SELF CUP PRODUCTS AND THE THETA CHARACTERISTIC TORSOR

BJORN POONEN AND ERIC RAINS

Abstract. We give a general formula relating self cup products in cohomology to connecting maps in nonabelian cohomology, and apply it to obtain a formula for the self cup product associated to the Weil pairing.

1. Introduction

We prove a general statement about cohomology, Theorem 2.5 that reinterprets the self cup product map

\[ H^1(M) \to H^2(M \otimes M) \]
\[ x \mapsto x \cup x \]

as the connecting map of cohomology for a certain sequence

\[ 1 \to M \otimes M \to \mathbb{U} M \to M \to 1 \]

involving a canonical nonabelian central extension \( \mathbb{U} M \). The proof of Theorem 2.5 can be read with group cohomology in mind, but we prove it for an arbitrary site since later we need it for fppf cohomology. The sheaf \( \mathbb{U} M \) has other properties as well: for example, there is a map \( M \to (\mathbb{U} M)^{ab} \) that is universal for quadratic maps from \( M \) to a (variable) abelian sheaf.

As an application of Theorem 2.5, we answer a question of B. Gross, who asked when the self cup product associated to the Weil pairing on the 2-torsion of the Jacobian \( A := \text{Jac} X \) of a curve \( X \) is 0. The Weil pairing


induces a symmetric bilinear pairing

\[ \langle , \rangle : H^1(A[2]) \times H^1(A[2]) \to H^2(\mathbb{G}_m). \]

We prove the identity

\[ \langle x, x \rangle = \langle x, c_T \rangle, \]  \hspace{1cm} (1)

where \( c_T \) is a particular canonical element of \( H^1(A[2]) \). Namely, \( c_T \) is the class of the torsor under \( A[2] \) parametrizing the theta characteristics on \( X \).

We have been vague about the field of definition of our curve; in fact, it is not too much harder to work over an arbitrary base scheme. (See Theorem 3.9) Moreover, we prove a
version with Jacobians replaced by arbitrary abelian schemes $A$, in which $c_T$ is replaced by
an element $c_\lambda \in H^1(\hat{\mathbb{A}}[2])$. (See Theorem 3.4.)

With a view to applications of these theorems, we give many criteria for the vanishing of
$c_\lambda$ and $c_T$, some of which generalize earlier results of M. Atiyah and D. Mumford: see
Proposition 3.6 and Remark 3.10. We also give an example over $\mathbb{Q}$ for which $c_T \neq 0$, and
an example over $\mathbb{Q}$ for which $c_T$ is nonzero but locally trivial.

As further motivation, some of our results, namely Proposition 2.9, Proposition 3.6, and
Theorem 3.5 are used in [PR12] to study the distribution of Selmer groups.

2. Some homological algebra

2.1. A tensor algebra construction. We will define a functor $U$ from the category of
$\mathbb{Z}$-modules to the category of groups, the goal being Theorem 2.5. Let $M$ be a $\mathbb{Z}$-module.
Let $TM = \bigoplus_{i \geq 0} T^i M$ be the tensor algebra. Then $T^{\geq n} M = \bigoplus_{i \geq n} T^i M$ is a 2-sided ideal of
$TM$. Let $T^{< n} M$ be the quotient ring $TM/T^{\geq n} M$. Let $UM$ be the kernel of $(T^{< 3} M)^\times \to (T^{< 1} M)^\times = \mathbb{Z}^\times = \{\pm 1\}$. The grading on $TM$ gives rise to a filtration of $UM$, which yields the
following central extension of groups

$$1 \to M \otimes M \to UM \xrightarrow{\pi} M \to 1. \quad (2)$$

Elements of $UM$ may be written as $1 + m + t$ where $m \in M$ and $t \in M \otimes M$, and should be
multiplied as follows:

$$(1 + m + t)(1 + m' + t') = 1 + (m + m') + ((m \otimes m') + t + t').$$

The surjection $UM \to M$ admits a set-theoretic section $s: M \to UM$ sending $m$ to $1 + m$.
If $m, m' \in M$, then

$$s(m) s(m') s(m + m')^{-1} = m \otimes m' \quad (3)$$

in $M \otimes M \subseteq UM$.

A simple computation verifies the following universal property of $UM$:

**Proposition 2.1.** The map $s: M \to UM$ is universal for set maps $\sigma: M \to G$ to a group
$G$ such that $(m, m') \mapsto \sigma(m)\sigma(m')\sigma(m + m')^{-1}$ is a bilinear function from $M \times M$ to an
abelian subgroup of $G$.

A quadratic map $q: M \to G$ is a set map between abelian groups such that $(m, m') \mapsto q(m + m') - q(m) - q(m')$ is bilinear. (Perhaps “pointed quadratic map” would be better
terminology; for instance, the quadratic maps $q: \mathbb{Q} \to \mathbb{Q}$ are the polynomial functions of
degree at most 2 sending 0 to 0.) Proposition 2.1 implies:

**Corollary 2.2.** The map $M \to (UM)^{ab}$ is universal for quadratic maps from $M$ to an
abelian group. The map $M \to (UM)^{ab} \otimes \mathbb{F}_2$ is universal for quadratic maps from $M$ to an
abelian group such that the image is killed by 2.

