TWO-COVERINGS OF JACOBIANS OF CURVES OF GENUS TWO

E. VICTOR FLYNN, DAMIANO TESTA, AND RONALD VAN LUIJK

Abstract. Given a curve C of genus 2 defined over a field k of characteristic different from 2, with Jacobian variety J, we show that the two-coverings corresponding to elements of a large subgroup of $\mathrm{H}^1\big(\mathrm{Gal}(k^{\mathrm{s}}/k), J[2](k^{\mathrm{s}})\big)$ (containing the Selmer group when k is a global field) can be embedded as intersection of 72 quadrics in $\mathbb{P}^{15}_k$, just as the Jacobian J itself. Moreover, we actually give explicit equations for the models of these twists in the generic case, extending the work of Gordon and Grant which applied only to the case when all Weierstrass points are rational. In addition, we describe elegant equations on the Jacobian itself, and answer a question of Cassels and the first author concerning a map from the Kummer surface in $\mathbb{P}^3$ to the desingularized Kummer surface in $\mathbb{P}^5$.

1. Introduction

The number of rational points on a curve of geometric genus at least two defined over a number field is finite by Faltings' Theorem [7] . However, for any fixed number field k, it is not known whether there exists an algorithm that takes such a curve C/k as input and computes the set $C(k)$ of all its rational points. There are advanced techniques that often work in practice, such as the Chabauty-Coleman method [5] and the Mordell-Weil sieve (see [2, 11, 21]). Bjorn Poonen [18] has shown, subject to two natural heuristic assumptions, that with probability 1 the latter method is indeed capable of determining whether or not a given curve of genus at least 2 over a number field contains a rational point; this assumes the existence of a Galois-invariant divisor of degree 1 on the curve.

Both methods assume the knowledge of the finitely generated Mordell-Weil group $J(k)$ of the Jacobian J of the curve C over the number field k, or at least of a subgroup of finite index; in particular it assumes the knowledge of the rank of the group $J(k)$, which in general is hard to find, but can be bounded by a so-called two-descent.

Let k be any field with separable closure k^{s} and let C be a smooth projective curve over k with Jacobian J. Taking Galois invariants of the short exact sequence

$$0 \longrightarrow J[2](k^{\mathrm{s}}) \longrightarrow J(k^{\mathrm{s}}) \xrightarrow{[2]} J(k^{\mathrm{s}}) \longrightarrow 0$$

associated to multiplication by 2 gives a long exact sequence of which the first connecting map induces an injective homomorphism

$$\iota\colon\ J(k)/2J(k) \to \mathrm{H}^1\big(\mathrm{Gal}(k^{\mathrm{s}}/k), J[2](k^{\mathrm{s}})\big).$$

If $J(k)$ is finitely generated and its torsion subgroup is known, then the rank of $J(k)$ is easy to read off from the size of $J(k)/2J(k)$, and thus from its image under ι. A two-descent consists of bounding this image. When k is a global field, the image of ι is contained in the so-called Selmer group, which is finite and computable (see [3, 19, 20]).

We restrict our attention to the case that C has genus 2 and the characteristic of k is not equal to 2. The elements of $\mathrm{H}^1\big(\mathrm{Gal}(k^{\mathrm{s}}/k), J[2](k^{\mathrm{s}})\big)$ can be represented by two-coverings of J, which are twists of the multiplication-by-2 map as defined in the next section. The elements in the image of ι correspond to those two-coverings that have a k-rational point. When k is a global field, the elements of the Selmer group correspond to those two-coverings that are locally solvable everywhere.

Date: May 7, 2009.

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

Key words and phrases. Coverings, Jacobians, Homogeneous spaces.

The main goal of this paper is to show that the two-coverings corresponding to elements of a large subgroup of $\mathrm{H}^1\big(\mathrm{Gal}(k^s/k), J[2](k^s)\big)$ (containing the Selmer group when k is a global field) can be embedded as intersection of 72 quadrics in $\mathbb{P}^{15}_k$, just as the Jacobian itself. Moreover, we investigate various representations of $J[2](k^s)$ and certain extensions, in order to actually give explicit equations for the models of these twists, cf. Theorem 7.4. A better understanding of these representations has allowed us to find simple and symmetric equations also for the Jacobian. We work over a generic field k, where all coefficients in the equation $y^2 = f(x)$ for C are independent transcendentals, as well as the coefficients of the element in $k[X]/f$ that determines the twist of J. This field is far to big to find the equations of the twist by brute force.

These models are useful in practice to find rational points on the twists, and thus to decide whether a given two-covering corresponds to an element in the image of ι. As a further application, we expect that our explicit models will prove useful in the study of heights on Jacobians. We also answer a question by Cassels and the first author [4, Section 16.6] in Remark 3.8.

The explicit equations we shall give for nontrivial two-coverings corresponding to elements of the Selmer group generalize to any curve of genus 2 those given by Gordon and Grant in [12] for the special case where all Weierstrass points are rational.

In Section 2 we set up the necessary cohomological sequences, give a description of the large subgroup of $\mathrm{H}^1\big(\mathrm{Gal}(k^s/k), J[2](k^s)\big)$ that was mentioned (see Corollary 2.9), define two-coverings, Selmer groups, and prove some known results about two-coverings for completeness. In Section 3 we find models of the Jacobian J in $\mathbb{P}^{15}$, its Kummer surface $\mathcal{X}$ in $\mathbb{P}^9$, and the minimal desingularization $\mathcal{Y}$ of $\mathcal{X}$ in $\mathbb{P}^5$ on which for every $P \in J[2]$, the action of translation by P is just given by negating some of the coordinates. Another description of the desingularized Kummer surface is given in Section 4. This is used in Section 5 to understand how the linear action of $J[2](k^s)$ on the model of J in $\mathbb{P}^{15}$ can be obtained from the action on $\mathcal{X} \subset \mathbb{P}^3$ and $\mathcal{Y} \subset \mathbb{P}^5$. In Section 6 we first show theoretically how the action of $J[2](k^s)$ on $J \subset \mathbb{P}^{15}$ can be diagonalized and then also do so explicitly. In Section 7 we describe how to use the models and this diagonalized action to obtain the desired twists.

The authors thank Nils Bruin, Alexei Skorobogatov and Michael Stoll for useful discussions and remarks. The first two authors thank EPSRC for support through grant number EP/F060661/1. The first and third author thank the International Center for Transdisciplinary Studies at Jacobs University Bremen for support and hospitality. The second author thanks Jacobs University Bremen and was partially funded by DFG grant STO-299/4-1. The third author thanks the University of British Columbia, Simon Fraser University, PIMS, and Warwick University.

2. Set-up

Let k be a field of characteristic not equal to two, k^s a separable closure of k, and $f = \sum_{i=0}^{6} f_i X^i \in k[X]$ a separable polynomial with $f_6 \neq 0$. Denote by Ω the set of the six roots of f in k^s, so that $k(\Omega)$ is the splitting field of f over k in k^s. Let C be the smooth projective curve of genus 2 over k associated to the affine curve in $\mathbb{A}^2_{x,y}$ given by $y^2 = f(x)$. Let J denote the Jacobian of C and $J[2]$ its two-torsion subgroup. We denote the multiplication-by-2 map on J by [2]. All two-torsion points are defined over $k(\Omega)$, i.e., $J[2](k(\Omega)) = J[2](k^s)$. Let $W \subset C$ be the set of Weierstrass points of C, corresponding to the set $\{(\omega, 0) \ : \ \omega \in \Omega\}$ of points on the affine curve. Choose a canonical divisor K_C of C. For any $w \in W$, the divisor $2(w)$ is linearly equivalent to K_C and $\sum_{w \in W}(w)$ is linearly equivalent to $3K_C$.

There is a morphism $C \times C \to J$ sending (P, Q) to the divisor class $(P) + (Q) - K_C$, which factors through the symmetric square $C^{(2)}$. The induced map $C^{(2)} \to J$ is birational and each nonzero element of $J[2](k^s)$ is represented by $(w_1) - (w_2) \sim (w_2) - (w_1) \sim (w_1) + (w_2) - K_C$ for a unique unordered pair $\{w_1, w_2\}$ of distinct Weierstrass points. This yields a Galois equivariant bijection between nonzero two-torsion points and unordered pairs of distinct elements in Ω.

Set $L = k[X]/f$ and $L^s = L \otimes_k k^s$. By abuse of notation we denote the image of X in L and L^s by X as well. For any $\omega \in \Omega$, let φ_ω denote the k^s-linear map $L^s \to k^s$ that sends X to ω. By the Chinese Remainder Theorem, the induced map $\varphi = \bigoplus_{\omega \in \Omega} \varphi_\omega \colon L^s \to \bigoplus_{\omega \in \Omega} k^s$ is an isomorphism

of k^{s}-algebras that sends X to $(\omega)_\omega$. The induced Galois action on $\bigoplus_\omega k^{\mathrm{s}}$ is given by

$$\sigma\big((c_\omega)_\omega\big) = \big(\sigma(c_{\sigma^{-1}(\omega)})\big)_\omega$$

for all $\sigma \in \mathrm{Gal}(k^{\mathrm{s}}/k)$. For any commutative ring R we write $\mu_2(R)$ for the kernel of the homomorphism $R^* \to R^*$ that sends x to x^2. We sometimes abbreviate $\mu_2(k^{\mathrm{s}}) = \mu_2(k)$ to μ_2. The isomorphism φ induces an isomorphism of groups $\mu_2(L^{\mathrm{s}}) \to \bigoplus_{\omega\in\Omega} \mu_2(k^{\mathrm{s}})$.

The norm map $N_{L/k}$ from L to k, sending $\alpha \in L^{\mathrm{s}}$ to $\prod_\omega \varphi_\omega(\alpha)$, induces homomorphisms from $\mu_2(L^{\mathrm{s}})$ and $\mu_2(L^{\mathrm{s}})/\mu_2(k^{\mathrm{s}})$ to $\mu_2(k^{\mathrm{s}})$, both of which we denote by N and refer to as norms. The kernel M of N on $\mu_2(L^{\mathrm{s}})$ is generated by elements $\alpha_{\omega_1,\omega_2}$ defined by $\varphi_\omega(\alpha_{\omega_1,\omega_2}) = -1$ if and only if $\omega \in \{\omega_1, \omega_2\}$. Let $\beta\colon M \to J[2](k^{\mathrm{s}})$ be the homomorphism that maps $\alpha_{\omega_1,\omega_2}$ to the difference of Weierstrass points $\big((\omega_1, 0)\big) - \big((\omega_2, 0)\big)$. Finally, let $\epsilon\colon J[2](k^{\mathrm{s}}) \to \mu_2(L^{\mathrm{s}})/\mu_2(k^{\mathrm{s}})$ be the homomorphism that sends $\big((\omega_1, 0)\big) - \big((\omega_2, 0)\big)$ to the class of $\alpha_{\omega_1,\omega_2}$. We get the following diagram of short exact sequences. For more details, see [19, Sections 6 and 7].

(1)

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \mu_2(k^{\mathrm{s}}) & = & \mu_2(k^{\mathrm{s}}) & & & & \\
 & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & M & \longrightarrow & \mu_2(L^{\mathrm{s}}) & \xrightarrow{N} & \mu_2(k^{\mathrm{s}}) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle\beta} & & \downarrow & & \| & & \\
1 & \longrightarrow & J[2](k^{\mathrm{s}}) & \xrightarrow{\epsilon} & \frac{\mu_2(L^{\mathrm{s}})}{\mu_2(k^{\mathrm{s}})} & \xrightarrow{N} & \mu_2(k^{\mathrm{s}}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & & &
\end{array}$$

There are natural isomorphisms

$$\mathrm{Hom}\left(\mu_2(L^{\mathrm{s}}), \mu_2\right) \cong \mathrm{Hom}\left(\bigoplus_\omega \mu_2, \mu_2\right) \cong \bigoplus_\omega \mathrm{Hom}(\mu_2, \mu_2) \cong \bigoplus_\omega \mu_2 \cong \mu_2(L^{\mathrm{s}}),$$

so $\mu_2(L^{\mathrm{s}})$ is self-dual. The corresponding perfect pairing $\mu_2(L^{\mathrm{s}}) \times \mu_2(L^{\mathrm{s}}) \to \mu_2$ sends (α_1, α_2) to $(-1)^r$ with $r = \#\{\omega \in \Omega : \varphi_\omega(\alpha_1) = \varphi_\omega(\alpha_2) = -1\}$. The pairing induces a perfect pairing on $M \times \mu_2(L^{\mathrm{s}})/\mu_2$ and on $J[2](k^{\mathrm{s}}) \times J[2](k^{\mathrm{s}})$, where it coincides with the Weil pairing, which we denote by e_W. We conclude that M and $\mu_2(L^{\mathrm{s}})/\mu_2$ are each other's duals, that $J[2](k^{\mathrm{s}})$ is self-dual, and that the entire Diagram (1) is self-dual under reflection in the obvious diagonal. The element $-1 \in M$ corresponds to the character of $\mu_2(L^{\mathrm{s}})/\mu_2$ that is the norm map $N\colon \mu_2(L^{\mathrm{s}})/\mu_2 \to \mu_2$.

We define the Brauer group $\mathrm{Br}(k)$ of k as $\mathrm{H}^2(\mathrm{Gal}(k^{\mathrm{s}}/k), (k^{\mathrm{s}})^*)$. We only use its two-torsion subgroup $\mathrm{Br}(k)[2]$, which is isomorphic to $\mathrm{H}^2(\mathrm{Gal}(k^{\mathrm{s}}/k), \mu_2(k^{\mathrm{s}}))$. Recall that there are natural isomorphisms $\mathrm{H}^1(\mathrm{Gal}(k^{\mathrm{s}}/k), \mu_2(k^{\mathrm{s}})) \cong k^*/(k^*)^2$ and $\mathrm{H}^1(\mathrm{Gal}(k^{\mathrm{s}}/k), \mu_2(L^{\mathrm{s}})) \cong L^*/(L^*)^2$. Taking long exact sequences of Galois cohomology, we find the following commutative diagram (cf. [19,

Section 8]).

(2)

$$\begin{array}{ccccccccc}
 & & & & k^*/(k^*)^2 & = & k^*/(k^*)^2 & & \\
 & & & & \downarrow & & \downarrow & & \\
\mu_2(L) & \xrightarrow{N} & \mu_2(k) & \longrightarrow & \mathrm{H}^1(M) & \longrightarrow & L^*/(L^*)^2 & \xrightarrow{N} & k^*/(k^*)^2 \\
\downarrow & & \| & & \downarrow{\scriptstyle \beta_*} & & \downarrow & & \| \\
\mathrm{H}^0\left(\frac{\mu_2(L^{\mathrm{s}})}{\mu_2(k^{\mathrm{s}})}\right) & \xrightarrow{N} & \mu_2(k) & \longrightarrow & \mathrm{H}^1(J[2](k^{\mathrm{s}})) & \xrightarrow{\epsilon_*} & \mathrm{H}^1\left(\frac{\mu_2(L^{\mathrm{s}})}{\mu_2(k^{\mathrm{s}})}\right) & \xrightarrow{N_*} & k^*/(k^*)^2 \\
 & & & & \Upsilon\downarrow & & \downarrow & & \\
 & & & & \mathrm{Br}(k)[2] & = & \mathrm{Br}(k)[2] & &
\end{array}$$

Here and from now on, $\mathrm{H}^1(*)$ stands for the Galois cohomological group $\mathrm{H}^1(\mathrm{Gal}(k^{\mathrm{s}}/k), *)$. We often abbreviate $\mathrm{H}^1(J[2](k^{\mathrm{s}}))$ further to $\mathrm{H}^1(J[2])$. Let Υ denote the connecting homomorphism $\Upsilon\colon \mathrm{H}^1(J[2]) \to \mathrm{Br}(k)[2]$ (see Diagram (2)).

Definition 2.1. *A global field is a finite extension of $\mathbb{Q}$ or a finite extension of $\mathbb{F}_p(t)$ for some prime p. A local field is the completion of a global field at some place.*

Proposition 2.2. *Assume that k is a global field or a local field. Then the composition of the map $\iota\colon J(k)/2J(k) \to \mathrm{H}^1(J[2])$ with the map Υ is zero.*

Proof. As in [19, Section 3], we let the period of a curve D over a field K be the greatest common divisor of the degrees of all K-rational divisor classes of D. If k is a local field, then since the genus g of C equals 2, by [19, Proposition 3.4], the period of C divides $g-1=1$, so it equals 1, and by [19, Proposition 3.2], this implies that the natural inclusion $\mathrm{Pic}^0 C \to \mathrm{H}^0(\mathrm{Pic}^0 C_{k^{\mathrm{s}}}) = J(k)$ is an isomorphism. If k is a global field, then by the local argument, the period of C over any completion equals 1, and by [19, Proposition 3.3], this implies again that the inclusion $\mathrm{Pic}^0 C \to J(k)$ is an isomorphism (see also last paragraph of [19, Section 4]). We conclude that in either case the inclusion $\rho\colon \mathrm{Pic}^0 C \to J(k)$ is an isomorphism. Let $\mathrm{Pic}^{(2)} C$ denote the subgroup of divisor classes of even degree in $\mathrm{Pic}\, C$. By [19, Section 9], there is a homomorphism $\tau\colon \mathrm{Pic}^{(2)} C \to \mathrm{H}^1(J[2])$ whose image is contained in the kernel of Υ (see [19, Corollary 9.5]), and such that the restriction of τ to $\mathrm{Pic}^0 C$ factors as the composition of the map $\overline{\rho}\colon \mathrm{Pic}^0 C \to J(k)/2J(k)$ induced by ρ and the map ι. Since $\overline{\rho}$ is surjective, we conclude that the image of ι is indeed contained in the kernel of Υ. □

We denote the kernel of Υ by $P^1(J[2])$.

Remark 2.3. *Suppose k is a global field. For each place v of k we let k_v denote the completion of k at v and*

$$\iota_v\colon J(k_v)/2J(k_v) \to \mathrm{H}^1\big(\mathrm{Gal}(k_v^{\mathrm{s}}/k_v, J[2](k_v^{\mathrm{s}}))\big)$$

the connecting map defined analogously to $\iota\colon J(k)/2J(k) \to \mathrm{H}^1(J[2])$. We get a natural diagram

$$\begin{array}{ccccc}
J(k)/2J(k) & \xrightarrow{\iota} & \mathrm{H}^1(k, J[2](k^{\mathrm{s}})) & \longrightarrow & \mathrm{H}^1(k, J(k^{\mathrm{s}})) \\
\downarrow & & \downarrow & \searrow & \downarrow \\
\prod_v J(k_v)/2J(k_v) & \xrightarrow{(\iota_v)_v} & \prod_v \mathrm{H}^1(k_v, J[2](k_v^{\mathrm{s}})) & \longrightarrow & \prod_v \mathrm{H}^1(k_v, J(k_v^{\mathrm{s}}))
\end{array}$$

and define the Selmer group $\mathrm{Sel}^2(J,k)$ to be the kernel of $\mathrm{H}^1(k, J[2](k^{\mathrm{s}})) \to \prod_v \mathrm{H}^1(k_v, J(k_v^{\mathrm{s}}))$, i.e., the inverse image under the middle vertical map of the image of the lower-left horizontal map. Then the image of ι is contained in $\mathrm{Sel}^2(J,k)$. It follows from Proposition 2.2, applied to all k_v, and the fact that the natural diagonal map $\mathrm{Br}\, k \to \prod_v \mathrm{Br}\, k_v$ is injective, that the Selmer group $\mathrm{Sel}^2(J,k)$ is contained in $P^1(J[2])$.

By Diagram (2), the kernel of the homomorphism $\mathrm{H}^1\big(\mu_2(L^{\mathrm{s}})/\mu_2(k^{\mathrm{s}})\big) \to \mathrm{Br}(k)[2]$ is isomorphic to the image of L^*/L^{*2} in $\mathrm{H}^1\big(\mu_2(L^{\mathrm{s}})/\mu_2(k^{\mathrm{s}})\big)$ and this image is isomorphic to $L^*/L^{*2}k^*$. This implies that ϵ_* induces a homomorphism $\kappa\colon P^1(J[2]) \to L^*/L^{*2}k^*$. By Proposition 2.2, we may compose κ and ι.

Definition 2.4. *The composition $\kappa \circ \iota\colon J(k)/2J(k) \to L^*/L^{*2}k^*$ is called the Cassels map.*

Proposition 2.5. *The Cassels map $J(k)/2J(k) \to L^*/L^{*2}k^*$ sends the class of the divisor $\big((x_1, y_1)\big) + \big((x_2, y_2)\big) - K_C$ on C to $(X - x_1)(X - x_2)$.*

Proof. See [8, Proposition 2] and [19, Sections 5 and 9]. □

The kernel of the homomorphism ϵ_* appearing in Diagram (2) equals the image of $\mu_2(k)$ in $\mathrm{H}^1(J[2])$ and thus has order 1 or 2. As this image of $\mu_2(k)$ is contained in the image of β_* (see Diagram (2)), it is contained in $P^1(J[2])$, so we have $\ker\epsilon_* = \ker\kappa$. The image of $-1 \in \mu_2(k)$ in $\mathrm{H}^1(J[2])$ is represented by any cocycle that sends σ to $(\sigma(w_0)) - (w_0)$ for some fixed $w_0 \in W$, see [19, Lemma 9.1]. There is a simple condition based on how the polynomial f factors that says whether or not this cocycle represents the trivial class [19, Lemma 11.2] and thus whether or not $\ker\kappa$ is trivial. More subtle is the Cassels kernel, which is defined as the intersection $\ker\kappa \cap \mathrm{Sel}^2(J, k)$, cf. Remark 2.3. The Cassels kernel measures the difference between the Selmer group $\mathrm{Sel}^2(J, k)$ and its image under κ, which is known as the *fake Selmer group*. Michael Stoll [28, Section 5] gives conditions that tell whether or not the Cassels kernel is trivial. Whether or not the kernel of the Cassels map, which injects through ι into the Cassels kernel, is trivial is a question that is more subtle yet again, cf. [4, Lemmas 6.4.1 and 6.5.1].

We would like to get a better understanding of the elements of $\mathrm{Sel}^2(J, k)$ and look more generally at the elements of $P^1(J[2])$. To give a more concrete description of $P^1(J[2])$, we first give a description of $\mathrm{H}^1(M)$, which maps onto $P^1(J[2])$. Let Γ denote the subgroup of $L^* \times k^*$ consisting of all pairs (δ, n) satisfying $N_{L/k}(\delta) = n^2$, and let $\chi\colon L^* \to \Gamma$ be the homomorphism that sends ε to $(\varepsilon^2, N(\varepsilon))$.

Proposition 2.6. *There is a unique isomorphism $\gamma\colon \Gamma/\operatorname{im}(\chi) \to \mathrm{H}^1(M)$ that sends the class of (δ, n) to the class of the cocycle $\sigma \mapsto \sigma(\varepsilon)/\varepsilon$, where $\varepsilon \in L^{\mathrm{s}}$ is any element satisfying $\varepsilon^2 = \delta$ and $N(\varepsilon) = n$. The composition of γ with the map $\mathrm{H}^1(M) \to L^*/(L^*)^2$ sends (δ, n) to δ. The kernel $\ker\epsilon_* = \ker\kappa$ is generated by the image of $(1, -1) \in \Gamma/\operatorname{im}(\chi)$ under the composition of γ with the map $\beta_*\colon \mathrm{H}^1(M) \to \mathrm{H}^1(J[2])$.*

Proof. Let Γ^{s} denote the subgroup of $L^{\mathrm{s}*} \times k^{\mathrm{s}*}$ consisting of all pairs (δ, n) satisfying $N_{L/k}(\delta) = n^2$ and extend χ to a map from $L^{\mathrm{s}*}$ to Γ^{s} by $\chi(\varepsilon) = (\varepsilon^2, N(\varepsilon))$. Then χ is surjective and its kernel is M. Let p denote the projection map $p\colon \Gamma^{\mathrm{s}} \to L^{\mathrm{s}*}$. Taking Galois invariants in the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & M & \longrightarrow & L^{\mathrm{s}*} & \xrightarrow{\chi} & \Gamma^{\mathrm{s}} & \longrightarrow & 1 \\
 & & \downarrow & & \| & & \downarrow{\scriptstyle p} & & \\
1 & \longrightarrow & \mu_2(L^{\mathrm{s}}) & \longrightarrow & L^{\mathrm{s}*} & \xrightarrow{x\mapsto x^2} & L^{\mathrm{s}*} & \longrightarrow & 1
\end{array}$$

we obtain the following diagram.

$$\begin{array}{ccccccc}
L^* & \xrightarrow{\chi} & \Gamma & \xrightarrow{d} & \mathrm{H}^1(M) & \longrightarrow & \mathrm{H}^1(L^{\mathrm{s}*}) \\
\| & & \downarrow{\scriptstyle p} & & \downarrow & & \\
L^* & \xrightarrow{x\mapsto x^2} & L^* & \longrightarrow & \mathrm{H}^1(\mu_2(L^{\mathrm{s}})) & \longrightarrow & \mathrm{H}^1(L^{\mathrm{s}*})
\end{array}$$

Let $d\colon \Gamma \to \mathrm{H}^1(M)$ be the connecting homomorphism in this diagram. It sends (δ, n) to the class represented by the cocycle $\sigma \mapsto \sigma(\varepsilon)/\varepsilon$ for any fixed $\varepsilon \in L^{\mathrm{s}*}$ with $\chi(\varepsilon) = (\delta, n)$, i.e., with $\varepsilon^2 = \delta$ and $N(\varepsilon) = n$. By a generalization of Hilbert's Theorem 90 we have $\mathrm{H}^1(L^{\mathrm{s}*}) = 1$ (see [24, Exercise X.1.2]). We conclude that d is surjective and therefore induces an isomorphism

$\gamma\colon \Gamma/\operatorname{im}\chi \to \mathrm{H}^1(M)$. We also recover the isomorphism $\mathrm{H}^1(\mu_2(L^{\mathrm{s}})) \cong L^*/(L^*)^2$ that was used to get Diagram (2). From the commutativity of the diagram we conclude that the composition

$$\Gamma/\operatorname{im}\chi \to \mathrm{H}^1(M) \to \mathrm{H}^1(\mu_2(L^{\mathrm{s}*})) \to L^*/(L^*)^2$$

is induced by p, i.e., it is given by sending (δ, n) to δ. Chasing the arrows in the last diagram (all that is needed is the surjectivity of d and the left-most vertical map), we find that d maps the kernel of p surjectively to the kernel of the map $\mathrm{H}^1(M) \to \mathrm{H}^1(\mu_2(L^{\mathrm{s}*})) \cong L^*/L^{*2}$, which maps surjectively to $\ker\epsilon_* = \ker\kappa$ by Diagram (2). The last statement of the proposition now follows from the fact that the kernel of p is generated by $(1,-1)$. □

Remark 2.7. *Note that for each $(\delta, n) \in \Gamma$ we can find an $\varepsilon \in L^{\mathrm{s}}$ as in Proposition 2.6 as follows. For each $\omega \in \Omega$, choose an $\varepsilon_\omega \in k^{\mathrm{s}}$ with $\varepsilon_\omega^2 = \varphi_\omega(\delta)$. Then the element*

$$\varepsilon = \big(\varepsilon_\omega\big)_{\omega\in\Omega} \in \bigoplus_{\omega\in\Omega} k^{\mathrm{s}} \cong L^{\mathrm{s}}$$

satisfies $\varepsilon^2 = \delta$ and $N(\varepsilon) = \prod_\omega \varepsilon_\omega = \pm n$. By changing the sign of one of the ε_ω if necessary, we obtain $N(\varepsilon) = n$. The cocycle in Proposition 2.6 can then also be written as

$$\sigma \mapsto \left(\frac{\sigma\big(\varepsilon_{\sigma^{-1}(\omega)}\big)}{\varepsilon_\omega}\right)_{\omega\in\Omega} \in M \subset \bigoplus_{\omega\in\Omega} \mu_2(k^{\mathrm{s}}).$$

Note also that by changing the sign of an even number of the ε_ω, we change ε by an element of M, so we change the cocycle by a coboundary.

