ON BINARY QUARTICS AND THE CASSELS-TATE PAIRING

TOM FISHER

ABSTRACT. We use the invariant theory of binary quartics to give a new formula for the Cassels-Tate pairing on the 2-Selmer group of an elliptic curve. Unlike earlier methods, our formula does not require us to solve any conics. An important role in our construction is played by a certain $K3$ surface defined by a $(2, 2, 2)$-form.

1. INTRODUCTION

Let E be an elliptic curve over a number field K. The Mordell-Weil theorem tells us that the abelian group $E(K)$ is finitely generated, but there is no known algorithm guaranteed to compute its rank. Instead, for each integer $n \geq 2$ there is an exact sequence of abelian groups

$$0 \to E(K)/nE(K) \to S^{(n)}(E/K) \to Ш(E/K)[n] \to 0.$$

The n-Selmer group $S^{(n)}(E/K)$ is finite and effectively computable. Computing $S^{(n)}(E/K)$ gives an upper bound for the rank of $E(K)$, but this will be sharp only if the n-torsion of the Tate-Shafarevich group $Ш(E/K)$ is trivial.

Cassels [4] showed that there is an alternating pairing

$$\langle\ .\ \rangle_{\mathrm{CT}} : S^{(n)}(E/K) \times S^{(n)}(E/K) \to \mathbb{Q}/\mathbb{Z}$$

whose kernel is the image of $S^{(n^2)}(E/K)$. By computing this pairing, our upper bound for the rank of $E(K)$ improves from that obtained by n-descent to that obtained by n^2-descent. In view of the generalisation to abelian varieties, due to Tate, the pairing is known as the Cassels-Tate pairing.

Cassels [6] also described a method for computing the pairing in the case $n = 2$. His method involves solving conics over the field of definition of each 2-torsion point on E. More recently, Donnelly [10] found a method that only involves solving conics over K, and implemented this in `Magma` [3]. In this article we use the invariant theory of binary quartics to give a self-contained account of a version of his method that is relatively simple to implement.

Since this article was first written, Jiali Yan has written her PhD thesis [18], extending some of these ideas to Jacobians of genus 2 curves, and Bill Allombert has implemented our method for computing the pairing as part of the function `ellrank` in `pari/gp` [15]. I thank them both, and also Steve Donnelly and John Cremona, for useful discussions.

Date: 31st August 2022.

2. Binary quartics

A *binary quartic* over a field K is a homogeneous polynomial $g \in K[x,z]$ of degree 4. Binary quartics g_1 and g_2 are K*-equivalent* if

$$g_2(x,z) = \lambda^2 g_1(\alpha x + \gamma z, \beta x + \delta z)$$

for some $\lambda, \alpha, \beta, \gamma, \delta \in K$ with $\lambda(\alpha\delta - \beta\gamma) \neq 0$. They are *properly* K-equivalent if in addition $\lambda(\alpha\delta - \beta\gamma) = \pm 1$. The invariants of the binary quartic

$$g(x,z) = ax^4 + bx^3 z + cx^2 z^2 + dxz^3 + ez^4 \tag{1}$$

are

$$\begin{aligned} I &= 12ae - 3bd + c^2, \\ J &= 72ace - 27ad^2 - 27b^2 e + 9bcd - 2c^3. \end{aligned}$$

The binary quartics g_1 and g_2 have invariants related by $I(g_2) = \lambda^4(\alpha\delta - \beta\gamma)^4 I(g_1)$ and $J(g_2) = \lambda^6(\alpha\delta - \beta\gamma)^6 J(g_1)$. In particular, properly equivalent binary quartics have the same invariants. The discriminant is $\Delta = 16(4I^3 - J^2)/27$. We say that g is K*-soluble* if there exist $x, z \in K$, not both zero, such that $g(x,z)$ is a square in K. The reason for this terminology is that if $\Delta(g) \neq 0$ then there is a smooth projective curve C of genus one with affine equation $y^2 = g(x,1)$, and we are asking that $C(K) \neq \emptyset$. As shown by Weil [17], the Jacobian of C is the elliptic curve

$$E_{I,J}: \quad y^2 = x^3 - 27Ix - 27J. \tag{2}$$

Now let K be a number field, and M_K its set of places. A binary quartic over K is *everywhere locally soluble* if it is K_v-soluble for all places $v \in M_K$. We note that every elliptic curve over K can be written in the form (2) for some $I, J \in K$ with $4I^3 - J^2 \neq 0$.

Lemma 2.1. *Let $I, J \in K$ with $4I^3 - J^2 \neq 0$. Then*

$$S^{(2)}(E_{I,J}/K) = \left\{ \begin{array}{c} \textit{everywhere locally soluble} \\ \textit{binary quartics over } K \\ \textit{with invariants } I \textit{ and } J \end{array} \right\} / (\textit{proper } K\textit{-equivalence}).$$

Proof. The case $K = \mathbb{Q}$ is proved in [2], the only simplification in this case being that (since the only roots of unity in $\mathbb{Q}$ are ± 1) equivalent quartics with the same invariants are always properly equivalent (even in the cases where $I = 0$ or $J = 0$). The general case is similar. $\square$

Although Lemma 2.1 specifies $S^{(2)}(E_{I,J}/K)$ as a set, the group law is not obvious. The following description is taken from [8], [9]. Let L be the étale algebra

$K[\varphi]$ where φ is a root of $X^3 - 3IX + J = 0$. Then the binary quartic (1) has *cubic invariant*

$$z(g) = \frac{4a\varphi + 3b^2 - 8ac}{3}.$$

By a change of coordinates (that is, replacing g by a properly equivalent quartic) we may assume that $z(g)$ is a unit in L. The group law on $S^{(2)}(E_{I,J}/K)$ is then given by multiplying the cubic invariants in $L^\times/(L^\times)^2$. The method for converting an element of $L^\times/(L^\times)^2$ back to a binary quartic does, however, involve solving a conic over K.

