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

In [3], Cassels defined a pairing on the 2-Selmer group of an elliptic curve over a number field. It shares some properties with the extension of the Cassels-Tate pairing to the 2-Selmer group of an elliptic curve over a number field. 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 of an elliptic curve over a number field. The fact that it is alternating gives information on the structure of the Shafarevich-Tate group. For $n \geq 2$, its extension from the n-torsion of a Shafarevich-Tate group to an n-Selmer group can be used to determine the image of the n^2-Selmer group in the n-Selmer group. This sometimes enables the determination of which elements of the n-Selmer group come from elements of the Mordell-Weil group and which come from elements of the Shafarevich-Tate group. The Cassels-Tate pairing is, unfortunately, quite difficult to evaluate in practice. The pairing defined by Cassels on the 2-Selmer group of an elliptic curve, however, is quite straightforward to evaluate. So it is useful to prove that the two pairings are equal on the 2-Selmer group of an elliptic curve.

In Section 2, we give the Weil-pairing definition and a new definition of the Cassels-Tate pairing extended to the n-Selmer group of an elliptic curve, under a hypothesis that is always satisfied for n a prime. In Section 3 we present the definition of the pairing defined by Cassels on 2-Selmer groups of elliptic curves. In Section 4 we present a large diagram and prove it is commutative. We also discuss why our methods do not easily generalise to n-Selmer groups for $n > 2$. We use this diagram to prove our main theorem in Section 5 that the pairing defined by Cassels is the same as the Cassels-Tate pairing on the 2-Selmer group of an elliptic curve over a number field.

Date: October 8, 2007.

2000 *Mathematics Subject Classification.* Primary 11G05; Secondary 11G07.

Key words and phrases. Cassels-Tate pairing, elliptic curve, 2-Selmer group.

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.

Recently, Swinnerton-Dyer [13] has generalised Cassels' pairing on the 2-Selmer group, to a pairing between the m-Selmer group and the 2-Selmer group. In parallel with the results described above, we show that this pairing is again the Cassels-Tate pairing.

2. 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 $m,n \geq 2$ be integers. We are interested in the restriction of this pairing to the n-torsion $Ш(K,E)[n]$, or more generally to $Ш(K,E)[m] \times Ш(K,E)[n]$. Let $S^n(K,E)$ denote the n-Selmer group of E over K. The group $Ш(K,E)[n]$ is isomorphic to the quotient of $S^n(K,E)$ by the image of $E(K)/nE(K)$ under the coboundary map. We write $\langle\ ,\ \rangle_{\mathrm{CT}}$ for the extension of the Cassels-Tate pairing to $S^m(K,E) \times S^n(K,E)$. By definition this pairing is trivial on the images of $E(K)/mE(K)$ and $E(K)/nE(K)$.

If M is a $\mathrm{Gal}(\overline{K}/K)$-module, then we denote $Z^i(\mathrm{Gal}(\overline{K}/K),M)$ and $H^i(\mathrm{Gal}(\overline{K}/K),M)$ by $Z^i(K,M)$ and $H^i(K,M)$, respectively.

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

$$H^2(K,E[n]) \to \prod_v H^2(K_v,E[n]), \qquad (2.1)$$

where v runs over all places of K, is injective. This is known for n a prime [2, Lemma 5.1]. (The injectivity does not hold for $E[n]$ replaced by an arbitrary finite Galois module. See [10, III.4.7] for a counter-example.) From Section 3 onwards we restrict to the case $n = 2$, so our hypothesis will be automatically satisfied.