Remark 2.8. *By* [19, Section 6]*, the group M is isomorphic to the two-torsion subgroup $J_{\mathfrak{m}}[2]$ of the so-called generalized Jacobian $J_{\mathfrak{m}}$. In the general setting and notation of* [19] *it is possible to prove as in the proof of Proposition 2.6 that $\mathrm{H}^1(J_{\mathfrak{m}}[\phi])$ is isomorphic to $\Gamma_p/\chi_p(L^*)$, where $\Gamma_p \subset L^* \times k^*$ consists of all pairs (δ, n) with $N(\delta) = n^p$ and $\chi_p\colon L^* \to \Gamma_p$ sends ε to $(\varepsilon^p, N(\varepsilon))$.*

The following corollary provides the description of the group $P^1(J[2])$ that we shall use in Section 4.

Corollary 2.9. *The composition of $\gamma\colon \Gamma/\operatorname{im}(\chi) \to \mathrm{H}^1(M)$ of Proposition 2.6 with the map $\beta_*\colon \mathrm{H}^1(M) \to \mathrm{H}^1(J[2])$ of Diagram 2 induces an isomorphism $\Gamma/(k^* \cdot \operatorname{im}(\chi)) \to P^1(J[2])$.*

Proof. The kernel $P^1(J[2])$ of Υ is isomorphic to the image of $\mathrm{H}^1(M)$ in $\mathrm{H}^1(J[2])$, which is isomorphic to $\mathrm{H}^1(M)/k^*$. The statement now follows immediately from Proposition 2.6. □

We now interpret the elements of $\mathrm{H}^1(J[2])$ as certain twists of the Jacobian J. The remainder of this section is well known.

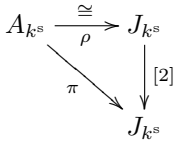
Definition 2.10. *Let K be any extension of k, and X a variety over k; a K/k-twist of X is a variety Y over k such that there exists an isomorphism $Y_K \to X_K$. Two K/k-twists are isomorphic if they are isomorphic over k.*

Proposition 2.11. *Let K be a Galois extension of k and let X be a quasi-projective variety over k. There is a natural bijection between the set of isomorphism classes of K/k-twists of X and $\mathrm{H}^1(\mathrm{Gal}(K/k), \mathrm{Aut}(X_K))$ that sends a twist A to the class of the cocycle $\sigma \mapsto \varphi\circ\sigma(\varphi^{-1})$ for a fixed choice of isomorphism $\varphi\colon A_{k^{\mathrm{s}}} \to X_{k^{\mathrm{s}}}$.*

Proof. See [25, Chapter III, § 1, Proposition 5]. □

We can embed $J[2](k^{\mathrm{s}})$ into $\mathrm{Aut}(J_{k^{\mathrm{s}}})$ by sending $P \in J[2](k^{\mathrm{s}})$ to the automorphism T_P that is translation by P. This induces a map $\mathrm{H}^1(J[2]) \to \mathrm{H}^1(\mathrm{Aut}(J_{k^{\mathrm{s}}}))$, through which every element in $\mathrm{H}^1(J[2])$ is associated to some k^{s}/k-twist of J by Proposition 2.11. These particular twists carry the structure of a two-covering, defined below.

Definition 2.12. *A two-covering of J is a surface A over k together with a morphism $\pi\colon A \to J$ over k, such that there exists an isomorphism $\rho\colon A_{k^s} \to J_{k^s}$ with $\pi = [2] \circ \rho$. In other words, ρ makes the following diagram commutative.*



An isomorphism $(A_1, \pi_1) \to (A_2, \pi_2)$ between two two-coverings is an isomorphism $h\colon A_1 \to A_2$ over k with $\pi_1 = \pi_2 \circ h$.

Although two 2-coverings (A_1, π_1) and (A_2, π_2) may be non-isomorphic while A_1 and A_2 are isomorphic as twists, we often just talk about a two-covering A of J, regarding the covering map π as implicit. For any two-torsion point $P \in J[2](k^s)$, let T_P denote the automorphism of J given by translation by P. The following lemma shows that the isomorphism ρ in Definition 2.12 is well defined up to translation by a two-torsion point.

Lemma 2.13. *Let (A, π) be a two-covering of J, and let $\rho, \rho'\colon A_{k^s} \to J_{k^s}$ be two isomorphisms satisfying $[2] \circ \rho = \pi = [2] \circ \rho'$. Then there is a unique point $P \in J[2](k^s)$ such that $\rho' = T_P \circ \rho$.*

Proof. Define a map $\tau\colon A_{k^s} \to J_{k^s}$ by $\tau(R) = \rho'(R) - \rho(R)$. Then for each $R \in A(k^s)$ we have $2\tau(R) = 2\rho'(R) - 2\rho(R) = \pi(R) - \pi(R) = 0$, so $\tau(R) \in J[2](k^s)$. Since $J[2](k^s)$ is discrete, τ is continuous, and A_{k^s} is irreducible, we find that τ is constant, say $\tau(R) = P$ for some fixed P. Then $\rho' = T_P \circ \rho$. The point P is unique, because if $\rho' = T_S \circ \rho$ for some point S, then $S = \tau(R)$ for all $R \in A(k^s)$. □

Lemma 2.14. *Let A be a two-covering of J and choose an isomorphism ρ as in Definition 2.12. Then for each Galois automorphism $\sigma \in \mathrm{Gal}(k^s/k)$ there is a unique point $P \in J[2](k^s)$ satisfying $\rho \circ \sigma(\rho^{-1}) = T_P$. The map $\sigma \mapsto P$ induces a well-defined cocycle class τ_A in $\mathrm{H}^1(J[2])$ that does not depend on the choice of ρ. The map that sends a two-covering B to τ_B yields a bijection between the set of isomorphism classes of two-coverings of J and the set $\mathrm{H}^1(J[2])$.*

Proof. The unique existence of P follows from Lemma 2.13 applied to $\rho' = \sigma(\rho)$. It is easily checked that for fixed ρ the map $\sigma \mapsto P$ is a cocycle. By Lemma 2.13, another choice for ρ differs from ρ by composition with T_P for some $P \in J[2](k^s)$, so the corresponding cocycle differs from the original one by a coboundary, and the cocycle class τ_A is independent of ρ. Suppose A_1 and A_2 are two-coverings of J with the same corresponding cocycle class in $\mathrm{H}^1(J[2])$. For $i = 1, 2$, choose an isomorphism $\rho_i\colon (A_i)_{k^s} \to J_{k^s}$. Then the two cocycles $\sigma \mapsto \rho_1 \circ \sigma(\rho_1^{-1})$ and $\sigma \mapsto \rho_2 \circ \sigma(\rho_2^{-1})$ differ by a coboundary. After composing ρ_2 with T_P for some $P \in J[2](k^s)$, we may assume this coboundary is trivial, so $\rho_1 \circ \sigma(\rho_1^{-1}) = \rho_2 \circ \sigma(\rho_2^{-1})$ for all $\sigma \in \mathrm{Gal}(k^s/k)$. It follows that the isomorphism $\rho_2^{-1} \circ \rho_1$ is Galois invariant, so A_1 and A_2 are isomorphic over k. We deduce that the map $B \mapsto \tau_B$ is injective. For surjectivity, suppose $c\colon \mathrm{Gal}(k^s/k) \to J[2](k^s)$ is a cocycle. Composition with the map $J[2](k^s) \to \mathrm{Aut}\, J(k^s)$ gives a cocycle with values in $\mathrm{Aut}\, J(k^s)$, which corresponds by Proposition 2.11 to a twist A of J in the sense that there is an isomorphism $\varphi\colon A_{k^s} \to J_{k^s}$ such that the cocycle $\sigma \mapsto \varphi \circ \sigma(\varphi^{-1})$ equals c. It follows that $[2] \circ \varphi$ is defined over the ground field and makes A into a two-covering that maps to the cocycle class of c. □

Proposition 2.15. *Let A be a two-covering of J corresponding to the cocycle class $\xi \in \mathrm{H}^1(J[2])$. Then A contains a k-rational point if and only if ξ is in the image of $\iota\colon J(k)/2J(k) \to \mathrm{H}^1(J[2])$.*

Proof. The inclusion $T\colon J[2](k^s) \to \mathrm{Aut}\, J_{k^s}$ that sends $P \in J[2](k^s)$ to T_P induces a map $T_*\colon \mathrm{H}^1(J[2]) \to \mathrm{H}^1(\mathrm{Aut}\, J_{k^s})$. Set $\eta = T(\xi)$. Suppose $g\colon A_{k^s} \to J_{k^s}$ is an isomorphism that gives A its two-covering structure, so that the composition $[2] \circ g$ is defined over k. Then η is the class of the cocycle $\psi \in Z^1(\mathrm{Aut}\, J_{k^s})$ given by $\psi(\sigma) = g \circ \sigma(g)^{-1}$.

Suppose there is a point $P \in J(k)$ such that $\xi = \iota(\overline{P})$ where $\overline{P}$ is the image of P in $J(k)/2J(k)$. Then η is also the class of the cocycle $\varphi \in Z^1(\mathrm{Aut}\, J_{k^s})$ given by $\varphi(\sigma) = T_{\sigma(Q)-Q}$ for any fixed Q with $2Q = P$. This implies that φ and ψ are cohomologous, so there is an automorphism

$m \in \operatorname{Aut} J_{k^s}$ such that $\varphi(\sigma) = m \circ \psi(\sigma) \circ \sigma(m)^{-1}$ for all $\sigma \in \mathrm{Gal}(k^s/k)$. Choose such an m and set $h = m \circ g$ and $R = h^{-1}(-Q) \in A$. Then for all $\sigma \in \mathrm{Gal}(k^s/k)$ we have $h \circ \sigma(h)^{-1} = T_{\sigma(Q)-Q}$, so

$$\begin{aligned}\sigma(R) = \sigma(h^{-1}(-Q)) = \sigma(h)^{-1}(-\sigma(Q)) = (h^{-1} \circ h \circ \sigma(h)^{-1})(-\sigma(Q)) = \\ = (h^{-1} \circ T_{\sigma(Q)-Q})(-\sigma(Q)) = h^{-1}(-Q) = R.\end{aligned}$$

We conclude that R is k-rational.

Conversely, suppose that A contains a k-rational point, say $R \in A(k)$. Set $Q = -g(R)$ and $P = 2Q$. Take any $\sigma \in \mathrm{Gal}(k^s/k)$. Then by Lemma 2.14 there is a point $S \in J[2](k^s)$ such that $\psi(\sigma) = g \circ \sigma(g)^{-1} = T_S$. We get

$$\begin{aligned}S - \sigma(Q) = T_S(-\sigma(Q)) = g((\sigma(g)^{-1})(-\sigma(Q)) \\ = g(\sigma(g^{-1}(-Q))) = g(\sigma(R)) = g(R) = -Q,\end{aligned}$$

so $S = \sigma(Q) - Q$. From $0 = 2S = 2\sigma(Q) - 2Q = \sigma(P) - P$ we find that P is fixed by σ. As this holds for all choices of σ we find that P is k-rational. Its image $\iota(\overline{P})$ is the class represented by the cocycle that sends σ to $T_{\sigma(Q)-Q}$, which by the above equals ξ. □

Remark 2.16. *Let k be a global field. The Selmer group $\mathrm{Sel}^2(J,k) \subset \mathrm{H}^1(J[2](k^s))$ consists of those elements of $\mathrm{H}^1(J[2](k^s))$ that restrict to elements in the image of $\iota_v \colon J(k_v)/2J(k_v) \to \mathrm{H}^1(k_v, J[2](k_v^s))$ for every place v of k, see Remark 2.3. By Proposition 2.15 these elements correspond under the map of Lemma 2.14 to those two-coverings of J that have a point locally everywhere. Again by Proposition 2.15, an element of $\mathrm{Sel}^2(J,k)$ maps to zero in the Tate-Shafarevich group if and only if the corresponding two-covering contains a rational point.*

Although we do not need it in this paper, it is worth noting that two-covers of J are not just twists of J, but can in fact be given the structure of a k-torsor under J. This implies that if a two-covering of J has a rational point, then it is in fact isomorphic to J over k. The following proposition (see [26, Proposition 3.3.2 (ii)] for the proof) tells us how to give a two-covering the structure of a k-torsor under J.

Proposition 2.17. *Let (A, π) be a two-covering of J, and let $\rho \colon A_{k^s} \to J_{k^s}$ be an isomorphism satisfying $[2] \circ \rho = \pi$. Then there exists a unique morphism $\tau \colon J \times A \to A$ given by $\tau(R, a) = \rho^{-1}(R + \rho(a))$, which is independent of the choice of ρ, and which gives A the structure of a k-torsor under J.*

As mentioned in the introduction, our goal is to give an explicit model in $\mathbb{P}^{15}$ of the two-coverings of J corresponding to elements of $P^1(J[2])$, as defined just after Proposition 2.2. In particular this includes the two-coverings corresponding to elements of $\mathrm{Sel}^2(J,k)$, see Remarks 2.3 and 2.16.

3. Models of the Jacobian and its Kummer surface

We continue to use the notation of Section 2. Let $[-1]$ denote the automorphism of J given by multiplication by -1. The *Kummer surface $\mathcal{X}$ of J* is defined to be the quotient $J/\langle[-1]\rangle$. It has 16 singularities, all ordinary double points coming from the fixed points of $[-1]$, i.e., the two-torsion points of J. Let $\mathcal{Y}$ be the blow-up of $\mathcal{X}$ in these singular points. Then $\mathcal{Y}$ is a smooth K3 surface, which we call the *desingularized Kummer surface of J* to distinguish it from the singular Kummer surface $\mathcal{X}$ of J. In many places in the literature, $\mathcal{Y}$ is also referred to as the Kummer surface of J. We denote the (-2)-curve on $\mathcal{Y}$ above the singular point of $\mathcal{X}$ corresponding to $P \in J[2]$ by E_P. Let J' be the blow-up of J in its two-torsion points. We denote the (-1)-curve on J' above the point $P \in J[2]$ by F_P. The involution $[-1]$ on J lifts to an involution on J' such that the quotient is isomorphic to $\mathcal{Y}$. In other words, there is a morphism $J' \to \mathcal{Y}$, with ramification

divisor $\sum_{P\in J[2]} F_P$, that makes the following diagram commutative, cf. [14, Diagram (2.2)].

$$\begin{array}{ccc} J' & \longrightarrow & J \\ \downarrow & & \downarrow \\ \mathcal{Y} & \longrightarrow & \mathcal{X} \end{array}$$

Let K_C be the canonical divisor of C that is supported at the points at infinity, i.e., $K_C = (\infty^+) + (\infty^-)$, where ∞^+ and ∞^- are the two points at infinity, which may not be defined over the ground field individually. We let ι_h denote the hyperelliptic involution on C that sends (x_0, y_0) to $(x_0, -y_0)$. We have $\iota_h(\infty^\pm) = \infty^\mp$. For any point Q on C the divisor $(Q) + (\iota_h(Q))$ is linearly equivalent to K_C.

The map $p\colon C \times C \to J$ that sends (P, Q) to the divisor $(P) + (Q) - K_C$ factors through the symmetric square $C^{(2)}$ of C. The induced map $C^{(2)} \to J$ is birational (see [16, Theorem VII.5.1]). In fact, it describes $C^{(2)}$ as the blow-up of J at the origin $\mathcal{O}$ of J; the inverse image of $\mathcal{O}$ is the curve on $C^{(2)}$ that consists of all (unordered) pairs $\{Q, \iota_h(Q)\}$. We may therefore identify the function field $k(J)$ of J with that of $C^{(2)}$, which consists of the functions in the function field

$$k(C \times C) = k(x_1, x_2)[y_1, y_2]/\big(y_1^2 - f(x_1), y_2^2 - f(x_2)\big)$$

of $C \times C$ invariant under the exchange of the indices. As for any points P, Q on C the divisor $(P)+(Q)-K_C$ is linearly equivalent to $-(\iota_h(P)+\iota_h(Q)-K_C)$, it follows that $[-1]$ on J is induced through p by the involution ι_h. Therefore the induced automorphism $[-1]^*$ of $k(J)$ fixes x_1 and x_2 and changes the sign of y_1 and y_2. For any function $g \in k(J)$ we say that g is *even* or *odd* if we have $[-1]^*(g) = g$ or $[-1]^*(g) = -g$ respectively.

For any Weierstrass point $w \in W$ of C we define Θ_w to be the divisor on J that is the image under p of the divisor $C \times \{w\}$ on $C \times C$. It consists of all divisor classes represented by $(P) - (w)$ for some point P on C. The doubles of these so-called theta-divisors are all linearly equivalent. By abuse of notation, we will write $2n\Theta$ for the divisor class of $2n\Theta_w$ for any integer n and any Weierstrass point w. Although Θ itself is not a well-defined divisor class modulo linear equivalence, it is well defined modulo numerical equivalence. We have $\Theta^2 = 2$ (in general, on a Jacobian of dimension g we have $\Theta^g = g!$, see [17, Section 1]). Also, we have $h^0(n\Theta_w) = n^2$ for any integer $n > 0$ and any $w \in W$; the linear systems $|2\Theta_w|$, $|3\Theta_w|$, and $|4\Theta_w|$ determine morphisms of J to $\mathbb{P}^3$, $\mathbb{P}^8$, and $\mathbb{P}^{15}$ respectively.

Proposition 3.1. *Suppose $w \in W$ is a Weierstrass point defined over k. The linear system $|2\Theta_w|$ induces a morphism of J to $\mathbb{P}^3_k$ that is the composition of the quotient map $J \to \mathcal{X}$ and a closed embedding of $\mathcal{X}$ into $\mathbb{P}^3_k$. The linear systems $|3\Theta_w|$ and $|4\Theta_w|$ induce closed embeddings of J into $\mathbb{P}^8_k$ and $\mathbb{P}^{15}_k$ respectively.*

Proof. See [17, Section 5, Case d)]. □

Unfortunately, in full generality we cannot use the linear system $|3\Theta_w|$ to give an explicit model of J in $\mathbb{P}^8_k$, as this system may not be defined over the ground field k. If C contains a rational Weierstrass point w, then Θ_w is defined over the ground field and a model of J in $\mathbb{P}^8$ can be found by sending the rational Weierstrass point to infinity, thus reducing to the case that C is given by an equation of the form $y^2 = h(x)$ where h is of degree 5, see [13]. The explicit twisting we perform in Section 7 was done in [12] in the case that all Weierstrass points are defined over the ground field.

For any divisor D on a variety S over k, let $\mathcal{L}(D)$ denote the k-vector space $\mathrm{H}^0(S, \mathcal{O}_S(D))$. Let $\Theta_\pm$ denote the divisor on J that is the image under p of the divisor $C \times \{\infty^\pm\}$ on $C \times C$. Then $\Theta_+ + \Theta_-$ is a rational divisor in $|2\Theta|$, so the maps induced by $|2\Theta|$ and $|4\Theta|$ can always be defined over the ground field. The first author has given explicit bases for the vector spaces $\mathcal{L}(\Theta_+ + \Theta_-)$

and $\mathcal{L}(2(\Theta_+ + \Theta_-))$ in [9]. Set

$$k_1 = 1, \qquad k_2 = x_1 + x_2, \qquad k_3 = x_1 x_2,$$

$$k_4 = \frac{2f_0 + f_1 k_2 + 2f_2 k_3 + f_3 k_2 k_3 + 2f_4 k_3^2 + f_5 k_2 k_3^2 + 2f_6 k_3^3 - 2y_1 y_2}{(x_1 - x_2)^2},$$

$$k_{ij} = k_{ji} = k_i k_j \quad (\text{for } 1 \leq i, j \leq 4),$$

$$b_i = \frac{x_2^{i-1} y_1 - x_1^{i-1} y_2}{x_1 - x_2} \quad (\text{for } 1 \leq i \leq 4), \tag{3}$$

$$b_5 = \frac{1}{2f_6} \frac{G(x_1, x_2) y_1 - G(x_2, x_1) y_2}{(x_1 - x_2)^3},$$

$$b_6 = -\frac{1}{4f_6}\big(f_1 b_1 + 2f_2 b_2 + 3f_3 b_3 + 4f_4 b_4 + 4f_5 b_5 - f_5 k_3 b_3 + f_5 k_2 b_4 - 2f_6 k_3 b_4 + 2f_6 k_2 b_5\big),$$

with

$$G(r, s) = 4f_0 + f_1(r + 3s) + 2f_2 s(r + s) + f_3 s^2(3r + s) + 4f_4 r s^3 + f_5 s^4(5r - s) + 2f_6 r s^4(r + s).$$

Define the functions $a_0, a_1, \ldots, a_{15}$ by

$$\begin{aligned}
&a_0 = k_{44}, && a_1 = -f_1 b_1 - 2\textstyle\sum_{i=2}^{6} f_i b_i, && a_2 = f_5 b_4 + 2f_6 b_5,\\
&a_3 = k_{34}, && a_4 = \tfrac{1}{2}(k_{24} - f_1 k_{11} - f_3 k_{13} - f_5 k_{33}), && a_5 = k_{14},\\
&a_6 = b_4, && a_7 = b_3, && a_8 = b_2,\\
&a_9 = b_1, && a_{10} = k_{33}, && a_{11} = k_{23},\\
&a_{12} = k_{13}, && a_{13} = k_{12}, && a_{14} = k_{11},\\
&a_{15} = k_{22} - 4k_{13}.
\end{aligned} \tag{4}$$

The functions $a_0, \ldots, a_{15}$ are the functions used in [4, Sections 2.1–2] as $z_0, \ldots, z_{15}$.

Proposition 3.2. *The sequence (k_1, k_2, k_3, k_4) is a basis for $\mathcal{L}(\Theta_+ + \Theta_-)$. The sequences $(a_i)_{i=0}^{15}$ and $(k_{11}, k_{12}, \ldots, k_{44}, b_1, \ldots, b_6)$ are bases for $\mathcal{L}(2(\Theta_+ + \Theta_-))$.*

Proof. One checks that the functions k_1, k_2, k_3, k_4 are regular except for a pole of order at most one along Θ_+ and Θ_-, so they are contained in $\mathcal{L}(\Theta_+ + \Theta_-)$. Since the function $y_1 y_2$ is not contained in the subfield $k(x_1, x_2)$ of $k(J)$, it follows that these functions are linearly independent. As $\mathcal{L}(\Theta_+ + \Theta_-)$ has dimension 4, they indeed form a basis. A similar argument works for the vector space $\mathcal{L}(2(\Theta_+ + \Theta_-))$. Alternatively, one checks that $a_0, \ldots, a_{15}$ are the functions defined in [4, Sections 2.1–2], where it is proved that they indeed form a basis of $\mathcal{L}(2(\Theta_+ + \Theta_-))$. From (4) it then follows immediately that the sequence $(k_{11}, k_{12}, \ldots, k_{44}, b_1, \ldots, b_6)$ is a basis of $\mathcal{L}(2(\Theta_+ + \Theta_-))$ as well. □

Corollary 3.3. *The quotient map $J \to \mathcal{X}$ is given by $D \mapsto [k_1(D) : k_2(D) : k_3(D) : k_4(D)]$ or $D \mapsto [k_{1i}(D) : k_{2i}(D) : k_{3i}(D) : k_{4i}(D)]$ for any $1 \leq i \leq 4$.*

Proof. This follows immediately from Propositions 3.1 and 3.2. □

For any k-vector space V we denote the multiplication on the symmetric algebra $\operatorname{Sym} V = \bigoplus_{d=0}^{\infty} \operatorname{Sym}^d V$ by $(g, h) \mapsto g * h$ to avoid confusion with a possibly already existing product. In particular this implies that for every positive integer d the natural quotient map $V^{\otimes d} \to \operatorname{Sym}^d V$ is given by $v_1 \otimes \cdots \otimes v_d \mapsto v_1 * \cdots * v_d$.

Remark 3.4. *Under the natural map $\operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-) \to \mathcal{L}(2(\Theta_+ + \Theta_-))$ that sends $g * h$ to gh, the element $k_i * k_j$ maps to k_{ij}. The fact that $\{k_{ij}\}_{i,j}$ is a linearly independent set is equivalent to the fact that this map is injective, which is in turn equivalent to the fact that there are no quadratic polynomials vanishing on the image of $\mathcal{X}$ in $\mathbb{P}^3$ embedded by $|2\Theta|$. For the rest of this paper we freely identify $\operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$ with its image in $\mathcal{L}(2(\Theta_+ + \Theta_-))$.*

Remark 3.5. *Note that $(k_{ij})_{i,j}$ and $(a_0, a_3, a_4, a_5, a_{10}, \ldots, a_{15})$ are bases of the 10-dimensional space of even functions, while $(b_i)_i$ and $(a_1, a_2, a_6, a_7, a_8, a_9)$ are bases of the 6-dimensional space of odd functions. It follows from Propositions 3.1 and 3.2 that together they give an embedding of J into $\mathbb{P}^{15}$. By definition of the k_{ij}, the projection of $\mathbb{P}^{15}$ onto the 10 even coordinates factors as the map from J to $\mathbb{P}^3$ given by k_1, k_2, k_3, k_4 and the 2-uple embedding from $\mathbb{P}^3$ to $\mathbb{P}^9$. Again by Propositions 3.1 and 3.2 it follows that this map from J to $\mathbb{P}^9$ is the composition of the quotient map $J \to \mathcal{X}$ and a closed embedding of $\mathcal{X}$ into $\mathbb{P}^9$.*

We now study the projection onto the odd coordinates; this gives the desingularization of $\mathcal{X}$. By abuse of notation we also write $2n\Theta$ or $\Theta_\pm$ for the divisor class on J' that is the pull-back of $2n\Theta$ or $\Theta_\pm$ on J under the blow-up map $J' \to J$ for any integer n.