3. Statement of results

In this section we state our new formula for the Cassels-Tate pairing on the 2-Selmer group of an elliptic curve. First we need some more invariant theory. The binary quartic (1) has Hessian

$$\begin{aligned} h(x,z) = (3b^2 - 8ac)x^4 + 4(bc - 6ad)x^3z + 2(2c^2 - 24ae - 3bd)x^2z^2 \\ + 4(cd - 6be)xz^3 + (3d^2 - 8ce)z^4. \end{aligned}$$

There are exactly three linear combinations of $g(x,z)$ and $h(x,z)$ that are singular (i.e. have repeated roots). Following [9] this prompts us to put

$$G(x,z) = \frac{1}{3}\left(4\varphi g(x,z) + h(x,z)\right), \tag{3}$$

$$H(x,z) = \frac{1}{12}\frac{\partial^2 G}{\partial x^2} + \frac{2}{9}(I - \varphi^2)z^2, \tag{4}$$

so that $G(1,0)G(x,z) = H(x,z)^2$. We note that $z(g) = G(1,0) = H(1,0)$.

Theorem 3.1. *Let $I, J \in K$ with $4I^3 - J^2 \neq 0$. Let g_1, g_2, g_3 be everywhere locally soluble binary quartics over K with invariants I and J. Let $H_1(x,z)$ be the binary quadratic form (4), with coefficients in $L = K[\varphi]$, associated to g_1. Suppose that $z(g_1)z(g_2)z(g_3) = m^2$ for some $m \in L^\times$, and write*

$$\frac{z(g_2)z(g_3)}{m} H_1(x,z) = \alpha_1(x,z) + \beta_1(x,z)\varphi + \gamma_1(x,z)\varphi^2 \tag{5}$$

where $\alpha_1, \beta_1, \gamma_1 \in K[x,z]$. For each $v \in M_K$ we choose $x_v, z_v \in K_v$ with $g_1(x_v, z_v)$ a square in K_v and $\gamma_1(x_v, z_v) \neq 0$. If $g_2(1,0) \neq 0$ then the Cassels-Tate pairing on $S^{(2)}(E_{I,J}/K)$ is given by

$$\langle [g_1], [g_2] \rangle_{\mathrm{CT}} = \prod_{v \in M_K} (g_2(1,0), \gamma_1(x_v, z_v))_v \tag{6}$$

where $(\ ,\ )_v : K_v^\times/(K_v^\times)^2 \times K_v^\times/(K_v^\times)^2 \to \mu_2$ is the Hilbert norm residue symbol.

Remark 3.2. (i) If we wish to compute the pairing starting only with g_1 and g_2, then we first change coordinates so that $z(g_1)$ and $z(g_2)$ are units in L, multiply these together, and then compute g_3 by solving a conic over K. This conic is the same as the one that has to be solved in Donnelly's method [10].
(ii) We show in Remark 8.3 that the binary quadratic form γ_1 is not identically zero. Therefore, by our assumption that g_1 is everywhere locally soluble, it is always possible to choose $x_v, z_v \in K_v$ with the stated properties.
(iii) The assumption that $g_2(1,0) \neq 0$ is no limitation, since if $g_2(1,0) = 0$ then $[g_2] = 0$ in the 2-Selmer group, which certainly implies the pairing is trivial.
(iv) By definition the Cassels-Tate pairing takes values in $\mathbb{Q}/\mathbb{Z}$. In our formula it takes values in μ_2. It should be understood that we have identified $\mu_2 = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.
(v) Since $\langle\ ,\ \rangle_{\mathrm{CT}}$ is alternating and bilinear and $[g_1] + [g_2] + [g_3] = 0$ we have $\langle [g_1], [g_2] \rangle_{\mathrm{CT}} = \langle [g_1], [g_3] \rangle_{\mathrm{CT}}$. So we may equally write $g_2(1,0)$ or $g_3(1,0)$ in (6). Notice however that the binary quartics g_2 and g_3 do both contribute to the pairing via (5). Moreover we must use the exact formulae for $z(g_1)$, $z(g_2)$ and $z(g_3)$, these being linear in φ. It is not enough just to know these quantities up to squares, since this would change the left hand side of (5).
(vi) If $E(K)[2] = 0$ then m is uniquely determined up to sign. By the product formula for the Hilbert norm residue symbol this makes no difference to (6). If $E(K)[2] \neq 0$ then there are more choices for m, but it turns out (see the proof of Theorem 8.2) that we may use any one of these to compute the pairing.

Remark 3.3. The product over all places in Theorem 3.1 is a finite product. Indeed, outside an easily determined finite set of places, we have

(i) v is a finite prime, with residue field of size at least 11.
(ii) g_1 and γ_1 have v-adically integral coefficients, with $v \nmid \Delta(g_1)\,\mathrm{content}(\gamma_1)$.
(iii) $g_2(1,0)$ is a v-adic unit and $v \nmid 2$.

Under conditions (i) and (ii) we can pick our local point (by Hensel lifting a smooth point on the reduction that is not a root of γ_1) such that $\gamma_1(x_v, z_v)$ is a unit. It follows by (iii) that the local contribution at v is trivial.

