Modular polynomials on Hilbert surfaces

Enea Milio, Damien Robert

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, and give an application to the CRT method to construct class polynomials.

1 Introduction

1.1 Context

Isogenies play an important role in elliptic curve cryptography. They allow to transfert the DLP from one curve to a possibly weaker one [GHS02; Smi09]; they are used by the SEA point counting algorithm [Sch95; Mor95; Elk97], but also by the CRT algorithms to compute class polynomials [Sut11; ES10] and modular polynomials [BLS12]. Splitting the multiplication using isogenies can improve the arithmetic [DIK06; Gau07], taking isogenies reduce the impact of side channel attacks [Sma03], and they allow to construct normal basis of a finite field [CL09]. They have also been used to construct hash functions [CLG09] or to build cryptosystems [Tes06; RS06].

In dimension 1, the ℓ-modular polynomials ϕ_ℓ parametrize couple of elliptic curves E_1 and E_2 that are ℓ-isogenous over the algebraic closure. They can be computed in quasi-linear time [Eng09] 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 [EM02].

Principally polarized complex abelian surfaces (which are generically Jacobians of hyperelliptic curves) are parametrized by the Siegel threefold $\mathfrak{H}_g/\mathrm{Sp}_4(\mathbb{Z})$ (with $g = 2$) where $\mathfrak{H}_g$ is the Siegel space of symmetric $g \times g$ complex matrices with totally positive imaginary part. The Siegel threefold is an algebraic variety birationally equivalent to the three dimensional algebraic space, and is parametrized by the three Igusa invariants [Igu60; Igu62]. One can then generalize modular polynomials to this setting: the ℓ-modular polynomials classify couple of principally polarized abelian surfaces (A, B) which admit an ℓ-isogeny $A \to B$. 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 three 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 $X_0(\ell) = \mathfrak{H}_g/\Gamma^0(\ell)$. These polynomials have been studied in [Gau00; BL09] and computed for $\ell = 2$ in [Dup06]. A generalization of these modular polynomials using smaller Siegel modular invariants have more recently been computed in [Mil15].

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 is $\ell^3 + \ell^2 + \ell + 1$. Already these polynomials for $\ell = 7$ takes 29GB to write (even using the smaller theta invariants), 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 [BGL11; LR13]. But this is not always possible using only ℓ-isogenies.

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 polarized in general. The isogenous abelian surface admits a principal polarization if and only if there exists a real totally positive endomorphism $\beta \in \mathrm{End}^{s,++}(A)$ of norm ℓ 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 couple of β-isogenous abelian surfaces (A, B). Generically, a complex abelian surface A has no real endomorphisms, so to define β-modular polynomials we need to restrict to a sublocus 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 classes of principally polarized abelian surfaces A with $\mathrm{End}^{s,++}(A) \subset \mathcal{O}_K$. 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 an Humbert surface, and use the tools already known there, especially those described in [Dup06; Mil15] for the computation of ℓ-modular polynomials.

1.2 Outline

We study several parametrizations of the Humbert surfaces. The Siegel moduli threefold is parametrized by the three Igusa functions, and in [Mil15] a cover of the Siegel space given by level 2 theta constant is also used to give smaller modular polynomials.

Pulling back the Igusa functions to the Humbert surface gives rational coordinates which can be used to define modular polynomials. Likewise pulling back the 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.

We describe in Section 2.3 an algorithm which, given a period matrix $\tau \in \mathcal{H}^g$ compute the above invariants in quasi-linear time. We also give an algorithm, which given the value of the above invariants, compute the corresponding period matrix $\tau \in \mathcal{H}^g$ in time quasi-linear. (See Theorem 3.4). For the modular polynomials computations, these algorithms are crucial for the evaluation (resp the interpolation) step, but they have independent interest. For instance the fast evaluation would speed up the algorithms described in [LY11; LNY15] for computing class polynomials via Gundlach invariants. The 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 [Dup06].

The main result of the paper is the computation of modular polynomials on the Hilbert (or Humbert) surface. When $\beta \in \mathcal{O}_K$ is a totally positive prime, we define β-isogenies and

β-modular polynomial in Section 4.1. There are two cases:

- When the norm of β is a prime number 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 and the β-modular polynomials parametrize all couple of principally polarized abelian surfaces with maximal real multiplication and admitting a cyclic isogeny of degree ℓ;
- Otherwise β is an inert prime number $\ell \in \mathbb{Z}$. In this case the ℓ-modular polynomials (on the Hilbert moduli space) parametrize ℓ-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 ℓ-modular polynomials parametrize all $\ell^2 + 1$ abelian surfaces $B = A/V$ where V is furthermore stable under the action of the real multiplication.

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 field). 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 3.13 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 on the case where $K = \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ since this allows us to compare different kind of invariants.

Finally Martindale and Streng 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 we need for the interpolation 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 constant (as mentioned by translating back and forth to the Siegel space and using [Dup06]). 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 in [Lab16; LT16]. However in dimension 2 we do obtain a quasi-linear algorithm which is much faster than the linear algebra approach used by Martindale and Streng.

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, which is the image of the previous map. We conclude this Section by looking at covers of the 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 work even when we have relations between our invariants. In Section 3.4 we apply the previous Section to explain how to interpolate with Gundlach invariants and pull-backs of the Igusa and theta functions. Lastly we conclude the Section by giving in Section 3.5 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 the isogenies preserving real multiplication and give some applications in Section 4.2. In Section 4.3, we define the modular polynomials depending on these isogenies, explain some of their properties and give an algorithm to compute them in quasi-linear time.

Finally in Section 5, we describe some polynomials we have computed. In particular Section 5.4 look in more details the denominators of Hilbert modular polynomials, which describe very interesting modular curves.

Thanks We thank Pierre-Jean Spaenlehauer to have succesfully done the Gröbner basis expressing the Gundlach invariants in term of the Igusa invariants for $D = 2$. We thank David Kohel which suggested us to look at [EK14] to get invariants for more Humbert or Hilbert surfaces. We thank Ernst Kani for helpfull discussions regarding his results in [Kan] and John Boxall for pointing us to the results of Ernst Kani.

2 Hilbert and Siegel modular spaces

2.1 Siegel modular space

The Siegel upper half-space in dimension 2 is the set $\mathcal{H}_2 = \{\Omega \in M_2(\mathbb{C}) \mid \Omega \text{ is symmetric and } \Im(\Omega) > 0\}$. It is a moduli space for principally polarized abelian surfaces: such a surface is a torus $\mathbb{C}^2/(\mathbb{Z}^4 + \Omega\mathbb{Z}^4)$ for some $\Omega \in \mathcal{H}_2$ (see [BL03]), and the principal polarization is induced by the Hermitian form given by $\Im(\Omega)^{-1}$.

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 of the quotient space $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$. It is a moduli space for isomorphism classes of principally polarized abelian surfaces.

Let Γ be a finite subgroup of $\mathrm{Sp}_4(\mathbb{Z})$ 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 $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z})$ 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.*

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 $b = \left(\begin{smallmatrix} b_0 \\ b_1 \end{smallmatrix}\right)$ in $\{0, 1\}^2$

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

Of the 16 theta constants, 6 are identically zero and we denote $\mathcal{P} = \{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}$ 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 $\mathrm{Sp}_4(\mathbb{Z})$

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

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

(see for example [Dup06; Str10; Wen03] for the exact definition).

We define the Eisenstein serie 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 matrices $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ in $\mathrm{Sp}_4(\mathbb{Z})$ up to left multiplication by $\mathrm{SL}_2(\mathbb{Z})$. Let

$$\chi_{10} = -2^{-12}3^{-5}5^{-2}7^{-1}53^{-1}43867(\psi_4\psi_6 - \psi_{10}) \qquad \text{and}$$
$$\chi_{12} = 2^{-13}3^{-7}5^{-3}7^{-2}337^{-1}131\cdot 593(3^27^2\psi_4^3 + 2\cdot 5^3\psi_6^2 - 691\psi_{12})$$

be two Siegel modular cusps forms of weight 10 and 12 respectively. These series can be written in terms of theta constants. Indeed we have $\psi_4 = 2^{-2}h_4$, $\psi_6 = 2^{-2}h_6$, $\chi_{10} = -2^{-14}h_{10}$ and $\chi_{12} = 2^{-17}3^{-1}h_{12}$. The graded ring of holomorphic 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 Igusa invariants (see [Igu60; Igu62]).

Remark 2.1. For practical computations we use different invariants introduced by Streng in his thesis [Str10] whose denominators are respectively χ_{10}, χ_{10}^2, χ_{10}^2 and hence give smaller modular polynomials (see [Mil15]).

Let $\Gamma(2) = \{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z}) : \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \equiv I_2 \bmod 2\}$. 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 $\Gamma(2)$ ([Mum84]).

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 diagonals elements of X. It is a normal subgroup of $\mathrm{Sp}_4(\mathbb{Z})$ of index 11520. The quotients of theta functions $b_i(\Omega) = \theta_i(\Omega/2)/\theta_0(\Omega/2)$ 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 [Man94; Mil15]).

2.2 Hilbert modular space

We refer to [Van12; Bru08; Gor02; Fre90; Nag83] for more details on Hilbert modular forms and Hilbert surfaces.

Let D 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 $\mathcal{O}_K$ 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 conjugate of a in $\mathcal{O}_K$. We consider $K \subset \mathbb{R}$ and $\sqrt{D} > 0$. We then 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 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot (\tau_1, \tau_2) = \left(\frac{a\tau_1+b}{c\tau_1+d}, \frac{\overline{a}\tau_2+\overline{b}}{\overline{c}\tau_2+\overline{d}}\right)$. 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*. 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 [BL03; EK14]).

Let $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(K) : a, d \in \mathcal{O}_K, b \in \partial_K^{-1} \text{ and } c \in \partial_K\}$. As $K = \mathbb{Q}(\sqrt{D})$, we have that $\partial_K = \sqrt{\Delta_K}\mathcal{O}_K$ and $\partial_K^{-1} = \frac{1}{\sqrt{\Delta_K}}\mathcal{O}_K$. The isomorphisms $\phi_\pm : \mathrm{SL}_2(\mathcal{O}_K) \to \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}), \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & b/\sqrt{\Delta_K} \\ c\sqrt{\Delta_K} & d \end{smallmatrix}\right)$ and $\phi_\pm : \mathcal{H}_1^+ \times \mathcal{H}_1^- \to \mathcal{H}_1^2, (\tau_1, \tau_2) \mapsto (\tau_1\sqrt{\Delta_K}, -\tau_2\sqrt{\Delta_K})$ induce an isomorphism between the group action of $\mathrm{SL}_2(\mathcal{O}_K)$ on $\mathcal{H}_1^+ \times \mathcal{H}_1^-$ and the group action of $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ on $\mathcal{H}_1^2$ ([EK14, Section 3]).

If $\tau = (\tau_1, \tau_2) \in \mathcal{H}_1^2$, the corresponding abelian surface is given by the torus $\mathbb{C}^2/(\mathbf{\Phi}(\mathcal{O}_K) \oplus \mathbf{\Phi}(\partial_K^{-1})\tau)$ where $\Phi : K \to \mathbb{C}^2$ is given by the two real embeddings, 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 $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ is generated by the matrices $\left(\begin{smallmatrix} 1 & 1/\sqrt{\Delta_K} \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & \omega/\sqrt{\Delta_K} \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1/\sqrt{\Delta_K} \\ \sqrt{\Delta_K} & 0 \end{smallmatrix}\right)$.

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

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

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 $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ via $\sigma\gamma\sigma = \left(\begin{smallmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$, for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$. It is straightforward to check that this is compatible with the action on $\mathcal{H}_1^2$. We call the group $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) \rtimes \langle\sigma\rangle$ the symmetric Hilbert modular group. For a function $f : \mathcal{H}_1^2 \to \mathbb{C}$ and $\gamma \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) \rtimes \langle\sigma\rangle$ we denote $f^\gamma(\tau) = f(\gamma.\tau)$.

Definition 2.2. 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 verifies $f(\sigma(\tau)) = f(\tau)$ 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 it is symmetric when the forms are.

Remark 2.3. Note that a modular form f is then automatically holomorphic at the cusps $\mathrm{SL}_2(\mathcal{O}_K)\backslash\mathbb{P}^1(K) \simeq \mathrm{Cl}(\mathcal{O}_K)$.

Theorem 2.4. *The Hilbert modular surface is rational for $D = 2, 3, 5, 6, 7, 13, 15, 17, 21, 33$.*

Proof. See [HZ77, Theorem 2] □

For the study of Humbert surfaces in Section 2.4 we will be interested in symmetric Hilbert modular forms and functions. For the simplicity of the exposition, we now assume that the fundamental unit ϵ has norm -1 and $\epsilon > 0$. Let $\alpha = \mathrm{diag}(1, \frac{\sqrt{\Delta_K}}{\epsilon})$. Then $\phi_0 : \tau \in \mathcal{H}_1^2 \mapsto \frac{\epsilon}{\sqrt{\Delta_K}}\tau \in \mathcal{H}_1^2$ and $\phi_0 : \gamma \in \mathrm{SL}_2(\mathcal{O}_K) \mapsto \alpha\gamma\alpha^{-1} \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ are bijections which induce an isomorphism between the action of $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ on $\mathcal{H}_1^2$ and the action of $\mathrm{SL}_2(\mathcal{O}_K)$ on $\mathcal{H}_1^2$. 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 $j = 1, 2$.

Proposition 2.5. *Let g be a holomorphic Hilbert modular form for $SL_2(\mathcal{O}_K)$ of weight k. Then it has 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 [LY11, Proposition 3.2]. □

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 $A_2(\mathrm{SL}_2(\mathcal{O}_K)) = \bigoplus A_{\mathbb{Z}}(\mathrm{SL}_2(\mathcal{O}_K))_k$. Define the 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

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

and $\kappa_k = \zeta_K(k)^{-1}(2\pi)^{2k}((k-1)!)^{-2}\Delta_K^{1/2-k}$ (by [Nag83, Equation (1.5)]).

Lemma 2.6.

- *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 [Nag83, Lemma 1.1]. □

The 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 $\{1, \bar{\epsilon}\}$, which gives a nice expression of q_1 and q_2. We have

Theorem 2.7. *In the case $K = \mathbb{Q}(\sqrt{2})$, we put*

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

Then G_2, F_4 and F_6 are in $A_{\mathbb{Z}}(SL_2(\mathcal{O}_K))_k$ for $k = 2, 4, 6$ respectively. Furthermore, they form a minimal set of generators of $A_{\mathbb{Z}}(SL_2(\mathcal{O}_K))$ over $\mathbb{Z}$.

Proof. See [Nag83, Theorem 1]. □

Theorem 2.8. *In the case $K = \mathbb{Q}(\sqrt{2})$, the field of symmetric meromorphic Hilbert modular functions for $SL_2(\mathcal{O}_K)$ are rational functions of*

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

We call J_1 and J_2 the Gundlach invariants *for K.*

Proof. A proof of this theorem will be given later in page 14. □

Theorem 2.9. *In the case $K = \mathbb{Q}(\sqrt{5})$, we put*

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

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

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

The four modular forms G_2, F_6, F_{10} and F_{12} are in $A_{\mathbb{Z}}(SL_2(\mathcal{O}_K))_k$ for $k = 2, 6, 10$ and 12 respectively. Furthermore, they form a minimal set of generators of $A_{\mathbb{Z}}(SL_2(\mathcal{O}_K))$ over $\mathbb{Z}$.

Proof. See [Gun63] or [Nag83, Theorem 2]. □

Theorem 2.10. *In the case $K = \mathbb{Q}(\sqrt{5})$, the field of symmetric meromorphic Hilbert modular functions for $SL_2(\mathcal{O}_K)$ are rational functions of*

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

We call J_1 and J_2 the Gundlach invariants *for K.*

Proof. See [Gun63] or the proof in page 14.

