Open access • Journal Article • DOI:10.4310/MRL.2011.V18.N6.A18

Self cup products and the theta characteristic torsor — Source link

Bjorn Poonen, Eric M. Rains

Institutions: Massachusetts Institute of Technology, California Institute of Technology

Published on: 01 Nov 2011 - Mathematical Research Letters (International Press)

Topics: Nonabelian cohomology, Cup product, Cohomology, Weil pairing and Theta characteristic

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

$$\begin{aligned} H^1(M) &\to H^2(M \otimes M) \\ x &\mapsto x \cup x \end{aligned}$$

as the connecting map of cohomology for a certain sequence

$$1 \to M \otimes M \to \mathscr{U} M \to M \to 1$$

involving a canonical nonabelian central extension $\mathscr{U} M$. 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 $\mathscr{U} M$ has other properties as well: for example, there is a map $M \to (\mathscr{U} M)^{\mathrm{ab}}$ 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 about the self cup product associated to the Weil pairing on the 2-torsion of the Jacobian $A := \operatorname{Jac} X$ of a curve X. The Weil pairing

$$e_2 \colon A[2] \times A[2] \to \mathbb{G}_m$$

induces a symmetric bilinear pairing

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

We prove the identity

$$\langle x, x \rangle = \langle x, c_{\mathcal{T}} \rangle, \tag{1}$$

where $c_{\mathcal{T}}$ is a particular canonical element of $\mathrm{H}^1(A[2])$. Namely, $c_{\mathcal{T}}$ 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 $c_{\mathcal{T}}$ is replaced by an element $c_\lambda \in \mathrm{H}^1(\widehat{A}[2])$. (See Theorem 3.4.)

Date: April 10, 2011.
2010 *Mathematics Subject Classification.* Primary 18G50; Secondary 11G10, 11G30, 14G25, 14K15.
Key words and phrases. Weil pairing, theta characteristic, self cup product.
B. P. was partially supported by NSF grant DMS-0841321.

With an eye towards applications of these theorems, we give many criteria for the vanishing of c_λ and $c_{\mathcal{T}}$, 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 $\mathbb{Q}_3$ for which $c_{\mathcal{T}} \neq 0$, and an example over $\mathbb{Q}$ for which $c_{\mathcal{T}}$ is nonzero but locally trivial.

As further motivation, some of our results, namely Proposition 2.9 and Theorem 3.9, are used in [PR11] 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

$$1 \to M \otimes M \to UM \xrightarrow{\pi} M \to 1. \tag{2}$$

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 $s\colon M \to UM$ sending m to $1+m$. If $m, m' \in M$, then

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

in $M \otimes M \subseteq UM$.

A simple computation verifies the following universal property of UM:

Proposition 2.1. *The map $s\colon M \to UM$ is universal for set maps $\sigma\colon M \to G$ 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 $q\colon M \to G$ 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 $q\colon \mathbb{Q} \to \mathbb{Q}$ are the polynomial functions of degree at most 2 sending 0 to 0.) Proposition 2.1 implies:

Corollary 2.2. *The map $M \to (UM)^{\mathrm{ab}}$ is universal for quadratic maps from M to an abelian group. The map $M \to (UM)^{\mathrm{ab}} \otimes \mathbb{F}_2$ 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

$$0 \to S^2 M \to (UM)^{\mathrm{ab}} \to M \to 0,$$

where $SM = \bigoplus_{n \geq 0} S^n M$ is the symmetric algebra. In particular,

$$(UM)^{\mathrm{ab}} \simeq \ker\left((S^{<3}M)^\times \to (S^{<1}M)^\times\right).$$

(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

$$0 \to \bigwedge^2 M \to (UM)^{\mathrm{ab}} \otimes \mathbb{F}_2 \to M \to 0,$$

and

$$(UM)^{\mathrm{ab}} \otimes \mathbb{F}_2 \simeq \ker\left((\bigwedge^{<3} M)^\times \to (\bigwedge^{<1} M)^\times \right).$$

