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

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 $\mathcal{L}_\ell$.

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 $\mathcal{L}_\ell$ 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 $\mathcal{L}_\ell$ that accelerate isogeny problem-solving (e.g., 100× 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 [17] 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 $\operatorname{Hom}(\mathcal{A}, \mathcal{B})$ and the ring of endomorphisms $\mathcal{A} \mapsto \mathcal{A}$ by $\operatorname{End} \mathcal{A}$. In the context of linear algebra, it is often more convenient to work with the $\mathbb{Q}$-vector spaces $\operatorname{Hom}^0(\mathcal{A}, \mathcal{B}) := \operatorname{Hom}(\mathcal{A}, \mathcal{B}) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\operatorname{End}^0 \mathcal{A} := \operatorname{End} \mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Q}$. For an abelian variety $\mathcal{A}$ defined over a number field K, computing $\operatorname{End}_K(\mathcal{A})$ is a harder problem than computing $\operatorname{End}_{\bar{K}}(\mathcal{A})$; see [21, lemma 5.1] for details.

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

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 $\operatorname{End}_K(\mathcal{A})$ determines the $\mathbb{Z}$-module of K-rational endomorphisms. Extending scalars to $\bar{K}$, we compute $\operatorname{End}_{\bar{K}}(\mathcal{A}) = \operatorname{End}_K(\mathcal{A}) \otimes_{\mathbb{Z}} \bar{K}$, leveraging the finite generation of $\operatorname{End}_K(\mathcal{A})$ and the algebraic closure of $\bar{K}$. The lemma follows from the existence of such an extension procedure. □

A homomorphism $f : \mathcal{A} \to \mathcal{B}$ is called an **isogeny** if $\operatorname{Img} f = \mathcal{B}$ and $\ker f$ is a finite group scheme. If an isogeny $\mathcal{A} \to \mathcal{B}$ 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 $f : \mathcal{A} \to \mathcal{B}$ is defined as the degree of the function field extension

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

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

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

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* $f : \mathcal{A} \to \mathcal{B}$*, 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 $f : \mathcal{A} \to \mathcal{B}$ is an isogeny with $\ker f = \mathcal{K}$. Conversely, for an isogeny $f : \mathcal{A} \to \mathcal{B}$, 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. □

Isogenous abelian varieties have commensurable endomorphism rings: if $\mathcal{A}$ and $\mathcal{B}$ are isogenous, then $\operatorname{End}^0(\mathcal{A}) \cong \operatorname{End}^0(\mathcal{B})$. This follows from the existence of isogenies $f : \mathcal{A} \to \mathcal{B}$ and $g : \mathcal{B} \to \mathcal{A}$ 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*

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

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 $\mathcal{A} \sim \prod_{i=1}^r \mathcal{A}_i^{n_i}$, 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 $\mathrm{End}^0(\mathcal{A})$. □

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, $\mathrm{End}^0(\mathcal{A})$ 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. □

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 $\mathcal{A} \to \mathcal{B}$ with kernel isomorphic to H; (ii) given $\mathcal{A}$ and H, determining $\mathcal{B} := \mathcal{A}/H$ and the isogeny $\mathcal{A} \to \mathcal{B}$; (iii) given $\mathcal{A}$ and $\mathcal{B}$, determining if they are isogenous and computing a rational expression for an isogeny $\mathcal{A} \to \mathcal{B}$. For a survey and conjectures, see [15].

The scalar multiplication by n map $[n] : \mathcal{A} \to \mathcal{A}$ is an isogeny with kernel a group scheme of order $n^{2 \dim \mathcal{A}}$; see [26]. We denote $\mathcal{A}[n] = \ker[n](\bar{k})$, whose elements are the n-**torsion points** of $\mathcal{A}$.

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

$$f \circ \hat{f} = \hat{f} \circ f = [n]. \tag{4}$$

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 $\hat{f} : \mathcal{B} \to \mathcal{A}$ 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 $\deg f = n$. □

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

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

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. □

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 [26]). Represent $\mathcal{A}$ as $\mathbb{C}^g/\Lambda$, 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 $\operatorname{Im}(\tau) > 0$. A theta function with characteristic $[a, b]$, where $a, b \in \mathbb{Q}^g$, is defined as

$$\theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z, \tau) = \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i (n+a)^t \tau (n+a) + 2\pi i (n+a)^t (z+b) \right), \tag{6}$$

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

$$\theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z+m, \tau) = \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z, \tau),$$

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

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

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:

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

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 $z' = z + \tau n$:

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

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

Theta functions are sections of line bundles on $\mathcal{A}$. For a level n theta structure, define the functions $\theta \left[\begin{smallmatrix} 0 \\ b \end{smallmatrix} \right] (z, \tau/n)$, where $b \in (\mathbb{Z}/n\mathbb{Z})^g$. These form a basis for the space of sections $\Gamma(\mathcal{A}, \mathscr{L}_0^n)$, where $\mathscr{L}_0$ is the line bundle associated with the principal polarization, and $\mathscr{L}_0^n$ 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

$$\varphi_n : \mathcal{A} \to \mathbb{P}^{n^g - 1}, \quad z \mapsto \left(\theta \left[\begin{smallmatrix} 0 \\ b \end{smallmatrix} \right] (z, \tau/n) \right)_{b \in (\mathbb{Z}/n\mathbb{Z})^g}. \tag{7}$$

For $n \geq 3$, φ_n is an embedding, realizing $\mathcal{A}$ as a projective variety (see [34], Chapter II).

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

Proof. The line bundle $\mathscr{L}_0^n$ 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 $\mathbb{P}^{n^g-1}$. □

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 ([34], Chapter III) provides the functional equation:

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

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*

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

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 [34], Chapter II). □

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 $4a^t b \mod 2$. 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. □

These results underpin the geometric and analytic properties of abelian varieties, with theta functions serving as both coordinates and invariants (see [34] for a comprehensive treatment).

4. Kummer Surfaces

Given an abelian surface $\mathcal{A}$ over a field k, the Kummer surface $\operatorname{Kum}(\mathcal{A})$ is defined as the quotient $\mathcal{A}/\langle \pm 1 \rangle$, where the involution $\iota : \mathcal{A} \to \mathcal{A}$ acts by $\iota(x) = -x$. This quotient is a singular surface with 16 ordinary double points, each corresponding to a 2-torsion point in $\mathcal{A}[2] = \{x \in \mathcal{A}(\bar{k}) \mid 2x = 0\}$, the set of which has cardinality $2^{2\cdot 2} = 16$ over an algebraically closed field. The minimal resolution of $\operatorname{Kum}(\mathcal{A})$ is a smooth K3 surface, obtained by blowing up each double point to introduce a (-2)-curve (see [35] for details). For an abelian surface $\mathcal{A}$ equipped with a principal polarization, the level 2 theta functions induce a map into projective space. Specifically, 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 $\operatorname{Kum}(\mathcal{A}) \to \mathbb{P}^3$. If $\mathcal{A}$ is not a product of elliptic curves, this morphism is an embedding, and the image is a quartic surface in $\mathbb{P}^3$ with 16 nodes reflecting the 2-torsion structure (see [2, Theorem 4.8.1]).