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E[n] & \longrightarrow & E[mn] & \xrightarrow{\cdot n} & E[m] & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E[n] & \longrightarrow & E & \xrightarrow{\cdot n} & E & \longrightarrow & 0 \end{array}$$

to obtain a commutative diagram

$$\begin{array}{ccccc} H^1(K,E[mn]) & \xrightarrow{\cdot n} & H^1(K,E[m]) & \longrightarrow & H^2(K,E[n]) \\ & & \downarrow & & \downarrow \\ & & \prod_v H^1(K_v,E) & \longrightarrow & \prod_v H^2(K_v,E[n]) \end{array}$$

By the above hypothesis, there exists $c \in H^1(K,E[mn])$ with $nc = a$. We represent c by a cocycle $\gamma \in Z^1(K,E[mn])$; then $\alpha = n\gamma \in Z^1(K,E[m])$ represents a. For each place v of K, the cocycle $\mathrm{res}_v(\alpha) = \alpha_v$ in $Z^1(K_v,E(\overline{K}_v))$ is a coboundary. So there exists $\beta_v \in E(\overline{K}_v)$ such that $\alpha_v = d\beta_v$ (recall $d\beta_v$ is the cocycle $\sigma \mapsto {}^\sigma\beta_v - \beta_v$). Take $Q_v \in E(\overline{K}_v)$ such that $nQ_v = \beta_v$. Consider $dQ_v - \gamma_v \in Z^1(K_v,E[n])$, where γ_v is the restriction of γ. Let $\cup_e$ be the cup product pairing induced by the Weil pairing from $H^1(K_v,E[n]) \times H^1(K_v,E[n])$ to

$H^2(K_v, \mu_n)$. For $s, s' \in H^1(K_v, E[n])$ define $\langle s, s'\rangle_{\mathrm{inv}\circ\cup_e,v}$ to be the composition of $\cup_e$ with the invariant map. We define $\langle a, a'\rangle_1 = \sum_v \langle [dQ_v - \gamma_v], a'\rangle_{\mathrm{inv}\circ\cup_e,v}$.

Proposition 2.2. *Let $a \in S^m(K,E)$ and $a' \in S^n(K,E)$. We have $\langle a, a'\rangle_1 = \langle a, a'\rangle_{\mathrm{CT}}$.*

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

Remark 2.3. The general form of the Weil-pairing definition, avoiding the hypothesis that (2.1) is injective, is given in [5, p. 97]. This variant is used in [6] to generalise Proposition 2.2 to abelian varieties.

Let C and D be torsors (*i.e.*, principal homogeneous spaces) under E. A morphism $\pi : D \to C$ is called an *n-covering* if $\pi(P + Q) = nP + \pi(Q)$ for all $P \in E$ and $Q \in D$. If $C = E$ is the trivial torsor, this coincides with the usual notion of n-covering of E. For $Q_1, Q_2 \in D$ we write $Q_1 - Q_2$ for the point on E determined by the fact D is a torsor under E. Following [12, Chapter 6] we define the coboundary map $\delta_\pi : C(K) \to H^1(K, E[n])$ by sending $P \in C(K)$ to the class of $dQ = (\sigma \mapsto {}^\sigma Q - Q)$ where $Q \in D(\overline{K})$ with $\pi Q = P$.

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 isomorphsim 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 $Q \in D(\overline{K})$ with $\pi(Q) = 0$ then we can take $\psi : P \mapsto P - Q$, in which case D is represented by $-dQ$. Note also that if $C \to E$ is an m-covering of E and $D \to C$ is an n-covering of C, then $D \to E$ is an mn-covering of E. If $D \to E$ corresponds to $b \in H^1(K, E[mn])$, then $C \to E$ corresponds to $nb \in H^1(K, E[m])$.

We give a new definition of the Cassels-Tate pairing, again under the hypothesis that (2.1) is injective. Let C be an m-covering of E over K representing a. By the hypothesis, a is divisible by n in the Weil-Châtelet group. So there is an n-covering $\pi : D \to C$ defined over K. Let v be a place of K. Since a is trivial in $H^1(K_v, E(\overline{K}_v))$, there is a point $P_v \in C(K_v)$. We define $\langle a, a'\rangle_2 = \sum_v \langle \delta_\pi(P_v), a'\rangle_{\mathrm{inv}\circ\cup_e,v}$.

