LMS J. Comput. Math. 13 (2010) 451–460 © 2010 Authors
doi:10.1112/S1461157010000185

The yoga of the Cassels–Tate pairing

Tom Fisher, Edward F. Schaefer and Michael Stoll

Abstract

Cassels has described a pairing on the 2-Selmer group of an elliptic curve which shares some properties with the Cassels–Tate pairing. In this article, we prove that the two pairings are the same.

1. *Introduction*

Let E be an elliptic curve defined over a number field K, and let $S^2(K, E)$ denote its 2-Selmer group (see Section 2 for a definition). In [**3**], Cassels defined a pairing on $S^2(K, E)$. It shares some properties with the extension of the Cassels–Tate pairing to $S^2(K, E)$. He wrote 'It seems highly probable that the two definitions are always equivalent, but the present writer is no longer an adept of the relevant yoga.' (see [**3**, p. 115]). In this article, we prove that the two pairings are the same.

The Cassels–Tate pairing is an alternating and bilinear pairing on the Shafarevich–Tate group Ш(K, E) of E. The fact that it is alternating gives information on the structure of the Shafarevich–Tate group. For an integer $n \geqslant 2$, its extension from the n-torsion of Ш(K, E) to the n-Selmer group $S^n(K, E)$ can be used to determine the image of the n^2-Selmer group in the n-Selmer group. This information can be helpful in determining which elements of the n-Selmer group come from K-rational points on E and which give rise to non-trivial elements of the Shafarevich–Tate group. The usual cohomological definitions of the Cassels–Tate pairing make it difficult to evaluate the pairing in practice. The pairing defined by Cassels on the 2-Selmer group, however, uses more concrete objects like elements of field extensions of K and functions on a curve, and it is quite straightforward to evaluate. Therefore, it is useful to prove that the two pairings are equal.

We first set some notation and recall the definition of the Selmer and Shafarevich–Tate groups in Section 2. Then, in Section 3, we give the 'Weil-pairing definition' and a new definition of the Cassels–Tate pairing extended to the n-Selmer group, under a hypothesis that is always satisfied for n a prime. In Section 4 we present the definition of the pairing defined by Cassels on 2-Selmer groups and mention a generalisation of Cassels' definition due to Swinnerton-Dyer [**14**] that gives a pairing between $S^n(K, E)$ and $S^2(K, E)$ for arbitrary n. In Section 5 we present a large diagram and prove that it is commutative. We use this diagram in Section 6 to prove our main theorem that the pairing defined by Cassels is the same as the Cassels–Tate pairing. We also discuss why Cassels' definition does not easily generalise to n-Selmer groups for $n > 2$.

2. *Notation*

In this section, we set some (fairly standard) notation and recall the definition of the Selmer and Shafarevich–Tate groups.

Let K be a field with separable closure $\overline{K}$. We denote by $\mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K. If M is a $\mathrm{Gal}(\overline{K}/K)$-module, then the group $Z^i(\mathrm{Gal}(\overline{K}/K), M)$ of continuous i-cocycles

Received 26 May 2010.

2000 Mathematics Subject Classification 11G05 (primary), 11G07 (secondary).

https://doi.org/10.1112/S1461157010000185 Published online by Cambridge University Press

on $\mathrm{Gal}(\overline{K}/K)$ with values in M will be denoted by $Z^i(K, M)$. The Galois cohomology group $H^i(\mathrm{Gal}(\overline{K}/K), M)$ will likewise be denoted by $H^i(K, M)$. The class in $H^i(K, M)$ of a cocycle $\xi \in Z^i(K, M)$ is denoted by $[\xi]$. We write M_K for the set of all places of the number field K. For $v \in M_K$ we fix an embedding of $\overline{K}$ in $\overline{K}_v$. The restriction maps $Z^i(K, M) \to Z^i(K_v, M)$ and $H^i(K, M) \to H^i(K_v, M)$ will be denoted by res_v.

If E is an elliptic curve defined over K and $n \geqslant 2$ is an integer, we denote by $[n]$ the multiplication-by-n map on E and by $E[n]$ the n-torsion subgroup of E, considered as a $\mathrm{Gal}(\overline{K}/K)$-module. Similarly, μ_n denotes the nth roots of unity as a $\mathrm{Gal}(\overline{K}/K)$-module. Otherwise, $G[n]$ denotes the n-torsion subgroup of an abelian group G.

Now let K be a number field. The exact sequence of Galois modules

$$0 \to E[n] \to E(\overline{K}) \xrightarrow{[n]} E(\overline{K}) \to 0$$

induces a short exact sequence in cohomology:

$$0 \to \frac{E(K)}{nE(K)} \to H^1(K, E[n]) \to H^1(K, E(\overline{K}))[n] \to 0.$$

There are analogous sequences with K replaced by a completion K_v. The restriction maps induce a map

$$H^1(K, E(\overline{K})) \to \bigoplus_{v \in M_K} H^1(K_v, E(\overline{K}_v))$$

whose kernel is the *Shafarevich–Tate group* Ш(K, E) of E. The *n-Selmer group* of E, $S^n(K, E)$, is the preimage of Ш$(K, E)[n] \subset H^1(K, E(\overline{K}))[n]$ in $H^1(K, E[n])$. We then have the standard short exact sequence

$$0 \to \frac{E(K)}{nE(K)} \to S^n(K, E) \to \text{Ш}(K, E)[n] \to 0. \tag{2.1}$$

3. *Two definitions of the Cassels–Tate pairing*

Let E be an elliptic curve defined over K, a number field. The Cassels–Tate pairing is a pairing on Ш(K, E) taking values in $\mathbb{Q}/\mathbb{Z}$. We refer to [2] for the original definition. In the terminology of [6] this is the 'homogeneous space definition'.