2.2. **Sheaves of groups.** In the rest of Section 2, $\mathcal{C}$ is a site. Let $\mathfrak{Gp}_{\mathcal{C}}$ be the category of sheaves of groups on $\mathcal{C}$, and let $\mathfrak{Ab}_{\mathcal{C}}$ be the category of sheaves of abelian groups on $\mathcal{C}$. For $M \in \mathfrak{Ab}_{\mathcal{C}}$, write $\mathrm{H}^i(M)$ for $\mathrm{Ext}^i(\mathbb{Z}, M)$, where $\mathbb{Z}$ is the constant sheaf; in other words, $\mathrm{H}^i(-)$ is the i^{th} right derived functor of $\mathrm{Hom}(\mathbb{Z}, -)$ on $\mathfrak{Ab}_{\mathcal{C}}$. For $M \in \mathfrak{Gp}_{\mathcal{C}}$, define $\mathrm{H}^0(M)$ as $\mathrm{Hom}(\mathbb{Z}, M)$ and define $\mathrm{H}^1(M)$ in terms of torsors as in [Gir71, §III.2.4]. The definitions are compatible for $M \in \mathfrak{Ab}_{\mathcal{C}}$ 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 $\mathrm{H}^i(M)$ is just group cohomology.

All the constructions and results of Section 2.1 have sheaf analogues. In particular, for $M \in \mathfrak{Ab}_{\mathcal{C}}$ we obtain $\mathscr{U} M \in \mathfrak{Gp}_{\mathcal{C}}$ fitting in exact sequences

$$1 \to M \otimes M \to \mathscr{U} M \to M \to 1 \tag{4}$$

$$0 \to S^2 M \to (\mathscr{U} M)^{\mathrm{ab}} \to M \to 0, \tag{5}$$

and, if $2M = 0$,

$$0 \to \bigwedge^2 M \to (\mathscr{U} M)^{\mathrm{ab}} \otimes \mathbb{F}_2 \to M \to 0. \tag{6}$$

2.3. **Self cup products.**

Theorem 2.5. *For $M \in \mathfrak{Ab}_{\mathcal{C}}$, the connecting map $\mathrm{H}^1(M) \to \mathrm{H}^2(M \otimes M)$ induced by* (4) *(see* [Gir71, §IV.3.4.1]*) maps each x to $x \cup x$.*

Proof. Let $x \in \mathrm{H}^1(M) = \mathrm{Ext}^1(\mathbb{Z}, M)$. Let

$$0 \to M \to X \xrightarrow{\alpha} \mathbb{Z} \to 0 \tag{7}$$

be the corresponding extension. Let $X_1 := \alpha^{-1}(1)$, which is a sheaf of torsors under M.

We will construct a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & M \otimes M \arrow[r] & \mathscr{U} M \arrow[r, "\pi"] & M \arrow[r] & 1 \\
1 \arrow[r] & M \otimes M \arrow[r] \arrow[u, equal] \arrow[d, equal] & G \arrow[r, "\delta"] \arrow[u] \arrow[d] & G' \arrow[r] \arrow[u] \arrow[d] & 1 \\
0 \arrow[r] & M \otimes M \arrow[r] & X \otimes M \arrow[r, "\epsilon"] & M \arrow[r] & 0
\end{tikzcd} \tag{8}$$

of sheaves of groups, with exact rows. The first row is (4). The last row, obtained by tensoring (7) with M, is exact since $\mathbb{Z}$ is flat. Let G be the sheaf of $(u, t) \in \mathscr{U} M \oplus (X \otimes M)$ such that $\pi(u) = \epsilon(t)$ in M. The vertical homomorphisms emanating from G are the two projections. Let $\delta \colon G \to \mathscr{U} X$ send (u, t) to $u - t$. Then $\ker \delta = M \otimes M$, embedded diagonally in G. Let $G' = \delta(G)$. Explicitly, if e is a section of X_1, then G' consists of sections of $\mathscr{U} X$

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 $x' \in \mathrm{H}^1(G')$. Moreover, $\mathscr{U}X \to X$ restricts to a *torsor* map $X' \to X_1$ compatible with $G' \to M$, so $\mathrm{H}^1(G') \to \mathrm{H}^1(M)$ 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 $\mathrm{H}^1(M) \to \mathrm{H}^2(M \otimes M)$ from the first row, equals the image of x' under the connecting map $\mathrm{H}^1(G') \to \mathrm{H}^2(M \otimes M)$ from the second row, which equals the image of x under the connecting homomorphism $\mathrm{H}^1(M) \to \mathrm{H}^2(M \otimes M)$ from the third row. This last homomorphism is $y \mapsto x \cup y$, 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). $\square$

