Math. Proc. Camb. Phil. Soc. (2024), **177**, 415–437
doi:10.1017/S0305004124000318
First published online 6 December 2024

Computing the Cassels–Tate pairing for genus two jacobians with rational two-torsion points

BY JIALI YAN
University of Cambridge, 28 Howards Lane, SW15 6NQ, London.
e-mail: jialiyan.lele@gmail.com

(*Received* 24 *January* 2022*; revised* 20 *March* 2024*; accepted* 12 *September* 2024)

Abstract

In this paper, we give an explicit formula as well as a practical algorithm for computing the Cassels–Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ where J is the Jacobian variety of a genus two curve under the assumption that all points in $J[2]$ are K-rational. We also give an explicit formula for the Obstruction map $\mathrm{Ob}: H^1(G_K, J[2]) \to \mathrm{Br}(K)$ under the same assumption. Finally, we include a worked example demonstrating that we can improve the rank bound given by a 2-descent via computing the Cassels–Tate pairing.

2020 Mathematics Subject Classification: 11G30 (Primary); 11G10 (Secondary)

1. *Introduction*

For any principally polarised abelian variety A defined over a number field K, Cassels and Tate [Cas59], [Cas62] and [Tat62] constructed a pairing

$$Ш(A) \times Ш(A) \to \mathbb{Q}/\mathbb{Z},$$

that is nondegenerate after quotienting out by the maximal divisible subgroup of $Ш(A)$. This pairing is called the Cassels–Tate pairing and it naturally lifts to a pairing on Selmer groups. One application of this pairing is in improving the bound on the Mordell–Weil rank $r(A)$ obtained by performing a standard descent calculation. More specifically, since the map $Ш(A)/nШ(A) \mapsto (Ш(A)[n])^*$ is injective, which is the middle vertical map in the diagram on page 88 of [Mil06], the kernel of the Cassels–Tate pairing on $\mathrm{Sel}^n(A) \times \mathrm{Sel}^n(A)$ is equal to the image of the natural map $\mathrm{Sel}^{n^2}(A) \to \mathrm{Sel}^n(A)$ induced from the map $A[n^2] \xrightarrow{n} A[n]$. This shows that carrying out an n-descent and computing the Cassels–Tate pairing on $\mathrm{Sel}^n(A) \times \mathrm{Sel}^n(A)$ gives the same rank bound as obtained from n^2-descent where $\mathrm{Sel}^{n^2}(A)$ needs to be computed.

There have been many results on computing the Cassels–Tate pairing in the case of elliptic curves, such as [Cas98], [Don15], [Fis16], [vB], [vBF18], [Fis03], [FN14]. We are interested in the natural problem of generalising the different algorithms for computing the Cassels–Tate pairing for elliptic curves to compute the pairing for abelian varieties of higher dimensions.

In Section 2, we give the preliminary results needed for the later sections, including the homogeneous space definition of the Cassels–Tate pairing. In Section 3, we state and prove an explicit formula for the pairing $\langle\ ,\ \rangle_{CT}$ on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ where J is the Jacobian variety of a genus two curve under the assumption that all points in $J[2]$ are K-rational. In Section 4, we describe a practical algorithm for computing the pairing $\langle\ ,\ \rangle_{CT}$ using the formula in Section 3. In Section 5, we also give an explicit formula for the Obstruction map $\mathrm{Ob}: H^1(G_K, J[2]) \to \mathrm{Br}(K)$ under the assumption that all points in $J[2]$ are defined over K generalising the result in the elliptic curve case [**O'N02**, proposition 3·4], [**Cla05**, theorem 6]. Finally, in Section 7, we include a worked example demonstrating that computing the Cassels–Tate pairing can indeed improve the rank bound coming from a 2-descent to the rank bound coming from a 4-descent. The content of this paper is based on Chapter 4 of the thesis of the author [**Yan**].

2. *Preliminary Results*

2·1. *The set-up*

In this paper, we are working over a number field K. For any field k, we let $\bar{k}$ denote its algebraic closure and let $\mu_n \subset \bar{k}$ denote the n^{th} roots of unity in $\bar{k}$. We let G_k denote the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$.

Let $\mathcal{C}$ be a general *genus two curve* defined over K, which is a smooth projective curve. It can be given in the following hyperelliptic form:

$$\mathcal{C}: y^2 = f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

where $f_i \in K, f_6 \neq 0$ and the discriminant $\triangle(f) \neq 0$, which implies that f has distinct roots in $\bar{K}$. Note that we choose to not use the quintic representation of the genus 2 curve because using the degree 6 form simplifies some computations and makes the final formula slightly more symmetric and elegant.

We let J denote the *Jacobian variety* of $\mathcal{C}$, which is an abelian variety of dimension two defined over K that can be identified with $\mathrm{Pic}^0(\mathcal{C})$. We denote the identity element of J by $\mathcal{O}_J$. We also denote the two points at infinity on $\mathcal{C}$ by ∞^+, ∞^-. Via the natural isomorphism $\mathrm{Pic}^2(\mathcal{C}) \to \mathrm{Pic}^0(\mathcal{C})$ sending $[P_1 + P_2] \mapsto [P_1 + P_2 - \infty^+ - \infty^-]$, a point $P \in J$ can be identified with an unordered pair of points of $\mathcal{C}$, $\{P_1, P_2\}$. This identification is unique unless $P = \mathcal{O}_J$, in which case it can be represented by any pair of points on $\mathcal{C}$ in the form $\{(x, y), (x, -y)\}$ or $\{\infty^+, \infty^-\}$. Suppose the roots of f are denoted by $\omega_1, ..., \omega_6$ and let $(\omega_1, 0), ..., (\omega_6, 0)$ be all the *Weierstrass points* on $\mathcal{C}$. Then $J[2] = \{\mathcal{O}_J, \{(\omega_i, 0), (\omega_j, 0)\}$ for $i \neq j\}$. Also, for a point $P \in J$, we let $\tau_P : J \to J$ denote the translation by P on J.

As described in [**CF96**, chapter 3, section 3], suppose $\{P_1, P_2\}$and $\{Q_1, Q_2\}$ represent $P, Q \in J[2]$ where P_1, P_2, Q_1, Q_2 are Weierstrass points. Then the Weil paring is given by the formula

$$e_2(P, Q) = (-1)^{|\{P_1,P_2\} \cap \{Q_1,Q_2\}|}.$$

2·2. *Theta divisor and Kummer surface*

A *theta divisor*, denoted by Θ, is defined to be any divisor on J that is the image of the divisor $\{P\} \times \mathcal{C} + \mathcal{C} \times \{P\}$ on $\mathrm{Sym}^2\mathcal{C}$ under the birational morphism $\mathrm{Sym}^2\mathcal{C} \to J$, for some Weierstrass point $P \in \mathcal{C}$. The Jacobian variety J is a principally polarised abelian variety via $\lambda : J \to J^\vee$ sending $Q \in J$ to $[\tau_Q^*\Theta - \Theta]$. It can be checked that $2\Theta \sim \Theta^+ + \Theta^-$, where Θ^+ denotes the divisor on J that corresponds to the divisor $\{\infty^+\} \times \mathcal{C} + \mathcal{C} \times \{\infty^+\}$ on $\mathcal{C} \times \mathcal{C}$

and similarly for Θ^-. In particular, this implies that the divisor class of $2n\Theta$ is defined over the base field K, for any positive integer n.

The *Kummer surface*, denoted by $\mathcal{K}$, is the quotient of J via the involution $[-1] : P \mapsto -P$. The fixed points under the involution are the 16 points of order dividing 2 on J and these map to the 16 nodal singular points of $\mathcal{K}$ (the *nodes*). General theory, as in [**Mil08**, theorem 11·1], [**Mum70**, page 150], shows that the linear system of $n\Theta$ on J has dimension n^2. Moreover, $|2\Theta|$ is base point free and induces a morphism from J to $\mathbb{P}^3$ defined over K while $|4\Theta|$ is very ample and induces an embedding from J to $\mathbb{P}^{15}$ defined over K.

2·3. *Explicit embeddings of J and $\mathcal{K}$*

From Section 2·2, we know that $\dim \mathcal{L}(2\Theta) = 4$ and $2\Theta \sim \Theta^+ + \Theta^-$. Let $\{k_1, k_2, k_3, k_4\}$ denote the basis of $\mathcal{L}(\Theta^+ + \Theta^-)$ as defined in [**CF96**, chapter 3, section 1]. We will restate the definition here for completeness. Denote a generic point on the Jacobian J of $\mathcal{C}$ by $\{(x, y), (u, v)\}$. There is then a morphism from J to $\mathbb{P}^3$ given by

$$k_1 = 1, k_2 = (x + u), k_3 = xu, k_4 = \beta_0,$$

where

$$\beta_0 = \frac{F_0(x, u) - 2yv}{(x - u)^2}$$

with $F_0(x, u) = 2f_0 + f_1(x + u) + 2f_2(xu) + f_3(x + u)(xu) + 2f_4(xu)^2 + f_5(x + u)(xu)^2 + 2f_6(xu)^3$. The image of this morphism is the Kummer surface $\mathcal{K} \subset \mathbb{P}^3$ defined by the vanishing of the quartic polynomial $G(k_1, k_2, k_3, k_4)$ as specified in [**CF96**, chapter 3, section 1]. From now on, we denote this morphism by $J \overset{|2\Theta|}{\to} \mathcal{K} \subset \mathbb{P}^3$. We note that it maps $\mathcal{O}_J$ to $(0 : 0 : 0 : 1)$.

Remark 2·1. Suppose $P \in J[2]$. Since the polarisation map λ is a group homomorphism, we have $\tau_P^*(2\Theta) \sim 2\Theta$. This implies that translation by P on J induces a linear isomorphism on $\mathcal{K} \subset \mathbb{P}^3$.

We now look at the embedding of J in $\mathbb{P}^{15}$ induced by $|4\Theta|$. Let $k_{ij} = k_i k_j$, for $1 \leq i \leq j \leq 4$. Since $\mathcal{K}$ is irreducible and defined by a polynomial of degree 4, $k_{11}, k_{12}, ..., k_{44}$ are 10 linearly independent even elements in $\mathcal{L}(2\Theta^+ + 2\Theta^-)$. Six further odd basis elements $b_1, b_2, ...b_6$ in $\mathcal{L}(2\Theta^+ + 2\Theta^-)$ are given explicitly in [**FTvL12**, section 3]. A function g on J is *even* when it is invariant under the involution $[-1] : P \mapsto -P$ and is *odd* when $g \circ [-1] = -g$.

Unless stated otherwise, we will use the basis $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$ for $\mathcal{L}(2\Theta^+ + 2\Theta^-)$ to embed J in $\mathbb{P}^{15}$. The following theorem gives the defining equations of J.

THEOREM 2·2 ([**Fly90**, therorem 1·2], [**Fly93**, therorem 1·2]). *Let J be the Jacobian variety of the genus two curve $\mathcal{C}$ defined by $y^2 = f_6x^6 + ... + f_1x + f_0$. The 72 quadratic forms over $\mathbb{Z}[f_0, ..., f_6]$ given in* [**Fly90**, appendix A] *are a set of defining equations for the projective variety given by the embedding of J in $\mathbb{P}^{15}$ induced by the basis of $\mathcal{L}(2\Theta^+ + 2\Theta^-)$ with explicit formulae given in* [**Fly90**, definition 1·1] *or* [**Fly93**, definition 1·1]. *The change of basis between this basis of $\mathcal{L}(2\Theta^+ + 2\Theta^-)$ and $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$ is given in* [**FTvL12**, section 3].

2·4. *Principal homogeneous spaces and 2-coverings*

A *principal homogeneous space* or *torsor* for J defined over a field K is a variety V together with a morphism $\mu : J \times V \to V$, both defined over K, that induces a simply transitive action on the $\bar{K}$-points.

We say (V_1, μ_1) and (V_2, μ_2) are isomorphic over a field extension K_1 of K if there is an isomorphism $\phi : V_1 \to V_2$ defined over K_1 that respects the action of J.

A 2-*covering* of J is a variety X defined over K together with a morphism $\pi : X \to J$ defined over K, such that there exists an isomorphism $\phi : X \to J$ defined over $\bar{K}$ with $\pi = [2] \circ \phi$. An isomorphism $(X_1, \pi_1) \to (X_2, \pi_2)$ between two 2-coverings is an isomorphism $h : X_1 \to X_2$ defined over K with $\pi_1 = \pi_2 \circ h$. We sometimes denote (X, π) by X when the context is clear.

It can be checked that a 2-covering is a principal homogeneous space. The short exact sequence $0 \to J[2] \to J \xrightarrow{2} J \to 0$ induces the connecting map in the long exact sequence

$$\delta : J(K) \to H^1(G_K, J[2]). \tag{2·1}$$

The following two propositions are proved in [FTvL12].

