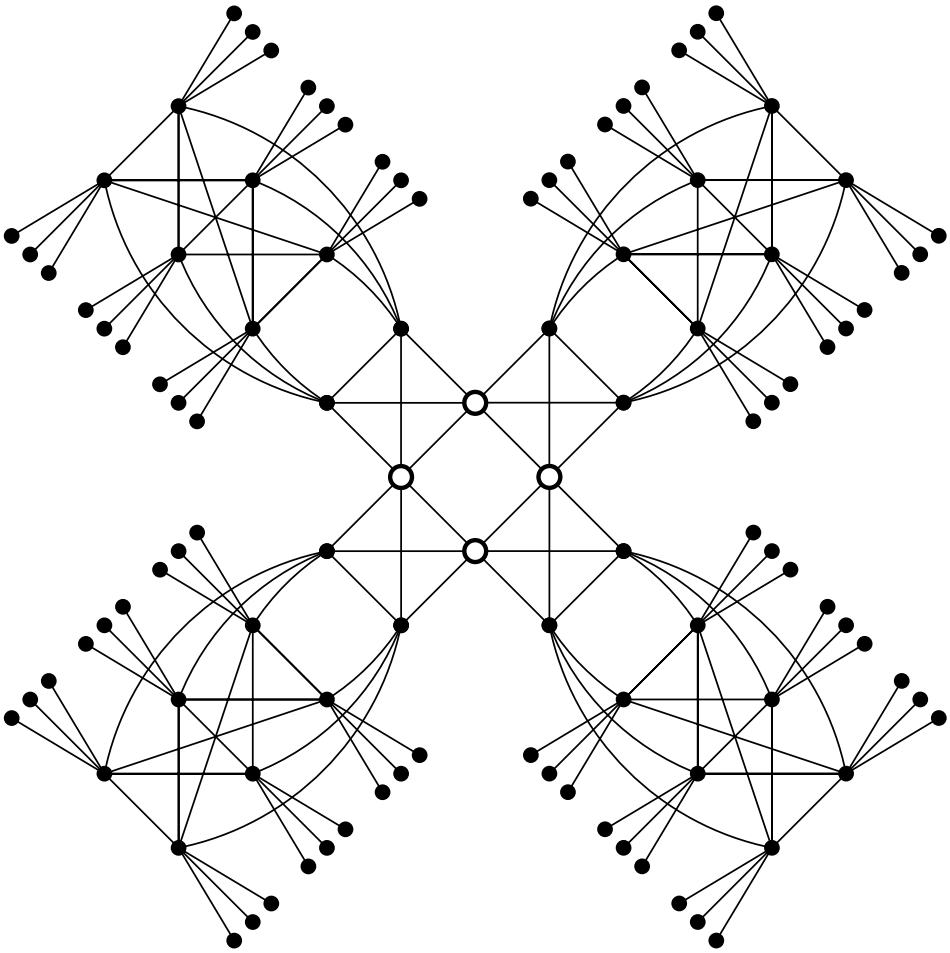
Explicit Algorithms for Humbert Surfaces

David Gruenewald



A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Pure Mathematics at the University of Sydney, December 2008.

Summary

In this work, we investigate methods for computing equations of Humbert surfaces – moduli spaces for principally polarized abelian surfaces having endomorphism ring isomorphic to a real quadratic order. Our main approach is to use Fourier expansions of modular forms and apply 'Runge's method' to find relations among them. We find equations of Humbert components in a number of different models including the Rosenhain model, the symmetric Satake model, Runge's model and level 1 models. We then take intersections of Humbert surfaces to produce equations describing Shimura curves. For small discriminants, we find parametrizations of Humbert components which allow us to construct rational points. Amongst these we search for modular Jacobian surfaces defined over the rationals. We reduce our Humbert equations modulo p to study 'congruence primes' – primes at which the reduction mod p of a modular Jacobian surface splits as a product of elliptic curves. In the final chapter, we compute $(3,3)$-isogeny relations which are used to improve the CRT-method to compute Igusa class polynomials; Humbert surfaces are shown to significantly improve this algorithm.

Statement

This thesis contains no material which has been accepted for the award of any other degree or diploma. All work in this thesis, except where duly attributed to another person, is believed to be original.

CONTENTS

Acknowledgements

First and foremost, I wish to thank my supervisor David Kohel for his encouragement, kindness, infinite patience and unwavering dedication to my doctoral endeavours. I shall cherish the many mathematical expeditions we went on, both abroad and in the Carslaw building.

I am indebted to the School of Mathematics and Statistics and the University of Sydney which has been a wonderful provider over the years. Also to Shona Yu for making the maths postgrads one big happy family - it's not the same without you.

To the number theory seminar postgrads who have contributed to my mathematical development: Hai-Trung Ho, Stephen Meagher, Ben Smith and Steve Enright-Ward. Also Ley Wilson who has helped me remove 80% of the grammatical errors (finding the remaining 20% has been left as an exercise for the reader).

Special thanks to the postdocs passing through Sydney who've helped me along the way: Claus Fieker, Martine Girard, Robert Carls, John Voight and Steve Donnelly. Also to the Magma group for their computer algebra software which I use intensively.

To Kristin Lauter for inviting me to Microsoft Research to do a summer internship this year. Together with Reinier Bröker we accomplished a great deal and I had a lot of fun at the same time. I thank Microsoft Research for its hospitality.

One of the best things that eventuated as a result of starting a PhD at Sydney University was getting invited to tutor at the National Mathematics Summer School (NMSS). I've met the most amazing people down there and hold them in high esteem.

Last but not least, to my family for their love which sustains me.

Introduction

Georges Humbert (1859–1921) obtained a doctorate in mathematics in 1885 for his thesis *"Sur les courbes de genre un"*. Since that time, the study of elliptic curves has grown immensely and with the help of modern computers, conjectures like Birch and Swinnerton-Dyer conjecture encourage further investigations both theoretical and computational. For higher genus curves on the other hand, less has been achieved in terms of explicit calculation. In relatively recent times more attention has been focused on computing with genus 2 curves, beginning in 1989 when hyperelliptic curve cryptography was proposed by Koblitz [**42**]. By virtue of the zeta function, all genus 2 curves over a finite field have complex multiplication by a quartic CM field and as a consequente, CM-points have been intensely studied. Less attention has been given to genus 2 Jacobians having different endomorphism algebras, for example indefinite $\mathbb{Q}$-quaternion algebras or real quadratic fields. Humbert [**29**] found relations (defining a surface) in terms of hyperelliptic roots which determine when a principally polarized abelian surface has endomorphism ring isomorphic to a quadratic order of discriminant Δ for values $\Delta = 1, 4, 5, 8$. Humbert surface equations were later studied by Hecke [**26**] and Franke [**15**] in their dissertations. By the early 1980's, the theory of Humbert surfaces was well and truly established [**72**], yet it would take another 17 years before anybody computed a new Humbert surface explicitly (admittedly, many equations were calculated for Hilbert modular surfaces which are closely related). In 1999, Runge [**64**] computed models of components of Humbert surfaces, which included models for five new discriminants. His motivation was to compute Shimura curves (quaternionic multiplication) in the intersection of Humbert surfaces. Our motivation is somewhat broader, for we also apply the results to explicit CM-theory, endomorphism computations and the investigation of modular abelian surfaces. The fact that every quartic CM field contains a real quadratic field means that a CM point can be identified as a point on a Humbert surface. This can be used to great effect in speeding up the CRT method for computing Igusa class polynomials and speeding up endomorphism ring computations (Section 7.9).

Chapter 1 provides reference to the background material on abelian varieties and moduli spaces. Here we describe classical theta functions and Satake compactifications as well as provide some examples of moduli spaces of abelian surfaces having a real multiplication (RM) structure (Hilbert modular surfaces).

Chapter 2 is an overview of Humbert surfaces. The main result of Section 2.1 is Humbert's Lemma (Theorem 2.9) which says that the locus H_Δ of principally polarized abelian surfaces having real multiplication by a quadratic order of discriminant Δ is a two dimensional irreducible subvariety (called a *Humbert surface*) of the Siegel modular threefold $\mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z})$ and can be described in $\mathcal{H}_2$ by a single linear relation:

$$\tau_3 = k\tau_1 + \ell\tau_2$$

where $\tau = \left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{smallmatrix}\right) \in \mathcal{H}_2$ and $\Delta = 4k + \ell$. In Section 2.2 we see that Humbert surfaces are degree 2 quotients of Hilbert modular surfaces.

We then detail our Humbert surface computations in Chapter 3. The method used to find Humbert relations involves Fourier expansions of modular forms. These expansions are constructed using theta constants for which explicit expansions are known. Finding an algebraic relation between these modular forms reduces to searching for a linear relation between monomials, each represented as a power series. This algorithm ("Runge's method" [**64**]) is applied to various models of moduli spaces with level structure, for example the Rosenhain model which has level 2 structure. Another level 2 model which we investigate is the *symmetric Satake* model $X[2]$ in $\mathbb{P}^5$ due to van der Geer [**72**]. The projection map down to level 1 is a Galois cover by the group S_6, where S_6 acts by permutations on the coordinate functions of $\mathbb{P}^5$. Geometric properties (stabilizer of a component in S_6, number of components, degree) are known for Humbert components in this model and assist with their computation.

Chapter 4 summarizes the arithmetic theory of quaternion algebras and paves the way for Chapter 5 where we identify 'Shimura curves' – curves appearing in the intersection of Humbert surfaces. Technically speaking these are quotients of Shimura curves by Atkin-Lehner subgroups, the precise groups determined by Victor Rotger in his PhD thesis [**60**]. This method was given by Hashimoto and Murabayashi in [**25**] who found Shimura curves of discriminant 6 and 10 using Humbert's original equations for H_5 and H_8. At the time, the only other known equations of Humbert surfaces were H_1 and H_4 which limited the method. Using the symmetric Satake model, Besser [**6**] computed Shimura curves of discriminants 6, 10 and 15 by hand, where the discriminant 15 curve appears in the intersection of two distinct Humbert components of discriminant 8. Using yet another model, Runge [**64**] extended the list of discriminants of Humbert components but

did not publish any Shimura curve equations. We provide algorithms to automate the process and produce some equations for larger examples.

In Chapter 6 we parametrize some of our Humbert components and find 2-parameter families of points on level 1 Humbert surfaces. Using these we can find rational points on level 1 Humbert surfaces. We also find rational points for which the RM is defined over $\mathbb{Q}$. The recently proven generalized Shimura-Taniyama conjecture implies that these abelian surfaces are modular, i.e. isogenous to a 2-dimensional factor of $J_0(N)$ for some N. We then work in the other direction and study the reduction of modular Jacobians at primes p using Humbert surfaces mod p.

The final chapter is joint work with Kristin Lauter and Reinier Bröker at Microsoft Research and is essentially self contained. Using the Fourier expansions method of Chapter 3, we compute $(3,3)$-isogeny relations. We use them to make the Galois action on the CM-moduli explicit, improving the CRT-method to compute Igusa class polynomials. The last section demonstrates that Humbert surfaces can be used to speed up parts of the algorithms even further.

The cover picture is a connected component of the $(3,3)$-isogeny graph for the quartic CM field $K = \mathbb{Q}[X]/(X^4 + 22X^2 + 73)$. The white dots represent principally polarized abelian surfaces over $\mathbb{F}_{1609}$ whose endomorphism ring is isomorphic to the ring of integers of K. See Example 7.17 for the details.

Many of the computations are too large to include in this thesis. For convenience, the data has been made accessible online at

http://echidna.maths.usyd.edu.au/∼davidg/thesis.html .

CHAPTER 1

Abelian Varieties and their Moduli Spaces

This chapter is divided into two parts. The first part provides reference for the theory of complex abelian varieties and the classification of their endomorphism algebras. The second part describes moduli spaces of abelian varieties. Our exposition is based on Birkenhake-Lange [**7**], and Rosen [**59**].

Definition 1.1. *An* abelian variety A *defined over a field* k *is a projective group variety over* k.

It can be shown that the group law on an abelian variety is necessarily commutative. Considered as a variety over the complex numbers, an abelian variety is analytically isomorphic to a complex torus. The converse is not true: in dimensions greater than one, not all complex tori are abelian varieties. We undertake a study of the precise conditions as to when a complex torus is an abelian variety.

1.1. Complex tori

Definition 1.2. *A* complex torus of dimension g *is a quotient* V/Λ *where* V *is a complex vector space of dimension* g *and* Λ *is a lattice (discrete free* $\mathbb{Z}$*-module) of rank* $2g$.

Let us study complex analytic morphisms between complex tori. Since translations are clearly morphisms, we can compose an arbitrary morphism with a translation so it suffices to restrict our attention to homomorphisms - morphisms that send 0 to 0.

Lemma 1.3. *Let* $T_1 = V_1/\Lambda_1$ *and* $T_2 = V_2/\Lambda_2$ *be complex tori and let* $\alpha : T_1 \longrightarrow T_2$ *be a holomorphic map with* $\alpha(0) = 0$. *Then* α *is a homomorphism that is induced by a* $\mathbb{C}$*-linear map* $\tilde{\alpha} : V_1 \longrightarrow V_2$ *satisfying* $\tilde{\alpha}(\Lambda_1) \subseteq \Lambda_2$. *We call* $\tilde{\alpha}$ *the* analytic representation *of* α.

Proof. By the universal property of the projection map $\pi_2 : V_2 \longrightarrow T_2$, the map $\alpha \circ \pi_1$ lifts to a holomorphic map $\tilde{\alpha} : V_1 \longrightarrow V_2$ which makes the following diagram commutative.

$$\begin{array}{ccc} V_1 & \xrightarrow{\tilde{\alpha}} & V_2 \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ T_1 & \xrightarrow{\alpha} & T_2 \end{array}$$

We necessarily have $\tilde{\alpha}(\Lambda_1) \subseteq \Lambda_2$ and $\tilde{\alpha}$ is uniquely determined mod Λ_2, so if we specify $\tilde{\alpha}(0) = 0$ then $\tilde{\alpha}$ is unique. From the commutative diagram $\tilde{\alpha}(v + \lambda) \equiv \tilde{\alpha}(v)$ mod Λ_2 if λ is in Λ_1 so $\frac{\partial \tilde{\alpha}}{\partial v_i}(v + \lambda) = \frac{\partial \tilde{\alpha}}{\partial v_i}(v)$ for all λ in Λ_1. So for $i = 1, \ldots, g$ we have that $\frac{\partial \tilde{\alpha}}{\partial v_i}$ is a holomorphic function on the compact complex manifold T_1, hence by Liouville's Theorem all the partial derivatives are constant, so $\tilde{\alpha}$ is linear. Hence $\tilde{\alpha}$ is a homomorphism and therefore α is as well. □

Proposition 1.4. *If $\alpha : T_1 \longrightarrow T_2$ is a homomorphism then $\alpha(T_1)$ is a subtorus of T_2 and $\ker \alpha$ is a closed subgroup of T_1. The connected component $(\ker \alpha)^0$ is a subtorus and is of finite index in $\ker \alpha$.*

Proof. See Birkenhake-Lange [**7**, Proposition 1.2.4]. □

If $f : T_1 \longrightarrow T_2$ is a nonzero homomorphism, then nf is nonzero for all nonzero integers n. Hence there is a natural embedding

$$\mathrm{Hom}(T_1, T_2) \longrightarrow \mathrm{Hom}(T_1, T_2) \otimes \mathbb{Q} =: \mathrm{Hom}_0(T_1, T_2)\,.$$

Definition 1.5. *A homomorphism $\alpha : T_1 \longrightarrow T_2$ of complex tori is called an* isogeny *if it is surjective and has finite kernel. The cardinality of the kernel is called the* degree *of α.*

Example 1.6. (multiplication by n). Let $T = V/\Lambda$ be a complex torus of dimension g. The map $[n]_T : T \longrightarrow T,\ x \mapsto nx$ is an isogeny with kernel equal to $(\frac{1}{n}\Lambda)/\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

The following lemma demonstrates the importance of multiplication maps.

Lemma 1.7. *Let T_1, T_2 be complex tori and let $\alpha : T_1 \longrightarrow T_2$ be an isogeny of degree d. There exists a unique isogeny $\underline{\alpha} : T_2 \longrightarrow T_1$ satisfying $\alpha \circ \underline{\alpha} = [d]_{T_2}$ and $\underline{\alpha} \circ \alpha = [d]_{T_1}$.*

Proof. See Birkenhake-Lange [**7**, Proposition 1.2.6]. □

Note that the above lemma tells us that an isogeny f in $\mathrm{Hom}(T_1, T_2)$ has an inverse in $\mathrm{Hom}(T_2, T_1) \otimes \mathbb{Q}$, namely $(\deg f)^{-1}\underline{f}$.

1.2. Projective embeddings

A complex torus $A = V/\Lambda$ is an abelian variety if and only if it can be embedded into projective space. To do this, one needs to find an ample divisor on A. First we briefly describe the necessary divisor theory.

A *Cartier divisor* on a complex manifold M is given by an equivalence class of families $\{(U_\alpha, f_\alpha)\}$ where the U_α form an open covering of M, where $f_\alpha \neq 0$ is meromorphic on U_α, and f_α/f_β is holomorphic on $U_\alpha \cup U_\beta$ for all α, β. Two families $\{(U_\alpha, f_\alpha)\}$ and $\{(U_\beta, g_\beta)\}$ are equivalent if f_α/g_β is nowhere zero and holomorphic on $U_\alpha \cup U_\beta$. A divisor D is said to be *effective* (or *positive*), written $D \geq 0$, if the defining functions f_α are holomorphic for all α. One can check this property is independent of the choice of representative.

The sum of two divisors is

$$\{(U_\alpha, f_\alpha) \colon \alpha \in I\} + \{(U_\beta, g_\beta) \colon \beta \in J\} = \{(U_\alpha \cap U_\beta, f_\alpha g_\beta) \colon \alpha \in I, \beta \in J\}\,.$$

The set of divisors on M form an abelian group, written as $\mathrm{Div}(M)$. We define the set of *principal divisors* $\mathrm{Prin}(M) \subset \mathrm{Div}(M)$ to be the divisors of the form

$$\mathrm{div}(f) = \{(f, M)\}\,.$$

Let N be another complex manifold. A complex analytic map $p : M \longrightarrow N$ induces a map

$$\begin{array}{rcl} p^* : \mathrm{Div}(N) & \longrightarrow & \mathrm{Div}(M) \\ \{(W_\alpha, g_\alpha)\} & \longmapsto & \{(p^{-1}W_\alpha, g_\alpha \circ p)\} \end{array}$$

called the *pullback* of p.

Let $\mathbb{C}(M)$ to be the set of meromorphic functions on M. For any divisor D we have the associated the vector space of meromorphic functions

$$\mathcal{L}(D) = \{f \in \mathbb{C}(M) : (f) + D \geq 0\}\,.$$

Write $\ell(D)$ for the dimension of $\mathcal{L}(D)$ and let $f_0, \ldots, f_n$ be a basis of $\mathcal{L}(D)$. Then we obtain a complex analytic map

$$\begin{array}{rcl} \varphi_D : X & \longrightarrow & \mathbb{P}^n \\ x & \longmapsto & (f_0(x) : \ldots : f_n(x)) \end{array}$$

where $n = \ell(D) - 1$. Note that φ_D is only well defined if $\ell(D) \geq 1$.

Theorem 1.8. *(Cousin's Theorem) Every divisor on $\mathbb{C}^g$ is principal.*

Proof. See Birkenhake-Lange [**7**, Lemma 2.1.1]. □

Let $T = V/\Lambda$ be a complex torus and $\pi : V \longrightarrow T$ be the natural projection map. Given a meromorphic function $f : T \longrightarrow \mathbb{C}$, we have that $\pi^* f = f \circ \pi : V \longrightarrow \mathbb{C}$. Write $g = \pi^* f$, then $g(v + \lambda) = g(v)$ for all λ in Λ hence g is Λ-periodic. Let $t_a : V \longrightarrow V, x \mapsto x + a$ be translation by a. Let $D' = \{(f_i, U_i)\}$ be a divisor on T, then $D = \pi^* D' = \{(\pi^* f_i, \pi^{-1} U_i)\}$ is a divisor on V which satisfies $t_\lambda^* D = D$ for all $\lambda \in \Lambda$. By Cousin's Theorem, $D = \operatorname{div}(f)$ for some f in $\mathbb{C}(V)$. So $t_\lambda^* D = D$ gives us $f(z + \lambda) = U_\lambda(z) f(z)$ for all λ in Λ, where $U_\lambda(z)$ is a nowhere vanishing holomorphic function (called a *factor of automorphy*). We can write $U_\lambda(z) = \mathbf{e}(h_\lambda(z))$ where $\mathbf{e}(z) = \exp(2\pi i z)$. The function $h_\lambda(z)$ must satisfy

$$h_{\lambda_1+\lambda_2}(z) = h_{\lambda_1}(z + \lambda_2) + h_{\lambda_2}(z) \mod \mathbb{Z}\,.$$

The simplest and most important example is

$$h_\lambda(z) = L(z, \lambda) + J(\lambda)$$

where $L(z, \lambda)$ is linear in z. These define factors of automorphy of theta functions.

Definition 1.9. *(Theta functions) Let $L : V \times \Lambda \longrightarrow \mathbb{C}$ and $J : \Lambda \longrightarrow \mathbb{C}$ be maps as above. A* theta function of type (L, J) *is a meromorphic function θ on V such that*

$$\theta(z + \lambda) = \mathbf{e}(L(z, \lambda) + J(\lambda))\theta(z)$$

for all $z \in V$ and $\lambda \in \Lambda$.

The following theorem is a sharper form of Cousin's Theorem for complex tori and indicates the important rôle theta functions will play.

Theorem 1.10. *(Poincaré) Let D' be a divisor on T. Then $\pi^* D' = \operatorname{div}(\theta)$ where θ is a meromorphic theta function.*

Proof. See Lang [**45**, Ch. X §1]. □

Proposition 1.11. *Let θ_1 and θ_2 be theta functions with respect to a lattice Λ, and suppose they define the same divisor. Then there exists a quadratic form Q, a linear form R and a constant S such that*

$$\theta_1(z)/\theta_2(z) = \exp(Q(z) + R(z) + S)\,. \tag{1.12}$$

A theta function of the form $\exp(Q(z) + R(z) + S)$ is called a trivial theta function.

Proof. See Hindry-Silverman [**27**, Lemma A.5.2.3]. □

Corollary 1.13. *We have $\operatorname{div}(\theta_1) = \operatorname{div}(\theta_2 \theta)$ as divisors on V, where θ is any trivial theta function.*

Definition 1.14. *A* Riemann form *on V/Λ is a Hermitian form $H : V \times V \longrightarrow \mathbb{C}$ with the property that $\operatorname{Im} H(\Lambda, \Lambda) \subseteq \mathbb{Z}$.*

Lemma 1.15. *There is a one-to-one correspondence between Hermitian forms $H : V \times V \longrightarrow \mathbb{C}$ and alternating forms $E : V \times V \longrightarrow \mathbb{R}$ which satisfy $E(ix, iy) = E(x, y)$ given by*

$$E = \operatorname{Im} H\,, \qquad H(x, y) = E(ix, y) + iE(x, y)\,.$$

Proof. See Birkenhake-Lange [**7**, Lemma 2.1.7]. □

For this reason, some authors define a Riemann form to be $\operatorname{Im} H$ instead of H. From the functional equation of the theta function, one can show that $L(z, \lambda)$ is $\mathbb{Z}$-linear, and since $V = \Lambda \otimes \mathbb{R}$, it can be extended to give a map $L : V \times V \longrightarrow \mathbb{C}$ which is $\mathbb{R}$-linear in the second variable and $\mathbb{C}$-linear in the first variable.

Proposition 1.16. *Let θ be a theta function of type (L, J) with respect to the the lattice Λ. Define $E(z, w) := L(z, w) - L(w, z)$. Then E is a real valued bilinear alternating form and takes integral values on $\Lambda \times \Lambda$. Hence $H(x, y) = E(ix, y) + iE(x, y)$ defines a Riemann form on V/Λ. Furthermore, H depends only on the divisor $D = \operatorname{div}(\theta)$. Given two divisors D and D' we have that $H_{D+D'} = H_D + H_{D'}$, that is to say the map $D \to H_D$ is a group homomorphism.*

Proof. See Hindry-Silverman [**27**, p. 99]. □

As an immediate corollary of the previous Proposition and Corollary 1.13 we have:

Corollary 1.17. *The Riemann form corresponding to a trivial theta function is zero.*

We now study the homomorphism $D \to H_D$ more closely.

Lemma 1.18. *Let θ_0 be a theta function with respect to a lattice Λ and let H be its Riemann form. Then there exists a theta function θ with the same divisor (hence the same Riemann form) such that the functional equation is*

$$\theta(z + \lambda) = \exp(\pi H(z, \lambda) + \frac{\pi}{2} H(\lambda, \lambda) + 2\pi i K(\lambda))\theta(z)\,,$$

where $K : \Lambda \longrightarrow \mathbb{R}$ is a function satisfying

$$\mathbf{e}(K(\lambda + \mu)) = \mathbf{e}(K(\lambda))\mathbf{e}(K(\mu))\mathbf{e}(\frac{1}{2} E(\lambda, \mu))\,.$$

Proof. See Hindry-Silverman [**27**, Lemma A.5.2.6]. □

Let $L(\theta)$ be the vector space of all theta functions with the same functional equation as θ. Note that $\mathcal{L}(\operatorname{div}(\theta)) \cong L(\theta)$ via $\theta \mapsto \theta/\theta_0$ where

θ_0 can be taken to be any fixed element of $L(\theta)$. Hence choosing a basis $\theta_0, \ldots, \theta_n$ for $L(\theta)$, we get a holomorphic map

$$\begin{aligned} \phi_D : V/\Lambda &\longrightarrow \mathbb{P}^n \\ z &\longmapsto (\theta_0(z) : \ldots : \theta_n(z)) \end{aligned}$$

Definition 1.19. *A divisor D on a complex torus is said to be* very ample *if ϕ_D is an embedding. We say D is* ample *if some positive multiple of D is very ample.*

If a complex torus can be embedded into projective space, then one can apply Chow's theorem [**21**, p. 167] which says that a complex submanifold of projective space is a projective algebraic variety.

Proposition 1.20. *The Riemann form associated to a theta function is positive definite.*

Proof. See Hindry-Silverman [**27**, Proposition A.5.2.5(a)]. □

Theorem 1.21. *Let D be an effective divisor on a complex torus. The Riemann form attached to D is nondegenerate if and only if D is ample*

Proof. See Hindry-Silverman [**27**, Theorem A.5.2.7]. □

Remark 1.22. If D is degenerate then $L(\theta_D)$ consists of *degenerate* theta functions. Such functions give embeddings of subtori of strictly smaller dimension. See Lang [**45**].

The dimension of $L(\theta)$ for a nondegenerate theta function is given by Frobenius' Theorem. First, a lemma.

Lemma 1.23. *(Frobenius) Let Λ be a free abelian group of rank $2g$. Let E be a nondegenerate bilinear alternating form on Λ with values in $\mathbb{Z}$. There exist positive integers $d_1, \ldots, d_g$ (called the* invariants *of E) with $d_i \mid d_{i+1}$ and a basis $e_1, \ldots, e_g, f_1, \ldots, f_g$ of Λ such that*

$$E(e_i, e_j) = E(f_i, f_j) = 0 \text{ and } E(e_i, f_j) = d_i \delta_{ij} \, .$$

The product $d_1 \cdots d_g =: \mathrm{Pf}(E)$ is the square root of the determinant of E and is called the Pfaffian *of E. A basis with the properties above is called a* symplectic (or Frobenius) *basis for Λ. If we set $M = diag(d_1, \ldots, d_g)$ then the matrix of E with respect to the symplectic basis has the form $\begin{pmatrix} 0 & M \\ -M & 0 \end{pmatrix}$.*

Proof. See Hindry-Silverman [**27**, Lemma A.5.3.1]. □

Theorem 1.24. *(Frobenius) Let θ be a theta function with nondegenerate Riemann form H for the complex torus V/Λ. Let $\{e_1, \ldots, e_g, f_1, \ldots, f_g\}$ be a symplectic basis for the form $E = \operatorname{Im} H$ on Λ and let $d_1, \ldots, d_g$ be the associated invariants. Then*

a) *The sets* $\{e_1, \ldots, e_g\}$ *and* $\{f_1, \ldots, f_g\}$ *both form* $\mathbb{C}$*-bases of* V*,*
b) *After multiplication by a suitable trivial theta function, the functional equation of* θ *takes the form*

$$\theta(z + f_i) = \theta(z) \text{ and } \theta(z + e_i) = \theta(z)\mathbf{e}(d_i z_i + c_i)\,,$$

Such functions are known as classical *theta functions.*
c) $\dim L(\theta) = \mathrm{Pf}(E)$.

Proof. See Hindry-Silverman [**27**, Lemma A.5.3.2, Theorem A.5.3.3]. □

Remark 1.25. There is a similar theorem for degenerate theta functions. See Lang [**45**].

1.3. The Appell-Humbert theorem

In the previous section we showed that there was a correspondence between divisors on complex tori and theta functions of a certain type. Namely, given a divisor on $T = V/\Lambda$ we can construct a normalised theta function with factor of automorphy $\chi(\lambda)\cdot\exp(\pi H(z,\lambda)+\frac{\pi}{2}H(\lambda,\lambda))$ where $\chi(\lambda) := \mathbf{e}(K(\lambda))$ satisfies

$$\chi(\lambda + \mu) = (-1)^{E(\lambda,\mu)}\chi(\lambda)\chi(\mu)\,.$$

Definition 1.26. *Write* $\mathbb{C}_1$ *for the complex numbers with absolute value equal to* 1*. A function* $\chi : \Lambda \longrightarrow \mathbb{C}_1$ *satisfying the above relation is called a* semicharacter *for* H*.*

We now set up the notation needed to describe the Appell-Humbert Theorem. Define $\mathcal{P}(V/\Lambda)$ to be the set of pairs (H, χ) where H is a Riemann form on V and χ is a semicharacter for H. The correspondence is simply

$$D \longmapsto \pi^* D = \mathrm{div}(\theta) \longmapsto (H, \chi)\,.$$

From now on write D_t to denote the divisor D translated by t. Let $T = V/\Lambda$ be a complex torus. Recall that $\mathrm{Prin}(T)$ is the set of principal divisors on T. Such divisors are of the form $\mathrm{div}(f)$ where f is a meromorphic function on T. The pullback $\pi^*(f)$ to V is Λ-periodic hence has trivial factor of automorphy so $(H, \chi) = (0, 1)$. We say two divisors are *linearly equivalent* if their difference is in $\mathrm{Prin}(T)$. Define $\mathrm{Div}^{\mathrm{alg}}(T) \subset \mathrm{Div}(T)$ to be

$$\{D' \in \mathrm{Div}(T) | D' \text{ is linearly equivalent to } D_t - D,\ D \in \mathrm{Div}(T), t \in V\}\,,$$

elements of which are said to be *algebraically equivalent* to 0. It is clear from the correspondence that such divisors have Riemann form equal to 0. We have $\mathrm{Prin}(T) \subset \mathrm{Div}^{\mathrm{alg}}(T) \subset \mathrm{Div}(T)$. We say two divisors are *algebraically equivalent* if their difference is in $\mathrm{Div}^{\mathrm{alg}}(T)$.

Define the following groups:

$$\begin{aligned} \text{The Néron-Severi group:} \qquad & \mathrm{NS}(T) = \mathrm{Div}(T)/\mathrm{Div}^{\mathrm{alg}}(T)\,, \\ \text{the Picard group:} \qquad & \mathrm{Pic}(T) = \mathrm{Div}(T)/\mathrm{Prin}(T)\,, \\ \text{and} \qquad & \mathrm{Pic}^0(T) = \mathrm{Div}^{\mathrm{alg}}(T)/\mathrm{Prin}(T)\,. \end{aligned}$$

It follows immediately that the sequence below is exact:

$$0 \longrightarrow \mathrm{Pic}^0(T) \longrightarrow \mathrm{Pic}(T) \longrightarrow \mathrm{NS}(T) \longrightarrow 0\,.$$

The following theorem fully describes the divisor-theta function correspondence.

Theorem 1.27. *(Appell-Humbert) The following diagram is commutative, where the rows are exact sequences.*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Hom}(\Lambda, \mathbb{C}_1) & \xrightarrow{\alpha} & \mathcal{P}(V/\Lambda) & \xrightarrow{\beta} & \mathrm{NS}(T) & \longrightarrow & 0 \\ & & \downarrow \cong & & \downarrow L \cong & & \downarrow = & & \\ 1 & \longrightarrow & \mathrm{Pic}^0(T) & \longrightarrow & \mathrm{Pic}(T) & \longrightarrow & \mathrm{NS}(T) & \longrightarrow & 0 \end{array}$$

The map α sends χ to $(0, \chi)$ and the map β sends (H, χ) to a divisor corresponding to H under the middle vertical isomorphism.

Proof. See Birkenhake-Lange [**7**, §2.2]. □

1.4. The dual abelian variety

Let $T = V/\Lambda$ be a complex torus of dimension g. The exponential map $\mathbf{e} : \mathbb{R} \longrightarrow \mathbb{C}_1$ gives rise to an exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R}) \xrightarrow{\mathbf{e}} \mathrm{Hom}(\Lambda, \mathbb{C}_1) \longrightarrow 1\,,$$

thus $\mathrm{Hom}(\Lambda, \mathbb{C}_1)$ is isomorphic to $\mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})/\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z}) \cong \mathbb{R}^{2g}/\mathbb{Z}^{2g}$. Below we show that $\mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$ can be given a complex structure (so that it becomes a complex vector space) hence $\mathrm{Pic}^0(T) \cong \mathrm{Hom}(\Lambda, \mathbb{C}_1)$ is a complex torus called the *dual complex torus*.

Consider the space $\mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C})$ of antilinear functionals on V,

$$\mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C}) := \{ f \in \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{C}) : f(\alpha t) = \overline{\alpha} f(t),\ \alpha \in \mathbb{C},\ t \in V \}\,.$$

This vector space is isomorphic to $\mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$ via the isomorphism

$$\begin{array}{rcl} \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R}) & \xrightarrow{\varphi} & \mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C}) \\ g(z) & \longmapsto & f(z) = -g(iz) + ig(z) \\ \mathrm{Im}\, f(z) = g(z) & \longleftarrow & f(z)\,. \end{array}$$

Under this map, the complex structure of $\mathrm{Hom}_{\overline{\mathbb{C}}}(V,\mathbb{C})$ gets transferred to $\mathrm{Hom}_{\mathbb{R}}(V,\mathbb{R})$, so $\mathrm{Hom}(\Lambda,\mathbb{C}_1)\cong V^*/\Lambda^*$ where

$$V^* = \varphi(\mathrm{Hom}_{\mathbb{R}}(V,\mathbb{R})) = \mathrm{Hom}_{\overline{\mathbb{C}}}(V,\mathbb{C}) \quad \text{and}$$
$$\Lambda^* = \varphi(\mathrm{Hom}_{\mathbb{Z}}(\Lambda,\mathbb{Z})) = \{f \in V^* \mid \mathrm{Im}\, f(\Lambda) \subseteq \mathbb{Z}\}$$

is a lattice in V^*. Explicitly we have the following:

Lemma 1.28. *The map* $\zeta : V^*/\Lambda^* \longrightarrow \mathrm{Hom}(\Lambda,\mathbb{C}_1)$ *defined by*

$$f \longmapsto \mathbf{e}(\mathrm{Im}\, f(\cdot))$$

is an isomorphism.

Lemma 1.29. *Let* $\bar{v}$ *be an element of* T *with representative* v*. For any divisor* $D = L(H,\chi)$ *in* $\mathrm{Pic}(X)$ *we have*

$$D_{\bar{v}} = L(H, \chi\cdot \mathbf{e}(\mathrm{Im}\, H(v,\cdot))$$

Proof. See Birkenhake-Lange [**7**, Lemma 3.2]. □

Corollary 1.30. *Every element of* $\mathrm{Hom}(\Lambda,\mathbb{C}_1)$ *is of the form*

$$\lambda \mapsto \mathbf{e}(\mathrm{Im}\, H(v,\lambda))$$

for some v *in* V*.*

We now construct a map from T to $\mathrm{Pic}^0(T)$.

Proposition 1.31. *Given a divisor* X *on* T*, define* $\phi_X : T \longrightarrow \mathrm{Pic}^0(T)$ *by* $\phi_X(t) = X - X_t$*. If* X *is ample then* ϕ_X *is surjective with finite kernel of order* $\det(E) = \mathrm{Pf}(E)^2$*.*

Proof. All that needs to be proved is the kernel claim. Using the isomorphism $\mathrm{Pic}(T)\cong\mathrm{Hom}(\Lambda,\mathbb{C}_1)$ we have that

$$\ker(\phi_X) \cong \{v \in V : E(t,\lambda) \in \mathbb{Z} \text{ for all } \lambda \in \Lambda\}/\Lambda\,.$$

Let $\{e_1,\ldots,e_g,f_1,\ldots,f_g\}$ be a symplectic basis so the matrix of E has the form $\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}$ where $D = \mathrm{diag}(d_1,\ldots,d_g)$ where g is the dimension of T. Identifying Λ with $\mathbb{Z}^{2g}$ we have

$$\ker(\phi_X) = (D^{-1}\mathbb{Z}/\mathbb{Z})^2 \cong (\mathbb{Z}/d_1\mathbb{Z}\oplus\ldots\oplus\mathbb{Z}/d_g\mathbb{Z})^2\,,$$

a finite group of the desired order. □

If H is a nondegenerate Riemann form on T, then $\phi_H : t \mapsto H(t,\cdot)$ is an isomorphism of V with V^* as complex vector spaces. One checks that $\phi_H(\Lambda)\subset\Lambda^*$ so we have a surjective homomorphism $V/\Lambda \to V^*/\Lambda^*$.

Proposition 1.32. *Suppose* $X = L(\chi,H)$*. The map* $\phi_H : V \longrightarrow \mathrm{Hom}_{\overline{\mathbb{C}}}(V,\mathbb{C})$ *above is the analytic representation of* $\phi_X : T \longrightarrow \mathrm{Pic}^0(T)$*.*

Proof. The claim follows immediately from the commutative diagram

$$\begin{array}{ccc} T & \xrightarrow{\phi_H} & V^*/\Lambda^* \\ {\scriptstyle \phi_X}\downarrow & & \cong\downarrow{\scriptstyle \zeta} \\ \mathrm{Pic}^0(T) & \xrightarrow{\cong} & \mathrm{Hom}(\Lambda, \mathbb{C}_1) \end{array}$$

where ζ is the isomorphism in Lemma 1.28 and the bottom isomorphism is given by the Appell-Humbert Theorem 1.27. □

Proposition 1.33. *If A is a complex abelian variety, then $\mathrm{Pic}^0(A)$ is a complex abelian variety called the* dual abelian variety.

Proof. Let $A \cong V/\Lambda$ and let H be a nondegenerate Riemann form with respect to A. Let φ denote the isomorphism $t \mapsto H(t, \cdot)$ inducing ϕ_H. Define

$$H^*(\xi, \eta) = H(\varphi_H^{-1}(\xi), \varphi_H^{-1}(\eta)) \text{ for } \xi, \eta \text{ in } V\,.$$

While H^* is certainly a Hermitian form on V^*, the imaginary part $\mathrm{Im}\, H^*$ need not be integer valued on $\Lambda^* \times \Lambda^*$. Since $\ker(\phi_H)$ is finite (by the previous two propositions), it follows that $\phi_H^{-1}(\Lambda^*)/\Lambda$ is a finite abelian group, having exponent k say. Since ku is in Λ for any u in $\phi_H^{-1}(\Lambda^*)$, it follows that kH^* is a Riemann form, proving that $\mathrm{Pic}^0(A)$ is a complex abelian variety. □

Write $\hat{A} := \mathrm{Pic}^0(A)$ to denote the dual abelian variety of A. We list some properties of the dual.

Proposition 1.34. *Let A, A_1, A_2 and A_3 be complex abelian varieties.*

a) $\widehat{\widehat{A}} \cong A$ *by double anti-duality.*
b) *If $f : A_1 \longrightarrow A_2$ is a homomorphism then the $\hat{f} : \widehat{A}_2 \longrightarrow \widehat{A}_1$ is a homomorphism induced by pulling back divisors.*
c) *If $0 \to A_1 \to A_2 \to A_3 \to 0$ is an exact sequence of complex abelian varieties then $0 \to \widehat{A}_3 \to \widehat{A}_2 \to \widehat{A}_1 \to 0$ is also exact.*
d) *If $f : A_1 \longrightarrow A_2$ is an isogeny then $\hat{f} : \widehat{A}_2 \longrightarrow \widehat{A}_1$ is an isogeny of the same degree.*

Proof. See Birkenhake-Lange [**7**, §2.4]. □

1.5. Polarizations

Let A be an abelian variety. Loosely speaking, a polarization on A is a set of projective embeddings of A, each differing only by a translation (algebraic equivalence).

Definition 1.35. *A polarization is a set $\mathcal{C}(H) = \{rH : r \in \mathbb{Q}^+\}$ where H is a positive definite nondegenerate Riemann form.*

The map $\phi_H : A \longrightarrow \hat{A}$ is an isogeny with analytic representation $t \mapsto H(t, \cdot)$. Let n be a positive integer. The analytic representation of ϕ_{nH} factors as $t \mapsto nt \mapsto H(nt, \cdot) = nH(t, \cdot)$ hence ϕ_{nH} factors through an isogeny $\phi_H[n]$.

Remark 1.36. In the algebraic setting, a polarization is an equivalence class $\mathcal{C}(X)$ of divisors in $NS(A)$ where X and Y are equivalent if and only if there exist positive integers m, n satisfying $mX = nY$.

Since Riemann forms must take integer values on the lattice, there is a "smallest" Riemann form H' in $\mathcal{C}(H)$ for which all integer multiples of H' are Riemann forms. A divisor Y corresponding to H' is called a *basic polar divisor*. It has the property that $\mathcal{C}(Y) = \{mY : m \in \mathbb{Z}_{>0}\}$ and that for any H in $\mathcal{C}(H')$ we have $\phi_H = \phi_{H'}[n]$ for some positive integer n.

Definition 1.37. *A* morphism *of polarized complex abelian varieties*

$$\varphi : (A_1, \mathcal{C}(H_1)) \longrightarrow (A_2, \mathcal{C}(H_2))$$

is a morphism $\varphi : A_1 \longrightarrow A_2$ such that the pullback $\varphi^* H_2$ defined by

$$\varphi^* H_2(z, w) := H_2(\varphi(z), \varphi(w))$$

is in $\mathcal{C}(H_1)$.

Abusing notation, we shall write $\mathrm{Hom}(A_1, A_2)$ for the set of morphisms of *polarized* abelian varieties when the polarizations on A_1, A_2 are known. Similarly, write $\mathrm{End}(A)$ for the endomorphism ring of a polarized abelian variety when the polarization on A is understood.

Theorem 1.38. *The automorphism group of a polarized abelian variety is finite.*

Proof. See Lang [**46**, p. 70]. □

If $(A, \mathcal{C}(H))$ is a polarized complex abelian variety, then $\phi_H : A \longrightarrow \hat{A}$ is an isogeny of degree $\det E = \mathrm{Pf}(E)^2$ where $E = \mathrm{Im}\, H$. A *principally polarized* abelian variety is a polarized abelian variety $(A, \mathcal{C}(H))$ for which there exists a (unique) Riemann form H' in $\mathcal{C}(H)$ satisfying $\mathrm{Pf}(\mathrm{Im}\, H') = 1$. This induces an isomorphism between A and its dual.

Proposition 1.39. *Every polarized complex abelian variety is isogenous to a principally polarized abelian variety.*

Proof. Let $(A, \mathcal{C}(H))$ be a polarized abelian variety of dimension g. As usual we have $A \cong V/\Lambda$ and $E = \mathrm{Im}\, H$ being integer valued on $\Lambda \times \Lambda$. Let

$\{\lambda_1, \ldots, \lambda_{2g}\}$ be a symplectic basis for Λ. In particular, $E(\lambda_j, \lambda_{g+j}) = d_j$ for some positive integers $d_1 | \cdots | d_g$. Define a new lattice

$$\Lambda' = \sum_{j=1}^{g} \frac{1}{d_j} \lambda_j \mathbb{Z} + \sum_{j=1}^{g} \lambda_{g+j} \mathbb{Z}\,,$$

then E as an alternating form on Λ' is integer valued and has determinant 1. Let $A' = V/\Lambda'$, then the natural projection $A \to A'$ is an isogeny of degree $d_1 \cdots d_g$ and A' is principally polarized by E. □

1.6. The Rosati involution

Let $(A, \mathcal{C})$ be a polarized abelian variety. Define

$$\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}.$$

This is known as the the *endomorphism algebra* of $(A, \mathcal{C})$. Let X be an ample divisor in $\mathcal{C}$. Then $\phi_X : A \longrightarrow \hat{A}$ is an isogeny, hence has an inverse in $\mathrm{Hom}(\hat{A}, A) \otimes \mathbb{Q}$. Every endomorphism $\rho : A \longrightarrow A$ has a dual morphism $\hat{\rho} : \hat{A} \longrightarrow \hat{A}$, and the map $\rho \mapsto \hat{\rho}$ extends to a map $\mathrm{End}^0(A) \mapsto \mathrm{End}^0(\hat{A})$. Define the *Rosati involution (with respect to $\mathcal{C}$)* to be $\rho^\dagger := \phi_X^{-1} \circ \hat{\rho} \circ \phi_X$. This formula for $\rho^\dagger$ is independent of the choice of X, since

$$\phi_{nX}^{-1} \hat{\rho} \phi_{nX} = n^{-1} \phi_X^{-1} \hat{\rho} n \phi_X = \rho^\dagger$$

as multiplication by n commutes with all endomorphisms.