Let $n, n' \geqslant 2$ be integers. We are interested in the restriction of this pairing to the n-torsion Ш$(K, E)[n]$, or more generally to Ш$(K, E)[n] \times$ Ш$(K, E)[n']$. By (2.1) the Cassels–Tate pairing extends to a pairing on Selmer groups

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} : S^n(K, E) \times S^{n'}(K, E) \to \mathbb{Q}/\mathbb{Z}. \tag{3.1}$$

By definition this pairing is trivial on the images of $E(K)/nE(K)$ in $S^n(K, E)$ and of $E(K)/n'E(K)$ in $S^{n'}(K, E)$.

We recall an alternative definition of the Cassels–Tate pairing, called in [6] the 'Weil-pairing definition'. For simplicity, we assume that the natural map

$$H^2(K, E[n']) \to \prod_{v \in M_K} H^2(K_v, E[n']) \tag{3.2}$$

is injective. This is known for n' a prime, see [2, Lemma 5.1]. (The injectivity does not hold for $E[n']$ replaced by an arbitrary finite Galois module. See [11, III.4.7] for a counter-example.) From Section 4 onwards we restrict to the case $n' = 2$, so our hypothesis will be automatically satisfied.

https://doi.org/10.1112/S1461157010000185 Published online by Cambridge University Press

Let $a \in S^n(K, E)$ and $a' \in S^{n'}(K, E)$. We apply Galois cohomology over K and its completions K_v to

$$\begin{tikzcd}
0 \arrow[r] & E[n'] \arrow[r] \arrow[d, equal] & E[nn'] \arrow[r, "{[n']}"] \arrow[d] & E[n] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E[n'] \arrow[r] & E \arrow[r, "{[n']}"] & E \arrow[r] & 0
\end{tikzcd}$$

to obtain the following commutative diagram.

$$\begin{tikzcd}
H^1(K, E[nn']) \arrow[r, "{[n']_*}"] & H^1(K, E[n]) \arrow[r] \arrow[d] & H^2(K, E[n']) \arrow[d] \\
 & \prod_{v \in M_K} H^1(K_v, E(\overline{K}_v)) \arrow[r] & \prod_{v \in M_K} H^2(K_v, E[n'])
\end{tikzcd}$$

By the hypothesis that (3.2) is injective, there exists $b \in H^1(K, E[nn'])$ with $[n']_* b = a$. We represent b by a cocycle $\beta \in Z^1(K, E[nn'])$; then $\alpha := n'\beta \in Z^1(K, E[n])$ represents a. For each place v of K, the cocycle $\mathrm{res}_v(\alpha)$ in $Z^1(K_v, E(\overline{K}_v))$ is a coboundary. So there exists $P_v \in E(\overline{K}_v)$ such that $\mathrm{res}_v(\alpha) = dP_v$, where we write d for the coboundary map, that is dP_v is the cocycle $\sigma \mapsto {}^\sigma P_v - P_v$. Take $Q_v \in E(\overline{K}_v)$ such that $n'Q_v = P_v$. Then $dQ_v - \mathrm{res}_v(\beta) \in Z^1(K_v, E[n'])$.

The Weil pairing $e_{n'} : E[n'] \times E[n'] \to \mu_{n'}$ induces a cup product pairing

$$\cup_e : H^1(K_v, E[n']) \times H^1(K_v, E[n']) \to H^2(K_v, \mu_{n'}).$$

We define, for $x, y \in H^1(K_v, E[n'])$,

$$\langle x, y \rangle_{e,v} = \mathrm{inv}_v(x \cup_e y) \tag{3.3}$$

where $\mathrm{inv}_v : H^2(K_v, \mu_{n'}) \to \mathbb{Q}/\mathbb{Z}$ is the invariant map. Then there exists a pairing $\langle \cdot, \cdot \rangle_1 : S^n(K, E) \times S^{n'}(K, E) \to \mathbb{Q}/\mathbb{Z}$ given by

$$\langle a, a' \rangle_1 = \sum_{v \in M_K} \langle [dQ_v - \mathrm{res}_v(\beta)], \mathrm{res}_v(a') \rangle_{e,v}. \tag{3.4}$$

Proposition 3.5. *Let $a \in S^n(K, E)$ and $a' \in S^{n'}(K, E)$. We have $\langle a, a' \rangle_1 = \langle a, a' \rangle_{\mathrm{CT}}$. In particular, $\langle a, a' \rangle_1$ does not depend on the choices made in the definition.*

Proof. See [**2**, Proof of Lemma 4.1] or [**4**, §2.2]. □

Remark 3.6. The general form of the Weil-pairing definition, avoiding the hypothesis that (3.2) is injective, is given in [**5**, p. 97]. This variant is used in [**6**] to generalise Proposition 3.5 to abelian varieties.

The definition (3.4) given above is not very practical if one wants to evaluate the pairing on two given Selmer group elements. In order to get closer to a more workable definition, we make use of the interpretation of the elements of $S^n(K, E)$ as (isomorphism classes) of n-coverings of E that have points everywhere locally. We want to replace the multiplication-by-n' map relating P_v and Q_v in the definition above by a suitable covering. For this, we have to generalise the notion of n-covering to torsors under E.

Let C and D be torsors (that is, principal homogeneous spaces) under E. A morphism $\pi : D \to C$ is called an *n-covering* if $\pi(P + \mathfrak{Q}) = nP + \pi(\mathfrak{Q})$ for all $P \in E$ and $\mathfrak{Q} \in D$. If $C = E$ is the trivial torsor, this coincides with the usual notion of n-covering of E. For $\mathfrak{Q}_1, \mathfrak{Q}_2 \in D$

https://doi.org/10.1112/S1461157010000185 Published online by Cambridge University Press

we write $\mathfrak{Q}_1 - \mathfrak{Q}_2$ for the point P on E such that $P + \mathfrak{Q}_2 = \mathfrak{Q}_1$ where $+$ denotes the action of E on D.

