

ISOGENIES, KUMMER SURFACES, THETA FUNCTIONS

ADRIAN CLINGHER, ANDREAS MALMENDIER, AND TONY SHASKA

ABSTRACT. This paper explores the geometry and computation of (ℓ, ℓ) -isogenies between abelian surfaces, focusing on Jacobians of genus 2 curves and their Kummer surfaces. We establish a comprehensive framework integrating abelian varieties, theta functions, and Kummer surface embeddings, leveraging the Torelli theorem to connect genus 2 curves with their principally polarized Jacobians. Theta functions of level 2 embed Kummer surfaces into \mathbb{P}^3 , enabling both theoretical analysis and practical computations. We generalize Richelot's $(2,2)$ -isogenies to arbitrary odd ℓ , developing efficient algorithms for computing these isogenies.

CONTENTS

1. Introduction	2
2. Abelian varieties	3
3. Theta Functions	5
4. Jacobian Varieties	7
4.1. Jacobian surfaces	7
5. Endomorphism Ring of Abelian Varieties	7
6. Genus 2 Curves, their Jacobians, and associated Kummer surfaces	10
6.1. Principal Polarizations and Torelli Theorem	11
6.2. Göpel groups and Theta divisors	13
6.3. Richelot Isogenies	14
7. Kummer Surfaces	17
7.1. Kummer surfaces associated with principal polarization	17
7.2. Kummer Surface and Shioda-Inose Surface	24
8. (n, n) -Split Jacobians	24
8.1. The case of $(2, 2)$ -Split Jacobians	27
8.2. Loci of (ℓ, ℓ) -Split Jacobians	31
9. Computing higher (ℓ, ℓ) -Isogenies	31
9.1. The ℓ -tuple embedding	32
9.2. Computing (n, n) -Isogenies via Kummer Surface	33
9.3. The Lubicz-Robert Formula for Computing (ℓ, ℓ) -Isogenies on Kummer Surfaces	34
10. Cryptanalytic Implications of (ℓ, ℓ) -Split Jacobians	35
10.1. The Costello et al. Attack	36
10.2. Impact on Genus 2 Cryptography	36
10.3. Requirements for a Full Break	36
10.4. Connection to This Work	37
11. Conclusion and Future Work	37
References	38

1. INTRODUCTION

Abelian varieties, as projective algebraic groups, generalize elliptic curves to higher dimensions and play a central role in algebraic geometry and number theory. This paper focuses on abelian surfaces—two-dimensional abelian varieties—with particular emphasis on Jacobians of genus 2 curves, which exhibit intricate geometric and arithmetic properties that enrich pure mathematical theory and hold promise for applied contexts, notably cryptography.

The advent of isogeny-based cryptography has spotlighted abelian varieties, where isogenies—surjective homomorphisms with finite kernels—underpin the security of protocols like the Supersingular Isogeny Diffie-Hellman (SIDH) by leveraging the computational hardness of isogeny problems on supersingular elliptic curves. Extending this paradigm to abelian surfaces enhances security through larger ℓ^4 -torsion groups and richer endomorphism algebras, potentially improving efficiency over elliptic curve systems. However, computing (ℓ, ℓ) -isogenies, especially for $\ell > 2$, poses significant challenges due to increased kernel complexity, necessitating techniques beyond classical Richelot isogenies and prompting scrutiny of their cryptographic vulnerabilities.

Theta functions are essential in this endeavor, serving as analytic tools defined on an abelian variety’s universal cover with quasi-periodic properties tied to its lattice structure. They provide explicit coordinates for embedding abelian varieties into projective spaces, facilitating both theoretical insights and practical computations. For abelian surfaces, level 2 theta functions embed the Kummer surface—the quotient by its inversion involution—into \mathbb{P}^3 , encoding moduli via theta constants, or thetanulls, crucial for our geometric and computational framework.

Genus 2 curves, smooth projective curves of genus 2, yield principally polarized abelian surfaces as their Jacobians, linked by the Torelli theorem, which identifies a curve with its Jacobian’s theta divisor up to isomorphism. Their Kummer surfaces, featuring the (16,6)-configuration of nodes and tropes, provide a computational platform. We explore (ℓ, ℓ) -isogenies, with kernels as maximal isotropic subgroups of ℓ -torsion points, generalizing Richelot’s (2,2)-isogenies to odd primes ℓ . Efficient computation of these isogenies is vital for genus 2 cryptographic applications, yet their security hinges on understanding split Jacobians—those isogenous to elliptic curve products—and their loci \mathcal{L}_ℓ .

This paper integrates the theoretical foundations of abelian varieties, theta functions, and Kummer surfaces with advanced computational and cryptanalytic insights for (ℓ, ℓ) -isogenies. Sections 2–6 establish the background, detailing abelian surfaces, endomorphism rings, theta properties, and genus 2 geometry, including \mathcal{L}_ℓ for $\ell = 2, 3, 5, 7, 11$. Sections 7–8 develop computational methods, from Richelot constructions to the Lubicz-Robert formula, achieving $O(\ell^2)$ complexity for odd ℓ . Section 9 examines cryptanalytic implications, highlighting attacks exploiting \mathcal{L}_ℓ that accelerate isogeny problem-solving (e.g., $100\times$ faster for 1000-bit primes), assessing their impact on protocols like the Castryck-Decru-Smith hash, and outlining requirements for a full break. We conclude in Section 10 with reflections on these contributions, bridging geometry, computation, and cryptography to advance genus 2 Jacobians in next-generation protocols.

2. ABELIAN VARIETIES

We assume some familiarity with algebraic curves and abelian varieties. For some of the basic definitions, we refer to [1] among other places.

Let \mathcal{A}, \mathcal{B} be abelian varieties over a field k . We denote the \mathbb{Z} -module of homomorphisms $\mathcal{A} \mapsto \mathcal{B}$ by $\text{Hom}(\mathcal{A}, \mathcal{B})$ and the ring of endomorphisms $\mathcal{A} \mapsto \mathcal{A}$ by $\text{End } \mathcal{A}$. In the context of linear algebra, it is often more convenient to work with the \mathbb{Q} -vector spaces $\text{Hom}^0(\mathcal{A}, \mathcal{B}) := \text{Hom}(\mathcal{A}, \mathcal{B}) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\text{End}^0 \mathcal{A} := \text{End } \mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Q}$. For an abelian variety \mathcal{A} defined over a number field K , computing $\text{End}_K(\mathcal{A})$ is a harder problem than computing $\text{End}_{\bar{K}}(\mathcal{A})$; see [2, lemma 5.1] for details.

Lemma 1. *If there exists an algorithm to compute $\text{End}_K(\mathcal{A})$ for any abelian variety of dimension $g \geq 1$ defined over a number field K , then there is an algorithm to compute $\text{End}_{\bar{K}}(\mathcal{A})$.*

Proof. Since $K \subseteq \bar{K}$, any endomorphism of \mathcal{A} over \bar{K} restricts to an endomorphism over K after base change, but the converse requires additional structure. An algorithm for $\text{End}_K(\mathcal{A})$ determines the \mathbb{Z} -module of K -rational endomorphisms. Extending scalars to \bar{K} , we compute $\text{End}_{\bar{K}}(\mathcal{A}) = \text{End}_K(\mathcal{A}) \otimes_{\mathbb{Z}} \bar{K}$, leveraging the finite generation of $\text{End}_K(\mathcal{A})$ and the algebraic closure of \bar{K} . The lemma follows from the existence of such an extension procedure. \square

A homomorphism $f : \mathcal{A} \rightarrow \mathcal{B}$ is called an **isogeny** if $\text{Im } f = \mathcal{B}$ and $\ker f$ is a finite group scheme. If an isogeny $\mathcal{A} \rightarrow \mathcal{B}$ exists, we say that \mathcal{A} and \mathcal{B} are isogenous. This relation is symmetric, as shown in lemma 3. The degree of an isogeny $f : \mathcal{A} \rightarrow \mathcal{B}$ is defined as the degree of the function field extension

$$(1) \quad \deg f := [K(\mathcal{A}) : f^*K(\mathcal{B})].$$

This equals the order of the group scheme $\ker(f)$. The group of \bar{k} -rational points has order $\#(\ker f)(\bar{k}) = [K(\mathcal{A}) : f^*K(\mathcal{B})]^{sep}$, where $[K(\mathcal{A}) : f^*K(\mathcal{B})]^{sep}$ is the degree of the maximal separable subextension. An isogeny f is **separable** if and only if

$$(2) \quad \# \ker f(\bar{k}) = \deg f,$$

equivalently, if $\ker f$ is étale.

Lemma 2. *For any abelian variety \mathcal{A}/k , there is a one-to-one correspondence between finite subgroup schemes $\mathcal{K} \leq \mathcal{A}$ and isogenies $f : \mathcal{A} \rightarrow \mathcal{B}$, where \mathcal{B} is determined up to isomorphism. Moreover, $\mathcal{K} = \ker f$, $\mathcal{B} = \mathcal{A}/\mathcal{K}$, f is separable if and only if \mathcal{K} is étale, and then $\deg f = \#\mathcal{K}(\bar{k})$.*

Proof. Given a finite subgroup scheme $\mathcal{K} \leq \mathcal{A}$, the quotient $\mathcal{B} = \mathcal{A}/\mathcal{K}$ is an abelian variety over k , and the natural projection $f : \mathcal{A} \rightarrow \mathcal{B}$ is an isogeny with $\ker f = \mathcal{K}$. Conversely, for an isogeny $f : \mathcal{A} \rightarrow \mathcal{B}$, the kernel $\mathcal{K} = \ker f$ is finite, and $\mathcal{B} \cong \mathcal{A}/\mathcal{K}$ by the quotient structure. The map $\mathcal{K} \mapsto \mathcal{A}/\mathcal{K}$ is injective (distinct kernels yield distinct quotients) and surjective (every isogeny arises this way), establishing the bijection. Separability of f implies $\ker f$ is étale, and $\deg f = \#\mathcal{K}(\bar{k})$ holds in this case due to the étale order matching the field extension degree. \square

Isogenous abelian varieties have commensurable endomorphism rings: if \mathcal{A} and \mathcal{B} are isogenous, then $\text{End}^0(\mathcal{A}) \cong \text{End}^0(\mathcal{B})$. This follows from the existence of isogenies $f : \mathcal{A} \rightarrow \mathcal{B}$ and $g : \mathcal{B} \rightarrow \mathcal{A}$ such that $g \circ f = [n]$, inducing an isomorphism on rational endomorphism algebras.

Theorem 1 (Poincaré-Weil). *Let \mathcal{A} be an abelian variety. Then \mathcal{A} is isogenous to*

$$(3) \quad \mathcal{A}_1^{n_1} \times \mathcal{A}_2^{n_2} \times \cdots \times \mathcal{A}_r^{n_r},$$

where (up to permutation) \mathcal{A}_i , for $i = 1, \dots, r$, are simple, non-isogenous abelian varieties, and the factors $\mathcal{A}_i^{n_i}$ are uniquely determined up to isogenies.

Proof. Since \mathcal{A} is an abelian variety, its isogeny class contains a product of powers of simple abelian varieties. Let $\mathcal{A} \cong \prod_{i=1}^r \mathcal{A}_i^{n_i}$, where \mathcal{A}_i are simple and pairwise non-isogenous. The uniqueness follows from the Jordan-Hölder theorem for abelian varieties: any two such decompositions have isomorphic factors with equal multiplicities, up to permutation, due to the indecomposability of simple varieties and the structure of $\text{End}^0(\mathcal{A})$. \square

Corollary 1. *If \mathcal{A} is an absolutely simple abelian variety, then every endomorphism not equal to 0 is an isogeny.*

Proof. For \mathcal{A} absolutely simple, $\text{End}^0(\mathcal{A})$ is a division algebra. A non-zero endomorphism ϕ has trivial kernel (since $\ker \phi \neq \mathcal{A}$ and \mathcal{A} has no proper subvarieties as a simple variety), hence is an isogeny. \square

Fix a field k and an abelian variety \mathcal{A} over k . Let H be a finite subgroup of \mathcal{A} . From a computational perspective, we consider: (i) finding all abelian varieties \mathcal{B} over k such that there exists an isogeny $\mathcal{A} \rightarrow \mathcal{B}$ with kernel isomorphic to H ; (ii) given \mathcal{A} and H , determining $\mathcal{B} := \mathcal{A}/H$ and the isogeny $\mathcal{A} \rightarrow \mathcal{B}$; (iii) given \mathcal{A} and \mathcal{B} , determining if they are isogenous and computing a rational expression for an isogeny $\mathcal{A} \rightarrow \mathcal{B}$. For a survey and conjectures, see [3].

The scalar multiplication by n map $[n] : \mathcal{A} \rightarrow \mathcal{A}$ is an isogeny with kernel a group scheme of order $n^{2 \dim \mathcal{A}}$; see [4]. We denote $\mathcal{A}[n] = \ker[n](\bar{k})$, whose elements are the n -torsion points of \mathcal{A} .

Lemma 3. *Let $f : \mathcal{A} \rightarrow \mathcal{B}$ be an isogeny of degree n . Then there exists an isogeny $\hat{f} : \mathcal{B} \rightarrow \mathcal{A}$ such that*

$$(4) \quad f \circ \hat{f} = \hat{f} \circ f = [n].$$

The isogeny \hat{f} is called the **dual** of f .

Proof. Define \hat{f} via the dual abelian variety and the polarization induced by f . Since f is an isogeny, there exists a unique $\hat{f} : \mathcal{B} \rightarrow \mathcal{A}$ such that $f \circ \hat{f} = [n]$ on \mathcal{B} and $\hat{f} \circ f = [n]$ on \mathcal{A} , satisfying the duality condition due to the finite kernel's order matching $\deg f = n$. \square

Theorem 2. *Let \mathcal{A}/k be an abelian variety, $p = \text{char } k$, and $\dim \mathcal{A} = g$.*

- i) If $p \nmid n$, then $[n]$ is separable, $\#\mathcal{A}[n] = n^{2g}$, and $\mathcal{A}[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.*
- ii) If $p \mid n$, then $[n]$ is inseparable, and there exists an integer $0 \leq i \leq g$ such that*

$$(5) \quad \mathcal{A}[p^m] \cong (\mathbb{Z}/p^m\mathbb{Z})^i, \text{ for all } m \geq 1.$$

Proof. If $p \nmid n$, $[n]$ is separable as its derivative is non-zero, and $\mathcal{A}[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ follows from the étale nature of the kernel over \bar{k} . If $p \mid n$, $[n]$ includes a power of the Frobenius, making it inseparable, and the p -torsion structure depends on the p -rank i , determined by the dimension of the p -divisible group. \square

If $i = g$, \mathcal{A} is **ordinary**; if $\mathcal{A}[p^s](\bar{K}) = \mathbb{Z}/p^{ts}\mathbb{Z}$, it has p -**rank** t . For $\dim \mathcal{A} = 1$, it is **supersingular** if p -rank is 0; \mathcal{A} is **supersingular** if isogenous to a product of supersingular elliptic curves.

3. THETA FUNCTIONS

Let \mathcal{A} be an abelian variety of dimension g over an algebraically closed field k , which we take as \mathbb{C} for simplicity; the arguments extend to fields of characteristic p coprime to relevant integers via algebraic theta functions (see [4]). Represent \mathcal{A} as \mathbb{C}^g/Λ , where $\Lambda = \mathbb{Z}^g + \tau\mathbb{Z}^g$ is a lattice, and τ is a symmetric $g \times g$ matrix in the Siegel upper half-space \mathbb{H}_g , satisfying ${}^t\tau = \tau$ and $\text{Im}(\tau) > 0$. A theta function with characteristic $[a, b]$, where $a, b \in \mathbb{Q}^g$, is defined as

$$(6) \quad \theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i(n+a)^t \tau (n+a) + 2\pi i(n+a)^t (z+b)),$$

for $z \in \mathbb{C}^g$. The series converges absolutely due to the positive definiteness of $\text{Im}(\tau)$, ensuring that $\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau)$ is holomorphic on \mathbb{C}^g . These functions are quasi-periodic with respect to the lattice Λ : for $m \in \mathbb{Z}^g$,

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z+m, \tau) = \theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau),$$

and for $n \in \mathbb{Z}^g$,

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z+\tau n, \tau) = \exp(-\pi i n^t \tau n - 2\pi i n^t (z+b)) \theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau).$$

When $a, b \in \{0, 1/2\}^g$, the characteristic is half-integer, and the parity is even if $4a^t b$ is even, odd if $4a^t b$ is odd, reflecting the function's symmetry properties.

Proof of Quasi-Periodicity. For the first property, substitute $z+m$ into the definition:

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z+m, \tau) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i(n+a)^t \tau (n+a) + 2\pi i(n+a)^t (z+m+b)).$$

Since $(n+a)^t m = n^t m + a^t m$ and $n, m \in \mathbb{Z}^g$, the exponential term $\exp(2\pi i n^t m) = 1$, and $a^t m$ is rational, so the sum reindexes to itself, yielding equality. For the second, let $z' = z + \tau n$:

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z+\tau n, \tau) = \sum_{k \in \mathbb{Z}^g} \exp(\pi i(k+a)^t \tau (k+a) + 2\pi i(k+a)^t (z+\tau n+b)).$$

Set $k = n - m$, adjust the sum, and compute the difference in exponents, factoring out $\exp(-\pi i n^t \tau n - 2\pi i n^t (z+b))$ due to the symmetry ${}^t\tau = \tau$, confirming the multiplier. \square

Theta functions are sections of line bundles on \mathcal{A} . For a level n theta structure, define the functions $\theta \begin{bmatrix} 0 \\ b \end{bmatrix} (z, \tau/n)$, where $b \in (\mathbb{Z}/n\mathbb{Z})^g$. These form a basis for the space of sections $\Gamma(\mathcal{A}, \mathcal{L}_0^n)$, where \mathcal{L}_0 is the line bundle associated with the principal polarization, and \mathcal{L}_0^n is its n -th tensor power. The dimension of this space is n^g , reflecting the number of distinct characteristics $b \in (\mathbb{Z}/n\mathbb{Z})^g$. This basis induces a morphism

$$(7) \quad \varphi_n : \mathcal{A} \rightarrow \mathbb{P}^{n^g-1}, \quad z \mapsto (\theta \begin{bmatrix} 0 \\ b \end{bmatrix} (z, \tau/n))_{b \in (\mathbb{Z}/n\mathbb{Z})^g}.$$

For $n \geq 3$, φ_n is an embedding, realizing \mathcal{A} as a projective variety (see [5], Chapter II).

Theorem 3 (Embedding Theorem). *For an abelian variety \mathcal{A} of dimension g over \mathbb{C} with a principal polarization, the morphism $\varphi_n : \mathcal{A} \rightarrow \mathbb{P}^{n^g-1}$ is an embedding for $n \geq 3$.*

Proof. The line bundle \mathcal{L}_0^n is ample for $n \geq 1$, and for $n \geq 3$, it is very ample, meaning it separates points and tangent vectors. For distinct points $x, y \in \mathcal{A}$, there exists $b \in (\mathbb{Z}/n\mathbb{Z})^g$ such that $\theta \left[\begin{smallmatrix} 0 \\ b \end{smallmatrix} \right] (x, \tau/n) \neq \theta \left[\begin{smallmatrix} 0 \\ b \end{smallmatrix} \right] (y, \tau/n)$, as the functions span a space large enough to distinguish cosets modulo Λ . For a point x and tangent vector $v \in T_x \mathcal{A}$, the directional derivative $D_v \theta \left[\begin{smallmatrix} 0 \\ b \end{smallmatrix} \right] (x, \tau/n) \neq 0$ for some b , due to the completeness of the basis. Thus, φ_n is injective with injective differential, embedding \mathcal{A} into \mathbb{P}^{n^g-1} . \square

A key result is the transformation law under the symplectic group $\mathrm{Sp}(2g, \mathbb{Z})$, which acts on \mathbb{H}_g . For $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(2g, \mathbb{Z})$, define the transformed period matrix $\tau' = (A\tau + B)(C\tau + D)^{-1}$ and $z' = z(C\tau + D)^{-1}$. Shimura ([5], Chapter III) provides the functional equation:

$$(8) \quad \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z', \tau') = \kappa(\gamma) \det(C\tau + D)^{1/2} \exp(\pi i z(C\tau + D)^{-1} C z^t) \theta \left[\begin{smallmatrix} a' \\ b' \end{smallmatrix} \right] (z, \tau),$$

where $\kappa(\gamma)$ is a constant, and a', b' are transformed characteristics. This law governs the behavior of theta functions under automorphisms of \mathcal{A} .

Theorem 4 (Riemann Theta Relation). *For $z_1, z_2 \in \mathbb{C}^g$, the theta functions satisfy*

$$(9) \quad \theta(z_1 + z_2)\theta(z_1 - z_2) = \sum_{m \in (\mathbb{Z}/2\mathbb{Z})^g} \theta \left[\begin{smallmatrix} m/2 \\ 0 \end{smallmatrix} \right] (2z_1)\theta \left[\begin{smallmatrix} m/2 \\ 0 \end{smallmatrix} \right] (2z_2),$$

where $\theta(z) = \theta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right] (z, \tau)$.

Proof. Consider the product $\theta(z_1 + z_2)\theta(z_1 - z_2)$ as a sum over $n, m \in \mathbb{Z}^g$. Pair terms with $n+m$ and $n-m$, adjust indices, and use the periodicity properties. The right-hand side arises from a Fourier expansion of the product, with the half-integer characteristics $m/2$ accounting for the doubling $2z_1, 2z_2$. The identity holds by the analytic continuation and symmetry of theta functions (see [5], Chapter II). \square

The values $\theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (0, \tau)$, called theta constants or thetanulls, are significant. For a principally polarized \mathcal{A} , they determine τ up to the action of $\mathrm{Sp}(2g, \mathbb{Z})$, parametrizing the moduli space \mathcal{A}_g . When $a, b \in \{0, 1/2\}^g$, there are 2^{2g} such constants, half even and half odd, reflecting the 2-torsion structure $\mathcal{A}[2]$.

Lemma 4. *The theta constants $\theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (0, \tau)$ for $a, b \in \{0, 1/2\}^g$ are zero if and only if the characteristic $[a, b]$ is odd.*

Proof. The parity depends on $4a^t b \pmod{2}$. If odd, the summand $\exp(\pi i(n + a)^t \tau(n + a))$ at $z = 0$ pairs terms n and $-n - 2a$, with opposite signs due to the linear term $2\pi i(n + a)^t b$, canceling to zero. If even, no such cancellation occurs, and the constant is non-zero generically. \square

These results underpin the geometric and analytic properties of abelian varieties, with theta functions serving as both coordinates and invariants (see [5] for a comprehensive treatment).

4. JACOBIAN VARIETIES

Let \mathcal{X} be a curve of positive genus over k , and assume there exists a k -rational point $P_0 \in \mathcal{X}(k)$ with attached prime divisor \mathfrak{p}_0 . There exists an abelian variety $\text{Jac}_k(\mathcal{X})$ over k and a uniquely determined embedding

$$(10) \quad \phi_{P_0} : \mathcal{X} \rightarrow \text{Jac}_k(\mathcal{X}) \quad \text{with} \quad \phi_{P_0}(P_0) = 0_{\text{Jac}_k(\mathcal{X})},$$

satisfying:

- (1) For all extension fields L of k , $\text{Jac}_L \mathcal{X} = \text{Pic}_{\mathcal{X}_L}^0(L)$, with this equality given functorially.
- (2) For any abelian variety \mathbb{A} and morphism $\eta : \mathcal{X} \rightarrow \mathbb{A}$ sending P_0 to $0_{\mathbb{A}}$, there exists a unique homomorphism $\psi : \text{Jac}(\mathcal{X}) \rightarrow \mathbb{A}$ such that $\psi \circ \phi_{P_0} = \eta$.