It is easily seen that $(\rho_1 \circ \rho_2)^\dagger = \rho_2^\dagger \circ \rho_1^\dagger$, and combined with the following proposition we can prove that $\rho \mapsto \rho^\dagger$ is an involution on $\mathrm{End}^0(A)$.

Proposition 1.40. *$H(\rho z, w) = H(z, \rho^\dagger w)$ for all z, w in V. That is, $\rho^\dagger$ is the adjoint of ρ with respect to H. Hence $\rho^{\dagger\dagger} = \rho$.*

Proof. We have a nondegenerate pairing $V \times V^* \to \mathbb{C}$ given by $\langle z, g \rangle = g(z)$. If ρ is in $\mathrm{End}(A)$ then its dual satisfies $\langle \rho z, g \rangle = \langle z, \hat{\rho} g \rangle$. We have that $\langle z, \phi_H w \rangle = H(w, z)$ for all z, w in V, so

$$H(\rho^\dagger w, z) = H(\phi_H^{-1} \hat{\rho} \phi_X w, z) = \langle z, \hat{\rho} \phi_H w \rangle = \langle \rho z, \phi_H w \rangle = H(w, \rho z)\,.$$

Taking complex conjugates of both sides produces the desired equality. □

Remark 1.41. If $(A, \mathcal{C})$ is principally polarized, then by taking X to be the basic polar divisor, the map $\phi_X : A \longrightarrow \hat{A}$ is an isomorphism in which case the Rosati involution is an involution of the endomorphism *ring* $\mathrm{End}(A)$ as well as the endomorphism algebra.

The Rosati involution plays a crucial rôle in the classification of endomorphism algebras of abelian varieties.

Theorem 1.42. *Let* Tr *denote the trace map on the* $\mathbb{Q}$*-algebra* $\mathrm{End}^0(A)$. *Then* $\mathrm{Tr}(\rho\rho^\dagger) > 0$ *for all nonzero* ρ *in* $\mathrm{End}^0(A)$.

Proof. See Birkenhake-Lange [**7**, Theorem 5.1.8]. □

It follows that an endomorphism algebra of a polarized abelian variety must have an involution $f \mapsto f^\dagger$ such that $f \mapsto \mathrm{Tr}(f^\dagger f)$ is a positive definite quadratic form.

1.7. Endomorphisms of abelian varieties

Let $A = V/\Lambda$ and $A' = V'/\Lambda'$ be abelian varieties. Recall Lemma 1.3 which says that we have an injective homomorphism of abelian groups

$$\begin{aligned} \rho_a : \mathrm{Hom}(A, A') &\longrightarrow \mathrm{Hom}_{\mathbb{C}}(V, V') \\ f &\longmapsto \tilde{f} \end{aligned}$$

called the analytic representation of $\mathrm{Hom}(A, A')$. The restriction of $\tilde{f}$ to the lattice Λ is $\mathbb{Z}$-linear. In fact $\tilde{f}|_\Lambda$ determines f and $\tilde{f}$ completely, thus we get an injective homomorphism

$$\begin{aligned} \rho_r : \mathrm{Hom}(A, A') &\longrightarrow \mathrm{Hom}_{\mathbb{C}}(\Lambda, \Lambda') \\ f &\longmapsto \tilde{f}|_\Lambda \end{aligned}$$

called the *rational representation* of $\mathrm{Hom}(A, A')$.

Suppose $\dim A = g$ and $\dim A' = g'$. Then choosing bases for Λ and Λ', a homomorphism $\Lambda \to \Lambda'$ is given by a $2g \times 2g'$ integral matrix and conversely, so $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda') \cong \mathbb{Z}^{4gg'}$. Therefore, since any subgroup of $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda')$ must be isomorphic to $\mathbb{Z}^m$, the injectivity of ρ_r implies the following.

Proposition 1.43. $\mathrm{Hom}(A, A') \cong \mathbb{Z}^m$ *for some* $m \leq 4gg'$.

Let $A'' = V''/\Lambda''$ be a third abelian variety. If $f : A \longrightarrow A'$ and $f' : A' \longrightarrow A''$ are homomorphisms then the uniqueness of lifts gives us the identity $\rho_a(f')\rho_a(f) = \rho_a(f'f)$. It follows that if $A = A'$ then ρ_a and ρ_r are representations of the ring $\mathrm{End}(A)$ and $\mathrm{End}^0(A)$.

Definition 1.44. *Let* V/Λ *be a complex torus. Fix a* $\mathbb{C}$*-basis* $e_1, \ldots, e_g$ *for* V *and fix a* $\mathbb{Z}$*-basis* $\lambda_1, \ldots, \lambda_{2g}$ *for* Λ. *Let* Π *denote the* $g \times 2g$ *matrix whose column vectors are given by* $\lambda_1, \ldots, \lambda_{2g}$ *with repect to the* e_i *basis. Explicitly, write each* $\lambda_j = \sum_{i=1}^g w_{ji} e_i$, *then* $\Pi = (w_{ij})$. *The matrix* Π *is called a* period matrix.

Remark 1.45. It is clear that a period matrix is dependent on the bases chosen for V and Λ. Some authors prefer to interchange rows and columns and their period matrices have dimensions $2g \times g$. We shall make every effort to be consistent according to our definition above.

Proposition 1.46. *Π is a period matrix of a complex torus of dimension g if and only if the complex $2g \times 2g$ matrix $\binom{\Pi}{\overline{\Pi}}$ is nonsingular.*

Proof. See Birkenhake-Lange [**7**, Proposition 1.1.2]. □

Suppose $A = V/\Lambda$ has a period matrix Π and $A' = V'/\Lambda'$ has period matrix Π' with respect to some bases of V, Λ and V', Λ' respectively. Let $f : A \longrightarrow A'$ be a homomorphism. Then the linear transformation $\rho_a(f)$ can be written as a $g \times g'$ complex matrix R_a with respect to the chosen bases. Similarly $\rho_r(f)$ is represented by a $2g \times 2g'$ integral matrix R_r. In terms of matrices, the condition $\rho_a(f)(\Lambda) \subset \Lambda'$ corresponds to the relation

$$R_a\Pi = \Pi' R_r \,. \tag{1.47}$$

Conversely any complex $g \times g'$ matrix R_a and integral $2g \times 2g'$ matrix R_r satisfying the above relation defines a homomorphism $A \to A'$.

Proposition 1.48. *The extended rational representation*

$$\rho_r \otimes \mathbb{C} \to \mathrm{End}^0(A) \otimes \mathbb{C} \to \mathrm{End}_{\mathbb{C}}(\Lambda \otimes \mathbb{C}) \cong \mathrm{End}_{\mathbb{C}}(V \times V)$$

is equivalent to $\rho_a \oplus \overline{\rho_a}$.

Proof. Fix bases for V and Λ and let Π denote the corresponding period matrix of $A = V/\Lambda$. Let f be an endomorphism of A. If C and R are matrices of ρ_a and ρ_r with respect to the chosen bases respectively, then by the relation (1.47) we have

$$\begin{pmatrix} C & 0 \\ 0 & \overline{C} \end{pmatrix} \begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix} = \begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix} R \,.$$

Since $\binom{\Pi}{\overline{\Pi}}$ is nonsingular by Proposition 1.46, we are done. □

Let $f : A \longrightarrow A'$ be an isogeny. Then the degree of f is the cardinality of $\ker(f)$ which equals the index of the subgroup $\rho_r(f)(\Lambda)$ in Λ. In the special case where f is an endomorphism of A we have $\Lambda = \Lambda'$ and thus

$$\deg(f) = \det \rho_r(f) \,.$$

From this we deduce that $\deg(f'f) = \deg(f')\deg(f)$ when f', f are isogenies and their composition is well defined.

1.8. Classification of endomorphism algebras

For the most part we state the classification theorems of this section without proof. Proofs can be found in Birkenhake-Lange [**7**, Ch. 5].

An abelian variety is called *simple* is it does not contain any abelian subvarieties other than itself and 0. We can now state Poincaré's Complete Reducibility Theorem.

Theorem 1.49. *(Poincaré) Given an abelian variety X there is an isogeny*

$$X \longrightarrow X_1^{n_1} \times \ldots \times X_r^{n_r}$$

where the X_i are simple abelian varieties not isogenous to each other. Moreover, the X_i and n_i are uniquely determined up to isogenies and permutations.

Proof. See Birkenhake-Lange [**7**, Theorem 5.3.7]. □

Corollary 1.50. $\mathrm{End}^0(X)$ *is a semisimple $\mathbb{Q}$-algebra: if $X \to X_1^{n_1} \times \ldots \times X_r^{n_r}$ is an isogeny then*

$$\mathrm{End}^0(X) \cong \mathbb{M}_{n_1}(F_1) \oplus \ldots \oplus \mathbb{M}_{n_r}(F_r)$$

where $F_i = \mathrm{End}^0(X_i)$ are skew fields of finite dimension over $\mathbb{Q}$.

Proof. Without loss of generality we may assume that $X = X_1^{n_1} \times \ldots \times X_r^{n_r}$ where the X_i are simple and non-isogenous. We have

$$\begin{aligned} \mathrm{End}^0(X) &= \bigoplus_{i,j=1}^{r} \mathrm{Hom}_0(X_i^{n_i}, X_j^{n_j}), \\ &= \bigoplus_{i \neq j} \mathrm{Hom}_0(X_i, X_j)^{\oplus n_i n_j} \oplus \bigoplus_{i=1}^{r} \mathbb{M}_{n_i}(\mathrm{End}^0(X_i)). \end{aligned}$$

If $f : X_i \longrightarrow X_j$ is a homomorphism with $i \neq j$ then the image of f is an abelian subvariety of $X_j^{n_j}$. Since X_i is simple, the connected part of the kernel of f is either zero (in other words $\ker(f)$ is finite) or X_i. If the kernel is finite then f is an isogeny which contradicts the hypothesis, therefore f is the zero map. We have shown that $\mathrm{Hom}_0(X_i, X_j) = 0$ for $i \neq j$. All that is left to show is that $\mathrm{End}^0(X_i)$ is a skew field. Let f be a nonzero endomorphism of X_i. Since X_i is simple, the kernel of f must be finite and the image of f must be X_i. That is, f is an isogeny hence has an inverse in $\mathrm{End}^0(X_i)$. Finally, $\mathrm{End}^0(X_i)$ is finite dimensional by Proposition 1.43, completing the proof. □

The classification of endomorphism algebras of abelian varieties reduces to that of simple abelian varieties by the corollary above. Let X be a simple abelian variety of dimension g and let $\mathcal{C}$ be a polarization on X. Then $F = \mathrm{End}^0(X)$ is a skew field of finite dimension over $\mathbb{Q}$. With respect to the polarization, the Rosati involution $f \mapsto f^\dagger$ is an involution such that $f \mapsto \mathrm{Tr}_r(f^\dagger f)$ is a positive definite quadratic form.

Lemma 1.51. *Any finite dimensional simple $\mathbb{R}$-algebra B is isomorphic to M where M is either $\mathbb{M}_r(\mathbb{R}), \mathbb{M}_r(\mathbb{C})$ or $\mathbb{M}_r(\mathbb{H})$ where $\mathbb{H}$ is the skew field of*

Hamiltonian quaternions. Each of these three matrix algebras has a natural involution $x \mapsto x^*$ given by

$$x^* = \begin{cases} {}^t x & \text{for } \mathbb{M}_r(\mathbb{R}) \\ {}^t \bar{x} & \text{for } \mathbb{M}_r(\mathbb{C}) \text{ and } \mathbb{M}_r(\mathbb{H}). \end{cases}$$

Any isomorphism $B \cong M$ can be composed with an automorphism of M to obtain an isomorphism $\varphi : B \to M$ satisfying $\varphi(x') = \varphi(x)^*$ where $x \mapsto x'$ is some involution on B.

Proof. See Birkenhake-Lange [**7**, Lemma 5.5.1]. □

For the rest of this section let $(F, \, ')$ be a skew field F of finite dimension over $\mathbb{Q}$ equipped with a positive nvolution $' : F \longrightarrow F$. The involution restricts to an involution on the center K of F, whose fixed field we denote by K_0.

Lemma 1.52. *K_0 is a totally real number field.*

Proof. See Birkenhake-Lange [**7**, Lemma 5.5.2]. □

Definition 1.53. *We say that $(F, \, ')$ is* of the first kind *if $K = K_0$. Otherwise we say $(F, \, ')$ is* of the second kind.

A skew field F is called a *quaternion algebra* over K if $[K : \mathbb{Q}] = 4$. Such an algebra has a canonical involution $x \mapsto \overline{x} = \mathrm{Tr}_{F/K}(x) - x$.

Theorem 1.54. *$(F, \, ')$ is a skew field of finite dimension over $\mathbb{Q}$ with positive involution of the first kind if and only if K is a totally real number field and one of the following cases holds:*

a) *$F = K$ and $x' = x$ for all x in F,*
b) *F is a quaternion algebra over K and for every embedding $\sigma : K \hookrightarrow \mathbb{R}$*

$$F \otimes_\sigma \mathbb{R} \cong \mathbb{M}_2(\mathbb{R}) \, .$$

Such an algebra is called a totally indefinite quaternion algebra. *Moreover, there is an element a in F with a^2 totally negative in K such that the involution is given by $x \mapsto x' = a^{-1}\overline{x}a$.*
c) *F is a quaternion algebra over K and for every embedding $\sigma : K \hookrightarrow \mathbb{R}$*

$$F \otimes_\sigma \mathbb{R} \cong \mathbb{H} \, .$$

Such an algebra is called a totally definite quaternion algebra. *Moreover the involution is given by $x \mapsto x' = \overline{x}$.*

Proof. See Birkenhake-Lange [**7**, Lemma 5.5.3]. □

Lemma 1.55. *Suppose $(F, ')$ is of the second kind. Then the center K is totally complex and the restriction of the involution to K is complex conjugation.*

Proof. See Birkenhake-Lange [**7**, Lemma 5.5.4]. □

For any skew field F, the degree $[F : K]$ of F over its center K is always a square, say d^2.

Theorem 1.56. *Let $(F, ')$ be a skew field of finite dimension over $\mathbb{Q}$ with positive involution $x \mapsto x'$ of the second kind. Then for every embedding $\sigma : K \hookrightarrow \mathbb{C}$ we have an isomorphism*

$$\varphi : F \otimes_\sigma \mathbb{C} \longrightarrow \mathbb{M}_d(\mathbb{C})$$

such that $x \mapsto x'$ extends via φ to the canonical involution $X \mapsto {}^t\overline{X}$ on $\mathbb{M}_d(\mathbb{C})$.

Proof. See Birkenhake-Lange [**7**, Theorem 5.5.6]. □

The following proposition gives restrictions on the possible pairs $(F, ')$.

Proposition 1.57. *Let $(X, \mathcal{C})$ be a simple polarized abelian variety of dimension g. Then $F = \mathrm{End}^0(X)$ is a skew field of finite dimension over $\mathbb{Q}$ with positive involution $x \mapsto x^\dagger$, the Rosati involution with respect to $\mathcal{C}$. Let K denote the center of F and K_0 the fixed field of the Rosati involution restricted to K. Denote*

$$[F : K] = d^2,\ [K : \mathbb{Q}] = e,\ \textit{and}\ [K_0 : \mathbb{Q}] = e_0\,.$$

Then we have the following restrictions for these values:

$F = \mathrm{End}^0(X)$	d	e_0	*restriction*
totally real number field	1	e	$e \mid g$
quaternion algebra	2	e	$2e \mid g$
$(F, ')$ *of the second kind*	d	$\frac{1}{2}e$	$e_0 d^2 \mid g$

Proof. See Birkenhake-Lange [**7**, Proposition 5.5.7]. □

We now have necessary conditions for a pair $(F, ')$ to be the endomorphism algebra of a simple abelian variety. The example below shows that these conditions are not sufficient. Even so, for fixed g, apart from some exceptions, one can construct simple abelian varieties for each type of endomorphism algebra listed in the table. See Birkenhake-Lange [**7**, Chapter 9] or Shimura [**66**] for details.

Example 1.58. (Classification of endomorphism algebras of abelian surfaces) Let A be an abelian surface. If A is simple then $\mathrm{End}^0(A)$ can be

a) $\mathbb{Q}$
b) a real quadratic field
c) a purely imaginary extension of a real quadratic field (CM field)
d) an totally indefinite quaternion algebra over $\mathbb{Q}$

If A is not simple then it is isogenous to a product of elliptic curves $E_1 \times E_2$. If E_1 is not isogenous to E_2 then $\mathrm{End}^0(A) = \mathbb{Q} \times \mathbb{Q}$. If E_1 is isogenous to E_2 then $\mathrm{End}^0(A) = \mathbb{M}_2(k)$, where k equals either $\mathbb{Q}$ or an imaginary quadratic field, the latter occuring when the E_i have complex multiplication. Note that the endomorphism algebra cannot be a totally definite quaternion algebra, and that an abelian surface which has CM by an imaginary quadratic field K has an endomorphism ring strictly containing K (either an indefinite quaternion algebra or $\mathbb{M}_2(K)$).

In this thesis we shall study abelian varieties of dimension two, the main focus being on principally polarized abelian surfaces whose endomorphism algebra is a real quadratic field.

Moduli spaces

For the rest of this chapter we review the theory of moduli spaces of complex abelian varieties, mainly using Birkenhake-Lange [**7**] as our reference.

A *(coarse) moduli space* for a set of complex abelian varieties with additional structure is a complex analytic space whose points correspond to elements of the set. Most commonly the sets used are isomorphism classes of abelian varieties with a given polarization and level structure.

The original definition of a polarization as an equivalence class, which we used in the previous chapter and was given by Weil in the 1940's, is not well suited for studying moduli problems. When studying isomorphism classes of abelian varieties it is essential to fix a Riemann form which produces a projective embedding. From now on, a polarization will refer to a Riemann form rather than an equivalence class.

1.9. The Riemann relations

We need criteria to determine whether two abelian varieties are isomorphic to each other. This can be done by looking at period matrices.

Let $X = V/\Lambda$ be a complex torus of dimension g. By fixing bases of V and Λ, we can write down a period matrix Ω for X. The Riemann relations provide necessary and sufficient conditions for Ω to be the period matrix of a polarized abelian variety.

Theorem 1.59. *$X = \mathbb{C}^g/\Omega\mathbb{Z}^{2g}$ is an abelian variety if and only if there is a nondegenerate alternating $2g \times 2g$ matrix A with integer entries such that*

a) $\Omega A^{-1}\,{}^t\Omega = 0$,
b) $i\,\Omega A^{-1}\,{}^t\overline{\Omega} > 0$.

These two equations are known as the Riemann relations. The matrix A is the alternating form defining a polarization on X.

Proof. Suppose that there exists a nondegenerate integer-valued alternating form E on Λ. Denote by A the matrix of E with respect to a fixed basis of Λ. Extend E to $\Lambda \otimes \mathbb{R} = V$. We know from Lemma 1.15 that $H : V \times V \longrightarrow C$ defined by

$$H(z, w) = E(iz, w) + iE(z, w)$$

is a Hermitian form. The theorem follows immediately from the following lemma. □

Lemma 1.60.

a) *H is a Hermitian form on $\mathbb{C}^g$ if and only if $\Omega A^{-1}\,{}^t\Omega = 0$,*
b) *H is positive definite if and only if $i\,\Omega A^{-1}\,{}^t\overline{\Omega} > 0$.*

Proof. See Birkenhake-Lange [**7**, Lemmas 4.2.2 and 4.2.3]. □

In the special case where the basis for Λ is a Frobenius basis, the matrix of A is $\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}$ and the Riemann relations are

$$\Omega_2 D^{-1}\,{}^t\Omega_1 - \Omega_1 D^{-1}\,{}^t\Omega_2 = 0\,,$$
$$i\Omega_2 D^{-1}\,{}^t\overline{\Omega}_1 - i\Omega_1 D^{-1}\,{}^t\overline{\Omega}_2 > 0\,,$$

where $\Omega = (\Omega_1\ \Omega_2)$.

1.10. The Siegel upper half space

In this section, we show how to identify a polarized abelian variety of dimension g with a point in Siegel's upper half space $\mathcal{H}_g$.

Suppose $X = V/\Lambda$ is an abelian variety of dimension g with a polarization H of type $D = \operatorname{diag}(d_1, \ldots d_g)$. Let $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ be a symplectic basis for $\operatorname{Im} H$. Take $e_i = \frac{1}{d_i}\mu_i$. Then by Frobenius' Theorem 1.24, the e_i form a basis of V. With respect to the chosen bases, we have period matrix (Z, D) where Z is a $g \times g$ complex matrix. The Riemann relations say that

$$^tZ - Z = 0\,,$$
$$i(^t\overline{Z} - Z) > 0$$

and so Z is a point in the complex analytic space

$$\mathcal{H}_g = \{Z \in \mathbb{M}_g(\mathbb{C}) \mid {}^tZ = Z \text{ and } \operatorname{Im} Z > 0\}\,,$$

known as the *Siegel upper half space* of degree g. Conversely, given a matrix Z in $\mathcal{H}_g$, we can construct a complex torus $X_Z = \mathbb{C}^g/(Z\ D)\mathbb{Z}^{2g}$ which is an abelian variety of polarization type D thanks to the Riemann relations.

We have shown the following:

Proposition 1.61. *Given a polarization type D, the Siegel upper half space $\mathcal{H}_g$ is a moduli space for polarized abelian varieties of type D with symplectic basis.*

We now find a moduli space for the set of isomorphism classes of abelian varieties with polarization type D. The equivalence classes of isomorphic abelian varieties will be orbits of points in $\mathcal{H}_g$ under the action of a subgroup of $\mathrm{Sp}_{2g}(\mathbb{R})$. To begin we first reacquaint the reader with symplectic groups.

For any ring $\mathcal{R}$ the symplectic groups are defined to be the sets

$$\mathrm{Sp}_{2g}(\mathcal{R}) = \left\{ M \in GL_{2g}(\mathcal{R}) \mid {}^tM \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} M = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \right\}.$$

We have the following useful lemma which can be easily verified.

Lemma 1.62.

a) $\mathrm{Sp}_{2g}(\mathcal{R})$ *is closed under transposition.*

b) *Let* $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_{2g}(\mathcal{R})$ *where* α *is a* $g \times g$ *matrix. Then the following are equivalent:*

(i) $M \in \mathrm{Sp}_{2g}(\mathcal{R})$,

(ii) ${}^t\alpha\gamma$ *and* ${}^t\beta\delta$ *are symmetric and* ${}^t\alpha\delta - {}^t\gamma\beta = I_g$,

(iii) $\alpha^t\beta$ *and* $\gamma^t\delta$ *are symmetric and* $\alpha^t\delta - \beta^t\gamma = I_g$.

Proposition 1.63. *The group* $\mathrm{Sp}_{2g}(\mathbb{R})$ *acts biholomorphically from the left on* $\mathcal{H}_g$ *by*

$$Z \mapsto M(Z) := (\alpha Z + \beta)(\gamma Z + \delta)^{-1}$$

for all $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ *in* $\mathrm{Sp}_{2g}(\mathbb{R})$.

Proof. See Birkenhake-Lange [**7**, Proposition 8.2.2] □

Proposition 1.64. *Let Z, Z' be in $\mathcal{H}_g$. Then the following are equivalent:*

a) $(X_Z, H_Z) \cong (X_{Z'}, H_{Z'})$ *are isomorphic abelian varieties of polarization type D.*

b) $Z' = M(Z)$ *for some M in G_D, where*

$$G_D := \{M \in \mathrm{Sp}_{2g}(\mathbb{Q}) | {}^tM\Lambda_D \subseteq \Lambda_D\},$$

and $\Lambda_D = \left(\begin{smallmatrix} 0 & D \\ -D & 0 \end{smallmatrix}\right)\mathbb{Z}^{2g}$.

Proof. Suppose $\varphi : (X_{Z'}, H_{Z'}) \to (X_Z, H_Z)$ is an isomorphism. Choose symplectic bases so that the period matrices are $(Z'\ D)$ and $(Z\ D)$ respectively. Write R_a, R_r for the transformation matrices of the analytic and rational representations of φ respectively. From (1.47) we have $R_a(Z'\ D) = (Z\ D)R_r$ where both R_a and R_r are invertible. Rewrite this equation as

$$R_a(Z'\ I_g) = (Z\ I_g) \left(\begin{smallmatrix} I_g & 0 \\ 0 & D \end{smallmatrix}\right) R_r \left(\begin{smallmatrix} I_g & 0 \\ 0 & D \end{smallmatrix}\right)^{-1}.$$

Write $N = \left(\begin{smallmatrix} I_g & 0 \\ 0 & D \end{smallmatrix}\right) R_r \left(\begin{smallmatrix} I_g & 0 \\ 0 & D \end{smallmatrix}\right)^{-1} = {}^t\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ (the transpose is an artifact of our choice of notation for period matrices being $g \times 2g$ instead of $2g \times g$). Then $(R_aZ'\ R_a) = (Z^t\alpha + {}^t\beta\ Z^t\gamma + {}^t\delta)$. Since R_a is invertible, it follows that $Z' = (Z^t\gamma + {}^t\delta)^{-1}(Z^t\alpha + {}^t\beta)$. Taking transposes of both sides and remembering that both Z and Z' are symmetric matrices, we obtain $Z' = (\alpha Z + \beta)(\gamma Z + \delta)^{-1} = {}^tN(Z)$. Since $\varphi^* H_{Z'} = H_Z$ we have ${}^tR_r \left(\begin{smallmatrix} 0 & D \\ -D & 0 \end{smallmatrix}\right) R_r = \left(\begin{smallmatrix} 0 & D \\ -D & 0 \end{smallmatrix}\right)$, or equivalently ${}^tN \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} N = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$, hence N is a symplectic matrix with rational entries. Moreover we have $N\Lambda_D \subseteq \Lambda_D$ by definition of N. Taking $M = {}^tN$ proves the first implication. For the converse, if $Z' = M(Z)$ then the matrix $\left(\begin{smallmatrix} I_g & 0 \\ 0 & D \end{smallmatrix}\right)^{-1} M \left(\begin{smallmatrix} I_g & 0 \\ 0 & D \end{smallmatrix}\right)$ is the rational representation of an isomorphism $(X_{Z'}, H_{Z'}) \to (X_Z, H_Z)$ with respect to the symplectic bases determined by Z and Z'. □

Corollary 1.65. *The quotient space $\mathcal{H}_g/G_D$ is a moduli space for isomorphism classes of abelian varieties of polarization type D. In particular, $\mathcal{H}_g/\mathrm{Sp}_{2g}(\mathbb{Z})$ is a moduli space for isomorphism classes of principally polarized abelian varieties.*

Remark 1.66. From the above proof, observe that for any $Z \in \mathcal{H}_g$ and $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ in G_D, the isomorphism $\mu : X_Z \to X_{M(Z)}$ has representation matrices

$$\begin{aligned} \rho_a(\mu) &= {}^t(\gamma Z + \delta)^{-1} \\ \rho_r(\mu) &= \left(\begin{smallmatrix} I_g & 0 \\ 0 & D \end{smallmatrix}\right)^{-1} {}^tM^{-1} \left(\begin{smallmatrix} I_g & 0 \\ 0 & D \end{smallmatrix}\right) \end{aligned}$$

with respect to the chosen bases.

1.11. Classical theta functions

We now describe the classical Riemann theta functions. These functions have highly desirable properties. Their explicit presentation makes them ideal for computations, and the fact that they depend holomorphically on $\tau \in \mathcal{H}_g$ means they can be used in constructions of projective embeddings of moduli spaces.

Let τ be an element of $\mathcal{H}_g$. Suppose θ' is a theta function with respect to the lattice $\Lambda_\tau = \tau\mathbb{Z}^g \oplus \mathbb{Z}^g$ having automorphy factor $f(z, \lambda)$. By Frobenius'

Theorem 1.24, $\dim L(\theta') = 1$. That is to say θ' is the unique theta function (up to a scalar factor) for the lattice Λ_τ with automorphy factor f.

Define the Riemann theta function to be

$$\theta(z,\tau) = \sum_{m\in\mathbb{Z}^g} \mathbf{e}\left(\frac{1}{2}m\tau^t m + m^t z\right) .$$

Up to a scalar, it is the unique theta function with respect to Λ_τ having automorphy factor $f_0(z, \tau a + b) = \mathbf{e}(-\frac{1}{2}a\tau^t a - z^t a)$.

Let $c_1, c_2 \in \mathbb{R}^g$ be row vectors. Define the *(classical) theta function with characteristic* (c_1, c_2) to be

$$\theta\left[\begin{smallmatrix} c_1 \\ c_2 \end{smallmatrix}\right](z,\tau) = \sum_{m\in\mathbb{Z}^g} \mathbf{e}\left(\frac{1}{2}(m+c_1)\tau^t(m+c_1) + (m+c_1)^t(z+c_2)\right) .$$

It satisfies the functional equation

$$\theta\left[\begin{smallmatrix} c_1 \\ c_2 \end{smallmatrix}\right](z+\tau a+b,\tau) = \mathbf{e}\left(-\frac{1}{2}{}^t a\tau a - za + c_1 b - c_2 a\right)\theta\left[\begin{smallmatrix} c_1 \\ c_2 \end{smallmatrix}\right](z,\tau) .$$

Note that the Riemann theta function is just the theta function with characteristic $(0,0)$. The fact that the imaginary part of τ is positive definite ensures that the series converges absolutely and uniformly on every compact subset of $\mathbb{C}^g \times \mathcal{H}_g$. Hence $\theta\left[\begin{smallmatrix} c_1 \\ c_2 \end{smallmatrix}\right]$ is holomorphic on $\mathbb{C}^g \times \mathcal{H}_g$ for any characteristic (see [**7**, Proposition 8.5.4]).

Proposition 1.67.

a) *Let $D = \operatorname{diag}(d_1, ..., d_g)$ be a polarization type. Then $\theta\left[\begin{smallmatrix} c_1 \\ c_2 \end{smallmatrix}\right]$ is a theta function with automorphy factor f_0 with respect to the lattice $\tau\mathbb{Z}^g \oplus D\mathbb{Z}^g$ if and only if (c_1, c_2) is in $D^{-1}\mathbb{Z}^g \oplus \mathbb{Z}^g$.*

b) *The functions $\theta\left[\begin{smallmatrix} c_i \\ 0 \end{smallmatrix}\right]$ where c_i ranges over a set of representatives of $D^{-1}\mathbb{Z}^g/\mathbb{Z}^g$, form a basis of the vector space of classical theta functions for the divisor on $\mathbb{C}^g/(\tau\mathbb{Z}^g \oplus D\mathbb{Z}^g)$ with automorphy factor f_0.*

Proof. See [**7**, Remark 8.5.3]. □

Thus classical theta functions give a constructive proof of Frobenius' result in Theorem 1.24 that $\dim L(\theta) = d_1 \cdots d_g$.

There are numerous identities involving theta functions with characteristics. Two particular identities of future use to us are

$$\theta\left[\begin{smallmatrix} c_1+d_1 \\ c_2+d_2 \end{smallmatrix}\right](z,\tau) = \theta\left[\begin{smallmatrix} c_1 \\ c_2 \end{smallmatrix}\right](z,\tau) \tag{1.68}$$

which holds for all $c_i \in \mathbb{R}^g$ and all $d_i \in \mathbb{Z}^g$, as well as Igusa's transformation formula which is stated in a slightly weaker form below.

Theorem 1.69. *(Igusa's transformation formula) For all (z,τ) in $\mathbb{C}^g \times \mathcal{H}_g$, characteristics $c = (x,y) \in \mathbb{R}^{2g}$ and $M = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in \mathrm{Sp}_{2g}(\mathbb{Z})$, we have the formula*

$$\theta\left[\begin{smallmatrix}x'\\ y'\end{smallmatrix}\right]({}^t(\gamma\tau+\delta)^{-1}z, M(\tau)) = \zeta \mathbf{e}\left(\frac{1}{2}{}^t z(\gamma\tau+\delta)^{-1}z\right)\det(\gamma\tau+\delta)^{\frac{1}{2}}\theta\left[\begin{smallmatrix}x\\ y\end{smallmatrix}\right](z,\tau)$$

where $\zeta = \zeta(c,M)$ is an eighth root of unity and

$$(x',y') = (x,y)M^{-1} + \frac{1}{2}((\gamma^t\delta)_0, (\alpha^t\beta)_0)$$

where the notation X_0 is used to denote the row vector determined by the diagonal entries of X.

Proof. See [**36**, Chapter V]. □

1.12. Satake compactifications

Let Γ be a subgroup of finite index in $\mathrm{Sp}_{2n}(\mathbb{Z})$. The quotient $\mathcal{H}_n/\Gamma$ has a natural compactification called the *Satake compactification*.

1.12.1. Analytic description.

Let

$$D_n = \left\{V \in \mathbb{M}_n(\mathbb{C}) \mid {}^tV = V \text{ and } V\overline{V} < I_n\right\}$$

This is the image of $\mathcal{H}_n$ under the Cayley isomorphism

$$\Phi_n : \tau \mapsto (\tau - iI_n)(\tau + iI_n)^{-1}.$$

The action of Γ on $\mathcal{H}_n$ gives rise to an action on D_n which can be extended to the closure

$$\overline{D}_n = \left\{V \in \mathbb{M}_n(\mathbb{C}) \mid {}^tV = V \text{ and } V\overline{V} \leq I_n\right\}.$$

For $0 \leq r \leq n$ let $D_{n,r}$ be the image of the embedding of D_r in $\overline{D}_n$ given by $\tau \mapsto \left(\begin{smallmatrix}\tau & 0\\ 0 & I_{n-r}\end{smallmatrix}\right)$. Then

$$\overline{D}_n = \bigcup_{0\leq r\leq n} \bigcup_{g\in \mathrm{Sp}_{2n}(\mathbb{R})} gD_{n,r}\,.$$

Let

$$D_n^* = \bigcup_{0\leq r\leq n} \bigcup_{g\in \mathrm{Sp}_{2n}(\mathbb{Q})} gD_{n,r}\,.$$

The Satake compactification of $D_n/\Gamma \cong \mathcal{H}_n/\Gamma$ as a set is $D_n^*/\Gamma \cong \mathcal{H}_n^*/\Gamma$. It can be given the structure of a normal analytic space.

Example 1.70 (Satake compactification of $\mathcal{H}_1/\Gamma_1(2)$)**.** Define $\Gamma_n(r)$ to be the kernel of $\mathrm{Sp}_{2n}(\mathbb{Z}) \to \mathrm{Sp}_{2n}(\mathbb{Z}/r\mathbb{Z})$. Consider the situation for $n = 1$. We have $D_{1,1} = D_1 = \{v \in \mathbb{C} : |v| < 1\}$, $D_{1,0} = \{1\}$, $\Phi_1^{-1}D_1 = \mathcal{H}_1$ and $\Phi_1^{-1}D_{1,0} = \{i\infty\}$. So $\mathcal{H}_1^* = \mathcal{H}_1 \cup \mathrm{Sp}_2(\mathbb{Q})\{i\infty\}$ and the Satake compactification of $\mathcal{H}_1/\Gamma$ consists of the union of $\mathcal{H}_1/\Gamma$ together with the Γ-orbits of $\mathrm{Sp}_2(\mathbb{Q})\{i\infty\} = \mathbb{Q} \cup \{i\infty\}$ called *cusps*. The compactification of $X(1) = \mathcal{H}_1/\mathrm{Sp}_2(\mathbb{Z})$ has just one cusp since $\mathrm{Sp}_2(\mathbb{Q})\{i\infty\} = \mathrm{Sp}_2(\mathbb{Z})\{i\infty\}$. The compactification of $X(2) = \mathcal{H}_1^*/\Gamma_1(2)$ has three cusps with representatives $i\infty$, 0 and 1. The natural quotient map $X(2) \to X(1)$ is a Galois cover with Galois group $\mathrm{Sp}_2(\mathbb{Z})/\Gamma_1(2) \cong \mathrm{Sp}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$ which acts on the three cusps of $X(2)$ by permutations.

The following space we shall be studying in further detail later on.

Example 1.71. The Satake compactification of $\mathcal{H}_2/\Gamma_2(2)$ was studied by van der Geer [**72**]. It is is the union of $\mathcal{H}_2/\Gamma_2(2)$ plus 15 copies of $\mathcal{H}_1/\Gamma_1(2)$ and 15 points. Each one-dimensional boundary component is compactified by three of the 15 points (i.e. three cusps of $X(2)$) and each of the 15 points is a cusp of three copies of $\mathcal{H}_1/\Gamma_1(2)$.

1.12.2. Algebraic description.

Definition 1.72. *A Siegel modular form of weight k on Γ is a holomorphic function $f : \mathcal{H}_n \to \mathbb{C}$ satisfying*

$$f\left((\alpha\tau + \beta)(\gamma\tau + \delta)^{-1}\right) = \det(\gamma\tau + \delta)^k f(\tau) \text{ for all } \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in \Gamma.$$

The set of such functions form a vector space $M_k(\Gamma)$. Denote by

$$M^*(\Gamma) = \bigoplus_{k\geq 0} M_k(\Gamma)$$

the graded ring of Siegel modular forms. A theorem of Baily and Borel [**2**] says that for large enough k, a basis of $M_k(\Gamma)$ defines an embedding of $\mathcal{H}_n^*/\Gamma$ into projective space. Thus the Satake compactification is the projective variety given by $\mathrm{Proj}\, M^*(\Gamma)$ which contains $\mathcal{H}_g/\Gamma$ as an open dense subset.

1.13. Hilbert modular surfaces

To end this chapter, we look at an example of a moduli space parametrizing abelian surfaces with real multiplication $F \supsetneq \mathbb{Q}$. Table 1.57 implies that F must be a real quadratic field.

Let $\mathcal{O}$ be an order of F. Write

$$\widehat{\mathcal{O}} = \{x \in F \mid \mathrm{Tr}_{F/\mathbb{Q}}(xy) \in \mathbb{Z} \text{ for all } y \in \mathcal{O}\}$$

to denote the dual of $\mathcal{O}$ with respect to the trace. Let $\mathcal{M} = \mathcal{O} \oplus \mathfrak{a}$ with $\mathfrak{a} \subset \widehat{\mathcal{O}}$ an invertible $\mathcal{O}$-module. This is a $\mathbb{Z}$-module of rank 4 having an $\mathcal{O}$-module structure. By embedding this lattice into $\mathbb{C}^2$ we can form a complex torus with a natural $\mathcal{O}$-multiplication induced from the lattice.

Let us make the notion of $\mathcal{O}$-multiplication more precise.

Definition 1.73. *Let $(K, ')$ denote a skew field over $\mathbb{Q}$ with positive involution $'$ and let $\rho : K \to \mathbb{M}_g(\mathbb{C})$ be a representation. A polarized abelian variety with endomorphism structure $(K, ', \rho)$ is a triplet (X, H, ι) where*

a) *the pair (X, H) is a polarized abelian variety and $\iota : K \hookrightarrow \mathrm{End}^0(X)$ is equivalent to ρ after identifying $\mathrm{End}^0(A)$ with a subalgebra of $\mathbb{M}_g(\mathbb{C})$ via the analytic representation of X,*
b) *the Rosati involution of $\mathrm{End}^0(X)$ with respect to H extends to the involution $'$ on K via ι.*

If $R \subset K$ is a subring for which $\iota(R) \subset \mathrm{End}(X)$ we say that X has multiplication by R.

Note that for real quadratic fields the Rosati involution is trivial so the second condition is automatically satisfied.

We now make the notion of isomorphism precise.

Definition 1.74. *Suppose (X_1, H_1, ι_1) and (X_2, H_2, ι_2) are polarized abelian varieties with endomorphism structure $(K, ', \rho)$. An isomorphism of polarized abelian varieties with endomorphism structure $f : (X_1, H_1, \iota_1) \to (X_2, H_2, \iota_2)$ is an isomorphism $f : (X_1, H_1) \to (X_2, H_2)$ of polarized abelian varieties which preserves the endomorphism structure in the sense that $f \circ \iota_2(a) = \iota_1(a) \circ f$ for all $a \in F$.*

Now we shall construct abelian surfaces with multiplication by $\mathcal{O}$. First we need some notation. The two real embeddings $F \hookrightarrow \mathbb{R}$ give an isomorphism $F \otimes \mathbb{R} \cong \mathbb{R}^2$; identify $a \mapsto (a^{(1)}, a^{(2)})$ under this embedding. Write pairs $(a, b) \in (F \otimes \mathbb{R})^2$ as column vectors $\alpha = {}^t(a^{(1)}, b^{(1)}, a^{(2)}, b^{(2)})$. For $z = (z_1, z_2)$ in $\mathcal{H}_1^2$ define

$$\begin{array}{rcl} J_z : (F \otimes \mathbb{R})^2 & \to & \mathbb{C}^2 \\ \alpha & \mapsto & \left(\begin{smallmatrix} z_1 & 1 & 0 & 0 \\ 0 & 0 & z_2 & 1 \end{smallmatrix}\right) \alpha = \begin{pmatrix} a^{(1)} z_1 + b^{(1)} \\ a^{(2)} z_2 + b^{(2)} \end{pmatrix} \end{array}$$

which is an $\mathbb{R}$-linear isomorphism.

Proposition 1.75. *$J_z(\mathcal{M})$ is a lattice in $\mathbb{C}^2$ and $X_z = \mathbb{C}^2 / J_z(\mathcal{M})$ is a complex torus with real multiplication by $\mathcal{O}$ where the endomorphism structure $\rho : F \to \mathbb{M}_2(\mathbb{C})$ is given by $\rho(a) = \mathrm{diag}(a^{(1)}, a^{(2)})$. The Hermitian form*

$$H_z(x, y) = {}^t x \, \mathrm{diag}(\mathrm{Im}\, z_1, \mathrm{Im}\, z_2)^{-1} \, \overline{y} \, .$$

defines a polarization on X_z.

Proof. It is clear that $J_z(\mathcal{M})$ is a lattice when $z \in (\mathbb{C} \setminus \mathbb{R})^2$. The map $\rho(a) : (v_1, v_2) \mapsto (a^{(1)}v_1, a^{(2)}v_2)$ is linear and preserves $J_z(\mathcal{M})$, hence is an endomorphism of X_z. Thus ρ is an embedding of F into $\mathrm{End}^0(X_z)$, identifying $\mathcal{O}$ with $\mathrm{End}(X_z)$.

Observe that H_z is positive definite if and only if $z \in \mathcal{H}^2$. Let E_z denote $\operatorname{Im} H_z$. The matrix of $H_z(J_z(\alpha), J_z(\beta))$ is

$$ {}^t\mathrm{diag}\left((z_1\ 1), (z_2\ 1)\right) \cdot \mathrm{diag}\left(\operatorname{Im} z_1, \operatorname{Im} z_2\right)^{-1} \cdot \overline{\mathrm{diag}\left((z_1\ 1), (z_2\ 1)\right)}. $$

The imaginary part of this matrix is $\mathrm{diag}(T, T)$ where $T = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. From this we deduce that

$$ E_z(J_z(\alpha), J_z(\beta)) = \mathrm{Tr}_{F/\mathbb{Q}}({}^t\alpha \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \beta)\,. $$

Lastly, by construction of $\mathcal{M}$ this trace form takes integral values on $\mathcal{M}$ and hence H_z is a nondegenerate Riemann form. □

Remark 1.76. Changing $\mathcal{M}$ changes the polarization type: $\mathcal{O} \oplus \mathfrak{a}$ has polarization type (d_1, d_2) if and only if the elementary divisors of the quotient $\widehat{\mathcal{O}}/\mathfrak{a}$ are $[d_1, d_2]$. This can be seen from the trace form. In particular, $\mathcal{O} \oplus \widehat{\mathcal{O}}$ has principal polarization type.

The space $\mathcal{H}_1 \times \mathcal{H}_1$ is a moduli space for abelian surfaces with real multiplication given by F. We have a componentwise action of $\mathrm{Sp}_2(\mathbb{R}) \times \mathrm{Sp}_2(\mathbb{R})$ on $\mathcal{H}_1 \times \mathcal{H}_1$. Note that $\mathrm{Sp}_2 = \mathrm{SL}_2$ so the action on $\mathcal{H}_1$ is the usual action on the upper half plane by Mobius transformations. Define

$$ G(\mathcal{M}) = \{(M_1, M_2) \in \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R}) \mid \mathrm{diag}({}^tM_1, {}^tM_2)\mathcal{M} \subset \mathcal{M}\} $$

where we consider $\mathcal{M} \subset (F \otimes \mathbb{R})^2 = \mathbb{R}^4$. We have the following proposition.