Proposition 3.6. *There are direct sum decompositions*

$$\begin{aligned}\mathcal{L}\big(2(\Theta_+ + \Theta_-)\big) &= \langle \textit{even coordinates} \rangle \oplus \langle \textit{odd coordinates} \rangle \\ &= \mathrm{Sym}^2\big(\mathcal{L}(\Theta_+ + \Theta_-)\big) \oplus \mathcal{L}\big(2(\Theta_+ + \Theta_-)\big)(-J[2]) \\ &\simeq \mathrm{H}^0\big(\mathcal{X}, \varphi^*\mathcal{O}_{\mathbb{P}^3}(2)\big) \oplus \mathrm{H}^0\big(J', \mathcal{O}_{J'}\big(2(\Theta_+ + \Theta_-) - \textstyle\sum_P F_P\big)\big)\end{aligned}$$

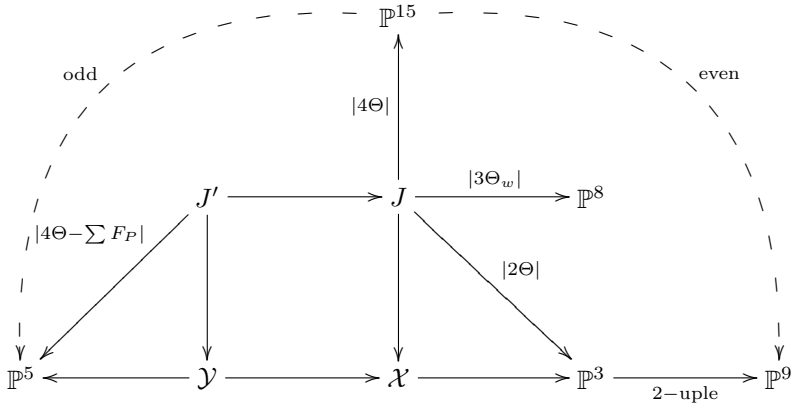
where $\mathcal{L}\big(2(\Theta_+ + \Theta_-)\big)(-J[2])$ is the subspace of $\mathcal{L}\big(2(\Theta_+ + \Theta_-)\big)$ of sections vanishing on the two-torsion points and $\varphi\colon \mathcal{X} \to \mathbb{P}^3$ is the embedding of $\mathcal{X}$ into $\mathbb{P}^3$ associated to $|\Theta_+ + \Theta_-|$. Furthermore, the projection of $J \subset \mathbb{P}^{15}$ away from the even coordinates determines a rational map

$$\begin{aligned} J &\dashrightarrow \mathbb{P}^5 \\ D &\longmapsto [b_1(D) : \ldots : b_6(D)]\end{aligned}$$

which induces the morphism $J' \to \mathbb{P}^5$ associated to the linear system $|4\Theta - \sum_P F_P|$ on J', and factors as the quotient map $J' \to \mathcal{Y}$ and a closed embedding $\mathcal{Y} \to \mathbb{P}^5$.

Proof. The decomposition into even and odd coordinates is immediate, since the characteristic of the field k is different from 2. The vector space $\mathcal{L}\big(2(\Theta_+ + \Theta_-)\big)(-J[2])$ contains all the odd functions; the reverse inclusion is a consequence of [1, Exercise VIII.22.9, p. 104]. This establishes the second decomposition. The third decomposition follows at once from the previous ones. The second part of the proposition follows. □

In the following diagram we summarize the maps that we described.



The ideal of the image of J in $\mathbb{P}^{15}$ is generated by 72 quadrics (see [9]). There are 21 linearly independent quadrics in just the even functions, which define the image of $\mathcal{X}$ in $\mathbb{P}^9$. A 20-dimensional subspace of the space generated by these quadrics is spanned by the equations of the form $k_{ij}k_{rs} = k_{ir}k_{js}$ for $1 \le i, j, r, s \le 4$, which define the image of $\mathbb{P}^3$ in $\mathbb{P}^9$ under the 2-uple embedding. From the quartic that defines the image of $\mathcal{X}$ in $\mathbb{P}^3$ we find another quadric in only

the even functions, namely

$$\begin{aligned} g_{\mathcal{X}} \;=\; & (-4f_0f_2+f_1^2)k_{11}^2 - 4f_0f_3k_{11}k_{12} - 2f_1f_3k_{11}k_{13} - 4f_0k_{11}k_{14} - 4f_0f_4k_{12}^2 + \\ & (4f_0f_5-4f_1f_4)k_{12}k_{13} - 2f_1k_{11}k_{24} + (-4f_0f_6+2f_1f_5-4f_2f_4+f_3^2)k_{13}^2 - \\ & 4f_2k_{11}k_{34} - 4f_0f_5k_{12}k_{22} + (8f_0f_6-4f_1f_5)k_{13}k_{22} + (4f_1f_6-4f_2f_5)k_{13}k_{23} - \\ & 2f_3k_{13}k_{24} - 2f_3f_5k_{13}k_{33} - 4f_4k_{13}k_{34} - 4k_{14}k_{34} - 4f_0f_6k_{22}^2 - 4f_1f_6k_{22}k_{23} - \\ & 4f_2f_6k_{23}^2 + k_{24}^2 - 4f_3f_6k_{23}k_{33} - 2f_5k_{23}k_{34} + (-4f_4f_6+f_5^2)k_{33}^2 - 4f_6k_{33}k_{34}. \end{aligned} \tag{5}$$

Set

$$\begin{aligned} e_1 &= 2f_0b_1 + f_1b_2, \\ e_2 &= f_3b_3 + 2(f_4b_4 + f_5b_5 + f_6b_6), \\ e_3 &= f_5b_4 + 2f_6b_5. \end{aligned}$$

Then the four entries $\mathcal{Q}_1, \dots, \mathcal{Q}_4$ of the vector

$$\begin{pmatrix} 0 & e_1 & -e_2 & -b_4 \\ -e_1 & 0 & -e_3 & b_3 \\ e_2 & e_3 & 0 & -b_2 \\ b_4 & -b_3 & b_2 & 0 \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \end{pmatrix} = \begin{pmatrix} \mathcal{Q}_1 \\ \mathcal{Q}_2 \\ \mathcal{Q}_3 \\ \mathcal{Q}_4 \end{pmatrix} \tag{6}$$

are linear combinations of the functions k_ib_l that vanish on J. Multiplying each $\mathcal{Q}_i$ by any of the four k_j gives 16 linear combinations $k_j\mathcal{Q}_i$ of the functions $k_{ij}b_l$, and thus 16 vanishing quadrics $k_j\mathcal{Q}_i$ in the k_{ij} and the b_j. Since the matrix in (6) is antisymmetric, the linear combination $k_1\mathcal{Q}_1 + k_2\mathcal{Q}_2 + k_3\mathcal{Q}_3 + k_4\mathcal{Q}_4$ is identically zero. It can be checked that this is the only linear combination of the $k_j\mathcal{Q}_i$ that vanishes identically, so we obtain a 15-dimensional subspace of odd quadrics that vanish on J. Replacing each b_i by b_{i-1}, with b_0 defined so that $\sum_{i=0}^{6} f_ib_i = 0$ for notational convenience, we get another 15-dimensional subspace of odd quadrics that also vanish on J. These equations together give the full 30-dimensional subspace of the odd vanishing quadrics.

We are 21 quadrics short of 72. Note that the space of quadratic polynomials in $b_1, \dots, b_6$ has dimension 21. The remaining 21 vanishing quadrics express the quadratic polynomials in the b_i in terms of the k_{ij}. We have for instance

$$\begin{aligned} b_1^2 &= f_2k_{11}^2 + f_3k_{11}k_{12} + k_{11}k_{14} + f_6k_{11}k_{33} + f_4k_{12}^2 - f_5k_{12}k_{13} + f_5k_{12}k_{22} - 2f_6k_{13}k_{22} + f_6k_{22}^2, \\ 2b_1b_2 &= -f_1k_{11}^2 + f_3k_{11}k_{13} + 2f_4k_{11}k_{23} + k_{11}k_{24} - f_5k_{11}k_{33} - 2f_6k_{12}k_{33} + 2f_5k_{13}k_{22} + 2f_6k_{22}k_{23}, \\ b_2^2 &= f_0k_{11}^2 + f_4k_{13}^2 + k_{13}k_{14} + f_5k_{13}k_{23} + f_6k_{22}k_{33}, \\ 2b_2b_3 &= 2f_0k_{11}k_{12} + f_1k_{11}k_{13} - f_3k_{13}^2 + k_{13}k_{24} + f_5k_{13}k_{33} + 2f_6k_{23}k_{33}, \\ b_3^2 &= f_0k_{11}k_{22} + f_1k_{11}k_{23} + f_2k_{11}k_{33} + k_{14}k_{33} + f_6k_{33}^2, \\ 2b_3b_4 &= -f_1k_{11}k_{33} - 2f_0k_{12}k_{13} + 2f_0k_{12}k_{22} + 2f_2k_{12}k_{33} + 2f_1k_{13}k_{22} + f_3k_{13}k_{33} + k_{24}k_{33} - f_5k_{33}^2, \\ b_4^2 &= f_0k_{11}k_{33} - 2f_0k_{13}k_{22} - f_1k_{13}k_{23} + f_0k_{22}^2 + f_1k_{22}k_{23} + f_2k_{23}^2 + f_3k_{23}k_{33} + f_4k_{33}^2 + k_{33}k_{34}. \end{aligned} \tag{7}$$

For the full list, see [10].

Remark 3.7. *The 42-dimensional space of even vanishing quadratic polynomials contains a 3-dimensional subspace of quadratic polynomials that only involve $b_1, \dots, b_6$. These describe the image of $\mathcal{Y}$ in $\mathbb{P}^5$. With respect to the sequence $(b_1, \dots, b_6)$, the symmetric matrices R^jT with*

$$R = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -f_0f_6^{-1} \\ 1 & 0 & 0 & 0 & 0 & -f_1f_6^{-1} \\ 0 & 1 & 0 & 0 & 0 & -f_2f_6^{-1} \\ 0 & 0 & 1 & 0 & 0 & -f_3f_6^{-1} \\ 0 & 0 & 0 & 1 & 0 & -f_4f_6^{-1} \\ 0 & 0 & 0 & 0 & 1 & -f_5f_6^{-1} \end{pmatrix} \qquad \textit{and} \qquad T = \begin{pmatrix} f_1 & f_2 & f_3 & f_4 & f_5 & f_6 \\ f_2 & f_3 & f_4 & f_5 & f_6 & 0 \\ f_3 & f_4 & f_5 & f_6 & 0 & 0 \\ f_4 & f_5 & f_6 & 0 & 0 & 0 \\ f_5 & f_6 & 0 & 0 & 0 & 0 \\ f_6 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and $0 \leq j \leq 2$ correspond to quadratic polynomials that span this subspace. The reader is encouraged to compute the matrices R^jT for $1 \leq j \leq 7$, which will come back in Section 4.

Remark 3.8. *Note that we can use the last* 21 *given even quadrics to describe the rational map from $\mathcal{X}$ to $\mathcal{Y}$. Indeed, a general point P on $\mathcal{Y} \subset \mathbb{P}^5$ is given by $[b_r(P)b_1(P) : \cdots : b_r(P)b_6(P)]$ for any fixed r. As mentioned above, all quadratic polynomials in the b_i can be expressed as quadratics in the k_{ij}, or as quartics in the k_i. The corresponding expressions for $b_rb_1, \ldots, b_rb_6$ induce a map from $\mathcal{X}$ to $\mathcal{Y}$ that is the rational inverse of the blow-up morphism $\mathcal{Y} \to \mathcal{X}$. This morphism can be described explicitly as*

$$[b_1 : \cdots : b_6] \mapsto [k_1 : k_2 : k_3 : k_4] = [b_1b_3 - b_2^2 : b_1b_4 - b_2b_3 : b_2b_4 - b_3^2 : \\ f_0b_1^2 + f_1b_1b_2 + f_2b_2^2 + f_3b_2b_3 + f_4b_3^2 + f_5b_3b_4 + f_6b_4^2],$$

which can be checked either by expressing the quadratic polynomials in the b_i in terms of the k_{ij}, or by checking directly that for instance $b_1b_3 - b_2^2 = -y_1y_2$. Furthermore, as this map only involves b_1, b_2, b_3, and b_4, it factors through the projection of $\mathbb{P}^5$ on the $\mathbb{P}^3$ with coordinates $b_1, \ldots, b_4$. The image of $\mathcal{Y}$ under this projection is the Weddle surface (see [4, Chapter 5]*), which is given by*

$$f_0b_1^3b_4 - 3f_0b_1^2b_2b_3 + f_1b_1^2b_2b_4 - f_1b_1^2b_3^2 + 2f_0b_1b_2^3 - f_1b_1b_2^2b_3 + f_2b_1b_2^2b_4 - \\ 2f_2b_1b_2b_3^2 - f_3b_1b_3^3 - f_4b_1b_3^2b_4 - f_5b_1b_3b_4^2 - f_6b_1b_4^3 + f_1b_2^4 + f_2b_2^3b_3 + f_3b_2^3b_4 + \\ 2f_4b_2^2b_3b_4 + f_5b_2^2b_4^2 - f_4b_2b_3^3 + f_5b_2b_3^2b_4 + 3f_6b_2b_3b_4^2 - f_5b_3^4 - 2f_6b_3^3b_4 = 0.$$

This answers the question in [4, Section 16.6] *to describe the map $\mathcal{X} \to \mathcal{Y}$ explicitly.*

4. Another description of the desingularized Kummer surface

The description of the desingularized Kummer surface given in this section is also given in [4, Chapter 16]. As in [15], we also extend it to twists of the surface. This new description serves several purposes. First of all, over k^{s} it allows us a find a set of three *diagonal* quadratic forms that describe $\mathcal{Y}$. Second, it helps us to understand the action of $J[2]$ on our explicit model of $\mathcal{Y}$ in $\mathbb{P}^5$. In fact these two purposes are closely related.

Consider the projective space $\mathbb{P}(L) \cong (L - \{0\})/k^*$ over k with $L = k[X]/f$ as before. Its homogeneous coordinate ring is $\mathrm{Sym}(\hat{L}) = \bigoplus_{n \geq 0} \mathrm{Sym}^n(\hat{L})$, where $\hat{L} = \mathrm{Hom}(L, k)$ is the dual of L. One important basis of L, though not particularly convenient to work with, is the power basis $1, X, \ldots, X^5$. Its dual basis of $\hat{L}$ is $p_0, \ldots, p_5$, where p_i just gives the coefficient of X^i, so that for each $z \in L$ we have $z = \sum_{i=0}^5 p_i(z)X^i$. This dual basis determines a coordinate system on $\mathbb{P}(L)$.

For any $\delta \in L^*$, let $C_0^{(\delta)}, \ldots, C_5^{(\delta)} \in \mathrm{Sym}^2(\hat{L})$ be quadratic forms such that $C_j^{(\delta)}(z) = p_j(\delta z^2)$, and let $V_\delta \subset \mathbb{P}(L)$ be the variety defined by $C_3^{(\delta)} = C_4^{(\delta)} = C_5^{(\delta)} = 0$. Then $V_\delta(k^{\mathrm{s}})$ is the image in $\mathbb{P}(L^{\mathrm{s}}) = (L^{\mathrm{s}} \setminus \{0\})/k^{\mathrm{s}*}$ of the subset

$$\mathcal{V}_\delta = \{\xi \in L^{\mathrm{s}} \setminus \{0\} \ : \ \delta\xi^2 = rX^2 + sX + t \text{ for some } r, s, t \in k^{\mathrm{s}}\} \subset L^{\mathrm{s}} \setminus \{0\}$$

for any $\delta \in L^*$. Recall that the Cassels map $\kappa \circ \iota \colon J(k)/2J(k) \to L^*/{L^*}^2k^*$ sends the class of the divisor $\big((x_1, y_1)\big) + \big((x_2, y_2)\big) - K_C$ to $(X - x_1)(X - x_2)$. Therefore, if the class of $\delta \in L^*$ in $L^*/{L^*}^2k^*$ is in the image of the Cassels map, then there exists a $\xi \in L^*$ and $s, t, c \in k^*$ such that $\delta\xi^2 = c(X^2 - sX + t)$, i.e., such that $(\xi \cdot k^*) \in \mathbb{P}(L)$ is contained in V_δ.

In this section we will see that V_1 is isomorphic to the desingularized Kummer surface $\mathcal{Y}$ and that V_δ is a twist of V_1 for every $\delta \in L^*$. If δ has square norm, say $N(\delta) = n^2$, then there is a two-covering A of the Jacobian J corresponding to the cocycle class in $\mathrm{H}^1(J[2])$ that is the image of $(\delta, n) \in \Gamma$ under the map in Corollary 2.9; in Section 7 we will see that V_δ is a quotient of A.

Note that although we used p_i to define $C_i^{(\delta)} \in \mathrm{Sym}^2(\hat{L})$, we have not yet expressed the quadrics $C_i^{(\delta)}$ in terms of any basis of $\hat{L}$. Before we do so, and thus describe V_δ explicitly with respect to various bases of $\hat{L}$, we make some basis-free remarks.

For any $a \in L^*$, let m_a denote the linear automorphism of L given by multiplication by a, and let $\hat{m}_a$ be its dual automorphism of $\hat{L}$, so that for every $h \in \hat{L}$ and every $z \in L$ we have $\hat{m}_a(h)(z) = h(m_a(z)) = h(az)$. The automorphism of $\hat{L} \otimes_k \ldots \otimes_k \hat{L}$ induced by the action of $\hat{m}_a$

on each factor $\hat{L}$ induces an automorphism of $\mathrm{Sym}^n(\hat{L})$ for every n, which we also denote by $\hat{m}_a$. In particular we have $\hat{m}_a(C_i^{(\delta)})(z) = p_i(\delta\cdot(az)(az)) = p_i(\delta a^2 z^2) = C_i^{(\delta a^2)}(z)$ for all $z \in L^{\mathrm{s}}$ and all $i \in \{0,\dots,5\}$. The automorphism of $\hat{L}\otimes_k \dots \otimes_k \hat{L}$ induced by the action of $\hat{m}_a$ on exactly one copy of $\hat{L}$ induces an automorphism of $\mathrm{Sym}^n(\hat{L})$ that we denote by $\hat{m}_a^\circ$. Note that on $\mathrm{Sym}^n(\hat{L})$ we have $(\hat{m}_a^\circ)^n = \hat{m}_a$.

Proposition 4.1. *For any $\delta,\xi \in L^*$, the automorphism m_ξ of $\mathbb{P}(L)$ induces an isomorphism from $V_{\delta\xi^2}$ to V_δ.*

Proof. As mentioned above, for $i \in \{0,\dots,5\}$ and for all $z \in L^{\mathrm{s}}$ we have $\hat{m}_\xi(C_i^{(\delta)})(z) = C_i^{(\delta\xi^2)}(z)$. Since V_δ is defined by $C_3^{(\delta)} = C_4^{(\delta)} = C_5^{(\delta)} = 0$ and $V_{\delta\xi^2}$ by $C_3^{(\delta\xi^2)} = C_4^{(\delta\xi^2)} = C_5^{(\delta\xi^2)} = 0$, we conclude that m_ξ induces an isomorphism from $V_{\delta\xi^2}$ to V_δ. □

Corollary 4.2. *For any $\delta \in L^*$, the surfaces V_δ and V_1 are isomorphic over k^{s}.*

Proof. Choose $\varepsilon \in L^{\mathrm{s}*}$ with $\varepsilon^2 = \delta$ and apply Proposition 4.1 with $\xi = \varepsilon^{-1}$. □

Corollary 4.3. *The map $\mu_2(L^{\mathrm{s}}) \to \mathrm{Aut}(\mathbb{P}(L^{\mathrm{s}}))$ that sends ξ to m_ξ induces an injective homomorphism $\mu_2(L^{\mathrm{s}})/\mu_2 \to \mathrm{Aut}\big((V_\delta)_{k^{\mathrm{s}}}\big)$.*

Proof. By Proposition 4.1 we get a homomorphism $\psi\colon \mu_2(L^{\mathrm{s}}) \to \mathrm{Aut}\big((V_\delta)_{k^{\mathrm{s}}}\big)$. Clearly we have $\mu_2 \subset \ker\psi$. Choose $\varepsilon \in L^{\mathrm{s}*}$ with $\varepsilon^2 = \delta$ and let $P \in \mathbb{P}(L)$ be the image of ε^{-1} in $\mathbb{P}(L) = (L-\{0\})/k^{\mathrm{s}*}$. Note that we have $P \in (V_\delta)_{k^{\mathrm{s}}}$. Suppose that $\xi \in \ker\psi$, so the automorphism m_ξ induces the identity on V_δ. Then $m_\xi(P) = P$, so $\xi\varepsilon^{-1} = c\varepsilon^{-1}$ for some $c \in k^{\mathrm{s}*}$. We conclude $\xi = c \in \mu_2(L^{\mathrm{s}}) \cap k^{\mathrm{s}*} = \mu_2(k^{\mathrm{s}})$, so $\ker\psi = \mu_2$ and ψ induces an injection $\mu_2(L^{\mathrm{s}})/\mu_2 \to \mathrm{Aut}\big((V_\delta)_{k^{\mathrm{s}}}\big)$. □

We have $\hat{m}_a^\circ(C_j^{(\delta)})(z) = p_j(\delta(az)z) = C_j^{(\delta a)}(z)$ for $j \in \{0,\dots,5\}$, so in particular we find $\hat{m}_\delta^\circ(C_j^{(1)}) = C_j^{(\delta)}$. Note, however, that the action of $\hat{m}_\delta^\circ$ on $\mathrm{Sym}^2\hat{L}$ is not induced in the normal way by the action of $\hat{m}_\delta$ on $\hat{L}$, so this last equality does not imply that we get an isomorphism between V_δ and V_1 defined over the field of definition of δ. Still, it does help us to get a better understanding of the quadrics that define V_δ. For $a = X$ and any $z \in L$ we have

$$\begin{aligned}\sum_{j=0}^{5} \hat{m}_X^\circ(C_j^{(\delta)})(z)\,X^j &= \sum_{j=0}^{5} p_j(\delta(Xz)z)X^j = X\cdot\delta z^2 = X\left(\sum_{j=0}^{5} C_j^{(\delta)}(z)\,X^j\right)\\ &= -\frac{f_0}{f_6}C_5^{(\delta)}(z) + \sum_{j=1}^{5}\left(C_{j-1}^{(\delta)}(z) - \frac{f_j}{f_6}C_5^{(\delta)}(z)\right)X^j,\end{aligned}$$

where the last equality can also be interpreted as coming from the fact that with respect to the basis $(1,X,\dots,X^5)$, the action of m_X on L is given by multiplication from the left by the matrix R of Remark 3.7. Comparing coefficients of X^{j+1}, we conclude by downward induction on j that

$$f_6 C_j^{(\delta)} = f_{j+1}C_5^{(\delta)} + f_{j+2}\hat{m}_X^\circ C_5^{(\delta)} + \dots + f_6(\hat{m}_X^\circ)^{5-j}C_5^{(\delta)}, \tag{8}$$

for $0 \le j \le 5$. For every integer $j \ge 0$, set

$$Q_j^{(\delta)} = (\hat{m}_X^\circ)^j C_5^{(\delta)} = ((\hat{m}_X^\circ)^j \circ \hat{m}_\delta^\circ)C_5^{(1)}. \tag{9}$$

Then we can write (8) as

$$f_6\big(C_0^{(\delta)}\ \ C_1^{(\delta)}\ \ \cdots\ \ C_5^{(\delta)}\big) = \big(Q_0^{(\delta)}\ \ Q_1^{(\delta)}\ \ \cdots\ \ Q_5^{(\delta)}\big)\cdot T, \tag{10}$$

with the matrix T of Remark 3.7. From (10) we deduce

$$\begin{aligned} Q_0^{(\delta)} &= C_5^{(\delta)},\\ Q_1^{(\delta)} &= C_4^{(\delta)} - f_5 f_6^{-1} C_5^{(\delta)},\\ Q_2^{(\delta)} &= C_3^{(\delta)} - f_5 f_6^{-1} C_4^{(\delta)} + (f_5^2 f_6^{-2} - f_4 f_6^{-1})C_5^{(\delta)}.\end{aligned} \tag{11}$$

Proposition 4.4. *For any $\delta \in L^*$, the surface V_δ is given by $Q_0^{(\delta)} = Q_1^{(\delta)} = Q_2^{(\delta)} = 0$.*

Proof. This follows immediately from the fact that $Q_0^{(\delta)}, Q_1^{(\delta)}, Q_2^{(\delta)}$ are linear combinations of $C_3^{(\delta)}, C_4^{(\delta)}, C_5^{(\delta)}$ and vice versa. □

Proposition 4.5. *Write $\delta \in L^*$ as $\delta = \sum_{i=0}^5 d_i X^i$. Then for any integer $j \geq 0$ we have $Q_j^{(\delta)} = \sum_{i=0}^5 d_i (\hat{m}_X^\circ)^{i+j}(C_5^{(1)})$.*

Proof. We have $\hat{m}_\delta^\circ = \sum_{i=0}^5 d_i (\hat{m}_X^\circ)^i$, so this follows directly from (9). □

Propositions 4.4 and 4.5 show that in order to give explicit equations in terms of some coordinate system on $\mathbb{P}(L)$ for V_δ with $\delta = \sum_{i=0}^5 d_i X^i$, it suffices to know $C_5^{(1)}$ in terms of the basis of $\hat{L}$ that corresponds to that system and $\hat{m}_X^\circ$ with respect to that basis. Note also that for $\xi = \sum_{i=0}^5 c_i X^i$ we have $\hat{m}_\xi^\circ = \sum_{i=0}^5 c_i (\hat{m}_X^\circ)^i$, so knowing $\hat{m}_X^\circ$ with respect to any basis, we know which linear combination of its powers gives $\hat{m}_\xi^\circ$ with respect to that basis.

