AN ANALOG OF THE EDWARDS MODEL FOR JACOBIANS OF GENUS 2 CURVES

E. V. FLYNN AND KAMAL KHURI-MAKDISI

Abstract. We give the explicit equations for a $\mathbf{P}^3 \times \mathbf{P}^3$ embedding of the Jacobian of a curve of genus 2, which gives a natural analog for abelian surfaces of the Edwards curve model of elliptic curves. This gives a much more succinct description of the Jacobian variety than the standard version in $\mathbf{P}^{15}$. We also give a condition under which, as for the Edwards curve, the abelian surfaces have a universal group law.

1. Introduction

In [BL07] (generalising the form given in [Edw07]) a version of the model of an elliptic curve and its group law are given, which have a particularly elegant explicit description, subject to the existence of D_1, a point of order 4, defined over the ground field. An interpretation of this embedding is to say that, if D is any point on the standard Weierstrass model of an elliptic curve, then we map D into $\mathbf{P}^1 \times \mathbf{P}^1$, via the projective x-coordinate of D, together with the projective x-coordinate of $D + D_1$. This model becomes more succinct if we diagonalise the coordinates on $\mathbf{P}^1$ with respect to addition by E_1, where $E_1 = 2D_1$ is of order 2.

In this article, we give an analog for Jacobians of curves of genus 2, which have D_1, a point of order 4 defined over the ground field, as well as E_2, a point of order 2 independent from $E_1 = 2D_1$. We make use of the embedding of the Kummer surface in $\mathbf{P}^3$, given on p.18 of [CF96]. Our embedding of a point D on the Jacobian variety into $\mathbf{P}^3 \times \mathbf{P}^3$ will be via the image of D, together with the image of $D + D_1$ on the Kummer surface. This model becomes more succinct if we diagonalise the coordinates on $\mathbf{P}^3$ with respect to addition by both E_1 and E_2.

In Section 2, we develop these ideas geometrically; the main results will be Theorem 2.27, which describes how many independent defining equations there are of each bidegree, and Theorem 2.28 which describes the degree of the equations in the matrices which give the group law. In Section 3, we give a brief derivation of the Edwards curve, in the above style, explaining how the group law is universal when a specified point is not defined over the ground field; when we say that the group law is universal, we are referring to its application to rational points over the base field. In Section 4, we derive our $\mathbf{P}^3 \times \mathbf{P}^3$ embedding of the Jacobian variety

1991 *Mathematics Subject Classification.* 11G30, 11G10, 14H40.

Key words and phrases. Jacobian, Abelian Variety.

February 7, 2024.

Both authors thank Michael Stoll for organizing the Rational Points 2019 workshop in Schney, where they began working together on this problem. The second named author (KKM) gratefully acknowledges generous funding and a supportive research environment during long scientific visits at both the Max Planck Institute for Mathematics in Bonn (2021) and the Institute for Advanced Study in Princeton (2022, with funding from the Charles Simonyi Endowment).

of our genus 2 curve, giving explicitly a set of defining equations for the variety in Theorem 4.2 (using Theorem 2.27 to know that we have a complete set of defining equations), and its group law in Theorem 4.1. These are considerably more succinct than the standard versions in $\mathbf{P}^{15}$, such as those described in [CF96]. We also give a twisted version of the abelian surface, analogous to the twist performed on Edwards curves. In Section 5, we also give in Corollary 5.2 (a consequence of Theorem 5.1) a condition on the parameters under which, as for the Edwards curve, the abelian surfaces have a universal group law. The situation here is more subtle since the degenerate locus is geometrically a possibly reducible curve (rather than a pair of points, as in the elliptic curve case), and so we need to construct a condition on the parameters that prevents this curve from having any points over the ground field.

2. Generators of the ideal of relations

Our intention in this section is to describe a $\mathbf{P}^3 \times \mathbf{P}^3$ embedding of the Jacobian of a genus two curve; the main results will be Theorem 2.27, which describes how many independent defining equations there are of each bidegree, and Theorem 2.28 which describes the degree of the equations in the matrices which give the group law. Note that the statements of Theorem 2.27 and Theorem 2.28 are what will be used later in Section 4; otherwise, the notation and objects in Section 2 will not be required later. Any reader who is primarily interested in the results of Sections 4 and 5 (and not interested in the justification of the theorems in this section) is welcome just to read the statements of Theorem 2.27 and Theorem 2.28, and otherwise proceed to Section 3.

We work with the Jacobian $\mathfrak{J}$ of a genus two curve $\mathcal{C}$ throughout, viewing $\mathfrak{J}$ as $\mathrm{Pic}^0\mathcal{C}$. Then $\mathfrak{J}$ is a principally polarized abelian surface. The article [LR16], which does not limit itself to Jacobians (or for that matter to dimension 2), already introduces the idea of using the Kummer coordinates of a point $p \in \mathfrak{J}$, along with the Kummer coordinates of $p+p_0$ for a fixed p_0 that is not a 2-torsion point. They consider a general p_0, and observe that the resulting map $\mathfrak{J} \to \mathbf{P}^3 \times \mathbf{P}^3$ given by $p \mapsto (\kappa(p), \kappa(p+p_0))$ for the Kummer map κ gives an embedding of $\mathfrak{J}$ into $\mathbf{P}^3 \times \mathbf{P}^3$, provided p_0 is not a point of order 2. They also prove a number of results and give effective methods to work with $\mathfrak{J}$, using differential additions and other constructions that involve viewing the fibre of κ (or its translate) over a rational point of $\mathfrak{J}$ as the spectrum of a two-dimensional algebra over the ground field, so as to capture the two preimages in $\mathfrak{J}$ even if they are not individually rational.

In this article, we restrict to $p_0 = D_1$, a point of exact order 4, and will impose in Section 4 certain rationality conditions on the subgroup $H \subset \mathfrak{J}$ generated by D_1 and a second point D_2 of exact order 4. We alert the reader that H is not isotropic under the Weil pairing on $\mathfrak{J}[4]$: in fact, $e_4(D_1, D_2) = -1$. On the other hand, the subgroup $2H \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ is isotropic in $\mathfrak{J}[2]$, and corresponds to the kernel of a Richelot isogeny.

We first describe the Edwards-like construction over an algebraically closed field $\overline{K}$, without worrying about rationality over the ground field K. In this section, we routinely identify $\mathcal{C}$ and $\mathfrak{J}$ with their set of $\overline{K}$-valued points. We require $\overline{K}$ not to be of characteristic 2, so as to invoke the basic addition formula of Mumford (p. 324 in Section 3 of [Mum66]; see also Theorem 8 of [Kem89a]). This addition formula, which follows from the isogeny theorem for algebraic theta functions, is an algebraic generalization of the analytic addition formula (2.3) for complex theta

series. The algebraic formulas we write down, Theorem 2.2 and Corollary 2.6, are direct consequences of the basic addition formula, but it is helpful for us to write them down explicitly and concretely, with a careful note of isomorphisms such as $h = h_{p,q}$ in (2.18) and $\phi \circ j$ in (2.22).

If the reader is willing to accept that the structure of our results for general $\overline{K}$ is completely mirrored by the structure when $\overline{K} = \mathbf{C}$, then it may be helpful to consult an earlier version of this article, available at

`https://arxiv.org/abs/2211.01450v2`

where a shorter analytic version of the argument in this section is given, using explicit computations with complex theta functions.

Preliminaries. For a (geometric) point $x \in \mathfrak{J}$, we denote by $T_x : \mathfrak{J} \to \mathfrak{J}$ the translation map: thus $T_x(p) = p + x$. For $k \in \mathbf{Z}$, we denote by $[k] : \mathfrak{J} \to \mathfrak{J}$ the multiplication by k. For $k \geq 2$, with k invertible in $\overline{K}$ (mostly $k = 2$ or $k = 4$), we write $\mathfrak{J}[k]$ for the kernel of $[k]$. Then $\mathfrak{J}[k]$ is isomorphic to $(\mathbf{Z}/k\mathbf{Z})^4$.

The abelian surface $\mathfrak{J}$ is principally polarized; let $\mathcal{L}$ be a symmetric line bundle on $\mathfrak{J}$ (meaning $[-1]^*\mathcal{L} \cong \mathcal{L}$) giving rise to the principal polarization. Then the isomorphism class of $\mathcal{L}$ is unique up to replacing $\mathcal{L}$ by $T_x^*\mathcal{L}$ for some $x \in \mathfrak{J}[2]$. Nonetheless, the isomorphism class of $\mathcal{L}^2$ (hence also of any even power of $\mathcal{L}$) is unique; in the terminology of [Mum66], the bundle $\mathcal{L}^2$ is totally symmetric.

When $\overline{K} = \mathbf{C}$, we can view $\mathfrak{J}$ analytically as the complex torus $\mathbf{C}^2/(\mathbf{Z}^2 + \Omega\mathbf{Z}^2)$, where $\mathbf{Z}^2$ and $\mathbf{C}^2$ are spaces of column vectors, and $\Omega \in \mathcal{H}_2$ is a point in the Siegel upper half-space; that is, Ω is a symmetric matrix in $M_2(\mathbf{C})$ whose imaginary part is positive definite. In that setting, one can use complex-analytic theta functions to describe global sections of the powers $\mathcal{L}^k$ of (one choice of) the line bundle $\mathcal{L}$. We normalize our complex theta functions as follows.

Definition 2.1. Let $k \geq 1$, and let $\beta \in \mathbf{Z}^2$. For $z \in \mathbf{C}^2$ we define

$$\theta_{k,\beta}(z) = \sum_{n \in \beta + k\mathbf{Z}^2} e\left(\frac{n \cdot \Omega n}{2k} + n \cdot z\right), \tag{2.1}$$

where $e(x) = \exp(2\pi i x)$ for $x \in \mathbf{C}$, and $\cdot$ is the standard bilinear product on $\mathbf{C}^2$, so $n \cdot \Omega n = {}^t n \Omega n$ and $n \cdot z = {}^t n z$. Note that $\theta_{k,\beta}$ depends only on the image of β in $(\mathbf{Z}/k\mathbf{Z})^2$. In terms of theta functions with characteristics (see [Mum83], page 123), we have $\theta_{k,\beta}(z) = \theta\left[\begin{smallmatrix}\beta/k \\ 0\end{smallmatrix}\right](k\Omega, kz)$.

In the above analytic setting, it is standard that the functions $\{\theta_{k,\beta}\}_{\beta \in (\mathbf{Z}/k\mathbf{Z})^2}$ are a basis for $H^0(\mathfrak{J}, \mathcal{L}^k)$. Here the space $H^0(\mathfrak{J}, \mathcal{L}^k)$ can be identified with the space of holomorphic functions $f : \mathbf{C}^2 \to \mathbf{C}$ which transform according to

$$\begin{aligned} f(z + \ell) &= f(z), \qquad \ell \in \mathbf{Z}^2, \\ (f|_k m)(z) := e(km \cdot \Omega m/2 + km \cdot z) f(z + \Omega m) &= f(z), \qquad m \in \mathbf{Z}^2. \end{aligned} \tag{2.2}$$

We also have the standard addition formula, for $\beta, \beta' \in \mathbf{Z}^2$ and $z, w \in \mathbf{C}^2$:

$$\theta_{k,\beta}(z + w)\theta_{k,\beta'}(z - w) = \sum_{c \in (\mathbf{Z}/2\mathbf{Z})^2} \theta_{2k,\beta+\beta'+kc}(z)\theta_{2k,\beta-\beta'+kc}(w). \tag{2.3}$$

In the above, the sum is over representatives $c \in \{{}^t(0,0), {}^t(1,0), {}^t(0,1), {}^t(1,1)\}$, so kc makes sense as a 2-torsion element in $(\mathbf{Z}/2k\mathbf{Z})^2$.

For general $\overline{K}$, we will use an algebraic version of the above formula, primarily in the case where $k = 2$ and $2k = 4$. We will also need the analog of another formula that relates specific linear combinations of the $\{\theta_{4,\gamma}(z)\}_\gamma$ to the shifted theta functions $\theta_{1,0}(2z+\alpha/2+\Omega\beta/2)$, evaluated at $2z$. These shifted theta functions are essentially sections of $T_x^*\mathcal{L}$, where $x \in \mathfrak{J}[2]$ corresponds to $\alpha/2 + \Omega\beta/2 \in \mathbf{C}^2$.

We first pin down canonical bases of $H^0(\mathfrak{J}, \mathcal{L}^k)$ in terms of algebraic theta functions, summarizing what we need from Sections 1–3 of [Mum66]. We follow Mumford's normalization, with some notation from [Kem89a]. For any $k \geq 1$ that is invertible in $\overline{K}$ (mainly $k \in \{2, 4\}$), it is standard that the translates of $\mathcal{L}^k$ that are isomorphic to $\mathcal{L}^k$ are exactly the translates by k-torsion points:

$$\{x \in \mathfrak{J} \mid T_x^*\mathcal{L}^k \cong \mathcal{L}^k\} = \mathfrak{J}[k]. \tag{2.4}$$

Mumford constructs the theta group $\mathcal{G}_k$ of $\mathcal{L}^k$ (more generally, he constructs the theta group of any ample line bundle of separable type) as a central extension

$$0 \to \overline{K}^* \to \mathcal{G}_k \to \mathfrak{J}[k] \to 0. \tag{2.5}$$

Here an element $\tilde{x} \in \mathcal{G}_k$ with image $x \in \mathfrak{J}[k]$ is actually a pair $\tilde{x} = (x, \phi)$ with a choice of isomorphism $\phi : \mathcal{L}^k \to T_x^*\mathcal{L}^k$. We can view ϕ concretely as an algebraic family of isomorphisms between the fibers $\mathcal{L}_p^k$ and $(T_x^*\mathcal{L}^k)_p = \mathcal{L}_{p+x}^k$, where $\mathcal{L}_p^k$ and $\mathcal{L}_{p+x}^k$ are one-dimensional vector spaces over $\overline{K}$:

$$\phi_p : \mathcal{L}_p^k \to \mathcal{L}_{p+x}^k, \qquad p \in \mathfrak{J}. \tag{2.6}$$

We also have an important action of $\mathcal{G}_k$ on the space $H^0(\mathfrak{J}, \mathcal{L}^k)$. Working through the definition of $U_z(s)$ on p. 295 of [Mum66], we can describe the action concretely as follows. View any section $s \in H^0(\mathfrak{J}, \mathcal{L}^k)$ as an algebraic family of "values" $s(p) \in \mathcal{L}_p^k$ at each varying fiber. Then the action of $\tilde{x} = (x, \phi)$ produces a section $\tilde{x} * s \in H^0(\mathfrak{J}, \mathcal{L}^k)$ with values

$$(\tilde{x} * s)(p) = \phi_{p-x}(s(p - x)), \qquad p \in \mathfrak{J}. \tag{2.7}$$

The Weil pairing associated to $\mathcal{L}^k$ is an alternating map that takes two elements $x, y \in \mathfrak{J}[k]$ to a kth root of unity $e_k(x, y) \in \overline{K}^*$ given by the commutator

$$e_k(x, y) = \tilde{x}\tilde{y}\tilde{x}^{-1}\tilde{y}^{-1}. \tag{2.8}$$

Here $\tilde{x}, \tilde{y} \in \mathcal{G}_k$ are any lifts of the elements $x, y \in \mathfrak{J}[k]$.

Mumford shows that the group $\mathcal{G}_k$ has the structure of a Heisenberg group, and that its action on $H^0(\mathfrak{J}, \mathcal{L}^k)$ has a canonical structure up to isomorphism. Take a symplectic decomposition

$$\mathfrak{J}[k] = A_k \oplus B_k, \tag{2.9}$$

where $A_k, B_k \subset \mathfrak{J}[k]$ are subgroups with $A_k \cong B_k \cong (\mathbf{Z}/k\mathbf{Z})^2$, and such that each of A_k and B_k is isotropic for the Weil pairing; then e_k sets up a perfect pairing between A_k and B_k. One can split the extension $\mathcal{G}_k$ over each of A_k and B_k, leading to two different injective group homomorphisms (written with the same tilde notation)

$$A_k \to \mathcal{G}_k, \qquad a \mapsto \tilde{a}; \qquad\qquad B_k \to \mathcal{G}_k, \qquad b \mapsto \tilde{b}. \tag{2.10}$$

We denote by $\tilde{A}_k$ and $\tilde{B}_k$ the images of these two homomorphisms.

In Mumford's treatment, one takes a theta structure on $\mathcal{G}_k$. This includes a specific choice of isomorphism between B_k and $(\mathbf{Z}/k\mathbf{Z})^2$; then A_k is isomorphic to $\mathrm{Hom}(B_k, \overline{K}^*)$, by identifying $a \in A_k$ with $l_a : B_k \to \overline{K}^*$ given by $l_a(b) = e_k(b, a)$. The theta structure also includes appropriate choices of lifts of these identifications

to $\tilde{A}_k$ and $\tilde{B}_k$. Then Mumford shows that the action of $\mathcal{G}_k$ on $H^0(\mathfrak{J}, \mathcal{L}^k)$ is isomorphic to a Schrödinger representation on the space he calls $V(\delta)$, which in our situation consists of $\overline{K}$-valued functions on $(\mathbf{Z}/k\mathbf{Z})^2$ (see p. 297 of [Mum66] for the precise action of a general $\mathcal{G}(\delta)$ on $V(\delta)$).

For this article, it will be easier to reword this action (while still keeping Mumford's normalization) in the language used on pp. 68–69 of [Kem89a]. So we will in fact replace Mumford's space $V(\delta)$ with the space W_k of $\overline{K}$-valued functions on B_k. With this modification, the actions of elements of $\tilde{A}_k$ and $\tilde{B}_k$ on a function $(f : B_k \to \overline{K}) \in W_k$ are given by:

$$(\tilde{a} * f)(b') = l_a(b')f(b') = e_k(b', a)f(b'), \qquad (\tilde{b} * f)(b') = f(b + b'). \tag{2.11}$$

These correspond to the operators $U_{(1,0,l_a)}$ and $U_{(1,b,1)}$ of Mumford. (The operator $U_{(\lambda,b,l_a)}$ corresponds to the product $\lambda\tilde{a}\tilde{b} \in \mathcal{G}_k$.)

For our application, it is easier to write everything in terms of the action of the lifts $\tilde{a}$ and $\tilde{b}$ on the basis $\{\delta_c\}_{c\in B_k}$ for the space W_k. Here, as usual, $\delta_c(b') = 1$ precisely when $b' = c$, and $\delta_c(b') = 0$ otherwise. We then have

$$\tilde{a} * \delta_c = e_k(c, a)\delta_c, \qquad \tilde{b} * \delta_c = \delta_{c-b}, \qquad a \in A_k, \qquad b, c \in B_k. \tag{2.12}$$

We can now define the algebraic theta functions. The key idea here is that the representation of $\mathcal{G}_k$ on $H^0(\mathfrak{J}, \mathcal{L}^k)$ is isomorphic to the above representation on W_k. Moreover, this representation is irreducible. Hence there exists an isomorphism, which by Schur's Lemma is unique up to a scalar in $\overline{K}^*$, between W_k and $H^0(\mathfrak{J}, \mathcal{L}^k)$. With respect to this isomorphism, each basis element $\delta_c \in W_k$ corresponds to a section $\theta_{[k],c} \in H^0(\mathfrak{J}, \mathcal{L}^k)$, with the same transformation properties as in (2.12). This determines the $\{\theta_{[k],c}\}_{c\in B_k}$ up to a common constant factor. Rewriting b' instead of $c \in B_k$, we therefore obtain the following action on the various $\theta_{[k],b'} \in H^0(\mathfrak{J}, \mathcal{L}^k)$:

$$\tilde{a} * \theta_{[k],b'} = e_k(b', a)\theta_{[k],b'}, \qquad \tilde{b} * \theta_{[k],b'} = \theta_{[k],b'-b}. \tag{2.13}$$

In the complex analytic setting for all the above, where $\mathfrak{J} = \mathbf{C}^2/\Lambda$ with the lattice $\Lambda = \mathbf{Z}^2 + \Omega\mathbf{Z}^2$, the analogs of the above constructions are $J_k = \frac{1}{k}\Lambda/\Lambda = A_k \oplus B_k$, with A_k being (the image in $\mathfrak{J}$ of) $\frac{1}{k}\mathbf{Z}^2$, and B_k being (the image of) $\frac{1}{k}\Omega\mathbf{Z}^2$. Viewing global sections of $\mathcal{L}^k$ as functions satisfying (2.2), we have the following action of our lifts $\tilde{a}, \tilde{b} \in \mathcal{G}_k$. Note the minus signs, similarly to (2.7), as well as the notation $f|_k m$ from (2.2), where we now allow $m = -\beta/k \in \mathbf{Q}^2$.

$$(\widetilde{\left[\frac{\alpha}{k}\right]} * f)(z) = f(z - \frac{\alpha}{k}), \qquad \widetilde{\left[\Omega\frac{\beta}{k}\right]} * f = f|_k(\frac{-\beta}{k}), \qquad \alpha, \beta \in \mathbf{Z}^2. \tag{2.14}$$

The algebraic theta function $\theta_{[k],\Omega\beta'/k}$ then corresponds to our analytic theta function $\theta_{k,\beta'}$. The Weil pairing over $\mathbf{C}$ is characterized by $e_k(\Omega\beta/k, \alpha/k) = e(-\beta\cdot\alpha/k)$.

We now return to general $\overline{K}$, and present Mumford's addition formula for algebraic theta functions in terms of the concrete formalism above. The product abelian variety $\mathfrak{J} \times \mathfrak{J}$ is equipped with two projection maps $\pi_1, \pi_2 : \mathfrak{J} \times \mathfrak{J} \to \mathfrak{J}$ to the first and second factors. We consider on $\mathfrak{J} \times \mathfrak{J}$ the line bundle $\mathcal{L}^k \boxtimes \mathcal{L}^k = \pi_1^*\mathcal{L}^k \otimes \pi_2^*\mathcal{L}^k$. Its fiber at the point $(p, q) \in \mathfrak{J} \times \mathfrak{J}$ is the one-dimensional $\overline{K}$-vector space $\mathcal{L}_p^k \otimes \mathcal{L}_q^k$. A theta structure on $\mathcal{G}_k$ for $\mathcal{L}^k$ gives rise to a closely related theta structure for $\mathcal{L}^k \boxtimes \mathcal{L}^k$. We note in particular that $H^0(\mathfrak{J} \times \mathfrak{J}, \mathcal{L}^k \boxtimes \mathcal{L}^k)$ has a canonical basis

$\{\theta_{[k],b} \boxtimes \theta_{[k],b'}\}_{b,b' \in B_k}$. Here the notation $s \boxtimes t$, for $s, t \in H^0(\mathfrak{J}, \mathcal{L}^k)$, is defined by

$$s \boxtimes t = (\pi_1^* s) \otimes (\pi_2^* t). \tag{2.15}$$

The value of the section $s \boxtimes t$ at the point (p, q) is of course

$$(s \boxtimes t)(p, q) = s(p) \otimes t(q) \in \mathcal{L}_p^k \otimes \mathcal{L}_q^k = (\mathcal{L}^k \boxtimes \mathcal{L}^k)_{(p,q)}. \tag{2.16}$$

As Mumford explains in Section 3 of [Mum66], the algebraic addition formula comes out of the isogeny $\xi : \mathfrak{J} \times \mathfrak{J} \to \mathfrak{J} \times \mathfrak{J}$ given by $\xi(p, q) = (p+q, p-q)$. Mumford shows algebraically that we have an isomorphism $h : \xi^*(\mathcal{L}^k \boxtimes \mathcal{L}^k) \cong \mathcal{L}^{2k} \boxtimes \mathcal{L}^{2k}$. (When $\overline{K} = \mathbf{C}$, this isomorphism is easy to see analytically.) We can view h as an algebraic family of isomorphisms between the fibers of the two line bundles, similarly to the situation in (2.6). We thus obtain a family of isomorphisms $\{h_{p,q}\}_{(p,q) \in \mathfrak{J} \times \mathfrak{J}}$ between the one-dimensional fibers $(\xi^*(\mathcal{L}^k \boxtimes \mathcal{L}^k))_{(p,q)} = \mathcal{L}_{p+q}^k \otimes \mathcal{L}_{p-q}^k$, and $(\mathcal{L}^{2k} \boxtimes \mathcal{L}^{2k})_{(p,q)} = \mathcal{L}_p^{2k} \otimes \mathcal{L}_q^{2k}$:

$$h_{p,q} : \mathcal{L}_{p+q}^k \otimes \mathcal{L}_{p-q}^k \to \mathcal{L}_p^{2k} \otimes \mathcal{L}_q^{2k}. \tag{2.17}$$

We can now finally invoke Mumford's fundamental addition formula on p. 324 of [Mum66], to obtain the following formula. In contrast to the analytic situation, this result needs k to be even, unless (as in Theorem 6 of [Kem89a]) we allow a possible modification to the original $\mathcal{L}$.