Example 3.4. Let $E/\mathbb{Q}$ be the elliptic curve

$$y^2 + y = x^3 - x^2 - 929x - 10595$$

labelled $571a1$ in [7]. A 2-descent shows that $S^{(2)}(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, and its non-zero elements are represented by

$$\begin{aligned} g_1(x,z) &= -11x^4 + 68x^3z - 52x^2z^2 - 164xz^3 - 64z^4, \\ g_2(x,z) &= -4x^4 - 60x^3z - 232x^2z^2 - 52xz^3 - 3z^4, \\ g_3(x,z) &= -31x^4 - 78x^3z + 32x^2z^2 + 102xz^3 - 53z^4. \end{aligned}$$

Each of these binary quartics has invariants $I = 44608$ and $J = 18842960$, and discriminant $\Delta = -2^{12} \cdot 571$. By (5), with $m = \frac{1}{9}(20\varphi^2 - 8656\varphi + 936032)$, we get

$$\gamma_1(x, z) = \frac{4}{9}(5x^2 - 16xz - 12z^2).$$

For each odd prime p there is a smooth $\mathbb{F}_p$-point on the reduction of $y^2 = g_1(x, 1)$ mod p, whose x-coordinate is not a root of $5x^2 - 16x - 12 = 0$. Indeed we checked this claim directly for $p = 3, 5, 7, 11$ and 571, and for all other primes it follows by Hasse's bound. Therefore the odd primes make no contribution to (6).

To compute the contribution at $p = 2$ we write $g_1(x, 1) = x^4 + 4q(x)$ where

$$q(x) = -3x^4 + 17x^3 - 13x^2 - 41x - 16.$$

By Hensel's lemma the equation $q(x) = 0$ has a root in $\mathbb{Z}_2$ with $x = 2^4 + O(2^5)$. But then $\gamma_1(x, 1) \equiv 5 \mod (\mathbb{Q}_2^\times)^2$, and since $(5, -1)_2 = 1$ the contribution is again trivial. Finally, since $g_1(15, 4) > 0$ and $\gamma_1(15, 4) < 0$, there is a contribution from the real place. This shows that the Cassels-Tate pairing on $S^{(2)}(E/\mathbb{Q})$ is non-trivial, and hence $\operatorname{rank} E(\mathbb{Q}) = 0$.

4. The Cassels-Tate pairing

There are two standard definitions of the Cassels-Tate pairing (in the case of elliptic curves) called in [11], [16] the *homogeneous space definition* and the *Weil pairing definition*. Both definitions appear in Cassels' original paper [4], although the method in [6] (see also [12]) is a variant of the Weil pairing definition. In this section we review the homogeneous space definition, and highlight its connection with the Brauer-Manin obstruction.

Let K be a field with separable closure $\overline{K}$. We write $H^i(K, -)$ for the Galois cohomology group $H^i(\mathrm{Gal}(\overline{K}/K), -)$. Let C/K be a smooth projective curve. We define

$$\mathrm{Br}(C) = \ker \left(H^2(K, \overline{K}(C)^\times) \to H^2(K, \mathrm{Div}\, C) \right). \tag{7}$$

It is shown in the Appendix to [14] that this is equivalent to the usual definition $\mathrm{Br}(C) = H^2_{\text{ét}}(C, \mathbb{G}_m)$. Identifying $\mathrm{Br}(K) = H^2(K, \overline{K}^\times)$, there is a natural map

$$\mathrm{Br}(K) \to \mathrm{Br}(C). \tag{8}$$

We will need the following two facts, whose proofs we give below.

(i) For $P \in C(K)$ there is an evaluation map

$$\mathrm{Br}(C) \to \mathrm{Br}(K)\,; \ A \mapsto A(P).$$

This is a group homomorphism, and a section to the map (8). Moreover the evaluation maps behave functorially with respect to all field extensions.

(ii) Suppose C is a smooth curve of genus one, with Jacobian elliptic curve E. If $H^3(K, \overline{K}^\times) = 0$ then there is an isomorphism

$$\Psi_C : \frac{H^1(K,E)}{\langle [C] \rangle} \xrightarrow{\sim} \frac{\mathrm{Br}(C)}{\mathrm{Br}(K)}. \tag{9}$$

Now let E be an elliptic curve over a number field K. Let C and D be principal homogeneous spaces under E. Since $H^3(K, \overline{K}^\times) = 0$ for K a number field, we have $\Psi_C([D]) = A \mod \mathrm{Br}(K)$ for some $A \in \mathrm{Br}(C)$. Now suppose that C and D are everywhere locally soluble. For each place $v \in M_K$ we pick a local point $P_v \in C(K_v)$. The Cassels-Tate pairing $Ш(E/K) \times Ш(E/K) \to \mathbb{Q}/\mathbb{Z}$ is defined by

$$\langle [C], [D] \rangle_{\mathrm{CT}} = \sum_{v \in M_K} \mathrm{inv}_v(A(P_v)) \tag{10}$$

where $\mathrm{inv}_v : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ is the local invariant map. As this form of the definition makes clear, if $\langle [C], [D] \rangle_{\mathrm{CT}} \neq 0$ then the genus one curve C is a counter-example to the Hasse Principle explained by the Brauer-Manin obstruction.

We check that the pairing is well defined, i.e. it does not depend on the choices of A and of the P_v. By class field theory there is an exact sequence

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_{v \in M_K} \mathrm{Br}(K_v) \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

It follows that if we change A by adding an element of $\mathrm{Br}(K)$ then the pairing (10) is unchanged. Next, since the class of D is trivial in $H^1(K_v, E)$, the analogue of (9) over K_v shows that the restriction of A to the Brauer group of C/K_v is constant, i.e. it belongs to the image of $\mathrm{Br}(K_v)$. Therefore the pairing (10) does not depend on the choice of local points P_v.