The quotient construction leverages the group structure of $\mathcal{A}$. The involution ι is an automorphism of order 2, and its fixed points, the 2-torsion points, map to singularities on $\operatorname{Kum}(\mathcal{A})$. 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 number of such points, 16, follows from the structure of the 2-torsion subgroup $\mathcal{A}[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$ over $\bar{k}$, as the dimension of $\mathcal{A}$ is 2. The embedding into $\mathbb{P}^3$ arises from the symmetry of the theta functions under ι, and the quartic nature of the image reflects the degree of the line bundle $\mathscr{L}_0^2$ associated with the doubled principal polarization.

Lemma 5. *Let $\mathcal{A}$ be a principally polarized abelian surface over $\mathbb{C}$, not isomorphic to a product of elliptic curves. The map $\varphi_2 : \operatorname{Kum}(\mathcal{A}) \to \mathbb{P}^3$ 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, $\varphi_2 : \mathcal{A} \to \mathbb{P}^3$ factors through the quotient $\pi : \mathcal{A} \to \operatorname{Kum}(\mathcal{A})$, inducing a well-defined map $\overline{\varphi_2} : \operatorname{Kum}(\mathcal{A}) \to \mathbb{P}^3$. For $\mathcal{A}$ principally polarized, the line bundle $\mathscr{L}_0^2$ corresponds to 2Θ, where Θ is the theta divisor. The space of sections $\Gamma(\mathcal{A}, \mathscr{L}_0^2)$ is 4-dimensional, spanned by the θ_i. If $\mathcal{A}$ is not a product $E_1 \times E_2$, the polarization ensures $\mathscr{L}_0^2$ is very ample on $\operatorname{Kum}(\mathcal{A})$, separating points and tangent vectors. Specifically, for distinct points $x, y \in \operatorname{Kum}(\mathcal{A})$ (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 $\operatorname{Kum}(\mathcal{A})$ as a quartic surface with 16 nodes at the images of $\mathcal{A}[2]$. □

4.1. Jacobian Varieties and Surfaces.

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 $\operatorname{Jac}_k(\mathcal{X})$ over k and a uniquely determined embedding

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

satisfying:

(1) For all extension fields L of k, $\operatorname{Jac}_L \mathcal{X} = \operatorname{Pic}^0_{\mathcal{X}_L}(L)$, with this equality given functorially.

(2) For any abelian variety $\mathbb{A}$ and morphism $\eta : \mathcal{X} \to \mathbb{A}$ sending P_0 to $0_{\mathbb{A}}$, there exists a unique homomorphism $\psi : \operatorname{Jac}(\mathcal{X}) \to \mathbb{A}$ such that $\psi \circ \phi_{P_0} = \eta$.

This $\operatorname{Jac}(\mathcal{X})$, 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 $\operatorname{Pic}^0_{\mathcal{X}_L}(L)$.

Lemma 6. *The Jacobian* $\operatorname{Jac}(\mathcal{X})$ *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 $\phi_1 : \mathcal{X} \to \mathcal{J}_1$ and $\phi_2 : \mathcal{X} \to \mathcal{J}_2$. By property (2), there exist homomorphisms $\psi_{12} : \mathcal{J}_1 \to \mathcal{J}_2$ and $\psi_{21} : \mathcal{J}_2 \to \mathcal{J}_1$ 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 $\psi_{21} \circ \psi_{12} = \operatorname{id}_{\mathcal{J}_1}$. Similarly, $\psi_{12} \circ \psi_{21} = \operatorname{id}_{\mathcal{J}_2}$, establishing an isomorphism $\mathcal{J}_1 \cong \mathcal{J}_2$. □

Let L/k be a finite algebraic extension. Then $\operatorname{Jac}_L \mathcal{X}$ is the scalar extension of $\operatorname{Jac} \mathcal{X}$ with L, forming a fiber product with projection $p : \operatorname{Jac}_L \mathcal{X} \to \operatorname{Jac} \mathcal{X}$. The norm map is p_*, and the conorm map is p^*. If $f : \mathcal{X} \to \mathcal{D}$ is a surjective morphism of curves sending P_0 to Q_0, there exists a unique surjective homomorphism $f_* : \operatorname{Jac} \mathcal{X} \to \operatorname{Jac} \mathcal{D}$ such that $f_* \circ \phi_{P_0} = \phi_{Q_0}$. If $\operatorname{Jac} \mathcal{X}$ is simple and $\eta : \mathcal{X} \to \mathcal{D}$ 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 [17].

Abelian varieties of dimension 2 are termed abelian surfaces. When $\mathcal{A} = \operatorname{Jac}(\mathcal{X})$, the Kummer surface $\operatorname{Kum}(\operatorname{Jac}(\mathcal{X}))$ inherits properties from the curve via the embedding φ_2. The 16 nodes correspond to the 2-torsion points of $\operatorname{Jac}(\mathcal{X})$, and the quartic surface in $\mathbb{P}^3$ reflects the polarization's structure, with theta constants determining its equation.

4.2. Kummer Surface and Shioda-Inose Surface.

For an abelian surface $\mathcal{A} = \operatorname{Jac}(\mathcal{X})$, one can attach two K3 surfaces: the Kummer surface and its double cover, the Shioda-Inose surface. Let $\mathfrak{i}$ be the involution on $\operatorname{Jac}(\mathcal{X})$ given by $\mathfrak{i} : \mathfrak{p} \to -\mathfrak{p}$. The quotient $\operatorname{Jac}(\mathcal{X})/\{\mathbb{I}, \mathfrak{i}\}$ is a singular surface with 16 ordinary double points, denoted the *Kummer surface* $\operatorname{Kum}(\operatorname{Jac}(\mathcal{X}))$; see [24].

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

$$\begin{tikzcd}
\operatorname{Jac}(\mathcal{X}) \arrow[dr, dashed, "\pi_0"] & & \mathcal{Y} \arrow[dl, dashed, "\pi_1"] \\
& \operatorname{Kum}(\operatorname{Jac}(\mathcal{X})) &
\end{tikzcd} \tag{11}$$

called a Shioda-Inose structure, induces an isomorphism of integral Hodge structures between the transcendental lattices of $\operatorname{Jac}(\mathcal{X})$ and $\mathcal{Y}$ (see [35]). Specifically, $\mathcal{Y}$ admits an involution fixing the holomorphic (2,0)-form, with quotient $\operatorname{Kum}(\operatorname{Jac}(\mathcal{X}))$, and the degree 2 map $p : \mathcal{Y} \to \operatorname{Kum}(\operatorname{Jac}(\mathcal{X}))$ satisfies a Hodge isometry between $T(\mathcal{Y})(2)$ and $T(\operatorname{Kum}(\operatorname{Jac}(\mathcal{X})))$; see [24].