**Remark 2.3.**

(a) The commutator $[1 + m + t, 1 + m' + t]$, equals $m \otimes m' - m' \otimes m$, so we have an exact
sequence of abelian groups

$$0 \to S^2 M \to (UM)^{ab} \to M \to 0.$$
where \( SM = \bigoplus_{n \geq 0} S^n M \) is the symmetric algebra. In particular,
\[
(UM)^{ab} \simeq \ker \left( (S^{<3} M)^{\times} \to (S^{<1} M)^{\times} \right).
\]

(b) Similarly, if \( 2M = 0 \), then \( (1 + m + t)^2 = 1 + m \otimes m \), so we obtain an exact sequence of \( \mathbb{F}_2 \)-vector spaces
\[
0 \to \bigwedge^2 M \to (UM)^{ab} \otimes \mathbb{F}_2 \to M \to 0,
\]
and
\[
(UM)^{ab} \otimes \mathbb{F}_2 \simeq \ker \left( \bigwedge^{<3} M^{\times} \to \bigwedge^{<1} M^{\times} \right).
\]

2.2. Sheaves of groups. In the rest of Section 2, \( \mathcal{C} \) is a site. Let \( \mathfrak{S} \mathfrak{p}_C \) be the category of sheaves of groups on \( \mathcal{C} \), and let \( \mathfrak{A} \mathfrak{b}_C \) be the category of sheaves of abelian groups on \( \mathcal{C} \). For \( M \in \mathfrak{A} \mathfrak{b}_C \), write \( H^i(M) \) for \( \text{Ext}^i(\mathcal{Z}, M) \), where \( \mathcal{Z} \) is the constant sheaf; in other words, \( H^i(\mathcal{Z}) \) is the \( i \)th right derived functor of \( \text{Hom}(\mathcal{Z}, \mathcal{-}) \) on \( \mathfrak{A} \mathfrak{b}_C \). For \( M \in \mathfrak{S} \mathfrak{p}_C \), define \( H^0(M) = \text{Hom}(\mathcal{Z}, M) \) and define \( H^1(M) \) in terms of torsors as in [Gir71, \S III.2.4]. The definitions are compatible for \( M \in \mathfrak{A} \mathfrak{b}_C \) and \( i = 0,1 \) [Gir71, Remarque III.3.5.4].

Remark 2.4. The reader may prefer to imagine the case for which sheaves are \( G \)-sets for some group \( G \), abelian sheaves are \( \mathbb{Z}G \)-modules, and \( H^i(M) \) is just group cohomology.

All the constructions and results of Section 2.1 have sheaf analogues. In particular, for \( M \in \mathfrak{A} \mathfrak{b}_C \) we obtain \( \mathfrak{A} \mathfrak{b} M \in \mathfrak{S} \mathfrak{p}_C \) fitting in exact sequences
\[
1 \to M \otimes M \to \mathfrak{A} \mathfrak{b} M \to M \to 1 \tag{4}
\]
and, if \( 2M = 0 \),
\[
0 \to \bigwedge^2 M \to (\mathfrak{A} \mathfrak{b} M)^{ab} \to M \to 0. \tag{6}
\]

2.3. Self cup products.

Theorem 2.5. For \( M \in \mathfrak{A} \mathfrak{b}_C \), the connecting map \( H^1(M) \to H^2(M \otimes M) \) induced by (4) (see [Gir71, \S IV.3.4.1]) maps each \( x \) to \( x \cup x \).

Proof. Let \( x \in H^1(M) = \text{Ext}^1(\mathcal{Z}, M) \). Let
\[
0 \to M \to X \xrightarrow{\alpha} \mathcal{Z} \to 0 \tag{7}
\]
be the corresponding extension. Let \( X_1 := \alpha^{-1}(1) \), which is a sheaf of torsors under \( M \).

We will construct a commutative diagram
\[
\begin{array}{ccccccccc}
1 & \to & M \otimes M & \to & \mathfrak{A} \mathfrak{b} M & \xrightarrow{\pi} & M & \to & 1 \\
& \downarrow & & \downarrow & & \downarrow & & & \\
1 & \to & M \otimes M & \to & G & \xrightarrow{\delta} & G' & \to & 1 \\
& \downarrow & & \downarrow & & \downarrow & & & \\
0 & \to & M \otimes M & \to & X \otimes M & \xrightarrow{\epsilon} & M & \to & 0
\end{array}
\]
of sheaves of groups, with exact rows. The first row is (4). The last row, obtained by tensoring (7) with \( M \), is exact since \( \mathcal{Z} \) is flat. Let \( G \) be the sheaf of \((u, t) \in \mathfrak{A} \mathfrak{b} M \oplus (X \otimes M)\) such that \( \pi(u) = \epsilon(t) \) in \( M \). The vertical homomorphisms emanating from \( G \) are the two...
homomorphism is \( y \). Under the connecting homomorphism \( H \) connecting map \( H \) of the form \( 1 + m - e \otimes m + t \) with \( m \in M \) and \( t \in M \otimes M \). The vertical homomorphisms emanating from \( G' \) are induced by the map \( G \to M \) sending \( (u, t) \) to \( \pi(u) = \epsilon(t) \).

A calculation shows that \( 1 + X_1 + M \otimes M \) is a right torsor \( X' \) under \( G' \), corresponding to some \( x' \in H^1(G') \). Moreover, \( \mathcal{U} X \to X \) restricts to a torsor map \( X' \to X_1 \) compatible with \( G' \to M \), so \( H^1(G') \to H^1(M) \) sends \( x' \) to \( x \).

By [Gir71, §IV.3.4.1.1], the commutativity of \( 8 \) shows that the image of \( x \) under the connecting map \( H^1(M) \to H^2(M \otimes M) \) from the first row, equals the image of \( x' \) under the connecting map \( H^1(G') \to H^2(M \otimes M) \) from the second row, which equals the image of \( x \) under the connecting homomorphism \( H^1(M) \to H^2(M \otimes M) \) from the third row. This last homomorphism is \( y \to x \cup y \), so it maps \( x \) to \( x \cup x \) (cf. [Yon58], which explains this definition of \( x \cup y \) for extensions of modules over a ring).