This $\text{Jac}(\mathcal{X})$, called the *Jacobian variety* of \mathcal{X} , maps a prime divisor \mathfrak{p} of degree 1 on \mathcal{X}_L to $[\mathfrak{p} - \mathfrak{p}_0]$ in $\text{Pic}_{\mathcal{X}_L}^0(L)$.

Lemma 5. *The Jacobian $\text{Jac}(\mathcal{X})$ is unique up to isomorphism among abelian varieties satisfying the above properties.*

Proof. Suppose \mathcal{J}_1 and \mathcal{J}_2 satisfy the conditions with embeddings $\phi_1 : \mathcal{X} \rightarrow \mathcal{J}_1$ and $\phi_2 : \mathcal{X} \rightarrow \mathcal{J}_2$. By property (2), there exist homomorphisms $\psi_{12} : \mathcal{J}_1 \rightarrow \mathcal{J}_2$ and $\psi_{21} : \mathcal{J}_2 \rightarrow \mathcal{J}_1$ such that $\psi_{12} \circ \phi_1 = \phi_2$ and $\psi_{21} \circ \phi_2 = \phi_1$. Composing, $\psi_{21} \circ \psi_{12} \circ \phi_1 = \phi_1$. Since $\phi_1(\mathcal{X})$ generates \mathcal{J}_1 as a group (by the Abel-Jacobi theorem), and \mathcal{J}_1 is abelian, $\psi_{21} \circ \psi_{12}$ acts as the identity on a dense subset, hence $\psi_{21} \circ \psi_{12} = \text{id}_{\mathcal{J}_1}$. Similarly, $\psi_{12} \circ \psi_{21} = \text{id}_{\mathcal{J}_2}$, establishing an isomorphism $\mathcal{J}_1 \cong \mathcal{J}_2$. \square

Let L/k be a finite algebraic extension. Then $\text{Jac}_L \mathcal{X}$ is the scalar extension of $\text{Jac} \mathcal{X}$ with L , forming a fiber product with projection $p : \text{Jac}_L \mathcal{X} \rightarrow \text{Jac} \mathcal{X}$. The norm map is p_* , and the conorm map is p^* . If $f : \mathcal{X} \rightarrow \mathcal{D}$ is a surjective morphism of curves sending P_0 to Q_0 , there exists a unique surjective homomorphism $f_* : \text{Jac} \mathcal{X} \rightarrow \text{Jac} \mathcal{D}$ such that $f_* \circ \phi_{P_0} = \phi_{Q_0}$. If $\text{Jac} \mathcal{X}$ is simple and $\eta : \mathcal{X} \rightarrow \mathcal{D}$ is a separable cover of degree > 1 , then $\mathcal{D} \cong \mathbb{P}^1$, as any non-trivial quotient of a simple abelian variety is trivial. For details, see [1].

4.1. Jacobian surfaces.

5. ENDOMORPHISM RING OF ABELIAN VARIETIES

The endomorphism ring of an abelian variety is a fundamental invariant that encodes its algebraic symmetries and arithmetic structure. For an abelian variety \mathcal{A} of dimension g over a field k , we define $\text{End}(\mathcal{A})$ as the ring of regular morphisms $\phi : \mathcal{A} \rightarrow \mathcal{A}$ that preserve the group operation, satisfying $\phi(x+y) = \phi(x) + \phi(y)$ for all $x, y \in \mathcal{A}(k')$ over any extension field k' . Equipped with addition and composition, and with the identity map as the unit, $\text{End}(\mathcal{A})$ forms a \mathbb{Z} -module, but its full complexity emerges in the rational endomorphism algebra $\text{End}^0(\mathcal{A}) = \text{End}(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$, a finite-dimensional \mathbb{Q} -algebra. Over an algebraically closed field such as \mathbb{C} or $\overline{\mathbb{Q}}$, this algebra provides insight into the variety's isogeny class and geometric properties.

An endomorphism $\phi \in \text{End}(\mathcal{A})$ is an isogeny if it is surjective with a finite kernel, its degree $\deg \phi$ being the order of $\ker \phi$ as a group scheme. Such a ϕ has a dual isogeny $\hat{\phi} : \mathcal{A} \rightarrow \mathcal{A}$ such that $\phi \circ \hat{\phi} = [\deg \phi]$, where $[n] : \mathcal{A} \rightarrow \mathcal{A}$ denotes multiplication by n . A key property across all dimensions is that $\text{End}^0(\mathcal{A})$

is invariant under isogeny: if \mathcal{A} and \mathcal{B} are isogenous abelian varieties, meaning there exists an isogeny $f : \mathcal{A} \rightarrow \mathcal{B}$, then their rational endomorphism algebras are isomorphic. To see this, consider f with dual \hat{f} satisfying $f \circ \hat{f} = [n]$. The map $\Phi : \text{End}(\mathcal{B}) \rightarrow \text{End}(\mathcal{A})$ given by $\Phi(\phi) = f \circ \phi \circ \hat{f}$ is a ring homomorphism, and extending it to $\text{End}^0(\mathcal{B})$ via $\Phi'(\phi) = \frac{1}{n} f \circ \phi \circ \hat{f}$ yields an isomorphism, as Φ' is injective (if $f \circ \phi \circ \hat{f} = 0$, then $\phi = 0$ since f and \hat{f} are isogenies) and surjective via the inverse map adjusted by scalars (see [4], Chapter III, §19). This invariance underpins the study of endomorphism algebras across isogeny classes.

For an abelian variety \mathcal{A} , the structure of $\text{End}^0(\mathcal{A})$ depends on its decomposition. The Poincaré-Weil theorem asserts that \mathcal{A} is isogenous to $\mathcal{A}_1^{n_1} \times \cdots \times \mathcal{A}_r^{n_r}$, where the \mathcal{A}_i are simple (having no non-trivial abelian subvarieties) and pairwise non-isogenous, with the factors uniquely determined up to permutation and isogeny ([4], Chapter III, §15). If \mathcal{A} is simple, $\text{End}^0(\mathcal{A})$ is a division algebra over its center Z , and $[Z : \mathbb{Q}] \cdot [\text{End}^0(\mathcal{A}) : Z] = (\dim \mathcal{A})^2 = g^2$. If \mathcal{A} is not simple, $\text{End}^0(\mathcal{A})$ is a product of the endomorphism algebras of its factors, adjusted for isogenies.

When we narrow our focus to abelian surfaces, where $\dim \mathcal{A} = 2$, the classification of $\text{End}^0(\mathcal{A})$ becomes more precise, especially over $\overline{\mathbb{Q}}$. Here, an endomorphism ϕ acts on a 2-dimensional variety, and the possible structures of $\text{End}^0(\mathcal{A})$ are richly detailed by Albert's classification, as refined in [6]. For a principally polarized abelian surface \mathcal{A} —where a polarization $\lambda : \mathcal{A} \rightarrow \hat{\mathcal{A}}$ to the dual has degree 1—the algebra $\text{End}_{\overline{\mathbb{Q}}}^0(\mathcal{A})$ can be one of several types: \mathbb{Q} , a real quadratic field (e.g., $\mathbb{Q}(\sqrt{d})$, $d > 0$ square-free), a CM field of degree 4 over \mathbb{Q} (a totally imaginary quadratic extension of a real quadratic field), a non-split quaternion algebra over \mathbb{Q} (e.g., $\left(\frac{a,b}{\mathbb{Q}}\right)$, $a, b \in \mathbb{Q}^\times$), a direct sum $F_1 \oplus F_2$ where each F_i is \mathbb{Q} or an imaginary quadratic field (e.g., $\mathbb{Q}(\sqrt{-d})$), or a matrix algebra from the Mumford-Tate group with center F being \mathbb{Q} or an imaginary quadratic field.

To understand this classification, consider the isogeny decomposition of an abelian surface. If \mathcal{A} is simple, $\text{End}^0(\mathcal{A})$ is a division algebra, and since $\dim \mathcal{A} = 2$, we have $[Z : \mathbb{Q}] \cdot [\text{End}^0(\mathcal{A}) : Z] = 2^2 = 4$. If the center $Z = \mathbb{Q}$, then $\text{End}^0(\mathcal{A})$ has dimension 1 (just \mathbb{Q}), 2 (a real quadratic field), or 4 (a CM field or quaternion algebra). A real quadratic field like $\mathbb{Q}(\sqrt{2})$ indicates real multiplication, where endomorphisms embed the field into the algebra of 2×2 matrices over \mathbb{R} . A CM field, such as $\mathbb{Q}(\sqrt{2}, i)$, arises from complex multiplication, doubling a quadratic field with an imaginary unit, and has dimension 4 over \mathbb{Q} . A non-split quaternion algebra, like $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, also has dimension 4 and occurs in special cases, often in positive characteristic. If \mathcal{A} is not simple, it is isogenous to $E_1 \times E_2$, where $\dim E_i = 1$, and $\text{End}^0(\mathcal{A}) = \text{End}^0(E_1) \oplus \text{End}^0(E_2)$, with each $\text{End}^0(E_i)$ being \mathbb{Q} (dimension 1) or an imaginary quadratic field (dimension 2), yielding the direct sum type. The Mumford-Tate case involves a center F (\mathbb{Q} or $\mathbb{Q}(\sqrt{-d})$), where $\text{End}^0(\mathcal{A})$ forms a matrix algebra constrained by the surface's Hodge structure.

Theorem 5 (Albert's Classification for Abelian Surfaces). *Let \mathcal{A} be a principally polarized abelian surface over $\overline{\mathbb{Q}}$. Then $\text{End}^0(\mathcal{A})$ is isomorphic to one of the following:*

- (1) \mathbb{Q} ,
- (2) a real quadratic field,
- (3) a CM field of degree 4 over \mathbb{Q} ,

- (4) a non-split quaternion algebra over \mathbb{Q} ,
- (5) $F_1 \oplus F_2$ where $F_i = \mathbb{Q}$ or an imaginary quadratic field,
- (6) a matrix algebra over a center F where $F = \mathbb{Q}$ or an imaginary quadratic field.

Proof. Since \mathcal{A} is an abelian surface over $\overline{\mathbb{Q}}$, its dimension is 2, and by the Poincaré-Weil theorem (Theorem 1), \mathcal{A} is isogenous to a product $\mathcal{A}_1^{n_1} \times \cdots \times \mathcal{A}_r^{n_r}$, where the \mathcal{A}_i are simple abelian varieties, pairwise non-isogenous, and the decomposition is unique up to permutation and isogeny. Given $\dim \mathcal{A} = 2$, only two cases arise: (i) \mathcal{A} is simple ($r = 1$, $n_1 = 1$), or (ii) $\mathcal{A} \cong E_1 \times E_2$, where $\dim E_1 = \dim E_2 = 1$. The rational endomorphism algebra $\text{End}^0(\mathcal{A}) = \text{End}(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is semi-simple due to the principal polarization's Rosati involution, and its structure depends on this decomposition.

Case 1: \mathcal{A} is simple. If \mathcal{A} is simple, $\text{End}^0(\mathcal{A})$ is a division algebra over its center Z , a number field over \mathbb{Q} , and the dimension formula holds: $[Z : \mathbb{Q}] \cdot [\text{End}^0(\mathcal{A}) : Z] = (\dim \mathcal{A})^2 = 4$. Since \mathcal{A} is principally polarized, the Rosati involution $\phi \mapsto \phi^\dagger$ (where $\phi^\dagger = \hat{\lambda}^{-1} \circ \phi \circ \lambda$, $\lambda : \mathcal{A} \rightarrow \hat{\mathcal{A}}$ the polarization) is positive definite, fixing Z and constraining $\text{End}^0(\mathcal{A})$ to be a division algebra with involution. We consider possible dimensions of Z :

- (1) If $Z = \mathbb{Q}$, then $[Z : \mathbb{Q}] = 1$, and $[\text{End}^0(\mathcal{A}) : \mathbb{Q}] = 4$. Possible division algebras over \mathbb{Q} of dimension 4 include:
 - (a) \mathbb{Q} itself, dimension 1, where $\text{End}^0(\mathcal{A}) = \mathbb{Q}$, and every non-zero endomorphism is an isogeny (multiplication by a rational).
 - (b) A real quadratic field, e.g., $\mathbb{Q}(\sqrt{d})$, $d > 0$ square-free, dimension 2, where $\text{End}^0(\mathcal{A})$ embeds into $M_2(\mathbb{R})$ via real multiplication, satisfying the dimension constraint with $[\text{End}^0(\mathcal{A}) : Z] = 2$.
 - (c) A CM field of degree 4, e.g., $\mathbb{Q}(\sqrt{d}, i)$, a totally imaginary quadratic extension of a real quadratic field, dimension 4, with $[\text{End}^0(\mathcal{A}) : Z] = 1$, compatible with complex multiplication and the involution (conjugation).
 - (d) A non-split quaternion algebra over \mathbb{Q} , e.g., $\left(\frac{a,b}{\mathbb{Q}}\right)$, $a, b \in \mathbb{Q}^\times$, dimension 4, with $[\text{End}^0(\mathcal{A}) : Z] = 1$, where the standard involution (conjugation) is positive definite under the polarization.
- (2) If Z is a quadratic field (real or imaginary), $[Z : \mathbb{Q}] = 2$, then $[\text{End}^0(\mathcal{A}) : Z] = 2$. Here, $\text{End}^0(\mathcal{A})$ is a division algebra over a quadratic field:
 - (a) For $Z = \mathbb{Q}(\sqrt{d})$, $d > 0$, $\text{End}^0(\mathcal{A})$ could be a quaternion algebra over Z (dimension 4 over Z , but 8 over \mathbb{Q}), exceeding 4, so this is not possible unless $\text{End}^0(\mathcal{A}) = Z$, already covered.
 - (b) For $Z = \mathbb{Q}(\sqrt{-d})$, similar constraints apply; a CM field over an imaginary quadratic field has dimension 8 over \mathbb{Q} , ruling it out.
- (3) If Z is quartic, $[Z : \mathbb{Q}] = 4$, then $[\text{End}^0(\mathcal{A}) : Z] = 1$, so $\text{End}^0(\mathcal{A}) = Z$, a CM field, as above.

Thus, for simple \mathcal{A} , $\text{End}^0(\mathcal{A})$ is \mathbb{Q} , a real quadratic field, a CM field of degree 4, or a non-split quaternion algebra over \mathbb{Q} .

Case 2: $\mathcal{A} \cong E_1 \times E_2$. If \mathcal{A} is not simple, it is isogenous to $E_1 \times E_2$, where E_1 and E_2 are elliptic curves over $\overline{\mathbb{Q}}$. Then $\text{End}^0(\mathcal{A}) = \text{End}^0(E_1) \oplus \text{End}^0(E_2)$, as

endomorphisms respect the product structure (no cross-terms exist unless $E_1 \cong E_2$). For an elliptic curve E_i over $\overline{\mathbb{Q}}$:

- (1) $\text{End}^0(E_i) = \mathbb{Q}$ if E_i has no complex multiplication (CM), dimension 1.
- (2) $\text{End}^0(E_i) = \mathbb{Q}(\sqrt{-d})$, an imaginary quadratic field, if E_i has CM, dimension 2.

Thus, $\text{End}^0(\mathcal{A}) = F_1 \oplus F_2$, where $F_i = \text{End}^0(E_i)$, yielding dimensions $1+1 = 2$ or $2+2 = 4$ over \mathbb{Q} . If $E_1 \cong E_2$, $\text{End}^0(\mathcal{A}) \cong M_2(F)$, where $F = \text{End}^0(E_1)$, a matrix algebra over \mathbb{Q} (dimension 4) or an imaginary quadratic field (dimension 8), but the principal polarization constrains this to a division algebra unless adjusted by the Hodge structure.

When \mathcal{A} 's Hodge structure (over \mathbb{C}) defines a Mumford-Tate group, $\text{End}^0(\mathcal{A})$ may be a matrix algebra over a center F . For $\dim \mathcal{A} = 2$, $F = \mathbb{Q}$ gives $M_2(\mathbb{Q})$ (dimension 4), or $F = \mathbb{Q}(\sqrt{-d})$ gives a division algebra (dimension 4 over F , 8 over \mathbb{Q}), but the polarization restricts to $M_2(\mathbb{Q})$ or reduces to prior cases ([6], §4; [5], Chapter IV).

The dimension bound 4 and semi-simplicity (via Rosati) limit $\text{End}^0(\mathcal{A})$ to these types. Higher-degree fields or algebras (e.g., dimension 8) exceed $\dim \mathcal{A}^2 = 4$, and the polarization excludes non-division or non-positive cases, completing the classification. \square

A principal polarization $\lambda : \mathcal{A} \rightarrow \hat{\mathcal{A}}$ induces the Rosati involution $\phi \mapsto \phi^\dagger = \hat{\lambda}^{-1} \circ \hat{\phi} \circ \lambda$, fixing the center and ensuring $\text{End}^0(\mathcal{A})$ is semi-simple. The trace form $\langle \phi, \psi \rangle = \text{tr}(\phi^\dagger \circ \psi)$ is positive definite: for $\phi \neq 0$, $\text{tr}(\phi^\dagger \circ \phi) > 0$, as $\phi^\dagger \circ \phi$ is a non-zero symmetric endomorphism, and the polarization's positivity on $\hat{\mathcal{A}}$ guarantees this (see [4], Chapter IV, §21). Thus, $\text{End}^0(\mathcal{A})$ decomposes into simple algebras matching Albert's types.

The dimension of $\text{End}^0(\mathcal{A})$ for an abelian surface is at most 4, reflecting $g = 2$. If \mathcal{A} is simple, it is 1, 2, or 4; if a product, it sums to 2 or 4. For a Jacobian $\text{Jac}(\mathcal{X})$, $\text{End}_{\overline{\mathbb{Q}}}^0(\text{Jac } \mathcal{X})$ is typically \mathbb{Q} unless \mathcal{X} has special symmetries, yielding richer structures as detailed in [6].

6. GENUS 2 CURVES, THEIR JACOBIANS, AND ASSOCIATED KUMMER SURFACES

Since our focus later will be on cryptosystems based on isogenies of Jacobians of genus two curves, we present here the essential facts about such curves, which have become ingrained in mathematical folklore. For further details, the interested reader may consult [7, 8]. Let \mathcal{X} be a genus 2 curve defined over a field k . A curve of genus 2 is a smooth, projective, geometrically irreducible algebraic curve with genus $g = 2$, meaning its geometric genus—computed as the dimension of the space of holomorphic differentials over an algebraically closed field—is 2. The gonality of \mathcal{X} , denoted $\gamma_{\mathcal{X}}$, is the minimal degree of a non-constant morphism from \mathcal{X} to \mathbb{P}^1 , and for genus 2 curves, $\gamma_{\mathcal{X}} = 2$. This implies that \mathcal{X} is hyperelliptic, admitting a degree 2 covering $\pi : \mathcal{X} \rightarrow \mathbb{P}^1$, which we call the hyperelliptic projection. By Hurwitz's formula, applied to this double cover, the number of branch points r satisfies $2g - 2 = -2 \cdot 2 + r$, so $2 \cdot 2 - 2 = r - 4$, hence $r = 6$. These 6 branch points in $\mathbb{P}^1(\bar{k})$ are the images of the Weierstrass points of \mathcal{X} , points where the hyperelliptic involution (an automorphism of order 2) fixes the curve. The moduli space of genus 2 curves, denoted \mathcal{M}_2 , parameterizes such curves up to isomorphism

and has dimension $r - 3 = 6 - 3 = 3$, reflecting the 3 degrees of freedom in their configuration after projective transformations.

The arithmetic structure of \mathcal{M}_2 was profoundly studied by Igusa in his seminal paper [9], building on earlier work by Clebsch, Bolza, and others. He introduced a set of invariants $J_2, J_4, J_6, J_8, J_{10}$, known as the Igusa invariants, which uniquely determine the isomorphism class of a genus 2 curve over an algebraically closed field. These invariants are homogeneous polynomials in the coefficients of a defining equation, with degrees 2, 4, 6, 8, and 10, respectively, and we refer to [10] for a comprehensive treatment of their properties and relations. Two genus 2 curves \mathcal{X} and \mathcal{X}' are isomorphic over \bar{k} if and only if there exists $l \in \bar{k}^*$ such that $J_{2i}(\mathcal{X}) = l^{2i} J_{2i}(\mathcal{X}')$ for $i = 1, \dots, 5$, a condition reflecting the projective weighting of the invariants. When $\text{char } k \neq 2$, the invariant J_8 is redundant, expressible in terms of J_2, J_4, J_6 , and J_{10} , simplifying the classification.

Henceforth, we assume $\text{char } k \neq 2$, ensuring a standard form for the curve's equation. Under this condition, \mathcal{X} can be represented by an affine Weierstrass equation

$$(11) \quad y^2 = f(x) = a_6 x^6 + \dots + a_1 x + a_0,$$

over \bar{k} , where $f(x)$ is a monic polynomial of degree 6 with distinct roots, and the discriminant $\Delta_f = J_{10} \neq 0$ guarantees smoothness. Thus, we will be considering the weighted projective space $\mathbb{P}_{(2,4,6,10)}(k)$ using the invariants J_2, J_4, J_6, J_{10} and the space

$$(12) \quad \mathbb{P}_{(2,4,6,10)}(k) \setminus \{J_{10} = 0\},$$

where $J_{10} \neq 0$ excludes singular curves. From now on, by invariants of a genus 2 curve, we mean J_2, J_4, J_6, J_{10} , and by a genus 2 curve, we refer to its isomorphism class, represented as a moduli point $\mathbf{p} = [J_2 : J_4 : J_6 : J_{10}] \in \mathbb{P}_{(2,4,6,10)}(k)$.

6.1. Principal Polarizations and Torelli Theorem. The Jacobian $\text{Jac}(\mathcal{X})$ of a genus 2 curve \mathcal{X} is an abelian surface, a 2-dimensional principally polarized abelian variety, constructed as the Picard group $\text{Pic}^0(\mathcal{X})$ of degree 0 divisor classes on \mathcal{X} . Given a k -rational point $P_0 \in \mathcal{X}(k)$, the embedding $\phi_{P_0}: \mathcal{X} \rightarrow \text{Jac}(\mathcal{X})$, defined by $P \mapsto [P - P_0]$, maps \mathcal{X} into $\text{Jac}(\mathcal{X})$ with $\phi_{P_0}(P_0) = 0$. This embedding is canonical up to translation, and $\text{Jac}(\mathcal{X})$ is functorial: for any extension L/k , $\text{Jac}_L(\mathcal{X}) = \text{Pic}_{\mathcal{X}_L}^0(L)$. The hyperelliptic involution $\iota: \mathcal{X} \rightarrow \mathcal{X}$, swapping sheets of the cover π , induces an involution $\iota_*: \text{Jac}(\mathcal{X}) \rightarrow \text{Jac}(\mathcal{X})$ with $\iota_*(D) = -D$, which we also denote by $-\mathbb{I}$ and which is central to the later construction of Kummer surfaces.

A map $f: \mathcal{X} \rightarrow \mathcal{D}$ between curves induces homomorphisms $f^*: \text{Jac}(\mathcal{D}) \rightarrow \text{Jac}(\mathcal{X})$ (pullback) and $f_*: \text{Jac}(\mathcal{X}) \rightarrow \text{Jac}(\mathcal{D})$ (pushforward), reflecting the functorial nature of the Jacobian. When f is a maximal covering—i.e., not factoring through an isogeny—these maps reveal the Jacobian's structure. For an abelian surface \mathcal{A} , a polarization is an isogeny $\lambda: \mathcal{A} \rightarrow \hat{\mathcal{A}}$ to the dual, and \mathcal{A} is principally polarized if $\deg \lambda = 1$. The theta divisor $\Theta \subset \text{Jac}(\mathcal{X})$, image of ϕ_{P_0} , provides such a polarization, making $\text{Jac}(\mathcal{X})$ a principal case.

