Modular polynomials on Hilbert surfaces
Enea Milio, Damien Robert

To cite this version:
Enea Milio, Damien Robert. Modular polynomials on Hilbert surfaces. Journal of Number Theory, 2020, 10.1016/j.jnt.2020.04.014. hal-01520262v3

HAL Id: hal-01520262
https://hal.science/hal-01520262v3
Submitted on 9 Jan 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Modular polynomials on Hilbert surfaces

Enea Milio, Damien Robert

Contents

1 Introduction .......................................................... 3
  1.1 Context .................................................................. 3
  1.2 Results .................................................................. 4
  1.3 Outline .................................................................. 6

2 Hilbert and Siegel modular spaces .................................. 6
  2.1 Siegel modular space ............................................. 6
  2.2 Hilbert modular space ............................................ 8
  2.3 From Hilbert to Siegel .......................................... 9
  2.4 Humbert surfaces ................................................ 10
  2.5 Symmetric and non symmetric covers of the Humbert surface .. 12

3 Equations for Hilbert surfaces ..................................... 14
  3.1 Generators of the field of Hilbert modular functions ......... 14
  3.2 Fast evaluation of Hilbert modular functions ............... 15
  3.3 Interpolation by Hilbert modular functions ................. 17
  3.4 Equations for covers of Hilbert surfaces .................... 19

4 Modular polynomials .................................................. 21
  4.1 Isogenies preserving real multiplication ..................... 21
  4.2 Modular functions for $\beta$-isogenies ....................... 24
  4.3 Computing modular polynomials .............................. 26

5 Results ........................................................................ 28
  5.1 Case $D = 2$ ......................................................... 29
  5.2 Case $D = 5$ ......................................................... 30
  5.3 Examples of isogenous curves .................................. 31

A Exemple of invariants on Hilbert and Humbert surfaces .... 38
  A.1 Pullback of Siegel invariants ................................. 38
  A.2 Gundlach invariants for $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ .. 38
  A.3 Gundlach and pullbacks of the Igusa invariants .......... 41
  A.4 Other invariants .................................................. 42
  A.5 Components of Humbert surfaces of level 2 and $(2,4)$ .... 43
B Examples of Hilbert modular polynomials 45
   B.1 Modular polynomials in Gundlach invariants ....................... 45
   B.2 Modular polynomials in theta invariants ......................... 48
Abstract

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

1 Introduction

1.1 Context

Isogenies play an important role in elliptic curve cryptography. They allow to transfer the discrete logarithm problem from one curve to a possibly weaker one [24, 65]; they are used by the Schoof–Elkies–Atkin (SEA) point counting algorithm [62, 52, 17], but also by the CRT algorithms to compute class polynomials [67, 20] and modular polynomials [7]. Splitting the multiplication using isogenies can improve the efficiency of the arithmetic [13, 27], taking isogenies to mask the points reduces the impact of side channel attacks [64], and isogenies are used to construct normal basis of a finite field [11]. They have also been used to construct hash functions [10] and to build cryptosystems [69, 60], in particular quantum-resistant cryptosystems [12].

In dimension 1, the $\ell$-modular polynomials $\phi_\ell$ parametrize pairs of elliptic curves $E_1$ and $E_2$ that are $\ell$-isogenous over the algebraic closure. They can be computed in quasi-linear time [19] 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 $\ell$-isogenous whenever $\phi_\ell(j(E_1), j(E_2)) = 0$. Other modular invariants have been proposed which yield smaller polynomials [22].

Principally polarized complex abelian surfaces (which are generically Jacobians of hyperelliptic curves) are parametrized by the Siegel threefold $\text{Sp}_{2g}(\mathbb{Z})/\mathcal{H}_g$ (with $g = 2$) where $\mathcal{H}_g$ 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 projective space, and is parametrized by the three Igusa invariants [37, 38]. One can then generalize modular polynomials to this setting: the $\ell$-modular polynomials classify pairs of principally polarized abelian surfaces $(A, B)$ which admit an $\ell$-isogeny $A \to B$. More precisely the $\ell$-modular polynomials evaluated on the three Igusa invariants of $A$ describe a dimension 0 subvariety of the Siegel threefold of degree $\ell^3 + \ell^2 + \ell + 1$ whose geometric points correspond to the triples of Igusa invariants of the $\ell$-isogenous abelian surfaces $B$. Alternatively, these modular polynomials describe the image of $X_0(\ell)$ inside $X_0(1) \times X_0(1)$ where $X_0(\ell) = \Gamma^0(\ell)/\mathcal{H}_g$ and $\Gamma^0(\ell) = \{ (a \ b) \in \text{SL}_2(\mathbb{Z}) : \ell | b \}$. These polynomials have been studied in [26, 5] and computed for $\ell = 2$ in [16]. Generalizations of these modular polynomials using smaller Siegel modular invariants have more recently been computed in [51].

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 29 GB 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 $\ell$-isogenies does not allow one to explore the full isogeny graph of principally polarized abelian surfaces. In the CRT method to compute class polynomials, one key step of the algorithm is to take an abelian surface in the right isogeny graph, and then use isogenies to find an abelian surface with maximal complex multiplication [6, 47]. But this is not always possible using only $\ell$-isogenies [8, Theorem 9.4].

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

Let $O_K$ be a maximal real quadratic order of discriminant $\Delta_K$. The Hilbert moduli space is a surface parametrizing isomorphism classes of principally polarized abelian surfaces $A$ together with an embedding $O_K \to \text{End}^+(A)$. Let $\beta \in O_K$ be a totally positive element of norm $\ell$. In this article, we define $\beta$-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 [16, 51] for the computation of $\ell$-modular polynomials.

1.2 Results

We study several parametrizations of the Humbert surfaces. The Siegel moduli threefold is parametrized by the three Igusa functions, and in [51] 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.

For the modular polynomial computations, we need an algorithm for the evaluation step and one for the interpolation step. The first algorithm computes, given a period matrix $\tau \in \mathcal{H}_g^1$, the above invariants at some precision $N$ in quasi-linear time in the precision $N$. The second one, given the value of the above invariants, computes a corresponding period matrix $\tau \in \mathcal{H}_g^2$ in time quasi-linear in the requested precision. Instead of doing computation on Humbert surfaces, our idea is to translate back and forth between the Hilbert moduli space and the Siegel moduli space where in the latter space both algorithms have been developed by Dupont in [16]. The translations is based on the work of Igusa [37, 38], Gundlach [31, 32], Resnikoff
In the case of Humbert surfaces of discriminant 5, we have inverted the formulas of [46, Proposition 4.5] expressing the pullback of the Igusa invariants in function of the Gundlach invariants (see Appendix B.1). In the case of Humbert surfaces of discriminant 8, we link in Theorem A.14 and Corollary A.15 the Gundlach invariants with the pullback of the Igusa invariants, as was done by Resnikoff for discriminant 5. These algorithms are described in Section 3.2 (see also Theorem 3.4).

The main result of the paper is the computation of modular polynomials on the Hilbert (or Humbert) surface. When \( \beta \in O_K \) is a totally positive prime, we define \( \beta \)-isogenies and \( \beta \)-modular polynomials in Section 4.1. There are two cases:

- If the norm of \( \beta \) is a prime number \( \ell \), then the \( \beta \)-isogenies correspond to isogenies with cyclic kernel \( V \subset A[\beta] \subset A[\ell] \). All \( \beta \)-isogenies then preserve real multiplication and the \( \beta \)-modular polynomials parametrize all pairs of principally polarized abelian surfaces with maximal real multiplication and admitting a cyclic isogeny of degree \( \ell \);

- Otherwise \( \beta \) is an inert prime number \( \ell \in \mathbb{Z} \). In this case the \( \ell \)-modular polynomials (on the Hilbert moduli space) parametrize \( \ell \)-isogenies between abelian surfaces with maximal real multiplication. By contrast to the Siegel \( \ell \)-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 \( \ell \)-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 \( \beta \)-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 3.11 which gives an evaluation/interpolation algorithm to compute covers of Hilbert surfaces. Adapting this Theorem to the cover parametrizing \( \beta \)-isogenies then yields Theorem 4.15.

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

Finally Martindale and Streng [50] 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 [16]). In particular our algorithm can not be extended to higher dimension as long as the work of Dupont on the generalization of the AGM is not extended to dimension greater than 2. Work in this direction has been done by Labrande and Thomé in [42, 44]. However in dimension 2, we do obtain a quasi-linear algorithm, while there is no complexity analysis in [50], and our algorithm...
is practical since we have computed large polynomials. Our main limitation was the intrinsic
size of the modular polynomials (see Tables 1,2,3) and not the speed of the computations.

1.3 Outline

The remainder of this article is organized as follows. In Section 2, we define the Siegel (in
Section 2.1) and the Hilbert spaces (in Section 2.2) and describe the corresponding moduli
data. We also give generators for the fields of modular functions on these spaces. Then in
Section 2.3, we analyze the forgetful map from the Hilbert modular surface to the Siegel space.
In Section 2.4, we focus on the Humbert surfaces. An Humbert surface is the image of a given
Hilbert modular surface by previous map. We conclude this Section by looking at covers of an
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 works even when we have relations between our invariants. Lastly we conclude
the Section by giving in Section 3.4 an algorithm to compute covers of Hilbert surface.

Section 4 is concerned with modular polynomials on Hilbert surfaces. First in Section 4.1,
we define the isogenies preserving real multiplication. In Section 4.3, we define the modu-
lar 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. See also Appendix B,
where we apply the results of the previous sections on Gundlach invariants and pullbacks of
the theta functions.

Thanks  We thank Pierre-Jean Spaenlehauer to have succesfully computed the Gröbner basis
expressing the Gundlach invariants in term of the Igusa invariants for $D = 2$. We thank David
Kohel who suggested us to look at the work of Elkies and Kumar [18] to get invariants for
more Humbert or Hilbert surfaces (see Appendix A.4). We thank the anonymous reviewer for
his careful reading and his many comments and suggestions.

2  Hilbert and Siegel modular spaces

2.1 Siegel modular space

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

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

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

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

$$\theta[a/b] (\Omega) = \sum_{n \in \mathbb{Z}^g} \exp(i \pi \langle n + a \Omega(n + a) + 2i \pi \langle n + a \rangle b).$$

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

$$\theta_{a_0+2b_1+4a_0+8a_1}(\Omega) := \theta[a/2] (\Omega).$$

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 $\text{Sp}_4(\mathbb{Z})$

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

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

(see for example [39, Page 848], [16, Section 6.3.3] or [66, Section 7.1] for the exact definition).

We define the Siegel Eisenstein series $\psi_k$ 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 \(\begin{pmatrix} A & B \\ C & D \end{pmatrix}\) in $\text{Sp}_4(\mathbb{Z})$ up to left multiplication by $\text{SL}_2(\mathbb{Z})$. Let

$$\chi_{10} = -2^{-12}3^{-5}5^{-2}7^{-1}13^{-1}43867(\psi_4 \psi_6 - \psi_{10})$$

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 by Igusa [39, Page 848] that $\psi_4 = 2^{-2}h_4$, $\psi_6 = 2^{-2}h_6$, $\chi_{10} = 2^{-14}h_{10}$ and $\chi_{12} = 2^{-17}3^{-1}h_{12}$. The graded ring of holomorphic Siegel modular forms for $\text{Sp}_4(\mathbb{Z})$ is the polynomial ring of $\psi_4$, $\psi_6$, $\chi_{10}$ and $\chi_{12}$. We define the Igusa invariants from these last modular forms:

\begin{equation}
(1) \quad j_1 = 2 \cdot 3^5 \frac{\chi_{12}^7}{\chi_{10}^3}, \quad j_2 = 2^{-3}3^3 \frac{\psi_4 \chi_{12}^3}{\chi_{10}^4} \quad \text{and} \quad j_3 = 2^{-5}3 \left( \frac{\psi_6 \chi_{12}^7}{\chi_{10}^3} + 2 \cdot 3 \cdot 2 \chi_{12} \right).
\end{equation}

The field of Siegel modular functions for $\text{Sp}_4(\mathbb{Z})$ is $\mathbb{C}(j_1, j_2, j_3)$. Generically, two principally polarized abelian surfaces are isomorphic if and only if they have the same three Igusa invariants. (In [37, 38], Igusa has defined 10 absolute invariants, which allows to characterize all abelian surfaces up to isomorphisms over the algebraic closure of the base field.)

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

\begin{equation}
(2) \quad r_1 = \frac{\theta_1^6 \theta_2^9}{\theta_3^4 \theta_4^4}, \quad r_2 = \frac{\theta_1^6 \theta_2^9}{\theta_3^4 \theta_4^4} \quad \text{and} \quad r_3 = \frac{\theta_1^6 \theta_2^9}{\theta_3^4 \theta_4^4}
\end{equation}
are Siegel modular functions for $\Gamma(2)$ called the Rosenhain invariants. They are generators for the field of modular functions belonging to $\Gamma(2)$ (see Mumford [55, Section 8]).

Let $\Gamma(2, 4) = \{(\frac{\alpha}{\beta}, \frac{\gamma}{\delta}) \in \text{Sp}_4(\mathbb{Z}) : (\frac{\alpha}{\beta}, \frac{\gamma}{\delta}) \equiv I_4 \text{ mod } 2 \text{ and } B_0 \equiv C_0 \equiv 0 \text{ mod } 4\}$, where $X_0$ denotes the vector composed of the diagonals elements of $X$. It is a normal subgroup of $\text{Sp}_4(\mathbb{Z})$ 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 Manni [49, Theorem 1]).

### 2.2 Hilbert modular space

We refer to [71, 9, 29, 23, 56] for more details on Hilbert modular forms and Hilbert surfaces.

Let $D > 0$ be a square-free integer and $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field. Its discriminant $\Delta_K$ is $D$ if $D \equiv 1$ mod 4 and $4D$ if $D \equiv 2, 3$ mod 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 $D \equiv 1$ mod 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 $\alpha + \beta\sqrt{D} = a - \beta\sqrt{D}$.

The set $\mathcal{H}^+_1 = \{z \in \mathbb{C} : \Re(z) > 0\}$ 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 $\text{SL}_2(\mathcal{O}_K)$ acts on the left on $\mathcal{H}^+_1 \times \mathcal{H}^-_1$ by $(\frac{a}{c}, \frac{b}{d}) \cdot (\tau_1, \tau_2) = (\frac{a \tau_1 + b}{c \tau_1 + d}, \frac{a \tau_2 + b}{c \tau_2 + d})$. The Baily-Borel compactification of the quotient space $\text{SL}_2(\mathcal{O}_K) \backslash \mathcal{H}^+_1 \times \mathcal{H}^-_1$ is the Hilbert modular surface (see for example [71, Section 7]). It parametrizes principally polarized abelian surfaces $(A, \theta)$ with real multiplication by the maximal order $\mathcal{O}_K$, with an explicit embedding $\mu : \mathcal{O}_K \to \text{End}(A)$ (see [3, Chapter 9]).

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

We have group isomorphisms

$$\phi_\pm : \text{SL}_2(\mathcal{O}_K) \to \text{SL}_2(\mathcal{O}_K \oplus \partial_K), \quad (\frac{a}{c}, \frac{b}{d}) \mapsto (\frac{a}{c \sqrt{\Delta_K}}, \frac{b}{d})$$

and the following diagram is commutative

$$\text{SL}_2(\mathcal{O}_K) \times \mathcal{H}^+_1 \times \mathcal{H}^-_1$$

$$\downarrow$$

$$\text{SL}_2(\mathcal{O}_K \oplus \partial_K) \times \mathcal{H}^+_1 \times \mathcal{H}^-_1$$

$$\downarrow$$

$$\mathcal{H}^+_1 \times \mathcal{H}^-_1$$

(see [18, Section 3]). If $\tau = (\tau_1, \tau_2) \in \mathcal{H}^+_1$, the corresponding abelian surface is given by the torus $\mathbb{C}^2/(\Phi(\mathcal{O}_K) \oplus (\tau_1 \tau_2 \Phi(\partial_K^{-1}))$ 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: $E(x_1 + x_2 \tau, y_1 + y_2 \tau) = \text{tr}_{K/\mathbb{Q}}(x_1 y_2 - x_2 y_1)$. From the definition of $\partial_K^{-1}$ we get indeed that $E$ induces a principal polarization.