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 Section 4.3 these invariants will give smaller modular polynomials. 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. □

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 $\tau^* = \left(\begin{smallmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{smallmatrix}\right)$, $x^* = \left(\begin{smallmatrix} x & 0 \\ 0 & \overline{x} \end{smallmatrix}\right)$ and $\gamma^* = \left(\begin{smallmatrix} a^* & b^* \\ c^* & d^* \end{smallmatrix}\right)$. Fix $\{e_1, e_2\}$ a $\mathbb{Z}$-basis of $\mathcal{O}_K$ and define the matrices $R = \left(\begin{smallmatrix} e_1 & e_2 \\ \overline{e_1} & \overline{e_2} \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} {}^tR & 0 \\ 0 & R^{-1} \end{smallmatrix}\right)$ and the maps

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

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

Proposition 2.11. *The map ϕ_{e_1,e_2} satisfy:*

- $\phi_{e_1,e_2}^{-1}(Sp_4(\mathbb{Z})) = SL_2(\mathcal{O}_K \oplus \partial_K^{-1})$;
- $\phi_{e_1,e_2}(\gamma \cdot \tau) = \phi_{e_1,e_2}(\gamma) \cdot \phi_{e_1,e_2}(\tau)$ *for all* $\gamma \in SL_2(\mathcal{O}_K \oplus \partial_K^{-1})$ *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* $\gamma \in Sp_4(\mathbb{Z})$ *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* $\gamma \in Sp_4(\mathbb{Z})$ *such that* $\phi_{e_1,e_2}(\sigma(\tau)) = \gamma \cdot \phi_{e_1,e_2}(\tau)$*. We denote* M_σ *this* γ*, and this allows us to extend* ϕ_{e_1,e_2} *to* $SL_2(\mathcal{O}_K \oplus \partial_K^{-1}) \rtimes \langle\sigma\rangle$.

Proof. See [LY11, Proposition 3.1]. □

Thus, the map ϕ_{e_1,e_2} gives a holomorphic map from $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})\backslash\mathcal{H}_1^2$ 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 $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ and $<\sigma>$ as subgroups of $\mathrm{Sp}_4(\mathbb{Z})$, we will often note $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})\sigma$ the group $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) \rtimes \langle\sigma\rangle$.

We will often work with the basis $e_1 = 1$ and $e_2 = \omega$. We will denote ϕ instead of $\phi_{1,\omega}$. We have then $\phi(\tau) = \left(\begin{smallmatrix} \tau_1+\tau_2 & \tau_1\omega+\tau_2\overline{\omega} \\ \tau_1\omega+\tau_2\overline{\omega} & \tau_1\omega^2+\tau_2\overline{\omega}^2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \mathcal{H}_2$ and it verifies

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

Moreover, set

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

The matrix M_σ satisfies

$$\phi(\sigma(\tau)) = M_\sigma \cdot \phi(\tau). \tag{5}$$

Consider now $\gamma = \left(\begin{smallmatrix} a+a'\omega & (b+b'\omega)/\sqrt{\Delta_K} \\ \sqrt{\Delta_K}(c+c'\omega) & d+d'\omega \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$. Then

$$\phi(\gamma) = \begin{cases} \begin{pmatrix} a & a' & b' & b+b' \\ (\frac{D-1}{4})a' & a+a' & b+b' & b+(\frac{D+3}{4})b' \\ (\frac{D-1}{4})c'-c & c & d & (\frac{D-1}{4})d' \\ c & c' & d' & d+d' \end{pmatrix} & \text{if } D \equiv 1 \bmod 4; \\ \begin{pmatrix} a & a' & b' & b \\ Da' & a & b & Db' \\ Dc' & c & d & Dd' \\ c & c' & d' & d \end{pmatrix} & \text{if } D \equiv 2,3 \bmod 4. \end{cases} \tag{6}$$

For $D = 2, 5$, the fundamental unit has norm -1 and it can 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 Section 2.2. Let $\phi_1 := \phi_{1,\bar{\epsilon}}$ and $\phi_\epsilon := \phi_1 \circ \phi_0$ where ϕ_0 denote the isomorphisms introduced in Section 2.2. The map ϕ_ϵ verifies similar equalities as in Proposition 2.11 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 $\mathcal{H}_2$.

For a basis $\{e_1, e_2\}$, we give now 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.

Proposition 2.12. *Let*

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

be a holomorphic Siegel modular form for $Sp_4(\mathbb{Z})$ of weight k. 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

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

Here, $Q_T(x_1, x_2) = (x_1, x_2) T \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right)$ is the positive definite quadratic form associated to T and

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

is the dual of $Sym_2(\mathbb{Z})$. Finally, $q^T = e^{2i\pi \mathrm{tr}(T\Omega)}$.

Proof. See [LY11, 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 2.13. *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 [Res74, Theorem 1]. □

Corollary 2.14. *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 also [LY11, Proposition 4.5]. □

Using Proposition 2.12 and comparing the different Fourier series (as done in [Res74] in the case $D = 5$) we have found

Theorem 2.15. *For $K = \mathbb{Q}(\sqrt{2})$ we have*

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

Corollary 2.16. *One has*

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

2.4 Humbert surfaces

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 2.17 (Humbert's Lemma)**.** *Let* $\Omega = \left(\begin{smallmatrix}\Omega_1 & \Omega_2\\ \Omega_2 & \Omega_3\end{smallmatrix}\right)$ *satisfying 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* $\gamma \in Sp_4(\mathbb{Z})$ *such that* $\gamma \cdot \Omega = \left(\begin{smallmatrix}\Omega_1' & \Omega_2'\\ \Omega_2' & \Omega_3'\end{smallmatrix}\right)$ *satisfies a unique normalized singular relation of the form:*

$$k\Omega_1' + \ell\Omega_2' - \Omega_3' = 0 \tag{7}$$

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

Proof. See [Hum99; Hum00; Hum01]. □

Remark 2.18.

- Equations (3) and (7) are of the same type;
- Let $\Omega \in \mathcal{H}_2$ be a matrix equivalent to a matrix satisfying (7). Then Ω satisfy necessarily a singular relation of discriminant Δ;
- Let $\Omega \in \mathcal{H}_2$ satisfying a singular relation of discriminant Δ. A constructive algorithm to find γ as in the Humbert's Lemma can be found in [BW03; Run99].

Proposition 2.19. *For any* $\Delta \equiv 0$ *or* $1 \bmod 4$*,* $\Delta > 0$*, the set* $H_\Delta := \{\Omega \in Sp_4(\mathbb{Z})\backslash\mathcal{H}_2 : \Omega$ *satisfies a primitive singular relation of discriminant* $\Delta\}$ *is a surface which we call a* Humbert surface of discriminant Δ*.*

Proof. See [BW03, Corollary 4.6 and Proposition 4.7] or [Gru08, Proposition 2.11]. □

Proposition 2.20. *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* $\Omega \notin \bigcup_{m>0} H_{m^2}$*;*
- $\Omega \in H_\Delta$*, if and only if* $End(\mathcal{A}_\Omega) \otimes \mathbb{Q}$ *contains* $\mathbb{Q}(\sqrt{\Delta})$*, if and only if 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 $End(\mathcal{A}_\Omega) \otimes \mathbb{Q}$ 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 [BW03, Proposition 4.9] or [Gru08, Corollary 2.10, Proposition 2.15]. □

We denote now $\tilde{\Gamma}(1) = \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$. Proposition 2.11 and Equations (3), (4) and (5) say that the images by ϕ 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 ϕ 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). Similarly, ϕ_ϵ also maps to the Humbert surface because it is the composition of $\phi_{1,\bar{\epsilon}}$ with an automorphism of the Humbert surface. More precisely, the Hilbert surface maps onto the Humbert surface:

Proposition 2.21. *The following diagram is commutative:*

$$\begin{array}{ccccc} \tilde{\Gamma}(1)\backslash\mathcal{H}_1^2 & \longleftarrow & \mathcal{H}_1^2 & \xrightarrow{\psi} & \mathcal{H}_2 \\ & \searrow^{\pi} & \downarrow & & \downarrow \\ & & (\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma)\backslash\mathcal{H}_1^2 & \xrightarrow{\rho} & Sp_4(\mathbb{Z})\backslash\mathcal{H}_2 \end{array}$$

where ψ is either ϕ_{e_1,e_2} or ϕ_ϵ, 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 [Van82]. 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*.

Lemma 2.22. *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 functions fields $F(Y) \dashrightarrow F(X)$ is surjective.*

Proof. 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. □

Corollary 2.23. *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. 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.

Proposition 2.21 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 2.22, 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} whose locus is exactly H_1, the set of abelian surfaces isomorphic to a product of elliptic curves. By Proposition 2.20 the intersection of H_1 and H_{Δ_K} is a (union of) curves, so the Igusa invariants are well defined on $H_{\Delta_K} \setminus H_1$. □

Proof of Theorems 2.8 and 2.10. By Corollary 2.23, any symmetric Hilbert modular function is a rational fraction with complex coefficients in the pullbacks of the Igusa invariants. By Corollaries 2.16 and 2.14, 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. □

2.5 Symmetric and non symmetric covers of the Humbert surface

We study here the covers of the Hilbert modular surface $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) \backslash \mathcal{H}_1^2$ given by a subgroup $\tilde{\Gamma}$ of finite index in $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$.

Remark 2.24. By [Ser70] a group $\tilde{\Gamma}$ of finite index in $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ is necessarily a level subgroup, meaning that it contains a congruence subgroup $\tilde{\Gamma}(n)$ (see Definition 2.28).

Lemma 2.25. *Let $\mathcal{G}$ be a subgroup of $SL_2(\mathcal{O}_K \oplus \partial_K^{-1}) \rtimes \langle \sigma \rangle$ of finite index. If $\sigma \notin \mathcal{G}$ then $\mathcal{G} \subset SL_2(\mathcal{O}_K \oplus \partial_K^{-1})$. Otherwise $\mathcal{G} = \tilde{\Gamma} \rtimes \langle \sigma \rangle$ for a subgroup $\tilde{\Gamma} \subset SL_2(\mathcal{O}_K \oplus \partial_K^{-1})$ 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 $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$. It remains to check that σ normalize $\tilde{\Gamma}$. But since $\mathcal{G}$ is a group, $\sigma\tilde{\Gamma}\sigma^{-1} = \bar{\tilde{\Gamma}} \subset \mathcal{G}$, so $\bar{\tilde{\Gamma}} = \tilde{\Gamma}$. □

Definition 2.26. 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 2.27. $H_{\mathcal{G}}$ admits a (Baily-Borel) compactification, which in turn admits a smooth birational model. In this article we only work with invariants of the Hilbert modular function field, so only up to birational equivalence, so we don't distinguish between these models.

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 $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ action on $\mathcal{H}^2$ via the automorphism $\phi_\pm$ of Section 2.2.

Definition 2.28. Let

$$\tilde{\Gamma}(n) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K) : a \equiv d \equiv 1 \bmod n,\ b \equiv c \equiv 0 \bmod n \right\}. \tag{8}$$

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

$$\begin{aligned} \tilde{\Gamma}(2,4) &= \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \tilde{\Gamma}(2) : b \equiv c \equiv 0 \bmod 4 \right\}, \\ \tilde{\Gamma}(2,4) &= \left\{ \left(\begin{smallmatrix} a & (b+b'\omega) \\ (c+c'\omega) & d \end{smallmatrix}\right) \in \tilde{\Gamma}(2) : b' \equiv c' \equiv 0 \bmod 4 \right\} \end{aligned} \tag{9}$$

respectively.

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

$$\tilde{\Gamma}(n) = \left\{ \left(\begin{smallmatrix} a & b/\sqrt{\Delta_K} \\ \sqrt{\Delta_K}c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) : a \equiv d \equiv 1 \bmod n,\ b \equiv c \equiv 0 \bmod n \right\}. \tag{10}$$

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

$$\begin{aligned} \tilde{\Gamma}(2,4) &= \left\{ \left(\begin{smallmatrix} a & b/\sqrt{\Delta_K} \\ \sqrt{\Delta_K}c & d \end{smallmatrix}\right) \in \tilde{\Gamma}(2) : b \equiv c \equiv 0 \bmod 4 \right\}, \\ \tilde{\Gamma}(2,4) &= \left\{ \left(\begin{smallmatrix} a & (b+b'\omega)/\sqrt{\Delta_K} \\ \sqrt{\Delta_K}(c+c'\omega) & d \end{smallmatrix}\right) \in \tilde{\Gamma}(2) : b' \equiv c' \equiv 0 \bmod 4 \right\} \end{aligned} \tag{11}$$

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

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 $H^{\Gamma}_{\Delta_K} = \pi^{-1}(H_{\Delta_K})$ in $\Gamma\backslash\mathcal{H}_2$ is called a *Humbert surface component*.

Let $\mathcal{G} = \phi^{-1}(\Gamma)$ and $\tilde{\Gamma} = \mathcal{G} \cap \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$. If the matrix M_σ is not in Γ, then $\mathcal{G} = \tilde{\Gamma}$, otherwise $\mathcal{G} = \tilde{\Gamma} \cup \tilde{\Gamma}\sigma$. By Proposition 2.21 we get that the following diagram is commutative:

$$\begin{array}{ccc} \mathcal{H}_1^2 & \xrightarrow{\psi} & \mathcal{H}_2 \\ \downarrow & & \downarrow \\ \mathcal{G}\backslash\mathcal{H}_1^2 & \xrightarrow{\rho} & \Gamma\backslash\mathcal{H}_2 \end{array}$$

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

Proposition 2.29. *Suppose that $b_1, \ldots, b_k$ are modular functions for Γ which generate the function field $\mathbb{C}(\Gamma)$ and that the restriction of $b_1, \ldots, b_k$ is well defined on the component $H^{\mathcal{G}}_{\Delta_K}$ (on an open set). Then $\rho^* b_1, \ldots, \rho^* b_k$ 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 Corollary 2.23. □

We have seen that by Corollary 2.23 we can take $\tilde{\mathrm{j}}_k = \phi^* \mathrm{j}_k$, for $k = 1, 2, 3$, as invariants on the symmetric Hilbert modular surface. These functions are algebraically dependent. Similarly, we want to apply Proposition 2.29 to the functions $\tilde{b}_k = \phi^* b_k$ and $\tilde{r}_k = \phi^* r_k$ for $k = 1, 2, 3$.

Theorem 2.30. *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 (6), we have that $\phi^{-1}(\Gamma(2,4)) \cap \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) = \tilde{\Gamma}(2,4)$. 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 (4) belongs to $\Gamma(2,4)$. Similarly, $\phi^{-1}(\Gamma(2)) \cap \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) = \tilde{\Gamma}(2)$ 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 2.29 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. □

Proposition 2.31. *The subgroups* $\tilde{\Gamma}(2)$ *and* $\tilde{\Gamma}(2,4)$ *of* $\tilde{\Gamma}(1)$ *are of index*

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

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 $D \equiv 5 \bmod 8$;
- $\mathbb{Z}/4\mathbb{Z}[X]/(X^2)$ 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 2.32. *The number of Humbert surfaces 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. See [Run99]. An heuristic argument for $\Gamma(2,4)$ is that given $P(b_1,b_2,b_3)$, the Humbert component $H_{\Delta_K}^{\mathcal{G}}$ which is the image of ϕ and $\Omega = \phi(\tau) \in \mathcal{H}_2$, then for any $\gamma \in \mathrm{Sp}_4(\mathbb{Z})/\Gamma(2,4)$, we have that $P(b_i(\gamma\Omega)) = 0$ only for the matrices γ which come from the image of $\phi(\tilde{\Gamma}(1)/\tilde{\Gamma}(2,4))$ and of $\phi(\tilde{\Gamma}(1)/\tilde{\Gamma}(2,4)\sigma)$ in $\mathrm{Sp}_4(\mathbb{Z})/\Gamma(2,4)$. The number of components corresponds to the number

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

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 $\Gamma(2)$.

This is easier to see via the modular interpretation. Let $\Gamma = \Gamma(2)$ (respectively $\Gamma(2,4)$). Then an element of $\Gamma\backslash H_2$ 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 $\Gamma\backslash H_2 \to \mathrm{Sp}_4(\mathbb{Z})\backslash H_2$ corresponds to forgetting this extra structure, and the fibers form a

torsor under the isomorphisms of this extra structure, which are equal to $\mathrm{Sp}_4(\mathbb{Z})/\Gamma(2)$ (resp. $\mathrm{Sp}_4(\mathbb{Z})/\Gamma(2,4)$).

