde{\Gamma}(2,4) \cup \tilde{\Gamma}(2,4)\sigma)\backslash\mathcal{H}_1^2 \to \mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$ which is injective. The coefficients of the Fourier series of the $\tilde{b}_i$ are in $\mathbb{Q}$ because it is the case of the Hilbert theta series (see [48]). □

Note that there are three polynomials so that given $\tilde{b}_1$, $\tilde{b}_2$ and $\tilde{b}_3$, one can obtain the values $\tilde{b}_{1,\beta}^{\gamma}$, $\tilde{b}_{2,\beta}^{\gamma}$ and $\tilde{b}_{3,\beta}^{\gamma}$ for any $\gamma \in C_\beta$.

If $D \equiv 1 \bmod 4$ we are in the non symmetric case, so we compute non symmetric modular polynomials.

Remark B.11. When $D = 2$, Equation (28) says that we have to consider only two modular functions as $\tilde{b}_1$ is determined by $\tilde{b}_2$ and $\tilde{b}_3$. In particular the corresponding Humbert component is a rational surface.

$\overline{\beta}$-modular polynomials: As Φ_β is a minimal polynomial, it is the unique irreducible and monic polynomial which satisfies, for any $\tau \in \mathcal{H}_1^2$, $\Phi_\beta(\tilde{b}_{1,\beta}(\tau), \tilde{b}_1(\tau), \tilde{b}_2(\tau), \tilde{b}_3(\tau)) = 0$. We can look at what happens on $\sigma(\tau)$. The matrix M_σ of Equation (8) acts as follows: $(b_1^{M_\sigma}, b_2^{M_\sigma}, b_3^{M_\sigma}) = (b_1, b_2, b_3)$ if $D \equiv 2,3 \bmod 4$ and $(b_1^{M_\sigma}, b_2^{M_\sigma}, b_3^{M_\sigma}) = (b_3, b_2, b_1)$ if $D \equiv 1 \bmod 4$.

So when $D \equiv 2,3 \bmod 4$ the b_i are symmetric and the β-modular polynomials are symmetric, they encode both the β and the $\overline{\beta}$-isogenies, as is the case for the Gundlach invariants.

However $(\tilde{b}_1^{\sigma}, \tilde{b}_2^{\sigma}, \tilde{b}_3^{\sigma}) = (\tilde{b}_3, \tilde{b}_2, \tilde{b}_1)$ if $D \equiv 1 \bmod 4$. The irreducible and monic polynomial $\Phi_\beta(\tilde{b}_{1,\beta}^{\sigma}, \tilde{b}_1^{\sigma}, \tilde{b}_2^{\sigma}, \tilde{b}_3^{\sigma})$ has the same roots as $\Phi_\beta(\tilde{b}_{1,\beta}, \tilde{b}_1, \tilde{b}_2, \tilde{b}_3)$ and thus by unicity, these polynomials have to be equal. Thus, if $D \equiv 1 \bmod 4$, $\Phi_\beta(\tilde{b}_{3,\overline{\beta}}, \tilde{b}_3, \tilde{b}_2, \tilde{b}_1) = \Phi_\beta(\tilde{b}_{1,\beta}, \tilde{b}_1, \tilde{b}_2, \tilde{b}_3)$ and it is possible to obtain the value $\tilde{b}_{3,\overline{\beta}}(\tau)$ for any $\tau \in \mathcal{H}_1^2$ using the β-modular polynomials. We have then, still acting by σ,

$$\tilde{b}_{2,\overline{\beta}}(\tau) = \Psi_{2,\beta}(\tilde{b}_{3,\overline{\beta}}(\tau), \tilde{b}_3(\tau), \tilde{b}_2(\tau), \tilde{b}_1(\tau)) / \Phi'_\beta(\tilde{b}_{3,\overline{\beta}}(\tau), \tilde{b}_3(\tau), \tilde{b}_2(\tau), \tilde{b}_1(\tau)) \quad \text{and}$$

$$\tilde{b}_{1,\overline{\beta}}(\tau) = \Psi_{3,\beta}(\tilde{b}_{3,\overline{\beta}}(\tau), \tilde{b}_3(\tau), \tilde{b}_2(\tau), \tilde{b}_1(\tau)) / \Phi'_\beta(\tilde{b}_{3,\overline{\beta}}(\tau), \tilde{b}_3(\tau), \tilde{b}_2(\tau), \tilde{b}_1(\tau)).$$

We conclude that once we have the β-modular polynomials, we get the $\overline{\beta}$-modular polynomials for free.