Since $\text{SL}_2(\mathcal{O}_K)$ is generated by the matrices $(\frac{1}{1}, \frac{1}{1})$, $(\frac{0}{1}, \frac{1}{1})$, $(\frac{1}{1}, -\frac{1}{1})$, the group $\text{SL}_2(\mathcal{O}_K \oplus \partial_K)$ is generated by the matrices $(\frac{1}{1/\sqrt{\Delta_K}}, \frac{1}{\omega/\sqrt{\Delta_K}})$ and $(\frac{0}{\sqrt{\Delta_K}^{-1}/\sqrt{\Delta_K}}, \frac{0}{0})$. \[8\]
For $\lambda \in K$ and $\tau = (\tau_1, \tau_2) \in H^2_1$, we denote
\[
\lambda \tau = (\lambda \tau_1, \lambda \tau_2), \quad N(\tau) = \tau_1 \tau_2 \quad \text{and} \quad \text{tr}(\tau) = \tau_1 + \tau_2.
\]

We define $\sigma$ to be the involution $\sigma : (\tau_1, \tau_2) \in H^2_1 \mapsto (\tau_2, \tau_1) \in H^2_1$. We let $\sigma$ act by conjugation on $SL_2(O_K + \partial_K)$ via $\sigma \cdot \gamma = \left( \frac{1}{\gamma_0} \right) \gamma \left( \frac{1}{\gamma_0} \right) \in SL_2(O_K + \partial_K)$, for $\gamma = \left( \frac{a \ b}{c \ d} \right) \in SL_2(O_K + \partial_K)$. It is straightforward to check that this is compatible with the action on $H_1^2$. We call the group $SL_2(O_K + \partial_K) \rtimes \langle \sigma \rangle$ the symmetric Hilbert modular group. For a function $f : H_1^2 \to \mathbb{C}$ and $\gamma \in SL_2(O_K + \partial_K) \rtimes \langle \sigma \rangle$ we denote $f^\gamma(\tau) = f(\gamma \tau)$.

**Definition 2.1.** Let $\Gamma$ be a subgroup of $SL_2(K)$ commensurable with $SL_2(O_K)$. A holomorphic function $f$ on $H_1^2$ is called a Hilbert modular form of weight $k$ for the subgroup $\Gamma$ if it satisfies for any $\gamma = \left( \frac{a \ b}{c \ d} \right) \in \Gamma$ and $\tau = (\tau_1, \tau_2) \in H^2_1$ the condition $f(\gamma \tau) = N(c \tau + d)^k f(\tau)$. If moreover it satisfies $f(\sigma(\tau)) = f(\tau)$ for all $\tau \in H^2_1$, 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, for some choice of forms.

**Remark 2.2.** A modular form $f$ is then automatically holomorphic at the set of cusps $SL_2(O_K) \setminus \mathbb{P}^1(K) \simeq \text{Cl}(O_K)$ (see for example [9, Section 1.3] for more details).

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

### 2.3 From Hilbert to Siegel

Let $\tau = (\tau_1, \tau_2) \in H^2_1$, $x \in K$ and $\gamma = \left( \frac{a \ b}{c \ d} \right) \in SL_2(K)$. We denote $\tau^x = \left( \begin{smallmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{smallmatrix} \right)$, $x^* = \left( \begin{smallmatrix} x & 0 \\ 0 & 1/x \end{smallmatrix} \right)$ and $\gamma^* = \left( \begin{smallmatrix} a^* & b^* \\ c^* & d^* \end{smallmatrix} \right)$. Fix $\{e_1, e_2\}$ a $\mathbb{Z}$-basis of $O_K = \mathbb{Z} + \omega \mathbb{Z}$ ($\omega$ is defined in the beginning of the previous section) and define the matrices $R = \left( \begin{smallmatrix} e_1 & e_2 \\ \tau_1 & \tau_2 \end{smallmatrix} \right)$ and $S = \left( \begin{smallmatrix} i \tau & 0 \\ 0 & R^{-1} \end{smallmatrix} \right)$ and the maps
\[
\phi_{e_1,e_2} : H^2_1 \to H_2 \quad \text{and} \quad \phi_{e_1,e_2} : SL_2(K) \to \text{Sp}_4(\mathbb{Q})
\]
\[
\tau \mapsto [R \tau^x R] \quad \text{and} \quad \gamma \mapsto Sp_4(\mathbb{Q})
\]
\[
(6)
\]
Recall that $SL_2(O_K + \partial_K) = \{ \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in SL_2(K) : a, d \in O_K, b \in 1/\sqrt{\Delta_K} O_K$ and $c \in \sqrt{\Delta_K} O_K$.

**Proposition 2.3.** The map $\phi_{e_1,e_2}$ satisfies:

- $\phi_{e_1,e_2}^1(Sp_4(\mathbb{Z})) = SL_2(O_K + \partial_K)$;
- $\phi_{e_1,e_2}(\gamma \cdot \tau) = \phi_{e_1,e_2}(\gamma) \cdot \phi_{e_1,e_2}(\tau)$ for all $\gamma \in SL_2(O_K + \partial_K)$ and $\tau \in H^2_1$;
- If $f_1, f_2$ is another $\mathbb{Z}$-basis of $O_K$, then there exists some $\gamma \in Sp_4(\mathbb{Z})$ such that for all $\tau \in H^2_1$, $\phi_{e_1,e_2}(\tau) = \gamma \cdot \phi_{f_1,f_2}(\tau)$;
- 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 $M_\sigma$ this $\gamma$, and this allows us to extend $\phi_{e_1,e_2}$ to $SL_2(O_K + \partial_K) \rtimes \langle \sigma \rangle$.

**Proof.** See for example [46, Proposition 3.1]. For the convenience of the reader, we give more details on the key part of the proof in the reference above. Let $A = C^2/(\Phi(\partial_K) + \tau^* \Phi(O_K))$ be the abelian surface corresponding to $\tau$. Then $\Phi(O_K) = RZ^2$ and if $(f_1, f_2)$ denotes the dual basis with respect to the trace of $(e_1, e_2)$, then $\Phi(\partial_K) = R^\vee Z^2$ with $R^\vee = \left( \begin{smallmatrix} f_1 \\ f_2 \end{smallmatrix} \right)$. The lattice $\Phi(\partial_K) \oplus \tau^* \Phi(O_K) = R^\vee Z^2 \oplus \tau^* RZ^2$ is isomorphic to $Z^2 \oplus R^\vee -1 \tau^* \tau RZ^2$ via the change of variable $z \mapsto R^\vee -1 z$. But an easy computation shows that $iR R^\vee = 1$ so $R^\vee -1 = iR$. \qed
Thus, the map $\phi_{e_1,e_2}$ gives a holomorphic map from $\text{SL}_2(\mathcal{O}_K \oplus \partial_K) \backslash \mathcal{H}_1^2$ to $\text{Sp}_4(\mathbb{Z}) \backslash \mathcal{H}_2$ which is independent of the choice of the basis of $\mathcal{O}_K$. It also sends $\tau$ and $\sigma(\tau)$ to the same point of $\text{Sp}_4(\mathbb{Z}) \backslash \mathcal{H}_2$. Since $\phi_{e_1,e_2}$ allows us to identify $\text{SL}_2(\mathcal{O}_K \oplus \partial_K)$ and $\langle \sigma \rangle$ as subgroups of $\text{Sp}_4(\mathbb{Z})$, we will note $\text{SL}_2(\mathcal{O}_K \oplus \partial_K) \cup \text{SL}_2(\mathcal{O}_K \oplus \partial_K)\sigma$ the group $\text{SL}_2(\mathcal{O}_K \oplus \partial_K) \times \langle \sigma \rangle$.

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

$$\begin{align*}
\frac{D-1}{4} \Omega_1 + \Omega_2 - \Omega_3 &= 0, \quad \text{if } D \equiv 1 \mod 4; \\
D \Omega_1 - \Omega_3 &= 0, \quad \text{if } D \equiv 2, 3 \mod 4.
\end{align*}$$

Moreover, set

$$M_\sigma = \left\{ \begin{array}{ll}
\left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1 \end{array}\right) & \text{if } D \equiv 1 \mod 4; \\
\left(\begin{array}{cccc}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1 \end{array}\right) & \text{if } D \equiv 2, 3 \mod 4.
\end{array}\right.$$\hfill(8)

We have found that the matrix $M_\sigma$ satisfies

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

Consider now $\gamma = \left(\begin{array}{c} \frac{a+a'\omega}{\sqrt{\Delta_K(e+c')\omega}} \\
\frac{b+b'\omega}{\sqrt{\Delta_K}} \end{array}\right) \in \text{SL}_2(\mathcal{O}_K \oplus \partial_K)$. Then

$$\phi_{1,\omega}(\gamma) = \left\{ \begin{array}{ll}
\left(\begin{array}{c} a \\
\frac{(\frac{D+1}{2})a'}{\sqrt{\Delta_K}} \\
b \\
\frac{(\frac{D+1}{2})b'}{\sqrt{\Delta_K}} \end{array}\right) & \text{if } D \equiv 1 \mod 4; \\
\left(\begin{array}{c} a \\
\frac{(D-1)c'-c}{\sqrt{\Delta_K}} \\
b \\
\frac{(D-1)d'-d}{\sqrt{\Delta_K}} \end{array}\right) & \text{if } D \equiv 2, 3 \mod 4.
\end{array}\right.$$\hfill(10)

### 2.4 Humbert surfaces

Humbert surfaces have been first studied by Humbert in [34, 35, 36]. Let $\Omega = \left(\begin{array}{cc} \Omega_1 & \Omega_2 \\
\Omega_2 & \Omega_3 \end{array}\right) \in \mathcal{H}_2$ and $a, b, c, d, e \in \mathbb{Z}$. We can equation the form:

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

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

**Theorem 2.4** (Humbert’s Lemma). Let $\Omega = \left(\begin{array}{cc} \Omega_1 & \Omega_2 \\
\Omega_2 & \Omega_3 \end{array}\right)$ 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 $\gamma \in \text{Sp}_4(\mathbb{Z})$ such that $\gamma \cdot \Omega = \left(\begin{array}{cc} \Omega'_1 & \Omega'_2 \\
\Omega'_2 & \Omega'_3 \end{array}\right)$ satisfies a normalized singular relation of the form:

$$k\Omega'_1 + \ell\Omega'_2 - \Omega'_3 = 0$$

where $k$ and $\ell$ are determined uniquely by $\Delta = 4k + \ell$ and $\ell \in \{0, 1\}$.
Proof. See [34, 35, 36] or for example Birkenhake-Wilhelm [4, Proposition 4.5] or Runge [61, Theorem 2].

Remark 2.5. Let $\Omega \in \mathcal{H}_2$. It can satisfy many singular relations of different discriminants. If it satisfies a singular relation of discriminant $\Delta$, a constructive algorithm to find $\gamma$ as in Humbert’s Lemma can be found in [4, 61]. Conversely, let $\Omega \in \mathcal{H}_2$ be a matrix equivalent to a matrix satisfying (11). Then $\Omega$ satisfy necessarily a singular relation of discriminant $\Delta$. By (7)

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

Proof. See [4, Corollary 4.6 and Proposition 4.7] or [30, Proposition 2.11].

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

- $A_\Omega$ is simple if and only if $\Omega \notin \bigcup_{m>0} H_m$;
- If $\Omega \in H_\Delta$, then $\text{End}(A_\Omega)$ contains the maximal order of $\mathbb{Q}(\sqrt{\Delta})$, i.e., equivalently, there exists a symmetric endomorphism of discriminant $\Delta$ on $A_\Omega$;
- if $\Omega \in H_\Delta \cap H_{\Delta'}$, then either $A_\Omega$ is simple and $\text{End}(A_\Omega) \otimes \mathbb{Q}$ is a totally indefinite quaternion algebra over $\mathbb{Q}$, or $A_\Omega$ is isogenous to $E \times E$, where $E$ is an elliptic curve.

Proof. See [4, Proposition 4.9] or [30, Corollary 2.10, Proposition 2.15].

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

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

\[
\begin{array}{ccc}
\tilde{\Gamma}(1) \setminus \mathcal{H}^1_1 & \xrightarrow{\phi_{e_1,e_2}} & \mathcal{H}_2 \\
\downarrow_{\pi} & & \downarrow \rho \\
(\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma) \setminus \mathcal{H}^1_1 & \xrightarrow{\rho} & \text{Sp}_4(\mathbb{Z})/\mathcal{H}_2
\end{array}
\]

where $\pi$ is a map of degree 2 and $\rho$ is a map generically of degree 1 onto the Humbert surface $H_{\Delta_K}$.

Proof. See Van der Geer [70, Page 328] for the map $\rho$ and the commutativity of the rectangular part of the diagram. The fact that $\pi$ is of degree 2 is obvious. It remains to see that $\rho \circ \pi$ is generically of degree 2. But $H_{\Delta_K}$ is the locus of principally polarized abelian surfaces $(A,\theta)$ with real multiplication by $\mathcal{O}_K$, and the preimages correspond to explicit embeddings $\mu : \mathcal{O}_K \to \text{End}(A)$. Generically there are only two such embeddings which differ by the real conjugation, which corresponds to the action of $\sigma$. 

11
The analytic quotient space \((\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma) \backslash \mathcal{H}_1^2\) is called a symmetric Hilbert modular surface; it is birational to the Humbert surface.

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

**Proof.** This is a well-known result. We give the proof in Appendix A.1. \(\square\)

### 2.5 Symmetric and non symmetric covers of the Humbert surface

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

When \(\Gamma = \text{SL}_2(\mathbb{Z})\), 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 \(\text{SL}_2(\mathcal{O}_K)\) acting on \(\mathcal{H}^+ \times \mathcal{H}^-\) and then transport them to the model of \(\text{SL}_2(\mathcal{O}_K \oplus \partial K)\) action on \(\mathcal{H}^2\) via the automorphism \(\phi_{\pm}\) of Equation (4).

**Definition 2.10.** Let

\[(12) \quad \tilde{\Gamma}(n) = \left\{ \begin{array}{l} \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \text{SL}_2(\mathcal{O}_K) : a \equiv d \equiv 1 \pmod{n}, b \equiv c \equiv 0 \pmod{n} \end{array} \right\}. \]

Define then for \(D \equiv 1 \pmod{4}\) and \(D \equiv 2, 3 \pmod{4}\)

\[(13) \quad \tilde{\Gamma}(2, 4) = \left\{ \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \tilde{\Gamma}(2) : b \equiv c \equiv 0 \pmod{4} \right\}, \]

\[(14) \quad \tilde{\Gamma}(2, 4) = \left\{ \left( \begin{array}{cc} a & (b_1 + b_2\omega) \\ c_1 + c_2\omega & d \end{array} \right) \in \tilde{\Gamma}(2) : b_2 \equiv c_2 \equiv 0 \pmod{4} \right\} \]

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

**Remark 2.11.** By Serre [63] a group \(\tilde{\Gamma}\) of finite index in \(\text{SL}_2(\mathcal{O}_K \oplus \partial K)\) is necessarily a congruence subgroup, meaning that it contains the congruence subgroup \(\tilde{\Gamma}(n)\) for some positive integer \(n\).
Lemma 2.12. Let \( \mathcal{G} \) be a subgroup of \( SL_2(O_K \oplus \partial_K) \rtimes \langle \sigma \rangle \) of finite index. If \( \sigma \notin \mathcal{G} \) then \( \mathcal{G} \subset SL_2(O_K \oplus \partial_K) \). Otherwise \( \mathcal{G} = \tilde{\Gamma} \rtimes \langle \sigma \rangle \) for a subgroup \( \tilde{\Gamma} \subset SL_2(O_K \oplus \partial_K) \) of finite index and normalized by \( \sigma \) (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 \( \tilde{\Gamma} \subset SL_2(O_K \oplus \partial_K) \). It remains to check that \( \sigma \) normalizes \( \tilde{\Gamma} \). But since \( \mathcal{G} \) is a group, \( \tilde{\Gamma} = \sigma \tilde{\Gamma} \sigma^{-1} \subset \mathcal{G} \), so \( \tilde{\Gamma} = \tilde{\Gamma} \).

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

Consider now \( \Gamma \) a subgroup of \( Sp_4(Z) \) of finite index. The projection \( \pi : \Gamma \backslash H_2 \to Sp_4(Z) \backslash H_2 \) is a finite map. Recall that if \( \Delta_K \) is the discriminant of \( O_K \), we denote by \( H_{\Delta_K} \) the Humbert surface of discriminant \( \Delta_K \). An irreducible component of \( H_{\Delta_K}^{\Gamma} = \pi^{-1}(H_{\Delta_K}) \) in \( \Gamma \backslash H_2 \) is called a Humbert surface component.

Let \( \mathcal{G} = \phi_{1,0}^{-1}(\Gamma) \) and \( \tilde{\mathcal{G}} = \mathcal{G} \cap SL_2(O_K \oplus \partial_K) \). If the matrix \( M_\sigma \) of Equation (8) is not in \( \Gamma \), then \( \mathcal{G} = \tilde{\mathcal{G}} \), otherwise \( \mathcal{G} = \tilde{\mathcal{G}} \cup \tilde{\mathcal{G}} \sigma \). By Proposition 2.8 we get that the following diagram is commutative:

\[
\begin{array}{ccc}
H_1^2 & \phi_{1,0} & H_2 \\
\downarrow & & \downarrow \\
\mathcal{G} \backslash H_1^2 & \rho & \Gamma \backslash H_2
\end{array}
\]

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

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

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

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

We have seen that by Lemma 2.9 we can take \( \tilde{i}_k = \phi_{1,0}^* i_k \), for \( k = 1, 2, 3 \), as invariants on a symmetric Hilbert modular surface. These functions are algebraically dependent. Similarly, we will apply Proposition 2.15 to the functions \( \tilde{b}_k = \phi_{1,0}^* b_k \) and \( \tilde{r}_k = \phi_{1,0}^* r_k \) for \( k = 1, 2, 3 \). Recall Equations (1), (2) and (3) for the definitions of these invariants.

