CUP PRODUCTS ON CURVES OVER FINITE FIELDS

FRAUKE M. BLEHER AND TED CHINBURG

Abstract. In this paper we compute cup products of elements of the first étale cohomology group of μ_ℓ over a smooth projective geometrically irreducible curve C over a finite field k when ℓ is a prime and $\#k \equiv 1 \bmod \ell$. Over the algebraic closure of k, such products are values of the Weil pairing on the ℓ-torsion of the Jacobian of C. Over k, such cup products are more subtle due to the fact that they naturally take values in $\mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell$ rather than in the group $\tilde{\mu}_\ell$ of ℓ^{th} roots of unity in k^*.

1. Introduction

The object of this paper is to compute various cup products and multilinear products in the étale cohomology of smooth projective geometrically irreducible curves C over a finite field k. Let ℓ be a prime such that $q = \#k \equiv 1 \bmod \ell$. Then k^* contains the group $\tilde{\mu}_\ell$ of all ℓ^{th} roots of unity in an algebraic closure $\overline{k}$ of k. Let $\overline{C} = \overline{k} \otimes_k C$. By [9, §20] and [3, Dualité §3], the cup product

$$\mathrm{H}^1(\overline{C}, \mu_\ell) \times \mathrm{H}^1(\overline{C}, \mu_\ell) \to \mathrm{H}^2(\overline{C}, \mu_\ell^{\otimes 2}) = \tilde{\mu}_\ell \tag{1.1}$$

can be identified with the Weil pairing

$$\langle\ ,\ \rangle_{\mathrm{Weil}} : \mathrm{Jac}(\overline{C})[\ell] \times \mathrm{Jac}(\overline{C})[\ell] \to \tilde{\mu}_\ell \tag{1.2}$$

via the natural identification of $\mathrm{H}^1(\overline{C}, \mu_\ell)$ with the ℓ-torsion $\mathrm{Jac}(\overline{C})[\ell]$ of the Jacobian of $\overline{C}$. We will study the corresponding cup product pairing

$$\cup\ : \mathrm{H}^1(C, \mu_\ell) \times \mathrm{H}^1(C, \mu_\ell) \to \mathrm{H}^2(C, \mu_\ell^{\otimes 2}) = \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell \tag{1.3}$$

over the finite field k. We will also consider the trilinear map

$$\mathrm{H}^1(C, \mathbb{Z}/\ell) \times \mathrm{H}^1(C, \mu_\ell) \times \mathrm{H}^1(C, \mu_\ell) \to \mathrm{H}^3(C, \mu_\ell^{\otimes 2}) = \tilde{\mu}_\ell. \tag{1.4}$$

One interest of such trilinear maps comes from key sharing schemes; see [2].

One can naturally identify $\mathrm{H}^1(C, \mu_\ell)$ with the quotient of

$$D(C) = \{a \in k(C)^* : \mathrm{div}_C(a) \in \ell \cdot \mathrm{Div}(C)\}$$

by the subgroup $(k(C)^*)^\ell$. Let $[a] \in \mathrm{H}^1(C, \mu_\ell)$ be the cohomology class determined by $a \in D(C)$. Let $\mathrm{Pic}(C)$ be the divisor class group of C, and let $\mathrm{Pic}^0(C)$ be the group of divisor classes of degree 0. There is a surjection $\mathrm{H}^1(C, \mu_\ell) \to \mathrm{Pic}^0(C)[\ell]$ which sends $[a]$ to the ℓ-torsion divisor class $[\mathrm{div}_C(a)/\ell]$ of $\mathrm{div}_C(a)/\ell$. We will view $\mathrm{Pic}^0(C)[\ell]$ as a subgroup of $\mathrm{Pic}^0(\overline{C})[\ell] = \mathrm{Jac}(\overline{C})[\ell]$.

Since C is geometrically irreducible over k, there is a divisor of C that has degree 1 by [11, Cor. 5, §VII.5], which implies there must a point 0_C for which $d(0_C)$ is prime to ℓ. Let π be a uniformizing parameter in the local ring $\mathcal{O}_{C,0_C}$. An element $a \in D(C)$ will be said to be normalized at 0_C with respect to π if the Laurent expansion of a at 0_C has leading coefficient in $k(0_C)^\ell$. The set $\mathrm{H}^1(C, \mu_\ell)_{0_C}$ of classes $[a]$ represented by $a \in D(C)$ that are normalized at 0_C does not depend on the choice of π and is a codimension one $\mathbb{Z}/\ell$-submodule of $\mathrm{H}^1(C, \mu_\ell)$. The notion of normalized

2010 *Mathematics Subject Classification.* Primary 14F20, 11G20; Secondary 14H45.