PROPOSITION 2·3 [FTvL12, lemma 2·14] *Let (X, π) be a 2-covering of J defined over K and choose an isomorphism $\phi : X \to J$ such that $\pi = [2] \circ \phi$. Then for each $\sigma \in G_K$, there is a unique point $P \in J[2](\bar{K})$ satisfying $\phi \circ \sigma(\phi^{-1}) = \tau_P$. The map $\sigma \mapsto P$ is a cocycle whose class in $H^1(G_K, J[2])$ does not depend on the choice of ϕ. This yields a bijection between the set of isomorphism classes of 2-coverings of J and the set $H^1(G_K, J[2])$.*

PROPOSITION 2·4 [FTvL12, proposition 2·15] *Let X be a 2-covering of J corresponding to the cocycle class $\epsilon \in H^1(G_K, J[2])$. Then X contains a K-rational point (equivalently X is a trivial principal homogeneous space) if and only if ϵ is in the image of the connecting map δ in* (2·1).

We also state and prove the following proposition which is useful for the computation of the Cassels–Tate pairing later in Sections 4·2 and 4·3. A *Brauer–Severi* variety is a variety defined over K that is isomorphic to a projective space over $\bar{K}$.

PROPOSITION 2·5. *Let (X, π) be a 2-covering of J, with $\phi \circ [2] = \pi$. Then the linear system $|\phi^*(2\Theta)|$ determines a map $X \to S$ defined over K, where S is a Brauer–Severi variety. Also, there exists an isomorphism ψ defined over $\bar{K}$ making the following diagram commute*:

$$\begin{tikzcd} X \arrow[r, "|\phi^*(2\Theta)|"] \arrow[d, "\phi"] & S \arrow[d, "\psi"] \\ J \arrow[r, "|2\Theta|"] & \mathbb{P}^3. \end{tikzcd} \tag{2·2}$$

In particular, if (X, π) corresponds to a Selmer element via the correspondence in Proposition 2·3*, then the Brauer–Severi variety S is isomorphic to $\mathbb{P}^3$.*

Proof. Since (X, π) is a 2-covering of J, by Proposition 2·3, we have that for each $\sigma \in G_K$, $\phi \circ (\phi^{-1})^\sigma = \tau_P$ for some $P \in J[2]$. By Remark 2·1, we have $\tau_P^*(2\Theta) \sim 2\Theta$ which implies that $\phi^*(2\Theta) \sim (\phi^\sigma)^*(2\Theta)$, hence the morphism induced by $|\phi^*(2\Theta)|$ is defined over K.

Now if (X,π) corresponds to a Selmer element, then X everywhere locally has a point by Proposition 2·4, and hence S everywhere locally has a point. Since the Hasse principle holds for Brauer–Severi varieties by [**CM96**, corollary 2·6], we know that S has a point over K and hence it is isomorphic to $\mathbb{P}^3$ by [**GS06**, theorem 5·1·3].

We now make some observations and give some notation.

Remark 2·6. Let $\epsilon \in \mathrm{Sel}^2(J)$, and let $(J_\epsilon, \pi_\epsilon)$ denote the 2-covering corresponding to ϵ. There exists an isomorphism ϕ_ϵ defined over $\bar{K}$ such that $[2]\circ\phi_\epsilon = \pi_\epsilon$. Then, by Proposition 2·5, we have the following commutative diagram:

$$\begin{tikzcd}
J_\epsilon \arrow[r, "|\phi_\epsilon^*(2\Theta)|"] \arrow[d, "\phi_\epsilon"] & \mathbb{P}^3 \arrow[d, "\psi_\epsilon"] \\
J \arrow[r, "|2\Theta|"] & \mathbb{P}^3.
\end{tikzcd} \qquad (2·3)$$

The image of J_ϵ under the morphism induced by $|\phi_\epsilon^*(2\Theta)|$ is a surface, denoted by $\mathcal{K}_\epsilon$, which we call the *twisted Kummer surface* corresponding to ϵ. Also ψ_ϵ is a linear isomorphism $\mathbb{P}^3 \to \mathbb{P}^3$ defined over $\bar{K}$, and $\psi_\epsilon|_{\mathcal{K}_\epsilon} : \mathcal{K}_\epsilon \to \mathcal{K}$ is also an isomorphism over $\bar{K}$. For simplicity of notation later, we may also refer to this map from $\mathcal{K}_\epsilon \to \mathcal{K}$ as ψ_ϵ

Notation 2·7 Suppose $(J_\epsilon, \pi_\epsilon)$ is the 2-covering of J corresponding to $\epsilon \in H^1(G_K, J[2])$. The involution $[-1]: P \mapsto -P$ on J induces an involution ι_ϵ on J_ϵ such that $\phi_\epsilon \circ \iota_\epsilon = [-1]\circ\phi_\epsilon$, where $[2]\circ\phi_\epsilon = \pi_\epsilon$. Moreover, the degree two morphism $J_\epsilon \xrightarrow{|\phi_\epsilon^*(2\Theta)|} \mathcal{K}_\epsilon \subset \mathbb{P}^3$ in (2·3) is precisely the quotient by ι_ϵ and so an alternative definition of $\mathcal{K}_\epsilon$ is as the quotient of J_ϵ by ι_ϵ. We call a function g on J_ϵ *even* if it is invariant under ι_ϵ and *odd* if $g\circ\iota_\epsilon = -g$.

2·5. *Definition of the Cassels–Tate Pairing*

There are four definitions of the Cassels–Tate pairing stated and proved equivalent in [**PS99**]. In this paper we will only be using the homogeneous space definition of the Cassels–Tate pairing. We recall this definition now. Suppose $a, a' \in Ш(J)$. Via the polarization λ, we get $a' \mapsto b$ where $b \in Ш(J^\vee)$ Let X be the (locally trivial) principal homogeneous space defined over K representing a. Then $\mathrm{Pic}^0(X_{\bar{K}})$ is canonically isomorphic as a G_K-module to $\mathrm{Pic}^0(J_{\bar{K}}) = J^\vee(\bar{K})$. Therefore, $b \in Ш(J^\vee) \subset H^1(G_K, J^\vee)$ represents an element in $H^1(G_K, \mathrm{Pic}^0(X_{\bar{K}}))$.

Now consider the exact sequence:

$$0 \to \bar{K}(X)^*/\bar{K}^* \to \mathrm{Div}^0(X_{\bar{K}}) \to \mathrm{Pic}^0(X_{\bar{K}}) \to 0.$$

We can then map b to an element $b' \in H^2(G_K, \bar{K}(X)^*/\bar{K}^*)$ using the long exact sequence associated to the short exact sequence above. Since K is a number field, we know that $H^3(G_K, \bar{K}^*) = 0$ as proved in [**CF67**, chapter VII, section 11·4]. So b' has a lift $f' \in H^2(G_K, \bar{K}(X)^*)$ via the long exact sequence induced by the short exact sequence $0 \to \bar{K}^* \to \bar{K}(X)^* \to \bar{K}(X)^*/\bar{K}^* \to 0:$

$$H^2(G_K, \bar{K}^*) \to H^2(G_K, \bar{K}(X)^*) \to H^2(G_K, \bar{K}(X)^*/\bar{K}^*) \to H^3(G_K, \bar{K}^*) = 0. \qquad (2·4)$$

Next we show that $f'_v \in H^2(G_{K_v}, \bar{K}_v(X)^*)$ is the image of an element $c_v \in H^2(G_{K_v}, \bar{K_v}^*)$. This is because $b \in Ш(J^\vee)$ is locally trivial which implies its image b' is locally trivial. Then the statement is true by the exactness of local version of sequence (2·4).

We then can define

$$\langle a, b\rangle = \sum_v \mathrm{inv}_v(c_v) \in \mathbb{Q}/\mathbb{Z}.$$

The Cassels–Tate pairing $Ш(J) \times Ш(J) \rightarrow \mathbb{Q}/\mathbb{Z}$ is defined by

$$\langle a, a'\rangle_{CT} := \langle a, \lambda(a')\rangle.$$

We sometimes refer to $\mathrm{inv}_v(c_v)$ above as the local Cassels–Tate pairing between a, a' $Ш(J)$ for a place v of K. Note that the local Cassels–Tate pairing depends on the choice of $f' \in H^2(G_K, \bar{K}(X)^*)$. We make the following remarks that are useful for the computation of the Cassels–Tate pairing.

Remark 2·8.

(i) By [PS99], we know that the homogeneous space definition of the Cassels–Tate pairing is independent of all the choices we make.

(ii) Via the map $\mathrm{Sel}^2(J) \rightarrow Ш(J)[2]$, the definition of the Cassels–Tate pairing on $Ш(J)[2] \times Ш(J)[2]$ naturally lifts to a pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$. In fact, from now on, we will only be considering $\langle \epsilon, \eta\rangle_{CT}$ for $\epsilon, \eta \in \mathrm{Sel}^2(J)$. The principal homogeneous space X in the definition is always taken to be the 2-covering of J corresponding to ϵ. One can compute c_v by evaluating f'_v at a point in $X(K_v)$ provided that one avoids the zeros and poles of f'_v. Note that $X(K_v) \neq \emptyset$ by Proposition 2·4.

2·6. *Explicit 2-coverings of J*

Let $\omega_1, ..., \omega_6$ denote the 6 roots of f. Recall, as in Proposition 2·3, that the isomorphism classes of 2-coverings of J are parameterised by $H^1(G_K, J[2])$. For the explicit computation of the Cassels–Tate pairing, we need the following result on the explicit 2-coverings of J corresponding to elements in $\mathrm{Sel}^2(J)$. We note that this theorem in fact works over any field of characteristic different from 2.

THEOREM 2·9 [FTvL12, proposition 7·2, theorem 7·4, appendix B] *Let J be the Jacobian variety of a genus two curve defined by* $y^2 = f(x)$ *where f is a degree* 6 *polynomial and* $\epsilon \in \mathrm{Sel}^2(J)$. *Embed J in* $\mathbb{P}^{15}$ *via the coordinates* $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$. *There exists* $J_\epsilon \subset \mathbb{P}^{15}$ *defined over K with Galois invariant coordinates* $u_0, ..., u_9, v_1, ..., v_6$ *and a linear isomorphism* $\phi_\epsilon : J_\epsilon \rightarrow J$ *defined over* $\bar{K}$ *such that* $(J_\epsilon, [2] \circ \phi_\epsilon)$ *is a 2-covering of J whose isomorphism class corresponds to the cocycle class* ϵ. *Moreover,* ϕ_ϵ *can be explicitly represented by the* 16×16 *matrix* $R = \begin{bmatrix} R_1 & 0 \\ 0 & R_2 \end{bmatrix}$ *for some* 10×10 *matrix* R_1 *and some* 6×6 *matrix* R_2.

Remark 2·10. The explicit formula for ϕ_ϵ is given in the beginning of [FTvL12, section 7] and it depends only on ϵ and the underlying genus two curve. Note that the coordinates $u_0, ..., u_9, v_1, ..., v_6$ are derived from another set of coordinates $c_0, ..., c_9, d_1, ..., d_6$ defined in

[**FTvL12**, definitions 6·9, 6·11] where $c_0, ..., c_9$ are even and $d_1, ..., d_6$ are odd. This set of coordinates are in general not Galois invariant, however, they are in the case where all points of $J[2]$ are defined over the base field. More details can be found in [**Yan**, remark 1·11·2].

3. *Formula for the Cassels–Tate Pairing*

From now on we assume that our genus 2 curve $\mathcal{C}$ is defined by $y^2 = f(x)$ where all roots of f are defined over K. In other words $\mathcal{C}$ has all its Weierstrass points defined over K. This is equivalent to the condition that all points in $J[2]$ are defined over K. In this section, under the above assumption, we state and prove an explicit formula for the Cassels–Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$.

Let the genus two curve $\mathcal{C}$ be of the form

$$\mathcal{C} : y^2 = \lambda(x - \omega_1)(x - \omega_2)(x - \omega_3)(x - \omega_4)(x - \omega_5)(x - \omega_6),$$

where $\lambda, \omega_i \in K$ and $\lambda \neq 0$. Its Jacobian variety is denoted by J.

The two-torsion subgroup $J[2]$ has basis

$$\begin{aligned} P &= \{(\omega_1, 0), (\omega_2, 0)\}, \ \ Q = \{(\omega_1, 0), (\omega_3, 0)\}, \\ R &= \{(\omega_4, 0), (\omega_5, 0)\}, \ \ S = \{(\omega_4, 0), (\omega_6, 0)\}. \end{aligned}$$

By the discussion at the end of Section 2·1, the Weil pairing is given relative to this basis by:

$$W = \begin{bmatrix} 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \end{bmatrix}. \tag{3·1}$$

More explicitly, W_{ij} denotes the Weil pairing between the i^{th} and j^{th} generators.

We now show that this choice of basis determines an isomorphism $H^1(G_K, J[2]) \cong (K^*/(K^*)^2)^4$. Consider the map $J[2] \xrightarrow{w_2} (\mu_2(\bar{K}))^4$, where w_2 denotes taking the Weil pairing with P, Q, R, S. Since P, Q, R, S form a basis for $J[2]$ and the Weil pairing is a nondegenerate bilinear pairing, we get that w_2 is injective. This implies that w_2 is an isomorphism as $|J[2]| = |(\mu_2(\bar{K}))^4| = 16$. We then get

$$H^1(G_K, J[2]) \xrightarrow{w_{2,*}} H^1(G_K, (\mu_2(\bar{K}))^4) \cong (K^*/(K^*)^2)^4, \tag{3·2}$$

where $w_{2,*}$ is induced by w_2 and $\cong$ is the Kummer isomorphism derived from Hilbert's Theorem 90. Since the map (3·2) is an isomorphism, we can represent elements in $H^1(G_K, J[2])$ by elements in $(K^*/(K^*)^2)^4$.