Proposition 1.77. *Let z and z' be points of $\mathcal{H}_1 \times \mathcal{H}_1$. The polarized abelian varieties (X_z, H_z) and $(X_{z'}, H_{z'})$ with endomorphism structure (F, ρ) are isomorphic if and only if there is an M in $G(\mathcal{M})$ such that $z' = M(z)$.*

Proof. See Birkenhake-Lange [**7**, Proposition 9.2.2] □

Corollary 1.78. *The space $\mathcal{A}(\mathcal{M}) = \mathcal{H}_1 \times \mathcal{H}_1/G(\mathcal{M})$ is a moduli space for isomorphism classes of polarized abelian surfaces with endomorphism structure (F, ρ) associated to the F-module $\mathcal{M}$.*

The action of $G(\mathcal{M})$ on $\mathcal{H}_1 \times \mathcal{H}_1$ is proper and discontinuous, hence $\mathcal{A}(\mathcal{M})$ is a complex analytic variety of dimension 2 called a *Hilbert modular surface*.

Let $\mathcal{M} = \mathcal{O}_F \oplus \widehat{\mathcal{O}}_F$. By Remark 1.76 and the corollary above, $\mathcal{A}(\mathcal{M})$ parametrizes principally polarized abelian surfaces with real multiplication

by the maximal order $\mathcal{O}_F$. We already know that $\mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z})$ parametrizes all principally polarized abelian surfaces, so there exists a "forgetful map" $\mathcal{H}_1 \times \mathcal{H}_1/G(\mathcal{O}_F \oplus \widehat{\mathcal{O}}_F) \to \mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z})$ which maps the Hilbert modular surface into Siegel space. The image of such a map is subvariety of dimension 2 called a *Humbert surface*, which is the focus of the next chapter.

CHAPTER 2

Humbert Surfaces

Let A_τ be a principally polarized abelian surface determined by $\tau = \left(\begin{smallmatrix}\tau_1 & \tau_2\\ \tau_2 & \tau_3\end{smallmatrix}\right) \in \mathcal{H}_2$. An element of $\mathrm{End}(A_\tau)$ is given by equations

$$\begin{aligned} f \cdot \tau &= \tau\alpha + \beta \\ f \cdot \mathbf{1}_2 &= \tau\gamma + \delta = f \end{aligned}$$

with $f \in \mathbb{M}_2(\mathbb{C})$ and $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in \mathbb{M}_4(\mathbb{Z})$. Substituting the second equation into the first gives $\tau\gamma\tau + \delta\tau - \tau\alpha - \beta = 0$. Subtracting this from the transposed equation $\tau^t\gamma\tau + \tau^t\delta - {}^t\alpha\tau - {}^t\beta$ gives us

$$\tau({}^t\gamma - \gamma)\tau + \tau({}^t\delta + \alpha) + (-\delta - {}^t\alpha)\tau + (\beta - {}^t\beta) = 0\,.$$

This equation is nontrivial if and only if $f \notin \mathbb{Z} \cdot \mathbf{1}_2$, that is to say A_τ has extra endomorphisms. We obtain a quadratic equation in the matrix entries of τ called a Humbert equation. In this chapter we shall undertake a study of Humbert equations and their zero sets in the Siegel modular threefold $\mathcal{A}_2 = \mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z})$ known as Humbert surfaces. This exposition is largely based on [**8**, §4] which details the work of Humbert.

2.1. Real multiplication and Humbert surfaces

Let A_τ be a principally polarized abelian surface and let f be an endomorphism of A_τ. Recall from Section 1.7 that the analytic and algebraic representations of f are connected by the relation

$$\rho_{a,\tau}(f)(\tau\ I_2) = (\tau\ I_2)\rho_{r,\tau}(f). \tag{2.1}$$

Definition 2.2.

a) *An endomorphism f of an abelian variety X is said to be* symmetric *if it is fixed under the Rosati involution. Write*

$$\mathrm{End}^s(X) = \{f \in \mathrm{End}(X) : f^\dagger = f\}$$

to denote the subgroup of symmetric endomorphisms.

b) *An endomorphism $f \in \mathrm{End}(X)$ is said to be* primitive *if $\frac{1}{n}f \notin \mathrm{End}(X)$ for all integers $n > 1$.*

Lemma 2.3. *$f \in \mathrm{End}(A_\tau)$ is symmetric if and only if $\rho_r(f) = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & {}^t\alpha \end{smallmatrix}\right)$ with $\alpha = \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$, $\beta = \left(\begin{smallmatrix} 0 & b \\ -b & 0 \end{smallmatrix}\right)$, $\gamma = \left(\begin{smallmatrix} 0 & c \\ -c & 0 \end{smallmatrix}\right)$ whose coefficients satisfy*

$$a_2\tau_1 + (a_4 - a_1)\tau_2 - a_3\tau_3 + b(\tau_2^2 - \tau_1\tau_3) + c = 0\,. \tag{2.4}$$

Proof. The Rosati involution is the adjoint operator for the imaginary part of the Hermitian form H which has matrix $J = \left(\begin{smallmatrix} 0 & I_2 \\ -I_2 & 0 \end{smallmatrix}\right)$. In terms of matrices we have ${}^t\rho_r(f)J = J\rho_r(f^\dagger)$ for any endomorphism f, so $f = f^\dagger$ if and only if ${}^t\rho_r(f)J = J\rho_r(f)$, in which case $\rho_r(f)$ has the stated form. Using (2.1) we obtain $(\rho_a(f)\tau,\ \rho_a(f)) = (\tau\alpha + \gamma,\ \tau\beta + {}^t\alpha)$. Eliminating $\rho_r(f)$ produces the equality of skew symmetric matrices $\tau\beta\tau + {}^t\alpha\tau - \tau\alpha - \gamma = 0$ from which we obtain (2.4). □

Conversely, if $\tau = \left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{smallmatrix}\right) \in \mathcal{H}_2$ satisfies an equation of the form

$$a\tau_1 + b\tau_2 + c\tau_3 + d(\tau_2^2 - \tau_1\tau_3) + e = 0 \tag{2.5}$$

then $\mathrm{End}(A_\tau)$ contains a symmetric endomorphism f_0 with rational representation matrix

$$R_0 := \rho_r(f_0) = \begin{pmatrix} 0 & a & 0 & d \\ -c & b & -d & 0 \\ 0 & e & 0 & -c \\ -e & 0 & a & b \end{pmatrix}.$$

Following Humbert, we call an equation of the form (2.5) a *singular relation*.

Observe that if $\gcd(a, b, c, d, e) = 1$ then f_0 is primitive; in this case we shall call the corresponding singular relation *primitive*. Also, note that if f is scalar multiplication by n then $\rho_r(f) = nI_4$ trivially satisfies (2.4). By Lemma 2.3 we have that $n + mf_0$ are symmetric endomorphisms of A_τ.

Proposition 2.6. *The subset of endomorphisms $\{n + mf_0 : n, m \in \mathbb{Z}\} \subset \mathrm{End}^s(X)$ is a ring isomorphic to $\mathbb{Z}[t]/(t^2 - bt + ac + de)$, a quadratic order of discriminant $\Delta(f_0) = b^2 - 4ac - 4de$.*

Proof. From (2.1), the analytic representation matrix of f_0 is seen to be

$$\rho_a(f_0) = \tau\begin{pmatrix} 0 & d \\ -d & 0 \end{pmatrix} + \begin{pmatrix} 0 & a \\ -c & b \end{pmatrix} = \begin{pmatrix} -d\tau_2 & d\tau_1 - c \\ -d\tau_3 + a & d\tau_2 + b \end{pmatrix}$$

which has trace b and determinant

$$-d\big(a\tau_1 + b\tau_2 + c\tau_3 + d(\tau_2^2 - \tau_1\tau_3)\big) + ac = ac + de$$

since (2.5) holds. As f_0 satisfies its analytic characteristic polynomial $f_0^2 - bf_0 + ac + de = 0$, we have that the map $\{n + mf_0 : n, m \in \mathbb{Z}\} \to \mathbb{Z}[t]/(t^2 - bt + ac + de)$ which sends $f_0 \mapsto t$ is a ring isomorphism. □

Definition 2.7. *The discriminant of a singular relation* (2.5) *is defined to be* $\Delta = b^2 - 4ac - 4de$.

So far we have studied singular relations on $\mathcal{H}_2$. Humbert showed that under the natural projection $\mathcal{H}_2 \to \mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z}) = \mathcal{A}_2$, all singular relations with the same discriminant define zero sets in $\mathcal{H}_2$ which are equivalent under the action of $\mathrm{Sp}_4(\mathbb{Z})$ and conversely.

Lemma 2.8. *Let f_0 be a primitive symmetric endomorphism of discriminant $\Delta = 4k + \ell$ with $\ell \in \{0, 1\}$. There exists a matrix $M \in \mathrm{Sp}_4(\mathbb{Z})$ such that*

$$ {}^tM^{-1}\rho_r(f_0)\,{}^tM = \begin{pmatrix} \alpha & 0 \\ 0 & {}^t\alpha \end{pmatrix} \text{ where } \alpha = \begin{pmatrix} 0 & k \\ 1 & \ell \end{pmatrix}. $$

Proof. The reader is referred to either the article by Birkenhake-Wilhelm [**8**] or Runge [**64**] for a constructive algorithm. □

Theorem 2.9. *(Humbert's Lemma) Let $\tau = \left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{smallmatrix}\right) \in \mathcal{H}_2$ satisfy the singular relation*

$$ a\tau_1 + b\tau_2 + c\tau_3 + d(\tau_2^2 - \tau_1\tau_3) + e = 0 $$

of discriminant $\Delta = b^2 - 4ac - 4de$. Then there is a matrix $M \in \mathrm{Sp}_4(\mathbb{Z})$ such that $M(\tau) = \left(\begin{smallmatrix} \tau_1' & \tau_2' \\ \tau_2' & \tau_3' \end{smallmatrix}\right)$ satisfies a unique normalized singular relation of the form

$$ k\tau_1' + \ell\tau_2' - \tau_3' = 0 $$

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

Proof. Without loss of generality we can assume $\gcd(a, b, c, d, e) = 1$. Remark 1.66 implies that the rational representations $\rho_{r,\tau}$ and $\rho_{r,M(\tau)}$ are related by

$$ \rho_{r,M(\tau)} = {}^tM^{-1}\rho_{r,\tau}\,{}^tM. $$

Thus it suffices to find a matrix $M \in \mathrm{Sp}_4(\mathbb{Z})$ such that

$$ {}^tM^{-1}\rho_{r,\tau}(f_0)^tM = \begin{pmatrix} A & 0 \\ 0 & {}^tA \end{pmatrix} \text{ where } A = \begin{pmatrix} 0 & k \\ 1 & \ell \end{pmatrix}. $$

This is the content of the previous lemma. □

Corollary 2.10. *Let A be a principally polarized abelian surface. The following are equivalent:*

a) *$A \cong A_\tau$ for some $\tau \in \mathcal{H}_2$ satisfying*

$$ a\tau_1 + b\tau_2 + c\tau_3 + d(\tau_2^2 - \tau_1\tau_3) + e = 0. $$

b) *$\mathrm{End}^s(A)$ contains a subring isomorphic to a real quadratic order $\mathbb{Z}[t]/(t^2 - bt + ac + de)$ of discriminant $\Delta = b^2 - 4ac - 4de$,*

c) *$\mathrm{End}(A)$ contains a symmetric endomorphism f_Δ with discriminant $\Delta = b^2 - 4ac - 4de$.*

For any $\Delta \equiv 0$ or $1 \bmod 4$, define

$$\begin{aligned} H_\Delta &:= \left\{ \tau \in \mathcal{A}_2 \ : \ \begin{array}{c} \tau \text{ satisfies a primitive singular} \\ \text{relation of discriminant } \Delta \end{array} \right\} \\ &= \{ A_\tau \in \mathcal{A}_2 \ : \ \mathrm{End}^s(A_\tau) \ni f \text{ primitive}, \Delta(f) = \Delta \}. \end{aligned}$$

Proposition 2.11. *Let $\Delta \equiv 0$ or 1 mod 4. We have that $H_\Delta = \emptyset$ for $\Delta < 0$ and $H_0 = \mathcal{A}_2$. If $\Delta > 0$ then H_Δ is a surface which we call a* Humbert surface of discriminant Δ.

Proof. Suppose $A_\tau \in H_\Delta$ with principal polarization given by a Hermitian form H. Let $f \in \mathrm{End}^s(A_\tau)$ have discriminant Δ. Write $F = \rho_a(f)$ and consider the form $H'(z,w) = H(Fz, w)$. Clearly H' is linear in z and conjugate linear in w. Since the Rosati involution is the adjoint operator for H and f is symmetric, we have $H(Fz,w) = H(z, F^\dagger w) = H(z, Fw)$ and so

$$H'(w,v) = H(Fw, v) = H(w, Fv) = \overline{H(Fv, w)} = \overline{H'(v,w)}.$$

Thus H' is hermitian. If λ is an eigenvalue of F with eigenvector v then $H'(v,v) = H(Fv,v) = \lambda H(v,v)$. Therefore the two eigenvalues of F are real. If λ_1 and λ_2 are the eigenvalues of F then the discriminant of f equals $\Delta = (\lambda_1 - \lambda_2)^2 \geq 0$. Hence $H_\Delta = \emptyset$ when $\Delta < 0$. If $\Delta = 0$ then $\lambda_1 = \lambda_2$ then f is scalar multiplication by λ_1 which is contained in $\mathrm{End}(A_\tau)$ for all $\tau \in \mathcal{A}_2$, hence $H_0 = \mathcal{A}_2$. □

Example 2.12. A point $\left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{smallmatrix}\right)$ in H_1 can be described by the singular relation $\tau_2 = 0$. The corresponding principally polarized abelian surface A_τ is isomorphic to the product of two elliptic curves $E_1 \times E_2$ with j-invariants $j(\tau_1)$ and $j(\tau_2)$ respectively.

In more generality, we will show that abelian surfaces which are isogenous to products of elliptic curves lie on Humbert surfaces of square discriminant.

Lemma 2.13. *Suppose (X, H) is a non-simple principally polarized abelian surface. There exists m for which there is an isogeny of degree m^2:*

$$(X, H) \to (Y, H|_Y) \times (Z, H|_Z)$$

where Y and Z are elliptic curves and the induced polarizations have degree m.

Proof. The existence of an isogeny is the contents of Poincaré's Complete Reducibility Theorem 1.49. See [**7**, Corollary 12.1.2] for a proof that the induced polarizations have the same degree. □

Proposition 2.14. *Let m be a positive integer. The Humbert surface H_{m^2} is a moduli space for isomorphism classes of principally polarized abelian surfaces which split as a product of two elliptic curves via an isogeny of degree m^2.*

Proof. Suppose $\mathrm{End}(A_\tau)$ contains a symmetric endomorphism f of discriminant m^2. The eigenvalues of its analytic representation are integers λ and μ and since $m^2 = (\lambda - \mu)^2 > 0$ we know that $\lambda \neq \mu$. The endomorphism $f - \mu$ has characteristic equation $t^2 - mt = 0$ hence the image $\mathrm{im}(f - \mu) = E_1$ is a one dimensional abelian subvariety. Then the complementary abelian subvariety $\mathrm{im}(m - (f - \mu)) = \mathrm{im}(f - \lambda) = E_2$ is one dimensional and the theory of norm-endomorphisms [**7**, §5.3] gives us an isogeny $A_\tau \to E_1 \times E_2$ of the correct degree. Conversely given a degree m^2 isogeny as in the proposition, the theory of norm-endomorphisms produces a symmetric endomorphism of the desired discriminant. □

The following proposition summarises the moduli interpretation results of this section.

Proposition 2.15. *Let $\Delta \neq \Delta'$ be squarefree discriminants. We have the following:*

a) *A_τ is simple if and only if $\tau \notin \bigcup_{m>0} H_{m^2}$.*
b) *If $\tau \in H_\Delta$ then $\mathrm{End}^0(A_\tau)$ contains $\mathbb{Q}(\sqrt{\Delta})$.*
c) *If $\tau \in H_\Delta \cap H_{\Delta'}$ then either A_τ is simple and $\mathrm{End}^0(A_\tau)$ is a totally indefinite quaternion algebra over $\mathbb{Q}$, or A_τ is isogenous to $E \times E$ where E is an elliptic curve.*

Proof. The first two statements are clear. If $\tau \in H_\Delta \cap H_{\Delta'}$ then $\mathrm{End}^s(A_\tau) \otimes \mathbb{Q}$ contains both $\mathbb{Q}(\sqrt{\Delta})$ and $\mathbb{Q}(\sqrt{\Delta'})$, hence the dimension of $\mathrm{End}^0(\mathcal{A}_\tau)$ as a $\mathbb{Q}$-vector space is at least 3. From Example 1.58, the only possibilities for $\mathrm{End}^0(\mathcal{A}_\tau)$ with this restriction are indefinite quaternion algebras in which case A_τ is simple, or $\mathbb{M}_2(k)$ in which case A_τ is isogenous to $E \times E$ where E is a CM elliptic curve with $\mathrm{End}^0(E) = k$. □

2.2. Humbert surface embeddings

To end this chapter, we construct a map $\mathcal{H}_1 \times \mathcal{H}_1 \hookrightarrow \mathcal{H}_2$ which induces the "forgetful map", showing that the Humbert surface of discriminant Δ can be represented as the embedding of a Hilbert modular surface for $\mathbb{Q}(\sqrt{\Delta})$.

Let F be a real quadratic field with discriminant Δ_0 and ring of integers $\mathcal{O}_F$. Let $\mathcal{O}_f$ be a suborder in $\mathcal{O}_F$ of index f . Choose a basis u_1, u_2 of

$$\widehat{\mathcal{O}}_f = \{x \in F \mid \mathrm{Tr}(xy) \in \mathbb{Z} \text{ for all } y \in \mathcal{O}_f\},$$

the dual of $\mathcal{O}_f$ with respect to the trace. Set $R = \left(\begin{smallmatrix} u_1 & u_1' \\ u_2 & u_2' \end{smallmatrix}\right)$, where u_i' is the Galois conjugate of u_i.

Proposition 2.16. *Define an embedding*

$$\begin{aligned} \rho_R : \quad \mathcal{H}_1^2 &\to \mathcal{H}_2 \\ (z_1, z_2) &\mapsto R \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} {}^t R \,. \end{aligned}$$

The image of $\mathcal{H}^2$ in $\mathcal{H}_2$ is a given by a Humbert singular relation of discriminant $\Delta_0 f^2$.

Proof. Firstly observe that R is in $\mathrm{GL}_2(\mathbb{R})$ since the u_i form a basis of a totally real field. This shows that ρ_R is injective. The image of the map is seen to consist of symmetric matrices and since $\mathrm{Im}\, z_i > 0$, the relation

$$\mathrm{Im}\, \left(R \left(\begin{smallmatrix} z_1 & 0 \\ 0 & z_2 \end{smallmatrix}\right) {}^t R \right) = R \left(\begin{smallmatrix} \mathrm{Im}\,(z_1) & 0 \\ 0 & \mathrm{Im}\,(z_2) \end{smallmatrix}\right) {}^t R \;>\; 0$$

shows that the image of ρ_R lies in $\mathcal{H}_2$. Let $\tau = \left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{smallmatrix}\right) = \rho_R(\left(\begin{smallmatrix} z_1 & 0 \\ 0 & z_2 \end{smallmatrix}\right))$. Then

$$\begin{aligned} \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} &= R^{-1} \tau \, {}^t R^{-1} \\ &= (\det R)^{-2} \begin{pmatrix} u_2' & -u_1' \\ -u_2 & u_1 \end{pmatrix} \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \begin{pmatrix} u_2' & -u_2 \\ -u_1' & u_1 \end{pmatrix} . \end{aligned}$$

It follows that the only restriction on τ is given by the relation obtained from an off-diagonal entry:

$$(\det R)^{-2}(-u_2 u_2' \tau_1 + (u_1' u_2 + u_1 u_2')\tau_2 - u_1 u_1' \tau_3) = 0.$$

Take $x_1 = 1, x_2 = w$ as our fixed basis of $\mathcal{O}_f$ where w has discriminant $\Delta := \Delta_0 f^2 = 4k + \ell$ and satisfies $w^2 - \ell w - k = 0$ with $\ell \in \{0, 1\}$. Define the trace matrix $T = (\mathrm{Tr}(x_i x_j))$. Then a basis for $\widehat{\mathcal{O}}_f$ is given by

$$\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = T^{-1} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \Delta^{-1} \begin{pmatrix} \ell^2 + 2k & -\ell \\ -\ell & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} .$$

By writing the u_i, u_i' in terms of the basis of $\mathcal{O}_f$, we compute that

$$\begin{aligned} (\det R)^{-2} &= \Delta, \\ u_2 u_2' &= N(u_2) = -\Delta^{-1}, \\ u_1' u_2 + u_1 u_2' &= \mathrm{Tr}(u_1' u_2) = \ell \Delta^{-1}, \\ u_1 u_1' &= N(u_1) = k \Delta^{-1}. \end{aligned}$$

Thus we obtain the Humbert equation

$$\tau_1 - \ell \tau_2 - k \tau_3 = 0$$

which has discriminant $\ell^2 + 4k = 4k + \ell = \Delta$ since $\ell \in \{0, 1\}$. This completes the proof. □

Denote by $\mathrm{SL}_2(\mathcal{O}_f, \widehat{\mathcal{O}}_f) \subset \mathrm{SL}_2(F)$ the group

$$\left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(F) \mid \alpha, \delta \in \mathcal{O}_f,\ \gamma \in \widehat{\mathcal{O}}_f,\ \beta \in \widehat{\mathcal{O}}_f^{-1} \right\}$$

which acts on $\mathcal{H}_1^2$ in the following manner:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} (z_1, z_2) = \left(\frac{\alpha z_1 + \beta}{\gamma z_1 + \delta}\, , \frac{\alpha' z_2 + \beta'}{\gamma' z_2 + \delta'} \right).$$

Under the identification $\mathrm{SL}_2(F) \hookrightarrow \mathrm{SL}_2(F \otimes \mathbb{R}) \cong \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$, one can verify that $\mathrm{SL}_2(\mathcal{O}_f, \widehat{\mathcal{O}}_f)$ is the same as the group $G(\mathcal{O}_f \oplus \widehat{\mathcal{O}}_f)$ defined at the end of the last chapter.

Define a homomorphism

$$\begin{array}{rcl} \varphi_R : \mathrm{SL}_2(\mathcal{O}_f, \widehat{\mathcal{O}}_f) & \to & \mathrm{Sp}_4(\mathbb{Z}) \\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} & \mapsto & \begin{pmatrix} R & 0 \\ 0 & {}^tR^{-1} \end{pmatrix} \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ \overline{\gamma} & \overline{\delta} \end{pmatrix} \begin{pmatrix} R^{-1} & 0 \\ 0 & {}^tR \end{pmatrix} \end{array}$$

where $\overline{x}$ stands for $\begin{pmatrix} x & 0 \\ 0 & x' \end{pmatrix}$, $x \in F$.

Proposition 2.17. *(*[**72**, p. 328]*) The maps ρ_R and φ_R give rise to a commutative diagram*

$$\begin{array}{ccc} \mathcal{H}_1^2 & \xrightarrow{\rho_R} & \mathcal{H}_2 \\ {\scriptstyle \Gamma}\downarrow & & \downarrow{\scriptstyle \varphi_R(\Gamma)} \\ \mathcal{H}_1^2/\Gamma \cup \Gamma\sigma & \xrightarrow{\rho} & \mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z}) \end{array}$$

where $\Gamma = \mathrm{SL}_2(\mathcal{O}_f, \widehat{\mathcal{O}}_f)$, σ is the involution $(z_1, z_2) \mapsto (z_2, z_1)$ of $\mathcal{H}_1^2$, and where ρ is a map generically of degree 1 onto the Humbert surface H_Δ.

The analytic quotient space $\mathcal{H}^2/\Gamma \cup \Gamma\sigma$ is called a *symmetric Hilbert modular surface*. The involution σ identifies abelian surfaces whose real multiplication differ by conjugation.

The picture for square discriminants is similar. See [**72**, p. 328].

CHAPTER 3

Computing Humbert Surfaces

The aim of this chapter is to produce algebraic models for Humbert surfaces. Igusa [**31**] showed that the Satake compactification of the Siegel modular threefold $\mathcal{A}_2 = \mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z})$ is $\mathrm{Proj}\,\mathbb{C}[\psi_4, \psi_6, \chi_{10}, \chi_{12}]$, a weighted projective space with weights indicated by subscripts. The Siegel modular threefold is open and dense in the Satake compactification and has function field $\mathbb{C}(j_1, j_2, j_3)$ where $j_i(\tau)$ are algebraically independent modular functions of weight zero. It follows from the last chapter that for every positive discriminant Δ there is an irreducible polynomial $H_\Delta(j_1, j_2, j_3)$ whose zero set is the Humbert surface of discriminant Δ. Unfortunately working with this model is impractical due to the enormous degrees and coefficients of the polynomial. One fares better by working in a finite cover of the moduli space, adding some level structure. Runge [**64**] constructed an algorithm to compute Humbert components in the cover $\mathcal{H}_2/\Gamma^*(2,4)$ using theta functions and their Fourier expansions. We shall apply Runge's method to various practical models of $\mathcal{A}_2(2) = \mathcal{H}_2/\Gamma(2)$, the Siegel modular threefold with level-2 structure.

3.1. Fourier expansions of theta functions

As we shall be working exclusively with theta functions of half integral characteristics throughout this chapter, such objects warrant special notation. Let $m = (m_1, \ldots, m_{2g})$ be an integer row vector. Set $m' = (m_1, \ldots, m_g)$ and $m'' = (m_{g+1}, \ldots, m_{2g})$. We write $\theta_m(z,\tau)$ to denote the theta function with half integral characteristics given by $\theta\left[\begin{smallmatrix} \frac{1}{2}m' \\ \frac{1}{2}m'' \end{smallmatrix}\right](z,\tau)$. Define the *theta constant* $\theta_m(\tau)$ by setting $z = 0$ in $\theta_m(z,\tau)$, which has the Fourier expansion

$$\theta_m(z,\tau) = \sum_{p \in \mathbb{Z}^g} \mathbf{e}\left(\frac{1}{2}\left(p + \frac{m'}{2}\right)\tau\,{}^t\!\left(p + \frac{m'}{2}\right) + \left(p + \frac{m'}{2}\right){}^t\!\left(z + \frac{m''}{2}\right)\right).$$

Igusa [**33**] shows that the quotients θ_m/θ_n are modular functions for the group $\Gamma_g(4,8)$ where

$$\Gamma_g(2k,4k) = \left\{\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \Gamma_g(2k) \mid (\alpha\,{}^t\!\beta)_0 \equiv (\gamma\,{}^t\!\delta)_0 \equiv 0 \pmod{4k}\right\}$$

is a normal subgroup of $\Gamma_g(1)$ having index 2^{2g} in $\Gamma_g(2k)$.

Let us describe the Fourier expansion of theta constants restricted to a Humbert surface of discriminant $\Delta \equiv 0$ or $1 \bmod 4$, adapted from ideas in Runge's paper [**64**]. Write $\Delta = 4k + \ell$ where ℓ is either 0 or 1, and k is uniquely determined. From Humbert's Lemma 2.9, the Humbert surface of discriminant Δ can be defined by the set

$$H_\Delta = \left\{ \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & k\tau_1 + \ell\tau_2 \end{pmatrix} \in \mathcal{H}_2 \right\}$$

modulo the usual $\mathrm{Sp}_4(\mathbb{Z})$ equivalence relation. Let a, b, c, d be integers. If we restrict the theta constant θ_{abcd} to H_Δ we get

$$\theta_{abcd}(\tau) = \sum_{(x_1,x_2)\in\mathbb{Z}^2} e^{\pi i(x_1c+x_2d)} r^{(2x_1+a)^2+k(2x_2+b)^2} q^{2(2x_1+a)(2x_2+b)+\ell(2x_2+b)^2}$$

where $r = e^{2\pi i\tau_1/8}$ and $q = e^{2\pi i\tau_2/8}$. Unfortunately q has negative exponents which computationally makes it difficult to work with this expansion. To overcome this difficulty, make the invertible substitution $r = pq$ to produce the expansion

$$\sum_{(x_1,x_2)\in\mathbb{Z}^2} (-1)^{x_1c+x_2d} p^{(2x_1+a)^2+k(2x_2+b)^2} q^{(2x_1+a+2x_2+b)^2+(k+\ell-1)(2x_2+b)^2}$$

which is computationally more favourable, being a power series with integer coefficients. Call the above expansion the *Fourier expansion of* θ_{abcd} *restricted to* H_Δ.

At a later stage we will need to know how to invert elements of $\mathbb{Q}[[p, q]]$ where possible. It is well known fact about power series rings that if $f(p, q)$ is in $\mathbb{Q}[[p, q]]$ with $f(0, 0) \neq 0$, then $f(p, q)$ is a unit with inverse given by the geometric series

$$f(0,0)^{-1} \sum_{n\geq 0} \left(1 - \frac{f(p,q)}{f(0,0)}\right)^n.$$

An implementation on a computer uses truncated Fourier expansions, where arithmetic is done in $\mathbb{Q}[[p, q]]/(p^N, q^N)$ for some positive N. It is easy to see that the geometric ratio has zero constant term, in particular $(1 - f/f(0, 0))^k \in (p^N, q^N)$ for $k \geq N$ so the above formula converges to the truncated expansion of f^{-1} for any chosen precision.

3.2. Degree formula

To compute equations for Humbert surfaces it is desirable to know the degree of the polynomial relation in advance. Fortunately much arithmetic-geometric information is known about Humbert surfaces and more generally Hilbert modular surfaces (see [**28**], [**73**]). We begin with a lemma.

Lemma 3.1. *The subgroup of* $\mathrm{Sp}_4(\mathbb{Z})$ *which fixes points* $\tau \in \mathcal{H}_2$ *satisfying a singular relation*

$$a\tau_1 + b\tau_2 + c\tau_3 + d(\tau_2^2 - \tau_1\tau_3) + e = 0$$

of discriminant $\Delta = b^2 - 4ac - 4de$ *has order* 2 *if* $\Delta = 1$ *or* 4 *and is trivial otherwise.*

Proof. Gottschling determined all fixed points and their isotropy subgroups. From [**20**, Satz 3] the 2-dimensional families of fixed points are seen to satisfy singular relations of discriminants 1 and 4, both having nontrivial isotropy groups of order 2. One can verify that the discriminant 1 points given by $\tau_2 = 0$ are fixed by $\mathrm{diag}(-1, 1, -1, 1)$ and the singular relation $\tau_1 = \tau_3$ of discriminant 4 is fixed by the matrix $\left(\begin{smallmatrix} U & 0 \\ 0 & U \end{smallmatrix}\right)$ with $U = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. □

This motivates the following:

Definition 3.2. *The order of the isotropy subgroup of* H_Δ *in* $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$ *is*

$$v(\Delta) = \begin{cases} \frac{1}{2} & \text{if } \Delta = 1 \text{ or } 4, \\ 1 & \text{otherwise.} \end{cases}$$

Note that we can make a similar definition for Humbert surface components in $\Gamma\backslash\mathcal{H}_2$ where Γ is a *normal* subgroup of $\mathrm{Sp}_4(\mathbb{Z})$.

Define $\Gamma_0(N) \leq \mathrm{SL}_2(\mathbb{Z})$ by

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv 0 \pmod{N} \right\}.$$

As $\Gamma_0(4) \subset \Gamma_1(4, 8)$, it follows that the genus 1 theta functions of half integral characteristics $\theta_{00}, \theta_{01}, \theta_{10}, \theta_{11}$ are modular forms of half integral weight for $\Gamma_0(4)$. Define

$$C(\tau) = \frac{1}{4}\theta_{00}(\tau)(\theta_{00}(\tau)^4 - 5\theta_{10}(\tau))^4.$$

(This is misprinted in [**64**, p. 10]). The Fourier coefficients have arithmetical significance.

Lemma 3.3. *The Fourier expansion of* $C(\tau)$ *has the form*

$$1 - \sum_{\Delta > 0} a_\Delta q^\Delta, \quad q = e^{2\pi i\tau}$$

where $a_\Delta = 0$ *if* $\Delta \equiv 2, 3 \pmod 4$*, and*

$$a_\Delta - 24 \sum_{x \in \mathbb{Z}} \sigma_1\left(\frac{\Delta - x^2}{4}\right) = \begin{cases} 12\Delta - 2 & \text{if } \Delta \text{ is a square}, \\ 0 & \text{otherwise} \end{cases} \tag{3.4}$$

when $\Delta \equiv 0, 1 \pmod 4$.

Proof. The function $\frac{1}{120}C(\tau)$ is studied in Henri Cohen's article [**12**]. There, the Fourier coefficient of q^N is denoted $H(2,N)$ and the corresponding formula for these numbers is given in [**12**, Proposition 4.1]. □

Δ	1	4	5	8	9	12	13	16	17	20	21	24	25
a_Δ	10	70	48	120	250	240	240	550	480	528	480	720	1210

TABLE 1. First few values of a_Δ.

Define the Humbert surface divisor

$$G_\Delta = \sum_{\substack{x\geq 1\\ x^2|\Delta}} v(\Delta/x^2) H_{\Delta/x^2}.$$

We now state a famous result of van der Geer, from which the degree of any Humbert surface component in any Galois cover can be derived.

Theorem 3.5. *(*[**28**, Theorem 8.10]*) The degree of G_Δ equals $\frac{1}{2}a_\Delta$. In particular, we have*

$$\sum_{\substack{x\geq 1\\ x^2|\Delta}} v(\Delta/x^2)\deg(H_{\Delta/x^2}) = \frac{1}{2}a_\Delta.$$

which allows one to compute the degree of H_Δ recursively.

What this says is that H_Δ is the zero divisor of a Siegel modular form and the weight can be determined by the theorem. Computing these modular forms is the ultimate goal of this chapter.

3.3. Runge's method

We describe an algorithm to find an irreducible component of H_Δ in any finite cover of $\mathcal{A}_2$.

First we describe Runge's computations. Define $\Gamma^*(2,4) \trianglelefteq \Gamma(2,4)$ by the exact sequence [**63**, Lemma 2.1]:

$$1 \to \Gamma^*(2,4) \to \Gamma(2,4) \to \langle \mathrm{diag}(-1,1,-1,1)\rangle \to 1\,.$$

It is a normal subgroup of $\mathrm{Sp}_4(\mathbb{Z})$ of index 23040. Runge [**64**] showed that the Satake compactification of $\mathcal{H}_2/\Gamma^*(2,4)$ is isomorphic to $\mathbb{P}^3$ with homogeneous coordinate ring generated by four theta constants $f_0 = \theta_{0000}$, $f_1 = \theta_{0100}$, $f_2 = \theta_{1000}$, $f_3 = \theta_{1100}$. By writing out Fourier expansions of the f_i restricted to H_Δ to high enough precision, he was able to find a polynomial relation between the f_i. This is a *component* of the Humbert surface in $\mathcal{H}_2/\Gamma^*(2,4)$ which maps down to H_Δ in $\mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z})$ under the quotient map.

Since $\Gamma^*(2,4)$ is normal in $\mathrm{Sp}_4(\mathbb{Z})$, all Humbert components $F_{\Delta,i}$ are hypersurfaces in $\mathcal{H}_2/\Gamma^*(2,4)$ of the same degree. The quotient group $\mathrm{Sp}_4(\mathbb{Z})/\Gamma^*(2,4)$ acts on the set of components. By determining the number of components and the isotropy groups, Theorem 3.5 is used to produce a degree formula for Humbert components in this model.

Proposition 3.6. *(*[**64**, p. 10]*) The number of Humbert components in* $\mathcal{H}_2/\Gamma^*(2,4)$ *is*

$$m(\Delta) = \begin{cases} 10 & \text{if } \Delta \equiv 1 \bmod 8, \\ 60 & \text{if } \Delta \equiv 0 \bmod 4, \\ 6 & \text{if } \Delta \equiv 5 \bmod 8. \end{cases}$$

The degree of any Humbert component $F_{\Delta,i}$ *in* $\mathcal{H}_2/\Gamma^*(2,4)$ *is given by a recursive formula*

$$a_\Delta = \sum_{x>0} v(\Delta/x^2) m(\Delta/x^2) \deg(F_{(\Delta/x^2),i})$$

where

$$v(x) = \begin{cases} 1/2 & \text{if } x = 1 \\ 1 & \text{if } x \geq 2, x \equiv 0, 1 \bmod 4 \\ 0 & \text{otherwise} \end{cases}$$

and a_Δ *is the coefficient of Cohen's modular form calculated using* (3.4).

Δ	1	4	5	8	9	12	13	16	17	20	21	24
$\deg(F_{\Delta,i})$	2	1	8	2	24	4	40	8	48	8	80	12
Δ	25	28	29	32	33	36	37	40	41	44	45	48
$\deg(F_{\Delta,i})$	120	16	120	16	144	24	200	28	192	28	240	32
Δ	49	52	53	56	57	60	61	64	65	68	69	72
$\deg(F_{\Delta,i})$	336	40	280	40	336	48	440	64	384	48	480	60

TABLE 2. Degrees of Runge Humbert components.

The algorithm is very simple. We have f_0, f_1, f_2, f_3 represented as truncated power series. We know the degree of the relation we are searching for. To find an algebraic relation of degree d, compute all homogeneous monomials in the f_i of degree d and use linear algebra to find linear dependencies between the monomials.

Using this method, Runge computed equations of Humbert components whose degree was at most 16. By making use of observed symmetries of $\Gamma^*(2,4)/\mathrm{Sp}_4(\mathbb{Z})$ that fix Humbert components we are able to compute components whose degrees are at most 48, which includes all the even non-square discriminants less than 70 (see [**22**]).

We now generalize this method to any finite cover:

Algorithm 3.7. Let $\phi : \mathcal{A}' \to \mathcal{A}_2$ be a finite cover of $\mathcal{A}_2$. Then the preimage $\phi^{-1}H_\Delta$ is a union of Humbert components $H_\Delta^{(i)}$. Given functions $\{f_i(\tau)\}_{i=1,\ldots,n}$ generating the function field of $\mathcal{A}'$, compute $H_\Delta^{(i)}(f_1,\ldots,f_n)$ as follows:

a) Calculate the degree of the Humbert components $H_\Delta^{(i)}$ (given by a formula).
b) Compute power series representations of the $f_i(\tau)$ restricted to $H_\Delta \subset \mathcal{H}_2$.
c) Solve $H_\Delta^{(i)}(f_1,\ldots,f_n) = 0$ in the power series ring (truncated series with large precision) using linear algebra.

In addition, if ϕ is a Galois cover and we understand the action of the Galois group explicitly, then we can compute all the $H_\Delta^{(i)}$ from the Galois orbit of one component.

We shall refer to this algorithm as *Runge's method*. Let us now give a simple analysis of its space requirements and runtime.

Proposition 3.8. *Let m be the number of monomials to be evaluated and let N be the precision of the truncated power series used. Assume that each power series coefficient can be computed in constant time and that the arithmetic operations in the ring $\mathbb{Z}[p,q]/(p^N,q^N)$ are of order N^2. Then, the runtime of Runge's method is $O(m^2N^2)$ and the space complexity is $O(mN^2)$.*

Proof. The algorithm decomposes into three parts: computing power series to precision N, evaluating m monomials and computing the row-kernel of an $m \times N$ matrix. We have the following table:

Algorithm step	Space	Time
Compute power series to precision N	N^2	N^2
Evaluate m monomials	mN^2	mN^2
Computing row-kernel of a $m \times N^2$ matrix	mN^2	m^2N^2
Total complexity	mN^2	m^2N^2

The first two lines are straightforward given our assumptions. The space complexity for the kernel calulation is simply the number of matrix entries which is mN^2. From Cohen [**13**, §2.3.1], we see that the runtime for computing the row-kernel of an $r \times c$ matrix is r^2c, so our table is correct. This completes the proof. □

Remark 3.9. The success of Runge's method is contingent on having high enough precision such that the computed kernel has dimension one. In particular, the number of power series terms must be greater than the number of monomials, which means that the runtime is $o(m^3)$.

Any finite cover of the Siegel modular threefold is 3-dimensional, hence the number of monomials of degree d is proportional to d^3. It follows from the above remark that the runtime of finding a Humbert relation of degree d is of order $o(d^9)$.

3.4. Satake models of level 2

In [**72**] van der Geer constructs a model in $\mathbb{P}^4$ for the Satake compactification of the Siegel modular threefold of level 2 using fourth powers of even theta functions of half integral characteristics. The symmetric group S_6 acts on these functions. He then states that by changing the action of S_6 by an outer automorphism, we may obtain a model in $\mathbb{P}^5$ where S_6 acts by permuting the coordinate functions $x_1, \ldots, x_6$. In this section we explicitly construct this model of the Satake compactification $X[2] = \mathcal{H}_2^*/\Gamma_2(2)$ in $\mathbb{P}^5$ using theta functions of half integral characteristics. This model is ideal for computing Humbert surfaces as each level 2 Humbert component is fixed by a subgroup G of S_6 which means that the Humbert equations are G-invariant polynomials. This reduces the number of monomials one has to evaluate in Runge's method and reduces the size of the matrix by a constant factor.

3.4.1. A model of $X[2]$ in $\mathbb{P}^4$. Igusa [**32**] showed that the space of modular forms of weight 2 for $\Gamma_2(2)$ defines an embedding of $\mathcal{H}_2^*/\Gamma_2(2)$ into projective space. A nice model can be constructed by working with theta functions of half integral characteristics.

Let $m = (m_1, \ldots, m_4)$ be an integer row vector. Set $m' = (m_1, m_2)$ and $m'' = (m_3, m_4)$. Recall the theta function with half integral characteristic m has Fourier expansion

$$\theta_m(z,\tau) = \sum_{p \in \mathbb{Z}^2} \mathbf{e}\left(\frac{1}{2}\left(p + \frac{m'}{2}\right)\tau\,{}^t\left(p + \frac{m'}{2}\right) + \left(p + \frac{m'}{2}\right){}^t\left(z + \frac{m''}{2}\right)\right).$$

We make note of three theta function identities [**33**]. Firstly, the substitution $p \mapsto -p - m'$ shows

$$\theta_m(-z,\tau) = (-1)^{m'\cdot m''}\theta_m(z,\tau)$$

which says that θ_m is even (or odd) as a function of z if and only if $m'\cdot m'' = m_1m_3 + m_2m_4$ is even (or odd). It follows that all the odd theta constants are zero.

Let $n \in \mathbb{Z}^4$ be another characteristic. Identity (1.68) says that

$$\theta_{m+2n}(z,\tau) = (-1)^{m'\cdot n''}\theta_m(z,\tau)$$

which shows that it is enough to know the theta functions/constants θ_m as m ranges over a set of representatives of $\mathbb{Z}^4/(2\mathbb{Z})^4$, for which we take the set

of vectors whose entries are in $\{0,1\}$. There are sixteen theta functions of half integral characteristics, ten even and six odd. There are ten even theta constants.

The third identity is a specialisation of Igusa's transformation formula (see Theorem 1.69) for theta constants θ_m. Let $m \in \mathbb{Z}^4$ be a characteristic. For a symplectic matrix $T = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z})$ write $T \cdot m := mT^{-1} + ((\gamma\,{}^t\delta)_0, (\alpha\,{}^t\beta)_0)$ where X_0 denotes the row vector determined by the diagonal entries of X. Then

$$\theta_{T\cdot m}\left(T(\tau)\right) = \varepsilon(T,m)\det(\gamma\tau+\delta)^{1/2}\theta_m(\tau)$$

where $\varepsilon(T,m)$ is a certain eighth root of unity depending only on T, m and the sign ambiguity of the choice of square root.

Lemma 3.10.

a) *The characteristic $T \cdot m$ has the same parity as m.*
b) *If $T \equiv I_2$ mod 2 then $T \cdot m = m$. Hence $\Gamma_2(1)/\Gamma_2(2) \cong \mathrm{Sp}_4(\mathbb{F}_2)$ acts on the characteristics.*
c) *The action of $\mathrm{Sp}_4(\mathbb{F}_2)$ on the six odd characteristics is transitive and gives an isomorphism between S_6 and $\mathrm{Sp}_4(\mathbb{F}_2)$.*

Proof. See Igusa [**32**, p. 398]. □

By fixing the ordering of the odd characteristics to be

$$0101, 0111, 1011, 1010, 1110, 1101$$

we can write down this isomorphism $R : S_6 \to \mathrm{Sp}_4(\mathbb{F}_2)$ explicitly on the generators:

$$R_{(12)} = \begin{pmatrix} I_2 & \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right) \\ 0 & I_2 \end{pmatrix}, \qquad R_{(123456)} = \begin{pmatrix} 0 & \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) \\ \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right) & I_2 \end{pmatrix}.$$

The following proposition is obtained by examining $\epsilon(T,m)$ in Igusa's transformation formula more closely.

Proposition 3.11.

a) *$\varepsilon(T,m)$ is a fourth root of unity for all $T \in \Gamma_2(2)$, hence the fourth powers $\theta_m^4(\tau)$ are Siegel modular forms for $\Gamma_2(2)$.*
b) *Let $T = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ be in $\mathrm{Sp}_4(\mathbb{Z})$. We have the identity*

$$\theta^4_{T\cdot m}\left(T(\tau)\right) = (-1)^{m'\,{}^t\beta\delta\,{}^tm' + m''\,{}^t\alpha\gamma\,{}^tm''} \cdot \det(\gamma\tau+\delta)^2 \cdot \theta^4_m(\tau)$$

which holds for characteristics $m \in \mathbb{Z}^4$.