Key words and phrases. cup product and multilinear product and Weil pairing.

The first author was supported in part by NSF Grant No. DMS-1801328.

The second author was supported in part by NSF SaTC Grants No. CNS-1513671 and CNS-1701785.

classes goes back to work of Miller in [6] on the efficient computation of the Weil pairing. A one-dimensional $\mathbb{Z}/\ell$-complement to $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ is the space $k^*/(k^*)^\ell = \mathrm{H}^1(k,\mu_\ell)$ of classes of the form $[s]$ with $s \in k^*$. The latter space is also the kernel of the surjection $\mathrm{H}^1(C,\mu_\ell) \to \mathrm{Pic}^0(C)[\ell]$.

Theorem 1.1. *Suppose C has genus 1 and $\ell > 2$. For $[a],[b] \in \mathrm{H}^1(C,\mu_\ell)_{0_C}$ one has*

$$[a] \cup [b] = \frac{1}{d(0_C)} \cdot ([0_C] \otimes \langle [\mathfrak{a}],[\mathfrak{b}] \rangle_{\mathrm{Weil}}) \quad \text{in} \quad \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell = \mathrm{H}^2(C,\mu_\ell^{\otimes 2}) \tag{1.5}$$

where $\mathfrak{a} = \mathrm{div}_C(a)/\ell$, $\mathfrak{b} = \mathrm{div}_C(b)/\ell$ and $[0_C]$ is the class of the divisor of degree $d(0_C)$ defined by the point 0_C.

The corresponding result when $\ell = 2$ is more complicated; see Theorem 6.4. Note that to give C in Theorem 1.1 the structure of an elliptic curve, one must specify a point of degree 1, which could be taken to be 0_C.

For curves of arbitrary positive genus, the cup product on classes in $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ is more subtle.

Theorem 1.2. *Suppose C has arbitrary positive genus and that 0_C is a closed point of degree $d(0_C)$ prime to ℓ. Suppose $\ell > 2$ or that $\ell = 2$ and the normalized classes $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ do not have dimension 1. The following two conditions are equivalent:*

i. *The image of the cup product map $\mathrm{H}^1(C,\mu_\ell)_{0_C} \times \mathrm{H}^1(C,\mu_\ell)_{0_C} \to \mathrm{H}^2(C,\mu_\ell^{\otimes 2})$ spans a $\mathbb{Z}/\ell$-subspace of $\mathrm{H}^2(C,\mu_\ell^{\otimes 2})$ of dimension less than or equal to 1.*
ii. *For all $a,b \in D(C)$ such that $[a],[b] \in \mathrm{H}^1(C,\mu_\ell)_{0_C}$, one has*

$$[a] \cup [b] = \frac{1}{d(0_C)} \cdot ([0_C] \otimes \langle [\mathfrak{a}],[\mathfrak{b}] \rangle_{\mathrm{Weil}}) \quad \text{in} \quad \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell = \mathrm{H}^2(C,\mu_\ell^{\otimes 2})$$

where $\mathfrak{a} = \mathrm{div}_C(a)/\ell$ and $\mathfrak{b} = \mathrm{div}_C(b)/\ell$.

We give in §8 infinitely many curves C of genus 2 for which the equivalent conditions (i) and (ii) of Theorem 1.2 do not hold for $\ell = 3$. The size of the image of the cup product in an analogous number theoretic situation arising from the theory of cyclotomic fields is discussed by McCallum and Sharifi in [5].

When C has genus 1 in Theorem 1.2 and $\ell > 2$, the cup product in part (i) of Theorem 1.2 is an alternating pairing on a vector space of dimension at most 2 over $\mathbb{Z}/p$. Therefore condition (i) holds, consistent with Theorem 1.1. When C has genus 1 and $\ell = 2$, condition (i) of Theorem 1.2 need not hold, and the possibilities are analyzed in Remark 7.3.

We now discuss the nature of the cup product on classes that are not normalized. As noted above, for C of arbitrary genus, $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ has codimension 1 in $\mathrm{H}^1(C,\mu_\ell)$ with a complement being provided by the one-dimensional $\mathbb{Z}/\ell$-vector subspace $k^*/(k^*)^\ell \subset D(C)/(k(C)^*)^\ell$. By the anti-commutativity and bilinearity of the cup product, the determination of cup products is reduced to these two cases: (i) both classes are in $\mathrm{H}^1(C,\mu_\ell)_{0_C}$, and (ii) the first class is in $k^*/(k^*)^\ell$. We now focus on case (ii).