We now mention a few bases. The first we have already seen, namely the basis $(1, X, \ldots, X^5)$ of L over k with corresponding dual basis $(p_0, p_1, \ldots, p_5)$. For the second, note that the set $\{\varphi_\omega : \omega \in \Omega\}$ is an unordered basis of $\hat{L}^{\mathrm{s}}$ over k^{s} with $\varphi_\omega \colon L^{\mathrm{s}} \to k^{\mathrm{s}}, X \mapsto \omega$ as before. Set $\overline{P}_\omega = \prod_{\theta \in \Omega \setminus \{\omega\}} (X - \theta)$ and $\lambda_\omega = \overline{P}_\omega(\omega)$. Then $P_\omega = \lambda_\omega^{-1} \overline{P}_\omega$ is the corresponding Lagrange polynomial. We have $\varphi_\omega(P_\theta) = P_\theta(\omega) = \delta_{\omega\theta}$, where $\delta_{\omega\theta}$ is the Kronecker-delta function, which equals 1 if $\omega = \theta$ and 0 otherwise. So $\{P_\omega : \omega \in \Omega\}$ is the unordered basis of L^{s} over k^{s} that is dual to $\{\varphi_\omega : \omega \in \Omega\}$, with P_ω corresponding to φ_ω for all $\omega \in \Omega$. The set $\{\overline{P}_i : \omega \in \Omega\}$ is also an unordered basis of L^{s}, whose dual basis is $\{\overline{\varphi}_\omega : \omega \in \Omega\}$ with $\overline{\varphi}_\omega = \lambda_\omega^{-1} \varphi_\omega$. This gives a third pair of bases. Note that $P_\omega \cdot P_\theta = \delta_{\omega\theta} P_\omega$, so we have a very easy multiplication table for the P_ω.

Proposition 4.6. *In terms of the φ_ω and the $\overline{\varphi}_\omega$ we have*

$$Q_j^{(\delta)} = \sum_\omega \omega^j \lambda_\omega^{-1} \varphi_\omega(\delta) \varphi_\omega^2 = \sum_\omega \omega^j \overline{\varphi}_\omega(\delta) \varphi_\omega^2 = \sum_\omega \omega^j \lambda_\omega \varphi_\omega(\delta) \overline{\varphi}_\omega^2$$

for all integers $j \geq 0$ and all $\delta \in L^*$.

Proof. For any $z \in L$ and $\delta \in L^*$ we have $z = \sum_\omega \phi_\omega(z) P_\omega$ and $\delta = \sum_\omega \phi_\omega(\delta) P_\omega$, so from $P_i \cdot P_j = \delta_{ij} P_i$ we find $\delta X^j z^2 = \sum_\omega \omega^j \phi_\omega(\delta) \phi_\omega(z)^2 P_\omega$. We conclude that for all $z \in L^{\mathrm{s}}$ we have

$$Q_j^{(\delta)}(z) = (\hat{m}_X^\circ)^j (C_5^{(\delta)})(z) = p_5(\delta(X^j z) z) = p_5 \left(\sum_\omega \omega^j \varphi_\omega(\delta) \varphi_\omega(z)^2 P_\omega \right).$$

Since the coefficient of X^5 in P_ω is λ_ω^{-1}, we find $Q_j^{(\delta)} = \sum_\omega \omega^j \lambda_\omega^{-1} \varphi_\omega(\delta) \varphi_\omega^2$. The other expressions follow immediately from $\overline{\varphi}_\omega = \lambda_\omega^{-1} \varphi_\omega$. □

Because multiplication among the P_ω is very easy, and multiplication by X is just multiplication of P_ω by ω for each ω, the equations come out as simple as they do. Unfortunately, the P_ω and corresponding φ_ω are in general not defined over the ground field k. The fourth basis $(g_1, \ldots, g_6)$ with

$$\begin{aligned}
g_1 &= f_1 + f_2 X + f_3 X^2 + f_4 X^3 + f_5 X^4 + f_6 X^5, \\
g_2 &= f_2 + f_3 X + f_4 X^2 + f_5 X^3 + f_6 X^4, \\
g_3 &= f_3 + f_4 X + f_5 X^2 + f_6 X^3, \\
g_4 &= f_4 + f_5 X + f_6 X^2, \\
g_5 &= f_5 + f_6 X, \\
g_6 &= f_6,
\end{aligned}$$

is defined over k. Note that while multiplication by X with respect to the basis $(1, X, \ldots, X^5)$ is given by multiplication from the left by the matrix R of Remark 3.7, with respect to the basis $(g_1, \ldots, g_6)$ it is given by multiplication from the left by the transpose R^{t} of R, or, equivalently, by multiplication from the right by R. Also multiplication among the g_i is given by relatively easy

formulas. Note that the matrix T of Remark 3.7 describes the transformation between the bases $(1, X, \dots, X^5)$ and $(g_1, \dots, g_6)$. Let $(v_1, \dots, v_6)$ be the basis of $\hat{L}$ dual to the basis $(g_1, \dots, g_6)$ of L.

Proposition 4.7. *Take $\delta = \sum_{i=0}^{5} d_i X^i \in L^*$. Then for every integer $j \geq 0$, in terms of $v_1, \dots, v_6$ the quadratic form $f_6^{-1} Q_j^{(\delta)}$ corresponds to the symmetric matrix $\sum_{i=0}^{5} d_i R^{i+j} T$.*

Proof. For every $z \in L^{\mathrm{s}}$ we have $z = \sum_{i=1}^{6} v_i(z) g_i$. Writing z^2 as a linear combination of $1, X, \dots, X^5$, we find that the quadratic form $C_5^{(1)}$ in terms of the v_i corresponds to the symmetric matrix $f_6 T$. As mentioned before, multiplication by X with respect to the basis $(g_1, \dots, g_6)$ corresponds to multipliction by the matrix R from the right. This describes exactly the induced action on the v_i, so we conclude that for all integers $j \geq 0$, with respect to the basis $(v_1, \dots, v_6)$, the quadratic form $(\hat{m}_X^{\circ})^j(C_5^{(1)})$ corresponds to the symmetric matrix $R^j T$. The proposition therefore follows from Proposition 4.5. □

Remark 4.8. *As V_δ is given by $Q_0^{(\delta)} = Q_1^{(\delta)} = Q_2^{(\delta)} = 0$, we only need Proposition 4.7 for $j = 0, 1, 2$ to find equations for V_δ. Therefore, the required exponents of R in R^{i+j} vary from 0 to 7. As mentioned in Remark 3.7, it is worth writing down $R^n T$ for all n with $0 \leq n \leq 7$ to see how simple the equations are.*

Corollary 4.9. *In terms of the coordinates $v_1, \dots, v_6$ of $\mathbb{P}(L)$, the surface V_1 is given by quadratic polynomials that correspond to the symmetric matrices T, RT, and R^2T.*

Proof. The surface V_1 is given by $Q_0^{(1)}$, $Q_1^{(1)}$, and $Q_2^{(1)}$. The corollary therefore follows immediately from Proposition 4.7. □

By Remark 3.7, the surface $\mathcal{Y} \subset \mathbb{P}^5$ is given in terms of the coordinates $b_1, \dots, b_6$ by quadratic forms that correspond to the symmetric matrices T, RT, and R^2T. These are the same matrices as in Corollary 4.9, so $\mathcal{Y}$ and V_1 are isomorphic.

Definition 4.10. *Let $r_{\mathcal{Y}}$ denote the isomorphism $r_{\mathcal{Y}} \colon \mathcal{Y} \to V_1$ given by $[b_1 : \dots : b_6] \mapsto \sum_{i=1}^{6} b_i g_i$, or equivalently, in terms of the coordinate system $v_1, \dots, v_6$, by $v_i = b_i$ for all i, and let $r_J \colon J \dashrightarrow V_1$ denote the composition of $r_{\mathcal{Y}}$ with the rational quotient map $J \dashrightarrow \mathcal{Y}$, so that $r_J(D) = \sum_{i=1}^{6} b_i(D) g_i \in L^{\mathrm{s}}$ (see Proposition 3.6).*

Cassels and the first author [4, Section 16.3] also describe a rational map $J \dashrightarrow V_1$, which sends the class of the divisor $D = \big((x_1, y_1)\big) + \big((x_2, y_2)\big) - K_C$ to the image in $\mathbb{P}(L^{\mathrm{s}})$ of the element $\xi = M(X)(X - x_1)^{-1}(X - x_2)^{-1}$, where $M(X)$ is the unique cubic polynomial such that the curve $y = M(x)$ meets the curve given by $y^2 = f(x)$ twice at (x_1, y_1) and (x_2, y_2). Moreover, if $H(X)$ denotes the quadratic polynomial whose image in L^{s} equals ξ^2, then the roots of $H(x)$ are the x-coordinates of the points R_1, R_2 on C with $2D \sim R_1 + R_2 - K_C$ and in fact we have $\big((y - M(x))/H(x)\big) = 2D - (R_1 + R_2 - K_C)$. The following proposition tells us that this map coincides with r_J.

Proposition 4.11. *Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ be points of C and suppose that they are not Weierstrass points and that $x_1 \neq x_2$. Let $M(X)$ be the unique cubic polynomial such that the curve $y = M(x)$ meets the curve given by $y^2 = f(x)$ twice in P_1 and P_2 and set $\xi = M(X)(X - x_1)^{-1}(X - x_2)^{-1} \in L^{\mathrm{s}}$. Then we have $y_1 y_2 \xi = \sum_{i=1}^{6} b_i(D) g_i$ with $D = [(P_1) + (P_2) - K_C]$.*

Proof. First note that $b_i(D)$ is as given in (3), except that x_1, x_2, y_1, y_2 are now elements of the ground field k^{s}, rather than transcendental elements over k in the function field of $C \times C$. For any distinct $c, d \in k^{\mathrm{s}}$, set

$$g_{c,d}(X) = (c - d)^{-2}(X - c)^2(X - d), \qquad \text{and} \qquad h_{c,d}(X) = (c - d)^{-3}(X - c)^2(2X + c - 3d).$$

Then

$$g_{c,d}(c) = g'_{c,d}(c) = h_{c,d}(c) = h'_{c,d}(c) = g_{c,d}(d) = h'_{c,d}(d) = 0, \qquad g'_{c,d}(d) = h_{c,d}(d) = 1,$$

so the polynomial

$$\tilde{M}(X) = \frac{f'(x_2)}{2y_2} g_{x_1,x_2}(X) + \frac{f'(x_1)}{2y_1} g_{x_2,x_1}(X) + y_2 h_{x_1,x_2}(X) + y_1 h_{x_2,x_1}(X)$$

satisfies $\tilde{M}(x_i) = y_i$ and $\tilde{M}'(x_i) = \frac{f'(x_i)}{2y_i}$ for $i = 1, 2$. From $M(x_i) = y_i$ and $M'(x_i) = \frac{f'(x_i)}{2y_i}$ we find that x_1 and x_2 are distinct double roots of the cubic polynomial $M - \tilde{M}$, and we conclude $M = \tilde{M}$. Note that for any constant $d \in k^{\mathrm{s}}$, the quintic polynomial $(f(X) - f(d))/(X - d)$ equals $\sum_{i=1}^{6} d^{i-1} g_i$. In L^{s} we have $f(X) = 0$, so if $f(d) \neq 0$, then we have

$$\frac{1}{X - d} = -f(d)^{-1} \cdot \frac{f(X) - f(d)}{X - d} = -f(d)^{-1} \sum_{i=1}^{6} d^{i-1} g_i,$$

and thus for any $c \in k^{\mathrm{s}}$ we find

$$\frac{(c-d)^3 h_{c,d}}{(X-c)(X-d)} = 2X - c - d - \frac{(c-d)^2}{X-d} = 2X - c - d + \frac{(c-d)^2}{f(d)} \sum_{i=1}^{6} d^{i-1} g_i.$$

We also have $(c-d)^3 g_{c,d} (X-c)^{-1} (X-d)^{-1} = (c-d)(X-c)$ and may therefore write

$$\begin{aligned} 2(x_1 - x_2)^3 y_1 y_2 \xi &= 2(x_1 - x_2)^3 y_1 y_2 M(X) (X - x_1)^{-1} (X - x_2)^{-1} \\ &= f'(x_2) y_1 (x_1 - x_2)(X - x_1) - f'(x_1) y_2 (x_2 - x_1)(X - x_2) \\ &\quad + 2y_1 y_2 (2X - x_1 - x_2)(y_2 - y_1) \\ &\quad + 2y_1 y_2 \left(y_2 \frac{(x_1 - x_2)^2}{f(x_2)} \sum_{i=1}^{6} x_2^{i-1} g_i - y_1 \frac{(x_1 - x_2)^2}{f(x_1)} \sum_{i=1}^{6} x_1^{i-1} g_i \right). \end{aligned} \tag{12}$$

The last line of (12) is already written as a linear combination of $g_1, \ldots, g_6$. To write the first two lines of the right-hand side of (12) as a linear combination of $g_1, \ldots, g_6$ as well, we use $1 = f_6^{-1} g_6$ and $X = f_6^{-1} g_5 - f_5 f_6^{-1} g_6$. Using $y_i^2 = f(x_i)$, we obtain $y_1 y_2 \xi = \sum_{i=1}^{6} \overline{b}_i g_i$ for

$$\begin{aligned} \overline{b}_i &= \frac{x_2^{i-1} y_1 - x_2^{i-1} y_2}{x_1 - x_2}, \qquad 1 \leq i \leq 4, \\ \overline{b}_5 &= \frac{G(x_1, x_2) y_1 - G(x_2, x_1) y_2}{2 f_6 (x_1 - x_2)^3}, \\ \overline{b}_6 &= \frac{H(x_1, x_2) y_1 - H(x_2, x_1) y_2}{2 f_6^2 (x_1 - x_2)^3}, \end{aligned}$$

with

$$\begin{aligned} G(r, s) &= 2 f_6 (r - s)^2 s^4 + (r - s) f'(s) + 4 f(s), \\ H(r, s) &= 2 f_6^2 s^5 (r - s)^2 - (r - s)(f_5 + f_6 r) f'(s) - 2(2 f_5 + f_6 (r + s)) f(s). \end{aligned}$$

Indeed, from (3) we get $\overline{b}_i = b_i(D)$, which proves the proposition. □

Remark 4.12. *Cassels and the first author* [4] *also show how to make the rational quotient map $J \dashrightarrow \mathcal{Y}$ explicit. However, their formula (16.3.8) is missing a factor $x - u$ and $u - x$ in the terms $-2F(x, X)$ and $-2F(u, X)$ respectively. Here x and u stand for our x_1 and x_2.*

By Propositions 4.4 and 4.6, we have three diagonal quadratic forms in terms of the coordinate system $\{\varphi_\omega\}_\omega$ that describe V_1 over k^{s} and, through $r_{\mathcal{Y}}$, also $\mathcal{Y}$. We could have already given an explicit linear automorphism of $\mathbb{P}^5$ to give these equations for $\mathcal{Y}$ in the previous section, but through the relation between $\mathcal{Y}$ and V_1 it comes more natural.

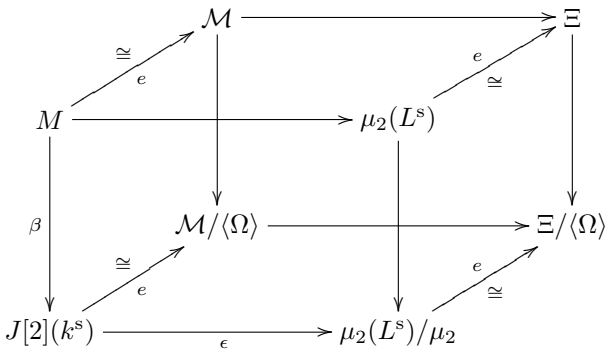
Remark 4.13. *By Corollary 4.3 we have an action of $\mu_2(L^{\mathrm{s}})/\mu_2$ on V_1. Through the injection $\epsilon\colon J[2](k^{\mathrm{s}}) \to \mu_2(L^{\mathrm{s}})/\mu_2$ of Section 2, this induces an action of $J[2](k^{\mathrm{s}})$ on V_1, and thus on $\mathcal{Y}$. On the coordinate system $\{\varphi_\omega\}_\omega$ this action corresponds to negating some of the coordinates, so we have simultaneously diagonalized the action of all two-torsion points on V_1 and $\mathcal{Y}$.*

It is, however, a priori not obvious that this action of $J[2]$ coincides with the action on $\mathcal{Y}$ that is induced by the action on J given by translation, even though it may be hard to imagine any other action by $J[2]$. This is indeed never claimed in [4]*, even though the action is mentioned* [4, Section 16.2]*. In the next section we will see that the actions do coincide.*

5. The action by the two-torsion subgroup

For any $P \in J[2](k^{\mathrm{s}})$ the translation $T_P \in \mathrm{Aut}(J_{k^{\mathrm{s}}})$ commutes with $[-1]$, so it induces automorphisms of $\mathcal{X}$ and $\mathcal{Y}$, both of which we denote by T_P as well. Unless specifically mentioned otherwise, whenever we refer to the action of $J[2](k^{\mathrm{s}})$ on $\mathcal{X}$, $\mathcal{Y}$ or J, we mean this action. In this section we describe the action of $J[2](k^{\mathrm{s}})$ on J in $\mathbb{P}^{15}$ by first analyzing its action on the models of $\mathcal{X}$ in $\mathbb{P}^3$ and $\mathbb{P}^9$ and the model of $\mathcal{Y}$ in $\mathbb{P}^5$. These actions are all linear, induced by actions on the $k(\Omega)$-vector spaces $\mathcal{L}(2(\Theta_+ + \Theta_-))$, $\mathcal{L}(\Theta_+ + \Theta_-)$, $\mathrm{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$, and $\mathcal{L}(2(\Theta_+ + \Theta_-) - \sum_P F_P)$ respectively. As no model is contained in a hyperplane, the actions on these vector spaces are well defined up to a constant.

Purely for notational convenience, we first define some groups isomorphic to the groups in Diagram (1). Let Ξ denote the group of subsets of Ω, where the multiplication is given by taking symmetric differences, i.e., for $I_1, I_2 \subset \Omega$ we have $I_1 \cdot I_2 = (I_1 \cup I_2) \setminus (I_1 \cap I_2)$. The identity element of Ξ is the empty set. To each element $x \in \mu_2(L^{\mathrm{s}}) \cong \bigoplus_\omega \mu_2$ we can associate the set $\{\omega \in \Omega \ : \ \varphi_\omega(x) = -1\}$, which induces an isomorphism $e\colon \mu_2(L^{\mathrm{s}}) \to \Xi$. We have $e(-1) = \Omega$, and multiplication by -1 on $\mu_2(L^{\mathrm{s}})$ corresponds to taking complements. There is an induced isomorphism $e\colon \mu_2(L^{\mathrm{s}})/\mu_2 \to \Xi/\langle\Omega\rangle$ and elements of $\Xi/\langle\Omega\rangle$ can be viewed as partitions of Ω into two subsets. The perfect pairing described in Section 2 corresponds to the pairing $\Xi \times \Xi \to \mu_2$ that sends (I_1, I_2) to $(-1)^r$ with $r = \#(I_1 \cap I_2)$. We denote this pairing by $(I_1, I_2) \mapsto (I_1 : I_2)$. The subgroup $\mathcal{M} = e(M) \subset \Xi$ consist of subsets of even cardinality. The subgroup $e(J[2](k^{\mathrm{s}})) = \mathcal{M}/\langle\Omega\rangle \subset \Xi/\langle\Omega\rangle$ consists of partitions of Ω into two subsets of even cardinality; any nontrivial such partition has a subset of cardinality 2, say $\{\omega_1, \omega_2\}$, and it corresponds to the class of the divisor $\big((\omega_1, 0)\big) + \big((\omega_2, 0)\big) - K_C$. The partitions of Ω into two parts of odd cardinality are contained in $\big(\Xi/\langle\Omega\rangle\big) \setminus \big(\mathcal{M}/\langle\Omega\rangle\big) = (\Xi \setminus \mathcal{M})/\langle\Omega\rangle$, where the last quotient is not a quotient of groups, but a quotient of the set $\Xi \setminus \mathcal{M}$ by the group action induced by multiplication by Ω, i.e., by taking complements. We get the following commutative diagram, cf. Diagram (1).



First we describe the action of $J[2](k^{\mathrm{s}})$ on the model of X in $\mathbb{P}^3$, that is, the action, up to a constant, on $\mathcal{L}(\Theta_+ + \Theta_-)$. Note that saying that $\{\omega_1, \omega_2\}$ is contained in the partition $e(P)$ for $P \in J[2](k^{\mathrm{s}})$ is equivalent to saying that P is nonzero and corresponds to the pair $\{\omega_1, \omega_2\}$, or more precisely, to the class of the divisor $\big((\omega_1, 0)\big) + \big((\omega_2, 0)\big) - K_C$.

Proposition 5.1. *Take $P \in J[2](k^{\mathrm{s}})$ and $\omega_1, \omega_2 \in \Omega$ such that $\{\omega_1, \omega_2\} \in e(P)$. Set $g(x) = (x - \omega_1)(x - \omega_2)$ and $h(x) = f(x)/g(x)$. Write $g = x^2 + g_1 x + g_0$ and $h = h_4 x^4 + h_3 x^3 + \ldots + h_0$. The automorphism T_P on the model of $\mathcal{X} \subset \mathbb{P}^3$ defined by $\mathcal{L}(\Theta_+ + \Theta_-)$ is induced by the linear automorphism $\mathcal{L}(\Theta_+ + \Theta_-)$ defined by $\sum_{i=1}^4 a_i k_i \mapsto \sum_{i=1}^4 a_i' k_i$ with $(a_1'\, a_2'\, a_3'\, a_4') = (a_1\, a_2\, a_3\, a_4) \cdot M_P$*

where

$$M_P = \begin{pmatrix} h_0 + g_0h_2 - g_0^2h_4 & g_0h_3 - g_0g_1h_4 & g_1h_3 - g_1^2h_4 + 2g_0h_4 & 1 \\ -g_0h_1 - g_0g_1h_2 + g_0^2h_3 & h_0 - g_0h_2 + g_0^2h_4 & h_1 - g_1h_2 - g_0h_3 & -g_1 \\ -g_1^2h_0 + 2g_0h_0 + g_0g_1h_1 & -g_1h_0 + g_0h_1 & -h_0 + g_0h_2 + g_0^2h_4 & g_0 \\ M_{4,1} & M_{4,2} & M_{4,3} & M_{4,4} \end{pmatrix},$$

and

$$\begin{aligned} M_{4,1} &= -g_1h_0h_1 + g_1^2h_0h_2 + g_0h_1^2 - 4g_0h_0h_2 - g_0g_1h_1h_2 + g_0g_1h_0h_3 - g_0^2h_1h_3 \\ M_{4,2} &= g_1^2h_0h_3 - g_1^3h_0h_4 - 2g_0h_0h_3 - g_0g_1h_1h_3 + 4g_0g_1h_0h_4 + g_0g_1^2h_1h_4 - 2g_0^2h_1h_4 \\ M_{4,3} &= -g_0h_1h_3 - g_0g_1h_2h_3 + g_0g_1h_1h_4 + g_0g_1^2h_2h_4 + g_0^2h_3^2 - 4g_0^2h_2h_4 - g_0^2g_1h_3h_4 \\ M_{4,4} &= -h_0 - g_0h_2 - g_0^2h_4 \end{aligned}$$

Moreover, we have $\det M_P = \operatorname{Res}(g,h)^2$ *and* $M_P^2 = \operatorname{Res}(g,h) \cdot \mathrm{Id}$*, where* $\operatorname{Res}(g,h)$ *is the resultant of* g *and* h*.*

Proof. See [4, Section 3.2]. □

Remark 5.2. *Note that as* M_P *in Proposition 5.1 is acting from the right on the coefficients with respect to the basis* (k_1, k_2, k_3, k_4)*, it acts from the left on the dual and we can describe the action of* T_P *on* $\mathcal{X} \subset \mathbb{P}^3$ *by* $[k_1 : k_2 : k_3 : k_4] \mapsto [k_1' : k_2' : k_3' : k_4']$ *with* $(k_1'\, k_2'\, k_3'\, k_4')^{\mathrm{t}} = M_P(k_1\, k_2\, k_3\, k_4)^{\mathrm{t}}$*.*

Definition 5.3. *For nonzero* $P \in J[2](k^{\mathrm{s}})$*, let* $T_{4,P}$ *denote the linear automorphism of* $\mathcal{L}(\Theta_+ + \Theta_-)$ *described in Proposition 5.1 and let* $T_{10,P}$ *denote the linear automorphism of* $\operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$ *defined by* $T_{10,P} = (\operatorname{Res}(g,h))^{-1} \operatorname{Sym}^2 T_{4,P}$ *with* g, h *as in Proposition 5.1. Let* $T_{4,0}$ *and* $T_{10,0}$ *denote the identity of* $\mathcal{L}(\Theta_+ + \Theta_-)$ *and* $\operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$ *respectively.*

The integer n in the subscript of $T_{n,P}$ equals the dimension of the vector space on which the automorphism $T_{n,P}$ acts. For any finite-dimensional vector space W of dimension n, let $\mathrm{SL}(W)$ denote the group of linear automorphisms of W with determinant 1, and set $\mathrm{PSL}(W) = \mathrm{SL}(W)/\mu_n$, where $\mu_n \subset \mathrm{SL}(W)$ is the subgroup of scalar automorphisms induced by multiplication by the n-th roots of unity.