Lemma 7. *The Shioda-Inose structure induces an isomorphism between the transcendental lattices* $T(\operatorname{Jac}(\mathcal{X}))$ *and* $T(\mathcal{Y})$*, up to scaling.*

Proof. The transcendental lattice $T(\mathrm{Jac}(\mathcal{X}))$ is the orthogonal complement of the Néron-Severi group in $H^2(\mathrm{Jac}(\mathcal{X}), \mathbb{Z})$. The map $\pi_0 : \mathrm{Jac}(\mathcal{X}) \to \mathrm{Kum}(\mathrm{Jac}(\mathcal{X}))$ contracts the 2-torsion cycles, and $p : \mathcal{Y} \to \mathrm{Kum}(\mathrm{Jac}(\mathcal{X}))$ doubles the lattice, with the involution on $\mathcal{Y}$ preserving the (2,0)-form. The Hodge structure on $T(\mathcal{Y})$ aligns with $T(\mathrm{Jac}(\mathcal{X}))$ 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. □

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

$$y^2 + a_1(t)xy + a_3(t)y = x^2 + a_2(t)x^2 + a_4(t)x + a_6(t), \tag{12}$$

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

$$Y^2 = 4X^3 - g_2(t)X - g_3(t), \tag{13}$$

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

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 $\mathrm{End}(\mathcal{A})$ as the ring of regular morphisms $\phi : \mathcal{A} \to \mathcal{A}$ 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, $\mathrm{End}(\mathcal{A})$ forms a $\mathbb{Z}$-module, but its full complexity emerges in the rational endomorphism algebra $\mathrm{End}^0(\mathcal{A}) = \mathrm{End}(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$, 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 $\phi \in \mathrm{End}(\mathcal{A})$ 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 $\hat{\phi} : \mathcal{A} \to \mathcal{A}$ such that $\phi \circ \hat{\phi} = [\deg \phi]$, where $[n] : \mathcal{A} \to \mathcal{A}$ denotes multiplication by n. A key property across all dimensions is that $\mathrm{End}^0(\mathcal{A})$ is invariant under isogeny: if $\mathcal{A}$ and $\mathcal{B}$ are isogenous abelian varieties, meaning there exists an isogeny $f : \mathcal{A} \to \mathcal{B}$, then their rational endomorphism algebras are isomorphic. To see this, consider f with dual $\hat{f}$ satisfying $f \circ \hat{f} = [n]$. The map $\Phi : \mathrm{End}(\mathcal{B}) \to \mathrm{End}(\mathcal{A})$ given by $\Phi(\phi) = f \circ \phi \circ \hat{f}$ is a ring homomorphism, and extending it to $\mathrm{End}^0(\mathcal{B})$ 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 [26], Chapter III, §19). This invariance underpins the study of endomorphism algebras across isogeny classes.

For an abelian variety $\mathcal{A}$, the structure of $\mathrm{End}^0(\mathcal{A})$ 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 ([26], Chapter III, §15). If $\mathcal{A}$ is simple, $\mathrm{End}^0(\mathcal{A})$ is a division algebra over its center Z, and $[Z : \mathbb{Q}] \cdot [\mathrm{End}^0(\mathcal{A}) : Z] = (\dim \mathcal{A})^2 = g^2$. If $\mathcal{A}$ is not simple, $\mathrm{End}^0(\mathcal{A})$ 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 $\operatorname{End}^0(\mathcal{A})$ becomes more precise, especially over $\overline{\mathbb{Q}}$. Here, an endomorphism ϕ acts on a 2-dimensional variety, and the possible structures of $\operatorname{End}^0(\mathcal{A})$ are richly detailed by Albert's classification, as refined in [28]. For a principally polarized abelian surface $\mathcal{A}$—where a polarization $\lambda : \mathcal{A} \to \hat{\mathcal{A}}$ to the dual has degree 1—the algebra $\operatorname{End}^0_{\mathbb{Q}}(\mathcal{A})$ 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, $\operatorname{End}^0(\mathcal{A})$ is a division algebra, and since $\dim \mathcal{A} = 2$, we have $[Z : \mathbb{Q}] \cdot [\operatorname{End}^0(\mathcal{A}) : Z] = 2^2 = 4$. If the center $Z = \mathbb{Q}$, then $\operatorname{End}^0(\mathcal{A})$ 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 $\operatorname{End}^0(\mathcal{A}) = \operatorname{End}^0(E_1) \oplus \operatorname{End}^0(E_2)$, with each $\operatorname{End}^0(E_i)$ 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 $\operatorname{End}^0(\mathcal{A})$ 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 $\operatorname{End}^0(\mathcal{A})$ is isomorphic to one of: $\mathbb{Q}$, a real quadratic field, a CM field of degree 4 over $\mathbb{Q}$, a non-split quaternion algebra over $\mathbb{Q}$, $F_1 \oplus F_2$ where $F_i = \mathbb{Q}$ or an imaginary quadratic field, or 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 $\operatorname{End}^0(\mathcal{A}) = \operatorname{End}(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$ 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, $\operatorname{End}^0(\mathcal{A})$ is a division algebra over its center Z, a number field over $\mathbb{Q}$, and the dimension formula holds: $[Z : \mathbb{Q}] \cdot [\operatorname{End}^0(\mathcal{A}) : Z] = (\dim \mathcal{A})^2 = 4$. Since $\mathcal{A}$ is principally polarized, the Rosati involution $\phi \mapsto \phi^\dagger$ (where $\phi^\dagger = \hat{\lambda}^{-1} \circ \hat{\phi} \circ \lambda$, $\lambda : \mathcal{A} \to \hat{\mathcal{A}}$ the polarization) is positive definite, fixing Z and constraining $\operatorname{End}^0(\mathcal{A})$ to be a division algebra with involution. We consider possible dimensions of Z:

- If $Z = \mathbb{Q}$, then $[Z : \mathbb{Q}] = 1$, and $[\operatorname{End}^0(\mathcal{A}) : \mathbb{Q}] = 4$. Possible division algebras over $\mathbb{Q}$ of dimension 4 include:

  - $\mathbb{Q}$ itself, dimension 1, where $\mathrm{End}^0(\mathcal{A}) = \mathbb{Q}$, and every non-zero endomorphism is an isogeny (multiplication by a rational).
  - A real quadratic field, e.g., $\mathbb{Q}(\sqrt{d})$, $d > 0$ square-free, dimension 2, where $\mathrm{End}^0(\mathcal{A})$ embeds into $M_2(\mathbb{R})$ via real multiplication, satisfying the dimension constraint with $[\mathrm{End}^0(\mathcal{A}) : Z] = 2$.
  - 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 $[\mathrm{End}^0(\mathcal{A}) : Z] = 1$, compatible with complex multiplication and the involution (conjugation).
  - 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 $[\mathrm{End}^0(\mathcal{A}) : Z] = 1$, where the standard involution (conjugation) is positive definite under the polarization.
- If Z is a quadratic field (real or imaginary), $[Z : \mathbb{Q}] = 2$, then $[\mathrm{End}^0(\mathcal{A}) : Z] = 2$. Here, $\mathrm{End}^0(\mathcal{A})$ is a division algebra over a quadratic field:
  - For $Z = \mathbb{Q}(\sqrt{d})$, $d > 0$, $\mathrm{End}^0(\mathcal{A})$ could be a quaternion algebra over Z (dimension 4 over Z, but 8 over $\mathbb{Q}$), exceeding 4, so this is not possible unless $\mathrm{End}^0(\mathcal{A}) = Z$, already covered.
  - 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.
- If Z is quartic, $[Z : \mathbb{Q}] = 4$, then $[\mathrm{End}^0(\mathcal{A}) : Z] = 1$, so $\mathrm{End}^0(\mathcal{A}) = Z$, a CM field, as above.