In the case $C = E$, there is a standard bijection between the n-coverings of E up to K-isomorphism, and the Galois cohomology group $H^1(K, E[n])$. It is defined as follows. Let $\psi : D \to E$ be an isomorphism of curves over $\overline{K}$ with $[n] \circ \psi = \pi$. Then ${}^\sigma\psi \circ \psi^{-1}$ is translation by some $\xi_\sigma \in E[n]$ and we identify the K-isomorphism class of D with the class of $\sigma \mapsto \xi_\sigma$ in $H^1(K, E[n])$. If $\mathfrak{D}_0 \in D(\overline{K})$ with $\pi(\mathfrak{D}_0) = 0$ then we can take $\psi : \mathfrak{Q} \mapsto \mathfrak{Q} - \mathfrak{D}_0$, in which case D is represented by $-d\mathfrak{D}_0$.

Note also that if $C \to E$ is an n-covering of E and $D \to C$ is an n'-covering of C, then the composition $D \to E$ is an nn'-covering of E. If $D \to E$ corresponds to $c \in H^1(K, E[nn'])$, then $C \to E$ corresponds to $[n']_* c \in H^1(K, E[n])$.

We give a new definition of the Cassels–Tate pairing, again under the hypothesis that (3.2) is injective. Let C be an n-covering of E over K representing $a \in S^n(K, E)$. By the hypothesis, there exists $b \in H^1(K, E[nn'])$ with $[n']_* b = a$. Twisting $E \xrightarrow{[n']} E \xrightarrow{[n]} E$ by these cohomology classes gives $D \xrightarrow{\pi} C \to E$ where $\pi : D \to C$ is an n'-covering defined over K. Following [13, Chapter 6] we define a map

$$\delta_\pi : C(K) \to H^1(K, E[n']); \quad \mathfrak{P} \mapsto d\mathfrak{Q} := [\sigma \mapsto {}^\sigma\mathfrak{Q} - \mathfrak{Q}] \tag{3.7}$$

where $\mathfrak{Q} \in D(\overline{K})$ with $\pi(\mathfrak{Q}) = \mathfrak{P}$. Let v be a place of K. The analogue of this map with K replaced by K_v will be denoted by $\delta_{\pi,v}$. Since the image of a in $H^1(K_v, E(\overline{K}_v))$ is trivial, there exists a point $\mathfrak{P}_v \in C(K_v)$. We can now define $\langle \cdot, \cdot \rangle_2 : S^n(K, E) \times S^{n'}(K, E) \to \mathbb{Q}/\mathbb{Z}$ by

$$\langle a, a' \rangle_2 = \sum_{v \in M_K} \langle \delta_{\pi,v}(\mathfrak{P}_v), \mathrm{res}_v(a') \rangle_{e,v}. \tag{3.8}$$

The main advantage of this definition is that it uses the K_v-points $\mathfrak{P}_v$ on C rather than the $\overline{K}_v$-points P_v on E. We will see that Cassels' version will allow us to replace the cohomology classes by more concrete objects.

Proposition 3.9. *Let $a \in S^n(K, E)$ and $a' \in S^{n'}(K, E)$. We have $\langle a, a' \rangle_2 = \langle a, a' \rangle_1$. In particular, $\langle a, a' \rangle_2$ does not depend on the choice of $\mathfrak{P}_v$ or on the covering $D \to C$.*

Proof. Let $\mathfrak{C}_0 \in C(\overline{K})$ and $\mathfrak{D}_0 \in D(\overline{K})$ such that $\mathfrak{C}_0$ covers 0 on E and $\mathfrak{D}_0$ covers $\mathfrak{C}_0$. Since $n'(d\mathfrak{D}_0) = d\mathfrak{C}_0$ represents $-a$, we can take the element $\beta \in Z^1(K, E[nn'])$, appearing in definition (3.4) of the pairing $\langle \cdot, \cdot \rangle_1$, to be $-d\mathfrak{D}_0$. For each place v of K we are given $\mathfrak{P}_v \in C(K_v)$. Let $P_v = \mathfrak{P}_v - \mathfrak{C}_0$, then $dP_v = -d\mathfrak{C}_0$; this represents $\mathrm{res}_v(a)$ in $H^1(K_v, E[n])$. Take $Q_v \in E(\overline{K}_v)$ with $n'Q_v = P_v$. Then $dQ_v - \mathrm{res}_v(\beta) = d(Q_v + \mathfrak{D}_0)$ and $\pi(Q_v + \mathfrak{D}_0) = P_v + \mathfrak{C}_0 = \mathfrak{P}_v$. Hence $\delta_{\pi,v}(\mathfrak{P}_v)$ is represented by the cocycle $dQ_v - \mathrm{res}_v(\beta)$, and by inspection of the definitions (3.4) and (3.8) it follows that $\langle a, a' \rangle_1 = \langle a, a' \rangle_2$. □

4. *The Cassels pairing*

In [3], Cassels defined a bilinear pairing $\langle \cdot, \cdot \rangle_{\mathrm{Cas}}$ on $S^2(K, E)$ taking values in μ_2 and having the following properties. The element $a \in S^2(K, E)$ is in the image of $S^4(K, E)$ precisely when $\langle a, a' \rangle_{\mathrm{Cas}} = +1$ for all $a' \in S^2(K, E)$. For all $a \in S^2(K, E)$ we have $\langle a, a \rangle = +1$. These are properties of the Cassels–Tate pairing on a 2-Selmer group as well (where we replace μ_2 with $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$). The pairing is defined in terms of quadratic Hilbert norm residue symbols.