Let us explain the construction of a principal polarization on $\text{Jac}(\mathcal{X})$ in more detail: The Siegel three-fold is the quasi-projective variety of dimension three, obtained from the Siegel upper half-plane \mathbb{H}_2 of degree two¹ divided by the action

¹By definition \mathbb{H}_2 is the set of two-by-two symmetric matrices over \mathbb{C} whose imaginary part is positive definite

of the modular transformations $\Gamma_2 := \mathrm{Sp}_4(\mathbb{Z})$, i.e.,

$$(13) \quad \mathbb{A}_2 = \mathbb{H}_2/\Gamma_2.$$

Each $\tau = \begin{pmatrix} \tau_{11} & \tau_{12} \\ \tau_{12} & \tau_{22} \end{pmatrix} \in \mathbb{H}_2$ determines a complex abelian surface $\mathcal{A} = \mathbb{C}^2/\Lambda$ obtained from the lattice $\Lambda = \langle \mathbb{Z}^2 \oplus \tau \mathbb{Z}^2 \rangle$ with the period matrix $(\mathbb{I}_2, \tau) \in \mathrm{Mat}(2, 4; \mathbb{C})$. We consider two abelian surfaces \mathcal{A} and $\tilde{\mathcal{A}}$ isomorphic if and only if there is an element $M \in \Gamma_2$ such that $\tilde{\tau} = M(\tau)$. The *canonical principal polarization* of \mathcal{A} is given by the positive definite hermitian forms \mathbf{h} on \mathbb{C}^2 such that $\alpha = \mathrm{Im} \mathbf{h}(\Lambda, \Lambda) \subset \mathbb{Z}$ where α is the Riemann form $\alpha(x_1 + x_2\tau, y_1 + y_2\tau) = x_1^t \cdot y_2 - y_1^t \cdot x_2$ on $\mathbb{Z}^2 \oplus \tau \mathbb{Z}^2$.

This hermitian form determines a line bundle $\mathcal{L} \rightarrow \mathcal{A}$ in the Néron-Severi lattice $\mathrm{NS}(\mathcal{A})$. A general fact from linear algebra asserts that one can always choose a basis of Λ such that α is given by the matrix $\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}$ with $D = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ where $d_1, d_2 \in \mathbb{N}$, $d_1, d_2 \geq 0$, and d_1 divides d_2 . For a principal polarization one has $(d_1, d_2) = (1, 1)$. Since transformations in Γ_2 preserve the Riemann form α , it follows that the Siegel three-fold is also the set of isomorphism classes of principally polarized abelian surfaces, i.e., abelian surfaces with a polarization of type $(1, 1)$. We also define the subgroup $\Gamma_2(2) = \{M \in \Gamma_2 \mid M \equiv \mathbb{I} \pmod{2}\}$ such that $\Gamma_2/\Gamma_2(2) \cong S_6$ where S_6 is the permutation group of six elements representing the permutations of the roots of the right hand side of Equation (98) when we have identification $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$.

For a principally polarized abelian variety \mathcal{A} the line bundle \mathcal{L} defining its principal polarization is ample and satisfies $h^0(\mathcal{L}) = 1$. There exists an effective divisor Θ such that $\mathcal{L} = \mathcal{O}_{\mathcal{A}}(\Theta)$, uniquely defined only up to translations. The divisor $\Theta \in \mathrm{NS}(\mathcal{A})$ is called a *theta divisor* associated with the polarization. It is known that the abelian surface \mathcal{A} is not the product of two elliptic curves if and only if Θ is an irreducible divisor. Torelli's theorem states that the map sending a curve \mathcal{X} to its Jacobian $\mathrm{Jac}(\mathcal{X})$, that is $\mathcal{X} \mapsto (\mathrm{Jac}(\mathcal{X}), \Theta)$, is injective and defines a birational map $\mathcal{M}_2 \dashrightarrow \mathbb{A}_2$ which restricts to a rational map $\mathcal{M}_2(2) \dashrightarrow \mathbb{A}_2(2)$ between the coarse moduli spaces of smooth curves of genus two with marked Weierstrass points and principally polarized abelian surfaces with marked level-two structures, respectively. Conversely, if the period matrix τ of a principally polarized abelian variety \mathcal{A} is not equivalent to a point with $\tau_{12} = 0$ relative to Γ_2 , then a Θ -divisor on \mathcal{A} is given by a non-singular curve \mathcal{X} of genus-two, i.e., $\Theta = [\mathcal{X}]$ such that $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$. Thus, a principally polarized abelian surface is either the Jacobian of a smooth curve of genus two with a theta divisor or the product of two complex elliptic curves, with the product polarization. In particular, the moduli space \mathcal{M}_2 has a compactification \mathbb{A}_2^* as the weighted projective space $\mathbb{P}_{(2,4,6,10)}(k)$ using the invariants J_2, J_4, J_6, J_{10} and

$$(14) \quad \mathbb{A}_2 \cong \mathbb{P}_{(2,4,6,10)}(k) \setminus \{J_{10} = 0\}.$$

Igusa proved [11, 12] that the ring of modular forms is generated by the Siegel modular forms $\psi_4, \psi_6, \chi_{10}, \chi_{12}$ and by one more cusp form χ_{35} of odd weight 35 ²

²For a detailed introduction to Siegel modular forms relative to Γ_2 , Humbert surfaces, and the Satake compactification of the Siegel modular threefold we refer to Freitag's book [13].

whose square is the following polynomial [11, p. 849] in the even generators

(15)

$$\begin{aligned} \chi_{35}^2 = & \frac{1}{2^{12} 3^9} \chi_{10} (2^{24} 3^{15} \chi_{12}^5 - 2^{13} 3^9 \psi_4^3 \chi_{12}^4 - 2^{13} 3^9 \psi_6^2 \chi_{12}^4 + 3^3 \psi_4^6 \chi_{12}^3 \\ & - 2 \cdot 3^3 \psi_4^3 \psi_6^2 \chi_{12}^3 - 2^{14} 3^8 \psi_4^2 \psi_6 \chi_{10} \chi_{12}^3 - 2^{23} 3^{12} 5^2 \psi_4 \chi_{10}^2 \chi_{12}^3 + 3^3 \psi_6^4 \chi_{12}^3 \\ & + 2^{11} 3^6 37 \psi_4^4 \chi_{10}^2 \chi_{12}^2 + 2^{11} 3^6 5 \cdot 7 \psi_4 \psi_6^2 \chi_{10}^2 \chi_{12}^2 - 2^{23} 3^9 5^3 \psi_6 \chi_{10}^3 \chi_{12}^2 \\ & - 3^2 \psi_4^7 \chi_{10}^2 \chi_{12} + 2 \cdot 3^2 \psi_4^4 \psi_6^2 \chi_{10}^2 \chi_{12} + 2^{11} 3^5 5 \cdot 19 \psi_4^3 \psi_6 \chi_{10}^3 \chi_{12} \\ & + 2^{20} 3^8 5^3 11 \psi_4^2 \chi_{10}^4 \chi_{12} - 3^2 \psi_4 \psi_6^4 \chi_{10}^2 \chi_{12} + 2^{11} 3^5 5^2 \psi_6^3 \chi_{10}^3 \chi_{12} - 2 \psi_4^6 \psi_6 \chi_{10}^3 \\ & - 2^{12} 3^4 \psi_4^5 \chi_{10}^4 + 2^2 \psi_4^3 \psi_6^3 \chi_{10}^3 + 2^{12} 3^4 5^2 \psi_4^2 \psi_6^2 \chi_{10}^4 + 2^{21} 3^7 5^4 \psi_4 \psi_6 \chi_{10}^5 \\ & - 2 \psi_6^5 \chi_{10}^3 + 2^{32} 3^9 5^5 \chi_{10}^6). \end{aligned}$$

Hence, the expression $Q := 2^{12} 3^9 \chi_{35}^2 / \chi_{10}$ is a polynomial of degree 60 in the even generators. Igusa also proved that each Siegel modular form (with trivial character) of odd weight is divisible by the form χ_{35} .

Igusa [11, p. 848] proved that the relations between the Igusa invariants of a binary sextic $y^2 = f(x)$ defining a smooth genus-two curve \mathcal{X} and the even Siegel modular forms for the associated principally polarized abelian surface $\mathcal{A} = \text{Jac}(\mathcal{X})$ with period matrix τ are as follows:

$$\begin{aligned} (16) \quad J_2(f) &= -2^3 \cdot 3 \frac{\chi_{12}(\tau)}{\chi_{10}(\tau)}, \\ J_4(f) &= 2^2 \psi_4(\tau), \\ J_6(f) &= -\frac{2^3}{3} \psi_6(\tau) - 2^5 \frac{\psi_4(\tau) \chi_{12}(\tau)}{\chi_{10}(\tau)}, \\ J_{10}(f) &= -2^{14} \chi_{10}(\tau) \neq 0. \end{aligned}$$

Here, the Igusa invariant J_{10} is the discriminant of the sextic $f(x)$ and we are using the same normalization as in [14, 15].

6.2. Göpel groups and Theta divisors. For an abelian surface \mathcal{A} , such as the Jacobian $\mathcal{A} = \text{Jac}(\mathcal{X})$ of a genus 2 curve \mathcal{X} over a field k , the group of 2-torsion points $\mathcal{A}[2]$ consists of elements $x \in \mathcal{A}(\bar{k})$ satisfying $2x = 0$, forming a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g} = (\mathbb{Z}/2\mathbb{Z})^4$ over k when $\text{char } k \neq 2$. Translation by a 2-torsion point is an isomorphism of \mathcal{A} , mapping $\mathcal{A}[2]$ to itself, preserving its structure under the Weil pairing, which defines an alternating bilinear form on $\mathcal{A}[2]$. A subspace $\mathcal{K} \subset \mathcal{A}[2]$ is isotropic if the Weil pairing vanishes on $\mathcal{K} \times \mathcal{K}$, and a maximal isotropic subspace, or Göpel group, has dimension 2 (containing 4 points, as $2^2 = 4$).

Let us explain the construction of Göpel groups in more detail: For the Jacobian $\mathcal{A} = \text{Jac}(\mathcal{X})$ of a genus-two curve \mathcal{X} , every nontrivial 2-torsion point is a difference of Weierstrass points $P_i \in \mathcal{X}$ for $1 \leq i \leq 6$. In fact, the sixteen order-two points of \mathcal{A} are obtained using the embedding of the curve into the connected component of the identity in the Picard group, i.e., $\mathcal{X} \hookrightarrow \text{Jac}(\mathcal{X}) \cong \text{Pic}^0(\mathcal{X})$. We obtain the 15 elements $P_{ij} = [P_i + P_j - 2P_6] \in \mathcal{A}[2]$ with $1 \leq i < j \leq 6$ and set $P_0 = P_{66} = [0]$. For $\{i, j, k, l, m, n\} = \{1, \dots, 6\}$, the group law on $\mathcal{A}[2]$ is given by the relations

$$(17) \quad P_0 + P_{ij} = P_{ij}, \quad P_{ij} + P_{ij} = P_0, \quad P_{ij} + P_{kl} = P_{mn}, \quad P_{ij} + P_{jk} = P_{ik}.$$

The space $\mathcal{A}[2]$ of two-torsion points admits a symplectic bilinear form, the aforementioned Weil pairing such that the two-dimensional, maximal isotropic subspace

of $\mathcal{A}[2]$ with respect to the Weil pairing are the Göpel groups. It is then easy to check that there are exactly 15 inequivalent Göpel groups, and they are of the form

$$(18) \quad \{P_0, P_{ij}, P_{kl}, P_{mn}\}$$

such that $\{i, j, k, l, m, n\} = \{1, \dots, 6\}$.

The standard theta divisor $\Theta = \Theta_6 = \{[P - P_6] \mid P \in \mathcal{X}\}$ contains the six order-two points P_0, P_{i6} for $1 \leq i \leq 5$. Likewise for $1 \leq i \leq 5$, the five translates $\Theta_i = P_{i6} + \Theta$ contain P_0, P_{i6}, P_{ij} with $j \neq i, 6$, and the ten translates $\Theta_{ij6} = P_{ij} + \Theta$ for $1 \leq i < j \leq 5$ contain $P_{ij}, P_{i6}, P_{j6}, P_{kl}$ with $k, l \neq i, j, 6$ and $k < l$. Conversely, each order-two point lies on exactly six of the divisors, namely

$$(19) \quad P_0 \in \Theta_i \quad \text{for } i = 1, \dots, 6,$$

$$(20) \quad P_{i6} \in \Theta_i, \Theta_6, \Theta_{ij6} \quad \text{for } i = 1, \dots, 5 \text{ with } j \neq i, 6,$$

$$(21) \quad P_{ij} \in \Theta_i, \Theta_j, \Theta_{kl6} \quad \text{for } 1 \leq i < j \leq 5 \text{ with } k, l \neq i, j, 6 \text{ and } k < l.$$

Hence, we have a configuration of sixteen elements $P_0, P_{ij} \in \mathcal{A}[2]$ and sixteen theta divisors $\Theta, \Theta_i, \Theta_{ijk}$, where each theta divisor contains six order-two points, and where each order-two point is contained in six theta divisors. This configuration is called *the 16₆ configuration on the abelian surface*.

Moreover, we call the divisors $\{\Theta_i\}$ and $\{\Theta_{jk6}\}$ with $1 \leq i \leq 6$ and $1 \leq j < k < 6$, the six *odd* and the ten *even* theta divisors, respectively. In this way, the odd theta divisors are the six translates of the curve \mathcal{X} by P_{i6} with $1 \leq i \leq 6$, and thus with the six Weierstrass points P_i on the curve \mathcal{X} . Furthermore, there is a one-to-one correspondence between pairs of odd theta divisors and two-torsion points on $\mathcal{A}[2]$ since $\Theta_i \cap \Theta_j = \{P_0, P_{ij}\}$, and, in turn, unordered pairs $\{P_i, P_j\}$ of Weierstrass points since $P_{ij} = P_{i6} + P_{j6}$.

6.3. Richelot Isogenies. Richelot isogenies provide a classical framework for studying (2,2)-isogenies between principally polarized abelian surfaces, particularly Jacobians of genus 2 curves. Note that the abelian surfaces are here in general *not* split. It is well-known that the quotient $\hat{\mathcal{A}} = \mathcal{A}/\mathcal{K}$ by a Göpel group \mathcal{K} is again a principally polarized abelian surface, as detailed in [16, Sec. 23]. The natural projection $\Psi: \mathcal{A} \rightarrow \hat{\mathcal{A}}$ is an isogeny with kernel \mathcal{K} , called a *(2,2)-isogeny* because $\deg \Psi = |\mathcal{K}| = 4 = 2^2$, reflecting a kernel of rank 2 over $\mathbb{Z}/2\mathbb{Z}$.

Analytically, over \mathbb{C} , if $\mathcal{A} = \mathbb{C}^2/\Lambda$ with $\Lambda = \mathbb{Z}^2 \oplus \tau\mathbb{Z}^2$ and $\tau \in \mathbb{H}_2$, a Göpel group $\mathcal{K} \subset \mathcal{A}[2]$ corresponds to a 2-dimensional subspace of $\frac{1}{2}\Lambda/\Lambda$. The quotient $\hat{\mathcal{A}} = \mathcal{A}/\mathcal{K}$ can be represented as $\mathbb{C}^2/\hat{\Lambda}$, where $\hat{\Lambda} = \mathbb{Z}^2 \oplus 2\tau\mathbb{Z}^2$, adjusting the lattice to double the period in one direction. The isogeny is then

$$(22) \quad \begin{aligned} \Psi: \quad \mathcal{A} = \mathbb{C}^2 / \langle \mathbb{Z}^2 \oplus \tau\mathbb{Z}^2 \rangle &\rightarrow \hat{\mathcal{A}} = \mathbb{C}^2 / \langle \mathbb{Z}^2 \oplus 2\tau\mathbb{Z}^2 \rangle \\ (z, \tau) &\mapsto (z, 2\tau), \end{aligned}$$

mapping points modulo the coarser lattice, with kernel \mathcal{K} generated by representatives of $\mathcal{A}[2]$ spanning a rank-2 subgroup.

Consider two maximal isotropic subgroups $\mathcal{K}, \mathcal{K}' \subset \mathcal{A}[2]$ such that $\mathcal{K} + \mathcal{K}' = \mathcal{A}[2]$ and $\mathcal{K} \cap \mathcal{K}' = \{P_0\}$, where P_0 is the identity. Set $\hat{\mathcal{A}} = \mathcal{A}/\mathcal{K}$, and let $\hat{\mathcal{K}}$ be the image of \mathcal{K}' in $\hat{\mathcal{A}}$ under the quotient map $\Psi: \mathcal{A} \rightarrow \hat{\mathcal{A}}$. Since $|\mathcal{K}| = 4$ and $|\mathcal{K}'| = 4$, with intersection of size 1, we have $|\mathcal{K} + \mathcal{K}'| = |\mathcal{K}| \cdot |\mathcal{K}'| / |\mathcal{K} \cap \mathcal{K}'| = 4 \cdot 4 / 1 = 16 = |\mathcal{A}[2]|$, confirming $\mathcal{K} + \mathcal{K}' = \mathcal{A}[2]$. The quotient $\hat{\mathcal{A}}/\hat{\mathcal{K}}$ is isomorphic to \mathcal{A} , and the composition $\hat{\Psi} \circ \Psi: \mathcal{A} \rightarrow \hat{\mathcal{A}} \rightarrow \mathcal{A}$, where $\hat{\Psi}: \hat{\mathcal{A}} \rightarrow \hat{\mathcal{A}}/\hat{\mathcal{K}}$, is multiplication by 2

on \mathcal{A} , i.e., $(z, \tau) \mapsto (2z, \tau)$. To verify, note that $\ker(\Psi) = \mathcal{K}$, and $\ker(\hat{\Psi}) = \hat{\mathcal{K}}$, so $\ker(\hat{\Psi} \circ \Psi)$ includes all points mapping to $\hat{\mathcal{K}}$ under Ψ , which is $\mathcal{K} + \mathcal{K}' = \mathcal{A}[2]$, as $\Psi^{-1}(\hat{\mathcal{K}}) = \mathcal{K}'$. Thus, $\deg(\hat{\Psi} \circ \Psi) = |\mathcal{A}[2]| = 16$, and since $[2]$ has degree $2^{2g} = 16$ for $g = 2$, the isogenies compose to $[2]$.

For $\mathcal{A} = \text{Jac}(\mathcal{X})$, where \mathcal{X} is a smooth genus 2 curve, we explore whether $\hat{\mathcal{A}} = \text{Jac}(\hat{\mathcal{X}})$ for another genus 2 curve $\hat{\mathcal{X}}$, and how their moduli relate. Richelot addressed this geometrically in [17], with modern treatments in [18]. Over \mathbb{C} , $\mathcal{A}[2]$ has $2^{2g} = 16$ points, and there are 15 Göpel groups (computed as the number of 2-dimensional isotropic subspaces in $(\mathbb{Z}/2\mathbb{Z})^4$ under the symplectic form induced by the Weil pairing). Each corresponds to a (2,2)-isogeny, and Richelot's construction identifies $\hat{\mathcal{X}}$ explicitly. Given \mathcal{X} with equation $Y^2 = f_6(X, Z)$, a sextic in homogeneous coordinates, any factorization $f_6 = A \cdot B \cdot C$ into three quadratic polynomials A, B, C defines a curve $\hat{\mathcal{X}}$ via

$$(23) \quad \Delta_{ABC} \cdot Y^2 = [A, B][A, C][B, C],$$

where $[A, B] = A'B - AB'$ with $A' = \frac{dA}{dx}$ (assuming a dehomogenized coordinate $x = X/Z$), and Δ_{ABC} is the determinant of the coefficients of A, B, C in the basis $\{x^2, xz, z^2\}$. It was shown in [18] that $\text{Jac}(\mathcal{X})$ and $\text{Jac}(\hat{\mathcal{X}})$ are (2,2)-isogenous, and there are exactly 15 such factorizations (corresponding to partitions of 6 roots into 3 pairs), yielding all distinct (2,2)-isogenous principally polarized abelian surfaces to $\text{Jac}(\mathcal{X})$.

The geometric insight stems from the isomorphism $S_6 \cong \text{Sp}(4, \mathbb{F}_2)$, where S_6 permutes the 6 Weierstrass points of \mathcal{X} (or theta divisors containing a fixed 2-torsion point), and $\text{Sp}(4, \mathbb{F}_2)$ acts on $\mathcal{A}[2]$. As explained above, each Göpel group corresponds to a choice of pairing the Weierstrass points, inducing precisely the 15 Richelot isogenies. For \mathcal{X} in Rosenhain form

$$(24) \quad \mathcal{X}: \quad y^2 = xz(x-z)(x-\lambda_1z)(x-\lambda_2z)(x-\lambda_3z),$$

with roots at $0, 1, \lambda_1, \lambda_2, \lambda_3, \infty$, a factorization groups these into pairs, and (23) produces $\hat{\mathcal{X}}$.

6.3.1. An explicit model using theta constants. To compute these isogenies explicitly, we adopt a theta function approach, following [19]. For $\mathcal{A} = \text{Jac}(\mathcal{X})$, consider Göpel groups $\mathcal{K} = \{P_0, P_{15}, P_{23}, P_{46}\}$ and $\mathcal{K}' = \{P_0, P_{12}, P_{34}, P_{56}\}$, where $\mathcal{A}[2] = \{P_{ij}\}_{i < j}$ labels the 2-torsion points, with $P_0 = P_{66}$ the identity. These satisfy $\mathcal{K} + \mathcal{K}' = \mathcal{A}[2]$ and $\mathcal{K} \cap \mathcal{K}' = \{P_0\}$, as $|\mathcal{K} + \mathcal{K}'| = 4 \cdot 4 / 1 = 16$. Set $\hat{\mathcal{A}} = \mathcal{A}/\mathcal{K}$, and let $\hat{\mathcal{K}}$ be the image of \mathcal{K}' in $\hat{\mathcal{A}}$. We aim to relate the Rosenhain roots of \mathcal{X} :

$$(25) \quad \mathcal{X}: \quad y^2 = xz(x-z)(x-\lambda_1z)(x-\lambda_2z)(x-\lambda_3z),$$

where $\lambda_4 = 0, \lambda_5 = 1, \lambda_6 = \infty$, to those of $\hat{\mathcal{X}}$:

$$(26) \quad \hat{\mathcal{X}}: \quad y^2 = x(x-1)(x-\Lambda_1)(x-\Lambda_2)(x-\Lambda_3).$$

Theta functions provide coordinates on $\text{Jac}(\mathcal{X})$ and $\text{Jac}(\hat{\mathcal{X}})$. For a period matrix $\tau \in \mathbb{H}_2$, the values of the level 2 theta functions $\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau/2)$, with $a, b \in (\mathbb{Z}/2\mathbb{Z})^2$ at $z = 0$, called *theta constants*, determine the moduli. Denote $\theta_i = \theta \begin{bmatrix} a_i \\ b_i \end{bmatrix} (0, \tau/2)$ for \mathcal{X} and $\Theta_i = \theta \begin{bmatrix} b_i \\ a_i \end{bmatrix} (0, \tau)$ for $\hat{\mathcal{X}}$, with characteristics forming Göpel groups. For $\mathcal{K} = \{P_0, P_{15}, P_{23}, P_{46}\}$, corresponding to

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

we label $\theta_1, \theta_2, \theta_3, \theta_4$. The isogeny $\Psi : \text{Jac}(\mathcal{X}) \rightarrow \text{Jac}(\hat{\mathcal{X}})$ modifies the lattice, and the dual theta constants Θ_i for $\hat{\mathcal{X}}$ relate to θ_i via the isogeny's action. Results in [19] and [20] give

$$(27) \quad \Lambda_1 = \frac{\Theta_1^2 \Theta_3^2}{\Theta_2^2 \Theta_4^2}, \quad \Lambda_2 = \frac{\Theta_3^2 \Theta_8^2}{\Theta_4^2 \Theta_{10}^2}, \quad \Lambda_3 = \frac{\Theta_1^2 \Theta_8^2}{\Theta_2^2 \Theta_{10}^2},$$

though we refine this with a Göpel quartet $\{\Theta_1, \Theta_2, \Theta_3, \Theta_4\}$ for consistency.