Changing β by a unit: Note that in the case where two pairs $(\beta, \overline{\beta})$ and $(\beta', \overline{\beta'})$ of totally positive elements, whose product is ℓ, differ by an even factor of ϵ (this always happens when ϵ has norm -1), we have that $\beta' = \epsilon^{2n}\beta = \left(\begin{smallmatrix} \epsilon^n & 0 \\ 0 & \epsilon^{-n} \end{smallmatrix}\right)\beta$. Thus for any $\tau \in \mathcal{H}_1^2$, if we compute $\tilde{b}_{i,\beta}(\tau)$, for $i = 1, 2, 3$, from $\tilde{b}_i(\tau)$ and using the β-modular polynomials, then we have $\tilde{b}_{i,\beta'}(\tau) = \tilde{b}_i\left(\left(\begin{smallmatrix} \epsilon^{-n} & 0 \\ 0 & \epsilon^{n} \end{smallmatrix}\right)\frac{1}{\beta}\tau\right)$ and knowing how the matrix $\left(\begin{smallmatrix} \epsilon^{-n} & 0 \\ 0 & \epsilon^{n} \end{smallmatrix}\right)$ acts on the $\tilde{b}_{i,\beta}$, we can compute the $\tilde{b}_{i,\beta'}$ from the $\tilde{b}_{i,\beta}$. In this case, it is useless to compute the β'-modular polynomials.

Example B.12. When $D = 2, 5$ or 13, a fundamental unit $\epsilon > 1$ has norm -1.

- If $D = 2$, we have that $(\tilde{b}_{1,\epsilon^2}, \tilde{b}_{2,\epsilon^2}, \tilde{b}_{3,\epsilon^2}) = (\tilde{b}_1, \tilde{b}_3, \tilde{b}_2)$;
- If $D = 5$, we have that $(\tilde{b}_{1,\epsilon^2}, \tilde{b}_{2,\epsilon^2}, \tilde{b}_{3,\epsilon^2}) = (\tilde{b}_3, \tilde{b}_1, \tilde{b}_2)$;
- If $D = 13$, we have that $(\tilde{b}_{1,\epsilon^2}, \tilde{b}_{2,\epsilon^2}, \tilde{b}_{3,\epsilon^2}) = (\tilde{b}_2, \tilde{b}_3, \tilde{b}_1)$.

When the norm of $\epsilon > 0$ is 1, then if $\ell = \beta\overline{\beta}$, we also have $\ell = \beta'\overline{\beta'}$, where $\beta' = \epsilon\beta$. The multiplication by ϵ does not come from the action of a matrix and the previous argument does not work.

Example B.13. When $D = 55$, the fundamental unit $\epsilon = 89 + 12\sqrt{55}$ has norm 1 and for $\ell = 5$, we can choose $\beta = 15 + 2\sqrt{55}$ and $\beta' = \epsilon\beta = 2655 + 358\sqrt{55}$. As 2 and 358 are even, we can define two triplets of "non-equivalent" modular polynomials (by Propositions B.9 and B.10) .

Symmetries: We can proceed in the same way with matrices $\gamma \in \tilde{\Gamma}(2,4)\backslash\tilde{\Gamma}(1)$ having special properties. If γ permutes the $\tilde{b}_i$ and the $\tilde{b}_{i,\beta}$, this says that there are symmetries in the modular polynomials. In particular, if γ satisfies $(\tilde{b}_1^\gamma, \tilde{b}_2^\gamma, \tilde{b}_3^\gamma) = (\tilde{b}_1, \tilde{b}_3, \tilde{b}_2)$ and $(\tilde{b}_{1,\beta}^\gamma, \tilde{b}_{2,\beta}^\gamma, \tilde{b}_{3,\beta}^\gamma) = (\tilde{b}_{1,\beta}, \tilde{b}_{3,\beta}, \tilde{b}_{2,\beta})$, this means that

$$\Phi_\beta(X, \tilde{b}_1, \tilde{b}_2, \tilde{b}_3) = \Phi_\beta(X, \tilde{b}_1, \tilde{b}_3, \tilde{b}_2)$$

and consequently that

$$\Psi_{2,\beta}(X, \tilde{b}_1, \tilde{b}_3, \tilde{b}_2) = \Psi_{3,\beta}(X, \tilde{b}_1, \tilde{b}_2, \tilde{b}_3)$$

so that we only need to compute the first two β-modular polynomials, as the third one is deduced from the second one. For example, this happens for $D = 6$, $\ell = 73$, $\beta = 13 - 4\sqrt{6}$ and for $D = 10$, $\ell = 41$, $\beta = 9 - 2\sqrt{10}$.