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 $\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma/\mathcal{G}$ 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 if $D \equiv 2,3 \bmod 4$. 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 $\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma/\mathcal{G}$ permute the fibers. Since this quotient is isomorphic to $\phi(\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma)\Gamma(2)/\Gamma(2)$ (resp. to $\phi(\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma)\Gamma(2,4)/\Gamma(2,4)$) this means that the action of $\mathrm{Sp}_4(\mathbb{Z})/\left(\phi(\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma)\Gamma(2)\right)$ (resp. $\mathrm{Sp}_4(\mathbb{Z})/\phi(\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma)\Gamma(2,4)$), which is not compatible with $\mathcal{O}_K$, permutes the components. □

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

$$\begin{array}{c} b_1 - \frac{1}{2}(b_2^2+b_3^2) = 0; \\ -b_1^4 - b_2^4 - 4b_3^2 - 2b_1^2b_2^2 + 4b_1b_2 + 4b_1b_2b_3^2 = 0; \\ \frac{-1}{2}(\sum_i b_i^4 + \sum_i\sum_{j\neq i}(b_ib_j)^4) + b_1b_2b_3(1+\sum_i b_i^4 - b_1b_2b_3) = 0 \end{array} \tag{12}$$

and similarly for $\Gamma(2)$ and $D = 2$ only

$$\begin{array}{c} ((16r_3^2-16r_3)r_2^2 + (-16r_3^2+16r_3)r_2)r_1^4 + ((-16r_3^2+16r_3)r_2^3 + (-16r_3^3+16r_3^2)r_2^2 + \\ (16r_3^3-16r_3)r_2)r_1^3 + (-r_2^4 + (16r_3^3-16r_3+2)r_2^3 + (-14r_3^2+14r_3-1)r_2^2 + \\ (-16r_3^3+14r_3^2+2r_3)r_2 + (-r_3^4+2r_3^3-r_3^2))r_1^2 + (2r_3r_2^4 + (-16r_3^3+14r_3^2-2r_3)r_2^3 + \\ (14r_3^3-12r_3^2)r_2^2 + (2r_3^4-2r_3^3)r_2)r_1 + (-r_3^2r_2^4 + 2r_3^3r_2^3 - r_3^4r_2^2) = 0. \end{array} \tag{13}$$

For $D = 3$, the equations are too big to be put in the paper. The computation of these equations is explained in [Gru08], where the equations for many discriminants can be found. We managed to directly recompute the equations for the small discriminants by evaluating the invariants at many matrices and by solving a linear algebra system.

3 Invariants of Hilbert surfaces

3.1 Generators of the field of Hilbert modular functions

Let $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ be a subgroup of finite index. We note $H_{\tilde{\Gamma}} = \tilde{\Gamma}\backslash\mathcal{H}_1^2$ 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.

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 $SL_2(\mathcal{O}_K \oplus \partial_K^{-1})$ 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 $\mathbb{C}_{\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})\sigma}$, we can take $i_1, i_2 \in \mathbb{C}_{\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})\sigma}$. They are then symmetric, so $H_{\mathcal{G}}$ is symmetric if and only if i_3 is symmetric. □

Usually working with symmetric Hilbert modular surface yields invariants easier to compute. For instance while $H_{\tilde{\Gamma}(1)}$ is not often a rational surface according to Theorem 2.4, from [EK14] we have that $H_{\tilde{\Gamma}(1),\sigma}$ is a rational surface for every fundamental discriminent $\Delta_K < 100$. 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 Section 4.1.

Note that by the general theory of Shimura varieties $H_{\mathcal{G}}$ has a (birational) model defined over an algebraic number field F. In fact by [Van12, 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 $E(i_1, i_2, i_3) = 0$ will have coefficients in $c_k \in F(X_1, X_2)$ where $E = \sum c_k(i_1, i_2) i_3^k$.

But it is important to know in practice when the Hilbert invariants we work with are defined over a number field F: it is when their Fourier coefficients have value in 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 among the i_k and $H_{\mathcal{E}}$ the corresponding birational model of $H_{\mathcal{G}}$. Then 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 in F.*

Proof. The proof uses a similar argument as [BL09, 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 unknown) 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 among the Hilbert functions i_k will lie in a subfield of F, one needs to look at the Galois action on the Fourier coefficients.

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;

- For the interpolation, 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.

Theorem 3.4. *Assume that $\tilde{\Gamma} \supset \tilde{\Gamma}(2,4)$, $\mathcal{G} = \tilde{\Gamma}$ or $\mathcal{G} = \tilde{\Gamma} \cup \tilde{\Gamma}\sigma$, and i_1, i_2, i_3 such that $F(H_{\mathcal{G}}) = F(i_1, i_2, i_3)$, where F is the field of definition of $H_{\mathcal{G}}$. Assume that we are given the Fourier coefficients of the invariants i_1, i_2, i_3. Then both the map $\mathcal{G}\backslash\mathcal{H}_1^2 \to \mathbb{C}^3, \tau \mapsto (i_1(\tau), i_2(\tau), i_3(\tau))$ and its inverse can be computed in time quasi-linear in the precision.*

Proof. We first do the symmetric case. According to Theorem 2.30 the functions $\tilde{b}_k$ for $k = 1, 2, 3$ are generators for the function field $F(H_{\tilde{\Gamma}(2,4)})$ when $D \equiv 1 \bmod 4$ and $F(H_{\tilde{\Gamma}(2,4)\cup\tilde{\Gamma}(2,4)\sigma})$ when $D \equiv 2, 3 \bmod 4$. In both case this means that the invariants i_k can be expressed as rational functions in the $\tilde{b}_k$: $i_k = R_k(\tilde{b}_1, \tilde{b}_2, \tilde{b}_3)$.

Computing these rational functions is just a pre-computation step and can be done 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).

By [Dup06; Mil15] given a Siegel matrix $\Omega \in \mathcal{H}_2$, evaluating the $b_k(\Omega)$ can be done in time quasi-linear in the precision. Given a period matrix $\tau \in \mathcal{H}_1^2$, one can use the map ϕ from Section 2.3 to get $\Omega = \phi(\tau) \in \mathcal{H}_2$, the values of $\tilde{b}_k(\tau) = b_k(\phi(\tau))$ in time quasi-linear, and then the values of $i_k(\tau) = R_k(\tilde{b}_1(\tau), \tilde{b}_2(\tau), \tilde{b}_3(\tau))$.

For the converse, the (restriction of the) Igusa invariants $\tilde{\mathrm{j}}_1, \tilde{\mathrm{j}}_2, \tilde{\mathrm{j}}_3$ can also be expressed as rational functions in the invariants i_1, i_3, i_3. From the values of these three invariants, one can then compute the values of the Igusa invariants, and thus recover using [Dup06; Mil15] a matrix $\Omega \in \mathcal{H}_2$ giving these values in time quasi-linear.

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 $\gamma.\Omega$ satisfy a normalized singular relation. By Section 2.3, $\gamma.\Omega$ is in the image of ϕ, so one can compute $\tau = \phi^{-1}(\gamma.\Omega) \in \mathcal{H}_1^2$. It then only remains to compute all classes of τ under the action of the finite group $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})/\mathcal{G}$ to find a τ' such that $(i_1(\tau'), i_2(\tau'), i_3(\tau'))$ has the required values.

For the non symmetric case, recovering τ 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, and can not be expressed as a rational function in the $\tilde{b}_k$. 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, and choosing the correct one only require an evaluation with small precision of i_3 using its Fourier series. □

Remark 3.5. In practice, while the pre-computation step does not affect the asymptotic complexity, it is important to optimize 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 as outlined in Section 3.3. Indeed since we know by [Mil15; Dup06] how to obtain a period matrix Ω from the values of the b_k, it is possible to use fast algorithms for the interpolation. We note that this method 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).

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.

3.3 Interpolation by Hilbert modular functions

For the interpolation approach of the computation of modular polynomials, we will interpolate the coefficients of these polynomials as rational functions in term of the chosen modular invariants i_1, i_2, i_3.

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).

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 first handle the case where $H_{\mathcal{G}}$ is a rational surface, hence $F(H_{\mathcal{G}})$ can be written as $F(J_1, J_2)$, using only two primary invariants. For the interpolation step we write

$$c = c(J_1, J_2) = \frac{A(J_1, J_2)}{B(J_1, J_2)} = \frac{\sum_{m=0}^{d_{J_1}^A} \sum_{n=0}^{d_{J_2}^A} a_{m,n} J_1^m J_2^n}{\sum_{m=0}^{d_{J_1}^B} \sum_{n=0}^{d_{J_2}^B} b_{m,n} J_1^m J_2^n} = \frac{\sum_{m=0}^{d_{J_1}^A} a_m(J_2) J_1^m}{\sum_{m=0}^{d_{J_1}^B} b_m(J_2) J_1^m}.$$

Let z_m for $m = 1, \ldots, d_T^A + d_T^B + 2$, where T designes the total degree, such that $(J_1(z_m), J_2(z_m))$ is of the form $(u_m, v u_m)$ for a fixed $v \in \mathbb{C}$. Interpolate to find the univariate rational fraction $c(J_1, vJ_1)$ and write the fraction such that the coefficient of degree 0 of the denominator is 1. Compute in this way the fractions $c(J_1, v_n J_1)$ for $n = 1, \ldots, \max(d_{J_2}^A, d_{J_2}^B) + 1$. Interpolate the polynomials a_m and b_m to obtain $c(J_1, J_1 J_2)$ and substitute J_2 by J_2/J_1 to obtain c. Note that we have to consider the total degree to interpolate correctly the fractions. More details can be found in [Mil15, Section 2], in particular a complexity analysis.

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 $d_T = \max(d_T^A, d_T^B)$ and $d_{J_2} = \max(d_{J_2}^A, d_{J_2}^B)$.

We now describe the general case, where 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 before we would like to work with values z_j with the property that $(i_1(z_j), i_2(z_j), i_3(z_j))$ is of the form $(u_m, v_n u_m, w_r u_m)$, where 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, so that for fixed i_1 and i_2, the values i_3 can take are determined (moreover, they will not be of the form $w_r u_m$ and the number of values will be inferior to the degree in i_3). A solution to this problem consists to remark that $F(i_1, i_2, i_3)/(E) = F(i_1, i_2)[i_3]/(E)$. 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 $c_i \in F(i_1, i_2)$.

The interpolation is done as follows. For sufficiently many values u_m and v_n, compute the d roots w_r of $E(u_m, v_n u_m, x)$. For $r = 1, \ldots, d$, find $z_r \in \mathcal{H}_1^2$ such that $(i_1(z_r), i_2(z_r), i_3(z_r)) =$

$(u_m, v_n u_m, w_r)$ and evaluate $c(z_r) = \sum_{i=0}^{d-1} c_i(u_m, v_n u_m) w_r^i$. Since $w_r = i_3(z_r)$, we first interpolate c as a univariate polynomial in i_3 by interpoling on the d values w_r to recover the d coefficients $c_i(u_m, v_n u_m)$ It remains to do the interpolation of the coefficients c_i to recover them as rational functions in i_1, i_2 as was outlined above.

We summarize this discussion by the theorem

Theorem 3.6. *Let $\mathcal{G}$ be a subgroup of finite index in $SL_2(\mathcal{O}_K \oplus \partial_K^{-1}) \cup SL_2(\mathcal{O}_K \oplus \partial_K^{-1})\sigma$. Let i_1, i_2, i_3 generating $\mathbb{C}_\mathcal{G}$ be such that the evaluation 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 in the precision.*

Let $E(i_1, i_2, i_3)$ the equation describing the Hilbert surface $H_\mathcal{G}$, and d the degree $\deg_{i_3}(E)$ of i_3 in E.

Let c a Hilbert modular function in $\mathbb{C}_\mathcal{G}$, then c can be written as $c = \sum_{k=0}^{d-1} c_k(i_1, i_2) i_3^k$. We let d_T be the maximal total degree of all the coefficients c_k (where the degree of a rational function is the maximal of the degree of its numerator and denominator), and d_{i_2} the maximal degree in i_2 of the coefficients c_k.

Then if c can be evaluated in time quasi-linear in the precision, then the coefficients c_k can be computed in precision N in time $\tilde{O}(dd_T d_{i_2} N)$.

Assume furthermore that the c_k lie in a number field F. Let N be the maximal height of the rational coefficients of each c_k. Then the coefficients c_k can be recovered exactly in time $\tilde{O}(dd_T d_{i_2} N)$.

In the case that $\mathcal{H}_\mathcal{G}$ is a rational surface so that we only need two primary invariants i_1 and i_2, then c can be interpolated in time $\tilde{O}(d_T d_{i_2} N)$.

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

$$O(dd_T d_{i_2}) + O(d)\tilde{O}(d_T d_{i_2} N) + O(d_T d_{i_2})\tilde{O}(dN) \subset \tilde{O}(dd_T d_{i_2} N). \tag{14}$$

Given a coefficient $c_k \in \mathbb{C}$ computed at precision $O(N)$, if c_k lie in a number field F then one can use the LLL algorithm [LLL82] to recover $c_k \in F$. Using fast version of LLL this reconstruction step can be done in time $\tilde{O}(N)$ (See [NSV11]).

In the case that $\mathcal{H}_\mathcal{G}$ is a rational surface, the evaluation step will be executed $O(d_T d_{i_2})$ times and we will interpolate 1 bivariate rational fraction. The complexity is then

$$O(d_T d_{i_2})\tilde{O}(N) + \tilde{O}(d_T d_{i_2} N) \subset \tilde{O}(d_T d_{i_2} N). \tag{15}$$

□

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 among 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 [Bec94; Kal97]), the interpolation step will interpolate the correct expression of the rational function.

3.4 Example of invariants

3.4.1 Gundlach invariants

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 Theorem 2.8 and 2.10. The only small difference is that for convenience we will use the map ϕ_ϵ defined in Section 2.3 rather than the map ϕ 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 Section 2.3 (see Corollaries 2.16 and 2.14). 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 form defining the Igusa invariants are very simple (see Theorems 2.15 and 2.13).

We outline the algorithm (Algorithm 3.7) to find $\tau \in \mathcal{H}_1^2$ from the values $J_1(\tau)$ and $J_2(\tau)$.

Algorithm 3.7: τ from $(J_1(\tau), J_2(\tau))$

Data: The values $J_1(\tau)$ and $J_2(\tau)$, the working precision N
Result: τ modulo $\mathrm{SL}_2(\mathcal{O}_K) \cup \mathrm{SL}_2(\mathcal{O}_K)\sigma$

1 Compute $\mathrm{j}_1(\Omega)$, $\mathrm{j}_2(\Omega)$, $\mathrm{j}_3(\Omega)$, where $\Omega \in \mathcal{H}_2$ such that $\Omega = \phi_\epsilon(\tau)$;
2 Deduce the period matrix Ω (modulo $\mathrm{Sp}_4(\mathbb{Z})$) from the three Igusa invariants;
3 Find some $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ such that $\phi_\epsilon(\tau) = \gamma\Omega$ and deduce τ;

The first step can be done using Corollary 2.14 or 2.16. The second is explained in [Dup06; Mil15] and can be done in $\tilde{O}(N)$ (under some conjecture [Dup06, Conjecture 9.1], the computation is simplified because we do not need to compute low precision theta functions to get the correct sign in the Borchardt mean). For the third step, remark that for $D = 5$, if $\tau \in \mathcal{H}_1^2$, then $\phi_\epsilon(\tau) = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \mathcal{H}_2$ verifies by definition $\Omega_1 + \Omega_2 - \Omega_3 = 0$. The second step provides $\Omega' \in \mathcal{H}_2$ which is more precisely in the Humbert surface H_5. Thus by Humbert Lemma we know there exists a matrix $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ such that $\Omega'' = \gamma\Omega' = \left(\begin{smallmatrix} \Omega_1'' & \Omega_2'' \\ \Omega_2'' & \Omega_3'' \end{smallmatrix}\right)$ verifies $\Omega_1'' + \Omega_2'' - \Omega_3'' = 0$ (see Remark 2.18 for the computation of γ). We have then $\tau^* = ((\frac{\epsilon}{\sqrt{\Delta_K}})^*)^{-1}\, {}^tR^{-1}\Omega''R^{-1}$. For $D = 2$, $\phi_\epsilon(\tau)$ verifies $\Omega_1 + 2\Omega_2 - \Omega_3 = 0$ and we can adapt the algorithm to find the matrix γ. Thus

Corollary 3.8. *Given $J_1(\tau)$ and $J_2(\tau)$, where J_1 and J_2 are the Gundlach invariants for $D = 2$ or 5 and $\tau \in \mathcal{H}_1^2$, then we can find $\tau \in (SL_2(\mathcal{O}_K) \cup SL_2(\mathcal{O}_K)\sigma)\backslash\mathcal{H}_1^2$ in $\tilde{O}(N)$ time.*

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 $\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$, 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, the relations expressing the Igusa invariants in term of the Gundlach invariants are sufficiently simple to be inverted by a Gröbner basis.