We need some preparations for the definition of the pairing. The group $S^2(K, E)$ is a subgroup of $H^1(K, E[2])$. Let $\overline{A}$ be the finite étale algebra that is the Galois module of maps from $E[2]\backslash 0$ to $\overline{K}$. Then $\mu_2(\overline{A})$ is the Galois module of maps from $E[2]\backslash 0$ to μ_2. Let A denote the $\mathrm{Gal}(\overline{K}/K)$-invariants of $\overline{A}$. If E is given by $y^2 = F(x)$ where $F(x) = x^3 + a_2x^2 + a_4x + a_6$

https://doi.org/10.1112/S1461157010000185 Published online by Cambridge University Press

with $a_i \in K$, then $\overline{A} \cong \overline{K}[T]/(F(T))$ and $A \cong K[T]/(F(T))$. Let $\theta_1, \theta_2, \theta_3$ be the three roots of $F(x)$ in $\overline{K}$. We have $A \cong \prod^{\diamondsuit} K(\theta_j)$ where $\prod^{\diamondsuit}$ denotes taking the product over a set of representatives for the $\mathrm{Gal}(\overline{K}/K)$-orbits of the set of θ_j. Let $T_j = (\theta_j, 0) \in E[2]\backslash 0$ and define

$$w : E[2] \to \mu_2(\overline{A}), \quad w(P) = (T_j \mapsto e_2(P, T_j)).$$

Then w induces an injective homomorphism

$$w_* : H^1(K, E[2]) \to H^1(K, \mu_2(\overline{A})).$$

See [7] for a proof of the injectivity. Let r_j be the map from $H^1(K, \mu_2(\overline{A}))$ to $H^1(K(\theta_j), \mu_2)$ given by restriction and evaluation at T_j. Shapiro's lemma shows that the map

$$r = \prod\nolimits^{\diamondsuit} r_j : H^1(K, \mu_2(\overline{A})) \to H^1(A, \mu_2) := \prod\nolimits^{\diamondsuit} H^1(K(\theta_j), \mu_2)$$

is an isomorphism. For each j, we have a Kummer isomorphism from $H^1(K(\theta_j), \mu_2)$ to $K(\theta_j)^\times/(K(\theta_j)^\times)^2$. This induces an isomorphism

$$k = \prod\nolimits^{\diamondsuit} k_j : H^1(A, \mu_2) \to A^\times/(A^\times)^2.$$

Composing the three maps w_*, r and k gives an injective group homomorphism

$$w_1 = k \circ r \circ w_* : H^1(K, E[2]) \to A^\times/(A^\times)^2. \tag{4.1}$$

This is the map that is used in 2-descent computations to represent cohomology classes by elements of $A^\times$, which are much easier to handle. Note that the image of w_1 is equal to the kernel of the norm map from $A^\times/(A^\times)^2$ to $K^\times/(K^\times)^2$.

We are now ready to give the definition of $\langle \cdot, \cdot \rangle_{\mathrm{Cas}}$. Let $a, a' \in S^2(K, E)$. The element $a \in S^2(K, E)$ is represented by a 2-covering C (which Cassels denotes $\mathcal{D}_\Lambda$) of E. Cassels [3] gives an explicit construction of rational functions f_j on C (which he denotes $\frac{L_j}{L_0}$), defined over $K(\theta_j)$, with the following three properties:

(i) $\mathrm{div}(f_j) = 2\mathcal{D}_j$ where $[\mathcal{D}_j] \mapsto T_j = (\theta_j, 0)$ under the isomorphism of $\mathrm{Pic}^0(C)$ and E;

(ii) each K-isomorphism of $K(\theta_i)$ to $K(\theta_j)$ sending θ_i to θ_j sends f_i to f_j;

(iii) the product $f_1 f_2 f_3$ is a square in $K(C)$, say $f_1 f_2 f_3 = h^2$.

Swinnerton-Dyer [14] shows that such functions exist for arbitrary locally soluble n-coverings C of E. Using these functions, we construct a 2-covering $\overline{D}$ of C over $\overline{K}$ by setting $f_j = u_j^2$ for an indeterminate u_j $(j = 1, 2, 3)$, together with $u_1 u_2 u_3 = h$. Define a Galois action on $\overline{K}(\overline{D})$ in such a way that it permutes the u_j in the same way as the θ_j, and let D over K be the curve corresponding to the fixed field of this action. The covering $\overline{D} \to C$ then descends to a covering $D \to C$ defined over K. (If $C = E$, this generalises the usual choice of $f_j = x - \theta_j$ that is used in 2-descent computations.) We write f for the element of $A \otimes_K K(C)$ given by $T_j \mapsto f_j$.