Proof. From [**34**, p. 226] we have $\varepsilon(T,m) = \kappa(T)\mathbf{e}(\phi_m(T))$ with $\phi_m(T) = -1/8 \cdot (m'\,{}^t\beta\delta\,{}^tm' + m''\,{}^t\alpha\gamma\,{}^tm'' + 2m'\,{}^t\beta\gamma\,{}^tm'' - 2(m'\,{}^t\delta - m''\,{}^t\gamma)(\alpha\,{}^t\beta)_0)$. Since $m', m'' \in \mathbb{Z}^2$ we obtain

$$\varepsilon(T,m)^4 = \kappa(T)^4(-1)^{m'\,{}^t\beta\delta\,{}^tm' + m''\,{}^t\alpha\gamma\,{}^tm''}.$$

Since matrices in $\Gamma_2(2)$ are the identity mod 2, we see that $\varepsilon(T,m)^4 = \kappa(T)^4$ for all $T \in \Gamma_2(2)$. The proposition now follows from the fact that $\kappa(T)^4 = 1$ for all $T \in \mathrm{Sp}_4(\mathbb{Z})$; see Birkenhake-Lange [**7**, §8.6, Ex 8.11(9)] for a proof. □

Define a right action of $T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{R})$ on functions $f : \mathcal{H}_2 \to \mathbb{C}$ by writing $f \circ [T](\tau) = \det(c\tau + d)^{-2} f\left(T(\tau)\right)$. Then by the proposition above, $\theta_m^4 \circ [T] = \pm\theta^4_{T^{-1}\cdot m}$ for all $T \in \mathrm{Sp}_4(\mathbb{Z})$ with $\Gamma_2(2)$ acting trivially. Thus S_6 acts on the vector space M spanned by the ten even theta fourth powers.

In [**32**] Igusa computed the representation

$$\langle T\rangle : \theta_m^4 \mapsto \theta_m^4 \circ [T^{-1}] = \theta^4_{T\cdot m}.$$

It is the five dimensional irreducible representation corresponding to the partition $6 = 2 + 2 + 2$.

Theorem 3.12. *(*[**72**, IX 3.2]*) The* 10 *modular forms* θ_m^4 *span the five dimensional vector space* $M_2(\Gamma_2(2)) = M$ *and define an embedding* $X[2] \to \mathbb{P}^4 \subset \mathbb{P}^9$ *of the Satake compactification. The image is the quartic threefold defined by*

$$u_2^2 - 4u_4 = 0$$

where $u_k = \sum \theta_m^{4k}$ *sums over all even characteristics.*

The S_6-action can be described elegantly using a different notation for the theta fourth powers as found in van der Geer [**28**, Ch. 9], motivated by Thomae's formula. For each partition $(ijk)(\ell mn)$ of $\{i,j,k,\ell,m,n\} = \{1,2,\ldots,6\}$, define $\theta(ijk)(k\ell m)$ by first setting

$$\begin{aligned}
t_1 &:= \theta(124)(356) = \theta^4_{1000}\,, & t_2 &:= \theta(125)(346) = \theta^4_{1100}\,,\\
t_3 &:= \theta(126)(345) = \theta^4_{1111}\,, & t_4 &:= \theta(123)(456) = \theta^4_{1001}\,,\\
t_5 &:= \theta(135)(246) = \theta^4_{0000}\,, & t_6 &:= \theta(145)(236) = \theta^4_{0001}\,,\\
t_7 &:= \theta(156)(234) = \theta^4_{0110}\,, & t_8 &:= \theta(146)(235) = \theta^4_{0010}\,,\\
t_9 &:= \theta(136)(245) = \theta^4_{0011}\,, & t_{10} &:= \theta(134)(256) = \theta^4_{0100}\,,
\end{aligned}$$

then, for any permutation $\sigma \in S_6$ satisfying $\{\sigma(i),\sigma(j),\sigma(k)\} = \{i,j,k\}$, we declare that

$$\theta(\sigma(i),\sigma(j),\sigma(k))(\sigma(\ell),\sigma(m),\sigma(n)) = \mathrm{sign}(\sigma)\,\theta(ijk)(\ell mn).$$

A representation of S_6 on M is given by

$$\sigma :\ \theta(ijk)(\ell mn) \longmapsto \theta(\sigma(i),\sigma(j),\sigma(k))(\sigma(\ell),\sigma(m),\sigma(n)).$$

Proposition 3.13. *The above representation of* S_6 *on described on the* $\theta(ijk)(\ell mn)$ *is equal to Igusa's representation* $\langle\cdot\rangle$ *via the isomorphism* $R : S_6 \to \mathrm{Sp}_4(\mathbb{Z})/\Gamma_2(2)$ *defined earlier. That is to say* $\sigma = \langle R_\sigma\rangle$.

Proof. Simply compute both representations on the generators of S_6 and observe that they are indeed identical. □

All linear relations between the theta fourth powers arise from Riemann's theta formula [**33**, p. 232] and have a very nice symmetric form.

Proposition 3.14. *The $\theta(ijk)(\ell mn)$ satisfy the relations*

$$\theta(ijk)(\ell mn) - \theta(ij\ell)(kmn) - \theta(ijm)(\ell kn) - \theta(ijn)(\ell mk) = 0.$$

We defer the proof until Section 3.5 where we make use of Thomae's formula.

The t_i with $i = 6, 7 \ldots, 10$ form a basis of $M = \mathrm{Span}\{t_1, \ldots t_{10}\}$. The other t_i can be represented in terms of this basis producing five linear relations:

$$\begin{aligned} t_1 &= t_6 - t_8 + t_{10} \\ t_2 &= -t_8 + t_9 + t_{10} \\ t_3 &= t_7 - t_8 + t_9 \\ t_4 &= t_6 + t_7 - t_8 \\ t_5 &= t_6 + t_7 - t_8 + t_9 + t_{10}\,. \end{aligned}$$

The basis determines an explicit embedding $X[2] \to \mathbb{P}^4$ as in Theorem 3.12.

3.4.2. A model of $X[2]$ in $\mathbb{P}^5$. The symmetric group S_6 is unique in that it is the only symmetric group which has an outer automorphism [**61**, Ch. 7 §2]. It is an automorphism of order two which interchanges the conjugacy classes in S_6 corresponding to the partitions $2+1+1+1+1$ and $2+2+2$. A look at the character table for S_6 shows that if we twist the S_6-action on M by an outer automorphism, we get a representation corresponding to the partition $6 = 5 + 1$. This representation has a nice "symmetric" realization as

$$\left\{ (x_1, \ldots, x_6) \in \mathbb{C}^6 \ : \ \sum_{1 \le i \le 6} x_i = 0 \right\} \cong \mathbb{C}^5$$

where S_6 acts by permuting the coordinates.

We now change model explicitly. We shall use the outer automorphism $\alpha : S_6 \to S_6$ defined by

$$\begin{aligned} (12) &\mapsto (16)(23)(45), \\ (123456) &\mapsto (46)(235). \end{aligned}$$

Our task is to find six functions $x_1, \ldots, x_6$ in M such that $gx_i = x_{\alpha(g)(i)}$ where the action on the right hand side of the equality is the natural permutation action on $\{1, 2, \ldots, 6\}$. We find these in the following manner.

Observe that $\alpha^{-1}(g)x_6 = x_6$ for all g in S_5, the group of permutations fixing the element 6. Write $\sigma = \alpha^{-1}(12345) = (14326)$ and define

$$\begin{aligned} v &= t_7 + \sigma t_7 + \sigma^2 t_7 + \sigma^3 t_7 + \sigma^4 t_7 \\ &= t_7 + t_8 + t_9 - t_{10} + t_4 \,. \end{aligned}$$

By construction, $\sigma v = v$ and one can easily compute that $\alpha^{-1}(12)v = v$, hence v is fixed by all of $\alpha^{-1}(S_5)$. Thus we can set $x_6 = v$. To find the other x_i, simply compute $\alpha^{-1}(i6)x_6$. In terms of the basis of M, we obtain

$$\begin{aligned} x_1 &= t_6 - t_7 + t_9 + 2t_{10} \\ x_2 &= -2t_6 - t_7 + t_9 - t_{10} \\ x_3 &= t_6 - t_7 - 2t_9 - t_{10} \\ x_4 &= t_6 + 2t_7 - 3t_8 + t_9 + 2t_{10} \\ x_5 &= -2t_6 - t_7 + 3t_8 - 2t_9 - t_{10} \\ x_6 &= t_6 + 2t_7 + t_9 - t_{10} \,. \end{aligned}$$

One can verify that the x_i sum to zero. The symmetric relation $u_2^2 - 4u_4$ between the t_i in Theorem 3.12 gives us a degree 4 relation symmetric in the x_i.

Theorem 3.15. *([**72**, p. 348]) Changing the action of S_6 by an outer automorphism, we can find equations for $X[2]$ embedded in $\mathbb{P}^5$ given by*

$$\begin{aligned} s_1 = 0 \,, \\ s_2^2 - 4s_4 = 0 \,, \end{aligned}$$

where $s_k = \sum_{i=1}^6 x_i^k$ are the k-th power sums in the coordinates of $\mathbb{P}^5$. In this model, S_6 acts by permuting the coordinates $x_1, \ldots, x_6$.

Proof. All that remains to be shown is the correctness of the stated degree four relation. The linear transformation back to the t_i is given by the equations

$$\begin{aligned} &3t_1 = x_1 + x_3 + x_4, \quad 3t_2 = x_1 + x_2 + x_4, \quad 3t_3 = x_1 + x_3 + x_5, \\ &3t_4 = x_1 + x_2 + x_5, \quad 3t_5 = x_2 + x_3 + x_5, \quad 3t_6 = x_2 + x_4 + x_5, \\ &3t_7 = x_1 + x_2 + x_3, \quad 3t_8 = x_2 + x_3 + x_4, \quad 3t_9 = x_3 + x_4 + x_5, \\ &3t_{10} = x_1 + x_4 + x_5. \end{aligned}$$

Substituting these expressions for t_i into the degree 4 relation $u_2^2 - 4u_4$ produces a polynomial $r(x_1, \ldots, x_6)$. With the help of Gröbner basis machinery we calculate that $r = ms_1 - \frac{1}{27}(s_2^2 - 4s_4)$ where m is a cubic polynomial. Since both s_1 and r vanish on $X[2]$, it follows that $s_2^2 - 4s_4$ does as well. □

Thus we are able to compute Fourier expansions of the coordinate functions x_i explicitly since they are simply linear combinations of theta fourth powers which we know how to compute from Section 3.1.

We now state some results about the geometry of this model in $\mathbb{P}^5$.

Proposition 3.16. *(*[**6**, §4],[**72**, §1]*) The boundary components of $\mathcal{H}_2/\Gamma_2(2)$ in $X[2]$ form the singular locus of the embedding into $\mathbb{P}^5$. For each partition of $\{1,\dots,6\}$ into three disjoint pairs $(ij)(k\ell)(mn)$ there is a one-dimensional boundary component $\infty_{(ij)(k\ell)(mn)}$ given by additional equations*

$$x_i = x_j,\ x_k = x_\ell,\ x_m = x_n,\ x_i + x_k + x_m = 0\,.$$

For each pair $\{i,j\}$ in $\{1,\dots,6\}$ there is a zero-dimensional boundary point $\infty_{\{i,j\}}$ whose coordinates satisfy $x_i = x_j = 2$ and $x_k = -1$ for all other k.

Each 0-dimensional boundary component lies on three 1-dimensional boundary components and each 1-dimensional boundary component lies on three 0-dimensional boundary components.

Besser [**5**, §7] determined the number of components of H_Δ in $X[2]$.

Proposition 3.17. *Let Δ be a positive integer congruent to 0 or 1 mod 4. Then*

a) *If $\Delta \equiv 1 \pmod 8$ then $H_\Delta \subset X[2]$ has 10 components labelled $(H_\Delta)_{(ijk)}$, each corresponding to a partition of $\{1,\dots,6\}$ into two triples. The component $(H_\Delta)_{(ijk)}$ contains the 9 boundary points $\infty_{\{p,q\}}$ which have $p \in \{i,j,k\}$ and $q \notin \{i,j,k\}$.*
b) *If $\Delta \equiv 5 \pmod 8$ then $H_\Delta \subset X[2]$ has 6 components labelled $(H_\Delta)_{(i)}$. The component $(H_\Delta)_{(i)}$ contains the 5 boundary points $\infty_{\{i,j\}}$ with $i \neq j$.*
c) *If Δ is an even discriminant then $H_\Delta \subset X[2]$ has 15 components labelled $(H_\Delta)_{(ij)}$. The component $(H_\Delta)_{(ij)}$ contains the 6 boundary points $\infty_{\{k,l\}}$ with $\{k,l\} \cap \{i,j\} = \emptyset$. If Δ is a square then $(H_\Delta)_{(ij)}$ contains an additional boundary point $\infty_{\{i,j\}}$.*

Once again, we have a formula for the degree of the polynomial $F_{\Delta,i}$ defining Humbert components which can be derived from Theorem 3.5. From Proposition 3.17, the number of Humbert components is given by

$$m(\Delta) = \begin{cases} 10 & \text{if } \Delta \equiv 1 \bmod 8, \\ 15 & \text{if } \Delta \equiv 0 \bmod 4, \\ 6 & \text{if } \Delta \equiv 5 \bmod 8. \end{cases}$$

The degree of any Humbert component $F_{\Delta,i}$ in $X[2]$ is given by a recursive formula

$$a_\Delta = 4 \sum_{x>0} m(\Delta/x^2) \deg(F_{(\Delta/x^2),i})$$

where a_Δ is the coefficient of Cohen's modular form calculated using (3.4).

Δ	1	4	5	8	9	12	13	16	17	20	21	24	25
$\deg(F_{\Delta,i})$	1	1	2	2	6	4	10	8	12	8	20	12	30
Δ	28	29	32	33	36	37	40	41	44	45	48	49	52
$\deg(F_{\Delta,i})$	16	30	16	36	24	50	28	48	28	60	32	84	40

TABLE 3. Degrees of Satake Humbert components in $X[2]$.

3.4.3. Computations. We now have enough information to implement Runge's method and produce some Humbert components with level 2 structure. We know how to compute the Fourier expansions and know the degree of the equation. The defining equations of $X[2]$ will always be satisfied by the Humbert component. By removing monomials divisible by x_6 or x_5^4, we can avoid these defining relations from being detected. Using this method, we calculated Humbert components for small discriminants.

Δ	computed Humbert equation	component label
1	$x_1 + x_2 + x_5$	(125)
4	$x_3 - x_5$	(35)
5	$x_1^2 - 2x_1x_2 - 2x_1x_3 - 2x_1x_4 - 2x_1x_5 - 2x_2^2 - 2x_2x_3 - 2x_2x_4 - 2x_2x_5 - 2x_3^2 - 2x_3x_4 - 2x_3x_5 - 2x_4^2 - 2x_4x_5 - 2x_5^2$	(1)
8	$8x_1^2 + 8x_1x_2 + 8x_1x_3 + 8x_1x_4 + 8x_1x_5 - 7x_2^2 - 10x_2x_3 + 8x_2x_4 + 8x_2x_5 - 7x_3^2 + 8x_3x_4 + 8x_3x_5 + 8x_4^2 + 8x_4x_5 + 8x_5^2$	(23)

TABLE 4. Satake Humbert components for small discriminants.

Using these equations and Proposition 3.17 we can determine which Humbert component we are actually computing for each discriminant class mod 8 by substituting in all the zero-dimensional boundary points and seeing which $\infty_{\{i,j\}}$ lie on the component. Looking at the constant terms in the Fourier expansions of the x_i, we learn that our Fourier expansions are power series expansions centred at $\infty_{\{1,6\}}$.

Now that we know the exact component for each discriminant class mod 8, we can take advantage of the symmetries. The lemma below follows from Proposition 3.17.

Lemma 3.18. *Write $S = \{1, \ldots, 6\} = \{i, j, k, \ell, m, n\}$. Then*

a) *If $\Delta \equiv 1 \pmod 8$ then $(H_\Delta)_{(ijk)}$ is fixed by symmetries in S_6 which preserve the partition $S = \{i, j, k\} \cup \{\ell, m, n\}$. As an abstract group it contains $S_3 \times S_3$ as a subgroup of index 2.*
b) *If $\Delta \equiv 5 \pmod 8$ then $(H_\Delta)_{(i)}$ is fixed by symmetries in S_6 which preserve the partition $S = \{i\} \cup \{j, k, \ell, m, n\}$. As an abstract group it is isomorphic to S_5.*
c) *If Δ is an even discriminant then $(H_\Delta)_{(ij)}$ is fixed by symmetries in S_6 which preserve the partition $S = \{i, j\} \cup \{k, \ell, m, n\}$. As an abstract group it is isomorphic to $S_2 \times S_4$.*

Write $\mathrm{Sym}(T)$ for the symmetric group which acts on $\{x_i : i \in T\}$ fixing all other x_j. Let I be the set $\{2, 3\}, \{1, 2, 5\}, \{3, 5\}$ or $\{1\}$ according to whether Δ is congruent to $0, 1, 4$ or $5 \pmod 8$. In all four cases the symmetry group for H_Δ contains $G = \mathrm{Sym}(I) \times \mathrm{Sym}(J)$ where $J = \{1, \ldots, 6\} \backslash I$. So the Humbert equations will be G-invariant and we expect the defining polynomial to be G-invariant in the x_i (the only known equation where the polynomial is not G-invariant is for discriminant 4 which can be blamed on the small degree). With this in mind, we look for a nice basis for G-invariant polynomials.

Lemma 3.19. *Write $s_k = \sum_{i=1}^6 x_i^k$ for the k-th symmetric power sum and write $p_k = p_{k,I} = \sum_{i \in I} x_i^k$ for the partial k-th power sum. There are isomorphisms of graded rings*

$$\begin{aligned} \mathbb{C}[x_1, \ldots, x_6]^G &\cong \mathbb{C}[\{x_i : i \in I\}]^{\mathrm{Sym}(I)} \otimes \mathbb{C}[\{x_i : i \in J\}]^{\mathrm{Sym}(J)} \\ &\cong \mathbb{C}[\{x_i : i \in I\}]^{\mathrm{Sym}(I)} \otimes \mathbb{C}[x_i, \ldots, x_6]^{S_{|J|}} \\ &\cong \mathbb{C}[p_1, \ldots, p_{|I|}][s_1, \ldots, s_{|J|}] \,. \end{aligned}$$

Remark 3.20. It follows that any G-invariant Humbert component is uniquely represented in the polynomial ring

$$\mathbb{C}[s_2, s_3, s_5, s_6, p_1, \ldots, p_{|I|}] \cong \mathbb{C}[p_1, \ldots, p_{|I|}][s_1, \ldots, s_6]/(s_1, s_2^2 - 4s_4) \,.$$

By using these (weighted) monomials instead of the x_i, the linear algebra computation is reduced by a constant factor whilst the equations have symmetry which was lacking before.

In the literature, equations have only been calculated up to discriminant 8 (see [**6**, p. 305-307] and [**72**, §8]). We have computed equations up to discriminant 40. Below is a table of Humbert components for discriminants up to 16. The other equations can be found at the web address [**22**].

Δ	Humbert component
1	$x_1 + x_2 + x_5$
4	$x_3 - x_5$
5	$s_2 - 3p_1^2$
8	$4s_2 - 9p_1^2 - 6p_2$
9	$384p_1s_2s_3 + (816p_1^4 - 768p_1^2p_2)s_2 + 256s_3^2$ $+(864p_1^3 - 768p_1p_2 - 1024p_3)s_3 - 259p_1^6$ $-1728p_1^3p_3 + 768p_1^2p_2^2 + 1024p_3^2$
12	$16s_2^2 + (-168p_1^2 - 48p_2)s_2 - 128p_1s_3$ $-111p_1^4 + 684p_1^2p_2 + 36p_2^2$
13	$225s_2^5 + 83025p_1^2s_2^4 - 1248000p_1s_2^3s_3 + 7191450p_1^4s_2^3$ $+2867200s_2^2s_3^2 - 8659200p_1^3s_2^2s_3 + 3133440p_1s_2^2s_5$ $-85855950p_1^6s_2^2 - 24576000p_1^2s_2s_3^2 - 14745600s_2s_3s_5$ $+37728000p_1^5s_2s_3 + 46080000p_1^3s_2s_5 + 320203125p_1^8s_2$ $-11059200p_1^4s_3^2 + 67829760p_1^2s_3s_5 + 131155200p_1^7s_3$ $+18874368s_5^2 - 272609280p_1^5s_5 - 388854675p_1^{10}$
16	$36864p_1^2s_2^3 + 98304p_1s_2^2s_3 + (165888p_1^4 - 552960p_1^2p_2$ $+36864p_2^2)s_2^2 + 65536s_2s_3^2 + (221184p_1^3 - 786432p_1p_2)s_2s_3$ $+(167040p_1^6 - 1259136p_1^4p_2 + 2294784p_1^2p_2^2 - 152064p_2^3)s_2$ $+(16384p_1^2 - 131072p_2)s_3^2 + (46848p_1^5 - 531456p_1^3p_2$ $+1170432p_1p_2^2)s_3 + 27657p_1^8 - 435528p_1^6p_2$ $+1928664p_1^4p_2^2 - 2636064p_1^2p_2^3 + 156816p_2^4$

TABLE 5. Satake Humbert components up to discriminant 16.

3.5. Rosenhain models

In this section we produce families of genus 2 curves whose Jacobians have real multiplication by applying Runge's method to find Humbert components expressed as equations in terms of Rosenhain invariants.

Torelli's theorem says that the map sending a curve C to its Jacobian variety $\mathrm{Jac}(C)$ is injective and defines a birational map between the moduli space of genus 2 curves denoted $\mathcal{M}_2$, and $\mathcal{A}_2$. In fact, the image of the Torelli map is precisely the complement of H_1 in $\mathcal{A}_2$.

Given a genus 2 curve $y^2 = \prod_{i=1}^{6}(x - u_i)$ over the complex numbers, we can send three of the u_i to $0, 1, \infty$ via a fractional linear transformation to get an isomorphic curve with a *Rosenhain model*:

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3).$$

The λ_i are called *Rosenhain invariants*. The ordered tuple

$$(0, 1, \infty, \lambda_1, \lambda_2, \lambda_3)$$

determines an ordering of the Weierstrass points and a level 2 structure on the corresponding Jacobian, that is, determines a point of $\mathcal{A}_2(2)$.

Let $\mathcal{M}_2(2)$ denote the moduli space of genus 2 curves together with a full level 2 structure. The points of $\mathcal{M}_2(2)$ are given by triples $(\lambda_1, \lambda_2, \lambda_3)$ where the λ_i are all distinct and different from 0 and 1. The forgetful morphism $\mathcal{M}_2(2) \to \mathcal{M}_2$ is a Galois covering of degree $720 = |S_6|$ where S_6 acts on the Weierstrass 6-tuple by permutations, followed by renormalising the first three coordinates to $(0, 1, \infty)$.

As functions on $\mathcal{M}_2(2)$, the Rosenhain invariants generate the coordinate ring of $\mathcal{M}_2(2)$ and hence generate the function field of $\mathcal{A}_2(2)$.

3.5.1. Thomae's formula. To compute with Rosenhain invariants, we express them in terms of theta functions using Thomae's result [**54**].

Let C be a genus 2 curve with projective model $y^2 z = \prod_{i=1}^{6} (\beta_i x - \alpha_i z)$. Let $B = \{1, ..., 6\}$ be an indexing set for the six branch points $\{b_i = (\alpha_i : \beta_i) \in \mathbb{P}^1 : i = 1, ..., 6\}$ and let $U = \{1, 3, 5\}$. For subsets S, T of B let $S \circ T := (S \cup T) \setminus (S \cap T)$ denote the symmetric difference. Define the following half integral characteristics

$$\eta_1 = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{bmatrix}\ ,\ \eta_2 = \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 0 \end{bmatrix}\ ,\ \eta_3 = \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}\ ,$$
$$\eta_4 = \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}\ ,\ \eta_5 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}\ ,\ \eta_6 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

using our original notation for characteristics (see Section 1.11), and set $\eta_S = \sum_{k \in S} \eta_k$ for $S \subset B$, where $\eta_\emptyset = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ and the sum is matrix addition mod 1.

There is a simple relationship between $\theta[\eta_S]$ notation and van der Geer's notation.

Lemma 3.21. *Write $B = \{i, j, k, \ell, m, n\}$. If $i < j < k$ and $\ell < m < n$ then*

$$\theta(ijk)(\ell mn) = \theta[\eta_{\{i,j,k\} \circ U}]^4 = \theta[\eta_{\{\ell,m,n\} \circ U}]^4 .$$

This can easily be verified. This fact together with Thomae's formula will allow us to confirm the truth of the linear relations in Proposition 3.14.

Theorem 3.22. *(Thomae's formula) There exists a nonzero constant c such that for all $S \subset B$ with $|S|$ even, we have*

$$\theta[\eta_S]^4 = \begin{cases} 0 & \text{if } |S \circ U| \neq 3\,, \\ c(-1)^{|S \cap U|} \prod_{\substack{i \in (S \circ U), \\ j \in B \setminus (S \circ U)}} (\alpha_i \beta_j - \alpha_j \beta_i)^{-1} & \text{if } |S \circ U| = 3\,. \end{cases}$$

Proof. See Mumford [**54**, Ch. 8]. □

Corollary 3.23. *The linear relations*

$$\theta(ijk)(\ell mn) - \theta(ij\ell)(kmn) - \theta(ijm)(\ell kn) - \theta(ijn)(\ell mk) = 0.$$

as stated in Proposition 3.14 are true.

Proof. Use Thomae's formula to write each theta fourth power term as a function of the of the roots. The result then follows from algebraic manipulation. □

If one of the branch points is the point at infinity, Thomae's formula simplifies somewhat. Order the points so that $b_6 = (1:0)$ and $b_i = (u_i : 1)$ for $i \neq 6$ where $u_i = \alpha_i/\beta_i$. The product then takes the form

$$c(-1)^{|S\cap U|} \prod_{\substack{i\in(S\circ U),\\ j\in B'\setminus(S\circ U)}} (u_i - u_j)^{-1}$$

where $B' = \{1, ..., 5\}$.

Proposition 3.24. *(*[**54**, Corollary 8.13]*) Suppose we have five finite branch points* $(u_i : 1)$ *indexed by* $B' = \{k, \ell, m, w_1, w_2\} \subset \{1, ..., 6\}$. *Then*

$$\frac{(u_k - u_\ell)^2}{(u_k - u_m)^2} = \frac{\theta[\eta_{\{w_1,k,\ell\}\circ U}]^4 \theta[\eta_{\{w_2,k,\ell\}\circ U}]^4}{\theta[\eta_{\{w_1,k,m\}\circ U}]^4 \theta[\eta_{\{w_2,k,m\}\circ U}]^4}\,. \tag{3.25}$$

Using this and the identity

$$1 + \left(\frac{u_k - u_\ell}{u_k - u_m}\right)^2 - \left(\frac{u_m - u_\ell}{u_m - u_k}\right)^2 = 2\left(\frac{u_k - u_\ell}{u_k - u_m}\right)$$

we can write $\frac{u_k - u_\ell}{u_k - u_m}$ *as a rational function of theta fourth powers.*

Proof. Let $B' = V_1 \cup V_2 \cup \{k\}$ be a partition of the five branch points with $|V_i| = 2$. From Thomae's formula we obtain the identity

$$\frac{\prod_{i\in V_1}(u_k - u_i)}{\prod_{i\in V_2}(u_k - u_i)} = (-1)^{k+1}\frac{\theta[\eta_{(V_2\cup\{k\})\circ U}]^4}{\theta[\eta_{(V_1\cup\{k\})\circ U}]^4}\,.$$

Apply this to the pair $V_1 = \{w_1, \ell\}, V_2 = \{w_2, m\}$ and then to $V_1 = \{w_1, m\}, V_2 = \{w_2, \ell\}$. Taking the quotient of these two equations produces the result. □

Remark 3.26. If we take square roots of both sides of (3.25) we find that

$$\frac{u_k - u_\ell}{u_k - u_m} = \pm\frac{\theta[\eta_{\{w_1,k,\ell\}\circ U}]^2 \theta[\eta_{\{w_2,k,\ell\}\circ U}]^2}{\theta[\eta_{\{w_1,k,m\}\circ U}]^2 \theta[\eta_{\{w_2,k,m\}\circ U}]^2}\,. \tag{3.27}$$

Since we can express $\frac{u_k - u_\ell}{u_k - u_m}$ in terms of theta fourth powers, the sign can be determined by looking at Fourier expansions or evaluations.

We now construct a particular set of Rosenhain invariants from theta functions. Firstly, send u_4, u_5, u_6 to $1, 0, \infty$ using the fractional linear transformation $x \mapsto \frac{u_4-u_6}{u_4-u_5} \cdot \frac{x-u_5}{x-u_6}$. Then the squared ratios $\left(\frac{u_5-u_\ell}{u_5-u_4}\right)^2 \mapsto u_\ell^2$ get mapped to squares of roots. The following result is obtained using the above remark and Proposition 3.24.

Proposition 3.28. *Let τ be a period matrix of a genus 2 curve. There is a Rosenhain model $y^2 = x(x-1)(x-u_1)(x-u_2)(x-u_3)$ for which $u_\ell(\tau) = \frac{1}{2}(1+\Theta_\ell(\tau))$ where*

$$\Theta_\ell(\tau) = \frac{\theta[\eta_{\{w_1,\ell,5\}\circ U}]^4\theta[\eta_{\{w_2,\ell,5\}\circ U}]^4 - \theta[\eta_{\{w_1,\ell,4\}\circ U}]^4\theta[\eta_{\{w_2,\ell,4\}\circ U}]^4}{\theta[\eta_{\{w_1,4,5\}\circ U}]^4\theta[\eta_{\{w_2,4,5\}\circ U}]^4}$$

and $\{w_1, w_2, \ell\} = \{1, 2, 3\}$. Explicitly,

$$u_1 = \frac{1}{2}\left(\frac{\theta_{0000}^4\theta_{0010}^4 - \theta_{0100}^4\theta_{0110}^4}{\theta_{0001}^4\theta_{0011}^4}\right) = \frac{\theta_{0000}^2\theta_{1100}^2}{\theta_{0011}^2\theta_{1111}^2},$$
$$u_2 = \frac{1}{2}\left(\frac{\theta_{1100}^4\theta_{0010}^4 - \theta_{1000}^4\theta_{0110}^4}{\theta_{0001}^4\theta_{1111}^4}\right) = \frac{\theta_{0010}^2\theta_{1100}^2}{\theta_{0001}^2\theta_{1111}^2},$$
$$u_3 = \frac{1}{2}\left(\frac{\theta_{1100}^4\theta_{0000}^4 - \theta_{1000}^4\theta_{0100}^4}{\theta_{0011}^4\theta_{1111}^4}\right) = \frac{\theta_{0000}^2\theta_{0010}^2}{\theta_{0011}^2\theta_{0001}^2}.$$

3.5.2. Computations. As a function of $\tau \in \mathcal{A}_2$ there are 720 different Rosenhain invariant triples, any of which may be used. Let

$$e_1 = \frac{\theta_{0000}^2\theta_{0010}^2}{\theta_{0011}^2\theta_{0001}^2},\ e_2 = \frac{\theta_{0010}^2\theta_{1100}^2}{\theta_{0001}^2\theta_{1111}^2},\ e_3 = \frac{\theta_{0000}^2\theta_{1100}^2}{\theta_{0011}^2\theta_{1111}^2}.$$

be our ordered Rosenhain triple. For each of the six theta functions used above, consider the Fourier expansion restricted to $H_{4k+\ell}$ as seen in Section 3.1. Observe that θ_{0000}, θ_{0011}, θ_{0010} and θ_{0001} have constant term 1, hence are invertible, but $\theta_{1100} = 2p^{1+k}q^{k+\ell-1} + \dots$ and $\theta_{1111} = -2p^{1+k}q^{k+\ell-1} + \dots$ have zero constant term. Fortunately one can show that $\theta_{1100}, \theta_{1111}$ are in the ideal $(p^{1+k}q^{k+\ell-1})\mathbb{Q}[[p,q]]$, hence by cancelling out the $p^{1+k}q^{k+\ell-1}$ factors, the quotient $\theta_{1100}/\theta_{1111}$ makes sense in $\mathbb{Q}[[p,q]]$. Thus we are able to compute the Rosenhain invariants as Fourier expansions restricted to a Humbert surface.

Once we have a bound on the degree of the polynomial $F_\Delta(e_1, e_2, e_3)$ defining a Humbert component, we can apply Runge's method to find such equations. The degree of a Humbert component $F_\Delta^*(x_1, \dots, x_6) = 0$ in the Satake compactification gives an upper bound for $\deg F_\Delta(e_1, e_2, e_3)$. From computational evidence it appears $\deg F_\Delta = \deg F_\Delta^*$ for nonsquare discriminants Δ and that $\deg F_{n^2} = (1 - \frac{1}{n}) \deg F_{n^2}^*$ for all n.

Δ	1	4	5	8	9	12	13	16	17	20	21	24
$\deg(F_\Delta)$	1	2	8	8	16	16	40	24	48	32	80	48

TABLE 6. Table of degrees for Rosenhain Humbert components.

Example 3.29. ($\Delta = 1$). Points of H_1 are not Jacobians of hyperelliptic curves so they cannot have a valid Weierstrass model. Applying Runge's method we find two components $e_1 = e_2$ and $e_2 = e_3$ and permuting the roots we obtain nine relations in total

$$e_i - e_j = 0,\ i \neq j\ ,\ e_i = 0\ ,\ e_i - 1 = 0\ ,\ i, j \in \{1, 2, 3\}.$$

These are the necessary and sufficient conditions for a Rosenhain model to be degenerate.

When $\Delta \neq 1$, the Torelli map $\mathcal{M}_2(2) \to \mathcal{A}_2(2) \setminus H_1$ is an isomorphism on H_Δ. In particular, this means that the fixed groups of the Humbert components in this model can be deduced from that of the level 2 Satake model.

As we know, S_6 acts on the Rosenhain invariants via the natural action on $(0, 1, \infty, e_1, e_2, e_3)$. By pulling back the action on the Satake x_i coordinates via the outer automorphism α of Subsection 3.4.2 we can determine the action on the roots.

Lemma 3.30. *A subgroup $G \leq S_6$ fixes a level 2 Satake component if and only if $\alpha^{-1}(G)$ fixes a Rosenhain component.*

Let h_Δ be the Humbert component computed using the above algorithm. With the help of Lemma 3.18 we can now find the fixed groups for this Rosenhain component explicitly. The fixed group of h_Δ for even discriminant splits into two cases,

$$\mathrm{Fix}_{S_6}(h_{4k}) = \begin{cases} G & \text{if } k \text{ is odd} \\ g^{-1}Gg & \text{if } k \text{ is even} \end{cases}$$

where $G \subset S_6$ is a group of order 48 generated by three elements

$$(0, e_1, e_3, \infty, e_2, 1),\ (e_1, e_2) \text{ and } (1, e_1, e_3, e_2);$$

the conjugating element is $g = (1, \infty)(e_1, e_2, e_3)$. Excluding discriminant 1 which is a special case, the fixed group of $\Delta \equiv 1 \pmod 8$ is a group of order 72 generated by

$$(0, e_1)(1, e_2)(\infty, e_3),\ (1, \infty),\ (e_1, e_2) \text{ and } (e_2, e_3).$$

For $\Delta \equiv 5 \pmod 8$ the fixed group is a group of order 120 generated by

$$(0, e_1)(1, e_2)(\infty, e_3),\ (1, e_3, e_2, e_1, \infty) \text{ and } (\infty, e_1, e_3, e_2).$$

By making use of some of the simpler fixed group symmetries, we can reduce the size of the linear algebra computation. For example, the discriminant 12 component h_{12} satisfies $h_{12}(e_2, e_1, e_3) = h_{12}(e_1, e_2, e_3)$ which means we only need roughly half the number of evaluated power series since $e_1^a e_2^b e_3^c$ and $e_1^b e_2^a e_3^c$ have the same coefficient.

With the exception of discriminant 21, we have managed to produce Humbert components for all the discriminants listed in the table (see [**22**]). This extends the equations found in the literature ([**29**], [**25**]) which go up to discriminant 8.

3.6. Descent to level 1

We describe two naïve algorithms to compute level 1 Humbert surfaces. The first approach is to symmetrize a level 2 Humbert component in the Satake model in $\mathbb{P}^5$ to form a giant symmetric polynomial in $x_1, \ldots x_6$ which we can express as a polynomial in the symmetric power sum polynomials $s_1, \ldots s_6$. Eliminating the variables s_1 and s_4 using the relations $s_1 = 0$ and $4s_4 = s_2^2$, we obtain a polynomial in s_2, s_3, s_5, s_6 which are modular forms for $\mathrm{Sp}_4(\mathbb{Z})$ of weights $4, 6, 10, 12$ respectively. This method works in theory, but in practice the degree of the polynomial as given by Theorem 3.5 prohibitively large. Indeed, the only example we were able to calculate using this method was discriminant 5 which has the smallest degree of 24.

An alternative method is to use Runge's method directly with level 1 modular forms. We managed to find Humbert equations for discriminants up to 13 before running out of memory. But this method does not take advantage of knowing the level 2 equation.

We now describe an algorithm which constructs the Humbert equation from working over finite fields and lifting the coefficients. As our level 1 model uses the "non-standard" forms s_2, s_3, s_5, s_6 , we describe a few of the common level 1 models which people use and the maps between them.

3.6.1. Igusa's generators. Igusa [**31**, §IV] showed that the graded ring of even weight modular forms for $\mathrm{Sp}_4(\mathbb{Z})$ is generated by two Eisenstein series ψ_4, ψ_6 and two cusp forms χ_{10}, χ_{12} with the subscripts denoting the weights. Since the vector spaces of modular forms of weights 4 and 6 are both one-dimensional, it follows that ψ_4 and ψ_6 are constant multiples of s_2 and s_3. By comparing the constant terms in their respective Fourier expansions we find that $\psi_4 = 12^{-1} s_2$ and $\psi_6 = 12^{-1} s_3$. From [**32**, §3] the cusp

forms are defined by

$$\chi_{10} = -2^{-14} \prod_{\text{even}} \theta_m^2 \,,$$
$$\chi_{12} = 2^{-15} 3^{-4} 11^{-1} \left(2^3 \psi_6^2 - 2^2 11 \psi_4^3 + 3^2 \sum_{\text{even}} \theta_m^{24} \right) .$$

By developing the Fourier expansions, we can use linear algebra to write the s_i in terms of the four modular form generators:

$$\begin{aligned} s_2 &= 12\psi_4 \,, \\ s_3 &= 12\psi_6 \,, \\ s_5 &= 60\psi_4\psi_6 - 2^{14}3^5 5\chi_{10} \,, \\ s_6 &= 108\psi_4^3 + 24\psi_6^2 + 2^{15}3^7\chi_{12} \,. \end{aligned}$$

Thus we can produce equations of Humbert surfaces in the Satake compactification $\mathcal{A}_2^* = \operatorname{Proj}\left(\mathbb{C}[\psi_4, \psi_6, \chi_{10}, \chi_{12}]\right)$ using the same set of generators.

3.6.2. Different models. The affine subvariety of $\mathcal{A}_2^*$ defined by $\chi_{10} \neq 0$ is the coarse moduli space for genus 2 curves. Define the *Igusa-Clebsch invariants* I_2, I_4, I_6, I_{10} by the following system of equations [**35**]:

$$\begin{aligned} -2^{14}\chi_{10} &= I_{10} \,, \\ 2^{17}3\chi_{12} &= I_2 I_{10} \,, \\ 2^2\psi_4 &= I_4 \,, \\ 2^3\psi_6 &= (I_2 I_4 - 3I_6) \,. \end{aligned}$$

They arise as invariants of binary sextics when working over a field of characteristic not $2, 3$ or 5. In particular, I_{10} is the discriminant. The *absolute Igusa-Clebsch invariants* are defined to be

$$i_1 = I_2^5/I_{10}, \;\; i_2 = I_2^3 I_4/I_{10}, \;\; i_3 = I_2^2 I_6/I_{10} \,.$$

They generate the function field of $\mathcal{M}_2$ and hence $\mathcal{A}_2$.

The Igusa-Clebsch invariants reduce to zero mod 2 which renders them useless in characteristic two. The *Igusa invariants* $J_2, J_4, J_6, J_8, J_{10}$ are

defined by the equations [**30**, p. 621–2]

$$\begin{aligned} J_2 &= 2^{-3} I_2 \,, \\ J_{10} &= 2^{-12} I_{10} \,, \\ J_4 &= 2^{-5} 3^{-1} (4J_2^2 - I_4) \,, \\ J_6 &= 2^{-6} 3^{-2} (8J_2^3 - 160 J_2 J_4 - I_6) \,, \\ J_8 &= 2^{-2} (J_2 J_6 - J_4^2) \,. \end{aligned}$$

and work in all characteristics (note that J_8 is extraneous when the characteristic is not two).

The simple nature of the above transformations allow us to transfer between different models with ease. For the most part we shall be using the Satake s_i power sums.

3.6.3. Equations over finite fields. Let $\mathbb{F}_p$ be a field of characteristic p. From our previous work we can compute equations for all the level 2 Humbert components $H_\Delta^{(i)}(x_1, \ldots, x_6)$ using the Satake compactification model $X[2]$ in $\mathbb{P}^5$. Whilst it is computationally expensive to form the product algebraically, there is no such difficulty in evaluating the product at random points of $X[2]$ as we simply evaluate each individual Humbert component and multiply the evaluations together. We know the product of the level 2 components can be written as a polynomial in the symmetric functions $s_1, \ldots, s_6$ where $s_k = \sum x_i^k$. Since points on $X[2]$ satisfy $s_1 = 0$ and $4s_4 = s_2^2$, we are able to use linear algebra to determine a unique polynomial in s_2, s_3, s_5, s_6 defining the level 1 Humbert surface H_Δ of discriminant Δ. Here is the basic algorithm.

Algorithm 3.31. Given a level 2 Humbert component of discriminant Δ in $X[2]$, we calculate the level 1 Humbert surface of discriminant Δ by following the steps below:

a) Compute a set $\mathcal{S}$ of random points on $X[2](\mathbb{F}_p)$.
b) Evaluate the symmetrized product of the level 2 components by evaluating each component separately and forming the product.
c) Evaluate all weighted monomials in s_2, s_3, s_5, s_6 of degree equal to the degree of the symmetrized product.
d) Use linear algebra to find linear relations between the evaluated monomials and the evaluated symmetrized product.

If $\mathcal{S}$ is large enough we will find a unique relation which defines the level 1 Humbert surface.

We construct random points on $X[2](\mathbb{F}_p)$ as follows. The Satake compactification is three dimensional so we need three independent parameters

$a, b, c \in \mathbb{F}_p$. Consider the projective point

$$(u : a : b : c : 1 : -(u + a + b + c + 1)) \in \mathbb{P}^5$$

which satisfies $s_1 = 0$. The relation $s_2^2 - 4s_4 = 0$ defines a quartic equation in u with coefficients in $\mathbb{F}_p$. The roots of this equation in $\mathbb{F}_p$ determine points of $X[2](\mathbb{F}_p)$.

The degree of $H_\Delta(s_2, s_3, s_5, s_6)$ as a weighted homogeneous polynomial equals the degree of the symmetrized product, hence is known.

For each random point, evaluate the symmetrized product and all the monomials of weighted degree $\deg(H_\Delta)$. Since the symmetrized product can be written as a linear combination of the monomials, the same must be true for the evaluations. By taking enough random points on $X[2](\mathbb{F}_p)$ we can use linear algebra to determine the coefficient vector uniquely up to scalar multiplication. Thus we can compute the equation for H_Δ over $\mathbb{F}_p$.

3.6.4. CRT method. The following useful result is due to Wang (see [**52**] for the background). It allows us to reconstruct rational numbers from their reduction mod m provided m is large enough.

Let $H : \mathbb{Q} \to \mathbb{Z}_{\geq 0}$ be the exponential height function defined by $H(n/d) = \max(|n|, |d|)$. Write $S_M = \{r \in \mathbb{Q} | H(r) \leq M\}$ for set of rationals whose height is bounded by M. We have the following:

Theorem 3.32. *(Rational Reconstruction) Let n and d be coprime integers. Let m be a positive integer satisfying $\gcd(m, d) = 1$. Let $u \equiv n/d \pmod{m}$ and write $M = H(n/d)$. Then*

a) *If $m > 2M^2$ the reduction map $\pi : S_M \to \mathbb{Z}/m\mathbb{Z}$ is injective. That is to say, for any $0 \leq u < m$ there is at most one rational number n/d which satisfies $n/d \equiv u \pmod{m}$.*
b) *Euclid's algorithm applied to the pair (m, u) determines an inverse to π.*

The asymtotic time complexity for this algorithm is $O(\log^2 m)$.