We now prove the facts we quoted in (i) and (ii) above.

(i) For $P \in C(K)$ there is a short exact sequence of Galois modules

$$0 \longrightarrow \mathcal{O}_P^\times \longrightarrow \overline{K}(C)^\times \xrightarrow{\mathrm{ord}_P} \mathbb{Z} \longrightarrow 0$$

where $\mathcal{O}_P$ is the local ring at P. Taking Galois cohomology gives an exact sequence

$$0 \longrightarrow H^2(K, \mathcal{O}_P^\times) \longrightarrow H^2(K, \overline{K}(C)^\times) \xrightarrow{\mathrm{ord}_P} H^2(K, \mathbb{Z}).$$

It follows by (7) that each element of $\mathrm{Br}(C)$ can be represented by a cocycle taking values in $\mathcal{O}_P^\times$, and so can be evaluated at P.

(ii) There is an exact sequence of Galois modules

$$0 \to \overline{K}^\times \to \overline{K}(C)^\times \to \mathrm{Div}\, C \to \mathrm{Pic}\, C \to 0,$$

where $\mathrm{Div}\, C$ and $\mathrm{Pic}\, C$ are the divisor group and Picard group for C over $\overline{K}$. Splitting into short exact sequences, and taking Galois cohomology, gives the following exact sequences

$$\begin{tikzcd}
& & H^2(K,\overline{K}^\times) \arrow[d] & \\
& & H^2(K,\overline{K}(C)^\times) \arrow[d] & \\
H^1(K,\operatorname{Div} C) \arrow[r] & H^1(K,\operatorname{Pic} C) \arrow[r] & H^2(K,\overline{K}(C)^\times/\overline{K}^\times) \arrow[r] \arrow[d] & H^2(K,\operatorname{Div} C) \\
& & H^3(K,\overline{K}^\times) &
\end{tikzcd}$$

By Shapiro's lemma and the fact that $H^1(K,\mathbb{Z}) = 0$ we have $H^1(K,\operatorname{Div} C) = 0$. It follows by (7) and a diagram chase that there is an exact sequence

$$\operatorname{Br}(K) \to \operatorname{Br}(C) \to H^1(K,\operatorname{Pic} C) \to H^3(K,\overline{K}^\times). \tag{11}$$

In fact, had we started from the definition $\operatorname{Br}(C) = H^2_{\text{ét}}(C,\mathbb{G}_m)$, then (11) would follow from the Hochschild–Serre spectral sequence.

If C is a smooth curve of genus one with Jacobian E, then taking Galois cohomology of the exact sequence

$$0 \longrightarrow \operatorname{Pic}^0 C \longrightarrow \operatorname{Pic} C \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0$$

gives

$$\mathbb{Z} \xrightarrow{\delta} H^1(K,E) \longrightarrow H^1(K,\operatorname{Pic} C) \longrightarrow 0 \tag{12}$$

with $\delta(1) = [C]$. If $H^3(K,\overline{K}^\times) = 0$ then from (11) and (12) we obtain the isomorphism Ψ_C.

5. Cyclic extensions

The definition of the map Ψ_C in the last section simplifies when we evaluate it on classes split by a cyclic extension L/K. Let $G = \operatorname{Gal}(L/K)$ be generated by σ of order n. We recall that for A a G-module, the Tate cohomology groups are

$$\widehat{H}^0(G,A) = \frac{\ker(\Delta|A)}{\operatorname{im}(N|A)} \quad \text{and} \quad \widehat{H}^1(G,A) = \frac{\ker(N|A)}{\operatorname{im}(\Delta|A)}$$

where $\Delta = 1-\sigma$ and $N = 1+\sigma+\ldots+\sigma^{n-1}$ satisfy $\Delta N = N\Delta = 0$ in $\mathbb{Z}[G]$.

For $b \in K^\times$ there is a cyclic K-algebra with basis $1, v, \ldots, v^{n-1}$ as an L-vector space, and multiplication determined by $v^n = b$ and $vx = \sigma(x)v$ for all $x \in L$. We write $(L/K,b)$ for the class of this algebra in $\operatorname{Br}(K) = H^2(K,\overline{K}^\times)$. Likewise if $f \in K(C)^\times$ then $(L/K,f)$ is an element of $H^2(K,\overline{K}(C)^\times)$.

Lemma 5.1. *Suppose $\Xi \in \operatorname{Div}^0_L C$ with $N_{L/K}(\Xi) = \operatorname{div}(f)$ for some $f \in K(C)^\times$. If ξ is the image of Ξ under*

$$\widehat{H}^1(G, \operatorname{Pic}^0_L C) \cong H^1(G, \operatorname{Pic}^0_L C) \xrightarrow{\text{inf}} H^1(K, E)$$

then $\Psi_C(\xi) = (L/K, f)$.

Proof. We follow the construction of Ψ_C in Section 4. We start with the exact sequence of G-modules

$$0 \to L^\times \to L(C)^\times \to \operatorname{Div}_L C \to \operatorname{Pic}_L C \to 0.$$

Splitting into short exact sequences, and taking Galois cohomology, gives a diagram as before. The connecting map

$$\widehat{H}^1(G, \operatorname{Pic}_L C) \to \widehat{H}^0(G, L(C)^\times / L^\times)$$

is now given by $\Xi \mapsto f$. Therefore $\Psi_C(\xi)$ is the image of f under the map

$$\frac{K(C)^\times}{N_{L/K}(L(C)^\times)} = \widehat{H}^0(G, L(C)^\times) \cong H^2(G, L(C)^\times) \xrightarrow{\text{inf}} H^2(K, \overline{K}(C)^\times).$$

This is the cyclic algebra $(L/K, f)$ as required. □

6. Pairs of binary quartics and $(2,2)$-forms

Let C be a smooth curve of genus one. First suppose, as in Section 2, that C is defined by a binary quartic g. Then $C \to \mathbb{P}^1$ is a double cover ramified over the 4 roots of g. We write H for the hyperplane section (i.e., fibre of the map $C \to \mathbb{P}^1$), and ι for the involution on C with $Q + \iota(Q) \sim H$ for all $Q \in C$.