**Example 2.6.** If \( M = \mathbb{Z}/2\mathbb{Z} \), then \( [4] \) is the sequence of constant sheaves

\[
0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0,
\]

which induces the Bockstein morphism \( H^1(X, \mathbb{Z}/2\mathbb{Z}) \to H^2(X, \mathbb{Z}/2\mathbb{Z}) \). So Theorem 2.5 recovers the known result that for any topological space \( X \), the self-cup-product \( H^1(X, \mathbb{Z}/2\mathbb{Z}) \to H^2(X, \mathbb{Z}/2\mathbb{Z}) \) is the Bockstein morphism. (See properties (5) and (7) of Steenrod squares in Section 4.L of [Hat10].)

**Remark 2.7.** In group cohomology, if we represent a class in \( H^1(M) \) by a cochain \( \zeta \), then one can check that the coboundary of \( s \circ \zeta \) equals the difference of \( \zeta \cup \zeta \) and the image of \( \zeta \) under the connecting map. A similar argument using Čech cochains gives an alternate proof of the general case of Theorem 2.5 as we now explain.

By [Gir71, Théorème 0.2.6], we may replace \( C \) by a site with one having an equivalent topos in order to assume that \( C \) has finite fiber products, and in particular, a final object \( S \). Then the natural map \( \check{H}^1(M) \to H^1(M) \) is an isomorphism [Gir71, Remarque III.3.6.5(5)], so any \( x \in H^1(M) \) is represented by a 1-cocycle \( m \) for some covering \( (S'_i \to S)_{i \in I} \). For simplicity, let us assume that the covering consists of one morphism \( S' \to S \) (the general case is similar). Let \( S'' = S' \times S \), and \( S''' = S' \times S' \times S' \). Let \( \pi_{23}, \pi_{13}, \pi_{12} : S''' \to S'' \) be the projections. So \( m \in M(S''') \) satisfies \( \pi_{13} m = \pi_{12} m + \pi_{23} m \). Applying the section \( M \to \mathcal{U} M \) yields a 1-cocohain \( 1 + m \in (\mathcal{U} M)(S''') \). Its 2-coboundary in \( (M \otimes M)(S''') \subset (\mathcal{U} M)(S''') \) represents the image of \( x \) under the connecting map \( H^1(M) \to H^2(M \otimes M) \) [Gir71, Corollaire IV.3.5.4(ii)]. On the other hand, the definition of the 2-coboundary given in [Gir71, Corollaire IV.3.5.4] together with \( [5] \) shows that it is \( \pi_{12} m \otimes \pi_{23} m \in (M \otimes M)(S''') \), whose class in \( H^2(M \otimes M) \) represents \( x \cup x \), by definition.

Let \( M, N \in \mathfrak{Ab}_C \). Let \( \beta \in H^0(\text{Hom}(M \otimes M, N)) \). (The bold face in \( \text{Hom}, \text{Ext} \), etc., indicates that we mean the sheaf versions.) Using \( \beta \), construct an exact sequence

\[
0 \to N \to \mathcal{U}_\beta \to M \to 0
\]

(9)
as the pushout of \( [4] \) by \( \beta : M \otimes M \to N \).

If \( \beta \) is symmetric, then \( \mathcal{U}_\beta \) is abelian, and we let \( \epsilon_\beta \) be the class of \( [9] \) in \( \text{Ext}^1(M, N) \). If \( \beta \) is symmetric and \( \text{Ext}^1(M, N) = 0 \), then applying \( \text{Hom}(-, N) \) to \( [5] \) yields

\[
0 \to \text{Hom}(M, N) \to \text{Hom}((\mathcal{U} M)^{\text{ab}}, N) \to \text{Hom}(S^2 M, N) \to 0
\]
and a connecting homomorphism sends $\beta \in H^0(\text{Hom}(S^2M, N))$ to an element $c_\beta \in H^1(\text{Hom}(M, N))$.

**Corollary 2.8.** Then the following maps $H^1(M) \to H^2(N)$ are the same, when defined:

(a) The composition

$$H^1(M) \xrightarrow{\Delta} H^1(M) \times H^1(M) \xrightarrow{\cup} H^2(M \otimes M) \xrightarrow{\beta} H^2(N).$$

(b) The connecting homomorphism $H^1(M) \to H^2(N)$ associated to $\beta$.

(c) The pairing with $\epsilon_\beta$ under the Yoneda product

$$\text{Ext}^1(M, N) \times H^1(M) \to H^2(N)$$

(if $\beta$ is symmetric).

(d) The pairing with $c_\beta$ under the evaluation cup product

$$H^1(\text{Hom}(M, N)) \times H^1(M) \to H^2(N)$$

(if $\beta$ is symmetric and $\text{Ext}^1(M, N) = 0$).

**Proof.** Theorem 2.5 and functoriality implies the equality of (a) and (b). Standard homological algebra gives equality of (b), (c), and (d). \qed

2.4. Commutator pairings.

**Proposition 2.9.** Let $1 \to A \to B \xrightarrow{p} C \to 1$ be an exact sequence in $\mathcal{E}_p_C$, with $A$ central in $B$, and $C$ abelian. Let $q : H^1(C) \to H^2(A)$ be the connecting map. Given $c_1, c_2 \in C$, we can lift them locally to $b_1, b_2$ and form their commutator $[b_1, b_2] := b_1 b_2^{-1} b_1^{-1} b_2^{-1} \in A$; this induces a homomorphism $[ , ] : C \otimes C \to A$. For $\gamma_1, \gamma_2 \in H^1(C)$, we have that $q(\gamma_1 + \gamma_2) - q(\gamma_1) - q(\gamma_2)$ equals the image of $-\gamma_1 \cup \gamma_2$ under the homomorphism $H^2(C \otimes C) \to H^2(A)$ induced by $[ , ]$.