Before stating and proving the formula for the Cassels–Tate pairing, we first state and prove the following lemma.

LEMMA 3·1. *For $\epsilon \in \mathrm{Sel}^2(J)$, let $(J_\epsilon, \pi_\epsilon)$ denote the corresponding 2-covering of J. Hence, there exists an isomorphism $\phi_\epsilon : J_\epsilon \to J$ defined over $\bar{K}$ such that $[2] \circ \phi_\epsilon = \pi_\epsilon$. Suppose $T \in J(K)$ and $T_1 \in J(\bar{K})$ satisfy $2T_1 = T$. Then:*

(i) *there exists a K-rational divisor D_T on J_ϵ which represents the divisor class of $\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))$;*

(ii) *let D and D_T be K-rational divisors on J_ϵ representing the divisor class of $\phi_\epsilon^*(2\Theta)$ and $\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))$ respectively. Then $D_T - D \sim \phi_\epsilon^*(\tau_T^*\Theta - \Theta)$. Suppose T is a two-torsion point. Then $2D_T - 2D$ is a K-rational principal divisor. Hence, there exists a K-rational function f_T on J_ϵ such that div$(f_T) = 2D_T - 2D$.*

Proof. By the definition of a 2-covering, $[2] \circ \phi_\epsilon = \pi_\epsilon$ is a morphism defined over K. Also, by Proposition 2·3, $\phi_\epsilon \circ (\phi_\epsilon^{-1})^\sigma = \tau_{\epsilon_\sigma}$ for all $\sigma \in G_K$, where $(\sigma \mapsto \epsilon_\sigma)$ is a cocycle representing ϵ. Since $[2] \circ \tau_{T_1} \circ \phi_\epsilon = \tau_T \circ [2] \circ \phi_\epsilon = \tau_T \circ \pi_\epsilon$ and τ_T is defined over K, $(J_\epsilon, \tau_T \circ \pi_\epsilon)$ is also a 2-covering of J. We compute $\tau_{T_1} \circ \phi_\epsilon \circ ((\tau_{T_1} \circ \phi_\epsilon)^{-1})^\sigma = \tau_{T_1} \circ \phi_\epsilon \circ (\phi_\epsilon^{-1})^\sigma \circ \tau_{-\sigma(T_1)} = \tau_{\epsilon_\sigma} \circ \tau_{T_1} \circ \tau_{-\sigma(T_1)}$, for all $\sigma \in G_K$. This implies the 2-covering $(J_\epsilon, \tau_T \circ \pi_\epsilon)$ corresponds to the element in $H^1(G_K, J[2])$ that is represented by the cocycle $(\sigma \mapsto \epsilon_\sigma + T_1 - \sigma(T_1))$. Hence, $(J_\epsilon, \tau_T \circ \pi_\epsilon)$ is the 2-covering of J corresponding to $\epsilon + \delta(T)$, where δ is the connecting map as in (2·1). By Proposition 2·5, there exists a commutative diagram:

$$\begin{tikzcd}
J_\epsilon \arrow[r, "|\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))|"] \arrow[d, "\tau_{T_1} \circ \phi_\epsilon"] & \mathbb{P}^3 \arrow[d, "\psi_\epsilon"] \\
J \arrow[r, "|2\Theta|"] & \mathbb{P}^3,
\end{tikzcd}$$

where the morphism $J_\epsilon \xrightarrow{|\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))|} \mathbb{P}^3$ is defined over K. So the pull back of a hyperplane section via this morphism gives us a rational divisor D_T representing the divisor class of $\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))$ as required by (i).

Since the polarisation $\lambda : J \to J^\vee$ is an isomorphism and $2T_1 = T$, we have

$$\left[\phi_\epsilon^*(\tau_T^*\Theta - \Theta)\right] = \phi_\epsilon^*(\lambda(T)) = 2\phi_\epsilon^*(\lambda(T_1)) = \left[\phi_\epsilon^*(\tau_{T_1}^*(2\Theta)) - \phi_\epsilon^*(2\Theta)\right] = [D_T - D].$$

The fact that T is a two-torsion point implies that $2\phi_\epsilon^*(\lambda(T)) = 0$. Hence, $2D_T - 2D$ is a K-rational principal divisor which gives (ii).

The following remark explains how we will use Lemma 3·1 in the formula for the Cassels–Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$.

Remark 3·2. Applying Lemma 3·1(i) with $T = \mathcal{O}_J, P, Q, R, S \in J[2]$ gives divisors $D = D_{\mathcal{O}_J}$ and D_P, D_Q, D_R, D_S. Then by Lemma 3·1(ii), there exist K-rational functions f_P, f_Q, f_R, f_S on J_ϵ such that div$(f_T) = 2D_T - 2D$ for $T = P, Q, R, S$.

THEOREM 3·3. *Let J be the Jacobian variety of a genus two curve $\mathcal{C}$ defined over a number field K where all points in J[2] are defined over K. For any $\epsilon, \eta \in \mathrm{Sel}^2(J)$, let $(J_\epsilon, [2] \circ \phi_\epsilon)$ be the 2-covering of J corresponding to ϵ where $\phi_\epsilon : J_\epsilon \to J$ is an isomorphism defined over $\bar{K}$. Fix a choice of basis P, Q, R, S for J[2], such that the Weil pairing is given relative to this basis by the matrix (3·1). Let (a, b, c, d) denote the image of η via $H^1(G_K, J[2]) \cong (K^*/(K^*)^2)^4$, where this is the isomorphism induced by taking the Weil pairing with P, Q, R, S. Let f_P, f_Q, f_R, f_S be the K-rational functions on J_ϵ defined in Remark 3·2. Then the Cassels–Tate pairing $\langle\, , \rangle_{CT} : \mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J) \to \{\pm 1\}$ is given by*

$$\langle \epsilon, \eta \rangle_{CT} = \prod_{place\ v} (f_P(P_v), b)_v (f_Q(P_v), a)_v (f_R(P_v), d)_v (f_S(P_v), c)_v,$$

where $(\ ,\ )_v$ *denotes the Hilbert symbol for a given place* v *of* K *and* P_v *is an arbitrary choice of a local point on* $J_\epsilon(K_v)$ *avoiding the zeros and poles of* f_P, f_Q, f_R, f_S.

Proof. We know $\eta \in H^1(G_K, J[2])$ corresponds to $(a, b, c, d) \in (K^*/(K^*)^2)^4$ via taking the Weil pairing with P, Q, R, S. Hence, η is represented by the cocycle

$$\sigma \mapsto \tilde{b}_\sigma P + \tilde{a}_\sigma Q + \tilde{d}_\sigma R + \tilde{c}_\sigma S,$$

where $\sigma \in G_K$ and for each element $x \in K^*/(K^*)^2$, we define $\tilde{x}_\sigma \in \{0, 1\}$ such that $(-1)^{\tilde{x}_\sigma} = \sigma(\sqrt{x})/\sqrt{x}$.

Then the image of η in $H^1(G_K, \mathrm{Pic}^0(J_\epsilon))$ is represented by the cocycle that sends $\sigma \in G_K$ to

$$\tilde{b}_\sigma \phi_\epsilon^*[\tau_P^*\Theta - \Theta] + \tilde{a}_\sigma \phi_\epsilon^*[\tau_Q^*\Theta - \Theta] + \tilde{d}_\sigma \phi_\epsilon^*[\tau_R^*\Theta - \Theta] + \tilde{c}_\sigma \phi_\epsilon^*[\tau_S^*\Theta - \Theta].$$

By Remark 3·2, there exist K-rational divisors D_P, D_Q, D_R, D_S on J_ϵ such that the above cocycle sends $\sigma \in G_K$ to

$$\tilde{b}_\sigma[D_P - D] + \tilde{a}_\sigma[D_Q - D] + \tilde{d}_\sigma[D_R - D] + \tilde{c}_\sigma[D_S - D].$$

We need to map this element in $H^1(G_K, \mathrm{Pic}^0(J_\epsilon))$ to an element in $H^2(G_K, \bar{K}(J_\epsilon)^*/\bar{K}^*)$ via the connecting map induced by the short exact sequence

$$0 \to \bar{K}(J_\epsilon)^*/\bar{K}^* \to \mathrm{Div}^0(J_\epsilon) \to \mathrm{Pic}^0(J_\epsilon) \to 0.$$

Hence, by the formula for the connecting map and the fact that the divisors D, D_P, D_Q, D_R, D_S are all K-rational, we get that the corresponding element in $H^2(G_K, \bar{K}(J_\epsilon)^*/\bar{K}^*)$ has image in $H^2(G_K, \mathrm{Div}^0(J_\epsilon))$ represented by the following cocycle:

$$\begin{aligned}(\sigma, \tau) \mapsto & (\tilde{b}_\tau - \tilde{b}_{\sigma\tau} + \tilde{b}_\sigma)(D_P - D) + (\tilde{a}_\tau - \tilde{a}_{\sigma\tau} + \tilde{a}_\sigma)(D_Q - D) \\ & + (\tilde{d}_\tau - \tilde{d}_{\sigma\tau} + \tilde{d}_\sigma)(D_R - D) + (\tilde{c}_\tau - \tilde{c}_{\sigma\tau} + \tilde{c}_\sigma)(D_S - D),\end{aligned}$$

for $\sigma, \tau \in G_K$.

It can be checked that, for $x \in K^*/(K^*)^2$ and $\sigma, \tau \in G_K$, we get $\tilde{x}_\tau - \tilde{x}_{\sigma\tau} + \tilde{x}_\sigma = 2$ if both σ and τ flip $\sqrt{x}$ and otherwise it is equal to zero. Define $\iota_{\sigma,\tau,x} = 1$ if both σ and τ flip $\sqrt{x}$ and otherwise $\iota_{\sigma,\tau,x} = 0$. Note that the map that sends $x \in K^*/(K^*)^2$ to the class of $(\sigma, \tau) \mapsto \iota_{\sigma,\tau,x}$ explicitly realizes the map $K^*/(K^*)^2 \cong H^1(G_K, \frac{1}{2}\mathbb{Z}/\mathbb{Z}) \subset H^1(G_K, \mathbb{Q}/\mathbb{Z}) \to H^2(G_K, \mathbb{Z})$. Then, for $\sigma, \tau \in G_K$, the cocycle in the last paragraph sends (σ, τ) to

$$\iota_{\sigma,\tau,b} \cdot 2(D_P - D) + \iota_{\sigma,\tau,a} \cdot 2(D_Q - D) + \iota_{\sigma,\tau,d} \cdot 2(D_R - D) + \iota_{\sigma,\tau,c} \cdot 2(D_S - D).$$

Hence, by Remark 3·2, the corresponding element in $H^2(G_K, \bar{K}(J_\epsilon)^*/\bar{K}^*)$ is represented by

$$(\sigma, \tau) \mapsto \left[f_P^{\iota_{\sigma,\tau,b}} \cdot f_Q^{\iota_{\sigma,\tau,a}} \cdot f_R^{\iota_{\sigma,\tau,d}} \cdot f_S^{\iota_{\sigma,\tau,c}}\right],$$

for all $\sigma, \tau \in G_K$.

For each place v of K, following the homogeneous space definition of $\langle \epsilon, \eta \rangle_{CT}$ as given in Section 2·5, we obtain an element in $H^2(G_{K_v}, \bar{K}_v^*)$ from the long exact sequence induced by the short exact sequence $0 \to \bar{K}_v^* \to \bar{K}_v(J_\epsilon)^* \to \bar{K}_v(J_\epsilon)^*/\bar{K}_v{}^* \to 0$. The long exact sequence is the local version of (2·4) with X replaced by J_ϵ. By Remark 2·8(ii), this element in

$H^2(G_{K_v}, \bar{K_v}^*)$ can be represented by

$$(\sigma, \tau) \mapsto f_P(P_v)^{\iota_{\sigma,\tau,b}} \cdot f_Q(P_v)^{\iota_{\sigma,\tau,a}} \cdot f_R(P_v)^{\iota_{\sigma,\tau,d}} \cdot f_S(P_v)^{\iota_{\sigma,\tau,c}},$$

for all $\sigma, \tau \in G_K$ and some local point $P_v \in J_\epsilon(K_v)$ avoiding the zeros and poles of f_P, f_Q, f_R, f_S.