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 $\mathrm{H}^1(X, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{H}^2(X, \mathbb{Z}/2\mathbb{Z})$. So Theorem 2.5 recovers the known result that for any topological space X, the self-cup-product $\mathrm{H}^1(X, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{H}^2(X, \mathbb{Z}/2\mathbb{Z})$ 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 $\mathrm{H}^1(M)$ by a cochain ζ, then one can check that the coboundary of $s \circ \zeta$ equals the difference of $\zeta \cup \zeta$ and the image of ζ 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 $\mathcal{C}$ by a site with one having an equivalent topos in order to assume that $\mathcal{C}$ has finite fiber products, and in particular, a final object S. Then the natural map $\check{\mathrm{H}}^1(M) \to \mathrm{H}^1(M)$ is an isomorphism [Gir71, Remarque III.3.6.5(5)], so any $x \in \mathrm{H}^1(M)$ 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 $S'' = S' \times_S S'$, and $S''' = S' \times_S S' \times_S S'$. Let $\pi_{23}, \pi_{13}, \pi_{12} \colon S''' \to S''$ be the projections. So $m \in M(S'')$ satisfies $\pi_{13}^* m = \pi_{12}^* m + \pi_{23}^* m$. Applying the section $M \to \mathscr{U}M$ yields a 1-cochain $1 + m \in (\mathscr{U}M)(S'')$. Its 2-coboundary in $(M \otimes M)(S''') \subseteq (\mathscr{U}M)(S''')$ represents the image of x under the connecting map $\mathrm{H}^1(M) \to \mathrm{H}^2(M \otimes M)$ [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 (3) shows that it is $\pi_{12}^* m \otimes \pi_{23}^* m \in (M \otimes M)(S''')$, whose class in $\mathrm{H}^2(M \otimes M)$ represents $x \cup x$, by definition.

Let $M, N \in \mathfrak{Ab}_{\mathcal{C}}$. Let $\beta \in \mathrm{H}^0(\mathbf{Hom}(M \otimes M, N))$. (The bold face in **Hom**, **Ext**, etc., indicates that we mean the sheaf versions.) Using β, construct an exact sequence

$$0 \to N \to \mathscr{U}_\beta \to M \to 0 \tag{9}$$

as the pushout of (4) by $\beta \colon M \otimes M \to N$.

If β is symmetric, then $\mathscr{U}_\beta$ is abelian, and we let ϵ_β be the class of (9) in $\mathrm{Ext}^1(M, N)$. If β is symmetric and $\mathbf{Ext}^1(M, N) = 0$, then applying $\mathbf{Hom}(-, N)$ to (5) yields

$$0 \to \mathbf{Hom}(M, N) \to \mathbf{Hom}((\mathscr{U}M)^{\mathrm{ab}}, N) \to \mathbf{Hom}(S^2 M, N) \to 0$$

and a connecting homomorphism sends $\beta \in \mathrm{H}^0(\mathbf{Hom}(S^2 M, N))$ to an element $c_\beta \in \mathrm{H}^1(\mathbf{Hom}(M, N))$.

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

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

(b) *The connecting homomorphism* $\mathrm{H}^1(M) \to \mathrm{H}^2(N)$ *associated to* (9).
(c) *The pairing with* ϵ_β *under the Yoneda product*

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

(if β *is symmetric).*
(d) *The pairing with* c_β *under the evaluation cup product*

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

(if β *is symmetric and* $\mathbf{Ext}^1(M, N) = 0$*).*

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

2.4. **Commutator pairings.**

Proposition 2.9. *Let* $1 \to A \to B \xrightarrow{\rho} C \to 1$ *be an exact sequence in* $\mathfrak{Gp}_{\mathcal{C}}$*, with* A *central in* B*, and* C *abelian. Let* $q\colon \mathrm{H}^1(C) \to \mathrm{H}^2(A)$ *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* $[b_1, b_2] := b_1 b_2 b_1^{-1} b_2^{-1} \in A$*; this induces a homomorphism* $[\ ,\ ]\colon C \otimes C \to A$*. For* $\gamma_1, \gamma_2 \in \mathrm{H}^1(C)$*, 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* $\mathrm{H}^2(C \otimes C) \to \mathrm{H}^2(A)$ *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 $\sigma\colon C^2 \to Q$ 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

$$\sigma((c_1', c_2'))\, \sigma((c_1, c_2) + (c_1', c_2'))^{-1}\, \sigma((c_1, c_2)) = [c_1', c_2^{-1}] = -[c_1', c_2] \tag{10}$$