Next we suppose that $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ is defined by a $(2,2)$-form, i.e., a polynomial $f(x_1, z_1; x_2, z_2)$ that is homogeneous of degree 2 in each of the sets of variables x_1,z_1 and x_2,z_2. Projecting C to either factor gives a double cover of $\mathbb{P}^1$. The corresponding binary quartics are obtained by writing f as a binary quadratic form in one of the sets of variables, and taking its discriminant. We write $\operatorname{pr}_1, \operatorname{pr}_2 : C \to \mathbb{P}^1$ for the projection maps. Let H_1, H_2 and ι_1, ι_2 be the corresponding hyperplane sections and involutions.

Lemma 6.1. *Let $C = \{f(x_1, z_1; x_2, z_2) = 0\} \subset \mathbb{P}^1 \times \mathbb{P}^1$ as above.*

(i) *The composite $\iota_1 \iota_2$ is translation by some $P \in E = \operatorname{Jac}(C)$. Moreover the isomorphism $\operatorname{Pic}^0(C) \cong E$ sends $[H_1 - H_2] \mapsto P$.*

(ii) *If $H_i = \operatorname{pr}_i^*(1:0)$ then*

$$\operatorname{div}(f(x_1, z_1; 1, 0)/z_1^2) = H_2 + \iota_1^* H_2 - 2H_1.$$

Proof. (i) If $Q \in C$ then $\iota_2 Q + \iota_1\iota_2 Q \sim H_1$ and $Q + \iota_2 Q \sim H_2$. Subtracting one from the other gives $[\iota_1\iota_2 Q - Q] = [H_1 - H_2]$ as required.
(ii) The specified rational function on C factors via pr_1 and is therefore invariant under pull back by ι_1. It has a zero at each point in the support of H_2, and a double pole at each point in the support of H_1. Since there are no other poles, and the divisor has degree 0, it must therefore be as stated. □

Remark 6.2. Lemma 6.1(i) is closely related to Poncelet's Porism, as described in [13]. Our use of $(2,2)$-forms was inspired by the treatment in [1].

We write $\mathrm{disc}_k(f)$ for the discriminant of f when it is viewed as a binary quadratic form in the kth set of variables.

Lemma 6.3. *Let $C = \{f(x_1, z_1; x_2, z_2) = 0\} \subset \mathbb{P}^1 \times \mathbb{P}^1$ as above. Let $a \in K^\times$ and let C_1, C_2 be the following quadratic twists of C.*

$$\begin{aligned} C_1 : \qquad & ay^2 = \mathrm{disc}_2(f) \\ C_2 : \qquad & ay^2 = \mathrm{disc}_1(f) \end{aligned}$$

Then $\Psi_{C_1}([C_2]) = (K(\sqrt{a})/K, f(x_1, z_1; 1, 0)/z_1^2)$.

Proof. If $a \in (K^\times)^2$ then C_1 and C_2 are isomorphic over K and so by (9) we have $\Psi_{C_1}([C_2]) = 0$. We may therefore suppose that $a \notin (K^\times)^2$. Let $L = K(\sqrt{a})$ and $G = \mathrm{Gal}(L/K) = \{1, \sigma\}$. We claim there is a divisor $\Xi \in \mathrm{Div}^0_L(C_1)$ such that

(i) C_2 is the twist of C_1 by the class of Ξ in $\widehat{H}^1(G, \mathrm{Pic}^0_L(C_1))$, and
(ii) $N_{L/K}(\Xi) = \mathrm{div}(f(x_1, z_1; 1, 0)/z_1^2)$.

Then by Lemma 5.1 we have $\Psi_{C_1}([C_2] - [C_1]) = (L/K, f(x_1, z_1; 1, 0)/z_1^2)$. Since Ψ_{C_1} is a group homomorphism and $\Psi_{C_1}([C_1]) = 0$ this proves the lemma.

We construct Ξ as follows. We factor the projection map $\mathrm{pr}_i : C \to \mathbb{P}^1$ as

$$C \xrightarrow{\phi_i} C_i \xrightarrow{\xi_i} \mathbb{P}^1$$

where ϕ_i is the quadratic twist map (an isomorphism defined over L), and $\xi_i = (x_i : z_i)$ is the natural double cover. Let $D_i = \xi_i^*(1:0)$ and $H_i = \phi_i^* D_i = \mathrm{pr}_i^*(1:0)$. We put $\phi = \phi_1\phi_2^{-1}$ and $\Xi = \phi_* D_2 - D_1$. We now prove (i) and (ii).

(i) Let ι_1 and ι_2 be the involutions on C defined before Lemma 6.1. Since $\sigma(\phi_1) = \phi_1\iota_1$ and $\sigma(\phi_2) = \phi_2\iota_2$ it follows that $\sigma(\phi)\phi^{-1} = \phi_1\iota_1\iota_2\phi_1^{-1}$. Identifying C and C_1 via ϕ_1, and hence Ξ with $H_2 - H_1$, it follows by Lemma 6.1 that $\sigma(\phi)\phi^{-1}$ is translation by some $P \in E = \mathrm{Jac}(C_1)$, and the isomorphism $\mathrm{Pic}^0(C_1) \cong E$ sends $[\Xi] \mapsto -P$. The minus sign does not matter since $|G| = 2$.