Let v be a place of K. For γ_j, $\kappa_j \in K_v(\theta_j)^\times/(K_v(\theta_j)^\times)^2$ we let $(\gamma_j, \kappa_j)_{K_v(\theta_j)}$ denote the quadratic Hilbert norm residue symbol. Let $\overline{A}_v = A \otimes_K \overline{K}_v$ and $A_v = A \otimes_K K_v$ be its $\mathrm{Gal}(\overline{K}_v/K_v)$-invariants. Then $A_v \cong \prod^{\diamondsuit} K_v(\theta_j)$, where this $\prod^{\diamondsuit}$ is taken over $\mathrm{Gal}(\overline{K}_v/K_v)$-orbits. Let

$$(\gamma, \kappa)_{A_v} = \prod\nolimits^{\diamondsuit} (\gamma_j, \kappa_j)_{K_v(\theta_j)}$$

where $\gamma, \kappa \in A_v^\times/(A_v^\times)^2$ and γ_j, κ_j are their images in $K_v(\theta_j)^\times/(K_v(\theta_j)^\times)^2$. Since $A \subset A_v$ it also makes sense for $(\cdot, \cdot)_{A_v}$ to take an element of $A^\times/(A^\times)^2$ as one of its arguments. Since C represents an element in $S^2(K, E)$, there is a point $\mathfrak{P}_v \in C(K_v)$ (which Cassels calls $\mathfrak{C}_v$). Now Cassels defines $\langle \cdot, \cdot \rangle_{\mathrm{Cas}} : S^2(K, E) \times S^2(K, E) \to \mu_2$ by

$$\langle a, a' \rangle_{\mathrm{Cas}} = \prod_{v \in M_K} (f(\mathfrak{P}_v), w_1(a'))_{A_v} \tag{4.2}$$

where w_1 is the map defined in (4.1). Cassels shows that the value of the pairing does not depend on the choice of f or on the choice of $\mathfrak{P}_v$. This will also follow from our main result

https://doi.org/10.1112/S1461157010000185 Published online by Cambridge University Press

Theorem 6.3 below. Using Swinnerton-Dyer's more general construction of $D \to C$ in [14], one obtains a pairing on $S^n(K,E) \times S^2(K,E)$, for which the analogue of Theorem 6.3 can be proved in the same way.

The advantage of this definition is that it allows us to work with $w_1(a') \in A^\times/(A^\times)^2$, which is how a' is usually represented when we compute the 2-Selmer group, and that it uses objects like f and $\mathfrak{P}_v$ coming directly from the geometric representation C of a. Cassels' explicit construction of the f_j makes it practical to compute the pairing.

5. *The main diagram*

Now let us introduce figure (5.1) which shows a diagram that relates the pairing $\langle\cdot,\cdot\rangle_{e,v}$ defined in (3.3) with the quadratic Hilbert symbol $(\cdot,\cdot)_{A_v}$ used in the definition of Cassels' pairing (4.2). We will show that the diagram commutes. This will then enable us to identify the Cassels and Cassels–Tate pairings (see Section 6).

$$\begin{tikzcd}
H^1(K_v,E[2]) \arrow[d, "w_{*,v}"'] & \times & H^1(K_v,E[2]) \arrow[d, "w_{*,v}"'] \arrow[r, "\cup_e"] \arrow[dr, phantom, "(1)"] & H^2(K_v,\mu_2) \arrow[dr, equal] & \\
H^1(K_v,\mu_2(\overline{A}_v)) \arrow[d, "r_v"', "\cong"] & \times & H^1(K_v,\mu_2(\overline{A}_v)) \arrow[r, "\cup_m"] \arrow[d, "r_v"', "\cong"] \arrow[dr, phantom, "(2)"] & H^2(K_v,\mu_2(\overline{A}_v)) \arrow[r, "N_*"] \arrow[d, "r'_v"', "\cong"] & H^2(K_v,\mu_2) \arrow[dd, "\mathrm{inv}'"] \\
H^1(A_v,\mu_2) \arrow[d, "k_v"', "\cong"] & \times & H^1(A_v,\mu_2) \arrow[r, "\cup"] \arrow[d, "k_v"', "\cong"] \arrow[dr, phantom, "(4)"] & H^2(A_v,\mu_2) \arrow[d, "\prod^\diamondsuit \mathrm{inv}'_j"] \arrow[r, phantom, "(3)"] & \\
A_v^\times/(A_v^\times)^2 & \times & A_v^\times/(A_v^\times)^2 \arrow[r, "\prod^\diamondsuit (\cdot,\cdot)_{K_v(\theta_j)}"] & \prod^\diamondsuit \mu_2 \arrow[r, "\nu"] & \mu_2
\end{tikzcd} \tag{5.1}$$

Let us explain the various maps occurring in the diagram.

The maps w_*, r and k defined in the last section have local analogues, denoted by $w_{*,v}$, r_v and k_v.

We identify $\mu_2 \otimes \mu_2 = \mu_2$ via $(-1)^p \otimes (-1)^q = (-1)^{pq}$. Since $\mu_2(\overline{A}_v)$ is the Galois module of maps from $E[2]\backslash 0$ to μ_2, this identification induces a map

$$m : \mu_2(\overline{A}_v) \otimes \mu_2(\overline{A}_v) \to \mu_2(\overline{A}_v).$$

Let $\cup_m$ be the cup product map induced by m.

We define

$$N : \mu_2(\overline{A}_v) \to \mu_2; \quad (T \mapsto \beta(T)) \mapsto \prod_{T \in E[2]\backslash 0} \beta(T),$$

and let N_* be the map it induces on H^2.

In the same way as above for the H^1 in the global situation, let r'_j be the map from $H^2(K_v,\mu_2(\overline{A}_v))$ to $H^2(K_v(\theta_j),\mu_2)$ obtained by restriction and evaluation at T_j. Shapiro's lemma shows again that the map

$$r'_v = \prod\nolimits^\diamondsuit r'_j : H^2(K_v,\mu_2(\overline{A}_v)) \to H^2(A_v,\mu_2) := \prod\nolimits^\diamondsuit H^2(K_v(\theta_j),\mu_2)$$

is an isomorphism.

Let $\cup_j$ be the cup product map from $H^1(K_v(\theta_j),\mu_2) \times H^1(K_v(\theta_j),\mu_2)$ to $H^2(K_v(\theta_j),\mu_2)$ (using the identification $\mu_2 \otimes \mu_2 = \mu_2$ again) and $\cup = \prod^\diamondsuit \cup_j$.