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

$$\begin{tikzcd} 1 \arrow[r] & C^2 \otimes C^2 \arrow[r] \arrow[d] & \mathscr{U}(C^2) \arrow[r] \arrow[d] & C^2 \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & A \arrow[r] & Q \arrow[r] & C^2 \arrow[r] & 1 \end{tikzcd} \tag{11}$$

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 $(\gamma_1, \gamma_2) \in \mathrm{H}^1(C^2)$ to $(\gamma_1, \gamma_2) \cup (\gamma_1, \gamma_2) \in \mathrm{H}^2(C^2 \otimes C^2)$, by Theorem 2.5. The connecting map for the second row is a composition $\mathrm{H}^1(C^2) \to \mathrm{H}^1(C^3) \to \mathrm{H}^2(A^3) \to \mathrm{H}^2(A)$, so it maps (γ_1, γ_2) to $q(\gamma_1 + \gamma_2) - q(\gamma_1) - q(\gamma_2)$. Finally, the left vertical map sends $(\gamma_1, \gamma_2) \cup (\gamma_1, \gamma_2) \in \mathrm{H}^2(C^2 \otimes C^2)$ to the image of $-\gamma_1 \cup \gamma_2$ under the commutator pairing $\mathrm{H}^2(C \otimes C) \to \mathrm{H}^2(A)$. So compatibility of the connecting maps yields the result. $\square$

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

$$\begin{aligned} \tau_a \colon A_T &\to A_T \\ x &\mapsto a + x \end{aligned}$$

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

$$\begin{aligned} \phi_{\mathscr{L}} \colon A &\to \mathbf{Pic}_{A/S} \\ a &\mapsto \tau_a^* \mathscr{L} \otimes \mathscr{L}^{-1} \end{aligned} \tag{12}$$

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

$$\begin{aligned} \mathbf{Pic}_{A/S} &\to \mathbf{Hom}(A, \mathbf{Pic}_{A/S}) \\ \mathscr{L} &\mapsto \phi_{\mathscr{L}}. \end{aligned}$$

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

$$0 \to \widehat{A} \to \mathbf{Pic}_{A/S} \to \mathbf{Hom}_{\text{self-dual}}(A, \widehat{A}) \to 0. \tag{13}$$

Remark 3.1. Let k be a field, let k_s be a separable closure contained in an algebraic closure $\overline{k}$, and let $G_k = \operatorname{Gal}(k_s/k)$. For an abelian variety A over k, the group $\operatorname{Hom}_{\text{self-dual}}(A, \widehat{A})$ of global sections of $\mathbf{Hom}_{\text{self-dual}}(A, \widehat{A})$ may be identified with the G_k-invariant subgroup of the Néron-Severi group $\operatorname{NS} A_{k_s}$. (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-$(\operatorname{char} k)$ torsion points in $A(k_s)$ to points in $\widehat{A}(k_s)$.)

For any homomorphism of abelian schemes $\lambda \colon A \to B$, let $A[\lambda] := \ker \lambda$.

3.2. **Symmetric line sheaves.** Multiplication by an integer n on A induces a pullback homomorphism $[n]^*\colon \mathbf{Pic}_{A/S} \to \mathbf{Pic}_{A/S}$. Let $\mathbf{Pic}^{\mathrm{Sym}}_{A/S}$ be the kernel of $[-1]^* - [1]^*$ on $\mathbf{Pic}_{A/S}$. More concretely, because $A \to S$ has a section, we have $\mathbf{Pic}^{\mathrm{Sym}}_{A/S}(T) = \operatorname{Pic}^{\mathrm{Sym}}(A \times_S T)/\operatorname{Pic} T$ for each S-scheme T, where $\operatorname{Pic}^{\mathrm{Sym}}(A \times_S T)$ is the group of isomorphism classes of symmetric line sheaves on $A \times_S T$. Since $[-1]^*$ acts as -1 on $\widehat{A}$ and as $+1$ on $\mathbf{Hom}_{\text{self-dual}}(A, \widehat{A})$, and since multiplication-by-2 on $\widehat{A}$ is surjective, the snake lemma applied to $[-1]^* - [1]^*$ acting on (13) yields an exact sequence