The Richelot isogeny corresponds to factoring $f_6 = xz(x-z)(x-\lambda_1z)(x-\lambda_2z)(x-\lambda_3z)$ into

$$A = (x - \lambda_1z)(x - z), \quad B = (x - \lambda_2z)(x - \lambda_3z), \quad C = x(x - \infty z),$$

adjusting for homogeneity (e.g., $C = xz$ at infinity). Applying (23), we compute $\hat{\mathcal{X}}$ and its Igusa invariants, which are rational functions of $\{\theta_1, \theta_2, \theta_3, \theta_4\}$. A quadratic twist $\hat{\mathcal{X}}^{(\mu)}$ with

$$\mu = \frac{(\theta_1\theta_2 - \theta_3\theta_4)^2(\theta_1^2 + \theta_2^2 - \theta_3^2 - \theta_4^2)(\theta_1^2 - \theta_2^2 + \theta_3^2 - \theta_4^2)}{4\theta_1\theta_2\theta_3\theta_4(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2)(\theta_1^2 - \theta_2^2 - \theta_3^2 + \theta_4^2)}$$

adjusts the roots to

$$(28) \quad \begin{aligned} \Lambda_1 &= \frac{(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2)(\theta_1^2 - \theta_2^2 - \theta_3^2 + \theta_4^2)}{(\theta_1^2 + \theta_2^2 - \theta_3^2 - \theta_4^2)(\theta_1^2 - \theta_2^2 + \theta_3^2 - \theta_4^2)}, \\ \Lambda_2 &= \frac{(\theta_1^2 - \theta_2^2 - \theta_3^2 + \theta_4^2)(\theta_1^2\theta_2^2 + \theta_3^2\theta_4^2 + 2\theta_1\theta_2\theta_3\theta_4)}{(\theta_1^2 - \theta_2^2 + \theta_3^2 - \theta_4^2)(\theta_1^2\theta_2^2 - \theta_3^2\theta_4^2)}, \\ \Lambda_3 &= \frac{(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2)(\theta_1^2\theta_2^2 + \theta_3^2\theta_4^2 + 2\theta_1\theta_2\theta_3\theta_4)}{(\theta_1^2 + \theta_2^2 - \theta_3^2 - \theta_4^2)(\theta_1^2\theta_2^2 - \theta_3^2\theta_4^2)}, \end{aligned}$$

matching the Richelot construction's invariants, verifying isomorphism.

For $\mathcal{K}' = \{P_0, P_{12}, P_{34}, P_{56}\}$, the dual isogeny $\hat{\Psi} : \hat{\mathcal{A}} \rightarrow \mathcal{A} = \hat{\mathcal{A}}/\mathcal{K}'$ uses $\hat{A} = [B, C]$, $\hat{B} = [A, C]$, $\hat{C} = [A, B]$, reconstructing \mathcal{X} . New moduli

$$\lambda'_1 = \frac{\lambda_1 + \lambda_2\lambda_3}{l}, \quad \lambda'_2 = \frac{\lambda_2 + \lambda_1\lambda_3}{l}, \quad \lambda'_3 = \frac{\lambda_3 + \lambda_1\lambda_2}{l},$$

with $l^2 = \lambda_1\lambda_2\lambda_3$, and similarly for Λ'_i , relate symmetrically, as shown in [20].

Proposition 1. *The moduli of \mathcal{X} in (24) and $\hat{\mathcal{X}}$ in (26) satisfy*

$$(29) \quad \begin{aligned} \Lambda'_1 &= 2 \frac{2\lambda'_1 - \lambda'_2 - \lambda'_3}{\lambda'_2 - \lambda'_3}, & \lambda'_1 &= 2 \frac{2\Lambda'_1 - \Lambda'_2 - \Lambda'_3}{\Lambda'_2 - \Lambda'_3}, \\ \Lambda'_2 - \Lambda'_1 &= -\frac{4(\lambda'_1 - \lambda'_2)(\lambda'_1 - \lambda'_3)}{(\lambda'_1 + 2)(\lambda'_2 - \lambda'_3)}, & \lambda'_2 - \lambda'_1 &= -\frac{4(\Lambda'_1 - \Lambda'_2)(\Lambda'_1 - \Lambda'_3)}{(\Lambda'_1 + 2)(\Lambda'_2 - \Lambda'_3)}, \\ \Lambda'_3 - \Lambda'_1 &= -\frac{4(\lambda'_1 - \lambda'_2)(\lambda'_1 - \lambda'_3)}{(\lambda'_1 - 2)(\lambda'_2 - \lambda'_3)}, & \lambda'_3 - \lambda'_1 &= -\frac{4(\Lambda'_1 - \Lambda'_2)(\Lambda'_1 - \Lambda'_3)}{(\Lambda'_1 - 2)(\Lambda'_2 - \Lambda'_3)}. \end{aligned}$$

Hence, there is a Richelot isogeny realizing the (2, 2)-isogeny

$$(30) \quad \Psi : \mathcal{A} = \text{Jac}(\mathcal{X}) \longrightarrow \hat{\mathcal{A}} = \text{Jac}(\hat{\mathcal{X}}) = \mathcal{A}/\mathcal{K},$$

for the maximal isotropic subgroup \mathcal{K} .

7. KUMMER SURFACES

Given an abelian surface \mathcal{A} over a field k , the (singular) Kummer surface \mathcal{K} is defined as the quotient $\mathcal{A}/\langle -\mathbb{I} \rangle$, where the involution $-\mathbb{I}: \mathcal{A} \rightarrow \mathcal{A}$ acts by $P \mapsto -P$. The quotient $\text{Jac}(\mathcal{X})/\langle -\mathbb{I} \rangle$ is a singular algebraic variety of dimension 2 with 16 ordinary double points, each corresponding to a 2-torsion point in $\mathcal{A}[2] = \{P \in \mathcal{A}(\bar{k}) \mid 2P = 0\}$, the set of which has cardinality $2^{2 \cdot 2} = 16$ over an algebraically closed field.

The quotient construction of \mathcal{K} leverages the group structure of \mathcal{A} : the involution $-\mathbb{I}$ is an automorphism of order two, and its fixed points, the 2-torsion points, map to singularities on \mathcal{K} . Each singularity is locally isomorphic to the quotient of \mathbb{C}^2 by the action $z \mapsto -z$, an A_1 singularity, characterized by a quadratic cone. The minimal resolution is denoted the *Kummer surface* $\text{Kum}(\mathcal{A})$ and is the smooth K3 surface, obtained by blowing up each double point by gluing in an exceptional (-2) -curve; see [21] and [22] for details. Conversely, there is a map $\text{Kum}(\mathcal{A}) \rightarrow \mathcal{K}$ contracting the (-2) curves.

7.1. Kummer surfaces associated with principal polarization. For an abelian surface \mathcal{A} equipped with a principal polarization, the level 2 theta functions induce a map into projective space \mathbb{P}^3 . Specifically, assume that \mathcal{A} is not a product of elliptic curves, if $\mathcal{A} = \mathbb{C}^2/\Lambda$ with a period matrix $\tau \in \mathbb{H}_2$, the functions $\varphi_2(z) = \left(\theta \left[\begin{smallmatrix} 0 \\ i/2 \end{smallmatrix} \right] (z, \tau/2)\right)_{i \in (\mathbb{Z}/2\mathbb{Z})^2}$ satisfy $\varphi_2(z) = \varphi_2(-z)$, defining a morphism $\text{Kum}(\mathcal{A}) \rightarrow \mathbb{P}^3$; see [23, Theorem 4.8.1]. We have the following:

Lemma 6. *Let \mathcal{A} be a principally polarized abelian surface over \mathbb{C} , not isomorphic to a product of elliptic curves. The map $\varphi_2: \text{Kum}(\mathcal{A}) \rightarrow \mathbb{P}^3$ defined by $\varphi_2(z) = \left(\theta \left[\begin{smallmatrix} 0 \\ i/2 \end{smallmatrix} \right] (z, \tau/2)\right)_{i \in (\mathbb{Z}/2\mathbb{Z})^2}$ is an embedding.*

Proof. The theta functions $\theta_i(z) = \theta \left[\begin{smallmatrix} 0 \\ i/2 \end{smallmatrix} \right] (z, \tau/2)$ for $i \in (\mathbb{Z}/2\mathbb{Z})^2$ are even, satisfying $\theta_i(-z) = \theta_i(z)$ due to the characteristic's symmetry under the involution ι . Thus, $\varphi_2: \mathcal{A} \rightarrow \mathbb{P}^3$ factors through the quotient $\pi: \mathcal{A} \rightarrow \text{Kum}(\mathcal{A})$, inducing a well-defined map $\overline{\varphi}_2: \text{Kum}(\mathcal{A}) \rightarrow \mathbb{P}^3$. For \mathcal{A} principally polarized, the line bundle \mathcal{L}_0^2 corresponds to 2Θ , where Θ is the theta divisor. The space of sections $\Gamma(\mathcal{A}, \mathcal{L}_0^2)$ is 4-dimensional, spanned by the θ_i . If \mathcal{A} is not a product $E_1 \times E_2$, the polarization ensures \mathcal{L}_0^2 is very ample on $\text{Kum}(\mathcal{A})$, separating points and tangent vectors. Specifically, for distinct points $x, y \in \text{Kum}(\mathcal{A})$ (not both in $\mathcal{A}[2]$), there exists i such that $\theta_i(x) \neq \theta_i(y)$, and for a point x with tangent direction v , some θ_i has non-zero derivative along v . Thus, $\overline{\varphi}_2$ embeds $\text{Kum}(\mathcal{A})$ as a quartic surface with 16 nodes at the images of $\mathcal{A}[2]$. \square

Considering the principally polarized abelian surface $\mathcal{A} = \text{Jac}(\mathcal{X})$, not isomorphic to a product of elliptic curves, with the standard theta divisor $\Theta \cong [\mathcal{X}]$, the morphism is an embedding and its image is a quartic surface in \mathbb{P}^3 with theta constants determining its equation. The quartic nature of the image reflects the degree of the line bundle \mathcal{L}_0^2 associated with the doubled principal polarization. The image of each two-torsion point is a singular point on the Kummer surface \mathcal{K} and called a *node*. That is, the nodes P_{ij} are the images of the two-torsion points $P_{ij} \in \mathcal{A}[2]$. Similarly, any theta divisor is mapped to the intersection of the singular Kummer surface with a plane. We call such a singular plane a *trope*. Hence, we have a configuration of sixteen nodes and sixteen tropes, where each contains

six nodes, and such that the intersection of each two is along two nodes. This configuration is called the 16_6 configuration on the Kummer surface.

7.1.1. *Kummer surfaces associated with odd theta characteristics.* The Jacobian $\text{Jac}(\mathcal{X})$ of a smooth genus two curve is birational to the symmetric product $\text{Sym}^2(\mathcal{X})$. Let us consider the function field of $\text{Sym}^2(\mathcal{X}) = (\mathcal{X} \times \mathcal{X})/\langle\sigma\rangle$ where σ interchanges two copies of \mathcal{X} . For a smooth genus-two curve \mathcal{X} in Rosenhain form (24), the function field of the variety $\text{Sym}^2(\mathcal{X})/\langle\iota \times \iota\rangle$ – where $\iota \times \iota$ is the involution on $\text{Sym}^2(\mathcal{X})$ induced by the hyperelliptic involution ι on \mathcal{X} – is generated by $z_1 = z^{(1)}z^{(2)}$, $z_2 = x^{(1)}z^{(2)} + x^{(2)}z^{(1)}$, $z_3 = x^{(1)}x^{(2)}$, and $\tilde{z}_4 = y^{(1)}y^{(2)}$, subject to the relation

$$(31) \quad \mathcal{W}: \quad \tilde{z}_4^2 = z_1 z_3 (z_1 - z_2 + z_3) \prod_{i=1}^3 (\lambda_i^2 z_1 - \lambda_i z_2 + z_3).$$

Equation (31) is a special case of a *double sextic surface*, i.e., the double cover of $\mathbb{P}^2 = \mathbb{P}(z_1, z_2, z_3)$ branched on the union of six lines (and hence over a sextic curve). The minimal resolution of a double sextic surface is always a K3 surface; see [24]. Equation (31) is known as *Shioda sextic* associated with $\text{Jac}(\mathcal{X})$; see [25]. It follows that the minimal resolution of \mathcal{W} is isomorphic to the Kummer surface $\text{Kum}(\text{Jac} \mathcal{X})$.

In Equation (31) the double cover of \mathbb{P}^2 is branched along the six lines \mathbb{T}_i with $1 \leq i \leq 6$, given by

$$(32) \quad \lambda_i^2 z_1 - \lambda_i z_2 + z_3 = 0 \text{ with } 1 \leq i \leq 3, \quad z_1 = 0, \quad z_1 - z_2 + z_3 = 0, \quad z_3 = 0.$$

These six lines are tangent to the common conic $K_2 = z_2^2 - 4z_1z_3 = 0$. Conversely, it is easy to see that any six lines tangent to a common conic can always be brought into the form of Equations (32) using a projective transformation. Humbert proved that the Kummer plane $(\mathbb{P}^2; \mathbb{T}_1, \dots, \mathbb{T}_6)$ inherits essential information of the principally polarized abelian surface $\mathcal{A} = \text{Jac}(\mathcal{X})$ itself; see [26].

The Shioda sextic is closely related to two quartic equations, known as the *Baker quartic* and *Cassels-Flynn quartic*. The Baker quartic is obtained directly from the Shioda sextic \mathcal{W} in Equation (32), using parameters

$$(33) \quad \begin{aligned} L_4 &= 1 + \lambda_1 + \lambda_2 + \lambda_3, & L_3 &= \lambda_1 + \lambda_2 + \lambda_3 + \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_1\lambda_3, \\ L_1 &= \lambda_1\lambda_2\lambda_3, & L_2 &= \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_1\lambda_3 + \lambda_1\lambda_2\lambda_3, \end{aligned}$$

and a variable transformation given by

$$(34) \quad \begin{aligned} \mathbf{W} &= K_2 z_1, & \mathbf{X} &= K_2 z_2, & \mathbf{Y} &= K_2 z_3, \\ \mathbf{Z} &= 2\tilde{z}_4 - (L_1 z_1^2 z_2 - 2L_2 z_1^2 z_3 + L_3 z_1 z_2 z_3 - 2L_4 z_1 z_3^2 + z_2 z_3^2). \end{aligned}$$

Equation (31) is then equivalent to the quartic surface \mathcal{U} in $\mathbb{P}^3 = \mathbb{P}(\mathbf{W}, \mathbf{X}, \mathbf{Y}, \mathbf{Z})$ given by the vanishing locus of the *Baker determinant*, i.e.,

$$(35) \quad \mathcal{U}: \quad \begin{vmatrix} 0 & L_1 \mathbf{W} & -\mathbf{Z} & \mathbf{Y} \\ L_1 \mathbf{W} & 2L_2 \mathbf{W} + 2\mathbf{Z} & L_3 \mathbf{W} - \mathbf{Y} & \mathbf{X} \\ -\mathbf{Z} & L_3 \mathbf{W} - \mathbf{Y} & 2L_4 \mathbf{W} - 2\mathbf{X} & \mathbf{W} \\ \mathbf{Y} & \mathbf{X} & \mathbf{W} & 0 \end{vmatrix} = 0.$$

The Baker determinant was first derived in [27].

In addition to K_2 introduced above, we also define homogeneous polynomials $K_l = K_l(z_1, z_2, z_3)$ of degree $4 - l$ for $l = 0, 1$ with

$$(36) \quad \begin{aligned} K_2 &= z_2^2 - 4z_1z_3, & K_1 &= -2z_2z_3^2 - 2L_1z_1^2z_2 + 4L_2z_1^2z_3 - 2L_3z_1z_2z_3 + 4L_4z_1z_3^2, \\ K_0 &= L_1^2z_1^4 - 2L_1L_3z_1^3z_3 + (2L_1 - 4L_2L_4 + L_3^2)z_1^2z_3^2 + 4L_1L_4z_1^2z_2z_3 \\ &\quad + 3(-2L_1z_2^2z_3 + 2L_2z_2z_3^2 - L_3z_3^3)z_1 + z_3^4. \end{aligned}$$

A variable transformation in Equation (31), given by

$$(37) \quad \tilde{z}_4 = \frac{1}{4}(K_2z_4 + 2K_1),$$

or, equivalently, the variable transformation in Equation (35), given by

$$(38) \quad \mathbf{W} = K_2 z_1, \quad \mathbf{X} = K_2 z_2, \quad \mathbf{Y} = K_2 z_3, \quad \mathbf{Z} = K_2 z_4 + K_1,$$

yields the quartic projective surface \mathcal{K} in $\mathbb{P}^3 = \mathbb{P}(z_1, z_2, z_3, z_4)$ given by

$$(39) \quad \mathcal{K}: \quad K_2(z_1, z_2, z_3) z_4^2 + K_1(z_1, z_2, z_3) z_4 + K_0(z_1, z_2, z_3) = 0.$$

The quartic appeared in Cassels and Flynn [28, Sec. 3] and is called the *Cassels-Flynn quartic*. In summary, for the principally polarized abelian surface \mathcal{A} with the standard Theta divisor $\Theta \cong [\mathcal{X}]$ and polarizing line bundle $\mathcal{L} = \mathcal{O}_{\mathcal{A}}(\Theta)$ we have the following; see [29]:

Proposition 2. *Assume that $\lambda_1, \lambda_2, \lambda_3$ are the Rosenhain roots of a smooth genus-two curve \mathcal{X} . The surfaces in Equations (31), (35), and (7.2) are birational equivalent over $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$. The minimal resolution is isomorphic to the Kummer surface $\text{Kum}(\mathcal{A})$ associated with $(\mathcal{A} = \text{Jac}(\mathcal{X}), \mathcal{L} = \mathcal{O}_{\mathcal{A}}(\Theta))$.*

In the complete linear system $|2\Theta|$ on $\text{Jac}(\mathcal{X})$, the odd symmetric Theta divisors Θ_i on $\text{Jac}(\mathcal{X})$ are mapped to six tropes \mathbb{T}_i in Equation (32). For a given integer i with $1 \leq i \leq 5$, the nodes P_0 and P_{ij} or P_{ji} all lie on the plane \mathbb{T}_i . In [20] it was shown that Thomae's formula then provides an explicit relation between the odd tropes and the odd theta functions of genus two:

Remark 1. *There is a unique bijection between the six tropes $\mathbb{T}_1, \dots, \mathbb{T}_6$, i.e., the images of the odd symmetric theta divisors Θ_i on $\text{Jac}(\mathcal{X})$, and the squares of the odd Theta functions $\theta_{11}^2(z), \dots, \theta_{16}^2(z)$ such that Equations (32) coincide with the Mumford relations for odd theta functions*

7.1.2. *Kummer surfaces associated with even theta characteristics.* We also give an algebraic description of a singular Kummer variety $\mathcal{A}/\langle -\mathbb{I} \rangle$ associated with a principally polarized abelian variety $(\mathcal{A}, \mathcal{L})$ associated with some even theta characteristics; see results in [23]. Let \mathcal{L} be the ample line symmetric bundle of an abelian surface \mathcal{A} defining its principal polarization and consider the rational map $\varphi_{\mathcal{L}^2}: \mathcal{A} \rightarrow \mathbb{P}^3$ associated with the line bundle \mathcal{L}^2 . Its image $\varphi_{\mathcal{L}^2}(\mathcal{A})$ is a quartic surface in \mathbb{P}^3 which in projective coordinates $[w : x : y : z]$ can be written as

$$(40) \quad \begin{aligned} 0 &= \xi_0(w^4 + x^4 + y^4 + z^4) + \xi_4 wxyz \\ &\quad + \xi_1(w^2z^2 + x^2y^2) + \xi_2(w^2x^2 + y^2z^2) + \xi_3(w^2y^2 + x^2z^2), \end{aligned}$$

with $[\xi_0 : \xi_1 : \xi_2 : \xi_3 : \xi_4] \in \mathbb{P}^4$. Any general member of the family (40) is smooth. As soon as the surface is singular at a general point, it must have sixteen singular nodal points because of its symmetry. The discriminant turns out to be

a homogeneous polynomial of degree eighteen in the parameters $[\xi_0 : \xi_1 : \xi_2 : \xi_3 : \xi_4] \in \mathbb{P}^4$ and was determined in [23, Sec. 7.7 (3)]. Thus, the Kummer surfaces form an open set among the hypersurfaces in Equation (40) with parameters $[\xi_0 : \xi_1 : \xi_2 : \xi_3 : \xi_4] \in \mathbb{P}^4$, namely the ones that make the only irreducible factor of degree three in the discriminant vanish, i.e.,

$$(41) \quad \xi_0 (16\xi_0^2 - 4\xi_1^2 - 4\xi_2^2 - 4\xi_3^2 + \xi_4^2) + 4\xi_1\xi_2\xi_3 = 0.$$

Setting $\xi_0 = 1$ and using the affine moduli $\xi_1 = -A$, $\xi_2 = -B$, $\xi_3 = -C$, $\xi_4 = 2D$, we obtain the normal form of a nodal quartic surface. Thus, we say that a *Hudson quartic* is the surface in $\mathbb{P}^3(w, x, y, z)$ given by

$$(42) \quad \begin{aligned} 0 &= w^4 + x^4 + y^4 + z^4 + 2Dwxyz \\ &\quad - A(w^2z^2 + x^2y^2) - B(w^2x^2 + y^2z^2) - C(w^2y^2 + x^2z^2), \end{aligned}$$

where $A, B, C, D \in \mathbb{C}$ such that

$$(43) \quad D^2 = A^2 + B^2 + C^2 + ABC - 4.$$

The Hudson quartic in Equation (42) is invariant under the transformations changing signs of two coordinates, generated by

$$[w : x : y : z] \rightarrow [-w : -x : y : z], \quad [w : x : y : z] \rightarrow [-w : x : -y : z],$$

and under the permutations of variables, generated by $[w : x : y : z] \rightarrow [x : w : z : y]$ and $[w : x : y : z] \rightarrow [y : z : w : x]$.