Thus, for simple $\mathcal{A}$, $\mathrm{End}^0(\mathcal{A})$ 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 $\mathrm{End}^0(\mathcal{A}) = \mathrm{End}^0(E_1) \oplus \mathrm{End}^0(E_2)$, as endomorphisms respect the product structure (no cross-terms exist unless $E_1 \cong E_2$). For an elliptic curve E_i over $\overline{\mathbb{Q}}$:

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

Thus, $\mathrm{End}^0(\mathcal{A}) = F_1 \oplus F_2$, where $F_i = \mathrm{End}^0(E_i)$, yielding dimensions $1{+}1 = 2$ or $2{+}2 = 4$ over $\mathbb{Q}$. If $E_1 \cong E_2$, $\mathrm{End}^0(\mathcal{A}) \cong M_2(F)$, where $F = \mathrm{End}^0(E_1)$, 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, $\mathrm{End}^0(\mathcal{A})$ 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 ([28], §4; [34], Chapter IV).

The dimension bound 4 and semi-simplicity (via Rosati) limit $\mathrm{End}^0(\mathcal{A})$ 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. □

A principal polarization $\lambda : \mathcal{A} \to \hat{\mathcal{A}}$ induces the Rosati involution $\phi \mapsto \phi^\dagger = \hat{\lambda}^{-1} \circ \hat{\phi} \circ \lambda$, fixing the center and ensuring $\mathrm{End}^0(\mathcal{A})$ is semi-simple. The trace form

$\langle \phi, \psi \rangle = \operatorname{tr}(\phi^\dagger \circ \psi)$ is positive definite: for $\phi \neq 0$, $\operatorname{tr}(\phi^\dagger \circ \phi) > 0$, as $\phi^\dagger \circ \phi$ is a non-zero symmetric endomorphism, and the polarization's positivity on $\hat{A}$ guarantees this (see [26], Chapter IV, §21). Thus, $\operatorname{End}^0(\mathcal{A})$ decomposes into simple algebras matching Albert's types.

The dimension of $\operatorname{End}^0(\mathcal{A})$ 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 $\operatorname{Jac}(\mathcal{X})$, $\operatorname{End}^0_{\mathbb{Q}}(\operatorname{Jac} \mathcal{X})$ is typically $\mathbb{Q}$ unless $\mathcal{X}$ has special symmetries, yielding richer structures as detailed in [28].

6. Genus 2 Curves and Their Jacobians

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 [25,31]. 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 $\pi : \mathcal{X} \to \mathbb{P}^1$, 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 [19], 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 [1] 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 $l \in \bar{k}^\star$ 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 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 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

$$y^2 = f(x) = a_6 x^6 + \cdots + a_1 x + a_0, \tag{14}$$

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. The moduli space $\mathcal{M}_2$, via the Torelli morphism, identifies with the moduli space $\mathbb{A}_2$ of principally polarized abelian surfaces that are not products of elliptic curves. The Torelli morphism $\mathcal{X} \mapsto (\operatorname{Jac}(\mathcal{X}), \Theta)$, where $\operatorname{Jac}(\mathcal{X})$ is the Jacobian of $\mathcal{X}$ and Θ is the theta divisor, embeds $\mathcal{M}_2$ into $\mathbb{A}_2$, which has a compactification $\mathbb{A}_2^\star$ as the weighted projective space $\mathbb{P}_{(2,4,6,10)}(k)$ using the invariants J_2, J_4, J_6, J_{10}. Thus,

$$\mathbb{A}_2 \cong \mathbb{P}_{(2,4,6,10)}(k) \setminus \{J_{10} = 0\}, \tag{15}$$

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 $\mathfrak{p} = [J_2 : J_4 : J_6 : J_{10}] \in \mathbb{P}_{(2,4,6,10)}(k)$.

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

A map $f : \mathcal{X} \to \mathcal{D}$ between curves induces homomorphisms $f^* : \mathrm{Jac}(\mathcal{D}) \to \mathrm{Jac}(\mathcal{X})$ (pullback) and $f_* : \mathrm{Jac}(\mathcal{X}) \to \mathrm{Jac}(\mathcal{D})$ (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 $\lambda : \mathcal{A} \to \hat{\mathcal{A}}$ to the dual, and $\mathcal{A}$ is principally polarized if $\deg \lambda = 1$. The theta divisor $\Theta \subset \mathrm{Jac}(\mathcal{X})$, image of ϕ_{P_0}, provides such a polarization, making $\mathrm{Jac}(\mathcal{X})$ a principal case in $\mathbb{A}_2$.

6.1. (n,n)**-Split Jacobians.** A fascinating aspect of genus 2 Jacobians is their potential decomposability. Let $\psi : \mathcal{X} \to E_1$ 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 $E_2 := \mathrm{Jac}(\mathcal{X})/E_1$, defined as the quotient by the connected component of $\ker(\psi_*)$, such that $\mathrm{Jac}(\mathcal{X})$ is isogenous to $E_1 \times E_2$ via an isogeny of degree n^2. We call $\mathrm{Jac}(\mathcal{X})$ (n,n)**-decomposable** or (n,n)**-split**, a property studied in [16]. 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 [31], [33], and [23], respectively.

Consider a genus 2 curve $\mathcal{X}$ and a maximal covering $\psi_1 : \mathcal{X} \to E_1$ of degree n. The induced map $\psi_1^* : E_1 \to \mathrm{Jac}(\mathcal{X})$ is injective, embedding E_1 as a subvariety, and $\psi_{1,*} : \mathrm{Jac}(\mathcal{X}) \to E_1$ has kernel $\ker(\psi_{1,*})$, an elliptic curve E_2 since $\dim \mathrm{Jac}(\mathcal{X}) = 2$ and $\dim E_1 = 1$ (see [32]). Fixing a Weierstrass point $P \in \mathcal{X}$, the embedding

$$\begin{aligned} i_P : \mathcal{X} &\to \mathrm{Jac}(\mathcal{X}) \\ x &\mapsto [(x) - (P)] \end{aligned} \tag{16}$$

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

$$0 \to E_2 \xrightarrow{g} \mathrm{Jac}(\mathcal{X}) \xrightarrow{\psi_{1,*}} E_1 \to 0, \tag{17}$$

and its dual

$$0 \to E_1 \xrightarrow{\psi_1^*} \mathrm{Jac}(\mathcal{X}) \xrightarrow{g^*} E_2 \to 0. \tag{18}$$

If $\deg(\psi_1) = 2$ or odd, $\psi_2 : \mathcal{X} \to E_2$ is unique up to elliptic curve isomorphism, as shown in [33]. The Hurwitz space $\mathbb{H}_\sigma$ 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 [31] (for $n = 2$), [33] (for $n = 3$), and [23] (for $n = 5$). We say $\mathcal{X}$ has an (n, n)-decomposable Jacobian if $\mathrm{Jac}(\mathcal{X})$ admits such a structure, with E_1 and E_2 as its components.

For every $D = J_{10} > 0$, the Humbert hypersurface $H_D \subset \mathcal{M}_2$ parameterizes curves $\mathcal{X}$ whose Jacobians admit an optimal action by the order $\mathcal{O}_D$, a condition tied to embeddings of quadratic fields (see [18]). Points on 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 product E^2 where E is an elliptic curve, a phenomenon prominent on Shimura curves.