Theorem 2.2. *Suppose that k is both even and invertible in $\overline{K}$. Choose a symplectic decomposition $\mathfrak{J}[2k] = A_{2k} \oplus B_{2k}$; this also determines a decomposition $\mathfrak{J}[k] = A_k \oplus B_k$, with $B_k = [2]B_{2k} = B_{2k} \cap \mathfrak{J}[k]$, and an analogous A_k. Then there exist compatible theta structures on $\mathcal{G}_k$ and $\mathcal{G}_{2k}$, which give rise to specific choices of bases $\{\theta_{[k],b}\}_{b \in B_k}$ and $\{\theta_{[2k],d}\}_{d \in B_{2k}}$, respectively for $H^0(\mathfrak{J}, \mathcal{L}^k)$ and $H^0(\mathfrak{J}, \mathcal{L}^{2k})$, that satisfy, for all $p, q \in \mathfrak{J}$:*

$$\begin{aligned} &h_{p,q}(\theta_{[k],b_1}(p+q) \otimes \theta_{[k],b_2}(p-q)) \\ &\quad = \sum_{c \in B_{2k} \cap \mathfrak{J}[2]} \theta_{[2k],d_1+d_2+c}(p) \otimes \theta_{[2k],d_1-d_2+c}(q). \end{aligned} \tag{2.18}$$

Here $b_1, b_2 \in B_k$, and we choose $d_1, d_2 \in B_{2k}$ satisfying $2d_1 = b_1, 2d_2 = b_2$. (The sum on the right hand side is independent of the choices of d_1, d_2.)

Proof. The only point to make here is that $\mathcal{L}^k$ is totally symmetric because k is even, so we can apply Mumford's construction of symmetric compatible theta structures. One then translates Mumford's fundamental addition formula, while carefully working through all the definitions, and following the normalizations of [Mum66] and our concrete expressions above for the isomorphisms. As Mumford points out, one can choose the isomorphisms so as to make the common constant factor λ in his formula equal to 1.

The formula (2.18) is parallel to the statements in Theorem 8 of [Kem89a] and Theorem 6.5 of [Kem91], but the normalizations in Kempf appear to be slightly different (for example, an element of the theta group in [Kem91] is defined using an isomorphism from $T_x^* \mathcal{L}^k$ to $\mathcal{L}^k$ and not its inverse), so we preferred to follow scrupulously the treatment in [Mum66]. □

Remark 2.3. In the works cited above, the compatible theta structures can be set up so that the actions of both negation $[-1] : \mathfrak{J} \to \mathfrak{J}$ and doubling $[2] : \mathfrak{J} \to \mathfrak{J}$ become transparent. We will not need these in full generality. We will however

treat "by hand" a specific case of the action of doubling, which does not seem to be included in the results of [Mum66] because the original line bundle $\mathcal{L}$ is not totally symmetric. The result on doubling that we need is included in [Kem89a] and [Kem88], but we will make it more explicit below.

From now on, we limit ourselves to using (2.18) only when $k = 2$. We first note the standard "diagonalization" of (2.18) obtained by introducing a character $\chi : B_2 \to \overline{K}^*$ and forming the linear combination $\sum_{c\in B_2} \chi(c)\theta_{[2],b+c} \boxtimes \theta_{[2],c}$. The character χ, which takes values in $\{\pm 1\}$, can be written as $\chi(c) = e_4(c, \alpha)$ for some choice of $\alpha \in A_4$; the character χ depends only on the coset of α in A_4/A_2. Indeed, $e_4(\cdot, \cdot)$ is isotropic on the points of $\mathfrak{J}[2] = A_2 \oplus B_2 \subset \mathfrak{J}[4] = A_4 \oplus B_4$. Let us also write $b = 2d$ for some choice of $d \in B_4$. Applying ξ^* to our linear combination above, followed by the isomorphisms $h_{p,q}$, we obtain from (2.18) the following important identity for all $p, q \in \mathfrak{J}$:

$$h_{p,q}\Big(\sum_{c\in B_2} e_4(c, \alpha)\theta_{[2],2d+c}(p + q) \otimes \theta_{[2],c}(p - q)\Big) = F_{d,\alpha}(p) \otimes F_{d,\alpha}(q), \tag{2.19}$$

where for $d \in B_4$ and $\alpha \in A_4$ we have

$$F_{d,\alpha} = \sum_{c\in B_2} e_4(c, \alpha)\theta_{[4],d+c} \in H^0(\mathfrak{J}, \mathcal{L}^4). \tag{2.20}$$

As already observed, $F_{d,\alpha}$ is unchanged if we add an element of A_2 to α; note however that if we add an element $b' \in B_2$ to d, then $F_{d+b',\alpha} = e_4(b', \alpha)F_{d,\alpha}$ (remember that $e_4(b', \alpha) \in \{\pm 1\}$, because b' is 2-torsion). It is easy to see that the $F_{d,\alpha}$ form a basis of $H^0(\mathfrak{J}, \mathcal{L}^4)$ as α and d run over any fixed choice of representatives for each coset in A_4/A_2 and B_4/B_2.

We now wish to relate $F_{d,\alpha}$ to the pullback via [2] of a translate $T_x^*(\theta_{[1],0}) \in H^0(\mathfrak{J}, T_x^*\mathcal{L})$, for a suitable $x \in \mathfrak{J}[2]$. This is a known result, and is easy to show analytically, when $\overline{K} = \mathbf{C}$, The general case is covered in the next to last paragraph of [Kem88], immediately following the proof of Theorem 7 there. We state and prove the result in the language of this article. Recall that our choice of symmetric line bundle $\mathcal{L}$ is only unique in the first place up to translation by an element of $\mathfrak{J}[2]$. Moreover, since $\mathcal{L}$ is symmetric, we have $[2]^*\mathcal{L} \cong \mathcal{L}^4$.

Proposition 2.4. *Up to translating $\mathcal{L}$ by a 2-torsion point, we can identify $F_{0,0}$ with a nonzero constant multiple of $[2]^*\theta_{[1],0}$. To absorb the constant, we choose a specific isomorphism $j : [2]^*\mathcal{L} \to \mathcal{L}^4$, giving rise to a family of isomorphisms $j_p : ([2]^*\mathcal{L})_p = \mathcal{L}_{2p} \to \mathcal{L}_p^4$, for which*

$$F_{0,0}(p) = j_p(\theta_{[1],0}(2p)), \qquad p \in \mathfrak{J}. \tag{2.21}$$

Proof. Consider 2-torsion elements $a \in A_2 \subset A_4$ and $b \in B_2 \subset B_4$, as well as their lifts $\tilde{a}, \tilde{b} \in \mathcal{G}_4$. These lifts generate a partial splitting of the extension $\mathcal{G}_4$ over $\mathfrak{J}[2] = A_2 \oplus B_2$, which is a maximal isotropic subgroup of $\mathfrak{J}[4]$ under the Weil pairing e_4. The section $F_{0,0}$ is invariant under the action of these lifts from $\mathfrak{J}[2]$. Now this partial splitting gives descent data for $\mathcal{L}^4$ under all translations by $\mathfrak{J}[2]$: see pp. 290–291 of [Mum66]. The descent produces a line bundle $\tilde{\mathcal{L}}$ on $\mathfrak{J}$, and an isomorphism $j : [2]^*\tilde{\mathcal{L}} \to \mathcal{L}^4$. We can also descend $F_{0,0}$ to a nonzero global section of $\tilde{\mathcal{L}}$. The proof will be complete once we show that $\tilde{\mathcal{L}}$ is in fact a translate $T_x^*\mathcal{L}$, for some $x \in \mathfrak{J}[2]$, for we then replace $\mathcal{L}$ by $\tilde{\mathcal{L}}$, and we know that (the new) $H^0(\mathfrak{J}, \mathcal{L})$ is one-dimensional, with basis $\theta_{[1],0}$. We finally adjust j by a constant to obtain (2.21).

To show our assertion about $\tilde{\mathcal{L}}$, note first that $[2]^*\mathcal{L}$ and $[2]^*\tilde{\mathcal{L}}$ are both isomorphic to $\mathcal{L}^4$. Hence $\mathcal{L}^{-1}\otimes\tilde{\mathcal{L}}$ is in the kernel of the homomorphism $[2]^* : \mathrm{Pic}\mathfrak{J} \to \mathrm{Pic}\mathfrak{J}$. The effect of $[2]^*$ on the Néron-Severi group is to multiply by 4, but $NS(\mathfrak{J})$ is torsion-free. Hence $\mathcal{L}^{-1}\otimes\tilde{\mathcal{L}}$ belongs to $\mathrm{Pic}^0\mathfrak{J}$, which implies that $\tilde{\mathcal{L}}\otimes\mathcal{L}^{-1}$ is isomorphic to $T_x^*\mathcal{L}\otimes\mathcal{L}^{-1}$ for some $x\in\mathfrak{J}$, via the usual isomorphism $\Phi : \mathfrak{J}\to\mathrm{Pic}^0\mathfrak{J}$ given by $\Phi(x) = T_x^*\mathcal{L}\otimes\mathcal{L}^{-1}$. We have thus shown that $\tilde{\mathcal{L}}\cong T_x^*\mathcal{L}$. Take any $y\in\mathfrak{J}$ with $2y = x$. We know that $\mathcal{L}^4\cong[2]^*\tilde{\mathcal{L}}\cong[2]^*T_x^*\mathcal{L}$, and this last is isomorphic to $T_y^*[2]^*\mathcal{L}\cong T_y^*\mathcal{L}^4$. We deduce that $4y = 0$ and hence that x is a 2-torsion point. □

Remark 2.5. One can give a more conceptual proof of the above proposition. The different choices of lifts from $\mathfrak{J}[2]\to\mathcal{G}_4$ correspond to different ways to descend $\mathcal{L}^4$ along $\mathfrak{J}[2]$ to varying line bundles. One of these descents gives $\tilde{\mathcal{L}}$, while another gives $\mathcal{L}$. But any two lifts $\mathfrak{J}[2]\to\mathcal{G}_4$ differ by a character of $\mathfrak{J}[2]$ with values in $\{\pm1\}$, and such a character can be obtained by a Weil pairing with a fixed 2-torsion point which corresponds to our x. Essentially the same argument about changing $\tilde{\mathcal{L}}$ to $\mathcal{L}$ appears in Lemma 5 of [Kem89a] (see also Theorem 6 there). Compare also to property (5) on p. 228 of [Mum70] (under "Functorial properties of e^L").

Corollary 2.6. *Let $d\in B_4$ and $\alpha\in A_4$. Define the element $\tilde{x} = (x,\phi) = \widetilde{(-d)}(\tilde{\alpha})\in\mathcal{G}_4$; hence $x = -d+\alpha$ and $\phi : \mathcal{L}^4\to T_{-d+\alpha}^*\mathcal{L}^4$ is the corresponding isomorphism. We then have, for all $p\in\mathfrak{J}$:*

$$F_{d,\alpha}(p) = \phi_{p+d-\alpha}\circ j_{p+d-\alpha}(\theta_{[1],0}(2p+2d-2\alpha)). \tag{2.22}$$

Proof. By (2.13), we have $F_{d,\alpha} = \tilde{x} * F_{0,0}$. Now apply (2.7) to obtain the above formula. □

Our main use of (2.22) will be to determine conditions under which $F_{d,\alpha}$ vanishes or not at certain points, by reducing the question to whether $\theta_{[1],0}$ vanishes at the corresponding points. We first state a mostly standard result about $\theta_{[1],0}$.

Lemma 2.7. *Recall that $\mathfrak{J}$ is the Jacobian of a genus 2 curve $\mathcal{C}$, and that $0\neq\theta_{[1],0}\in H^0(\mathfrak{J},\mathcal{L})$, where $\mathcal{L}$ is a symmetric line bundle giving the principal polarization.*

1. *Among the 16 points of $\mathfrak{J}[2]$, we have that $\theta_{[1],0}$ vanishes at precisely 6 of them (and is nonzero at the remaining 10 points).*
2. *$\theta_{[1],0}$ does not vanish at any point $p\in\mathfrak{J}$ whose order is precisely 4, in other words, for $p\in\mathfrak{J}[4]-\mathfrak{J}[2]$.*

Proof. Write Θ for the vanishing locus of $\theta_{[1],0}$. We know that Θ is a symmetric theta divisor on $\mathfrak{J}$, so it is the image of $\mathcal{C}$ under a suitable Abel-Jacobi map into $\mathfrak{J}$. Let $\{w_0,\dots,w_5\}\subset\mathcal{C}$ be the six Weierstrass points. Then one choice of symmetric theta divisor is the set $\mathcal{C}_0 = \mathcal{C}-w_0\subset\mathfrak{J}$, by which we mean the set of all divisor classes of the form $[v-w_0]\in\mathfrak{J} = \mathrm{Pic}^0\mathcal{C}$, parametrized by $v\in\mathcal{C}$. Then $\mathcal{O}_{\mathfrak{J}}(\mathcal{C}_0)$ is a symmetric line bundle in the algebraic equivalence class of $\mathcal{L}$. Hence $\mathcal{L}$, which is also symmetric, is isomorphic to the translate of $\mathcal{O}_{\mathfrak{J}}(\mathcal{C}_0)$ by some 2-torsion point $x\in\mathfrak{J}[2]$. This means that Θ is the set of points $\{[v-w_0]+x \mid v\in\mathcal{C}\}$, where v varies on $\mathcal{C}$ and $x\in\mathfrak{J}[2]$ is a fixed 2-torsion point.

Let us prove the first assertion above. For a 2-torsion point $p\in\mathfrak{J}[2]$ to lie on Θ, we require $p-x$ to be a 2-torsion point of the form $[v-w_0]$. But the only such 2-torsion points are the six points $\{[w_i-w_0] \mid 0\le i\le 5\}$. This gives us precisely six choices of p where $\theta_{[1],0}(p) = 0$.

As for the second assertion, it says that when p has exact order 4, then $p - x$ cannot be of the form $[v - w_0]$ for $v \in \mathcal{C}$. Note that in fact $p - x$ also has exact order 4. Suppose to the contrary that $[v - w_0]$ were a point of exact order 4. Then $4v - 4w_0$ would be the divisor of an element ϕ of the function field $\overline{K}(\mathcal{C})$. Let us take a model for $\mathcal{C}$ over $\overline{K}$ given by an equation of the form $Y^2 = (X - a_1) \cdots (X - a_5)$, where w_0 is the point at infinity, and where for $i \geq 1$, $w_i = (a_i, 0)$ for distinct $a_1, \ldots, a_5 \in \overline{K}$. Then X has a double pole at w_0, and Y has a quintuple pole at w_0. Now the only singularity of ϕ is a quadruple pole at w_0, so $\phi = c_2 X^2 + c_1 X + c_0$ with $c_2 \neq 0$; we can harmlessly assume $c_2 = 1$. Factor $\phi = (X - b_1)(X - b_2)$, with $b_1, b_2 \in \overline{K}$. If $b_1 \neq b_2$, then ϕ cannot have a quadruple zero at just one point $v \in \mathcal{C}$; thus $\phi = (X - b_1)^2$. But then v has coordinates (b_1, c) for some $c \in \overline{K}$; if we had $c \neq 0$, then ϕ would also vanish at a second point $(b_1, -c) \in \mathcal{C}$. Thus the only possibility is to have $c = 0$, and $b_1 \in \{a_1, \ldots, a_5\}$. But then $v = (b_1, 0)$ would be one of the Weierstrass points, and $[v - w_0]$ would be a point of order 2, not of exact order 4. □

The first part of the following corollary is basically a precise statement in our setting of the difference between even and odd theta-characteristics for the curve $\mathcal{C}$.

Corollary 2.8. *Let $d \in B_4$ and let $\alpha \in A_4$.*

1. *The value $F_{d,\alpha}(0)$ is zero when $e_4(2d, \alpha) = -1$, and is nonzero otherwise (when $e_4(2d, \alpha) = 1$).*
2. *Let $q \in \mathfrak{J}$ be a point of exact order 8. Then $F_{d,\alpha}(q) \neq 0$.*

Proof. The second assertion follows directly from (2.22) and the second part of Lemma 2.7. Let us prove the first assertion. Observe first that $e_4(2d, \alpha) = e_2(2d, 2\alpha)$, with $2\alpha \in A_2$ and $2d \in B_2$. Moreover, there are six pairs $(b, a) \in B_2 \times A_2$ for which $e_2(b, a) = -1$; namely, to each of the three nonzero choices of $b \in B_2$, there correspond precisely two choices of $a \in A_2$ that give a nontrivial Weil pairing with b. Now put $q = 0$ in (2.19) to obtain

$$h_{p,0}\Big(\sum_{c \in B_2} e_4(c, \alpha)\theta_{[2],2d+c}(p) \otimes \theta_{[2],c}(p)\Big) = F_{d,\alpha}(p) \otimes F_{d,\alpha}(0). \tag{2.23}$$

The expression S within parentheses on the left hand side is a linear combination of products of two sections of $\mathcal{L}^2$. Multiplication of two sections of the same line bundle is commutative, as is familiar over $\mathbf{C}$ (for example, set $w = 0$ in (2.3)). Here is a pedantic proof of commutativity in our algebraic context: the fiber $V = \mathcal{L}_p^2$ is a one-dimensional $\overline{K}$-vector space, so for $v, v' \in V$ we have $v \otimes v' = v' \otimes v$ in the one-dimensional space $V \otimes V = \mathcal{L}_p^4$. Using the fact that $4d = 0$, we deduce that

$$\begin{aligned} S &:= \sum_{c \in B_2} e_4(c, \alpha)\theta_{[2],2d+c}(p) \otimes \theta_{[2],c}(p) \\ &= \sum_{c \in B_2} e_4(c, \alpha)\theta_{[2],c}(p) \otimes \theta_{[2],2d+c}(p) \\ &= \sum_{c' \in B_2} e_4(2d + c', \alpha)\theta_{[2],2d+c'}(p) \otimes \theta_{[2],c'}(p) \\ &= e_4(2d, \alpha)S. \end{aligned} \tag{2.24}$$

Thus when $e_4(2d, \alpha) = -1$, we must have $S = 0$ for all p, so $F_{d,\alpha}(p) \otimes F_{d,\alpha}(0) = 0$. Since $F_{d,\alpha}$ is a nonzero element of $H^0(\mathfrak{J}, \mathcal{L}^4)$, we deduce that $F_{d,\alpha}(0) = 0$, and

hence that $\theta_{[1],0}(2d-2\alpha)=0$. Now $2d-2\alpha$ is a 2-torsion point (and is equal to $2d+2\alpha$), and we have just listed six 2-torsion points where $\theta_{[1],0}$ vanishes. (These correspond to the odd theta-characteristics.) By our lemma, these are the only such 2-torsion points; hence, when $e_4(2d,\alpha)=1$ (an even theta-characteristic), we must have $\theta_{[1],0}(2d-2\alpha)\neq 0$, hence $F_{d,\alpha}(0)\neq 0$. □

We remark incidentally that when $\mathfrak{J}$ is not a Jacobian, but rather a principally polarized abelian surface that is the product of two elliptic curves, then $\theta_{[1],0}$ vanishes at one of the even theta-characteristics, so vanishes at precisely seven 2-torsion points. Over $\mathbf{C}$, we can see this by taking $\Omega=\begin{pmatrix}\tau_1 & 0\\ 0 & \tau_2\end{pmatrix}$, in which case the analytic $\theta_{1,0}$ vanishes both at the six odd theta-characteristics and at one even theta-characteristic, corresponding to $2\alpha=\frac{1}{2}\binom{1}{1}$ and $2d=\frac{1}{2}\Omega\binom{1}{1}=\frac{1}{2}\binom{\tau_1}{\tau_2}$.

The embedding into $\mathbf{P}^3\times\mathbf{P}^3$. We first describe the Kummer map $\kappa:\mathfrak{J}\to\mathbf{P}^3$ that is associated to $\mathcal{L}^2$. In our isotropic subgroup $A_4\subset\mathfrak{J}[4]$, we fix a point D_1 of exact order 4. Let $E_1=2D_1\in A_2\cong(\mathbf{Z}/2\mathbf{Z})^2$, let $E_2\in A_2$ be a second 2-torsion point, and define $E_3=E_1+E_2$; hence $A_2=\{0,E_1,E_2,E_3\}$. (In Section 4, we will also write $E_0=0$, and take a point D_2 with $2D_2=E_2$, then write $D_3=D_1+D_2$; however, the 4-torsion points D_2 and D_3 will not belong to A_4.) We also assign names to the points of B_2 as $B_2=\{0=b_{00},b_{10},b_{01},b_{11}\}$, according to their Weil pairing with E_1 and E_2:

$$e_2(b_{ij},E_1)=(-1)^i,\qquad e_2(b_{ij},E_2)=(-1)^j. \tag{2.25}$$

These names appear briefly here in (2.26), and they will make a later appearance in Lemmas 2.19 and 2.24. Using the above notation, we rename our basis $\{\theta_{[2],b}\}_{b\in B_2}$ for $H^0(\mathfrak{J},\mathcal{L}^2)$ as

$$Q_{00}=\theta_{[2],b_{00}},\qquad Q_{10}=\theta_{[2],b_{10}},\qquad Q_{01}=\theta_{[2],b_{01}},\qquad Q_{11}=\theta_{[2],b_{11}}. \tag{2.26}$$

Hence the componentwise actions of the lifts $\widetilde{E_1},\widetilde{E_2},\widetilde{E_3}\in\mathcal{G}_2$ on the 4-tuple of sections $(Q_{00},Q_{10},Q_{01},Q_{11})$ are given by

$$\begin{aligned}\widetilde{E_1}*(Q_{00},Q_{10},Q_{01},Q_{11})&=(Q_{00},-Q_{10},Q_{01},-Q_{11}),\\ \widetilde{E_2}*(Q_{00},Q_{10},Q_{01},Q_{11})&=(Q_{00},Q_{10},-Q_{01},-Q_{11}),\\ \widetilde{E_3}*(Q_{00},Q_{10},Q_{01},Q_{11})&=(Q_{00},-Q_{10},-Q_{01},Q_{11}).\end{aligned} \tag{2.27}$$

The Kummer map is then

$$\kappa(p)=[Q_{00}(p),Q_{10}(p),Q_{01}(p),Q_{11}(p)]\in\mathbf{P}^3,\qquad p\in\mathfrak{J}. \tag{2.28}$$

Note carefully the notation within square brackets for projective coordinates. Here the values $Q_j(p)$ for $j\in\{00,01,10,11\}$ all belong to the same one-dimensional space $\mathcal{L}^2_p$, so strictly speaking the projective coordinates that we wrote down are not elements of $\overline{K}$. However, their "ratios" give a well defined point in $\mathbf{P}^3$, as usual. (This uses the fact that $\mathcal{L}^2$ is base point free, so the values $\{Q_j(p)\}_j$ can never all vanish for the same p.) It is standard that $\kappa(-p)=\kappa(p)$, and that the image of κ is in bijection with (the geometric points of) $\mathfrak{J}/\{[\pm1]\}$. References for these facts are Chapter 3 of [CF96], Section 4.8 of [BL04], and Section 10.4 of [Kem91]. The image of κ is called the Kummer surface, and is the zero set of a quartic equation

in the Q_j, called the Kummer quartic. Our identities (2.27) imply the following identities between projective points:

$$\begin{aligned}\kappa(p-E_1) &= [Q_{00}(p-E_1), Q_{10}(p-E_1), Q_{01}(p-E_1), Q_{11}(p-E_1)]\\ &= [Q_{00}(p), -Q_{10}(p), Q_{01}(p), -Q_{11}(p)],\\ \kappa(p-E_2) &= [Q_{00}(p), Q_{10}(p), -Q_{01}(p), -Q_{11}(p)],\\ \kappa(p-E_3) &= [Q_{00}(p), -Q_{10}(p), -Q_{01}(p), Q_{11}(p)].\end{aligned} \tag{2.29}$$

This is because applying the same isomorphism ϕ_{p-E_i} (associated to $\widetilde{E_i}$) to all four coordinates does not change the projective point. Note of course also that $-E_i = E_i$.