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

$$J_2/J_1 = (1/6912\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2 - 1/2304\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_3 - 1/3359232\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^3 + 1/373248\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3 +$$

$$1/864\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^2 - 1/124416\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2\phi^*\mathrm{j}_3^2 + 1/124416\phi^*\mathrm{j}_1\phi^*\mathrm{j}_3^3 + 1/3359232\phi^*\mathrm{j}_2^4 -$$
$$1/1119744\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3)/(\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^2 + 1/1944\phi^*\mathrm{j}_2^4 - 1/648\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3);$$

$$J_1 = -(45349632\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2^4 - 2584929024/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3 - 499571546112/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2^3 +$$
$$11019960576/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3^2 + 1410554953728/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3 - 20815481088/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_2\phi^*\mathrm{j}_3^3 +$$
$$14693280768/5\phi^*\mathrm{j}_1^3\phi^*\mathrm{j}_3^4 - 186624\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^6 + 16236288/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3 - 12380449536/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^5 -$$
$$23514624\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3^2 + 146887458048/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3 + 31972578951168/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^4 +$$
$$90699264\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3^3 - 651402114048/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3^2 - 90275517038592/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3 -$$
$$196515072\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3^4 + 1279948013568/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3^3 + 226748160\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2\phi^*\mathrm{j}_3^5 -$$
$$940369969152/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_2\phi^*\mathrm{j}_3^4 - 544195584/5\phi^*\mathrm{j}_1^2\phi^*\mathrm{j}_3^6 + 192\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^8 - 22464/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^7\phi^*\mathrm{j}_3 -$$
$$18289152/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^7 + 229824/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^6\phi^*\mathrm{j}_3^2 + 260527104/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^6\phi^*\mathrm{j}_3 + 30051689472/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^6 -$$
$$1342656/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3^3 - 1482541056/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3^2 - 171240210432/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3 +$$
$$979776\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3^4 + 4212476928/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3^3 + 243799621632/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3^2 -$$
$$2286144\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3^5 - 5976073728/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3^4 + 16656192/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3^6 +$$
$$3386105856/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2^2\phi^*\mathrm{j}_3^5 - 13856832/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_2\phi^*\mathrm{j}_3^7 + 5038848/5\phi^*\mathrm{j}_1\phi^*\mathrm{j}_3^8 - 320\phi^*\mathrm{j}_2^9 +$$
$$5568\phi^*\mathrm{j}_2^8\phi^*\mathrm{j}_3 - 155520\phi^*\mathrm{j}_2^8 - 40320\phi^*\mathrm{j}_2^7\phi^*\mathrm{j}_3^2 + 4572288/5\phi^*\mathrm{j}_2^7\phi^*\mathrm{j}_3 + 3869835264/5\phi^*\mathrm{j}_2^7 +$$
$$155520\phi^*\mathrm{j}_2^6\phi^*\mathrm{j}_3^3 - 6718464/5\phi^*\mathrm{j}_2^6\phi^*\mathrm{j}_3^2 - 336960\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3^4 + 388800\phi^*\mathrm{j}_2^4\phi^*\mathrm{j}_3^5 - 186624\phi^*\mathrm{j}_2^3\phi^*\mathrm{j}_3^6)/$$
$$(\phi^*\mathrm{j}_2^8 - 42/5\phi^*\mathrm{j}_2^7\phi^*\mathrm{j}_3 - 7776/5\phi^*\mathrm{j}_2^7 + 117/5\phi^*\mathrm{j}_2^6\phi^*\mathrm{j}_3^2 - 108/5\phi^*\mathrm{j}_2^5\phi^*\mathrm{j}_3^3);$$

In the case $D = 2$, the equations are too large to be included in the paper.
We then have the following algorithm:

Algorithm 3.9: Evaluation of $J_1(\tau)$ and $J_2(\tau)$, for $\tau \in \mathcal{H}_1^2$

Data: $\tau \in \mathcal{H}_1^2$ and a working precision N
Result: $J_1(\tau)$ and $J_2(\tau)$

1 Compute $\Omega = \phi_\epsilon(\tau)$ at precision N;
2 Compute $\mathrm{j}_1(\Omega)$, $\mathrm{j}_2(\Omega)$ and $\mathrm{j}_3(\Omega)$;
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 [Dup06]. The evaluation of the Igusa invariants can be done in $\tilde{O}(N)$ by [ET14]. For the third, we use the equations above.

Corollary 3.10. *We can evaluate the Gundlach invariants $J_1(\tau)$ and $J_2(\tau)$ for $D = 2$ or 5 at any point $\tau \in \mathcal{H}_1^2$ with a complexity in $\tilde{O}(N)$ time.*

3.4.2 Pullbacks of theta functions

We now outline efficient procedures for the computation of the $\tilde{b}_i(\tau)$ 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 3.9, the third step being trivial as $\tilde{b}_i = \phi^* b_i$, and has the same complexity. For the second procedure, we also proceed as in Algorithm 3.7, 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 [Mil15]). The difficulty is in the third step. Indeed, we are able to find γ such that $\phi(\tau) = \gamma\Omega$, but γ is not necessarily in $\Gamma(2,4)$ so that we only find τ modulo $\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma$ ($\tilde{\Gamma}(1) = \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ here) 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 $D \equiv 2,3 \bmod 4$. A solution consists to compute beforehand all the classes of $\tilde{\Gamma}(1)/\tilde{\Gamma}(2,4)$ and of $\tilde{\Gamma}(1)/\tilde{\Gamma}(2,4)\sigma$ and see how they are sent to the classes of $\mathrm{Sp}_4(\mathbb{Z})/\Gamma(2,4)$. It suffices to find in which class of $\mathrm{Sp}_4(\mathbb{Z})/\Gamma(2,4)$ γ belongs to to find a corresponding matrix $\tilde{\gamma}$ in $\tilde{\Gamma}(1)/\tilde{\Gamma}(2,4)$ or in $\tilde{\Gamma}(1)/\tilde{\Gamma}(2,4)\sigma$. Then we have $\phi(\tilde{\gamma}^{-1}\tau) = \phi(\tilde{\gamma}^{-1})\phi(\tau) = \gamma^{-1}\gamma\Omega = \Omega$. Thus

Corollary 3.11. *We can evaluate the three $\tilde{b}_i(\tau)$ for $\tau \in \mathcal{H}_1^2$ in $\tilde{O}(N)$ time and we can find τ modulo $\tilde{\Gamma}(2,4)$, or modulo $\tilde{\Gamma}(2,4) \cup \tilde{\Gamma}(2,4)\sigma$ according to the cases, from the values $\tilde{b}_i(\tau)$ with this same complexity.*

Note that when we use the function $\tilde{b}_i$ 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 12 for the equations for $D = 2,3,5$ and to [Gru08] for larger discriminants.

3.4.3 Non symmetric invariants

By [BGL+16], non-symmetric Gundlach invariants for $\mathbb{Q}(\sqrt{5})$ can be obtained considering the Hilbert modular forms

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

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

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

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

We cannot directly efficiently evaluate J_3. However we can use Equation (16) to compute J_3^2 and the correct square root is determined by the precomputed Fourier serie of J_3. The polynomials obtained are smaller than the symmetric ones. We refer to [BGL+16; Mar16] for more details on the polynomials coming from these invariants.

The paper [EK14] contains a lot of other invariants. For instance, still for $\mathbb{Q}(\sqrt{5})$, the authors prove that the Humbert surface H_5 is birational to $\mathbb{P}^2_{g,h}$ and that a birational model over $\mathbb{Q}$ of the non symmetric Hilbert modular surface is given by the double cover of $\mathbb{P}^2_{g,h}$

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

As this surface is also rational, a parametrization is obtained, given by the modular functions m and n. We have

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

and

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

(See [EK14, Section 6]). Using these equations, we have found the relations $g = -J_1/(6J_2^2)$, $h = J_1^2/J_2^5$ and $z = -F_5^3 F_{15}/(2F_6^5)$ 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 equation of the double cover given above in a similar strategy as the one for J_3.

More generally in [EK14] equations are given for every quadratic field $\mathbb{Q}(\sqrt{D})$ for all thirty fundamental discriminants D with $1 < D < 100$. We can then use invariants for other fields than $\mathbb{Q}(\sqrt{5})$. The difficulty residing in the optimization of these invariants: for instance for computing modular polynomials it is better that they have the same denominator.

3.5 Equations for covers of Hilbert surfaces

Let $\mathcal{G}_2 \subset \mathcal{G}_1 \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})\sigma$ be level 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 the same tool as described below will apply.

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 the 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 $\Psi_k \in \mathbb{C}_{\mathcal{G}_1}[X]$ defined such that $j_k \Phi_j'(j) = \Psi_k(j)$. 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 [GHK+06, Section 3].

Lemma 3.12. $\Psi_k(X) = \sum_{\gamma \in \mathcal{G}_1/\mathcal{G}_2} j_k^\gamma \Phi_j(X)/(X - j^\gamma)$.

Proof. Let M/K be a finite Galoisian extension of Galois group G, and for $f \in M$ and $\gamma \in G$ note 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 $\Phi(X) = \prod_{\gamma \in G_1/G_2}(X - j^\gamma)$.

Let $J \in K_2$, then there exists $Q \in K_1[X]$ such that $J = Q(j)$. The Hecke representation is given by a polynomial $\Psi \in K[X]$ such that $J\Phi'(j) = \Psi(j)$.

Since $J^\gamma = Q(j^\gamma)$, the polynomial Q can be computed by a Lagrange interpolation. Indeed, evaluating $\sum_{\delta\in G_1/G_2} J^\delta \prod_{\delta'\neq\delta}(X-j^{\delta'})/(j^\delta - j^{\delta'})$ at j^γ gives J^γ. Now, this expression is equal to $\sum_{\delta\in G_1/G_2} J^\delta \prod_{\delta'\neq\delta}(X-j^{\delta'})/\Phi'(j^\delta) = \sum_{\delta\in G_1/G_2} J^\delta\Phi(X)/((X-j^\sigma)\Phi'(j^\delta))$ and we deduce that taking $\Psi(X) = \sum_{\delta\in G/H} J^\delta\Phi(X)/(X-j^\delta)$, we have the property $J^\gamma\Phi'(j^\gamma) = \Psi(j^\gamma)$.

We apply this to the extension $\mathbb{C}_{\tilde\Gamma(n)}/\mathbb{C}_{\mathrm{SL}_2(\mathcal{O}_K\oplus\partial_K^{-1})\cup\mathrm{SL}_2(\mathcal{O}_K\oplus\partial_K^{-1})\sigma}$ where $\tilde\Gamma(n)$ is a level subgroup included in $\mathcal{G}_2$. Indeed this is a Galoisian extension of Galois group $(\mathrm{SL}_2(\mathcal{O}_K\oplus\partial_K^{-1})\cup \mathrm{SL}_2(\mathcal{O}_K\oplus\partial_K^{-1})\sigma)/\tilde\Gamma(n)$, and we apply the result above to $G_1 = \mathcal{G}_1/\tilde\Gamma(n)$ and $G_2 = \mathcal{G}_2/\tilde\Gamma(n)$ with the notations of the Lemma. □

Theorem 3.13. *Assume that we are given*

- $\mathbb{C}_{\mathcal{G}_1} = \mathbb{C}(i_1,i_2,i_3)$ *for invariants on which the inversion of the evaluation can be computed in time quasi-linear in the precision;*
- *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* d *the degree* $\deg_{i_3}(E)$ *of* i_3 *in* E*;*
- $\mathbb{C}_{\mathcal{G}_2} = \mathbb{C}_{\mathcal{G}_1}(j)$ *for a Hilbert modular function* j *which admits a fast evaluation algorithm;*
- $\mathbb{C}_{\mathcal{G}_2} = \mathbb{C}(j_1,j_2,j_3)$ *for Hilbert modular functions* j_1,j_2,j_3 *which admit a fast evaluation algorithm;*
- *and assume that all the modular functions* $i_1,i_2,i_3,j,j_1,j_2,j_3$ *have Fourier coefficients in an algebraic number field* $F\subset\mathbb{C}$*.*

Let $\Phi(X,i_1,i_2,i_3) = \prod_{\gamma\in\mathcal{G}_1/\mathcal{G}_2}(X-j^\gamma) = X^D + \sum_{m=0}^{D-1} c_m(i_1,i_2,i_3)X^m$ *be the minimal polynomial of* j *over* $\mathbb{C}_{\mathcal{G}_1}$*, where* $D = \#\mathcal{G}_1/\mathcal{G}_2$*. Let* $\Psi_k\in\mathbb{C}_{\mathcal{G}_1}[X]$ *be the polynomial defined by Lemma 3.12 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*

$$\Phi(j)=0,\quad j_1\Phi'(j)=\Psi_1(j),\quad j_2\Phi'(j)=\Psi_2(j),\quad j_3\Phi'(j)=\Psi_3(j). \tag{17}$$

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* $c_{mn}\in F(i_1,i_2)$*.*

We let d_T *be the maximal total degree of all these 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} *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 ben computed in time* $\tilde O(dd_Td_{i_2}DN)$*.*

In the case that $\mathbb{C}_{\mathcal{G}_1}$ *is a rational surface so that we only need two primary invariants* i_1 *and* i_2*, the computation can be done in time* $\tilde O(d_Td_{i_2}DN)$*.*

Proof. As i_1,i_2,i_3,j have Fourier coefficients in F, the same argument as in Lemma 3.2 or [BL09, 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, so we can also write $c_{mn}\in F(i_1,i_2)$.

To compute the polynomial Φ, we take several (well chosen) $\tau\in\mathcal{H}_1^2$ and evaluate $\Phi(j(\tau)) = \prod_{\gamma\in\mathcal{G}_1/\mathcal{G}_2}(X-j(\gamma.\tau))$.

Computing each value $j(\gamma.\tau)$ in precision N can be done with a complexity in $D\tilde O(N)$ time. Using a subproduct tree (see [GJ99, Section 10.1]), $\Phi(j(\tau))$ can be obtained in $\tilde O(DN)$ time.

Separating the coefficients according to powers of X gives the values $c_m(i_1(\tau), i_2(\tau), i_3(\tau))$. This is a procedure to obtain the evaluation of the functions $c_m \in F(i_1, i_2, i_3)$ at any point $\tau \in \mathcal{H}_1^2$. We can thus recover the c_m by interpolation. By Section 3.3 and Theorem 3.6, to recover Φ, the evaluation step will be executed $O(dd_T d_{i_2})$ times and we will interpolate $O(dD)$ bivariate rational fractions and do $O(Dd_T d_{i_2})$ interpolation of an 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 $\tilde{O}(N)$ ([NSV11]).

The final complexity is then

$$O(dd_T d_{i_2})\tilde{O}(DN) + O(dD)\tilde{O}(d_T d_{i_2} N) + O(Dd_T d_{i_2})\tilde{O}(dN) \subset \tilde{O}(dd_T d_{i_2} DN). \tag{18}$$

The same algorithm work 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.

In the case that $\mathbb{C}_{\mathcal{G}_1}$ is a rational surface, then to compute Φ, the evaluation step will be executed $O(d_T d_{i_2})$ times and we will interpolate D bivariate rational fractions. The complexity is then

$$O(d_T d_{i_2})\tilde{O}(DN) + D\tilde{O}(d_T d_{i_2} N) \subset \tilde{O}(d_T d_{i_2} DN). \tag{19}$$

□

4 Modular polynomials

4.1 Isogenies preserving real multiplication

The main goal of this paper is to define modular polynomials, which parametrizes isogenies between principally polarized abelian surfaces with real multiplication by $\mathcal{O}_K$.

We first give more details on isogenies preserving the real multiplication and their applications.

Let (A, θ_A) be a principally polarized abelian surface, 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 whenever B admits a principal polarization. If θ_B is such a principal polarization, then $\theta = f^*\theta_B$ is a polarization on A. By [BL03, Proposition 5.2.1 and Theorem 5.2.4], the Neron-Severi group of A is isomorphic to the group of totally positive elements of $\mathrm{End}^s(A)$, where we denote by $\mathrm{End}^s(A)$ the endomorphisms commuting with the Rosati involution induced by θ_A. 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 $A[\beta]$. Looking at degrees, we also get that $\#V = N_{K/\mathbb{Q}}(\beta)$.