A different quartic hypersurface equation is due to Kummer [30] and Borchardt [31]. We say that a *Göpel quartic* is the surface in $\mathbb{P}^3(P, Q, R, S)$ given by

$$(44) \quad \Phi^2 - 4\delta^2 SPQR = 0,$$

with

$$(45) \quad \Phi = P^2 + Q^2 + R^2 + S^2 - \alpha(PS + QR) - \beta(PQ + RS) - \gamma(PR + QS),$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ such that

$$(46) \quad \delta^2 = \alpha^2 + \beta^2 + \gamma^2 + \alpha\beta\gamma - 4.$$

We have the following:

Proposition 3. *The Hudson quartic in Equation (42) is isomorphic to the Göpel quartic in Equation (44), for suitable sets of parameters (A, B, C, D) satisfying Equation (43) and $(\alpha, \beta, \gamma, \delta)$ satisfying Equation (46). In particular, the quartic hypersurfaces are isomorphic to the singular Kummer variety associated with a principally polarized abelian surface $(\mathcal{A}, \mathcal{L})$.*

Proof. We first introduce complex numbers $[w_0 : x_0 : y_0 : z_0] \in \mathbb{P}^3$ such that

$$(47) \quad \begin{aligned} A &= \frac{w_0^4 - x_0^4 - y_0^4 + z_0^4}{w_0^2 z_0^2 - x_0^2 y_0^2}, \quad B = \frac{w_0^4 + x_0^4 - y_0^4 - z_0^4}{w_0^2 x_0^2 - y_0^2 z_0^2}, \quad C = \frac{w_0^4 - x_0^4 + y_0^4 - z_0^4}{w_0^2 y_0^2 - x_0^2 z_0^2}, \\ D &= \frac{w_0 x_0 y_0 z_0 \prod_{\epsilon, \epsilon' \in \{\pm 1\}} (w_0^2 + \epsilon x_0^2 + \epsilon' y_0^2 + \epsilon \epsilon' z_0^2)}{(w_0^2 z_0^2 - x_0^2 y_0^2)(w_0^2 x_0^2 - y_0^2 z_0^2)(w_0^2 y_0^2 - x_0^2 z_0^2)}, \end{aligned}$$

and

$$(48) \quad \alpha = 2 \frac{w_0^2 y_0^2 + x_0^2 z_0^2}{w_0^2 y_0^2 - x_0^2 z_0^2}, \quad \beta = 2 \frac{w_0^2 x_0^2 + y_0^2 z_0^2}{w_0^2 x_0^2 - y_0^2 z_0^2}, \quad \gamma = 2 \frac{w_0^2 z_0^2 + x_0^2 y_0^2}{w_0^2 z_0^2 - x_0^2 y_0^2},$$

$$\delta^2 = 16 \frac{w_0^4 x_0^4 y_0^4 z_0^4 \prod_{\epsilon, \epsilon' \in \{\pm 1\}} (w_0^2 + \epsilon x_0^2 + \epsilon' y_0^2 + \epsilon \epsilon' z_0^2)}{(w_0^2 y_0^2 - x_0^2 z_0^2)^2 (w_0^2 x_0^2 - y_0^2 z_0^2)^2 (w_0^2 z_0^2 - x_0^2 y_0^2)^2}.$$

Then, the linear transformation given by

$$(49) \quad \begin{aligned} P &= w_0 w + x_0 x + y_0 y + z_0 z, \\ Q &= w_0 w + x_0 x - y_0 y - z_0 z, \\ R &= w_0 w - x_0 x - y_0 y + z_0 z, \\ S &= w_0 w - x_0 x + y_0 y - z_0 z, \end{aligned}$$

transforms Equation (44) into Equation (42). \square

Lemma 7. *Using the same notation as in Equation (47), the sixteen nodes of the Hudson quartic (42) are given by*

$$\begin{aligned} &[w_0 : x_0 : y_0 : z_0], [-w_0 : -x_0 : y_0 : z_0], [-w_0 : x_0 : -y_0 : z_0], [-w_0 : x_0 : y_0 : -z_0], \\ &[x_0 : w_0 : z_0 : y_0], [-x_0 : -w_0 : z_0 : y_0], [-x_0 : w_0 : -z_0 : y_0], [-x_0 : w_0 : z_0 : -y_0], \\ &[y_0 : z_0 : w_0 : x_0], [-y_0 : -z_0 : w_0 : x_0], [-y_0 : z_0 : -w_0 : x_0], [-y_0 : z_0 : w_0 : -x_0], \\ &[z_0 : y_0 : x_0 : w_0], [-z_0 : -y_0 : x_0 : w_0], [-z_0 : y_0 : -x_0 : w_0], [-z_0 : y_0 : x_0 : -w_0]. \end{aligned}$$

In particular, for generic parameters (A, B, C, D) , no node is contained in the coordinate planes $w = 0$, $x = 0$, $y = 0$, or $z = 0$.

We also set

$$(50) \quad \begin{aligned} p_0^2 &= w_0^2 + x_0^2 + y_0^2 + z_0^2, & q_0^2 &= w_0^2 + x_0^2 - y_0^2 - z_0^2, \\ r_0^2 &= w_0^2 - x_0^2 + y_0^2 - z_0^2, & s_0^2 &= w_0^2 - x_0^2 - y_0^2 + z_0^2. \end{aligned}$$

We have the following:

Lemma 8. *The nodes of the Göpel quartic (44) are given by*

$$\begin{aligned} &[p_0^2 : q_0^2 : r_0^2 : s_0^2], [q_0^2 : p_0^2 : s_0^2 : r_0^2], [r_0^2 : s_0^2 : r_0^2 : q_0^2], [s_0^2 : r_0^2 : q_0^2 : p_0^2], \\ &[w_0 x_0 + y_0 z_0 : w_0 x_0 - y_0 z_0 : 0 : 0], [w_0 x_0 - y_0 z_0 : w_0 x_0 + y_0 z_0 : 0 : 0], \\ &[0 : 0 : w_0 x_0 + y_0 z_0 : w_0 x_0 - y_0 z_0], [0 : 0 : w_0 x_0 - y_0 z_0 : w_0 x_0 + y_0 z_0], \\ &[w_0 z_0 + x_0 y_0 : 0 : w_0 z_0 - x_0 y_0 : 0], [0 : w_0 z_0 + x_0 y_0 : 0 : w_0 z_0 - x_0 y_0], \\ &[w_0 z_0 - x_0 y_0 : 0 : w_0 z_0 + x_0 y_0 : 0], [0 : w_0 z_0 - x_0 y_0 : 0 : w_0 z_0 + x_0 y_0], \\ &[w_0 y_0 + x_0 z_0 : 0 : 0 : w_0 y_0 - x_0 z_0], [0 : w_0 y_0 + x_0 z_0 : w_0 y_0 - x_0 z_0 : 0], \\ &[0 : w_0 y_0 - x_0 z_0 : w_0 y_0 + x_0 z_0 : 0], [w_0 y_0 - x_0 z_0 : 0 : 0 : w_0 y_0 + x_0 z_0]. \end{aligned}$$

7.1.3. *An explicit model using Theta functions.* We provide an explicit model for the Göpel quartic in terms of Theta functions. We have the following:

Proposition 4. *For the surface in \mathbb{P}^3 given by Equation (44), the coordinates are given by*

$$(51) \quad [P : Q : R : S] = [\theta_1(z)^2 : \theta_2(z)^2 : \theta_3(z)^2 : \theta_4(z)^2],$$

and the moduli parameters are

$$(52) \quad \alpha = \frac{\theta_1^4 - \theta_2^4 - \theta_3^4 + \theta_4^4}{\theta_1^2 \theta_4^2 - \theta_2^2 \theta_3^2}, \quad \beta = \frac{\theta_1^4 + \theta_2^4 - \theta_3^4 - \theta_4^4}{\theta_1^2 \theta_2^2 - \theta_3^2 \theta_4^2}, \quad \gamma = \frac{\theta_1^4 - \theta_2^4 + \theta_3^4 - \theta_4^4}{\theta_1^2 \theta_3^2 - \theta_2^2 \theta_4^2},$$

$$\delta = \frac{\theta_1 \theta_2 \theta_3 \theta_4 \prod_{\epsilon, \epsilon' \in \{\pm 1\}} (\theta_1^2 + \epsilon \theta_2^2 + \epsilon' \theta_3^2 + \epsilon \epsilon' \theta_4^2)}{(\theta_1^2 \theta_2^2 - \theta_3^2 \theta_4^2) (\theta_1^2 \theta_3^2 - \theta_2^2 \theta_4^2) (\theta_1^2 \theta_4^2 - \theta_2^2 \theta_3^2)}.$$

Proof. A direct computation shows that the non-vanishing elliptic variables $[P : Q : R : S] = [\theta_1(z)^2 : \theta_2(z)^2 : \theta_3(z)^2 : \theta_4(z)^2]$ satisfy Equation (44), with

$$(53) \quad \alpha = 2 \frac{\Theta_1^2 \Theta_3^2 + \Theta_2^2 \Theta_4^2}{\Theta_1^2 \Theta_3^2 - \Theta_2^2 \Theta_4^2}, \quad \beta = 2 \frac{\Theta_1^2 \Theta_2^2 + \Theta_3^2 \Theta_4^2}{\Theta_1^2 \Theta_2^2 - \Theta_3^2 \Theta_4^2}, \quad \gamma = 2 \frac{\Theta_1^2 \Theta_4^2 + \Theta_2^2 \Theta_3^2}{\Theta_1^2 \Theta_4^2 - \Theta_2^2 \Theta_3^2}.$$

The moduli parameter can be re-written

$$(54) \quad \alpha = \frac{\theta_1^4 - \theta_2^4 - \theta_3^4 + \theta_4^4}{\theta_1^2 \theta_4^2 - \theta_2^2 \theta_3^2}, \quad \beta = \frac{\theta_1^4 + \theta_2^4 - \theta_3^4 - \theta_4^4}{\theta_1^2 \theta_2^2 - \theta_3^2 \theta_4^2}, \quad \gamma = \frac{\theta_1^4 - \theta_2^4 + \theta_3^4 - \theta_4^4}{\theta_1^2 \theta_3^2 - \theta_2^2 \theta_4^2}.$$

such that over $\mathcal{A}_2(4, 8)$ the modulus δ is given as

$$\delta = \frac{\theta_1 \theta_2 \theta_3 \theta_4 \prod_{\epsilon, \epsilon' \in \{\pm 1\}} (\theta_1^2 + \epsilon \theta_2^2 + \epsilon' \theta_3^2 + \epsilon \epsilon' \theta_4^2)}{(\theta_1^2 \theta_2^2 - \theta_3^2 \theta_4^2) (\theta_1^2 \theta_3^2 - \theta_2^2 \theta_4^2) (\theta_1^2 \theta_4^2 - \theta_2^2 \theta_3^2)}.$$

□

Remark 2. The transformation $[w : x : y : z] \rightarrow [-w : x : y : z]$ is an isomorphism between a Hudson quartic in Equation (42) with moduli (A, B, C, D) and the one with $(A, B, C, -D)$. Moreover, the two quartics coincide exactly along the coordinate planes $w = 0$, $x = 0$, $y = 0$, or $z = 0$.

We also provide an explicit model for the Hudson quartic in terms of Theta functions. In terms of Theta functions, the relation between Equation (42) and Equation (44) was first determined by Borchardt [31]. We have the following:

Proposition 5. The surface in \mathbb{P}^3 given by Equation (42) is isomorphic to the singular Kummer variety where the coordinates are given by

$$(55) \quad [w : x : y : z] = [\Theta_1(2z) : \Theta_2(2z) : \Theta_3(2z) : \Theta_4(2z)],$$

and the moduli parameters are

$$(56) \quad A = \frac{\Theta_1^4 - \Theta_2^4 - \Theta_3^4 + \Theta_4^4}{\Theta_1^2 \Theta_4^2 - \Theta_2^2 \Theta_3^2}, \quad B = \frac{\Theta_1^4 + \Theta_2^4 - \Theta_3^4 - \Theta_4^4}{\Theta_1^2 \Theta_2^2 - \Theta_3^2 \Theta_4^2}, \quad C = \frac{\Theta_1^4 - \Theta_2^4 + \Theta_3^4 - \Theta_4^4}{\Theta_1^2 \Theta_3^2 - \Theta_2^2 \Theta_4^2},$$

$$D = \frac{\Theta_1 \Theta_2 \Theta_3 \Theta_4 \prod_{\epsilon, \epsilon' \in \{\pm 1\}} (\Theta_1^2 + \epsilon \Theta_2^2 + \epsilon' \Theta_3^2 + \epsilon \epsilon' \Theta_4^2)}{(\Theta_1^2 \Theta_2^2 - \Theta_3^2 \Theta_4^2) (\Theta_1^2 \Theta_3^2 - \Theta_2^2 \Theta_4^2) (\Theta_1^2 \Theta_4^2 - \Theta_2^2 \Theta_3^2)}.$$

Proof. Comparing Equations (53) and (48), we find a solution in terms of Theta function given by

$$(57) \quad [w_0 : x_0 : y_0 : z_0] = [\Theta_1 : \Theta_2 : \Theta_3 : \Theta_4].$$

Equations (49) are equivalent to

$$(58) \quad \begin{aligned} \theta_1^2(z) &= \Theta_1 \Theta_1(2z) + \Theta_2 \Theta_2(2z) + \Theta_3 \Theta_3(2z) + \Theta_4 \Theta_4(2z), \\ \theta_2^2(z) &= \Theta_1 \Theta_1(2z) + \Theta_2 \Theta_2(2z) - \Theta_3 \Theta_3(2z) - \Theta_4 \Theta_4(2z), \\ \theta_3^2(z) &= \Theta_1 \Theta_1(2z) - \Theta_2 \Theta_2(2z) - \Theta_3 \Theta_3(2z) + \Theta_4 \Theta_4(2z), \\ \theta_4^2(z) &= \Theta_1 \Theta_1(2z) - \Theta_2 \Theta_2(2z) + \Theta_3 \Theta_3(2z) - \Theta_4 \Theta_4(2z). \end{aligned}$$

Comparing Equations (49) with Equations (58), the coordinates can be expressed in terms of Theta functions with non-vanishing elliptic arguments as

$$[w : x : y : z] = [\Theta_1(2z) : \Theta_2(2z) : \Theta_3(2z) : \Theta_4(2z)].$$

□

The map $\pi : \mathbb{P}(w, x, y, z) \rightarrow \mathbb{P}(P, Q, R, S)$ with $P = w^2, \dots, S = z^2$ is 8 : 1 outside the coordinate planes. The map π induces a covering of a reducible octic surface in \mathbb{P}^3 given by

$$(59) \quad (\Psi - 2Dwxyz) (\Psi + 2Dwxyz) = 0,$$

with

$$\Psi = w^4 + x^4 + y^4 + z^4 - A(w^2y^2 + y^2z^2) - B(w^2z^2 + x^2y^2) - C(w^2x^2 + y^2z^2),$$

onto the Göpel quartic in Equation (44) with $\alpha = A, \beta = B, C = \gamma$, and $D = \delta$. We can assume that the Hudson quartic and Göpel quartic are the singular Kummer varieties associated with two principally polarized abelian varieties, say \mathcal{A} and $\hat{\mathcal{A}}$, respectively. We have the following:

Proposition 6. *The map $\pi : \mathbb{P}(w, x, y, z) \rightarrow \mathbb{P}(P, Q, R, S)$ with $P = w^2, \dots, S = z^2$ restricted to the Hudson quartic onto the Göpel quartic with $\alpha = A, \beta = B, C = \gamma$, and $D = \delta$, is induced by a (2, 2)-isogeny $\Psi : \mathcal{A} \rightarrow \hat{\mathcal{A}}$.*

Proof. The rational map π is 4:1 from the Hudson quartic onto the Göpel quartic. The map $\pi : \mathbb{P}(w, x, y, z) \rightarrow \mathbb{P}(P, Q, R, S)$ maps the sixteen nodes on the Göpel-Hudson quartic in Lemma 7 to four nodes on the Göpel quartic in Lemma 8. □

The Rosenhain roots of the genus 2 curve \mathcal{X} in Equation (25) generate the rational function field $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$ of the moduli space $\mathbb{A}_2(2)$ of principally polarized abelian surfaces $\mathcal{A} = \text{Jac}(\mathcal{X})$ with level-2 structure. The moduli A, B, C, D of the Hudson quartic (42) are then given by the rational functions

$$(60) \quad \begin{aligned} A &= 2 \frac{\lambda_1 + 1}{\lambda_1 - 1}, \quad B = 2 \frac{\lambda_1\lambda_2 + \lambda_1\lambda_3 - 2\lambda_2\lambda_3 - 2\lambda_1 + \lambda_2 + \lambda_3}{(\lambda_2 - \lambda_3)(\lambda_1 - 1)}, \quad C = 2 \frac{\lambda_3 + \lambda_2}{\lambda_3 - \lambda_2}, \\ D &= 4 \frac{\lambda_1 - \lambda_2\lambda_3}{(\lambda_2 - \lambda_3)(\lambda_1 - 1)}. \end{aligned}$$

Similarly, the Rosenhain roots of the genus 2 curve $\hat{\mathcal{X}}$ in Equation (26) generate the rational function field $\mathbb{Q}(\Lambda_1, \Lambda_2, \Lambda_3)$ of the moduli space $\hat{\mathbb{A}}_2(2)$ of (2, 2)-isogenous principally polarized abelian surfaces with level-2 structure. In turn, the moduli $\alpha, \beta, \gamma, \delta$ of the Göpel quartic (44) are given by the rational functions

$$(61) \quad \begin{aligned} \alpha &= 2 \frac{\Lambda_1 + 1}{\Lambda_1 - 1}, \quad \beta = 2 \frac{\Lambda_1\Lambda_2 + \Lambda_1\Lambda_3 - 2\Lambda_2\Lambda_3 - 2\Lambda_1 + \Lambda_2 + \Lambda_3}{(\Lambda_2 - \Lambda_3)(\Lambda_1 - 1)}, \quad \gamma = 2 \frac{\Lambda_3 + \Lambda_2}{\Lambda_3 - \Lambda_2}, \\ \delta &= \frac{4(\Lambda_1 - \Lambda_2\Lambda_3)}{(\Lambda_1 - 1)(\Lambda_3 - \Lambda_2)}. \end{aligned}$$

In summary, we have the following:

Theorem 6.

- (1) *The singular Kummer variety associated with the Jacobian $\text{Jac}(\mathcal{X})$ of the genus-two curve \mathcal{X} in Rosenhain normal form given by Equation (25) is the image of $[\Theta_1(2z) : \Theta_2(2z) : \Theta_3(2z) : \Theta_4(2z)]$ in \mathbb{P}^3 which satisfies Equation (42) with moduli given by Equations (60).*

- (2) The singular Kummer variety associated with the Jacobian $\text{Jac}(\hat{\mathcal{X}})$ of the $(2,2)$ -isogenous curve $\hat{\mathcal{X}}$ in Rosenhain normal form (26) is the image of $[\theta_1^2(z) : \theta_2^2(z) : \theta_3^2(z) : \theta_4^2(z)]$ in \mathbb{P}^3 which satisfies Equation (44) with moduli given by Equations (61).

7.2. Kummer Surface and Shioda-Inose Surface. For an abelian surface $\mathcal{A} = \text{Jac}(\mathcal{X})$, one can attach two K3 surfaces: the Kummer surface discussed above and its double cover, the *Shioda-Inose surface*.

The Inose surface, $\mathcal{Y} := SI(\text{Jac}(\mathcal{X}))$, is a double cover of $\text{Kum}(\text{Jac}(\mathcal{X}))$. Shioda and Inose showed that the diagram of rational maps,

$$(62) \quad \begin{array}{ccc} \text{Jac}(\mathcal{X}) & & \mathcal{Y} \\ & \searrow \pi_0 & \swarrow \pi_1 \\ & \text{Kum}(\text{Jac}(\mathcal{X})) & \end{array}$$

called a Shioda-Inose structure, induces an isomorphism of integral Hodge structures between the transcendental lattices of $\text{Jac}(\mathcal{X})$ and \mathcal{Y} (see [21]). Specifically, \mathcal{Y} admits an involution fixing the holomorphic $(2,0)$ -form, with quotient $\text{Kum}(\text{Jac}(\mathcal{X}))$, and the degree 2 map $p : \mathcal{Y} \rightarrow \text{Kum}(\text{Jac}(\mathcal{X}))$ satisfies a Hodge isometry between $T(\mathcal{Y})(2)$ and $T(\text{Kum}(\text{Jac}(\mathcal{X})))$; see [22].

Lemma 9. *The Shioda-Inose structure induces an isomorphism between the transcendental lattices $T(\text{Jac}(\mathcal{X}))$ and $T(\mathcal{Y})$, up to scaling.*

Proof. The transcendental lattice $T(\text{Jac}(\mathcal{X}))$ is the orthogonal complement of the Néron-Severi group in $H^2(\text{Jac}(\mathcal{X}), \mathbb{Z})$. The map $\pi_0 : \text{Jac}(\mathcal{X}) \rightarrow \text{Kum}(\text{Jac}(\mathcal{X}))$ contracts the 2-torsion cycles, and $p : \mathcal{Y} \rightarrow \text{Kum}(\text{Jac}(\mathcal{X}))$ doubles the lattice, with the involution on \mathcal{Y} preserving the $(2,0)$ -form. The Hodge structure on $T(\mathcal{Y})$ aligns with $T(\text{Jac}(\mathcal{X}))$ via π_1 , and the scaling by 2 in $T(\mathcal{Y})(2)$ matches the degree of the cover, ensuring an isometry of integral lattices. \square

An elliptic surface $\mathcal{E}(\bar{k}(t))$ over \mathbb{P}^1 with a section has a Weierstrass equation

$$(63) \quad y^2 + a_1(t)xy + a_3(t)y = x^2 + a_2(t)x^2 + a_4(t)x + a_6(t),$$

where $a_i(t)$ are rational functions. If it has a singular fiber, the Mordell-Weil group $\mathcal{E}(\bar{k}(t))$ relates to the Néron-Severi group of the K3 surface via the Shioda-Tate theorem. For $\text{Kum}(\text{Jac}(\mathcal{X}))$, an elliptic fibration $\pi : \text{Kum}(\text{Jac}(\mathcal{X})) \rightarrow \mathbb{P}^1$ can be constructed, with a Weierstrass model

$$(64) \quad Y^2 = 4X^3 - g_2(t)X - g_3(t),$$

where $g_2(t)$ and $g_3(t)$ are polynomials of degrees 4 and 6, derived from the theta embedding's coordinates.

8. (n, n) -SPLIT JACOBIANS

We have seen above that sets of abelian surfaces with the same endomorphism ring form sub-varieties within \mathbb{A}_2 . In fact, we showed that the endomorphism ring of principally polarized abelian surface tensored with \mathbb{Q} is either a quartic CM field, an indefinite quaternion algebra, a real quadratic field or in the generic case \mathbb{Q} . Irreducible components of the corresponding subsets in \mathbb{A}_2 have dimensions 0, 1, 2 and are known as CM points, Shimura curves, and Humbert surfaces, respectively.

The latter can be related to a fascinating aspect of genus 2 Jacobians, namely their potential *decomposability*.

Let $\psi : \mathcal{X} \rightarrow E_1$ be a maximal degree n covering to an elliptic curve E_1 , meaning $\deg \psi = n$ and ψ does not factor through an isogeny of E_1 . Then, there exists another elliptic curve $E_2 := \text{Jac}(\mathcal{X})/E_1$, defined as the quotient by the connected component of $\ker(\psi_*)$, such that $\text{Jac}(\mathcal{X})$ is isogenous to $E_1 \times E_2$ via an isogeny of degree n^2 . We call $\text{Jac}(\mathcal{X})$ (n, n) -**decomposable** or (n, n) -**split**, a property studied in [32]. The locus of such curves in \mathcal{M}_2 forms a 2-dimensional irreducible subvariety, with explicit computations for $n = 2, 3, 5$ given in [7], [33], and [34], respectively.

Consider an irreducible, smooth, projective curve of genus two \mathcal{X} and a maximal covering $\psi_1 : \mathcal{X} \rightarrow E_1$ of degree n . The induced map $\psi_1^* : E_1 \rightarrow \text{Jac}(\mathcal{X})$ is injective, embedding E_1 as a subvariety, and $\psi_{1,*} : \text{Jac}(\mathcal{X}) \rightarrow E_1$ has kernel $\ker(\psi_{1,*})$, an elliptic curve E_2 since $\dim \text{Jac}(\mathcal{X}) = 2$ and $\dim E_1 = 1$ (see [35]). Fixing a Weierstrass point $P \in \mathcal{X}$, the embedding

$$(65) \quad \begin{aligned} i_P : \mathcal{X} &\rightarrow \text{Jac}(\mathcal{X}) \\ x &\mapsto [(x) - (P)] \end{aligned}$$

maps \mathcal{X} into $\text{Jac}(\mathcal{X})$. Let $g : E_2 \rightarrow \text{Jac}(\mathcal{X})$ be the natural inclusion, with dual $g^* : \text{Jac}(\mathcal{X}) \rightarrow E_2$. Define $\psi_2 = g^* \circ i_P : \mathcal{X} \rightarrow E_2$, a morphism to E_2 . This yields exact sequences:

$$(66) \quad 0 \rightarrow E_2 \xrightarrow{g} \text{Jac}(\mathcal{X}) \xrightarrow{\psi_{1,*}} E_1 \rightarrow 0,$$

and its dual

$$(67) \quad 0 \rightarrow E_1 \xrightarrow{\psi_1^*} \text{Jac}(\mathcal{X}) \xrightarrow{g^*} E_2 \rightarrow 0.$$

If $\deg(\psi_1) = 2$ or odd, $\psi_2 : \mathcal{X} \rightarrow E_2$ is unique up to elliptic curve isomorphism, as shown in [33]. The Hurwitz space \mathbb{H}_σ of such covers embeds as a 2-dimensional subvariety $\mathcal{L}_n \subset \mathcal{M}_2$, with equations in terms of J_2, J_4, J_6, J_{10} given in [7] (for $n = 2$), [33] (for $n = 3$), and [34] (for $n = 5$). We say \mathcal{X} has an (n, n) -decomposable Jacobian if $\text{Jac}(\mathcal{X})$ admits such a structure, with E_1 and E_2 as its components.