We now translate everything by D_1. Write $\mathcal{L}' = T_{D_1}^*\mathcal{L}$ for the shifted line bundle. Then a basis $\{P_j\}_j$ for $H^0(\mathfrak{J}, (\mathcal{L}')^2)$ is given by $P_j = T_{D_1}^* Q_j$. Concretely, for $j \in \{00, 10, 01, 11\}$, we have

$$P_j(p) = Q_j(p + D_1) \in (\mathcal{L}'_p)^2 = \mathcal{L}^2_{p+D_1}. \qquad p \in \mathfrak{J}. \tag{2.30}$$

The projective map κ' associated to $(\mathcal{L}')^2$ sends p to $\kappa'(p) = \kappa(p + D_1)$. The image of κ' is given by the same Kummer quartic equation, this time in the $\{P_j\}$. Combining κ and κ' gives our fundamental embedding of $\mathfrak{J}$ into $\mathbf{P}^3 \times \mathbf{P}^3$:

$$p \mapsto (\kappa(p), \kappa'(p)) = ([P_i(p)]_i, [Q_j(p)]_j) \in \mathbf{P}^3 \times \mathbf{P}^3. \tag{2.31}$$

For comparison with Section 4, where we pay attention to rationality over a base field K, we note that the K-rational coordinates $([u_i]_i, [y_j]_j)$ on $\mathbf{P}^3 \times \mathbf{P}^3$ that appear in that section transform in a "diagonalized" way under the K-rational isotropic 2-torsion subgroup $A_2 = \{E_0, E_1, E_2, E_3\}$, similarly to (2.27) but with a slightly different order of coordinates: see (4.15). Each space where A_2 acts by a given character is one-dimensional; hence each u_i from Section 4 is then a different nonzero constant multiple of a corresponding $Q_{i'}$, and similarly each y_j is a multiple of a corresponding $P_{j'}$. These nonzero constants belong to $\overline{K}$, but not necessarily to K itself. Moreover, the nonzero elements $b \in B_2$ are in general not K-rational. The lifts $\tilde{b}$ of these elements to $\mathcal{G}_2$ permute the Q (and P) coordinates, but their action on the u_i (and y_j) combines a permutation with a rescaling of each coordinate by a different factor in $\overline{K}^*$; essentially, the action is by an element of the normalizer of the diagonal algebraic torus in $GL(4, \overline{K})$.

When $\overline{K} = \mathbf{C}$, we can describe the Q and P coordinates analytically by

$$\begin{aligned} Q_{00} &= \theta_{2,(0,0)}(z), \qquad Q_{10} = \theta_{2,(1,0)}(z),\\ Q_{01} &= \theta_{2,(0,1)}(z), \qquad Q_{11} = \theta_{2,(1,1)}(z),\\ P_j(z) &= Q_j(z + (1/4, 0)),\end{aligned} \tag{2.32}$$

where we write vectors as rows instead of columns for typographical convenience.

Relations between the P and Q coordinates, and dimensions of each homogeneous component of the bigraded ideal. Our goal is to study the equations of $\mathfrak{J}$ under the embedding (2.31), as well as formulas for the group law. The natural setting for all this is the bigraded polynomial ring in eight variables

$$R = \overline{K}[\{P_i\}, \{Q_j\}] = \oplus_{d,e \geq 0} R_{d,e}, \tag{2.33}$$

where here the P_i and Q_j are the coordinates on $\mathbf{P}^3 \times \mathbf{P}^3$ (in particular, they are algebraically independent), and $R_{d,e}$ is the summand consisting of bihomogeneous

polynomials $f(\{P_i\},\{Q_j\})$ of bidegree (d,e) in the Ps and Qs. When we view the Ps and Qs instead as sections of the line bundles $(\mathcal{L}')^2$ and $\mathcal{L}^2$, and take products of such sections, we can map a monomial such as (to take a random example) $P_{10}^3Q_{00}Q_{01} \in R_{3,2}$ into a space such as $H^0(\mathfrak{J},(\mathcal{L}')^6\otimes\mathcal{L}^4)$. Let us write

$$\mathcal{M}_{d,e} = (\mathcal{L}')^{2d}\otimes\mathcal{L}^{2e}, \qquad V_{d,e} = H^0(\mathfrak{J},\mathcal{M}_{d,e}). \tag{2.34}$$

(Note for later use that $\mathcal{M}_{d,e}$ is algebraically equivalent to $\mathcal{L}^{2(d+e)}$.) The multiplication map that we just defined on monomials extends to a $\overline{K}$-linear map

$$\mu = \mu_{d,e} : R_{d,e} \to V_{d,e} \qquad f \mapsto \overline{f}. \tag{2.35}$$

We will generally distinguish f from its image $\mu(f) = \overline{f}$, but we reserve the right to be occasionally sloppy, especially when $\mu_{d,e}$ is injective.

The ideal I defining the image of $\mathfrak{J}$ under (2.31) is a bigraded ideal of R, with

$$I_{d,e} = \ker\mu_{d,e}. \tag{2.36}$$

We will denote by $\overline{R}$ the bigraded quotient ring R/I, so $\overline{R}_{d,e} \cong \operatorname{image}\mu_{d,e} \subset V_{d,e}$. We view $\overline{R}_{d,e}$ as a subspace of $V_{d,e}$, and point out that for some (d,e), it is a proper subset; see Remark 2.11.

We now compute, in stages, the dimensions of $I_{d,e}$ and of $\overline{R}_{d,e}$. First note the following basic dimension counts.

Proposition 2.9. *For $d,e \geq 0$, we have $\dim R_{d,e} = \binom{d+3}{3}\binom{e+3}{3}$ and $\dim V_{d,e} = 4(d+e)^2$.*

Proof. The first statement holds because there are $\binom{d+3}{3}$ monomials of degree d in the four variables $\{P_i\}$, and $\binom{e+3}{3}$ monomials in the $\{Q_j\}$. The second statement amounts to Riemann-Roch for the abelian surface $\mathfrak{J}$, because $\mathcal{M}_{d,e}$ is algebraically equivalent to the $2(d+e)$th power of the principal polarization bundle $\mathcal{L}$. □

When one of d or e is zero, then the dimensions are easy to compute, as a consequence of the known structure of the Kummer embedding.

Proposition 2.10. *For $k \leq 3$, we have $I_{k,0} = 0$; for $k \geq 4$, we have $\dim I_{k,0} = \dim R_{k-4,0}$. Hence*

$$\dim\overline{R}_{k,0} = \begin{cases} \dim R_{k,0} = \binom{k+3}{3}, & \text{if } k \leq 3, \\ \dim R_{k,0} - \dim R_{k-4,0} = 2k^2+2, & \text{if } k \geq 4. \end{cases} \tag{2.37}$$

An analogous result holds for $I_{0,k}$ and $\overline{R}_{0,k}$. Note in fact that the above formulas imply that $\dim\overline{R}_{k,0} = \dim\overline{R}_{0,k} = 2k^2+2$ for all $k \geq 1$.

Proof. Elements of $I_{k,0}$ are the same as degree k relations between the $\{P_i\}$ that do not involve any of the $\{Q_j\}$. All relations in the $\{P_i\}$ alone are generated by the quartic equation $r = r(P_{00},P_{10},P_{01},P_{11})$ that defines the Kummer surface. Hence, for $k \geq 4$, we have $I_{k,0} = rR_{k-4,0}$. The ring R is a domain, so $I_{k,0}$ has the same dimension as $R_{k-4,0}$. Finally, when $k \in \{1,2,3\}$, then one easily checks that $\binom{k+3}{3} = 2k^2+2$. □

Remark 2.11. In particular, $\overline{R}_{k,0} \neq V_{k,0}$ for $k \geq 2$; for example, $\dim\overline{R}_{2,0} = 10 < 16 = \dim V_{2,0}$.

Our next goal is to show that, in fact, $\overline{R}_{d,e} = V_{d,e}$ whenever $d,e \geq 1$. We begin with the case of $\overline{R}_{1,1}$.

Proposition 2.12. *In the setting of our construction, with $\mathfrak{J}$ the Jacobian of a curve $\mathcal{C}$, the space $\overline{R}_{1,1}$ is equal to all of $V_{1,1}$; equivalently, $I_{1,1} = 0$, and the set of sixteen products P_iQ_j is linearly independent and hence a basis of $\overline{R}_{1,1} = V_{1,1}$.*

Proof. We are equivalently asserting the surjectivity of the multiplication map $H^0(\mathfrak{J}, (\mathcal{L}')^2) \otimes H^0(\mathfrak{J}, \mathcal{L}^2) \to H^0(\mathfrak{J}, \mathcal{M}_{1,1})$. This surjectivity (hence bijectivity, since both spaces are 16-dimensional) follows from part 2 of Lemma 2.7 here, combined with Theorem 3 in the appendix of [Kem88]. Note that the statement there has a typographical mistake; see the statement of Theorem 2.1 of [PSM21] and the comments just preceding their Remark 2.4. We reproduce the argument from [Kem88] in our setting. Take a point $q \in \mathfrak{J}$ such that $2q = D_1$; hence q has exact order 8, and $\mathcal{M}_{1,1} = (\mathcal{L}')^2 \otimes \mathcal{L}^2 = (T_{2q}^*\mathcal{L}^2) \otimes \mathcal{L}^2$ is isomorphic to $(T_q^*\mathcal{L}^2) \otimes (T_q^*\mathcal{L}^2)$, hence to $T_q^*\mathcal{L}^4$. As mentioned just after (2.20), the $\{F_{d,\alpha}\}$ form a basis of $H^0(\mathfrak{J}, \mathcal{L}^4)$ when d and α range over coset representatives for B_4/B_2 and A_4/A_2; thus the $\{T_q^*F_{d,\alpha}\}$, which are a basis for $H^0(\mathfrak{J}, T_q^*\mathcal{L}^4)$, can be identified with a basis for $H^0(\mathfrak{J}, \mathcal{M}_{1,1})$.

Now replace p in (2.19) by $p' = p + q$. This yields, for each choice of d and α, a linear combination of values $P_i(p) \otimes Q_j(p)$, which is equal (up to the isomorphism $h_{p+q,q}$) to $F_{d,\alpha}(p+q) \otimes F_{d,\alpha}(q)$. We can view $F_{d,\alpha}(p+q)$ as the value at p of the section $T_q^*F_{d,\alpha} \in H^0(\mathfrak{J}, T_q^*\mathcal{L}^4)$. Moreover, at least up to isomorphism, we can view $F_{d,\alpha}(q)$, which belongs to the fixed one-dimensional space $\mathcal{L}_q^4$, as a nonzero element of $\overline{K}$, by the second assertion of Corollary 2.8. This means that the image of our multiplication map contains a nonzero multiple of each basis element of $H^0(\mathfrak{J}, \mathcal{M}_{1,1})$, and is hence surjective. □

We now show that all the "larger" $\overline{R}_{d,e}$ are equal to their corresponding (d, e). We introduce the notation

$$(d, e) \geq (d', e') \quad :\Longleftrightarrow \quad d \geq d' \text{ and } e \geq e'. \tag{2.38}$$

Proposition 2.13. *Let $(d, e) \geq (1, 1)$. Then $\overline{R}_{d,e} = V_{d,e}$; that is, the multiplication map $\mu_{d,e}$ is surjective.*

Proof. This is an application of a result of Kempf that first appeared in [Kem89b], but this reference is less widely available than others. The proof of Kempf is reproduced in Theorem 10.1 of [Mum91], in language that works over an arbitrary $\overline{K}$. (Over $\mathbf{C}$, one can also see Theorem 6.8(c) of [Kem91], which is easily adaptable to general $\overline{K}$, and Proposition 7.3.4 of [BL04]). The result of Kempf is as follows: let $\mathcal{L}_1, \mathcal{L}_2$ be ample line bundles on $\mathfrak{J}$ with $\mathcal{L}_i$ algebraically equivalent to $\mathcal{L}^{\ell_i}$. Assume that $(\ell_1, \ell_2) \geq (2, 3)$ or that $(\ell_1, \ell_2) \geq (3, 2)$, in the sense of (2.38). The theorem then states that the map $H^0(\mathfrak{J}, \mathcal{L}_1) \otimes H^0(\mathfrak{J}, \mathcal{L}_2) \to H^0(\mathfrak{J}, \mathcal{L}_1 \otimes \mathcal{L}_2)$ is surjective. Applying this to our $\mathcal{M}_{d,e}$ and either $\mathcal{M}_{1,0}$ or $\mathcal{M}_{0,1}$, this means that if $d + e \geq 2$ then the "product" $V_{d,e} \cdot V_{1,0}$ is equal to $V_{d+1,e}$, and similarly $V_{d,e} \cdot V_{0,1} = V_{d,e+1}$. By a notation such as $V_{d,e} \cdot V_{1,0}$, we mean the set of all finite sums $\sum_i a_i \cdot b_i$ with each $a_i \in V_{d,e}$ and $b_i \in V_{1,0}$. In other words, $V_{d,e} \cdot V_{1,0}$ is the image of the multiplication map $V_{d,e} \otimes V_{1,0} \to V_{d+1,e}$.

We now proceed by induction, from the base case $(d, e) = (1, 1)$, to obtain our result. (Surjectivity of the multiplication maps in R or $\overline{R}$ is immediate: for example, $R_{d,e} \cdot R_{1,0} = R_{d+1,e}$.) □

Corollary 2.14. *For $(d,e) \geq (1,1)$, we have $\dim I_{d,e} = \dim R_{d,e} - \dim V_{d,e} = \binom{d+3}{3}\binom{e+3}{3} - 4(d+e)^2$. As a special case, and after some simple algebra, $\dim I_{k,1} = \dim I_{1,k} = 4\binom{k+1}{3} = 4\dim R_{k-2,0} = 4\dim R_{0,k-2}$ when $k \geq 1$.*

The result of Kempf on relations; consequences for ideal generators.

Definition 2.15. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be ample line bundles on $\mathfrak{J}$. The space of relations $\mathfrak{R}(\mathcal{L}_1, \mathcal{L}_2)$ is defined by

$$\mathfrak{R}(\mathcal{L}_1, \mathcal{L}_2) = \ker(H^0(\mathfrak{J}, \mathcal{L}_1) \otimes H^0(\mathfrak{J}, \mathcal{L}_2) \to H^0(\mathfrak{J}, \mathcal{L}_1 \otimes \mathcal{L}_2)). \tag{2.39}$$

The space $\mathfrak{R}(\mathcal{M}_{d',e'}, \mathcal{M}_{d'',e''})$ provides information about the bigraded component $I_{d'+d'',e'+e''}$ of our ideal of relations.

The following theorem is again due to Kempf [Kem89b]. See Theorem 6.14 and Proposition 6.15 of [Kem91]; or, alternatively, Theorem 10.10 of [Mum91]; or also Proposition 7.4.3 of [BL04] and the subsequent method of proof of their Theorem 7.4.1. All these references follow the original argument of Kempf.

Theorem 2.16. *Let $\mathcal{L}_1$, $\mathcal{L}_2$, and $\mathcal{L}_3$ be ample line bundles on $\mathfrak{J}$, with $\mathcal{L}_i$ algebraically equivalent to $\mathcal{L}^{\ell_i}$. Assume that $\ell_3 \geq 2$ and that either $(\ell_1, \ell_2) \geq (2,5)$ or $(\ell_1, \ell_2) \geq (3,4)$. Then the following map of vector spaces is surjective:*

$$\mathfrak{R}(\mathcal{L}_1, \mathcal{L}_2) \otimes H^0(\mathfrak{J}, \mathcal{L}_3) \to \mathfrak{R}(\mathcal{L}_1, \mathcal{L}_2 \otimes \mathcal{L}_3). \tag{2.40}$$

Let us describe the map in (2.40) explicitly. Consider a tensor $\sum_i s_i \otimes t_i \in \mathfrak{R}(\mathcal{L}_1, \mathcal{L}_2)$. This means that for each i, we have $s_i \in H^0(\mathfrak{J}, \mathcal{L}_1)$ and $t_i \in H^0(\mathfrak{J}, \mathcal{L}_2)$, and that furthermore $\sum_i s_i \cdot t_i = 0$ in $H^0(\mathfrak{J}, \mathcal{L}_1 \otimes \mathcal{L}_2)$. Let $u \in H^0(\mathfrak{J}, \mathcal{L}_3)$. Then $(\sum_i s_i \otimes t_i) \otimes u$ is mapped to the element $\sum_i s_i \otimes (t_i \cdot u) \in \mathfrak{R}(\mathcal{L}_1, \mathcal{L}_2 \otimes \mathcal{L}_3)$, where each $t_i \cdot u$ belongs to $H^0(\mathfrak{J}, \mathcal{L}_2 \otimes \mathcal{L}_3)$.

We will apply Theorem 2.16 twice. Proposition 2.17 below is not strictly speaking necessary: we will later use a different method to show in Proposition 2.26 that the result holds with the weaker assumption that $k \geq 2$. However, the notation here is simpler than in the proof of Proposition 2.18 below, so this first proof is easier to digest, and can serve as a guide to the proof of Proposition 2.18. The notation $R_{1,0} \cdot I_{k,1}$ was defined in the proof of Proposition 2.13.

Proposition 2.17. *Let $k \geq 3$. Then $R_{1,0} \cdot I_{k,1} = I_{k+1,1}$ and $R_{0,1} \cdot I_{1,k} = I_{1,k+1}$.*

Proof. The two statements are symmetric, so we prove only the first assertion. The key step will be to apply Theorem 2.16 with $\mathcal{L}_1 = \mathcal{M}_{1,0}$, $\mathcal{L}_2 = \mathcal{M}_{k-1,1}$, and $\mathcal{L}_3 = \mathcal{M}_{1,0}$. Hence $\ell_1 = 2$, $\ell_2 = 2k \geq 6$, and $\ell_3 = 2$, and we will invoke the surjectivity of (2.40) at an opportune moment.

Consider an element $f \in I_{k+1,1}$; our goal is to express f in terms of elements of $I_{k,1}$. Writing f in terms of the coordinates $\{P_i\}$ and $\{Q_j\}$ (recall these are respectively bases of $R_{1,0}$ and $R_{0,1}$), we can (nonuniquely) write f in the form $f = \sum_i P_i g_i$ with $g_i \in R_{k,1}$. Let $\overline{g}_i \in \overline{R}_{k,1}$ be the image of g_i when we map it to $\overline{R}_{k,1} = H^0(\mathfrak{J}, \mathcal{M}_{k,1})$. Since $f \in I_{k+1,1}$, we deduce that $\sum_i P_i \otimes \overline{g}_i \in \mathfrak{R}(\mathcal{M}_{1,0}, \mathcal{M}_{k,1})$.

At this point, invoke the surjectivity of (2.40) to obtain a preimage of $\sum_i P_i \otimes \overline{g}_i$. This preimage has the form $\sum_j r_j \otimes P_j \in \mathfrak{R}(\mathcal{M}_{1,0}, \mathcal{M}_{k-1,1}) \otimes R_{1,0}$. Each $r_j \in \mathfrak{R}(\mathcal{M}_{1,0}, \mathcal{M}_{k-1,1})$ can be written as $r_j = \sum_i P_i \otimes \overline{A}_{ij}$ with $\overline{A}_{ij} \in \overline{R}_{k-1,1}$; let $A_{ij} \in R_{k-1,1}$ be a representative of $\overline{A}_{ij}$. The fact that $r_j \in \mathfrak{R}(\mathcal{M}_{1,0}, \mathcal{M}_{k-1,1})$ means that it maps to zero in $\overline{R}_{k,1}$, so for each j we have

$$\sum_i P_i A_{ij} \in I_{k,1}. \tag{2.41}$$

We thus have a preimage $\sum_j(\sum_i P_i \otimes \overline{A}_{ij}) \otimes P_j$ that maps to $\sum_{i,j} P_i \otimes \overline{A_{ij}P_j} = \sum_i P_i \otimes \overline{g}_i$. This last equality takes place inside $\mathfrak{R}(\mathcal{M}_{1,0}, \mathcal{M}_{k,1})$, which is a subspace of $R_{1,0} \otimes \overline{R}_{k,1}$. Now the $\{P_i\}$ are a basis for $R_{1,0}$, so for each i, $\sum_j \overline{A_{ij}P_j} = \overline{g}_i$ inside $\overline{R}_{k,1}$; in other words, $g_i \equiv \sum_j A_{ij}P_j \pmod{I_{k,1}}$ for all i. Hence we obtain

$$f = \sum_i P_i g_i \equiv \sum_{i,j} P_i A_{ij} P_j \pmod{R_{1,0} \cdot I_{k,1}} \equiv 0 \pmod{I_{k,1} \cdot R_{1,0}}, \tag{2.42}$$

where the last congruence holds by (2.41). Hence $f \in R_{1,0} \cdot I_{k,1}$, as desired. □

Proposition 2.18. *Let $d', e' \geq 2$. Then $R_{1,0} \cdot I_{d',e'} = I_{d'+1,e'}$, and we similarly have $R_{0,1} \cdot I_{d',e'} = I_{d',e'+1}$.*

Proof. As before, we prove only the first assertion. Write $d' = d+1$ and $e' = e+1$ with $d, e \geq 1$. We will apply Theorem 2.16 with $\mathcal{L}_1 = \mathcal{M}_{1,1}$, $\mathcal{L}_2 = \mathcal{M}_{d,e}$, and $\mathcal{L}_3 = \mathcal{M}_{1,0}$. This time we use the basis $\{P_iQ_j\}_{i,j}$ for the sixteen-dimensional space $R_{1,1} = \overline{R}_{1,1} = H^0(\mathfrak{J}, \mathcal{M}_{1,1})$. The fact that $d, e \geq 1$ also ensures that $\overline{R}_{d,e} = H^0(\mathfrak{J}, \mathcal{M}_{d,e})$.

Consider an element $f \in I_{d'+1,e'} = I_{d+2,e+1}$. Similarly to the proof of Proposition 2.17, write $f = \sum_{i,j} P_iQ_j g_{ij}$, with $g_{ij} \in R_{d+1,e}$. Once again, $\sum_{i,j} P_iQ_j \otimes \overline{g}_{ij} \in \mathfrak{R}(\mathcal{M}_{1,1}, \mathcal{M}_{d+1,e})$, and this comes from a tensor $\sum_{i,j,k}(P_iQ_j \otimes \overline{A}_{ijk}) \otimes P_k$ with each $\sum_{i,j} P_iQ_j \otimes \overline{A}_{ijk} \in \mathfrak{R}(\mathcal{M}_{1,1}, \mathcal{M}_{d,e})$, for all k. By the same reasoning as before (that is, the fact that we have a basis for $\overline{R}_{1,1}$), we deduce that for all i, j, $g_{ij} \equiv \sum_k A_{ijk}P_k \pmod{I_{d+1,e}}$. Hence $f \equiv \sum_{i,j,k} P_iQ_jA_{ijk}P_k \pmod{R_{1,1} \cdot I_{d+1,e}}$; note here that $R_{1,1} \cdot I_{d+1,e} \subset R_{1,0} \cdot I_{d+1,e+1}$.