Theorem 2.16. The functions \( \tilde{r}_k \) and \( \tilde{b}_k \) for \( k = 1, 2, 3 \) are generators for the field of Hilbert modular functions invariants by \( \tilde{\Gamma}(2) \) and \( \tilde{\Gamma}(2, 4) \), if \( D \equiv 1 \mod 4 \), and by \( \tilde{\Gamma}(2) \cup \tilde{\Gamma}(2)\sigma \) and \( \tilde{\Gamma}(2, 4) \cup \tilde{\Gamma}(2, 4)\sigma \), if \( D \equiv 2, 3 \mod 4 \), respectively.
Proof. By Equation (10), we have that \( \phi_{1,\omega}^{-1}(\Gamma(2,4)) \cap \text{SL}_2(\mathcal{O}_K \oplus \partial_K) = \hat{\Gamma}(2,4) \). Thus, the functions \( b_k \) are modular for \( \hat{\Gamma}(2,4) \). Moreover, if \( D \equiv 2,3 \mod 4 \), then these functions are also modular for \( \hat{\Gamma}(2,4)\sigma \), as the matrix \( M_\sigma \) of Equation (8) belongs to \( \Gamma(2,4) \). Similarly, \( \phi_{1,\omega}^{-1}(\Gamma(2)) \cap \text{SL}_2(\mathcal{O}_K \oplus \partial_K) = \hat{\Gamma}(2) \) and the \( r_k \) are modular for \( \hat{\Gamma}(2) \) and also by \( \hat{\Gamma}(2)\sigma \) when \( D \equiv 2,3 \mod 4 \). We conclude using Proposition 2.15 and the fact that the \( b_i \) (resp. \( r_i \)) are generators for the field of Siegel modular functions invariants by \( \Gamma(2,4) \) (resp. \( \Gamma(2) \)). The pullbacks are indeed well defined because the denominators of these invariants divide \( \chi_{10} \), so the locus of the denominators are components above the Humbert surface \( H_1 \). \( \square \)

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

3 Equations for Hilbert surfaces

3.1 Generators of the field of Hilbert modular functions

Let \( \hat{\Gamma} \subset \text{SL}_2(\mathcal{O}_K \oplus \partial_K) \) be a subgroup of finite index. We note \( H_{\hat{\Gamma}} = \hat{\Gamma} \backslash \mathcal{H}_1^2 \) the corresponding Hilbert modular surface, and \( H_{\hat{\Gamma},\sigma} = (\hat{\Gamma} \cup \hat{\Gamma}\sigma) \backslash \mathcal{H}_1^2 \) the corresponding symmetric Hilbert modular surface. We let \( \mathcal{G} = \hat{\Gamma} \) in the first case, and \( \mathcal{G} = \hat{\Gamma} \cup \hat{\Gamma}\sigma \) in the second one. Recall that \( \mathbb{C}_G \) is defined in Definition 2.13.

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

**Proof.** Since \( H_{\mathcal{G}} \) is a surface, the field of Hilbert modular functions \( \mathbb{C}_G \) is of transcendence degree 2. By the primitive element theorem, \( \mathbb{C}_G \) 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 \( \mathbb{C}_G \) is algebraic over \( \mathbb{C}_{\text{SL}_2(\mathcal{O}_K \oplus \partial_K) \cap \text{SL}_2(\mathcal{O}_K \oplus \partial_K)\sigma} \), we can take \( i_1, i_2 \in \mathbb{C}_{\text{SL}_2(\mathcal{O}_K \oplus \partial_K) \cap \text{SL}_2(\mathcal{O}_K \oplus \partial_K)\sigma} \). They are then symmetric, so \( H_{\mathcal{G}} \) is symmetric if and only if \( i_3 \) is symmetric. \( \square \)

Usually working with symmetric Hilbert modular surface yields invariants easier to compute. For instance while \( H_{\hat{\Gamma}(1)} \) is not often a rational surface according to Theorem A.16, from Elkies and Kumar [18] we have that \( H_{\hat{\Gamma}(1),\sigma} \) is a rational surface for every fundamental discriminant \( \Delta_K < 100 \). Hence for these surfaces we need only two birational primary invariants to define the modular polynomials. The drawback of symmetric modular surfaces is that they can not be used for all the applications of isogenies as we will see in Example 4.17.

Note that by the general theory of Shimura varieties \( H_{\mathcal{G}} \) has a (birational) model defined over an algebraic number field \( F \). In fact by Van Der Geer [71, Section X.4], the Hilbert surface can be defined over \( \mathbb{Q} \), and its connected components over an abelian extension of \( \mathbb{Q} \). In particular if the invariants \( i_1, i_2, i_3 \) come from this model defined over \( F \), the equation \( E(i_1, i_2, i_3) = 0 \) can be written as \( E = \sum c_k(i_1, i_2)j_k^3 \), where \( c_k \in F(i_1, i_2) \).

The lemma below show that if the Hilbert invariants have their Fourier coefficients are in a number field \( F \) then they are defined over \( F \). In practice the invariants we use for computation (pullbacks of Igusa invariants, pullbacks of theta functions, Gundlach invariants) even have Fourier coefficients in \( \mathbb{Q} \).
Theorem 3.4. Let \( i_1, \ldots, i_n \) be Hilbert modular functions generating the Hilbert modular field \( \mathbb{C}_e \), and let \( \mathcal{E} \) be the ideal of equations between the \( i_k \) and \( H_\mathcal{E} \) the corresponding birational model of \( H \). 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 over \( F \).

Proof. The proof uses a similar argument of Bröker and Lauter in [5, Theorem 5.2]. If we fix a monomial ordering, the generators of \( \mathcal{E} \) are uniquely determined when they form a Gröbner basis. This Gröbner basis induces a set of linear relations on the Fourier coefficients of the \( i_k \) from which its coefficients (as 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 between the Hilbert functions \( i_k \) as in Lemma 3.2 will lie in a polynomial ring over a proper subfield of \( F \), one needs to look at the Galois action on the Fourier coefficients (which lie in \( F \) by hypothesis).

3.2 Fast evaluation of Hilbert modular functions

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

- For the evaluation, given \( \tau = (\tau_1, \tau_2) \in \mathcal{G} \setminus H_*^2 \) we need to be able to compute the invariants \((i_1(\tau), i_2(\tau), i_3(\tau)) \) in \( \mathbb{C}^3 \) in time quasi-linear in the required precision;

- Given the value of \((i_1(\tau), i_2(\tau), i_3(\tau)) \) in \( \mathbb{C}^3 \) we need to be able to recover the matrix \( \tau \in \mathcal{G} \setminus H_*^2 \) in time quasi-linear in the required precision. This allows us to have well-chosen evaluation points so that we can do the interpolation of trivariate rational fractions.

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

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

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

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

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

Proof. We first do the symmetric case.

By Enge and Thomé in [21, Theorem 5.8, Remark 5.9], given a Siegel matrix $\Omega \in H_2$, evaluating the $b_k(\Omega)$ can be done in time quasi-linear in the precision (see also [16, 42, 44] on this subject), if we neglect the loss of precision. Given a period matrix $\tau \in H_2^1$, one can use the map $\phi_{1,\omega}$ from Section 2.3 to get $\Omega = \phi_{1,\omega}(\tau) \in H_2$, then we compute the values of $b_k(\tau) = b_k(\phi_{1,\omega}(\tau))$ in time quasi-linear, and finally we deduce the values of $i_k(\tau) = R_k(\tilde{b}_1(\tau), \tilde{b}_2(\tau), \tilde{b}_3(\tau))$.

For the inverse, the (restriction of the) Igusa invariants $i_1, i_2, i_3$ can also be expressed as rational functions in the invariants $i_1, i_2, i_3$. From the values $(i_1(\tau), i_2(\tau), i_3(\tau))$, one can then compute $(\tilde{i}_1(\tau), \tilde{i}_2(\tau), \tilde{i}_3(\tau))$. Using [16] (in particular [16, Théorème 9.3] and [16, Pages 200 and 223] of Dupont), we compute in time quasi-linear in $N$ an approximation to precision $N$ of a matrix $\Omega \in H_2$ which is equivalent modulo $Sp_4(\mathbb{Z})$ to $\phi_{1,\omega}(\tau)$. The matrix $\Omega$ lies in the Humbert surface of discriminant $\Delta_K$, so it satisfies a singular relation. By Section 2.4 there is a constructive algorithm to find $\gamma \in Sp_4(\mathbb{Z})$ such that $\gamma.\Omega$ satisfies a normalized singular relation. By Section 2.3, $\gamma.\Omega$ is in the image of $\phi_{1,\omega}$, so one can compute $\tau' = \phi_{1,\omega}^{-1}(\gamma.\Omega) \in H_2^1$. It then only remains to compute all classes of $\tau'$ under the action of the finite group $G/\SL_2(\mathcal{O}_K \oplus \phi_K)$ to find a $\tau''$ in the same class as $\tau$ modulo $G$.

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

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

In practice, it is important to optimize the speed of the computation of the invariants $i_k$ as rational functions of the $b_k$ to be able to do concrete computations. Rather than using linear algebra, one can use an interpolation approach. This approach requires to be able to obtain, from the values $(b_1(\Omega), b_2(\Omega), b_3(\Omega))$, a period matrix $\Omega'$ equivalent to $\Omega$ modulo $\Gamma(2, 4)$, at some given precision. We know how to do it by [51, 16]. It also requires the equation $P(b_1, b_2, b_3) = 0$ of the Humbert component described by the $\tilde{b}_k$. We refer to Section 3.3 for more details about the interpolation.

Likewise, to recover $\tau$, 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 $\Omega$, hence the matrix $\tau$.

Remark 3.6. In the first paragraph of the second page of [44] about the computation of theta functions in genus $g > 1$ in quasi-linear time, Labrande and Thomé explain that they deliberately omit dealing with the precision losses because they expect that the loss of precision
is not significant asymptotically. Indeed, this is what the analysis done by Labrande in genus $g = 1$ in [43] concludes.

### 3.3 Interpolation by Hilbert modular functions

Let $H_G$ be a Hilbert surface defined over $F$ of level $G = \Gamma$ or $G = \Gamma \cup \Gamma_\sigma$, and $c$ a Hilbert modular function in $F(H_G)$. We assume that the invariants $i_1, i_2, i_3$ are such that the map \( \tau \in G/H^2 \rightarrow (i_1(\tau), i_2(\tau), i_3(\tau)) \) can be inverted in time quasi-linear (see Theorem 3.4) at the working precision. We explain how to get a fast interpolation algorithm to express $H$ using only two primary invariants. Thus $\tau \in G\backslash H$ is a Hilbert surface defined over $\mathbb{Q}$.

#### Case where $H_G$ is a rational surface.

In this case, $F(H_G)$ can be written as $F(J_1, J_2)$ using only two primary invariants. Thus $c$ is a bivariate rational function in $J_1$ and $J_2$. The interpolation of $c$ is explained in [51, Section 2], where a complexity analysis is given. We explain it briefly. We compute $c(J_1, J_2)$ by computing first by interpolation $c(J_1, J_1 J_2)$ and then by substituting $J_2$ with $J_2/J_1$. Assume that we can write

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

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

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

#### General case.

Here, we have three invariants $i_1, i_2, i_3$ where $i_1$ and $i_2$ are primary, and $i_3$ is a secondary invariant, so there is an equation $E(i_1, i_2, i_3) = 0$ describing the surface $H_G$. 

17
Like in the previous case and as in [51, Section 2], we would like to work with points $z_j \in \mathcal{H}_1^2$ with the property that $(i_1(z_j), i_2(z_j), i_3(z_j))$ is of the form $(u_m, v_n u_m, v_r u_m)$, 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 $z$ Theorem 3.7. to recover them as rational functions in $\mathbb{Q}(K)$, we first interpolate $c_i$. The interpolation is done as follows. For sufficiently many values $u_m$ and $v_n$, compute the $d$ roots $w_r$ of $E(u_m, v_n u_m, X_3)$. 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 $c$ at $z_r$ to obtain $c(z_r) = \sum_{i=0}^{d-1} c_i(u_m, v_n u_m) w_r^i$. Since $w_r = i_3(z_r)$, we first interpolate $c$ as a univariate polynomial in $i_3$ by interpolating on the $d$ values $w_r$ to recover the $d$ coefficients $c_i(u_m, v_n u_m)$. This allows us to evaluate the bivariate rational functions $c_i(i_1, i_2)$ at a given point $z_r$. It remains to do the interpolation of the coefficients $c_i$ to recover them as rational functions in $i_1, i_2$ as was done in the previous case, where $H_G$ was a rational surface. We summarize this discussion by the following theorem.

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

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

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

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

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

$$O(d_T d_{i_2}) + O(d) \hat{O}(d_T d_{i_2} N) + O(d_T d_{i_2}) \hat{O}(d N) \subset \hat{O}(d_T d_{i_2} N).$$

Given a coefficient $c_k \in \mathbb{C}$ computed at precision $N$, if $c_k$ lie in $F(i_1, i_2)$, where $F \subset \mathbb{C}$ is a number field, then one can use the LLL algorithm [48] to recover $c_k \in F$. More precisely, if $h$ is the maximal (logarithmic) height of the coefficients $c_k$ seen in $\mathbb{C}$, then $N$ can be bounded by
a term in $O(h)$. Using fast versions of LLL this reconstruction step can be done in time $\tilde{O}(N)$ (according to Novocin, Stehlé and Villard [57]).}

\[\square\]

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

More generally a similar technique could be used if we had several secondary invariants $i_3, i_4, \ldots i_l$. There is no unique expression of $c$ in terms of the $i_k$ due to the equations between the invariants $i_k$. But for the interpolation to work we need to interpolate the same rational function expression. A solution is to fix a monomial ordering, since this defines a unique rational function expressing $c$ modulo the corresponding Gröbner basis. As long as the partial evaluation of the Gröbner basis corresponds to the Gröbner basis of the partial evaluation of the equation (see [2, 40]), the interpolation step will interpolate the correct expression of the rational function.

### 3.4 Equations for covers of Hilbert surfaces

Let $G_2 \subset G_1 \subset \text{SL}_2(\mathcal{O}_K \oplus \mathcal{O}_K) \cup \text{SL}_2(\mathcal{O}_K \oplus \mathcal{O}_K) \sigma$ be congruence subgroups. Then $H_{G_2} \to H_{G_1}$ is a covering. Let $i_1, i_2, i_3$ be Hilbert modular functions such that $C_{G_1} = \mathbb{C}(i_1, i_2, i_3)$ and $j_1, j_2, j_3$ be Hilbert modular functions such that $C_{G_2} = \mathbb{C}(j_1, j_2, j_3)$.

To describe the cover $H_{G_2} \to H_{G_1}$ 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 $H_{G_1}$, 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 $G_1$ (respectively $G_2$), but these relations can be computed with the same tool as for the relations between $i_1, i_2, i_3, j_1, j_2, j_3$.

Let $i_1, i_2, i_3$ be generators of the Hilbert modular field $C_{G_1}$ 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 $C_{G_2}/C_{G_1}$. Such a generator always exists by the primitive element theorem. The cover $H_{G_2} \to H_{G_1}$ is then (up to birationality) uniquely described by

- the minimal polynomial $\Phi_j \in C_{G_1}[X]$ of $j$ over $C_{G_1}$;
- and polynomials $Q_k \in C_{G_1}[X]$ such that $j_k = Q_k(j)$.

In practice it is more convenient to use the polynomial $\Psi_k \in C_{G_1}[X]$ of minimal degree such that $j_k \Phi_j(j) = \Psi_k(j)$ than the polynomials $Q_k$. The polynomial $\Psi_k$ is called the Hecke representation of $j_k$ and is more convenient for computations than $Q_k$ because it has smaller coefficients [28, Section 3].

**Lemma 3.9.** The polynomial $\Psi_k$ is $\Psi_k(X) = \sum_{\gamma \in G_1 \setminus G_1} j_k^\gamma \Phi_j(X)/(X - j^\gamma)$.

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

19
Indeed, evaluating \( \sum_{\delta \in \mathbb{G}_2} J^\delta \prod_{\delta' \neq \delta} (X - j^{\delta'}) / (j^\delta - j^{\delta'}) \) at \( j^\gamma \) gives \( J^\gamma \). Now, this expression is equal to \( \sum_{\delta \in \mathbb{G}_2} J^\delta \prod_{\delta' \neq \delta} (X - j^{\delta'}) / \Phi'(j^\delta) = \sum_{\delta \in \mathbb{G}_2} J^\delta \Phi(X)/(X - j^\delta) \Phi'(j^\delta) \) and we deduce that taking \( \Psi(X) = \sum_{\delta \in \mathbb{G}_2} J^\delta \Phi(X)/(X - j^\delta) \), we have the property \( J^\gamma \Phi'(j^\gamma) = \Psi(j^\gamma) \).

We apply this to the extension \( \mathbb{C}_{\tilde{\Gamma}(n)}/\mathbb{C}_{\text{SL}_2(O_K \oplus \mathcal{O}_K) \cup \text{SL}_2(O_K \oplus \mathcal{O}_K)^2} \) where \( \tilde{\Gamma}(n) \) is a congruence subgroup included in \( \mathbb{G}_2 \). Indeed this is a Galois extension of Galois group \( \tilde{\Gamma}(n) \setminus (\text{SL}_2(O_K \oplus \mathcal{O}_K) \cup \text{SL}_2(O_K \oplus \mathcal{O}_K)^2) \), and we apply the result above to \( G_1 = \tilde{\Gamma}(n)^\gamma \mathbb{G}_1 \) and \( G_2 = \tilde{\Gamma}(n)^\gamma \mathbb{G}_2 \) with the notations of the Lemma.