Hence, the above element in $\mathrm{Br}(K_v) \cong H^2(G_{K_v}, \bar{K_v}^*)$ is the class of the tensor product of quaternion algebras

$$(f_P(P_v), b) \otimes (f_Q(P_v), a) \otimes (f_R(P_v), d) \otimes (f_S(P_v), c).$$

Then, by identifying $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ with $\mu_2 = \{1, -1\}$, we have that

$$\begin{aligned}&\mathrm{inv}\big((f_P(P_v), b) \otimes (f_Q(P_v), a) \otimes (f_R(P_v), d) \otimes (f_S(P_v), c)\big)\\ &\quad = (f_P(P_v, b)_v (f_Q(P_v), a)_v (f_R(P_v), d)_v (f_S(P_v), c)_v,\end{aligned}$$

where $(\ ,\ )_v$ denotes the Hilbert symbol: $K_v^* \times K_v^* \to \{1, -1\}$, as required.

Remark 3·4. In Section 6, we will directly show that the formula for the Cassels–Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ given in Theorem 3·3 is a finite product.

Remark 3·5. The formula in Theorem 3·3 is analogous to that in the elliptic curve case when all the two torsion points of the elliptic curve is defined over K. By section 6 in [**FSS10**], the pairing defined by Cassels in [**Cas98**] is the Cassels–Tate pairing and takes the following form as in section 4 in [**FSS10**]. Let $C \to E$ be a 2 covering representing $\epsilon \in \mathrm{Sel}^2(E)$. Let $\mathrm{Sel}^2(E) \hookrightarrow (K^*/K^{*2})^3$ be the corresponding embedding to the standard embedding of $E[2] \hookrightarrow \mu_2^3$ via the Weil paring. Suppose $\eta \in \mathrm{Sel}^2(E)$ is represented by $\eta = (a_1, a_2, a_3) \in (K^*/K^{*2})^3$ with $a_1a_2a_3$ a square in K. Then there are K-rational functions f_1, f_2, f_3 on C such that $f_1f_2f_3 = h^2$ for some function h on C and the Cassels–Tate pairing takes the form

$$\langle \epsilon, \eta \rangle_{CT} = \prod_{\text{place } v} (f_1(p_v), a_1)_v (f_2(p_v), a_2)_v (f_3(p_v), a_3)_v.$$

Here $(\ ,\ )_v$ denotes the Hilbert symbol: $K_v^* \times K_v^* \to \{1, -1\}$ and p_v is a local point on C, which exists since C everywhere locally has a point. Now using the fact that $a_1a_2a_3$ is a square and $f_1f_2f_3 = h^2$ and bilinearity of the Hilbert symbol, the above formula simplifies to

$$\langle \epsilon, \eta \rangle_{CT} = \prod_{\text{place } v} (f_1(p_v), a_2)_v (f_2(p_v), a_1)_v,$$

which is indeed very similar to the formula given in Theorem 3·3.

4. *Explicit Computation*

In this section, we explain how we explicitly compute the Cassels–Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ using the formula given in Theorem 3·3, under the assumption that all points in $J[2]$ are defined over K. We fix $\epsilon \in \mathrm{Sel}^2(J)$ and $(J_\epsilon, [2] \circ \phi_\epsilon)$, the 2-covering of J corresponding to ϵ where $\phi_\epsilon : J_\epsilon \to J$ is the isomorphism defined over $\overline{K}$ given by a linear change of coordinates on $\mathbb{P}^{15}$ as in Theorem 2·9. The statement of Theorem 3·3 suggests that we need to compute the K-rational divisors D, D_P, D_Q, D_R, D_S on J_ϵ and the K-rational functions f_P, f_Q, f_R, f_S on J_ϵ, as in Remark 3·2.

4·1. *Computing the twist of the Kummer surface*

We describe a practical method for computing a linear isomorphism $\psi_\epsilon : \mathbb{P}^3 \to \mathbb{P}^3$ corresponding to ϵ, which maps $\mathcal{K}_\epsilon \to \mathcal{K}$. More explicitly, we need to compute ψ_ϵ such that $\psi_\epsilon(\psi_\epsilon^{-1})^\sigma$ is the action of translation by $\epsilon_\sigma \in J[2]$ on $\mathcal{K}$ and $(\sigma \mapsto \epsilon_\sigma)$ is a cocycle representing ϵ. Since all points in $J[2]$ are defined over K, the coboundaries in $B^1(G_K, J[2])$ are trivial. Therefore, these conditions determine ψ_ϵ uniquely up to precomposing by a linear change of coordinates defined over K.

For each $T \in J[2]$, we have an explicit formula for $M_T \in \mathrm{GL}_4(K)$, given in [**CF96**, chapter 3, section 2], representing the action of translation by $T \in J[2]$ on the Kummer surface $\mathcal{K} \subset \mathbb{P}^3$. It can be checked that $\{M_T, T \in J[2]\}$ form a basis of $\mathrm{Mat}_4(K)$. Let $c_P, c_Q, c_R, c_S \in K$ be such that $M_P^2 = c_P I, M_Q^2 = c_Q I, M_R^2 = c_R I$, and $M_S^2 = c_S I$. The explicit formulae for c_P, c_Q, c_R, c_S can also be found in [**CF96**, chapter 3, section 2]. Moreover, by [**CF96**, chapter 3, section 3] and the Weil pairing relationship among the generators P, Q, R, S of $J[2]$ specified by (3·1), we know that $[M_P, M_Q] = [M_R, M_S] = -I$ and the commutators of the other pairs are trivial.

Suppose $(a, b, c, d) \in (K^*/(K^*)^2)^4$ represents ϵ. Let $A \in \mathrm{GL}_4(\bar{K})$ represent the linear isomorphism ψ_ϵ and let $M'_T = A^{-1}M_TA \in \mathrm{GL}_4(\bar{K})$ represent the action of T on the twisted Kummer $\mathcal{K}_\epsilon$. It can be checked, see [**Yan**, lemma 3·2·1] for details, that the set of matrices in $\mathrm{PGL}_4(\bar{K})$ that commute with M_T in $\mathrm{PGL}_4(\bar{K})$ for all $T \in J[2]$ is $\{[M_T], T \in J[2]\}$. This implies that any $B \in \mathrm{GL}_4(\bar{K})$ such that $[M'_T] = [B^{-1}M_TB] \in \mathrm{PGL}_4(\bar{K})$ for all $T \in J[2]$ is equal to a multiple of M_{T_0} composed with A for some $T_0 \in J[2]$ and so also represents ψ_ϵ. Hence, it will suffice to compute the matrices M'_T.

Consider $[M'_T] \in \mathrm{PGL}_4(\bar{K})$ and $\sigma \in G_K$. We have

$$[M'_T]([M'_T]^{-1})^\sigma = [A^{-1}M_TA(A^{-1})^\sigma M_T^{-1}A^\sigma] \in \mathrm{PGL}_4(\bar{K}).$$

Recall that for each element $x \in K^*/(K^*)^2$, we define $\tilde{x}_\sigma \in \{0, 1\}$ such that $(-1)^{\tilde{x}_\sigma} = \sigma(\sqrt{x})/\sqrt{x}$. Since $[A(A^{-1})^\sigma] = [M_P^{\tilde{b}_\sigma} M_Q^{\tilde{a}_\sigma} M_R^{\tilde{d}_\sigma} M_S^{\tilde{c}_\sigma}]$ and M_T commutes with M_P, M_Q, M_R, M_S in $\mathrm{PGL}_4(K)$, we get that $[M'_T]([M'_T]^{-1})^\sigma = I \in \mathrm{PGL}_4(\bar{K})$ for all $\sigma \in G_K$. Therefore we have $[M'_T]$ is in $\mathrm{PGL}_4(K)$. This means that we can redefine $M'_T = \lambda_T A^{-1}M_TA$ for some $\lambda_T \in \bar{K}$ such that $M'_T \in \mathrm{GL}_4(K)$, by choosing a K defined representative.

Let $N_P = 1/\sqrt{c_P}M_P, N_Q = 1/\sqrt{c_Q}M_Q, N_R = 1/\sqrt{c_R}M_R, N_S = 1/\sqrt{c_S}M_S$. Then $N_T^2 = I$ for $T = P, Q, R, S$. Define $N'_T = A^{-1}N_TA \in \mathrm{GL}_4(\bar{K})$ for $T = P, Q, R, S$. We note that N'_T, M'_T represent the same element in $\mathrm{PGL}_4(\bar{K})$ and $N'^2_T = I$ for each $T = P, Q, R, S$. Suppose $M'^2_P = \alpha_P I, M'^2_Q = \alpha_Q I, M'^2_R = \alpha_R I, M'^2_S = \alpha_S I$. Then $N'_T = 1/\sqrt{\alpha_T}M'_T$ for each $T = P, Q, R, S$. Note that there might be some sign issues here but they will not affect the later computation. Since

$$N'_P(N'^{-1}_P)^\sigma = A^{-1}N_PA(A^{-1})^\sigma(N_P^{-1})^\sigma A^\sigma,$$

via $N_P = 1/\sqrt{c_P}M_P$, $N'_P = 1/\sqrt{\alpha_P}M'_P$ with $M_P, M'_P \in \mathrm{GL}_4(K)$, the fact that $[A(A^{-1})^\sigma] = [M_P^{\tilde{b}_\sigma} M_Q^{\tilde{a}_\sigma} M_R^{\tilde{d}_\sigma} M_S^{\tilde{c}_\sigma}]$, and the fact that M_P commutes with $M_P, M_R, M_S \in GL_4(K)$ and $M_PM_Q = -M_QM_P$, we can derive that

$$\frac{\sigma(\sqrt{\alpha_P})}{\sqrt{\alpha_P}} = (-1)^{\tilde{a}_\sigma}\frac{\sigma(\sqrt{c_P})}{\sqrt{c_P}} = \frac{\sigma(\sqrt{a})}{\sqrt{a}}\frac{\sigma(\sqrt{c_P})}{\sqrt{c_P}},$$

and similar equations hold for Q,R,S too.

This implies that $\alpha_P = c_P a$ up to squares in K and so via rescaling M'_P by elements in K, we have $M'^2_P = c_P aI$. Similarly, $M'^2_Q = c_Q bI, M'^2_R = c_R cI, M'^2_S = c_S dI$. We note that we also have $[M'_P, M'_Q] = [M'_R, M'_S] = -I$ and the commutators of the other pairs are trivial. This implies that

$$\mathrm{Mat}_4(K) \cong (c_P a, c_Q b) \otimes (c_R c, c_S d)$$

$$M'_P \mapsto i_1 \otimes 1, M'_Q \mapsto j_1 \otimes 1, M'_R \mapsto 1 \otimes i_2, M'_S \mapsto 1 \otimes j_2,$$

where $(c_P a, c_Q b)$ and $(c_R c, c_S d)$ are quaternion algebras with generators i_1, j_1 and i_2, j_2 respectively. In Section 5, we will interpret this isomorphism as saying that the image of ϵ via the obstruction map is trivial.

Let $A = (c_P a, c_Q b), B = (c_R c, c_S d)$. By the argument above, we know $A \otimes B$ represents the trivial element in $\mathrm{Br}(K)$ and an explicit isomorphism $A \otimes B \cong \mathrm{Mat}_4(K)$ will give us the explicit matrices M'_P, M'_Q, M'_R, M'_S we seek. Since the classes of A, B are in $\mathrm{Br}[2]$, we have A, B representing the same element in $\mathrm{Br}(K)$. This implies that $A \cong B$ over K, by Wedderburn's Theorem. We have the following lemma.

Lemma 4·1. *Consider a tensor product of two quaternion algebras $A \otimes B$, where $A = (\alpha, \beta)$, $B = (\gamma, \delta)$, with generators i_1, j_1 and i_2, j_2 respectively. Suppose there is an isomorphism $\psi : B \xrightarrow{\sim} A$ given by*

$$i_2 \mapsto a_1 \cdot 1 + b_1 \cdot i_1 + c_1 \cdot j_1 + d_1 \cdot i_1 j_1,$$
$$j_2 \mapsto a_2 \cdot 1 + b_2 \cdot i_1 + c_2 \cdot j_1 + d_2 \cdot i_1 j_1.$$

Then there is an explicit isomorphism

$$A \otimes B \cong Mat_4(K)$$

given by

$$i_1 \otimes 1 \mapsto M_{i_1} := \begin{bmatrix} 0 & \alpha & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

$$j_1 \otimes 1 \mapsto M_{j_1} := \begin{bmatrix} 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & -\beta \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}$$

$$1 \otimes i_2 \mapsto M_{i_2} := \begin{bmatrix} a_1 & b_1 \cdot \alpha & c_1 \cdot \beta & -d_1 \cdot \alpha\beta \\ b_1 & a_1 & -d_1 \cdot \beta & c_1 \cdot \beta \\ c_1 & d_1 \cdot \alpha & a_1 & -b_1 \cdot \alpha \\ d_1 & c_1 & -b_1 & a_1 \end{bmatrix}$$

$$1 \otimes j_2 \mapsto M_{j_2} := \begin{bmatrix} a_2 & b_2 \cdot \alpha & c_2 \cdot \beta & -d_2 \cdot \alpha\beta \\ b_2 & a_2 & -d_2 \cdot \beta & c_2 \cdot \beta \\ c_2 & d_2 \cdot \alpha & a_2 & -b_2 \cdot \alpha \\ d_2 & c_2 & -b_2 & a_2 \end{bmatrix}$$

Proof. We have that $A \otimes A^{op}$ is isomorphic to a matrix algebra. More specifically, $A \otimes A^{op} \cong \mathrm{End}_K(A)$ via $u \otimes v \mapsto (x \mapsto uxv)$, which makes $A \otimes A^{op} \cong \mathrm{Mat}_4(K)$ after picking a basis for A. Hence,

$$\begin{aligned} A \otimes B^{op} &\cong \mathrm{Mat}_4(K) \\ u \otimes v &\mapsto (x \mapsto ux\psi(v)). \end{aligned}$$

More explicitly, fixing the basis of A to be $\{1, i_1, j_1, i_1 j_1\}$, the isomorphism is as given in the statement of the lemma.