Proposition 2.4. *Let $a \in S^m(K,E)$ 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 the P_v.*

Proof. Let $R_C \in C(\overline{K})$ and $R_D \in D(\overline{K})$ such that R_C covers 0 on E and R_D covers R_C. Since $n(dR_D) = dR_C$ represents $-a$, we can choose $\gamma \in Z^1(K, E[mn])$, as defined above, to be $-dR_D$. For each place v of K we are given $P_v \in C(K_v)$. Let $\beta_v = P_v - R_C$, then $d\beta_v = -dR_C$; this represents $a \in H^1(K_v, E[m])$. Take $Q_v \in E(\overline{K}_v)$ with $nQ_v = \beta_v$. Then $dQ_v - \gamma_v = d(Q_v + R_D)$ and $\pi(Q_v + R_D) = \beta_v + R_C = P_v$. Hence $\delta_\pi(P_v)$ is represented by the cocycle $dQ_v - \gamma_v$ appearing in the definition of $\langle\ ,\ \rangle_1$. □

3. The Cassels pairing

In [3], Cassels defined a bilinear pairing $\langle\ ,\ \rangle_{\mathrm{Cas}}$ on $S^2(K,E)$ taking values in μ_2 with 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.

A mild generalisation of Cassels' construction, due to Swinnerton-Dyer [13], gives a pairing $S^m(K,E) \times S^2(K,E) \to \mu_2$. We work with this generalised form of the pairing, which we continue to denote $\langle\ ,\ \rangle_{\mathrm{Cas}}$. It reduces to Cassels' definition in the case $m = 2$.

We prepare to recall 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 $E[2] \setminus 0$ to $\overline{K}$. Then $\mu_2(\overline{A})$ is the Galois module of maps from $E[2] \setminus 0$ to μ_2. Let A denote the $\mathrm{Gal}(\overline{K}/K)$-invariants of $\overline{A}$. Let E be given by $y^2 = F(x)$ where $F(x) = x^3 + a_2x^2 + a_4x + a_6$ with $a_i \in K$. Then $A \cong K[T]/(F(T))$. 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 one element from each $\mathrm{Gal}(\overline{K}/K)$-orbit of the set of θ_j's. Let $T_j = (\theta_j, 0) \in E[2] \setminus 0$ and define $w : E[2] \to \mu_2(\overline{A})$ by $w(P) = (T_j \mapsto e_2(P, T_j))$. Then w induces an injective homomorphism from $H^1(K,E[2])$ to $H^1(K,\mu_2(\overline{A}))$, which we also denote w. Let r_j be the restriction map from $H^1(K,\mu_2(\overline{A}))$ to $H^1(K(\theta_j),\mu_2)$. Shapiro's Lemma shows that the map $r = \prod^{\diamondsuit} r_j$ is an isomorphism of $H^1(K,\mu_2(\overline{A}))$ with $\prod^{\diamondsuit} H^1(K(\theta_j),\mu_2)$, which we denote $H^1(A,\mu_2)$. 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, which we denote k, from $H^1(A,\mu_2)$ to $A^\times/(A^\times)^2$. Note that the image of $H^1(K,E[2])$ in $A^\times/(A^\times)^2$, under $k \circ r \circ w$, is equal to the kernel of the norm from $A^\times/(A^\times)^2$ to $K^\times/(K^\times)^2$.

We recall the definition of $\langle\ ,\ \rangle_{\mathrm{Cas}}$. Let $a \in S^m(K,E)$ and $a' \in S^2(K,E)$. Let $M = k \circ r \circ w(a')$ be the element of $A^\times/(A^\times)^2$ representing a'. The element $a \in S^m(K,E)$ is represented by an m-covering C (which Cassels denotes $\mathcal{D}_\Lambda$) of E. Swinnerton-Dyer [13] shows that there are rational functions f_j on C, 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 $f_1f_2f_3$ is a square in $K(C)$.

He then shows that a 2-covering of C may be defined by setting each f_j equal to the square of an indeterminate. In the case $m = 2$, Cassels gives an explicit construction of the f_j (which he denotes $\frac{L_j}{L_0}$) and this makes it practical to compute the pairing. We write f for the element of $A \otimes_K K(C)$ given by $T_j \mapsto f_j$.