Finally, $\sum_{i,j,k} P_iQ_jA_{ijk}P_k = \sum_k(\sum_{i,j} P_iQ_jA_{ijk})P_k \equiv 0 \pmod{I_{d+1,e+1} \cdot R_{1,0}}$ and so we have shown the desired result, that $f \in R_{1,0} \cdot I_{d+1,e+1} = R_{1,0} \cdot I_{d',e'}$. □

Constructing specific elements of $I_{1,2}$ and $I_{2,1}$. Our next goal is to study more carefully certain relations between the $\{P_i\}$ and the $\{Q_j\}$, and to deduce from these a specific basis for each of $I_{1,2}$ and $I_{2,1}$. These bases will allow us to prove Proposition 2.26 below, which strengthens Proposition 2.17 and allows us to reach the principal result of this section, Theorem 2.27, giving our structural results on the bidegrees that are enough to generate the ideal I.

In the setting of algebraic theta functions, we give a construction that is closely related to the result in (4.17), (4.18), and (4.19). We actually discovered those relations in Section 4 earlier in our investigations, based on heuristics on where to expect them, but we need to first carry out a similar computation here, so as to make Theorem 2.27 available to us at the correct moment when we use it later.

We first observe that (2.23) identifies certain quadratic expressions in the $\{Q_j\}$ in terms of the sections $F_{d,\alpha} \in H^0(\mathfrak{J}, \mathcal{L}^4)$. Here, we can view the quadratic expressions in the $\{Q_j\}$ as elements of the 10-dimensional space $R_{0,2}$; since $I_{0,2} = 0$, we can identify $R_{0,2}$ both with $\overline{R}_{0,2}$ and with its 10-dimensional image inside $H^0(\mathfrak{J}, \mathcal{L}^4)$. It follows from the proof of Corollary 2.8 that this image is spanned by those $F_{d,\alpha}$ for which $F_{d,\alpha}(0) \neq 0$, equivalently, for which $e_4(2d, \alpha) = 1$.

We wish to obtain a similar identification for the quadratic expressions in the $\{P_j\}$, in other words for the elements of $R_{2,0}$. Since the $\{P_j\}$ are translations of the $\{Q_j\}$ by D_1, this means that we need to translate the $F_{d,\alpha}$. This amounts to

the action of $\widetilde{(-D_1)} = (-D_1, \phi) \in \tilde{A}_4 \subset \mathcal{G}_4$. According to (2.13) and (2.7), we have

$$\begin{aligned} \widetilde{(-D_1)} * F_{d,\alpha} &= \sum_{c \in B_2} e_4(c,\alpha) e_4(d+c, -D_1) \theta_{[4],d+c} = e_4(d,-D_1) F_{d,\alpha-D_1}, \\ \phi_{p+D_1}(F_{d,\alpha}(p+D_1)) &= e_4(d,-D_1) F_{d,\alpha-D_1}(p). \end{aligned} \tag{2.43}$$

Replace p by $p + D_1$ in (2.23), and write $\hat{h}_{0,p} = (\phi_{p+D_1} \otimes \mathrm{id}_{\mathcal{L}_0^4}) \circ h_{p+D_1,0}$ to obtain

$$\begin{aligned} \hat{h}_{p,0}\Big(\sum_{c \in B_2} e_4(c,\alpha) \theta_{[2],2d+c}(p+D_1) \otimes \theta_{[2],c}(p+D_1) \Big) \\ = e_4(d,-D_1) F_{d,\alpha-D_1}(p) \otimes F_{d,\alpha}(0). \end{aligned} \tag{2.44}$$

Thus the image of $R_{2,0}$ in $H^0(\mathfrak{J}, \mathcal{L}^4)$ is spanned by those $F_{d,\alpha-D_1}$ for which $F_{d,\alpha}(0) \neq 0$. In other words, the image is spanned by those $F_{d,\alpha}$ for which $F_{d,\alpha+D_1}(0) \neq 0$, equivalently, for which $e_4(2d, \alpha + D_1) = 1$.

Let us identify those $F_{d,\alpha}$ that appear in the intersection of the images of $R_{0,2}$ and $R_{0,2}$. The next lemma shows that there are essentially 6 such common choices of $F_{d,\alpha}$, where we limit d and α to one fixed representative of each coset in B_4/B_2 and A_4/A_2, respectively. Equivalently, let us list the corresponding pairs $(2d, 2\alpha) \in B_2 \times A_2$. Recall the notation $B_2 = \{0 = b_{00}, b_{10}, b_{01}, b_{11}\}$ from (2.25) and (2.26).

Lemma 2.19. *The set of pairs $(2d, 2\alpha)$ for which $F_{d,\alpha}$ belongs to the image of both $R_{0,2}$ and $R_{2,0}$ is*

$$\{(0,0), (0,E_1), (0,E_2), (0,E_3), (b_{01},0), (b_{01},E_1)\}. \tag{2.45}$$

Proof. First note that if $b \in B_2$ and $\alpha \in A_4$, we have $e_4(b,\alpha) = e_2(b, 2\alpha)$; this is property (4) on p. 228 of [Mum70] (and it holds more generally for all $b \in \mathfrak{J}[2]$ and $\alpha \in \mathfrak{J}[4]$). Our desired condition on $(2d, 2\alpha)$ is therefore equivalent to $e_2(2d, 2\alpha) = e_2(2d, 2\alpha + E_1) = 1$, because $2D_1 = E_1$. In particular, $e_2(2d, E_1) = 1$, which forces $2d \in \{0, b_{01}\}$. The rest of the calculation is easy. □

From now until the end of the proof of Proposition 2.26, it is convenient to introduce notation for the six common sections $F_{d,\alpha}$ that we have just identified above. First choose any $\alpha_1, \alpha_2, \alpha_3 \in A_4$ with $2\alpha_i = E_i = -E_i$ (for example, we can take $\alpha_1 = D_1$, but the choice of the α_i does not matter). Next choose $\delta \in B_4$ with $2\delta = b_{01}$. Note that $(e_4(\delta, -D_1))^2 = e_4(b_{01}, -D_1) = e_2(b_{01}, E_1) = 1$. Hence $e_4(\delta, -D_1) \in \{\pm 1\}$. We can modify if necessary our initial choice of δ by replacing it with $\delta + b_{10}$; this does not change 2δ, but it modifies $e_4(\delta, -D_1)$ by a factor of $e_4(b_{10}, -D_1) = e_2(b_{10}, E_1) = -1$. So without loss of generality, we can arrange for $e_4(\delta, -D_1) = 1$. We now write

$$\begin{aligned} &S_{00} = F_{0,0}, \quad S_{10} = F_{0,\alpha_1}, \quad S_{01} = F_{0,\alpha_2}, \quad S_{11} = F_{0,\alpha_3}, \\ &s_{00} = S_{00}(0), \quad s_{10} = S_{10}(0), \quad s_{01} = S_{01}(0), \quad s_{11} = S_{11}(0), \\ &T_0 = F_{\delta,0}, \quad T_1 = F_{\delta,\alpha_1}, \quad t_0 = T_0(0), \quad t_1 = T_1(0). \end{aligned} \tag{2.46}$$

Here $S_{00}, S_{10}, S_{01}, S_{11}, T_0, T_1 \in H^0(\mathfrak{J}, \mathcal{L}^4)$, and $s_{00}, s_{10}, s_{01}, s_{11}, t_0, t_1 \in \mathcal{L}_0^4$. Note that by our discussion above, the Thetanullwerte $s_{00}, \ldots, t_1$ are all nonzero.

We now have the following explicit formulas.

Proposition 2.20. *In the formulas below, we use multiplicative notation to write tensor products of elements of fibers of the same line bundle; see the pedantic remark about multiplication in the proof of Corollary 2.8. This means that we write, for*

example, $P_{00}(p)\otimes P_{00}(p)$ (or respectively $P_{00}(p)\otimes P_{01}(p)$) as $P_{00}(p)^2$ (or respectively $P_{00}(p)P_{01}(p)$). We then have, for $p \in \mathfrak{J}$:

$$
\begin{aligned}
\hat{h}_{p,0}(P_{00}(p)^2 + P_{10}(p)^2 + P_{01}(p)^2 + P_{11}(p)^2) &= S_{10}(p) \otimes s_{00},\\
\hat{h}_{p,0}(P_{00}(p)^2 - P_{10}(p)^2 + P_{01}(p)^2 - P_{11}(p)^2) &= S_{00}(p) \otimes s_{10},\\
\hat{h}_{p,0}(P_{00}(p)^2 + P_{10}(p)^2 - P_{01}(p)^2 - P_{11}(p)^2) &= S_{11}(p) \otimes s_{01},\\
\hat{h}_{p,0}(P_{00}(p)^2 - P_{10}(p)^2 - P_{01}(p)^2 + P_{11}(p)^2) &= S_{01}(p) \otimes s_{11},\\
\hat{h}_{p,0}(2(P_{00}(p)P_{01}(p) + P_{10}(p)P_{11}(p))) &= T_1(p) \otimes t_0,\\
\hat{h}_{p,0}(2(P_{00}(p)P_{01}(p) - P_{10}(p)P_{11}(p))) &= T_0(p) \otimes t_1,\\
h_{p,0}(Q_{00}(p)^2 + Q_{10}(p)^2 + Q_{01}(p)^2 + Q_{11}(p)^2) &= S_{00}(p) \otimes s_{00},\\
h_{p,0}(Q_{00}(p)^2 - Q_{10}(p)^2 + Q_{01}(p)^2 - Q_{11}(p)^2) &= S_{10}(p) \otimes s_{10},\\
h_{p,0}(Q_{00}(p)^2 + Q_{10}(p)^2 - Q_{01}(p)^2 - Q_{11}(p)^2) &= S_{01}(p) \otimes s_{01},\\
h_{p,0}(Q_{00}(p)^2 - Q_{10}(p)^2 - Q_{01}(p)^2 + Q_{11}(p)^2) &= S_{11}(p) \otimes s_{11},\\
h_{p,0}(2(Q_{00}(p)Q_{01}(p) + Q_{10}(p)Q_{11}(p))) &= T_0(p) \otimes t_0,\\
h_{p,0}(2(Q_{00}(p)Q_{01}(p) - Q_{10}(p)Q_{11}(p))) &= T_1(p) \otimes t_1.
\end{aligned}
\tag{2.47}
$$

Proof. The above is just a restatement of our formulas (2.23) and (2.44), using the fact that $P_j(p) = \theta_{[2],b_j}(p + D_1)$ and $Q_j(p) = \theta_{[2],b_j}(p)$. Note that in the sums over $c \in B_2 = \{b_{00}, b_{10}, b_{01}, b_{11}\}$ we have $e_4(c, \alpha_i) = e_2(c, E_i)$, whose values are given in (2.25). □

Our next result uses Proposition 2.20 to deduce a projective equality between points in $\mathbf{P}^5$. The six coordinates of these points correspond to the six common sections $F_{d,\alpha}$ from above. As in the discussion following (2.28), we allow the coordinates in $\mathbf{P}^5$ to be elements of the same one-dimensional vector space instead of $\overline{K}$. Note also that if V and W are both one-dimensional vector spaces, and $h : V \to W$ is an isomorphism, then we always have $[h(v_1), \ldots, h(v_6)] = [v_1, \ldots, v_6]$. We will use this tacitly throughout. One example is with $V = \mathcal{L}_p^2 \otimes \mathcal{L}_p^2 = \mathcal{L}_p^4$, a fiber of our line bundle, and the isomorphism $h_{p,0} : \mathcal{L}_p^2 \otimes \mathcal{L}_p^2 \to \mathcal{L}_p^4 \otimes \mathcal{L}_0^4 = W$. We also choose an isomorphism $\mathcal{L}_0^4 \cong \overline{K}$, and identify the Thetanullwerte $s_{00}, \ldots, t_1$ with elements $\tilde{s}_{00}, \ldots, \tilde{t}_1 \in \overline{K}$ (which, as we know, are nonzero). This allows us to replace a tensor such as $S_{00}(p) \otimes s_{00} \in W$ by a product $\tilde{s}_{00} S_{00}(p) \in \mathcal{L}_p^4$ inside projective coordinates.

Proposition 2.21. *For every $p \in \mathfrak{J}$, the projective point (note the unusual order of the coordinates)*

$$
[Q_{01}(p)^2, Q_{01}(p)Q_{00}(p), Q_{00}(p)^2, Q_{11}(p)^2, Q_{11}(p)Q_{10}(p), Q_{10}(p)^2] \in \mathbf{P}^5 \tag{2.48}
$$

is equal to $[\tilde{A}(p),\tilde{B}(p),\tilde{C}(p),\tilde{D}(p),\tilde{E}(p),\tilde{F}(p)]$*, where* $\tilde{A},\dots,\tilde{F}\in H^0(\mathfrak{J},\mathcal{L}^4)$ *are given by*

$$\begin{aligned}
\tilde{A}&=\tilde{s}_{00}S_{00}+\tilde{s}_{10}S_{10}-\tilde{s}_{01}S_{01}-\tilde{s}_{11}S_{11},\\
\tilde{B}&=\tilde{t}_0T_0+\tilde{t}_1T_1,\\
\tilde{C}&=\tilde{s}_{00}S_{00}+\tilde{s}_{10}S_{10}+\tilde{s}_{01}S_{01}+\tilde{s}_{11}S_{11},\\
\tilde{D}&=\tilde{s}_{00}S_{00}-\tilde{s}_{10}S_{10}-\tilde{s}_{01}S_{01}+\tilde{s}_{11}S_{11},\\
\tilde{E}&=\tilde{t}_0T_0-\tilde{t}_1T_1,\\
\tilde{F}&=\tilde{s}_{00}S_{00}-\tilde{s}_{10}S_{10}+\tilde{s}_{01}S_{01}-\tilde{s}_{11}S_{11}.
\end{aligned}\tag{2.49}$$

Moreover, there exist elements $A,\dots,F\in R_{2,0}$ *for which the projective point* $[A(p),B(p),C(p),D(p),E(p),F(p)]$ *is equal to the vector in* (2.48)*. Specifically, define the elements* $\hat{S}_{00},\dots,\hat{T}_1\in R_{2,0}$ *by*

$$\begin{aligned}
\hat{S}_{00}&=\tilde{s}_{10}^{-1}(P_{00}^2-P_{10}^2+P_{01}^2-P_{11}^2),\\
\hat{S}_{10}&=\tilde{s}_{00}^{-1}(P_{00}^2+P_{10}^2+P_{01}^2+P_{11}^2),\\
\hat{S}_{01}&=\tilde{s}_{11}^{-1}(P_{00}^2-P_{10}^2-P_{01}^2+P_{11}^2),\\
\hat{S}_{11}&=\tilde{s}_{01}^{-1}(P_{00}^2+P_{10}^2-P_{01}^2-P_{11}^2),\\
\hat{T}_0&=\tilde{t}_1^{-1}(2(P_{00}P_{01}-P_{10}P_{11})),\\
\hat{T}_1&=\tilde{t}_0^{-1}(2(P_{00}P_{01}+P_{10}P_{11})).
\end{aligned}\tag{2.50}$$

Then define, in a way parallel to (2.49)*,* $A=\tilde{s}_{00}\hat{S}_{00}+\tilde{s}_{10}\hat{S}_{10}-\tilde{s}_{01}\hat{S}_{01}-\tilde{s}_{11}\hat{S}_{11}$*,* $B=\tilde{t}_0\hat{T}_0+\tilde{t}_1\hat{T}_1$*, and so forth, until* $F=\tilde{s}_{00}\hat{S}_{00}-\tilde{s}_{10}\hat{S}_{10}+\tilde{s}_{01}\hat{S}_{01}-\tilde{s}_{11}\hat{S}_{11}$*.*

Proof. The first assertion amounts to combining the equations in (2.47) to obtain statements such as $h_{p,0}(4Q_{0,1}(p)^2)=S_{00}(p)\otimes s_{00}+S_{10}(p)\otimes s_{10}-S_{01}(p)\otimes s_{01}-S_{11}(p)\otimes s_{11}$, and similarly for $h_{p,0}$ applied to 4 times the other components of (2.48). The isomorphism $h_{p,0}$ and the common factor 4, as well as the identification of $\mathcal{L}_0^4$ with $\overline{K}$, do not affect the projective point.

The second assertion holds because the $\hat{S}_j$ (similarly for $\hat{T}_0,\hat{T}_1$) are precisely those elements of $R_{2,0}$ that satisfy $\hat{h}_{p,0}(\hat{S}_j(p))=S_j(p)$, once we take into account the identification of $\mathcal{L}_0^4$ with $\overline{K}$. Thus we have an equality of projective points $[\tilde{A}(p),\dots,\tilde{F}(p)]=[A(p),\dots,F(p)]$. □

We can finally give the promised elements of $I_{2,1}$ and a formula for the Kummer quartic in $I_{4,0}$ (this is the quartic that defines the image of κ'). Essentially the same result holds with the roles of the Ps and Qs reversed, giving us elements of $I_{1,2}$ and $I_{0,4}$. Note however that when we replace Q_j by P_j, which amounts to translation by D_1, we replace each P_j (itself already a translate of Q_j by D_1) with the result of translating Q_j by $E_1=2D_1$; so we replace P_j by $\widetilde{E_1}*Q_j\in\{\pm Q_j\}$. This introduces some sign changes, but does not affect the structure of the result.

Proposition 2.22. *With the abovementioned elements* $A,B,C,D,E,F\in R_{2,0}$ *from Proposition 2.21, we have that the following elements belong to the ideal* I*:*

$$Q_{00}A-Q_{01}B,\quad Q_{00}B-Q_{01}C,\quad Q_{10}D-Q_{11}E,\quad Q_{10}E-Q_{11}F\in I_{2,1}.\tag{2.51}$$

We also obtain

$$AC - B^2, \quad DF - E^2 \in I_{4,0}. \tag{2.52}$$

Both $AC - B^2$ and $DF - E^2$ must be multiples of the Kummer quartic; in fact, they are equal, and

$$\begin{aligned} AC - B^2 &= DF - E^2 \\ &= \frac{\tilde{s}_{00}^2}{\tilde{s}_{10}^2}(P_{00}^2 - P_{10}^2 + P_{01}^2 - P_{11}^2)^2 \\ &\quad + \frac{\tilde{s}_{10}^2}{\tilde{s}_{00}^2}(P_{00}^2 + P_{10}^2 + P_{01}^2 + P_{11}^2)^2 \\ &\quad - \frac{\tilde{s}_{01}^2}{\tilde{s}_{11}^2}(P_{00}^2 - P_{10}^2 - P_{01}^2 + P_{11}^2)^2 \\ &\quad - \frac{\tilde{s}_{11}^2}{\tilde{s}_{01}^2}(P_{00}^2 + P_{10}^2 - P_{01}^2 - P_{11}^2)^2 \\ &\quad - 4\frac{\tilde{t}_0^2}{\tilde{t}_1^2}(P_{00}P_{01} - P_{10}P_{11})^2 \\ &\quad - 4\frac{\tilde{t}_1^2}{\tilde{t}_0^2}(P_{00}P_{01} + P_{10}P_{11})^2. \end{aligned} \tag{2.53}$$

Proof. Consider any of the expressions in (2.51) and (2.52). To show that such an expression belongs to the ideal I, we must check that it vanishes at all $p \in \mathfrak{J}$. This follows from the equality between the projective point $[A(p), B(p), \ldots, F(p)]$ and the projective point $[Q_{01}(p)^2, Q_{01}(p)Q_{00}(p), \ldots, Q_{10}(p)^2]$ from (2.48). For example, $Q_{00}(p)A(p) - Q_{01}(p)B(p)$ (which is technically an element of $\mathcal{L}_p^2 \otimes (\mathcal{L}_p')^4$) is "proportional" to the element $Q_{00}(p)(Q_{01}(p)^2) - Q_{01}(p)(Q_{01}(p)Q_{00}(p))$, which belongs to $\mathcal{L}_p^2 \otimes \mathcal{L}_p^4 = \mathcal{L}_p^6$. This element vanishes, because taking products in tensor powers of $\mathcal{L}_p$ is commutative.

At this point, it is also possible to prove (2.53) directly by expressing all of $A, \ldots, F$ in terms of the P_i and expanding. This is too large to do by hand in that form, but the computation becomes quite approachable if we use our elements $\hat{S}_{00}, \ldots, \hat{T}_1 \in R_{2,0}$, as given in (2.50). We have

$$\begin{aligned} AC - B^2 &= (\tilde{s}_{00}\hat{S}_{00} + \tilde{s}_{10}\hat{S}_{10})^2 - (\tilde{s}_{01}\hat{S}_{01} + \tilde{s}_{11}\hat{S}_{11})^2 - (\tilde{t}_0\hat{T}_0 + \tilde{t}_1\hat{T}_1)^2, \\ DF - E^2 &= (\tilde{s}_{00}\hat{S}_{00} - \tilde{s}_{10}\hat{S}_{10})^2 - (\tilde{s}_{01}\hat{S}_{01} - \tilde{s}_{11}\hat{S}_{11})^2 - (\tilde{t}_0\hat{T}_0 - \tilde{t}_1\hat{T}_1)^2. \end{aligned} \tag{2.54}$$

One-quarter of the difference is then

$$\begin{aligned} 4^{-1}((AC - B^2) - (DF - E^2)) &= \tilde{s}_{00}\tilde{s}_{10}\hat{S}_{00}\hat{S}_{10} - \tilde{s}_{01}\tilde{s}_{11}\hat{S}_{01}\hat{S}_{11} - \tilde{t}_0\tilde{t}_1\hat{T}_0\hat{T}_1 \\ &= (P_{00}^2 - P_{10}^2 + P_{01}^2 - P_{11}^2)(P_{00}^2 + P_{10}^2 + P_{01}^2 + P_{11}^2) \\ &\quad - (P_{00}^2 - P_{10}^2 - P_{01}^2 + P_{11}^2)(P_{00}^2 + P_{10}^2 - P_{01}^2 - P_{11}^2) \\ &\quad - 4(P_{00}P_{01} - P_{10}P_{11})(P_{00}P_{01} + P_{10}P_{11}) \\ &= (P_{00}^2 + P_{01}^2)^2 - (P_{10}^2 + P_{11}^2)^2 - (P_{00}^2 - P_{01}^2)^2 + (P_{10}^2 - P_{11}^2)^2 \\ &\quad - 4P_{00}^2P_{01}^2 + 4P_{10}^2P_{11}^2 \\ &= 0. \end{aligned} \tag{2.55}$$

The common value of $AC - B^2$ and $DF - E^2$ is the parts of (2.54) that are not affected by the sign changes between the two lines. In other words,

$$\begin{aligned} &AC - B^2 = DF - E^2 \\ &= \tilde{s}_{00}^2\hat{S}_{00}^2 + \tilde{s}_{10}^2\hat{S}_{10}^2 - \tilde{s}_{01}^2\hat{S}_{01}^2 - \tilde{s}_{11}^2\hat{S}_{11}^2 - \hat{t}_0^2\hat{T}_0^2 - \hat{t}_1^2\hat{T}_1^2, \end{aligned} \tag{2.56}$$

and this proves (2.53). □

Remark 2.23. We note that the constants such as $\frac{\tilde{s}_{00}^2}{\tilde{s}_{10}^2}$ and $\frac{\tilde{t}_0^2}{\tilde{t}_1^2}$ appearing in (2.53) are independent of the identification made between $\mathcal{L}_0^4$ and $\overline{K}$; they could equally well have been written as $\frac{s_{00}^2}{s_{10}^2}$ and $\frac{t_0^2}{t_1^2}$, with the obvious interpretation of quotients of (nonzero) elements of $\mathcal{L}_0^4$.