Theorem 1.3. *Suppose C has arbitrary genus, $s \in k^* \subset D(C)$ and $b \in D(C)$. Let $\mathfrak{b} = \mathrm{div}_C(b)/\ell$, and as before let $[\mathfrak{b}]$ be the corresponding element of $\mathrm{Pic}^0(C)[\ell]$. Then*

$$[s] \cup [b] = d\mathcal{L}([\mathfrak{b}]) \otimes s^{\frac{q-1}{\ell}} \in \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell = \mathrm{H}^2(C,\mu_\ell^{\otimes 2}) \tag{1.6}$$

where

$$d\mathcal{L} : \mathrm{Pic}(C)[\ell] \to \mathrm{Pic}^0(C)/\ell \cdot \mathrm{Pic}^0(C)$$

is a homomorphism defined in Proposition 5.1 which we call the Legendre derivative of Frobenius. Here $[s] \cup [b] = 0$ if $b \in k^*$.

The proof of Theorem 1.3 relies on a cup product formula that is a function field counterpart of work of McCallum and Sharifi in [5]; see Theorem 3.1. Miller gives in [6] a polynomial time algorithm for computing the Weil pairing. One consequence is that for elliptic curves C over finite

fields, the difficulty of computing cup products arises from the case in Theorem 1.3 rather than from that in Theorem 1.1. In consequence, one can compute the (non-degenerate) triple product

$$\mathrm{H}^1(C,\mathbb{Z}/\ell)\times\mathrm{H}^1(C,\mu_\ell)\times\mathrm{H}^1(C,\mu_\ell)\to\mathrm{H}^3(C,\mu_\ell^{\otimes 2})=\tilde{\mu}_\ell \tag{1.7}$$

quickly when the second and third arguments are normalized at some point 0_C.

We now outline the contents of the sections of this paper. In §2, we set up the notation and assumptions for the remainder of the paper and we collect some results on étale cohomology groups. In §3, we prove in Theorem 3.1 a cup product formula that is a function field counterpart of work of McCallum and Sharifi in [5]. In Theorem 3.4, we then connect this to the Weil pairing. In §4, we prove various results that are necessary for analyzing the formula in Theorem 3.1. In §5, we consider restrictions of the cup product maps (1.4) and (1.3) that are connected to the derivative of the arithmetic Frobenius. In particular, in Proposition 5.1, we introduce the Legendre derivative of Frobenius, and we prove Theorem 5.3 which implies Theorem 1.3. In §6, we focus on the genus one case. In particular, we prove Theorem 6.2 when $\ell>2$, which implies Theorem 1.1. We also analyze the case when $\ell=2$ in Theorem 6.4. In §7, we consider curves of arbitrary positive genus and prove Theorem 1.2 (see Theorem 7.1). In §8, we construct an infinite family of curves of genus two for which neither (i) nor (ii) of Theorem 1.2 hold when $\ell=3$; see Theorem 8.6.

Acknowledgements

The authors would like to thank D. Boneh, M. Bright, H. W. Lenstra Jr., R. Sharifi, A. Silverberg and A. Venkatesh for conversations related to this article.

2. Étale cohomology groups

Throughout this paper we will assume C is a smooth projective geometrically irreducible curve of genus $g\geq 1$ over a finite field k of order q. We will suppose ℓ is a prime such that $q\equiv 1 \bmod \ell$, so that k^* contains a group $\tilde{\mu}_\ell$ of order ℓ. Let $k(C)$ be the function field of C and let $\overline{k(C)}$ be a separable closure of $k(C)$. Let $\mathrm{Div}(C)$ be the divisor group of C, let $\mathrm{Pic}(C)$ be the Picard group of C, and let $\mathrm{Pic}^0(C)$ be the group of divisor classes of degree 0. Let $\overline{k}$ be a fixed algebraic closure of k, and let $\overline{C}=C\otimes_k\overline{k}$.