On the other hand, the Humbert surface H_Δ with invariant Δ is the space of principally polarized abelian surfaces admitting a symmetric endomorphism with discriminant Δ . It turns out that Δ always is a positive integer satisfying $\Delta \equiv 0, 1 \pmod{4}$ and uniquely determined H_Δ . In fact, H_Δ is the image inside \mathbb{A}_2 under the projection of the rational divisor associated with the equation

$$(68) \quad a \tau_{11} + b \tau_{12} + c \tau_{22} + d(\tau_{12}^2 - \tau_{11} \tau_{22}) + e = 0,$$

with integers a, b, c, d, e satisfying $\Delta = b^2 - 4ac - 4de$ and $\tau = \begin{pmatrix} \tau_{11} & \tau_{12} \\ \tau_{12} & \tau_{22} \end{pmatrix} \in \mathbb{H}_2$. The following was proven by Birkenhake and Lange in [36]:

Theorem 7. *For $n \in \mathbb{N}$ the Humbert surface H_{n^2} is the locus of principally polarized abelian surfaces $(\mathcal{A}, \mathcal{L}) \in \mathbb{A}_2$ admitting an isogeny of degree n^2 , given by*

$$(69) \quad \hat{\Psi} : (E_1 \times E_2, \mathcal{O}_{E_1}(n) \boxtimes \mathcal{O}_{E_2}(n)) \longrightarrow (\mathcal{A}, \mathcal{L}),$$

where $\mathcal{O}_{E_l}(n)$ is a line bundle of degree n on an elliptic curve \mathcal{E}_l for $l = 1, 2$.

For example, inside of \mathbb{A}_2 sit the Humbert surfaces H_1 and H_4 that are defined as the images under the projection of the rational divisor associated to $\tau_{12} = 0$ and $\tau_{11} - \tau_{22} = 0$, respectively. In fact, the singular locus of \mathbb{A}_2 has H_1 and H_4 as its

two connected components. As analytic spaces, H_1 and H_4 are each isomorphic to the Hilbert modular surface

$$(70) \quad ((\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})) \rtimes \mathbb{Z}_2) \backslash (\mathbb{H} \times \mathbb{H}).$$

In terms of Siegel modular forms in Section 6.3 we have the following characterization, see [37]:

Proposition 7. *The vanishing divisor of the cusp form χ_{10} is the Humbert surface H_1 , i.e., a period point τ is equivalent to a point with $\tau_{12} = 0$ relative to Γ_2 if and only if $\chi_{10}(\tau) = 0$. The vanishing divisor of Q is the Humbert surface H_4 , i.e., a period point τ is equivalent to a point with $\tau_{11} = \tau_{22}$ relative to Γ_2 if and only if $Q = 0$.*

It is known that one has $\chi_{10}(\tau) = 0$ if and only if the principally polarized abelian surface \mathcal{A} is a product of two elliptic curves $\mathcal{A} = E_{\tau_{11}} \times E_{\tau_{22}}$ with the transcendental lattice $\mathrm{T}_{\mathcal{A}} = H \oplus H$; see [14]. Here, H denotes the lattice \mathbb{Z}^2 with quadratic form $q(\vec{v}) = 2v_1v_2$. Moreover, for $Q(\tau) = 0$ the transcendental lattice of the corresponding abelian surface \mathcal{A} is given by $\mathrm{T}_{\mathcal{A}} = H \oplus \langle 2 \rangle \oplus \langle -2 \rangle$. Here, $\langle m \rangle$ denotes the rank-one lattice $\mathbb{Z}v$ with $q(v) = m$. Similarly, for $\tau \in H_{n^2}$, the transcendental lattice of \mathcal{A} is given by $\mathrm{T}_{\mathcal{A}} = H \oplus \langle n \rangle \oplus \langle -n \rangle$.

Considering $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$ as above, the isogeny in the above theorem is precisely $\hat{\Psi} = \psi_1^* \times \psi_2^*$. The Humbert hypersurface H_{Δ} then parameterizes curves \mathcal{X} whose Jacobians admit an optimal action by the order \mathcal{O}_{Δ} , a condition tied to embeddings of quadratic fields (see [38]). In particular, H_{n^2} correspond to curves with (n, n) -split Jacobians, reflecting isogenies to products of elliptic curves. A point in $H_{m^2} \cap H_{n^2}$ ($m \neq n$) indicates either a simple abelian surface with quaternionic multiplication by an indefinite quaternion algebra over \mathbb{Q} , or a self-product E^2 where E is an elliptic curve, a phenomenon prominent on Shimura curves.

Proposition 8. *$\mathrm{Jac}(\mathcal{X})$ is a geometrically simple abelian variety if and only if it is not (n, n) -decomposable for some $n > 1$. Equivalently, if $\mathrm{Jac}(\mathcal{X})$ is split over k , then there exists an integer $n \geq 2$ such that $\mathrm{Jac}(\mathcal{X})$ is (n, n) -split.*

Proof. Suppose $\mathrm{Jac}(\mathcal{X})$ is geometrically simple, i.e., simple over \bar{k} . By the Poincaré-Weil theorem, $\mathrm{Jac}(\mathcal{X})$ is isogenous to $\mathcal{A}_1^{n_1} \times \cdots \times \mathcal{A}_r^{n_r}$, and simplicity over \bar{k} implies $r = 1$, $n_1 = 1$, with $\mathcal{A}_1 = \mathrm{Jac}(\mathcal{X})$. If $\mathrm{Jac}(\mathcal{X})$ were (n, n) -decomposable, there would exist a maximal degree n covering $\psi : \mathcal{X} \rightarrow E_1$, inducing an isogeny $\mathrm{Jac}(\mathcal{X}) \rightarrow E_1 \times E_2$ of degree n^2 , where E_1, E_2 are elliptic curves. Over \bar{k} , this isogeny splits $\mathrm{Jac}(\mathcal{X})$ into a product of 1-dimensional varieties, contradicting simplicity unless $n = 1$, which is trivial (as $\deg \psi = 1$ implies $\mathcal{X} \cong E_1$, contradicting $g = 2$). Thus, $\mathrm{Jac}(\mathcal{X})$ is not (n, n) -decomposable for any $n > 1$.

Conversely, if $\mathrm{Jac}(\mathcal{X})$ is not (n, n) -decomposable for any $n > 1$, suppose it is not geometrically simple. Then over k , $\mathrm{Jac}(\mathcal{X}) \cong E_1 \times E_2$, with $\dim E_i = 1$. By the theory of maximal coverings ([32]), there exists a degree $n > 1$ map $\psi : \mathcal{X} \rightarrow E_1$ (e.g., projection via a correspondence), making $\mathrm{Jac}(\mathcal{X})$ isogenous to $E_1 \times E_2$, hence (n, n) -split, a contradiction. Thus, $\mathrm{Jac}(\mathcal{X})$ must be simple over \bar{k} .

For the equivalent statement, if $\mathrm{Jac}(\mathcal{X})$ is split over k (isogenous to $E_1 \times E_2$ over k), there exists a maximal covering $\psi : \mathcal{X} \rightarrow E_1$ of degree $n \geq 2$, as genus 2 curves admit non-trivial maps to elliptic curves, inducing the (n, n) -split structure (see [35], §3). \square

This characterization connects the geometric simplicity of $\text{Jac}(\mathcal{X})$ to its indecomposability, a key property for later isogeny studies.

In terms of the Kummer plane in Section 7.1.1 we have the following:

Remark 3. In [36] the geometry of the Kummer plane was determined over several Humbert surfaces H_Δ . In particular, the following statement were proven [36, Cor. 7.2] and [36, Cor. 7.3]:

$\Delta = 4$: if $(\mathcal{A}, \mathcal{L}) \in H_4$ if and only if (numbering the six lines on its Kummer plane $(\mathbb{P}^2; \mathbb{T}_1, \dots, \mathbb{T}_6)$ suitably) the three points $\mathbb{T}_1 \cap \mathbb{T}_2$, $\mathbb{T}_3 \cap \mathbb{T}_4$, $\mathbb{T}_5 \cap \mathbb{T}_6$ are collinear.

$\Delta = 16$: if $(\mathcal{A}, \mathcal{L}) \in H_{16}$ then its Kummer plane $(\mathbb{P}^2; \mathbb{T}_1, \dots, \mathbb{T}_6)$ admits a cubic passing smoothly through three of the 15 points $\mathbb{T}_m \cap \mathbb{T}_n$ and touching the singular lines \mathbb{T}_n in the remaining intersection points with even multiplicity. Conversely, if $(\mathbb{P}^2; \mathbb{T}_1, \dots, \mathbb{T}_6)$ admits such a curve, then $(\mathcal{A}, \mathcal{L}) \in H_\Delta$ with $\Delta \in \{4, 8, 12, 16, 20\}$.

For the transcendental lattice it follows $\text{T}_{\text{Kum}(\mathcal{A})} \cong \text{T}_{\mathcal{A}}(2)$ [39, Thm. 10]. In particular we have

$$(71) \quad \text{T}_{\text{Kum}(\mathcal{A})} = H(2) \oplus \langle 4 \rangle \oplus \langle -4 \rangle \text{ for } (\mathcal{A}, \mathcal{L}) \in H_4.$$

Generally, for $\mathcal{A} \in H_{n^2}$ it follows from [39] that $\text{Kum}(\mathcal{A})$ has Picard rank 18, and the transcendental lattice is given by

$$(72) \quad \text{T}_{\text{Kum}(\mathcal{A})} \cong \text{T}_{\mathcal{A}}(2) = H(2) \oplus \langle 2n \rangle \oplus \langle -2n \rangle.$$

8.1. The case of (2, 2)-Split Jacobians. The case of a smooth genus 2 curve \mathcal{X} with a (2, 2)-split Jacobian was described by Bolza [40] explicitly. In particular, he proved that the Jacobian $\text{Jac}(\mathcal{X})$ for a smooth genus-two curve \mathcal{X} is (2, 2)-split if and only if $Q(\tau) = 0$; see Proposition 7.

8.1.1. Bolza's representation. Bolza also proved that one can always represent this extra involution as $[X : Y : Z] \mapsto [-X : Y : Z]$ if the genus 2 curve is given in the form

$$(73) \quad \mathcal{X}: \quad Y^2 = X^6 + s_1 X^4 Z^2 + s_2 X^2 Z^4 + Z^6.$$

One uses Equations (16) and Equation (15) to check that $Q = 2^{12} 3^9 \chi_{35}^2 / \chi_{10}$ always vanishes for such a genus-two curve.

Given the elliptic involution, its composition with the hyperelliptic involution defines a second elliptic involution. The two involutions define two elliptic subfields of degree two for the function field of \mathcal{X} . We introduce the elliptic curves E_l in $\mathbb{P}^2 = \mathbb{P}(x_l, y_l, z_l)$ for $l = 1, 2$, given by

$$(74) \quad E_1: y_1^2 z_1 = x_1^3 + s_2 x_1^2 z_1 + s_1 x_1 z_1^2 + z_1^3, \quad E_2: y_2^2 z_2 = x_2^3 + s_1 x_2^2 z_2 + s_2 x_2 z_2^2 + z_2^3,$$

where E_1 and E_2 have the j-invariants $j_1 = j(E_1)$ and $j_2 = j(E_2)$ with

$$(75) \quad j_1 = \frac{2^8 (3s_1 - s_2^2)^3}{4(s_1^3 + s_2^3) - (s_1 s_2)^2 - 18s_1 s_2 + 27}, \quad j_2 = \frac{2^8 (3s_2 - s_1^2)^3}{4(s_1^3 + s_2^3) - (s_1 s_2)^2 - 18s_1 s_2 + 27},$$

respectively. Here, we use the standard normalization of the j-invariant where the square torus with the complex structure i satisfies $j = 1728 = 12^3$. The degree-two quotient maps $\psi_l: \mathcal{X} \rightarrow E_l$ associated with the involutions are given by

$$(76) \quad \psi_1: \mathcal{X} \longrightarrow E_1, \quad [X : Y : Z] \mapsto [x_1 : y_1 : z_1] = [XZ^2 : Y : X^3],$$

and

$$(77) \quad \psi_2 : \mathcal{X} \longrightarrow E_2, \quad [X : Y : Z] \mapsto [x_2 : y_2 : z_2] = [X^2 Z : Y : Z^3],$$

respectively, for $XZ \neq 0$.

8.1.2. Pringsheim's representation. One can also start with a smooth genus-two curve \mathcal{X} in Rosenhain form given by Equation (24). We use the aforementioned relations between the Igusa invariants and the Siegel modular forms to expand the generators of the ring of modular forms in terms of the Rosenhain roots. We obtain

$$(78) \quad \begin{aligned} & -\frac{2^{22}\chi_{35}^2(\tau)}{\chi_{10}^4(\tau)} = (\lambda_1 - \lambda_2\lambda_3)^2(\lambda_2 - \lambda_1\lambda_3)^2(\lambda_3 - \lambda_1\lambda_2)^2 \\ & \times (\lambda_1 - \lambda_2 - \lambda_3 + \lambda_2\lambda_3)^2(-\lambda_1 + \lambda_2 - \lambda_3 + \lambda_1\lambda_3)^2(-\lambda_1 - \lambda_2 + \lambda_3 + \lambda_1\lambda_2)^2 \\ & \times (\lambda_1\lambda_2 + \lambda_1\lambda_3 - \lambda_2\lambda_3 - \lambda_1)^2(\lambda_1\lambda_2 + \lambda_2\lambda_3 - \lambda_1\lambda_3 - \lambda_2)^2(\lambda_1\lambda_3 + \lambda_2\lambda_3 - \lambda_1\lambda_2 - \lambda_3)^2 \\ & \times \begin{cases} (\lambda_1\lambda_2 - \lambda_1\lambda_3 - \lambda_1 + \lambda_3)^2(\lambda_1\lambda_3 - \lambda_2\lambda_3 - \lambda_1 + \lambda_3)^2(\lambda_1\lambda_2 - \lambda_2\lambda_3 - \lambda_1 + \lambda_2)^2 \\ (\lambda_1\lambda_2 - \lambda_1\lambda_3 + \lambda_1 - \lambda_2)^2(\lambda_1\lambda_3 - \lambda_2\lambda_3 + \lambda_2 - \lambda_3)^2(\lambda_1\lambda_2 - \lambda_2\lambda_3 - \lambda_2 + \lambda_3)^2. \end{cases} \end{aligned}$$

The vanishing divisor of Equation (78) defines fifteen components in $\mathbb{H}_2/\Gamma_2(2)$ of discriminant $\Delta = 4$. Notice that each line in Equation (78) is arranged to be invariant under permutations of the three roots $\lambda_1, \lambda_2, \lambda_3$. Pringsheim proved the following statement³ in [41]:

Proposition 9 (Pringsheim). *There are exactly 15 components in $\mathbb{H}_2/\Gamma_2(2)$ covering H_4 . Each of the component is equivalent to $\tau_{11} = \tau_{22}$ relative to the modular group Γ_2 . Moreover, there is a transposition of the six roots $(\lambda_1, \lambda_2, \lambda_3, 0, 1, \infty)$ in $\Gamma_2/\Gamma_2(2) \cong S_6$ that permutes each pair of components.*

We will use component $\lambda_1 = \lambda_2\lambda_3$ in Proposition 9 to construct a smooth genus-two curve in Rosenhain normal form admitting an elliptic involution. That is, we consider the smooth genus-two curve \mathcal{X} , given by

$$(79) \quad \mathcal{X}: \quad Y^2 = XZ(X - Z)(X - \lambda_2\lambda_3Z)(X - \lambda_2Z)(X - \lambda_3Z),$$

with a discriminant given by

$$(80) \quad \lambda_2^6\lambda_3^6(\lambda_2 - 1)^4(\lambda_3 - 1)^4(\lambda_2\lambda_3 - 1)^4(\lambda_2 - \lambda_3)^2.$$

Let us denote by $\Lambda_l \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ the modular parameter for the elliptic curves E_l in $\mathbb{P}^2 = \mathbb{P}(x_l, y_l, z_l)$ for $l = 1, 2$ defined by the *Legendre normal form*

$$(81) \quad E_l : \quad y_l^2 z_l = x_l(x_l - z_l)(x_l - \Lambda_l z_l),$$

with the hyperelliptic involution given by $u_l : [x_l : y_l : z_l] \mapsto [x_l : -y_l : z_l]$. One easily checks the following:

Lemma 10. *The function field of the smooth genus-two curve \mathcal{X} contains the subfields given by the function fields of the elliptic curves E_l for $l = 1, 2$ if*

$$(82) \quad \Lambda_1\Lambda_2 = \frac{(\lambda_2 + \lambda_3)^2 - 4\lambda_2\lambda_3}{(1 - \lambda_2)^2(1 - \lambda_3)^2}, \quad \Lambda_1 + \Lambda_2 = -\frac{2(\lambda_2 + \lambda_3)}{(1 - \lambda_2)(1 - \lambda_3)}.$$

We then have the following:

³We corrected two minor typos in the statement of the main theorem.

Proposition 10. *Assume that $\lambda_2, \lambda_3 \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ satisfy $\lambda_2 \neq \lambda_3^{\pm 1}$, and the moduli of the curves \mathcal{X} and E_l in Equations (79) and (81) satisfy Equations (82). Quotient maps $\psi_l : \mathcal{X} \rightarrow E_l$ for $l = 1, 2$ are given by*

$$(83) \quad \psi_l : \mathcal{X} \longrightarrow E_l, \quad [X : Y : Z] \mapsto [x_l : y_l : z_l] \text{ for } l = 1, 2,$$

with

$$(84) \quad [x_l : y_l : z_l] = [r(X - \lambda_2 Z)(X - \lambda_3 Z)XZ : (X - (-1)^l qZ)Y : r^3 X^2 Z^2],$$

for $XZ \neq 0$, and $[x_l : y_l : z_l] = [1 : 0 : 0]$ otherwise. Here, q, r are square roots of $q^2 = \lambda_2 \lambda_3$ and $r^2 = (1 - \lambda_2)(1 - \lambda_3)$, respectively. The elliptic involutions j_l on \mathcal{X} , given by

$$(85) \quad j_l : [X : Y : Z] \mapsto [\lambda_2 \lambda_3 Z : (-1)^{l+1} \lambda_2 \lambda_3 q Y : X],$$

satisfy $\psi_l \circ j_l = \psi_l$ for $l = 1, 2$.

Proof. The genus-two curve \mathcal{X} in Equation (79) is assumed to be smooth. Thus, one must have $\lambda_2, \lambda_3 \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ and $\lambda_2 \neq \lambda_3^{\pm 1}$. The remainder of the proof follows by explicit computation. We note that a choice of square root for r is changed by composing ψ_l with the elliptic involution on E_l . The choice of square root for q is changed by interchanging $\psi_1 \leftrightarrow \psi_2$. \square

Remark 4. *Using a covering space of $c\lambda_1 = \lambda_2 \lambda_3$ in Proposition 9, given by the set of tuples (k_1, k_2) with $\lambda_l = k_l^2$ for $l = 2, 3$ and $\lambda_1 = (k_2 k_3)^2$, we obtain for the modular parameters of the elliptic-curve quotients E_l in Lemma 10 the following algebraic solutions of Equation (82):*

$$(86) \quad \Lambda_1 = -\frac{(k_2 - k_3)^2}{(1 - k_2^2)(1 - k_3^2)}, \quad \Lambda_2 = -\frac{(k_2 + k_3)^2}{(1 - k_2^2)(1 - k_3^2)}.$$

A change of square roots $(k_2, k_3) \mapsto (\pm k_2, \pm k_3)$ leaves Equations (86) invariant, whereas the change $(k_2, k_3) \mapsto (\pm k_2, \mp k_3)$ interchanges Λ_1 and Λ_2 . This means that the elliptic curves E_l with level-two structure can be constructed over $\mathbb{Q}(k_2, k_3)$ as a finite field extension of $\mathbb{Q}(\Lambda_1, \Lambda_2)$.

8.1.3. *Legendre's gluing construction.* The Weierstrass points P_i of the curve \mathcal{X} in Equation (79), given by

$$(87) \quad \begin{aligned} P_1 &: [\lambda_2 \lambda_3 : 0 : 1], & P_2 &: [\lambda_2 : 0 : 1], & P_3 &: [\lambda_3 : 0 : 1], \\ P_4 &: [0 : 0 : 1], & P_5 &: [1 : 0 : 1], & P_6 &: [1 : 0 : 0], \end{aligned}$$

are the fixed points of the hyperelliptic involution. The two elliptic involutions j_l in Equation (85) for $l = 1, 2$ (each) pairwise interchange the Weierstrass points, i.e.,

$$(88) \quad j_l : P_2 \leftrightarrow P_3, \quad P_1 \leftrightarrow P_5, \quad P_4 \leftrightarrow P_6.$$

The points $Q_{l,\pm}$, given by

$$(89) \quad \begin{aligned} Q_{1,\pm} &: [-q : \pm i q^{\frac{3}{2}}(k_2 k_3 + 1)(k_2 + k_3) : 1], \\ Q_{2,\pm} &: [q : \pm q^{\frac{3}{2}}(k_2 k_3 - 1)(k_2 - k_3) : 1], \end{aligned}$$

are the ramification points of ψ_l in Equation (83) for $l = 1$ and $l = 2$, respectively. The involution j_1 fixes the points $Q_{1,+}$ and $Q_{1,-}$, and interchanges the points $Q_{2,+} \leftrightarrow Q_{2,-}$. An analogous statements holds for the involution j_2 . The hyperelliptic involution of the curve \mathcal{X} interchanges the elements of the two pairs simultaneously, i.e., $Q_{l,+} \leftrightarrow Q_{l,-}$ for $l = 1, 2$.

The pairs $\{P_2, P_3\}$, $\{P_1, P_5\}$, $\{Q_{2,+}, Q_{2,-}\}$, and $\{P_5, P_6\}$ are mapped by ψ_1 to the two-torsion points $p_0 : [x_1 : y_1 : z_1] = [0 : 0 : 1]$, $p_1 : [1 : 0 : 1]$, $p_{\Lambda_1} : [\Lambda_1 : 0 : 1]$, and the identity $p_\infty : [1 : 0 : 0]$ in E_1 . Similarly, the pairs $\{P_2, P_3\}$, $\{P_1, P_5\}$, $\{Q_{1,+}, Q_{1,-}\}$, and $\{P_5, P_6\}$ are mapped by ψ_2 to the two-torsion points $p_0 : [x_2 : y_2 : z_2] = [0 : 0 : 1]$, $p_1 : [1 : 0 : 1]$, $p_{\Lambda_2} : [\Lambda_2 : 0 : 1]$, and the identity $p_\infty : [1 : 0 : 0]$ in E_2 .