**Proof.** That the commutator induces a homomorphism is a well-known simple computation. Pulling back $1 \to A^3 \to B^3 \to C^3 \to 1$ by the homomorphism $C^2 \to C^3$ sending $(c_1, c_2)$ to $(c_1, c_2, c_1 + c_2)$ and then pushing out by the homomorphism $A^3 \to A$ sending $(a_1, a_2, a_3)$ to $a_3 - a_2 - a_1$ yields an exact sequence $1 \to A \to Q \to C^2 \to 1$. Here $Q = B'/B''$ where $B'$ is the subgroup sheaf of $(b_1, b_2, b_3) \in B^3$ satisfying $\rho(b_3) = \rho(b_1) + \rho(b_2)$, and $B''$ is the subgroup sheaf of $B^3$ generated by sections $(a_1, a_2, a_3) \in A^3$ with $a_3 = a_1 + a_2$. The surjection $Q \to C^2$ admits a section $\sigma : C^2 \to Q$ defined locally as follows: given $(c_1, c_2)$ lifting to $(b_1, b_2) \in B^2$, send it to the image of $(b_1, b_2, b_1 b_2)$ in $Q$ (this is independent of the choice of lifts, since we work modulo $B''$). A calculation shows that

$$\sigma((c_1', c_2')) \sigma((c_1, c_2) + (c_1', c_2'))^{-1} \sigma((c_1, c_2)) = [c_1', c_2^{-1}] = [-[c_1', c_2]$$

in $A$, and the three factors on the left may be rotated since the right hand side is central in $Q$. Proposition 2.1 and (10) yield the middle vertical map in the commutative diagram

$$1 \to C^2 \otimes C^2 \xrightarrow{\nabla} \mathcal{H}(C^2) \to C^2 \to 1$$

with exact rows, and the left vertical map sends $(c_1, c_2) \otimes (c_1', c_2')$ to $-[c_1, c_2]$. The connecting map for the first row sends $(\gamma_1, \gamma_2) \in H^1(C^2)$ to $(\gamma_1, \gamma_2) \cup (\gamma_1, \gamma_2) \in H^2(C^2 \otimes C^2)$, by Theorem 2.5. The connecting map for the second row is a composition $H^1(C^2) \to H^1(C^3) \to$
the Néron-Severi group \( NS \) of global sections of \( \text{Hom}_{k}(H, k) \). Finally, the left vertical map sends \( (\gamma_1, \gamma_2) \cup (\gamma_1, \gamma_2) \in H^2(C^2 \otimes C^2) \) to the image of \(-\gamma_1 \cup \gamma_2 \) under the commutator pairing \( H^2(C \otimes C) \rightarrow H^2(A) \). So compatibility of the connecting maps yields the result. \( \Box \)

**Remark 2.10.** Yu. Zarhin [Zar74] proved Proposition 2.9 in the special case of group cohomology, by an explicit calculation with cocycles. Using the approach of Remark 2.7, that argument can be adapted to give a second proof of Proposition 2.9 in the general case.

### 3. Abelian schemes

#### 3.1. The relative Picard functor

Let \( A \to S \) be an abelian scheme. Let \( \text{Pic}_{A/S} \) be its relative Picard functor on the big fppf site of \( S \). Trivialization along the identity section shows that \( \text{Pic}_{A/S}(T) \simeq \text{Pic}(A \times_S T)/\text{Pic} T \) for each \( S \)-scheme \( T \) (see Proposition 4 on page 204 of [BLR90]). We generally identify line sheaves with their classes in \( \text{Pic} \). For an \( S \)-scheme \( T \) and \( a \in A(T) \), let

\[
\tau_a: A_T \to A_T \quad x \mapsto a + x
\]

be the translation-by-\( a \) morphism. Given a line sheaf \( \mathcal{L} \) on \( A \), the theorem of the square implies that

\[
\phi_{\mathcal{L}}: A \to \text{Pic}_{A/S} \quad a \mapsto \tau_a^* \mathcal{L} \otimes \mathcal{L}^{-1}
\]

is a homomorphism. If we vary the base and vary \( \mathcal{L} \), we obtain a homomorphism of fppf-sheaves

\[
\text{Pic}_{A/S} \to \text{Hom}(A, \text{Pic}_{A/S}) \quad \mathcal{L} \mapsto \phi_{\mathcal{L}}.
\]

Its kernel is denoted \( \text{Pic}^0_{A/S} \). Using the fact that \( \text{Pic}_{A/S} \) is an algebraic space, and the fact that \( \text{Pic}^0_{A/S} \) is an open subfunctor of \( \text{Pic}_{A/S} \) (which follows from [SGA 6, Exposé XIII, Théorème 4.7]), one can show that \( \text{Pic}^0_{A/S} \) is another abelian scheme \( \hat{A} \) over \( S \) [FC90, p. 3]. The image of \( \phi_{\mathcal{L}} \) is contained in \( \hat{A} \), so we may view \( \phi_{\mathcal{L}} \) as a homomorphism \( A \to \hat{A} \). Moreover, \( \phi_{\mathcal{L}} \) equals its dual homomorphism \( \phi_{\mathcal{L}_\tau} \). In fact, we have the following exact sequence of fppf-sheaves,

\[
0 \to \hat{A} \to \text{Pic}_{A/S} \to \text{Hom}_{\text{self-dual}}(A, \hat{A}) \to 0,
\]

in which the surjectivity of the last map \( \mathcal{L} \mapsto \phi_{\mathcal{L}} \) is [DP94, Proposition 1.2].

**Remark 3.1.** Let \( k \) be a field, let \( k_s \) be a separable closure contained in an algebraic closure \( \overline{k} \), and let \( G_k = \text{Gal}(k_s/k) \). For an abelian variety \( A \) over \( k \), the group \( \text{Hom}_{\text{self-dual}}(A, \hat{A}) \) of global sections of \( \text{Hom}_{\text{self-dual}}(A, \hat{A}) \) may be identified with the \( G_k \)-invariant subgroup of the Néron-Severi group \( NS A_{k_s} \). (For the case \( k = \overline{k} \) see [Mum70], in particular Corollary 2 on page 178 and Theorem 2 on page 188 and the remark following it. The general case follows because any homomorphism defined over \( \overline{k} \) is in fact defined over \( k_s \), since it maps the Zariski-dense set of prime-to-\( (\text{char } k) \) torsion points in \( A(k_s) \) to points in \( \hat{A}(k_s) \).)