By taking $A = (c_P a, c_Q b), B = (c_R c, c_S d)$ in Lemma 4·1, we know that the matrices M'_P, M'_Q, M'_R, M'_S and $M_{i_1}, M_{j_1}, M_{i_2}, M_{j_2}$ are equal up to conjugation by a matrix $C \in \mathrm{GL}_4(K)$ via the Noether Skolem Theorem. After a change of coordinates for $\mathcal{K}_\epsilon \subset \mathbb{P}^3$ according to C, we have that M'_P, M'_Q, M'_R, M'_S are equal to $M_{i_1}, M_{j_1}, M_{i_2}, M_{j_2}$. Lemma 4·1 therefore reduces the problem of computing the M'_T to that of computing an isomorphism between the two quaternion algebras. See [**Yan**, corollary 4·2·3] for the description of an explicit algorithm. Finally we solve for a matrix A such that $M'_T = \lambda_T A^{-1} M_T A$ for some $\lambda_T \in \bar{K}$ and $T = P, Q, R, S$ by linear algebra.

4·2. *Explicit computation of D*

In this section, we explain a method for computing the K-rational divisor D on J_ϵ representing the divisor class $\phi_\epsilon^*(2\Theta)$. The idea is to compute it via the commutative diagram (2·3) in Remark 2·6.

By Theorem 2·9, there is an explicit isomorphism $\phi_\epsilon : J_\epsilon \to J$ defined over $\overline{K}$ given by a linear change of coordinates on $\mathbb{P}^{15}$. We write $u_0, ..., u_9, v_1, ..., v_6$ for the coordinates on the ambient space of $J_\epsilon \subset \mathbb{P}^{15}$ and write $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$ for the coordinates on the ambient space of $J \subset \mathbb{P}^{15}$. By the same theorem, ϕ_ϵ is represented by a block diagonal matrix consisting of a block of size 10 corresponding to the even basis elements and a block of size 6 corresponding to the odd basis elements. Following Section 4·1, we can compute an explicit isomorphism $\psi_\epsilon : \mathbb{P}^3 \to \mathbb{P}^3$, that maps $\mathcal{K}_\epsilon \to \mathcal{K}$, where $\mathcal{K}_\epsilon$ is the twisted Kummer surface corresponding to ϵ. We write $k'_1, ..., k'_4$ for the coordinates on the ambient space of $\mathcal{K}_\epsilon \subset \mathbb{P}^3$. Recall that since all points in $J[2]$ are defined over K, all coboundaries in $B^1(G_K, J[2])$ are trivial. So, we have that $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma$ and $\psi_\epsilon(\psi_\epsilon^{-1})^\sigma$ both give the action of translation by some $\epsilon_\sigma \in J[2]$ such that $(\sigma \mapsto \epsilon_\sigma)$ represents $\epsilon \in \mathrm{Sel}^2(J)$.

Define $k'_{ij} = k'_i k'_j$. The isomorphism $\psi_\epsilon : \mathbb{P}^3_{k'_i} \to \mathbb{P}^3_{k_i}$, induces a natural isomorphism $\tilde{\psi_\epsilon} : \mathbb{P}^9_{k'_{ij}} \to \mathbb{P}^9_{k_{ij}}$. More explicitly, suppose ψ_ϵ is represented by the 4×4 matrix A where $(k'_1 : ..., k'_4) \mapsto \left(\sum_{i=1}^4 A_{1i} k'_i : ... : \sum_{i=1}^4 A_{4i} k'_i\right)$. Then $\tilde{\psi_\epsilon} : \mathbb{P}^9_{k'_{ij}} \to \mathbb{P}^9_{k_{ij}}$ is given by $(k'_{11} : k'_{12} : ... : k'_{44}) \mapsto \left(\sum_{i,j=1}^4 A_{1i} A_{1j} k'_{ij} : \sum_{i,j=1}^4 A_{1i} A_{2j} k'_{ij} : ... : \sum_{i,j=1}^4 A_{4i} A_{4j} k'_{ij}\right)$.

On the other hand, the isomorphism $\phi_\epsilon : \mathbb{P}^{15}_{\{u_i,v_i\}} \to \mathbb{P}^{15}_{\{k_{ij},b_i\}}$ induces a natural isomorphism $\tilde{\phi_\epsilon} : \mathbb{P}^9_{u_i} \to \mathbb{P}^9_{k_{ij}}$ represented by the 10×10 block of the matrix representing ϕ_ϵ. Since $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma$ and $\psi_\epsilon(\psi_\epsilon^{-1})^\sigma$ both give the action of translation by some $\epsilon_\sigma \in J[2]$, we get $\tilde{\phi_\epsilon}(\tilde{\phi_\epsilon}^{-1})^\sigma = \tilde{\psi_\epsilon}(\tilde{\phi_\epsilon}^{-1})^\sigma$. Therefore, $\tilde{\psi_\epsilon}^{-1}\tilde{\phi_\epsilon}$ is defined over K.

Now let $v : \mathbb{P}^3 \to \mathbb{P}^9$ be the Veronese embedding that sends $(x_0 : x_1 : x_2 : x_3)$ to $(x_0^2 : x_0x_1 : \ldots : x_3^2)$ and let $\mathcal{K}_{\mathbb{P}^9_{k_{ij}}}$ and $\mathcal{K}_{\epsilon,\mathbb{P}^9_{k'_{ij}}}$ be the corresponding image of $\mathcal{K}$ and $\mathcal{K}_\epsilon$ in $\mathbb{P}^9_{k_{ij}}$ and $\mathbb{P}^9_{k'_{ij}}$ via the Veronese embedding. Furthermore, let $\mathcal{K}_{\epsilon,\mathbb{P}^9_{u_i}}$ be the image of J_ϵ via the projection map $\mathbb{P}^{15}_{u_i,v_i} \to \mathbb{P}^9_{u_i}$. The various maps between projective spaces are summarised in the following commutative diagram.

$$\begin{tikzcd}
\mathbb{P}^{15}_{\{u_i,v_i\}} \arrow[r, "proj"] \arrow[d, "\phi_\epsilon"] & \mathbb{P}^9_{u_i} \arrow[rr, "(\tilde{\psi_\epsilon})^{-1}\tilde{\phi_\epsilon}"] \arrow[dr, "\tilde{\phi_\epsilon}"] & & \mathbb{P}^9_{k'_{ij}} \arrow[dl, "\tilde{\psi_\epsilon}"] \\
\mathbb{P}^{15}_{\{k_{ij},b_i\}} \arrow[rr, "proj"] & & \mathbb{P}^9_{k_{ij}} &
\end{tikzcd} \tag{4·1}$$

Restricting these maps to J, $\mathcal{K}$ and their twists (and using the same names for these restricted maps) we obtain the following commutative diagram that decomposes the standard commutative diagram (2·3).

$$\begin{tikzcd}
J_\epsilon \arrow[r, "proj"] \arrow[d, "\phi_\epsilon"] & \mathcal{K}_{\epsilon,\mathbb{P}^9_{u_i}} \arrow[rr, "(\tilde{\psi_\epsilon})^{-1}\tilde{\phi_\epsilon}"] \arrow[dr, "\tilde{\phi_\epsilon}"] & & \mathcal{K}_{\epsilon,\mathbb{P}^9_{k'_{ij}}} \arrow[r, "g_2"] \arrow[dl, "\tilde{\psi_\epsilon}"] & \mathcal{K}_\epsilon \arrow[d, "\psi_\epsilon"] \\
J \arrow[rr, "proj"] & & \mathcal{K}_{\mathbb{P}^9_{k_{ij}}} \arrow[rr, "g_1"] & & \mathcal{K}
\end{tikzcd} \tag{4·2}$$

Here $g_1 : (k_{11} : \ldots : k_{44}) \mapsto (k_{11} : \ldots : k_{14})$ and $g_2 : (k'_{11} : \ldots : k'_{44}) \mapsto (k'_{11} : \ldots : k'_{14})$ are the projection maps, which are the one sided inverse of Veronese embedding. The composition of the morphisms on the bottom row gives the standard morphism $J \xrightarrow{|2\Theta|} \mathcal{K} \subset \mathbb{P}^3$ and the composition of the morphisms on the top row gives $J_\epsilon \xrightarrow{|\phi_\epsilon^*(2\Theta)|} \mathcal{K}_\epsilon \subset \mathbb{P}^3$.

Let D be the pull back on J_ϵ via the horizontal map, as in diagram (4·2), $J_\epsilon \to \mathcal{K}_\epsilon$ of the hyperplane section given by $k'_1 = 0$. This implies that D is a K-rational divisor on J_ϵ representing the class of $\phi_\epsilon^*(2\Theta)$. Moreover, the pull back on J_ϵ via the map $J_\epsilon \to \mathcal{K}_{\epsilon,\mathbb{P}^9_{k'_{ij}}}$ as in (4·2) of the hyperplane section given by $k'_{11} = 0$ is $2D$.

4·3. *Explicit computation of D_P, D_Q, D_R, D_S*

In this section, we explain how to compute the K-rational divisors D_P, D_Q, D_R, D_S defined in Remark 3·2. More explicitly, for $T \in J[2]$, we give a method for computing a K-rational divisor D_T on J_ϵ representing the divisor class of $\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))$ for some T_1 on J such that $2T_1 = T$. Recall that we assume all points in $J[2]$ are defined over K and we have an explicit isomorphism $\phi_\epsilon : J_\epsilon \to J$ such that $(J_\epsilon, [2] \circ \phi_\epsilon)$ is the 2-covering of J corresponding to $\epsilon \in \mathrm{Sel}^2(J)$. Recall $\delta : J(K) \to H^1(G_K, J[2])$ in (2·1). We first prove the following lemma.

LEMMA 4·2. *Let $T \in J(K)$. Suppose $\phi_{\epsilon+\delta(T)} : J_{\epsilon+\delta(T)} \to J$ is an isomorphism over $\bar{K}$ and $(J_{\epsilon+\delta(T)}, [2] \circ \phi_{\epsilon+\delta(T)})$ is the 2-covering of J corresponding to $\epsilon + \delta(T) \in H^1(G_K, J[2])$. Let $T_1 \in J$ such that $2T_1 = T$. Then, $\phi^{-1}_{\epsilon+\delta(T)} \circ \tau_{T_1} \circ \phi_\epsilon : J_\epsilon \to J_{\epsilon+\delta(T)}$ is defined over K.*

Proof. Using the same argument as in the proof of Lemma 3·1(i), we know that $(J_\epsilon, [2] \circ \tau_{T_1} \circ \phi_\epsilon)$ is the 2-covering of J corresponding to $\epsilon + \delta(T) \in H^1(G_K, J[2])$. Since all points in $J[2]$ are defined over K, we have $\tau_{T_1} \circ \phi_\epsilon \circ ((\tau_{T_1} \circ \phi_\epsilon)^{-1})^\sigma = \phi_{\epsilon+\delta(T)} \circ (\phi^{-1}_{\epsilon+\delta(T)})^\sigma$, as required.

Let $T \in J(K)$ with $2T_1 = T$. Consider the commutative diagram below which is formed of two copies of the standard diagram (2·3). In this diagram all the horizontal maps are defined over K. By Lemma 4·2, the composition of the three vertical maps on the left is defined over K, even though the individual maps are only defined over $\overline{K}$. The composition of the four wavy arrows is therefore defined over K. Pulling back a hyperplane section on $\mathcal{K}_{\epsilon+\delta(T)} \subset \mathbb{P}^3$ via this composition gives a K-rational divisor D_T on J_ϵ representing the divisor class $\phi^*_\epsilon(\tau^*_{T_1}(2\Theta))$. If we further assume that $T \in J[2]$ then the composition of the three vertical maps on the left is given by a change of coordinates on $\mathbb{P}^{15}$ and so by a 16×16 matrix defined over K.

$$\begin{tikzcd}
\mathbb{P}^{15} \supset J_\epsilon \arrow[r, "|\phi^*_\epsilon(2\Theta)|"] \arrow[d, squiggly, "\phi_\epsilon"'] & \mathcal{K}_\epsilon \subset \mathbb{P}^3 \arrow[d, "\psi_\epsilon"] \\
\mathbb{P}^{15} \supset J \arrow[r, "|2\Theta|"] \arrow[d, squiggly, "\tau_{T_1}"'] & \mathcal{K} \subset \mathbb{P}^3 \\
\mathbb{P}^{15} \supset J \arrow[r, "|2\Theta|"] \arrow[d, squiggly, "(\phi_{\epsilon+\delta(T)})^{-1}"'] & \mathcal{K} \subset \mathbb{P}^3 \\
\mathbb{P}^{15} \supset J_{\epsilon+\delta(T)} \arrow[r, squiggly, "|\phi^*_{\epsilon+\delta(T)}(2\Theta)|"] & \mathcal{K}_{\epsilon+\delta(T)} \subset \mathbb{P}^3 \arrow[u, "\psi_{\epsilon+\delta(T)}"']
\end{tikzcd} \tag{4·3}$$

The bottom horizontal morphism $J_{\epsilon+\delta(T)} \xrightarrow{|\phi^*_{\epsilon+\delta(T)}(2\Theta)|} \mathcal{K}_{\epsilon+\delta(T)} \subset \mathbb{P}^3$ can be explicitly computed using the algorithm in Section 4·2 with the Selmer element ϵ replaced by $\epsilon + \delta(T)$. Also, by Theorem 2·9, we have explicit formulae for ϕ_ϵ and $\phi_{\epsilon+\delta(T)}$. Hence, to explicitly compute D_T, we need to compute a pullback by τ_{T_1}, for some T_1 such that $2T_1 = T$.