We still need to show that the common value of $AC - B^2$ and $DF - F^2$ is not zero. To do this, we need to study the values of the Thetanullwerte $\tilde{s}_j$ and $\tilde{t}_i$, as well as their relation to the values $q_j = Q_j(0) \in \mathcal{L}_0^2$. Analogously to our previous definition, we choose an isomorphism between $\mathcal{L}_0^2$ and $\overline{K}$, under which each q_j can be identified with $\tilde{q}_j \in \overline{K}$, for $j \in \{00, 10, 01, 10\}$. Hence $\kappa(0) = [\tilde{q}_{00}, \tilde{q}_{10}, \tilde{q}_{01}, \tilde{q}_{11}]$.

We choose our identification between the q_j and the $\tilde{q}_j$ so as to have actual equality in the corresponding equations from (2.47), when $p = 0$, after also composing with the isomorphisms $h_{0,0}$; otherwise, we would only have an equality of projective points. Having done all this, we obtain the following identities:

$$\begin{aligned} \tilde{q}_{00}^2 + \tilde{q}_{10}^2 + \tilde{q}_{01}^2 + \tilde{q}_{11}^2 &= \tilde{s}_{00}^2, \\ \tilde{q}_{00}^2 - \tilde{q}_{10}^2 + \tilde{q}_{01}^2 - \tilde{q}_{11}^2 &= \tilde{s}_{10}^2, \\ \tilde{q}_{00}^2 + \tilde{q}_{10}^2 - \tilde{q}_{01}^2 - \tilde{q}_{11}^2 &= \tilde{s}_{01}^2, \\ \tilde{q}_{00}^2 - \tilde{q}_{10}^2 - \tilde{q}_{01}^2 + \tilde{q}_{11}^2 &= \tilde{s}_{11}^2, \\ 2(\tilde{q}_{00}\tilde{q}_{01} + \tilde{q}_{10}\tilde{q}_{11}) &= \tilde{t}_0^2, \\ 2(\tilde{q}_{00}\tilde{q}_{01} - \tilde{q}_{10}\tilde{q}_{11}) &= \tilde{t}_1^2. \end{aligned} \tag{2.57}$$

One can proceed similarly with the $P_j(0)$, if desired; we do not need them for the treatment here.

Lemma 2.24. *Assume (as is the case in Section 4) that the quotient abelian variety $\mathfrak{J}' = \mathfrak{J}/A_2$ is the Jacobian of a genus 2 curve $\mathcal{C}'$, where $\mathcal{C}'$ is related to $\mathcal{C}$ via a Richelot isogeny. Then $\tilde{q}_{00}$, $\tilde{q}_{10}$, $\tilde{q}_{01}$, and $\tilde{q}_{11}$, are all nonzero.*

Proof. We apply Lemma 2.7 to $\mathcal{C}'$ and $\mathfrak{J}'$. Essentially, the $\tilde{q}_j$s are even theta characteristics for $\mathfrak{J}'$. Since we have not set up extended theta structures that include an explicit action of $[-1]$, we prove our lemma by a slightly different approach.

The line bundle $\mathcal{L}^2$ on $\mathfrak{J}$ descends to a symmetric line bundle $\widehat{\mathcal{L}}$ on $\mathfrak{J}'$, along the lift from A_2 to $\tilde{A}_2 \subset \mathcal{G}_2$. Moreover, $\widehat{\mathcal{L}}$ gives a principal polarization on $\mathfrak{J}'$. This means that we can view Q_{00}, which is invariant under $\tilde{A}_2$, as the (unique, up to a scalar) nonzero element of $H^0(\mathfrak{J}', \widehat{\mathcal{L}})$; thus Q_{00} plays the same role as $\theta_{[1],0} \in H^0(\mathfrak{J}, \mathcal{L})$, so Q_{00} vanishes at precisely 6 points of $\mathfrak{J}'[2]$.

The points of $\mathfrak{J}'[2]$ correspond to points of $(A_4 \oplus B_2)/A_2$. Represent each such point as $\alpha + b$, where $\alpha \in \{0, \alpha_1, \alpha_2, \alpha_3\}$ as in the discussion immediately after Lemma 2.19, and $b \in \{0 = b_{00}, b_{10}, b_{01}, b_{11}\}$. Since $\widetilde{b_j} * Q_{00} = Q_j$ for $j \in \{00, 10, 01, 11\}$, the question of whether $Q_{00}(\alpha + b_j) = 0$ is equivalent to whether

$Q_j(\alpha) = 0$, and this vanishing occurs for precisely six of the 16 choices for the pair (j, α). On the other hand, we have $\kappa(\alpha_i) = \kappa(-\alpha_i)$, but also $-\alpha_i = \alpha_i - E_i$. Hence we can use (2.29) to obtain identities of projective points, such as for example

$$\begin{aligned} \kappa(\alpha_1) &= [Q_{00}(\alpha_1), Q_{10}(\alpha_1), Q_{01}(\alpha_1), Q_{11}(\alpha_1)] \\ = \kappa(\alpha_1 - E_1) &= [Q_{00}(\alpha_1), -Q_{10}(\alpha_1), Q_{01}(\alpha_1), -Q_{11}(\alpha_1)]. \end{aligned} \tag{2.58}$$

This equality in $\mathbf{P}^3$ implies that either $Q_{10}(\alpha_1) = Q_{11}(\alpha_1) = 0$, or that $Q_{00}(\alpha_1) = Q_{01}(\alpha_1) = 0$. This identifies two points of $\mathfrak{J}'[2]$ where Q_{00} vanishes. Similarly, using α_2 and α_3, we identify four more points where Q_{00} vanishes. This brings our total to six, which are all associated to points of $\mathfrak{J}'[2]$ with $\alpha \neq 0$. In particular, all the $Q_j(0)$ are nonzero, as desired. □

Lemma 2.25. *The expression $AC - B^2 = DF - E^2$ is a nonzero element of $I_{4,0} \subset R_{4,0}$; it is therefore the Kummer quartic equation.*

Proof. Under the hypotheses of Lemma 2.24, this follows from the fact that the coefficient of $P_{00}P_{01}P_{10}P_{11}$ in (2.53) is a constant times $\frac{\tilde{t}_0^2}{\tilde{t}_1^2} - \frac{\tilde{t}_1^2}{\tilde{t}_0^2}$, whose numerator, $\tilde{t}_0^4 - \tilde{t}_1^4$ is, by (2.57), a constant times $\tilde{q}_{00}\tilde{q}_{01}\tilde{q}_{10}\tilde{q}_{11}$, which is nonzero in this setting.

The proof in the general case takes more work. If (2.53) is zero, then all its coefficients must vanish. Equating the coefficients of $P_{00}^2P_{10}^2$, $P_{00}^2P_{11}^2$, and P_{00}^4 to zero, we obtain that the only way that (2.53) could be zero is if

$$\frac{\tilde{s}_{00}^2}{\tilde{s}_{10}^2} = \frac{\tilde{s}_{10}^2}{\tilde{s}_{00}^2} = \frac{\tilde{s}_{01}^2}{\tilde{s}_{11}^2} = \frac{\tilde{s}_{11}^2}{\tilde{s}_{01}^2}. \tag{2.59}$$

But then the common value of (2.59) is equal to its own reciprocal, so must be ± 1.

In case this common value is 1, then the equalities $\tilde{s}_{00}^2 = \tilde{s}_{10}^2$ and $\tilde{s}_{01}^2 = \tilde{s}_{11}^2$ imply by (2.57) that $\tilde{q}_{10} = \tilde{q}_{11} = 0$. This means that $\kappa(0) = [\tilde{q}_{00}, 0, \tilde{q}_{01}, 0]$. But then we would have $\kappa(0) = \kappa(E_1)$, by (2.29). This contradicts the fact that the Kummer map sends two points $p, q \in \mathfrak{J}$ to the same point $\kappa(p) = \kappa(q) \in \mathbf{P}^3$ if and only if $p = \pm q$; see for example Step I in the proof of Theorem 4.8.1 of [BL04]. (Their proof works over an arbitrary field; note that the divisor Θ is isomorphic to $\mathcal{C}$, and is therefore an irreducible variety.) The case when the common value of (2.59) is -1 is analogous, since in that case we would obtain instead $\tilde{q}_{00} = \tilde{q}_{01} = 0$. □

We can finally prove the stronger version of Proposition 2.17.

Proposition 2.26. *For $k \geq 2$, we have $R_{k-2,0} \cdot I_{2,1} = I_{k,1}$ and $R_{0,k-2} \cdot I_{1,2} = I_{1,k}$.*

Proof. As usual, we only treat the case of $I_{k,1}$. For the purposes of this proof, we write $R_{*,0} = \oplus_{d \geq 0} R_{d,0} = \overline{K}[\{P_i\}]$, the ring of polynomials in the P_i alone. We also identify $R_{*,1} = \oplus_{d \geq 0} R_{d,1}$ with $(R_{*,0})^4$, using the basis $\{Q_j\}$. We similarly identify $I_{*,1} = \oplus_{d \geq 0} I_{d,1}$ with an $R_{*,0}$-submodule of $(R_{*,0})^4$. In this setting, the four elements of $I_{2,1}$ listed in (2.51) correspond to the vectors

$$(A, -B, 0, 0), \qquad (B, -C, 0, 0), \qquad (0, 0, D, -E), \qquad (0, 0, E, -F). \tag{2.60}$$

Our goal is to show that the $R_{*,0}$-submodule of $(R_{*,0})^4$ generated by these four vectors corresponds precisely to $I_{*,1}$. Now these four vectors are linearly independent, even over the field of fractions of $R_{*,0}$ (that is, the field of rational functions in the P_i, viewed as independent transcendentals). Indeed, putting together these vectors into a 4×4 matrix with entries in $R_{*,0}$, this matrix is block diagonal, with

its 2×2 subblocks having determinants $-AC + B^2$ and $-DF + E^2$. As we have seen, these determinants are equal and nonzero.

The above implies that our four elements of $I_{2,1}$ generate a free $R_{*,0}$-module of rank four, and this free module is itself a submodule of $I_{*,1}$. Now the dimension of the bidegree $(k, 1)$ component of this free module is exactly $4 \dim R_{k-2,0}$, by viewing each element of the $(k, 1)$-homogeneous component as a linear combination of our four vectors, with coefficients in $R_{k-2,0}$. We also know that $\dim I_{k,1} = 4 \dim R_{k-2,0}$, by Corollary 2.14. So we have proved our desired result.

Our proof yields expressions for each of $(-AC + B^2, 0, 0, 0)$, $(0, -AC + B^2, 0, 0)$, $(0, 0, -DF + E^2, 0)$, and $(0, 0, 0, -DF + E^2)$ as an R-linear combination of our original four vectors. In other words, the product of the Kummer quartic by each Q_j is an easy combination of the elements from $I_{2,1}$: for example, $C(Q_{00}A - Q_{01}B) - B(Q_{00}B - Q_{01}C) = Q_{00}(AC - B^2) \in I_{4,1}$. This gives a good way to see how our four elements of $I_{2,1}$ actually generate all multiples of the Kummer quartic in $I_{d,e}$ when $e \geq 1$. On some level, the homogeneous component $I_{4,0}$ is only needed to generate the $I_{k,0}$ for $k \geq 4$. □

Putting all the above results together, we obtain the our basic structural result about generators for the bigraded ideal of relations between the P_is and the Q_js. We state this slightly more generally, to bring out the parts of the construction that will matter in Section 4, when we carry out similar computations while working carefully over a field of definition for the original curve $\mathcal{C}$.

Theorem 2.27. *Let $\mathfrak{J}$ be the Jacobian of a genus 2 curve $\mathcal{C}$ over a field K that is not of characteristic 2. Let $\mathcal{L}$ be a symmetric line bundle on $\mathfrak{J}$ that gives rise to the principal polarization on $\mathfrak{J}$, so that $\dim H^0(\mathfrak{J}, \mathcal{L}^2) = 4$ and this linear series yields the Kummer embedding of $\mathfrak{J}/[\pm 1]$ into $\mathbf{P}^3$. Also let $\mathcal{L}'$ be the translate of $\mathcal{L}$ by a point of order 4 in $\mathfrak{J}(K)$, and consider the resulting embedding $\mathfrak{J} \hookrightarrow \mathbf{P}^3 \times \mathbf{P}^3$ associated to the linear series of $\mathcal{L}^2$ and $(\mathcal{L}')^2$. Then the resulting bigraded ideal I of relations in this model is generated by:*

- *$I_{0,4}$ and $I_{4,0}$, which are each 1-dimensional,*
- *$I_{1,2}$ and $I_{2,1}$, which are each 4-dimensional, and*
- *$I_{2,2}$, which is 36-dimensional.*

Moreover, there are no equations of bidegree $(1, 1)$, that is, $I_{1,1} = 0$.

Proof. The dimensions of the components $I_{d,e}$, and the ranks of the multiplication maps from $R_{d,e} \times I_{d',e'} \to I_{d+d',e+e'}$, are unaffected by passing from K to its algebraic closure $\overline{K}$. We may therefore place ourselves in the situation that was studied in this section, with the Kummer embedding given by κ, in terms of the $\{Q_j\}$ coordinates, and the embedding into $\mathbf{P}^3 \times \mathbf{P}^3$ being given by the Ps and the Qs. In that case, the relations in bidegrees $(0, 4)$ and $(4, 0)$ generate all relations of bidegrees $(0, k)$ and $(k, 0)$, by the proof of Proposition 2.10. The relations in bidegrees $(1, 2)$ and $(2, 1)$ generate all relations of bidegrees $(1, k)$ and $(k, 1)$, by Proposition 2.26. The relations in bidegree $(2, 2)$ generate all the $I_{d,e}$ with $d, e \geq 2$, by Proposition 2.18. The dimensions of all the $I_{d,e}$ have also been calculated above, in Proposition 2.10 and Corollary 2.14. □

We will also need a result about the relations between the P_i and Q_j on sums and differences of points on $\mathfrak{J}$. This follows from combining Proposition 2.12 with Theorem 2.2.

Theorem 2.28. *There exist polynomials A_{ij}, with coefficients in $\overline{K}$, and of multidegree $(1,1,1,1)$ in the four sets of variables $\{P_{i'}(p)\}, \{Q_{j'}(p)\}, \{P_{k'}(r)\}, \{Q_{\ell'}(r)\}$, such that for all $p, r \in \mathfrak{J}$, the 4×4 matrices below are projectively equal:*

$$\Big[P_i(p+r)Q_j(p-r)\Big]_{i,j} = \Big[A_{ij}\big(\{P_{i'}(p)\}, \{Q_{j'}(p)\}, \{P_{k'}(r)\}, \{Q_{\ell'}(r)\}\big)\Big]_{i,j}. \tag{2.61}$$

The essential claim here is that the coefficients of A_{ij} do not depend on the points p, r. Projective equality of matrices can be viewed as equality in $\mathbf{P}^{15}$, if one enumerates the entries of each matrix in the same order.

Proof. This proof uses similar ideas to the proof of Theorem 2.12. Once again, let $q \in \mathfrak{J}$ satisfy $2q = D_1$. In the setting of (2.18), we have

$$\begin{aligned} &h_{p+q,r+q}(\theta_{[2],b_1}(p+r+D_1) \otimes \theta_{[2],b_2}(p-r)) \\ &\qquad = \sum_{c \in B_2} \theta_{[4],d_1+d_2+c}(p+q) \otimes \theta_{[4],d_1-d_2+c}(r+q). \end{aligned} \tag{2.62}$$

As b_1 and b_2 vary over all of B_2, the left hand side of the above equation gives the entries of the projective matrix $[P_i(p+r)Q_j(p-r)]_{i,j}$; as usual, the isomorphism $h_{p+q,r+q}$ respects projective equality. In the analogous matrix made out of the right hand side of (2.62), we can view $\theta_{[4],d_1+d_2+c}(p+q)$ as the value at p of a section of $T_q^*\mathcal{L}^4$, just as in the proof of Proposition 2.12, where the section in question can be interpreted as an element of $R_{1,1}$; so we can express each $\theta_{[4],d_1+d_2+c}(p+q)$ (up to projective equivalence) as a polynomial of bidegree $(1,1)$ in the variables $\{P_{i'}(p)\}, \{Q_{j'}(p)\}$. Similarly, we can view each expression $\theta_{[4],d_1-d_2+c}(r+q)$ as the value at r of another element of $R_{1,1}$, in other words as a polynomial of bidegree $(1,1)$ in the variables $\{P_{i'}(r)\}, \{Q_{j'}(r)\}$. These identifications are all made up to projective equivalence, in other words up to a common "constant factor" that is independent of any d in $\theta_{[4],d}$. Each term in the sum on the right, being a product $\theta_{[4],d_1+d_2+c}(p+q) \otimes \theta_{[4],d_1-d_2+c}(r+q)$, can therefore be viewed as a certain polynomial of multidegree $(1,1,1,1)$ in our four sets of variables. Adding up all these polynomials produces the desired A_{ij}.

For the diligent reader, here is a sketch of a more explicit, but messier, proof of this theorem, following an approach that is similar to that in Propositions 2.20 and 2.21. Each $P_i(p+r)Q_j(p-r)$ can be written as a linear combination of expressions analogous to the left hand side of (2.19). In somewhat loose notation, let us write these analogous expressions as $\sum_{c \in B_2} e_4(c,\alpha) P_{2d+c}(p+r)Q_c(p-r)$, which we can identify (projectively) as the product $F_{d,\alpha}(p+q)F_{d,\alpha}(r+q)$. Specializing to $r = 0$ gives a (projective) identity between $[\sum_{c \in B_2} e_4(c,\alpha) P_{2d+c}(p)Q_c(p)]_{d,\alpha}$ and $[\tilde{f}_{d,\alpha} F_{d,\alpha}(p+q)]_{d,\alpha}$; a similar identity holds when $p = 0$. Here we have identified the nonvanishing theta constants $F_{d,\alpha}(q)$ with field elements $\tilde{f}_{d,\alpha} \in \overline{K}^*$. Write $U_{d,\alpha} = \sum_{c \in B_2} e_4(c,\alpha) P_{2d+c} Q_c \in R_{1,1}$. We then projectively identify the three 16-tuples $\Big[\sum_{c \in B_2} e_4(c,\alpha) P_{2d+c}(p+r)Q_c(p-r)\Big]_{d,\alpha}$, $\Big[F_{d,\alpha}(p+q) \otimes F_{d,\alpha}(r+q)\Big]_{d,\alpha}$, and $\Big[\tilde{f}_{d,\alpha}^{-2} U_{d,\alpha}(p) U_{d,\alpha}(r)\Big]_{d,\alpha}$. Taking corresponding linear combinations of the entries of the first and third 16-tuples produces the identification in (2.61). □

Remark 2.29. Throughout our discussion, the line bundle $\mathcal{M}_{1,1}$ and its sections have figured prominently. The reason is that if we compose our embedding $\mathfrak{J} \to \mathbf{P}^3 \times \mathbf{P}^3$ with the Segre map $\mathbf{P}^3 \times \mathbf{P}^3 \hookrightarrow \mathbf{P}^{15}$, this gives precisely the projective

embedding of $\mathfrak{J}$ that is given by $\mathcal{M}_{1,1}$. Since this line bundle is algebraically equivalent to $\mathcal{L}^4$, the ideal describing the image of $\mathfrak{J}$ in $\mathbf{P}^{15}$ is the usual homogeneous ideal in 16 variables that is generated by 72 quadrics. These quadric generators correspond to the 36 basis elements of $I_{2,2}$, combined with the 36 quadrics describing the image of the Segre map: these are $(P_iQ_j)(P_kQ_\ell) - (P_iQ_\ell)(P_kQ_j)$. It follows that, in our bigraded ring R, our ideal I is in fact the saturation of the ideal generated by $I_{2,2}$. This explains the important role played by $I_{2,2}$ in this section.

3. An approach for an explicit derivation of the Edwards curve

Recall the model for the Edwards curve in [BL07] (generalising the form given in [Edw07]):

$$U^2 + Y^2 = 1 + dU^2Y^2. \tag{3.1}$$

This has a universal group law, provided that d is non-square over the ground field. In this section, we present a style of deriving the Edwards curve and choices for its group law, which make use of a $\mathbf{P}^1 \times \mathbf{P}^1$ embedding, arising from the projective x-coordinates of a point D and $D + D_1$, where D_1 is a fixed point of order 4. We shall then imitate this style and notation when we describe our genus 2 approach in the next section.

We first describe a general elliptic curve $\mathcal{C}$, defined over a field K, not of characteristic 2, which has a point D_1 of order 4. Then $E_1 = 2D_1$ will have order 2, and there will be a 2-isogeny ϕ from $\mathcal{C}$ to a curve $\mathcal{C}'$ of the form $y^2 = x(x-\alpha)(x-\beta)$. (Here we have imposed the additional requirement that all the 2-torsion points of $\mathcal{C}'$ are defined over K.) Say that $(\alpha, 0) = \phi(D_1)$ so that α is square. Scale α to 1, take $\mathcal{C}'$ to have the form $y^2 = x(x-1)(x-d)$, and then we may use the standard 2-isogeny with kernel $\langle(0,0)\rangle$ from $y^2 = x(x^2+h_1x+h_2)$ to $y^2 = x(x^2-2h_1x+h_1^2-4h_2)$ (as given on p.74 of [Sil86]) to find the curve

$$\mathcal{C} : y^2 = x(x^2 + 2(1+d)x + (1-d)^2), \tag{3.2}$$

which has $D_1 = (1-d, 2(1-d))$ of order 4, and $E_1 = 2D_1 = (0,0)$ of order 2.

For any point D on $\mathcal{C}$, we let $[k_1, k_2] = \big[k_1(D), k_2(D)\big] \in \mathbf{P}^1$ denote the projective x-coordinate, so that $x(D) = k_2(D)/k_1(D)$. Then addition by E_1 induces $[k_1, k_2] \mapsto [k_2, (1-d)^2k_1]$; this can be described by the projective linear transformation

$$\begin{pmatrix} k_1 \\ k_2 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 \\ (1-d)^2 & 0 \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \end{pmatrix}, \tag{3.3}$$

and this matrix has eigenvalues $1-d$ and $d-1$ with eigenvectors $\binom{1}{1-d}$ and $\binom{-1}{1-d}$, respectively. We can perform a change of basis which diagonalises the effect of addition by E_1, namely:

$$\begin{pmatrix} k_1 \\ k_2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1-d & 1-d \end{pmatrix} \begin{pmatrix} l_1 \\ l_2 \end{pmatrix}. \tag{3.4}$$

Now let E_0 denote the identity element, let E_1 be as above, and let E_2, E_3 be the other points of order 2 on $\mathcal{C}$. For any point D on $\mathcal{C}$, let $l(D)$ denote $[l_1(D), l_2(D)] \in \mathbf{P}^1$. Then: $l(E_0) = [1,1]$, $l(E_1) = [1,-1]$, $l(E_2) = [-\sqrt{d}, 1]$ and $l(E_3) = [\sqrt{d}, 1]$. Addition by these points maps $[l_1, l_2]$ to, respectively: $[l_1, l_2]$, $[l_1, -l_2]$, $[-\sqrt{d}\, l_2, l_1]$ and $[\sqrt{d}\, l_2, l_1]$. Further, if D_1 is the point of order 4 given above, then $l(D_1) = [1, 0]$.