Moreover, if γ satisfies $\tilde{b}_k^\gamma = i^{\alpha_k}\tilde{b}_k$ and $\tilde{b}_{k,\beta}^\gamma = i^{\beta_k}\tilde{b}_{k,\beta}$, for $k = 1, 2, 3$ and $\alpha_k, \beta_k \in \{0, 1, 2, 3\}$ (i is the imaginary unit), then the exponents of the $\tilde{b}_k$ at each coefficient of the modular polynomials satisfy some relations modulo 4. As we compute the modular polynomials by evaluation/interpolation, this can be used to decrease the number of evaluations.

The existence of these matrices depends on D and β. They can be searched for before the computation of the polynomials. We give some examples of relations between the exponents in Section 5 (see Equation (24)). Similar arguments have already been used in [55, Sections 5.2 and 5.3] for the computation of ℓ-modular polynomials.

Denominator: Let $\mathcal{L}_\beta$ be the locus of the principally polarized abelian surfaces z modulo $\tilde{\Gamma}(2,4)$ with real multiplication by $\mathcal{O}_K$ for which z, or $\sigma(z)$ in the case $D \equiv 2, 3 \bmod 4$, is β-isogenous to z' such that $\phi_{1,\omega}(z')$ is isogenous to a product of elliptic curves by the 2-isogeny $\phi_{1,\omega}(z') \to \phi_{1,\omega}(z')/2$ and such that $\theta_0(\phi_{1,\omega}(z')/2) = 0$.

Proposition B.14. *The denominators of the modular polynomials Φ_β and $\Psi_{k,\beta}$ are divisible by a polynomial L_β in $\mathbb{Q}[\tilde{b}_1, \tilde{b}_2, \tilde{b}_3]$ describing $\mathcal{L}_\beta$.*

Proof. Let $z \in \mathcal{L}_\beta$ and let c_i be a coefficient of Φ_β. Then there is some $\gamma \in (\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta))\backslash\tilde{\Gamma}(2,4)$ such that $\tilde{b}_{1,\beta}^{\gamma}$, or $\tilde{b}_{1,\beta}^{\gamma\sigma}$ if $D \equiv 2, 3 \bmod 4$, is infinite. Indeed, recall that $b_i = \frac{\theta_i}{\theta_0}(\Omega/2)$ and that by [16, Proposition 6.5 and Corollary 6.1], exactly one theta constant vanishes at Ω if and only if Ω is isomorphic to a product of elliptic curves. We conclude using the same arguments as in the proof of Theorem B.6. □

The reason for which we have introduced modular polynomials with the $\tilde{b}_i$ invariants was to obtain smaller polynomials compared to the ones with the Gundlach invariants or with the pullbacks of the Igusa invariants. But by Theorem B.9, the β-modular polynomials are not defined for all ℓ splitting in totally positive factors. We have two ways to deal with this problem, as explained in Remark 4.19. The first one is finding a subset of $\tilde{\Gamma}(2,4)$ for which $\tilde{b}_{i,\beta}$ is invariant (we are in the case $D \equiv 2, 3 \bmod 4$). Recall that the definition of $\tilde{\Gamma}(2,4)$ changes depending on whether $D \equiv 1 \bmod 4$ or $D \equiv 2, 3 \bmod 4$ (see Equations (16) and (17)). Let $\tilde{\Gamma}'$ be the group defined as $\tilde{\Gamma}(2,4)$ in the case $D \equiv 1 \bmod 4$. This subgroup is of index 4 in $\tilde{\Gamma}(2,4)$ and we consider the quotient $(\tilde{\Gamma}' \cap \tilde{\Gamma}^0(\beta))\backslash\tilde{\Gamma}(2,4)$, containing $4(\ell+1)$ classes, to define our polynomials. The second one is taking other invariants, in particular the Rosenhain invariants $\tilde{r}_i = \phi_{1,\omega}^* r_i$. We have already seen that they are generators for the field of Hilbert modular functions invariant under $\tilde{\Gamma}(2)$ (see Theorem 2.16) and $\tilde{r}_{i,\beta}$ for $i = 1, 2, 3$ is always invariant under $\tilde{\Gamma}(2) \cap \tilde{\Gamma}^0(\beta)$. All the results of this section can be adapted to these invariants.