Conversely, let $\beta \in \mathcal{O}_K^{++}$ and note θ^β the polarization induced from θ_A by 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 [Rob13; Dud16; DDR]. We are mainly interested with cyclic isogenies of prime degree ℓ, these are induced by β of norm ℓ. We sum up the discussion above 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 exists cyclic isogenies of degree ℓ (possibly defined over an extension of the field of definition of (A,θ)) if there exists a totally positive element $\beta \in \mathcal{O}_K^{++}$ of norm ℓ. And conversely if the abelian surfaces lying on the Humbert surface admit cyclic isogenies of degree ℓ generically, then there exists such an β.*

We will apply this when $\beta = \ell \in \mathbb{Z}$ is a prime number, and when β is a totally positive element of $\mathcal{O}_K$ of norm ℓ. When $\beta = \ell$, the Weil pairing is the usual pairing e_ℓ on $A[\ell]$, and the corresponding ℓ-isogenies come from isotropic kernels of degree ℓ^2. 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 $\mathrm{Sp}_4(\mathbb{Z})/\Gamma^0(\ell)$). The computation of the corresponding modular polynomials is described in [Mil15]. On the Hilbert side of things, not all such isogenies stay on the Humbert surface. Indeed this is the case if and only if the kernel is stable under the real multiplication by $\mathcal{O}_K$. Since the Weil pairing is compatible with endomorphisms, as a $\mathcal{O}_K$ module $A[\ell]$ 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 $\mathrm{SL}_2(\mathcal{O}_K)/\Gamma^0(\ell)$ on the symplectic basis (e_1, e_2).

Proposition 4.3.

- *If ℓ is inert in $\mathcal{O}_K$ then there are ℓ^2+1 ℓ-isogenies stable under the real multiplication;*
- *If ℓ is split in $\mathcal{O}_K$ then there are $(\ell+1)^2$ ℓ-isogenies stable under the real multiplication;*
- *If ℓ is ramified in $\mathcal{O}_K$ then there are $\ell^2+\ell$ ℓ-isogenies stable under the real multiplication.*

Proof. If ℓ is inert, then $\mathrm{SL}_2(\mathcal{O}_K)/\tilde{\Gamma}^0(\ell)$ is given by the matrices $\left(\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right)$ for $x \in \mathcal{O}_K/\ell\mathcal{O}_K$ and $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$, which yields ℓ^2+1 matrices. One way to see that is to remark that $\mathrm{SL}_2(\mathcal{O}_K)/\tilde{\Gamma}^0(\ell)$ is a quotient of $\mathrm{SL}_2(\mathcal{O}_K)/\tilde{\Gamma}(\ell) = \mathrm{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K) = \mathrm{SL}_2(\mathbb{F}_{\ell^2})$ and count the matrices in $\tilde{\Gamma}^0(\ell)/\tilde{\Gamma}(\ell)$.

If ℓ splits as $(\ell) = \ell_1\ell_2$, then $\#\mathrm{SL}_2(\mathcal{O}_K)/\tilde{\Gamma}^0(\ell) = \#\mathrm{SL}_2(\mathcal{O}_K)/\tilde{\Gamma}^0(\ell_1) \times \#\mathrm{SL}_2(\mathcal{O}_K)/\tilde{\Gamma}^0(\ell_2)$ so we get $(\ell+1)^2$ elements. Again one way to see it is that $\mathrm{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K) \simeq \mathrm{SL}_2(\mathcal{O}_K/\ell_1\mathcal{O}_K) \times \mathrm{SL}_2(\mathcal{O}_K/\ell_2\mathcal{O}_K) \simeq \mathrm{SL}_2(\mathbb{F}_\ell)^2$.

Lastly if ℓ is ramified, then $\mathrm{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K) \simeq \mathrm{SL}_2(\mathbb{F}_\ell[x]/x^2)$ is of size $\ell^6-\ell^4$ and counting matrices in $\tilde{\Gamma}^0(\ell)/\tilde{\Gamma}(\ell)$ we get that there are $\ell^2(\ell^2-\ell)$ of them so $\#\mathrm{SL}_2(\mathcal{O}_K)/\tilde{\Gamma}^0(\ell) = \ell^2+\ell$. □

Next 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.

Proposition 4.4. *Let β be a totally positive element of norm ℓ. There are $\ell+1$ β-isogenies. They correspond to cyclic kernels of size ℓ in $A[\beta]$, which are stable by $\mathcal{O}_K$.*

Proof. 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 $\mathcal{O}_K/\beta\mathcal{O}_K \simeq \mathbb{F}_\ell$, the elements of $\mathcal{O}_K$ act by scalar multiplication on $A[\beta]$ so they stabilize all the cyclic subgroups. And indeed since $\mathrm{SL}_2(\mathcal{O}_K)/\Gamma(\beta) \simeq \mathrm{SL}_2(\mathbb{F}_\ell)$ it is easy to check that $\mathrm{SL}_2(\mathcal{O}_K)/\Gamma^0(\beta)$ 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 $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$.

Indeed since $\mathcal{O}_K/\beta\mathcal{O}_K \simeq \mathbb{Z}/\ell\mathbb{Z}$, we have that $\mathrm{SL}_2(\mathcal{O}_K)/\Gamma^0(\beta) \simeq \mathrm{SL}_2(\mathbb{Z})/\Gamma^0(\ell)$ whose set of representatives is well known. □

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 split as a β-isogeny and a $\overline{\beta}$-isogeny (which may be defined over an extension of greater degree). So in the split case we only need to compute β and $\overline{\beta}$ Hilbert modular polynomials.

Lemma 4.5. *Let $\ell = \beta\overline{\beta}$ be a splitting of ℓ into totally positive ideals. 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 $\epsilon^{-1}(V)$ is 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 real endomorphism $\hat{\epsilon}\epsilon$ where $\hat{\cdot}$ denote the Rosati involuation. More generally, if β is totally positive, then $\epsilon^*\theta = \theta^{\hat{\epsilon}\beta\epsilon}$.

In particular, if $f : A \to B$ is an β-isogeny, then $f \circ \epsilon$ is an $\hat{\epsilon}\beta\epsilon$ 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. Also Section 3 to compute invariants on the corresponding Hilbert surfaces can also be generalized to this case, and so are the computation of the modular polynomials for O.

4.2 Applications of isogenies and modular polynomials

There are a lot of applications to isogenies, here we only describe one of them. The CM method allows one to generate abelian surfaces with a prescribed number of points (depending on the CM field F). This is particularly important for pairings applications of cryptography since this is the only way to control the embedding degree. The output of the CM method are polynomials P_F describing the (invariants of) locus of all abelian surfaces with CM by O_F; it is a remarkable fact of Complex Multiplication theory that these polynomials give the equations of the class field of the reflex field of F corresponding to the Shimura class group.

One method to compute these polynomials described in [LR13] is the CRT approach which compute all abelian surfaces with multiplication by O_F over several primes p (carefully chosen

so that they split completely in the class field), and then use the Chinese Reminder Theorem to recover the polynomials P_F (which are defined over the real field of the reflex field of F).

To speed up this method, a key step is to first find an abelian surface in the correct isogeny class. Its endomorphism ring is then an order in F. Then one computes isogenies increasing the endomorphism ring until we get to O_F. It is not the purpose of this article to describe the very rich structure of the isogeny graph (which is layered under the real multiplication orders, the top layer being composed of the product of several volcanoes). We refer to [Rob15; IMR+13] for more details.

We just remark that it is easy to see that when O is a real order which is not maximal in ℓ, then there are no cyclic isogenies (see Proposition 4.2). But there are still ℓ-isogenies, and there is always one which can decrease the ℓ-adic valuation of the conductor of the real multiplication order. Taking ℓ-isogenies, we can then go up to maximal real multiplication (at least locally in ℓ), where we can now use Hilbert modular polynomials to stay with maximal real endomorphism and increase the size of the endomorphism ring (even if for simplicity we restrict to the maximal real order $\mathcal{O}_K$, everything is easily generalized to an order maximal at ℓ as we remarked above).

If $\ell = \alpha\overline{\alpha}$ splits into principal ideals generated by totally positive elements, the only way to be sure to go up the isogeny graph to find an abelian surface with real multiplication by O_F is to be able to compute α-modular polynomials and $\overline{\alpha}$-modular polynomial (which each form a volcano by [IT14]). If ℓ is inert, then this time we need Hilbert ℓ-modular polynomial (the ℓ-isogeny graph preserving real multiplication also forming a volcano in this case, by an easy adaptation of the arguments of [IT14]).

But climbing a volcano can be done using modular polynomials as in the case of elliptic curves [FM02].

4.3 Computing modular polynomials

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. Let $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ be a level subgroup containing $\tilde{\Gamma}(n)$ for a n prime to L. We want to apply the results of Section 3.5 to the extension $\mathbb{C}_{\tilde{\Gamma}^0(\beta)\cap\tilde{\Gamma}}/\mathbb{C}_{\tilde{\Gamma}}$.

We first want to give an explicit set of representatives of $\tilde{\Gamma}/\tilde{\Gamma}^0(\beta)\cap\tilde{\Gamma}$. Recall that there in an isomorphism $\phi_\pm : \mathrm{SL}_2(\mathcal{O}_K) \to \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$, so that by looking at the preimage by $\phi_\pm$ we can assume here that $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K)$ (this is more convenient to study the quotient). 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 $\tilde{\Gamma}/\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)$ is of cardinality $L+1$.*

Proof. $\tilde{\Gamma}/\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta) \simeq \tilde{\Gamma}\tilde{\Gamma}^0(\beta)/\tilde{\Gamma}^0(\beta)$ so by Propositions 4.3 and 4.4 it suffices to prove that $\tilde{\Gamma}\tilde{\Gamma}^0(\beta) = \tilde{\Gamma}(1)$. So it suffices to prove that $\tilde{\Gamma}(n)\tilde{\Gamma}(L) = \tilde{\Gamma}(1)$, which is obvious by the Chinese reminder theorem.

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

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

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

We can give a different proof using the matrices R, S and T: the $L+1$ matrices of C_β are clearly in differents classes of the quotient $\tilde{\Gamma}/\tilde{\Gamma}^0(\beta)$. Remark that ${}^tT = ST^{-1}S^{-1} \in \tilde{\Gamma}^0(\beta)$ and ${}^tR = SR^{-1}S^{-1} \in \tilde{\Gamma}^0(\beta)$ and that $\tilde{\Gamma}$ is generated by S, ${}^tT$ and ${}^tR$. For all $i \in \{0, \dots, L\}$, ${}^tTT^i$ and ${}^tRT^i$ are in the class of T^i while ${}^tTS$ and ${}^tRS$ are in the class of S. Moreover, ST^i is in the class of S and $SS = -I_2$ 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 $\gamma \in \tilde{\Gamma}(1)/\tilde{\Gamma}^0(\beta)$ 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 gives 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 $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$. 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 2.25 $\tilde{\Gamma}$ is stable under the real conjugation.

Let i_1, i_2, i_3 be generators of the Hilbert modular field $\mathbb{C}_{\mathcal{G}}$. (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 $\tilde{\Gamma}$. Then if j is symmetric, then $\mathbb{C}_{(\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta))\rtimes\langle\sigma\rangle} = \mathbb{C}(i_1, i_2, i_3, j)$, 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 case, we only do the case $\mathcal{G} = \tilde{\Gamma}$. We have seen in the proof of Lemma 3.12 that the extension $\mathbb{C}_{\tilde{\Gamma}(Ln)}/\mathbb{C}_{\tilde{\Gamma}(1)\cup\tilde{\Gamma}(1)\sigma}$ is Galoisian of Galois group $(\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma)/\tilde{\Gamma}(Ln)$. Let $K_1 = \mathbb{C}_{\tilde{\Gamma}}(j) = \mathbb{C}(i_1, i_2, i_3, j)$ and $K_2 = \mathbb{C}_{\tilde{\Gamma}(Ln)}^{\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)/\tilde{\Gamma}(Ln)} = \mathbb{C}_{\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)}$. Then $K_1 \subset K_2$ and we want to prove the 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 would deduce that $K_1 = \mathbb{C}_{\tilde{\Gamma}}$ or $K_1 = K_2$. By assumption, only the last possibility can be true. Since the quotient is isomorphic to $\tilde{\Gamma}(1)/\tilde{\Gamma}^0(\beta)$ by Lemma 4.8 it suffice to prove this for $\tilde{\Gamma} = \tilde{\Gamma}(1)$.

Let $\pi : \tilde{\Gamma} \twoheadrightarrow \mathrm{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K)$. If β is of norm $L = \ell$ prime (so that ℓ) 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 [Kin05, 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 $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in G$, whith $B(0) \neq 0$. If A is invertible (namely $A(0) \neq 0$) then $\left(\begin{smallmatrix} 1 & 0 \\ -AC & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} A^{-1} & 0 \\ 0 & A \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & A^{-1}B \\ 0 & 1 \end{smallmatrix}\right) \in G$ 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 $\mathrm{SL}_2(\mathcal{O}_K)$, 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. □

We want to compute modular polynomials classifying all β-isogenies from an abelian surface with real multiplication by $\mathcal{O}_K$. 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 note $\pi : (A, \theta, V) \to (A, \theta) \times (A/V, \theta')$ where θ' is the polarization induced on A/V by θ^β. This defines an algebraic map (a modular correspondence) $H_{\tilde{\Gamma}(\beta)} \to H_{\tilde{\Gamma}(1)} \times H_{\tilde{\Gamma}(1)}$. 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 $z \in \tilde{\Gamma}\backslash\mathcal{H}_1^2$, the β-isogenous varieties are $\frac{1}{\beta}\gamma \cdot z$ for $\gamma \in \tilde{\Gamma}/\tilde{\Gamma}^0(\beta)$. 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 $\gamma \in \tilde{\Gamma}/\tilde{\Gamma}^0(\beta)$.

More generally, for a group $\tilde{\Gamma}$ containing a level subgroup $\tilde{\Gamma}(n)$ with n prime 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 $H_{\tilde{\Gamma}\cap\tilde{\Gamma}(\beta)}$ correspond to a triple (A, θ, V) as above together with an extra level structure G defined by $\tilde{\Gamma}$. To define the modular correspondence 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 $\gamma_\beta = \left(\begin{smallmatrix} a & b/\beta \\ c\beta & d \end{smallmatrix}\right) \in \tilde{\Gamma}(1)$.

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* $i^\gamma_\beta(z) = i(\frac{1}{\beta}\gamma \cdot z)$. *Then for* $\gamma \in \tilde{\Gamma}^0(\beta)$,

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

Corollary 4.14. *Let* i *be a Hilbert modular function for* $\tilde{\Gamma} \subset SL_2(\mathcal{O}_K \oplus \partial_K^{-1})$. *Let* $\tilde{\Gamma}_\beta = \{\gamma \in SL_2(\mathcal{O}_K \oplus \partial_K^{-1}) \mid \gamma_\beta \in \tilde{\Gamma}\} \subset \tilde{\Gamma}^0(\beta)$. *Then* i_β *is modular 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*

$$\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta) = \tilde{\Gamma} \cap \tilde{\Gamma}_\beta. \tag{20}$$

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 $\tilde{\Gamma}$ satisfy Equation (20) (such is the case when $\tilde{\Gamma} = \tilde{\Gamma}(n)$ is a congruence subgroup), one can then define the modular correspondence as $H_{\tilde{\Gamma}\cap\tilde{\Gamma}(\beta)} \to H_{\tilde{\Gamma}} \times H_{\tilde{\Gamma}}, z \mapsto ((i_1(z), i_2(z), i_3(z)), (i_1(z/\beta), i_2(z/\beta), i_3(z/\beta)))$ 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 level subgroup such that* $\tilde{\Gamma}(2,4) \subset \tilde{\Gamma} \subset SL_2(\mathcal{O}_K \oplus \partial_K^{-1})$. *Let* $\beta \in \mathcal{O}_K^{++}$ *be a prime 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* $\tilde{\Gamma}/\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$.