Recall the standard result (see, for example, Definition 2.1 in [Fly95]) that, for points D, E on $\mathcal{C}$, the 2×2 matrix $\big(k_i(D+E)k_j(D-E)+k_j(D+E)k_i(D-E)\big)$ is projectively equal to a 2×2 matrix of forms which are biquadratic in $[k_1(D), k_2(D)]$ and $[k_1(E), k_2(E)]$. If we perform the linear change in coordinates to the l-coordinates, we see that these have a particularly simple form. Indeed, if we let $[u_1, u_2] = [l_1(D), l_2(D)]$ and $[v_1, v_2] = [l_1(E), l_2(E)]$ and define the $B_{ij} = B_{ij}([u_1, u_2], [v_1, v_2])$ by:

(3.5)
$$\Big(B_{ij}\Big) = \begin{pmatrix} -du_1^2v_2^2 - du_2^2v_1^2 + du_2^2v_2^2 + u_1^2v_1^2 & (1-d)u_1u_2v_1v_2 \\ (1-d)u_1u_2v_1v_2 & -du_2^2v_2^2 - u_1^2v_1^2 + u_1^2v_2^2 + u_2^2v_1^2 \end{pmatrix}$$

then the 2×2 matrices $\big(B_{ij}\big)$ and $\big(l_i(D+E)l_j(D-E) + l_j(D+E)l_i(D-E)\big)$ are projectively equal.

We now embed our elliptic curve $\mathcal{C}$ into $\mathbf{P}^1\times\mathbf{P}^1$, using the embedding:

$$D \mapsto \Big([u_1, u_2], [y_1, y_2]\Big) = \Big(\big[l_1(D), l_2(D)\big], \big[l_1(D+D_1), l_2(D+D_1)\big]\Big). \tag{3.6}$$

Since $l(D_1) = [1, 0]$, we can substitute $v_1 = 1, v_2 = 0$ into (3.5) to see that the matrix $\big(l_i(D+D_1)l_j(D-D_1) + l_j(D+D_1)l_i(D-D_1)\big)$ is projectively the same as

$$\begin{pmatrix} -du_2^2 + u_1^2 & 0 \\ 0 & -u_1^2 + u_2^2 \end{pmatrix}. \tag{3.7}$$

Furthermore, $\big(l_i(D+D_1)l_j(D-D_1)+l_j(D+D_1)l_i(D-D_1)\big)$ is the same as $\big(l_i(D+D_1)l_j(D+D_1+E_1)+l_j(D+D_1)l_i(D+D_1+E_1)\big)$. If we use that $y_i = l_i(D+D_1)$ and the fact that addition by E_1 induces $[l_1, l_2] \mapsto [l_1, -l_2]$, we see that our matrix is also projectively equal to

$$\begin{pmatrix} 2y_1^2 & 0 \\ 0 & -2y_2^2 \end{pmatrix}. \tag{3.8}$$

Since (3.7) and (3.8) are projectively equal, we see that

$$(-du_2^2 + u_1^2)(-y_2^2) = (-u_1^2 + u_2^2)y_1^2. \tag{3.9}$$

If we now define the affine variables $U = u_2/u_1$ and $Y = y_2/y_1$ then $-(-dU^2 + 1)Y^2 = -1+U^2$, giving $U^2+Y^2 = 1+dU^2Y^2$, which is the equation of the Edwards curve.

By an analog of Theorem 2.28, the matrix $\big(l_i(D+E)l_j(D-E+D_1)\big)_{i,j}$ is projectively the same as a matrix whose entries are linear combinations of the terms of the form $l_{i_1}(D)l_{i_2}(E)l_{i_3}(D+D_1)l_{i_4}(E+D_1)$. If we let, for $i\in\{1,2\}$,

$$u_i = l_i(D),\ y_i = l_i(D+D_1),\ v_i = l_i(E),\ z_i = l_i(E+D_1), \tag{3.10}$$

then we may regard $\big([u_1, u_2], [y_1, y_2]\big)$ and $\big([v_1, v_2], [z_1, z_2]\big)$ as two arbitrary points on the $\mathbf{P}^1\times\mathbf{P}^1$ embedding of our curve. We thus know that there is a matrix $\big(A_{ij}\big)$, where each $A_{ij} = A_{ij}\big(([u_1, u_2], [y_1, y_2]), ([v_1, v_2], [z_1, z_2])\big)$ is a linear combination of terms of the form $u_{i_1}v_{i_2}y_{i_3}z_{i_4}$, with the property that $\big(A_{ij}\big) = \big(l_i(D+E)l_j(D-E+D_1)\big)$. Each A_{ij} has 16 coefficients, and so there are 64 coefficients to be found. These can be determined just from the linear equations in the coefficients arising from the cases when: (i) D is general and E is any of the 2-torsion points, (ii) E is general and D is any of the 2-torsion points, and (iii) $D = E = D_1$. This gives

$$\Big(A_{ij}\Big) = \begin{pmatrix} u_1v_1y_1z_1 - du_2v_2y_2z_2 & u_1v_2y_2z_1 - u_2v_1y_1z_2 \\ -u_1v_1y_2z_2 + u_2v_2y_1z_1 & -u_1v_2y_1z_2 + u_2v_1y_2z_1 \end{pmatrix}. \tag{3.11}$$

We see that any column of $\big(A_{ij}\big)$ gives the u-coordinates of $D+E$.

There should also be a matrix $\big(J_{ij}\big) = \big(l_i(D+E+D_1)l_j(D-E)\big)$, and indeed we see that

$$\begin{aligned}
&J_{ij}\big(([u_1,u_2],[y_1,y_2]),([v_1,v_2],[z_1,z_2])\big)\\
&= J_{ij}\big(([l_1(D),l_2(D)],[l_1(D+D_1),l_2(D+D_1)]),\\
&\qquad ([l_1(E),l_2(E)],[l_1(E+D_1),l_2(E+D_1)])\big)\\
&= l_i(D+E+D_1)l_j(D-E)\\
&= l_j(D-E)l_i(D+E+D_1)\\
&= A_{ji}\big(([l_1(D),l_2(D)],[l_1(D+D_1),l_2(D+D_1)]),\\
&\qquad ([l_1(-E),l_2(-E)],[l_1(-E+D_1),l_2(-E+D_1)])\big)\\
&= A_{ji}\big(([l_1(D),l_2(D)],[l_1(D+D_1),l_2(D+D_1)]),\\
&\qquad ([l_1(E),l_2(E)],[l_1(E-D_1),l_2(E-D_1)])\big)\\
&= A_{ji}\big(([l_1(D),l_2(D)],[l_1(D+D_1),l_2(D+D_1)]),\\
&\qquad ([l_1(E),l_2(E)],[l_1(E+E_1+D_1),l_2(E+E_1+D_1)])\big)\\
&= A_{ji}\big(([l_1(D),l_2(D)],[l_1(D+D_1),l_2(D+D_1)]),\\
&\qquad ([l_1(E),l_2(E)],[l_1(E+D_1),-l_2(E+D_1)])\big)\\
&= A_{ji}\big(([u_1,u_2],[y_1,y_2]),([v_1,v_2],[z_1,-z_2])\big).
\end{aligned} \tag{3.12}$$

So, if we define

$$J_{ij}\big(([u_1,u_2],[y_1,y_2]),([v_1,v_2],[z_1,z_2])\big) = A_{ji}\big(([u_1,u_2],[y_1,y_2]),([v_1,v_2],[z_1,-z_2])\big) \tag{3.13}$$

this gives

$$\Big(J_{ij}\Big) = \begin{pmatrix} u_1v_1y_1z_1 + du_2v_2y_2z_2 & u_1v_1y_2z_2 + u_2v_2y_1z_1 \\ u_1v_2y_2z_1 + u_2v_1y_1z_2 & u_1v_2y_1z_2 + u_2v_1y_2z_1 \end{pmatrix}. \tag{3.14}$$

We see that $\big(J_{ij}\big) = \big(l_i(D+E+D_1)l_j(D-E)\big)$ and that any column of $\big(J_{ij}\big)$ gives the y-coordinates of $D+E$.

We now have a description of the group law for our $\mathbf{P}^1\times\mathbf{P}^1$ embedding; namely, $D+E$ is given by any column of $\big(A_{ij}\big)$ together with any column of $\big(J_{ij}\big)$. If we write our original points in affine coordinates (U,Y) and (V,Z), where $U=u_2/u_1$, $Y=y_2/y_1$, $V=v_2/v_1$ and $Z=z_2/z_1$, then the sum could be given by any of

$$\begin{aligned}
\Big(A_{21}/A_{11}, J_{21}/J_{11}\Big) &= \Big((-YZ+UV)/(1-dUVYZ),(VY+UZ)/(1+dUVYZ)\Big),\\
\Big(A_{21}/A_{11}, J_{22}/J_{12}\Big) &= \Big((-YZ+UV)/(1-dUVYZ),(VZ+UY)/(YZ+UV)\Big),\\
\Big(A_{22}/A_{12}, J_{21}/J_{11}\Big) &= \Big((-VZ+UY)/(VY-UZ),(VY+UZ)/(1+dUVYZ)\Big),\\
\Big(A_{22}/A_{11}, J_{22}/J_{12}\Big) &= \Big((-VZ+UY)/(VY-UZ),(VZ+UY)/(YZ+UV)\Big),
\end{aligned} \tag{3.15}$$

which the same as the group law in [BL07], after taking account of the fact that we are taking $(1,0)$ as the identity, whereas $(0,1)$ is taken to be the identity element in [BL07]. We can think of the columns of the matrices $\big(A_{ij}\big)$ and $\big(J_{ij}\big)$ as giving all variations of the group law.

We finally note that, if $A_{11} = A_{21} = 0$ then

$$y_1 z_1 A_{11} + d y_2 z_2 A_{21} = u_1 v_1 (y_1^2 z_1^2 - d y_2^2 z_2^2) = 0. \tag{3.16}$$

Suppose that d is non-square over the ground field K. Since $[u_1, u_2], [y_1, y_2] \in \mathbf{P}^1$ and satisfy (3.9), it follows that u_1 and y_1 are nonzero (which also has the consequence that the the affine coordinate $U = u_2/u_1$ is always well defined, and so the above affine variety has no points at infinity). Similarly, v_1 and z_1 are nonzero. This is inconsistent with (3.16), and so we see that, provided d is non-square, we can never have $A_{11} = A_{21} = 0$; similarly, we can never have any of $A_{12} = A_{22} = 0$, $J_{11} = J_{21} = 0$ or $J_{12} = J_{22} = 0$, and so there are no exceptional cases for any of the above versions of the group law.

We can see how the existence of an always nonzero coordinate and the existence of a universal group law follow from the fact that, on our original elliptic curve (3.2), our condition that d is non-square forces the point $(d-1, 2(d-1)\sqrt{d})$ to be not defined over the ground field; this in turn forces u_1 to be always nonzero for all points $\big([u_1, u_2], [y_1, y_2]\big)$ defined over the ground field; that is to say, $l_1(D)$ is nonzero for any D defined over the ground field. For any two points D, E, since $\big(A_{ij}\big) = \big(l_i(D+E) l_j(D-E+D_1)\big)$ it follows that $\big[A_{11}, A_{21}\big] = \big[l_1(D+E) l_1(D-E+D_1), l_2(D+E) l_1(D-E+D_1)\big] = [l_1(D+E), l_2(D+E)]$ cannot have both entries 0, since $l_1(D-E+D_1)$ is nonzero. Similarly J_{11}, J_{21} are not both zero. Yet another interpretation is to note that the intersection of our elliptic curve with the condition $u_1 = 0$ is by (3.9) the pair of points $\{([0,1], [1, \pm\sqrt{d}])\} \subset \mathbf{P}^1 \times \mathbf{P}^1$. Our condition on d ensures that this pair of points is collectively but not individually defined over the ground field. This serves to ensure that each of $[A_{11}, A_{21}]$ and $[J_{11}, J_{21}]$ is a well defined projective point with a nonzero coordinate, and we have a universal group law.

Of course, even if d is square, our matrices A, J in (3.11) and (3.14) still give a description of the group law which covers all possibilities; it is merely that there will not be a specified column which covers all possibilities; rather, one will need to use one column for some cases and another column for others, or more generally one can use a linear combination of columns, which gives the same projective point.

We note in passing that, since negation has the effect: $\big([u_1, u_2], [y_1, y_2]\big) \mapsto \big([u_1, u_2], [y_1, -y_2]\big)$, we may replace y_2 with $\sqrt{\varkappa} y_2$, for any nonsquare $\varkappa \in K$, and the result will still be defined over K. This is due to the fact that the nontrivial Galois action $\sqrt{\varkappa} \mapsto -\sqrt{\varkappa}$ has the same effect as negation, so that the variety is taken to itself under this action. After replacing y_2 with $\sqrt{\varkappa} y_2$, we obtain the affine model $U^2 + \varkappa Y^2 = 1 + d\varkappa U^2 Y^2$, which is a quadratic twist of the original curve, and is birationally equivalent over K to the twisted Edwards curve, described in [BBJ+08].

4. An analog for Jacobians of genus 2 curves

In this section, we shall derive our $\mathbf{P}^3 \times \mathbf{P}^3$ embedding of the Jacobian variety of a genus 2 curve, giving explicitly a set of defining equations for the variety in Theorem 4.2 and its group law in Theorem 4.1.

The standard embedding of the Kummer surface. We shall first describe a standard embedding of the Kummer surface, which will be given in (4.2). For a

general curve of genus 2

$$y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0, \tag{4.1}$$

defined over a ground field K (not of characteristic 2). we may represent elements of the Jacobian variety by $\{(x_1, y_1), (x_2, y_2)\}$, as a shorthand for the divisor class of $(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-$, where ∞^+ and ∞^- denote the points on the non-singular curve that lie over the singular point at infinity. The role of the projective x-coordinate in the previous section will be performed by the Kummer surface, which has an embedding (see p.18 of [CF96]) in $\mathbf{P}^3$ given by $[k_1, k_2, k_3, k_4]$, where

$$k_1 = 1,\ k_2 = x_1 + x_2,\ k_3 = x_1x_2,\ k_4 = (F_0(x_1, x_2) - 2y_1y_2)/(x_1 - x_2)^2, \tag{4.2}$$

and where

$$\begin{aligned} F_0(x_1, x_2) =& 2f_0 + f_1(x_1 + x_2) + 2f_2(x_1x_2) + f_3(x_1x_2)(x_1 + x_2) \\ &+ 2f_4(x_1x_2)^2 + f_5(x_1x_2)^2(x_1 + x_2) + 2f_6(x_1x_2)^3. \end{aligned} \tag{4.3}$$

The defining equation of the Kummer surface is given by

$$R(k_1, k_2, k_3)k_4^2 + S(k_1, k_2, k_3)k_4 + T(k_1, k_2, k_3) = 0, \tag{4.4}$$

where R, S, T are given by:

$$\begin{aligned} R(k_1, k_2, k_3) &= k_2^2 - 4k_1k_3, \\ S(k_1, k_2, k_3) &= -2\left(2k_1^3f_0 + k_1^2k_2f_1 + 2k_1^2k_3f_2 + k_1k_2k_3f_3 + 2k_1k_3^2f_4\right. \\ &\quad \left. + k_2k_3^2f_5 + 2k_3^3f_6\right), \\ T(k_1, k_2, k_3) &= -4k_1^4f_0f_2 + k_1^4f_1^2 - 4k_1^3k_2f_0f_3 - 2k_1^3k_3f_1f_3 - 4k_1^2k_2^2f_0f_4 \\ &\quad + 4k_1^2k_2k_3f_0f_5 - 4k_1^2k_2k_3f_1f_4 - 4k_1^2k_3^2f_0f_6 + 2k_1^2k_3^2f_1f_5 \\ &\quad - 4k_1^2k_3^2f_2f_4 + k_1^2k_3^2f_3^2 - 4k_1k_2^3f_0f_5 + 8k_1k_2^2k_3f_0f_6 - 4k_2^4f_0f_6 \\ &\quad - 4k_1k_2^2k_3f_1f_5 + 4k_1k_2k_3^2f_1f_6 - 4k_1k_2k_3^2f_2f_5 - 2k_1k_3^3f_3f_5 \\ &\quad - 4k_2^3k_3f_1f_6 - 4k_2^2k_3^2f_2f_6 - 4k_2k_3^3f_3f_6 - 4k_3^4f_4f_6 + k_3^4f_5^2. \end{aligned}$$

Our aim now is to follow the style of the previous section and derive a $\mathbf{P}^3 \times \mathbf{P}^3$ embedding of the Jacobian variety, arising from the images on the Kummer surface of the point D (on the Jacobian) and $D + D_1$, where D_1 is a fixed point of order 4.

Forcing the existence of two independent points of order 4. We shall next describe a general genus 2 curve $\mathcal{C}$ whose Jacobian has independent points D_1, D_2 of order 4; the model for such a curve wll be given in (4.8). Then $E_1 = 2D_1$ and $E_2 = 2D_2$ will have order 2. We shall also insist that $\langle E_1, E_2\rangle$ is a maximal isotropic subgroup which is the kernel of a Richelot isogeny, as described on p.89 of [CF96]. These requirements force the Jacobian to be isogenous to the Jacobian of a curve $\mathcal{C}'$ with full 2-torsion. After a linear change in variable, the curve $\mathcal{C}'$ is given by $y^2 = x(x-1)(x-\alpha)(x-\beta)(x-\gamma)$, which is $y^2 = H_1(x)H_2(x)H_3(x)$, where $H_1(x) = x$, $H_2(x) = (x-1)(x-\alpha)$ and $H_3(x) = (x-\beta)(x-\gamma)$. Suppose that the kernel of the dual isogeny consists of the identity, $\{\infty, (0,0)\}$, $\{(1,0), (\alpha,0)\}$ and $\{(\beta,0), (\gamma,0)\}$. The points D_1, D_2 of order 4 on the Jacobian of $\mathcal{C}$ must map to points of order 2 outside the above mentioned kernel; say that D_1 and D_2 map respectively to $\{(1,0), \infty\}$ and $\{(\beta,0), \infty\}$. As an aside, we note that $\{(1,0), \infty\}$ and $\{(\beta,0), \infty\}$ have a nontrivial Weil pairing, so the original points D_1, D_2 do not generate an isotropic subgroup of the 4-torsion in the Jacobian of $\mathcal{C}$, even though their doubles E_1, E_2 do generate an isotropic subgroup of the 2-torsion.

From the standard maps on p.106 of [CF96], the rationality of D_1 and D_2 forces all of 1, $(1-\beta)(1-\gamma)$, β and $(\beta-1)(\beta-\alpha)$ to be squares. This is solved by:

$$\alpha = \underline{a}^2 + b^2 - \underline{a}^2 b^2,\ \beta = b^2,\ \gamma = b^2\underline{c}^2 - \underline{c}^2 + 1. \tag{4.5}$$

We shall now increase the generality by only requiring that E_1, E_2, D_1 are defined over the ground field, but not necessarily D_2. We let $a = \underline{a}^2$, $c = \underline{c}^2$, so that

$$\alpha = a + b^2 - ab^2,\ \beta = b^2,\ \gamma = b^2 c - c + 1, \tag{4.6}$$

where a, b, c are arbitrary members of some ground field K, which is not of characteristic 2. If we define the h_{ij} by $H_j = H_j(x) = h_{j2}x^2 + h_{j1}x + h_{j0}$, then we recall that the general formula for the isogenous curve $\mathcal{C}$ is

$$y^2 = \Delta\big(H_2'H_3 - H_2H_3'\big)\big(H_3'H_1 - H_3H_1'\big)\big(H_1'H_2 - H_1H_2'\big), \tag{4.7}$$

where $\Delta = \det(h_{ij})$. If we apply this to our specific H_1, H_2, H_3, we see that our original curve (after absorbing the factor $(b-1)^2(b+1)^2/ac$ into y^2 by a quadratic twist of the y-coordinate) has the form

$$\mathcal{C} : y^2 = g\big((f+1)x^2 - 2gx + b^2 f - de\big)\big(x^2 - b^2 d\big)\big(x^2 + e\big), \tag{4.8}$$

where

$$\begin{aligned} d &= b^2c - c + 1, \\ e &= ab^2 - a - b^2, \\ f &= a + c - 1, \\ g &= b^2 c + a. \end{aligned} \tag{4.9}$$

We require that the discriminant of $\mathcal{C}$ is nonzero, which is equivalent to the condition that $2abcdefg(a-1)(b^2-1)(c-1)$ is nonzero. Let $\mathfrak{J} = \mathrm{Jac}(\mathcal{C})$, the Jacobian of $\mathcal{C}$. Let E_0 be the identity element in $\mathfrak{J}$, and let $E_1 = \{(g + (b^2-1)\sqrt{acf})/(a+c), 0), (g - (b^2-1)\sqrt{acf})/(a+c), 0)\}$, $E_2 = \{(b\sqrt{d}, 0), (-b\sqrt{d}, 0)\}$ and $E_3 = \{(\sqrt{-e}, 0), (-\sqrt{-e}, 0)\}$ be the points of order 2 on $\mathfrak{J}$ corresponding to the three quadratic factors given on the right hand side of (4.8). These are all defined over the ground field K. For any $D \in \mathfrak{J}$, let $k(D) = [k_1(D), k_2(D), k_3(D), k_4(D)]$ denote the image of D in the above embedding of the Kummer surface. Let D_1, D_2, D_3 be points of order 4 such that $2D_1 = E_1$, $2D_2 = E_2$ and $2D_3 = E_3$ (chosen so that $D_3 = D_1 + D_2$). It can be checked directly (see the file [Fly22]) that D_1 is defined over the ground field K. Furthermore, D_2, D_3 are defined over $K(\sqrt{a}, \sqrt{c})$.

Diagonalising addition by the order two elements E_1, E_1. We know (see p.22 of [CF96]) that addition by any point of order 2 gives a linear map on the Kummer surface. We simultaneously diagonalise addition by E_1 and E_2 (as described in the file [Fly22]) using the following linear change of basis for the Kummer surface.

$$\begin{pmatrix} l_1 \\ l_2 \\ l_3 \\ l_4 \end{pmatrix} = Q \begin{pmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \end{pmatrix} \tag{4.10}$$

where $Q = (Q_{ij})$ is the 4×4 matrix with entries:

$$\begin{aligned}
Q_{11} &= 2gb^2e(b^4c^2 - 2b^2c^2 + 2b^2c + c^2 + a - c),\\
Q_{12} &= -2g^2b^2e,\\
Q_{13} &= 2g(a^2b^2 + ab^2c - b^4c - a^2 - 2ab^2 - ac + a),\\
Q_{14} &= 1,\\
Q_{21} &= -2gd(a^2b^4 - 2a^2b^2 - ab^4 + b^4c + a^2 + 2ab^2),\\
Q_{22} &= 2g^2d,\\
Q_{23} &= -2g(ab^4c + b^4c^2 - ab^2c - b^4c - b^2c^2 + 2b^2c + a),\\
Q_{24} &= 1,\\
Q_{31} &= 2gb^2(a^2b^4c + ab^4c^2 - 2a^2b^2c - 2ab^4c - 2ab^2c^2\\
&\qquad + a^2c + 4ab^2c + ac^2 + b^4c - 2ac + a),\\
Q_{32} &= -2b^2g^2,\\
Q_{33} &= 2g(ab^4c - 2ab^2c + ab^2 + ac + b^2c),\\
Q_{34} &= -1,\\
Q_{41} &= -2gde(b^4c + a),\\
Q_{42} &= 2g^2de,\\
Q_{43} &= -2g(-b^4c^2 + a^2b^2 + b^2c^2 - a^2 - ab^2 - b^2c),\\
Q_{44} &= -1.
\end{aligned} \tag{4.11}$$

For any $D \in \mathfrak{J}$, we let $l(D) = [l_1(D), l_2(D), l_3(D), l_4(D)]$. We first note that, after this linear change in coordinates, the equation of the Kummer surface is considerably simplified:

$$\begin{aligned}
&\big(bg(acl_1l_2 - fl_3l_4)\big)^2 =\\
&\big(b^2(ac(fl_1^2 - el_2^2) + cefl_3^2 - afl_4^2)\big)\big(ac(dl_1^2 + b^2fl_2^2) - f(adl_3^2 + b^2cl_4^2)\big).
\end{aligned} \tag{4.12}$$

As above, we let E_0 denote the identity element, and let E_1, E_2, E_3 be the points of order 2 above. Then: $l(E_0) = [1, 1, -1, -1]$, $l(E_1) = [1, 1, 1, 1]$, $l(E_2) = [1, -1, -1, 1]$ and and $l(E_3) = [1, -1, 1, -1]$. Addition by these points maps a general $[l_1, l_2, l_3, l_4]$ to, respectively: $[l_1, l_2, l_3, l_4]$, $[l_1, l_2, -l_3, -l_4]$, $[l_1, -l_2, l_3, -l_4]$ and $[l_1, -l_2, -l_3, l_4]$. Further, if D_1, D_2, D_3 are the points of order 4 given above, then $l(D_1) = [b, 1, 0, 0]$, $l(D_2) = [0, 1, 0, -\sqrt{a}]$ and $l(D_3) = [1, 0, 0, \sqrt{c}]$.