(ii) By Lemma 6.1(ii) with $H_1 = \phi_1^* D_1$ and $H_2 = \phi_2^* D_2$ we have

$$\begin{aligned}\operatorname{div}(f(x_1, z_1; 1, 0)/z_1^2) &= \phi_{1*}(\phi_2^* D_2 + \iota_1^* \phi_2^* D_2 - 2\phi_1^* D_1) \\ &= \phi_* D_2 + \sigma(\phi_* D_2) - 2D_1 \\ &= N_{L/K}(\Xi).\end{aligned}$$

□

7. Triples of binary quartics and $(2,2,2)$-forms

Let E/K be an elliptic curve. An n-covering of E is a pair (C, ν) where C is a smooth curve of genus one, and $\nu : C \to E$ is a morphism, such that, for some choice of isomorphism $\psi : C \to E$ defined over $\overline{K}$, there is a commutative diagram

$$\begin{tikzcd} C \arrow[d, "\psi"'] \arrow[dr, "\nu"] & \\ E \arrow[r, "\times n"'] & E \end{tikzcd}$$

The n-coverings of E are parametrised by $H^1(K, E[n])$.

Suppose that C_1, C_2, C_3 are 2-coverings of E that sum to zero in $H^1(K, E[2])$. We pick isomorphisms $\psi_i : C_i \to E$ as above, and let $\varepsilon_i = (\sigma \mapsto \sigma(\psi_i)\psi_i^{-1})$ be the corresponding cocycle in $Z^1(\mathrm{Gal}(\overline{K}/K), E[2])$. Our hypothesis is that $\varepsilon_1 + \varepsilon_2 + \varepsilon_3$ is a coboundary. However, by adjusting the choice of ψ_3, we may suppose that $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 = 0$. It may then be checked that the morphism

$$\begin{aligned}\mu : C_1 \times C_2 \times C_3 &\to E \\ (P_1, P_2, P_3) &\mapsto \psi_1(P_1) + \psi_2(P_2) + \psi_3(P_3)\end{aligned}$$

is defined over K.

Remark 7.1. We are still free to replace ψ_3 by $P \mapsto \psi_3(P) + T$ for $T \in E(K)[2]$, and for this reason there are $\#E(K)[2]$ choices for the map μ.

Suppose further that C_1, C_2, C_3 are defined by binary quartics g_1, g_2, g_3 with the same invariants I and J. Let $\pi : C_1 \times C_2 \times C_3 \to \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ be the map that projects to the x-coordinates. Then $S = \pi(\mu^{-1}(0_E))$ is a surface in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$. Geometrically it is the Kummer surface $(E \times E)/\{\pm 1\}$.

We write $\operatorname{disc}_k(F)$ for the discriminant of a $(2,2,2)$ form F when it is viewed as a binary quadratic form in the kth set of variables.

Proposition 7.2. *The surface $S \subset \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ is defined by a $(2,2,2)$-form F. Moreover we may scale F so that it has coefficients in K, and for all permutations i, j, k of $1, 2, 3$ we have $\operatorname{disc}_k(F) = g_i g_j$.*

Proof. We first consider the special case where $C_1 = C_2 = C_3 = E$. Suppose that $P_1, P_2, P_3 \in E$ satisfy $P_1 + P_2 + P_3 = 0_E$. If we specify the x-coordinates of P_1 and

P_2, then in general this leaves two possibilities for the x-coordinate of P_3. The exceptional cases are when either P_1 or P_2 is a 2-torsion point.

Let $\Delta_i = \psi_i^{-1}(E[2])$ be the set of ramification points for $C_i \to \mathbb{P}^1$. We identify Δ_i with its image in $\mathbb{P}^1$, i.e., the set of roots of g_i. The observations in the last paragraph show that when we project onto the ith and jth factors, $S \to \mathbb{P}^1 \times \mathbb{P}^1$ is a double cover ramified over $\Delta_i \times \mathbb{P}^1$ and $\mathbb{P}^1 \times \Delta_j$. This shows that S is defined by a $(2,2,2)$-form F. Moreover $\mathrm{disc}_k(F) = \lambda_k g_i g_j$ for some $\lambda_1, \lambda_2, \lambda_3 \in K^\times$. We claim that (i) $\lambda_3 \in (K^\times)^2$ and (ii) $\lambda_1 = \lambda_2 = \lambda_3$. It is then clear we may rescale F so that $\lambda_1 = \lambda_2 = \lambda_3 = 1$.

(i) Let C_i have equation $y_i^2 = g_i(x_i, z_i)$. We note that $K(S) \subset K(C_1 \times C_2)$ is a quadratic extension of $K(\mathbb{P}^1 \times \mathbb{P}^1)$ with Kummer generator

$$\frac{\mathrm{disc}_3(F)}{z_1^4 z_2^4} = \frac{\lambda_3 g_1(x_1, z_1) g_2(x_2, z_2)}{z_1^4 z_2^4} = \lambda_3 \left(\frac{y_1 y_2}{z_1^2 z_2^2} \right)^2 .$$

Since this is a square in $K(C_1 \times C_2)$ it follows that $\lambda_3 \in (K^\times)^2$.