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

Define the modular polynomials:

$$\Phi_\beta(X, i_1, i_2, i_3) = \prod_{\gamma \in C_\beta} (X - i^\gamma_{1,\beta}), \quad \textit{and} \quad \Psi_{k,\beta}(X, i_1, i_2, i_3) = \sum_{\gamma \in C_\beta} i^\gamma_{k,\beta} \frac{\Phi_\beta(X, i_1, i_2, i_3)}{X - i^\gamma_{1,\beta}} \tag{21}$$

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 [Mil15, Theorem 34], the modular polynomials can be computed in quasi-linear time 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* $\mathcal{G}/((\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)) \cup (\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta))\sigma) \simeq \tilde{\Gamma}/\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)$, *otherwise we let* C_β *be a set of representatives of* $\mathcal{G}/(\mathcal{G} \cap \tilde{\Gamma}^0(\beta)) \simeq \left(\tilde{\Gamma}/\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)\right) \cup \left(\tilde{\Gamma}/\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)\right)\sigma$. *Then the same definition as in Equation 21 applies and the corresponding modular polynomials can be computed in quasi-linear time.*

Proof. This is Theorem 3.13, applied to (in the notations 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 notations of Theorem 3.13 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. 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 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 representative of $\tilde{\Gamma}/\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)$ 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 is the drawback for the applications of Section 4.2, hence the interest to also have non symmetric invariants, even if they are harder to compute.

Remark 4.18 (Changing β when $\tilde{\Gamma} = \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})\sigma$)**.** Recall that we denote by ϵ the 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 $\epsilon' z \in \mathcal{H}_1^2$).

If there exists $n \in \mathbb{Z}$ such that $\epsilon' = \epsilon^{2n}$, then the matrix $\gamma = \left(\begin{smallmatrix}\epsilon^n & 0\\ 0 & \epsilon^{-n}\end{smallmatrix}\right)$ 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, the 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)**.** For a group $\tilde{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$ that does not satisfy Equation 20, then this means that from a level structure G associated to a triple (A, θ, V) correspond several level structure G' on $(A/V, \theta')$.

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

Also, if $\tilde{\Gamma}$ does not contain a level subgroup $\tilde{\Gamma}(n)$ of level n prime to ℓ, then $\tilde{\Gamma}/\tilde{\Gamma}\cap\tilde{\Gamma}^0(\beta)$ may not be isomorphic to $\tilde{\Gamma}(1)/\tilde{\Gamma}^0(\beta)$, but only isomorphic to a subgroup. We can still compute modular polynomials, but they will not parametrize all β-isogenies, only those who 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 not invariant by $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\mathfrak{I})$ for 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 β. Rather the degree depends on the factorization of (β) into prime ideals.

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

Remark 4.20 (Denominators)**.** We would like to understand the denominators of the modular polynomials corresponding to invariants i_1, i_2, i_3. Heuristically if there are no random cancellation, the denominators are due to three factors (we let D be a common denominator):

- i_1, i_2, i_3 are not defined everywhere;
- Even if i_1, i_2, i_3 are defined they may not define a local embedding of the Hilbert surface. For instance in the Siegel threefold, the three Igusa invariants defined by Streng are not defined when $\chi_{10} = 0$, and they do not define a local embedding when $\chi_4 = 0$. To get an embedding of the full threefold, Igusa showed that we need 8 invariants (10 to have good reduction modulo 2), not 3. So in this case the invariants of the β-isogenous varieties are not well defined;
- The most interesting case from the point of view of moduli is when i_1, i_2, i_3 are well defined and induce a local embedding, but one of the isogenous invariant $i_k(\frac{1}{\beta}\gamma z)$ is not well defined.

  Most of our invariants have a denominator whose locus is inside the Humbert surface H_1 (or a component) of split abelian surfaces. In particular D will contain a (component of) abelian surfaces with real multiplication by $\mathcal{O}_K$ and which admits a split β-isogenous variety. By the Lemma below, such a locus is described by (a component of) an intersection of Humbert surface $H_{\Delta_K} \cap H_{m^2}$ where Δ_K is the discriminant of $\mathcal{O}_K$.

Lemma 4.21. *If A is an abelian surface isogenous to a product of elliptic curves $E_1 \times E_2$, then there exists m such that A is m-isogenous to $E_1 \times E_2$ (with the product polarization).*

Proof. See [Gru08, Lemma 2.13] and [BL03, Theorem 5.3.7, Corollary 12.1.2]. Note that m may be different from the norm of β! □

4.4 Modular polynomials with Gundlach invariants

Recall that J_1 and J_2 are the Gundlach invariants (see Theorems 2.8 and 2.10), which we know for $K = \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$.

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

Proposition 4.22. *Let $D = 2$ or 5 and ℓ be a prime number. Write $\ell = \beta\overline{\beta}$ with $\beta \in \mathcal{O}_K^{++}$. If ℓ is ramified, 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 ℓ is split, then the polynomials

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

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

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 $D = 2$ and 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 point 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 isogenous point of 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 because when this happens, the Gundlach invariants are not always defined).

Proposition 4.23. *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 [BL09, Lemma 6.2]. Let $z \in \mathcal{H}_1^2$ which is 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 at products of elliptic curves and by Theorem 2.13, we have $F_{10} = -4\phi_\epsilon^*\chi_{10}$ so that F_{10} also vanishes at product of elliptic curves. Thus J_1 and J_2 have poles at these values and there exists some $\gamma \in \tilde{\Gamma}/\tilde{\Gamma}^0(\beta)$ such that $J^\gamma_{1,\beta}(z)$ or $J^\gamma_{1,\overline{\beta}}(z)$ is infinite. The evaluation of c_i at z is a symmetric expression in the $J^\gamma_{1,\beta}(z)$ and in the $J^\gamma_{1,\overline{\beta}}(z)$. 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 2.15, we have that $\phi_\epsilon^*\chi_{10} = \frac{-1}{4}F_4F_6$, 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 4.24. *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; see also Remark 4.20). Moreover by Lemma 4.21 H_β is an intersection of Humbert surface.

4.5 Modular polynomials with theta constants

In this section, we define modular polynomials for any D square-free by using theta constants. These polynomials are available for all D, smaller than the ones that we get from the pull-backs of the Igusa invariants. Furthermore they illustrate nicely the different possibilities of

Theorem 4.15. Lastly this illustrates how to use the action of $(\mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1}) \cup \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})\sigma)/\tilde{\Gamma}(2,4)$ to prove symmetries of these polynomials and accelerate their computations.

The invariants we use are the pullbacks of the generators for the group $\Gamma(2,4)$ defined in Section 2.1 (see Section 3.4): $\tilde{b}_i = \phi^* b_i$ for $i = 1,2,3$, which are modular functions for $\tilde{\Gamma}(2,4)$, defined in Equation (11). Recall that we have Theorem 2.30. We denote in this section $\tilde{\Gamma} = \mathrm{SL}_2(\mathcal{O}_K \oplus \partial_K^{-1})$.

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

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

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 ask that $\ell \equiv 1 \bmod 4$ and else if $D \equiv 3 \bmod 4$, ℓ must necessarily verify $\ell \equiv 1 \bmod 4$. 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 4.25. *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 4.26. *Let ℓ be a prime number. Write $\ell = \beta\overline{\beta}$ with $\beta \in \mathcal{O}_K^{++}$ and C_β be a set of representatives of $\tilde{\Gamma}(2,4)/(\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta))$. If $D \equiv 1 \bmod 4$, then the polynomials*

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

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

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

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

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 (4) and (5): in the first case, by Proposition 2.21, 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 [LNY15]). □

Note that there is 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 4.27. When $D = 2$, Equation (12) 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 verifies, 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 happen on $\sigma(\tau)$. The matrix M_σ of Equation (4) 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 it 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 equals. 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 4.28. When $D = 2, 5$ or 13, the fundamental unit 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 ϵ 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 4.29. 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 4.25 and 4.26) .

Symmetries: We can proceed in the same way with matrices $\gamma \in \tilde{\Gamma}/\tilde{\Gamma}(2,4)$ 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 two first 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 verify some relations modulo 4. As we compute the modular polynomials by evaluation/interpolation (see Section 3.3), this can be used to decrease the number of evaluations.

The existence of these matrices depend on D and β. They can be searched before the computation of the polynomials. We give some examples of relations between the exponents in Section 5 (see Equation (22)). Similar arguments have already been used in [Mil15, 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 $\phi(z')$ is isogenous to a product of elliptic curves by the 2-isogeny $\phi(z') \to \phi(z')/2$ and such that $\theta_0(\phi(z')/2) = 0$.

Proposition 4.30. *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 $\gamma \in \tilde{\Gamma}(2,4)/(\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^0(\beta))$ 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 [Dup06, 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 4.23 (see also Remark 4.20). □

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 4.25, the β-modular polynomials are

not defined for all ℓ splitting in totally positives factors. We have two ways to deal with this problem, as explained in Remark 4.19. The first one consists to find a subset of $\tilde{\Gamma}(2,4)$ for which $\tilde{b}_{i,\beta}$ is invariant (we are in the case $D \equiv 2,3 \bmod 4$). A group which always work is the group $\tilde{\Gamma}'$ defined as $\tilde{\Gamma}(2,4)$ in the case $D \equiv 1 \bmod 4$ (see Equation 11). This subgroup is of index 4 in $\tilde{\Gamma}(2,4)$ and we consider the quotient $\tilde{\Gamma}(2,4)/(\tilde{\Gamma}' \cap \tilde{\Gamma}^0(\beta))$, containing $4(\ell+1)$ classes, to define our polynomials. The second one consists to take other invariants, in particular the Rosenhain invariants $\tilde{r}_i = \phi^* r_i$. We have already seen that they are generators for the field of Hilbert modular functions invariants by $\tilde{\Gamma}(2)$ (see Theorem 2.30) and $\tilde{r}_{i,\beta}$ for $i = 1,2,3$ is always invariant by $\tilde{\Gamma}(2) \cap \tilde{\Gamma}^0(\beta)$. All the results of this section can be adapted to these invariants.

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.

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

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

and for $\ell = 17$

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

Table 1 contains some informations 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 $D(J_1, J_2)$, 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.

We have computed the β-modular polynomials for $\ell = 17$, 41, 73, 89 and 97 (which are 1 modulo 4, see Proposition 4.25). By Remark 4.27, the β-modular polynomials are

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

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: Informations about the modular polynomials for $D = 2$

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

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

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 $\beta = 5 + 2\sqrt{2}$

$$\begin{array}{rcl} m & \equiv & 0 \bmod 2 \\ n+i & \equiv & 0 \bmod 2 \\ m+n & \equiv & i \bmod 4 \end{array} \quad \text{and} \quad \begin{array}{rcl} m & \equiv & 1 \bmod 2 \\ n+i & \equiv & 1 \bmod 2 \\ m+n & \equiv & i \bmod 4 \end{array} \tag{22}$$

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: Informations about the modular polynomials for $D = 2$

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 $\ell \equiv 1 \bmod 4$.

Taking $\ell = 7$ ($\ell \equiv 3 \bmod 4$), we have done as explained at the end of Section 4.5. 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 constated that the denominators of c_i and of d_i are of the form $D(J_1, J_2)^4$ except for $i = 2\ell + 1$ where it is $D(J_1, J_2)^2$. We have for example for $\ell = 11$

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

We have computed the β-modular polynomials 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 (12) and what we said in Section 4.5. Table 3 contains the same informations as Table 1, but the first part concern 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

First at all, 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 $p \neq \beta\overline{\beta}$ without loosing their meaning ([BGL11, 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 followinf 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: Informations 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 [Tat66]).

5.4 Denominators of the Hilbert modular polynomials and intersection of Humbert surfaces

From Remark 4.20, Propositions 4.23 and 4.24 we know that some factors (which we call the interesting factors) of the denominators of the Hilbert β-modular polynomials in the pullbacks of the Igusa invariants or in the Gundlach invariants for $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$ lie the locus L_β of abelian surfaces with real multiplication by $\mathcal{O}_K$ which are β-isogenous with a product of elliptic curves (endowed with the product polarization).

By Lemma 4.21, L_β is a curve inside an intersection of Humbert surfaces $H_{\Delta_K} \cap H_{m^2}$ where Δ_K is the discriminant of $\mathcal{O}_K$. The goal of this section is to describe L_β and this intersection in more details. (More precisely since we remove the uninteresting factors coming from the intersection of H_1 and H_{Δ_K}, we study $L_\beta \setminus H_1$).

First we explain how to find m. If $\beta = \ell$ is inert, then we can obviously take $m = \ell$. The interesting case is when β comes from a split prime ℓ. By Proposition 2.20, if A is an abelian surface, then $A \in H_{m^2}$ if and only if there is a symmetric endomorphism f on A of discriminant m^2. We recall (see [BL03, Section 1.1 and 1.2]) that an endomorphism f is induced by its analytic representation $\rho_a(f)$ which is given by a two by two matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. This matrix can also be seen as the action of f on the tangent space of A at the neutral point 0_A. The discriminant of f is then defined to be the discriminant of the characteristic polynomial of this matrix: $\Delta_f = (a+d)^2 - 4(ad-bc)$.

On a product of elliptic curves $E_1 \times E_2$ (seen as a torus in $\mathbb{C}^2$), the endomorphism given by the matrix $\gamma_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ on the tangent space at the neutral point is of discriminant 1. If $A \in L_\beta$ and f is the isogeny from A to $E_1 \times E_2$ (endowed with the product polarization), then pulling back the endomorphism γ_1 by f gives an endomorphism $f^*\gamma_1$ of A. If we compute the matrix associated to the action of $f^*\gamma_1$ on the tangent space, then its discriminant will give us a possible value of m. (As we will see below, the denominators lie in several H_{m^2} and changing the matrix γ_1 by others which have discriminant 1 will give other possible values of m). The following lemma allows us to compute the analytic representation of $f^*\gamma_1$.

Lemma 5.1. *Let $1, \omega$ as a basis of $\mathcal{O}_K$, and $R = \left(\begin{smallmatrix} 1 & \omega \\ 1 & \overline{\omega} \end{smallmatrix}\right)$ be the matrix given in Section 2.3 for the isomorphism ϕ.*

Let $f : A \to E_1 \times E_2$ be a β-isogeny, and denote $f^\vee$ the β-contragredient isogeny. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be the analytic representation of an endomorphism e of $E_1 \times E_2$. Then the analytic representation of $f^\vee \circ e \circ f$ is given by $\left(\begin{smallmatrix} \beta & 0 \\ 0 & \overline{\beta} \end{smallmatrix}\right) R\gamma R^{-1}$.

Proof. By Section 2.2, A is of the form $\mathbb{C}^2/(\mathbf{\Phi}(\mathcal{O}_K) \oplus \mathbf{\Phi}(\partial_K^{-1})\tau)$ for $\tau = (\tau_1, \tau_2) \in \mathcal{H}_1^2$ and $\mathbf{\Phi} = (\cdot, \bar{\cdot})$ is given by the two real embeddings of K. We can assume that the isogeny f is of the form

$$\mathbb{C}^2/\mathbf{\Phi}(\mathcal{O}_K) \oplus \mathbf{\Phi}(\partial_K^{-1})\tau \to \mathbb{C}^2/\mathbf{\Phi}(\mathcal{O}_K) \oplus \mathbf{\Phi}(\partial_K^{-1})(\tau/\beta), z \mapsto z$$

where $\tau/\beta = (\tau_1/\beta, \tau_2/\overline{\beta})$. The action on the tangent space of f is thus the identity.

The isogeny $f^\vee$ is then given by

$$\mathbb{C}^2/\mathbf{\Phi}(\mathcal{O}_K) \oplus \mathbf{\Phi}(\partial_K^{-1})(\tau/\beta) \to \mathbb{C}^2/\mathbf{\Phi}(\mathcal{O}_K) \oplus \mathbf{\Phi}(\partial_K^{-1})\tau, z \mapsto \beta.z$$

where $\beta.(z_1, z_2) = (\beta z_1, \overline{\beta} z_2)$. The action on the tangent space of f is thus $\left(\begin{smallmatrix} \beta & 0 \\ 0 & \overline{\beta} \end{smallmatrix}\right)$.

The product $E_1 \times E_2$ is of the form $\mathbb{C}^2/(\mathbb{Z}^2 \oplus \mathbb{Z}^2\Omega)$ where $\Omega = \left(\begin{smallmatrix} \tau_1' & 0 \\ 0 & \tau_2' \end{smallmatrix}\right) \in \mathcal{H}_2$. By definition, the action on the tangent space of e is given by γ.