Proposition 5.4. *If* $P \in J[2](k^{\mathrm{s}})$ *is nonzero, then* $T_{10,P}$ *has characteristic polynomial* $(\lambda-1)^6(\lambda+1)^4$*, and we have* $T_{10,P} \in \mathrm{SL}(\operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-))$*.*

Proof. Let $r \in k^{\mathrm{s}}$ satisfy $r^2 = \operatorname{Res}(g,h)$ with g, h as in Proposition 5.1. From Proposition 5.1 we conclude that the four eigenvalues $\lambda_1, \ldots, \lambda_4$ of $T_{4,P}$ satisfy $\lambda_i^2 = \operatorname{Res}(g,h) = r^2$. Not all eigenvalues are the same, as otherwise the action of T_P on $\mathcal{X} \subset \mathbb{P}^3$ would be trivial. From $\prod_i \lambda_i = \det T_{4,P} = r^4$ we conclude that the characteristic polynomial of $T_{4,P}$ equals $(\lambda^2 - r^2)^2$. Standard formulas imply that the characteristic polynomial of $T_{10,P} = r^{-2} \operatorname{Sym}^2 T_{4,P}$ is as claimed. It then also follows that the determinant equals 1. □

Proposition 5.5. *Let* $P \in J[2](k^{\mathrm{s}})$ *be any point. The automorphism* T_P *on the model of* $\mathcal{X} \subset \mathbb{P}^9$ *defined by* $\operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$ *is induced by the linear automorphism* $T_{10,P}$ *of* $\operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$*.*

Proof. For $P = 0$ this is trivial. Suppose P is nonzero. The model of $\mathcal{X}$ in $\mathbb{P}^9$ is the 2-uple embedding of its model in $\mathbb{P}^3$, so the first statement follows from Proposition 5.1, as $T_{10,P}$ equals $\operatorname{Sym}^2 T_{4,P}$ up to a constant. □

Definition 5.6. *Let* $\alpha\colon M \to \mu_2$ *be the function given by* $\alpha(m) = (-1)^r$*, where* $2r$ *is the number of* $\omega \in \Omega$ *with* $\varphi_\omega(m) = -1$*.*

Note that for all $m, m' \in M$ we have

$$e_W\big(\beta(m), \beta(m')\big) = \alpha(mm')\alpha(m)\alpha(m') \tag{13}$$

where e_W is the Weil pairing, as before.

Remark 5.7. *Michael Stoll ([27]) defines the group T' to be the group on the set $\mu_2 \times J[2](k^{\mathrm{s}})$ with multiplication given by*

$$\big(\alpha_1, P_1\big) \cdot \big(\alpha_2, P_2\big) = \big(\alpha_1\alpha_2 e_W(P_1, P_2), P_1 + P_2\big)$$

where e_W is the Weil pairing. It follows from (13) that the map $M \to T'$, $m \mapsto (\alpha(m), \beta(m))$ is an isomorphism.

Let $\rho_{10}\colon M \to \mathrm{SL}\big(\mathrm{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)\big)$ be the function given by $\rho_{10}(m) = \alpha(m)T_{10,\beta(m)}$.

Proposition 5.8. *The function ρ_{10} is a representation of M.*

Proof. For any $P, Q \in J[2](k^{\mathrm{s}})$ there is a constant $c(P,Q)$, given explicitly in [4, Section 3.3], such that $T_{4,P}T_{4,Q} = c(P,Q)T_{4,P+Q}$. As also noted in [27, Section 4], these constants are such that for all $P, Q \in J[2](k^{\mathrm{s}})$ we have $T_{10,P}T_{10,Q} = e_W(P,Q)T_{10,P+Q}$. We conclude that there is a representation $T' \to \mathrm{SL}\big(\mathrm{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)\big)$ given by $(\alpha, P) \mapsto \alpha T_{10,P}$, where T' is as in Remark 5.7. The function ρ_{10} is the composition of this representation and the homomorphism $M \to T'$ of Remark 5.7, so it is a representation as well. □

Remark 3.8 contains explicit equations for the morphism $\mathcal{Y} \to \mathcal{X}$ and its birational inverse. Together with Proposition 5.1 this allows us to construct explicit equations for the action of $J[2]$ on the model of $\mathcal{Y}$ in $\mathbb{P}^5(b_1, \ldots, b_6)$. These equations are too large to include here. From the corresponding action on the coordinate system $\{\varphi_\omega\}_\omega$, however, one would be able to see that the action is induced by the action of $\mu_2(L^{\mathrm{s}})/\mu_2$ on $V_1 \subset \mathbb{P}(L^{\mathrm{s}})$ through the inclusion $\epsilon\colon J[2](k^{\mathrm{s}}) \to \mu_2(L^{\mathrm{s}})/\mu_2$, cf. Remark 4.13. In Proposition 5.10 we prove this without heavy computations, using Section 4 instead of Proposition 5.1.

The isomorphism $r_{\mathcal{Y}}\colon \mathcal{Y} \to V_1$ given by $v_i \mapsto b_i$ of Definition 4.10 induces an isomorphism

$$r_{\mathcal{Y}}^*\colon \hat{L}^{\mathrm{s}} \to \mathcal{L}\left(2(\Theta_+ + \Theta_-) - \sum_P F_P\right),$$

defined over k. The natural action of $M \subset \mu_2(L^{\mathrm{s}})$ on $\hat{L}^{\mathrm{s}}$ is given by $M \to \mathrm{Aut}(\hat{L}^{\mathrm{s}})$, $a \mapsto \hat{m}_a$ as in Section 4. The determinant of $\hat{m}_a$ equals the norm $N_{L^{\mathrm{s}}/k^{\mathrm{s}}}(a) = 1$ for $a \in M$. This yields an injective representation

$$\rho_6\colon M \hookrightarrow \mathrm{SL}\left(\mathcal{L}\left(2(\Theta_+ + \Theta_-) - \sum_P F_P\right)\right), \quad a \mapsto r_{\mathcal{Y}}^* \circ \hat{m}_a \circ (r_{\mathcal{Y}}^*)^{-1}.$$

Proposition 5.9. *For any $a \in M$ the eigenvalues of $\rho_6(a)$ are $(\varphi_\omega(a))_{\omega\in\Omega}$. For $a \neq \pm 1$ the characteristic polynomial equals $\big(\lambda + \alpha(a)\big)^4\big(\lambda - \alpha(a)\big)^2$.*

Proof. For each $\omega \in \Omega$ the element $\varphi_\omega \in \hat{L}^{\mathrm{s}}$ is an eigenvector of $\hat{m}_a$ with eigenvalue $\varphi_\omega(a) \in \mu_2$. The eigenvalues of $\rho_6(a)$ are the same as those of $\hat{m}_a$. Suppose that $a \neq \pm 1$; exactly four of the eigenvalues equal -1 if and only if $\alpha(a) = 1$, otherwise exactly two of the eigenvalues equal -1. It follows that the characteristic polynomial is as claimed. □

Proposition 5.10. *For any $a \in M$ the automorphism $T_{\beta(a)}$ on the model of $\mathcal{Y} \subset \mathbb{P}^5$ defined by $\mathcal{L}(2(\Theta_+ + \Theta_-) - \sum_P F_P)$ is induced by $\rho_6(a) \in \mathrm{Aut}\,\mathcal{L}(2(\Theta_+ + \Theta_-) - \sum_P F_P)$.*

Proof. Take $S \in J[2](k^{\mathrm{s}})$, and let $D \in J(k^{\mathrm{s}}) \setminus J[2](k^{\mathrm{s}})$ be represented by the divisor $P_1 + P_2 - K_C$. Write $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ and suppose that P_1, P_2 are not Weierstrass points and that $x_1 \neq x_2$. Let $M_D(X)$ be the unique cubic polynomial such that the curve $y = M_D(x)$ meets the curve given by $y^2 = f(x)$ twice in P_1 and P_2 and set $\xi_D = M_D(X)(X - x_1)^{-1}(X - x_2)^{-1} \in L^{\mathrm{s}}$, where, by the usual abuse of notation, $M_D(X)$ refers to both the polynomial and its image in L^{s}. Let $H_D(X)$ be the quadratic polynomial whose image in L^{s} equals ξ_D^2. By the remark before Proposition 4.11, the roots of $H_D(x)$ are the x-coordinates of the points R_1, R_2 with $[(R_1) + (R_2) - K_C] = 2D$. Since $2D = 2(D + S)$, the polynomials H_D and H_{D+S} have the same roots, so ξ_{D+S}^2 and ξ_D^2 differ by a constant factor. If D is general enough, then ξ_D and ξ_{D+S} are invertible in L^{s}; it follows that ξ_{D+S}/ξ_D is contained in the subset $k^{\mathrm{s}*} \cdot \mu_2(L^{\mathrm{s}})$ of $L^{\mathrm{s}*}$, and its image in $L^{\mathrm{s}*}/k^{\mathrm{s}*}$ is therefore

contained in $\mu_2(L^{\mathrm{s}})/\mu_2$. We obtain a rational map $J \dashrightarrow \mu_2(L^{\mathrm{s}})/\mu_2, D \mapsto \xi_{D+S}/\xi_D \in L^{\mathrm{s}*}/k^{\mathrm{s}*}$, depending on S. Since $\mu_2(L^{\mathrm{s}})/\mu_2$ is discrete and J is connected, this map is constant with image $\{\zeta_S\}$. Let $\zeta_k\colon J[2](k^{\mathrm{s}}) \to \mu_2(L^{\mathrm{s}})/\mu_2$ be the map defined by $\zeta_k(S) = \zeta_S$. From the equalities

$$\zeta_{S+S'} = \frac{\xi_{D+S+S'}}{\xi_D} = \frac{\xi_{D+S+S'}}{\xi_{D+S}} \cdot \frac{\xi_{D+S}}{\xi_D} = \zeta_{S'} \cdot \zeta_S$$

we find that ζ_k is a homomorphism. By Proposition 4.11 the map r_J of Definition 4.10 sends D to the image of ξ_D in $\mathbb{P}(L^{\mathrm{s}})$. Suppose $S \neq 0$. Then for general D we have $D + S \neq \pm D$, so $r_J(D) \neq r_J(D + S)$, and therefore $\zeta_S = \xi_{D+S}/\xi_D \neq 1$ in $L^{\mathrm{s}*}/k^{\mathrm{s}*}$. We conclude that ζ_k is a Galois-equivariant injective homomorphism. We now show that ζ_k coincides with ϵ.

Consider the field $E = k(W_1, \ldots, W_6, F_6)$, where W_1, …, W_6, F_6 are independent transcendental elements over k, let $K \subset E$ be the field generated by the coefficients of the polynomial $F(X) = F_6 \prod_i (X - W_i)$ in X, and set $\Lambda^{\mathrm{s}} = K^{\mathrm{s}}[X]/(F(X))$. Thus $\operatorname{Spec}(K)$ is the generic point of the space of polynomials over k of degree 6 and E is a splitting field over K of the universal polynomial F. Let $\mathcal{J}$ be the Jacobian of the universal curve given by $y^2 = F(x)$. Apply the argument above with k, f, and L^{s} replaced by K, F, and Λ^{s} respectively to obtain a Galois-equivariant injective homomorphism $\zeta_K\colon \mathcal{J}[2](K^{\mathrm{s}}) \to \mu_2(\Lambda^{\mathrm{s}})/\mu_2$, and let $\epsilon_K\colon \mathcal{J}[2](K^{\mathrm{s}}) \to \mu_2(\Lambda^{\mathrm{s}})/\mu_2$ be the analogue of ϵ. The Galois group $\mathrm{Gal}(E/K)$ is isomorphic to the permutation group $\mathfrak{S}_6$ acting on $\{W_1, \ldots, W_6\}$. Let $Q \in \mathcal{J}[2](K^{\mathrm{s}})$ be non-zero, represented by the pair $\{W_i, W_j\}$, and identify $\mu_2(\Lambda^{\mathrm{s}})/\mu_2$ with the group of partitions of $\{W_1, \ldots, W_6\}$ into two subsets. Since ζ_K is Galois-equivariant, the element $\zeta_K(Q)$ is identified with a partition fixed by the stabilizer of the pair $\{W_i, W_j\}$. The element $\zeta_K(Q)$ is non-trivial because ζ_K is injective, so it follows that $\zeta_K(Q) \ni \{W_i, W_j\}$ and thus $\zeta_K(Q) = \epsilon_K(Q)$. We conclude that ζ_K coincides with ϵ_K on the generic point $\operatorname{Spec}(K)$. Therefore, the analogous homomorphisms coincide on a Zariski dense open set of the space of polynomials over k. By continuity, ζ_k and ϵ coincide as well.

We conclude that in $(L^{\mathrm{s}} \setminus \{0\})/k^{\mathrm{s}*}$ we have $\xi_{D+S} = \epsilon(S) \cdot \xi_D$ for all $S \in J[2](k^{\mathrm{s}})$ and all D in a dense open subset of J. Take any $a \in M$. For $a = \pm 1$ the statement is trivial, so we assume $a \neq \pm 1$ and set $P = \beta(a)$, so $P \neq 0$. The image of a in $\mu_2(L^{\mathrm{s}})/\mu_2$ is $\epsilon(\beta(a)) = \epsilon(P)$, so identifying $\mathbb{P}(L^{\mathrm{s}})$ with $(L^{\mathrm{s}} \setminus \{0\})/k^{\mathrm{s}*}$, we find

$$r_J(T_P(D)) = \xi_{D+P} = \epsilon(P)\xi_D = a \cdot \xi_D = m_a(\xi_D) = m_a(r_J(D))$$

in $(L^{\mathrm{s}} \setminus \{0\})/k^{\mathrm{s}*}$ for all $D \in J$. Hence the automorphism of V_1 induced by the action of T_P on J is induced by $\hat{m}_a \in \operatorname{Aut} \hat{L}^{\mathrm{s}}$. Since r_J is the composition of the rational quotient map $J \dashrightarrow \mathcal{Y}$ and the isomorphism $r_{\mathcal{Y}}\colon \mathcal{Y} \to V_1$, conjugation by $r_{\mathcal{Y}}$ and $r_{\mathcal{Y}}^*$ concludes the proof. □

Recall that $\mathcal{L}(2(\Theta_+ + \Theta_-) - \sum_P F_P)$ and $\operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$ can be viewed as subspaces of $\mathcal{L}(2(\Theta_+ + \Theta_-))$ (Propositions 3.2 and 3.6 and Remark 3.4) and we have

$$\mathcal{L}(2(\Theta_+ + \Theta_-)) \cong \mathcal{L}\big(2(\Theta_+ + \Theta_-) - \sum_P F_P\big) \oplus \operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-). \tag{14}$$

For convenience, we abbreviate $\mathcal{L}(2(\Theta_+ + \Theta_-))$ by $\mathcal{L}$ from now on. Let $\rho\colon M \to \mathrm{SL}(\mathcal{L})$ be the representation $\rho = \rho_6 \oplus \rho_{10}$.

Proposition 5.11. *For all $m \in M$ the automorphism $\rho(m)$ of $\mathcal{L}$ induces the automorphism $T_{\beta(m)}$ on $J \subset \mathbb{P}^{15}$.*

Proof. First we show that there is a function $\chi\colon M \to k^{\mathrm{s}*}$ such that for all $m \in M$ the automorphism $\rho_6(m) \oplus \chi(m) \cdot \rho_{10}(m)$ of $\mathcal{L}(2(\Theta_+ + \Theta_-))$ induces the automorphism $T_{\beta(m)}$ on $J \subset \mathbb{P}^{15}$. For $m = \pm 1$ we have $\beta(m) = 0 \in J[2](k^{\mathrm{s}})$, while $\rho_6(m) = m \cdot \mathrm{Id}$ and $\rho_{10}(m) = m \cdot \mathrm{Id}$, so we set $\chi(\pm 1) = 1$. Assume $m \neq \pm 1$. The action of T_P on J is linear, so it is induced by a linear automorphism $\mathcal{T}$ of $\mathcal{L}(2(\Theta_+ + \Theta_-))$. Since multiplication by -1 on J commutes with translation by two-torsion points, the induced action of T_P^* on the function field sends even functions to even functions and odd functions to odd functions. We conclude that $\mathcal{T}$ induces linear transformations of the subspace $\operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$ of even functions and of the subspace $\mathcal{L}(2(\Theta_+ + \Theta_-) - \sum_P F_P)$ of odd functions. These linear transformations induce the action of T_P on $\mathcal{X} \subset \mathbb{P}^9$ and $\mathcal{Y} \subset \mathbb{P}^5$

respectively, so up to constants they coincide with $\rho_{10}(m)$ and $\rho_6(m)$ respectively by Propositions 5.5 and 5.10. We conclude that there are $c, d \in k^{s*}$ such that $\mathcal{T} = d \cdot \rho_6(m) \oplus c \cdot \rho_{10}(m)$. After rescaling $\mathcal{T}$ we may assume $d = 1$, so there is a c such that $\mathcal{T} = \rho_6(m) \oplus c \cdot \rho_{10}(m)$ induces T_P. Set $\chi(m) = c$; this shows the existence of the function χ as claimed. Note that for all $m, m' \in M$, both

$$(\rho_6(m) \oplus \chi(m)\rho_{10}(m)) \cdot (\rho_6(m') \oplus \chi(m')\rho_{10}(m')) = \rho_6(mm') \oplus \chi(m)\chi(m')\rho_{10}(mm')$$

and $\rho_6(mm') \oplus \chi(mm')\rho_{10}(mm')$ induce $T_{\beta(mm')}$. It follows that we have $\chi(m)\chi(m') = \chi(mm')$, so χ is a representation. Since χ is 1-dimensional, it corresponds to an element of $\mathrm{Hom}(M, \mu_2) \cong \mu_2(L^s)/\mu_2$.

Set $\tau = \rho_6 \oplus (\chi \cdot \rho_{10})$, so that for each $m \in M$ the automorphism $T_{\beta(m)}$ on J is induced by $\tau(m)$. Note that ρ_6 and ρ_{10} are $\mathrm{Gal}(k(\Omega)/k)$-equivariant. For each $\sigma \in \mathrm{Gal}(k(\Omega)/k)$ and $m \in M$ the automorphism $\sigma(T_{\beta(m)}) = T_{\beta(\sigma(m))}$ is induced by both $\sigma(\tau(m))$ and $\tau(\sigma(m))$, so τ is also $\mathrm{Gal}(k(\Omega)/k)$-equivariant, and therefore χ is as well. If $\mathrm{Gal}(k(\Omega)/k)$ is isomorphic to the full permutation group $\mathfrak{S}_6$, then this implies that χ is constant, and thus trivial. As in the proof of Proposition 5.10, this is the case at the generic point of the space of polynomials over k of degree 6, therefore on a Zariski dense open subset of this space, and thus, by continuity, on the entire space. It follows that we have $\tau = \rho$ and we are done. □

Since M is abelian of exponent 2, its only irreducible representations are characters into μ_2. We have already seen in Section 2 that the character group $\mathrm{Hom}(M, \mu_2)$ is isomorphic to $\mu_2(L^s)/\mu_2$. Therefore, over k^s the representation ρ is the direct sum of 16 characters, corresponding to elements in $\mu_2(L^s)/\mu_2$. In characteristic 0, standard computations allow us to decide which characters exactly. In positive characteristic the same works, as long as we lift the characters to modular characters in characteristic 0, cf. [23, Chapter 18].

Proposition 5.12. *The representation $\rho\colon M \to \mathrm{SL}(\mathcal{L})$ is the direct sum of all characters of M that are not contained in $\epsilon(J[2](k^s))$, i.e., of all characters corresponding to the partitions of Ω into two parts of odd size. The subrepresentation ρ_6 is the direct sum of characters corresponding to partitions where one part consists of a single element. The subrepresentation ρ_{10} is the direct sum of characters corresponding to partitions into two parts of size* 3.

Proof. For any $m \in M$ with $m \neq \pm 1$, the characteristic polynomial of $\rho_{10}(m)$ equals $(\lambda - \alpha(m))^6(\lambda + \alpha(m))^4$ by Proposition 5.4. We find that the character χ_{10}, in case of characteristic 0, or the modular character χ_{10} associated to ρ as in [23, Chapter 18], in case of positive characteristic, is given by

$$\chi_{10}(m) = \begin{cases} 10\alpha(m) & \text{if } m = \pm 1, \\ 2\alpha(m) & \text{if } m \neq \pm 1. \end{cases}$$

Let τ be the direct sum of all ten characters of M in $\mu_2(L^s)/\mu_2$ that are associated to partitions of Ω into two parts of size 3. The (modular) character associated to τ is equal to χ_{10}. In characteristic 0, a representation of a finite group is determined up to isomorphism by its character, so we find that ρ and τ are isomorphic. In characteristic $p > 0$, a semisimple representation of a finite group whose order is not a multiple of p is determined up to isomorphism by its modular character by Brauer's Theorem (see [23, Section 18.2, Theorem 42, Corollary 1]). The representation ρ_{10} is semisimple because M is a finite 2-group and the characteristic of k is different from 2, so we conclude that ρ_{10} and τ are isomorphic in positive characteristic as well. Similarly, the (modular) character χ_6 associated to ρ_6 is given by

$$\chi_6(m) = \begin{cases} 6\alpha(m) & \text{if } m = \pm 1, \\ -2\alpha(m) & \text{if } m \neq \pm 1, \end{cases}$$

from which we deduce that ρ_6 is isomorphic to the direct sum of characters of M corresponding to partitions where one part consists of a single element. From $\rho = \rho_6 \oplus \rho_{10}$ we conclude that ρ is isomorphic to the direct sum of all characters corresponding to partitions into two odd parts. These are exactly the characters of M that are not contained in $\epsilon(J[2](k^s))$. □

Remark 5.13. *The argument for characteristic* 0 *in the proof of the statement of Proposition 5.12 about* ρ_{10} *is from Michael Stoll* [27, Section 4]. *Michael Stoll deduces the result for positive characteristic from an explicit computation that we also perform in the next section.*

6. Diagonalizing the action by the two-torsion subgroup

By Proposition 5.12, the representation $\rho\colon M \hookrightarrow \mathrm{SL}(\mathcal{L})$ is the direct sum of all characters of M that are not contained in $\epsilon(J[2](k^{\mathrm{s}}))$, i.e., the characters χ with $\chi(-1) = -1$. These characters correspond to partitions of Ω into two parts of odd size. Generically there are two Galois orbits, one consisting of ten partitions into parts of size 3, and one of six partitions of which one part contains only a single element. In this section we find an explicit Galois-invariant basis for $\mathcal{L}$ with each basis element corresponding to a character of M, so that the action of M on $\mathcal{L}$ is diagonal with respect to this basis.

Note that $\mathrm{Sym}(\mathcal{L})$ is the homogeneous coordinate ring of $\mathbb{P}(\hat{\mathcal{L}})$. For any nonnegative integer d, the vector space $\mathrm{Sym}^d \mathcal{L}$ is generated by all elements $g_1 * g_2 * \cdots * g_d$ with $g_1, g_2, \ldots, g_d \in \mathcal{L}$ (for notation see the comment before Remark 3.4). The action of $[-1]^*$ on $\mathcal{L}$, mapping $g(x)$ to $g(-x)$, induces an action on $\mathrm{Sym}(\mathcal{L})$ and we call $g \in \mathrm{Sym}(\mathcal{L})$ even or odd if $[-1]^*$ fixes or negates g respectively.

For each character $\chi \in \mu_2(L^{\mathrm{s}})/\mu_2$ of M with $\chi(-1) = -1$, choose a function $c_\chi \in \mathcal{L}$ so that ρ coincides on the space generated by c_χ with the character χ. Until we make explicit choices, in Definitions 6.10 and 6.12, we state some results that do not depend on these choices. By Proposition 5.12 such c_χ exist, are well defined up to a scalar, and form a basis of $\mathcal{L}$. If π is the partition of Ω into two parts of odd size corresponding to χ, then we also write $c_\pi = c_\chi$. We endow the coordinate ring $\mathrm{Sym}(\mathcal{L})$ with a $\mu_2(L^{\mathrm{s}})/\mu_2$-grading where the weight of c_χ is χ. The grading does not depend on the choice of the c_χ. For $\chi \in \mu_2(L^{\mathrm{s}})/\mu_2$, we let $(\mathrm{Sym}(\mathcal{L}))_\chi$ denote the subspace of homogeneous elements of weight χ; for any positive integer d, we set $\mathcal{L}_\chi^{(d)} = (\mathrm{Sym}(\mathcal{L}))_\chi \cap \mathrm{Sym}^d \mathcal{L}$, and we let $\mathcal{L}_{\chi,+}^{(d)}$ and $\mathcal{L}_{\chi,-}^{(d)}$ denote the subspaces of $\mathcal{L}_\chi^{(d)}$ of even and odd elements respectively.

Proposition 6.1. *For any* $\chi \in \mu_2(L^{\mathrm{s}})/\mu_2$ *and any nonnegative integer* d *we have decompositions* $\mathcal{L}_\chi^{(d)} \cong \mathcal{L}_{\chi,+}^{(d)} \oplus \mathcal{L}_{\chi,-}^{(d)}$ *and*

$$\mathrm{Sym}^d \mathcal{L} \cong \bigoplus_{\chi \in \mu_2(L^{\mathrm{s}})/\mu_2} \mathcal{L}_\chi^{(d)} \cong \bigoplus_{\chi \in \mu_2(L^{\mathrm{s}})/\mu_2} \left(\mathcal{L}_{\chi,+}^{(d)} \oplus \mathcal{L}_{\chi,-}^{(d)}\right).$$

Proof. The monomials of degree d in $\{c_\chi\}_{\chi \in \mu_2(L^{\mathrm{s}})/\mu_2}$ form an unordered basis of $\mathrm{Sym}^d \mathcal{L}$ as a k-vector space. By Proposition 5.12 these monomials are eigenfunctions for $[-1]^*$. It is also clear that all these monomials are homogeneous with respect to the grading by $\mu_2(L^{\mathrm{s}})/\mu_2$, so the various decompositions follow. □

Proposition 6.2. *For any* $\chi \in \mu_2(L^{\mathrm{s}})/\mu_2$ *and any nonnegative integer* d*, the representation* $\mathrm{Sym}^d \rho\colon M \to \mathrm{GL}(\mathrm{Sym}^d \mathcal{L})$ *acts as multiplication by* χ *on the subspace* $\mathcal{L}_\chi^{(d)} \subset \mathrm{Sym}^d \mathcal{L}$*, i.e., for each* $m \in M$ *and each* $x \in \mathcal{L}_\chi^{(d)}$ *we have* $(\mathrm{Sym}^d \rho)(m)(x) = \chi(m) \cdot x$.

Proof. By definition, the space $\mathcal{L}_\chi^{(d)}$ is generated by elements $g = g_1 * g_2 * \cdots * g_d$ with g_i of degree χ_i for some $\chi_i \in \mu_2(L^{\mathrm{s}})/\mu_2$ and $\prod_{i=1}^d \chi_i = \chi$. For any $m \in M$ we then have

$$\begin{aligned}(\mathrm{Sym}^d \rho)(m)(g) &= \rho(m)(g_1) * \cdots * \rho(m)(g_d) = \chi_1(m) g_1 * \cdots * \chi_d(m) g_d \\ &= (\chi_1(m) \cdots \chi_d(m)) \cdot (g_1 * \cdots * g_d) = \chi(m) \cdot g.\end{aligned}$$

It follows that we have $(\mathrm{Sym}^d \rho)(m)(x) = \chi(m) \cdot x$, for all $x \in \mathcal{L}_\chi^{(d)}$ and $m \in M$. □

Proposition 6.3. *The representation* $\mathrm{Sym}^2 \rho\colon M \to \mathrm{GL}(\mathrm{Sym}^2 \mathcal{L})$ *has kernel* μ_2 *and induces a representation from the quotient* $M/\mu_2 \cong J[2](k^{\mathrm{s}})$ *to* $\mathrm{SL}(\mathrm{Sym}^2 \mathcal{L})$.