(ii) Since g_1, g_2, g_3 have the same invariants I and J, we may reduce by the action of $\mathrm{SL}_2(\overline{K}) \times \mathrm{SL}_2(\overline{K}) \times \mathrm{SL}_2(\overline{K})$ to the case

$$g_1(x,z) = g_2(x,z) = g_3(x,z) = x^3 z - \tfrac{1}{3} I x z^3 - \tfrac{1}{27} J z^4.$$

The result then follows by symmetry. $\square$

Corollary 7.3. *Let C_1, C_2, C_3 and F be as above. If $a = g_3(1,0) \neq 0$ then*

$$\Psi_{C_1}([C_2]) = (K(\sqrt{a})/K, F(x_1, z_1; 1, 0; 1, 0)/z_1^2).$$

Proof. We put $f(x_1, z_1; x_2, z_2) = F(x_1, z_1; x_2, z_2; 1, 0)$. By Proposition 7.2 we have $\mathrm{disc}_1(f) = a g_2(x_2, z_2)$ and $\mathrm{disc}_2(f) = a g_1(x_1, z_1)$. The curves C_1 and C_2 are therefore isomorphic to those considered in Lemma 6.3. Applying Lemma 6.3 gives the result. $\square$

8. Computing the $(2,2,2)$-forms

To complete the proof of Theorem 3.1 we must explain how to compute the $(2,2,2)$-form F. As before it is helpful to first consider the special case where $C_1 = C_2 = C_3 = E$.

Let E be the elliptic curve $y^2 = x^3 + ax + b$. We consider the maps

$$\begin{array}{ccc} E \times E \times E & \xrightarrow{\mu} & E \\ \Big\downarrow{\scriptstyle \pi} & & \\ \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 & & \end{array}$$

where $\mu(P_1, P_2, P_3) = P_1 + P_2 + P_3$ and π is the map taking the x-coordinate of each point. An equation for $S = \pi(\mu^{-1}(0_E))$ is computed as follows.

Let $P_i = (x_i, y_i)$ for $i = 1, 2, 3$ be points on E with $P_1 + P_2 + P_3 = 0_E$. These points lie on a line, say $y = \lambda x + \nu$. Then as polynomials in x we have

$$x^3 + ax + b - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3).$$

Comparing the coefficients of the powers of x we obtain

$$\begin{aligned} \lambda^2 &= s_1, \\ 2\lambda\nu &= a - s_2, \\ \nu^2 &= b + s_3, \end{aligned}$$

where s_1, s_2, s_3 are the elementary symmetric polynomials in x_1, x_2, x_3. Eliminating λ and ν gives the equation

$$(a - s_2)^2 - 4s_1(b + s_3) = 0.$$

The required $(2, 2, 2)$-form F is obtained by homogenising this equation, i.e. we replace x_i by x_i/z_i and multiply through by $z_1^2 z_2^2 z_3^2$.

Remark 8.1. We have $F(x_1, 1; x_2, 1; x_3, 1) = W_0 x_3^2 - W_1 x_3 + W_2$ where

$$\begin{aligned} W_0 &= (x_1 - x_2)^2, \\ W_1 &= 2(x_1 x_2 + a)(x_1 + x_2) + 4b, \\ W_2 &= x_1^2 x_2^2 - 2a x_1 x_2 - 4b(x_1 + x_2) + a^2. \end{aligned}$$

These are the formulae used in [5, Chapter 17] to show that the height on an elliptic curve is a quadratic form.

We now turn to the general case. So let $S \subset \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ be as in Section 7. Let $z(g_i)$ be the cubic invariant, and write H_1, H_2, H_3 for the binary quadratic forms (4) over $L = K[\varphi]$ associated to g_1, g_2, g_3.

Theorem 8.2. *If $z(g_1)z(g_2)z(g_3) = m^2$ for some $m \in L^\times$, and*

$$\frac{H_1 H_2 H_3}{m} = F_0 + F_1\varphi + F_2\varphi^2 \tag{13}$$

where F_0, F_1, F_2 are $(2, 2, 2)$-forms defined over K, then S has equation $F_2 = 0$.

Proof. Let $P_i = (x_i : y_i : z_i) \in C_i$ for $i = 1, 2, 3$, with $\mu(P_1, P_2, P_3) = 0_E$. Let Q_i be the image of P_i under the covering map $C_i \to E$. By the formulae for the covering map coming from classical invariant theory (see for example [8, Proposition 4.2]), the x-coordinate of Q_i is

$$\xi_i = \frac{3h_i(x_i, z_i)}{4g_i(x_i, z_i)}. \tag{14}$$

We recall from Section 3 that

$$z(g_i)\frac{4\varphi g_i + h_i}{3} = H_i^2. \tag{15}$$

By (14), (15) and the equation $y_i^2 = g_i(x_i, z_i)$ for C_i we have

$$\xi_i + 3\varphi = \frac{9H_i^2}{4z(g_i)y_i^2}$$

and hence

$$\prod_{i=1}^{3}(\xi_i + 3\varphi) = \left(\frac{27H_1H_2H_3}{8my_1y_2y_3}\right)^2. \tag{16}$$

Since $Q_1 + Q_2 + Q_3 = 0_E$ these points lie on a line, say $y = \lambda x + \nu$ for some $\lambda, \nu \in K$. Then as a polynomial in x we have

$$x^3 - 27Ix - 27J - (\lambda x + \nu)^2 = (x - \xi_1)(x - \xi_2)(x - \xi_3).$$

Putting $x = -3\varphi$ gives

$$\prod_{i=1}^{3}(\xi_i + 3\varphi) = (\nu - 3\lambda\varphi)^2. \tag{17}$$

We first suppose $E(K)[2] = 0$. In this case L is a field, so comparing (16) and (17) we have

$$\frac{27H_1H_2H_3}{8my_1y_2y_3} = \pm(\nu - 3\lambda\varphi),$$

in $L(S)$. Taking the coefficient of φ^2 we see that F_2 vanishes on S. In general there are $\#E(K)[2]$ choices for the square root, up to sign, and these correspond to the $\#E(K)[2]$ choices in Remark 7.1.