Finally we glue everything together by looking at the change of basis on $\mathbb{C}^2$ which sends $\mathbf{\Phi}(\mathcal{O}_K)$ to $\mathbb{Z}^2$; this is given by the matrix R^{-1}. □

Example 5.2. For $\mathbb{Q}(\sqrt{2})$, $\omega = 1 + \sqrt{2}$:

- If $\beta = 2 + \sqrt{2}$ (of norm 2), we find that $f^*\gamma_1$ has discriminant 1, so we can take $m = 1$. Using $\gamma_2 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ instead, we get a $f^*\gamma_2$ of discriminant 3^2, so we can also take $m = 3$. So $L_\beta \subset H_8 \cap H_1 \cap H_9$.
- If $\beta = 3 + \sqrt{2}$ (of norm 7), we get respectively $f^*\gamma_i$ of discriminant 2^2 and 4^2. So $L_\beta \subset H_8 \cap H_4 \cap H_{16}$.
- If $\beta = 5 + 2\sqrt{2}$ (of norm 17), we get respectively $f^*\gamma_i$ of discriminant 3^2 and 7^2. So $L_\beta \subset H_8 \cap H_9 \cap H_{49}$.

For $\mathbb{Q}(\sqrt{5})$, $\omega = \frac{1+\sqrt{5}}{2}$:

- If $\beta = 3 - \omega$ (of norm 5) we find respectively $f^*\gamma_i$ of discriminant 3^2 and 2^2. So $L_\beta \subset H_5 \cap H_4 \cap H_9$.
- If $\beta = 4 - \omega$ (of norm 11), we get respectively $f^*\gamma_i$ of discriminant 4^2 and 3^2. So $L_\beta \subset H_5 \cap H_9 \cap H_{16}$.

Now we want to describe the intersection of $H_{\Delta_K} \cap H_{m^2}$ in more details. Some Humbert surfaces were computed in [Gru08] so we could compute the intersections from their equations but we use a different method.

As explained in [Mil15], the ℓ-modular polynomials (in the Siegel space) using Streng invariants have been computed for $\ell = 2, 3$. We explain in this section what happens if we substitute in these polynomials the Streng invariants by the Gundlach ones. Recall that the Streng invariants are the functions $\mathfrak{i}_1$, $\mathfrak{i}_2$, $\mathfrak{i}_3$ defined by

$$\mathfrak{i}_1 = \frac{h_4 h_6}{h_{10}} = \frac{\mathfrak{j}_2(\mathfrak{j}_2 - 3\mathfrak{j}_3)}{2\mathfrak{j}_1}, \qquad \mathfrak{i}_2 = \frac{h_4^2 h_{12}}{h_{10}^2} = \frac{\mathfrak{j}_2^2}{\mathfrak{j}_1}, \qquad \mathfrak{i}_3 = \frac{h_4^5}{h_{10}^2} = \frac{\mathfrak{j}_2^5}{\mathfrak{j}_1^3}. \tag{23}$$

By [BL09, Lemma 6.2], the denominators of these ℓ-modular polynomials are divisible by a polynomial D_ℓ which parametrizes the Humbert surface H_{ℓ^2} where we exclude the points in H_1. We recall that H_{ℓ^2} is a surface representing the principally polarized abelian surfaces which are ℓ-isogenous to a product of elliptic curves and that the Streng invariants are not defined at the product of elliptic curves.

Thus we have

$$D_\ell(\mathfrak{i}_1(\Omega), \mathfrak{i}_2(\Omega), \mathfrak{i}_3(\Omega)) = 0, \qquad \text{when} \quad \Omega \in H_{\ell^2} \backslash H_1.$$

Now consider the application $\phi_\epsilon : \mathrm{SL}_2(\mathcal{O}_K) \to \mathcal{H}_2$ for $K = \mathbb{Q}(\sqrt{\Delta})$ and $\Delta = 5, 8$. Let τ be in $\mathcal{H}_1^2$. Proposition 2.21 tells us that $\phi_\epsilon(\tau) \in H_{\Delta_K}$ and then

$$D_\ell(\mathfrak{i}_1(\phi_\epsilon(\tau)), \mathfrak{i}_2(\phi_\epsilon(\tau)), \mathfrak{i}_3(\phi_\epsilon(\tau))) = 0, \qquad \text{when} \quad \phi_\epsilon(\tau) \in (H_{\ell^2} \cap H_{\Delta_K}) \backslash H_1.$$

Now using the corollaries 2.14 and 2.16 and the equations relating the Igusa invariants with the Streng ones (Equation 23), it is possible to express the $\mathfrak{i}_k \circ \phi_\epsilon$ in function of the Gundlach invariants. This describe the intersection of $H_{\ell^2} \cap H_{\Delta_K}$ inside of H_{Δ_K} in term of the Gundlach invariants.

But, while the polynomial $D_\ell(\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)$ is irreducible, we have remarked that this is not the case of the polynomial $D_\ell(J_1, J_2)$. So the curve $H_{\ell^2} \cap H_{\Delta_K}$ splits into several components. We want to understand the factors and to do that we have to understand the intersection of two general Humbert surfaces. The reference for this are [Kan94; Kan14; Kan].

Definition 5.3. Let q be an integral positive definite quadratic form in r variables. Let

$$H(q) := \left\{ \Omega \in \mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z}) : \begin{array}{c} \{\text{discriminants of the primitive singular relations satisfied by } \Omega\} \\ = \{\text{integers which are represented primitively by } q\} \end{array} \right\}.$$

We call $H(q)$ a *generalized Humbert variety.*

By [Kan], $H(q)$ has codimension r in $\mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z})$ (and we refer to the papers cited above for more details on the moduli interpretation of $H(q)$). Now, if $r = 1$, $\Delta \equiv 0, 1 \bmod 4$ and $\Delta > 0$, then we have the equality $H_\Delta = H(\Delta x^2)$ (recall Proposition 2.19). Thus, the term *generalized Humbert variety* is justified. Moreover, it is a classical result that two equivalent forms (modulo $\mathrm{GL}_r(\mathbb{Z})$) q and q' represent the same integers. This implies by definition that $H(q) = H(q')$, but by [Kan14, Corollary 33], the reciprocity is also true. Then

$$H(q) = H(q') \iff q \approx q'.$$

Let q be an integral binary positive definite quadratic form: $q(x, y) = ax^2 + bxy + cy^2$. We denote this form $q = [a, b, c]$ and we denote by $q \to n$ the fact that q represent the integer n primitively. Let Δ and Δ' be two positive discriminants. Then the intersection of the corresponding Humbert surfaces is obviously:

$$H_\Delta \cap H_{\Delta'} = \bigcup_{\substack{q \to \Delta \\ q \to \Delta'}} H(q).$$

By [Kan], a form q as in the union satisfies $|\operatorname{disc}(q)| \leq 4\Delta\Delta'$. Thus, up to equivalence, there are finitely many forms in the union. Looking at the reduced forms is still not enough to compute the intersection of two Humbert surfaces, as a set $H(q)$ may be empty. We overcome this difficulty in the following way.

Definition 5.4. Let n, r, d be integers with $n \wedge d = 1$. We define by $T(n, r, d)$ the set of the integral binary quadratic forms $q = [a, b, c]$ such that

1. $\operatorname{disc}(q) = b^2 - 4ac = -16r^2 d$;
2. $q \to (rn)^2$;

3. $q(x,y) \equiv 0, 1 \bmod 4$, for all $x, y \in \mathbb{Z}$.

Theorem 5.5. *Let q be an integral binary quadratic form such that $q \to N^2$, for some $N \geq 1$. Then*

$$\begin{aligned} H(q) \neq \emptyset &\iff H(q) \text{ is an irreducible curve} \\ &\iff q \in T(N/r, r, d), \text{ for some } r|N \text{ and } d \geq 1 \text{ with } (N/r) \wedge d = 1 \end{aligned}$$

Proof. See [Kan]. □

Remark 5.6. When $r = 1$, by [FK09, Section 6] we are in the conditions of [Kan14], where the genus 2 curves whose Jacobian is isomorphic to a product of elliptic curves are studied (as a non polarized abelian surface!).

What is interesting for us from the point of view of moduli, is that a modular point in $H(q) \in T(N/r, r, d)$ corresponds to an abelian surface A which is N-isogenous to a product of elliptic curves $E_1 \times E_2$ which admits a cyclic isogeny f of degree d: $f : E_1 \to E_2$.

Proposition 5.7. *$L_\beta \backslash H_1$ is inside a union of curves $H(q)$ for quadratic forms $q \in T(N/r, r, L)$, which furthermore represent Δ_K, where L is the norm of β and N can be determined from Lemma 5.1 as in Example 5.2.*

Proof. Since $A \in H_{\Delta_K}$, q represents Δ_K by Definition 5.4. Since $A \in L_\beta$, there exists a β-isogeny $f : A \to E_1 \times E_2$. By Lemma 4.21 and Lemma 5.1, A is N-isogenous to $E_1 \times E_2$.

From the moduli interpretation above, it then suffices to check that there is a cyclic isogeny of degree L from E_1 to E_2. But the pullback of the principal polarization on A to $E_1 \times E_2$ by the β-contragredient isogeny $f^\vee$ gives a polarization of degree L, which is not a product polarization since $A \notin H_1$ by assumption on A. The structure of the Neron-Severi group on $E_1 \times E_2$ (see [Kan14, Section 6, Appendix]) implies that this polarization is induced by an isogeny of degree L from E_1 to E_2. □

Using the previous results, it is possible to compute intersections of Humbert surfaces. The ones we are interested in are:

$$\begin{aligned} H_4 \cap H_5 = &\ H([1,0,4]) \cup H([4,0,5]) \cup H([4,4,5]); \\ H_9 \cap H_5 = &\ H([4,0,5]) \cup H([5,2,9]) \cup H([5,4,8]); \\ H_4 \cap H_8 = &\ H([1,0,4]) \cup H([4,0,4]) \cup H([4,0,8]) \cup H([4,4,8]); \\ H_9 \cap H_8 = &\ H([1,0,8]) \cup H([8,0,9]) \cup H([5,4,8]) \cup H([8,4,9]) \cup H([8,8,9]). \end{aligned}$$

Looking at the factorization of $D_\ell(J_1, J_2)$, we try to identify the factors with the generalized Humbert varieties of these intersections. This allows us to compute the equations for the $H(q)$ in the intersection. We can also match these factors with factors of the denominators of the β-modular polynomials we have computed. This allows us to match L_β with the correct $H(q)$.

Case $K = \mathbb{Q}(\sqrt{2})$ and $\ell = 2$ ($H_4 \cap H_8$): The factorization of the polynomial $D_2(\mathfrak{i}_1 \circ \phi_\epsilon, \mathfrak{i}_2 \circ \phi_\epsilon, \mathfrak{i}_3 \circ \phi_\epsilon) = D_2(J_1, J_2)$ is $D_2(J_1, J_2) = 3^{10} J_1 (J_1 + 144)^{10} (J_1 + 4J_2)^2 (J_1^2 - J_1 J_2^2 + 2J_1 J_2 - 81J_1 + 64J_2^2)^2 (J_1^2 J_2 + 4J_1^2 - 288 J_1 J_2 - 1024 J_1 - 1728 J_2^2)$. We could think that there would be a bijection between the factors and the Humbert varieties in the intersection $H_4 \cap H_8$, but this is not true. Indeed, the form $[1,0,4]$ represents the number 1 primitively so that $\Omega \in H([1,0,4])$

implies $\Omega \in H_1$, which means that the variety associated to Ω is isomorphic to a product of elliptic curves and the invariants we use are not defined at such Ω.

For each factor, we tried to find a period matrix Ω, which makes this factor vanish (see Theorem 3.8), and for such a matrix we computed the discriminants of many primitive singular relations satisfied by Ω and compared these numbers with the numbers represented primitively by the forms in the intersection $H_4 \cap H_8$, according to Definition 5.3.

We have found:

$$\begin{array}{ll} H([4,0,4]) & J_1 + 4J_2 \\ H([4,4,8]) & J_1^2 - J_1J_2^2 + 2J_1J_2 - 81J_1 + 64J_2^2 \\ H([4,0,8]) & J_1^2J_2 + 4J_1^2 - 288J_1J_2 - 1024J_1 - 1728J_2^2 \end{array}$$

The factor corresponding to $H([4,4,8])$ is the common denominator of the β-modular polynomials for $\ell = 7$ (a split prime). From Example 5.2 we knew that $L_\beta \subset H_8 \cap H_4 \cap H_{16}$ and we check that indeed $[4,4,8]$ has discriminant -16×7 (see Proposition 5.7).

We focus now on the factors J_1 and $J_1 + 144$ in the denominator. Writing the pullbacks of the Streng invariants in function of J_1 and J_2 and putting $J_1 = 0$, we obtain $\phi_\epsilon^*\mathfrak{i}_1 = -972$, $\phi_\epsilon^*\mathfrak{i}_2 = 7776$, $\phi_\epsilon^*\mathfrak{i}_3 = 0$. But the last equality implies $\phi_\epsilon^* h_4 = 0$ (or equivalently $\phi_\epsilon^*\psi_4 = 0$) and thus $\phi_\epsilon^*\mathfrak{i}_1 = 0$ and $\phi_\epsilon^*\mathfrak{i}_2 = 0$ which is contradictory. Thus, J_1 can not be zero. Similarly, $J_1 + 144 = 0$ implies that the Streng invariants are 0 and thus $\phi_\epsilon^* h_4 = 0$. This can also be seen looking at the first equality of Theorem 2.15.

So these two factors correspond to the non interesting part of the denominator, as explained in Remark 4.20, and do not correspond to components of L_β.

Case $K = \mathbb{Q}(\sqrt{2})$ and $\ell = 3$ ($H_9 \cap H_8$): $D_3(J_1,J_2) = 2^{312}3^{21}(J_1+144)^{20}(J_1^3 + 3J_1^2J_2 - 162J_1^2 - 2268J_1J_2 + 6561J_1 - 5184J_2^2)(J_1^4 + 8J_1^3J_2 + 288J_1^3 - J_1^2J_2^3 + 14J_1^2J_2^2 + 5952J_1^2J_2 + 20736J_1^2 - 360J_1J_2^3 + 32992J_1J_2^2 - 3375J_2^4)^2(J_1^4J_2 + 3J_1^4 - 1332J_1^3J_2 - 3888J_1^3 + 6750J_1^2J_2^2 + 485028J_1^2J_2 + 1259712J_1^2 + 5346000J_1J_2^2 + 3779136J_1J_2 + 11390625J_2^3)(J_1^7 - J_1^6J_2^3 - 6J_1^6J_2^2 + J_1^6J_2 - 414J_1^6 + 428J_1^5J_2^3 + 2387J_1^5J_2^2 - 17760J_1^5J_2 + 431811J_1^5 + 17728J_1^4J_2^4 - 331952J_1^4J_2^3 - 2578856J_1^4J_2^2 + 6229197J_1^4J_2 - 80515134J_1^4 - 6145536J_1^3J_2^4 + 52974272J_1^3J_2^3 + 535037040J_1^3J_2^2 + 6116816412J_1^3J_2 + 37822859361J_1^3 - 91648000J_1^2J_2^5 - 6502153216J_1^2J_2^4 - 75793205760J_1^2J_2^3 - 197144611776J_1^2J_2^2 - 17565696000J_1J_2^5 - 7812042752J_1J_2^4 + 110592000000J_2^6)$

$$\begin{array}{ll} H([5,4,8]) & J_1^3 + 3J_1^2J_2 - 162J_1^2 - 2268J_1J_2 + 6561J_1 - 5184J_2^2 \\ H([8,8,9]) & J_1^4 + 8J_1^3J_2 + 288J_1^3 - J_1^2J_2^3 + 14J_1^2J_2^2 + \ldots \\ H([8,0,9]) & J_1^4J_2 + 3J_1^4 - 1332J_1^3J_2 - 3888J_1^3 + 6750J_1^2J_2^2 + \ldots \\ H([8,4,9]) & J_1^7 - J_1^6J_2^3 - 6J_1^6J_2^2 + J_1^6J_2 + \ldots \end{array}$$

Here, we have that $H([5,4,8])$ corresponds to the common denominator of the β modular polynomials for $\ell = 3$. Since $\ell = 3$ is inert, we knew that $L_3 \subset H_8 \cap H_9$, furthermore we check that $[5,4,8]$ is of discriminant -16×9. Also $H([8,4,9])$ corresponds to β dividing $\ell = 17$ (a split prime). Once again this was expected from Example 5.2 and the fact that the quadratic form has discriminant -16×17.