Let $\mathrm{inv}' : H^2(K_v,\mu_2) \to \mu_2$ be the composition of the invariant map with the isomorphism of $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ and μ_2, and likewise for $\mathrm{inv}'_j : H^2(K_v(\theta_j),\mu_2) \to \mu_2$.

Finally, let $\nu : \prod^\diamondsuit \mu_2 \to \mu_2$ be the usual product in μ_2.

https://doi.org/10.1112/S1461157010000185 Published online by Cambridge University Press

Theorem 5.2. *The diagram in figure* (5.1) *is commutative.*

We prove this theorem using the following lemmas. The first of these is simple but crucial.

Lemma 5.3. *Identify $\mu_2 \otimes \mu_2 = \mu_2$ as above. Then for all $P, Q \in E[2]$ we have*

$$e_2(P,Q) = \prod_{T \in E[2]\backslash 0} e_2(P,T) \otimes e_2(Q,T).$$

Proof. True by a simple case by case calculation. □

Lemma 5.4. *Diagram (1) in figure* (5.1) *is commutative.*

Proof. Let $\xi, \psi \in H^1(K_v, E[2])$ be represented by cocycles which, for ease of notation, we also write as ξ and ψ. We have $\xi \cup_e \psi : (\sigma,\tau) \mapsto e_2(\xi_\sigma, {}^{\sigma}\psi_\tau)$.

Now $w(\xi) : \sigma \mapsto (T \mapsto e_2(\xi_\sigma, T))$ for $T \in E[2]\backslash 0$ and similarly for $w(\psi)$. Thus

$$\begin{aligned} N_*(w(\xi) \cup_m w(\psi)) : (\sigma,\tau) \mapsto\ & N(m((S \mapsto e_2(\xi_\sigma, S)) \otimes {}^{\sigma}(T \mapsto e_2(\psi_\tau, T)))) \\ =\ & N(m((S \mapsto e_2(\xi_\sigma, S)) \otimes (T \mapsto {}^{\sigma}e_2(\psi_\tau, {}^{\sigma^{-1}}T)))) \\ =\ & N(m((S \mapsto e_2(\xi_\sigma, S)) \otimes (T \mapsto e_2({}^{\sigma}\psi_\tau, T)))) \\ =\ & N(T \mapsto e_2(\xi_\sigma, T) \otimes e_2({}^{\sigma}\psi_\tau, T)) \\ =\ & \prod_{T \in E[2]\backslash 0} e_2(\xi_\sigma, T) \otimes e_2({}^{\sigma}\psi_\tau, T) \in \mu_2 \otimes \mu_2. \end{aligned}$$

By Lemma 5.3 this is the same as $\xi \cup_e \psi$. □

Lemma 5.5. *Diagram (2) in figure* (5.1) *is commutative.*

Proof. Let $\xi, \psi \in H^1(K_v, \mu_2(\overline{A}_v))$. As in the proof of the previous lemma, we use the same symbols for cocycles representing these classes. Let $T_j = (\theta_j, 0) \in E[2]\backslash 0$. We must show that $r'_j(\xi \cup_m \psi)$ and $r_j(\xi) \cup_j r_j(\psi)$ are equal in $H^2(K_v(\theta_j), \mu_2 \otimes \mu_2)$. We find that they are represented by cocycles $(\sigma,\tau) \mapsto \xi_\sigma(T_j) \otimes ({}^{\sigma}\psi_\tau)(T_j)$ and $(\sigma,\tau) \mapsto \xi_\sigma(T_j) \otimes {}^{\sigma}(\psi_\tau(T_j))$. Since $\sigma(T_j) = T_j$ for all $\sigma \in \mathrm{Gal}(\overline{K}_v/K_v(\theta_j))$, these cocycles are equal. □

Lemma 5.6. *Diagram (3) in figure* (5.1) *is commutative.*

Proof. Let N_j denote the norm induced by taking the product over each element in the $\mathrm{Gal}(\overline{K}_v/K_v)$-orbit of θ_j. Recall that $\nu : \prod^{\diamondsuit} \mu_2 \to \mu_2$ is the usual product in μ_2, and let ν_* be the map it induces on H^2. Then the map N_* in figure (5.1) factors as the composite of $\prod^{\diamondsuit} N_{j,*}$ and ν_*.

We have $\overline{A}_v = \prod^{\diamondsuit} \overline{K_v(\theta_j)}$ where $\overline{K_v(\theta_j)} := K_v(\theta_j) \otimes_{K_v} \overline{K}_v$. Abusing notation slightly by writing r'_j for the corresponding map on $H^2(K_v, \mu_2(\overline{K_v(\theta_j)}))$, we obtain the following commutative diagram.

$$\begin{tikzcd} H^2(K_v, \mu_2(\overline{A}_v)) \arrow[r, phantom, "="] \arrow[d, "r'_v"] & \prod^{\diamondsuit} H^2(K_v, \mu_2(\overline{K_v(\theta_j)})) \arrow[r, "\prod^{\diamondsuit} N_{j,*}"] \arrow[d, "\prod^{\diamondsuit} r'_j"] \arrow[dr, phantom, "(5)"] & \prod^{\diamondsuit} H^2(K_v, \mu_2) \arrow[r, "\nu_*"] \arrow[d, "\prod^{\diamondsuit} \mathrm{inv}'"] \arrow[dr, phantom, "(6)"] & H^2(K_v, \mu_2) \arrow[d, "\mathrm{inv}'"] \\ H^2(A_v, \mu_2) \arrow[r, phantom, "="] & \prod^{\diamondsuit} H^2(K_v(\theta_j), \mu_2) \arrow[r, "\prod^{\diamondsuit} \mathrm{inv}'_j"] & \prod^{\diamondsuit} \mu_2 \arrow[r, "\nu"] & \mu_2 \end{tikzcd}$$