Let η be a geometric point of $\overline{C}$, which can then also be viewed as a geometric point of C. We have an exact sequence

$$1\to\pi_1(\overline{C},\eta)\to\pi_1(C,\eta)\to\mathrm{Gal}(\overline{k}/k)\to 1 \tag{2.1}$$

of étale fundamental groups in which $\mathrm{Gal}(\overline{k}/k)$ is isomorphic to the profinite completion $\hat{\mathbb{Z}}$ of $\mathbb{Z}$. There are natural isomorphisms

$$\mathrm{H}^1(k,\mathbb{Z}/\ell)=\mathrm{Hom}(\mathrm{Gal}(\overline{k}/k),\mathbb{Z}/\ell) \tag{2.2}$$

and

$$\mathrm{H}^1(C,\mathbb{Z}/\ell)=\mathrm{Hom}(\pi_1(C,\eta),\mathbb{Z}/\ell)\quad\text{and}\quad\mathrm{H}^1(\overline{C},\mathbb{Z}/\ell)=\mathrm{Hom}(\pi_1(\overline{C},\eta),\mathbb{Z}/\ell). \tag{2.3}$$

In fact, we have from [8, Prop. 2.9]:

Lemma 2.1. *For all $i\geq 0$, the natural homomorphisms*

$$\mathrm{H}^i(\pi_1(C,\eta),\mathbb{Z}/\ell)\to\mathrm{H}^i(C,\mathbb{Z}/\ell)\quad\textit{and}\quad\mathrm{H}^i(\pi_1(\overline{C},\eta),\mathbb{Z}/\ell)\to\mathrm{H}^i(\overline{C},\mathbb{Z}/\ell)$$

are isomorphisms.

The following lemma results directly from the spectral sequence

$$\mathrm{H}^p(\mathrm{Gal}(\overline{k}/k),\mathrm{H}^q(\overline{C},\mu_\ell))\Rightarrow\mathrm{H}^{p+q}(C,\mu_\ell)$$

together with the fact that $\mathrm{Gal}(\overline{k}/k)\cong\hat{\mathbb{Z}}$ has cohomological dimension one.

Lemma 2.2. *From (2.1) one has a split exact sequence of elementary abelian ℓ-groups*

$$0 \to \mathrm{Hom}(\mathrm{Gal}(\overline{k}/k), \mathbb{Z}/\ell) \to \mathrm{H}^1(C, \mathbb{Z}/\ell) \to \mathrm{H}^1(\overline{C}, \mathbb{Z}/\ell)^{\mathrm{Gal}(\overline{k}/k)} \to 0 \tag{2.4}$$

in which $\mathrm{Hom}(\mathrm{Gal}(\overline{k}/k), \mathbb{Z}/\ell)$ *is cyclic of order* ℓ *and* $\mathrm{H}^1(\overline{C}, \mathbb{Z}/\ell)$ *has order* ℓ^{2g}*. The sequence (2.4) is the* $\mathbb{Z}/\ell$ *dual of the sequence*

$$0 \to \mathrm{Pic}^0(C)/\ell \cdot \mathrm{Pic}^0(C) \to \mathrm{Pic}(C)/\ell \cdot \mathrm{Pic}(C) \to \mathbb{Z}/\ell \to 0 \tag{2.5}$$

resulting from the degree map $\mathrm{Pic}(C) \to \mathbb{Z}$ *and the Artin map* $\mathrm{Pic}(C) \to \pi_1(C, \eta)^{\mathrm{ab}}$*.*

The next lemma gives a description of $\mathrm{H}^i(C, \mu_\ell)$ for $i = 1, 2$.

Lemma 2.3. *Define*

$$D(C) = \{a \in k(C)^* : \mathrm{div}_C(a) \in \ell \cdot \mathrm{Div}(C)\}. \tag{2.6}$$

There are natural isomorphisms

$$\mathrm{H}^1(C, \mathbb{Z}/\ell) = \mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}/\ell) \quad \textit{and} \quad \mathrm{H}^1(C, \mu_\ell) = D(C)/(k(C)^*)^\ell, \tag{2.7}$$

and

$$\mathrm{H}^2(C, \mu_\ell) = \mathrm{Pic}(C)/\ell \cdot \mathrm{Pic}(C). \tag{2.8}$$

Proof. By [1, Lemma 4.3], there is an isomorphism $\mathrm{H}^1(C, \mu_\ell) = D(C)/(k(C)^*)^\ell$. Moreover, we have that $\mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}/\ell)$ is identified with $\mathrm{Hom}(\pi_1(C, \eta), \mathbb{Z}/\ell)$ via the Artin map, and that $\mathrm{Pic}(C)/\ell \cdot \mathrm{Pic}(C)$ is identified with $\mathrm{H}^2(C, \mu_\ell)$ via the Kummer sequence. □

Remark 2.4. The canonical isomorphism $\mathrm{H}^0(C, \mu_\ell) = \tilde{\mu}_\ell$ gives an isomorphism

$$\mathrm{H}^i(C, \mu_\ell) = \mathrm{H}^i(C, \mathbb{Z}/\ell) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell$$

for all $i \geq 0$.