Proof. See the article by Wang, Guy and Davenport [**75**]. □

Thus if we know the coefficients of level 1 Humbert equation for a large enough residue class ring $\mathbb{Z}/m\mathbb{Z}$ we can rationally reconstruct the coefficients. This can be done by either choosing a very large prime field or more efficiently, compute the equations modulo a set of smaller primes $\{p_i\}$ and use the Chinese Remainder Theorem (CRT) to obtain the equation modulo $\prod p_i$.

Algorithm 3.33. Given a level 2 Humbert component of discriminant Δ in $X[2]$, we can compute the level 1 Humbert surface H_Δ by doing the following:

a) Find a set of primes $\mathcal{P} = \{p_i\}$ for which the coefficients of H_Δ can be rationally reconstructed from the coefficients mod $\prod p_i$.
b) Use Algorithm 3.31 to compute H_Δ mod p_i for each $p_i \in \mathcal{P}$.
c) Use the Chinese Remainder Theorem to compute H_Δ mod $\prod p_i$.
d) Rationally reconstruct the coefficients.

Using this algorithm we were able to compute level 1 Humbert polynomials $H_\Delta(s_2, s_3, s_5, s_6)$ for discriminants up to 21 before running out of memory (see [**22**]). To give an idea of the complexity of these polynomials we describe the discriminant 21 calculation in more detail. The whole computation took 3 hours and 23 minutes on a 3.2 GHz Pentium 4 machine with 1 gigabyte of RAM. We calculated H_{21} mod p for the first 40 primes p in the interval $[2^{23} - 500, 2^{23} + 500]$, each equation taking roughly five minutes. The CRT and rational reconstruction was fast (under a second), not surprising since both are variants of the Euclidean algorithm which has asymtotic time complexity $O(\log^2 m)$. The polynomial $H_{21}(s_2, s_3, s_5, s_6)$ has degree 120; equivalently it is a modular form of weight 240. The largest integer occuring as a numerator or denominator of a coefficient is 380 binary digits long. By Theorem 3.32 we need a modulus of at least 761 binary digits to successfully perform rational reconstruction, so in hindsight we only needed to compute reductions for 34 primes.

CHAPTER 4

Shimura Curves

4.1. Quaternion algebras and orders

In this section we give a short exposition of the arithmetic of quaternion algebras based on Chapter 1 of [**1**]. The main reference for this subject is [**74**] and proofs of all the results we describe can be found there.

An algebra B over a field K is *central* if B has center K, and B is *simple* if B has no nontrivial two-sided ideals.

Definition 4.1. *A quaternion algebra B over a field K is a central simple algebra of dimension 4 over K.*

We shall always assume K is a number field. In this situation, a quaternion algebra over K has a K-basis $\{1, i, j, ij\}$ satisfying $i^2 = a,\ j^2 = b,\ ij = -ji$ for some units a, b in K. We write $B = \left(\frac{a,b}{K}\right)$ for this algebra.

Example 4.2. The $\mathbb{R}$-algebra $\left(\frac{-1,-1}{\mathbb{R}}\right)$ is the usual division ring of Hamilton quaternions denoted $\mathbb{H}$.

Example 4.3. The ring $\mathbb{M}_2(K) \cong \left(\frac{-1,1}{K}\right)$. More generally, if b is in K^{*2} then we have an isomorphism $\left(\frac{a,b}{K}\right) \cong \mathbb{M}_2(K)$ given by

$$a \mapsto \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \quad \text{and} \quad b \mapsto \begin{pmatrix} \sqrt{b} & 0 \\ 0 & -\sqrt{b} \end{pmatrix}.$$

Remark 4.4. Note that up to isomorphism the presentation $\left(\frac{a,b}{K}\right)$ is far from unique. For example, we have

$$\left(\frac{a,b}{K}\right) \cong \left(\frac{b,a}{K}\right) \cong \left(\frac{a,-ab}{K}\right) \cong \left(\frac{a,bu^2}{K}\right)$$

where u is a unit of K.

Every quaternion element α satisfies a monic quadratic equation

$$P_\alpha(X) = (X - \alpha)(X - \overline{\alpha})$$

with coefficients in K. Define the *reduced trace* and *reduced norm* of α by

$$\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} \text{ and } \mathrm{N}(\alpha) = \alpha\overline{\alpha}\,.$$

The conjugation map $\omega \mapsto \overline{\omega} = \mathrm{Tr}(\omega) - \omega$ fixes K and is a K-linear anti-involution, that is, $\overline{\overline{\alpha}} = \alpha$ and $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$.

Theorem 4.5. *The K-automorphisms of a K-quaternion algebra B are the inner automorphisms, that is, those of the form $w \mapsto bwb^{-1}$ where $b \in B^*$.*

Proof. This is a direct consequence of the Skolem–Noether theorem [**62**, Corollary 9.121]. □

By Wedderburn's Theorem [**58**, Ch. 1, Theorem 7.4], a quaternion algebra over K is either a central division K-algebra or is isomorphic to the matrix algebra $\mathbb{M}_2(K)$.

Definition 4.6. *Let B be a quaternion algebra over K. For each place v of K, $B_v := B \otimes_K K_v$ is a quaternion algebra over K_v. We say that B is ramified at v if B_v is a division algebra, otherwise we say B_v is split.*

In $\mathbb{M}_2(K)$, each matrix satisfies its characteristic polynomial which is of degree 2, so the reduced trace and norm are just the matrix trace and determinant respectively. The conjugation map sends $\omega = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ to $\overline{\omega} = \mathrm{Tr}(\omega)I_2 - \omega = \left(\begin{smallmatrix} \delta & -\beta \\ -\gamma & \alpha \end{smallmatrix}\right)$. This is also true of the reduced trace and norm of elements of B_v for any split place v.

The following theorem can be shown using class field theory.

Theorem 4.7. *(*[**74**, Ch. 3, Théorème 3.1]*)*

a) *A quaternion K-algebra B is ramified at a finite even number of places.*
b) *Two quaternion algebras are isomorphic if and only if they are ramified at the same places.*
c) *Given an even number of places of K, there exists a quaternion algebra over K which ramifies exactly at those places.*

Definition 4.8. *The reduced discriminant D_B of a quaternion K-algebra B is the product of prime ideals in $\mathcal{O}_K$ which ramify in B.*

Remark 4.9. If K has class number 1, we may identify the discriminant D_B with its generator in $\mathcal{O}_K$, up to units.

A quaternion algebra over $\mathbb{Q}$ is called *definite* if it ramifies at the infinite prime and called *indefinite* otherwise. It follows from the above theorem that the discriminants of indefinite quaternion algebras have an even number of prime factors whereas for definite quaternion algebras the number of primes factors in the discriminant is odd.

4.1.1. Orders. Let K be either $\mathbb{Q}$ or $\mathbb{Q}_p$ for some prime p. Let R be the ring of integers of K. Let B be a quaternion algebra over K. We introduce some new terminology in order to talk about orders.

An *R-lattice* in B is finitely generated torsion-free R-submodule of B which satisfies $I \otimes_R K = B$. These are analogous to fractional ideals in the

commutative setting. The inverse of an R-lattice I is defined by

$$I^{-1} = \{b \in B \mid IbI \subseteq I\}.$$

An element α of B is said to be *integral* over K if $\mathrm{Tr}(\alpha)$ and $n(\alpha)$ are in R. An R-lattice is said to be *integral* if all its elements are integral.

Definition 4.10. *An R-*order *of B is an R-lattice $\mathcal{O} \subset B$ which is also a ring. Equivalently, $\mathcal{O}$ is a ring of integral elements generating B over K.*

Given an R-lattice I, the left and right orders associated to I are defined by

$$\mathcal{O}_r(I) = \{b \in B \mid Ib \subseteq I\}, \qquad \mathcal{O}_l(I) = \{b \in B \mid bI \subseteq I\}.$$

The *reduced norm of an R-lattice I* is defined to be the fractional ideal in R generated by the reduced norms of elements of I.

From now on, $\mathcal{O}$ shall denote an R-order.

Definition 4.11. *The different $\mathcal{D}_\mathcal{O}$ of $\mathcal{O}$ is the two-sided ideal of $\mathcal{O}$ given by $\{b \in B \mid \mathrm{Tr}(b\mathcal{O}) \subset R\}^{-1}$. The reduced discriminant $D_\mathcal{O}$ of $\mathcal{O}$ is the reduced norm of $\mathcal{D}_\mathcal{O}$.*

Proposition 4.12. *The reduced discriminant has the following properties:*

a) *$D_\mathcal{O}^2$ is the ideal of R generated by*

$$\{\det(\mathrm{Tr}(w_i w_j)_{i,j=1,\ldots,4}) : w_k \in \mathcal{O}\}.$$

b) *If $\{v_1, \ldots, v_4\}$ is an R-basis for $\mathcal{O}$ then $D_\mathcal{O}^2$ is generated by*

$$\det(\mathrm{Tr}(v_i v_j)).$$

c) *If $\mathcal{O}' \subseteq \mathcal{O}$ is another R-order then $D_\mathcal{O}$ divides $D_{\mathcal{O}'}$. As a special case, $D_\mathcal{O} = D_{\mathcal{O}'}$ if $\mathcal{O}' = \mathcal{O}$.*

Proof. See Lemme 4.7 and Corollaire 4.8 in [**74**, Ch. I]. □

Each R-order is contained in a maximal order. Unlike the number field case, maximal orders are not unique in general.

Definition 4.13. *An Eichler R-order is an R-order in a quaternion algebra B which is the intersection of two maximal R-orders of B.*

Lemma 4.14. *Two R-orders are isomorphic if and only they are conjugate R-orders.*

Proof. This immediately follows from Theorem 4.5. □

The lemma below is easily verified.

Lemma 4.15. *Let $\Psi : B \to B'$ be an isomorphism of K-quaternion algebras. Then*

a) $\alpha \in B$ *is integral if and only if* $\Psi(\alpha)$ *is integral.*
b) $\mathcal{O} \subseteq B$ *is an* R*-order if and only if* $\Psi(\mathcal{O})$ *is an* R*-order. Thus* $\mathcal{O}$ *is maximal (resp. Eichler) if and only if* $\Psi(\mathcal{O})$ *is maximal (resp. Eichler).*
c) *If* $\mathcal{O} \subseteq B$ *is an* R*-order then* $D_{\Psi(\mathcal{O})} = D_{\mathcal{O}}$*. In particular, conjugate orders have the same discriminant.*

Fix a prime p. Recall that $B_p = B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is either a division algebra or a matrix algebra.

Lemma 4.16. *Let* B_p *be a division* $\mathbb{Q}_p$*-algebra. Then* B_p *contains a unique maximal* $\mathbb{Z}_p$*-order* $\mathcal{O}_p = \{b \in B_p \mid n(b) \in \mathbb{Z}_p\}$*. Hence* $\mathcal{O}_p$ *is the unique Eichler order in* B_p*.*

Proof. See [**58**, Theorem 12.8]. □

When B_p is a matrix algebra there are many maximal orders.

Lemma 4.17. *Let* $B_p = \mathbb{M}_2(\mathbb{Q}_p)$*. Then the maximal* $\mathbb{Z}_p$*-orders in* B_p *are the* $\mathrm{GL}_2(\mathbb{Q}_p)$*-conjugate orders of* $\mathcal{O}_p = \mathrm{GL}_2(\mathbb{Z}_p)$*.*

Proof. See [**58**, Theorem 17.3]. □

Proposition 4.18. *Let* $\mathcal{O}_p \subseteq \mathbb{M}_2(\mathbb{Q}_p)$ *be a* $\mathbb{Z}_p$*-order. The following are equivalent characterizations of an Eichler order:*

a) *There exists a unique pair* $\{\mathcal{O}, \mathcal{O}'\}$ *of maximal orders of* $\mathbb{M}_2(\mathbb{Q}_p)$ *such that* $\mathcal{O}_p = \mathcal{O} \cap \mathcal{O}'$*,*
b) *There exists a unique integer* $n \geq 0$ *such that* $\mathcal{O}_p$ *is conjugate to*

$$\mathcal{O}_{p,n} := \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^n\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix} = \mathbb{M}_2(\mathbb{Z}_p) \cap \begin{pmatrix} \mathbb{Z}_p & p^{-n}\mathbb{Z}_p \\ p^n\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$$

which is called the canonical Eichler order of level $p^n\mathbb{Z}_p =: N_{\mathcal{O}_p}$*.*

Proof. See [**1**, Proposition 1.53]. □

Definition 4.19. *Let* $\mathcal{O}_p$ *be an Eichler* $\mathbb{Z}_p$*-order in a quaternion* $\mathbb{Q}_p$*-algebra* B_p*. The level of* $\mathcal{O}_p$ *is defined to be the ideal in* $\mathbb{Z}_p$ *given by*

$$N_{\mathcal{O}_p} = \begin{cases} \mathbb{Z}_p & \text{if } B_p \text{ is a division algebra,} \\ N_{\varphi(\mathcal{O}_p)} & \text{where } \varphi : B_p \to \mathbb{M}_2(\mathbb{Q}_p) \text{ is an isomorphism.} \end{cases}$$

For the rest of the section let B be a quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O}$ be a $\mathbb{Z}$-order in B. Write $\mathcal{O}_p = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Proposition 4.20. *(*[**1**, Propositions 1.50, 1.51]*)*

a) $\mathcal{O}$ *is a maximal order if and only if* $\mathcal{O}_p$ *is a maximal order for all primes* p*.*

b) *$\mathcal{O}$ is a maximal order if and only if $D_{\mathcal{O}} = D_B$. In particular, all maximal orders have the same discriminant.*
c) *$\mathcal{O}$ is an Eichler order if and only if $\mathcal{O}_p$ is an Eichler order for all primes p.*

Definition 4.21. *The level $N_{\mathcal{O}}$ of an Eichler $\mathbb{Z}$-order $\mathcal{O}$ is the unique ideal N in $\mathbb{Z}$ such that N_p is the level of each $\mathcal{O}_p$ for all primes p.*

Proposition 4.22. *(*[**1**, Proposition 1.54]*)*

a) *If $\mathcal{O}$ is an Eichler order then $D_{\mathcal{O}} = D_B N_{\mathcal{O}}$ and $\gcd(D_B, N_{\mathcal{O}}) = 1$.*
b) *If $D_{\mathcal{O}} = D_B N$ is a squarefree integer then $\mathcal{O}$ is an Eichler order of level N.*
c) *If $\mathcal{O}$ and $\mathcal{O}'$ are conjugate orders then $\mathcal{O}$ and $\mathcal{O}'$ have the same level.*

Conversely, for each integer N coprime to the discriminant D_B there exists an Eichler order of level N in B (see [**1**, Corollary 1.58] which uses Proposition 5.1 in [**74**, Ch. III]).

Theorem 4.23. *Let B be an indefinite $\mathbb{Q}$-quaternion algebra. There is only one conjugacy class of Eichler orders having the same level.*

Proof. See [**74**, Ch. 3 §5]. A more general statement is given in [**74**, Ch. 3 Ex. 5.5]. □

4.2. Shimura curves

Let B be an indefinite quaternion algebra of discriminant D and fix an embedding $\Phi : B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{M}_2(\mathbb{R})$. Let $\mathcal{O}(D, N)$ be an Eichler order in B of level N. Write $\mathcal{O}^1(D, N) \subseteq \mathcal{O}(D, N)$ to denote the subgroup of units in $\mathcal{O}(D, N)$ having norm equal to 1. Define $\Gamma(D, N) = \Phi(\mathcal{O}^1(D, N))$. The group $\Gamma(D, N)$ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ hence acts on the upper half plane $\mathcal{H}$ by the usual fractional linear transformations. Up to isomorphism, the quotient $\Gamma(D, N)\backslash\mathcal{H}$ is independent of the choice of level-N Eichler order by Theorem 4.23. It is a Riemann surface called a *Shimura curve*. Shimura showed that it has a canonical model $X^D(N)$ as a projective curve defined over $\mathbb{Q}$ (see [**67**, Main Theorem I (3.2)]). Thus, there is a uniformizing function $j_{D,N} : \mathcal{H} \to X^D(N)(\mathbb{C})$ which factors through an isomorphism of $\Gamma(D, N)\backslash\mathcal{H}$ with a Zariski open subset of the complex points $X^D(N)(\mathbb{C})$.

Example 4.24. Take $B = \mathbb{M}_2(\mathbb{Q})$ which has discriminant 1. Consider the Eichler order of level N: $\mathcal{O}(1, N) = \{\left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{Z}\} \subset \mathbb{M}_2(\mathbb{Z})$. Using the canonical embedding $\Phi : \mathbb{M}_2(\mathbb{Q}) \hookrightarrow \mathbb{M}_2(\mathbb{R})$ we have $\Gamma(D, N) = \{\left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : a, b, c, d \in \mathbb{Z}\} =: \Gamma_0(N)$, the usual congruence subgroup of level N. The quotient $\Gamma_0(N)\backslash\mathcal{H}$ is not compact. By adding finitely

many cusps we can compactify to get the classical modular curve $X_0(N)$. A uniformizing function which can be used in this case is the classical j-invariant.

Example 4.25. When $D > 1$ the quotient $\Gamma(D, N)\backslash\mathcal{H}$ is compact.

4.2.1. The moduli interpretation. Recall from Example 1.58 that indefinite quaternion algebras arise as endomorphism rings of abelian surfaces. We now show that the $X^D(N)$ defined above are moduli spaces parametrizing isomorphism classes of principally polarized abelian surfaces with quaternionic multiplication (QM).

Fix a maximal order $\mathcal{O}$ of an indefinite $\mathbb{Q}$-quaternion algebra B of discriminant D. Choose a μ in $\mathcal{O}$ satisfying $\mu^2 = -D$ (such an element exists, see [**24**, p. 535]). By Theorem 1.54(b) this defines a positive involution $b^* := \mu^{-1}\overline{b}\mu$ where $b \mapsto \overline{b}$ is the canonical involution.

Consider triplets $(A, \iota, \mathcal{L})$ where A is an abelian surface, $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ is an embedding and $\mathcal{L}$ is a principal polarization on A such that the Rosati involution $\dagger : \mathrm{End}^0(A) \to \mathrm{End}^0(A)$ with respect to $\mathcal{L}$ stabilizes $B \subset \mathrm{End}^0(A)$ and induces the $*$-involution on $\mathcal{O}$. That is, $\iota(x)^\dagger = \iota(x^*)$ for all x in $\mathcal{O}$. Such a triplet is called a *principally polarized abelian surface with QM by* $\mathcal{O}$ (c.f. Definition 1.73). An isomorphism $\phi : (A_1, \iota_1, \mathcal{L}_1) \to (A_2, \iota_2, \mathcal{L}_2)$ is an isomorphism $\phi : A_1 \to A_2$ which induces an isomorphism of polarizations $\phi^*\mathcal{L}_2 = \mathcal{L}_1$ and respects the QM endomorphism structure: $\phi \circ \iota_1(x) = \iota_2(x) \circ \phi$ for all x in $\mathcal{O}$.

For $\tau \in \mathcal{H}$ define $A_\tau = \mathbb{C}^2/\mathcal{O}\binom{\tau}{1}$ where we view $\mathcal{O}$ as a subset of $\mathbb{M}_2(\mathbb{C})$ via the inclusions $\mathcal{O} \subset B \subset B \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{M}_2(\mathbb{R}) \subset \mathbb{M}_2(\mathbb{C})$. This determines a natural QM-structure $\iota_\tau : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ where $\mathcal{O}$ acts on the lattice by left multiplication. The bilinear function $E_\tau\left(x\binom{\tau}{1}, y\binom{\tau}{1}\right) := \mathrm{Tr}(\mu^{-1}x\overline{y})$ is a Riemann form defining a principal polarization $\mathcal{L}_\tau$. Thus $(A_\tau, \iota_\tau, \mathcal{L}_\tau)$ is a principally polarized abelian surface with QM by $\mathcal{O}$.

Theorem 4.26. *The map $\tau \mapsto (A_\tau, \iota_\tau, \mathcal{L}_\tau)$ induces an isomorphism between $\mathcal{O}^1\backslash\mathcal{H}$ and the moduli space of isomorphism classes of principally polarized complex abelian surfaces with QM by $\mathcal{O}$.*

Proof. See [**45**, Ch. IX] or [**7**, Ch. 9]. □

4.3. Shimura curve embeddings

Throughout this section, let $(A, \iota, \mathcal{L})$ be a principally polarized abelian surface with QM by a maximal order $\mathcal{O}$ in a $\mathbb{Q}$-quaternion algebra B having discriminant $D = p_1p_2\cdots p_{2r}$. Write E for the Riemann form attached to $\mathcal{L}$. By forgetting the QM-endomorphism structure, we have a map

$$\pi : [(A, \iota, L)] \mapsto [(A, \mathcal{L})]$$

which sends Shimura curves into the Siegel modular threefold $\mathcal{A}_2$. Similarly to the real multiplication (RM) case where the Hilbert modular surface factors through a degree 2 quotient, the map π factors through a quotient by a group of Atkin-Lehner involutions. The situation is more complicated than for RM because the QM structure is dependent on a choice of $\mu \in \mathcal{O}$ (up to conjugation by $\mathcal{O}$) satisfying $\mu^2 = -D$ which means the factor group depends on the pair $(\mathcal{O}, \mu)$. In his thesis, Rotger [**60**] studied these morphisms and found a criterion for determining the factor group, which we now describe.

Write $\mathrm{Nor}(\mathcal{O}) = \{\sigma \in B^* \,:\, \sigma\mathcal{O}\sigma^{-1} = \mathcal{O}\}$ to denote the normalizer of $\mathcal{O}$ in B^*.

Definition 4.27. *The Atkin-Lehner group is defined to be*

$$W = \mathrm{Aut}(\mathcal{O}^1) = \mathrm{Nor}(\mathcal{O}^1)/\mathcal{O}^1 = B^*/\mathbb{Q}^*.$$

It is a subgroup of the automorphism group of the Shimura curve $\mathcal{O}^1\backslash\mathcal{H}$. As an abstract group it is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2r}$ where $2r$ equals the number of prime divisors of D. Each element of W has a distinct norm dividing D so we can write

$$W = \{w_d : n(w_d) = d \text{ divides } D\}.$$

These automorphisms have a moduli interpretation:

Proposition 4.28. *For a nonzero $w \in \mathrm{End}^0(A)$ define $\mathcal{L}_w$ to be the polarization with Riemann form*

$$E_w(u, v) := E\left(\tfrac{w}{n(w)}u, wv\right).$$

Then an Atkin-Lehner element $w \in W$ sends the isomorphism class $[(A, \iota, \mathcal{L})]$ to $[(A, \iota_w, \mathcal{L}_w)]$ where $\iota_w : \beta \mapsto w^{-1}\iota(\beta)w$.

Proof. See Jordan's thesis [**37**]. □

Let $(\mathcal{O}, \mu)$ be a principally polarized maximal order, meaning that $\mu \in \mathcal{O}$ satisfies $\mu^2 = -D$. Write X_μ for the moduli space of abelian surfaces with QM by $\mathcal{O}$ and polarization given by μ. From Theorem 4.26 we know that $X_\mu \cong \mathcal{O}^1\backslash\mathcal{H}$ which is independent of μ. Write $\pi : X_\mu \to \mathcal{A}_2$ for the forgetful map $[(A, \iota, L)] \mapsto [(A, \mathcal{L})]$. To determine the image we need Rotger's notion of a twisting order.

Definition 4.29. *A twist of $(\mathcal{O}, \mu)$ is an element $\chi \in \mathrm{Nor}(\mathcal{O}) \cap \mathcal{O}$ such that $\chi^2 + n(\chi) = 0$ (ie. has zero trace) and $\chi\mu = -\mu\chi$. In particular we can write $B = \left(\frac{-D,-n(\chi)}{\mathbb{Q}}\right)$. We say $(\mathcal{O}, \mu)$ is twisting if it admits a twist $\chi \in \mathcal{O}$. We say that B is twisting if there exists a twisting maximal order.*

There is a simple criterion for determining whether a $\mathbb{Q}$-quaternion algebra is twisting or not.

Lemma 4.30. *B is twisting if and only if $B = \left(\frac{-D,m}{\mathbb{Q}}\right)$ for some positive m which divides D.*

Proof. First of all we claim that $\mathrm{Nor}(\mathcal{O}) \subset \mathrm{Nor}(\mathcal{O}^1)$. Let $y \in \mathrm{Nor}(\mathcal{O})$, then $y \in B^*$ satisfies $y\mathcal{O}y^{-1} = \mathcal{O}$ and clearly $y\mathcal{O}^1y^{-1} = \mathcal{O}^1$ which proves the claim. Let $\chi \in \mathcal{O}$ be a twisting element. Then $\mathrm{Tr}(\chi) = 0$ and χ is in $\mathrm{Nor}(\mathcal{O}) \subset \mathrm{Nor}(\mathcal{O}^1)$ by definition. The coset $\chi\mathcal{O}^1$ of $W = \mathrm{Nor}(\mathcal{O}^1)/\mathcal{O}^1$ consists of elements of norm $\mathrm{N}(\chi)$. Since W is the Atkin-Lehner group which consists elements whose norm are positive divisors of the discriminant, we are done. □

Example 4.31. The quaternion algebra of discriminant 15 can be represented by $\left(\frac{-15,3}{\mathbb{Q}}\right)$, hence it is twisting.

Definition 4.32. *The stable subgroup of $(\mathcal{O}, \mu)$ is defined as*

$$W_0 = \begin{cases} \langle w_D \rangle & \text{if } (\mathcal{O}, \mu) \text{ is non-twisting,} \\ \langle w_m, w_D \rangle & \text{if } (\mathcal{O}, \mu) \text{ admits a twist } \chi,\ \chi^2 = m. \end{cases}$$

We can now state Rotger's theorem.

Theorem 4.33. *The map $\pi : X_\mu \to \mathcal{A}_2$ factors through the quotient X_μ/W_0 by the stable subgroup, followed by a map*

$$X_\mu/W_0 \hookrightarrow \mathcal{A}_2$$

which is generically of degree one onto the image $\pi(X_\mu)$.

Proof. See [**60**, Ch. 4]. □

When working in the Siegel modular threefold, we shall abuse notation and call the image curve $\pi(X_\mu)$ a Shimura curve, with the understanding that the image is really a Shimura curve factored out by an Atkin-Lehner subgroup of order 2 or 4.

CHAPTER 5

Computing Shimura Curves

In this chapter we compute equations of Shimura curves by taking intersections of Humbert surfaces. This was first done by Hashimoto and Murabayashi [**25**] who computed level 2 Shimura components associated to maximal orders of discriminants 6 and 10 in the intersection $H_5 \cap H_8$.

5.1. Discriminant matrices

Let $R = \mathrm{End}(X)$ be the endomorphism ring of a principally polarized abelian surface X with QM. Then R is an order in an indefinite $\mathbb{Q}$-quaternion algebra B equipped with a polarization $\mu \in R$, $\mu^2 = -D$ which determines a Rosati involution on $\mathrm{End}^0(X)$. Call such a polarized order a *QM-order*.

We know that any $x \in B$ satisfies $x^2 - tx + n = 0$ where $t = \mathrm{Tr}(x)$, $n = \mathrm{N}(x)$ are the reduced trace, norm respectively. Its discriminant $\Delta(x) := \mathrm{Tr}(x)^2 - 4\mathrm{N}(x)$ defines a quadratic form

$$\Delta(x, y) = \frac{1}{2}(\Delta(x + y) - \Delta(x) - \Delta(y))$$

on B called the *discriminant form*.

Suppose R is a QM-order. The set of symmetric endomorphisms (recall Definition 2.2)

$$R^s = \{\alpha \in R \mid \mu^{-1}\overline{\alpha}\mu\}$$

forms a submodule of rank 3 over $\mathbb{Z}$, generated by elements $\{1, \alpha, \beta\}$. The discriminant restricts to a binary quadratic form on $R^s/\mathbb{Z} \cong \mathbb{Z}\alpha + \mathbb{Z}\beta$ and the associated matrix

$$S_R = \begin{pmatrix} \Delta(\alpha) & \Delta(\alpha, \beta) \\ \Delta(\alpha, \beta) & \Delta(\beta) \end{pmatrix}$$

is called the *discriminant matrix* of R with respect to $\langle \alpha, \beta \rangle$. Note that α and β are determined modulo $\mathbb{Z}$, up to a change of basis in $\mathrm{GL}_2(\mathbb{Z})$.

Proposition 5.1. *(*[**64**, Theorem 7]*) Let R be a QM-order with polarization μ. Then*

a) *We can write $R = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\alpha\beta$ where α, β are primitive symmetric endmorphisms of positive discriminant and satisfy $\mu = \alpha\beta - \beta\alpha$.*

b) *The discriminant matrix*

$$S_R = \begin{pmatrix} \Delta(\alpha) & \Delta(\alpha,\beta) \\ \Delta(\alpha,\beta) & \Delta(\beta) \end{pmatrix}$$

is positive definite. Moreover, $\mathrm{disc}(R) = \det(S_R)/4 \in \mathbb{Z}$.

c) *If R is a maximal order then the polarization is principal.*

A change of basis corresponds to changing the discriminant matrix to ${}^t g S_R g$ for some $g \in \mathrm{GL}_2(\mathbb{Z})$. Thus we can find a basis for which the discriminant matrix is $\mathrm{GL}_2(\mathbb{Z})$-reduced in the sense of binary quadratic forms. By definition, a $\mathrm{GL}_2(\mathbb{Z})$-reduced matrix $\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ satisfies $0 \leq 2b \leq a \leq c$.

A discriminant matrix is said to be *primitive* if the gcd of its entries is 1. We say that an integer Δ is *primitively represented* by a quadratic form S if there exists integers x and y which satisfy $S(x,y) = \Delta$ and $\gcd(x,y) = 1$.

It is clear that two QM-orders are isomorphic as $\mathbb{Z}$-algebras if and only if they have the same discriminant matrix.

Theorem 5.2. *(*[**64**, Theorem 10]*) If two QM-orders have the same primitive reduced discriminant matrix then the corresponding Shimura curves in $\mathcal{A}_2$ are isomorphic.*

Thus every primitive reduced discriminant matrix can be identified with a unique Shimura curve up to isomorphism.

Remark 5.3. Note that the primitivity condition is necessary. See [**64**, Example 13] for an example of two QM-orders which have the same discriminant matrix but produce nonisomorphic Shimura curves.

From Proposition 2.15 we know that moduli points in $\mathcal{A}_2$ which are in the intersection of two distinct Humbert surfaces contain a quaternion algebra in their endomorphism algebra (strict inclusion for CM points). Thus the irreducible components of such intersections are Shimura curves.

Conversely, Hashimoto [**24**] showed that a Shimura curve is contained in a Humbert surface of discriminant Δ if and only if Δ can be primitively represented by a certain quadratic form.

Theorem 5.4. *(*[**24**, Theorem 5.2], [**64**, Corollary 9]*) Let $\mathcal{O} = \mathbb{Z}[\omega]$ be a quadratic order of discriminant Δ. Let S_R be a discriminant matrix of a QM order R. The following are equivalent:*

a) *Δ is primitively represented by S_R.*

b) *There exists an embedding $\mathcal{O} \hookrightarrow R$ such that $R \cap \mathbb{Q}(\omega) = \mathcal{O}$.*

c) *A Shimura curve $\mathcal{C}$ with QM order R is contained in H_Δ.*

Moreover if we work in $\mathcal{A}_2$ or a finite cover, a Shimura curve component $\mathcal{C}^{(h)}$ is contained in the intersection $H^{(i)}_{\Delta(\alpha)} \cap H^{(j)}_{\Delta(\beta)}$ of two distinct Humbert

components if and only if we can write

$$ {}^tgS_Rg = \begin{pmatrix} \Delta(\alpha) & * \\ * & \Delta(\beta) \end{pmatrix} $$

for some $g \in \mathrm{GL}_2(\mathbb{Z})$.

Remark 5.5. This includes the case $\Delta(\alpha) = \Delta(\beta)$ for different components of the same discriminant.

Remark 5.6. If we weaken statement (a) by allowing non-primitive representations by S_R, we obtain embeddings $\mathcal{O} \hookrightarrow R$ which need not satisfy the "optimal embedding" criterion stated in (b).

Example 5.7. $H_5 \cap H_8$ contains four Shimura curves corresponding to the $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of discriminant matrices:

$$ \begin{pmatrix} 5 & 0 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 5 & 2 \\ 2 & 8 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ 4 & 8 \end{pmatrix} \sim \begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix} \text{ and } \begin{pmatrix} 5 & 6 \\ 6 & 8 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} $$

having order discriminants 10,9,6 and 4 respectively. This intersection was first computed by Hashimoto and Murabayashi [**25**].

Corollary 5.8. *Let S_R be a discriminant matrix of a QM-order R. Then S_R represents a square if and only if R is an Eichler order of level $\det(S_R)/4$ in a quaternion algebra of discriminant 1.*

Proof. From Proposition 2.14 we know that abelian surfaces on H_{δ^2} are non-simple and the endomorphism algebras of non-simple QM abelian surfaces are matrix algebras. □

This leads to a natural definition: a Shimura curve is said to be *non-simple* if the associated quaternion algebra has discriminant 1.

To conclude this section, we provide a method of determining whether a maximal order is twisting or non-twisting from its discriminant matrix.

Proposition 5.9. *Let $R = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\alpha\beta$ be a maximal QM-order in a quaternion algebra of discriminant D, where as usual α and β are Rosati-invariant. Let S_R be the discriminant matrix of R with respect to the basis above. Then R is a twisting order if and only S_R represents $4m > 0$ with m dividing D.*

Proof. By definition, R is twisting when there exists a $\chi \in \mathrm{Nor}(R) \cap R$ satisfying $\chi^2 = m > 0$ for some integer m dividing D. Equivalently, the real quadratic order $\mathbb{Z}[\chi]$ of discriminant $4m$ embeds in R. By Theorem 5.4 this occurs if and only if S_R represents $4m$. □

Remark 5.10. The above proposition can be made constructive: suppose R is a twisting order and we have found a pair $v = \binom{a}{b}$ such that ${}^t v S_R v = 4m$, then it follows from $\Delta(a\alpha + b\beta) = 4m$ that $\frac{1}{2}\mathrm{Tr}(a\alpha + b\beta) \in \mathbb{Z}$ and hence $\chi = a\alpha + b\beta - \frac{1}{2}\mathrm{Tr}(a\alpha + b\beta)$ is a twist in R satisfying $\chi^2 = m$.

Example 5.11. Consider the quaternion algebra B of discriminant $D = 2 \cdot 3 \cdot 5 \cdot 13$. We have that $B \cong \left(\frac{-D,m}{\mathbb{Q}}\right) \cong \left(\frac{-D,D/m}{\mathbb{Q}}\right)$ for $m = 2, 5$. There are two maximal orders of discriminant D corresponding to discriminant matrices $\left(\begin{smallmatrix} 5 & 0 \\ 0 & 312 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 8 & 4 \\ 4 & 197 \end{smallmatrix}\right)$. As we can represent $5x^2 + 312y^2 = 4 \cdot 5$ by $\binom{x}{y} = \binom{2}{0}$, the first order is twisting with stable subgroup $\langle w_5, w_D \rangle$. For the second order, since ${}^t v \left(\begin{smallmatrix} 8 & 4 \\ 4 & 197 \end{smallmatrix}\right) v = 4 \cdot 2$ for $v = \binom{1}{0}$, it is twisting with stable subgroup $\langle w_2, w_D \rangle$.

5.2. Shimura curves contained in H_1

From Example 2.12 we know that H_1 is a moduli space for principally polarized abelian surfaces which are isomorphic to the product of two elliptic curves. To have a Shimura curve contained in H_1, the reduced discriminant matrix must be of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 4N \end{smallmatrix}\right)$ for some positive N. Since $\gcd(1, 4N) = 1$, the discriminant matrix is primitive and hence describes a unique Shimura curve up to isomorphism. By Example 4.24 the Shimura curve is isomorphic to the classical modular curve $X_0(N)$. We shall describe the birational map $H_1 \to X_0(1) \times X_0(1)$ given by $\left(\begin{smallmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{smallmatrix}\right) \mapsto (\tau_1, \tau_2)$ in terms of modular functions which will allow us to use equations known for $X_0(N)$ to produce Shimura curves in H_1.

First let us recall some facts about modular curves and their functions. The graded ring of classical modular forms is generated by two Eisenstein series $E_4(\tau), E_6(\tau)$ of weights 4 and 6, normalized so that their Fourier expansion has constant term 1. Define the Ramanujan cusp form of weight twelve to be $\Delta(\tau) = 12^{-3}(E_4^3 - E_6^2)$. Then the classical j-invariant can be expressed as

$$j = \frac{E_4^3}{\Delta} = \frac{E_6^2}{\Delta} + 12^3.$$

As is well known, the modular curve $X_0(1) \cong \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}^*$ is a moduli space for isomorphism classes of elliptic curves over $\mathbb{C}$. It is isomorphic to $\mathbb{P}^1$ with coordinate ring $\mathbb{C}[j]$. The modular curve $X_0(N) \cong \Gamma_0(N)\backslash\mathcal{H}^*$ a moduli space for isomorphism classes of pairs (E, C) where E is an elliptic curve and $C \cong \mathbb{Z}/N\mathbb{Z}$ is a cyclic subgroup of the N-torsion $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$. Such a pair determines a cyclic N-isogeny $E \to E' = E/C$. There is a singular model for $X_0(N)$ which has coordinate ring

$$\mathbb{C}[j(\tau), j(N\tau)]$$

where $j(N\tau)$ is a root of the polynomial

$$\Phi_N(j(\tau), Y) = \prod_{\substack{C \subset E[N] \\ C \cong \mathbb{Z}/N\mathbb{Z}}} (Y - j(E/C)) \in \mathbb{C}(j(\tau))[Y].$$

We see that $X_0(N)$ has a plane affine model given by $\Phi_N(X, Y) = 0$ which we call the *modular equation* of level N.

Lemma 5.12. *For $N > 1$ we have $\Phi_N(X, Y) = \Phi_N(Y, X)$.*

Proof. Suppose $f : E \to E'$ is a cyclic N-isogeny. Then by Lemma 1.7 the dual isogeny $\underline{f} : E' \to E$ is also a cyclic N-isogeny. Thus interchanging X and Y leaves the polynomial Φ_N invariant. □

Now we describe the birational map $H_1 \to X_0(1) \times X_0(1)$ explicitly as an isomorphism of their function fields. In the Satake compactification $\mathcal{A}_2^* = \operatorname{Proj}(\mathbb{C}[\psi_4, \psi_6, \chi_{10}, \chi_{12}])$, the Humbert surface of discriminant 1 is given by the hypersurface $\chi_{10} = 0$. Consider the restriction of the other three modular form generators to H_1:

Lemma 5.13. *We have*

$$\psi_i \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix} = E_i(\tau_1)E_i(\tau_2)\ , \text{ for } i = 4 \text{ and } 6\,,$$

$$\chi_{12} \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix} = \Delta(\tau_1)\Delta(\tau_2).$$

Proof. See Klingen [**41**, §9]. □

Using these relations we obtain

$$\frac{\psi_6^2}{\chi_{12}} \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix} = (j(\tau_1) - 12^3)(j(\tau_2) - 12^3)\,,$$

$$\frac{\psi_4^3}{\chi_{12}} \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix} = j(\tau_1)j(\tau_2)\,, \tag{5.14}$$

$$\frac{\psi_4^3 - \psi_6^2}{12^3\chi_{12}} \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix} + 12^3 = j(\tau_1) + j(\tau_2)\,. \tag{5.15}$$

Therefore $j(\tau_1), j(\tau_2)$ are the roots of a quadratic polynomial with coefficients given by Siegel modular functions, so we can transfer between H_1 and $X_0(1) \times X_0(1)$ algebraically using these relations.

Example 5.16. The Shimura curve $H_1 \cap H_4$ consists of points on the diagonal $\{\left(\begin{smallmatrix} \tau_1 & 0 \\ 0 & \tau_1 \end{smallmatrix}\right)\}$ so $j(\tau_1) = j(\tau_2)$. This means that the quadratic polynomial with roots $j(\tau_1), j(\tau_2)$ has discriminant zero. Explicitly,

$$\left(\frac{\psi_4^3 - \psi_6^2}{12^3\chi_{12}} + 12^3\right)^2 - 4\frac{\psi_4^3}{\chi_{12}} = 0\,.$$

Multiplying through by χ_{12}^2 we obtain a polynomial relation in $\chi_{12}, \psi_6, \psi_4$. This equation together with $\chi_{10} = 0$ define the Shimura curve of discriminant 1.

The proposition below shows that for $N > 1$, determining the Shimura curve in $\mathcal{A}_2^*$ corresponding to the discriminant matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 4N \end{smallmatrix}\right)$ is equivalent to calculating the modular equation $\Phi_N(X, Y) = 0$.

Proposition 5.17. *We have*

$$\Phi_N(j_1, j_2) = \chi_{12}^{-d} F(\chi_{12}, \psi_6, \psi_4)$$

where F is an irreducible polynomial of weighted homogenous degree $12d$ and d is uniquely determined by N. The two equations $F = 0, \chi_{10} = 0$ define the Shimura curve $H_1 \cap H_{4N}$.

Proof. Since the Shimura curve with discriminant matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 4N \end{smallmatrix}\right)$ lives in H_1 we have $\chi_{10} = 0$ as one of the defining relations. By Lemma 5.12, the modular polynomial $\Phi_N(X, Y)$ is symmetric for $N > 1$ so we can rewrite $\Phi_N(j_1, j_2)$ as a polynomial in the elementary symmetric functions $u = j_1 + j_2$ and $v = j_1 j_2$. But we know from (5.14) and (5.15) that u and v can be expressed as Siegel modular functions. Hence we can write $\Phi_N(j_1, j_2) = \chi_{12}^{-d} F(\chi_{12}, \psi_6, \psi_4)$ for some weighted homogeneous polynomial F of degree $12d$. The rest of the proposition now follows. □

Remark 5.18. For $N = 1$ the modular polynomial $\Phi_1(X, Y) = X - Y$ is not symmetric. If we take the computed Shimura curve $H_1 \cap H_4$ in Example 5.16 and map the Siegel modular functions to j-invariants using 5.14 and 5.15 we obtain the "modular equation" $(X - Y)^2 = 0$. The multiplicity two is due to the fact that in $\mathcal{H}_2/\mathrm{Sp}_4(\mathbb{Z})$, the Humbert surface H_4 has nontrivial isotropy group of order 2 in $\mathrm{Sp}_4(\mathbb{Z})$ (see Lemma 3.1).

5.3. Level 2 Shimura components

From Theorem 5.4 we can determine the discriminant matrices of the Shimura components contained in the intersection of two level 2 Humbert surfaces. With the symmetric Satake model in $\mathbb{P}^5$, Besser [**6**] computed simple Shimura components of discriminants 6, 10 and 15 by hand using Humbert equations of discriminants 5 and 8. This can be automated by computing the primary decomposition of the (radical of the) ideal defining the Humbert intersection with a computer. Unfortunately the high degree of the components' equations combined with the high codimension of the variety in $\mathbb{P}^5$ makes the Gröbner calculations expensive. Also the output can be quite messy. For instance, when we decomposed $H_5 \cap H_8$ in the Satake model, the defining ideal for the discriminant 9 component had 16 Gröbner basis elements! For this reason we shall work rather with ambient

varieties of dimension 3. In this section we show how to compute level 2 Shimura components in terms of Rosenhain invariants.

Recall from Chapter 3 that the Rosenhain invariants e_1, e_2, e_3 generate the coordinate ring of $\mathcal{M}_2(2) \cong \mathcal{A}_2(2) - H_1$ and hence the function field of $\mathcal{A}_2(2)$. Using these functions we computed level 2 Humbert components $h_\Delta(e_1, e_2, e_3)$ for a handful of small discriminants. As we are working with coordinates in $\mathcal{M}_2(2) = \mathcal{A}_2(2) - H_1$, we will not be able to compute any Shimura components in H_1 using this model. The nine components of H_1 are given by degree 1 polynomials

$$e_i - e_j = 0,\ i \neq j\ ,\ e_i = 0\ ,\ e_i - 1 = 0\ ,\ i, j \in \{1, 2, 3\}.$$

which are hence invertible in the coordinate ring.

Let $f(e_1, e_2, e_3) = 0$ and $g(e_1, e_2, e_3) = 0$ be equations of two Humbert components. The obvious way to find components in the intersection would be to compute the primary decomposition of the (radical of the) ideal generated by f and g. The problem with this method in practice is the necessary use of Gröbner basis algorithms which have exponential complexity in the input size. Luckily when working with hypersurfaces there is an easier way which we outline below.

Take the resultant $R(f, g)$ of f and g with respect to one of the variables, e_1 say. By definition this is a polynomial in e_2 and e_3 which generates the elimination ideal $\mathbb{C}[e_1, e_2, e_3](f, g) \cap \mathbb{C}[e_2, e_3]$. Factorize the resultant. Each nontrivial factor (not an H_1 component) together with f and g defines an ideal corresponding to a Shimura component contained in the intersection.