Proposition 1. $\mathrm{Jac}(\mathcal{X})$ *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 $\psi : \mathcal{X} \to E_1$, inducing an isogeny $\mathrm{Jac}(\mathcal{X}) \to E_1 \times E_2$ 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 $\bar{k}$, $\mathrm{Jac}(\mathcal{X}) \sim E_1 \times E_2$, with $\dim E_i = 1$. By the theory of maximal coverings ([16]), there exists a degree $n > 1$ map $\psi : \mathcal{X} \to E_1$ (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 $\psi : \mathcal{X} \to E_1$ of degree $n \geq 2$, as genus 2 curves admit non-trivial maps to elliptic curves, inducing the (n, n)-split structure (see [32], §3). □

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

6.2. **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 $\mathcal{L}_\ell$ for $\ell = 2, 3, 5, 7, 11$, providing explicit equations in terms of Igusa invariants J_2, J_4, J_6, J_{10} (see [31], [33], [23] for $\ell = 2, 3, 5$). For $\ell = 2$, $\mathcal{L}_2$ aligns with Richelot's 15 isogenies (Section 7); for odd ℓ, $\mathcal{L}_\ell$ 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 $\mathcal{L}_\ell$ is critical. Over finite fields (e.g., $\mathbb{F}_{p^2}$), a split $\mathrm{Jac}(\mathcal{X}) \in \mathcal{L}_\ell$ 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. [6]. Their algorithm detects (ℓ, ℓ)-splittings using Kumar's parametrisations [20]—matching our $\mathcal{L}_\ell$—speeding up attacks by factors of 16–159 for p from 50 to 1000 bits. This weakens protocols like the Castryck-Decru-Smith hash [4], where split Jacobians enable faster collision finding, suggesting key selection avoid $\mathcal{L}_\ell$ to bolster security.

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

7. Richelot Isogenies of Abelian Surfaces

Richelot isogenies provide a classical framework for studying (2,2)-isogenies between principally polarized abelian surfaces, particularly Jacobians of genus 2 curves. For an abelian surface $\mathcal{A}$, such as the Jacobian $\mathcal{A} = \operatorname{Jac}(\mathcal{X})$ 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 $\bar{k}$ when 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 $2^2 = 4$). It is well-known that the quotient $\hat{\mathcal{A}} = \mathcal{A}/\mathcal{K}$ by such a Göpel group is again a principally polarized abelian surface, as detailed in [27, Sec. 23]. The natural projection $\psi : \mathcal{A} \to \hat{\mathcal{A}}$ 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 $\tau \in \mathbb{H}_2$ (the Siegel upper half-space), 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

$$\begin{gathered} \psi : \mathcal{A} = \mathbb{C}^2/\langle \mathbb{Z}^2 \oplus \tau\mathbb{Z}^2 \rangle \to \hat{\mathcal{A}} = \mathbb{C}^2/\langle \mathbb{Z}^2 \oplus 2\tau\mathbb{Z}^2 \rangle \\ (z, \tau) \mapsto (z, 2\tau), \end{gathered} \tag{19}$$

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 $\mathcal{K} \cap \mathcal{K}' = \{\mathfrak{p}_0\}$, where $\mathfrak{p}_0$ 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 $\psi : \mathcal{A} \to \hat{\mathcal{A}}$. 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 $\hat{\psi} \circ \psi : \mathcal{A} \to \hat{\mathcal{A}} \to \mathcal{A}$, where $\hat{\psi} : \hat{\mathcal{A}} \to \hat{\mathcal{A}}/\hat{\mathcal{K}}$, 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 $\mathcal{A} = \operatorname{Jac}(\mathcal{X})$, where $\mathcal{X}$ is a smooth genus 2 curve, we explore whether $\hat{\mathcal{A}} = \operatorname{Jac}(\hat{\mathcal{X}})$ for another genus 2 curve $\hat{\mathcal{X}}$, and how their moduli relate. Richelot addressed this geometrically in [30], with modern treatments in [3]. 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

$$\Delta_{ABC} \cdot Y^2 = [A, B][A, C][B, C], \tag{20}$$

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 [3] that $\operatorname{Jac}(\mathcal{X})$ and $\operatorname{Jac}(\hat{\mathcal{X}})$ 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 $\operatorname{Jac}(\mathcal{X})$.

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

$$\mathcal{X} : y^2 = xz(x - z)(x - \lambda_1 z)(x - \lambda_2 z)(x - \lambda_3 z), \tag{21}$$

with roots at $0, 1, \lambda_1, \lambda_2, \lambda_3, \infty$, a factorization groups these into pairs, and (20) produces $\hat{\mathcal{X}}$.

7.1. **A Theta Functions Approach.** To compute these isogenies explicitly, we adopt a theta function approach, following [29]. For $\mathcal{A} = \operatorname{Jac}(\mathcal{X})$, consider Göpel groups $\mathcal{K} = \{\mathfrak{p}_0, \mathfrak{p}_{15}, \mathfrak{p}_{23}, \mathfrak{p}_{46}\}$ and $\mathcal{K}' = \{\mathfrak{p}_0, \mathfrak{p}_{12}, \mathfrak{p}_{34}, \mathfrak{p}_{56}\}$, where $\mathcal{A}[2] = \{\mathfrak{p}_i\}_{i=0}^{15}$ labels the 2-torsion points, with $\mathfrak{p}_0$ the identity. These satisfy $\mathcal{K} + \mathcal{K}' = \mathcal{A}[2]$ and $\mathcal{K} \cap \mathcal{K}' = \{\mathfrak{p}_0\}$, 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 $\mathcal{X}$:

$$\mathcal{X} : y^2 = xz(x - z)(x - \lambda_1 z)(x - \lambda_2 z)(x - \lambda_3 z), \tag{22}$$

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

$$\hat{\mathcal{X}} : y^2 = x(x - 1)(x - \Lambda_1)(x - \Lambda_2)(x - \Lambda_3). \tag{23}$$

Theta functions provide coordinates on $\operatorname{Jac}(\mathcal{X})$ and $\operatorname{Jac}(\hat{\mathcal{X}})$. For a period matrix $\tau \in \mathbb{H}_2$, the level 2 theta functions $\theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z, \tau/2)$, with $a, b \in (\mathbb{Z}/2\mathbb{Z})^2$, embed $\operatorname{Kum}(\mathcal{A})$ into $\mathbb{P}^3$, and their values at $z = 0$ (theta constants) determine the moduli. Denote $\theta_i = \theta \left[\begin{smallmatrix} a_i \\ b_i \end{smallmatrix} \right] (0, \tau/2)$ for $\mathcal{X}$ and Θ_i for $\hat{\mathcal{X}}$, with characteristics forming Göpel groups. For $\mathcal{K} = \{\mathfrak{p}_0, \mathfrak{p}_{15}, \mathfrak{p}_{23}, \mathfrak{p}_{46}\}$, corresponding to

$$\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix} \right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix} \right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix} \right), \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix} \right),$$

we label $\theta_1, \theta_2, \theta_3, \theta_4$. The isogeny $\psi : \operatorname{Jac}(\mathcal{X}) \to \operatorname{Jac}(\hat{\mathcal{X}})$ 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 [29] and [5] give

$$\Lambda_1 = \frac{\Theta_1^2 \Theta_3^2}{\Theta_2^2 \Theta_4^2}, \quad \Lambda_2 = \frac{\Theta_3^2 \Theta_8^2}{\Theta_4^2 \Theta_{10}^2}, \quad \Lambda_3 = \frac{\Theta_1^2 \Theta_8^2}{\Theta_2^2 \Theta_{10}^2}, \tag{24}$$