Proof. For any $m \neq \pm 1$ the characteristic polynomial of $\rho(m)$ equals $(\lambda^2 - 1)^8$ by Propositions 5.4 and 5.9. It follows that $\mathrm{Sym}^2 \rho(m)$ has 64 of its eigenvalues equal to -1 and 72 of them equal to 1, so $\det \mathrm{Sym}^2 \rho(m) = 1$ and we find $\mathrm{Sym}^2 \rho(m) \in \mathrm{SL}(\mathrm{Sym}^2 \mathcal{L})$. By Proposition 5.12, the representation

ρ is the direct sum of characters χ of M not contained in $\epsilon(J[2](k^{\mathrm{s}}))$. For any two such characters χ_1, χ_2 we have $(\chi_1 \otimes \chi_2)(-1) = \chi_1(-1) \cdot \chi_2(-1) = (-1)^2 = 1$. This implies $(\rho \otimes \rho)(-1) = \mathrm{Id}$, so μ_2 is contained in the kernel of $\rho \otimes \rho \colon M \to \mathcal{L} \otimes \mathcal{L}$ and therefore also in the kernel of the subrepresentation $\mathrm{Sym}^2 \rho$. Therefore, $\mathrm{Sym}^2 \rho$ induces a representation $\rho^{(2)} \colon J[2](k^{\mathrm{s}}) \to \mathrm{SL}(\mathrm{Sym}^2 \mathcal{L})$. □

Definition 6.4. *Let $\rho^{(2)}$ denote the representation $J[2](k^{\mathrm{s}}) \to \mathrm{SL}(\mathrm{Sym}^2 \mathcal{L})$ induced by $\mathrm{Sym}^2 \rho$.*

Definition 6.5. *For $P \in J[2](k^{\mathrm{s}})$ we set $\mathcal{L}^{(2)}_P = \mathcal{L}^{(2)}_{\epsilon(P)}$ and $\mathcal{L}^{(2)}_{P,\pm} = \mathcal{L}^{(2)}_{\epsilon(P),\pm}$ with ϵ as in Section 2.*

Recall that $J[2](k^{\mathrm{s}})$ is self-dual through the perfect pairing $J[2](k^{\mathrm{s}}) \times J[2](k^{\mathrm{s}}) \to \mu_2$ described in Section 2, which coincides with the Weil pairing. For each $P \in J[2](k^{\mathrm{s}})$, let $\chi_P \colon J[2](k^{\mathrm{s}}) \to \mu_2$ denote the corresponding character.

Proposition 6.6. *For $P \in J[2](k^{\mathrm{s}})$, the representation $\rho^{(2)} \colon J[2](k^{\mathrm{s}}) \to \mathrm{SL}(\mathrm{Sym}^2 \mathcal{L})$ acts as multiplication by χ_P on the subspace $\mathcal{L}^{(2)}_P \subset \mathrm{Sym}^2 \mathcal{L}$, i.e., for each $R \in J[2](k^{\mathrm{s}})$ and each $x \in \mathcal{L}^{(2)}_P$ we have $\rho^{(2)}(R)(x) = \chi_P(R) \cdot x$.*

Proof. The representations $\mathrm{Sym}^2 \rho \colon M \to \mathrm{GL}(\mathrm{Sym}^2 \mathcal{L})$ and $\rho^{(2)} \colon J[2](k^{\mathrm{s}}) \to \mathrm{SL}(\mathrm{Sym}^2 \mathcal{L})$ are related by $\mathrm{Sym}^2 \rho = \rho^{(2)} \circ \beta$ according to Proposition 6.3, with $\beta \colon M \to J[2](k^{\mathrm{s}})$ as in Section 2. Take $P \in J[2](k^{\mathrm{s}})$. The character $\epsilon(P) \in \mu_2(L^{\mathrm{s}})/\mu_2$ of M equals $\chi_P \circ \beta$. For any $g \in \mathcal{L}^{(2)}_P$ and any $R \in J[2](k^{\mathrm{s}})$ we choose $m \in M$ such that $\beta(m) = R$ and we find

$$\rho^{(2)}(R)(x) = \rho^{(2)}(\beta(m))(x) = (\mathrm{Sym}^2 \rho)(m)(x) = (\epsilon(P))(m) \cdot x = \chi_P(\beta(m)) \cdot x = \chi_P(R) \cdot x.$$

This proves the proposition. □

Proposition 6.7. *The spaces $\mathcal{L}^{(2)}_{P,\pm}$ are $\rho^{(2)}$-invariant and we have*

$$\mathrm{Sym}^2 \mathcal{L} \cong \bigoplus_{P \in J[2]} \left(\mathcal{L}^{(2)}_{P,+} \oplus \mathcal{L}^{(2)}_{P,-} \right).$$

We have $\dim \mathcal{L}^{(2)}_{o,+} = 16$, $\dim \mathcal{L}^{(2)}_{o,-} = 0$ and $\dim \mathcal{L}^{(2)}_{P,+} = \dim \mathcal{L}^{(2)}_{P,-} = 4$ for nonzero $P \in J[2]$. Furthermore, $\mathcal{L}^{(2)}_{o,+}$ is generated by $\{c_\pi * c_\pi\}_\pi$. For nonzero $P \in J[2](k^{\mathrm{s}})$, corresponding to the pair $\{\omega_1, \omega_2\}$, the spaces $\mathcal{L}^{(2)}_{P,+}$ and $\mathcal{L}^{(2)}_{P,-}$ are generated by

$$\{c_{\omega_1} * c_{\omega_2}\} \cup \{c_{\theta_1\theta_2\omega_1} * c_{\theta_1\theta_2\omega_2} \ : \ \theta_1, \theta_2 \in \Omega \setminus \{\omega_1, \omega_2\},\ \theta_1 \neq \theta_2\}$$

and

$$\{c_\theta * c_{\omega_1\omega_2\theta} \ : \ \theta \in \Omega \setminus \{\omega_1, \omega_2\}\}$$

respectively, where in the subscript of c_π the partition π is abbreviated by the list of elements in one of the two parts.

Proof. The spaces $\mathcal{L}^{(2)}_{P,\pm}$ are $\rho^{(2)}$-invariant by Proposition 6.6. The $\mu_2(L^{\mathrm{s}})/\mu_2$-grading on $\mathrm{Sym}(\mathcal{L})$ takes values on $\mathcal{L}$ that are all outside $\epsilon(J[2](k^{\mathrm{s}}))$. The product of any two such elements is contained in $\epsilon(J[2](k^{\mathrm{s}}))$, so for any $\chi \in \mu_2(L^{\mathrm{s}})/\mu_2$ with $\chi \notin \epsilon(J[2](k^{\mathrm{s}}))$ we have $\mathcal{L}^{(2)}_\chi = 0$. From Proposition 6.1 we conclude

$$\mathrm{Sym}^2 \mathcal{L} \cong \bigoplus_{\chi \in \epsilon(J[2](k^{\mathrm{s}}))} \mathcal{L}^{(2)}_\chi = \bigoplus_{P \in J[2](k^{\mathrm{s}})} \mathcal{L}^{(2)}_P \cong \bigoplus_{P \in J[2](k^{\mathrm{s}})} \left(\mathcal{L}^{(2)}_{P,+} \oplus \mathcal{L}^{(2)}_{P,-} \right).$$

We identify $\mu_2(L^{\mathrm{s}})/\mu_2$ with the group of partitions of Ω into two parts, and $J[2](k^{\mathrm{s}})$ with the subgroup of partitions into parts of even size. For any partitions π, π' into odd parts the weight in $\mu_2(L^{\mathrm{s}})/\mu_2$ of the monomial $c_\pi * c_{\pi'}$ is the weight associated to the partition $\pi \cdot \pi'$, where the multiplication $\pi \cdot \pi'$ is induced by the multiplication in the group Ξ of subsets of Ω, namely by taking symmetric differences. It follows that indeed $c_\pi * c_\pi$ is contained in $\mathcal{L}^{(2)}_{o,+}$ for each π. For nonzero P corresponding to the pair $\{\omega_1, \omega_2\}$ it also follows that the elements that are claimed to generate $\mathcal{L}^{(2)}_{P,+}$ and $\mathcal{L}^{(2)}_{P,-}$ are indeed contained in $\mathcal{L}^{(2)}_P$. The fact that their parity is as claimed follows from Proposition 5.12 which says that c_π is even if π has two parts of size 3 and odd if one part of π consists of a single element. It follows that the claimed dimensions are at least a

lower bound for the dimensions. As the dimensions have to add up to 136, we find that the lower bounds are exact and that the spaces are indeed generated as claimed. □

Note that $\mathrm{Sym}(\mathcal{L})$ is the homogeneous coordinate ring of $\mathbb{P}(\hat{\mathcal{L}})$. The ideal $I \subset \mathrm{Sym}(\mathcal{L})$ of J is generated by 72 quadratic forms described in Section 3. Set $\mathcal{I} = I_2 = I \cap \mathrm{Sym}^2 \mathcal{L}$, so that $\mathcal{I}$ is the 72-dimensional subspace of $\mathrm{Sym}^2 \mathcal{L}$ of quadratic forms that vanish on J. In other words, $\mathcal{I}$ is the kernel of the map $\mathrm{Sym}^2 \mathcal{L} \to \mathcal{L}(4(\Theta_+ + \Theta_-))$ that sends $g * h$ to gh. Note that $\mathcal{I}$ is a $\rho^{(2)}(J[2](k^{\mathrm{s}}))$-invariant subspace of $\mathrm{Sym}^2 \mathcal{L}$ because $J \subset \mathbb{P}^{15}$ is $J[2](k^{\mathrm{s}})$-invariant. Set $\mathcal{I}_{P,\pm} = \mathcal{I} \cap \mathcal{L}^{(2)}_{P,\pm}$ for any point $P \in J[2](k^{\mathrm{s}})$ and every sign.

Proposition 6.8. *The spaces $\mathcal{I}_{P,\pm}$ are $\rho^{(2)}$-invariant and we have*

$$\mathcal{I} \cong \bigoplus_{P \in J[2]} (\mathcal{I}_{P,+} \oplus \mathcal{I}_{P,-}) .$$

We have $\dim \mathcal{I}_{o,+} = 12$, $\dim \mathcal{I}_{o,-} = 0$ and $\dim \mathcal{I}_{P,+} = \dim \mathcal{I}_{P,-} = 2$ for nonzero $P \in J[2]$. The representation $\rho^{(2)}$ induces a representation $\sigma\colon J[2](k^{\mathrm{s}}) \to \mathrm{SL}(\mathcal{I})$.

Proof. The spaces $\mathcal{I}_{P,\pm} = \mathcal{I} \cap \mathcal{L}^{(2)}_{P,\pm}$ are $\rho^{(2)}$-invariant because $\mathcal{I}$ and the spaces $\mathcal{L}^{(2)}_{P,\pm}$ are. For any $g \in \mathcal{I} \subset \mathrm{Sym}^2 \mathcal{L}$ we can write $g = \sum_{P \in J[2]} (g_{P,+} + g_{P,-})$ with $g_{P,\pm} \in \mathcal{L}^{(2)}_{P,\pm}$. Set $g_P = g_{P,+} + g_{P,-} \in \mathcal{L}^{(2)}_P$. Take any $Q \in J[2](k^{\mathrm{s}})$. Then we have

$$\begin{aligned}
&\sum_{R \in \ker \chi_Q} \rho^{(2)}(R)(g) - \sum_{R \notin \ker \chi_Q} \rho^{(2)}(R)(g) \\
&\quad = \sum_{R \in \ker \chi_Q} \sum_{P \in J[2]} \rho^{(2)}(R)(g_P) - \sum_{R \notin \ker \chi_Q} \sum_{P \in J[2]} \rho^{(2)}(R)(g_P) \\
&\quad = \sum_{P \in J[2]} \left(\sum_{R \in \ker \chi_Q} \chi_P(R) g_P - \sum_{R \notin \ker \chi_Q} \chi_P(R) g_P \right) \\
&\quad = \sum_{P \in J[2]} \left(\sum_{R \in J[2]} \chi_Q(R) \chi_P(R) \right) g_P = \sum_{P \in J[2]} \left(\sum_{R \in J[2]} \chi_{P+Q}(R) \right) g_P = 16 g_Q,
\end{aligned}$$

where the last identity follows from the fact that for any $P \neq Q$ the character χ_{P+Q} is nontrivial, so we have $\sum_{R \in J[2]} \chi_{P+Q}(R) = 0$ (see [22, Section VI.1, Proposition 4]). Since $\mathcal{I}$ is $\rho^{(2)}$-invariant, we conclude $g_Q \in \mathcal{I}$. As we have $g_{Q,\pm}(x) = \frac{1}{2}(g_Q(x) \pm g_Q(-x))$, we find $g_{Q,\pm}(x) \in \mathcal{I}$, and thus $g_{Q,\pm}(x) \in \mathcal{I}_{Q,\pm}$. This holds for all Q, so we get $\sum_{Q \in J[2]} (\mathcal{I}_{Q,+} + \mathcal{I}_{Q,-}) = \mathcal{I}$. Since all subspaces in this sum intersect trivially, the sum is a direct sum, which proves the first statement. In Section 3 we saw that the subspace of odd vanishing quadratic forms has dimension 30. This means that $\sum_{P \in J[2]} \dim \mathcal{I}_{P,-} = 30$. From $\dim \mathcal{I}_{o,-} = 0$ and symmetry we conclude $\dim \mathcal{I}_{P,-} = 2$ for nonzero $P \in J[2]$. Set $a = \dim \mathcal{I}_{o,+}$ and $b = \dim \mathcal{I}_{P,+}$ for any nonzero $P \in J[2]$. Then by symmetry we have $b = \dim \mathcal{I}_{P,+}$ for all nonzero $P \in J[2]$. We get $a + 15b = \sum_{P \in J[2]} \dim \mathcal{I}_{P,+} = 72 - 30 = 42$. From $a, b \geq 0$ and $a \leq \dim \mathcal{L}^{(2)}_{o,+} = 16$, we find $a = 12$ and $b = 2$. For any $P, Q \in J[2](k^{\mathrm{s}})$ and any sign, the eigenvalues of $\rho^{(2)}(Q)$ on $\mathcal{I}_{P,\pm}$ are all the same and in μ_2; because the dimension $\dim \mathcal{I}_{P,\pm}$ is even, the determinant of $\rho^{(2)}(Q)$ restricted to $\mathcal{I}_{P,\pm}$ equals 1. It follows that $\det \rho^{(2)}(Q) = 1$ for all $Q \in J[2](k^{\mathrm{s}})$ so $\rho^{(2)}(Q) \in \mathrm{SL}(\mathcal{I})$. □

Corollary 6.9. *The ideal $I \subset \mathrm{Sym}(\mathcal{L})$ of J is homogeneous with respect to the $\mu_2(L^{\mathrm{s}})/\mu_2$-grading.*

Proof. From Proposition 6.8 it follows that $\mathcal{I}$ can be generated by homogeneous elements. Since $\mathcal{I}$ generates I, it follows that also the ideal I can be generated by homogeneous elements, which proves that I is homogeneous. □

We are now ready to make everything explicit, including the choices of the c_π. However, instead of choosing a function $c_\pi \in \mathcal{L}$ for each partition of Ω into two parts of odd size as in Proposition 6.7, we choose a function c_I for each subset $I \subset \Omega$ of size 1 or 3 such that $c_I = -c_{\Omega \setminus I}$ if I has size 3.

To obtain an explicit function c_π for each partition $\pi = \{\pi_1, \pi_2\}$ one could choose a part π_i with $\#\pi_i \in \{1, 3\}$ and set $c_\pi = c_{\pi_i}$. As in Proposition 6.7, we often abbreviate the set I in the index by the list of its elements.

Definition 6.10. *For all $\omega \in \Omega$ define an element $c_\omega \in \mathcal{L}(2(\Theta_+ + \Theta_-))$ so that for all $j \in \{1, \dots, 6\}$ the relation $b_j = \sum_\omega \omega^{j-1} c_\omega$ holds.*

Note that $\{c_\omega\}_\omega$ is an unordered basis for $\mathcal{L}(2(\Theta_+ + \Theta_-) - \sum_P F_P)$, as the transformation matrix from it, with any order, to the basis $(b_1, \dots, b_6)$ is a Vandermonde matrix with nonzero determinant.

Lemma 6.11. *We have $r^*_{\mathcal{Y}}(\overline{\varphi}_\omega) = f_6 c_\omega$ for the isomorphism $r^*_{\mathcal{Y}} \colon k(V_1) \to k(\mathcal{Y})$ induced by $r_{\mathcal{Y}}$.*

Proof. The polynomial $\overline{P}_\omega = \prod_{\theta \in \Omega \setminus \{\omega\}} (X - \theta)$ from Section 4 satisfies

$$f_6 \overline{P}_\omega = \frac{f(X) - f(\omega)}{X - \omega} = \sum_{j=0}^{6} f_j \frac{X^j - \omega^j}{X - \omega} = \sum_{j=0}^{6} \sum_{i=1}^{j} f_j \omega^{i-1} X^{j-i} = \sum_{i=1}^{6} \omega^{i-1} g_i.$$

This relation between the unordered basis $\{\overline{P}\}_\omega$ of L^{s} and the basis $(g_1, \dots, g_6)$ induces a relation between their dual bases of $\hat{L}^{\mathrm{s}}$, namely $f_6 b_j = \sum_\omega \omega^{j-1} \overline{\varphi}_\omega$. Applying $r^*_{\mathcal{Y}}$, we obtain $f_6 v_j = f_6 r^*_{\mathcal{Y}}(b_j) = \sum_\omega \omega^{j-1} r^*_{\mathcal{Y}}(\overline{\varphi}_\omega)$. From the definition of c_ω we conclude $r^*_{\mathcal{Y}}(\overline{\varphi}_\omega) = c_\omega$. □

The following functions, up to a constant factor, were also used by Michael Stoll [27, Section 10].

Definition 6.12. *For any subset $I \subset \Omega$ with $\#I = 3$, let c_I be defined by*

$$4 \left(\prod_{\omega \in I} \prod_{\psi \in \Omega \setminus I} (\psi - \omega) \right) \cdot c_I = \sum_{1 \le i \le j \le 4} \lambda_{ij}(I) k_{ij}$$

with

$$\begin{aligned}
\lambda_{11} &= \sigma_2\sigma_3\tau_1\tau_2 + (4\sigma_1\sigma_3 - \sigma_2^2)\tau_1\tau_3 - \sigma_1\sigma_3\tau_2^2 + (\sigma_1\sigma_2 - \sigma_3)\tau_2\tau_3 + \sigma_3^2\tau_2 + \sigma_2\tau_3^2 - \sigma_2\sigma_3\tau_3,\\
\lambda_{12} &= -4\sigma_3\tau_1\tau_3 + 2\sigma_3\tau_2^2 - 2\sigma_2\tau_2\tau_3 - 2\sigma_2\sigma_3\tau_2 + (-4\sigma_1\sigma_3 + 2\sigma_2^2)\tau_3,\\
\lambda_{13} &= 2\sigma_2\tau_1\tau_3 + 2\sigma_2\sigma_3\tau_1 + 2\sigma_1\tau_2\tau_3 + 2\sigma_1\sigma_3\tau_2 - 2\tau_3^2 + 4\sigma_3\tau_3 - 2\sigma_3^2,\\
\lambda_{14} &= 2f_6^{-1}(\sigma_3\tau_1 + \sigma_1\tau_3),\\
\lambda_{22} &= -\sigma_3\tau_1\tau_2 + \sigma_2\tau_1\tau_3 + \sigma_1\sigma_3\tau_2 + (-\sigma_1\sigma_2 + 4\sigma_3)\tau_3,\\
\lambda_{23} &= 2\sigma_3\tau_1^2 - 2\sigma_1\tau_1\tau_3 - 2\sigma_1\sigma_3\tau_1 - 4\sigma_3\tau_2 + (2\sigma_1^2 - 4\sigma_2)\tau_3,\\
\lambda_{24} &= -2f_6^{-1}(\tau_3 + \sigma_3),\\
\lambda_{33} &= -\sigma_2\tau_1^2 + \sigma_1\tau_1\tau_2 + \tau_1\tau_3 + (\sigma_1\sigma_2 - \sigma_3)\tau_1 + (-\sigma_1^2 + 4\sigma_2)\tau_2 - \sigma_1\tau_3 + \sigma_1\sigma_3,\\
\lambda_{34} &= 2f_6^{-1}(\tau_2 + \sigma_2),\\
\lambda_{44} &= f_6^{-2},
\end{aligned}$$

where $\sigma_i = \sigma_i(I)$ and $\tau_i = \tau_i(I)$ are the i-th elementary symmetric polynomials in the elements of I and $\Omega \setminus I$ respectively.

Note that for all $i, j \in \{1, 2, 3, 4\}$ with $i \le j$ and all $I \subset \Omega$ with $\#I = 3$ we have $\lambda_{ij}(I) = \lambda_{ij}(\Omega \setminus I)$, while the coefficient $\prod_{\omega \in I} \prod_{\psi \in \Omega \setminus I} (\psi - \omega)$ of c_I in Definition 6.12 is negated when we replace I by $\Omega \setminus I$. We conclude that $c_I + c_{\Omega \setminus I} = 0$ for all I. The c_I generate $\mathrm{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$. More precisely, we have the following statement.

Proposition 6.13. *For all i, j with $1 \le i \le j \le 4$ we have $k_{ij} = \sum_I \kappa_{ij}(I) c_I$ with*

$$\begin{aligned}
\kappa_{11} &= \sigma_1,\\
\kappa_{12} &= \sigma_2,\\
\kappa_{13} &= \sigma_3,\\
\kappa_{14} &= f_6\big(\sigma_1\tau_1\tau_3 + 2\sigma_2\tau_3 + \sigma_3\tau_1^2\big),\\
\kappa_{22} &= \sigma_2\tau_1 + \sigma_3,\\
\kappa_{23} &= \sigma_3\tau_1,\\
\kappa_{24} &= f_6\big(\sigma_1\tau_2\tau_3 + \sigma_2\tau_1\tau_3 + \sigma_3^2\big),\\
\kappa_{33} &= \sigma_3\tau_2,\\
\kappa_{34} &= f_6\big(\sigma_2^2\tau_3 + \sigma_2\tau_2\tau_3 + 2\sigma_3\tau_1\tau_3\big),\\
\kappa_{44} &= f_6^2\big(\sigma_1^2\sigma_2\tau_2\tau_3 + 4\sigma_1^2\sigma_3\tau_1\tau_3 + \sigma_1\sigma_2\sigma_3\tau_1\tau_2 + \sigma_1\sigma_2\tau_3^2 + \sigma_1\sigma_3^2\tau_2\\
&\qquad + \sigma_1\sigma_3\tau_1\tau_2^2 + 3\sigma_1\sigma_3\tau_2\tau_3 + \sigma_2^2\tau_1^2\tau_3 + 4\sigma_2\sigma_3\tau_2^2 + 4\sigma_3^2\tau_3 + \sigma_3\tau_1\tau_2\tau_3\big),
\end{aligned}$$

where $\sigma_i = \sigma_i(I)$ and $\tau_i = \tau_i(I)$ are as in Definition 6.12.

Proof. Choose 10 subsets $I_1, \dots, I_{10} \subset \Omega$ with $\#I_r = 3$ for all r, so that every partition of Ω in two parts of size 3 contains one of $I_1, \dots, I_{10}$. Let G be the matrix whose r-th row is

$$\frac{1}{4}\left(\prod_{\omega\in I_r}\prod_{\psi\in\Omega\setminus I_r}(\psi-\omega)^{-1}\right)\cdot\begin{pmatrix}\lambda_{11}(I_r) & \lambda_{12}(I_r) & \lambda_{13}(I_r) & \cdots & \lambda_{44}(I_r)\end{pmatrix},$$

that is, the entries of G in the r-th row are the coefficients of c_{I_r} with respect to the basis $(k_{11}, k_{12}, \dots, k_{44})$. Then the r-th column of G^{-1} is

$$\begin{pmatrix}\kappa_{11}(I_r) - \kappa_{11}(\Omega\setminus I_r)\\ \kappa_{12}(I_r) - \kappa_{12}(\Omega\setminus I_r)\\ \vdots\\ \kappa_{44}(I_r) - \kappa_{44}(\Omega\setminus I_r)\end{pmatrix}$$

and its rows give the coefficients of the k_{ij} in terms of the basis $(c_{I_1}, \dots, c_{I_{10}})$. We therefore have $k_{ij} = \sum_{r=1}^{10}(\kappa_{ij}(I_r) - \kappa_{ij}(\Omega\setminus I_r))c_{I_r} = \sum_I \kappa_{ij}(I)c_I$, where the last sum is over all subset $I \subset \Omega$ with $\#I = 3$. □

For any set $I \subset \Omega$ we let $\chi_I \in \mu_2(L^{\mathrm{s}})/\mu_2$ be the character of M associated to the partition $\pi = \{I, \Omega\setminus I\}$. If $\#I$ is even, then μ_2 is contained in the kernel of χ_I and the induced character of $J[2](k^{\mathrm{s}})$ equals χ_P where $e(P) = \pi$ and χ_P is defined just before Proposition 6.6. Recall that Ξ is the group of all subsets of Ω. For any set $R \subset \Xi$ of representatives of all partitions of Ω into two parts of size 3, the set $\{c_I \ : \ I \in R\}$ is an unordered basis for $\mathrm{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$; the following proposition says that, with respect to the unordered basis $\{c_I \ : \ I \in R\} \cup \{c_\omega \ : \ \omega \in \Omega\}$ of $\mathcal{L}$, the representation ρ is diagonal.