Since S_6 acts on the Rosenhain Humbert components in $\mathcal{M}_2(2)$, it acts on their intersections producing isomorphic curves. For each Rosenhain orbit of Humbert intersections, choose a representative. Compute the nontrivial resultant factors for every representative. Each factor r corresponds to a Shimura curve with discriminant matrix $S^{(r)}$. The map $r \mapsto S^{(r)}$ always surjects onto the nontrivial discriminant matrices (not contained in H_1) but is not always injective. This is because the fixed group $\mathrm{Fix}(H_a \cap H_b)$ of a Rosenhain Humbert intersection will act nontrivially on the irreducible components $X_k \subset H_a \cap H_b$ for which $\mathrm{Fix}(X_k)$ is strictly contained in $\mathrm{Fix}(H_a \cap H_b)$. This allows the possibility of having isomorphic Shimura curves contained in the list.

To match up each discriminant matrix S with a resultant factor we use a third Humbert surface. Write $\mathcal{D}(a, b)$ for the set of discriminant matrices of Shimura curves in $H_a \cap H_b$. If the Shimura curve (component) is contained in (a component above) $H_a \cap H_b \cap H_c$ then S is in $\mathcal{D}(a, b) \cap \mathcal{D}(b, c)$. If we have identified all the nontrivial discriminant matrices apart from S (most conveniently when S is the sole element) then we should be able to find a

match for S by studying unmatched resultants appearing in both intersections.

We generalize this to multiple Humbert intersections.

Lemma 5.19. *Let $\{H_{a_k}^{(i_k)} : \ k = 0, \ldots, m\}$ be a set of distinct Humbert components with defining polynomials $\{f_{a_k}\}$ respectively. The resultant factors in $\bigcap_{k=0}^{m} H_{a_k}^{(i_k)}$ are precisely the factors of*

$$\gcd(\{R(f_{a_0}, f_{a_k}) \ : \ k = 0, \ldots, m\}).$$

The utility of the above lemma is twofold. Not only does it aid in factoring the resultant, it also allows us to compute Shimura curve components by choosing suitable Humbert discriminants.

Algorithm 5.20. To calculate a level 2 Shimura component $\mathcal{C}$ with reduced discriminant matrix $S = \left(\begin{smallmatrix} a & * \\ * & b \end{smallmatrix}\right)$ do the following:

a) Find a set of discriminants $M = \{c_1, \ldots, c_m\}$ representing S such that $H_a \cap H_b \cap \bigcap H_{c_\ell} = \mathcal{C}$.
b) Find a set of non-equivalent Humbert component intersections $H_a^{(i)} \cap H_b^{(j)} \cap \bigcap H_{c_\ell}^{(k_\ell)}$ and compute the list of nontrivial resultant factors using Lemma 5.19.

When combined with the defining polynomials of the two associated Humbert components $H_a^{(i)}$ and $H_b^{(j)}$, any one of these resultant factors define the Shimura component in the Rosenhain model up to isomorphism.

Proof. The only part that requires proof is that M is a finite set, the rest is clear from the previous discussion. Let S' be a discriminant matrix in $\mathcal{D}(a, b)$ different from S. As S and S' are not $\mathrm{GL}_2(\mathbb{Z})$-equivalent, there exists a discriminant c represented by S but not represented by S'. Thus by intersecting with $H_c^{(k)}$ we can excise at least one discriminant matrix. This shows that the set M has cardinality at most $|\mathcal{D}(a, b)| - 1$. □

Remark 5.21. If we are only interested in the abstract curve, project down to the affine plane with coordinate functions e_2 and e_3. The resultant factor gives a singular affine plane model for the Shimura component.

Remark 5.22. Now that we can compute Shimura curves associated to discriminant matrices, the question arises as to what extent we can identify an Eichler order $R = \mathcal{O}(D, N)$ from its discriminant matrix S_R. Corollary 5.8 determines the cases where $D = 1$. In general we know that $\mathrm{disc}(R) = DN$ where $\gcd(D, N) = 1$ and D is the product of a even number of distinct primes. For examples where $\mathrm{disc}(R)$ is the product of fewer than 4 distinct primes this is enough to deduce D and N.

5.3.1. Examples. First we shall compute level 2 Shimura components above the Shimura curves in $H_4 \cap H_5$. We have

$$\mathcal{D}(4,5) = \left\{ \begin{pmatrix} 4 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 2 & 5 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \right\}.$$

where we list nontrivial matrices first. There are two (non-simple since 4 is a square) Shimura curves with discriminants 5 and 4 to be identified. Up to the Rosenhain S_6-action there are two different ways to intersect components of H_4 and H_5. We discover that each intersection contains a single nontrivial resultant factor making two in total:

$$\begin{aligned} r_1 &= e_2^2e_3^2 - 4e_2^2e_3 + 4e_2^2 + 2e_2e_3^3 - 4e_2e_3^2 + 4e_2e_3 - 4e_2 + e_3^4 - 4e_3^3 + 4e_3^2\,, \\ r_2 &= e_2^8 - 4e_2^7e_3 - 2e_2^7 + 4e_2^6e_3^2 + 10e_2^6e_3 + 3e_2^6 - 12e_2^5e_3^2 - 16e_2^5e_3 - 2e_2^5 + \\ &\quad 27e_2^4e_3^2 + 8e_2^4e_3 + e_2^4 - 12e_2^3e_3^3 - 16e_2^3e_3^2 - 2e_2^3e_3 + 4e_2^2e_3^4 + \\ &\quad 10e_2^2e_3^3 + 3e_2^2e_3^2 - 4e_2e_3^4 - 2e_2e_3^3 + e_3^4\,. \end{aligned}$$

To settle the question of which r_i matches up to which discriminant matrix, we introduce a new Humbert component of discriminant 5. Following the same procedure, we have discriminant matrices

$$\mathcal{D}(5,5) = \left\{ \begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 2 & 5 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \right\}$$

when intersecting different components of H_5. Up to the Rosenhain action there is only one intersection. It produces two nontrivial resultant factors, one of them r_2 and a new polynomial r_3. Again there is a bijection between resultant factors and discriminant matrices. Since $\mathcal{D}(4,5) \cap \mathcal{D}(5,5)$ has only one nontrivial discriminant matrix, namely $\left(\begin{smallmatrix} 4 & 2 \\ 2 & 5 \end{smallmatrix}\right)$, we can match r_2 with this matrix. It follows that r_1 corresponds to discriminant matrix $\left(\begin{smallmatrix} 4 & 0 \\ 0 & 5 \end{smallmatrix}\right)$ and that r_3 corresponds to $\left(\begin{smallmatrix} 5 & 1 \\ 1 & 5 \end{smallmatrix}\right)$. So we have computed our first simple Shimura component of discriminant 6.

By carefully choosing components and discriminants we can build up a collection of Shimura component equations. The main bottleneck in computing Humbert intersections is working with the resultant polynomials, whose degree increases quadratically with the humbert polynomial degrees. Nonetheless we are able to compute 30 such intersections [**22**], which include 15 pairs $\{\Delta_1, \Delta_2\}$ of discriminants with $\Delta_i \leq 12$.

The largest intersection for which we identified the Shimura components was $H_5 \cap H_{13}$ which has discriminant matrices

$$\mathcal{D}(5,13) = \left\{ \begin{pmatrix} 5 & 1 \\ 1 & 13 \end{pmatrix}, \begin{pmatrix} 5 & 2 \\ 2 & 12 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 2 & 5 \end{pmatrix} \right\}$$

corresponding to QM-orders of discriminants $16, 14, 10$ and 4 respectively. Up to the Rosenhain action there are two different ways to intersect components of H_5 and H_{13} which we denote by I_1 and I_2. We find that I_1 produces four nontrivial resultant factors and I_2 has five, giving a total of nine Shimura components. Interestingly, the list of resultants has a duplicate, one copy in each intersection. As all the discriminant matrices are primitive, there are only 4 isomorphism classes of Shimura curves so we have some redundancy. After sucessfully matching, we found that I_1 consists of four isomorphic components of discriminant 4 and that I_2 contains all four non-isomorphic Shimura components as well as an additional discriminant 4 component.

5.4. Level 1 calculations

To compute equations of (level 1) Shimura curves we can use the same basic method as in the previous section using discriminant matrices.

Algorithm 5.23. To calculate a Shimura curve $\mathcal{C}$ with reduced discriminant matrix $S = \left(\begin{smallmatrix} a & * \\ * & b \end{smallmatrix}\right)$ do the following:

a) Find a set of discriminants $M = \{c_1, \ldots, c_m\}$ representing S such that $H_a \cap H_b \cap \bigcap H_{c_\ell} = \mathcal{C}$.
b) Use Lemma 5.19 to compute the nontrivial resultant factor.

This resultant factor together with the defining polynomials of the two associated Humbert surfaces defines a model for the Shimura curve.

For coprime Humbert discriminants we expect to find one resultant factor for each discriminant matrix appearing in $\mathcal{D}(a, b)$, but occasionally there is an extra factor which defines a subvariety of H_1. This accounts for possible intersection points on the boundary of the Satake compactification as well as split CM points in the intersection of two Shimura curves.

The combinatorial matching is far simpler for level 1 than for level 2 since the discriminant matrices are in bijection with candidate resultant factors. But since level 1 Humbert polynomials have larger degrees than their level 2 counterparts, the resultants have higher degrees and become more difficult to factorize. Another disadvantage of working in level 1 is that to find Shimura curves corresponding to $\left(\begin{smallmatrix} \Delta & * \\ * & \Delta \end{smallmatrix}\right)$ we cannot intersect two components of the same discriminant. This means we have to consider intersections involving larger discriminants. Nonetheless we have been able to compute a few small examples [**22**] arising from intersections of Humbert surfaces of discriminants bounded by 13.

We conclude this chapter by listing below the resultant factors for some simple Shimura curves $X(D, N)/W_0$ and compare the genus of each with that of the covering Shimura curve $X(D, N)$.

The Shimura curve of discriminant 6 corresponding to $\left(\begin{smallmatrix}5&1\\1&5\end{smallmatrix}\right)$:

$$18s_5 - 5s_3s_2\,.$$

The Shimura curve of discriminant 10 corresponding to $\left(\begin{smallmatrix}5&0\\0&8\end{smallmatrix}\right)$:

$$56250000s_5^2 - 41250000s_5s_3s_2 + 7562500s_3^2s_2^2 - 7203s_2^5\,.$$

The Shimura curve of discriminant 14 corresponding to $\left(\begin{smallmatrix}5&2\\2&12\end{smallmatrix}\right)$:

$$\begin{aligned}
&19960452488862131135629990118 4s_5^6 - 155365400618689004759651086080s_5^5s_3s_2\\
&+8057006191307951003736792000s_5^4s_3^2s_2^2 - 139678509104374511048148000s_5^4s_2^5\\
&+41174435827899924480000000000s_5^3s_3^5 + 113375746114100793402559200000s_5^3s_3^3s_2^3\\
&+16111816434294713837170200 0s_5^3s_3s_2^6 - 10597552085622620160000000000s_5^2s_3^6s_2\\
&+20513647061158550204965500 00s_5^2s_3^4s_2^4 - 11866388456774472825865500 0s_5^2s_3^2s_2^7\\
&+12069811765297234928306 25s_5^2s_2^{10} + 6340309142869094400000000000s_5s_3^7s_2^2\\
&-15194004999940052284225500 00s_5s_3^5s_2^5 + 52975857706230997344712500s_5s_3^3s_2^8\\
&-95792156867438372446875 0s_5s_3s_2^{11} + 21233664000000000000000000s_3^{10}\\
&-11058874316098560000000000 00s_3^8s_2^3 + 12129732195227727478256250 0s_3^6s_2^6\\
&-89456836258589633137500 00s_3^4s_2^9 + 19006380330840946914062 5s_3^2s_2^{12}\,.
\end{aligned}$$

Shimura curve of discriminant 15 corresponding to $\left(\begin{smallmatrix}5&0\\0&12\end{smallmatrix}\right)$:

$$\begin{aligned}
&256289062500000000s_5^4 - 279639843750000000s_5^3s_3s_2\\
&+92093677734375000 0s_5^2s_3^2s_2^2 - 15851861514000000 00s_5^2s_2^5\\
&-97258533398437500 00s_5s_3^3s_2^3 + 73592501886000000 0s_5s_3s_2^6\\
&-18750000000000000 0s_3^6s_2 + 27342343244628906 25s_3^4s_2^4\\
&-43813346998500000 0s_3^2s_2^7 + 5313924910103 04s_2^{10}\,.
\end{aligned}$$

The genus of the four curves $X(D,N)$ and the quotients we calculated are listed in the table below, where we write $W = \{w_d : d|N\}$ for the Atkin-Lehner group.

Shimura curve $X(D,N)$	$X(6,1)$	$X(10,1)$	$X(14,1)$	$X(15,1)$
Genus [**1**, Table A.8]	0	0	1	1
Discriminant matrix	$\left(\begin{smallmatrix}5&1\\1&5\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}5&0\\0&8\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}5&2\\2&12\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}5&0\\0&12\end{smallmatrix}\right)$
Quotient group W_0	W	W	$\langle w_{14}\rangle$	W
Genus of $X(D,N)/W_0$	0	0	0	0

If we know the genus of $X(D,N)$, the genus of $X(D,N)/W_0$ can be calculated from the Riemann-Hurwitz formula by determining the number of points fixed by the nontrivial Atkin-Lehner involutions. Fixed point formulae are known for these involutions (see Ogg [**55**]) and we have verified that our computed curves have the correct genus.

CHAPTER 6

Parametrizing Humbert Surfaces

In this chapter we search for rational points on Humbert surfaces, and where possible find rational parametrizations.

Of the various models of Humbert surfaces we have at our disposal, the Satake level 2 components appear to be the simplest. Our main approach will be to find level 2 points which map down to rational points on the level 1 Humbert surface via the map $(x_1 : \ldots : x_6) \mapsto (s_2 : s_3 : s_5 : s_6)$ where $s_k = \sum x_i^k$, $s_1 = 0$ and $s_2^2 = 4s_4$.

In Section 6.3 we look for modular abelian surfaces occuring as points on our Humbert surface models. We then determine the 'congruence primes' p for which a modular Jacobian surface splits over $\mathbb{F}_p$, using Humbert surface equations.

6.1. The Satake sextic

Recall the symmetric Satake coordinate functions $x_1, \ldots, x_6$ of van der Geer's model of $X[2]$ in $\mathbb{P}^5$ as defined in §3.4.2. In this section we determine the field of definition of the Satake x_i and make note of other useful properties related to its defining polynomial.

Lemma 6.1. *The x_i are roots of the* Satake sextic *polynomial*

$$X^6 - \frac{1}{2}s_2X^4 - \frac{1}{3}s_3X^3 + \frac{1}{16}s_2^2X^2 + (\frac{1}{6}s_2s_3 - \frac{1}{5}s_5)X + (\frac{1}{96}s_2^3 + \frac{1}{18}s_3^2 - \frac{1}{6}s_6)\,.$$

In other words, the field of definition $\mathbb{Q}(x_1, \ldots, x_6)$ for the sextuple $(x_1 : \ldots : x_6)$ is a splitting field of the above sextic polynomial over the field of definition $\mathbb{Q}(s_2, s_3, s_5, s_6)$ for the s_i.

Proof. First of all, $\prod(X - x_i) = X^6 - \sigma_1X^5 + \sigma_2X^4 - \ldots + \sigma_6$ where σ_i are the elementary symmetric functions in the x_i. These can be expressed in terms of symmetric power sums using the Newton-Girard relations:

$$\sum_{i=0}^{m}(-1)^i\sigma_i s_{m-i} = 0.$$

Eliminating s_1 and s_4 using the Satake relations $s_1 = 0$ and $s_4 = \frac{1}{4}s_2^2$ produces the desired coefficients. □

Using our knowledge of the symmetry groups of the level 2 Humbert components (Lemma 3.18), we are able to determine the Galois group of the Satake sextic polynomial given a point on a Humbert surface.

Proposition 6.2. *Suppose (s_2, s_3, s_5, s_6) is a rational point on the Humbert surface with discriminant Δ. Let $S(X) \in \mathbb{Q}[X]$ be the Satake sextic polynomial having roots x_i in a splitting field, indexed by $\{1, \ldots, 6\}$. We have the following:*

a) *If $\Delta \equiv 0 \pmod 4$ then $S(X)$ has a quadratic factor in $\mathbb{Q}[X]$ and has Galois group contained in $S_2 \times S_4$ which preserves the partition of roots $\{1, 2\} \cup \{3, 4, 5, 6\}$.*
b) *If $\Delta \equiv 5 \pmod 8$ then $S(X)$ has a linear factor in $\mathbb{Q}[X]$ and has Galois group contained in S_5 preserving $\{1\} \cup \{2, 3, 4, 5, 6\}$.*
c) *If $\Delta \equiv 1 \pmod 8$ then $S(X)$ is irreducible over $\mathbb{Q}$ and has Galois group contained in $(S_3 \times S_3) \rtimes C_2$ which preserves the partition $\{1, 2, 3\} \cup \{4, 5, 6\}$ (the C_2 interchanges the two subsets). There is a quadratic extension $K = \mathbb{Q}(x_1 + x_2 + x_3)$ of $\mathbb{Q}$ for which $S(X)$ decomposes as the product of two cubics in $K[X]$.*

Proof. The Galois groups are precisely the fixed groups of the level 2 symmetric Satake components of H_Δ mentioned in Lemma 3.18. Suppose $\Delta \not\equiv 1 \pmod 8$, then the Galois group of splitting field $\mathbb{Q}(x_1, \ldots, x_6)$ is $S_m \times S_{6-m}$ for $m = 1$ or 2. In each case, the subfield fixed by the normal subgroup $S_m \times \{1\}$ corresponds to $\mathbb{Q}(x_{m+1}, \ldots, x_6)$ and is Galois over $\mathbb{Q}$. It follows that $\prod(X - x_{m+1}) \cdots (X - x_6)$ is in $\mathbb{Q}[X]$ which shows that $S(X)$ decomposes into the product of two polynomials of degrees $6 - m$ and m. For the case $\Delta = 1 \pmod 8$, the Galois group of $\mathbb{Q}(x_1, \ldots, x_6)$ contains $S_3 \times S_3$ as a normal subgroup of index 2. Thus the fixed field $K = \mathbb{Q}(x_1, \ldots, x_6)^{S_3 \times S_3}$ is a quadratic extension of $\mathbb{Q}$. It is easily seen from the relation $s_1 = 0$ that $p_1 = x_1 + x_2 + x_3 \in K \setminus \mathbb{Q}$ and $p_1^2 \in \mathbb{Q}$, hence $K = \mathbb{Q}(p_1)$. The factorization argument from the previous case can be applied to $S(X)$ using K instead of $\mathbb{Q}$ and with $m = 3$. □

Recall Thomae's formula (Theorem 3.22) which we can rewrite as

$$\theta[\eta_{S\circ U}]^4 = \begin{cases} 0 & \text{if } |S| \neq 3\,, \\ c(-1)^{|S\cap U|} \prod_{\substack{i\in S,\\ j\in B\setminus S}} (\alpha_i\beta_j - \alpha_j\beta_i)^{-1} & \text{if } |S| = 3\,, \end{cases} \tag{6.3}$$

using the facts that $(S \circ U) \circ U = S$ and $|(S \circ U) \cap U| = 3 - |S \cap U|$. By permuting the six roots, we have an S_6-action $\mathcal{T}$ on the ten even theta fourth powers given explicitly by

$$\mathcal{T}_\sigma : \theta[\eta_{S\circ U}]^4 \longmapsto \theta[\eta_{\sigma(S)\circ U}]^4$$

where $\sigma(S) = \{\sigma(x) \,:\, x \in S\}$.

Proposition 6.4. *The representation $\mathcal{T}$ obtained from the S_6 action on the six roots equals the representation*

$$\sigma : \theta(ijk)(\ell mn) \longmapsto \theta(\sigma(i),\sigma(j),\sigma(k))(\sigma(\ell),\sigma(m),\sigma(n))$$

defined in §3.4.1.

Proof. Write $B = \{i,j,k,\ell,m,n\}$. Recall from Lemma 3.21 that if $i < j < k$ and $\ell < m < n$ then we have the identity

$$\theta(ijk)(\ell mn) = \theta[\eta_{\{i,j,k\}\circ U}]^4 = \theta[\eta_{\{\ell,m,n\}\circ U}]^4 .$$

It immediately follows that the representations are identical. □

Proposition 6.5. *Suppose $y^2 = f(x)$ is a genus 2 curve over $\mathbb{Q}$. Let G_f and G_S be the Galois groups of f and the Satake sextic polynomial respectively. Then there is an isomorphism $G_f \cong G_S$ induced via an outer automorphism of S_6.*

Proof. We need only consider the generic case $G_f = S_6$. By Proposition 6.4 the Galois action on the roots of $f(x)$ is equivalent to the S_6-action on the t_i. From Theorem 3.15, a change of basis to the Satake x_i coordinates twists the action by an outer automorphism of S_6. □

6.2. Rational parametrizations

In this section we find rational parametrizations of $\mathcal{A}_2^*(2)/\Gamma_\Delta$ for $\Delta \not\equiv 1 \pmod 8$ where Γ_Δ is the fixed group of a level 2 Humbert component. In the cases where the Humbert surfaces are rational, these aid in the construction of a rational parametrization. The Rosenhain model $\mathcal{M}_2(2)$ is rational and we shall parametrize Rosenhain Humbert components for small discriminants $\Delta \equiv 1 \pmod 8$ in $\mathcal{M}_2(2)/S_3$ where S_3 acts the Rosenhain invariants by permutations.

Definition 6.6. *A variety is* rational *if it is birationally equivalent to $\mathbb{P}^n$ (equivalently $\mathbb{A}^n$) for some n.*

In §3.4.3 we found the fixed groups for the Humbert components in the symmetric Satake model $X[2]$. Let Γ_Δ be the fixed group for a Humbert component of discriminant Δ. Then all the Humbert components of discriminant Δ project onto a single component H_Δ^Γ via the quotient map $X[2] \to X[2]/\Gamma_\Delta$. Note that $X[2]/\Gamma_\Delta$ consists of points invariant under the Galois action of Γ_Δ hence the sextic polynomials have the factorization patterns as in Proposition 6.2.

For $\Delta \not\equiv 1 \pmod 8$ we determined the Γ_Δ-invariant polynomial rings. We now show that these varieties are rational.

Proposition 6.7. *Let $\Delta \not\equiv 1 \pmod 8$ be a discriminant of a Humbert surface. The weighted homogeneous coordinate ring of $X[2]/\Gamma_\Delta$ is isomorphic to $\mathbb{C}[p_1, s_2, s_3, s_5]$ if $\Delta \equiv 5 \pmod 8$, or $\mathbb{C}[p_1, p_2, s_2, s_3]$ if $\Delta \equiv 0 \pmod 4$.*

Proof. See Lemma 3.19 and Remark 3.20. □

The dense open subset given by $p_1 \neq 0$ is isomorphic to $\mathbb{A}^3$, hence we deduce the following.

Corollary 6.8. *The spaces $X[2]/\Gamma_\Delta$ are rational when $\Delta \not\equiv 1 \pmod 8$.*

Remark 6.9. For $\Delta \equiv 1 \pmod 8$ the fixed group Γ_Δ is isomorphic to $(S_3 \times S_3) \rtimes C_2$. From Lemma 3.19, the ring of $(S_3 \times S_3)$-invariants is $\mathbb{C}[p_1, p_2, p_3, s_2, s_3]$, and on the affine piece $p_1 = 1$ we find that p_3 can be eliminated, hence $X[2]/(S_3 \times S_3)$ is rational. The coordinate ring of $X[2]/\Gamma_\Delta$ is

$$\mathbb{C}[p_1^2, p_2(s_2 - p_2), p_3(s_3 - p_3), s_2, s_3],$$

but it is not immediately obvious whether this is rational.

Now that we know the coordinate rings explicitly, the map down to $A_2^* = \operatorname{Proj}(\mathbb{C}[s_2, s_3, s_5, s_6])$ can be realized. In particular a parametrization of $H_\Delta^\Gamma \subset X[2]/\Gamma_\Delta$ gives rise to a two dimensional family of points on the level 1 Humbert surface H_Δ. We now look at the cases $\Delta \equiv 5 \pmod 8$ and $\Delta \equiv 0 \pmod 4$ in more detail.

6.2.1. $\Delta \equiv 5 \pmod 8$**.** The projection map $X[2]/\Gamma_\Delta \to \mathcal{A}_2^*$ is defined by

$$(p_1 : s_2 : s_3 : s_5) \longmapsto (s_2 : s_3 : s_5 : s_6),$$

hence s_6 can be written as a polynomial $f(p_1, s_2, s_3, s_5)$ of weighted degree six. It follows from Proposition 6.2 that the Galois group of the Satake sextic $S(X) = \prod(X - x_i)$ is contained in a copy of S_5 which fixes $p_1 = x_1 \in \mathbb{Q}$. By writing $S(p_1) = 0$ as a function of s_6 we determine f:

$$f(p_1, s_2, s_3, s_5) = 6p_1^6 - 3s_2p_1^4 - 2s_3p_1^3 + \tfrac{3}{8}s_2^2p_1^2 + (s_2s_3 - \tfrac{6}{5}s_5)p_1 + (\tfrac{1}{16}s_2^3 + \tfrac{1}{3}s_3^2).$$

We shall work with the affine patch $p_1 = 1$.

Example 6.10. ($\Delta = 5$). The Humbert surface equation H_5^Γ in $X[2]/\Gamma_5$ is given by $s_2 = 3p_1^2$. On the affine patch $p_1 = 1$ we have $s_2 = 3$ and we obtain the two-variable parametrization

$$s_2 = 3\,,\quad s_3 = a\,,\quad s_5 = b\,,\quad s_6 = f(1, 3, a, b) = -\frac{6}{5}b + \frac{1}{3}a^2 + a + \frac{33}{16}.$$

Example 6.11. ($\Delta = 13$). We use the Humbert equation for discriminant 13 from the table on page 49. Set $p_1 = 1$ and consider s_2 as a coefficient.

Then $H_{13}^{\Gamma}(s_2, s_3, s_5) \in \mathbb{Q}(s_2)[s_3, s_5]$ defines a conic over $\mathbb{Q}(s_2)$ which can be parametrized by

$$s_3 = \frac{f_3(s_2, u)}{d(s_2, u)}, s_5 = \frac{f_5(s_2, u)}{d(s_2, u)}$$

where u is a free parameter and

$$\begin{aligned} f_3(s_2, u) &= 4608u^2 + (-204s_2^2 - 3000s_2 + 17748)u \\ &\quad + \tfrac{1}{256}(s_2 - 3)(s_2^2 + 186s_2 - 759)^2, \\ f_5(s_2, u) &= 240\,(7s_2 + 3)\,u^2 - \tfrac{325}{4}(s_2 + 9)(s_2 - \tfrac{23}{5})(s_2 + \tfrac{33}{13})u \\ &\quad + \tfrac{5}{3072}(s_2 - 9)(s_2 - 3)(s_2^2 + 186s_2 - 759)^2, \\ d(s_2, u) &= (s_2 - 75)\left(64u - s_2^2 + 54s_2 - 267\right). \end{aligned}$$

The same approach works for $\Delta = 21$: on the affine patch $p_1 = 1$, the Humbert component is a singular genus 0 curve over $\mathbb{Q}(s_2)$.

6.2.2. $\Delta \equiv 0 \pmod 4$**.** The projection map $X[2]/\Gamma_\Delta \to \mathcal{A}_2^*$ is defined by

$$(p_1 : p_2 : s_2 : s_3) \longmapsto (s_2 : s_3 : s_5 : s_6),$$

hence s_5, s_6 can be written as polynomials in p_1, p_2, s_2, s_3. By Proposition 6.2, the Satake sextic factorizes as $S(X) = (X^2 + c_1X + c_0)T(X)$ where T is a monic quartic in $\mathbb{Q}[X]$ and $c_1 = -p_1$ and $c_0 = (p_1^2 - p_2)/2$. By using Lemma 6.1 and comparing coefficients, we find the following expressions for s_5 and s_6:

$$\begin{aligned} s_5 &= -\tfrac{5}{48}(12p_1^5 - 24p_1^3p_2 + 8p_1^2s_3 - 36p_1p_2^2 + 24p_1p_2s_2 - 3p_1s_2^2 \\ &\quad + 8p_2s_3 - 8s_2s_3), \\ s_6 &= \tfrac{1}{48}(36p_1^6 - 180p_1^4p_2 + 36p_1^4s_2 + 48p_1^3s_3 + 108p_1^2p_2^2 - 9p_1^2s_2^2 \\ &\quad - 48p_1p_2s_3 + 36p_2^3 - 36p_2^2s_2 + 9p_2s_2^2 + 3s_2^3 + 16s_3^2). \end{aligned}$$

These equations determine the projection map $X[2]/\Gamma_\Delta \to \mathcal{A}_2^*$ explicitly.

Example 6.12. ($\Delta = 8$). The Humbert equation for H_8^{Γ} is

$$4s_2 - 9p_1 - 6p_2 = 0.$$

To parametrize H_8, fix a value for p_1 and let p_2 be free. This determines s_2. Let s_3 be the second free variable. Then we can compute s_5 and s_6 from the formulae above.

Example 6.13. ($\Delta = 12$). The Humbert equation for H_{12}^{Γ} is

$$16s_2^2 + (-168p_1^2 - 48p_2)s_2 - 128p_1s_3 - 111p_1^4 + 684p_1^2p_2 + 36p_2^2 = 0\,.$$

As a polynomial in s_3 it has degree 1. Thus if we fix p_1 and let p_2 be free we can determine s_3. Take s_2 to be the second free variable, then the values for s_5 and s_6 follow from the formulae above.

6.2.3. Rosenhain parametrizations. We shall parametrize the Rosenhain models for Humbert surfaces of discriminant $\Delta \equiv 1 \pmod 8$. Recall that a genus 2 curve has a model of the form $y^2 = x(x-1)(x-e_1)(x-e_2)(x-e_3)$ called a Rosenhain model.

Lemma 6.14. *There is a level 2 Rosenhain component $H_\Delta(e_1, e_2, e_3) = 0$ having symmetry group $(S_3 \times S_3) \rtimes C_2 \leq S_6$ which preserves the partition of roots $R = \{0, 1, \infty\} \cup \{e_1, e_2, e_3\}$.*

Proof. We know from Propositions 6.2 and 6.5 that the Galois action on the six roots $R = \{u_i\}$ is isomorphic to $(S_3 \times S_3) \rtimes C_2$ acting on the Satake x_i preserving the partition $\{x_1, x_2, x_3\} \cup \{x_4, x_5, x_6\}$ via an outer automorphism of S_6. Since S_6 has only one subgroup of order 72 up to conjugation, the representations are conjugate. Thus the Galois action on R preserves the partition $\{u_1, u_2, u_3\} \cup \{u_4, u_5, u_6\}$ for some ordering of roots. There are ten Humbert components which are in bijection with the ten partitions of this type; exactly one of them satisfies the conditions of the lemma. □

For our parametrizations we shall use the Rosenhain component appearing in the lemma above.

We now compute a Humbert component in $\mathcal{M}_2(2)/S_3$ where S_3 is the permutation group for the Rosenhain invariants. Let v_1, v_2, v_3 be the elementary symmetric functions in e_1, e_2, e_3. Then we can write $H_\Delta(e_1, e_2, e_3)$ more simply as $H_\Delta(v_1, v_2, v_3)$ and the Rosenhain model becomes

$$y^2 = x(x-1)(x^3 - v_1x^2 + v_2x - v_3).$$

One of the advantages of this model is that it has good reduction properties (see [**23**]) and consequently the heights of the coefficients, the Rosenhain invariants and the v_i are small in comparison to other models. The obvious disadvantage is that the rational points produced give rise to hyperelliptic polynomials with a rather small Galois group, namely the Galois group of the cubic factor whereas we know that generically the Galois group has order $|(S_3 \times S_3) \rtimes C_2| = 72$.

Now for an example. We have Rosenhain models for discriminants 9 and 17 at our disposal. In terms of the v_i, the Rosehnain component for

discriminant 9 is

$$\begin{aligned}
&16v_1^6v_3^2 - 8v_1^5v_2^2v_3 - 128v_1^5v_3^2 + v_1^4v_2^4 + 32v_1^4v_2^2v_3 + 112v_1^4v_2v_3^2 - 128v_1^4v_3^3 \\
&+ 384v_1^4v_3^2 + 4v_1^3v_2^3v_3 - 96v_1^3v_2^2v_3^2 - 32v_1^3v_2^2v_3 + 128v_1^3v_2v_3^3 - 64v_1^3v_2v_3^2 \\
&- 296v_1^3v_3^3 - 512v_1^3v_3^2 - 8v_1^2v_2^5 + 32v_1^2v_2^4v_3 - 32v_1^2v_2^3v_3^2 - 96v_1^2v_2^3v_3 \\
&- 370v_1^2v_2^2v_3^2 + 2112v_1^2v_2v_3^3 - 1088v_1^2v_2v_3^2 - 1792v_1^2v_3^4 + 2208v_1^2v_3^3 + 256v_1^2v_3^2 \\
&+ 112v_1v_2^4v_3 - 64v_1v_2^3v_3^2 + 128v_1v_2^3v_3 - 1088v_1v_2^2v_3^3 + 2112v_1v_2^2v_3^2 + 2048v_1v_2v_3^4 \\
&- 6412v_1v_2v_3^3 + 2048v_1v_2v_3^2 - 1024v_1v_3^5 + 4256v_1v_3^4 - 3232v_1v_3^3 + 16v_2^6 \\
&- 128v_2^5v_3 + 384v_2^4v_3^2 - 128v_2^4v_3 - 512v_2^3v_3^3 - 296v_2^3v_3^2 + 256v_2^2v_3^4 + 2208v_2^2v_3^3 \\
&- 1792v_2^2v_3^2 - 3232v_2v_3^4 + 4256v_2v_3^3 - 1024v_2v_3^2 + 1536v_3^5 - 2343v_3^4 + 1536v_3^3 .
\end{aligned}$$

As an affine curve over $\mathbb{Q}(v_1)$, the equation defines a (singular) genus 0 curve, thus the surface is rationally parametrizable.

The equation for discriminant 17 is too big to display here (see [**22**]), not to mention too large for us to complete a similar genus calculation. But given a height bound we are able to compute a large number points which suggests that it is rational.

6.3. Modular abelian surfaces

Modular abelian surfaces provide examples of rational points on Humbert surfaces. In this section we attempt to find such points on our Humbert surface models.

For the remainder of of this chapter, RM will refer to real multiplication by an order in a real quadratic field, that is to say that the discriminant Δ is nonsquare.

Let A be an abelian surface defined over a number field $k \subset \mathbb{C}$. An endomorphism $\alpha \in \mathrm{End}(A)$ is said to be *defined over* k when its analytic representation $\rho_a : \mathbb{C}^2 \to \mathbb{C}^2$ is k-linear. Write $\mathrm{End}_k(A)$ for the set of such endomorphisms.

We are interested in finding abelian surfaces A defined over $\mathbb{Q}$ with RM where $\mathrm{End}(A) = \mathrm{End}_{\mathbb{Q}}(A)$. These objects are modular in the following sense.

Theorem 6.15. *(Generalized Shimura-Taniyama Conjecture) Any abelian variety over $\mathbb{Q}$ with RM defined over $\mathbb{Q}$ is modular, that is, isogenous to a factor of $J_0(N) = \mathrm{Jac}(X_0(N))$ for some N.*

The result follows from Serre's conjecture [**65**], the proof of which was only recently completed by Khare and Wintenberger ([**39**], [**40**]).

We make use of a fact about the Galois representation on the 2-torsion.

Proposition 6.16. *(*[**77**, Corollary 4.3.4]*) Let F be a real quadratic field with ring of integers $\mathcal{O}$, and let A be an abelian surface over k with principal polarization defined over k and an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}_k^s(A)$*

into the subring of symmetric endomorphisms defined over k. Let $\bar{\rho}_2$ be the Galois representation on $A[2]$, and write $G = \bar{\rho}_2(\mathrm{Gal}(\bar{k}/k))$. Then

a) *if 2 is inert in F then $G \hookrightarrow A_5$,*
b) *if 2 is split in F then $G \hookrightarrow S_3 \times S_3$,*
c) *if 2 is ramified in F then there is an exact sequence $1 \to H \to G \to K \to 1$ with $H \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^3$ and $K \hookrightarrow S_3$.*

If 2 is ramified in F, Bending [**4**] has shown that $G \hookrightarrow S_2 \times S_4$.

Corollary 6.17. *Suppose A is a principally polarized abelian surface over $\mathbb{Q}$ with RM by an order of discrimimant Δ, also defined over $\mathbb{Q}$. Let G denote the Galois group of the Satake sextic. Then*

a) *if $\Delta \equiv 5 \pmod 8$ then $G \hookrightarrow A_5 \leq S_5$,*
b) *if $\Delta \equiv 1 \pmod 8$ then $G \hookrightarrow S_3 \times S_3 \leq (S_3 \times S_3) \rtimes C_2$,*
c) *if $\Delta \equiv 0 \pmod 4$ then $G \hookrightarrow S_2 \times S_4$*

where the groups act on the Satake x_i as detailed in Proposition 6.2.

Proof. The splitting behaviour of 2 is governed by quadratic reciprocity. The rest follows the previous result and Proposition 6.2. □

The corollary gives us a necessary condition for an RM abelian surface to be modular. In his thesis John Wilson [**77**, Theorem 4.4.3] showed that this condition is sufficient in the case $\Delta = 5$. We conjecture that it is also sufficient for odd discriminants:

Conjecture 6.18. *Let (A, G, Δ) be as in the corollary above with Δ being odd. If we have*

$$G \hookrightarrow \begin{cases} A_5 & \text{when } \Delta \equiv 5 \pmod 8, \\ S_3 \times S_3 & \text{when } \Delta \equiv 1 \pmod 8 \end{cases}$$

then A has its RM defined over $\mathbb{Q}$.

For discriminants $\Delta \equiv 0 \pmod 4$ the analogous statement is false:

Example 6.19. The point $(\lambda_1, \lambda_2, \lambda_3) = (-1/3, -1/6, 7/6)$ lies on the Rosenhain model of H_8. Using van Wamelen's Magma code we can compute the analytic Jacobian of $y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$ as well as generators of its endomorphism ring to arbitrary precision. By examining the complex entries of the 2×2 matrices we are able to detect when the entries are rational numbers using continued fractions. In this example we find the $\sqrt{2}$ endomorphism is defined over $\mathbb{Q}(\sqrt{2})$. Another example is the point $(\lambda_1, \lambda_2, \lambda_3) = (2, 49/22, 25/11)$ on H_{12}; the $\sqrt{3}$ endomorphism can only be defined over fields containing $\mathbb{Q}(\sqrt{11})$. Both these moduli points have rational 2-torsion hence the Galois group of the Satake sextic is trivial, yet neither has endomorphism ring defined over $\mathbb{Q}$.

In his PhD thesis [**77**], John Wilson constructed a model for H_5 in $\mathcal{M}_2(2)$ and rationally parametrized the modular points. We now attempt to find (conjecturally) modular parametrizations of Humbert surfaces using our models.

6.3.1. $\Delta \equiv 5 \pmod 8$**.** In this case there is a particularly simple criterion for a moduli point (s_2, s_3, s_5, s_6) to be modular (conjecturally modular if $\Delta \neq 5$) in terms of the Satake sextic polynomial. We know $S(X) = (X - x_i)T(X)$ where $x_i \in \mathbb{Q}$ and the Galois group of $T(X)$ is contained in A_5. Thus the discriminant of T is a square in $\mathbb{Q}$. We will consider the situation where $x_i \neq 0$. Without loss of generality we take $x_1 = 1$ be the rational root of $S(X)$.

Example 6.20. ($\Delta = 5$). As before, we work in the affine patch $x_1 = 1$. When we substitute $(H_5)_{(1)}$: $s_2 = 3x_1^2 = 3$ into the discriminant of $S(X)/(X-1)$ we get a polynomial in the two remaining variables

$$(s_5 - \tfrac{5}{4}s_3)\left(5s_5^3 + (\tfrac{-27}{4}s_3 - \tfrac{306}{125})s_5^2 + (-2s_3^3 - \tfrac{177}{400}s_3^2 + \tfrac{63}{50}s_3 + \tfrac{27}{100})s_5 + \tfrac{4}{45}s_3^5 + \tfrac{59}{30}s_3^4 + \tfrac{811}{320}s_3^3 + \tfrac{21}{20}s_3^2 + \tfrac{9}{80}s_3\right)$$

which we want to be a nonzero square y^2. This defines an elliptic curve over $\mathbb{Q}(s_3)$ with distinguished rational point $y = 0, s_5 = \frac{5}{4}s_3$. Rational points on this elliptic surface produce the desired moduli points.

Example 6.21. ($\Delta = 13$). We use the parametrization from Section 6.2.1. The discriminant of $T(X)$ is a polynomial in $\mathbb{Q}[s_2, u]$. Finding modular points reduces to finding values for s_2, u such that the squarefree part of the discriminant polonynomial is a rational square. We discover that modular points must satisfy

$$y^2 = -3(s_2 - 3)Q(s_2, u)$$

where Q is an irreducible quartic polynomial in u with coefficients in $\mathbb{Q}[s_2]$. This is a genus 1 curve over $\mathbb{Q}[s_2]$. Finding points from scratch is near impossible as they have extremely large height. But if we are given a rational point, we can restrict to the genus 1 curve over $\mathbb{Q}$ which is now an elliptic curve and then we have elliptic curve machinery at our disposal to find further points.

6.3.2. $\Delta \equiv 1 \pmod 8$**.** In this case we only have Rosenhain parametrizations from §6.2.3 to work with. The Galois group of the hyperelliptic polynomial $x(x-1)(x^3 - v_1x^2 + v_2x - v_3)$ is contained in S_3 which acts by preserving the set of Rosenhain invariants $\{e_1, e_2, e_3\}$ and fixing the other roots. It follows from Conjecture 6.18 that all such points should have RM defined over $\mathbb{Q}$ and hence be modular.

Example 6.22. The point $(v_1, v_2, v_3) = (15/2, 0, 3/2)$ lies on H_9 and defines a hyperelliptic curve over $\mathbb{Q}$ whose Jacobian has real multiplication defined over $\mathbb{Q}$. But because the endomorphism algebra is not a real quadratic field, the Jacobian does not satisfy the hypotheses of the generalised Shimura-Taniyama conjecture. Using Qing Liu's `genus2reduction` program [**49**] we find that the odd part of conductor is $243 = 3^5$ which confirms that the curve is not modular over $\mathbb{Q}$ since otherwise the conductor would have to be square.

6.4. Congruence primes

In this section we use Humbert surfaces to classify the primes p for which a modular Jacobian surface splits as a product of elliptic curves. This allows us to 'predict' which coefficients of the associated modular form are in $\mathbb{Z}$. To begin we give the reader a brief account of Eichler-Shimura theory.

6.4.1. Eichler-Shimura theory. Let $N > 2$ be an integer and $S_2(N)$ the set of cusp forms of weight 2 for the Hecke subgroup $\Gamma_0(N)$. Let $f = \sum a_n q^n \in S_2(N)$ be a newform, that is, an eigenfunction for all the Hecke operators T_n, normalized so that $f|T_n = a_n f$. Then the L-function of f has an Euler product

$$L(s, f) := \sum_{n \geq 1} a_n n^{-s} = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p | N} (1 - a_p p^{-s})^{-1}$$

Shimura's construction associates an abelian variety to such a newform.

Theorem 6.23. *(*[**69**, Theorem 7.14]*) Let $f = \sum a_n q^n$ be a newform of weight 2 for $\Gamma_0(N)$. Let K_f be the subfield of $\mathbb{C}$ generated by all the a_n. Then there exists an abelian subvariety A_f of $J_0(N) = \mathrm{Jac}(X_0(N))$ and an embedding $\theta : K_f \hookrightarrow \mathrm{End}(A_f) \otimes \mathbb{Q}$ with the following properties:*

a) $\dim(A_f) = [K_f : Q]$,
b) $\theta(a_n) = T_n|_{A_f}$, *the restriction of the Hecke operator T_n to A_f,*
c) A_f *is defined over $\mathbb{Q}$.*

The pair (A_f, θ) is determined by the first two properties. Moreover, for every embedding $\sigma : K_f \hookrightarrow \mathbb{C}$, the function $f^\sigma = \sum a_n^\sigma q^n$ is a normalized eigenform.

The abelian variety A_f need not be principally polarizable. It has good reduction at primes $p \nmid N$. Eichler-Shimura theory relates the reduction of A_f over finite fields to Hecke operators.

Theorem 6.24. *(*[**69**, Theorem 7.15]*) The L-function of A_f over $\mathbb{Q}$ coincides up to a finite number of Euler factors (corresponding to primes of bad*

reduction, i.e. $p \mid N$*) with the product*

$$\prod_{\sigma}(1 - a_p^{\sigma}p^{-s} + p^{-2s})^{-1}.$$

For a prime of good reduction $p \nmid N$, the local Euler factors determine the numerator of the zeta function for the reduction $\widetilde{A}_f$ mod p. The characteristic polynomial of Frobenius is the (Weil) polynomial

$$\prod_{\sigma}(X^2 - a_p^{\sigma}X + p),$$

thus the trace of Frobenius equals the trace of the Hecke operator.