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

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 $\operatorname{Spec} k$ for a field k, but the same arguments apply over an arbitrary base scheme.) Given an abelian scheme A over S, there is a Weil pairing

$$e_2\colon A[2] \times \widehat{A}[2] \to \mathbb{G}_m. \tag{15}$$

For any homomorphism $\lambda\colon A \to \widehat{A}$, define $e_2^\lambda\colon A[2] \times A[2] \to \mathbb{G}_m$ by $e_2^\lambda(x,y) = e_2(x, \lambda y)$. If $\mathscr{L} \in \mathbf{Pic}_{A/S}(S)$, let $e_2^{\mathscr{L}} = e_2^{\phi_{\mathscr{L}}}$; 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*

$$\mathfrak{q}\colon A[2] \times \mathbf{Pic}^{\mathrm{Sym}}_{A/S} \to \boldsymbol{\mu}_2 \subset \mathbb{G}_m$$

such that:

(a) *The pairing is additive in the second argument:* $\mathfrak{q}(x, \mathscr{L} \otimes \mathscr{L}') = \mathfrak{q}(x, \mathscr{L})\mathfrak{q}(x, \mathscr{L}')$.
(b) *The restriction of* $\mathfrak{q}$ *to a pairing*

$$\mathfrak{q}\colon A[2] \times \widehat{A}[2] \to \mathbb{G}_m$$

is the Weil pairing e_2. *In particular, this restriction is bilinear.*
(c) *In general,* $\mathfrak{q}(x+y, \mathscr{L}) = \mathfrak{q}(x, \mathscr{L})\mathfrak{q}(y, \mathscr{L})e_2^{\mathscr{L}}(x,y)$.

Proof. See [Pol03, §13.1]. ☐

We can summarize Proposition 3.2 in the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \widehat{A}[2] \arrow[r] \arrow[d, "e_2"', "\wr"] & \mathbf{Pic}^{\mathrm{Sym}}_{A/S} \arrow[r] \arrow[d, "\mathfrak{q}"'] & \mathbf{Hom}_{\text{self-dual}}(A, \widehat{A}) \arrow[r] \arrow[d, "e_2^\bullet"'] & 0 \\
0 \arrow[r] & \mathbf{Hom}(A[2], \mathbb{G}_m) \arrow[r] & \mathbf{Hom}((\mathscr{U} A[2])^{\mathrm{ab}} \otimes \mathbb{F}_2, \mathbb{G}_m) \arrow[r] & \mathbf{Hom}(\bigwedge^2 A[2], \mathbb{G}_m) \arrow[r] & 0,
\end{tikzcd} \tag{16}$$

which we now explain. The top row is (14). The bottom row is obtained by applying $\mathbf{Hom}(-, \mathbb{G}_m)$ to (6) for $M = A[2]$, and using $\mathbf{Ext}^1(A[2], \mathbb{G}_m) = 0$ (a special case of [Wat71, Theorem 1, with the argument of §3 to change fpqc to fppf]). The vertical maps are the map $y \mapsto e_2(-, y)$, the map sending $\mathscr{L}$ to the homomorphism $(\mathscr{U} A[2])^{\mathrm{ab}} \otimes \mathbb{F}_2 \to \mathbb{G}_m$ corresponding to $\mathfrak{q}(-, \mathscr{L})$ (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

$$\begin{aligned} \mathrm{Hom}_{\text{self-dual}}(A, \widehat{A}) &\to \mathrm{H}^1(\widehat{A}[2]) \\ \lambda &\mapsto c_\lambda. \end{aligned} \tag{17}$$

We may interpret c_λ geometrically as the class of the torsor under $\widehat{A}[2]$ that parametrizes symmetric line sheaves $\mathscr{L}$ with $\phi_{\mathscr{L}} = \lambda$ (cf. [Pol03, §13.5]). Thus c_λ is the obstruction to finding $\mathscr{L} \in \mathrm{Pic}^{\mathrm{Sym}} A$ with $\phi_{\mathscr{L}} = \lambda$.