Proposition 6.14. *Let $I \subset \Omega$ be a subset of size 1 or 3. Then for each $a \in M$ we have $\rho(a)(c_I) = \chi_I(a)c_I$.*

Proof. For $a = \pm 1$ the action of $\rho(a)$ on $\mathcal{L}$ is given by multiplication by ± 1, so the statement is trivial. Suppose that $a \neq \pm 1$. First assume $I = \{\omega\}$ for some $\omega \in \Omega$ so that $c_I = c_\omega = f_6^{-1} r_{\mathcal{Y}}^*(\overline{\varphi}_\omega)$ by Proposition 6.11. Then we have

$$\begin{aligned}
\rho(a)(c_I) = \rho_6(a)(c_I) &= (r_{\mathcal{Y}}^* \circ \hat{m}_a \circ (r_{\mathcal{Y}}^*)^{-1})(c_I) = f_6^{-1} r_{\mathcal{Y}}^*(\hat{m}_a(\overline{\varphi}_\omega))\\
&= f_6^{-1}\varphi_\omega(a) r_{\mathcal{Y}}^*(\overline{\varphi}_\omega) = \varphi_\omega(a)c_I = \chi_I(a)c_I.
\end{aligned}$$

Now assume $\#I = 3$. Recall that we have a perfect pairing $\Xi \times \Xi \to \mu_2$ on the group Ξ of all subsets of Ω given by $(I_1, I_2) \mapsto (I_1 : I_2) = (-1)^r$ with $r = \#(I_1 \cap I_2)$, and that the map

$e\colon M \to \mathcal{M} \subset \Xi$ associates to each $m \in M$ a subset of Ω of even size. We have $\chi_I(a) = (e(a) : I)$. Let v_I denote the vector

$$v_I = (\ \lambda_{11}(I_r) \qquad \lambda_{12}(I_r) \qquad \lambda_{13}(I_r) \qquad \cdots \qquad \lambda_{44}(I_r)\ )$$

with λ_{ij} as in Definition 6.12. Set $P = \beta(a) \neq 0$ and let $\{\omega_1, \omega_2\}$ be the pair of roots defining P, so that $\Omega \setminus \{\omega_1, \omega_2\} = e(\alpha(a) \cdot a)$. With a computer algebra system it is easy to check that v_I is an eigenvector on the left of the symmetric square $M_P^{(2)}$ of the matrix M_P as in Proposition 5.1. In fact, for $M' = \mathrm{Res}(g,h)^{-1} M_P^{(2)}$ with g, h as in Proposition 5.1 as well, we have

$$v_I \cdot M' = (\Omega \setminus \{\omega_1, \omega_2\} : I) \cdot v_I = (e(\alpha(a) \cdot a) : I) \cdot v_I = \alpha(a)(e(a) : I) \cdot v_I = \alpha(a)\chi_I(a) \cdot v_I.$$

Since the action of $T_{4,P}$ is given by multiplication from the right by M_P by Proposition 5.1, the action of $T_{10,P}$ is given by multiplication by M' from the right. Up to a scalar, the entries of v_I are the coefficients of c_I with respect to the basis $(k_{11}, k_{12}, \ldots, k_{44})$, so we find $T_{10,P}(c_I) = \alpha(a)\chi_I(a) \cdot c_I$. We therefore get $\rho(a)(c_I) = \rho_{10}(a)(c_I) = \alpha(a) T_{10,P}(c_I) = \chi_I(a) \cdot c_I$. □

For each $P \in J[2](k^{\mathrm{s}})$ and each sign we now give quadratic forms that generate the subspace $\mathcal{L}^{(2)}_{P,\pm}$. All together these generate the ideal defining J in $\mathbb{P}(\hat{\mathcal{L}})$. The reason for defining functions c_I for each $I \subset \Omega$ of size 3 with $c_I = -c_{\Omega \setminus I}$, rather than defining a function for each partition into two parts of size 3, is that the quadratic forms are simpler if written in terms of the c_I. For each quadratic form we make choices whether to use c_I or $c_{\Omega \setminus I}$ for several I. It is worth checking that the quadratic forms obtained from different choices generate the same subspace.

Take any nonzero $P \in J[2](k^{\mathrm{s}})$, corresponding to the pair $\{\omega_1, \omega_2\}$. Then $\mathcal{L}^{(2)}_{P,-}$ is generated by the monomials $c_\theta * c_{\omega_1\omega_2\theta}$ for $\theta \notin \{\omega_1, \omega_2\}$ by Proposition 6.7. From the discussion around (6) in Section 3 we know that for each $l \in \{0, 1\}$ the quadratic form $Q_{4,l} = k_{11}b_{3+l} - k_{12}b_{2+l} + k_{13}b_{1+l}$ is contained in $\mathcal{I} \subset I$. By Proposition 6.8, the projection of $Q_{4,l}$ to $\mathcal{L}^{(2)}_{P,-}$ is also contained in $\mathcal{I}$. From $b_j = \sum_\omega \omega^{j-1} c_\omega$ and $k_{1j} = \sum_I \sigma_j(I) c_I$ for $1 \leq j \leq 3$, we find that this projection equals

$$\sum_{\theta \neq \omega_1, \omega_2} \left(\sum_{n=1}^{3} (\sigma_n(\{\theta, \omega_1, \omega_2\}) - \tau_n(\{\theta, \omega_1, \omega_2\}))\theta^{3+l-n} \right) c_\theta * c_{\omega_1\omega_2\theta}$$

$$= \sum_{\theta \neq \omega_1, \omega_2} \left(\theta^l \prod_{\psi \neq \theta, \omega_1, \omega_2} (\theta - \psi) \right) c_\theta * c_{\omega_1\omega_2\theta}. \tag{15}$$

By Proposition 6.8 we have $\dim \mathcal{I}_{P,-} = 2$, so the quadratic forms in (15) for $l = 0, 1$ generate $\mathcal{I}_{P,-}$. By Proposition 6.7 the space $\mathcal{L}^{(2)}_{P,+}$ is generated by the monomials $c_{\omega_1} * c_{\omega_2}$ and $c_{\theta_1\theta_2\omega_1} * c_{\theta_1\theta_2\omega_2}$ for $\theta_1, \theta_2 \neq \omega_1, \omega_2$ and $\theta_1 \neq \theta_2$. The projection of $\frac{1}{2}(k_{12}^2 - k_{11}k_{22}) \in \mathcal{I}$ to $\mathcal{L}^{(2)}_{P,+}$ equals

$$\sum_{\pi = \{\{\theta_1, \theta_2\}, \{\psi_1, \psi_2\}\}} \nu(\pi) \cdot c_{\theta_1\theta_2\omega_1} * c_{\theta_1\theta_2\omega_2}, \tag{16}$$

where the sum ranges over all three partitions of $\Omega \setminus \{\omega_1, \omega_2\}$ into two sets of cardinality 2 and $\nu(\pi) = (\theta_1 - \psi_1)(\theta_1 - \psi_2)(\theta_2 - \psi_1)(\theta_2 - \psi_2)$ for $\pi = \{\{\theta_1, \theta_2\}, \{\psi_1, \psi_2\}\}$. From Proposition 6.8 we conclude that the quadratic form (16) is contained in $\mathcal{I}_{P,+}$. Write $f = gh$ with $g = X^2 + g_1X + g_0 = (X - \omega_1)(X - \omega_2)$ and $h = h_4X^4 + h_3X^3 + h_2X^2 + h_1X + h_0$, and set $\lambda = 2h_2 + h_3g_1 - g_1^2 + 2g_0$. Let Q denote the right-hand side of the first equation in (7). Then we have $\frac{1}{4}\big(2(b_1^2 - Q) + f_6\lambda(k_{12}^2 - k_{11}k_{22})\big) \in \mathcal{I}$. The projection of this quadratic form to $\mathcal{L}^{(2)}_{P,+}$ equals

$$c_{\omega_1} * c_{\omega_2} + f_6 \cdot \sum_{\pi = \{\{\theta_1, \theta_2\}, \{\psi_1, \psi_2\}\}} \nu(\pi)(\theta_1 + \theta_2)(\psi_1 + \psi_2) \cdot c_{\theta_1\theta_2\omega_1} * c_{\theta_1\theta_2\omega_2}. \tag{17}$$

By Proposition 6.8 this projection is contained in $\mathcal{I}_{P,+}$. Again by Proposition 6.8 we have $\dim \mathcal{I}_{P,+} = 2$, so the quadratic forms in (16) and (17) generate $\mathcal{I}_{P,+}$.

For $\mathcal{I}_{0,+}$ we do not have generators that are as simple as those in (15), (16), and (17). The only simple quadratic forms in $\mathcal{I}_{0,+}$ that we know are

$$\sum_{\omega} \omega^j \lambda_\omega c_\omega^2 \tag{18}$$

for $j = 0, 1, 2$. By Lemma 6.11 these correspond to $Q_j^{(1)}$ in Proposition 4.6. Six quadratic forms that give a basis for $\mathcal{I}_{0,+} \cap \operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$ are the projections to $\mathcal{L}_{0,+}^{(2)}$ of the quadratic forms $k_{12}^2 - k_{11}k_{22}$, $k_{12}k_{13} - k_{11}k_{23}$, $k_{13}^2 - k_{11}k_{33}$, $k_{13}k_{23} - k_{12}k_{33}$, $k_{23}^2 - k_{22}k_{33}$, and the quadric $g_{\mathcal{X}}$ in (5) that defines the model of $\mathcal{X}$ inside the 2-uple embedding of $\mathbb{P}^3$ into $\mathbb{P}^9$. The first five of these quadrics together with the 15 quadrics (16) for all nonzero $P \in J[2](k^{\mathrm{s}})$ define the 2-uple embedding of $\mathbb{P}^3$ into $\mathbb{P}^9$. The whole subspace $\mathcal{I}_{0,+}$ is generated by these nine quadrics and the projections to $\mathcal{L}_{0,+}^{(2)}$ of the differences of the left- and right-hand side of the equations in (7). This concludes the description of generators for all subspaces $\mathcal{I}_{P,\pm}$. Explicit formulas are given in Appendix A.

7. The twists of the Jacobian

Let $\xi \in \mathrm{H}^1(J[2])$ be contained in the kernel $P^1(J[2])$ of the map $\Upsilon\colon \mathrm{H}^1(J[2]) \to \mathrm{Br}(k)[2]$ as defined in Section 2. In this section we determine explicitly a two-covering A of J whose k-isomorphism class corresponds to ξ. The kernel of Υ equals the image of the map $\beta_*\colon \mathrm{H}^1(M) \to \mathrm{H}^1(J[2])$ by the exactness of the left vertical sequence in Diagram (2). Let $\overline{\xi} \in \mathrm{H}^1(M)$ be a lift of ξ under β_*. By Proposition 2.6 there are elements $\varepsilon \in L^{\mathrm{s}}$, $\delta \in L^*$ and $n \in k^*$ such that $\varepsilon^2 = \delta$, $N_{L^{\mathrm{s}}/k^{\mathrm{s}}}(\varepsilon) = n$, and the class $\overline{\xi}$ is represented by the cocycle $\sigma \mapsto \sigma(\varepsilon)/\varepsilon$. For all $\omega \in \Omega$ we write $\varepsilon_\omega = \varphi_\omega(\varepsilon)$ and $\delta_\omega = \varphi_\omega(\delta)$, so that $\varepsilon_\omega^2 = \delta_\omega$ and $\prod_\omega \varepsilon_\omega = n$. For any subset $I \subset \Omega$ of cardinality 1 or 3, set

$$t_I = \begin{cases} \varepsilon_\omega & \text{if } \#I = 1, \\ \prod_{\omega\in I} \varepsilon_\omega + \prod_{\omega\in\Omega\setminus I} \varepsilon_\omega & \text{if } \#I = 3. \end{cases}$$

We assume that for all $I \subset \Omega$ with $\#I = 3$ we have that t_I is non-zero; if the field k is infinite, then it is easy to see that this can be achieved by choosing carefully ε, δ and n representing the class $\overline{\xi}$. Let $g\colon \mathbb{P}(\hat{\mathcal{L}}) \to \mathbb{P}(\hat{\mathcal{L}})$ be the linear automorphism induced by the linear map $g^*\colon \mathcal{L} \to \mathcal{L}$ given by $c_I \mapsto t_I \cdot c_I$. Note that the action on $\mathcal{L}$ is well defined, as $t_I = t_{\Omega\setminus I}$ for any $I \subset \Omega$ with $\#I = 3$. Even in the case $\varepsilon = \delta = n = 1$ the automorphism g is not the identity, though this can be arranged by replacing t_I by $\frac{1}{2}t_I$ for I with $\#I = 3$ throughout the rest of the paper. For each positive integer d, the automorphism g^* extends naturally to an automorphism of the k^{s}-vector space $\operatorname{Sym}^d \mathcal{L}$, which we also denote by g^*. Note that g^* preserves the $\mu_2(L^{\mathrm{s}})/\mu_2$-grading. Recall that for any subset $I \subset \Omega$ we have a character $\chi_I \in \mu_2(L^{\mathrm{s}})/\mu_2$ defined just before Proposition 6.14.

Lemma 7.1. *For any $I \subset \Omega$ and any Galois automorphism $\sigma \in \mathrm{Gal}(k^{\mathrm{s}}/k)$ we have*

$$\prod_{\omega\in I} \varepsilon_{\sigma(\omega)} = \chi_{\sigma(I)}\big(\sigma(\varepsilon)/\varepsilon\big) \cdot \sigma\Big(\prod_{\omega\in I} \varepsilon_\omega\Big).$$

If I has cardinality 1 or 3, then we have

$$\begin{aligned} t_{\sigma(I)} &= \chi_{\sigma(I)}\big(\sigma(\varepsilon)/\varepsilon\big) \cdot \sigma(t_I), \\ \sigma(g^*(c_I)) &= \chi_{\sigma(I)}\big(\sigma(\varepsilon)/\varepsilon\big) \cdot g^*(\sigma(c_I)). \end{aligned}$$

Proof. Let $m = \sigma(\varepsilon)/\varepsilon$ and $I_0 = \{\omega \in \Omega \,:\, \varepsilon_{\sigma(\omega)} = -\sigma(\varepsilon_\omega)\} = \sigma^{-1}(e(m))$ and set $r = \#(I \cap I_0)$. Thus we have $\chi_{\sigma(I)}(m) = (\sigma(I) : e(m)) = (I : \sigma^{-1}(e(m))) = (I : I_0) = (-1)^r$ and similarly $\chi_{\Omega\setminus\sigma(I)}(m) = (-1)^{6-r} = (-1)^r$. By definition of I_0 we have

$$\prod_{\omega\in I} \varepsilon_{\sigma(\omega)} = (-1)^r \prod_{\omega\in I} \sigma(\varepsilon_\omega) = \chi_{\sigma(I)}(m) \cdot \sigma\Big(\prod_{\omega\in I} \varepsilon_\omega\Big),$$

and the first part of the lemma is proved. The second equality follows immediately from the definition of t_I. We then have $\sigma(g^*(c_I)) = \sigma(t_I)\sigma(c_I) = \chi_{\sigma(I)}(m) t_{\sigma(I)} c_{\sigma(I)} = \chi_{\sigma(I)}(m) g^*(\sigma(c_I))$, which proves the last equality. □

Let A_ξ be the surface $g^{-1}(J)$ where J is embedded in $\mathbb{P}(\hat{\mathcal{L}})$ as before. Then g restricts to an isomorphism $A_\xi \to J$, defined over k^{s}, which we also denote by g. Note that A_ξ depends on the choice of δ, n, and ε.

Proposition 7.2. *The surface A_ξ is defined over k.*

Proof. Take any $P \in J[2](k^{\mathrm{s}})$ and set $\chi = \epsilon(P) \in \mu_2(L^{\mathrm{s}})/\mu_2$. Let $I_1, I_2 \subset \Omega$ be subsets of odd cardinality such that $c_{I_1} * c_{I_2} \in \mathcal{L}_P^{(2)} = \mathcal{L}_\chi^{(2)}$. For $j = 1, 2$, set $\chi_j = \chi_{I_j} \in \mu_2(L^{\mathrm{s}})/\mu_2$, so that c_{I_j} has weight χ_j and $c_{I_1} * c_{I_2}$ has weight $\chi_1\chi_2 = \chi$. Set $m = \sigma(\varepsilon)/\varepsilon$. Let $\sigma \in \mathrm{Gal}(k^{\mathrm{s}}/k)$ be any Galois automorphism. From Lemma 7.1 we find

$$\begin{aligned}(19)\qquad \sigma(g^*(c_{I_1} * c_{I_2})) &= \sigma(g^*(c_{I_1})) * \sigma(g^*(c_{I_2})) \\ &= \sigma(\chi_1)(m)g^*(\sigma(c_{I_1})) * \sigma(\chi_2)(m)g^*(\sigma(c_{I_2})) = \sigma(\chi)(m)g^*(\sigma(c_{I_1} * c_{I_2})).\end{aligned}$$

Since $\sigma(\chi)(m)$ only depends on σ and P, and $\mathcal{L}_P^{(2)}$ is generated by monomials by Proposition 6.1, we find $\sigma(g^*(q)) = \sigma(\chi)(m) \cdot g^*(\sigma(q)) = \pm g^*(\sigma(q))$ for each $q \in \mathcal{L}_P^{(2)}$. Set $E = \{q \ : \ q \in \mathcal{I}_P \text{ for some } P\}$. The set E generates the ideal I that defines the Jacobian J, so the set $g^*(E)$ generates the ideal that defines A_ξ. Since J is defined over k, we have $\sigma(E) = E$ from Proposition 6.8. We therefore have

$$g^*(E) = g^*(\sigma(E)) = \{g^*(\sigma(q)) \ : \ q \in E\} = \{\pm\sigma(g^*(q)) \ : \ q \in E\} = \sigma(g^*(E)).$$

We conclude that the ideal that defines A_ξ, which is generated by $g^*(E)$, is Galois invariant. By descent this implies that A_ξ is defined over k. □

We can make Proposition 7.2 explicit and give a Galois-invariant set of quadratic forms defining A_ξ, each defined over $k(\Omega)$. We have

$$\begin{aligned} t_{\{\omega_1\}}t_{\{\omega_2\}} &= \varepsilon_{\omega_1}\varepsilon_{\omega_2}, \\ t_{\{\theta\}}t_{\{\theta,\omega_1,\omega_2\}} &= \varepsilon_{\omega_1}\varepsilon_{\omega_2}\left(\delta_\theta + n\delta_{\omega_1}^{-1}\delta_{\omega_2}^{-1}\right), \\ t_{\{\theta_1,\theta_2,\omega_1\}}t_{\{\theta_1,\theta_2,\omega_2\}} &= \varepsilon_{\omega_1}\varepsilon_{\omega_2}\left(\delta_{\theta_1}\delta_{\theta_2} + \delta_{\psi_1}\delta_{\psi_2} + n(\delta_{\omega_1}^{-1} + \delta_{\omega_2}^{-1})\right), \\ t_{\{\omega\}}^2 &= \delta_\omega, \\ t_I^2 &= \prod_{\omega\in I}\delta_\omega + \prod_{\omega\in\Omega\setminus I}\delta_\omega + 2n \qquad (\#I = 3), \end{aligned}$$

where in the third identity ψ_1 and ψ_2 denote the two roots in $\Omega \setminus \{\omega_1, \omega_2, \theta_1, \theta_2\}$. Note that $n \in k$ and for each ω we have $\delta_\omega \in k(\Omega)$. This implies $t_I^2 \in k(\Omega)$ for each I with $\#I \in \{1, 3\}$. Since $\mathcal{L}_0^{(2)}$ is generated by square monomials $c_I * c_I$, we find that $g^*(q)$ is defined over $k(\Omega)$ for each $q \in \mathcal{I}_0$ that is itself defined over $k(\Omega)$. As before it is not worth writing this down here for a set of generators of $\mathcal{I}_0$ except for q as in (18), in which case we get

$$(20)\qquad g^*(q) = \sum_\omega \omega^j \lambda_\omega \delta_\omega c_\omega^2.$$

Suppose $P \in J[2](k^{\mathrm{s}})$ is nonzero and corresponds to the pair $\{\omega_1, \omega_2\}$. Then for each $q \in \mathcal{L}_P^{(2)}$ defined over $k(\Omega)$ the quadratic form $\varepsilon_{\omega_1}^{-1}\varepsilon_{\omega_2}^{-1}g^*(q)$ is defined over $k(\Omega)$. Applying this to (15), (16), and (17), we find that the intersection of the ideal of A_ξ with $\mathcal{L}_P^{(2)}$ is generated by

$$(21)\qquad \sum_{\theta\neq\omega_1,\omega_2}\left(\theta^l\prod_{\psi\neq\theta,\omega_1,\omega_2}(\theta-\psi)\right)\left(\delta_\theta + n\delta_{\omega_1}^{-1}\delta_{\omega_2}^{-1}\right)\cdot c_\theta * c_{\omega_1\omega_2\theta} \qquad (l = 0, 1),$$

$$(22)\qquad \sum_{\pi=\{\{\theta_1,\theta_2\},\{\psi_1,\psi_2\}\}}\nu(\pi)\left(\delta_{\theta_1}\delta_{\theta_2} + \delta_{\psi_1}\delta_{\psi_2} + n(\delta_{\omega_1}^{-1} + \delta_{\omega_2}^{-1})\right)\cdot c_{\theta_1\theta_2\omega_1} * c_{\theta_1\theta_2\omega_2},$$

$$c_{\omega_1} * c_{\omega_2} + f_6 \cdot \sum_{\pi=\{\{\theta_1,\theta_2\},\{\psi_1,\psi_2\}\}} \nu(\pi)(\theta_1+\theta_2)(\psi_1+\psi_2)\left(\delta_{\theta_1}\delta_{\theta_2}+\delta_{\psi_1}\delta_{\psi_2}+n(\delta_{\omega_1}^{-1}+\delta_{\omega_2}^{-1})\right)\cdot c_{\theta_1\theta_2\omega_1} * c_{\theta_1\theta_2\omega_2}. \tag{23}$$

Proposition 7.3. *For any Galois automorphism $\sigma \in \mathrm{Gal}(k^{\mathrm{s}}/k)$ there is a unique point $P(\sigma) \in J[2](k^{\mathrm{s}})$ such that $g\circ\sigma(g)^{-1} = T_{P(\sigma)}$ in $\mathrm{Aut}\, J$. The class $\xi \in \mathrm{H}^1(J[2])$ is represented by the cocycle $\sigma \mapsto P(\sigma)$.*

Proof. Set $P(\sigma) = \beta(\sigma(\varepsilon)/\varepsilon)$ for all $\sigma \in \mathrm{Gal}(k^{\mathrm{s}}/k)$. By Proposition 2.6 the class $\overline{\xi} \in \mathrm{H}^1(M)$ is represented by the cocycle $\sigma \mapsto \sigma(\varepsilon)/\varepsilon$, so $\xi \in \mathrm{H}^1(J[2])$ is represented by the cocycle $\sigma \mapsto \beta(\sigma(\varepsilon)/\varepsilon) = P(\sigma)$. Fix any Galois automorphism $\sigma \in \mathrm{Gal}(k^{\mathrm{s}}/k)$ and set $m = \sigma(\varepsilon)/\varepsilon$. Then $\beta(m) = P(\sigma)$, so the translation $T_{P(\sigma)}$ on $J \subset \mathbb{P}^{15}$ is induced by the automorphism $\rho(m) \in \mathrm{SL}(\mathcal{L})$ by Proposition 5.11. Take any subset $I \subset \Omega$ with $\#I \in \{1,3\}$. Then by Proposition 6.14 and Lemma 7.1 we have

$$\sigma(g^*)(\sigma(c_I)) = \sigma(g^*(c_I)) = \chi_{\sigma(I)}(m)g^*(\sigma(c_I)) = g^*\big(\chi_{\sigma(I)}(m)\sigma(c_I)\big) = g^*\big(\rho(m)(\sigma(c_I))\big).$$

This holds for all I, so we get $(g^{-1})^*\circ\sigma(g^*) = \rho(m)$. From $m^2 = 1$ we get $\rho(m) = \rho(m)^{-1}$, so we have $\rho(m) = \sigma(g^{-1})^*\circ g^*$ and thus $\rho(m)$ induces the automorphism $g\circ\sigma(g^{-1})$ on J. We conclude $T_{P(\sigma)} = g\circ\sigma(g^{-1})$. Clearly there is at most one point P such that $T_P = g\circ\sigma(g^{-1})$, so uniqueness follows. □

Let $\pi\colon A_\xi \to J$ denote the composition $\pi = [2]\circ g$. We are now ready to prove our main result.

Theorem 7.4. *The map π endows A_ξ with the structure of a two-covering of J whose isomorphism class corresponds to the cocycle class ξ.*

Proof. Let $\sigma \in \mathrm{Gal}(k^{\mathrm{s}}/k)$ be any Galois automorphism. By Proposition 7.3 there is a unique point $P \in J[2](k^{\mathrm{s}})$ such that $g\circ\sigma(g)^{-1} = T_P$, so $\sigma(g) = T_P\circ g$. Then

$$\sigma(\pi) = \sigma([2])\circ\sigma(g) = [2]\circ T_P\circ g = [2]\circ g = \pi,$$

because $[2]\circ T_P = [2]$ as $2P = 0$. This holds for all σ, so π is defined over k. Also A_ξ is defined over k by Proposition 7.2. There is an isomorphism $g\colon (A_\xi)_{k^{\mathrm{s}}} \to J_{k^{\mathrm{s}}}$ such that $\pi = [2]\circ g$, so π endows A_ξ with the structure of a two-covering of J. By Lemma 2.14 and Proposition 7.3 its k-isomorphism class corresponds to the cocycle class ξ. □

Recall that for any two-covering (A,π) of J the isomorphism $h\colon A_{k^{\mathrm{s}}} \to J_{k^{\mathrm{s}}}$ is well defined up to translation T_P by a two-torsion point P (Lemma 2.13). Since multiplication by -1 on J commutes with T_P, there is a well-defined involution $\iota\colon A \to A, x \mapsto h^{-1}(-h(x))$ of A, defined over k. On our two-covering A_ξ this involution is given by negating all six coordinates c_ω. The quotient $\mathcal{X}_\delta$ is the projection of A_ξ onto the 10 coordinates c_I for all $I \subset \Omega$ with $\#I = 3$. This quotient is isomorphic to $\mathcal{X}$ over k^{s}. The projection $\mathcal{Y}_\delta$ of A_ξ onto the coordinates c_ω for all ω is isomorphic to the blow-up of $\mathcal{X}_\delta$ in its 16 singular points. The surface $\mathcal{Y}_\delta$ is the vanishing set of the three quadratic forms given in (20). These correspond to the polynomials $Q_0^{(\delta)}, Q_1^{(\delta)}, Q_2^{(\delta)}$ in Proposition 4.6. This shows that the blow-up $\mathcal{Y}_\delta$ of the quotient $\mathcal{X}_\delta$ of the twist A_ξ of the Jacobian J is isomorphic to the twist V_δ of the blow-up $\mathcal{Y}$ of the quotient $\mathcal{X}$ of J.