For any homomorphism of abelian schemes \( \lambda: A \to B \), let \( A[\lambda] := \ker \lambda \).
3.2. Symmetric line sheaves. Multiplication by an integer \( n \) on \( A \) induces a pullback homomorphism \([n]*: \text{Pic}_{A/S} \to \text{Pic}_{A/S}\). Let \( \text{Pic}_{A/S}^{\text{Sym}} \) be the kernel of \([-1]^* - [1]^* \) on \( \text{Pic}_{A/S} \).

More concretely, because \( A \to S \) has a section, we have \( \text{Pic}_{A/S}^{\text{Sym}}(T) = \text{Pic}_{A/S}^{\text{Sym}}(A \times_S T)/\text{Pic} T \) for each \( S \)-scheme \( T \), where \( \text{Pic}_{A/S}^{\text{Sym}}(A \times_S T) \) is the group of isomorphism classes of symmetric line sheaves on \( A \times_S T \). Since \([-1]^* \) acts as \(-1\) on \( \hat{A} \) and as \(+1\) on \( \text{Hom}_{\text{self-dual}}(A, \hat{A}) \), and since multiplication-by-2 on \( \hat{A} \) is surjective, the snake lemma applied to \([-1]^* - [1]^* \) acting on (13) yields an exact sequence

\[
0 \to \hat{A}[2] \to \text{Pic}_{A/S}^{\text{Sym}} \to \text{Hom}_{\text{self-dual}}(A, \hat{A}) \to 0. \tag{14}
\]

3.3. The Weil pairing. We recall some facts and definitions that can be found in [Pol03, §10.4], for example. (In that book, \( S \) is Spec \( k \) for an algebraically closed field \( k \), but the arguments there apply also to \( T \)-valued points of abelian schemes over an arbitrary base scheme \( S \), functorially in the \( S \)-scheme \( T \), so by Yoneda’s lemma they yield the desired results over \( S \).) Given an abelian scheme \( A \) over \( S \), there is a Weil pairing

\[
e_2: A[2] \times \hat{A}[2] \to \mathbb{G}_m. \tag{15}
\]

For any homomorphism \( \lambda: A \to \hat{A} \), define \( e_2^\lambda: A[2] \times A[2] \to \mathbb{G}_m \) by \( e_2^\lambda(x, y) = e_2(x, \lambda y) \). If \( \mathcal{L} \in \text{Pic}_{A/S}(\hat{S}) \), let \( e_2^\mathcal{L} = e_2^{\mathcal{L} \cdot} \); this is an alternating bilinear pairing, and hence it is also symmetric.

3.4. Quadratic refinements of the Weil pairing.

**Proposition 3.2.** There is a (not necessarily bilinear) pairing of fppf sheaves

\[
q: A[2] \times \text{Pic}_{A/S}^{\text{Sym}} \to \mu_2 \subseteq \mathbb{G}_m
\]

such that:

(a) The pairing is additive in the second argument: \( q(x, \mathcal{L} \otimes \mathcal{L}') = q(x, \mathcal{L})q(x, \mathcal{L}') \).

(b) The restriction of \( q \) to a pairing

\[
q: A[2] \times \hat{A}[2] \to \mathbb{G}_m
\]

is the Weil pairing \( e_2 \). In particular, this restriction is bilinear.

(c) In general, \( q(x + y, \mathcal{L}) = q(x, \mathcal{L})q(y, \mathcal{L})e_2^\mathcal{L}(x, y) \).

**Proof.** This is essentially proved in [Pol03, §13.1]. The book [Pol03] assumes that \( S = \text{Spec } k \) for an algebraically closed field \( k \), but again (as in Section 3.3) the arguments there apply to scheme-valued points in the general case, so Yoneda’s lemma completes the proof. \( \square \)

We can summarize Proposition 3.2 in the commutative diagram

\[
\begin{array}{cccccc}
0 & \longrightarrow & \hat{A}[2] & \longrightarrow & \text{Pic}_{A/S}^{\text{Sym}} & \longrightarrow & \text{Hom}_{\text{self-dual}}(A, \hat{A}) & \longrightarrow & 0 \\
& & \downarrow e_2 & & \downarrow q & & \downarrow e_2^\bullet & & \\
0 & \longrightarrow & \text{Hom}(A[2], \mathbb{G}_m) & \longrightarrow & \text{Hom}((\mathcal{W} A[2])^{\text{ab}} \otimes \mathbb{F}_2, \mathbb{G}_m) & \longrightarrow & \text{Hom}(\wedge^2 A[2], \mathbb{G}_m) & \longrightarrow & 0, \\
\end{array}
\tag{16}
\]

which we now explain. The top row is (14). The bottom row is obtained by applying \( \text{Hom}(\cdot, \mathbb{G}_m) \) to (6) for \( M = A[2] \), and using \( \text{Ext}^1(A[2], \mathbb{G}_m) = 0 \). The vertical maps are the
map $y \mapsto e_2(-, y)$, the map sending $\mathcal{L}$ to the homomorphism $(\mathcal{W} A[2])^\text{ab} \otimes \mathbb{F}_2 \to \mathbb{G}_m$ corresponding to $q(-, \mathcal{L})$ (see Corollary 2.2), and the map $\lambda \mapsto e_2^\lambda$, respectively. Commutativity of the two squares are given by (b) and (c) in Proposition 3.2, respectively.