Remark 3.3. The map $\mathrm{H}^1(\widehat{A}[2]) \to \mathrm{H}^1(\widehat{A})$ sends c_λ to the element called c_λ in [PS99, §4]. If k is a global field and $S = \operatorname{Spec} k$, then this and [PS99, Corollary 2] imply that our c_λ lies in the 2-Selmer group of $\widehat{A}$.

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

$$x \underset{e_2^\lambda}{\cup} x = x \underset{e_2}{\cup} c_\lambda \tag{18}$$

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

Proof. The rightmost vertical map in (16) maps λ to e_2^λ. These are mapped by the horizontal connecting homomorphisms to $c_\lambda \in \mathrm{H}^1(\widehat{A}[2])$ and $c_{e_2^\lambda} \in \mathrm{H}^1(\mathbf{Hom}(A[2], \mathbb{G}_m))$, 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 $\mathbf{Ext}^1(A[2], \mathbb{G}_m) = 0$: 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_λ with c_{e^λ} via e_2. □

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 $A^* := \mathrm{Hom}_k(A, k)$ 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 $C^G \to \mathrm{H}^1(G, A)$ 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

$$0 \to (C^*)^G \to (B^*)^G \to (A^*)^G \to 0.$$

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

$$0 \to A^G \to B^G \to C^G \to \mathrm{H}^1(G, A)$$

implies that the connecting homomorphism $C^G \to \mathrm{H}^1(G, A)$ is 0. □

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

(a) $\operatorname{char} k \neq 2$ *and the image G of $G_k \to \operatorname{Aut} A[2](k_s)$ 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 $\mathbb{F}_2G$-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 $A[2] \to (\mathscr{U} A[2])^{\mathrm{ab}} \otimes \mathbb{F}_2$. Thus the top horizontal map in

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

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

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

$$\mathrm{H}^0(\mathbf{Hom}((\mathscr{U} M)^{\mathrm{ab}} \otimes \mathbb{F}_2, \mathbb{G}_m)) \to \mathrm{H}^0(\mathbf{Hom}(\bigwedge^2 M, \mathbb{G}_m)) \xrightarrow{\delta} \mathrm{H}^1(M^\vee). \tag{19}$$

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

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 $M = M_{el} \oplus M_{le} \oplus M_{ll}$ into étale-local, local-étale, and local-local subgroup schemes. Then $M^\vee = (M_{le})^\vee \oplus (M_{el})^\vee \oplus (M_{ll})^\vee$. The homomorphism $M \to M^\vee$ induced by the alternating pairing must map M_{el} to $(M_{le})^\vee$, and M_{le} to $(M_{el})^\vee$, and M_{ll} to $(M_{ll})^\vee$. In particular, $b = b_e + b_{ll}$ where b_e and b_{ll} are alternating pairings on $M_{el} \oplus M_{le}$ and M_{ll}, respectively. The pairing b_e necessarily has the form

$$(m_{el}, m_{le}), (m'_{el}, m'_{le}) \mapsto B(m_{el}, m'_{le}) B(m'_{el}, m_{le})$$

for some bilinear pairing $B\colon M_{el} \times M_{le} \to \boldsymbol{\mu}_2$. Then b_e comes from the quadratic map $(m_{el}, m_{le}) \mapsto B(m_{el}, m_{le})$.

It remains to consider the case $M = M_{ll}$. Then $M^\vee(k_s) = 0$. By [Mil06, Proposition III.6.1 and the paragraph preceding it], $\mathrm{H}^1(M^\vee) = \mathrm{H}^1(G_k, M^\vee(k_s)) = \mathrm{H}^1(G_k, 0) = 0$, 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_2^λ, the right kernel of e_2^λ contains the kernel K of $A[2] \overset{\lambda}{\twoheadrightarrow} \lambda(A[2])$. Since e_2^λ is alternating, the left kernel of e_2^λ contains K too. Thus e_2^λ induces a nondegenerate alternating pairing

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

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

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

be the morphism taking 0 to 1 and all other k_s-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_2^λ, so $c_\lambda = 0$. □