Simplified biquadratic forms on the Kummer surface. There is a result on Jacobians of genus two curves analogous to that mentioned previously for elliptic curves (see Theorem 3.4.1 of [CF96]) that, for points D, E on $\mathfrak{J}$, the 4×4 matrix $\big(k_i(D + E)k_j(D - E) + k_j(D + E)k_i(D - E)\big)$ is projectively equal to a 4×4 matrix of forms which are biquadratic in $[k_1(D), k_2(D), k_3(D), k_4(D)]$ and $[k_1(E), k_2(E), k_3(E), k_4(E)]$. If we perform the linear change in coordinates to the l-coordinates, we see that these have a simpler form.

Indeed, if we let $[u_1, u_2, u_3, u_4] = [l_1(D), l_2(D), l_3(D), l_4(D)]$ and $[v_1, v_2, v_3, v_4] = [l_1(E), l_2(E), l_3(E), l_4(E)]$ then there are biquadratic forms

$$B_{ij} = B_{ij}\big([u_1, u_2, u_3, u_4], [v_1, v_2, v_3, v_4]\big) \tag{4.13}$$

such that the 4×4 matrices $\big(B_{ij}\big)$ and $\big(l_i(D+E)l_j(D-E)+l_j(D+E)l_i(D-E)\big)$ are projectively equal. The B_{ij} are derived and given explicitly in the file [Fly22].

Embedding the Jacobian into $\mathbf{P}^3 \times \mathbf{P}^3$. We shall now embed our Jacobian $\mathfrak{J}$ into $\mathbf{P}^3 \times \mathbf{P}^3$, using the embedding:

(4.14)
$$\begin{aligned}
&D \mapsto \Big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\Big)\\
&= \Big(l(D), l(D+D_1)\Big)\\
&= \Big([l_1(D),l_2(D),l_3(D),l_4(D)],[l_1(D+D_1),l_2(D+D_1),l_3(D+D_1),l_4(D+D_1)]\Big).
\end{aligned}$$

Our aim for the rest of this section will be to describe the defining equations and group law for this embedding.

We note that there are the following linear maps on this embedding

$$\begin{aligned}
&D \mapsto -D\\
&: \big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big) \mapsto \big([u_1,u_2,u_3,u_4],[y_1,y_2,-y_3,-y_4]\big),\\
&D \mapsto D+E_1\\
&: \big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big) \mapsto \big([u_1,u_2,-u_3,-u_4],[y_1,y_2,-y_3,-y_4]\big),\\
&D \mapsto D+E_2\\
&: \big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big) \mapsto \big([u_1,-u_2,u_3,-u_4],[y_1,-y_2,y_3,-y_4]\big),\\
&D \mapsto D+E_3\\
&: \big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big) \mapsto \big([u_1,-u_2,-u_3,u_4],[y_1,-y_2,-y_3,y_4]\big),\\
&D \mapsto D+D_1\\
&: \big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big) \mapsto \big([y_1,y_2,y_3,y_4],[u_1,u_2,-u_3,-u_4]\big),\\
&D \mapsto D-D_1\\
&: \big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big) \mapsto \big([y_1,y_2,-y_3,-y_4],[u_1,u_2,u_3,u_4]\big),
\end{aligned} \tag{4.15}$$

from which it follows that

$$\begin{aligned}
&D \mapsto -D-D_1\\
&: \big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big) \mapsto \big([y_1,y_2,y_3,y_4],[u_1,u_2,u_3,u_4]\big),
\end{aligned} \tag{4.16}$$

which swaps the u_i and y_i. The above mappings generate a group of mappings which is isomorphic to $C_2 \times D_8$.

Using the biquadratic forms to obtain some of the defining equations. Since $l(D_1) = [b,1,0,0]$, we can substitute $v_1 = b, v_2 = 1, v_3 = 0, v_4 = 0$ into the B_{ij}, to give $M = \big(l_i(D+D_1)l_j(D-D_1)+l_j(D+D_1)l_i(D-D_1)\big)$, when we

find that (as derived in the file [Fly22])

$$\begin{aligned}
&\big[M_{1,1},M_{1,2},M_{2,2},M_{3,3},M_{3,4},M_{4,4}\big]\\
&\quad=\big[b^2(ac(-fu_1^2+eu_2^2)-cefu_3^2+afu_4^2),\\
&\qquad -bg(acu_1u_2-fu_3u_4),\\
&\qquad -ac(du_1^2+b^2fu_2^2)+f(adu_3^2+b^2cu_4^2),\\
&\qquad ab^2c(cu_1^2+au_2^2-fu_3^2-u_4^2),\\
&\qquad abcg(u_1u_2-u_3u_4),\\
&\qquad ac(adu_1^2-b^2ceu_2^2+deu_3^2-b^2fu_4^2)\big]
\end{aligned}\tag{4.17}$$

and all other entries are zero.

Furthermore, $\big(l_i(D+D_1)l_j(D-D_1)+l_j(D+D_1)l_i(D-D_1)\big)$ is the same as $\big(l_i(D+D_1)l_j(D+D_1+E_1)+l_j(D+D_1)l_i(D+D_1+E_1)\big)$. If we now use that $y_i=l_i(D+D_1)$ and the fact that addition by E_1 induces $[l_1,l_2,l_3,l_4]\mapsto[l_1,l_2,-l_3,-l_4]$, we see that our matrix is also projectively equal to N, which satisfies

$$\begin{aligned}
&\big[N_{1,1},N_{1,2},N_{2,2},N_{3,3},N_{3,4},N_{4,4}\big]\\
&=\big[y_1^2,y_1y_2,y_2^2,-y_3^2,-y_3y_4,-y_4^2\big].
\end{aligned}\tag{4.18}$$

Since (4.17) and (4.18) are projectively equal, we see that we now have a number of equations satisfied by $\big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big)$, namely anything of the form

$$M_{i_1,j_1}N_{i_2,j_2}-M_{i_2,j_2}N_{i_1,j_1}=0.\tag{4.19}$$

for any $i_1,j_1,i_2,j_2\in\{1,2,3,4\}$. For example, the following must be satisfied:

$$abcg(u_1u_2-u_3u_4)y_1y_2=bg(acu_1u_2-fu_3u_4)y_3y_4.$$

However, we can see from Theorem 2.27 that, unlike the elliptic curves situation, we do not yet have a complete set of defining equations. So, we shall now proceed to the equations for the group law since it will turn out that the group law equations will allow us to deduce the missing defining equations of our variety.

The group law for our $\mathbf{P}^3\times\mathbf{P}^3$ embedding. We can now derive the group law, which will soon be described in Theorem 4.1. We know from Theorem 2.28 that the projective matrix $\big(l_i(D+E)l_j(D-E+D_1)\big)$ is the same as a matrix whose entries are linear combinations of the terms of the form $l_{i_1}(D)l_{i_2}(E)l_{i_3}(D+D_1)l_{i_4}(E+D_1)$. If we let, for $i\in\{1,2,3,4\}$,

$$u_i=l_i(D),\ y_i=l_i(D+D_1),\ v_i=l_i(E),\ z_i=l_i(E+D_1),\tag{4.20}$$

then we may regard $\big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big)$ and $\big([v_1,v_2,v_3,v_4],[z_1,z_2,z_3,z_4]\big)$ as two arbitrary points on the $\mathbf{P}^3\times\mathbf{P}^3$ embedding of our Jacobian. We know that there is a matrix $\big(A_{ij}\big)$, where each

$$A_{ij}=A_{ij}\Big(\big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big),\big([v_1,v_2,v_3,v_4],[z_1,z_2,z_3,z_4]\big)\Big)$$

is a linear combination of terms of the form $u_{i_1}v_{i_2}y_{i_3}z_{i_4}$, with the property that $\big(A_{ij}\big)=\big(l_i(D+E)l_j(D-E+D_1)\big)$. These coefficients can be determined just from the linear equations in the coefficients arising from considering the effects of (i) translations by E_1,E_2,E_3 and D_1, (ii) swapping D and E, as well as the cases when: (iii) D is general and E is any of the 2-torsion points, (iv) E is general and

D is any of the 2-torsion points, and (v) $D = E = D_1$. These are derived in the file [Fly22] and give the following result.

$$\begin{aligned}
A_{11} &= -abc(u_1y_1(dv_1z_1 + bev_2z_2) + beu_2y_2(v_1z_1 - bv_2z_2)) \\
&\quad - bf(eu_3y_3(dv_3z_3 - bv_4z_4) - bu_4y_4(ev_3z_3 + bv_4z_4)), \\
A_{12} &= ab^2cf(u_1y_2(v_1z_2 - bv_2z_1) - u_2y_1(bv_1z_2 - v_2z_1)) \\
&\quad + b^2f^2(-u_3y_4(v_3z_4 - bv_4z_3) + u_4y_3(bv_3z_4 - v_4z_3)), \\
A_{13} &= abf(u_1y_3(dv_3z_1 - bv_4z_2) - u_3y_1(dv_1z_3 - bv_2z_4)) \\
&\quad + ab^2f(-u_2y_4(v_3z_1 - bv_4z_2) + u_4y_2(v_1z_3 - bv_2z_4)), \\
A_{14} &= b^2cf(u_1y_4(bv_4z_1 + ev_3z_2) - u_4y_1(bv_1z_4 + ev_2z_3)) \\
&\quad + b^2cef(u_2y_3(v_4z_1 - bv_3z_2) - u_3y_2(v_1z_4 - bv_2z_3)), \\
A_{22} &= ac(du_1y_1(v_1z_1 - bv_2z_2) - bu_2y_2(dv_1z_1 + bev_2z_2)) \\
&\quad + f(du_3y_3(ev_3z_3 + bv_4z_4) + bu_4y_4(dv_3z_3 - bv_4z_4)), \\
A_{23} &= b^2cf(-u_1y_4(v_4z_1 - bv_3z_2) + u_4y_1(v_1z_4 - bv_2z_3)) \\
&\quad + b^2cf(u_2y_3(bv_4z_1 + ev_3z_2) - u_3y_2(bv_1z_4 + ev_2z_3)), \\
A_{24} &= adf(-u_1y_3(v_3z_1 - bv_4z_2) + u_3y_1(v_1z_3 - bv_2z_4)) \\
&\quad + abf(u_2y_4(dv_3z_1 - bv_4z_2) - u_4y_2(dv_1z_3 - bv_2z_4)), \\
A_{33} &= abc(u_1y_1(dv_3z_3 - bv_4z_4) + bu_2y_2(ev_3z_3 + bv_4z_4)) \\
&\quad - abc(u_3y_3(dv_1z_1 + bev_2z_2) - bu_4y_4(v_1z_1 - bv_2z_2)), \\
A_{34} &= ab^2cf(-u_1y_2(v_3z_4 - bv_4z_3) + u_2y_1(bv_3z_4 - v_4z_3)) \\
&\quad + ab^2cf(u_3y_4(v_1z_2 - bv_2z_1) - u_4y_3(bv_1z_2 - v_2z_1)), \\
A_{44} &= ac(du_1y_1(ev_3z_3 + bv_4z_4) - beu_2y_2(dv_3z_3 - bv_4z_4)) \\
&\quad - ac(deu_3y_3(v_1z_1 - bv_2z_2) + bu_4y_4(dv_1z_1 + bev_2z_2)),
\end{aligned} \tag{4.21}$$

where A_{ij} for $i > j$ are defined by

$$\begin{aligned}
&A_{ij}\Big(\big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big),\big([v_1,v_2,v_3,v_4],[z_1,z_2,z_3,z_4]\big)\Big) \\
=&A_{ji}\Big(\big([y_1,y_2,y_3,y_4],[u_1,u_2,u_3,u_4]\big),\big([v_1,v_2,v_3,v_4],[z_1,z_2,z_3,z_4]\big)\Big),
\end{aligned} \tag{4.22}$$

due to the fact that $A_{ij}(D,E) = A_{ji}(-D-D_1,E)$. We see that any nonzero column of $\big(A_{ij}\big)$ gives the u-coordinates of $D+E$; this corresponds to a choice of j with $l_j(D-E+D_1) \neq 0$.

By the same reasoning as in the previous section, if we define

$$\begin{aligned}
&J_{ij}\Big(\big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big),\big([v_1,v_2,v_3,v_4],[z_1,z_2,z_3,z_4]\big)\Big) \\
&= A_{ji}\Big(\big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big),\big([v_1,v_2,v_3,v_4],[z_1,z_2,-z_3,-z_4]\big)\Big),
\end{aligned} \tag{4.23}$$

then $J_{ij} = l_i(D+E+D_1)l_j(D-E)$, and any nonzero column of $\big(J_{ij}\big)$ gives the y-coordinates of $D+E$.

The above discussion gives our desired description of the group law for our $\mathbf{P}^3 \times \mathbf{P}^3$ embedding.

Theorem 4.1. *Let D and E be given as elements of $\mathbf{P}^3 \times \mathbf{P}^3$, as above. Then the image of $D+E$ in $\mathbf{P}^3 \times \mathbf{P}^3$ is given by any column of $\big(A_{ij}\big)$ in the first $\mathbf{P}^3$,*

together with any column of $\big(J_{ij}\big)$ *in the second* $\mathbf{P}^3$*. More generally, we can take linear combinations of columns: for any choice of* $c_1,\dots,c_4$ *and* $c'_1,\dots,c'_4$ *for which* $\sum_j c_j l_j(D-E+D_1)\neq 0$ *and* $\sum_j c'_j l_j(D-E)\neq 0$*, we have that* $D+E$ *is represented by* $([\sum_j c_j A_{ij}]_i,[\sum_j c'_j J_{ij}]_i)\in\mathbf{P}^3\times\mathbf{P}^3$*.*

A complete set of defining equations. Let us return to the defining equations, which we shall shortly be in a position to describe completely in Theorem 4.2. To make upcoming expressions more succinct, we shall now define several quadratic forms. For $i\in\{1,2,3,4,5,6\}$, let $r_i=r_i(u_1,u_2,u_3,u_4)$ be the following quadrics in u_1,u_2,u_3,u_4, that we have already encountered before as certain $M_{i,j}$ in (4.17):

$$\begin{aligned}
r_1&=b^2(ac(-fu_1^2+eu_2^2)-cefu_3^2+afu_4^2),\\
r_2&=-bg(acu_1u_2-fu_3u_4),\\
r_3&=-ac(du_1^2+b^2fu_2^2)+f(adu_3^2+b^2cu_4^2),\\
r_4&=ab^2c(cu_1^2+au_2^2-fu_3^2-u_4^2),\\
r_5&=abcg(u_1u_2-u_3u_4),\\
r_6&=ac(adu_1^2-b^2ceu_2^2+deu_3^2-b^2fu_4^2).
\end{aligned}\tag{4.24}$$

For $i\in\{1,2,3,4,5,6\}$, let s_i be exactly the same quadric in y_1,y_2,y_3,y_4; that is, define:

$$s_i=r_i(y_1,y_2,y_3,y_4).\tag{4.25}$$

We recall that we previously found a number of quartic forms satisfied by u_1,u_2,u_3, u_4,y_1,y_2,y_3,y_4. The u_i and the y_i each satisfy the Kummer surface equation (4.12), giving a quartic form purely in the u_i, and another purely in the y_i, that is to say, forms of bidegrees $(4,0)$ and $(0,4)$. We also previously noted the projective equality in the arrays given in (4.17) and (4.18), which gives forms of bidegree $(2,2)$. These do not so far give a complete set of defining equations. What we now also have available is that the columns of the matrix $\big(A_{ij}\big)$ given in (4.21), are projectively equal, and we may use this for any specified choice of E to give further quartics. These quartics arise as the 2×2 minors of (A_{ij}), and they are of bidegree $(2,2)$, due to the fact that each entry of the matrix is itself of bidegree $(1,1)$ once E is fixed. We merely need to apply this for the choice $E=D_2$ in order to obtain the remaining forms of bidegree $(2,2)$. We may further derive from these every $u_i(u_2s_1-u_1s_2)$, for $i\in\{1,2,3,4\}$ and so deduce that $u_2s_1-u_1s_2$ must be satisfied. We may similarly deduce that $u_2s_2-u_1s_3$, $u_4s_4-u_3s_5$, $u_4s_5-u_3s_6$, $y_2r_1-y_1r_2$, $y_2r_2-y_1r_3$, $y_4r_4-y_3r_5$, $y_4r_5-y_3r_6$ are all satisfied. At this point, we are able to obtain a complete set of defining equations, as described in the next theorem.

Theorem 4.2. *Let* K *be any field, not of characteristic* 2*, and let* $a,b,c\in K$*. Let* $\mathcal{C}$ *be as defined in (4.8), where* d,e,f,g *are as in (4.9), with* $2abcdefg(a-1)(b^2-1)(c-1)$ *nonzero, and let* $\mathfrak{J}$ *be the Jacobian variety of* $\mathcal{C}$*. Let* $E_1,E_2,E_3\in\mathfrak{J}(K)$ *be the points of order* 2 *and* $D_1\in\mathfrak{J}(K)$ *the point of order* 4*, such that* $2D_1=E_1$*, described immediately after (4.9). For any* $D\in\mathfrak{J}(K)$*, let* $l(D)=[l_1(D),l_2(D),l_3(D),l_4(D)]$ *be the embedding of the Kummer surface given in (4.10). Embed the Jacobian variety into* $\mathbf{P}^3\times\mathbf{P}^3$ *according to the embedding* $\big(l(D),l(D+D_1)\big)$ *given in (4.14), and let* $\big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big)$ *be a member of this embedding. Furthermore, let* r_i *and* s_i *be the quadratic forms given in (4.24) and (4.25), for* $i\in$

$\{1,2,3,4,5,6\}$. *Then the following is a set of defining equations.*

$$
\begin{aligned}
&r_2^2 - r_1 r_3,\ s_2^2 - s_1 s_3,\\
&u_2 s_1 - u_1 s_2,\ u_2 s_2 - u_1 s_3,\ u_4 s_4 - u_3 s_5,\ u_4 s_5 - u_3 s_6,\\
&y_2 r_1 - y_1 r_2,\ y_2 r_2 - y_1 r_3,\ y_4 r_4 - y_3 r_5,\ y_4 r_5 - y_3 r_6,\\
&r_1 y_3^2 + r_4 y_1^2,\ r_1 y_4^2 + r_6 y_1^2,\ r_2 y_3 y_4 + r_5 y_1 y_2,\\
&a(bu_2 y_1 - u_1 y_2)(bu_4 y_3 - u_3 y_4) - (eu_3 y_2 + bu_4 y_1)(bu_2 y_3 - u_1 y_4),\\
&c(eu_3 y_3 + bu_4 y_4)(bu_2 y_2 - u_1 y_1) - f(bu_2 y_4 - u_1 y_3)(bu_4 y_2 - u_3 y_1).
\end{aligned}
\tag{4.26}
$$

Proof. It is checked in the file [Fly22] that all of the above are satisfied, and that they generate independent equations as follows: 1 of bidegree $(4,0)$, 1 of bidegree $(0,4)$, 16 of bidegree $(3,1)$, 16 of bidegree $(1,3)$, 36 of bidegree $(2,2)$, 4 of bidegree $(2,1)$ and 4 of bidegree $(1,2)$. The way that the independence of a collection of N equations is checked in [Fly22] is by finding a collection of N monomials appearing in the equations, and showing that the corresponding $N \times N$ matrix giving the coefficient of the ith monomial in the jth equation has a determinant that is divisible only by factors of the nonzero discriminant $2abcdefg(a-1)(b^2-1)(c-1)$. Thus the equations that we have found are independent for all values of the parameters that we are considering. From Theorem 2.27 we see that we must therefore have a complete set of defining equations. □

At this stage, we now have a complete description of our variety; (4.26) gives a set of defining equations, and the group law is given by any column of the matrix $\left(A_{ij}\right)$ given in (4.21) together with any column of $\left(J_{ij}\right)$ given in (4.23). It is apparent how much nicer both the defining equations and description of the group law are here, compared with the $\mathbf{P}^{15}$ embedding given in [CF96], where the defining equations were given as 72 quadrics, and the defining equations on the Jacobian variety were too enormous to be given explicitly in general.

We also note that the linear maps in (4.15) and (4.16) give rise to a number of symmetries in our defining equations. We see that the defining equations on the third line of (4.26) are the images of those on the second line of (4.26) under the transformation of (4.16). So, if we wish, this gives a still more succinct description in terms of a smaller number of defining equations, together with their orbits under (4.15) and (4.16)

Twists of our abelian surface. We note that, since the effect of negation, described in (4.15), negates y_3 and y_4, we may create a twist of our abelian surface by replacing these with $\sqrt{\varkappa_1}y_3, \sqrt{\varkappa_1}y_4$, and this will still be defined over the ground field K, for the same reasons as described in the previous section for elliptic curves. Similarly, $D \mapsto -D - E_1$ negates u_3, u_4 and $D \mapsto D + E_3$ negates u_2, u_4, y_2, y_4, so we have the following twists.

Definition 4.3. Let $\mathfrak{J}$ be as given in Theorem 4.2. For any nonsquare $\varkappa_1, \varkappa_2, \varkappa_3 \in K$, define $\mathfrak{J}^{(\varkappa_1,\varkappa_2,\varkappa_3)}$ to be the abelian surface, defined over K, whose defining equations are the same as those given in Theorem 4.2, except that u_1, u_2, u_3, u_4 are replaced by $u_1, \sqrt{\varkappa_3}u_2, \sqrt{\varkappa_2}u_3, \sqrt{\varkappa_2}\sqrt{\varkappa_3}u_4$, respectively, and y_1, y_2, y_3, y_4 are replaced by $y_1, \sqrt{\varkappa_3}y_2, \sqrt{\varkappa_1}y_3, \sqrt{\varkappa_1}\sqrt{\varkappa_3}y_4$, respectively.

5. Conditions for non-degeneracy of the group law

Our goal in this section is to find conditions on the parameters (analogous to the condition for Edwards curves that d is nonsquare) which will imply that the group law is universal; this will be stated in Corollary 5.2 (a consequence of Theorem 5.1).

Our strategy is to search for suitable $c_1, \ldots, c_4$ for which the sum $\sum_j c_j l_j(F)$ is nonzero for all K-rational divisors $F \in \mathfrak{J}$ (where the l_j are as defined in (4.10)). By Theorem 4.1, with such a choice of $\{c_j\}$ (and the same choice of $c'_j = c_j$), the expressions $\sum_j c_j l_j(D + E + D_1)$ and $\sum_j c_j l_j(D - E)$ will never be zero when D and E are themselves K-rational. This will yield a universal group law.