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

The Richelot isogeny corresponds to factoring $f_6 = xz(x - z)(x - \lambda_1 z)(x - \lambda_2 z)(x - \lambda_3 z)$ into

$$A = (x - \lambda_1 z)(x - z), \quad B = (x - \lambda_2 z)(x - \lambda_3 z), \quad C = x(x - \infty z),$$

adjusting for homogeneity (e.g., $C = xz$ at infinity). Applying (20), 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

$$\begin{aligned}
\Lambda_1 &= \frac{(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2)(\theta_1^2 - \theta_2^2 - \theta_3^2 + \theta_4^2)}{(\theta_1^2 + \theta_2^2 - \theta_3^2 - \theta_4^2)(\theta_1^2 - \theta_2^2 + \theta_3^2 - \theta_4^2)},\\
\Lambda_2 &= \frac{(\theta_1^2 - \theta_2^2 - \theta_3^2 + \theta_4^2)(\theta_1^2\theta_2^2 + \theta_3^2\theta_4^2 + 2\theta_1\theta_2\theta_3\theta_4)}{(\theta_1^2 - \theta_2^2 + \theta_3^2 - \theta_4^2)(\theta_1^2\theta_2^2 - \theta_3^2\theta_4^2)},\\
\Lambda_3 &= \frac{(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2)(\theta_1^2\theta_2^2 + \theta_3^2\theta_4^2 + 2\theta_1\theta_2\theta_3\theta_4)}{(\theta_1^2 + \theta_2^2 - \theta_3^2 - \theta_4^2)(\theta_1^2\theta_2^2 - \theta_3^2\theta_4^2)},
\end{aligned}\tag{25}$$

matching the Richelot construction's invariants, verifying isomorphism.

For $\mathcal{K}' = \{\mathfrak{p}_0, \mathfrak{p}_{12}, \mathfrak{p}_{34}, \mathfrak{p}_{56}\}$, the dual isogeny $\hat{\psi} : \hat{\mathcal{A}} \to \mathcal{A} = \hat{\mathcal{A}}/\hat{\mathcal{K}}$ 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 [5].

Proposition 2. *The moduli of $\mathcal{X}$ in (21) and $\hat{\mathcal{X}}$ in (23) satisfy*

$$\begin{aligned}
\Lambda_1' &= 2\frac{2\lambda_1' - \lambda_2' - \lambda_3'}{\lambda_2' - \lambda_3'}, & \lambda_1' &= 2\frac{2\Lambda_1' - \Lambda_2' - \Lambda_3'}{\Lambda_2' - \Lambda_3'},\\
\Lambda_2' - \Lambda_1' &= -\frac{4(\lambda_1' - \lambda_2')(\lambda_1' - \lambda_3')}{(\lambda_1' + 2)(\lambda_2' - \lambda_3')}, & \lambda_2' - \lambda_1' &= -\frac{4(\Lambda_1' - \Lambda_2')(\Lambda_1' - \Lambda_3')}{(\Lambda_1' + 2)(\Lambda_2' - \Lambda_3')},\\
\Lambda_3' - \Lambda_1' &= -\frac{4(\lambda_1' - \lambda_2')(\lambda_1' - \lambda_3')}{(\lambda_1' - 2)(\lambda_2' - \lambda_3')}, & \lambda_3' - \lambda_1' &= -\frac{4(\Lambda_1' - \Lambda_2')(\Lambda_1' - \Lambda_3')}{(\Lambda_1' - 2)(\Lambda_2' - \Lambda_3')}.
\end{aligned}\tag{26}$$

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

$$\psi : \mathcal{A} = \mathrm{Jac}(\mathcal{X}) \to \hat{\mathcal{A}} = \mathrm{Jac}(\hat{\mathcal{X}}) = \mathcal{A}/\mathcal{K},\tag{27}$$

for the maximal isotropic subgroup $\mathcal{K}$.

8. Computing (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

$$\phi : \mathrm{Jac}(\mathcal{X}) \to \mathrm{Jac}(\mathcal{Y}),\tag{28}$$

where $\mathcal{X}$ and $\mathcal{Y}$ are genus 2 curves over a field k with char $k \neq 2$, and $\mathrm{Jac}(\mathcal{X})$ and $\mathrm{Jac}(\mathcal{Y})$ are their Jacobians, each a 2-dimensional principally polarized abelian surface. Let $\Theta_{\mathcal{X}}$ and $\Theta_{\mathcal{Y}}$ denote the theta divisors on $\mathrm{Jac}(\mathcal{X})$ and $\mathrm{Jac}(\mathcal{Y})$, respectively, where $\Theta_{\mathcal{X}}$ is the image of $\mathcal{X}$ under an embedding such as $\phi_{P_0} : \mathcal{X} \to \mathrm{Jac}(\mathcal{X})$, $P \mapsto [(P) - (P_0)]$, 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 $\mathrm{Kum}(\mathrm{Jac}(\mathcal{Y})) = \mathrm{Jac}(\mathcal{Y})/\langle \pm 1\rangle$, 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 [13].

For $\mathcal{X}$ given by

$$y^2 = f(x) = a_6x^6 + \cdots + a_1x + a_0, \tag{29}$$

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

$$D_\infty := (1 : \sqrt{f(1)} : 0) + (1 : -\sqrt{f(1)} : 0), \tag{30}$$

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

$$W_{\mathcal{X}} := \sum_{i=1}^{6} (x_i, 0, z_i). \tag{31}$$

A canonical divisor on $\mathcal{X}$ is

$$\mathcal{K}_{\mathcal{X}} = W_{\mathcal{X}} - 2D_\infty, \tag{32}$$

as $\deg W_{\mathcal{X}} = 6$, $\deg D_\infty = 2$, and $2g-2 = 2$. A divisor $D \in \mathrm{Jac}(\mathcal{X})$ 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

$$\rho_{2\ell} : \mathbb{P}^2 \to \mathbb{P}^{2\ell}, \quad (x, y, z) \mapsto (z^{2\ell}, xz^{2\ell-1}, \dots, x^{2\ell-1}z, x^{2\ell}), \tag{33}$$

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

$$W := \langle \rho_{2\ell}(W_{\mathcal{X}}) \rangle \subset \mathbb{P}^{2\ell} \tag{34}$$

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

$$\mathcal{L}_{P,Q} = \begin{cases} \langle \rho_{2\ell}(P), \rho_{2\ell}(Q) \rangle & \text{if } P \notin \{Q, \tau(Q)\}, \\ T_{\rho_{2\ell}(P)}(\mathcal{R}_{2\ell}) & \text{otherwise,} \end{cases} \tag{35}$$

where τ is the hyperelliptic involution. Dolgachev and Lehavi ([13]) proved:

Theorem 6 (Dolgachev-Lehavi)**.** *Let $\mathcal{X}$ be a genus 2 curve, $S \subset \mathrm{Jac}(\mathcal{X})[\ell]$ an isotropic subgroup of order ℓ^2, and $\rho_{2\ell} : \mathcal{X} \to \mathcal{R}_{2\ell} \subset \mathbb{P}^{2\ell}$ 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 $\mathbb{P}^{2\ell} \to \mathbb{P}^3$ 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 $\mathrm{Jac}(\mathcal{Y}) \cong \mathrm{Jac}(\mathcal{X})/S$.