Diagram (5) commutes by the next lemma. That diagram (6) commutes is obvious. This proves the commutativity of diagram (3). □

https://doi.org/10.1112/S1461157010000185 Published online by Cambridge University Press

Lemma 5.7. *Let X_j be the* $\mathrm{Gal}(\overline{K}_v/K_v)$*-orbit of* T_j*. Then there is a commutative diagram*

$$\begin{tikzcd}
H^2(K_v, \mathrm{Map}(X_j, \mu_{2^\infty})) \arrow[r, "N_{j,*}"] \arrow[d, "r'_j"', "\cong"] & H^2(K_v, \mu_{2^\infty}) \arrow[d, "\mathrm{inv}"] \\
H^2(K_v(\theta_j), \mu_{2^\infty}) \arrow[r, "\mathrm{inv}_j"] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

Proof. Let $\iota : H^2(K_v, \mu_{2^\infty}) \to H^2(K_v, \mathrm{Map}(X_j, \mu_{2^\infty}))$ be induced by the inclusion of the constant maps. Then $r'_j \circ \iota$ is the restriction map from the 2-primary part of the Brauer group of K_v to the 2-primary part of the Brauer group of $K_v(\theta_j)$. By [**10**, Section 1, Theorem 3] it is multiplication by d_j on the invariants, where $d_j = [K_v(\theta_j) : K_v] = \#X_j$, and is therefore surjective. Since r'_j is an isomorphism (by Shapiro's lemma), it follows that ι is surjective. Then for $\eta \in H^2(K_v, \mu_{2^\infty})$ we compute

$$(\mathrm{inv} \circ N_{j,*})(\iota(\eta)) = d_j \mathrm{inv}(\eta) = (\mathrm{inv}_j \circ r'_j)(\iota(\eta)).$$

(Alternatively, the definitions in [**1**, Chapter III, Section 9] show that $N_{j,*} \circ (r'_j)^{-1}$ is corestriction, and the lemma then reduces to a well-known property of the invariant maps.) □

Lemma 5.8. *Diagram (4) in figure* (5.1) *is commutative.*

Proof. This is [**9**, XIV.2, Proposition 5] applied to each constituent field of A_v. □

Lemmas 5.4, 5.5, 5.6 and 5.8 together prove Theorem 5.2. Composing the maps in the last row of (5.1) gives the pairing $(\cdot,\cdot)_{A_v}$ defined at the end of Section 4. Let $w_{1,v} = k_v \circ r_v \circ w_{*,v}$ be the local analogue of the map (4.1). Writing the isomorphism $\frac{1}{2}\mathbb{Z}/\mathbb{Z} \cong \mu_2$ as $\alpha \mapsto (-1)^{2\alpha}$ we obtain the following.

Corollary 5.9. *Let* $s, s' \in H^1(K_v, E[2])$*. We have* $(-1)^{2\langle s,s'\rangle_{e,v}} = (w_{1,v}(s), w_{1,v}(s'))_{A_v}$.

This result allows us to express the pairing $\langle \cdot,\cdot\rangle_{e,v}$ in terms of the quadratic Hilbert symbol $(\cdot,\cdot)_{A_v}$. This will be the key for the proof of the main theorem in the next section.

6. *The main theorem*

Let C be a torsor under E and choose $f \in A \otimes_K K(C)$ as described in Section 4. Let $\pi : D \to C$ be the 2-covering obtained from f. The following lemma is a variant of [**8**, Theorem 2.3].

Lemma 6.1. *We have* $w_1(\delta_\pi(\mathfrak{P})) = f(\mathfrak{P}) \bmod (A^\times)^2$ *for all* $\mathfrak{P} \in C(K)$*, away from the zeros and poles of* f_j.

Proof. Let $\mathfrak{Q} \in D(\overline{K})$ with $\pi(\mathfrak{Q}) = \mathfrak{P}$. We recall from Section 4 that $r = \prod^\diamondsuit r_j$ and $k = \prod^\diamondsuit k_j$. So by (3.7) and (4.1) it suffices to show that, for each j,

$$k_j r_j w(d\mathfrak{Q}) = f_j(\mathfrak{P}) \mod (K(\theta_j)^\times)^2.$$

We have $r_j w(d\mathfrak{Q}) = (\sigma \mapsto e_2({}^\sigma\mathfrak{Q} - \mathfrak{Q}, T_j))$ in $H^1(K(\theta_j), \mu_2)$. The construction of D gives that $f_j \circ \pi = g_j^2$ for some rational function g_j on D, defined over $K(\theta_j)$. We claim that

$$e_2(S, T_j) = g_j(S + \mathfrak{X})/g_j(\mathfrak{X}) \tag{6.2}$$

for any $\mathfrak{X} \in D(\overline{K})$ for which the numerator and denominator are well-defined and non-zero. Indeed, since the Weil pairing is a geometric construction, we may identify (by a suitable choice

https://doi.org/10.1112/S1461157010000185 Published online by Cambridge University Press

of base points on C and D, defined over $\overline{K}$) the torsors C and D with E, and the 2-covering map $\pi : D \to C$ with multiplication-by-2 on E. Note that identifying D and E as torsors means that the action of E on D becomes the group law on E. Our claim now reduces to the definition of the Weil pairing in [**12**, Chapter III, Section 8].