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 $\tau_a \colon P \to P$ be the translation. Also, for $x \in P(S)$, let $\tau_x \colon A \to P$ be the torsor action. The maps τ_x^* for local choices of sections x induce a well-defined isomorphism $\mathbf{Pic}^0_{P/S} \simeq \mathbf{Pic}^0_{A/S}$ since any τ_a^* is the identity on $\mathbf{Pic}^0_{A/S}$. Let $\mathscr{L} \in \mathbf{Pic}_{P/S}(S)$. Generalizing (12), we define

$$\begin{aligned} \phi_{\mathscr{L}} \colon A &\to \mathbf{Pic}^0_{P/S} \simeq \mathbf{Pic}^0_{A/S} \\ a &\mapsto \tau_a^* \mathscr{L} \otimes \mathscr{L}^{-1}. \end{aligned}$$

We may view $\phi_{\mathscr{L}}$ as an element of $\mathrm{Hom}_{\text{self-dual}}(A, \widehat{A})$. If $x \in P(S)$, then $\phi_{\tau_x^* \mathscr{L}} = \phi_{\mathscr{L}}$.

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

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

$$\begin{aligned} \gamma \colon P^\iota &\to \mathbf{Pic}^{\mathrm{Sym}}_{A/S} \\ x &\to \tau_x^* \mathscr{L}. \end{aligned}$$

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

$$\gamma(a+x) = \tau_{a+x}^* \mathscr{L} = \tau_a^*(\tau_x^* \mathscr{L}) = \phi_{\tau_x^* \mathscr{L}}(a) \otimes \tau_x^* \mathscr{L} = \lambda(a) \otimes \gamma(x)$$

in $\mathbf{Pic}^{\mathrm{Sym}}_{A/S}$. In other words, γ is a torsor map (with respect to $\lambda \colon A[2] \to \widehat{A}[2]$) from the torsor P^ι (under $A[2]$) to the torsor (under $\widehat{A}[2]$) of line sheaves in $\mathbf{Pic}^{\mathrm{Sym}}_{A/S}$ with Néron-Severi class λ. Taking classes of these torsors yields $\lambda(c) = c_\lambda$. □

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],

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

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

Equivalently, $\mathcal{T} = P^\iota$. Let $c_\mathcal{T} \in \mathrm{H}^1(A[2])$ be the class of this torsor.

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

$$x \underset{e_2^\lambda}{\cup} x = x \underset{e_2^\lambda}{\cup} c_\mathcal{T} \tag{20}$$

in $\mathrm{H}^2(\mathbb{G}_m)$.

Proof. Proposition 3.7 with $P = \mathbf{Pic}^{g-1}_{X/S}$ and $\mathscr{L} = \Theta$ yields $c_\lambda = \lambda(c_\mathcal{T})$. So (18) in Theorem 3.4 becomes (20). □

Remark 3.10. If $S = \operatorname{Spec} k$ for a field k of characteristic not 2, and the action of G_k on $A[2](k_s)$ factors through a cyclic quotient, then Proposition 3.6(a) gives $c_\lambda = 0$, so $c_\mathcal{T} = 0$, recovering the result of M. Atiyah [Ati71, §5] that under these hypotheses X has a rational theta characteristic.

Similarly, if $S = \operatorname{Spec} k$ for a perfect field k of characteristic 2, then Proposition 3.6(b) gives $c_\lambda = 0$, so $c_\mathcal{T} = 0$. In fact, the proof produces a canonical k-point of $\mathcal{T}$. This generalizes an observation of Mumford [Mum71, p. 191] that a curve over an algebraically closed field of characteristic 2 has a canonical theta characteristic.

Additional criteria for the existence of a rational theta characteristic are given in [Sha11].

3.8. **Hyperelliptic Jacobians.**

Proposition 3.11. *If E is an elliptic curve, then $x \underset{e_2^\lambda}{\cup} x = 0$ for all $x \in \mathrm{H}^1(E[2])$. The same 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 $n \not\equiv 2 \pmod 4$ over a field of characteristic not* 2.