In analyzing cup product pairings it will be useful to have a complement for the image of the inflation homomorphism $\mathrm{H}^1(k, \mu_\ell) \to \mathrm{H}^1(C, \mu_\ell)$. Let $k(0_C)$ be the residue field of a closed point 0_C of C, and let $d(0_C) = [k(0_C) : k]$.

Definition 2.5. Suppose 0_C is a closed point of C with $d(0_C)$ prime to ℓ. Let π be a uniformizing parameter in the local ring $\mathcal{O}_{C,0_C}$. A function $f \in k(C)^*$ will be said to be normalized at 0_C with respect to π if the leading term in its Laurent expansion with respect to π lies in $(k(0_C)^*)^\ell$. A class in $\mathrm{H}^1(C, \mu_\ell)$ will be said to be normalized at 0_C with respect to π if it has the form $[f]$ for an f of this kind. Let $\mathrm{H}^1(C, \mu_\ell)_{0_C}$ be the subset of all such $[f]$.

Lemma 2.6. *There is a closed point* 0_C *of* C *with* $d(0_C)$ *prime to* ℓ*. The normalized classes* $\mathrm{H}^1(C, \mu_\ell)_{0_C}$ *are a codimension one* $\mathbb{Z}/\ell$ *subspace of* $\mathrm{H}^1(C, \mu_\ell)$ *that depends on* 0_C *but that does not depend on the choice of uniformizer* π *at* 0_C*. This subspace is a complement to the one dimensional subspace* $\mathrm{H}^1(k, \mu_\ell) = k^*/(k^*)^\ell$ *of* $\mathrm{H}^1(C, \mu_\ell)$*, and the restriction map sends* $\mathrm{H}^1(C, \mu_\ell)_{0_C}$ *isomorphically to* $\mathrm{H}^1(\overline{C}, \mu_\ell)^{\mathrm{Gal}(\overline{k}/k)}$*.*

Proof. Since C is geometrically irreducible over k, there is a divisor of C that has degree 1 by [11, Cor. 5, §VII.5], which implies there must a point 0_C for which $d(0_C)$ is prime to ℓ. If $f \in D(C)$ then $\mathrm{ord}_{0_C}(f)$ is a multiple of ℓ. Therefore if one replaces π by another uniformizing parameter π' at 0_C, the leading terms in the Laurent expansions of f with respect to π and π' differ by an element of $(k(0_C)^*)^\ell$. Therefore $\mathrm{H}^1(C, \mu_\ell)_{0_C}$ does not depend on the choice of π. Since $d = d(0_C)$ is prime to ℓ and $q \equiv 1 \bmod \ell$, the ratio $\#k(0_C)^*/\#k^* = (q^d - 1)/(q - 1) = 1 + q + \cdots q^{d-1}$ is congruent to d mod ℓ and therefore prime to ℓ. Hence the Sylow ℓ subgroups of k^* and $k(0_C)^*$ are the same. Therefore every $f \in D(C)$ is equal to $\tilde{f} \cdot s$ for some $\tilde{f}$ that is normalized at 0_C and some $s \in k^*$. It follows that $\mathrm{H}^1(C, \mu_\ell)_{0_C}$ is a complement to the one dimensional subspace $\mathrm{H}^1(k, \mu_\ell) = k^*/(k^*)^\ell$ of $\mathrm{H}^1(C, \mu_\ell)$. This and (2.4) imply the final statement of the lemma. □

Corollary 2.7. *Every element $[a]$ of $\mathrm{H}^1(C,\mu_\ell)$ has a unique expression as a product $[\tilde{a}]\cdot[r]$ with $\tilde{a}$ normalized at 0_C and $r\in k^*$. The classes $[\tilde{a}]$ and $[r]$ depend on $[a]$ and 0_C but not on the choice of uniformizer π at 0_C. Suppose $[b]\in \mathrm{H}^1(C,\mu_\ell)$ equals $[\tilde{b}]\cdot[s]$ with $\tilde{b}$ normalized at 0_C and $s\in k^*$. Then*

$$[a]\cup[b]=[\tilde{a}]\cup[\tilde{b}]+[r]\cup[\tilde{b}]+[\tilde{a}]\cup[s]=[\tilde{a}]\cup[\tilde{b}]+[r]\cup[\tilde{b}]-[s]\cup[\tilde{a}] \tag{2.9}$$