We will illustrate three attempts to find such a linear combination $s = \sum_j c_j l_j$ which does not vanish at any K-rational point of $\mathfrak{J}$. The first two attempts were instructive near misses, and the third attempt was successful in identifying a concrete set of conditions on the parameters which would ensure the nonvanishing of s on K-rational points.

The vanishing locus of s over the algebraic closure $\overline{K}$ of K is best understood in terms of linear series. Recall from Section 2 that s is a section of the line bundle $\mathcal{L}^2$. As in the proof of Lemma 2.7, let Θ, the theta-divisor, be the vanishing locus of $\theta_{[1],0}$; then $\mathcal{L} \cong \mathcal{O}_{\mathfrak{J}}(\Theta)$, and Θ is isomorphic to $\mathcal{C}$. Then the vanishing loci for the different choices of s are the divisors on $\mathfrak{J}$ belonging to the linear series $|2\Theta|$. For a generic choice of s (over $\overline{K}$), its vanishing locus is a smooth curve of genus 5; this follows from the adjunction formula, which in the case of an abelian surface says that a smooth genus g curve $\mathcal{X} \subset \mathfrak{J}$ has self-intersection $\mathcal{X} \cdot \mathcal{X} = 2g - 2$, since the canonical bundle on $\mathfrak{J}$ is trivial. So for a typical K-rational choice of s, we expect that the K-rational points where s vanishes are the K-rational points of a curve of genus 5; this is the phenomenon we observe in our first attempt below.

In our second and third attempts below, we start from the observation that for $p \in \mathfrak{J}(\overline{K})$, the divisor $(\Theta+p)\cup(\Theta-p)$ belongs to $|2\Theta|$. Here the two translates $\Theta \pm p$ of Θ intersect in two points, because $\Theta \cdot \Theta = 2$. (The intersection points might not be distinct.) For certain choices of p, we can hope that each of the two irreducible components $\Theta + p$ and $\Theta - p$ is defined over a common quadratic extension of K, and that the two components are conjugate to each other. In that situation, the only K-rational points on the union are potentially the intersection points between the two components.

When the two intersection points coincide at a point q, then this point is K-rational, and is the only K-rational vanishing point of s. This corresponds to our second attempt below. In our third attempt, we identify a situation and choice of s that does not vanish at any K-rational points. We believe, but have not checked the details, that in this situation the two points of intersection are individually defined over a quadratic extension of K, but not over K itself. The construction in our third attempt has a similar flavor to the constructions in Section 4.2 of [AKR12] and Section 2.1 of [AC12], which treat the case of the embedding of $\mathfrak{J}$ into $\mathbf{P}^{15}$.

Two near miss attempts. For our first attempt, let us imagine that $u_1 = 0$. Suppose also that the following are not squares in the ground field: $a, c, d, -e, -cef, af$, $cd, adf, -ae, cf$ (where d, e, f, g are as defined in (4.9)). Then, as shown in [Fly22], one can deduce directly from the defining equations that $u_2, u_3, u_4, y_1, y_2, y_3, y_4$ are all nonzero and that one can set $u_2 = 1, y_1 = 1$, and use the defining equations to

eliminate u_3, y_2; the defining equations then become equivalent to the affine curve:

$$\begin{aligned} u_4^2(-fy_4^2+ac)/(-b^2fy_4^2+acd) &= -y_4^2ace(c-1)^2, \\ ey_3^2(-fy_4^2+ac^2) &= -a^2c(-y_4^2+c). \end{aligned} \tag{5.1}$$

This is birationally equivalent to the following genus 5 affine curve:

$$\begin{aligned} -ace(fX^2-ac)(b^2fX^2-acd) &= Y^2, \\ -ce(X^2-c)(fX^2-ac^2) &= Z^2. \end{aligned} \tag{5.2}$$

In summary, provided that $a, c, d, -e, -cef, af, cd, adf, -ae, cf$ are non-square in the ground field K and provided that the curve (5.2) has no K-rational points, then any point $\big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big)$ will satisfy that u_1 and y_1 are nonzero, so that our projective variety is the same as the affine variety in $U_2 = u_2/u_1, U_3 = u_3/u_1, U_4 = u_4/u_1$ and $Y_2 = y_2/y_1, Y_3 = y_3/y_1, Y_4 = y_4/y_1$, and furthermore there is a universal group law given by the first column of matrix $\big(A_{ij}\big)$ given in (4.21) together with the first column of $\big(J_{ij}\big)$ given in (4.23). This could happen over $\mathbf{Q}$ but, for a given curve, could not happen for arbitrarily large finite fields, since the above genus 5 curve would eventually acquire points over these. Of course, even if the above conditions are not satisfied, these matrices will always give a complete description of the group law; it is merely that one then requires different columns for certain additions, rather than having any particular column apply universally.

As a second attempt, consider the situation when $k_3 = 0$, which corresponds to $D \in \mathfrak{J}(K)$ which is either of the form $\{(x,y),(0,b\sqrt{acdeg(de-b^2f)})\}$ or is the identity. Provided that $acdeg(de-b^2f)$ is nonsquare in K, we see that D can only be defined over K if it is the identity element, and this is the only intersection between $k_3 = 0$ and our variety $\mathfrak{J}$. The condition $k_3 = 0$, after the linear change in coordinates (4.10),(4.11), corresponds to $adu_1 - b^2ceu_2 - deu_3 + b^2fu_4$, and so this will only be zero when D is the identity. For any $\big([u_1,u_2,u_3,u_4],[y_1,y_2,y_3,y_4]\big)$, we see that this linear combination of the u-coordinates will only be zero when D is the identity, and the same linear combination of the y-coordinates will only be zero when $D = -D_1$. If we take our group law to be the same linear combination of the columns of A together with the same linear combination of the columns of J then, for any given D, this will only be degenerate when $E = D$ or $E = D + D_1$. This condition can never give a universal group law, but it does reduce the exceptional cases to these two values of E, corresponding to the fact that the curve which geometrically describes such cases only has two K-rational points.

Third and successful attempt. We shall obtain a universal group law under conditions merely that certain expressions are squares and others are non-squares over our ground field K; this will be stated in Corollary 5.2 (a consequence of Theorem 5.1). In order to obtain the situation we desire in our third attempt, we first impose the conditions that a and cf are squares in K, and that c is nonsquare in K. We recall that D_2 is the point of order 4 which satisfies $2D_2 = E_2$; it is given explicitly in [Fly22], defined over $K(\sqrt{a},\sqrt{c})$, and it is the image (under the map induced by $y \mapsto \sqrt{a}\sqrt{c}\ y$) of a point defined over K. The first and third conditions force D_2 to be defined over the field $K(\sqrt{c})$, and conjugation has the effect of negating the y-coordinates, which forces conjugation to correspond to negation on D_2. The second condition forces the first quadratic factor of $\mathcal{C}$ in (4.8) to have K-rational roots, giving two Weierstrass points. The conditions that a and $cf = c(a+c-1)$ are squares in K can be parametrised as follows. We first

set $a = s^2$ and $cf = c(a + c - 1) = u^2$, and deduce $c(s^2 + c - 1) = u^2$; we then use $(s, u) = (1, c)$ as our basepoint and define the parameter $\omega = (u-c)/(s-1)$. Solving for s gives $s = (2c\omega - \omega^2 - c)/(-\omega^2 + c)$. Hence $a = \big((2c\omega - \omega^2 - c)/(-\omega^2 + c)\big)^2$, which gives that $cf = \delta^2$, where $\delta = c(\omega^2 - 2\omega + c)/(\omega^2 - c)$. We can now think of our family $\mathfrak{J} = \mathfrak{J}_{\omega,b,c}$ as being parametrised by $\omega, b, c \in K$. One of the K-rational Weierstrass points on $\mathcal{C}$ is then $(x_0, 0)$, where $x_0 = (\omega^2 + 2\omega b^2 c - 2\omega c + c)/(\omega^2 + c)$. Suppose that $D \in \mathfrak{J}(K)$ has the form $\{(x, y), (x_0, 0)\} + D_2$. Since the conjugation $\sigma : \sqrt{c} \mapsto -\sqrt{c}$ negates D_2 this would force $\{(x, y), (x, -y)^\sigma\} = E_2$, which we can hope to prevent, by imposing mild constraints on the parameters. After describing such D in terms of our embedding, we find that it corresponds (the details are in the file [Fly22]) to the condition $cu_1 - \delta u_3 = 0$. This motivates taking the intersection of $cu_1 - \delta u_3 = 0$ and our variety, hoping that there are arithmetic conditions on the parameters which prevent this intersection having a K-rational point. This approach turned out to be successful, as described in the following theorem, where the condition is merely that three expressions in the parameters are nonsquares in K, similar to the nonsquare-d condition for Edwards curves.

Theorem 5.1. *Let $\mathfrak{J} = \mathfrak{J}_{a,b,c}$ be as given in Theorem 4.2, defined over a field K, not of characteristic 2. Let d, e, f, g be as defined in (4.9). Let*

$$a = \Big(\frac{\omega^2 - 2\omega c + c}{\omega^2 - c}\Big)^2, \tag{5.3}$$

for some $\omega \in K$, so that we may think of $\mathfrak{J} = \mathfrak{J}_{\omega,b,c}$ now as a family in terms of the parameters $\omega, b, c \in K$. Then $cf = \delta^2$, where $\delta = c(\omega^2 - 2\omega + c)/(\omega^2 - c)$, and $a = \rho^2$, where $\rho = (\omega^2 - 2\omega c + c)/(\omega^2 - c)$.

Suppose that $c, cd, g(g - b^2(c-1))$ are nonsquares in K. Then $cu_1 - \delta u_3$ and $cy_1 - \delta y_3$ are nonzero for every $\big([u_1, u_2, u_3, u_4], [y_1, y_2, y_3, y_4]\big) \in \mathfrak{J}(K)$.

Proof. First note that, since c is nonsquare, the expression $\omega^2 - c$ is nonzero. The defining equations given in (4.26) include $y_2r_2 - y_1r_3 = 0$, $y_4r_4 - y_3r_5 = 0$ and $r_2y_3y_4 + r_5y_1y_2 = 0$. If we now take the sum of: $r_5^2y_1$ times the first of these, $-r_2^2y_4$ times the second of these, and $-r_2r_5$ times the third of these, we obtain

$$r_2^2r_4y_4^2 = -r_3r_5^2y_1^2. \tag{5.4}$$

Imagine that $u_1 - (\delta/c)u_3 = 0$. Substituting $u_1 = (\delta/c)u_3$ into the above factors, we find that

$$\begin{aligned} r_2 &= -bg\delta u_3\big(au_2 - \frac{\delta}{c}u_4\big), \\ r_3 &= -b^2\delta^2(\rho u_2 + u_4)(\rho u_2 - u_4), \\ r_4 &= b^2c\rho^2(\rho u_2 + u_4)(\rho u_2 - u_4), \\ r_5 &= bcg\rho^2u_3\big(\frac{\delta}{c}u_2 - u_4\big). \end{aligned} \tag{5.5}$$

We now see that the two sides of (5.4), if nonzero, have quotient c modulo squares. We are assuming that c is nonsquare in K, so it follows that both sides of (5.4) must be zero. The factors b, c, g, δ, ρ are all factors of the discriminant of $\mathcal{C}$, which we are assuming to be nonzero. It follows that one of the other factors of the left hand side must be zero, namely one of: $\rho u_2 - u_4$, $\rho u_2 + u_4$, u_3, y_4 or $au_2 - (\delta/c)u_4$ must be zero.

Consider the case $\rho u_2 - u_4 = 0$. If we substitute both $u_1 = (\delta/c)u_3$ and $u_2 = u_4/\rho$ into the defining equation $r_2^2 - r_1 r_3$, this gives $4b^2g^2cf\omega^2(c-1)^2u_3^2u_4^2/(\omega^2-c)^2 = 0$, so that either $u_3 = 0$ or $u_4 = 0$, which forces either $u_1 = u_3 = 0$ or $u_2 = u_4 = 0$. For the subcase when $u_1 = u_3 = 0$, then the defining equations $y_2r_1 - y_1r_2$ and $y_4r_5 - y_3r_6$ give nonzero constants times $u_4^2y_2$ and $u_4^2y_3$, respectively; but $u_4 \neq 0$ (since otherwise all u-coordinates would be zero), so that now $y_2 = y_3 = 0$; putting this into the defining equation $s_2^2 - s_1s_3$ gives the factors $y_4^2 - cy_1^2$ and $b^2\delta^2y_4^2 - cd\rho^2y_1^2$; the fact that c and cd are nonsquares then forces $y_1 = y_4 = 0$, so that all y-coordinates are zero, a contradiction. The subcase $u_2 = u_4 = 0$ gives the same contradiction, using the same defininings equations. We deduce that the case $\rho u_2 - u_4 = 0$ is impossible.

The case when $\rho u_2 + u_4 = 0$ is also incompatible with c and cd being nonsquares, using the same defining equations as the previous case.

The remaining cases u_3, y_4 and $au_2 - (\delta/c)u_4$ are shown to be nonzero in a similar style (it is the last of these which uses the condition that $g(g - b^2(c-1))$ is non-square); we have put the details in the file [Fly22].

So we now have, in all cases, a contradiction arising from our initial assumption that $u_1 - (\delta/c)u_3 = 0$. It follows that $cu_1 - \delta u_3$ is always nonzero, as required. Since $[y_1, y_2, y_3, y_4]$ are the u-coordinates of $D + D_1 \in \mathfrak{J}(K)$, it follows that $cy_1 - \delta y_3$ is also always nonzero. □

We observe here that, as long as the conditions of Theorem 5.1 are satisfied, we can treat the elements of $\mathfrak{J}(K)$ in terms of affine coordinates in $\mathbf{A}^3(K) \times \mathbf{A}^3(K)$. Specifically, we may represent any member of $\mathfrak{J}(K)$ by $\big((U_2, U_3, U_4), (Y_2, Y_3, Y_4)\big)$, where each $U_i = u_i/(cu_1 - \delta u_3)$ and each $Y_i = y_i/(cy_1 - \delta y_3)$.

The existence of a universally nonzero linear combination of coordinates now gives a universal group law, as follows.

Corollary 5.2. *Let $\mathfrak{J} = \mathfrak{J}_{\omega,b,c}$ satisfy the same conditions as in Theorem 5.1, namely that $c, cd, g(g-b^2(c-1))$ are nonsquares in K. Let A and J be the matrices defined in (4.21) and (4.23), respectively. Then*

$$\begin{aligned}\Big(&\big[cA_{11} - \delta A_{13}, cA_{21} - \delta A_{23}, cA_{31} - \delta A_{33}, cA_{41} - \delta A_{43}\big],\\ &\big[cJ_{11} - \delta J_{13}, cJ_{21} - \delta J_{23}, cJ_{31} - \delta J_{33}, cJ_{41} - \delta J_{43}\big]\Big),\end{aligned} \tag{5.6}$$

gives a universal group law on $\mathfrak{J}(K)$.

Proof. The equations in (5.6) are the linear combination: c times the first column minus δ times the third column, for the matrices A and J, respectively. The entries of the first array are just $l_i(D+E)\big(cl_1(D - E + D_1) - \delta l_3(D - E + D_1)\big)$, for $i \in \{1, 2, 3, 4\}$. Since $D - E + D_1 \in \mathfrak{J}(K)$, we know from Theorem 5.1 that $cl_1(D - E + D_1) - \delta l_3(D - E + D_1)$ is nonzero, and so the elements of this array are not all zero, and they gives the u-coordinates of $D + E$. Similarly the elements of the second array are not all zero, and they give the y-coordinates of $D + E$, as required. □

Satisfiability of the conditions on the parameters. We should also comment on the satisfiability of the condition that $c, cd, g(g-b^2(c-1))$ are nonsquares in K. A sufficient condition (which is equivalent for a finite field) is for d to be square, and for c and $g(g - b^2(c-1))$ to be nonsquares. The condition for d to be square

is: $b^2c - c + 1 = x^2$, for some x. Regarding this as a conic in b, x, we may use the basepoint $(b, x) = (1, 1)$, and define the parameter $t = (x-1)/(b-1)$. After solving for b, we can write $b = (t^2 + c - 2t)/(t^2 - c)$ in terms of our parameter t. At this stage, we can think of ω, t, c as our parameters, and we now only require that c and $g(g - b^2(c-1))$ are nonsquares in K. Note that $g(g - b^2(c-1))$ modulo squares is the same as the following polynomial in our parameters ω, t, c.

$$\begin{aligned}
&2(t^2w^2 + ct^2 - 4ctw + cw^2 + c^2)\\
&(ct^2w^2 + c^2t^2 + 4c^2tw + c^2w^2 - 4ct^2w - 4ctw^2\\
&+ t^2w^2 + c^3 - 4c^2t - 4c^2w + ct^2 + 4ctw + cw^2 + c^2)\\
&(2c^2t^4w^2 - 2ct^4w^3 + t^4w^4 - 4c^3t^2w^2 - 2c^2t^4w + 4c^2t^2w^3 - 2t^3w^4\\
&+ 2c^4w^2 + 4c^3t^2w - 2c^3w^3 + c^2t^4 - 4c^2t^2w^2 + c^2w^4 + 4ct^3w^2\\
&- 2ctw^4 + 2t^2w^4 - 2c^4w - 2c^2t^3 + 4c^2tw^2 - 4ct^2w^2 + c^4 - 2c^3t + 2c^2t^2).
\end{aligned} \tag{5.7}$$

This has discriminant (with respect to t):

$$\begin{aligned}
&2^{40}c^{28}(c-1)^{20}(2cw^2 - 2cw - w^2 + c)^2(2c^2 - 2cw + w^2 - c)^2\\
&(2cw - w^2 - c)^{24}(-w^2 + c)^{24}(w^2 + c - 2w)^4,
\end{aligned} \tag{5.8}$$

and the coefficient of the highest power of t is:

$$2(w^2 + c)(cw^2 + c^2 - 4cw + w^2 + c)(2c^2w^2 - 2cw^3 + w^4 - 2c^2w + c^2). \tag{5.9}$$

Assuming that our field K contains nonsquares, take c to be any fixed nonsquare in K. Now let w be any member of K for which (5.8) and (5.9) are nonzero, which means avoiding at most 16 values in K, since automatically $-w^2 + c$ is nonzero. Let $\phi(t)$ denote the polynomial in t obtained by substituting these values of c, w into (5.7). This will be a degree 8 polynomial in t with no repeated roots, and our only remaining requirement is to choose values for t such that $\phi(t)$ is nonsquare in K (as well as avoiding any values of t for which the disciminant of our original curve is zero).

It is now clear that there are plentiful examples of our conditions being satisfied when K is a number field or a finite field of sufficiently large order. The curve $y^2 = \phi(t)$ is of genus 3 over K. For example, when K is a number field, by Faltings' Theorem [Fal83] this curve has only finitely many points, and so we need only avoid finitely many values of t. When $K = \mathbf{F}_q$ is a finite field with q elements, the Hasse-Weil bounds (see Chapter 3 of [Mor91]) tells us that the number of points over K on the curve $y^2 = \phi(t)$ is in the range from $q + 1 - 2g\sqrt{q}$ to $q + 1 + 2g\sqrt{q}$, where here $g = 3$ is the genus of this curve; hence roughly half of the values of $t \in K$ will give nonsquare values for $\phi(t)$. It follows from the above discussion that there will be examples in arbitrarily large finite fields for which the conditions are satisfied. As an explicit example, let $K = \mathbf{F}_{1201}$. Then the conditions are satisfied for $\omega = 6, b = 7, c = 11$, since then $c = 11, cd = 1015$ and $g(g - b^2(c-1)) = 202$ are all nonsquares in $\mathbf{F}_{1201}$.

Data Availability. Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Auxiliary Files. The supplementary information file [Fly22] includes details of the calculations performed using the computer algebra software Maple. The file is available from the website of the first-named author, as described in the references, and is also available as an ancillary file from `arxiv:2211.01450`. There is also a shortened version of this file [Fly23] which gives only the assignments of the main objects (such as the diagonalising change in basis, the defining equations and the group law), which can be used in any algebra package.

Conflict of Interest. The authors certify that there is no actual or potential conflict of interest in relation to this article.

References

[AC12] Christophe Arène and Romain Cosset, *Construction of a $\Bbbk$-complete addition law on Jacobians of hyperelliptic curves of genus two*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 574, Amer. Math. Soc., Providence, RI, 2012, pp. 1–14.

[AKR12] Christophe Arene, David Kohel, and Christophe Ritzenthaler, *Complete addition laws on abelian varieties*, LMS J. Comput. Math. **15** (2012), 308–316.

[BBJ+08] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters, *Twisted Edwards curves*, Progress in cryptology—AFRICACRYPT 2008, Lecture Notes in Comput. Sci., vol. 5023, Springer, Berlin, 2008, pp. 389–405.

[BL04] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, second ed., Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004.

[BL07] Daniel J. Bernstein and Tanja Lange, *Faster addition and doubling on elliptic curves*, Advances in cryptology—ASIACRYPT 2007, Lecture Notes in Comput. Sci., vol. 4833, Springer, Berlin, 2007, pp. 29–50.

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996.

[Edw07] Harold M. Edwards, *A normal form for elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), no. 3, 393–422.

[Fal83] Gerd Faltings, *Endlichkeitssätze für abelsche Varie"aten über Zahlkörpern*. Invent. Math. **73** (1983), no. 3, 349–366.

[Fly95] E. V. Flynn, *An explicit theory of heights*, Trans. Amer. Math. Soc. **347** (1995), no. 8, 3003–3015.

[Fly22] E. V. Flynn, *Maple file*, `https://people.maths.ox.ac.uk/flynn/genus2/maplefile` also available as an ancillary file for the arxiv preprint `arxiv:2211.01450`

[Fly23] E. V. Flynn, *Short file*, `https://people.maths.ox.ac.uk/flynn/genus2/shortfile` also available as an ancillary file for the arxiv preprint `arxiv:2211.01450`

[Kem88] George R. Kempf, *Multiplication over abelian varieties*, Amer. J. Math. **110** (1988), no. 4, 765–773.

[Kem89a] George R. Kempf, *Linear systems on abelian varieties*, Amer. J. Math. **111** (1989), no. 1, 65–94.

[Kem89b] George R. Kempf, *Projective coordinate rings of abelian varieties*, Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988), Johns Hopkins Univ. Press, Baltimore, MD, 1989, pp. 225–235.

[Kem91] George R. Kempf, *Complex abelian varieties and theta functions*, Universitext, Springer-Verlag, Berlin, 1991.

[LR16] David Lubicz and Damien Robert, *Arithmetic on abelian and Kummer varieties*, Finite Fields Appl. **39** (2016), 130–158.

[Mor91] Carlos Moreno, *Algebraic curves over finite fields*, Cambridge tracts in mathematics, vol. 97, Cambridge University Press, Cambridge, 1991.

[Mum66] D. Mumford, *On the equations defining abelian varieties. I*, Invent. Math. **1** (1966), 287–354.

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay by Oxford University Press, London, 1970.

[Mum83] David Mumford, *Tata lectures on theta. I*, Progress in Mathematics, vol. 28, Birkhäuser Boston, Inc., Boston, MA, 1983, With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman.

[Mum91] David Mumford, *Tata lectures on theta. III*, Progress in Mathematics, vol. 97, Birkhäuser Boston, Inc., Boston, MA, 1991, With the collaboration of Madhav Nori and Peter Norman.

[PSM21] Giuseppe Pareschi and Riccardo Salvati Manni, *2-torsion points on theta divisors*, Int. Math. Res. Not. IMRN (2021), no. 19, 14616–14628.

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

Mathematical Institute, University of Oxford, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, United Kingdom
E-mail address: flynn@maths.ox.ac.uk

Mathematics Department, American University of Beirut, Bliss Street, Beirut, Lebanon
E-mail address: kmakdisi@aub.edu.lb