6.4.2. Modular Jacobian surfaces. Let C be a genus 2 curve over $\mathbb{Q}$ whose Jacobian is modular of conductor N. This means $\mathrm{Jac}(C)$ is isogenous to an A_f where $f = \sum a_n q^n \in S_2(N)$ is a newform. Also we have $\mathrm{End}(A_f) \otimes \mathbb{Q} \cong K_f$, a real quadratic field and the $a_n \in K_f$ are algebraic integers. Let σ denote the nontrivial $\mathbb{Q}$-automorphism of K_f. For good primes $p \nmid N$, the reduction $\widetilde{A}_f$ over $\mathbb{F}_p$ is an abelian surface and has Weil polynomial

$$(X^2 - a_pX + p)(X^2 - a_p^{\sigma}X + p) \in \mathbb{Z}[X].$$

Question. For which primes is $a_p \in \mathbb{Z}$?
If $a_p \in \mathbb{Z}$, the Weil polynomial is $(X^2 - a_pX + p)^2$ which shows that $\widetilde{A}_f$ is isogenous over $\mathbb{F}_p$ to $E \times E$, where E is a (CM) elliptic curve over $\mathbb{F}_p$. Thus $\widetilde{A}_f$ is a point on H_{m^2} mod p for some m. This motivates the following definition.

Definition 6.25. *Let* A_f *be a principally polarizable modular abelian surface over* $\mathbb{Q}$ *with level* 1 *invariants* $s_2, s_3, s_5, s_6 \in \mathbb{Q}$*. Note that* $H_{\Delta(K_f)}(s_i) = 0$*. Let* B *be the set of primes* p *for which* $H_1(s_2, s_3, s_5, s_6) \equiv 0 \pmod{p}$*. A* congruence prime *for* A_f *is a prime* $p \notin B$ *satisfying*

$$H_{m^2}(s_2, s_3, s_5, s_6) \equiv 0 \pmod{p}$$

for some $m > 1$.

Remark 6.26. The set B consists of the primes dividing N (primes of bad reduction for A_f) together with $\{2, 3, 5\}$ which are the bad primes for level 1 Humbert models.

Proposition 6.27. *(Weil's Theorem) Let* $(A, \mathcal{L})$ *be a principally polarized abelian surface defined over a field* k*. Then* $(A, \mathcal{L})$ *is one and only one of three possibilities:*

a) *the polarized Jacobian of a genus* 2 *curve over* k*,*
b) *the product of two polarized elliptic curves over* k*,*

c) *the restriction of scalars of a polarized elliptic curve E over a quadratic extension K of k. In other words $(A, \mathcal{L})$ is simple over k, but over K is isomorphic to $E \times E^\sigma$ where σ is the nontrivial automorphism of K over k.*

Proof. See [**18**, Theorem 3.1]. □

Theorem 6.28. *Suppose p is a congruence prime for A_f. Then the Weil polynomial of $\widetilde{A}_f$ over $\mathbb{F}_p$ is either $(X^2 - a_p X + p)^2$ or $X^4 - a_{p^2}X^2 + p^2$. In the second case, the Weil polynomial over $\mathbb{F}_{p^2}$ is $(X^2 - a_{p^2}X + p^2)^2$.*

Proof. Without loss of generality we can assume A_f is principally polarized. Since p is a prime of good reduction, $\widetilde{A}_f/\mathbb{F}_p$ is principally polarized. By definition, $\widetilde{A}_f$ lies on H_{m^2} for some m, hence splits over $\overline{\mathbb{F}}_p$. Proposition 6.27 tells us that $\widetilde{A}_f$ will split over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$. The rest follows easily. □

A congruence prime p must satisfy $a_p \in \mathbb{Z}$ or $\mathrm{Tr}(a_p) = 0$. When $a_p \notin \mathbb{Z}$ we call p an *exceptional* prime. They are exceptional in the sense that amongst the primes dividing $H_{m^2}(s_i)$ the exceptional ones are scarce.

Lemma 6.29. *Let A be a QM abelian surface defined over $\overline{\mathbb{Q}}$ and p a prime of good reduction. Then the reduction $\widetilde{A}/\mathbb{F}_p$ is geometrically isogenous to the square of elliptic curve.*

Proof. Let $q = p^r$ be a finite field such that $\mathrm{End}(\widetilde{A}) = \mathrm{End}_{\mathbb{F}_q}(\widetilde{A})$. The Frobenius endomorphism π with respect to $\mathbb{F}_q$ lies in the center of $\mathrm{End}(\widetilde{A})$. Since A is a QM abelian surface, the center of $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathbb{Z})$ equals $\mathbb{Z}$. If $\pi \in \mathbb{Z}$ then A is supersingular. If $\pi \notin \mathbb{Z}$ then the center of $\mathrm{End}_{\overline{\mathbb{F}}_q}(\widetilde{A})$ strictly contains $\mathbb{Z}$, in which case we have $\mathrm{End}_{\overline{\mathbb{F}}_q}(\widetilde{A}) \cong \mathbb{M}_2(K)$ by the classification of endomorphism algebras for abelian surfaces (Example 1.58). We see that in both cases $\widetilde{A}$ is isogenous to the square of an elliptic curve. □

Remark 6.30. From the lemma, it follows that primes $p \notin B$ dividing *any* $H_\Delta(s_i)$ are congruence primes.

This helps us to understand why exceptional primes are the exception: congruence primes are points on mod p Humbert intersections $H_\Delta \cap H_{m^2}$ which are unions of Shimura curves (dimension 1). The exceptional primes correspond to CM points (dimension 0) on Shimura curves.

CHAPTER 7

Explicit CM-theory in Dimension 2

For a principally polarized abelian surface A with endomorphism ring isomorphic to the maximal order $\mathcal{O}_K$ in a quartic CM-field K, the Igusa invariants $j_1(A), j_2(A), j_3(A)$ generate an abelian extension of its reflex field. In this chapter [1] we give an explicit description of the Galois action of the class group of the reflex field on these Igusa values. The description we give is geometric and it can be expressed by maps between various Siegel modular varieties. We can explicitly compute this action for ideals of small norm, allowing us to compute various Igusa class polynomials modulo primes. Furthermore, we give a theoretical obstruction to a generalization of the 'isogeny volcano' algorithm to compute endomorphism rings of abelian surfaces over finite fields. While seemingly unconnected to CM-theory, we show that Humbert surfaces can be used to improve the running time of CRT-method.

7.1. Introduction

Class field theory describes the abelian extensions of a given number field K. For $K = \mathbb{Q}$, the Kronecker-Weber theorem tells us that every abelian extension of K is contained in a *cyclotomic extension*. In 1900, Hilbert asked for a similar 'explicit description' for higher degree number fields. This not-entirely well-posed problem, known as Hilbert's 12th problem, is still largely unsolved.

Besides $K = \mathbb{Q}$, the answer is only completely known for imaginary quadratic fields K. In this case, the solution is provided by *complex multiplication* theory [**71**, Ch. 2]. The techniques used can be generalized to *CM-fields* K, i.e., imaginary quadratic extensions of totally real fields. However, for general CM-fields we do not always get an explicit description of the full maximal abelian extension. From a computational perspective, the case of general CM-fields is far less developed than the imaginary quadratic case.

We will focus solely on degree 4 CM-fields K. For such fields, invariants of principally polarized abelian surfaces (p.p.a.s.) with endomorphism ring isomorphic to the maximal order $\mathcal{O}_K$ of K generate a subfield of the

[1] Excluding the final section, this chapter is joint work with Reinier Bröker and Kristin Lauter, undertaken as part of a summer internship at Microsoft Research in 2008.

Hilbert class field of the *reflex field* K_Φ of K. The reflex field K_Φ of K is a degree 4 subfield of the normal closure of K and equals K in the case K is Galois. To explicitly compute the resulting extension, we can compute an *Igusa class polynomial*

$$P_K = \prod_{\{A \ p.p.a.s. | \mathrm{End}(A)=\mathcal{O}_K\}/\cong} (X - j_1(A)) \in \mathbb{Q}[X],$$

if A is not isomorphic to a product of elliptic curves with the product polarization. Here, j_1 is one of the *three* Igusa invariants of A. A contrast with the case of imaginary quadratic fields – where we compute the *Hilbert class polynomial* – is that the polynomial P_K need not be irreducible over $\mathbb{Q}$, and it will typically not have integer coefficients.

There are various methods to explicitly compute the polynomial P_K. We can use complex arithmetic [**76**], p-adic arithmetic ([**17**], [**10**]) for $p = 2, 3$ or finite field arithmetic. However, none of these approaches exploit the action of $\mathrm{Gal}(K_r(j_1(A))/K_r)$ on a p.p.a.s. A that has endomorphism ring $\mathcal{O}_K$. The goal of this chapter is to make this Galois action explicit and give a method to compute it. Our algorithm to compute the Galois action significantly speeds up the 'CRT-approach' [**14**] to compute an Igusa class polynomial.

Besides speeding up the computation of Igusa class polynomials, our algorithm gives a method of computing *isogenies* between abelian surfaces over finite fields. Computing an isogeny is a basic computational problem in arithmetic geometry, and we expect that our algorithm can be used in a variety of contexts, ranging from point counting on Jacobians of curves to cryptographic protocols.

Our computations naturally lead to the study of the (l, l)-isogeny graph for abelian surfaces over finite fields. For elliptic curves, the l-isogeny graph looks like a 'volcano' and this observation forms the heart of the algorithm [**44**] to compute the endomorphism ring of an elliptic curve over a finite field. We show that for abelian surfaces, the (l, l)-isogeny does *not* have a volcano shape. This shows that a straightforward generalization of the elliptic curve algorithm to abelian surfaces is impossible.

The structure of this chapter is as follows. In Section 7.2 we recall the basic facts of complex multiplication theory, and in Section 7.3 we give a 'geometric description' of the Galois action. Our algorithm to compute this action is intrinsically linked to Siegel modular functions of higher level. Section 7.4 gives the definitions and properties of the four Siegel modular functions that we use. The algorithm to compute the Galois action is detailed in Section 7.5 and we apply it in Section 7.6 where we give a method to comptute an Igusa class polynomial modulo a prime p. This 'mod p computation' is the main improvement to the CRT-algorithm. We illustrate our

approach with various detailed examples in Section 7.7. Section 7.8 contains the obstruction to the volcano picture for abelian surfaces. The final Section 7.9 points out some additional improvements to the CRT-algorithm that rely on knowing equations of Humbert surfaces.

7.2. CM-theory

In this section we recall the basic facts of CM-theory for higher dimensional abelian varieties. Most of the material presented in this section is an adaptation to our needs of the definitions and proofs of Shimura's textbook [**70**].

7.2.1. CM-fields. A *CM-field* is an imaginary quadratic extension of a totally real number field. Throughout this article, we denote by K^+ the real quadratic subfield of a CM-field K. In the simplest case $K^+ = \mathbb{Q}$, the CM-fields are imaginary quadratic fields. We will solely focus on degree 4 fields K in this paper.

Let K be a fixed quartic CM-field, and let $\{\varphi_1, \ldots, \varphi_4\}$ be the embeddings of K into the complex numbers $\mathbb{C}$. A *CM-type* Φ is a choice of two embeddings such that we have $\Phi \cap \overline{\Phi} = \emptyset$. We interpret Φ in the natural way as a map $K \hookrightarrow \mathbb{C}^2$.

We say that a principally polarized abelian surface $A/\mathbb{C}$ has CM by the maximal order $\mathcal{O}_K$ if there exists an isomorphism $\mathcal{O}_K \xrightarrow{\sim} \mathrm{End}(A)$. The CM-type distinguishes these surfaces. More precisely, a surface A has *type* $\Phi = \{\varphi_1, \varphi_2\}$ if the complex representation $R_{\mathbb{C}}$ of the endomorphism algebra $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ satisfies

$$R_C \cong \varphi_1 \oplus \varphi_2.$$

If Φ has the additional property that it is *primitive*, i.e. it does not equal the lift of a CM-type of an imaginary quadratic subfield of K, then an abelian surface that has CM by $\mathcal{O}_K$ of type Φ is *simple* [**47**, Th. 1.3.6].

An automorphism σ of K induces an isomorphism $(A, \Phi) \xrightarrow{\sim} (A^\sigma, \Phi^\sigma)$ of CM abelian surfaces where $\Phi^\sigma = \{\varphi_1\sigma, \varphi_2\sigma\}$. This shows that conjugate CM-types produce the same sets of isomorphism classes of abelian surfaces.

If L denotes the normal closure of K, then we have

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, C_4 \text{ or } D_4$$

and the only case where we have non-primitive CM-types is the biquadratic case. We will mostly restrict ourselves to the *primitive* case in this article. In the Galois cases there is only one CM-type up to conjugacy and in the dihedral case there are two distinct CM-types.

Let (K, Φ) be a primitive quartic CM-field, and let Φ be a CM-type for K. For an $\mathcal{O}_K$-ideal, the abelian surface $A_I = \mathbb{C}^2/\Phi(I)$ is a 2-dimensional torus with type Φ by [**47**, Th. 4.1]. This surface need not admit a principal polarization. The dual variety of A_I is given by $\widehat{A_I} = \mathbb{C}^2/\Phi(\overline{I}\mathfrak{D}_K^{-1})$, where

$$\mathfrak{D}_K^{-1} = \{x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(x\mathcal{O}_K) \subseteq \mathbb{Z}\}$$

is the inverse different. If $\pi \in K$ satisfies $\Phi(\pi) \in (i\mathbb{R}_{>0})^2$ and $\pi I\overline{I} = \mathfrak{D}_K^{-1}$, then the map $A_I \to \widehat{A}_I$ given by

$$(z_1, z_2) \mapsto (\varphi_1(\pi)z_1, \varphi_2(\pi)z_2)$$

is an isomorphism ([**70**, p. 102–104]) and A_I is principally polarizable. All principally polarized abelian surfaces with CM by $\mathcal{O}_K$ of type Φ arise via this construction.

We extend Φ to a CM-type Φ' of L, and we define the *reflex field*

$$K_\Phi = \mathbb{Q}\Big(\Big\{\textstyle\sum_{\phi\in\Phi'} \phi(x) \mid x \in K\Big\}\Big).$$

The CM-type on K induces a CM-type $f_\Phi = \{\sigma^{-1}|_{K_\Phi} : \sigma \in \Phi'\}$ on the reflex field K_Φ. The field K_Φ is a subfield of L of degree 4. In particular, it equals K in the case K is Galois. If $L/\mathbb{Q}$ is dihedral, then K_Φ and K are not isomorphic. However, the two different CM-types yield isomorphic reflex fields in this case. Furthermore, we have

$$(K_\Phi)_{f_\Phi} = K$$

and the CM-type f_Φ corresponds to Φ.

7.2.2. Igusa invariants. Any principally polarized abelian surface over $\mathbb{C}$ is of the form $\mathbb{C}^2/(\mathbb{Z}^2 + \mathbb{Z}^2\tau)$ where τ is an element of the *Siegel upper half plane*

$$\mathcal{H}_2 = \{\tau \in \mathbb{M}_2(\mathbb{C}) \mid \tau \text{ symmetric, } \mathrm{Im}(\tau) \text{ positive definite}\}.$$

The moduli space of principally polarized abelian surfaces is 3-dimensional. Let j_1, j_2, j_3 be coordinates for this space. More precisely, two surfaces $A = A_\tau$ and $A' = A_{\tau'}$ are isomorphic if and only if

$$(j_1(\tau), j_2(\tau), j_3(\tau)) = (j_1(\tau'), j_2(\tau'), j_3(\tau'))$$

holds.

There are various choices that one can make for j_1, j_2, j_3 and there are different conventions about which choice is the 'right' one. We define the functions as follows. Let E_w be the Siegel Eisenstein series

$$E_w(\tau) = \sum_{c,d} (c\tau + d)^{-w},$$

where the sum ranges over all co-prime symmetric 2×2-integer matrices that are non-associated with respect to left-multiplication by $\mathrm{GL}(2,\mathbb{Z})$. With

$$\chi_{10} = \frac{-43867}{2^{12}\cdot 3^5\cdot 5\cdot 7\cdot 53}(E_4E_6 - E_{10})$$

and

$$\chi_{12} = \frac{131\cdot 593}{2^{13}\cdot 3^7\cdot 5^3\cdot 7^2\cdot 337}(3^2\cdot 7^2E_4^3 + 2\cdot 5^3E_4^6 - 691E_{12}),$$

we define the *Igusa functions* j_1, j_2, j_3 as

$$j_1 = 2\cdot 3^5\frac{\chi_{12}^5}{\chi_{10}^6}, \quad j_2 = 2^{-3}3^3\frac{E_4\chi_{12}^3}{\chi_{10}^4}, \quad j_3 = 2^{-5}\cdot 3\frac{E_6\chi_{12}^2}{\chi_{10}^3} + 2^{-3}\cdot 3^2\frac{E_4\chi_{12}^3}{\chi_{10}^4}.$$

Alternatively, one can express the Igusa functions in terms of *theta null values*, defined in Section 7.4. The (rather unwieldy) formulas for passing between two descriptions are given by Igusa, see [**35**, p. 848].

A 'weak version' of the main theorem of complex multiplication theory is that, for a primitive quartic CM-field K, the Igusa invariants of an abelian variety with CM by $\mathcal{O}_K$ generate an unramified abelian extension of a reflex field of K. More precisely, we have the following result.

Theorem 7.1. *Let K be a primitive quartic CM field and let Φ be a CM-type for K. Let I be an $\mathcal{O}_K$ ideal such that there exists a principal polarization on $A_I = \mathbb{C}^2/\Phi(I)$. Then the field $K_\Phi(j_1(A_I), j_2(A_I), j_3(A_I))$ is a subfield of the Hilbert class field of K_Φ. The polynomial*

$$P_K = \prod_{\{[A/\mathbb{C}]\,|\,\mathrm{End}(A)\cong\mathcal{O}_K\}} (X - j_1(A))$$

has rational coefficients. The same is true for the minimal polynomials Q_K, R_K of the j_2 and j_3-invariants.

Proof. It is proved in [**70**, Main Theorem 1, p. 112] that the composite of K_Φ with the field of moduli of A_I is contained in the Hilbert class field of K_Φ. It follows from [**68**, p. 525] that for primitive quartic CM fields K, the field of definition of A_I is contained in the field of moduli, thus proving the first statement. The fact that the polynomials have rational coefficients follows from the fact that A_I^σ is also of type (K,Φ), for σ an automorphism of $\mathbb{C}$ □

We will see in Corollary 7.4 that, for any CM-type Φ, there always exists an $\mathcal{O}_K$-ideal I as in the Theorem.

7.2.3. Galois action of the class group. We define a group $\mathfrak{C}(K)$ as

$$\left\{ (\mathfrak{a},\alpha) \;\middle|\; \begin{array}{c} \mathfrak{a} \text{ a fractional } \mathcal{O}_K\text{-ideal with } \mathfrak{a}\overline{\mathfrak{a}} = (\alpha) \\ \text{and } \alpha \in K^+ \text{ totally positive} \end{array} \right\} / \cong$$

where $(\mathfrak{a},\alpha) \cong (\mathfrak{b},\beta)$ if and only if there exists a unit $u \in K^*$ with $\mathfrak{b} = u\mathfrak{a}$ and $\beta = u\overline{u}\alpha$. The multiplication is defined componentwise, and $(\mathcal{O}_K, 1)$ is the neutral element of $\mathfrak{C}(K)$.

The group $\mathfrak{C}(K)$ naturally acts on the set $S(K,\Phi)$ of isomorphism classes of principally polarized abelian surfaces that have CM by $\mathcal{O}_K$ of a given type Φ. Indeed, any such surface is given by an ideal I determining the variety and a 'Φ-positive' element $\pi \in K$ giving the principal polarization. We now put

$$(\mathfrak{a},\alpha)\cdot(I,\pi) = (\mathfrak{a}^{-1}I, \alpha\pi)$$

for $(\mathfrak{a},\alpha) \in \mathfrak{C}(K)$. By [**70**, §14.6], the action of $\mathfrak{C}(K)$ on $S(K,\Phi)$ is transitive and free. In particular, we have $|\mathfrak{C}(K)| = |S(K,\Phi)|$.

Theorem 7.2. *Let K be a primitive quartic CM-field. The set $S(K)$ of isomorphism classes of principally polarized abelian surfaces with CM by $\mathcal{O}_K$ has cardinality*

$$|S(K)| = \begin{cases} |\mathfrak{C}(K)| & \text{if } \mathrm{Gal}(K/\mathbb{Q}) \cong C_4\,, \\ 2|\mathfrak{C}(K)| & \text{if } \mathrm{Gal}(K/\mathbb{Q}) \cong D_4\,. \end{cases}$$

Proof. We have that $|S(K,\Phi)| = |\mathfrak{C}(K)|$ which is independent of the choice of CM type Φ. Let n be the number of CM-types (up to conjugacy). The theorem follows immediately from the equality $|S(K)| = n|S(K,\Phi)|$. □

The structure of the group $\mathfrak{C}(K)$ is best described by the following theorem.

Theorem 7.3. *Let K be a primitive quartic CM-field. Then the sequence*

$$1 \longrightarrow (\mathcal{O}_{K^+}^*)^+/N_{K/K^+}(\mathcal{O}_K^*) \overset{u\mapsto(\mathcal{O}_K,u)}{\longrightarrow} \mathfrak{C}(K) \overset{(\mathfrak{a},\alpha)\mapsto\mathfrak{a}}{\longrightarrow} \mathrm{Cl}(\mathcal{O}_K) \overset{N_{K/K^+}}{\longrightarrow} \mathrm{Cl}^+(\mathcal{O}_{K^+}) \longrightarrow 1$$

is exact.

Proof. The exactness at $\mathfrak{C}(K)$ and $\mathrm{Cl}(\mathcal{O}_K)$ is the contents of [**70**, Prop. 14.5]. It remains to show that the sequence is exact at $\mathrm{Cl}^+(\mathcal{O}_{K^+})$. To prove this, we first prove [2] that there is a *finite* prime that is ramified in K/K^+.

Suppose that K/K^+ is unramified at all finite primes. By genus theory, we then have $K = K^+(\sqrt{n})$ with $n \in \mathbb{Z}$. However, K then has $\mathbb{Q}(\sqrt{n})$ as quadratic subfield and K is a biquadratic field. This contradicts our assumption that K is primitive.

[2] We thank Everett Howe for suggesting this argument.

As there is a finite prime of K^+ that ramifies in K, the extensions K/K^+ and $H^+(K^+)/K^+$ are linearly disjoint. Here, H^+ denotes the narrow Hilbert class field. By Galois theory, we then have

$$\mathrm{Gal}(H(K)/K) \twoheadrightarrow \mathrm{Gal}(KH^+(K^+)/K) \xrightarrow{\sim} \mathrm{Gal}(H^+(K^+)/K^+)$$

which proves the theorem. □

Corollary 7.4. *Let K be a primitive quartic CM-field. For any CM-type Φ, there are exactly*

$$\frac{|\mathrm{Cl}(\mathcal{O}_K)|}{|\mathrm{Cl}^+(\mathcal{O}_{K^+})|} \cdot |(\mathcal{O}_{K^+}^*)^+/N_{K/K^+}(\mathcal{O}_K^*)| \geq 1$$

isomorphism classes of principally polarized abelian surfaces that have CM by $\mathcal{O}_K$ of type Φ.

Let A be a principally polarized abelian surface that has CM by $\mathcal{O}_K$ of type Φ. The Galois group $\mathrm{Gal}(K_\Phi(j_1(A))/K_\Phi)$ acts in the following way on the set $S(K,\Phi)$. With f_Φ the CM-type on K_Φ induced by Φ, we define $N_\Phi : K_\Phi \to K$ by

$$N_\Phi(x) = \prod_{\varphi \in f_\Phi} \varphi(x).$$

For an $\mathcal{O}_{K_\Phi}$-ideal I, the $\mathcal{O}_K$-ideal $N_\Phi(I)$ is called the *typenorm* of I. We get a natural map $m : \mathrm{Cl}(\mathcal{O}_{K_\Phi}) \to \mathfrak{C}(K)$ defined by

$$m(\mathfrak{p}) = (N_\Phi(\mathfrak{p}), N_{K_\Phi/\mathbb{Q}}(\mathfrak{p})).$$

The Galois group of $K_\Phi(j_1(A))/K_\Phi$ is a quotient of $\mathrm{Gal}(H(K_\Phi)/K_\Phi) \cong \mathrm{Cl}(\mathcal{O}_{K_\Phi})$, and by [**70**, §15.2] the induced map

$$m : \mathrm{Gal}(K_\Phi(j_1(A))/K_\Phi) \to \mathfrak{C}(K)$$

is *injective*. This describes the Galois action. In Example 7.16 we will see that the map $\mathrm{Cl}(\mathcal{O}_{K_\Phi}) \to \mathfrak{C}(K)$ need not be injective.

We conclude Section 7.2 with the observation that the typenorm can be defined in a slightly different way as well. If $K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$, then we have $N_\Phi(\mathfrak{p}) = \mathfrak{p}^{1+\sigma^3}$. If K is not Galois, then we have $N_\Phi(\mathfrak{p}) = N_{L/K}(\mathfrak{p}\mathcal{O}_L)$.

7.3. Computing the CM-action

Throughout this section, we let K be a fixed primitive quartic CM-field. We also fix a CM-type $\Phi : K \to \mathbb{C}^2$. Let $A/\mathbb{C}$ be a principally polarized abelian surface that has complex multiplication by $\mathcal{O}_K$ of CM-type Φ. The condition that K is primitive ensures that A is *simple*, i.e., not isogenous to a product of elliptic curves. By Theorem 7.1 the field

$K_\Phi(j_1(A), j_2(A), j_3(A))$ that we get by adjoining the Igusa invariants of A to the reflex field K_Φ is a subfield of the Hilbert class field $H(K_\Phi)$ of K_Φ.

The Artin map induces an isomorphism

$$\mathrm{Gal}(H(K_\Phi)/K_\Phi) \xrightarrow{\sim} \mathrm{Cl}(\mathcal{O}_{K_\Phi})$$

between the Galois group of the extension $H(K_\Phi)/K_\Phi$ and the class group of the maximal order of K_Φ. The resulting action of $\mathrm{Cl}(\mathcal{O}_{K_\Phi})$ on the set of all principally polarized abelian surfaces that have CM by $\mathcal{O}_K$ of type Φ is given by the *typenorm map* m introduced in Section 7.2.

Let I be a $\mathcal{O}_{K_\Phi}$-ideal of norm l. We assume for simplicity that l is prime. We have $m(I) = (N_\Phi(I), l) = (J, l) \in \mathfrak{C}(K)$, where J is an $\mathcal{O}_K$-ideal of norm l^2.

Lemma 7.5. *Let I be an $\mathcal{O}_{K_\Phi}$-ideal of prime norm l with typenorm $N_\Phi(I) = J$. Then the $\mathcal{O}_K$-ideal J ideal divides $(l) \subset \mathcal{O}_K$.*

Proof. This is clear if $K/\mathbb{Q}$ is Galois. Indeed, in this case I and all its Galois conjugates divide (l) as $\mathcal{O}_K$-ideal.

If the normal closure L/K has Galois group D_4, then the ideal J is given by

$$J = N_{L/K}(I\mathcal{O}_L).$$

Since the splitting of l in K_Φ determines the splitting of l in K, a case-by-case check gives the lemma. We refer to [**19**, p. 38] for a list of all possible decompositions. □

For an $\mathcal{O}_K$-ideal M, we define the 'M-torsion' of the abelian surface A by

$$A[M] = \{P \in A(\mathbb{C}) \mid \forall \alpha \in M : \alpha(P) = 0\}.$$

We assume here that we have *fixed* an isomorphism $\mathrm{End}(A) \xrightarrow{\sim} \mathcal{O}_K$, meaning that M is an $\mathrm{End}(A)$-ideal as well. If M is generated by an integer n, then $A[M]$ equals the n-torsion $A[n]$.

Lemma 7.5 tells us that group $A[J]$ is a 2-dimensional subspace of the l-torsion $A[l]$ of A. The polarization of A induces a symplectic form called the *Weil pairing* on $A[l]$, and $A[l]$ is a *symplectic* vector space of dimension 4 over the finite field $\mathbb{F}_l$.

Lemma 7.6. *Let A be a p.p.a.s. and let R be a proper subgroup of $A[l]$. Then R is the kernel of an isogeny of principally polarized abelian surfaces $\varphi : A \to B$ if and only if $R \cong (\mathbb{Z}/l\mathbb{Z})^2$ is a maximal isotropic subgroup with respect to the Weil pairing. Such a φ is called an (l, l)-isogeny.*

Proof. See Milne [**51**, Proposition 16.8]. □

By CM-theory, $A[J]$ is isotropic with respect to the Weil pairing and hence

the map

$$A \to A/A[J]$$

is an (l,l)-*isogeny*.

The moduli space of all pairs (S,G), with S a principally polarized abelian surface over $\mathbb{C}$ and G a 2-dimensional isotropic subspace of $S[l]$ can be described by an ideal $V(l) \subset \mathbb{Q}[X_1,Y_1,Z_1,X_2,Y_2,Z_2]$. More precisely, the variety corresponding to $V(l)$ equals the Siegel modular variety $Y_0^{(2)}(l)$ introduced e.g. in [**57**]. As a complex Riemann surface, we have

$$Y_0^{(2)}(l) = \Gamma_0^{(2)}(l)\backslash\mathcal{H}_2,$$

with

$$\Gamma_0^{(2)}(l) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{Z}) \mid c \equiv 0_2 \bmod l \right\}.$$

If we specialize $V(l)$ at a point $(X_1,Y_1,Z_1) = (j_1(A),j_2(A),j_3(A))$ then the resulting ideal $V'(l)$ is 0-dimensional. The corresponding variety is a union of points corresponding to the '(l,l)-isogenous surfaces'. As there are $[\mathcal{H}_2 : \Gamma_0^{(2)}(l)] = (l^4-1)/(l-1)$ isotropic subspaces of dimension 2 in $A[l]$ by [**57**, Lemma 6.1], there are exactly $(l^4-1)/(l-1)$ solutions to the system of equations given by V'. By construction, the triple

$$(j_1(A/J), j_2(A/J), j_3(A/J))$$

is one of the solutions. There are l^3+l^2+l other solutions, and we will see in Section 7.6 that for CM-computations it is relatively easy to determine which of the solutions come from the typenorm of an $\mathcal{O}_{K_\Phi}$-ideal.

Unfortunately, the ideal $V(l)$ can only be computed for very small l. Indeed, the only case that has been done is $l=2$ and it takes roughly 50 Megabytes to store the three generators of V. By [**57**], knowing the ideal V for some prime l implies that we have an equation for the *Humbert surface* of discriminant l^2. As we have seen, computing level 1 Humbert surfaces is a hard problem and we do not expect that much progress can be made in computing V for primes $l > 2$.

7.4. Smaller functions

The Igusa functions introduced in Section 7.2 are 'too large' to be practical in our computation of the CM-action: we cannot compute an ideal describing the variety $Y_0^2(l)$ for primes $l > 2$. In this section we introduce smaller functions $f_1,\ldots,f_4$ that are more convenient from a computational perspective.

For $x,y \in \{0,1\}^2$, define the functions $\theta_{x,y} : \mathcal{H}_2 \to \mathbb{C}$ by

$$\theta_{x,y}(\tau) = \sum_{n\in\mathbb{Z}^2} \exp \pi i \left({}^t(n+\tfrac{x}{2})\tau(n+\tfrac{x}{2}) + {}^t(n+\tfrac{x}{2})y \right). \tag{7.7}$$

The functions $\theta_{x,y}$ are known as the 'theta null values' and arise naturally from the construction of theta functions [**33**]. The equality

$$\theta_{x,y}(\tau) = (-1)^{{}^t xy}\theta_{x,y}(\tau)$$

shows that of the sixteen theta nullvalues only ten of them are non-zero.

The fourth powers of the functions $\theta_{x,y}$ are Siegel modular forms of weight 2 for the congruence subgroup $\Gamma(2) \subset \mathrm{Sp}_4(\mathbb{Z})$. The Satake compactification $X(2)$ of the quotient $\Gamma(2)\backslash\mathcal{H}_2$ has a natural structure of a projective variety, and the fourth powers $\theta_{x,y}^4$ define an embedding of $X(2)$ into projective space.

Theorem 7.8. *Let $M_2(\Gamma(2))$ denote the $\mathbb{C}$-vector space of all Siegel modular forms of weight 2 for the group $\Gamma(2)$. Then the following holds: the space $M_2(\Gamma(2))$ is 5-dimensional and is spanned by the ten modular forms $\theta_{x,y}^4$. Furthermore, the map $X(2) \to \mathbb{P}^9$ defined by the functions $\theta_{x,y}^4$ is an embedding. The image is the quartic threefold in $\mathbb{P}^4$ defined by*

$$u_2^2 - 4u_4 = 0$$

with $u_k = \sum_{x,y} \theta_{x,y}^{4k}$.

Proof. See [**72**, Theorem 5.2]. □

It is well known that we have an inclusion

$$\mathbb{C}(j_1, j_2, j_3) \subseteq \mathbb{C}(\theta_{x,y}^4/\theta_{x',y'}^4)$$

where we use the convention that we consider *all* quotients of theta fourth powers. Indeed, the formulas that many people use to evaluate Igusa functions [**35**, p. 848] readily express j_1, j_2, j_3 in terms of $\theta_{x,y}^4$. The functions $\theta_{x,y}^4/\theta_{x',y'}^4$ are rational Siegel modular *functions* of level 2. Whereas a value $(j_1(\tau), j_2(\tau), j_3(\tau))$ depends only on the $\mathrm{Sp}_4(\mathbb{Z})$-equivalence class of $\tau \in \mathcal{H}_2$, a value $(\theta_{x,y}^4/\theta_{x',y'}^4)_{x,x',y,y'}$ depends on the $\Gamma(2)$-equivalence class of τ. Since the affine points of $\Gamma(2)\backslash\mathcal{H}_2 \subset X(2)$ correspond to isomorphism classes of triples $(A, \langle P, Q\rangle)$ consisting of a principally polarized 2-dimensional abelian variety A together with a basis P, Q of the 2-torsion, the functions $\theta_{x,y}^4/\theta_{x',y'}^4$ not only depend on the abelian variety in question but also on an ordering of its 2-torsion. For every isomorphism class $\mathrm{Sp}_4(\mathbb{Z})\tau$ of abelian varieties, there are $[\mathrm{Sp}_4(\mathbb{Z}) : \Gamma(2)] = 720$ values for the tuple $(\theta_{x,y}^4(\tau)/\theta_{x',y'}^4(\tau))_{x,x',y,y'}$. The functions $\theta_{x,y}^4/\theta_{x',y'}^4$ are 'smaller' than the Igusa functions in the sense that their Fourier coefficients are smaller. A natural idea is to get even smaller functions by considering the quotients $\theta_{x,y}/\theta_{x',y'}$ themselves instead of their fourth powers.

We define the four functions $f_1, f_2, f_3, f_4 : \mathcal{H}_2 \to \mathbb{C}$ by

$$f_1 = \theta_{(0,0),(0,0)} \quad f_2 = \theta_{(0,0),(1,1)} \quad f_3 = \theta_{(0,0),(1,0)} \qquad f_4 = \theta_{(0,0),(0,1)}.$$

We stress that the particular choice of the 'theta constants' is rather arbitrary, our only requirement is that we define four different functions. The three quotients $f_1/f_4, f_2/f_4, f_3/f_4$ are rational Siegel modular functions.

Theorem 7.9. *We have an inclusion* $\mathbb{C}(j_1, j_2, j_3) \subseteq \mathbb{C}(f_1, f_2, f_3, f_4)$. *Furthermore, the quotients* $f_1/f_4, f_2/f_4, f_3/f_4$ *are invariant under the subgroup* $\Gamma(8)$.

Proof. Five linear relations between the $\theta_{x,y}^4$ can be found explicitly using Proposition 3.14. The vector space $M(\Gamma(2))$ can be spanned by the set $\{f_1^4, \dots f_4^4, g^4\}$ where $g = \theta_{(0,1),(0,0)}$. The degree four relation in Theorem 7.8, together with the five linear relations yield that g^4 satisfies a degree four polynomial P over $L = \mathbb{C}(f_1, f_2, f_3, f_4)$. The polynomial P factors over L as a product of the two irreducible quadratic polynomials

$$P_-, P_+ = T^2 - (f_1^4 - f_2^4 + f_3^4 - f_4^4)T + (f_1^2 f_3^2 \pm f_2^2 f_4^2)^2.$$

By looking at the Fourier expansions of $f_1, \dots, f_4$ and g, we see that g^4 only satisfies the polynomial P_-. Hence, the extension $L(g^4)/L$ is quadratic and generated by a root of P_-.

For each of the two choices of a root of P_-, the other five fourth powers of theta functions will be uniquely determined. Indeed, the fourth powers are functions on the space $M(\Gamma(2))$ and this space is 5-dimensional by Theorem 7.8. This means that we get a priori get *two* Igusa triples (j_1, j_2, j_3) for every tuple (f_1, f_2, f_3, f_4). However, a close inspection of the formulas expressing the Igusa functions in terms of theta fourth powers yields that these Igusa triples coincide. Hence, the triple (j_1, j_2, j_3) does not depend on a choice of P_-. This proves the first statement in the theorem.

The second statement follows immediately from a result of Igusa. In [**33**, p. 242], he proves that the field M generated by *all* theta quotients is left invariant by a subgroup of $\Gamma(8)$. As the field $\mathbb{C}(f_1/f_4, f_2/f_4, f_3/f_4)$ is a subfield of M, Theorem 7.9 follows. □

As the functions $f_1/f_4, f_2/f_4, f_3/f_4$ are invariant under $\Gamma(8)$, the moduli interpretation is that they depend on an abelian variety together with a level 8-structure. We let $\mathrm{Stab}(f)$ be the stabilizer of $f_1/f_4, f_2/f_4, f_3/f_4$ inside the symplectic group $\mathrm{Sp}_4(\mathbb{Z})$. We have inclusions

$$\Gamma(8) \subset \mathrm{Stab}(f) \subset \mathrm{Sp}_4(\mathbb{Z})$$

and the quotient $Y(f) = \text{Stab}(f)\backslash\mathcal{H}_2$ has a natural structure of a quasi-projective variety by the Baily-Borel theorem [**2**]. However, this variety is not smooth.

We let

$$\mathbb{H}_2^* = \{\tau \in \mathcal{H}_2 \mid \tau \text{ is not } \text{Sp}_4(\mathbb{Z})\text{-equivalent to a diagonal matrix}\}$$

be the subset of $\mathcal{H}_2$ of those τ's that do not correspond to a product of elliptic curves. The argument in [**63**, §5] shows that $G = \Gamma(8)/\text{Stab}(f)$ acts freely on $Y(8)$. By [**53**, §2.7], the quotient $Y(f)^* = \text{Stab}(f)\backslash\mathbb{H}_2^*$ is a *smooth* variety.

Lemma 7.10. *The map $Y(f)^* \to Y(1)$ induced by the inclusion $\text{Stab}(f) \to \text{Sp}_4(\mathbb{Z})$ has degree 46080.*

Proof. We know that $\text{Stab}(f)$ has index $4^3 = 64$ in $\Gamma(2)$. The group $\Gamma(2)$ in turn has index 720 in $\text{Sp}_4(\mathbb{Z})$ and the lemma follows. □

The proof of Theorem 7.9 readily gives a means of computing an Igusa triple $(j_1(\tau), j_2(\tau), j_3(\tau))$ from a tuple $(f_1(\tau), \ldots, f_4(\tau))$. Conversely, it is 'classical' to compute an element $(f_1(\tau), \ldots, f_4(\tau))$ given a (finite) Igusa triple. Our computation follows the formulas for theta functions from the 19th century. We first compute the corresponding Igusa Clebsch invariants I_2, I_4, I_6, I_{10}. After applying the transformation (c.f. Subsection 3.6.2)

$$\begin{aligned} s_2 &= 3I_4 \\ s_3 &= 3/2(I_2I_4 - 3I_6) \\ s_5 &= 5/12 s_2 s_3 + 3^5 \cdot 5 I_{10} \\ s_6 &= 27/16 I_4^3 + 1/6 s_3^2 + 3^6/2^2 I_2 I_{10}, \end{aligned}$$

we compute the roots $x_1, \ldots, x_6$ of the Satake sextic polynomial

$$X^6 - \frac{1}{2}s_2X^4 - \frac{1}{3}s_3X^3 + \frac{1}{16}s_2^2X^2 + (\frac{1}{6}s_2s_3 - \frac{1}{5}s_5)X + (\frac{1}{96}s_2^3 + \frac{1}{18}s_3^2 - \frac{1}{6}s_6)$$

with coefficients in $\mathbb{Q}(s_2, s_3, s_5, s_6)$. One choice for $f_1^4, f_2^4, f_3^4, f_4^4$ is given by (c.f. formulae for the t_5, t_6, t_8, t_9 in the proof of Theorem 3.15):

$$\begin{aligned} f_1^4 &= (-x_1 - x_2 - x_4)/3, \\ f_2^4 &= (-x_1 - x_3 - x_4)/3, \\ f_3^4 &= (-x_1 - x_2 - x_3)/3, \\ f_4^4 &= (-x_2 - x_3 - x_4)/3. \end{aligned}$$

Finally, we extract fourth roots to find values for $(f_1(\tau), \ldots, f_4(\tau))$. There are $720 \cdot 64 = 46080$ possible values for this tuple.

7.5. The CM-action and level structure

We let $\mathrm{Stab}(f)$ be the stabilizer of the three quotients $f_1/f_4, f_2/f_4, f_3/f_4$ defined in Section 7.3. By Theorem 7.9, we have $\Gamma(8) \subseteq \mathrm{Stab}(f)$. For a prime $l > 2$, we now define

$$Y(f;l)^* = (\mathrm{Stab}(f) \cap \Gamma_0^{(2)}(l))\backslash \mathbb{H}_2^*$$

which we view as an equality of Riemann surfaces. By the Baily-Borel theorem, the space $Y(f;l)^*$ has a natural structure of a variety. Since we restricted to $\mathbb{H}_2^*$, the variety is now affine. Just like in the case $l = 1$ from the previous section, $Y(f;l)^*$ is smooth.

The moduli interpretation of $Y(f;l)^*$ is the following. Points are isomorphism classes of triples (S, G, L), where S is a Jacobian of a genus 2 curve over the complex numbers, G is a 2-dimensional isotropic subspace of $S[l]$ and L is a level 8-structure. The notion of isomorphism is that (S, G, L) and (S', G', L') are isomorphic if and only if there is an isomorphism of principally polarized abelian surfaces

$$\varphi : S \to S'$$

that satisfies $\varphi(G) = G'$ and $\varphi(L) = L'$.

Lemma 7.11. *The map $Y(f;l)^* \to Y(f)^*$ induced by the inclusion map $(\mathrm{Stab}(f) \cap \Gamma_0^{(2)}(l)) \to \mathrm{Stab}(f)$ has degree $(l^4-1)/(l-1)$ for primes $l > 2$.*

Proof. This is clear: the choice of a level 8-structure L is independent of the choice of a subspace of the l-torsion for $l > 2$. □

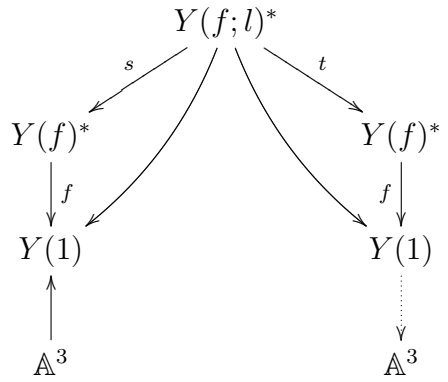
Besides the map $Y(f;l)^* \to Y(f)^*$ from the lemma, we also have a map $Y(f;l)^* \to Y(f)^*$ given by

$$(S, G, L) \mapsto (S/G, L').$$

Indeed, the isogeny $\varphi : S \to S/G$ induces an isomorphism

$$S[8] \to (S/G)[8]$$

and we have $L' = \varphi(L)$. It it not hard to see that this map also has degree $(l^4-1)/(l-1)$. Putting all the varieties together, the picture is as follows.



The map s sends $(S, G, L) \in Y(f;l)^*$ to $(S, L) \in Y(f)^*$ and t is the map induced by the isogeny $S \to S/G$. This diagram allows us to find all the abelian surfaces that are (l,l)-isogenous to a given surface A. Indeed, we first map the Igusa invariants $(j_1(A), j_2(A), j_3(A))$ to a point in $Y(1)$, say given by the Igusa-Clebsch invariants. We then *choose* (A, L) on $Y(f)^*$ lying over this point. Although there are 46080 choices for L, it does not matter which one we choose. Above (A, L), there are $(l^4-1)/(l-1)$ points in $Y(f;l)^*$ and via the map $t : Y(f;l)^* \to Y(f)^*$ we map all of those down to $Y(f)^*$. Forgetting the level 8-structure now yields $(l^4-1)/(l-1)$ points in $Y(1)$. If A is simple, i.e., not isogenous to a product of elliptic curves with the product polarization, we then can transform these into absolute Igusa invariants.

Assuming we can compute an ideal

$$V(f;l) \subset \mathbb{Q}[W_1, X_1, Y_1, Z_1, W_2, X_2, Y_2, Z_2]$$

defining the quasi-projective variety $Y(f;l)^*$, we derive the following algorithm to compute all (l,l)-isogenous abelian surfaces.