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

Let \( \Phi(X, i_1, i_2, i_3) = \prod_{\gamma \in \mathbb{G}_2} (X - j^\gamma) = X^L + \sum_{m=0}^{L-1} c_m(i_1, i_2, i_3) X^m \) be the minimal polynomial of \( j \) over \( \mathbb{C}_{\mathbb{G}_1} \), where \( L = \#\mathbb{G}_2 \). Let \( \Psi_k \in \mathbb{C}_{\mathbb{G}_1}[X] \) be the polynomial given in Lemma 3.9 for \( j_k \). A birational model of the cover \( \mathcal{H}_{\mathbb{G}_2} \rightarrow \mathcal{H}_{\mathbb{G}_1} \) is described by the equations

\[
\Phi(j) = 0, \quad j_1 \Phi'(j) = \Psi_1(j), \quad j_2 \Phi'(j) = \Psi_2(j), \quad j_3 \Phi'(j) = \Psi_3(j).
\]

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

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

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

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

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

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

- Compute each value \( j(\gamma, \tau) \) in precision \( N \). It can be done with a complexity in \( L\tilde{O}(N) \) time;
- Evaluate \( \Phi(j(\gamma)) = \prod_{\gamma \in \mathbb{G}_2} (X - j(\gamma, \tau)) \) using a subproduct tree (see [25, Section 10.1]). The polynomial \( \Phi(j(\gamma)) \) can be obtained in \( \tilde{O}(LN) \) time.
• Separating the coefficients according to powers of $X$ gives the values $c_m(i_1(\tau), i_2(\tau), i_3(\tau))$.

By Section 3.3 and Theorem 3.7, to recover $\Phi$, the evaluation step will be executed $O(dd_T d_{i_2})$ times and we will interpolate $O(dL)$ bivariate rational fractions and do $O(L d_T d_{i_2})$ interpolation of a univariate polynomial. Recall that given the coefficient $c_{mn} \in \mathbb{C}$ computed at precision $O(N)$, using the LLL algorithm to recover $c_{mn} \in F$ can be done in time $\tilde{O}(N)$ ([57]). The final complexity is then

\begin{equation}
O(dd_T d_{i_2})\tilde{O}(LN) + O(dL)\tilde{O}(d_T d_{i_2} N) + O(L d_T d_{i_2})\tilde{O}(dN) \subseteq \tilde{O}(dd_T d_{i_2} LN).
\end{equation}

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

\section{Modular polynomials}

\subsection{Isogenies preserving real multiplication}

We want now to define modular polynomials, which parametrize isogenies between principally polarized abelian surfaces with real multiplication by $O_K$. To achieve this, we need the following subgroups of $SL_2(O_K \oplus \partial_K)$

\begin{align}
\tilde{\Gamma}^0(\beta) &= \left\{ \left( \frac{a}{\sqrt{\Delta_K}} \frac{b}{\sqrt{\Delta_K}} \frac{c}{d} \right) \in SL_2(O_K \oplus \partial_K) : b \in \beta O_K \right\}, \\
\tilde{\Gamma}(\beta) &= \left\{ \left( \frac{a}{\sqrt{\Delta_K}} \frac{b}{\sqrt{\Delta_K}} \frac{c}{d} \right) \in SL_2(O_K \oplus \partial_K) : a - 1, d - 1, b, c \in \beta O_K \right\}
\end{align}

where $\beta \in O_K$ is a totally positive prime number. By abuse of notation, we use the same notation for their preimage by the isomorphism $\phi_\pm$ of Equation (4). Then the Hilbert cover $\tilde{\Gamma}^0(\beta) \backslash H_1^T$ parametrizes pairs $(A, B)$ of (principally polarised) abelian surfaces with real multiplication by $O_K$ together with a $\beta$-isogeny $A \to B$, or equivalently pairs $(A, K)$ where $A$ has real multiplication by $O_K$ and $K \subset A[\beta]$ is a kernel stable by $O_K$ and maximally isotropic for the $\beta$-Weil pairing.

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

It remains to see when $B$ admits a principal polarization. If $\theta_B$ is such a principal polarization, then $\theta = f^* \theta_B$ is a polarization on $A$. Denote by $\text{End}^s(A)$ the subring of endomorphisms of $A$ commuting with the Rosati involution induced by $\theta_A$. By [3, Proposition 5.2.1 and Theorem 5.2.4], the group isomorphism between the Néron-Severi group of $A$ and $\text{End}^s(A)$ induces a bijection between the polarizations of some degree $L$ of $A$ and the set $\text{End}^{s,++}(A)$ of totally positive symmetric endomorphisms of $A$ with analytic norm $L$. When $\text{End}^s(A) = O_K$ (which is the case generically for an element of the Hilbert surface), then $\theta$ comes from a totally positive element $\beta \in O_K^{++}$. Furthermore it is easy to check that $V$ is a totally isotropic subgroup for the Weil pairing $\epsilon_\beta$ on $A[\beta] = \{ P \in A(k) \mid \beta P = 0 \}$. Looking at degrees, we also get that $\#V = N_{K/Q}(\beta)$.
Conversely, let $\beta \in \mathcal{O}_K^{++}$ and note $\theta^\beta$ the polarization on $A$ induced from $\theta_A$ by $\beta$ (the polarization which arises from the composition of the polarization isogeny of $\theta_A$ with $\beta$), and $V \subset A[\beta]$ a maximal isotropic subgroup for the Weil pairing $e_\beta$. Then by descent theory, $\theta^\beta$ descends to a polarization $\theta_B$ on $B = A/V$, and since $V$ is maximal, $\theta_B$ is principal. To emphasize the role of $\beta$, we call the isogeny $f$ induced by $V$ a $\beta$-isogeny.

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

For more details we refer to [59, 14, 15] and in particular in [15, Theorem 1.1] of Dudeanu, Jetchev, Robert, and Vuille. We are mainly interested with cyclic isogenies of prime degree $\ell$, these are induced by $\beta$ of norm $\ell$. We sum up the discussion above by the following

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

We will compute modular polynomials when $\beta = \ell \in \mathbb{Z}$ is a prime number, and when $\beta$ is a totally positive element of $\mathcal{O}_K$ of norm $\ell$. We first give the degree of the cover $\hat{\Gamma}^0(\beta)\backslash \mathcal{H}_1^2 \to \text{SL}_2(\mathcal{O}_K \oplus \partial_K)\backslash \mathcal{H}_1^2$, since this will determine the degrees of the modular polynomials.

When $\beta = \ell$, the Weil pairing is the usual pairing $e_\ell$ on $A[\ell]$, and the corresponding $\ell$-isogenies come from isotropic kernels of degree $\ell^2$. 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 $\Gamma^0(\ell)\backslash \text{Sp}_4(\mathbb{Z})$). The computation of the corresponding modular polynomials is described in [16, 5, 51]. 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, $A[\ell]$, as a $\mathcal{O}_K$-module, is given by a symplectic basis $e_1, e_2$. To such a basis one can associate the subgroup $V = \mathcal{O}_Ke_1$ 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 $\hat{\Gamma}^0(\ell)\backslash \text{SL}_2(\mathcal{O}_K \oplus \partial_K)$ on the symplectic basis $(e_1, e_2)$.

**Proposition 4.3.** The number of $\ell$-isogenies whose kernel is stable under the real multiplication is

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

**Proof.** Using $\phi_+$, we have to find the cardinality of $\hat{\Gamma}^0(\ell)\backslash \text{SL}_2(\mathcal{O}_K)$. We compute it as the quotient of $\#\hat{\Gamma}(\ell)\backslash \text{SL}_2(\mathcal{O}_K)$ by $\#\hat{\Gamma}(\ell)\backslash \hat{\Gamma}^0(\ell)$. We use the group isomorphism $\psi : \hat{\Gamma}(\ell)\backslash \text{SL}_2(\mathcal{O}_K) \simeq \text{SL}_2(\ell\mathcal{O}_K/\mathcal{O}_K)$ and we compute the cardinality of $\hat{\Gamma}(\ell)\backslash \hat{\Gamma}^0(\ell)$ looking at its image by $\psi$. Moreover we use that $\ell\mathcal{O}_K/\mathcal{O}_K$ is isomorphic to $\mathbb{F}_\ell^2$ if $\ell$ is split, to $\mathbb{F}_{\ell^2}$ if $\ell$ is inert and to $\mathbb{F}_\ell[X]/(X^2)$ if $\ell$ is ramified.
If \( \ell \) is inert, \( \# \text{SL}_2(\mathbb{F}_\ell) = \ell^2(\ell^4 - 1) \) and \( \# \hat{\Gamma}(\ell) \backslash \hat{\Gamma}_0(\ell) = \ell^2(\ell^2 - 1) \). If \( \ell \) is split, \( \# \text{SL}_2(\mathbb{F}_\ell^2) = \ell^2(\ell^2 - 1)^2 \) and \( \# \hat{\Gamma}(\ell) \backslash \hat{\Gamma}_0(\ell) = \ell^2(\ell - 1)^2 \). If \( \ell \) is ramified, \( \# \text{SL}_2(\mathbb{F}_\ell[X]/(X^2)) = \ell^6 - \ell^4 \) and \( \# \hat{\Gamma}(\ell) \backslash \hat{\Gamma}_0(\ell) = \ell^2(\ell^2 - \ell) \). \( \square \)

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

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

**Proof.** We have seen that \( \beta \)-isogenies correspond to maximally isotropic kernels of size \( \ell \) in \( A[\beta] \). Since \( A[\beta] \) is of size \( \ell^2 \), such kernels are exactly the cyclic kernels of size \( \ell \). Since \( \beta \mathcal{O}_K \backslash \mathcal{O}_K \simeq \mathbb{F}_\ell \), the elements of \( \mathcal{O}_K \) act by scalar multiplication on \( A[\beta] \) so they stabilize all the cyclic subgroups. And indeed since \( \hat{\Gamma}(\beta) \backslash \text{SL}_2(\mathcal{O}_K) \simeq \text{SL}_2(\mathbb{F}_\ell) \) it is easy to check that \( \hat{\Gamma}_0(\beta) \backslash \text{SL}_2(\mathcal{O}_K) \) is of size \( \ell + 1 \) and a set of representatives is given by the matrices \( \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \) for \( x \in \{0, \ldots, \ell-1\} \) and \( \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \).

Indeed since \( \beta \mathcal{O}_K \backslash \mathcal{O}_K \simeq \ell \mathbb{Z} \backslash \mathbb{Z} \), we have that \( \hat{\Gamma}_0(\beta) \backslash \text{SL}_2(\mathcal{O}_K) \simeq \Gamma_0(\ell) \backslash \text{SL}_2(\mathbb{Z}) \) whose set of representatives is well known. \( \square \)

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

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

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

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

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

From this Lemma we deduce that the \( \epsilon^2 \beta \)-modular polynomial will be the same as the \( \beta \)-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 \( \ell \). It is also straightforward to adapt the results of Section 3 for computing invariants on the Hilbert surfaces of abelian surfaces with real multiplication by \( O \), and also to compute modular polynomials for such an \( O \).
4.2 Modular functions for $\beta$-isogenies

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

For simplicity, we now assume that $n$ is prime to $L$. We first want to give an explicit set of representatives of $\Gamma^0(\beta) \cap \tilde{\Gamma} \setminus \tilde{\Gamma}$. Recall that there in an isomorphism $\phi_\pm : \text{SL}_2(\mathcal{O}_K) \to \text{SL}_2(\mathcal{O}_K \oplus \partial K)$ defined in Equation (4), so that by looking at the preimage by $\phi_\pm$ we can assume here that $\tilde{\Gamma} \subset \text{SL}_2(\mathcal{O}_K)$ (this is more convenient to study the quotient). Recall that in this model, $\tilde{\Gamma}^0(\beta) = \{ (a \ b \ c \ d) \in \text{SL}_2(\mathcal{O}_K) : \beta | b \}$.

**Lemma 4.7.** Let $N$ be an integer. Then the map $\text{SL}_2(\mathcal{O}_K) \to \text{SL}_2(\mathcal{O}_K / N \mathcal{O}_K)$ 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 $\text{SL}_2(\mathcal{O}_K / N \mathcal{O}_K)$ is a product of local rings, it is generated by elementary matrices, so it suffices to lift these matrices.

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

**Proof.** The sets $\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta) \setminus \tilde{\Gamma}$ and $\tilde{\Gamma}^0(\beta) \setminus \tilde{\Gamma} \tilde{\Gamma}$ are in bijection so by Propositions 4.3 and 4.4 it suffices to prove that $\tilde{\Gamma}^0(\beta) \tilde{\Gamma} = \tilde{\Gamma}(1)$. So it suffices to prove that $\tilde{\Gamma}(L) \tilde{\Gamma}(n) = \tilde{\Gamma}(1)$, which is obvious by the Chinese Reminder Theorem.

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

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

By Lemma 4.8, the subgroup $\tilde{\Gamma}^0(\beta)$ of $\tilde{\Gamma}$ is of index $L + 1$ and the set of matrices $C_\beta = \{ M_1, M_2, i \in \{0, \ldots, L - 1\} \}$ is a set of representatives of the classes of $\tilde{\Gamma}^0(\beta) \setminus \tilde{\Gamma}$. We can give a different proof using the matrices $M_1$, $M_2$ and $M_3$: the $L+1$ matrices of $C_\beta$ are clearly in different classes of the quotient $\tilde{\Gamma}^0(\beta) \setminus \tilde{\Gamma}$. Remark that $^tM_2 = M_1 M_2^{-1} M_1^{-1} \in \tilde{\Gamma}^0(\beta)$ and $^tM_3 = M_1 M_3^{-1} M_1^{-1} \in \tilde{\Gamma}^0(\beta)$ and that $\tilde{\Gamma}$ is generated by $M_1$, $^tM_2$ and $^tM_3$. For all $i \in \{0, \ldots, L\}$, $^tM_2 M_2^i$ and $^tM_3 M_2^i$ are in the class of $M_2$ while $^tM_2 M_1$ and $^tM_3 M_1$ are in the class of $M_1$. Moreover, $M_1 M_2$ is in the class of $M_1$ and $M_1 M_1 = -I_2$ which shows that there can not be more than the $L + 1$ classes that we already know.

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

If $\gamma \in \tilde{\Gamma}^0(\beta) \setminus \text{SL}_2(\mathcal{O}_K)$ then there exists an element $\gamma' \in \tilde{\Gamma}^0(\beta)$ such that $\gamma' \gamma \in \tilde{\Gamma}(2, 4)$. For applications it is useful to have a constructive definition of $\gamma'$.
We look at \(\gamma'\) such that \(\gamma'\gamma \equiv 0 \text{ mod } 4\), namely such that \(\gamma' \equiv \gamma^{-1} \text{ mod } 4\), and such that \(\gamma' \equiv (\ast \ast) \mod \ell\). By the Chinese Remainder Theorem, these conditions modulo 4 and \(\ell\) gives a matrix \(\gamma''\) which must satisfy conditions modulo \(4\ell\) and by Lemma 4.7, \(\gamma''\) can be lifted to a matrix in \(\tilde{\Gamma}\).

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

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

Let \(j\) be a generator of the field extension \(\mathbb{C}_G/\mathbb{C}_G\). 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 \(\mathbb{C}_G\). Let \(j\) be a Hilbert modular function invariant by \(\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)\) but not by \(\tilde{\Gamma}\). Then \(\mathbb{C}_{\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)} = \mathbb{C}(i_1, i_2, i_3, j)\).

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

Let \(\pi : \hat{\Gamma} \to \text{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K)\). If \(\beta\) is of norm \(L = \ell\) prime (so that \(\ell\) is split, then \(\text{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K) \simeq \text{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^2\) and \(\pi(\tilde{\Gamma}^0(\beta)) = \{(* *),(\ast \ast)\}\). By King [41, Theorem 4.1], the set of triangular matrices of \(\text{SL}_2(\mathbb{Z}/\ell\mathbb{Z})\) is maximal and thus \(\pi(\tilde{\Gamma}^0(\beta))\) is maximal in \(\text{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^2\). As \(\pi\) is surjective, we deduce that \(\tilde{\Gamma}^0(\beta)\) is maximal in \(\hat{\Gamma}\).

If \(\beta = \ell\) is inert, then the image of \(\pi(\tilde{\Gamma}(\beta))\) is given by triangular matrices of \(\text{SL}_2(\mathcal{O}_K)\) so it is also maximal.