Let v be a prime of K. Since C represents an element in $S^m(K,E)$, there is a point $P_v \in C(K_v)$ (which Cassels calls $\mathfrak{C}_v$). For $\gamma_j,\ \delta_j \in K_v(\theta_j)^\times/(K_v(\theta_j)^\times)^2$ we let $(\gamma_j, \delta_j)_{K_v(\theta_j)}$ denote the quadratic Hilbert norm residue symbol. Let $\overline{A}_v = A \otimes_K \overline{K}_v$ and A_v 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 $(\gamma, \delta)_{A_v} = \prod^{\diamondsuit}(\gamma_j, \delta_j)_{K(\theta_j)_v}$ where $\gamma, \delta \in A_v^\times/(A_v^\times)^2$ and γ_j, δ_j are their images in $K_v(\theta_j)^\times/(K_v(\theta_j)^\times)^2$. Cassels defines $\langle a, a'\rangle_{\mathrm{Cas}} = \prod_v (f(P_v), M)_{A_v}$.

4. The main diagram

Now let us introduce Figure 4.1 which will enable us to prove that for $a \in S^m(K,E)$, $a' \in S^2(K,E)$ we have $\langle a, a'\rangle_{\mathrm{Cas}} = \langle a, a'\rangle_2$. We can define the maps w, r and k locally, in an analogous way, and it will not change the image of M, locally. So we will not change our notation for these maps.

$$
\begin{array}{ccccccccc}
H^1(K_v,E[2]) & \times & H^1(K_v,E[2]) & \xrightarrow{\ \cup_e\ } & H^2(K_v,\mu_2) & & & & \\
{\scriptstyle w}\big\downarrow & & {\scriptstyle w}\big\downarrow & & (1) & & \diagdown\!\!\diagdown & & \\
H^1(K_v,\mu_2(\overline{A}_v)) & \times & H^1(K_v,\mu_2(\overline{A}_v)) & \xrightarrow{\ \cup_t\ } & H^2(K_v,\mu_2(\overline{A}_v)) & \xrightarrow{\ N_*\ } & & & H^2(K_v,\mu_2) \\
{\scriptstyle r}\big\downarrow{\scriptstyle \cong} & & {\scriptstyle r}\big\downarrow{\scriptstyle \cong} & (2) & {\scriptstyle r}\big\downarrow{\scriptstyle \cong} & & & & \\
H^1(A_v,\mu_2) & \times & H^1(A_v,\mu_2) & \xrightarrow{\ \cup\ } & H^2(A_v,\mu_2) & & (3) & & \big\downarrow{\scriptstyle \mathrm{inv}} \\
{\scriptstyle k}\big\downarrow{\scriptstyle \cong} & & {\scriptstyle k}\big\downarrow{\scriptstyle \cong} & (4) & \big\downarrow{\scriptstyle \prod^{\diamondsuit}\mathrm{inv}_j} & & & & \\
A_v^\times/(A_v^\times)^2 & \times & A_v^\times/(A_v^\times)^2 & \xrightarrow{\ \prod^{\diamondsuit}(\ ,\ )_{K_v(\theta_j)}\ } & \prod^{\diamondsuit}\mu_2 & & \xrightarrow{\ \nu\ } & & \mu_2
\end{array}
\tag{4.1}
$$

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 $E[2] \setminus 0$ to μ_2, this identification induces a map $t : \mu_2(\overline{A}_v) \otimes \mu_2(\overline{A}_v) \to \mu_2(\overline{A}_v)$. Let $\cup_t$ be the cup product map via t. Define $N : \mu_2(\overline{A}_v) \to \mu_2$ by $(T \mapsto \gamma(T)) \mapsto \prod_T \gamma(T)$, and let N_* be the map it induces on H^2's. Let r_j be the restriction map from $H^2(K_v,\mu_2(\overline{A}_v))$ to $H^2(K_v(\theta_j),\mu_2)$. In the same was as for the H^1's, Shapiro's Lemma shows that the map $r = \prod^{\diamondsuit} r_j$ is an isomorphism of $H^2(K_v,\mu_2(\overline{A}_v))$ with $\prod^{\diamondsuit} H^2(K_v(\theta_j),\mu_2)$, which we denote $H^2(A_v,\mu_2)$. 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 $H^2(K_v(\theta_j),\mu_2)$ 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.