Putting $S = {}^\sigma\mathfrak{Q} - \mathfrak{Q}$ and $\mathfrak{X} = \mathfrak{Q}$ in (6.2) gives

$$e_2({}^\sigma\mathfrak{Q} - \mathfrak{Q}, T_j) = g_j({}^\sigma\mathfrak{Q})/g_j(\mathfrak{Q}) = {}^\sigma(g_j(\mathfrak{Q}))/g_j(\mathfrak{Q})$$

for any $\sigma \in \mathrm{Gal}(\overline{K}/K(\theta_j))$. Then $r_j w(d\mathfrak{Q}) = (\sigma \mapsto {}^\sigma(g_j(\mathfrak{Q}))/g_j(\mathfrak{Q}))$ and therefore

$$k_j r_j w(d\mathfrak{Q}) = g_j^2(\mathfrak{Q}) = f_j \pi(\mathfrak{Q}) = f_j(\mathfrak{P})$$

as required. □

The same statement holds over K_v, with the same proof.

Recall the pairings $\langle\cdot,\cdot\rangle_{\mathrm{CT}}$, $\langle\cdot,\cdot\rangle_1$, $\langle\cdot,\cdot\rangle_2$ and $\langle\cdot,\cdot\rangle_{\mathrm{Cas}}$, defined in (3.1), (3.4), (3.8) and (4.2), respectively. We can now prove our main result. We remark again that it easily generalises to $a \in S^n(K, E)$.

Theorem 6.3. *Let K be a number field and E an elliptic curve over K, and let $a, a' \in S^2(K, E)$. Let $\langle a, a'\rangle_{\mathrm{Cas}} \in \mu_2$ denote the pairing defined by Cassels in* [**3**]. *Let $\langle a, a'\rangle_{\mathrm{CT}} \in \frac{1}{2}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ denote the Cassels–Tate pairing. Writing the isomorphism $\frac{1}{2}\mathbb{Z}/\mathbb{Z} \cong \mu_2$ as $\alpha \mapsto (-1)^{2\alpha}$ we have*

$$\langle a, a'\rangle_{\mathrm{Cas}} = (-1)^{2\langle a,a'\rangle_{\mathrm{CT}}}.$$

Proof. The equality $\langle a, a'\rangle_{\mathrm{Cas}} = (-1)^{2\langle a,a'\rangle_2}$ is immediate from Corollary 5.9, the local analogue of Lemma 6.1, and the observation that $w_{1,v}(\mathrm{res}_v\, a')$ is the image of $w_1(a') \in A^\times/(A^\times)^2$ in $A_v^\times/(A_v^\times)^2$. Propositions 3.5 and 3.9 show that $\langle a, a'\rangle_2 = \langle a, a'\rangle_1 = \langle a, a'\rangle_{\mathrm{CT}}$. □

It would be desirable to have a definition of the Cassels–Tate pairing along the lines of Cassels' definition that does not require one of the arguments to be in the 2-Selmer group. Let us discuss why there is no obvious generalisation. Consider the pairing on $S^n(K, E)$. The nth power Hilbert symbol is only defined when $\mu_n \subset K$, so let us assume that this is the case. The heart of our proof is the commutativity of the diagram (5.1), leading to Corollary 5.9. Here an essential ingredient is Lemma 5.3, which only works for $n = 2$. For any n, the pairing $\cup_e$ is symmetric (the antisymmetry of the Weil pairing cancels that of the cup product), and the Hilbert symbol is antisymmetric. So, for $n > 2$, it is impossible to relate them in a similarly direct way as in Corollary 5.9.

Acknowledgements. The first and second author would like to thank the hospitality of Jacobs University Bremen. The second author was supported by a National Security Agency, Standard Grant and a Fulbright Award. The authors are grateful for the helpful comments of three anonymous referees.

References

1. K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics 87 (Springer, New York, 1994).

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

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

4. T. A. Fisher, 'The Cassels–Tate pairing and the Platonic solids', *J. Number Theory* 98 (2003) 105–155.

5. J. S. Milne, *Arithmetic duality theorems* (Academic Press, Boston, MA, 1986).

6. B. Poonen and M. Stoll, 'The Cassels–Tate pairing on polarized abelian varieties', *Ann. of Math.* (2) 150 (1999) 1109–1149.

https://doi.org/10.1112/S1461157010000185 Published online by Cambridge University Press

7. E. F. Schaefer, '2-descent on the Jacobians of hyperelliptic curves', *J. Number Theory* 51 (1995) no. 2, 219–232.

8. E. F. Schaefer, 'Computing a Selmer group of a Jacobian using functions on the curve', *Math. Ann.* 310 (1998) no. 3, 447–471.

9. J.-P. Serre, *Local fields* (Springer, New York, 1979).

10. J.-P. Serre, 'Local class field theory', *Algebraic number theory* (eds J. W. S. Cassels and A. Fröhlich; Academic Press, London, 1967) 129–161.

11. J.-P. Serre, *Galois cohomology* (Springer, Berlin, 2002).

12. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106 (Springer, New York, 1992).

13. S. Stamminger, 'Explicit 8-descent on elliptic curves', PhD Thesis, International University Bremen, 2005.

14. H. P. F. Swinnerton-Dyer, '2^n-descent on elliptic curves for all n', *J. London Math. Soc.* (2), to appear.

Tom Fisher
DPMMS
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB
United Kingdom

T.A.Fisher@dpmms.cam.ac.uk

Edward F. Schaefer
Department of Mathematics and Computer Science
Santa Clara University
Santa Clara, CA 95053
USA

eschaefer@scu.edu

Michael Stoll
Mathematisches Institut
Universität Bayreuth
95440 Bayreuth
Germany

Michael.Stoll@uni-bayreuth.de

https://doi.org/10.1112/S1461157010000185 Published online by Cambridge University Press