Proof. The linear system $|\ell\Theta_{\mathcal{X}}|$ on $\operatorname{Jac}(\mathcal{X})$ has dimension ℓ^2-1 (projective dimension of divisors modulo scalars), and for an isotropic S of order ℓ^2, $\operatorname{Jac}(\mathcal{Y}) = \operatorname{Jac}(\mathcal{X})/S$ 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 $\operatorname{Kum}(\operatorname{Jac}(\mathcal{Y}))$ 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 ℓ^2-1 secants $\mathcal{L}_e$ intersect H in points spanning a subspace N of dimension ℓ^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 $\operatorname{Jac}(\mathcal{Y}) \cong \operatorname{Jac}(\mathcal{X})/S$ ([13], Theorem 1). □

Smith ([36]) developed an algorithm using this theorem, effective for $\ell = 3$ ($|S| = 9$), refined in [7], [9], [10], and [11]. 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 [11] include optimized secant computations and invariant recovery.

8.1. Computing (n,n)-Isogenies via Kummer Surface.

For an (n,n)-isogeny $\phi : \operatorname{Jac}(\mathcal{X}) \to \operatorname{Jac}(\mathcal{Y})$ with kernel $S \subset \operatorname{Jac}(\mathcal{X})[n]$ of order n^2, the Kummer surface $\operatorname{Kum}(\operatorname{Jac}(\mathcal{X}))$ 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

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

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

Theorem 7. *For an isotropic $S \subset \operatorname{Jac}(\mathcal{X})[n]$ 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 $\operatorname{Jac}(\mathcal{Y}) \cong \operatorname{Jac}(\mathcal{X})/S$.*

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 $\operatorname{Kum}(\operatorname{Jac}(\mathcal{Y}))$. 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 $\operatorname{Jac}(\mathcal{X})/S$. □

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.

8.2. 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 $\operatorname{Kum}(\operatorname{Jac}(\mathcal{X}))$, 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 [22], offering a higher-dimensional analog to Vélu's formulas for elliptic curves. For a genus 2 curve $\mathcal{X}$ over a field k with char $k \neq 2$, the Jacobian $\operatorname{Jac}(\mathcal{X})$ is a principally polarized abelian surface, and its Kummer surface $\operatorname{Kum}(\operatorname{Jac}(\mathcal{X})) = \operatorname{Jac}(\mathcal{X})/\langle \pm 1 \rangle$ embeds into $\mathbb{P}^3$ via level 2 theta functions. An (ℓ,ℓ)-isogeny $\phi : \operatorname{Jac}(\mathcal{X}) \to \operatorname{Jac}(\mathcal{Y}) = \operatorname{Jac}(\mathcal{X})/S$, where $S \subset \operatorname{Jac}(\mathcal{X})[\ell]$ is an isotropic subgroup of order ℓ^2, requires determining both the codomain $\operatorname{Jac}(\mathcal{Y})$ and the map ϕ. The Lubicz-Robert formula achieves this by expressing theta coordinates in terms of sums over S.

Over $\mathbb{C}$, represent $\operatorname{Jac}(\mathcal{X}) = \mathbb{C}^2/\Lambda$ with $\Lambda = \mathbb{Z}^2 \oplus \tau\mathbb{Z}^2$, where $\tau \in \mathbb{H}_2$ is the period matrix. The ℓ-torsion subgroup $\operatorname{Jac}(\mathcal{X})[\ell] = \{P \in \operatorname{Jac}(\mathcal{X}) \mid [\ell]P = 0\}$ has order $\ell^{2g} = \ell^4$ for $g = 2$, and an isotropic $S \subset \operatorname{Jac}(\mathcal{X})[\ell]$ 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

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \tau) = \sum_{m\in\mathbb{Z}^2} \exp\left(\pi i(m + a)^t\tau(m + a) + 2\pi i(m + a)^t(z + b)\right), \tag{36}$$

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

The Lubicz-Robert formula addresses two tasks: computing the theta null points of $\operatorname{Jac}(\mathcal{Y})$ and evaluating ϕ at points in $\operatorname{Jac}(\mathcal{X})$. 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 $r \le 4$), and choose generators $s_1, s_2 \in S$ such that $S = \langle a_1s_1, a_2s_1, a_3s_2, a_4s_2\rangle$ in a suitable basis. The formula comprises:

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

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

  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 $P \in \operatorname{Jac}(\mathcal{X})$,

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

Theorem 8 (Lubicz-Robert)**.** *For an isotropic subgroup $S \subset \operatorname{Jac}(\mathcal{X})[\ell]$ of order ℓ^2, the theta coordinates $\hat{\theta}_i$ and $\phi(P)_i$ computed via the above formulas define the codomain $\operatorname{Jac}(\mathcal{Y}) = \operatorname{Jac}(\mathcal{X})/S$ and the isogeny $\phi : \operatorname{Jac}(\mathcal{X}) \to \operatorname{Jac}(\mathcal{Y})$, respectively, with complexity $O(\ell^2)$ field operations for a general $\ell = a_1^2 + \cdots + a_r^2$.*

Proof. Represent $\operatorname{Jac}(\mathcal{X}) = \mathbb{C}^2/\Lambda$, and $\operatorname{Jac}(\mathcal{Y}) = \mathbb{C}^2/\hat{\Lambda}$, where $\hat{\Lambda} = \mathbb{Z}^2 \oplus \ell\tau\mathbb{Z}^2 + S$. The theta functions on $\operatorname{Jac}(\mathcal{Y})$ are derived from $\operatorname{Jac}(\mathcal{X})$ 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 $r \le 4$, 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 $\operatorname{Jac}(\mathcal{Y})$'s theta structure ([22], Theorem 4.1). □

On $\operatorname{Kum}(\operatorname{Jac}(\mathcal{X}))$, $\hat{\theta}_i$ determine $\operatorname{Kum}(\operatorname{Jac}(\mathcal{Y}))$'s quartic equation, and $\phi(P)_i$ maps Kummer points, preserving the (16,6)-configuration (16 nodes from $\operatorname{Jac}(\mathcal{X})[2]$, each on 6 tropes). For $\mathcal{X} : y^2 = f(x)$, choose $S \subset \operatorname{Jac}(\mathcal{X})[\ell]$ (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 $\operatorname{Kum}(\operatorname{Jac}(\mathcal{X})) \to \operatorname{Kum}(\operatorname{Jac}(\mathcal{Y}))$, maintaining geometric properties ([26], Chapter III).