The top row of (16) gives a homomorphism

$$\text{Hom}_{\text{self-dual}}(A, \hat{A}) \to \text{H}^1(\hat{A}[2])$$

$$\lambda \mapsto c_\lambda.$$  \hfill (17)

By definition, $c_\lambda$ may be interpreted geometrically as the class of the torsor under $\hat{A}[2]$ that parametrizes symmetric line sheaves $\mathcal{L}$ with $\phi_\mathcal{L} = \lambda$ (cf. [Pol03, §13.5]). Thus $c_\lambda$ is the obstruction to finding a map $y \mapsto e_2(-, y)$. If $k$ is a global field and $S = \text{Spec} k$, then this and [PS99, Corollary 2] imply that our $c_\lambda$ lies in the 2-Selmer group of $\hat{A}$.

**Theorem 3.4.** For any $\lambda \in \text{Hom}_{\text{self-dual}}(A, \hat{A})$ and any $x \in \text{H}^1(A[2])$, we have

$$x \cup c_\lambda = x \cup e_2$$ \hfill (18)

in $\text{H}^2(\mathbb{G}_m)$, where the cup products are induced by the pairings underneath.

**Proof.** The rightmost vertical map in (16) maps $\lambda$ to $e_2^\lambda$. These are mapped by the horizontal connecting homomorphisms to $c_\lambda \in \text{H}^1(\hat{A}[2])$ and $c_{e_2} \in \text{H}^1(\text{Hom}(A[2], \mathbb{G}_m))$, which are identified by the leftmost vertical map $e_2$. Apply Corollary 2.8 with $M = A[2]$, $N = \mathbb{G}_m$, and $\beta = e_2^\lambda$, using $\text{Ext}^1(A[2], \mathbb{G}_m) = 0$: map (a) gives the left hand side of (18) and map (d) gives the right hand side of (18) (written backwards) because of the identification of $c_\lambda$ with $c_{e_2}$. \hfill \Box

### 3.5. Criteria for triviality of the obstruction.

The following lemma serves only to prove Proposition 3.6(a) below.

**Lemma 3.5.** Let $k$ be a field, and let $G$ be a finite cyclic group.

(a) Let $A$ be a finite-dimensional $kG$-module. Let $A^* := \text{Hom}_k(A, k)$ be the dual representation, and let $A^G$ be the subspace of $G$-invariant vectors. Then $\dim A^G = \dim(A^*)^G$.

(b) If $0 \to A \to B \to C \to 0$ is an exact sequence of finite-dimensional $kG$-modules, and the surjection $B^* \to A^*$ admits a section as $G$-sets, then the connecting homomorphism $C^G \to \text{H}^1(G, A)$ is 0.

**Proof.**

(a) Let $g$ be a generator of $G$. If $M$ is a matrix representing the action of $g$ on $A$, the action of $g^{-1}$ on $A^*$ is given by the transpose $M^t$. Then $\dim A^G = \dim \ker(M - 1) = \dim \ker(M^t - 1) = \dim(A^*)^G$, where the middle equality uses the fact that a matrix has the same rank as its transpose.

(b) The section gives the 0 at the right in

$$0 \to \text{(C*)}^G \to \text{(B*)}^G \to \text{(A*)}^G \to 0.$$
Taking dimensions and applying \( a \) yields \( \dim B^G = \dim A^G + \dim C^G \). This together with the exactness of

\[
0 \to A^G \to B^G \to C^G \to H^1(G, A)
\]

implies that the connecting homomorphism \( C^G \to H^1(G, A) \) is 0. \( \square \)

**Proposition 3.6.** Let \( \lambda: A \to \widehat{A} \) be a self-dual homomorphism of abelian varieties over a field \( k \). Suppose that at least one of the following hypotheses holds:

(a) \( \text{char } k \neq 2 \) and the image \( G \) of \( G_k \to \text{Aut } A[2](k) \) is cyclic.
(b) \( k \) is a perfect field of characteristic 2.
(c) \( k \) is \( \mathbb{R} \) or \( \mathbb{C} \).
(d) \( k \) is a nonarchimedean local field of residue characteristic not 2, and \( A \) has good reduction (i.e., extends to an abelian scheme over the valuation ring of \( k \)).
(e) \( k \) is a finite field.
(f) \( \lambda(A[2]) \) is an étale group scheme of rank at most 4.

Then \( c_\lambda = 0 \).

**Proof.**

(a) Apply Lemma 3.5(b) to the bottom row of (16), viewed as a sequence of \( \mathbb{F}_2 G \)-modules; it applies since the dual sequence is (6) for \( M := A[2] \), and the section \( s \) of Section 2.1 yields a \( G \)-set section \( A[2] \to (\mathbb{U} A[2])^{ab} \otimes \mathbb{F}_2 \). Thus the top horizontal map in

\[
\begin{array}{ccc}
\text{H}^0(G, \text{Hom}(\bigwedge^2 A[2], \mathbb{G}_m)) & \longrightarrow & \text{H}^1(G, \widehat{A}[2]) \\
\downarrow & & \downarrow \\
\text{H}^0(G_k, \text{Hom}(\bigwedge^2 A[2], \mathbb{G}_m)) & \longrightarrow & \text{H}^1(G_k, \widehat{A}[2])
\end{array}
\]

is 0. Thus \( \delta = 0 \). Now (16) shows that \( c_\lambda = \delta(e_2^\lambda) = 0 \).

(b) Let \( M := A[2] \), and let \( M^\vee := \text{Hom}(M, \mathbb{G}_m) = \widehat{A}[2] \) be its Cartier dual. The bottom row of (16) yields an exact sequence

\[
\text{H}^0(\text{Hom}((\mathbb{U} M)^{ab} \otimes \mathbb{F}_2, \mathbb{G}_m)) \to \text{H}^0(\text{Hom}(\bigwedge^2 M, \mathbb{G}_m)) \to \text{H}^1(M^\vee).
\]

It suffices to prove that \( \delta = 0 \), or that the first map is surjective. Equivalently, by the universal property of \((\mathbb{U} M)^{ab} \otimes \mathbb{F}_2\), we need each alternating pairing \( b: M \times M \to \mu_2 \) to be \( q(x + y) - q(x) - q(y) \) for some quadratic map \( q: M \to \mu_2 \).