Proof. For an elliptic curve E, the trivial line sheaf $\mathscr{O}_E$ is a theta characteristic defined over k. Now suppose that X is a hyperelliptic curve of genus g, so it is a degree-2 cover of a genus-0 curve Y. The class of a point in $Y(k_s)$ pulls back to a k-point of $\mathbf{Pic}^2_{X/k}$, and if g is odd, multiplying by $(g-1)/2$ gives a k-point of $\mathcal{T}$. On the other hand, if X has a rational Weierstrass point P, then $\mathscr{O}((g-1)P)$ is a theta characteristic defined over k. So $\mathcal{T}$ is trivial in all these cases. Now apply Theorem 3.9. $\square$

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 Δ be the set of zeros of f in k_s. As explained in [Mum71, p. 191], the group $A[2]$ and its torsor $\mathcal{T}$ can be understood explicitly in terms of Δ. 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 $\mathcal{T}$ 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 $c_{\mathcal{T}} \neq 0$.
(b) For $f(x) = x^6 + x + 6$ over $\mathbb{Q}$, we have

$$0 \neq c_{\mathcal{T}} \in \text{Ш}^1(\mathbb{Q}, A[2]) := \ker \left(\mathrm{H}^1(\mathbb{Q}, A[2]) \to \prod_{p \leq \infty} \mathrm{H}^1(\mathbb{Q}_p, A[2]) \right).$$

(*Proof:* The discriminant of f is $-\ell$, where ℓ is the prime 362793931. For $p \notin \{2, \ell\}$, the element $c_{\mathcal{T}}$ maps to 0 in $\mathrm{H}^1(\mathbb{Q}_p, A[2])$ 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 $c_{\mathcal{T}} \neq 0$.)

Acknowledgements

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

References

[Ati71] Michael F. Atiyah, *Riemann surfaces and spin structures*, Ann. Sci. École Norm. Sup. (4) **4** (1971), 47–62. MR0286136 (44 #3350) ↑3.10

[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) ↑3.1, 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. MR1083353 (92d:14036) ↑3.1

[Gir71] Jean Giraud, *Cohomologie non abélienne*, Springer-Verlag, Berlin, 1971 (French). Die Grundlehren der mathematischen Wissenschaften, Band 179. MR0344253 (49 #8992) ↑2.2, 2.5, 2.3, 2.7

[Hat10] Allen Hatcher, *Algebraic topology*, June 30, 2010. Downloaded from `http://www.math.cornell.edu/~hatcher/AT/ATpage.html` . ↑2.6

[Mil06] J. S. Milne, *Arithmetic duality theorems*, Second edition, BookSurge, LLC, 2006. MR881804 (88e:14028) ↑b

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970. MR0282985 (44 #219) ↑3.1

[Mum71] ———, *Theta characteristics of an algebraic curve*, Ann. Sci. École Norm. Sup. (4) **4** (1971), 181–192. MR0292836 (45 #1918) ↑3.10, 3.12

[Pol03] Alexander Polishchuk, *Abelian varieties, theta functions and the Fourier transform*, Cambridge Tracts in Mathematics, vol. 153, Cambridge University Press, Cambridge, 2003. MR1987784 (2004m:14094) ↑3.3, 3.4, 3.4

[PR11] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, April 10, 2011. Preprint. ↑1

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR1740984 (2000m:11048) ↑3.3

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR0236190 (38 #4488) ↑d

[SGA 6] *Théorie des intersections et théorème de Riemann-Roch*, Lecture Notes in Mathematics, Vol. 225, Springer-Verlag, Berlin, 1971 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1966–1967 (SGA 6); Dirigé par P. Berthelot, A. Grothendieck et L. Illusie. Avec la collaboration de D. Ferrand, J. P. Jouanolou, O. Jussila, S. Kleiman, M. Raynaud et J. P. Serre. MR0354655 (50 #7133) ↑3.1

[Sha11] Shahed Sharif, *A descent map for curves with totally degenerate semi-stable reduction*, March 14, 2011. Preprint. ↑3.10

[Wat71] William C. Waterhouse, *Principal homogeneous spaces and group scheme extensions*, Trans. Amer. Math. Soc. **153** (1971), 181–189. MR0269659 (42 #4554) ↑3.4

[Yon58] Nobuo Yoneda, *Note on products in* Ext, Proc. Amer. Math. Soc. **9** (1958), 873–875. MR0175957 (31 #233) ↑2.3

[Zar74] Ju. G. Zarhin, *Noncommutative cohomology and Mumford groups*, Mat. Zametki **15** (1974), 415–419 (Russian). MR0354612 (50 #7090) ↑2.10

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