If \(\ell\) is ramified, then \(\text{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K) \simeq \text{SL}_2(\mathbb{Z}/\ell\mathbb{Z})[X]/(X^2)\) and \(\pi(\tilde{\Gamma}^0(\beta))\) is the set of matrices of the form \((z xX)\) 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 \((\begin{array}{cc}A & B \\ C & D \end{array})\) \(\in G\), with \(B(0) = 0\). If \(A\) is invertible (namely \(A(0) \neq 0\)) then \((\begin{array}{cc}1 & 0 \\ -A & 1 \end{array})\) \((\begin{array}{cc}A & B \\ C & D \end{array})\) \(= \left(\begin{array}{cc}1 & -A^{-1}B \\ 0 & -1 \end{array}\right)\) \(\in G\) and \(A^{-1}B(0) \neq 0\) so that \(A^{-1}B = x_0 + x_1X\). Finally we have \(\left(\begin{array}{cc}1 & 0 \\ 0 & 1 \end{array}\right)\left(\begin{array}{cc}1 & -x_1X \\ 0 & 1 \end{array}\right) = \left(\begin{array}{cc}1 & x_0 \\ 0 & 1 \end{array}\right)\) from which we deduce that \((\frac{1}{0} \frac{1}{1}) \in G\). As this last matrix and the matrices \((\frac{1}{1} \frac{0}{0})\) and \((\frac{1}{0} \frac{1}{0})\) are all in \(G\) and are generators for \(\text{SL}_2(\mathcal{O}_K/\ell\mathcal{O}_K)\), we deduce that \(G = \pi(\hat{\Gamma})\), 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, \((\begin{array}{cc}A & B \\ C & D \end{array})\) \((\begin{array}{cc}1 & 0 \\ 0 & 1 \end{array})\) = \((\begin{array}{cc}A+B & B \\ C+D & D \end{array})\) and \((A+B)(0) \neq 0\), which ends the proof. \(\square\)
4.3 Computing modular polynomials

Using the notations of Section 4.2, we want to compute modular polynomials classifying all \( \beta \)-isogenies from an abelian surface with real multiplication by \( O_K \).

First consider the case \( \Gamma = \Gamma(1) \). Recall from Section 4.1 that geometrically, a point in \( H_{\Gamma_0(\beta)} \) corresponds to a triple \((A, \theta, V)\) with a principally polarized abelian surface \((A, \theta)\) and \( V \) the kernel of a \( \beta \)-isogeny (equivalently \( V \) is maximally isotropic for the \( \epsilon_\beta \) Weil pairing on \( A[\beta] \)). We note \( \pi : (A, \theta, V) \to (A, \theta) \times (A/V, \theta') \) where \( \theta' \) is the polarization induced on \( A/V \) by \( \theta \beta \). This defines an algebraic map (a modular correspondence) \( H_{\Gamma_0(\beta)} \to H_{\Gamma(1)} \times H_{\Gamma(1)} \). The \( \beta \)-modular polynomials describe the algebraic relations giving the image of this map.

Concretely, if \( i_1, i_2, i_3 \) generate \( \mathbb{C}(\Gamma(1)) \), the \( \beta \)-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 \( z \in H^2_1 \). In particular the \( \beta \)-modular polynomials classify the \( \beta \)-isogenies. Indeed if \( z \in \Gamma(1) \setminus H^2_1 \), the \( \beta \)-isogenous varieties are \( \frac{1}{\beta} \gamma \cdot z \) for \( \gamma \in \Gamma^0(\beta) \setminus \Gamma(1) \). Furthermore since \( \sigma \Gamma^0(\beta) \sigma = \Gamma^0(\beta) \), the \( \beta \)-isogenous varieties are given by \( \frac{1}{\beta} \gamma \cdot z \), for \( \gamma \in \Gamma^0(\beta) \setminus \Gamma(1) \).

Furthermore, by Lemma 4.13, the modular function \( i_1(z/\beta) \) is invariant by \( \Gamma^0(\beta) \), so by Proposition 4.11 is a generator of \( \mathbb{C}(H_{\Gamma_0(\beta)})/\mathbb{C}(H_{\Gamma(1)}) \). This implies that the modular correspondence \( H_{\Gamma_0(\beta)} \to H_{\Gamma(1)} \times H_{\Gamma(1)} \) is an embedding (at least birationally), so that the \( \beta \)-modular polynomials do give equations for \( H_{\Gamma_0(\beta)} \).

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

**Definition 4.12.** Let \( \gamma \in \Gamma^0(\beta) = (a/b \, \epsilon_\beta) \). We denote \( \gamma_\beta = (a/b^\beta \, \epsilon_\beta^{-1}) \in \Gamma(1) \).

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

\[
\begin{align*}
i_\beta^\gamma(z) &= i\left(\frac{1}{\beta} \gamma \cdot z\right) = i(\gamma_\beta \cdot (\frac{1}{\beta} z)) = i\gamma_\beta^\gamma (\frac{1}{\beta} z) \\
i_\beta^\gamma^\sigma(z) &= i\left(\frac{1}{\beta} \sigma z\right) = i\gamma_\beta^\gamma (\frac{1}{\beta} z) \\
i_\beta^\gamma^\sigma^\sigma(z) &= i\left(\frac{1}{\beta} \gamma_\beta \sigma \cdot z\right) = i\gamma_\beta^\gamma^\sigma^\sigma (\frac{1}{\beta} z)
\end{align*}
\]

**Corollary 4.14.** Let \( i \) be a Hilbert modular function for \( \hat{\Gamma} \subset \text{SL}_2(O_K + \partial_K) \). Let \( \hat{\Gamma}_\beta = \{ \gamma \in \text{SL}_2(O_K + \partial_K) \mid \gamma_\beta \in \hat{\Gamma}\} \subset \hat{\Gamma}^0(\beta) \). Then \( i_\beta \) is modular for \( \hat{\Gamma}_\beta \). Furthermore if \( i \) is symmetric and \( \beta = \beta \), then \( i_\beta \) is symmetric.

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

\[(22) \quad \hat{\Gamma} \cap \Gamma^0(\beta) = \hat{\Gamma} \cap \hat{\Gamma}_\beta.\]

Then if \( i \) is a Hilbert modular function for \( \hat{\Gamma} \), then \( i_\beta \) is a Hilbert modular function for \( \hat{\Gamma} \cap \Gamma^0(\beta) \).
If \( \tilde{\Gamma} \) satisfy Equation (22) (such is the case when \( \tilde{\Gamma} = \hat{\Gamma}(n) \) is a congruence subgroup), one can then define the modular correspondence as \( H_{\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)} \to H_{\tilde{\Gamma}} \times H_{\tilde{\Gamma}}, z \mapsto ((i_1(z), i_2(z), i_3(z)), (i_1(z/\beta), i_2(z/\beta), i_3(z/\beta))) \) for \( z \in H_{\tilde{\Gamma}}^3 \) and \( i_1, i_2, i_3 \) generating \( C_{\tilde{\Gamma}} \).

**Theorem 4.15.** Non symmetric case: let \( \tilde{\Gamma} \) be a congruence subgroup such that \( \tilde{\Gamma}(2,4) \subset \tilde{\Gamma} \subset SL_2(\mathcal{O}_K \oplus \partial K) \). 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 \( C_{\beta} \) be a set of representatives of \( \tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta) \tilde{\Gamma} \).

Let \( i_1, i_2, i_3 \) modular functions generating \( C_{\Gamma} \) and with Fourier coefficients in a number field \( F \).

Define the modular polynomials:

\[
\Phi_\beta(X, i_1, i_2, i_3) = \prod_{\gamma \in C_{\beta}} (X - i^{\gamma}_{1,\beta}), \quad \text{and} \quad \Psi_{k,\beta}(X, i_1, i_2, i_3) = \sum_{\gamma \in C_{\beta}} i^{\gamma}_{k,\beta} \frac{\Phi_{\beta}(X, i_1, i_2, i_3)}{X - i^{\gamma}_{1,\beta}} \]

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 \( \beta, \) only on \( i_1, i_2, i_3 \), and under the heuristics of [51, Theorem 34]), the modular polynomials can be computed in quasi-linear time in their size.

Symmetric case: Let \( G = \tilde{\Gamma} \cup \tilde{\Gamma} \sigma \). If \( \tilde{\beta} = \beta \) we let \( C_{\beta} \) be a set of representatives of \( (\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)) \cup (\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)) \sigma \) \( \tilde{\Gamma} \sigma \), if \( \tilde{\beta} = \beta \) we let \( C_{\beta} \) be a set of representatives of \( G \cap \tilde{\Gamma}^0(\beta) / \tilde{\Gamma} \). Let the same definition as in Equation (22) applies and the corresponding modular polynomials can be computed in quasi-linear time.

**Proof.** This is Theorem 3.11, 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 \( \mathbb{C}_{\tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta)} / \mathbb{C}_{\Gamma} \). Then in the notations of Theorem 3.10 we can use \( j = i_{k,\beta} \) (in Theorem 4.15 we assume \( k = 1 \)).

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

**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 \( \beta \)-modular polynomials for \( i_1, i_2, i_3 \).

**Example 4.17.**

- If \( \beta = \ell \) is an inert prime. Then \( \Phi_\ell \) has degree \( \ell^2 + 1 \) and \( \Psi_{k,\ell} \) has degree \( \ell^2 \). 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 \( \beta \) has norm \( \ell \), so \( \ell = \beta \bar{\beta} \) is split. Then if \( G = \tilde{\Gamma} \) is not symmetric, \( \Phi_\beta \) has degree \( \ell + 1 \) and \( \Psi_{k,\beta} \) has degree \( \ell \).

However if \( \sigma \in G \), so that \( G = \tilde{\Gamma} \times \langle \sigma \rangle \), then since the \( i_{k,\beta} \) are not symmetric, \( \Phi_\beta \) 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 \( \sigma \) as follows: if we let \( C_{\beta} \) be a set of representatives of \( \tilde{\Gamma} \cap \tilde{\Gamma}^0(\beta) \tilde{\Gamma} \) the modular polynomials are given by

\[
\Phi_{\beta}(X, i_1, i_2, i_3) = \prod_{\gamma \in C_{\beta}} (X - i^{\gamma}_{1,\beta})(X - i^{\gamma}_{1,\beta}) = \prod_{\gamma \in C_{\beta}} (X - i^{\gamma}_{1,\beta})(X - i^{\gamma}_{1,\beta}) \quad \text{and}
\]
Thus, in this case, guarantee the fact that Let \( \epsilon \) be a fundamental unit of \( \mathcal{O}_K \). Let \( \epsilon' \in \mathcal{O}_K^{\times} \), then there are also \( \epsilon' \)-isogenies. (We only consider totally positive units \( \epsilon' \) to guarantee the fact that \( \epsilon'z \in \mathcal{H}_2^{\times} \)). If there exists \( n \in \mathbb{Z} \) such that \( \epsilon' = \epsilon^{2n} \), then the matrix \( \gamma = \begin{pmatrix} \epsilon^n & 0 \\ 0 & \epsilon^{-n} \end{pmatrix} \) is in \( \tilde{\Gamma} \) and \( \gamma \cdot z = \epsilon'z \). Thus, in this case, \( i_k(\epsilon'z) = i_k(z) \), and, in particular, a \( \beta \)-isogeny is also an \( \epsilon' \)-isogeny. (For a more intrinsic proof see Lemma 4.5.) When \( D = 2 \) or \( 5 \), a fundamental unit \( \epsilon \) has norm \(-1\) while \( \epsilon' \in \mathcal{O}_K^{\times} \) has norm \( 1 \), so that the latter can always be written as an even power of \( \epsilon \). Thus, the choice of the splitting of \( \ell \) does not matter.

**Remark 4.18** (Changing \( \beta \) when \( \tilde{\Gamma} = \text{SL}_2(\mathcal{O}_K \oplus \partial K) \)). Let \( \epsilon \) be a fundamental unit of \( \mathcal{O}_K \). Let \( \epsilon' \in \mathcal{O}_K^{\times} \), then there are also \( \epsilon' \)-isogenies. (We only consider totally positive units \( \epsilon' \) to guarantee the fact that \( \epsilon'z \in \mathcal{H}_2^{\times} \)). If there exists \( n \in \mathbb{Z} \) such that \( \epsilon' = \epsilon^{2n} \), then the matrix \( \gamma = \begin{pmatrix} \epsilon^n & 0 \\ 0 & \epsilon^{-n} \end{pmatrix} \) is in \( \tilde{\Gamma} \) and \( \gamma \cdot z = \epsilon'z \). Thus, in this case, \( i_k(\epsilon'z) = i_k(z) \), and, in particular, a \( \beta \)-isogeny is also an \( \epsilon' \)-isogeny. (For a more intrinsic proof see Lemma 4.5.) When \( D = 2 \) or \( 5 \), a fundamental unit \( \epsilon \) has norm \(-1\) while \( \epsilon' \in \mathcal{O}_K^{\times} \) has norm \( 1 \), so that the latter can always be written as an even power of \( \epsilon \). Thus, the choice of the splitting of \( \ell \) does not matter.

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

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

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

Finally if \( \beta \in \mathcal{O}_K^{\times} \) is totally positive but not prime, it is easy to adapt Theorem 4.15 (if we suppose that \( i_1 \) is not invariant by \( \tilde{\Gamma} \cap \Gamma^0(\beta) \) for strict divisors ideal \( J \) of \( (\beta) \)). The only difference is on the degree of the polynomials, \( \Phi_\beta \) will not be of degree the norm of \( \beta \). Rather the degree depends on the factorization of \( (\beta) \) into prime ideals.

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

## 5 Results

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

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

### 5.1 Case \( D = 2 \)

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

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

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

\[
P(J_1, J_2) = J_1^2 - J_1J_2 + 2J_1J_2 - 81J_1 + 64J_2^2
\]

and for \( \ell = 17 \)

\[
P(J_1, J_2) = J_1^2 - J_1J_2^2 - 6J_1^2J_2 + J_1^2J_2 - 414J_1^6 + 428J_1^5J_2^3 + 2387J_1^5J_2^2 - 17760J_1^7J_2 + 431811J_1^6J_2^3 + 17728J_1^6J_2^2 - 331952J_1^5J_2^3 - 2578856J_1^5J_2^2 + 6229197J_1^4J_2^3 - 80515134J_1^4J_2^2 - 6145536J_1^5J_2^2 + 52974272J_1^5J_2^1 + \\
535037040J_1^3J_2^3 + 6116816412J_1^3J_2^2 + 3782285936J_1^3J_2 + 91648000J_1^2J_2^3 - 6502153216J_1^2J_2^2 - 7579320576J_1^2J_2 - 197144611776J_1^2J_2 + \\
1756596000J_1J_2^3 - 7812042752J_1J_2^2 + 1105920000J_1J_2.
\]

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

<table>
<thead>
<tr>
<th>( D )</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \ell = 2 )</td>
<td>( \ell = 7 )</td>
</tr>
<tr>
<td>2</td>
<td>8.5 KB</td>
</tr>
<tr>
<td>7</td>
<td>172 KB</td>
</tr>
<tr>
<td>17</td>
<td>5.8 MB</td>
</tr>
<tr>
<td>23</td>
<td>21 MB</td>
</tr>
<tr>
<td>31</td>
<td>70 MB</td>
</tr>
<tr>
<td>41</td>
<td>225 MB</td>
</tr>
<tr>
<td>47</td>
<td>400 MB</td>
</tr>
<tr>
<td>71</td>
<td>2.2 GB</td>
</tr>
</tbody>
</table>

Table 1: Informations about the modular polynomials for \( D = 2 \) (Gundlach invariants)

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

\[
\Phi_{\beta}(X, \tilde{b}_2, \tilde{b}_3) = X^{2\ell+2} + \sum_{i=0}^{2\ell+1} c_i(\tilde{b}_2, \tilde{b}_3)X^i \quad \text{and} \quad \Psi_{\beta}(X, \tilde{b}_2, \tilde{b}_3) = \sum_{i=0}^{2\ell+1} d_i(\tilde{b}_2, \tilde{b}_3)X^i.
\]
We have constated that the denominators of $c_i$ and $d_i$ are of the form $P(\tilde{b}_2, \tilde{b}_3)^2$ unless $i = 2\ell + 1$ where it is $P(\tilde{b}_2, \tilde{b}_3)$. For example, we have for $\ell = 17$ and $\beta = 5 + 2\sqrt{2}$

$$P(\tilde{b}_2, \tilde{b}_3) = \frac{\tilde{b}_3^5 \tilde{b}_3^{18}}{(3 \tilde{b}_3^3 - 6 \tilde{b}_3^4 + 1)\tilde{b}_2^6 + (15\tilde{b}_3^{10} - 24\tilde{b}_3^8 + 7\tilde{b}_3^2)\tilde{b}_2^{14} + (20\tilde{b}_3^{12} - 42\tilde{b}_3^8 + 9\tilde{b}_3^4 + 2)\tilde{b}_2^{18} + (15\tilde{b}_3^{14} - 48\tilde{b}_3^{10} + 37\tilde{b}_3^6 + 4\tilde{b}_3^2)\tilde{b}_2^{16} + (6\tilde{b}_3^{16} - 42\tilde{b}_3^{12} + 68\tilde{b}_3^8 - 26\tilde{b}_3^4 + 3)\tilde{b}_2^{20} + (\tilde{b}_3^8 - 24\tilde{b}_3^{14} + 37\tilde{b}_3^{10} + 8\tilde{b}_3^6 - \tilde{b}_3^2)\tilde{b}_2^{12} + (-6\tilde{b}_3^{16} + 9\tilde{b}_3^{12} - 26\tilde{b}_3^8 - 24\tilde{b}_3^4 + 2)\tilde{b}_2^{14} + (7\tilde{b}_3^{14} + 4\tilde{b}_3^{10} - \tilde{b}_3^6)\tilde{b}_2^{10} + (\tilde{b}_3^6 + 2\tilde{b}_3^2 + 3\tilde{b}_3^4 + 2)\tilde{b}_2^8 + \cdots}$$

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 $\sum_m \sum_{n,m,n} c_{i,m,n} \tilde{b}_2^m \tilde{b}_3^n$ (and similarly for $d_i$). We have then for $\ell = 17$ and $\beta = 5 + 2\sqrt{2}$

$$\begin{align*}
m &\equiv 0 \text{ mod } 2 & m &\equiv 1 \text{ mod } 2 \\
n + i &\equiv 0 \text{ mod } 2 & n + i &\equiv 1 \text{ mod } 2 \\
m + n &\equiv i \text{ mod } 4 & m + n &\equiv i \text{ mod } 4
\end{align*}$$

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 $m + n \equiv -i \text{ mod } 4$ for $c_i$ and $d_i$.