In fact, we will prove this for every finite commutative group scheme \( M \) over \( k \) with \( 2M = 0 \). Since \( k \) is perfect, there is a canonical decomposition \( M = M_{et} \oplus M_{et} \oplus M_{fl} \) into étale-local, local-étale, and local-local subgroup schemes. Then \( M^\vee = (M_{et})^\vee \oplus (M_{et})^\vee \oplus (M_{fl})^\vee \). The homomorphism \( M \to M^\vee \) induced by the alternating pairing must map \( M_{et} \) to \( (M_{et})^\vee \), and \( M_{et} \) to \( (M_{et})^\vee \), and \( M_{fl} \) to \( (M_{fl})^\vee \). In particular, \( b = b_e + b_{fl} \) where \( b_e \) and \( b_{fl} \) are alternating pairings on \( M_{et} \oplus M_{et} \) and \( M_{fl} \), respectively. The pairing \( b_e \) necessarily has the form

\[
(m_{et}, m_{et}), (m'_{et}, m'_{et}) \mapsto B(m_{et}, m'_{et})B(m'_{et}, m_{et})
\]

for some bilinear pairing \( B: M_{et} \times M_{et} \to \mu_2 \). Then \( b_e \) comes from the quadratic map \( (m_{et}, m_{et}) \mapsto B(m_{et}, m_{et}) \).
It remains to consider the case $M = M_\eta$. Then $M^\nu(k_\eta) = 0$. By Proposition III.6.1 and the paragraph preceding it, $H^1(M^\nu) = H^1(G_k, M^\nu(k_\eta)) = H^1(G_k, 0) = 0$, so $\delta = 0$.

(c) Follows from (a).

(d) The assumptions imply $k(A[2])$ is unramified over $k$ (see ST68 Theorem 1, for example), so (a) applies.

(e) Follows from (a) and (b).

(f) By definition of $e^\lambda_2$, the right kernel of $e^\lambda_2$ contains the kernel $K$ of $A[2] \xrightarrow{\lambda} \lambda(A[2])$. Since $e^\lambda_2$ is alternating, the left kernel of $e^\lambda_2$ contains $K$ too. Thus $e^\lambda_2$ induces a nondegenerate alternating pairing

\[ e': \lambda(A[2]) \times \lambda(A[2]) \to \mathbb{G}_m. \]

In particular, the étale group scheme $\lambda(A[2])$ has square order, which by assumption is 1 or 4. Let

\[ q': \lambda(A[2]) \to \mathbb{G}_m \]

be the morphism taking 0 to 1 and all other $k_\eta$-points of $\lambda(A[2])$ to $-1$. Then $q'$ is a quadratic form satisfying the identity $q'(x + y) - q'(x) - q'(y) = e'(x, y)$. Now $q := q' \circ \lambda$ is a quadratic form on $A[2]$ refining $e^\lambda_2$, so $c_\lambda = 0$. $\square$

3.6. Formula for the obstruction in the case of a line sheaf on a torsor. Let $P$ be a torsor under $A$. For $a \in A(S)$, let $\tau_a: P \to P$ be the translation. Also, for $x \in P(S)$, let $\tau_x: A \to P$ be the torsor action. The maps $\tau^*_x$ for local choices of sections $x$ induce a well-defined isomorphism $Pic^0_{P/S} \simeq Pic^0_{A/S}$ since any $\tau^*_a$ is the identity on $Pic^0_{A/S}$. Let $\mathcal{L} \in Pic_{P/S}(S)$. Generalizing (12), we define

\[ \phi_{\mathcal{L}}: A \to Pic^0_{P/S} \simeq Pic^0_{A/S} \]

\[ a \mapsto \tau^*_a \mathcal{L} \otimes \mathcal{L}^{-1}. \]

We may view $\phi_{\mathcal{L}}$ as an element of $Hom_{self-dual}(A, \hat{A})$. If $x \in P(S)$, then $\phi_{\tau^*_x \mathcal{L}} = \phi_{\mathcal{L}}$.

Proposition 3.7. Let $P$ be a torsor under $A$, equipped with an order-2 automorphism $\iota: P \to P$ compatible with $[-1]: A \to A$. The fixed locus $P^\iota$ of $\iota$ is a torsor under $A[2]$; let $c \in H^1(A[2])$ be its class. Let $\mathcal{L} \in Pic_{P/S}(S)$ be such that $\iota^* \mathcal{L} \simeq \mathcal{L}$, and let $\lambda = \phi_{\mathcal{L}}: A \to \hat{A}$. Then $c_\lambda = \lambda(c)$ in $H^1(\hat{A}[2])$.

Proof. If $x$ is a section of $P^\iota$, then $[-1]^{\ast} \tau^*_x \mathcal{L} \simeq \tau^*_x \iota^* \mathcal{L} \simeq \tau^*_x \mathcal{L}$, so we obtain a map

\[ \gamma: P^\iota \to Pic_{A/S}^{Sym} \]

\[ x \to \tau^*_x \mathcal{L}. \]