Theorem 4.2. *The diagram in Figure 4.1 is commutative.*

We prove this theorem using the following lemmas.

Lemma 4.3. *Identify $\mu_2 \otimes \mu_2 = \mu_2$ as above. Then for all $P, Q \in E[2]$ we have*

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

Proof. A trivial verification. □

Lemma 4.4. *Diagram (1) in Figure 4.1 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 $\xi \cup_e \psi : (\sigma,\tau) \mapsto e_2(\xi_\sigma, {}^\sigma\psi_\tau) \in H^2(K_v,\mu_2)$.

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

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

By Lemma 4.3 this is the same as $\xi \cup_e \psi$. □

Lemma 4.5. *Diagram (2) in Figure 4.1 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 $T_j = (\theta_j, 0) \in E[2] \setminus 0$. We must show that $r_j(\xi \cup_t \psi)$ 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 4.6. *Diagram (3) in Figure 4.1 is commutative.*

Proof. We have $\overline{A}_v = \prod^\diamondsuit \overline{K_v(\theta_j)}$ where $\overline{K_v(\theta_j)} := K_v(\theta_j) \otimes_{K_v} \overline{K}_v$. 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's. Then the map N_* in Figure 4.1 factors as the composite of $\prod^\diamondsuit N_j$ and ν_*.

We have the following commutative diagram

$$\begin{array}{ccccccc}
H^2(K_v, \mu_2(\overline{A}_v)) = & \prod^\diamondsuit H^2(K_v, \mu_2(\overline{K_v(\theta_j)})) & \xrightarrow{\prod^\diamondsuit N_j} & \prod^\diamondsuit H^2(K_v, \mu_2) & \xrightarrow{\nu_*} & H^2(K_v, \mu_2) \\
\downarrow r & \downarrow \prod^\diamondsuit r_j & (5) & \downarrow \prod^\diamondsuit \mathrm{inv} & (6) & \downarrow \mathrm{inv} \\
H^2(A_v, \mu_2) = & \prod^\diamondsuit H^2(K_v(\theta_j), \mu_2) & \xrightarrow{\prod^\diamondsuit \mathrm{inv}_j} & \prod^\diamondsuit \mu_2 & \xrightarrow{\nu} & \mu_2.
\end{array}$$

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

Lemma 4.7. *Let X_j be the* $\mathrm{Gal}(\overline{K}_v/K_v)$*-orbit of T_j. There is a commutative diagram*

$$\begin{array}{ccc}
H^2(K_v, \mathrm{Map}(X_j, \mu_{2^\infty})) & \xrightarrow{N_j} & H^2(K_v, \mu_{2^\infty}) \\
r_j \downarrow \cong & & \downarrow \mathrm{inv} \\
H^2(K_v(\theta_j), \mu_{2^\infty}) & \xrightarrow{\mathrm{inv}_j} & \mathbb{Q}/\mathbb{Z}.
\end{array}$$

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 $\mathrm{Br}(K_v)[2^\infty] \to \mathrm{Br}(K_v(\theta_j))[2^\infty]$. By [9, §1 Theorem 3] it is multiplication by d_j on the invariants, where $d_j = [K_v(\theta_j) : K_v] = \#X_j$, and therefore surjective. Since r_j is an isomorphism, 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,§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 4.8. *Diagram (4) in Figure 4.1 is commutative.*

Proof. This is [8, XIV.2 Prop. 5] applied to each constituent field of A_v. □

Lemmas 4.4, 4.5, 4.6, 4.8 together prove Theorem 4.2. Composing the maps in the last row of (4.1) gives the pairing $(\ ,\ )_{A_v}$ defined at the end of Section 3. Identifying $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ with μ_2 we obtain

Corollary 4.9. *Let $s, s' \in H^1(K_v, E[2])$. We have $\langle s, s'\rangle_{\mathrm{inv}\circ\cup_e, v} = (k\circ r\circ w(s), k\circ r\circ w(s'))_{A_v}$.*

Remark 4.10. It would be useful to have an analogue of Corollary 4.9 for elements of $H^1(K_v, E[n])$ for general n (or at least for n prime). Lemma 4.4 depends on the equality in Lemma 4.3, which in turn only works for $n = 2$. This prevents any obvious generalisation to other values of n. Another difficulty is that we use $\mu_2 \subset K_v$ in our proofs.