We associate with the branch locus of ψ_1 and ψ_2 the effective divisor of degree two $B_1 = [\psi_1(Q_{1,+}) + \psi_1(Q_{1,-})]$ on E_1 and $B_2 = [\psi_2(Q_{2,+}) + \psi_2(Q_{2,-})]$ on E_2 , respectively. One checks that for $\psi_1(Q_{1,\pm})$ one has $[x_1 : z_1] = [\Lambda_2 : 1]$, and for $\psi_2(Q_{2,\pm})$ one has $[x_2 : z_2] = [\Lambda_1 : 1]$. Because of $\text{Pic}^0(E_l) \cong E_l$ the line bundle $\mathcal{O}_{E_l}(B_l)$ associated with the branch locus B_l is equivalent to the line bundle $\mathcal{O}_{E_l}(2p_\alpha)$ if and only if

$$(90) \quad \psi_l(Q_{l,+}) \oplus \psi_l(Q_{l,-}) = 2p_\alpha = p_\alpha \oplus p_\alpha,$$

where \oplus refers to the addition with respect to the elliptic curve group law on E_l . Using the properties for ψ_l in Equation (83) one finds that

$$(91) \quad \psi_l(Q_{l,+}) \oplus \psi_l(Q_{l,-}) = 0,$$

and $p_\alpha \in E_l[2]$ is a two-torsion point. Thus, there are four line bundle $\mathcal{L}_l \rightarrow E_l$ such that $\mathcal{L}_l^{\otimes 2} \cong \mathcal{O}_{E_l}(B_l)$, namely $\mathcal{L}_l \cong \mathcal{O}_{E_l}(p_\alpha)$. It follows $h^0(\mathcal{E}_l, \mathcal{L}_l) = 1$ by the Riemann-Roch theorem. Conversely, the preimage of the vanishing locus of a section of $\mathcal{L}_l \rightarrow \mathcal{E}_l$ determines a unique double cover $\psi_l : \mathcal{X} \rightarrow E_l$. The composition on \mathcal{X} of the elliptic involution with the hyperelliptic involution defines a second elliptic involution, and a second elliptic-curve quotient is obtained. Thus, the data $(E_l, \mathcal{L}_l, B_l)$ for either $l = 1$ or $l = 2$ determines the curve \mathcal{X} uniquely. As we have seen, this data is equivalent to an (unordered) pair $\{\Lambda_1, \Lambda_2\}$ of modular parameters $\Lambda_1, \Lambda_2 \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ with $\Lambda_1 \neq \Lambda_2$. Legendre constructed an explicit model for \mathcal{X} over $\mathbb{Q}(\Lambda_1, \Lambda_2)$; this is often referred to as *Legendre's gluing method*. Following Serre's explanation [42, Sec. 27] of Legendre's gluing method we obtain:

Proposition 11. *Assume that $\Lambda_1, \Lambda_2 \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ satisfy $\Lambda_1 \neq \Lambda_2$, and the moduli of \mathcal{X} and E_l in Equations (79) and (81) satisfy Equations (82). The smooth genus-two curve, given by*

$$(92) \quad \tilde{\mathcal{X}}: \quad Y^2 = (X^2 - Z^2) \left(X^2 - \frac{\Lambda_1}{\Lambda_2} Z^2 \right) \left(X^2 - \frac{1 - \Lambda_1}{1 - \Lambda_2} Z^2 \right),$$

is isomorphic to \mathcal{X} over a finite field extension of $\mathbb{Q}(\lambda_2, \lambda_3)$. The curve is also isomorphic to each of the curves obtained by replacing $\{\Lambda_1, \Lambda_2\}$ in Equation (92) by one of the following pairs:

$$(93) \quad \left\{ \frac{1}{1 - \Lambda_1}, \frac{1}{1 - \Lambda_2} \right\}, \left\{ \frac{\Lambda_1 - 1}{\Lambda_1}, \frac{\Lambda_2 - 1}{\Lambda_2} \right\}, \left\{ \frac{1}{\Lambda_1}, \frac{1}{\Lambda_2} \right\}, \left\{ \frac{\Lambda_1}{\Lambda_1 - 1}, \frac{\Lambda_2}{\Lambda_2 - 1} \right\}, \{1 - \Lambda_1, 1 - \Lambda_2\}.$$

Proof. Using Remark 4 and denoting the Igusa-Clebsch invariants of any pairs genus-two curves in the statement of the proposition by $[J_2 : J_4 : J_6 : J_{10}]$ and $[J'_2 : J'_4 : J'_6 : J'_{10}]$, respectively, one checks that

$$(94) \quad [J_2 : J_4 : J_6 : J_{10}] = [s^2 J'_2 : s^4 J'_4 : s^6 J'_6 : s^{10} J'_{10}] = [J'_2 : J'_4 : J'_6 : J'_{10}]$$

with $s \in \mathbb{Q}(\lambda_2, \lambda_3, \sqrt{\lambda_2 \lambda_3})$. □

The six pairs, given by $\{\Lambda_1, \Lambda_2\}$ and Equation (93), correspond to the orbit of the data $(E_l, \mathcal{L}_l, B_l)$ under $\Gamma/\Gamma(2)$, i.e., the orbit under simultaneous action of the *anharmonic group* on an elliptic curve in Legendre form. The anharmonic group is generated by the two transformations $\Lambda \mapsto 1 - \Lambda, \Lambda/(\Lambda - 1)$.

Since the Picard group $\text{Pic}^0(\mathcal{X}) \cong \text{Jac}(\mathcal{X})$ consists of elements of the form $[P + Q - 2P_0]$ for $P, Q \in \mathcal{X}$, an isogeny Ψ of abelian surfaces is defined by setting

$$(95) \quad \Psi: \text{Jac } \mathcal{X} \longrightarrow E_1 \times E_2, \quad [P+Q-2P_0] \mapsto (\psi_1(P) \oplus \psi_1(Q), \psi_1(P) \oplus \psi_2(Q)).$$

It follows from the construction of the line bundles $\mathcal{L}_l \rightarrow E_l$ in Section 8.1.3 that the line bundle $\mathcal{L} \rightarrow \mathcal{A} = \text{Jac}(\mathcal{X})$ associated with the principal polarization of \mathcal{A} satisfies $\mathcal{L} \cong \Psi^*(\mathcal{L}_1 \boxtimes \mathcal{L}_2)$. Ψ is the dual isogeny to $\hat{\Psi}$ in Theorem 7. The elliptic involutions j_l on \mathcal{X} extend to involutions on the Jacobian $\mathcal{A} = \text{Jac}(\mathcal{X})$ that coincide on $\mathcal{A}[2]$. We denote this induced involution on $\mathcal{A}[2]$ by $j: \mathcal{A}[2] \rightarrow \mathcal{A}[2]$.

Given the marking $(P_1, \dots, P_6) = (\lambda_1 = \lambda_2\lambda_3, \lambda_2, \lambda_3, 0, 1, \infty)$ of the Weierstrass points for the curve \mathcal{X} as before, we have the following:

Proposition 12. *In the situation above, the kernel of $\Psi: \mathcal{A} = \text{Jac}(\mathcal{X}) \rightarrow E_1 \times E_2$ is given by the Göpel group*

$$(96) \quad \ker \Psi = \{P_0, P_{15}, P_{23}, P_{46}\} \cong (\mathbb{Z}/2\mathbb{Z})^2 \subset \mathcal{A}[2].$$

In particular, Ψ is a $(2, 2)$ -isogeny and $\hat{\mathcal{A}} = \mathcal{A}/\ker \Psi \cong E_1 \times E_2$ with $\text{T}_{\hat{\mathcal{A}}} = H \oplus H$.

Proof. The induced actions of the two elliptic involutions j_l on $\text{Jac}(\mathcal{X})$ fix the divisors P_{15}, P_{23}, P_{46} , and $[Q_{l,+} + Q_{l,-} - 2P_0]$. It follows from the explicit formulas for ψ_l in Proposition that $(P, Q) \in \ker \Psi$ if and only if $P, Q \in \mathcal{A}[2]$ and $j_l(P) = Q$ for $l = 1, 2$. \square

8.2. Loci of (ℓ, ℓ) -Split Jacobians. The locus $\mathcal{L}_\ell \subset \mathcal{M}_2$ of genus 2 curves over $\overline{\mathbb{Q}}$ whose Jacobians are (ℓ, ℓ) -split—isogenous to a product $E_1 \times E_2$ via an (ℓ, ℓ) -isogeny with kernel an isotropic subgroup of order ℓ^2 —is an irreducible 2-dimensional subvariety. We have computed \mathcal{L}_ℓ for $\ell = 2, 3, 5, 7, 11$, providing explicit equations in terms of Igusa invariants J_2, J_4, J_6, J_{10} (see [7], [33], [34] for $\ell = 2, 3, 5$). For $\ell = 2$, \mathcal{L}_2 aligns with Richelot’s 15 isogenies (Section 8.1); for odd ℓ , \mathcal{L}_ℓ is a Hurwitz space of degree- ℓ coverings, irreducible due to automorphism group transitivity, with dimension 2 from \mathcal{M}_2 ’s 3 minus the isotropy codimension.

In cryptography, identifying \mathcal{L}_ℓ is critical. Over finite fields (e.g., \mathbb{F}_{p^2}), a split $\text{Jac}(\mathcal{X}) \in \mathcal{L}_\ell$ reduces the superspecial isogeny problem’s complexity from $\tilde{O}(p)$ to elliptic curve subproblems $(\tilde{O}(\sqrt{p}))$, as exploited by Costello et al. [43]. Their algorithm detects (ℓ, ℓ) -splittings using Kumar’s parametrisations [44]—matching our \mathcal{L}_ℓ —speeding up attacks by factors of 16–159 for p from 50 to 1000 bits. This weakens protocols like the Castryck-Decru-Smith hash [45], where split Jacobians enable faster collision finding, suggesting key selection avoid \mathcal{L}_ℓ to bolster security.

While \mathcal{L}_ℓ doesn’t directly compute (ℓ, ℓ) -isogenies (Section 8), it validates results: if $\mathcal{X} \in \mathcal{L}_\ell$, $\text{Jac}(\mathcal{Y})$ should be split, benchmarking algorithms like Lubicz-Robert (Section 8.2). This dual role enhances both geometric classification and cryptanalysis.

9. COMPUTING HIGHER (ℓ, ℓ) -ISOGENIES

The Richelot isogenies treated earlier represent the simplest instance of a broader class of isogenies between abelian surfaces, specifically $(2, 2)$ -isogenies with kernels

of order 4. Here, we generalize to (ℓ, ℓ) -isogenies, where the kernel has order ℓ^2 , focusing on computational methods for Jacobians of genus 2 curves, leveraging their Kummer surfaces. Consider an isogeny

$$(97) \quad \phi: \text{Jac}(\mathcal{X}) \rightarrow \text{Jac}(\mathcal{Y}),$$

where \mathcal{X} and \mathcal{Y} are genus 2 curves over a field k with $\text{char } k \neq 2$, and $\text{Jac}(\mathcal{X})$ and $\text{Jac}(\mathcal{Y})$ are their Jacobians, each a 2-dimensional principally polarized abelian surface. Let $\Theta_{\mathcal{X}}$ and $\Theta_{\mathcal{Y}}$ denote the theta divisors on $\text{Jac}(\mathcal{X})$ and $\text{Jac}(\mathcal{Y})$, respectively, where $\Theta_{\mathcal{X}}$ is the image of \mathcal{X} under an embedding such as $\phi_{P_0}: \mathcal{X} \rightarrow \text{Jac}(\mathcal{X})$, $P \mapsto [(P) - (P_0)]$, for a base point $P_0 \in \mathcal{X}(k)$. The isogeny ϕ satisfies $\phi(\Theta_{\mathcal{X}}) \in |\ell\Theta_{\mathcal{Y}}|$, the linear system of divisors linearly equivalent to ℓ times $\Theta_{\mathcal{Y}}$. On the Kummer surface $\text{Kum}(\text{Jac}(\mathcal{Y})) = \text{Jac}(\mathcal{Y})/\langle \pm 1 \rangle$, embedded in \mathbb{P}^3 via level 2 theta functions, $\phi(\Theta_{\mathcal{X}})$ descends to a curve of degree 2ℓ , genus 0, and arithmetic genus $\frac{1}{2}(\ell^2 - 1)$, computable without explicitly determining ϕ , as shown in [46].

9.1. The ℓ -tuple embedding. For \mathcal{X} given by

$$(98) \quad y^2 = f(x) = a_6x^6 + \cdots + a_1x + a_0,$$

a monic sextic with $\Delta_f = J_{10} \neq 0$, the divisor at infinity is

$$(99) \quad D_{\infty} := (1 : \sqrt{f(1)} : 0) + (1 : -\sqrt{f(1)} : 0),$$

assuming a normalization where infinity points are $(1 : y : 0)$. The Weierstrass points are the roots of $f(x) = 0$, denoted $w_i = (x_i, z_i)$ for $i = 1, \dots, 6$, with $f(x_i/z_i) = 0$, forming the Weierstrass divisor

$$(100) \quad W_{\mathcal{X}} := \sum_{i=1}^6 (x_i, 0, z_i).$$

A canonical divisor on \mathcal{X} is

$$(101) \quad \mathcal{K}_{\mathcal{X}} = W_{\mathcal{X}} - 2D_{\infty},$$

as $\deg W_{\mathcal{X}} = 6$, $\deg D_{\infty} = 2$, and $2g - 2 = 2$. A divisor $D \in \text{Jac}(\mathcal{X})$ as $D = P + Q - D_{\infty}$, with $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, corresponds to an ideal $(a(x), y - b(x))$, where $a(x) = (x - x_P)(x - x_Q)$ is a monic polynomial of degree $d \leq 2$ (quadratic if $P \neq Q$, linear if $P = Q$), and $b(x)$ is a cubic interpolating y_P, y_Q .

To compute ϕ , embed \mathcal{X} via the ℓ -tuple map

$$(102) \quad \rho_{2\ell}: \mathbb{P}^2 \rightarrow \mathbb{P}^{2\ell}, \quad (x, y, z) \mapsto (z^{2\ell}, xz^{2\ell-1}, \dots, x^{2\ell-1}z, x^{2\ell}),$$

with image $\mathcal{R}_{2\ell}$, a rational normal curve of degree 2ℓ . Any $2\ell + 1$ points on $\mathcal{R}_{2\ell}$ are linearly independent, as the space of degree 2ℓ homogeneous polynomials has dimension $2\ell + 1$. For $\ell \geq 3$, the 6 points $\rho_{2\ell}(w_i)$ are independent ($6 < 7$ for $\ell = 3$), and

$$(103) \quad W := \langle \rho_{2\ell}(W_{\mathcal{X}}) \rangle \subset \mathbb{P}^{2\ell}$$

is 5-dimensional. The secant line $\mathcal{L}_{P,Q}$ is

$$(104) \quad \mathcal{L}_{P,Q} = \begin{cases} \langle \rho_{2\ell}(P), \rho_{2\ell}(Q) \rangle & \text{if } P \notin \{Q, \tau(Q)\}, \\ T_{\rho_{2\ell}(P)}(\mathcal{R}_{2\ell}) & \text{otherwise,} \end{cases}$$

where τ is the hyperelliptic involution. Dolgachev and Lehavi ([46]) proved:

Theorem 8 (Dolgachev-Lehavi). *Let \mathcal{X} be a genus 2 curve, $S \subset \text{Jac}(\mathcal{X})[\ell]$ an isotropic subgroup of order ℓ^2 , and $\rho_{2\ell} : \mathcal{X} \rightarrow \mathcal{R}_{2\ell} \subset \mathbb{P}^{2\ell}$ the ℓ -tuple embedding. There exists a hyperplane $H \subset \mathbb{P}^{2\ell}$ such that:*

- (i) H contains $W = \langle \rho_{2\ell}(W_{\mathcal{X}}) \rangle$,
- (ii) The intersections $H \cap \mathcal{L}_e$ for each non-zero $e \in S$ lie in a subspace $N \subset H$ of codimension 3.

The image of $\rho_{2\ell}(W_{\mathcal{X}})$ under the projection $\mathbb{P}^{2\ell} \rightarrow \mathbb{P}^3$ with center N lies on a conic \mathcal{C} , and the double cover of \mathcal{C} ramified over this divisor is a stable genus 2 curve \mathcal{Y} with $\text{Jac}(\mathcal{Y}) \cong \text{Jac}(\mathcal{X})/S$.

Proof. The linear system $|\ell\Theta_{\mathcal{X}}|$ on $\text{Jac}(\mathcal{X})$ has dimension $\ell^2 - 1$ (projective dimension of divisors modulo scalars), and for an isotropic S of order ℓ^2 , $\text{Jac}(\mathcal{Y}) = \text{Jac}(\mathcal{X})/S$ is principally polarized with theta divisor $\Theta_{\mathcal{Y}}$. Since $\deg \Theta_{\mathcal{X}} = 2$, $\phi(\Theta_{\mathcal{X}}) \in |\ell\Theta_{\mathcal{Y}}|$ has degree 2ℓ , projecting to a genus 0 curve in $\text{Kum}(\text{Jac}(\mathcal{Y}))$ with arithmetic genus $\frac{1}{2}(2\ell-1)(2\ell-2) = \ell^2 - 1$ by the adjunction formula. Embed \mathcal{X} via $\rho_{2\ell}$, where W has dimension 5 (6 points minus 1). The secant variety over S (order ℓ^2) requires a hyperplane H (dimension $2\ell - 1$) containing W . The $\ell^2 - 1$ secants \mathcal{L}_e intersect H in points spanning a subspace N of dimension $\ell^2 - 2$, codimension 3 in H (since $\ell^2 - 2 = 2\ell - 1 - 3$ for $\ell \geq 2$). Projection from N to \mathbb{P}^3 maps the 6 points to a conic \mathcal{C} (5 points determine a conic in \mathbb{P}^3), and the double cover ramified at 6 points has genus $1 + \frac{1}{2}(6 - 2) = 2$ by Riemann-Hurwitz, with $\text{Jac}(\mathcal{Y}) \cong \text{Jac}(\mathcal{X})/S$ ([46], Theorem 1). \square

Smith ([47]) developed an algorithm using this theorem, effective for $\ell = 3$ ($|S| = 9$), refined in [48], [49], [50], and [51]. For $\ell = 3$, $W \subset \mathbb{P}^6$, H is 5-dimensional, N is 2-dimensional, and the projection yields a conic in \mathbb{P}^3 . Improvements over [51] include optimized secant computations and invariant recovery.

9.2. Computing (n, n) -Isogenies via Kummer Surface. For an (n, n) -isogeny $\phi : \text{Jac}(\mathcal{X}) \rightarrow \text{Jac}(\mathcal{Y})$ with kernel $S \subset \text{Jac}(\mathcal{X})[n]$ of order n^2 , the Kummer surface $\text{Kum}(\text{Jac}(\mathcal{X}))$ provides a computational lens. Embedded in \mathbb{P}^3 , $\phi(\Theta_{\mathcal{X}}) \in |n\Theta_{\mathcal{Y}}|$ projects to a degree $2n$ curve. The embedding

$$\rho_{2n} : \mathbb{P}^2 \rightarrow \mathbb{P}^{2n}, \quad (x, y, z) \mapsto (z^{2n}, xz^{2n-1}, \dots, x^{2n}),$$

yields \mathcal{R}_{2n} , and $W = \langle \rho_{2n}(W_{\mathcal{X}}) \rangle$ is 5-dimensional.

Theorem 9. *For an isotropic $S \subset \text{Jac}(\mathcal{X})[n]$ of order n^2 , there exists a hyperplane $H \subset \mathbb{P}^{2n}$ containing W such that $H \cap \mathcal{L}_e$ for non-zero $e \in S$ span a subspace $N \subset H$ of codimension 3. The projection from N maps $\rho_{2n}(W_{\mathcal{X}})$ to a conic $\mathcal{C} \subset \mathbb{P}^3$, and the double cover of \mathcal{C} ramified at these 6 points is \mathcal{Y} with $\text{Jac}(\mathcal{Y}) \cong \text{Jac}(\mathcal{X})/S$.*

Proof. The proof mirrors the Dolgachev-Lehavi case. $|\ell\Theta_{\mathcal{X}}|$ has dimension $n^2 - 1$, and $\phi(\Theta_{\mathcal{X}})$ projects to degree $2n$ in $\text{Kum}(\text{Jac}(\mathcal{Y}))$. H (dimension $2n - 1$) contains W (dimension 5), and the $n^2 - 1$ secants span N (dimension $n^2 - 2$), codimension 3 in H . Projection to \mathbb{P}^3 yields a conic, and the double cover's genus is 2, with Jacobian $\text{Jac}(\mathcal{X})/S$. \square

For $n = 2$, this aligns with Richelot isogenies (\mathbb{P}^4 , N a point). For larger n , the algorithm scales, solving linear systems for H and N .

9.3. The Lubicz-Robert Formula for Computing (ℓ, ℓ) -Isogenies on Kummer Surfaces. The Lubicz-Robert formula provides an efficient method to compute (ℓ, ℓ) -isogenies directly on $\text{Kum}(\text{Jac}(\mathcal{X}))$, leveraging theta coordinates to bypass high-dimensional embeddings like $\rho_{2\ell}$. This approach is particularly effective for odd ℓ and builds on the foundational work of Lubicz and Robert in [52], offering a higher-dimensional analog to Vélu's formulas for elliptic curves.

For a genus 2 curve \mathcal{X} over a field k with $\text{char } k \neq 2$, the Jacobian $\text{Jac}(\mathcal{X})$ is a principally polarized abelian surface, and its Kummer surface $\text{Kum}(\text{Jac}(\mathcal{X})) = \text{Jac}(\mathcal{X})/\langle \pm 1 \rangle$ embeds into \mathbb{P}^3 via level 2 theta functions. An (ℓ, ℓ) -isogeny

$$\phi : \text{Jac}(\mathcal{X}) \rightarrow \text{Jac}(\mathcal{Y}) = \text{Jac}(\mathcal{X})/S,$$

where $S \subset \text{Jac}(\mathcal{X})[\ell]$ is an isotropic subgroup of order ℓ^2 , requires determining both the codomain $\text{Jac}(\mathcal{Y})$ and the map ϕ . The Lubicz-Robert formula achieves this by expressing theta coordinates in terms of sums over S .

Over \mathbb{C} , represent $\text{Jac}(\mathcal{X}) = \mathbb{C}^2/\Lambda$ with $\Lambda = \mathbb{Z}^2 \oplus \tau\mathbb{Z}^2$, where $\tau \in \mathbb{H}_2$ is the period matrix. The ℓ -torsion subgroup $\text{Jac}(\mathcal{X})[\ell] = \{P \in \text{Jac}(\mathcal{X}) \mid [\ell]P = 0\}$ has order $\ell^{2g} = \ell^4$ for $g = 2$, and an isotropic $S \subset \text{Jac}(\mathcal{X})[\ell]$ under the Weil pairing has order ℓ^2 . The level 2 theta functions with characteristics $[a, b]$, $a, b \in (\mathbb{Z}/2\mathbb{Z})^2$, are defined as

$$(105) \quad \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z, \tau) = \sum_{m \in \mathbb{Z}^2} \exp(\pi i(m+a)^t \tau(m+a) + 2\pi i(m+a)^t(z+b)),$$

and the embedding $\varphi_2 : \text{Jac}(\mathcal{X}) \rightarrow \mathbb{P}^3$, $z \mapsto (\theta_i(z))_{i=0}^3$ (e.g., characteristics $[0, 0]$, $[1/2, 0]$, $[0, 1/2]$, $[1/2, 1/2]$), factors through $\text{Kum}(\text{Jac}(\mathcal{X}))$ since $\theta_i(-z) = \theta_i(z)$. These coordinates, evaluated at $z = 0$, are the theta null points defining $\text{Kum}(\text{Jac}(\mathcal{X}))$'s quartic equation in \mathbb{P}^3 .