For sections $a \in A[2]$ and $x \in P^\iota$, we have

\[ \gamma(a + x) = \tau^*_a \iota^* \mathcal{L} = \tau^*_a (\iota^* \mathcal{L}) = \phi_{\iota^* \mathcal{L}}(a) \otimes \tau^*_x \mathcal{L} = \lambda(a) \otimes \gamma(x) \]

in $Pic_{A/S}^{Sym}$. In other words, $\gamma$ is a torsor map (with respect to $\lambda: A[2] \to \hat{A}[2]$) from the torsor $P^\iota$ (under $A[2]$) to the torsor (under $\hat{A}[2]$) of line sheaves in $Pic_{A/S}^{Sym}$ with Néron-Severi class $\lambda$. Taking classes of these torsors yields $\lambda(c) = c_\lambda$. $\square$
3.7. Application to Jacobians. Let \( X \to S \) be a family of genus-\( g \) curves, by which we mean a smooth proper morphism whose geometric fibers are integral curves of genus \( g \). (If \( g \neq 1 \), then the relative canonical sheaf or its inverse makes \( X \to S \) projective: see Remark 2 on page 252 of [BLR90].) By the statement and proof of Proposition 4 on page 260 of [BLR90],

\[
\begin{align*}
(1) \text{ There is a decomposition of functors } & \text{Pic}_{X/S} \simeq \bigsqcup_{n \in \mathbb{Z}} \text{Pic}^n_{X/S}.
(2) \text{ The subfunctor } & \text{Pic}^0_{X/S} \text{ is (represented by) a projective abelian scheme } A \text{ over } S.
(3) \text{ The subfunctor } & \text{Pic}^{g-1}_{X/S} \text{ is (represented by) a smooth projective scheme } P \text{ over } S, \text{ a torsor under } A. \text{ (If } g = 1, \text{ then } P = A.)
(4) \text{ The scheme-theoretic image of the “summing” map } X^{g-1} \to P \text{ is an effective relative Cartier divisor on } P \text{ (take this to be empty if } g = 0). \text{ Let } \Theta \text{ be the associated line sheaf on } P.
(5) \text{ The homomorphism } \lambda := \phi_\Theta : A \to \hat{A} \text{ is an isomorphism.}
(6) \text{ Define } \iota : P \to P \text{ by } \mathscr{T} \mapsto \omega_{X/S} \otimes \mathscr{T}^{-1}; \text{ then } \iota^* \Theta \simeq \Theta. \text{ (To prove this, one can reduce to the case where } S \text{ is a moduli scheme of curves with level structure, and then to the case where } S \text{ is the spectrum of a field, in which case it is a consequence of the Riemann-Roch theorem.)}
\end{align*}
\]

**Definition 3.8.** The theta characteristic torsor \( T \) is the closed subscheme of \( P = \text{Pic}^{g-1}_{X/S} \) parametrizing classes whose square is the canonical class \( \omega_{X/S} \in \text{Pic}^{2g-2}_X(S) \).

Equivalently, \( T = P^\chi \). Let \( c_T \in H^1(A[2]) \) be the class of this torsor.

**Theorem 3.9.** Let \( X \to S \) be a family of genus-\( g \) curves, and let \( A, \lambda, c_T \) be as above. Then \( c_\lambda = \lambda(c_T) \) in \( H^1(A[2]) \), and for any \( x \in H^1(A[2]) \) we have

\[
x \cup x = x \cup e_T \in H^2(\mathbb{G}_m).
\]

\( x \cup x = x \cup e_T \) holds for the Jacobian of any hyperelliptic curve \( X \) if it has a rational Weierstrass point or its genus is odd. In particular, this applies to \( y^2 = f(x) \) with \( f \) separable of degree \( n \neq 2 \) (mod 4) over a field of characteristic not 2.

\[
\begin{align*}
\text{(mod 4)}
\end{align*}
\]
Example 3.12. Suppose that $X$ is a genus 2 curve, the smooth projective model of $y^2 = f(x)$ where $f$ is a degree-6 separable polynomial over a field $k$ of characteristic not 2. Let $\Delta$ be the set of zeros of $f$ in $k$. As explained in [Mum71, p. 191], the group $A[2]$ and its torsor $T$ can be understood explicitly in terms of $\Delta$. Namely, for $m \in \mathbb{Z}/2\mathbb{Z}$, let $\mathcal{W}_m$ be the quotient of the sum-$m$ part of the permutation module $\mathbb{F}_2^{\Delta} \simeq \mathbb{F}_2^{2g+2}$ by the diagonal addition action of $\mathbb{F}_2$. Then the $G_k$-module $A[2]$ may be identified with $\mathcal{W}_0$, and its torsor $T$ may be identified with $\mathcal{W}_1$. Using this, one can show:

(a) For $f(x) = (x^2 + 1)(x^2 - 3)(x^2 + 3)$ over $\mathbb{Q}_3$, we have $c_T \neq 0$.

(b) For $f(x) = x^6 + x + 6$ over $\mathbb{Q}$, we have

$$0 \neq c_T \in \mathbb{H}_1(\mathbb{Q}, A[2]) := \ker \left( H^1(\mathbb{Q}, A[2]) \to \prod_{p \leq \infty} H^1(\mathbb{Q}_p, A[2]) \right).$$

(Proof: The discriminant of $f$ is $-\ell$, where $\ell$ is the prime 362793931. For $p \notin \{2, \ell\}$, the element $c_T$ maps to 0 in $H^1(\mathbb{Q}_p, A[2])$ by Proposition 3.6(c,d), and $f(x)$ has a zero in each of $\mathbb{Q}_2$ and $\mathbb{Q}_\ell$, so the same is true at those places. On the other hand, the Galois group of $f$ over $\mathbb{Q}$ is $S_6$, so $c_T \neq 0$.)

Acknowledgements

We thank Benedict Gross for the suggestion to look at the self cup product on $H^1(k, A[2])$ induced by the Weil pairing $e_2$ on a Jacobian. We also thank Brian Conrad and the referee for comments.

References


[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034) 3.7


[FC90] Gerd Faltings and Ching-Li Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 22, Springer-Verlag, Berlin, 1990. With an appendix by David Mumford. MR1083333 (92d:14036) 3.1


Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

E-mail address: poonen@math.mit.edu

URL: http://math.mit.edu/~poonen/

Department of Mathematics, California Institute of Technology, Pasadena, CA 91125

E-mail address: rains@caltech.edu