5. The main theorem

Let C be a torsor under E, and $f \in A \otimes_K K(C)$ as described in Section 3. Let $\pi : D \to C$ be the 2-covering obtained by setting each f_j equal to the square of an indeterminate. The following lemma is a variant of [7, Theorem 2.3].

Lemma 5.1. *We have $(k \circ r \circ w)(\delta_\pi(P)) = f(P) \mod (A^\times)^2$ for all $P \in C(K)$, away from the zeroes and poles of the f_j.*

Proof. Let $Q \in D(\overline{K})$ with $\pi(Q) = P$. It suffices to show that $f_j(P) = k_j r_j w(dQ) \mod (K(\theta_j)^\times)^2$.

We have $r_j w(dQ) = (\sigma \mapsto e_2({}^\sigma Q - Q, T_j))$ in $H^1(K(\theta_j), \mu_2)$. The construction of D gives that $f_j \circ \pi = t_j^2$ for some rational function t_j on D, defined over $K(\theta_j)$. We claim that $e_2(S, T_j) = t_j(S + X)/t_j(X)$ for any $X \in D(\overline{K})$ for which the numerator and denominator are well-defined and non-zero. Indeed, since the Weil pairing is a geometric construction we may identify D and E over $\overline{K}$. This is an identification as torsors under E, so the action of E on D is identified with the group law on E. Then π is the multiplication-by-2 map on E, and our claim reduces to the definition of the Weil pairing in [11, Chapter III, §8].

Putting $S = {}^\sigma Q - Q$ and $X = Q$ gives $e_2({}^\sigma Q - Q, T_j) = t_j({}^\sigma Q)/t_j(Q) = {}^\sigma(t_j(Q))/t_j(Q)$ for any $\sigma \in \mathrm{Gal}(K(\theta_j)/K)$. Then $r_j w(dQ) = (\sigma \mapsto {}^\sigma(t_j(Q))/t_j(Q))$ and $k_j r_j w(dQ) = t_j^2(Q) = f_j\pi(Q) = f_j(P)$. □

As usual we identify $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ with μ_2.

Theorem 5.2. *Let K be a number field and E an elliptic curve over K. Let $a \in S^m(K, E)$ and $a' \in S^2(K, E)$. We have $\langle a, a'\rangle_{\mathrm{Cas}} = \langle a, a'\rangle_2 = \langle a, a'\rangle_1 = \langle a, a'\rangle_{\mathrm{CT}}$.*

Proof. The identification $\langle a, a'\rangle_{\mathrm{Cas}} = \langle a, a'\rangle_2$ is immediate from Corollary 4.9 and the local analogue of Lemma 5.1. The other identifications were established in Section 2. □

References

[1] K.S. Brown, *Cohomology of groups*, GTM 87, Springer-Verlag, 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, Inc., Boston, Mass, 1986.

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

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

[8] J-P. Serre, *Local fields*, Springer-Verlag, New York, 1979.

[9] J-P. Serre, Local class field theory, in J.W.S. Cassels and A. Fröhlich (eds), *Algebraic Number Theory*, Academic Press, London, 1967, 129–161.

[10] J-P. Serre, *Galois cohomology*, Springer-Verlag, Berlin, 2002.

[11] J.H. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, New York, 1992.

[12] S. Stamminger, *Explicit 8-descent on elliptic curves*, PhD thesis, International University Bremen, 2005.

[13] H.P.F. Swinnerton-Dyer, 2^n*-descent on elliptic curves for all* n, draught, January 2007.

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

E-mail address: T.A.Fisher@dpmms.cam.ac.uk

Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, CA 95053, USA

E-mail address: eschaefer@scu.edu

School of Engineering and Science, Jacobs University Bremen, P.O.Box 750561, 28725 Bremen, Germany

E-mail address: m.stoll@jacobs-university.de