Case $K = \mathbb{Q}(\sqrt{5})$ and $\ell = 2$ ($H_4 \cap H_5$): $D_2(J_1,J_2) = 3^{10}(J_2 - 32)^2J_1^2(J_1^3 - 2J_1^2J_2^2 - 1000J_1^2J_2 + 50000J_1^2 + J_1J_2^4 + 1800J_1J_2^3 - 864J_2^5)$

$$\begin{array}{ll} H([4,4,5]) & J_2 - 32 \\ H([4,0,5]) & J_1^3 - 2J_1^2J_2^2 - 1000J_1^2J_2 + 50000J_1^2 + J_1J_2^4 + 1800J_1J_2^3 - 864J_2^5 \end{array}$$

The factor associated to $H([4,0,5])$ is the common denominator of the β-modular polynomials for β dividing $\ell = 5$ (a ramified prime) while the one associated to $H([4,4,5])$ is the common denominator of the modular polynomials for $\ell = 2$ (which is an inert prime). One can check that the quadratic forms have discriminant -16×5 and -16×4 respectively.

As previously, if we write the pullbacks of the Streng invariants in function of J_1 and J_2 and if we put $J_1 = 0$, then we obtain $\phi_\epsilon^*\mathfrak{i}_1 = -27J_2/8$, $\phi_\epsilon^*\mathfrak{i}_2 = 3J_2/32$ and $\phi_\epsilon^*\mathfrak{i}_3 = 0$ and we deduce that $J_1 = 0$ is equivalent to $\phi_\epsilon^* h_4 = 0$. This can also be deduced by the first equality of Theorem 2.13.

Case $K = \mathbb{Q}(\sqrt{5})$ and $\ell = 3$ ($H_9 \cap H_5$): $D_3(J_1,J_2) = 3^{21}(J_1^3 - 2J_1^2J_2^2 - 1000J_1^2J_2 + 50000J_1^2 + J_1J_2^4 + 1800J_1J_2^3 - 864J_2^5)(4J_1^4 + 12J_1^3J_2^2 + 8748J_1^3J_2 + 12882159J_1^3 + 30132J_1^2J_2^3 + 34698942J_1^2J_2^2 + 10857300264J_1^2J_2 + 2339378717616J_1^2 - 820125J_1J_2^4 + 34031907000J_1J_2^3 - 29524500000J_2^5)(4J_1^7 - 12J_1^6J_2^2 - 19236J_1^6J_2 + 119497519J_1^6 + 12J_1^5J_2^4 + 56972J_1^5J_2^3 - 387805052J_1^5J_2^2 - 278163835056J_1^5J_2 + 35953243171744J_1^5 - 4J_1^4J_2^6 - 55980J_1^4J_2^5 + 449730698J_1^4J_2^4 + 943837290960J_1^4J_2^3 - 133230692691392J_1^4J_2^2 + 6651010132099840J_1^4J_2 + 13001634695104256J_1^4 + 18500J_1^3J_2^7 - 215193500J_1^3J_2^6 - 1170430882000J_1^3J_2^5 + 388324233980000J_1^3J_2^4 - 32395226716512000J_1^3J_2^3 + 32609375J_1^2J_2^8 + 635091750000J_1^2J_2^7 - 718632513000000J_1^2J_2^6 + 34620677424000000J_1^2J_2^5 - 124875000000J_1J_2^9 + 601911000000000J_1J_2^8 - 182250000000000J_2^{10})$

$$\begin{array}{ll} H([4,0,5]) & J_1^3 - 2J_1^2J_2^2 - 1000J_1^2J_2 + 50000J_1^2 + J_1J_2^4 + 1800J_1J_2^3 - 864J_2^5 \\ H([5,4,8]) & 4J_1^4 + 12J_1^3J_2^2 + 8748J_1^3J_2 + 12882159J_1^3 + \ldots \\ H([5,2,9]) & 4J_1^7 - 12J_1^6J_2^2 - 19236J_1^6J_2 + 119497519J_1^6 + \ldots \end{array}$$

The variety $H([4,0,5])$ is associated to the denominator for $\ell = 5$ (ramified), $H([5,4,8])$ to $\ell = 3$ (inert) and $H([5,2,9])$ to $\ell = 11$ (split). And again the discrimant of these quadratic forms are respectively -16×5, -16×9 and -16×11.

The fact that the denominators for $\beta = \ell = 3$ do not correspond to the full $H_5 \cap H_9$ is that the latter is the locus of abelian surfaces with real multiplication by $\mathcal{O}_K$ which admit a 3-isogeny to a split abelian surface, while the former requires that the 3-isogeny to a split abelian surface is compatible with the real multiplication (so its kernel is stable under the action of $\mathcal{O}_K$). Hence it is not surprising that we only get a component.

Remark 5.8. We can see that $H([5,4,8])$ appears in $H_9 \cap H_8$ and in $H_9 \cap H_5$ so that we have two description of this variety.

More generally it seems from these computations that the component L_β of the denominator of the β-modular polynomials corresponds to only one $H(q)$; so it describes an irreducible curve in $H_{\Delta_K} \cap H_m$. It would be interesting to know if this is true in general, or only due to the small discriminants of the real quadratic fields in our examples. Secondly, if the denominator is indeed a $H(q)$, then it would be nice to have an intrinsic way to compute this q. We know that it has to satisfy the conditions of Proposition 5.7, does this determines q completely?

References

[BGL+16] S. Ballentine, A. Guillevic, E. Lorenzo García, C. Martindale, M. Massierer, B. Smith, and J. Top. "Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication". working paper or preprint. Dec. 2016. URL: https://hal.inria.fr/hal-01421031 (cit. on p. 24).

[Bec94] T. Becker. "On Gröbner bases under specialization". In: *Applicable Algebra in Engineering, Communication and Computing* 5.1 (1994), pp. 1–8 (cit. on p. 21).

[BL03] C. Birkenhake and H. Lange. *Complex abelian varieties*. Vol. 302. Grundlehren der Mathematischen Wissenschaften. Springer, 2003 (cit. on pp. 5, 7, 27, 35, 44).

[BW03] 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. 12, 13).

[BL09] 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. 2, 18, 26, 36, 45).

[BGL11] 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. arXiv: 0910.1848 (cit. on pp. 3, 42).

[BLS12] R. Bröker, K. Lauter, and A. Sutherland. "Modular polynomials via isogeny volcanoes". In: *Mathematics of Computation* 81.278 (2012), pp. 1201–1231. arXiv: 1001.0402 (cit. on p. 2).

[Bru08] J. H. Bruinier. "Hilbert modular forms and their applications". In: *The 1-2-3 of modular forms*. Springer, 2008, pp. 105–179 (cit. on p. 7).

[CLG09] D. Charles, K. Lauter, and E. Goren. "Cryptographic hash functions from expander graphs". In: *Journal of Cryptology* 22.1 (2009), pp. 93–113. ISSN: 0933-2790 (cit. on p. 2).

[CL09] 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. 2).

[DDR] J. Dimitar, A. Dudeanu, and D. Robert. "Computing cyclic isogenies using in genus 2" (cit. on p. 28).

[DIK06] 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. 2).

[Dud16] A. Dudeanu. "Computational Aspects of Jacobians of Hyperelliptic Curves". PhD thesis. École Polytechnique Fédérale de Lausanne, 2016 (cit. on p. 28).

[Dup06] R. Dupont. "Moyenne arithmético-géométrique, suites de Borchardt et applications". http://www.lix.polytechnique.fr/Labo/Regis.Dupont/. PhD thesis. École polytechnique, 2006 (cit. on pp. 2–4, 6, 19, 22, 23, 39).

[Elk97] N. Elkies. "Elliptic and modular curves over finite fields and related computational issues". In: *Computational perspectives on number theory: proceedings of a conference in honor of AOL Atkin, September 1995, University of Illinois at Chicago*. Vol. 7. Amer Mathematical Society. 1997, p. 21 (cit. on p. 2).

[EK14] 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. 5, 7, 18, 24, 25).

[Eng09] A. Enge. "Computing modular polynomials in quasi-linear time". In: *Math. Comp* 78.267 (2009), pp. 1809–1824 (cit. on p. 2).

[ES10] 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. 2).

[ET14] A. Enge and E. Thomé. "Computing class polynomials for abelian surfaces". In: *Experimental Mathematics* (2014) (cit. on p. 23).

[EM02] 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. 2).

[FM02] M. Fouquet and F. Morain. "Isogeny volcanoes and the SEA algorithm". In: *Algorithmic number theory (Sydney, 2002)*. Vol. 2369. Lecture Notes in Comput. Sci. Berlin: Springer, 2002, pp. 276–291. DOI: 10.1007/3-540-45455-1_23 (cit. on p. 30).

[Fre90] E. Freitag. "Hilbert modular forms". In: *Hilbert Modular Forms*. Springer, 1990, pp. 5–71 (cit. on p. 7).

[FK09] G. Frey and E. Kani. "Curves of genus 2 with elliptic differentials and associated Hurwitz spaces". In: *Contemporary Mathematics* 14 (2009), p. 33 (cit. on p. 47).

[GHS02] 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. 2).

[GJ99] 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. 26).

[Gau00] P. Gaudry. "Algorithmique des courbes hyperelliptiques et applications à la cryptologie". PhD thesis. École Polytechnique, 2000 (cit. on p. 2).

[Gau07] P. Gaudry. "Fast genus 2 arithmetic based on Theta functions". In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265 (cit. on p. 2).

[GHK+06] 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. 25).

[Gor02] E. Z. Goren. *Lectures on Hilbert modular varieties and modular forms*. American Mathematical Soc., 2002 (cit. on p. 7).

[Gru08] D. Gruenewald. "Explicit algorithms for Humbert surfaces". http://echidna.maths.usyd.edu.au/~davidg/thesis.html. PhD thesis. University of Sydney, 2008 (cit. on pp. 12, 13, 17, 24, 35, 45).

[Gun63] 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 p. 9).

[HZ77] 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. 8).

[Hum99] 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. 12).

[Hum00] 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. 12).

[Hum01] 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. 12).

[Igu60] J. Igusa. "Arithmetic variety of moduli for genus 2". In: *Annals of Mathematics* 72.3 (1960) (cit. on pp. 2, 6).

[Igu62] J. Igusa. "On Siegel modular forms of genus 2". In: *Johns Hopkins University Press* 84.1 (1962) (cit. on pp. 2, 6).

[IMR+13] S. Ionica, C. Martindale, D. Robert, and M. Streng. "Isogeny graphs of ordinary abelian surfaces over a finite field". Mar. 2013. In preparation. (Cit. on p. 30).

[IT14] S. Ionica and E. Thomé. "Isogeny graphs with maximal real multiplication." In: *IACR Cryptology ePrint Archive* 2014 (2014), p. 230 (cit. on p. 30).

[Kal97] M. Kalkbrener. "On the stability of Gröbner bases under specializations". In: *Journal of Symbolic Computation* 24.1 (1997), pp. 51–58 (cit. on p. 21).

[Kan] E. Kani. *Generalized Humbert Schemes and Intersections of Humbert Surfaces*. http://gmplib.org/. University of Iowa, Ames, Iowa, 27 April 2013 (cit. on pp. 5, 46, 47).

[Kan94] E. Kani. "Elliptic curves on abelian surfaces". In: *Manuscripta Mathematica* 84 (1 1994), pp. 199–223 (cit. on p. 46).

[Kan14] E. Kani. "The moduli spaces of Jacobians isomorphic to a product of two elliptic curves". In: *Journal of Number Theory* 139.1 (2014), pp. 138–174 (cit. on pp. 46, 47).

[Kin05] 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. 32).

[Lab16] H. Labrande. "Explicit computation of the Abel-Jacobi map and its inverse". PhD thesis. Université de Lorraine, 2016 (cit. on p. 4).

[LT16] 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. DOI: 10.1112/S1461157016000309 (cit. on p. 4).

[LNY15] K. Lauter, M. Naehrig, and T. Yang. "Hilbert theta series and invariants of genus 2 curves". In: *Journal of Number Theory* (2015) (cit. on pp. 3, 38).

[LY11] 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. 3, 8, 10, 11).

[LR13] 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*. Ed. by E. W. Howe and K. S. Kedlaya. Vol. 1. The Open Book Series. Berkeley: Mathematical Sciences Publisher, Nov. 2013, pp. 437–461. DOI: 10.2140/obs.2013.1.437. URL: http://www.normalesup.org/~robert/pro/publications/articles/classCRT.pdf. Slides: 2012-07-ANTS-SanDiego.pdf (30min, International Algorithmic Number Theory Symposium (ANTS-X), July 2012, San Diego, USA), HAL: hal-00734450, eprint: 2012/443. (Cit. on pp. 3, 29).

[LLL82] 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. 21).

[Man94] R. Manni. "Modular varieties with level 2 theta structure". In: *American Journal of Mathematics* 116 (1994), pp. 1489–1511 (cit. on p. 6).

[Mar16] C. Martindale. In preparation. PhD thesis. Universiteit Leiden, 2016 (cit. on p. 24).

[Mil15] 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. 2, 3, 6, 19, 20, 22, 24, 28, 33, 39, 45).

[Mor95] F. Morain. "Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques". In: *J. Théor. Nombres Bordeaux* 7 (1995), pp. 255–282 (cit. on p. 2).

[Mum84] D. Mumford. *Tata lectures on theta II*. Vol. 43. Progress in Mathematics. Birkhäuser, 1984 (cit. on p. 6).

[Nag83] 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. 7–9).

[NSV11] 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. 21, 27).

[Res74] 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 p. 11).

[Rob13] 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. 28).

[Rob15] D. Robert. "Isogenies, Polarisations and Real Multiplication". Journées C2 Codage et Cryptographie, La Londe-Les-Maures. Oct. 2015. URL: http://www.normalesup.org/~robert/pro/publications/slides/2015-10-C2-LaLondeLesMaures.pdf (cit. on p. 30).

[RS06] A. Rostovtsev and A. Stolbunov. "Public-key cryptosystem based on isogenies". In: *International Association for Cryptologic Research. Cryptology ePrint Archive* (2006). eprint: http://eprint.iacr.org/2006/145 (cit. on p. 2).

[Run99] 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. 12, 16).

[Sch95] R. Schoof. "Counting points on elliptic curves over finite fields". In: *J. Théor. Nombres Bordeaux* 7.1 (1995), pp. 219–254 (cit. on p. 2).

[Ser70] J.-P. Serre. "Le Probleme des Groupes de Congruence Pour SL_2". In: *Annals of Mathematics* 92.3 (1970), pp. 489–527. ISSN: 0003486X. URL: http://www.jstor.org/stable/1970630 (cit. on p. 14).

[Sma03] 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. 2).

[Smi09] B. Smith. *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves*. Feb. 2009. arXiv: 0806.2995 (cit. on p. 2).

[Str10] M. Streng. "Complex multiplication of abelian surfaces". PhD thesis. Universiteit Leiden, 2010 (cit. on p. 6).

[Sut11] A. Sutherland. "Computing Hilbert class polynomials with the Chinese remainder theorem". In: *Mathematics of Computation* 80.273 (2011), pp. 501–538 (cit. on p. 2).

[Tat66] J. Tate. "Endomorphisms of Abelian Varieties over Finite Fields". In: *Inventiones mathematicae* 2 (1966), pp. 133–144 (cit. on p. 44).

[Tes06] E. Teske. "An elliptic curve trapdoor system". In: *Journal of cryptology* 19.1 (2006), pp. 115–133 (cit. on p. 2).

[Van82] G. Van der Geer. "On the geometry of a Siegel modular threefold". In: *Math. Ann.* 260.3 (1982), pp. 317–350 (cit. on p. 13).

[Van12] G. Van Der Geer. *Hilbert modular surfaces*. Vol. 16. Springer Science & Business Media, 2012 (cit. on pp. 7, 18).

[Wen03] A. Weng. "Constructing hyperelliptic curves of genus 2 suitable for cryptography". In: *Mathematics of Computation* 72.241 (2003), pp. 435–458 (cit. on p. 6).