The Lubicz-Robert formula addresses two tasks: computing the theta null points of $\text{Jac}(\mathcal{Y})$ and evaluating ϕ at points in $\text{Jac}(\mathcal{X})$. For an isotropic S , represent $\ell = a_1^2 + a_2^2 + a_3^2 + a_4^2$ (by Lagrange's four-square theorem, with $r \leq 4$), and choose generators $s_1, s_2 \in S$ such that $S = \langle a_1 s_1, a_2 s_1, a_3 s_2, a_4 s_2 \rangle$ in a suitable basis. The formula comprises:

Theta null points of $\text{Jac}(\mathcal{Y})$:

$$\hat{\theta}_i = \sum_{s \in S} \prod_{u=1}^r \theta \left[\begin{smallmatrix} a_u \\ b_u \end{smallmatrix} \right] (s, \tau)_{\alpha_u i},$$

where $\theta \left[\begin{smallmatrix} a_u \\ b_u \end{smallmatrix} \right] (s, \tau)$ are level 2 theta functions at $s \in S$, and $\alpha_u i$ adjusts indices to align with the basis (e.g., a permutation or selection).

Point evaluation: For $P \in \text{Jac}(\mathcal{X})$,

$$\phi(P)_i = \sum_{s \in S} \prod_{u=1}^r \theta \left[\begin{smallmatrix} a_u \\ b_u \end{smallmatrix} \right] (P + s, \tau)_{\alpha_u i}.$$

Theorem 10 (Lubicz-Robert). *For an isotropic subgroup $S \subset \text{Jac}(\mathcal{X})[\ell]$ of order ℓ^2 , the theta coordinates $\hat{\theta}_i$ and $\phi(P)_i$ computed via the above formulas define the codomain $\text{Jac}(\mathcal{Y}) = \text{Jac}(\mathcal{X})/S$ and the isogeny $\phi : \text{Jac}(\mathcal{X}) \rightarrow \text{Jac}(\mathcal{Y})$, respectively, with complexity $O(\ell^2)$ field operations for a general $\ell = a_1^2 + \dots + a_r^2$.*

Proof. Represent $\text{Jac}(\mathcal{X}) = \mathbb{C}^2/\Lambda$, and $\text{Jac}(\mathcal{Y}) = \mathbb{C}^2/\hat{\Lambda}$, where $\hat{\Lambda} = \mathbb{Z}^2 \oplus \ell\tau\mathbb{Z}^2 + S$. The theta functions on $\text{Jac}(\mathcal{Y})$ are derived from $\text{Jac}(\mathcal{X})$ by summing over S , adjusting the lattice periodicity. For the null points, $\hat{\theta}_i$ aggregates contributions

from S , with the product $\prod_{u=1}^r \theta_{j_u}(s)$ reflecting the kernel's structure via $\ell = \sum a_u^2$. With $|S| = \ell^2$ and $r \leq 4$, the sum has ℓ^2 terms, each a product of $O(1)$ evaluations, totaling $O(\ell^2)$ operations. For $\phi(P)$, the sum ensures $\phi(P + s') = \phi(P)$ for $s' \in S$, as $\theta_{j_u}(P + s + s') = \theta_{j_u}(P + s)$, defining the quotient map. Isotropy preserves the principal polarization, as the Weil pairing vanishes on S , and the resulting $\hat{\theta}_i$ define $\text{Jac}(\mathcal{Y})$'s theta structure ([52], Theorem 4.1). \square

On $\text{Kum}(\text{Jac}(\mathcal{X}))$, $\hat{\theta}_i$ determine $\text{Kum}(\text{Jac}(\mathcal{Y}))$'s quartic equation, and $\phi(P)_i$ maps Kummer points, preserving the (16,6)-configuration (16 nodes from $\text{Jac}(\mathcal{X})[2]$, each on 6 tropes). For $\mathcal{X} : y^2 = f(x)$, choose $S \subset \text{Jac}(\mathcal{X})[\ell]$ (e.g., for $\ell = 3$, S of order 9 from combinations of 3-torsion points like $(x_i, 0)$). Compute $\theta_i(s)$ using the curve's equation, then $\hat{\theta}_i$ over S . The map ϕ respects $\text{Kum}(\text{Jac}(\mathcal{X})) \rightarrow \text{Kum}(\text{Jac}(\mathcal{Y}))$, maintaining geometric properties ([4], Chapter III).

Proposition 13. *The Lubicz-Robert formula on $\text{Kum}(\text{Jac}(\mathcal{X}))$ determines \mathcal{Y} 's equation via theta nulls $\hat{\theta}_i$, and ϕ 's action on $\text{Kum}(\text{Jac}(\mathcal{X}))$ preserves the (16,6)-configuration of tropes and nodes.*

Proof. The $\hat{\theta}_i$ define $\text{Kum}(\text{Jac}(\mathcal{Y}))$'s quartic in \mathbb{P}^3 , from which \mathcal{Y} 's Rosenhain form is derived via Igusa invariants ([52], §5). The (16,6)-configuration maps under ϕ to $\text{Jac}(\mathcal{Y})[2]$, preserving isotropy and structure, as the formula respects the Weil pairing's symmetry ([4], Chapter III). \square

This method also intersects with the geometric classification of genus 2 curves. The loci \mathcal{L}_ℓ , described in Subsection 6.2 as irreducible 2-dimensional subvarieties of \mathcal{M}_2 where $\text{Jac}(\mathcal{X})$ is (ℓ, ℓ) -split, can be computationally probed using the Lubicz-Robert formula. By computing $\hat{\theta}_i$ for a given \mathcal{X} and an isotropic S , one can determine if $[\mathcal{X}] \in \mathcal{L}_\ell$, aligning with detection algorithms by Costello et al. [43]. Our explicit computations for $\ell = 2, 3, 5, 7, 11$ provide test cases, validating the formula's efficiency and offering a bridge between geometric loci and cryptographic applications.

While \mathcal{L}_ℓ does not directly aid in computing ϕ , it provides a geometric testbed. Given $\mathcal{X} \in \mathcal{L}_\ell$, the formula yields $\text{Jac}(\mathcal{Y}) = E_1 \times E_2$, verifiable via invariants, but the computation proceeds independently of this property, relying solely on S .

This method contrasts with Dolgachev-Lehavi's $\mathbb{P}^{2\ell}$ approach, operating in \mathbb{P}^3 with $O(\ell^2)$ complexity, enhancing efficiency for odd ℓ . While \mathcal{L}_ℓ (Subsection 6.2) doesn't drive computation— ϕ is computed agnostically from S —it verifies splitting post-hoc, aligning with detection by Costello et al. [43]. Their use of \mathcal{L}_ℓ to accelerate attacks (e.g., 25x for 100-bit p) underscores its cryptographic role, not in computing ϕ , but in assessing security by identifying weak split Jacobians.

10. CRYPTANALYTIC IMPLICATIONS OF (ℓ, ℓ) -SPLIT JACOBIANS

The computational methods developed in Sections 7 and 8 for (ℓ, ℓ) -isogenies, alongside the geometric classification of \mathcal{L}_ℓ in Section 6, bear significant implications for the security of isogeny-based cryptographic protocols in genus 2. This section examines a recent cryptanalytic advancement leveraging split Jacobians, assesses its impact on existing systems, and delineates the advancements required to fully compromise genus 2 isogeny-based cryptography.

10.1. The Costello et al. Attack. A notable attack on the dimension 2 superspecial isogeny problem, due to Costello et al. [43], optimizes the earlier Costello-Smith algorithm [53] for finding an isogeny $\phi : \text{Jac}(\mathcal{X}) \rightarrow \text{Jac}(\mathcal{Y})$ between superspecial genus 2 Jacobians over \mathbb{F}_{p^2} . The original method employs random walks in the Richelot isogeny graph $\Gamma_2(2; p)$, where vertices are superspecial principally polarized abelian surfaces in $\mathcal{S}_2(p)$, to reach products $E_1 \times E_2 \in \mathcal{E}_2(p)$, followed by elliptic isogeny computations in $\tilde{O}(\sqrt{p})$ via Delfs-Galbraith [54]. With $\#\mathcal{S}_2(p) = O(p^3)$ and $\#\mathcal{E}_2(p) = O(p^2)$, this requires $\tilde{O}(p)$ bit operations.

The enhanced attack detects (ℓ, ℓ) -splittings for $\ell \leq 11$, using \mathcal{L}_ℓ equations to inspect approximately ℓ^3 neighbors per step (e.g., 40 for $\ell = 3$) via invariants, rather than computing full isogenies. This reduces the cost per step from 1176 \mathbb{F}_p -multiplications (Richelot) to as low as 35 (Table 5 in [43]), yielding speedups of 16–159 \times for p from 50 to 1000 bits. The asymptotic complexity remains $\tilde{O}(p/\ell^3)$, but the practical efficiency significantly improves cryptanalysis.

10.2. Impact on Genus 2 Cryptography. This acceleration impacts protocols reliant on the superspecial isogeny problem, such as the Castryck-Decru-Smith (CDS) hash function [45], which maps inputs via Richelot isogenies in $\Gamma_2(2; p)$. For a split $\text{Jac}(\mathcal{X}) \in \mathcal{L}_\ell$, the attack hastens reaching $\mathcal{E}_2(p)$, enabling faster collision finding—e.g., distinct paths to the same product—as noted by Florit and Smith [55]. For a 100-bit prime, a 25 \times speedup reduces security from $\tilde{O}(2^{100})$ to below 2^{96} , threatening underparameterized systems. However, for cryptographic sizes (e.g., 512 bits), a 100 \times factor (to $\tilde{O}(2^{509})$) remains secure against classical attacks, though it narrows the safety margin.

In a hypothetical genus 2 SIDH scheme, where the secret is an (ℓ^k, ℓ^k) -isogeny, the attack finds some path to $\mathcal{E}_2(p)$, not necessarily the secret ϕ . Its efficacy hinges on the codomain $\text{Jac}(\mathcal{Y})$ lying in \mathcal{L}_ℓ , but it doesn't recover the kernel S , limiting its threat to key exchange compared to hash functions. Thus, while impactful, it does not constitute a full break.

10.3. Requirements for a Full Break. To fully break genus 2 isogeny-based cryptography—reducing it to polynomial time or rendering it insecure practically—several advancements beyond this optimization are needed:

- (1) *Kernel Recovery:* A method to extract the secret kernel $S \subset \text{Jac}(\mathcal{X})[\ell^k]$ from public data (e.g., ϕ -images of torsion points), akin to the SIDH attacks. The ℓ^4 -sized torsion group and polarization complexity pose significant hurdles.
- (2) *Subexponential Algorithm:* A subexponential (e.g., $L_p[1/2]$) or polynomial-time solution to the general isogeny problem, possibly via optimal expansion of $\Gamma_2(\ell; p)$ (currently non-Ramanujan [55]) or endomorphism ring computation, remains elusive.
- (3) *Quantum Advantage:* A quantum algorithm (e.g., claw-finding variant) achieving $\text{poly}(\log p)$ time, beyond the current $\tilde{O}(\sqrt{p}/\ell^{3/2})$ from Grover's search, is unachieved for genus 2.
- (4) *Protocol Flaws:* Exploits like degree conversion (e.g., from $(2^n \ell, 2^n \ell)$ to (ℓ^k, ℓ^k) , conjectured in [43]) or torsion leakage could break specific designs, but no such method exists.

The Costello et al. attack optimizes an exponential-time problem, not breaking it fundamentally. A true break requires a paradigm shift—algebraic, geometric, or quantum—currently speculative.

10.4. Connection to This Work. Our computation of \mathcal{L}_ℓ for $\ell = 2, 3, 5, 7, 11$ (Subsection 6.2) and (ℓ, ℓ) -isogeny algorithms (Section 8) intersect with this cryptanalysis. While \mathcal{L}_ℓ doesn't accelerate isogeny computation (e.g., Lubicz-Robert's $O(\ell^2)$), it validates splitting post-computation and underpins the attack's detection, enhancing its scope. Extending \mathcal{L}_ℓ to larger ℓ or integrating with quantum methods could further refine security analysis, balancing constructive and cryptanalytic roles.

11. CONCLUSION AND FUTURE WORK

This paper has explored the intricate interplay between abelian varieties, theta functions, and Kummer surfaces, with a particular focus on abelian surfaces arising as Jacobians of genus 2 curves. By weaving together foundational algebraic geometry and advanced computational techniques, we have aimed to provide a comprehensive framework for understanding and computing (ℓ, ℓ) -isogenies, extending classical results like Richelot isogenies to arbitrary odd ℓ . Our journey began with the general theory of abelian varieties, establishing their endomorphism rings and isogeny properties, before narrowing to genus 2 Jacobians and their rich geometric structures. The subsequent development of computational methods, culminating in the application of the Lubicz-Robert formula on Kummer surfaces, represents a significant step forward in both theoretical insight and practical utility.

The theoretical backbone of our work—articulated in Sections 2 through 5—lays out the essential tools: the classification of endomorphism algebras via Albert's theorem, the quasi-periodic properties of theta functions, and the geometric realization of Kummer surfaces as quartic hypersurfaces in \mathbb{P}^3 . These foundations underpin the Torelli correspondence between genus 2 curves and their Jacobians, detailed in Section 6, where we characterized (n, n) -split Jacobians and their moduli via Humbert hypersurfaces. This connection is not merely academic; it bridges the analytic power of theta functions with the algebraic structure of curves, enabling precise computations of isogenies.

Sections 7 and 8 shift focus to computational challenges, beginning with Richelot's explicit constructions and generalizing to (ℓ, ℓ) -isogeny algorithms. The Lubicz-Robert formula, with its $O(\ell^2)$ complexity, stands out for its efficiency, offering a practical alternative to traditional approaches by computing directly on Kummer surfaces. Our work has significant implications for isogeny-based cryptography, suggesting enhanced security over elliptic curve protocols like SIDH through larger torsion groups and complex endomorphism structures.

Looking forward, our loci \mathcal{L}_ℓ for $\ell = 2, 3, 5, 7, 11$ reveal a cryptographic vulnerability: split Jacobians enable attacks like Costello et al.'s [43], reducing complexity (e.g., 100x for 1000-bit p). Avoiding \mathcal{L}_ℓ or exploiting its rarity ($5/p$ proportion) could strengthen protocols, while optimizing detection for larger ℓ or even ℓ (via new parametrisations) may refine cryptanalysis. Implementing these in SageMath could benchmark genus 2 SIDH variants, alongside exploring higher genera and supersingular surfaces for novel security paradigms.

In conclusion, this paper bridges classical geometry with modern computation, advancing our understanding of (ℓ, ℓ) -isogenies on abelian surfaces. By integrating theta functions, Kummer surfaces, and efficient algorithms, we contribute to both the mathematical foundations and their cryptographic potential, laying groundwork for future research at this vibrant intersection.

REFERENCES

- [1] Gerhard Frey and Tony Shaska, *Curves, Jacobians, and cryptography*, Algebraic curves and their applications, [2019] ©2019, pp. 279–344. MR3916746
- [2] Davide Lombardo, *Computing the geometric endomorphism ring of a genus 2 jacobian*, arxiv (2016).
- [3] Gerhard Frey, *Isogenies in theory and praxis*, Open problems in mathematics and computational science, 2014, pp. 37–68. MR3330877
- [4] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR2514037
- [5] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1971. Reprinted by Princeton University Press, 1994.
- [6] Frans Oort, *Endomorphism algebras of abelian varieties*, Algebraic geometry and commutative algebra, Vol. II, 1988, pp. 469–502. MR977774
- [7] Tanush Shaska and Helmut Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 2004, pp. 703–723. MR2037120
- [8] Andreas Malmendier and Tony Shaska, *A universal genus-two curve from Siegel modular forms*, SIGMA Symmetry Integrability Geom. Methods Appl. **13** (2017), Paper No. 089, 17. MR3731039
- [9] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR0114819
- [10] L. Beshaj, R. Hidalgo, S. Kruk, A. Malmendier, S. Quispe, and T. Shaska, *Rational points in the moduli space of genus two*, Higher genus curves in mathematical physics and arithmetic geometry, [2018] ©2018, pp. 83–115. MR3782461
- [11] Jun-ichi Igusa, *Modular forms and projective invariants*, Amer. J. Math. **89** (1967), 817–855. MR0229643
- [12] ———, *On the ring of modular forms of degree two over \mathbf{Z}* , Amer. J. Math. **101** (1979), no. 1, 149–183. MR527830
- [13] E. Freitag, *Siegelsche Modulfunktionen*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 254, Springer-Verlag, Berlin, 1983. MR871067
- [14] A. Malmendier and T. Shaska, *The Satake sextic in F -theory*, J. Geom. Phys. **120** (2017), 290–305. MR3712162
- [15] Andreas Malmendier and Tony Shaska, *A universal genus-two curve from Siegel modular forms*, SIGMA Symmetry Integrability Geom. Methods Appl. **13** (2017), Paper No. 089, 17. MR3731039
- [16] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR2514037
- [17] Fried. Jul. Richelot, *De transformatione integralium Abelianorum primi ordinis commentatio. Caput secundum. De computatione integralium Abelianorum primi ordinis*, J. Reine Angew. Math. **16** (1837), 285–341. MR1578135
- [18] Jean-Benoit Bost and Jean-Francois Mestre, *Moyenne arithmetico-géométrique et périodes des courbes de genre 1 et 2*, Gaz. Math. **38** (1988), 36–64. MR970659
- [19] E. Previato, T. Shaska, and G. S. Wijesiri, *Thetanulls of cyclic curves of small genus*, Albanian J. Math. **1** (2007), no. 4, 253–270. MR2367218
- [20] Adrian Clingher and Andreas Malmendier, *Normal forms for Kummer surfaces*, Integrable systems and algebraic geometry. Vol. 2, 2020, pp. 119–174. MR4421430
- [21] Tetsuji Shioda and Katsumi Inose, *On singular $k3$ surfaces*, Complex Analysis and Algebraic Geometry (1977), 119–136. A collection of papers dedicated to K. Kodaira.
- [22] A. Malmendier and T. Shaska, *From hyperelliptic to superelliptic curves*, Albanian J. Math. **13** (2019), no. 1, 107–200. MR3978315

- [23] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, Second, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004. MR2062673
- [24] Wolf Barth, *Even sets of eight rational curves on a K3-surface*, Complex geometry (Göttingen, 2000), 2002, pp. 1–25. MR1922094
- [25] Tetsuji Shioda, *Classical Kummer surfaces and Mordell-Weil lattices*, Algebraic geometry, 2007, pp. 213–221. MR2296439
- [26] Georges Humbert, *Sur les fonctionnes abéliennes singulières. I, II, III*, J. Math. Pures Appl. serie 5, V, 233–350 (1899); VI, 279–386 (1900); VII, 97–123 (1901).
- [27] H. F. Baker, *On a system of differential equations leading to periodic functions*, Acta Math. **27** (1903), no. 1, 135–156. MR1554977
- [28] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. MR1406090
- [29] Noah Braeger, Adrian Clingher, Andreas Malmendier, and Shantel Spatig, *Isogenies of certain K3 surfaces of rank 18*, Res. Math. Sci. **8** (2021), no. 4, Paper No. 57, 60. MR4323344
- [30] E. E. Kummer, *Über die Flächen vierten Grades, auf welchen Schaaren von Kegelschnitten liegen*, J. Reine Angew. Math. **64** (1865), 66–76. MR1579281
- [31] C. W. Borchardt, *über die Darstellung der Kummerschen Fläche vierter Ordnung mit sechzehn Knotenpunkten durch die Göpelsche biquadratische Relation zwischen vier Theta-functionen mit zwei Variabeln*, J. Reine Angew. Math. **83** (1877), 234–244. MR1579732
- [32] Gerhard Frey and Ernst Kani, *Correspondences on hyperelliptic curves and applications to the discrete logarithm*, 2011, pp. 1–19.
- [33] Tony Shaska, *Genus 2 fields with degree 3 elliptic subfields*, Forum Mathematicum **16** (2004), no. 2, 263–280. MR2039100
- [34] Kay Magaard, Tanush Shaska, and Helmut Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Forum Math. **21** (2009), no. 3, 547–566. MR2526800
- [35] Tony Shaska, *Curves of genus 2 with (n, n) decomposable jacobians*, Journal of Symbolic Computation **31** (2001), no. 5, 603–617. MR1828706
- [36] Christina Birkenhake and Hannes Wilhelm, *Humbert surfaces and the Kummer plane*, Trans. Amer. Math. Soc. **355** (2003), no. 5, 1819–1841. MR1953527
- [37] V. A. Gritsenko and V. V. Nikulin, *Igusa modular forms and “the simplest” Lorentzian Kac-Moody algebras*, Mat. Sb. **187** (1996), no. 11, 27–66. MR1438983
- [38] 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** (1995), no. 2, 271–296. MR1329525
- [39] D. R. Morrison, *On K3 surfaces with large Picard number*, Invent. Math. **75** (1984), no. 1, 105–121. MR728142
- [40] Oskar Bolza, *On binary sextics with linear transformations into themselves*, Amer. J. Math. **10** (1887), no. 1, 47–70. MR1505464
- [41] Alfred Pringsheim, *Zur Transformation zweiten Grades der hyperelliptischen Functionen erster Ordnung*, Math. Ann. **9** (1876), no. 4, 445–475. MR1509868
- [42] Jean-Pierre Serre, *Rational points on curves over finite fields*, notes by F. Gouvea of lectures at Harvard University (1985).
- [43] Maria Corte-Real Santos, Craig Costello, and Sam Frengley, *An algorithm for efficient detection of (n, n) -splittings and its application to the isogeny problem in dimension 2*, Public-key cryptography – pkc 2024, 2024, pp. 157–189.
- [44] Abhinav Kumar, *Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields*, Res. Math. Sci. **2** (2015), Art. 24, 46. MR3427148
- [45] Wouter Castryck, Thomas Decru, and Benjamin Smith, *Hash functions from superspecial genus-2 curves using richelot isogenies*, Journal of Mathematical Cryptology **14** (2020), no. 1, 268–292. Preprint available at Cryptology ePrint Archive, Paper 2019/296, <https://eprint.iacr.org/2019/296>.
- [46] I. Dolgachev and D. Lehavi, *On isogenous principally polarized abelian surfaces*, Curves and abelian varieties, 2008, pp. 51–69. MR2457735
- [47] Benjamin Smith, *Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method*, Arithmetic, geometry, cryptography and coding theory, 2012, pp. 159–170. MR2961408

- [48] Romain Cosset and Damien Robert, *Computing (ℓ, ℓ) -isogenies in polynomial time on Jacobians of genus 2 curves*, Math. Comp. **84** (2015), no. 294, 1953–1975. MR3335899
- [49] Craig Costello and Benjamin Smith, *The supersingular isogeny problem in genus 2 and beyond*, Post-quantum cryptography, [2020] ©2020, pp. 151–168. MR4139650
- [50] Luca De Feo, Cyril Hugouenq, Jérôme Plût, and Éric Schost, *Explicit isogenies in quadratic time in any characteristic*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 267–282. MR3540960
- [51] Thomas Decru and Sabrina Kunzweiler, *Efficient computation of $(3^n, 3^n)$ -isogenies*, Progress in cryptology—AFRICACRYPT 2023, [2023] ©2023, pp. 53–78. MR4638168
- [52] David Lubicz and Damien Robert, *Arithmetic on abelian and Kummer varieties*, Finite Fields Appl. **39** (2016), 130–158. MR3475546
- [53] Craig Costello and Benjamin Smith, *The supersingular isogeny problem in genus 2 and beyond*, Post-Quantum Cryptography (PQCrypto 2020) **12100** (2020), 151–168. MR4139650.
- [54] Christina Delfs and Steven D. Galbraith, *Computing isogenies between supersingular elliptic curves over \mathbb{F}_p* , Designs, Codes and Cryptography **78** (2016), no. 1, 329–346.
- [55] Enric Florit and Benjamin Smith, *Random and zig-zag sampling for genus-2 isogeny graphs*, 2022. Accessed via ePrint.