Since we need to apply the above argument for T running over our basis P, Q, R, S for $J[2]$, it would suffice to compute the translation maps $\tau_{T_1} : J \to J$ when $T_1 \in J[4]$. Each of these translation maps is given by a change of coordinates on $\mathbb{P}^{15}$ and so by a 16×16 matrix. We show how to compute a 10×16 submatrix in the following proposition. We then explain below why this is sufficient for our purposes.

PROPOSITION 4·3. *Suppose $T_1 \in J[4]$. Given the coordinates of $T_1 \in J \subset \mathbb{P}^{15}_{\{k_{ij}, b_i\}}$, we can compute a 10×16 matrix representing the composition of maps (say Ψ) in the second row of the following commutative diagram.*

$$\begin{tikzcd}
J \arrow[r, "\tau_{T_1}"] \arrow[d, hook] & J \arrow[d, hook] & \\
\mathbb{P}^{15}_{\{k_{ij},b_i\}} \arrow[r] & \mathbb{P}^{15}_{\{k_{ij},b_i\}} \arrow[r, "\mathrm{proj}"] & \mathbb{P}^{9}_{k_{ij}}
\end{tikzcd} \tag{4·4}$$

Proof. Let $T = 2T_1 \in J[2]$. Recall that we let M_T denote the action of translation by T on $\mathcal{K} \subset \mathbb{P}^3$. Then for any $P \in J$, we have $k_i(P+T) = \sum_{j=1}^{4} (M_T)_{ij} k_j(P)$ projectively as a vector of length 4, and projectively as a vector of length 10, $k_{ij}(P+T_1)$ is equal to

$$k_i(P+T_1)k_j(P+T_1) = k_i(P+T_1)\sum_{l=1}^{4}(M_T)_{jl}k_l(P-T_1) = \sum_{l=1}^{4}(M_T)_{jl}k_l(P-T_1)k_i(P+T_1).$$

By [Fly93, theorem 3.2], there exists a 4×4 matrix of bilinear forms $\phi_{ij}(P, T_1)$ that is projectively equal to the matrix $k_i(P-T_1)k_j(P+T_1)$. Moreover explicit formulae are given for these bilinear forms. Since we have an explicit formula for M_T in in [CF96, chapter 3, section 2], we can compute a 10×16 matrix representing Ψ as claimed in the statement of the proposition.

Remark 4·4. Suppose $2T_1 = T \in J[2]$. From the doubling formula on $\mathcal{K}$ as in [Fly93, appendix C], we can compute the coordinates of the image of T_1 on $\mathcal{K} \subset \mathbb{P}^3$ from the coordinates of the image of T on $\mathcal{K} \subset \mathbb{P}^3$. This gives the 10 even coordinates, $k_{ij}(T_1)$ and we can solve for the odd coordinates using the 72 defining equations of J as given in Theorem 2·2. Note that by Lemma 4·2, we know the field of definition of T_1 is contained in the composition of the field of definition of ϕ_ϵ and $\phi_{\epsilon+\delta(T)}$. Hence, we can compute this field explicitly which helps solving for this point using MAGMA [BCP97].

Consider $T \in J[2]$ with $T_1 \in J[4]$ such that $2T_1 = T$. We follow the discussion in Section 4·2 with ϵ replaced by $\epsilon + \delta(T)$. This gives a diagram analogous to (4·2). Let $k'_{1,T}, ..., k'_{4,T}$ be the coordinates on the ambient space of $\mathcal{K}_{\epsilon+\delta(T)} \subset \mathbb{P}^3$ and let $u_{0,T}, ..., u_{9,T}, v_{1,T}, ..., v_{6,T}$ be the coordinates on the ambient space of $J_{\epsilon+\delta(T)} \subset \mathbb{P}^{15}$. Let $k'_{ij,T} = k'_{i,T}k'_{j,T}$. Decomposing the lower half of the diagram (4·3) gives the commutative diagram below.

$$\begin{tikzcd}
\mathbb{P}^{15}_{\{u_i,v_i\}} \supset J_\epsilon \arrow[rr, "|\phi_\epsilon^*(2\Theta)|"] \arrow[d, squiggly, "\phi_\epsilon"'] & & \mathcal{K}_\epsilon \subset \mathbb{P}^3_{k'_i} \arrow[d, "\psi_\epsilon"] \\
\mathbb{P}^{15}_{\{k_{ij},b_i\}} \supset J \arrow[rr, "|2\Theta|"] \arrow[d, "\tau_{T_1}"'] \arrow[dr, squiggly, "\Psi"] & & \mathcal{K} \subset \mathbb{P}^3_{k_i} \\
\mathbb{P}^{15}_{\{k_{ij},b_i\}} \supset J \arrow[r, "\mathrm{proj}"'] & \mathcal{K}_{\mathbb{P}^9_{k_{ij}}} \arrow[r, "g_1"] \arrow[d, squiggly, "(\tilde{\psi}_{\epsilon+\delta(T)})^{-1}"] & \mathcal{K} \subset \mathbb{P}^3_{k_i} \\
\mathbb{P}^{15}_{\{u_{i,T},v_{i,T}\}} \supset J_{\epsilon+\delta(T)} \arrow[u, "\phi_{\epsilon+\delta(T)}"] \arrow[r] & \mathcal{K}_{\epsilon+\delta(T),\mathbb{P}^9_{k'_{ij},T}} \arrow[r, squiggly, "g_2"] & \mathcal{K}_{\epsilon+\delta(T)} \subset \mathbb{P}^3_{k'_{i,T}} \arrow[u, "\psi_{\epsilon+\delta(T)}"']
\end{tikzcd} \tag{4·5}$$

Recall Proposition 4·3 explains how Ψ can be explicitly computed and the composition of the wavy arrows in (4·5) is defined over K by Lemma 4·2. Let D_T be the pull back on J_ϵ via the wavy arrows in (4·5) of the hyperplane section given by $k'_{1,T}=0$. This implies that D_T is a K-rational divisor on J_ϵ representing the class of $\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))$. Moreover the pull back on J_ϵ via the composition of the first three wavy arrows in (4·5) of the hyperplane section given by $k'_{11,T}=0$ is $2D_T$.

We now apply the above discussion with $T=P,Q,R,S$ and obtain the divisors D_P,D_Q,D_R,D_S on J_ϵ described in Remark 3·2 as required.

Remark 4·5. From the above discussion and the discussion in Section 4·2, the K-rational functions f_P,f_Q,f_R,f_S in the formula for the Cassels–Tate pairing in Theorem 3·3 are quotients of linear forms in the coordinates of the ambient space of $J_\epsilon \subset \mathbb{P}^{15}$. They all have the same denominator, this being the linear form that cuts out the divisor $2D$.

5. *The Obstruction Map*

In this section, we will state and prove an explicit formula for the obstruction map $\mathrm{Ob}: H^1(G_K, J[2]) \to \mathrm{Br}(K)$. See below for the definition of this map. This generalizes a formula in the elliptic curve case due to O'Neil [**O'N02**, proposition 3·4], and later refined by Clark [**Cla05**, theorem 6]. Although this is not needed for the computation of the Cassels–Tate pairing, it explains why we needed to work with quaternion algebras in Section 4·1.

Definition 5·1. The obstruction map

$$\mathrm{Ob}: H^1(G_K, J[2]) \to H^2(G_K, \bar{K}^*) \cong \mathrm{Br}(K)$$

is the composition of the map $H^1(G_K, J[2]) \to H^1(G_K, \mathrm{PGL}_4(\bar{K}))$ induced by the action of translation of $J[2]$ on $\mathcal{K} \subset \mathbb{P}^3$, and the injective map $H^1(G_K, \mathrm{PGL}_4(\bar{K})) \to H^2(G_K, \bar{K}^*)$ induced from the short exact sequence $0 \to \bar{K}^* \to \mathrm{GL}_4(\bar{K}) \to \mathrm{PGL}_4(\bar{K}) \to 0$.

THEOREM 5·2. *Let J be the Jacobian variety of a genus two curve defined over a field K with char$(K) \neq 2$. Suppose all points in J[2] are defined over K. For $\epsilon \in H^1(G_K, J[2])$, represented by $(a,b,c,d) \in (K^*/(K^*)^2)^4$ as in Section* 3*, the obstruction map* $\mathrm{Ob}: H^1(G_K, J[2]) \to \mathrm{Br}(K)$ *sends ϵ to the class of the tensor product of two quaternion algebras:*

$$\mathrm{Ob}(\epsilon) = (c_P a, c_Q b) \otimes (c_R c, c_S d),$$

where $c_P, c_Q, c_R, c_S \in K$ are such that $M_P^2 = c_P I, M_Q^2 = c_Q I, M_R^2 = c_R I,$ and $M_S^2 = c_S I$ as defined in Section 4·1.

Proof. Let $N_P = 1/\sqrt{c_P} M_P, N_Q = 1/\sqrt{c_Q} M_Q, N_R = 1/\sqrt{c_R} M_R, N_S = 1/\sqrt{c_S} M_S \in \mathrm{GL}_4(\bar{K})$. Then N_P is a normalised representation in $\mathrm{GL}_4(\bar{K})$ of $[M_P] \in \mathrm{PGL}_4(K)$. Similar statements are true for Q, R, S. Notice that $N_P^2 = N_Q^2 = N_R^2 = N_S^2 = I$. So there is a uniform way of picking a representation in $\mathrm{GL}_4(\bar{K})$ for the translation induced by $\alpha_1 P + \alpha_2 Q + \alpha_3 R + \alpha_4 S$ for $\alpha_i \in \mathbb{Z}$, namely $N_P^{\alpha_1} N_Q^{\alpha_2} N_R^{\alpha_3} N_S^{\alpha_4}$.

https://doi.org/10.1017/S0305004124000318

Since $\epsilon \in H^1(K, J[2])$ is represented by $(a, b, c, d) \in (K^*/K^{*2})^4$ and P, Q, R, S satisfy the Weil pairing matrix (3·1), a cocycle representation of ϵ is:

$$\sigma \mapsto \tilde{b}_\sigma P + \tilde{a}_\sigma Q + \tilde{d}_\sigma R + \tilde{c}_\sigma S,$$

where for each element $x \in K^*/(K^*)^2$, we define $\tilde{x}_\sigma \in \{0, 1\}$ such that $(-1)^{\tilde{x}_\sigma} = \sigma(\sqrt{x})/\sqrt{x}$.