It remains to check that F_2 is not identically zero. For this we may work over an algebraically closed field. Then by a change of coordinates we may suppose that g_i and h_i are linear combinations of $x_i^4 + z_i^4$ and $x_i^2z_i^2$. The singular quartics in this pencil are $(x_i^2 - z_i^2)^2$, $(x_i^2 + z_i^2)^2$ and $(x_iz_i)^2$. Since $L \cong K \times K \times K$ we may identify H_i as a triple of binary quadratic forms. These are non-zero multiples of $x_i^2 - z_i^2$, $x_i^2 + z_i^2$ and x_iz_i, in this order if we made a suitable change of coordinates. (This last claim may be checked without any calculation if we use stereographic projection to identify the roots of the binary quadratic forms with the vertices of an octahedron, and then rotate the octahedron.) Therefore the space of $(2,2,2)$-forms spanned by F_0, F_1, F_2 contains the forms

$$(x_1^2 - z_1^2)(x_2^2 - z_2^2)(x_3^2 - z_3^2), \quad (x_1^2 + z_1^2)(x_2^2 + z_2^2)(x_3^2 + z_3^2), \quad x_1z_1x_2z_2x_3z_3.$$

Since these are linearly independent, it follows that F_2 is non-zero. $\square$

Proof of Theorem 3.1. Let $F = F_2$ be the equation for S in Theorem 8.2. We specialise the last two sets of variables in (13) to $(1, 0)$. Then comparing with (5) we have $F(x, z; 1, 0; 1, 0) = \gamma_1(x, z)$. By Corollary 7.3 we have

$$\Psi_{C_1}([C_2]) = (K(\sqrt{a})/K, \gamma_1(x, z)/z^2),$$

where $a = g_3(1, 0)$. Then by (10) we have

$$\langle [C_1], [C_2] \rangle_{\mathrm{CT}} = \sum_{v \in M_K} \mathrm{inv}_v(K_v(\sqrt{a})/K_v, \gamma_1(x_v, z_v)/z_v^2).$$

Subject to identifying $\mu_2 = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, the Hilbert norm residue symbol is given by

$$(a, b)_v = \mathrm{inv}_v(K_v(\sqrt{a})/K_v, b).$$

This gives the formula in Theorem 3.1, except that we have $g_3(1, 0)$ in place of $g_2(1, 0)$. As noted in Remark 3.2(v), this change does not matter. $\square$

Remark 8.3. To show that $\gamma_1(x, z)$ is not identically zero we show more generally that F cannot be made to vanish by specialising two of the sets of variables. Indeed, by considering F as given in Remark 8.1, it suffices to show that the polynomials W_0, W_1, W_2 never simultaneously vanish. This may be checked by setting $x_1 = x_2 = x$ and computing that the resultant of W_1 and W_2 is $2^8(4a^3 + 27b^2)^2$. This last expression is non-zero, by definition of an elliptic curve.

References

[1] M. Bhargava and W. Ho, Coregular spaces and genus one curves, *Camb. J. Math.* **4** (2016), no. 1, 1–119.

[2] B.J. Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves, I. *J. reine angew. Math.* **212** (1963) 7–25.

[3] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system, I. The user language, *J. Symbolic Comput.*, **24** (1997), 235–265.

[4] J.W.S. Cassels, Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung, *J. reine angew. Math.* **211** (1962) 95–112.

[5] J.W.S. Cassels, *Lectures on elliptic curves*, LMS Student Texts, **24**, Cambridge University Press, Cambridge, 1991.

[6] J.W.S. Cassels, Second descents for elliptic curves, *J. reine angew. Math.* **494** (1998), 101–127.

[7] J.E. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge University Press, Cambridge, 1997.

[8] J.E. Cremona, Classical invariants and 2-descent on elliptic curves, *J. Symbolic Comput.* **31** (2001), no. 1-2, 71–87.

[9] J.E. Cremona and T.A. Fisher, On the equivalence of binary quartics, *J. Symbolic Comput.* **44** (2009), no. 6, 673–682.

[10] S. Donnelly, *Algorithms for the Cassels-Tate pairing*, preprint, 2015.

[11] T.A. Fisher, The Cassels-Tate pairing and the Platonic solids, *J. Number Theory* **98** (2003), no. 1, 105–155.

[12] T.A. Fisher, E.F. Schaefer and M. Stoll, The yoga of the Cassels-Tate pairing, *LMS J. Comput. Math.* **13** (2010), 451–460.

[13] P. Griffiths and J. Harris, On Cayley's explicit solution to Poncelet's porism, *Enseign. Math.* (2) **24** (1978), no. 1-2, 31–40.

[14] S. Lichtenbaum, Duality theorems for curves over p-adic fields. *Invent. Math.* **7** (1969) 120–136.

[15] The PARI Group, PARI/GP version `2.13`, Univ. Bordeaux, 2022, `http://pari.math.u-bordeaux.fr/`

[16] B. Poonen and M. Stoll, The Cassels-Tate pairing on polarized abelian varieties, *Ann. of Math.* (2) **150** (1999), no. 3, 1109–1149.

[17] A. Weil, Remarques sur un mémoire d'Hermite, *Arch. Math. (Basel)* **5**, (1954) 197–202.

[18] J. Yan, *Computing the Cassels-Tate pairing for Jacobian varieties of genus two curves*, PhD thesis, University of Cambridge, 2021, `https://doi.org/10.17863/CAM.72729`

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK

Email address: `T.A.Fisher@dpmms.cam.ac.uk`