Algorithm 7.12. Let F be an algebraically closed field.
Input. A Jacobian A/F of a genus 2 curve given by its Igusa invariants, and the ideal $V(f;l)$ defining $Y(f;l)^*$.
Output. The Igusa invariants of all principally polarized abelian surfaces that are (l,l)-isogenous to A.

a) Compute Igusa-Clebsch invariants $(I_2, I_4, I_6, I_{10}) \in F^4$ corresponding to A.
b) Choose an element $(f_1, f_2, f_3, f_4) \in Y(f)^*$ that maps to the point (I_2, I_4, I_6, I_{10}) using the method described at the end of Section 7.4.
c) Specialize the ideal $V(f;l)$ in $(W_1, X_1, Y_1, Z_4) = (f_1, f_2, f_3, f_4)$ and solve the remaining system of equations.

d) For each solution found in the previous step, compute the corresponding point in $Y(1)$ using the method given in the proof of Theorem 7.9.

7.5.1. Computing $V(f;l)$. In this subsection, we give an algorithm to compute the ideal $V(f;l)$ needed in Algorithm 7.12. Our approach only terminates in a reasonable amount of time in the simplest case $l = 3$.

The Fourier expansion from Section 7.4 can be written in terms of the individual matrix entries, and with some minor modifications we can represent it as a power series with integer coefficients. Write $\tau = \left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{smallmatrix}\right) \in \mathcal{H}_2$, then

$$\theta_{(a,b),(c,d)}(\tau) \;=\; \sum_{(x_1,x_2)\in\mathbb{Z}^2} (-1)^{x_1c+x_2d} p^{(2x_1+a)^2} q^{(2x_1+a+2x_2+b)^2} r^{(2x_2+b)^2}$$

where $p = e^{2\pi i(\tau_1-\tau_2)/8}$, $q = e^{2\pi i\tau_2/8}$ and $r = e^{2\pi i(\tau_3-\tau_2)/8}$. We see that it is easy to compute Fourier expansions for the Siegel modular forms f_i.

One of the (l,l)-isogenous surfaces to $\mathbb{C}^2/(\mathbb{Z}^2 + \mathbb{Z}^2 \cdot \tau)$ is the surface $\mathbb{C}^2/(\mathbb{Z}^2 + \mathbb{Z}^2 \cdot l\tau)$, and we want to find a relation between the f_i's and the functions $f_i(l\tau)$. The expansion for $f_i(l\tau)$ can be constructed easily from the Fourier expansion of $f_i(\tau)$ by replacing p, q, r with p^l, q^l, r^l.

For increasing positive integers $d = 2, 3, \ldots$, we do the following. We compute all homogeneous monomials of degree d in $\{f_i(\tau), f_i(l\tau)\}$ represented as truncated power series and then use exact linear algebra to find linear dependencies between them. The basis of relations will 'stabilize' as the power series precision increases. There are two ways to check experimentally whether we have enough relations: $V(f;l)$ has the correct dimension and the projection maps have the correct degrees. Starting with $d = 2$, we search for homogeneous relations relations of degree d, then $d+1$ and so on, increasing the degree until we have enough relations.

Using this method we computed the ideal $V(f;3)$. The $(3,3)$-isogeny relations in $V(f;3)$ are given by 85 homogeneous polynomials of degree six. The whole ideal takes 35 kilobytes to store. The individual relations are fairly small, having at most 40 terms. Furthermore, the coefficients are 8-smooth and bounded by 200 in absolute value, which makes them amenable for computations.

We stress however that we *cannot* rigorously prove that the ideal $V(f;3)$ we found is correct. We only have 'emperical evidence' that it is correct.

The search for $l = 5$ is currently being undertaken using the above method. The degrees of the relations is at least 8; the number of homogeneous monomials is at the limits of computing resources using this method. This approach is rather simple-minded, and we expect that we need interpolation techniques to find the ideal $V(f;5)$.

Using a 3-dimensional subvariety of $\mathbb{P}^9$, Carls, Kohel and Lubicz [**10**] have found much smaller $(3,3)$-isogeny relations using theta constants with characteristics in $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$. To our knowledge, this is the only other $(3,3)$-isogeny relation ideal to have been computed up to now.

7.6. The CM-action over finite fields

The theory developed in Sections 7.3–7.6 uses the *complex analytic* definition of abelian surfaces and the Riemann surfaces $Y_0^{(2)}(l)$ and $Y(f;l)^*$. We now explain why we can use the results in *positive characteristic* as well. Firstly, if we take a prime p that splits completely in K, then by [**19**, Theorem 1] the reduction modulo p of an abelian surface $A/H(K_\Phi)$ with endomorphism ring $\mathcal{O}_K$ is *ordinary*. The reduced surface again has endomorphism ring $\mathcal{O}_K$.

Furthermore, one can naturally associate an algebraic stack $\mathfrak{A}_{\Gamma_0(p)}$ to $Y_0^{(2)}(l)$ and prove that the structural morphism $\mathfrak{A}_{\Gamma_0(p)} \to \mathrm{Spec}(\mathbb{Z})$ is smooth outside l, see [**11**, Corollary 6.1.1.]. In a more down-to-earth computational terminology, this means the moduli interpretation of the ideal $V \subset \mathbb{Q}[X_1, \ldots, Z_2]$ remains valid when we reduce the elements of V modulo a prime $p \neq l$.

The reduction of $Y(f;l)^*$ is slightly more complicated. The map $Y(8l) \to Y(f;l)^*$ is finite étale by [**38**, Theorem A.7.1.1.], where we now view the affine varieties $Y(f;l)^*$ and $Y(8l)$ as schemes. It is well known that the $Y(N)$ is smooth over $\mathrm{Spec}(\mathbb{Z}[1/N])$ for $N \geq 3$, so in particular, the scheme $Y(f;l)^*$ is smooth over $\mathrm{Spec}(\mathbb{Z}[1/(2l)])$. Again, this means that the moduli interpretation for the ideal $V(f;l) \subset \mathbb{Q}[W_1, \ldots, Z_2]$ remains valid when we reduce the elements of $V(f;l)$ modulo a prime $p \neq 2l$.

Lemma 7.13. *Let l be prime, and let $p \neq 2l$ be a prime that splits completely in a primitive CM-field K. Then, on input of the Igusa invariants of a principally polarized abelian surface $A/\overline{\mathbb{F}}_p$ with $\mathrm{End}(A) = \mathcal{O}_K$ and the ideal $V(f;l) \subset \overline{\mathbb{F}}_p[W_1, \ldots, Z_2]$, Algorithm 7.12 computes the Igusa invariants of all (l,l)-isogenous surfaces.*

Proof. Clear from the preceding discussion. □

Fix a primitive quartic CM-field K, and let $p \neq 2l$ be a prime that splits completely in the Hilbert class field of the reflex field K_Φ. In particular, p splits in K_Φ and as it splits in its normal closure L it will split completely in K as well. Hence, Lemma 7.13 applies. Because p splits completely in $H(K_\Phi)$, the Igusa invariants of an abelian surface $A/\overline{\mathbb{F}}_p$ with $\mathrm{End}(A) = \mathcal{O}_K$ are defined over the prime field $\mathbb{F}_p$.

If we apply Algorithm 7.12 to the point $(j_1(A), j_2(A), j_3(A))$ and the ideal $V(f; l)$, then we get $(l^4 - 1)/(l - 1)$ triples of Igusa invariants. All these triples are Igusa invariants of principally polarized abelian surfaces that have endomorphism *algebra* K. Some of these triples are defined over the prime field $\mathbb{F}_p$ and some are not. However, since p splits completely in the Hilbert class field of K_Φ, the Igusa invariants of the surfaces that have endomorphism ring $\mathcal{O}_K$ *are defined over the field* $\mathbb{F}_p$.

Algorithm 7.14.
Input. The Igusa invariants of a simple principally polarized abelian surface $A/\mathbb{F}_p$ with $\mathrm{End}(A) = \mathcal{O}_K$, and the ideal $V(f; l) \subset \mathbb{F}_p[W_1, \ldots, Z_2]$. Here, l is a prime such that there exists a prime ideal in K_Φ of norm l. Furthermore, we assume $p \neq 2l$.
Output. The Igusa invariants of all principally polarized abelian surfaces $A'/\mathbb{F}_p$ with $\mathrm{End}(A') = \mathcal{O}_K$ that are (l, l)-isogenous to A.

a) Apply Algorithm 7.12 to A and $V(f; l)$. Let S be the set of all Igusa invariants that are defined over $\mathbb{F}_p$.
b) For each $(j_1(A'), j_2(A'), j_3(A')) \in S$, construct a genus 2 curve C having these invariants using Mestre's algorithm ([**50**], [**9**]).
c) Apply the Freeman-Lauter algorithm [**16**] to test whether $\mathrm{Jac}(C)$ has endomorphism ring $\mathcal{O}_K$. Return the Igusa invariants of all the curves that pass this test.

We can predict beforehand *how many* triples will be returned by Algorithm 7.14. We compute the prime factorization

$$(l) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_k^{e_k}$$

of (l) in K_Φ. Say that we have $n \leq 4$ prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of norm l in this factorization, disregarding multiplicity. For each of these ideals $\mathfrak{p}_i$ we compute the typenorm map $m(\mathfrak{p}_i) \in \mathfrak{C}(K)$. The size of

$$\{m(\mathfrak{p}_1), \ldots, m(\mathfrak{p}_n)\} \subset \mathfrak{C}(K).$$

equals the number of triples computed by Algorithm 7.14.

7.6.1. Igusa class polynomials modulo p. The 'CRT-algorithm' to compute the Igusa class polynomials $P_K, Q_K, R_K \in \mathbb{Q}[X]$ of a primitive quartic CM-field K computes the reductions of these three polynomials modulo various primes p. For a given prime p that splits completely in the Hilbert class field of K_Φ, the method suggested in [**14**] is to loop over all p^3 possible Igusa invariants. For each of the invariants $(j_1(A'), j_2(A'), j_3(A'))$, we have to run an 'endomorphism ring test' to see if A' has endomorphism ring $\mathcal{O}_K$.

Algorithm 7.14 can be used to dramatically improve this algorithm of computing Igusa class polynomials modulo p. We compute the class group

$$\mathrm{Cl}(\mathcal{O}_{K_\Phi}) = \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_k \rangle$$

of the reflex field. Here, we take the generators $\mathfrak{p}_i$ to be of odd prime norm. For each of the norms $N_{K_\Phi/\mathbb{Q}}(\mathfrak{p}_i) = l_i$, we compute the ideal $V(f; l_i)$ describing the Siegel modular variety $Y(f; l_i)^*$.

Next, we try *random* triples of Igusa invariants over $\mathbb{F}_p$ until we find a triple $(j_1(A), j_2(A), j_3(A))$ corresponding to a surface A with $\mathrm{End}(A) = \mathcal{O}_K$. Analogous to [**3**], we now apply Algorithm 7.14 to this surface A for all primes l_i. To all new surfaces, we again apply Algorithm 7.14 for all primes l_i. We continue this until we find no new surfaces.

In contrast to the analogous genus 1 algorithm in [**3**], it is unlikely that we have found *all* surfaces with endomorphism ring $\mathcal{O}_K$. This is because Algorithm 7.14 finds surfaces having the *same* CM-type as the initial surface A, so in the dihedral case we are missing surfaces which use the second CM-type. Even in the cyclic case where there are $|\mathfrak{C}(K)|$ isomorphism classes, it is possible that the map

$$m : \mathrm{Cl}(\mathcal{O}_{K_\Phi}) \to \mathfrak{C}(K)$$

is not surjective, meaning that we cannot find all surfaces of a given CM-type. The solution is simple: we compute the cardinality of $S(K)$ using Theorem 7.2 and if the number of surfaces that we found is less than $|S(K)|$, we do a new random search and apply Algorithm 7.14 as before. Once we have found all surfaces with endomorphism ring $\mathcal{O}_K$, we simply expand

$$P_K = \prod_{\{A \ p.p.a.s. | \mathrm{End}(A) = \mathcal{O}_K\}/\cong} (X - j_1(A)) \in \mathbb{F}_p[X]$$

and likewise for Q_K and R_K. The difference with the method from [**14**] is that the search space is reduced from $O(p^3)$ to $O(p^3/|m(\mathrm{Cl}(\mathcal{O}_{K_\Phi}))|)$, an improvement by a factor of $|m(\mathrm{Cl}(\mathcal{O}_{K_\Phi}))|$.

The main bottleneck in our algorithm is that we have to compute the ideals $V(f; l)$ for various primes l. At the moment, we can only do this empirically in the simplest case $l = 3$. If we only use the primes ideal in $\mathcal{O}_{K_\Phi}$ of norm 3 then we typically get small factors of the Igusa class polynomials. We are forced to do more random searches to find the complete class polynomials.

7.7. Examples and applications

In this section we illustrate our algorithm by computing the Igusa class polynomials modulo primes p for various CM-fields. We point out the differences with the analogous genus 1 computations.

Example 7.15. In the first example we let $K = \mathbb{Q}[X]/(X^4+185X^2+8325)$ be a *cyclic* CM-field of degree 4. All CM-types are equivalent in this case, and the reflex field of K is K itself. The discriminant of K equals $5^2 \cdot 37^3$, and the real quadratic subfield of K is $K_0 = \mathbb{Q}(\sqrt{37})$. An easy computation shows that the narrow class group of K_0 is trivial. In particular, all ideal classes of K are principally polarizable, and we have

$$\mathfrak{C}(K) \cong \mathrm{Cl}(\mathcal{O}_K).$$

We compute $\mathrm{Cl}(\mathcal{O}_K) = \mathbb{Z}/10\mathbb{Z} = \langle \mathfrak{p}_3 \rangle$, where $\mathfrak{p}_3$ is a prime lying over 3. The prime ideal $\mathfrak{p}_3$ has norm 3, and its typenorm $N_\Phi(\mathfrak{p}_3)$ generates a subgroup of order 5 in $\mathrm{Cl}(\mathcal{O}_K)$.

The smallest prime that splits in the Hilbert class field of K is $p = 271$. We illustrate our algorithm by computing the Igusa class polynomials for K modulo this prime. First we do a 'random search' to find a principally polarized abelian surface over $\mathbb{F}_p$ with endomorphism ring $\mathcal{O}_K$ in the following way. We compute a generator π of the principal $\mathcal{O}_K$-ideal $\mathfrak{p}_3\overline{\mathfrak{p}}_3$. The element π has minimal polynomial

$$f = X^4 + 9X^3 + 331X^2 + 2439X + 73441 \in \mathbb{Z}[X].$$

If the Jacobian $\mathrm{Jac}(C)$ of a hyperelliptic curve C has endomorphism ring $\mathcal{O}_K$, then the Frobenius morphism of $\mathrm{Jac}(C)$ is a root of either $f(X)$ or $f(-X)$. With the factorization

$$f = (X-\tau_1)(X-\tau_2)(X-\tau_3)(X-\tau_4) \in K[X],$$

a *necessary* condition for $\mathrm{Jac}(C)$ to have endomorphism ring $\mathcal{O}_K$ is

$$\#C(\mathbb{F}_p) = p + 1 \pm (\tau_1+\tau_2+\tau_3+\tau_4) \in \{261, 283\}$$

and

$$\#\mathrm{Jac}(C)(\mathbb{F}_p) \in \{f(1), f(-1)\} = \{71325, 76221\}.$$

We try random values $(j_1, j_2, j_3) \in \mathbb{F}_p^3$ and write down a hyperelliptic curve C with those Igusa invariants using Mestre's algorithm ([**50**], [**9**]). If C satisfies the 2 conditions above, then we check whether $\mathrm{Jac}(C)$ has endomorphism ring $\mathcal{O}_K$ using the algorithm explained in [**16**]. If it passes this test, we are done. Otherwise, we select a new random value (j_1, j_2, j_3).

We find that $w_0 = (133, 141, 89)$ is a set of invariants for a surface $A/\mathbb{F}_p$ with endomorphism ring $\mathcal{O}_K$. We apply Algorithm 7.14 to w_0. The Igusa Clebsch invariants corresponding to w_0 are $[133, 54, 82, 56]$. With the notation from Section 7.4, we have $s_2 = 162, s_3 = 106, s_5 = 128, s_6 = 30$. The corresponding Satake sextic polynomial

$$g = X^6 + 190X^4 + 55X^3 + 82X^2 + 18X + 63 \in \mathbb{F}_p[X]$$

factors over $\mathbb{F}_{p^5}$ and we write $\mathbb{F}_{p^5} = \mathbb{F}_p(\alpha)$ where α satisfies $\alpha^5+2\alpha+265 = 0$. We express the six roots of g in terms of α and pick

$$\begin{aligned} f_1^4 &= 147\alpha^4 + 147\alpha^3 + 259\alpha^2 + 34\alpha + 110, \\ f_2^4 &= 176\alpha^4 + 211\alpha^3 + 14\alpha^2 + 134\alpha + 190, \\ f_3^4 &= 163\alpha^4 + 93\alpha^3 + 134\alpha^2 + 196\alpha + 115, \\ f_4^4 &= 226\alpha^4 + 261\alpha^3 + 99\alpha^2 + 9\alpha + 27 \end{aligned}$$

as values for the fourth powers of our Siegel modular functions. The fourth roots of $(f_1^4, f_2^4, f_3^4, f_4^4)$ are all defined over $\mathbb{F}_{p^{10}}$, but not every choice corresponds to the Igusa invariants of A however. We pick fourth roots (r_1, r_2, r_3, r_4) such that the polynomial P_- from Section 7.4 vanishes when evaluated at $(T, f_1, f_2, f_3, f_4) = (f_5^4, r_1, r_2, r_3, r_4)$. Here, f_5^4 is computed from the Igusa Clebsch invariants. For an arbitrary choice of fourth roots for r_1, r_2, r_3 there are two solutions $\pm r_4$ for $P_- = 0$ which we can easily identify. Take $\mathbb{F}_{p^{10}} = \mathbb{F}_p(\beta)$ where $\beta^{10} + \beta^6 + 133\beta^5 + 10\beta^4 + 256\beta^3 + 74\beta^2 + 126\beta + 6 = 0$. We find that the tuple (r_1, r_2, r_3, r_4) given by

$$\begin{aligned} r_1 &= 179\beta^9 + 69\beta^8 + 203\beta^7 + 150\beta^6 + 29\beta^5 + 258\beta^4 + 183\beta^3 + 240\beta^2 + 255\beta + 226, \\ r_2 &= 142\beta^9 + 105\beta^8 + 227\beta^7 + 244\beta^6 + 72\beta^5 + 155\beta^4 + 2\beta^3 + 129\beta^2 + 137\beta + 23, \\ r_3 &= 63\beta^9 + 112\beta^8 + 132\beta^7 + 244\beta^6 + 94\beta^5 + 40\beta^4 + 191\beta^3 + 263\beta^2 + 85\beta + 70, \\ r_4 &= 190\beta^9 + 41\beta^8 + 62\beta^7 + 170\beta^6 + 151\beta^5 + 240\beta^4 + 270\beta^3 + 56\beta^2 + 16\beta + 257 \end{aligned}$$

is a set of invariants for A together with some level 8-structure.

Next we specialize our ideal $V(f; 3)$ at $(W_1, X_1, Y_1, Z_1) = (r_1, r_2, r_3, r_4)$ and we solve the remaining system of 85 equations in four unknowns. Let (r_1', r_2', r_3', r_4') be the solution where

$$r_1' = 184\beta^9 + 48\beta^8 + 99\beta^7 + 83\beta^6 + 20\beta^5 + 232\beta^4 + 16\beta^3 + 223\beta^2 + 85\beta + 108.$$

The quadruple (r_1', r_2', r_3', r_4') are invariants of an abelian surface A' together with level 8-structure that is $(3, 3)$-isogenous to A. To map this quadruple to the Igusa invariants of A' we compute a root of the quadratic polynomial

$$P_-(T, r_1', r_2', r_3', r_4').$$

This root is a value for the theta fourth power f_5^4. Since we now know *all* theta fourth powers, we can apply the formulas relating theta functions and Igusa functions from Section 3.6 to find the Igusa triple $(238, 10, 158)$.

In total, we find 16 Igusa triples defined over $\mathbb{F}_p$. All these triples are Igusa invariants of surfaces that have endomorphism *algebra* K. To check which ones have endomorphism *ring* $\mathcal{O}_K$, we apply the algorithm from [**16**]. We find that only the four triples

$$(253, 138, 96),\ (257, 248, 58),\ (238, 10, 158),\ (140, 159, 219)$$

are invariants of surfaces with endomorphism ring $\mathcal{O}_K$. The fact that we find four new sets of invariants should come as no surprise. Indeed, there

are four ideals of norm 3 lying over 3 in $\mathcal{O}_K$ and each ideal gives us an isogenous variety.

As the typenorm map $m : \mathrm{Cl}(\mathcal{O}_K) \to \mathfrak{C}(K)$ is not surjective, we have to do a *second* random search to find a 'new' abelian surface with endomorphism ring $\mathcal{O}_K$. We apply our isogeny algorithm to $w_1 = (74, 125, 180)$ as before, and we again find four new sets of invariants:

$$(174, 240, 246), (193, 85, 15), (268, 256, 143), (75, 263, 182).$$

In the end we expand the Igusa polynomials

$$P_K = X^{10} + 92X^9 + 72X^8 + 217X^7 + 98X^6 + 195X^5 + 233X^4 + 140X^3 + 45X^2 + 123X + 171,$$
$$Q_K = X^{10} + 232X^9 + 195X^8 + 45X^7 + 7X^6 + 195X^5 + 173X^4 + 16X^3 + 33X^2 + 247X + 237,$$
$$R_K = X^{10} + 240X^9 + 57X^8 + 213X^7 + 145X^6 + 130X^5 + 243X^4 + 249X^3 + 181X^2 + 134X + 81$$

modulo $p = 271$.

Example 7.16. In the previous example, all the prime ideals of K lying over 3 gave rise to an isogenous abelian surface. This phenomenon does not always occur. Indeed, let K be a primitive quartic CM-field and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the prime ideals of norm 3. If we have a principally polarized abelian surface $A/\mathbb{F}_p$ with endomorphism ring $\mathcal{O}_K$, then the number of $(3, 3)$-isogenous abelian surfaces with the same endomorphism ring equals the cardinality of

$$\{m(\mathfrak{p}_1), \ldots, m(\mathfrak{p}_n)\}.$$

There are examples where this set has *less* than n elements.

Take the cyclic field $K = \mathbb{Q}[X]/(X^6 + 219X^2 + 10512)$. The class group of K is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The prime 3 ramifies in K, and we have $(3) = \mathfrak{p}_1^2\mathfrak{p}_2^2$. The primes $\mathfrak{p}_1, \mathfrak{p}_2$ in fact generate $\mathrm{Cl}(\mathcal{O}_K)$. It is easy to see that for this field we have

$$m(\mathfrak{p}_1) = m(\mathfrak{p}_2) \in \mathfrak{C}(K),$$

so we only find *one* isogenous surface.

Example 7.17. Our algorithm is not restricted to cyclic CM-fields. In this example we let $K = \mathbb{Q}[X]/(X^4 + 22X^2 + 73)$ be a CM-field with Galois group D_4. There are two equivalence classes of CM-types. We fix a CM-type $\Phi : K \to \mathbb{C}^2$ and let K_Φ be the reflex field for Φ. We have $K_\Phi = \mathbb{Q}[X]/(X^4 + 11X^2 + 12)$, and K and K_Φ have the same Galois closure L.

As the real quadratic subfield $K_0 = \mathbb{Q}(\sqrt{3})$ has narrow class group $\mathbb{Z}/2\mathbb{Z}$, the group $\mathfrak{C}(K)$ fits in an exact sequence

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathfrak{C}(K) \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

and a close inspection yields $\mathfrak{C}(K) \cong \mathbb{Z}/4\mathbb{Z}$. The prime 3 factors as

$$(3) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$$

in the reflex field, and we have $\mathrm{Cl}(\mathcal{O}_{K_\Phi}) = \mathbb{Z}/4\mathbb{Z} = \langle[\mathfrak{p}_1]\rangle$. The element $m(\mathfrak{p}_1) \in \mathfrak{C}(K)$ has order 4, and under the map $f : \mathfrak{C}(K) \to \mathrm{Cl}(\mathcal{O}_K) = \mathbb{Z}/4\mathbb{Z}$ the element $f(m(\mathfrak{p}_1))$ has order 2. We see that even though the ideal $N_{L/K}(\mathfrak{p}_1\mathcal{O}_L)$ has order 2 in the class group, the typenorm of $\mathfrak{p}_1$ has order 4.

Of the four ideal classes of K, only two ideal classes are principally polarizable for Φ. The other two ideal classes are principally polarizable for 'the other' CM-type. Furthermore, the two principally polarizable ideal classes each have *two* principal polarizations.

The prime $p = 1609$ splits completely in the Hilbert class field of K_Φ. As in Example 7.15, we do a random search to find that a surface $A/\mathbb{F}_p$ with Igusa invariants $w_0 = (1563, 789, 704) \in \mathbb{F}_p^3$ has endomorphism ring $\mathcal{O}_K$. We apply Algorithm 7.14 to this point. As output, we get w_0 again and two new points $w_1 = (1396, 1200, 1520)$ and $w_2 = (1350, 1316, 1483)$. The fact that we find w_0 again should come as no surprise since $m(\mathfrak{p}_3) \in \mathfrak{C}(K)$ is the trivial element. The points w_1 and w_2 correspond to $\mathfrak{p}_1$ and $\mathfrak{p}_2$.

As expected we compute that the cycle

$$w_0 = (1563, 789, 704) \xrightarrow{\mathfrak{p}_1} (1396, 1200, 1520) \xrightarrow{\mathfrak{p}_1} (1276, 1484, 7)$$
$$\xrightarrow{\mathfrak{p}_1} (1350, 1316, 1483) \xrightarrow{\mathfrak{p}_1} w_0$$

has length 4. To find the full Igusa class polynomial modulo p, we have to do a second random search. The remaining 4 points are $(782, 1220, 257)$, $(1101, 490, 1321)$, $(577, 35, 471)$, $(1154, 723, 1456)$.

7.8. Obstruction to isogeny volcanos

For an ordinary elliptic curve $E/\mathbb{F}_p$ over a finite field, it is nowadays relatively straightforward to compute the endomorphism ring $\mathrm{End}(E)$ (e.g. [**44**]). One first computes the endormorphism *algebra* K by computing the trace of the Frobenius morphism Frob of E. If the index $[\mathcal{O}_K : \mathbb{Z}[\mathrm{Frob}]]$ is only divisible by 'small primes' l, then we can use the l-isogeny graph to determine the endomorphism ring. We refer to [**44**] for the details of this algorithm. The algorithm depends on the fact that the graph of l-isogenies looks like an 'volcano'. More precisely, we have the following result.

Lemma 7.18. *Let $E, E'/\mathbb{F}_p$ be two ordinary elliptic curves whose endomorphism rings are isomorphic to the same order $\mathcal{O}$ in an imaginary quadratic field K. Suppose that $l \neq p$ is a prime such that the index $[\mathcal{O}_K : \mathcal{O}]$ is divisible by l. Then there are no isogenies of degree l between E and E'.*

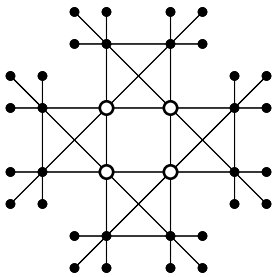
Proof. This result is well known, but we give the proof for convenience. Suppose that there does exist an isogeny $\varphi : E \to E'$ of degree l. By the Deuring lifting theorem [**48**, Theorem 13.14], we can lift φ to an isogeny $\widetilde{\varphi} : \widetilde{E} \to \widetilde{E}'$ defined over the ring class field for $\mathcal{O}$. By CM-theory, we can

write $E' = \mathbb{C}/I$ with I an *invertible* $\mathcal{O}$-ideal of norm l. But since l divides the index $[\mathcal{O}_K : \mathcal{O}]$, there are no invertible ideals of norm l. □

A natural question is whether we can compute the endomorphism ring of an ordinary principally polarized abelian surface $A/\mathbb{F}_p$ in a similar vein using (l, l)-isogenies. The extension of Schoof's algorithm [**56**] enables us to compute the endomorphism algebra of A. However, the analogue of Lemma 7.18 concerning (l, l)-isogenies between abelian surfaces does *not* hold in general. This is a theoretical obstruction to the heart of the 'straightforward generalization' of the algorithm for elliptic curves.

We first give an example where Lemma 7.18 fails for abelian surfaces.

Example 7.19. Take the point $(782, 1220, 257) \in \mathbb{F}_{1609}$ which we found in Example 7.17. Below we depict the connected component of the $(3, 3)$-isogeny graph (the second connected component is the the graph on the front cover). The white dots represent surfaces with endomorphism ring $\mathcal{O}_K$, the black dots are surfaces whose endomorphism ring has index l in $\mathcal{O}_K$. We observe that are are cycles in this graph other than at the 'surface' of the volcano.



The reason that these cycles can occur is the following. Just like in Lemma 7.18, we can lift an isogeny $\varphi : A \to A'$ to characteristic zero. By CM-theory, we can now write $A' = \mathbb{C}^2/\Phi(I)$ for some invertible $\mathcal{O}$-ideal of norm l. Here, Φ is a CM-type for K. Unlike the case of imaginary quadratic K, it can now happen that $\mathcal{O}$ does have invertible ideals of norm l. Indeed, if $K/\mathbb{Q}$ is not Galois then there can be both an invertible and a non-invertible $\mathcal{O}$-ideal of norm l. This is exactly what happens in the example above.

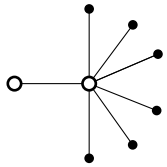
We observe that the analogue of Lemma 7.18 is true if the field K is Galois. The reason is that because $[\mathcal{O}_K : \mathcal{O}]$ is divisible by l there has to be at least one non-invertible ideal I lying over $l \in \mathbb{Z}$. All other ideals lying over l are Galois conjugate to I, so they are also non-invertible.

Another ingredient of the endomorphism ring algorithm for elliptic curves *can* fail if the endomorphism algebra is Galois however. In the elliptic curve case, it is essential that the l-isogeny graph is *regular*. More precisely, suppose that $E/\mathbb{F}_p$ has endomorphism ring $\mathcal{O}$ and let $\varphi : E \to E'$

be an isogeny from E to an elliptic curve E' with endomorphism ring of index l in $\mathrm{End}(E)$. If φ is defined over $\mathbb{F}_p$, then *all* $l+1$ isogenies of degree l are defined over $\mathbb{F}_p$. Otherwise we are at the 'base' of the volcano and there is a single l-isogeny mapping to an elliptic curve E'' with $[\mathrm{End}(E'') : \mathrm{End}(E)] = l$. If we exclude the 'base' vertices, the graph is $(l+1)$-regular.

The analogous statement is not true in dimension 2 as the following example shows.

Example 7.20. Consider the cyclic quartic CM field $K = \mathbb{Q}[X]/(X^4 + 12X^2 + 18)$ which has class number 2. The Igusa class polynomials have degree 2 and over $\mathbb{F}_{127}$ we find the corresponding moduli points $w_0 = (118, 71, 63)$, $w_1 = (98, 82, 56)$. The isogeny graph is not regular:



The white dots represent the points having maximal endomorphism ring. There are 7 points isogenous to w_1, which includes w_0. It is impossible to identify w_0 from the graph structure alone.

The reason that the regularity property fails in dimension 2 is the following. Let $K/\mathbb{Q}$ be a cyclic CM-field, and let $A/\mathbb{F}_p$ be an abelian surface with endomorphism ring $\mathcal{O}_K$. Let $\varphi : A \to A'$ be a degree l-isogeny. If the endomorphism ring $\mathcal{O}$ of A' is not isomorphic to $\mathcal{O}_K$ then, just like in the elliptic curve case, it will have index l in $\mathcal{O}_K$. If p splits into principal primes in $\mathcal{O}$, then A' will again be defined over $\mathbb{F}_p$.

However, there are *several* orders of index l in the maximal order $\mathcal{O}_K$. It can happen that p splits into principal primes in some of them, and not in others. In other words, the fact that A' is defined over $\mathbb{F}_p$ does not mean that all l-isogenous surface are defined over $\mathbb{F}_p$. This is exactly what happens in Example 7.19.

7.9. An improvement to the CM method

To conclude this thesis, we make note of two significant improvements to the explicit CM method to compute Igusa class polynomials mod p which utilize Humbert surfaces. The simple fact that a quartic CM field K contains a real quadratic subfield K^+ yields the following result.

Theorem 7.21. *Let A be a principally polarized abelian surface having CM by $\mathcal{O}_K$ and let Δ be the discriminant of K^+. Then the isomorphism class represented by A is a point on the Humbert surface of discriminant Δ.*

Proof. By Corollary 2.10(b), we know that H_Δ is the set of isomorphism classes of principally polarized abelian surfaces having endomorphism ring containing $\mathcal{O}_\Delta$, a quadratic order of discriminant Δ. If A has endomorphism ring isomorphic to $\mathcal{O}_K$ then it certainly contains $\mathcal{O}_K \cap K^+ = \mathcal{O}_{K^+}$ which completes the proof. □

Corollary 7.22. *Let (j_1, j_2, j_3) be Igusa invariants for a principally polarized abelian surface with CM by the maximal order $\mathcal{O}_K$. Then we have $H_\Delta(j_1, j_2, j_3) = 0$ where $\Delta = \mathrm{disc}(K^+)$.*

As a consequence, the random search space for computing Igusa class polynomials mod p is reduced from p^3 triples to the $|H_\Delta(\mathbb{F}_p)| = O(p^2)$ points on the Humbert surface mod p.

The second improvement to the algorithm is that the endomorphism check, which is a calculation requiring the computation of torsion subgroups over extension fields [**14**], in some cases can be improved if the point lies on a the Humbert surface.

Without going into the technical details, we sketch the basic steps of the endomorphism check. We know that $\mathrm{End}(A)$ contains $\mathcal{O} = \mathbb{Z}[\pi, \overline{\pi}]$. We find a set of representatives $\{\alpha_i\}$ for the quotient $\mathcal{O}_K/\mathcal{O}$, that is, a set which generates $\mathcal{O}_K$ over $\mathcal{O}$. There is an integer $n > 1$ such that $\beta_i = n\alpha_i \in \mathcal{O}$. For ease of argument we shall assume that p does not divide $[\mathcal{O}_K : \mathcal{O}]$. Since n is coprime to p, it follows from [**14**, Corollary 9] that α_i is in $\mathrm{End}(A)$ if and only if β_i acts as zero on the n-torsion $A[n]$. To do this check, decompose $A[n] = \oplus A[l_j^{e_j}]$ where $n = \prod l_j^{e_j}$, and for each j, evaluate β_i at at a spanning set of $A[l_j^{e_j}](\mathbb{F}_{p^k})$ where k is the splitting field degree.

Computing large torsion groups over extension fields is expensive and examples with large index are difficult to work with. If we know a larger order $\mathcal{O}'$ contained in $\mathrm{End}(A)$ to begin with, the index in $\mathrm{End}(A)$ will be smaller. In the case when A lies on the Humbert surface of discriminant $\Delta = \mathrm{disc}(K^+)$ we have the following.

Theorem 7.23. *Suppose A has endomorphism algebra isomorphic to a CM field K. If the isomorphism class represented by A is a point on $H_{\mathrm{disc}(K^+)}$, then $\mathrm{End}(A)$ contains $\mathcal{O}_{K^+}[\pi, \overline{\pi}]$.*

Proof. This is a straightforward application of the definition of a Humbert surface. □

If $\mathrm{End}(A) \supset \mathcal{O}_{K^+}[\pi, \overline{\pi}] \supsetneq \mathbb{Z}[\pi, \overline{\pi}]$ then we work with the smaller index $[\mathrm{End}(A) : \mathcal{O}_{K^+}[\pi, \overline{\pi}]]$, thus speeding up the endomorphism check.

The Humbert surfaces computed in this thesis have been used by David Kohel to extend the list of computed Igusa class polynomials in his database [**43**].

We hope the reader leaves with an appreciation of Humbert surfaces and the advantages of having explicit models for them.

References

[1] Montserrat Alsina and Pilar Bayer. *Quaternion orders, quadratic forms, and Shimura curves*, volume 22 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2004.

[2] W. L. Baily, Jr. and A. Borel. Compactification of arithmetic quotients of bounded symmetric domains. *Ann. of Math. (2)*, 84:442–528, 1966.

[3] J. Belding, R. Bröker, A. Enge, and K. Lauter. Computing hilbert class polynomials. In A. van der Poorten and A. Stein, editors, *Algorithmic Number Theory: 8th International Symposium, ANTS-VIII Banff, Canada, May 17-22, 2008 Proceedings*, volume 5011 of *Lecture Notes in Computer Science*, pages 282–295. Springer-Verlag, 2008.

[4] Peter Bending. *Curves of genus* 2 *with* $\sqrt{2}$ *multiplication*. PhD thesis, University of Oxford, 1998.

[5] Amnon Besser. On the equations defining families of Kummer surfaces of quaternionic multiplication type. Preprint.

[6] Amnon Besser. Elliptic fibrations of $K3$ surfaces and QM Kummer surfaces. *Math. Z.*, 228(2):283–308, 1998.

[7] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[8] Christina Birkenhake and Hannes Wilhelm. Humbert surfaces and the Kummer plane. *Trans. Amer. Math. Soc.*, 355(5):1819–1841 (electronic), 2003.

[9] Gabriel Cardona and Jordi Quer. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 71–83. World Sci. Publ., Hackensack, NJ, 2005.

[10] Robert Carls, David Kohel, and David Lubicz. Higher-dimensional 3-adic CM construction. *J. Algebra*, 319(3):971–1006, 2008.

[11] Ching-Li Chai and Peter Norman. Bad reduction of the Siegel moduli scheme of genus two with $\Gamma_0(p)$-level structure. *Amer. J. Math.*, 112(6):1003–1071, 1990.

[12] Henri Cohen. Sums involving the values at negative integers of L-functions of quadratic characters. *Math. Ann.*, 217(3):271–285, 1975.

[13] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[14] K. Eisenträger and K. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. To appear in Proceedings of 'Arithmetic, Geometry, and Coding Theory', (AGCT-10), Marseille (2005).

[15] Hans-Georg Franke. *Kurven in Hilbertschen Modulflächen und Humbertschen Flächen im Siegel-Raum*. Bonner Mathematische Schriften [Bonn Mathematical Publications], 104. Universität Bonn Mathematisches Institut, Bonn, 1977. Dissertation, Rheinische Friedrich-Wilhelms-Universität, Bonn, 1977.

[16] D. Freeman and K. Lauter. Computing endomorphism rings of jacobians of genus 2 curves over finite fields. In *Symposium on algebraic geometry and its applications*, pages 29–66. World Scientific, 2008.

[17] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The 2-adic CM method for genus 2 curves with application to cryptography. In *Asiacrypt 2006 (Shanghai)*, volume 4284 of *Lecture Notes in Computer Science*, pages 114Ű–129. Springer-Verlag, 2006.

[18] Josep González, Jordi Guàrdia, and Victor Rotger. Abelian surfaces of GL_2-type as Jacobians of curves. *Acta Arith.*, 116(3):263–287, 2005.

[19] Eyal Z. Goren. On certain reduction problems concerning abelian surfaces. *Manuscripta Math.*, 94(1):33–43, 1997.

[20] Erhard Gottschling. Über die Fixpunkte der Siegelschen Modulgruppe. *Math. Ann.*, 143:111–149, 1961.

[21] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry*. Wiley-Interscience [John Wiley & Sons], New York, 1978. Pure and Applied Mathematics.

[22] David Gruenewald. Humbert surface data. http://echidna.maths.usyd.edu.au/∼davidg/thesis.html.

[23] Jordi Guàrdia. Jacobian Nullwerte, periods and symmetric equations for hyperelliptic curves. *Ann. Inst. Fourier (Grenoble)*, 57(4):1253–1283, 2007.

[24] Ki-ichiro Hashimoto. Explicit form of quaternion modular embeddings. *Osaka J. Math.*, 32(3):533–546, 1995.

[25] Ki-ichiro Hashimoto and Naoki Murabayashi. Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two. *Tohoku Math. J. (2)*, 47(2):271–296, 1995.

[26] Erich Hecke. *Mathematische Werke*. Herausgegeben im Auftrage der Akademie der Wissenschaften zu Göttingen. Vandenhoeck &

Ruprecht, Göttingen, 1959.

[27] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[28] Friedrich Hirzebruch and Gerard van der Geer. *Lectures on Hilbert modular surfaces*, volume 77 of *Séminaire de Mathématiques Supérieures [Seminar on Higher Mathematics]*. Presses de l'Université de Montréal, Montreal, Que., 1981. Based on notes taken by W. Hausmann and F. J. Koll.

[29] Georges Humbert. Sur les fonctions abéliennes singulières. *Œuvres*, II:297–401, 1936.

[30] Jun-ichi Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72:612–649, 1960.

[31] Jun-ichi Igusa. On Siegel modular forms of genus two. *Amer. J. Math.*, 84:175–200, 1962.

[32] Jun-ichi Igusa. On Siegel modular forms of genus two. II. *Amer. J. Math.*, 86:392–412, 1964.

[33] Jun-ichi Igusa. On the graded ring of theta-constants. *Amer. J. Math.*, 86:219–246, 1964.

[34] Jun-ichi Igusa. On the graded ring of theta-constants. II. *Amer. J. Math.*, 88:221–236, 1966.

[35] Jun-ichi Igusa. Modular forms and projective invariants. *Amer. J. Math.*, 89:817–855, 1967.

[36] Jun-ichi Igusa. *Theta functions*. Springer-Verlag, New York, 1972. Die Grundlehren der mathematischen Wissenschaften, Band 194.

[37] Bruce W. Jordan. *On the Diophantine Arithmetic of Shimura Curves*. PhD thesis, Harvard University, 1981.

[38] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[39] Chandrashekhar Khare. Serre's modularity conjecture: the level one case. *Duke Math. J.*, 134(3):557–589, 2006.

[40] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture: (i) and (ii). Preprints available at http://www.math.utah.edu/∼shekhar/papers.html.

[41] Helmut Klingen. *Introductory lectures on Siegel modular forms*, volume 20 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1990.

[42] Neal Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989.

[43] David Kohel. Echidna database - complex multiplication class invariants in genus 2.

http://echidna.maths.usyd.edu.au/∼kohel/dbs/complex_multiplication2.html.

[44] David R. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkeley, 1996.

[45] Serge Lang. *Introduction to algebraic and abelian functions*, volume 89 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1982.

[46] Serge Lang. *Complex multiplication*, volume 255 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983.

[47] Serge Lang. *Complex multiplication*, volume 255 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983.

[48] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[49] Q. Liu. `genus2reduction`, 1994. Available at http://www.math.u-bordeaux1.fr/∼liu/G2R/.

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

[51] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[52] Michael Monagan. Maximal quotient rational reconstruction: an almost optimal algorithm for rational reconstruction. In *ISSAC 2004*, pages 243–249. ACM, New York, 2004.

[53] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[54] David Mumford. *Tata lectures on theta. II*, volume 43 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[55] A. P. Ogg. Real points on Shimura curves. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 277–307. Birkhäuser Boston, Boston, MA, 1983.

[56] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, 55(192):745–763, 1990.

[57] K. Lauter R. Bröker. Modular polynomials for genus 2. Submitted to London Math Society Journal of Mathematics and Computation, 2005.

[58] I. Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University

Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[59] Michael Rosen. Abelian varieties over $\mathbf{C}$. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 79–101. Springer, New York, 1986.

[60] Victor Rotger. *Abelian Varieties with Quaternionic Multiplication and their Moduli*. PhD thesis, Universitat de Barcelona, 2002.

[61] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[62] Joseph J. Rotman. *Advanced modern algebra*. Prentice Hall Inc., Upper Saddle River, NJ, 2002.

[63] Bernhard Runge. On Siegel modular forms. I. *J. Reine Angew. Math.*, 436:57–85, 1993.

[64] Bernhard Runge. Endomorphism rings of abelian surfaces and projective models of their moduli spaces. *Tohoku Math. J. (2)*, 51(3):283–303, 1999.

[65] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[66] Goro Shimura. On analytic families of polarized abelian varieties and automorphic functions. *Ann. of Math. (2)*, 78:149–192, 1963.

[67] Goro Shimura. Construction of class fields and zeta functions of algebraic curves. *Ann. of Math. (2)*, 85:58–159, 1967.

[68] Goro Shimura. On the zeta-function of an abelian variety with complex multiplication. *Ann. of Math. (2)*, 94:504–533, 1971.

[69] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[70] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998.

[71] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[72] G. van der Geer. On the geometry of a Siegel modular threefold. *Math. Ann.*, 260(3):317–350, 1982.

[73] Gerard van der Geer. *Hilbert modular surfaces*, volume 16 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988.

[74] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[75] P. S. Wang, M. J. T. Guy, and J. H. Davenport. p-adic reconstruction of rational numbers. In *SIGSAM Bulletin*, volume 16, pages 2–3. ACM, 1982.

[76] Annegret Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, 72(241):435–458 (electronic), 2003.

[77] John Wilson. *Curves of genus* 2 *with real multiplication by a square root of* 5. PhD thesis, University of Oxford, 1998.