Now consider the following commutative diagram of cochains:

$$\begin{tikzcd}
C^1(G_K, \bar{K}^*) \arrow[r] \arrow[d, "d"] & C^1(G_K, \mathrm{GL}_4) \arrow[r] \arrow[d, "d"] & C^1(G_K, \mathrm{PGL}_4) \arrow[d, "d"] \\
C^2(G_K, \bar{K}^*) \arrow[r] & C^2(G_K, \mathrm{GL}_4) \arrow[r] & C^2(G_K, \mathrm{PGL}_4).
\end{tikzcd}$$

Defining $N_\sigma = N_P^{\tilde{b}_\sigma} N_Q^{\tilde{a}_\sigma} N_R^{\tilde{d}_\sigma} N_S^{\tilde{c}_\sigma}$, we have

$$H^1(K, J[2]) \to H^1(G_K, \mathrm{PGL}_4)$$
$$(a, b, c, d) \mapsto (\sigma \mapsto [N_\sigma]).$$

Then $(\sigma \mapsto [N_\sigma]) \in C^1(G_K, \mathrm{PGL}_4)$ lifts to $(\sigma \mapsto N_\sigma) \in C^1(G_K, \mathrm{GL}_4)$ which is then mapped to

$$\Big((\sigma, \tau) \mapsto (N_\tau)^\sigma N_{\sigma\tau}^{-1} N_\sigma\Big) \in C^2(G_K, \mathrm{GL}_4).$$

Note that

$$N_P^\sigma = \left(\frac{1}{\sqrt{c_P}} M_P\right)^\sigma = \frac{1}{\sigma(\sqrt{c_P})} M_P = \frac{\sqrt{c_P}}{\sigma(\sqrt{c_P})} N_P = (-1)^{(\widetilde{c_P})_\sigma} N_P,$$

treating c_P in $K^*/(K^*)^2$. Similar results also hold for Q, R, S. Observe that for any $x \in K^*/(K^*)^2$ and $\sigma, \tau \in G_K$, we have $\tilde{x}_\tau - \tilde{x}_{\sigma\tau} + \tilde{x}_\sigma$ is equal to 0 or 2. Since $N_P^2 = N_Q^2 = N_R^2 = N_S^2 = I$, $[N_P, N_Q] = [N_R, N_S] = -I$ and the commutators of the other pairs are trivial, we have

$$\begin{aligned}
(N_\tau)^\sigma N_{\sigma\tau}^{-1} N_\sigma &= \left(N_P^{\tilde{b}_\tau} N_Q^{\tilde{a}_\tau} N_R^{\tilde{d}_\tau} N_S^{\tilde{c}_\tau}\right)^\sigma \cdot N_S^{-\tilde{c}_{\sigma\tau}} N_R^{-\tilde{d}_{\sigma\tau}} N_Q^{-\tilde{a}_{\sigma\tau}} N_P^{-\tilde{b}_{\sigma\tau}} \cdot N_P^{\tilde{b}_\sigma} N_Q^{\tilde{a}_\sigma} N_R^{\tilde{d}_\sigma} N_S^{\tilde{c}_\sigma} \\
&= (-1)^{(\widetilde{c_P})_\sigma \cdot \tilde{b}_\tau} \cdot (-1)^{(\widetilde{c_Q})_\sigma \cdot \tilde{a}_\tau} \cdot (-1)^{(\widetilde{c_R})_\sigma \cdot \tilde{d}_\tau} \cdot (-1)^{(\widetilde{c_S})_\sigma \cdot \tilde{c}_\tau} \\
&\quad \cdot N_P^{\tilde{b}_\tau} N_Q^{\tilde{a}_\tau} \cdot N_R^{\tilde{d}_\tau} N_S^{\tilde{c}_\tau} N_S^{-\tilde{c}_{\sigma\tau}} N_R^{-\tilde{d}_{\sigma\tau}} \cdot N_Q^{-\tilde{a}_{\sigma\tau}} N_P^{-\tilde{b}_{\sigma\tau}} N_P^{\tilde{b}_\sigma} N_Q^{\tilde{a}_\sigma} \cdot N_R^{\tilde{d}_\sigma} N_S^{\tilde{c}_\sigma} \\
&= (-1)^{(\widetilde{c_P})_\sigma \cdot \tilde{b}_\tau} \cdot (-1)^{(\widetilde{c_Q})_\sigma \cdot \tilde{a}_\tau} \cdot (-1)^{(\widetilde{c_R})_\sigma \cdot \tilde{d}_\tau} \cdot (-1)^{(\widetilde{c_S})_\sigma \cdot \tilde{c}_\tau} \\
&\quad \cdot N_P^{\tilde{b}_\tau} N_Q^{\tilde{a}_\tau} N_Q^{-\tilde{a}_{\sigma\tau}} N_P^{-\tilde{b}_{\sigma\tau}} N_P^{\tilde{b}_\sigma} N_Q^{\tilde{a}_\sigma} \cdot N_R^{\tilde{d}_\tau} N_S^{\tilde{c}_\tau} N_S^{-\tilde{c}_{\sigma\tau}} N_R^{-\tilde{d}_{\sigma\tau}} N_R^{\tilde{d}_\sigma} N_S^{\tilde{c}_\sigma} \\
&= (-1)^{(\widetilde{c_P})_\sigma \cdot \tilde{b}_\tau} \cdot (-1)^{(\widetilde{c_Q})_\sigma \cdot \tilde{a}_\tau} \cdot (-1)^{(\widetilde{c_R})_\sigma \cdot \tilde{d}_\tau} \cdot (-1)^{(\widetilde{c_S})_\sigma \cdot \tilde{c}_\tau} \cdot (-1)^{\tilde{a}_\sigma \cdot \tilde{b}_\tau} \\
&\quad \cdot (-1)^{\tilde{c}_\sigma \cdot \tilde{d}_\tau} \cdot I.
\end{aligned}$$

On the other hand, $(c_P, c_Q) \otimes (c_R, c_S)$ is isomorphic to $\langle M_P, M_Q, M_R, M_S \rangle = \mathrm{Mat}_4(K)$ which represents the identity element in the Brauer group. Hence, we have

$$(c_P a, c_Q b) \otimes (c_R c, c_S d) = (a, b) \otimes (c, d) \otimes (c_P, b) \otimes (c_Q, a) \otimes (c_R, d) \otimes (c_S, c),$$

which is precisely represented by a cocycle that sends (σ, τ) to

$$(-1)^{(\widetilde{c_P})_\sigma \cdot \tilde{b}_\tau} \cdot (-1)^{(\widetilde{c_Q})_\sigma \cdot \tilde{a}_\tau} \cdot (-1)^{(\widetilde{c_R})_\sigma \cdot \tilde{d}_\tau} \cdot (-1)^{(\widetilde{c_S})_\sigma \cdot \tilde{c}_\tau} \cdot (-1)^{\tilde{a}_\sigma \cdot \tilde{b}_\tau} \cdot (-1)^{\tilde{c}_\sigma \cdot \tilde{d}_\tau},$$

for all $\sigma, \tau \in G_K$ as required.

6. *Bounding the Set of Primes*

In this section, we directly show that the formula for $\langle \epsilon, \eta \rangle_{CT}$ in Theorem 3·3 is actually always a finite product, as mentioned in Remark 3·4. Since for a local field with odd residue characteristic, the Hilbert symbol between x and y is trivial when the valuations of x, y are both 0, it suffices to find a finite set S of places of K, such that outside S the first arguments of the Hilbert symbols in the formula for $\langle \epsilon, \eta \rangle_{CT}$ have valuation 0 for some choice of the local point P_v.

Let $\mathcal{O}_K$ be the ring of integers for the number field K. By rescaling the variables, we assume the genus two curve is defined by $y^2 = f(x) = f_6 x^6 + \cdots + f_0$ where the f_i are in $\mathcal{O}_K$.

The first arguments of the Hilbert symbols in the formula for $\langle \epsilon, \eta \rangle_{CT}$ are $f_P(P_v), f_Q(P_v)$, $f_R(P_v)$ or $f_S(P_v)$, where f_P, f_Q, f_R, f_S can be computed as the quotients of two linear forms in $\mathbb{P}^{15}$ with the denominators being the same, as explained in Remark 4·5. Since we know that the Cassels–Tate pairing is independent of the choice of the local points P_v as long as these are chosen to avoid all the zeros and poles, it suffices to make sure that there exists at least one local point P_v on J_ϵ for which the values of the quotients of the linear forms all have valuation 0 for all v outside S. The idea is to first reduce the problem to the residue field.

By Theorem 2·9 and Remark 2·10, we have an explicit formula for the isomorphism

$$J_\epsilon \xrightarrow{\phi_\epsilon} J.$$

It is given by a change of coordinates on the ambient space $\mathbb{P}^{15}$ and is defined over $K' = K(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d})$ where $\epsilon = (a, b, c, d) \in (K^*/(K^*)^2)^4$. Suppose ϕ_ϵ is represented by $M_\epsilon \in \mathrm{GL}_{16}(K')$. By scaling, we can assume that all entries of M_ϵ are in $\mathcal{O}_{K'}$, the ring of integers of K'.

Notation 6·1. Let K be a local field with valuation ring $\mathcal{O}_K$, uniformiser π and residue field k. Let $X \subset \mathbb{P}^N$ be a variety defined over K and $I(X) \subset K[x_0, ..., x_N]$ be the ideal of X. Then the reduction of X, denoted by $\bar{X}$, is the variety defined by the polynomials $\{\bar{f} : f \in I(X) \cap \mathcal{O}_K[x_0, ..., x_N]\}$. Here $\bar{f}$ is the polynomial obtained by reducing all the coefficients of f modulo π. Note that this definition of the reduction of a variety $X \subset \mathbb{P}^N$ defined over a local field K is equivalent to taking the special fibre of the closure of X in $\mathbb{P}^N_S$, where $S = \operatorname{Spec} \mathcal{O}_K$.

Let $S_0 = \{\text{places of bad reduction for } \mathcal{C}\} \cup \{\text{places dividing } 2\} \cup \{\text{infinite places}\}$. Fix a place $v \notin S_0$ of K and suppose it is above the prime p. We now treat J, J_ϵ and $\mathcal{C}$ as varieties defined over the local field K_v. Let $\mathcal{O}_v$ denote the valuation ring of K_v and $\mathbb{F}_q$ denote its residue field, where q is some power of p. It can be shown that $\bar{J}$ is also an abelian variety as the defining equations of J are defined over $\mathcal{O}_v$ and are derived algebraically in terms of the coefficients of the defining equation of the genus two curve $\mathcal{C}$ by Theorem 2·2. In fact, $\bar{J}$ is the Jacobian variety of $\bar{\mathcal{C}}$, the reduction of $\mathcal{C}$.

Now fix a place v' of K' above the place v of K. Let $\mathcal{O}_{v'}$ and $\mathbb{F}_{q^r}$ denote the valuation ring and the residue field of $K'_{v'}$. It can be checked that as long as v' does not divide $\det M_\epsilon \in \mathcal{O}_{K'}$, the reduction $\bar{M}_\epsilon$ of M_ϵ over the residue field $\mathbb{F}_{q^r}$ defines a linear isomorphism $\bar{J}_\epsilon \to \bar{J}$.

This linear isomorphism $\bar{M}_\epsilon$ implies that $\bar{J}_\epsilon$ is smooth whenever $\bar{J}$ is. In this case, $\bar{J}_\epsilon$ is a twist of $\bar{J}$ and is in fact a 2-covering of $\bar{J}$. Indeed, the surjectivity of the natural map $\mathrm{Gal}(K'_{v'}/K_v) \to \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ shows that $M_\epsilon(M_\epsilon^{-1})^\sigma = \tau_{P_\sigma}$ for all $\sigma \in \mathrm{Gal}(K'_{v'}/K_v)$ implies that $\bar{M}_\epsilon(\bar{M}_\epsilon{}^{-1})^{\bar{\sigma}} = \tau_{\bar{P_\sigma}}$ for all $\bar{\sigma} \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$. This means any principal homogeneous space of $\bar{J}$ over a finite field has a point by [Lan56, theorem 2] and so is trivial by Proposition 2·4. Therefore, there exists an isomorphism $\bar{J}_\epsilon \xrightarrow{\psi} \bar{J}$ defined over $\mathbb{F}_q$. Hence, as long as $v \notin S_0$ and v does not divide $N_{K'/K}(\det M_\epsilon)$, $\bar{J}_\epsilon$ has the same number of $\mathbb{F}_q$-points as $\bar{J}$. It is well known that the points on an abelian variety A of dimension g over the finite field $\mathbb{F}_q$, satisfies $(\sqrt{q}-1)^{2g} \leq |A(\mathbb{F}_q)|$. In our case, this means that the number of $\mathbb{F}_q$-points on $\bar{J}$ is bounded below by $(\sqrt{q}-1)^4$.

On the other hand, let $l_1, ..., l_5$ be the 5 linear forms that appear as numerator or denominator of f_P, f_Q, f_R, f_S. We can assume that the coefficients of l_i are in $\mathcal{O}_K$ by scaling, for all $i = 1, ..., 5$. Fix a place v of K that does not divide all the coefficients of l_i, for any $i = 1, ..., 5$. Let H_i be the hyperplane defined by the linear form l_i and $\bar{H}_i$ be its reduction, which is a hyperplane defined over the residue field $\mathbb{F}_q$. We need to bound the number of $\mathbb{F}_q$-points of $\bar{J}_\epsilon$ that lie on one of the hyperplanes $\bar{H}_i$. Let r_i be the number of irreducible components of $\bar{J}_\epsilon \cap \bar{H}_i$. By [Har77, chapter 1, theorem 7·2 (Projective dimension theorem) and Theorem 7·7], we know that each irreducible component C^i_j of $\bar{J}_\epsilon \cap \bar{H}_i$, where $j = 1, ..., r_i$, is a curve and the sum of degrees of all the irreducible components counting intersection multiplicity is $\deg \bar{J}_\epsilon = 32$. Letting $d^i_j = \deg C^i_j$, we have $\sum_{j=1}^{r_i} d^i_j \leq 32$ for all i.

LEMMA 6·2. *Let $C \subset \mathbb{P}^N$ be a curve of degree d. Then $\#C(\mathbb{F}_q) \leq d(q+1)$.*

Proof. We may assume that C is contained in no hyperplane. Then projection to the first two coordinates gives a nonconstant morphism $C \to \mathbb{P}^1$ of degree $\leq d$. Since $\#\mathbb{P}^1(\mathbb{F}_q) = q+1$, this gives the required bound.