<table>
<thead>
<tr>
<th>$\ell$</th>
<th>$m$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>221 KB</td>
<td>24 18 18 57 53 50 13</td>
</tr>
<tr>
<td>41</td>
<td>7.2 MB</td>
<td>64 56 56 144 140 132 38</td>
</tr>
<tr>
<td>73</td>
<td>81 MB</td>
<td>120 112 112 264 260 246 79</td>
</tr>
<tr>
<td>89</td>
<td>188 MB</td>
<td>152 138 138 325 317 309 102</td>
</tr>
<tr>
<td>97</td>
<td>269 MB</td>
<td>168 154 154 357 345 341 112</td>
</tr>
</tbody>
</table>

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

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

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

### 5.2 Case $D = 5$

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

$$\Phi_\beta(X, J_1, J_2) = X^{2\ell + 2} + \sum_{i=0}^{2\ell + 1} c_i(J_1, J_2)X^i \quad \text{and} \quad \Psi_\beta(X, J_1, J_2) = \sum_{i=0}^{2\ell + 1} d_i(J_1, J_2)X^i,$$
when \( \ell \) is split, then we have constated that the denominators of \( c_i \) and of \( d_i \) are of the form \( P(J_1, J_2) \) except for \( i = 2\ell + 1 \) where it is \( P(J_1, J_2)^2 \). We have for example for \( \ell = 11 \)

\[
P(J_1, J_2) = 4J_1^4 + (-12J_2^2 - 19236J_2 + 119497519)J_2^6 + (12J_2^4 + 56972J_2^2 - 278163835056J_2 + 35953243171744)J_2^8 + (-4J_2^6 - 55980J_2^4 + 449730698J_2^2 + 943837290960J_2^3 - 133230692691392J_2 + 13001634695104256)J_2^{10} + (18500J_2^8 - 215193500J_2^6 - 1170430882000J_2^4 + 3462067742400000J_2^2 + 635091750000J_2^6 - 718632513000000J_2^4 + 3462067742400000J_2^2 + (-124875000000J_2^8 + 601911000000000J_2^6)/J_2 - 182250000000000J_2^2).
\]

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

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

by Equation (28) and Appendix B.2. 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.

<table>
<thead>
<tr>
<th>( D )</th>
<th>Memory</th>
<th>( \beta )</th>
<th>( \tilde{b}_1 )</th>
<th>( \tilde{b}_2 )</th>
<th>( \tilde{b}_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>22 KB</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>11</td>
<td>3.5 MB</td>
<td>10</td>
<td>7</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td>19</td>
<td>33 MB</td>
<td>16</td>
<td>12</td>
<td>16</td>
<td>64</td>
</tr>
<tr>
<td>29</td>
<td>188 MB</td>
<td>25</td>
<td>20</td>
<td>25</td>
<td>100</td>
</tr>
<tr>
<td>31</td>
<td>248 MB</td>
<td>26</td>
<td>21</td>
<td>26</td>
<td>104</td>
</tr>
<tr>
<td>41</td>
<td>785 MB</td>
<td>35</td>
<td>29</td>
<td>35</td>
<td>140</td>
</tr>
<tr>
<td>59</td>
<td>3.6 GB</td>
<td>50</td>
<td>43</td>
<td>50</td>
<td>200</td>
</tr>
<tr>
<td>5</td>
<td>26 KB</td>
<td>16</td>
<td>8</td>
<td>8</td>
<td>31</td>
</tr>
<tr>
<td>11</td>
<td>308 KB</td>
<td>72</td>
<td>40</td>
<td>40</td>
<td>84</td>
</tr>
<tr>
<td>19</td>
<td>3.6 MB</td>
<td>128</td>
<td>96</td>
<td>96</td>
<td>132</td>
</tr>
<tr>
<td>29</td>
<td>21 MB</td>
<td>200</td>
<td>152</td>
<td>152</td>
<td>212</td>
</tr>
<tr>
<td>31</td>
<td>28 MB</td>
<td>216</td>
<td>160</td>
<td>160</td>
<td>224</td>
</tr>
<tr>
<td>41</td>
<td>115 MB</td>
<td>288</td>
<td>240</td>
<td>240</td>
<td>324</td>
</tr>
<tr>
<td>59</td>
<td>470 MB</td>
<td>424</td>
<td>352</td>
<td>352</td>
<td>440</td>
</tr>
</tbody>
</table>

Table 3: Informations about the modular polynomials for \( D = 5 \)

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

### 5.3 Examples of isogenous curves

The modular polynomials allow one to compute hyperelliptic curves with isogenous Jacobians. In particular over finite field as the \( \beta \)-polynomials found can be reduced modulo a prime number \( p \neq \beta \beta \) without loosing their meaning ([6, Section 6, page 511]).
We begin with examples of curves found when working on $\mathbb{Q}(\sqrt{2})$ and taking the Gundlach invariants. The Jacobians of the following curves are $(3 + \sqrt{2})$-isogenous over $\mathbb{F}_{2331}$:

$$
Y^2 = 356X^6 + 116X^5 + 1589X^4 + 986X^3 + 178X^2 + 1094X + 1229,
$$
$$
Y^2 = 144X^6 + 2096X^5 + 387X^4 + 1562X^3 + 478X^2 + 486X + 1718
$$

while the Jacobians of the following ones are $(5 + 2\sqrt{2})$-isogenous over $\mathbb{F}_{3452703}$:

$$
Y^2 = 288618938X^5 + 208826828X^4 + 73681500X^3 + 329580565X^2 + 193693317X + 328425210,
$$
$$
Y^2 = 229859713X^5 + 180037958X^4 + 95105703X^3 + 68631100X^2 + 32660205X + 107566399
$$

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

$$
Y^2 = 3476666651X^5 + 2997006123X^4 + 2343918968X^3 + 1313289865X^2 + 1251164949X + 1521154595,
$$
$$
Y^2 = 2390845907X^5 + 2649299485X^4 + 3307186776X^3 + 2143442296X^2 + 1448110737X^2 + 918458873X + 1476608496
$$

We also give two examples of pairs of curves computed with the $\beta$-modular polynomials with the Gundlach invariants for $\mathbb{Q}(\sqrt{5})$. First example of curves for $(4 - (1 + \sqrt{5})/2)$-isogenies over $\mathbb{F}_{5631}$:

$$
Y^2 = 13477X^5 + 6136X^4 + 35146X^3 + 28148X^2 + 7150X + 19730,
$$
$$
Y^2 = 2953X^5 + 26725X^4 + 14100X^3 + 6565X^2 + 22149X + 19740
$$

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

$$
Y^2 = 3739712X^6 + 4881762X^5 + 6611129X^4 + 5775262X^3 + 521647X^2 + 2066678X + 350732,
$$
$$
Y^2 = 2707309X^6 + 1535264X^5 + 311501X^4 + 2965267X^3 + 3507011X^2 + 101110X + 5795310
$$

Finally, we give pairs of curves, whose Jacobians are $(7 + 2\sqrt{2})$-isogenous over $\mathbb{F}_{562789}$, computed using the $\beta$-modular polynomials with the $\tilde{b}_i$ for $\mathbb{Q}(\sqrt{5})$:

$$
Y^2 = 540913X^5 + 353915X^4 + 118050X^3 + 355166X^2 + 424096X + 379433,
$$
$$
Y^2 = 231396X^5 + 474300X^4 + 200176X^3 + 335056X^2 + 345222X + 464702
$$

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

$$
Y^2 = 2531476X^5 + 900554X^4 + 1248025X^3 + 440959X^2 + 912166X + 4367293,
$$
$$
Y^2 = 1772175X^5 + 3557482X^4 + 848889X^3 + 4562893X^2 + 146681X + 475016
$$

The motivated reader can check that the curves are indeed isogenous in verifying that the curves have the same zeta function (by a result of Tate [68, Theorem 1]).
References


Institut de Mathématiques de Bordeaux, 351 Cours de la Libération, 33400 Talence, France
E-mail adress: damien.robert@inria.fr

École Polytechnique Fédérale de Lausanne, EPFL SB MathGeom GR-JET, Switzerland
E-mail adress: enea.milio@epfl.ch
A Example of invariants on Hilbert and Humbert surfaces

A.1 Pullback of Siegel invariants

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

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

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

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

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

In practice we used pullback of theta functions or Gundlach invariants to compute the (symmetric) Hilbert modular polynomials. The reader interested in computing them with pullback of Igusa invariants is advised to use a variant defined by Streng in [66] to get smaller coefficients.

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

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

$$\phi_0 : \mathcal{H}_1^2 \to \mathcal{H}_1^2 \quad \gamma \mapsto \frac{\epsilon}{\sqrt{\Delta_K}} \gamma$$

and

$$\phi_0 : \text{SL}_2(\mathcal{O}_K) \to \text{SL}_2(\mathcal{O}_K \oplus \partial_K) \quad \alpha \gamma \alpha^{-1} \mapsto \alpha \gamma \alpha^{-1}.$$

38
are group isomorphisms which induce a commutative diagram similar as the one in Equation (5). Note that when $\epsilon > 0$ has norm $-1$, then $\tau < 0$ so that $\sqrt{\Delta_K}$ is totally positive and $\phi_0(\tau) \in H^1$.

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

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

Let $g$ be a holomorphic Hilbert modular form for $SL_2(\mathcal{O}_K \oplus a)$ of weight $k$. Then it has a Fourier expansion

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

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

**Corollary A.3.** Let $g$ be a holomorphic Hilbert modular form for $SL_2(\mathcal{O}_K)$ of weight $k$. Then it has a Fourier expansion

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

**Proof.** See [46, Proposition 3.2]. By Proposition A.2 the Fourier coefficients are indexed by $\partial_K^{-1,++}$, but if $v \in \partial_K^{-1,++}$, then $v = \frac{\epsilon}{\sqrt{D}}t$ with $t = ae_1 + be_2 \in \mathcal{O}_K^{++}$.  

We denote by $A_\mathbb{Z}(SL_2(\mathcal{O}_K))_k$ the $\mathbb{Z}$-module of symmetric Hilbert modular forms of even weight $k$ with rational integral Fourier coefficients and put $A_\mathbb{Z}(SL_2(\mathcal{O}_K)) = \bigoplus A_\mathbb{Z}(SL_2(\mathcal{O}_K))_k$.

Define the Hilbert Eisenstein series of even weight $k \geq 2$:

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

where

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

and $\kappa_k = \zeta_K(k)^{-1}(2\pi)^{2k}((k - 1)!)^{-2}\Delta_K^{1/2-k}$ (by [56, Equation (1.5)])

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

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

- If $K = \mathbb{Q}(\sqrt{3})$, let $\epsilon = \frac{1+\sqrt{3}}{2}$. 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 $\kappa_{10} = 2^{5} \cdot 3 \cdot 5^{2} \cdot 11 \cdot 412751^{-1}$.

**Proof.** See [31, 32]. See also [56, Lemma 1.1].

The Hilbert Eisenstein series are symmetric Hilbert modular forms for $SL_2(\mathcal{O}_K)$ with coefficients in $\mathbb{Q}$. We focus now on the cases $D = 2, 5$ and we fix the basis $\{1, \overline{\epsilon}\}$, which gives a nice expression of $q_1$ and $q_2$. We have
Theorem A.5 (Nagaoka). In the case $K = \mathbb{Q}(\sqrt{2})$, we put

$$F_4 = 2^{-6} \cdot 3^{-2} \cdot 11(G_2^2 - G_4) \quad \text{and} \quad F_6 = \frac{-5 \cdot 7^2}{2^8 3^3 13} G_2^3 + \frac{11 \cdot 59}{2^8 3^2 5 \cdot 13} G_2 G_4 - \frac{19^2}{27 3^5 \cdot 13} G_6.$$  

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

Proof. See [56, Theorem 1]. See also [32, Page 119].

Theorem A.6 (Gundlach). In the case $K = \mathbb{Q}(\sqrt{2})$, the field of symmetric meromorphic Hilbert modular functions for $SL_2(O_K)$ are rational functions of

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

Proof. See [32, Page 119]. See also [53, Lemma 6] or Appendix A.3.

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

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

$$F_6 = \frac{67}{2^3 3^5 7^2} (G_2^2 - G_6),$$

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

and

$$F_{12} = 2^{-2} (F_6^2 - G_2 F_{10}).$$

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

Proof. See [56, Theorem 2]. See also [31, Satz 5].

Theorem A.9 (Gundlach). In the case $K = \mathbb{Q}(\sqrt{5})$, the field of symmetric meromorphic Hilbert modular functions for $SL_2(O_K)$ are rational functions of

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

Proof. See [31, Satz 6]. See also [54, Page 249] or the proof in Appendix A.3.

Note that it is usual to take the invariants $\frac{G_2^3}{F_{10}}$ and $\frac{F_6}{G_2^2}$. 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.

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

40
A.3 Gundlach and pullbacks of the Igusa invariants

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

\begin{equation}
\phi_1 := \phi_{1, \varepsilon} \quad \text{and} \quad \phi_\varepsilon := \phi_1 \circ \phi_0,
\end{equation}

where $\phi_0$ denote the isomorphisms of Equation (25). The map $\phi_\varepsilon$ satisfies similar equalities as in Proposition 2.3 between the action of $\text{SL}_2(\mathcal{O}_K)$ on $\mathcal{H}_2$ and the action of $\text{Sp}_4(\mathbb{Z})$ on $\mathcal{H}_2$. It also maps to the Humbert surface and Proposition 2.8 apply with $\phi_\varepsilon$ instead of $\phi_{e_1, e_2}$.

For a basis $\{e_1, e_2\}$, we give in Proposition A.11 the relation between the Fourier coefficients of a Siegel modular form $f$ and the coefficients of its pullback $\phi^\ast_{e_1, e_2} f$, which is a symmetric Hilbert modular form. Recall Equation (6) for the definition of $\phi_{e_1, e_2}$.

Proposition A.11. Let

\begin{equation}
f(\Omega) = a_f(0) + \sum_{T \in \text{Sym}_2(\mathbb{Z})^\vee,++} a_f(T)q^T
\end{equation}

be a holomorphic Siegel modular form for $\text{Sp}_4(\mathbb{Z})$ of weight $k$. Then its pullback $g = \phi^\ast_{e_1, e_2} f$ is a symmetric Hilbert modular form with the following Fourier expansion:

\begin{equation}
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},
\end{equation}

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

\begin{equation}
a_g(t) = \sum_{\substack{T \in \text{Sym}_2(\mathbb{Z})^\vee,++ \\\ Q_T(e_1, e_2) = t}} a_f(T).
\end{equation}

Here, $Q_T(x_1, x_2) = (x_1, x_2)T(\frac{x_1}{x_2})$ is the positive definite quadratic form associated to $T$ and

\begin{equation}
\text{Sym}_2(\mathbb{Z})^\vee = \left\{ T = \left( \begin{array}{cc} m_1 & \frac{1}{2}m \\ \frac{1}{2}m & m_2 \end{array} \right) : m_1, m \in \mathbb{Z} \right\}
\end{equation}

is the dual of $\text{Sym}_2(\mathbb{Z})$. Finally, $q^T = e^{2\pi i \text{tr}(T\Omega)}$.

Proof. See [46, Proposition 3.2].

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

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

\begin{align*}
\phi_\varepsilon^\ast \psi_4 &= G_2^2; \\
\phi_\varepsilon^\ast \psi_6 &= -\frac{42}{25}G_2^3 + \frac{67}{25}G_6 = G_2^3 - 2^3 3^3 F_6; \\
-4\phi_\varepsilon^\ast \chi_{10} &= F_{10}; \\
12\phi_\varepsilon^\ast \chi_{12} &= 3F_8^2 - 2G_2 F_{10}.
\end{align*}

Proof. See [58, Theorem 1].
Corollary A.13 (Lauter-Yang). One has

\[
\begin{align*}
\phi^*_1 &= 8J_1(3J_2^2/J_1 - 2)^5; \\
\phi^*_2 &= \frac{1}{2}J_1(3J_2^2/J_1 - 2)^3; \\
\phi^*_3 &= 2^{-3}J_1(3J_2^2/J_1 - 2)^2(4J_2^2/J_1 + 2^53^2J_2/J_1 - 3).
\end{align*}
\]

Proof. See [46, Proposition 4.5].