Proposition 3. *The Lubicz-Robert formula on* $\mathrm{Kum}(\mathrm{Jac}(\mathcal{X}))$ *determines* $\mathcal{Y}$*'s equation via theta nulls* $\hat{\theta}_i$*, and* ϕ*'s action on* $\mathrm{Kum}(\mathrm{Jac}(\mathcal{X}))$ *preserves the (16,6)-configuration of tropes and nodes.*

Proof. The $\hat{\theta}_i$ define $\mathrm{Kum}(\mathrm{Jac}(\mathcal{Y}))$'s quartic in $\mathbb{P}^3$, from which $\mathcal{Y}$'s Rosenhain form is derived via Igusa invariants ([22], §5). The (16,6)-configuration maps under ϕ to $\mathrm{Jac}(\mathcal{Y})[2]$, preserving isotropy and structure, as the formula respects the Weil pairing's symmetry ([26], Chapter III). □

This method also intersects with the geometric classification of genus 2 curves. The loci $\mathcal{L}_\ell$, described in Subsection 6.2 as irreducible 2-dimensional subvarieties of $\mathcal{M}_2$ where $\mathrm{Jac}(\mathcal{X})$ 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. [6]. 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 $\mathcal{L}_\ell$ does not directly aid in computing ϕ, it provides a geometric testbed. Given $\mathcal{X} \in \mathcal{L}_\ell$, the formula yields $\mathrm{Jac}(\mathcal{Y}) = E_1 \times E_2$, 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 $\mathcal{L}_\ell$ (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. [6]. Their use of $\mathcal{L}_\ell$ 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.

9. 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 $\mathcal{L}_\ell$ 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.

9.1. The Costello et al. Attack.

A notable attack on the dimension 2 superspecial isogeny problem, due to Costello et al. [6], optimizes the earlier Costello-Smith algorithm [8] for finding an isogeny $\phi : \mathrm{Jac}(\mathcal{X}) \to \mathrm{Jac}(\mathcal{Y})$ 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 [12]. 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 $\mathcal{L}_\ell$ 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 [6]), yielding speedups of 16–159× for p from 50 to 1000 bits. The asymptotic complexity remains $\tilde{O}(p/\ell^3)$, but the practical efficiency significantly improves cryptanalysis.

9.2. **Impact on Genus 2 Cryptography.** This acceleration impacts protocols reliant on the superspecial isogeny problem, such as the Castryck-Decru-Smith (CDS) hash function [4], which maps inputs via Richelot isogenies in $\Gamma_2(2;p)$. For a split $\mathrm{Jac}(\mathcal{X}) \in \mathcal{L}_\ell$, 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 [14]. For a 100-bit prime, a 25× 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× 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 $\mathrm{Jac}(\mathcal{Y})$ lying in $\mathcal{L}_\ell$, 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.

9.3. **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:

- *Kernel Recovery*: A method to extract the secret kernel $S \subset \mathrm{Jac}(\mathcal{X})[\ell^k]$ 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.
- *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 [14]) or endomorphism ring computation, remains elusive.
- *Quantum Advantage*: A quantum algorithm (e.g., claw-finding variant) achieving $\mathrm{poly}(\log p)$ time, beyond the current $\tilde{O}(\sqrt{p}/\ell^{3/2})$ from Grover's search, is unachieved for genus 2.
- *Protocol Flaws*: Exploits like degree conversion (e.g., from $(2^n\ell, 2^n\ell)$ to (ℓ^k, ℓ^k), conjectured in [6]) 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.

9.4. **Connection to This Work.** Our computation of $\mathcal{L}_\ell$ for $\ell = 2, 3, 5, 7, 11$ (Subsection 6.2) and (ℓ, ℓ)-isogeny algorithms (Section 8) intersect with this cryptanalysis. While $\mathcal{L}_\ell$ 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 $\mathcal{L}_\ell$ to larger ℓ or integrating with quantum methods could further refine security analysis, balancing constructive and cryptanalytic roles.

10. 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 $\mathcal{L}_\ell$ for $\ell = 2, 3, 5, 7, 11$ reveal a cryptographic vulnerability: split Jacobians enable attacks like Costello et al.'s [6], reducing complexity (e.g., 100x for 1000-bit p). Avoiding $\mathcal{L}_\ell$ 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] 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

[2] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, 2nd ed., Grundlehren der mathematischen Wissenschaften, vol. 302, Springer-Verlag, Berlin, Heidelberg, 2004. See Theorem 4.8.1 for the embedding of Kummer surfaces.

[3] Jean-Benoit Bost and Jean-Francois Mestre, *Moyenne arithmetico-géometrique et periodes des courbes de genre* 1 *et* 2, Gaz. Math. **38** (1988), 36–64. MR970659

[4] 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.

[5] Adrian Clingher and Andreas Malmendier, *Normal forms for Kummer surfaces*, Integrable systems and algebraic geometry. Vol. 2, 2020, pp. 119–174. MR4421430

[6] 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.

[7] 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

[8] Craig Costello and Benjamin Smith, *The supersingular isogeny problem in genus 2 and beyond*, Post-Quantum Cryptography (PQCrypto 2020) **12100** (2020), 151–168. MR4139650.

[9] ———, *The supersingular isogeny problem in genus 2 and beyond*, Post-quantum cryptography, [2020] ©2020, pp. 151–168. MR4139650

[10] Luca De Feo, Cyril Hugounenq, 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

[11] Thomas Decru and Sabrina Kunzweiler, *Efficient computation of $(3^n, 3^n)$-isogenies*, Progress in cryptology—AFRICACRYPT 2023, [2023] ©2023, pp. 53–78. MR4638168

[12] 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.

[13] I. Dolgachev and D. Lehavi, *On isogenous principally polarized abelian surfaces*, Curves and abelian varieties, 2008, pp. 51–69. MR2457735

[14] Enric Florit and Benjamin Smith, *Random and zig-zag sampling for genus-2 isogeny graphs*, 2022. Accessed via ePrint.

[15] Gerhard Frey, *Isogenies in theory and praxis*, Open problems in mathematics and computational science, 2014, pp. 37–68. MR3330877

[16] Gerhard Frey and Ernst Kani, *Correspondences on hyperelliptic curves and applications to the discrete logarithm*, 2011, pp. 1–19.

[17] Gerhard Frey and Tony Shaska, *Curves, Jacobians, and cryptography*, Algebraic curves and their applications, [2019] ©2019, pp. 279–344. MR3916746

[18] 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

[19] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR0114819

[20] 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

[21] Davide Lombardo, *Computing the geometric endomorphism ring of a genus 2 jacobian*, arxiv (2016).

[22] David Lubicz and Damien Robert, *Arithmetic on abelian and Kummer varieties*, Finite Fields Appl. **39** (2016), 130–158. MR3475546

[23] 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

[24] A. Malmendier and T. Shaska, *From hyperelliptic to superelliptic curves*, Albanian J. Math. **13** (2019), no. 1, 107–200. MR3978315

[25] 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

[26] 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

[27] ———, *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

[28] Frans Oort, *Endomorphism algebras of abelian varieties*, Algebraic geometry and commutative algebra, Vol. II, 1988, pp. 469–502. MR977774

[29] 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

[30] 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

[31] 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

[32] Tony Shaska, *Curves of genus 2 with $\langle n, n\rangle$ decomposable jacobians*, Journal of Symbolic Computation **31** (2001), no. 5, 603–617. MR1828706

[33] ______, *Genus 2 fields with degree 3 elliptic subfields*, Forum Mathematicum **16** (2004), no. 2, 263–280. MR2039100

[34] 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.

[35] 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.

[36] 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