By applying the above lemma to each C^i_j, we get the number of $\mathbb{F}_q$-points of $\bar{J}_\epsilon$ that lie on one of the hyperplanes $\bar{H}_i$, $i = 1, ..., 5$, is no more than

$$\sum_{i=1}^{5} \sum_{j=1}^{r_i} d^i_j \cdot (q+1) \leq 160(q+1).$$

We compute that for any $x 213$, we have $(\sqrt{x}-1)^4 160(x+1)$. Recall q is a power of p. Hence, if v is a place of K above the prime $p 213$ such that $v \notin S_0$ and v does not divide $N_{K'/K}(\det M_\epsilon)$ or all the coefficients of l_i for some i, we have a smooth $\mathbb{F}_q$-point on $\bar{J}_\epsilon$ which by Hensel's Lemma [HS00, exercise C·9(c)] lifts to the point P_v as required. This implies that the first arguments of the Hilbert symbols in the formula for the local Cassels–Tate pairing of $\langle \epsilon, \eta \rangle_{CT}$ have valuation 0. It can be checked that since $v \notin S_0$, the second arguments of these Hilbert symbols also have valuation 0. Hence, the formula for the Cassels–Tate is indeed always a finite product.

Note that in the case where $K = \mathbb{Q}$ or more generally if K has class number 1, we can always make the linear forms primitive by scaling. Therefore, in this case, the subset {places dividing all the coefficients of the denominator or the numerator of f_P, f_Q, f_R or f_S} is empty.

7. *Worked Example*

Now we demonstrate the algorithm with a worked example computed using MAGMA [**BCP97**]. In particular, we will see with this example, that computing the Cassels–Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ does improve the rank bound obtained via a 2-descent. This genus two curve was kindly provided by my PhD supervisor, Tom Fisher, along with a list of other genus two curves for me to test the algorithm.

Consider the following genus two curve

$$\mathcal{C} : y^2 = -10x(x+10)(x+5)(x-10)(x-5)(x-1).$$

Its Jacobian variety J has all its two-torsion points defined over $\mathbb{Q}$. A set of generators of $J[2]$ compatible with the Weil pairing matrix (3·1) are $P = \{(0,0),(-10,0)\}, Q = \{(0,0),(-5,0)\}, R = \{(10,0),(5,0)\}, S = \{(10,0),(1,0)\}$. We identify $H^1(G_{\mathbb{Q}}, J[2]) = (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^4$ as in Section 3. Consider $\epsilon, \eta \in \mathrm{Sel}^2(J)$ represented by $(-33, 1, -1, -11)$ and $(11, 1, -1, -11)$ respectively. The images of $[P]$, $[Q]$, $[R]$, $[S]$ via $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \to H^1(G_{\mathbb{Q}}, J[2])$, computed via the explicit formula as in [**CF96**, chapter 6, section 1], are $\delta([P]) = (-66, 1, 6, 22)$, $\delta([Q]) = (-1, 1, 3, 1)$, $\delta([R]) = (6, 3, 1, 3)$, $\delta([S]) = (22, 1, -3, -11)$. Now following the discussions in Sections 4·2 and 4·3, we can compute, using the coordinates $c_0, ..., c_9, d_1, ..., d_6$ for $J_\epsilon \in \mathbb{P}^{15}$ as described in Remark 2·10. We have

$$\begin{aligned}
k'_{11} &= 618874080c_0 - 496218440c_1 - 390547052c_3 + 205551080c_4 \\
&\quad + 384569291c_6 + 52868640c_8; \\
k'_{11,P} &= -36051078800000c_2 + 8111492730000c_3 + 265237150000c_7 \\
&\quad - 196928587500c_8 - 6786529337500c_9 + 22531924250d_2 \\
&\quad - 126449158891d_4 - 117221870375d_5 + 937774963000d_6; \\
k'_{11,Q} &= 134800c_1 + 235600c_3 + 62000c_4 + 52235c_6 + 60016d_1 - 5456d_5; \\
k'_{11,R} &= -30223125c_6 + 4050000c_8 - 49750d_3 + 709236d_4 \\
k'_{11,S} &= 4724524800c_1 + 8557722360c_3 + 13102732800c_4 + 1258642935c_6 \\
&\quad + 7291944000c_9 - 2709362304d_1 + 97246845d_2 + 8475710d_3 \\
&\quad + 30788208d_5.
\end{aligned}$$

Hence, we have explicit formulae for

$$f_P = \frac{k'_{11,P}}{k'_{11}}, f_Q = \frac{k'_{11,Q}}{k'_{11}}, f_R = \frac{k'_{11,R}}{k'_{11}}, f_S = \frac{k'_{11,S}}{k'_{11}}.$$

In particular, they are defined over $\mathbb{Q}$ as claimed. From Section 6, we compute that only primes below 213 can potentially contribute to $\langle \epsilon, \eta \rangle_{CT}$. Then, it turns out that the only nontrivial local Cassels–Tate pairings between ϵ and η are at places $11, 19, \infty$ and $\langle \epsilon, \eta \rangle_{CT} = -1$.

We find that $\mathrm{Sel}^2(J)$ has size 2^6 and is generated by $(-33, 1, -1, -11), (11, 1, -1, -11), (66, 1, 2, 22), (11, 1, 2, 22), (3, 3, 3, 3), (3, 1, 3, 1)$. Since $\mathcal{C}$ has rational points, the Cassels–Tate pairing can be shown to be alternating using [**PS99**, corollary 7]. Since all the two-torsion points on J are rational and $\langle \epsilon, \eta \rangle_{CT} = -1$, we get $|\ker\langle\ ,\ \rangle_{CT}| = 2^4$.

Indeed, we verified that the Cassels–Tate pairing matrix, with the generators of $\mathrm{Sel}^2(J)$ listed above, is

$$\begin{bmatrix} 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & -1 & -1 & 1 \end{bmatrix},$$

which is a rank 2 matrix.

As shown in [Yan, remark 1·9·4(ii)], in the case where all points in $J[2]$ are defined over the base field, computing the Cassels–Tate pairing on $\mathrm{Sel}^2(J)$ gives the same rank bound as obtained from carrying out a 4-descent, i.e. computing $\mathrm{Sel}^4(J)$, which can potentially give a better rank bound than the one given by a 2-descent. Let $r = \mathrm{rank}(J(\mathbb{Q}))$. In this example, the rank bound coming from 2-decent was $r \leq 2$ as $2^r = |J(\mathbb{Q})/2J(\mathbb{Q})|/|J(\mathbb{Q})[2]| \leq |\mathrm{Sel}^2(J)|/|J(\mathbb{Q})[2]| = 2^2$. Our calculations of the Cassels–Tate pairing on $\mathrm{Sel}^2(J)$ improves this bound and in fact shows that $r = 0$ as $2^r = |J(\mathbb{Q})/2J(\mathbb{Q})|/|J(\mathbb{Q})[2]| \leq |\ker\langle\,,\,\rangle_{CT}|/|J(\mathbb{Q})[2]| = 2^0$.

Remark 7·1. As the referee points out, it is also possible to prove that the rank of $J(\mathbb{Q})$ is zero in this example by carrying out a 2-descent on one of the Richelot-isogenous Jacobians. It would be interesting to find an example (still with full rational 2-torsion) where this does not work, i.e. all the isogenous abelian surfaces have non-trivial 2-torsion in Ш.

Acknowledgements. I express my sincere and deepest gratitude to my PhD supervisor, Tom Fisher, for his patient guidance and insightful comments at every stage during my research.I would like to thank my referee for the detailed and constructive comments.

REFERENCES

[vB] M. VAN BEEK. Computing the Cassels–Tate Pairing. PhD. thesis. University of Cambridge (2015).

[vBF18] M. VAN BEEK and T. A. FISHER. Computing the Cassels–Tate pairing on 3-isogeny Selmer groups via cubic norm equations. *Acta Arithmetica* **185**(4) (2018), 367–396. DOI 10.4064/AA171108-11-4.

[BCP97] W. BOSMA, J. CANNON, and C. PLAYOUST. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24**(3–4) (1997), 235–265. DOI 10.1006/jsco.1996.0125.

[Cas59] J. W. S. CASSELS. Arithmetic on Curves of Genus 1. I. On a conjecture of Selmer. *J. Reine Angew. Math.* **202** (1959), 52–99.

[Cas62] J. W. S. CASSELS. Arithmetic on curves of genus 1, IV. Proof of the Hauptver-mutung. *J. Reine Angew. Math.* **211** (1962), 95–112. DOI 10.1515/crll.1962.211.95.

[Cas98] J. W. S. CASSELS. Second Descents for Elliptic Curves. *J. Reine Angew. Math.* **494** (1998), 101–127. DOI 10.1515/crll.1998.001.

[CF96] J. W. S. CASSELS and E. V. FLYNN. Prolegomena to a MiddleBrow Arithmetic of Curves of Genus 2. London *Math. Soc.* Lecture Note Series, vol. 230 (Cambridge University Press, 1996).

[CF67] J. W. S. CASSELS and A. FROHLICH. Algebraic Number Theory. Proceedings of an instructional conference organised by the London Mathematical Society (a nano advanced study institute) with the support of the international union. (Academic Press Inc. London LTD., 1967).

[Cla05] P. L. CLARK. The Period-Index Problem in WC-Groups I: Elliptic Curves. *J. Number Theory* **114** (2005), 193–208. DOI 10.1016/j.jnt.2004.10.001.

[CM96] D. CORAY and C. MANOIL. On large Picard groups and the Hasse Principle for curves and K3 surfaces. *Acta Arithmetica* **76**(2) (1996), 165–189. DOI 10.4064/aa-76-2-165-189.

[Don15] S. DONNELLY. Algorithms for the Cassels–Tate pairing. (2015), preprint.

[Fis03] T. A. FISHER. The Cassels-Tate pairing and the Platonic solids. *J. Number Theory* **98**(1) (2003), 105–155. DOI 10.1016/S0022-314X(02)00038-0.

[FSS10] T.A. FISHER, E.F. SCHAEFER and M. STOLL. The yoga of the Cassels–Tate pairing, LMS. *J. Comput. Math*. **13** (2010), 451–460.

[Fis16] T. A. FISHER. On binary quartics and the Cassels–Tate pairing. (2016), preprint.

[FN14] T. A. FISHER and R. NEWTON. Computing the Cassels–Tate pairing on the 3-Selmer group of an elliptic curve. *J. Number Theory* **10**(7) (2014), 18811907. DOI 10.1142/S1793042114500602.

[Fly90] E. V. FLYNN. The Jacobian and Formal Group of a Curve of Genus 2 over an Arbitrary Ground Field. *Math. Proc. Camb. Phil. Soc.* **107**(3) (1990), 425–441. DOI 10.1017/S0305004100068729.

[Fly93] E. V. FLYNN. The Group Law on the Jacobian of a Curve of Genus 2. *J. Reine Angew. Math.* **439** (1993), 45–70.

[FTvL12] E. V. FLYNN, D. TESTA and R. VAN LUIJK. Two-Coverings of Jacobians of Curves of Genus 2. *Proc. London Math. Soc.* **104**(2) (2012), 387–429. DOI 10.1112/plms/pdr012.

[GS06] P. GILLE and T. SZAMUELY. Central Simple Algebras and Galois Cohomology. *Camb. Stud. Adv. Math.* vol. **101** (Cambridge University Press, 2006).

[Har77] R. HARTSHORNE. Algebraic Geometry. *Graduate Texts in Math.* vol. 52, (Springer, New York, NY, 1977).

[HS00] M. HINDRY and J. H. SILVERMAN. *Diophantine Geometry: An Introduction*. Graduate Texts in Math. 201, vol. 52 (Springer, 2000).

[Lan56] S. LANG. Algebraic groups over finite fields. *Amer. J. Math.* **78**(3) (1956), 555–563. DOI 10.2307/2372673.

[Mil06] J.S. MILNE. *Arithmetic Duality Theorems*. second edition (BookSurge, LLC, Charleston, SC, 2006).

[Mil08] J.S. MILNE. Abelian Varieties, second edition, 2008. Available at www.jmilne.org/math/.

[Mum70] D. MUMFORD. Abelian Varieties. Tata Institute of Fundamental Research Studies in Mathematics (Oxford University Press, 1970). Published for the Tata Institute of Fundamental Research, Bombay.

[O'N02] C. O'NEIL. The period-index obstruction for elliptic curves. *J. Number Theory* **95** (2002), 329–339. DOI 10.1006/jnth.2001.2770.

[PS99] B. POONEN and M. STOLL. The Cassels–Tate pairing on polarised abelian varieties. *Ann. of Math.* **150**(3) (1999), 1109-1149. DOI 10.2307/121064. MR1740984

[Tat62] J. TATE. *Duality theorems in Galois cohomology over number fields*. *Proc. Internat. Congr.* Mathematicians (Stockholm) (1962), 288–295 (Inst. Mittag-Leffer, Djursholm), (1963).

[Yan] J. YAN. Computing the Cassels–Tate pairing for Jacobian varieties of genus two curves. *Phd. thesis.* University of Cambridge (2021).