We did not find in the literature a similar result as Theorem A.12 for \( \mathbb{Q}(\sqrt{2}) \). Using Proposition A.11 and comparing the different Fourier series (as done in [58] in the case \( D = 5 \)) we have found

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

\[
\begin{align*}
\phi^*_4 &= G_2^2 + 144F_4; \\
\phi^*_6 &= G_2^3 - 648F_4G_2 - 1728F_6; \\
\phi^*_10 &= -\frac{1}{4}F_4F_6; \\
\phi^*_12 &= \frac{1}{12}G_2F_4F_6 + F_4^3 + F_6^2.
\end{align*}
\]

Corollary A.15. One has

\[
\begin{align*}
\phi^*_1 &= 8J_1^3/J_2(1 + 12/J_2 + 12J_2/J_1)^5; \\
\phi^*_2 &= J_1^2/J_2(1 + 144)(1 + 12/J_2 + 12J_2/J_1)^3; \\
\phi^*_3 &= 1/8(1 + 12/J_2 + 12J_2/J_1)^2(3J_1^3/J_2 + 16J_1^2/J_2 + 2304J_1^3/J_2^2 + 408J_1^2/J_2 + 2880J_1).
\end{align*}
\]

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

A.4 Other invariants

By Müller [54], non-symmetric Gundlach invariants for \( \mathbb{Q}(\sqrt{5}) \) can be obtained considering the Hilbert modular forms

\[
F_{15}^2 = 16(5^5F_{10}^3 - 5^3G_2^2F_6F_{10}/2 + G_2^2F_{10}/2^4 + 3^25^2G_2F_6^3F_{10}/2 - G_2^4F_6^2F_{10}/2^3 - 2 \cdot 3^3F_6^3 + G_2^3F_6^4/2^4),
\]

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

\[
J_3^2 = (J_1^3 + (-2J_2^2 - 1000J_2 + 50000)J_2^2 + (J_2^2 + 1800J_2^2)J_1 - 864J_2^2)/(16J_1^2).
\]

Müller gives an expression of \( F_5 \) and of \( F_{15} \) in terms of theta constants so \( J_3 \) can be efficiently evaluated at \( \tau \in \mathcal{H}^2 \). The polynomials obtained are smaller than the symmetric ones with \( J_1 \) and \( J_2 \) only, as they are not symmetric and thus parameterize only \( \beta \)-isogenies. We refer to Martindale [50] for more details on the polynomials coming from these invariants.

Similarly for \( \mathbb{Q}(\sqrt{2}) \), see the work of Müller [53].

In fact in these two cases the Hilbert surface is rational (that is birational to \( \mathbb{P}^2 \)):
Theorem A.16. The Hilbert modular surface is rational for $D = 2, 3, 5, 13, 17$.

Proof. See [33, Theorem 3].

The paper [18] of Elkies and Kumar allows to get the corresponding birational isomorphisms. For instance, for $\mathbb{Q}(\sqrt{5})$, they give an explicit birational isomorphism between the Humbert surface $H_5$ and $\mathbb{P}^2$ (different from the one induced by the Gundlach invariants), and show that a birational model over $\mathbb{Q}$ of the non symmetric Hilbert modular surface is given by the double cover of $\mathbb{P}^2$

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

As this surface is also rational, a parametrization is obtained, given by the modular functions $m$ and $n$. We have by [18, Section 6]

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

and

$$g = (m^2 - 5n^2 - 9)/30, \quad k = 3m(10g + 3)(15g + 2)/6250,$$

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

Using these equations, [18, Corollary 15] (linking the Igusa-Clebsh invariants with $g$ and $h$) and Theorem A.12, we have found the relations

$$(27) \quad g = -J_1/(6J_2^2), \quad h = J_1^2/J_2^2 \quad \text{and} \quad z = -F_3^2F_{15}/(2F_6^2)$$

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

More generally, equations for Humbert and Hilbert surfaces are given in [18] for every quadratic field $\mathbb{Q}(\sqrt{\Delta})$ for all thirty fundamental discriminants $\Delta$ with $1 < \Delta < 100$. We can then use their results to get non symmetric invariants for all these fields. Furthermore, the equation of the Humbert surface for these fields is always rational, so we only need two symmetric invariants (like the Gundlach case for $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{2})$) and don’t need to take the pullback of the Igusa invariants for these fields. The difficulty resides in the optimization of these invariants: for instance for computing modular polynomials it is better if they have the same denominator.

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

This is a complement to Section 2.5.

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

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

43
Proof. We do the proof for \( \Gamma(2,4) \) as the other one is similar. Note that \( \tilde{\Gamma}(1)/\tilde{\Gamma}(4) \simeq \text{SL}_2(\mathcal{O}_K/4\mathcal{O}_K) \). 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 \( D \equiv 1 \text{ mod } 8 \);
- \( \mathbb{Z}/4\mathbb{Z}[X]/(X^2 + X + 1) \) when 2 is inert, namely when \( D \equiv 5 \text{ mod } 8 \);
- \( \mathbb{Z}/4\mathbb{Z}[X]/(X^2 - D) \) when 2 is ramified, namely when \( D \equiv 2,3 \text{ mod } 4 \).

The cardinality of \( \text{SL}_2(\mathcal{O}_K/4\mathcal{O}_K) \) 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 \( D \equiv 1 \text{ mod } 4 \) and 16 when \( D \equiv 2,3 \text{ mod } 4 \). As these two sets are normal subgroups of \( \tilde{\Gamma}(1) \), the third isomorphism theorem of groups gives us the desired results. \( \square \)

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

\[
\begin{align*}
10 & \text{ if } D \equiv 1 \text{ mod } 8 \\
6 & \text{ if } D \equiv 5 \text{ mod } 8 \quad \text{and} \quad 10 & \text{ if } D \equiv 1 \text{ mod } 8 \\
15 & \text{ if } D \equiv 2,3 \text{ mod } 4 & 6 & \text{ if } D \equiv 5 \text{ mod } 8 \\
& & 60 & \text{ if } D \equiv 2,3 \text{ mod } 4
\end{align*}
\]

Proof. The numbers for \( \Gamma(2) \) are due to Besser and the others to Runge. See [61, Page 293]. An heuristic argument for \( \Gamma(2,4) \) is that given \( P(b_1,b_2,b_3) \), the Humbert component \( H^\Delta_{2,K} \) which is the image of \( \phi_{1,\omega} \) and \( \Omega = \phi_{1,\omega}(\tau) \in \mathcal{H}_2 \), then for any \( \gamma \in \Gamma(2,4)\backslash\text{Sp}_4(\mathbb{Z}) \), we have that \( P(b_1(\gamma\Omega)) = 0 \) only for the matrices \( \gamma \) which come from the image of \( \phi_{1,\omega}((\Gamma(2,4)\backslash\Gamma(1)) \) and of \( \phi_{1,\omega}(\Gamma(2,4)\sigma\backslash\Gamma(1)) \) in \( \Gamma(2,4)\backslash\text{Sp}_4(\mathbb{Z}) \). The number of components corresponds to the number

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

where \( v(D) \) is 1 if \( D \equiv 2, 3 \text{ mod } 4 \) and \( \frac{1}{2} \) if \( D \equiv 1 \text{ mod } 4 \). This argument works also for \( \Gamma(2) \).

(Recall that \( |\Gamma(2,4)\backslash\text{Sp}_4(\mathbb{Z})| = 11520 \) and \( |\Gamma(2)\backslash\text{Sp}_4(\mathbb{Z})| = 720 \).)

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

The same is true for the map \( H^\Delta_{2,K} \simeq \mathcal{G}\backslash\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma \backslash\mathcal{H}_2^\Delta \) and the action of \( \mathcal{G}\backslash\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma \) on the fibers, where \( \mathcal{G} = \Gamma(2) \) (resp. \( \tilde{\Gamma}(2,4) \) when \( D \equiv 1 \text{ mod } 4 \) and \( \tilde{\Gamma}(2)\backslash\Gamma(2)\sigma \) (resp. \( \tilde{\Gamma}(2,4) \cup \tilde{\Gamma}(2,4)\sigma \) when \( D \equiv 2,3 \text{ mod } 4 \). 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 \( H^\Delta_{2,K} \), then the action of \( \mathcal{G}\backslash\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma \) permutes the fibers. Since this quotient is isomorphic to \( \Gamma(2)\backslash\phi_{1,\omega}(\Gamma(1) \cup \tilde{\Gamma}(1)\sigma)\Gamma(2) \) (resp. to \( \Gamma(2,4)\backslash\phi_{1,\omega}(\Gamma(1) \cup \tilde{\Gamma}(1)\sigma)\Gamma(2,4) \) (resp. \( \Gamma(2)\backslash\phi_{1,\omega}(\Gamma(1) \cup \tilde{\Gamma}(1)\sigma)\)\Gamma(2)\backslash\text{Sp}_4(\mathbb{Z}) \) (resp. \( \Gamma(2,4)\backslash\phi_{1,\omega}(\Gamma(1) \cup \tilde{\Gamma}(1)\sigma)\Gamma(2,4)\backslash\text{Sp}_4(\mathbb{Z}) \)), which is not compatible with \( \mathcal{O}_K \), permutes the components. \( \square \)
We give the equations of the Humbert component corresponding to the image of \( \phi_{1,\omega} \) for \( \Gamma(2,4) \) and \( D = 2, 3, 5 \)

\[
\begin{align*}
    b_1 - \frac{1}{2}(b_2^2 + b_3^2) &= 0; \\
    -b_1^2 - b_1^3 - 4b_3^2 - 2b_1b_2 + 4b_1b_2b_3 &= 0; \\
    \frac{1}{2}(\sum_ib_i^3 + \sum_i\sum_j\neq_i(b_ib_j)^4) + b_1b_2b_3(1 + \sum_ib_i^3 - b_1b_2b_3) &= 0
\end{align*}
\]

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

\[
\begin{align*}
    \left((16r_3^2 - 16r_3)r_2^2 + (-16r_3^2 + 16r_3)r_22 + ((-16r_3^2 + 16r_3)r_2^3 + (-16r_3^2 + 16r_3)r_2^2 +
    
    (16r_3^2 - 16r_3)r_2^2 + (-r_2^2 + (16r_3^2 - 16r_3 + 2)r_2^3 + (-14r_3^2 + 14r_3 - 1)r_2^2 +
    
    (-16r_3^2 + 14r_3^2 + 2r_3)r_2 + (-r_2^2 + 2r_3^2 - r_3^2)r_2^2 + (2r_3r_2^4 + (-16r_3^2 + 14r_3^2 - 2r_3)r_2^2 +
    
    (14r_3^2 - 12r_2^2)r_2^2 + (2r_3^2 - 2r_3^2)r_22r_1 + (-r_2^2r_2^4 + 2r_3^2r_2^2 - r_3^2r_2^2) = 0.
\end{align*}
\]

These equations have been computed by Gruenewald in [30], where he gives equations for components of Humbert surfaces for many discriminants and many model.

### B Examples of Hilbert modular polynomials

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

#### B.1 Modular polynomials in Gundlach invariants

**Evaluation and inversion:** We first illustrate Theorem 3.4 for the Gundlach invariants \( J_1, J_2 \) defined for \( Q(\sqrt{2}) \) and \( Q(\sqrt{3}) \) in Definition A.7 and A.10. The only small difference is that we use the map \( \phi_{1,\omega} \) defined in Equation (26) rather than the map \( \phi_{1,\omega} \) (Equation (6)) to map Hilbert matrices \( \tau \in H^2_1 \) to Siegel matrices \( \Omega \in H_2 \).

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 A.13 and A.15). The expression is easier than the method outlined in Theorem 3.4 because the Gundlach invariants are expressed in terms of symmetric Hilbert modular forms whose relation to the pullbacks of the Siegel modular form defining the Igusa invariants are very simple (see Theorems A.12 and A.14).

We outline the algorithm (Algorithm B.1) to find \( \tau \in (SL_2(O_K) \cup SL_2(O_K)\sigma)\setminus H^2_1 \) from the values \( J_1(\tau) \) and \( J_2(\tau) \) at some precision \( N \).

**Algorithm B.1:** \( \tau \in (SL_2(O_K) \cup SL_2(O_K)\sigma)\setminus H^2_1 \) from \( (J_1(\tau), J_2(\tau)) \) at precision \( N \)

**Data:** The values \( J_1(\tau) \) and \( J_2(\tau) \), the working precision \( N \)

**Result:** \( \tau \) modulo \( SL_2(O_K) \cup SL_2(O_K)\sigma \) at precision \( N \)

1. Deduce \( j_1(\Omega), j_2(\Omega), j_3(\Omega) \) from \( J_1(\tau), J_2(\tau) \), where \( \Omega \in H_2 \) such that \( \Omega = \phi_{1,\omega}(\tau) \);
2. Deduce a period matrix \( \Omega' \) at precision \( N \) equivalent to \( \Omega \) modulo \( Sp_4(Z) \), up to the precision, from the three Igusa invariants;
3. Find some \( \gamma \in Sp_4(Z) \) such that \( \gamma\Omega' \) satisfies Equation (11) and deduce \( \tau \);
The first step can be done using Corollary A.13 or A.15. The second is explained in [16, 51] and can be done in $O(N)$. For the third step, remark that for $D = 5$, if $\tau \in \mathcal{H}_2$, then $\phi_{\tau}(\tau) = \begin{pmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{pmatrix}$ satisfies 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 $H$. Thus by Humbert’s Lemma we know there exists a matrix $\gamma \in \text{Sp}_4(\mathbb{Z})$ such that $\Omega'' = \gamma \Omega'$, $\Omega'' = \begin{pmatrix} \alpha' & \Omega_2' \\ \Omega_2' & \Omega_3' \end{pmatrix}$ satisfies $\Omega_1'' + \Omega_2'' - \Omega_3'' = 0$ (see Remark 2.5 for the computation of $\gamma$). We have then $\tau^* = (\frac{1}{\sqrt{\Delta_K}})^{-1} R^{-1} \Omega'' R^{-1}$ (see Section 2.3 for the notations). For $D = 2$, $\phi_{\tau}(\tau)$ satisfies $\Omega_1 + 2\Omega_2 - \Omega_3 = 0$ and we can adapt the algorithm to find the matrix $\gamma$. Thus

**Corollary B.2.** Given $J_1(\tau)$ and $J_2(\tau)$, where $J_1$ and $J_2$ are the Gundlach invariants for $D = 2$ or $5$ evaluated at some $\tau \in \mathcal{H}_2$, then we can find an approximation of $\tau \in (SL_2(\mathbb{O}_K) \cup SL_2(\mathbb{O}_K) \sigma) \setminus \mathcal{H}_2$ at precision $N$ in $O(N)$ 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 $b_k$. Here, since the Gundlach invariants are invariants for the full modular group $SL_2(\mathbb{O}_K \oplus \mathbb{O}_K)$, we can also express them directly in terms of the (pullbacks of the) Igusa invariants $i_1, i_2, i_3$. Rather than doing an interpolation using Section 3.3, Equations (A.13) and (A.15) expressing the Igusa invariants in term of the Gundlach invariants are sufficiently simple to be inverted using a Gröbner basis.