Appendix A. Generators for $\mathcal{I}_{0,+}$

Choose a set $\mathcal{S}$ of ten subsets of Ω, each of cardinality 3, such that for each partition $\pi = \{\pi_1,\pi_2\} \in \Xi/\langle\Omega\rangle$ of Ω into two parts of cardinality 3 there is a unique element of $\mathcal{S}$, denoted I_π, with $I_\pi \in \pi$. For each partition $\pi = \{\pi_1,\pi_2\} \in \Xi/\langle\Omega\rangle$ with $\#\pi_1 = \#\pi_2 = 3$ we set $c_\pi = c_{I_\pi}$; for all integers i,j with $1 \le i \le j \le 4$ we set

$$\mu_{ij}(\pi) = \kappa_{ij}(I_\pi) - \kappa_{ij}(\Omega \setminus I_\pi),$$

with κ_{ij} as in Proposition 6.13. Note that c_π and $\mu_{ij}(\pi)$ depend on the choice of $\mathcal{S}$, but their product $\mu_{ij}(\pi)c_\pi$, as well as $c_\pi * c_\pi$ and $\mu_{i_1j_1}(\pi)\cdot\mu_{i_2j_2}(\pi)$ for any i_1,j_1,i_2,j_2 do not, and we can write

$$k_{ij} = \sum_\pi \mu_{ij}(\pi)\, c_\pi$$

unambiguously, where π runs over all partitions of Ω into two parts of cardinality 3.

As mentioned at the end of Section 6, the space $\mathcal{I}_{0,+} \cap \operatorname{Sym}^2 \mathcal{L}(\Theta_+ + \Theta_-)$ is generated by the projection onto $\mathcal{L}^{(2)}_{0,+}$ of the quadratic forms $k_{12}^2 - k_{11}k_{22}$, $k_{12}k_{13} - k_{11}k_{23}$, $k_{13}^2 - k_{11}k_{33}$, $k_{13}k_{23} - k_{12}k_{33}$, $k_{23}^2 - k_{22}k_{33}$, and the quadric $g_{\mathcal{X}}$ in (5) that defines the model of $\mathcal{X}$ inside the 2-uple embedding of $\mathbb{P}^3$ into $\mathbb{P}^9$. These projections are

$$\begin{aligned}
&\sum_\pi (\mu_{12}(\pi)^2 - \mu_{11}(\pi)\mu_{22}(\pi))\, c_\pi * c_\pi,\\
&\sum_\pi (\mu_{12}(\pi)\mu_{13}(\pi) - \mu_{11}(\pi)\mu_{23}(\pi))\, c_\pi * c_\pi,\\
&\sum_\pi (\mu_{13}(\pi)^2 - \mu_{11}(\pi)\mu_{33}(\pi))\, c_\pi * c_\pi,\\
&\sum_\pi (\mu_{13}(\pi)\mu_{23}(\pi) - \mu_{12}(\pi)\mu_{33}(\pi))\, c_\pi * c_\pi,\\
&\sum_\pi (\mu_{23}^2(\pi) - \mu_{22}(\pi)\mu_{33}(\pi))\, c_\pi * c_\pi,\\
&\sum_\pi \mu_X(\pi)\, c_\pi * c_\pi,
\end{aligned}$$

with

$$\begin{aligned}
\mu_{\mathcal{X}} =&(-4f_0f_2 + f_1^2)\mu_{11}^2 - 4f_0f_3\mu_{11}\mu_{12} - 2f_1f_3\mu_{11}\mu_{13} - 4f_0\mu_{11}\mu_{14} - 4f_0f_4\mu_{12}^2 +\\
&(4f_0f_5 - 4f_1f_4)\mu_{12}\mu_{13} - 2f_1\mu_{11}\mu_{24} + (-4f_0f_6 + 2f_1f_5 - 4f_2f_4 + f_3^2)\mu_{13}^2 -\\
&4f_2\mu_{11}\mu_{34} - 4f_0f_5\mu_{12}\mu_{22} + (8f_0f_6 - 4f_1f_5)\mu_{13}\mu_{22} + (4f_1f_6 - 4f_2f_5)\mu_{13}\mu_{23} -\\
&2f_3\mu_{13}\mu_{24} - 2f_3f_5\mu_{13}\mu_{33} - 4f_4\mu_{13}\mu_{34} - 4\mu_{14}\mu_{34} - 4f_0f_6\mu_{22}^2 - 4f_1f_6\mu_{22}\mu_{23} -\\
&4f_2f_6\mu_{23}^2 + \mu_{24}^2 - 4f_3f_6\mu_{23}\mu_{33} - 2f_5\mu_{23}\mu_{34} + (-4f_4f_6 + f_5^2)\mu_{33}^2 - 4f_6\mu_{33}\mu_{34},
\end{aligned} \tag{24}$$

and where π runs again over all partitions of Ω into two parts of size 3. The three quadratic forms

$$\sum_\omega \omega^j \lambda_\omega c_\omega * c_\omega \tag{25}$$

for $j = 0, 1, 2$, mentioned in (18), are also contained in $\mathcal{I}_{0,+}$. The 12-dimensional space $\mathcal{I}_{0,+}$ is generated by these 9 quadratic forms and the projection onto $\mathcal{L}^{(2)}_{0,+}$ of the forms given in (7). These projections are

$$\sum_{\omega\in\Omega} \omega^r c_\omega * c_\omega - \sum_\pi \nu_r(\pi)\, c_\pi * c_\pi$$

for $r = 0, \dots, 6$ respectively, with

$$\begin{aligned}
\nu_0 &= f_2\mu_{11}^2 + f_3\mu_{11}\mu_{12} + \mu_{11}\mu_{14} + f_6\mu_{11}\mu_{33} + f_4\mu_{12}^2 - f_5\mu_{12}\mu_{13} + f_5\mu_{12}\mu_{22} - 2f_6\mu_{13}\mu_{22} + f_6\mu_{22}^2,\\
2\nu_1 &= -f_1\mu_{11}^2 + f_3\mu_{11}\mu_{13} + 2f_4\mu_{11}\mu_{23} + \mu_{11}\mu_{24} - f_5\mu_{11}\mu_{33} - 2f_6\mu_{12}\mu_{33} + 2f_5\mu_{13}\mu_{22} + 2f_6\mu_{22}\mu_{23},\\
\nu_2 &= f_0\mu_{11}^2 + f_4\mu_{13}^2 + \mu_{13}\mu_{14} + f_5\mu_{13}\mu_{23} + f_6\mu_{22}\mu_{33},\\
2\nu_3 &= 2f_0\mu_{11}\mu_{12} + f_1\mu_{11}\mu_{13} - f_3\mu_{13}^2 + \mu_{13}\mu_{24} + f_5\mu_{13}\mu_{33} + 2f_6\mu_{23}\mu_{33},\\
\nu_4 &= f_0\mu_{11}\mu_{22} + f_1\mu_{11}\mu_{23} + f_2\mu_{11}\mu_{33} + \mu_{14}\mu_{33} + f_6\mu_{33}^2,\\
2\nu_5 &= -f_1\mu_{11}\mu_{33} - 2f_0\mu_{12}\mu_{13} + 2f_0\mu_{12}\mu_{22} + 2f_2\mu_{12}\mu_{33} + 2f_1\mu_{13}\mu_{22} + f_3\mu_{13}\mu_{33} + \mu_{24}\mu_{33} - f_5\mu_{33}^2,\\
\nu_6 &= f_0\mu_{11}\mu_{33} - 2f_0\mu_{13}\mu_{22} - f_1\mu_{13}\mu_{23} + f_0\mu_{22}^2 + f_1\mu_{22}\mu_{23} + f_2\mu_{23}^2 + f_3\mu_{23}\mu_{33} + f_4\mu_{33}^2 + \mu_{33}\mu_{34}.
\end{aligned}$$

Note that all 16 quadratic forms in $\mathcal{I}_{0,+}$ given in this appendix are Galois invariant and can therefore also be expressed in the coordinates $k_{11}, k_{12}, \dots, k_{44}, b_1, \dots, b_6$ with coefficients in the ground field k.

Appendix B. Galois-invariant equations for the twist of the Jacobian

We continue with the notation of Section 7. In particular we have $\xi \in P^1(J[2]) \subset \mathrm{H}^1(J[2])$ and $\delta \in L$ and $n \in k$, such that $N_{L/k}(\delta) = n^2$ and such that $\gamma\big((\delta, n)\big) = \overline{\xi}$ with γ as in Proposition 2.6. We also have an element $\varepsilon \in L^{\mathrm{s}}$ such that $\varepsilon^2 = \delta$ and $N_{L^{\mathrm{s}}/k^{\mathrm{s}}}(\varepsilon) = n$, and A_ξ is the two-covering associated to ξ.

In this appendix we combine the previously given equations for A_ξ to Galois-invariant equations in terms of Galois-invariant coordinates. For the odd coordinates we use $b_1, \ldots, b_6$ as before. For the even coordinates we do not use a specific system as it seems very plausible that the equations can be expressed more compactly in terms of other coordinates than $k_{11}, k_{12}, \ldots, k_{44}$.

Let $\rho_0, \ldots, \rho_9$ be functions from the set of all subsets of Ω of cardinality 3 to $k(\Omega)$ such that for each i and each I we have $\rho_i(I) = -\rho_i(\Omega \setminus I)$ and for each Galois automorphism σ we have $\sigma(\rho_i(I)) = \rho_i(\sigma(I))$ and such that if $I_1, ..., I_{10}$ are subsets of size 3 representing all partitions in two parts of size 3, then the matrix $H = (\rho_i(I_j))_{i,j}$ is invertible. Then there is a unique basis $(u_0, \ldots, u_9)$ of $\mathrm{Sym}^2(\Theta_+ + \Theta_-)$ of Galois-invariant elements determined by

$$c_I = \sum_{i=0}^{9} \rho_i(I)\, u_i$$

for all subsets $I \subset \Omega$ of size 3. This is the basis of $\mathrm{Sym}^2(\Theta_+ + \Theta_-)$ that we use, and it depends on the functions ρ_i. For instance, if we index the ρ_i and u_i by pairs i, j, abbreviated by ij, with $1 \le i \le j \le 4$, rather than by integers, and we set

$$\rho_{ij}(I) = \frac{\lambda_{ij}(I)}{4 \prod_{\omega \in I} \prod_{\psi \notin I} (\psi - \omega)},$$

with λ_{ij} as in Definition 6.12, then we get $u_{ij} = k_{ij}$.

Remark B.1. *Note that if in a specific case the set of ten partitions into two parts of size three is the disjoint union of smaller Galois orbits, then for each Galois orbit T we could find a basis of Galois-invariant elements for the space generated by $\{c_\pi \,:\, \pi \in T\}$. This may yield more efficient equations than those coming from the general case.*

Choose 15 functions $h_1, \ldots, h_{15}$ from the set $J[2](k^{\mathrm{s}}) \setminus \{0\}$, or equivalently, the set of the 15 unordered pairs $\{\omega_1, \omega_2\} \subset \Omega$, to $k(\Omega)$ so that each h_r is Galois equivariant (i.e., for each $P \in J[2](k^{\mathrm{s}}) \setminus \{0\}$ and each Galois automorphism σ we have $h_r(\sigma(P)) = \sigma(h_r(P))$) and such that the matrix

$$\Big(h_r(P)\Big)_{\substack{1 \le r \le 15 \\ P \in J[2](k^{\mathrm{s}}) \setminus \{0\}}}$$

is invertible. Then for fixed $l \in \{0, 1\}$ the 15-dimensional subspace of $\mathrm{Sym}^2 \mathcal{L}$ generated by all quadratic forms of the form (21) with nonzero $P \in J[2](k^{\mathrm{s}})$ is also generated by the 15 quadratic forms

$$\begin{aligned}
&\sum_{P \leftrightarrow \{\omega_1, \omega_2\}} h_r(P) \left(\sum_{\theta \neq \omega_1, \omega_2} \Big(\theta^l \prod_{\psi \neq \theta, \omega_1, \omega_2} (\theta - \psi)\Big) (\delta_{\omega_1} \delta_{\omega_2} \delta_\theta + n)\, c_\theta * c_{\omega_1 \omega_2 \theta} \right) \\
&= \sum_{P \leftrightarrow \{\omega_1, \omega_2\}} h_r(P) \left(\sum_{\theta \neq \omega_1, \omega_2} \Big(\theta^l \prod_{\psi \neq \theta, \omega_1, \omega_2} (\theta - \psi)\Big) (\delta_{\omega_1} \delta_{\omega_2} \delta_\theta + n) \Big(\sum_{j=1}^{6} (S^{-1})_{\theta j} \cdot b_j \Big) * \Big(\sum_{i=0}^{9} \rho_i(\{\omega_1, \omega_2, \theta\})\, u_i \Big) \right) \\
&= \sum_{j=1}^{6} \sum_{i=0}^{9} \left(\sum_{\{\omega_1, \omega_2\}} h_r(P) \sum_{\theta \neq \omega_1, \omega_2} (S^{-1})_{\theta j} \Big(\theta^l \prod_{\psi \neq \theta, \omega_1, \omega_2} (\theta - \psi)\Big) \rho_i(\{\omega_1, \omega_2, \theta\})\, (\delta_{\omega_1} \delta_{\omega_2} \delta_\theta + n) \right) b_j * u_i
\end{aligned}$$

with $1 \le r \le 15$, where $(S^{-1})_{\theta j}$ is the entry in the row corresponding to θ and column j in the inverse of the matrix

$$S = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \omega_1 & \omega_2 & \cdots & \omega_6 \\ \vdots & \vdots & & \vdots \\ \omega_1^5 & \omega_2^5 & \cdots & \omega_6^5 \end{pmatrix}.$$

For each $l \in \{0,1\}$ these 15 quadratic forms are all Galois invariant.

Remark B.2. *Note that in specific cases, instead of summing over all nontrivial two-torsion points, in order to obtain Galois-invariant quadratic forms, it suffices to sum over all points in a Galois orbit; each orbit yields a quadratic form for each h_r, so that fewer than 15 functions h_r will suffice.*

Similarly, the subspace of $\mathrm{Sym}^2 \mathcal{L}$ generated by all quadratic forms of the form (22) with nonzero $P \in J[2](k^{\mathrm{s}})$ is also generated by the 15 quadratic forms

$$\sum_{i=0}^{9}\sum_{j=0}^{9}\left(\sum_{\{\omega_1,\omega_2\}} h_r(P) \sum_{\pi=\{\{\theta_1,\theta_2\},\{\psi_1,\psi_2\}\}} \nu(\pi)\,\rho_i(\{\theta_1,\theta_2,\omega_1\})\rho_j(\{\theta_1,\theta_2,\omega_2\})\cdot \right.$$
$$\left. (\delta_{\omega_1}\delta_{\omega_2}(\delta_{\theta_1}\delta_{\theta_2}+\delta_{\psi_1}\delta_{\psi_2})+n(\delta_{\omega_1}+\delta_{\omega_2}))\right) u_i * u_j$$

for $1 \le r \le 15$, each defined over k. And finally, the subspace of $\mathrm{Sym}^2 \mathcal{L}$ generated by all quadratic forms of the form (23) with nonzero $P \in J[2](k^{\mathrm{s}})$ is also generated by the 15 quadratic forms

$$\sum_{i=1}^{6}\sum_{j=1}^{6}\left(\sum_{\{\omega_1,\omega_2\}} h_r(P)(S^{-1})_{\omega_1 i}(S^{-1})_{\omega_2 j}\right) b_i * b_j$$
$$+ f_6 \cdot \sum_{i=0}^{9}\sum_{j=0}^{9}\left(\sum_{\{\omega_1,\omega_2\}} h_r(P) \sum_{\pi=\{\{\theta_1,\theta_2\},\{\psi_1,\psi_2\}\}} \nu(\pi)(\theta_1+\theta_2)(\psi_1+\psi_2)\,\rho_i(\{\theta_1,\theta_2,\omega_1\})\rho_j(\{\theta_1,\theta_2,\omega_2\})\cdot \right.$$
$$\left. (\delta_{\omega_1}\delta_{\omega_2}(\delta_{\theta_1}\delta_{\theta_2}+\delta_{\psi_1}\delta_{\psi_2})+n(\delta_{\omega_1}+\delta_{\omega_2}))\right) u_i * u_j$$

for $1 \le r \le 15$, each defined over the ground field k. All together, in this appendix we have seen 60 Galois-invariant quadratic forms generating the subspace of $\bigoplus_{P\neq 0} \mathcal{L}_P^{(2)} \subset \mathrm{Sym}^2 \mathcal{L}$ consisting of those forms that vanish on A_ξ. Recall that for each subset $I \subset \Omega$ of size 3, the element

$$t_I^2 = \prod_{\omega\in I} \delta_\omega + \prod_{\omega\notin I} \delta_\omega + 2n$$

is defined over $k(\Omega)$, with $\delta_\omega = \varphi_\omega(\delta)$. The 12-dimensional subspace of $\mathcal{L}_{0,+}^{(2)}$ of quadratic forms vanishing on A_ξ is generated by the forms obtained from those in Appendix A by substitution of $t_I c_I$ for c_I for each I. These new forms are

$$\sum_{\pi}(\mu_{12}(\pi)^2-\mu_{11}(\pi)\mu_{22}(\pi))\big(\prod_{\omega\in\pi_1}\delta_\omega+\prod_{\omega\in\pi_2}\delta_\omega+2n\big)\,c_\pi * c_\pi,$$
$$=\sum_{i=0}^{9}\sum_{j=0}^{9}\left(\sum_{\pi}(\mu_{12}(\pi)^2-\mu_{11}(\pi)\mu_{22}(\pi))\rho_i(\pi_1)\rho_j(\pi_1)\big(\prod_{\omega\in\pi_1}\delta_\omega+\prod_{\omega\in\pi_2}\delta_\omega+2n\big)\right) u_i * u_j$$

and, similary,

$$\sum_{i=0}^{9}\sum_{j=0}^{9}\left(\sum_{\pi}(\mu_{12}(\pi)\mu_{13}(\pi)-\mu_{11}(\pi)\mu_{23}(\pi))\rho_i(\pi_1)\rho_j(\pi_1)\big(\prod_{\omega\in\pi_1}\delta_\omega+\prod_{\omega\in\pi_2}\delta_\omega+2n\big)\right)u_i*u_j,$$

$$\sum_{i=0}^{9}\sum_{j=0}^{9}\left(\sum_{\pi}(\mu_{13}(\pi)^2-\mu_{11}(\pi)\mu_{33}(\pi))\rho_i(\pi_1)\rho_j(\pi_1)\big(\prod_{\omega\in\pi_1}\delta_\omega+\prod_{\omega\in\pi_2}\delta_\omega+2n\big)\right)u_i*u_j,$$

$$\sum_{i=0}^{9}\sum_{j=0}^{9}\left(\sum_{\pi}(\mu_{13}(\pi)\mu_{23}(\pi)-\mu_{12}(\pi)\mu_{33}(\pi))\rho_i(\pi_1)\rho_j(\pi_1)\big(\prod_{\omega\in\pi_1}\delta_\omega+\prod_{\omega\in\pi_2}\delta_\omega+2n\big)\right)u_i*u_j,$$

$$\sum_{i=0}^{9}\sum_{j=0}^{9}\left(\sum_{\pi}(\mu_{23}^2(\pi)-\mu_{22}(\pi)\mu_{33}(\pi))\rho_i(\pi_1)\rho_j(\pi_1)\big(\prod_{\omega\in\pi_1}\delta_\omega+\prod_{\omega\in\pi_2}\delta_\omega+2n\big)\right)u_i*u_j,$$

$$\sum_{i=0}^{9}\sum_{j=0}^{9}\left(\sum_{\pi}\mu_{\mathcal{X}}(\pi)\rho_i(\pi_1)\rho_j(\pi_1)\big(\prod_{\omega\in\pi_1}\delta_\omega+\prod_{\omega\in\pi_2}\delta_\omega+2n\big)\right)u_i*u_j,$$

and

$$\sum_{i=1}^{6}\sum_{j=1}^{6}\left(\sum_{\omega}\omega^r\lambda_\omega(S^{-1})_{\omega i}(S^{-1})_{\omega j}\delta_\omega\right)b_i*b_j$$

for $0\le r\le 2$ and

$$\sum_{i=1}^{6}\sum_{j=1}^{6}\left(\sum_{\omega}\omega^r(S^{-1})_{\omega i}(S^{-1})_{\omega j}\delta_\omega\right)b_i*b_j-$$
$$\sum_{i=0}^{9}\sum_{j=0}^{9}\left(\sum_{\pi}\nu_r(\pi)\rho_i(\pi_1)\rho_j(\pi_1)\big(\prod_{\omega\in\pi_1}\delta_\omega+\prod_{\omega\in\pi_2}\delta_\omega+2n\big)\right)u_i*u_j$$

for $0\le r\le 6$ with $\nu_r(\pi)$ as in Appendix A. These quadratic polynomials are all defined over the ground field k and so we have found a set of Galois-invariant quadratic forms that generate the ideal of polynomials vanishing on A_ξ.

Remark B.3. *If $\delta\in L=k[X]/(f)$ is given as $\delta=\sum_{i=0}^{5}d_iX^i$, then we have $\delta_\omega=\sum_{i=0}^{5}d_i\omega^i$ for each ω. Thus the given quadratic forms in terms of the coordinates $u_0,\dots,u_9,b_1,\dots,b_6$ have coefficients that are themselves polynomials in terms of $d_0,\dots,d_5$ and n with coefficients that are symmetric in the roots of f, so these coefficients can be expressed in terms of $f_0,\dots,f_6$.*

After finding Galois-invariant equations for the two-covering A_ξ, we end by giving the associated map $A_\xi\to J$ that is a twist of multiplication by 2 on J. Let G be the matrix whose r-th row is

$$\frac{1}{4}\left(\prod_{\omega\in I_r}\prod_{\psi\in\Omega\setminus I_r}(\psi-\omega)^{-1}\right)\cdot\begin{pmatrix}\lambda_{11}(I_r) & \lambda_{12}(I_r) & \lambda_{13}(I_r) & \cdots & \lambda_{44}(I_r)\end{pmatrix},$$

i.e., the coefficients of c_{I_r} with respect to the basis $(k_{11},k_{12},\dots,k_{44})$. Then G^{-1} is described in the proof of Proposition 6.13. Let H be the invertible matrix whose r-th row is

$$\begin{pmatrix}\rho_0(I_r) & \rho_1(I_r) & \rho_2(I_r) & \cdots & \rho_9(I_r)\end{pmatrix}.$$

Let T_1 be the diagonal matrix whose r-th diagonal entry is t_{I_r} for $1\le r\le 10$, and let T_2 be the diagonal matrix whose r-th diagonal entry is $t_{\{\omega_r\}}$ for $1\le r\le 6$, where the elements of Ω are numbered as in the definition of the matrix S. Then the isomorphism $g\colon (A_\xi)_{k^s}\to J_{k^s}$ of Section 7 is given by

$$(u_0:\cdots:u_9:b_1:\cdots:b_6)\mapsto(k_{11}:k_{12}:\cdots:k_{44}:b_1':\cdots:b_6')$$

with $(k_{11},k_{12},\dots,k_{44})^{\mathrm{t}}=G^{-1}T_1H(u_0,\dots,u_9)^{\mathrm{t}}$ and $(b_1',\dots,b_6')^{\mathrm{t}}=ST_2S^{-1}(b_1,\dots,b_6)^{\mathrm{t}}$. This map depends on the choice of ε, but the composition $[2]\circ g$ does not. This composition is defined over k and endows A_ξ with the structure of a two-covering by Theorem 7.4.

References

[1] A. Beauville. *Complex Algebraic Surfaces*, volume 34 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1996.

[2] N. Bruin and M. Stoll. The Mordell-Weil sieve: Proving non-existence of rational points on Curves. In preparation.

[3] J.W.S. Cassels. The Mordell-Weil Group of Curves of Genus 2. *Arithmetic and Geometry papers dedicated to I.R. Shafarevich on the occasion of his sixtieth birthday*, Vol. **1.** Arithmetic, 29–60, Birkhäuser, Boston, 1983.

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

[5] R.F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[6] N.D. Elkies. Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 33–63. Springer, Berlin, 2000.

[7] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[8] E.V. Flynn, B. Poonen, and E.F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Math. J.*, 90(3):435–463, 1997.

[9] E.V. Flynn. The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. *Math. Proc. Cambridge Philos. Soc.*, 107(3):425–441, 1990.

[10] E.V. Flynn. Defining equations of the Jacobian. `people.maths.ox.ac.uk/~flynn/genus2/jacobian.variety/defining.equations`.

[11] E.V. Flynn. The Hasse principle and the Brauer-Manin obstruction for curves. *Manuscripta Math.*, 115:437–466, 2004.

[12] D.M. Gordon and D. Grant. Computing the Mordell-Weil rank of Jacobians of curves of genus two. *Trans. Amer. Math. Soc.*, 337(2):807–824, 1993.

[13] D. Grant. Formal groups in genus two. *J. Reine Angew. Math.*, 411:96–121, 1990.

[14] T. Katsura. Generalized Kummer surfaces and their unirationality in characteristic *p*. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 34(1):1–41, 1987.

[15] A. Logan and R. van Luijk. Nontrivial elements of Sha explained through $K3$ surfaces. *Math. Comp.*, 78(265):441–483, 2009.

[16] J.S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

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

[18] B. Poonen. Heuristics for the Brauer-Manin obstruction for curves. *Experiment. Math.*, 15(4):415–420, 2006.

[19] B. Poonen and E.F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.*, 488:141–188, 1997.

[20] E.F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. *J. Number Theory*, 51:219–232, 1995.

[21] V. Scharaschkin. Local Global Problems and the Brauer-Manin Obstruction. PhD Thesis, University of Michigan, 1999.

[22] J.-P. Serre. *A course in arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1973. Translated from the French.

[23] J.-P. Serre. *Linear representations of finite groups*, volume 42 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott,

[24] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[25] J.-P. Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, English edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[26] A. Skorobogatov. *Torsors and rational points*, volume 144 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2001.

[27] M. Stoll. On the height constant for curves of genus two. *Acta Arith.*, 90(2):183–201, 1999.

[28] M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001.

Mathematical Institute, University of Oxford, 24-29 St Giles', OX1 3LB, Oxford, UK
E-mail address: `flynn@maths.ox.ac.uk`
E-mail address: `testa@maths.ox.ac.uk`

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA, Leiden, The Netherlands
E-mail address: `rvl@math.leidenuniv.nl`