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

$$J_2/J_1 = (1/6912\phi_1^{*}\phi_3^{*} \phi_4^{*})_2 - 1/2300\phi_1^{*}\phi_3^{*} \phi_4^{*} - 1/3359232\phi_1^{*}\phi_3^{*} \phi_4^{*} + 1/373248\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$+ 1/64\phi_1^{*}\phi_3^{*} \phi_4^{*} - 1/124416\phi_1^{*}\phi_3^{*} \phi_4^{*} + 1/124416\phi_1^{*}\phi_3^{*} \phi_4^{*} + 1/3359232\phi_1^{*}$$
$$+ 1/119744\phi_1^{*}\phi_3^{*} \phi_4^{*} + 1/1944\phi_1^{*}\phi_3^{*} \phi_4^{*} - 1/64\phi_1^{*}\phi_3^{*} \phi_4^{*};$$

$$J_1 = -(45349632\phi_1^{*}\phi_3^{*} \phi_4^{*} - 2584929024/5\phi_1^{*}\phi_3^{*} \phi_4^{*} - 499571546112/5\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$+ 1101960576/5\phi_1^{*}\phi_3^{*} \phi_4^{*} - 1410554953728/5\phi_1^{*}\phi_3^{*} \phi_4^{*} - 20815481088/5\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$+ 14693280768/5\phi_1^{*}\phi_3^{*} \phi_4^{*} - 186624\phi_1^{*}\phi_3^{*} \phi_4^{*} + 16236288/5\phi_1^{*}\phi_3^{*} \phi_4^{*} - 12380449536/5\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$- 23514624\phi_1^{*}\phi_3^{*} \phi_4^{*} - 1468674288/5\phi_1^{*}\phi_3^{*} \phi_4^{*} + 31972578951168/5\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$+ 90699264\phi_1^{*}\phi_3^{*} \phi_4^{*} - 65140211448/5\phi_1^{*}\phi_3^{*} \phi_4^{*} - 90275517038592/5\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$- 196515072\phi_1^{*}\phi_3^{*} \phi_4^{*} + 1279948013568/5\phi_1^{*}\phi_3^{*} \phi_4^{*} + 226748160\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$- 94036969152/5\phi_1^{*}\phi_3^{*} \phi_4^{*} - 544195584/5\phi_1^{*}\phi_3^{*} \phi_4^{*} + 192\phi_1^{*}\phi_3^{*} \phi_4^{*} - 22464/5\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$- 18289152/5\phi_1^{*}\phi_3^{*} \phi_4^{*} + 229824/5\phi_1^{*}\phi_3^{*} \phi_4^{*} + 265527104/5\phi_1^{*}\phi_3^{*} \phi_4^{*} + 30051689472/5\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$- 1342656/5\phi_1^{*}\phi_3^{*} \phi_4^{*} - 1482541056/5\phi_1^{*}\phi_3^{*} \phi_4^{*} - 171240210432/5\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$+ 979776\phi_1^{*}\phi_3^{*} \phi_4^{*} + 4212476928/5\phi_1^{*}\phi_3^{*} \phi_4^{*} + 243799621632/5\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$- 2286144\phi_1^{*}\phi_3^{*} \phi_4^{*} - 5976073728/5\phi_1^{*}\phi_3^{*} \phi_4^{*} + 16656192/5\phi_1^{*}\phi_3^{*} \phi_4^{*}$$
$$+ 3386105856/5\phi_1^{*}\phi_3^{*} \phi_4^{*} - 13856832/5\phi_1^{*}\phi_3^{*} \phi_4^{*} + 503884/5\phi_1^{*}\phi_3^{*} \phi_4^{*} - 320\phi_1^{*}$$
$$+ 5568\phi_1^{*} \phi_3^{*} \phi_4^{*} - 155520\phi_1^{*} \phi_3^{*} \phi_4^{*} + 4572288/5\phi_1^{*} \phi_3^{*} \phi_4^{*} + 3869835264/5\phi_1^{*} +$$
Proof. This is a corollary of Theorem 4.15. These polynomials depend only on linear in their size. Let Proposition B.5. Since we only have two invariants, this simplifies the definition of the modular polynomials:

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

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

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

$$
\Phi_\beta(X, J_1, J_2) = \prod_{\gamma \in \mathcal{C}_\beta} (X - J_{1,\beta}^\gamma)(X - J_{1,\beta}^{-\gamma}) \quad \text{and} \quad \Psi_\beta(X, J_1, J_2) = \sum_{\gamma \in \mathcal{C}_\beta} J_{2,\beta}^\gamma \frac{\Phi_\beta(X, J_1, J_2)}{X - J_{1,\beta}^\gamma} + \sum_{\gamma \in \mathcal{C}_\beta} J_{2,\beta}^{-\gamma} \frac{\Phi_\beta(X, J_1, J_2)}{X - J_{1,\beta}^{-\gamma}}
$$

lie in $\mathbb{Q}(J_1, J_2)[X]$. These polynomials depend only on $\ell$ 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 $\ell$ as $\mathbb{Q}(\sqrt{D})$ for $D = 2$ or $5$ has a fundamental unit of norm $-1$ (see the discussion in Remark 4.18). \(\square\)

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 $\beta$- or $\overline{\beta}$-isogenous points $z'$. Then $J_2(z') = \Psi_\beta(J_1(z'), J_1(z), J_2(z))/\Phi'_\beta(J_1(z'), J_1(z), J_2(z))$, where $\Phi'_\beta$ is the derivative of $\Phi_\beta$ with respect to the variable $X$. Thus, given $J_1(z)$ and $J_2(z)$, the $\beta$-modular polynomials allow one to compute all the Gundlach invariants at the isogenous points of $z$. 

47
Let $\mathcal{L}_\ell$ be the locus of the principally polarized abelian surfaces with real multiplication by $\mathcal{O}_K$ which are $\beta$- 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 B.6.** In the case where $D = 5$, the denominators of the modular polynomials $\Phi_\beta$ and $\Psi_\beta$ are divisible by a polynomial $L_\ell$ in $\mathbb{Q}[J_1, J_2]$ describing $\mathcal{L}_\ell$.

**Proof.** We adapt the proof of [5, Lemma 6.3]. Let $z \in \mathcal{H}_1^2$ which is $\beta$- or $\overline{\beta}$-isogenous to a product of elliptic curves and let $c_i$ be a coefficient of $\Phi_\beta$. The cusp form $\chi_{10}$ vanishes at products of elliptic curves and by Theorem A.12, we have $F_{10} = -4\phi_1^*\chi_{10}$ 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 $\gamma \in \Gamma^0(\beta) \setminus \Gamma(1)$ such that $J_{1,\beta}(z)$ or $J_{1,\overline{\beta}}(z)$ is infinite. The evaluation of $c_i$ at $z$ is a symmetric expression in the $J_{1,\beta}(z)$ and in the $J_{1,\overline{\beta}}(z)$. 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 $L_\ell$. The proof for $\Psi_\beta$ is similar. \hfill $\square$

If $D = 2$, the Gundlach invariants $J_1$ and $J_2$ have poles when $F_1(z) = 0$. Since by Theorem A.14, we have that $\phi_1^*\chi_{10} = -\frac{1}{2}F_3F_3$, the set of poles is a subset of the products of elliptic curves. We have thus to consider the subset $\mathcal{L}_\ell'$ of the surfaces $z$ such that $F_4(\frac{1}{2}\gamma \cdot z) = 0$ or $F_4(\frac{1}{2}\overline{\beta}\gamma \cdot z) = 0$ for some $\gamma \in C_\beta$.

**Proposition B.7.** In the case where $D = 2$, the denominators of the modular polynomials $\Phi_\beta$ and $\Psi_\beta$ are divisible by a polynomial $L_\ell'$ 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 $H_\beta$ of abelian surfaces which are $\beta$-isogenous to a product of elliptic curves (and which are not isomorphic to a product of elliptic curves).

### B.2 Modular polynomials in theta invariants

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

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

**Evaluation and inversion:** We now outline efficient procedures for the computation of the values $\tilde{b}_i(\tau)$ of Hilbert modular functions at any $\tau \in \mathcal{H}_1^4$ and for finding some $\tau \in \mathcal{H}_1^4$ from the $\tilde{b}_3(\tau)$. The first one is similar to Algorithm B.3, the third step being trivial as $\tilde{b}_i = \phi_{1,\omega}^*b_i$, and has the same complexity. For the second procedure, we also proceed as in Algorithm B.1, the first step being also trivial. For the second, it is possible to find $\Omega$ modulo $\Gamma(2,4)$ in $O(N)$ time (see [51]). The difficulty is in the third step. Indeed, we are able to find $\gamma$ such that $\phi_{1,\omega}(\tau) = \gamma\Omega$, but $\gamma$ is not necessarily in $\Gamma(2,4)$ so that we only find $\tau$ modulo $\tilde{\Gamma}(1) \cup \tilde{\Gamma}(1)\sigma$. 

48
A solution consists in computing beforehand all the classes of the quotient \( \Gamma(2,4) / \Gamma(1) \) and of \( \Gamma(2,4) \sigma \backslash \Gamma(1) \) and see how they are sent to the classes of \( \Gamma(2,4) \backslash \text{Sp}_{4}(\mathbb{Z}) \). It suffices to find in which class of \( \Gamma(2,4) \backslash \text{Sp}_{4}(\mathbb{Z}) \) the matrix \( \gamma \) belongs in to find a corresponding matrix \( \tilde{\gamma} \) in \( \Gamma(2,4) \backslash \Gamma(1) \) or in \( \Gamma(2,4) \sigma \backslash \Gamma(1) \). Then we have \( \phi_{1,\omega}(\tilde{\gamma}^{-1} \tau) = \phi_{1,\omega}(\tilde{\gamma}^{-1}) \phi_{1,\omega}(\tau) = \gamma^{-1} \gamma \Omega = \Omega \).

**Corollary B.8.** We can evaluate the three \( \tilde{b}_{i}(\tau) \) at precision \( N \) for \( \tau \in \mathcal{H}_{1}^{2} \) in \( \hat{O}(N) \) time and we can find \( \tau \) at precision \( N \) modulo \( \hat{\Gamma}(2,4) \), or modulo \( \hat{\Gamma}(2,4) \cup \hat{\Gamma}(2,4) \sigma \) according to the cases, from the values \( b_{i}(\tau) \) 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 (28) for the equations for \( D = 2, 3, 5 \) and to [30] for larger discriminants.

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

\[
\tilde{b}_{i,\beta} : \mathcal{H}_{1}^{2} \to \mathbb{C} \quad \tau \mapsto \tilde{b}_{i}(\frac{1}{\beta} \gamma \cdot \tau) \quad \text{and} \quad \tilde{b}_{i,\beta}^{\gamma} : \mathcal{H}_{1}^{2} \to \mathbb{C} \quad \tau \mapsto \tilde{b}_{i}(\frac{1}{\beta} \gamma \cdot \tau).
\]

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 \( \gamma_{\beta} \) is in \( \tilde{\Gamma}(2,4) \) (see Corollary 4.14). A simple calculation shows that this is always the case when \( D \equiv 1 \) mod 4. When \( D \equiv 2, 3 \) mod 4, this happens only when \( \beta \) is of the form \( a + b \omega \) with \( b \) even. If \( D \equiv 2 \) mod 4, this is equivalent to ask that \( \ell \equiv 1 \) mod 4 and else if \( D \equiv 3 \) mod 4, \( \ell \) must necessarily satisfy \( \ell \equiv 1 \) mod 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 \( \epsilon \). Thus

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

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

**Proposition B.10.** Let \( \ell \) be a prime number. Write \( \ell = \beta \) if \( \ell \) is inert and \( \ell = \beta \bar{\beta} \) if \( \ell \) is split with \( \beta \in \mathcal{O}_{K}^{+} \). Let \( C_{\beta} \) be a set of representatives of \( (\tilde{\Gamma}(2,4) \cap \tilde{\Gamma}^{0}(\beta)) \backslash \tilde{\Gamma}(2,4) \). If \( D \equiv 1 \) mod 4, then the polynomials

\[
\Phi_{\beta}(X, \tilde{b}_{1}, \tilde{b}_{2}, \tilde{b}_{3}) = \prod_{\gamma \in C_{\beta}} (X - \tilde{b}_{1,\beta}^{\gamma}), \quad \text{and} \quad \Psi_{k,\beta}(X, \tilde{b}_{1}, \tilde{b}_{2}, \tilde{b}_{3}) = \sum_{\gamma \in C_{\beta}} \tilde{b}_{k,\beta}^{\gamma} \frac{\Phi_{\beta}(X, \tilde{b}_{1}, \tilde{b}_{2}, \tilde{b}_{3})}{X - \tilde{b}_{1,\beta}^{\gamma}}
\]

49
for $k = 2, 3$ lie in $\mathbb{Q}(\tilde{b}_1, \tilde{b}_2, \tilde{b}_3)[X]$. If $D \equiv 2, 3 \pmod{4}$ and $\beta = a + b\omega$ with $b$ even, then

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

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

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 $D \equiv 1 \pmod{4}$ and $D \equiv 2, 3 \pmod{4}$ comes from Equations (8) and (9): in the first case, by Proposition 2.8, the map $\Gamma(2, 4) \setminus \mathcal{H}_4 \to \text{Sp}_d(\mathbb{Z}) \setminus \mathcal{H}_4$ is injective while in the second it is the map $(\Gamma(2, 4) \cup \Gamma(2, 4)\sigma) \setminus \mathcal{H}_4 \to \text{Sp}_d(\mathbb{Z}) \setminus \mathcal{H}_4$ 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 [45]).

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 $\tilde{b}_{3,\beta}^{\gamma\sigma}$ for any $\gamma \in \mathcal{C}_\beta$.

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

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

**$\beta$-modular polynomials:** As $\Phi_\beta$ is a minimal polynomial, it is the unique irreducible and monic polynomial which satisfies, for any $\tau \in \mathcal{H}_4$, $\Phi_\beta(\tilde{b}_1, \beta(\tau), \tilde{b}_2(\tau), \tilde{b}_3(\tau)) = 0$. We can look at what happen on $\sigma(\tau)$. The matrix $M_\sigma$ of Equation (8) acts as follows: $(b_1^{M_\sigma}, b_2^{M_\sigma}, b_3^{M_\sigma}) = (b_1, b_2, b_3)$ if $D \equiv 2, 3 \pmod{4}$ and $(b_1^{M_\sigma}, b_2^{M_\sigma}, b_3^{M_\sigma}) = (b_3, b_2, b_1)$ if $D \equiv 1 \pmod{4}$.

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

However $(b_1^{M_\beta}, b_2^{M_\beta}, b_3^{M_\beta}) = (b_3, b_2, b_1)$ if $D \equiv 1 \pmod{4}$. The irreducible and monic polynomial $\Phi_\beta(b_1^{M_\beta}, b_2^{M_\beta}, b_3^{M_\beta})$ has the same roots as $\Phi_\beta(\tilde{b}_1, \beta, \tilde{b}_2, \tilde{b}_3)$ and thus by unicity, these polynomials have to be equals. Thus, if $D \equiv 1 \pmod{4}$, $\Phi_\beta(b_3, b_3, b_3, b_3, b_3) = \Phi_\beta(\tilde{b}_1, \beta, \tilde{b}_1, \tilde{b}_1, \tilde{b}_1)$ and it is possible to obtain the value $\tilde{b}_{3,\beta}(\tau)$ for any $\tau \in \mathcal{H}_4$ using the $\beta$-modular polynomials. We have then, still acting by $\sigma$,

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

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

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

**Changing $\beta$ 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 $\ell$, differ by an even factor of $\epsilon$ (this always happens when $\epsilon$ 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 $\tau \in \mathcal{H}_4$, if we compute $\tilde{b}_{i,\beta}(\tau)$, for $i = 1, 2, 3$, from $b_i(\tau)$ and using the $\beta$-modular polynomials, then we have $\tilde{b}_{i,\beta'}(\tau) = \tilde{b}_{i,\beta}(\tau)$.
\( \tilde{b}_i \left( \left( \begin{array}{cc} e^{-n} & 0 \\ 0 & e^n \end{array} \right) \frac{1}{\beta} \right) \) and knowing how the matrix \( \left( \begin{array}{cc} e^{-n} & 0 \\ 0 & e^n \end{array} \right) \) 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 \( \beta' \)-modular polynomials.

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

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

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

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

**Symmetries:** We can proceed in the same way with matrices \( \gamma \in \tilde{\Gamma}(2, 4) \backslash \tilde{\Gamma}(1) \) having special properties. If \( \gamma \) permutes the \( \tilde{b}_i \) and the \( \tilde{b}_{i,\beta} \), this says that there are symmetries in the modular polynomials. In particular, if \( \gamma \) satisfies \( (\tilde{b}_1, \tilde{b}_2, \tilde{b}_3) = (\tilde{b}_1, \tilde{b}_3, \tilde{b}_2) \) and \( (\tilde{b}_1, \tilde{b}_2, \tilde{b}_3) = (\tilde{b}_1, \tilde{b}_3, \tilde{b}_2) \), 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 \( \beta \)-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 \( \gamma \) satisfies \( \tilde{b}_k = i^{\alpha_k} \tilde{b}_k \) and \( \tilde{b}_{k,\beta} = i^{\beta_k} \tilde{b}_{k,\beta} \), for \( k = 1, 2, 3 \) and \( \alpha_k, \beta_k \in \{0, 1, 2, 3\} \) (\( i \) is the imaginary unit), then the exponents of the \( \tilde{b}_k \) at each coefficient of the modular polynomials satisfy some relations modulo 4. As we compute the modular polynomials by evaluation/interpolation, this can be used to decrease the number of evaluations.

The existence of these matrices depend on \( D \) and \( \beta \). They can be searched before the computation of the polynomials. We give some examples of relations between the exponents in Section 5 (see Equation (24)). Similar arguments have already been used in [51, Sections 5.2 and 5.3] for the computation of \( \ell \)-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 \( D \equiv 2, 3 \mod 4 \), is \( \beta \)-isogenous to \( z' \) such that \( \phi_{1,\omega}(z') \) is isogenous to a product of elliptic curves by the 2-isogeny \( \phi_{1,\omega}(z') \to \phi_{1,\omega}(z')/2 \) and such that \( \theta_0(\phi_{1,\omega}(z')/2) = 0 \).

**Proposition B.14.** The denominators of the modular polynomials \( \Phi_\beta \) and \( \Psi_{k,\beta} \) are divisible by a polynomial \( L_\beta \) 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 $\Phi_\beta$. Then there is some $\gamma \in (\tilde{\Gamma}(2, 4) \cap \tilde{\Gamma}^0(\beta)) \backslash \tilde{\Gamma}(2, 4)$ such that $\tilde{b}_{1, \beta}^\gamma$, or $\tilde{b}_{1, \beta}^\sigma$ if $D \equiv 2, 3 \mod 4$, is infinite. Indeed, recall that $b_i = \frac{\theta_i}{\theta_0}(\Omega/2)$ and that by [16, Proposition 6.5 and Corollary 6.1], exactly one theta constant vanishes at $\Omega$ if and only if $\Omega$ is isomorphic to a product of elliptic curves. We conclude using the same arguments as in the proof of Theorem B.6.

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