Proof. This is clear from the fact that cup products are bilinear and anti-commutative, and $[r]\cup[s]=0$ since $[r]\cup[s]$ is the inflation of a class in $\mathrm{H}^2(k,\mu_\ell^{\otimes 2})=0$ to $\mathrm{H}^2(C,\mu_\ell^{\otimes 2})$. □

Remark 2.8. Corollary 2.7 reduces the computation of cup products of elements of $\mathrm{H}^1(C,\mu_\ell)$ to two cases: (i) both arguments are normalized classes with respect to some choice of closed point 0_C with $d(0_C)$ prime to ℓ, or (ii) the first argument is in $\mathrm{H}^1(k,\mu_\ell)$ and the second is normalized. The notion of elements of $D(C)$ normalized with respect to the choice of a uniformizer at $0_C\in C(k)$ comes from [6], which considered the case in which 0_C of the origin of an elliptic curve C.

We will need the following result later to reduce to the case in which 0_C has residue field k.

Theorem 2.9. *Suppose 0_C is a point of C whose residue field $k'=k(0_C)$ is a degree $d(0_C)$ extension of k with $d(0_C)$ prime to ℓ. Let $\pi: C'=k'\otimes_k C\to C$ be the second projection. The direct image homomorphism*

$$\pi_*:\mathrm{H}^2(C',\mu_\ell^{\otimes 2})=\mathrm{Pic}(C')\otimes_{\mathbb{Z}}\tilde{\mu}_\ell\to \mathrm{H}^2(C,\mu_\ell^{\otimes 2})=\mathrm{Pic}(C)\otimes_{\mathbb{Z}}\tilde{\mu}_\ell \tag{2.10}$$

is induced by the norm $\mathrm{Norm}_{C'/C}:\mathrm{Pic}(C')\to\mathrm{Pic}(C)$ and the identity map on $\tilde{\mu}_\ell$. Let $0_{C'}$ be a point of C' over 0_C. Then $0_{C'}$ is a point of $C'(k')$ and $\mathrm{Norm}_{C'/C}(0_{C'})=0_C$. Let $[a]',[b]'\in\mathrm{H}^1(C',\mu_\ell)$ be the pullbacks of $[a],[b]\in\mathrm{H}^1(C,\mu_\ell)$. One has

$$[a]\cup[b]=\frac{1}{d(0_C)}(\mathrm{Norm}_{C'/C}\otimes\mathrm{Id})([a]'\cup[b]'). \tag{2.11}$$

where Id *is the identity map on $\tilde{\mu}_\ell$. If $[a]$ and $[b]$ lie in $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ then $[a]',[b]'\in\mathrm{H}^1(C',\mu_\ell)_{0_{C'}}$.*

Proof. To show the claim in (2.10) it will suffice to show that

$$\pi_*:\mathrm{H}^2(C',\mu_\ell)=\mathrm{Pic}(C')\to\mathrm{H}^2(C,\mu_\ell)=\mathrm{Pic}(C)$$

equals $\mathrm{Norm}_{C'/C}$. This follows from the compatibility of the Kummer sequences of C' and C with respect to π_*. The point 0_C splits to C' so $\mathrm{Norm}_{C'/C}(0_{C'})=0_C$. The composition $\pi_*\circ\pi^*$ on every cohomology group $\mathrm{H}^i(C,\mu_\ell)$ is multiplication by the degree $d(0_C)$ of C' over C. By the compatibility of cup products with pullbacks this gives

$$d(0_C)\cdot([a]\cup[b])=\pi_*\circ\pi^*(([a]\cup[b])=\pi_*([a]'\cup[b'])=(\mathrm{Norm}_{C'/C}\otimes\mathrm{Id})([a]'\cup[b]')$$

which shows (2.11) since $d(0_C)$ is prime to ℓ. Finally, the last statement of the theorem follows from comparing Laurent expansions at 0_C and at $0_{C'}$. □

3. Formulas for étale cup product maps

In this section we first prove a cup product formula that is a function field counterpart of work of McCallum and Sharifi in [5] and we then connect this to the Weil pairing. We assume the notation of the previous section.

Theorem 3.1. *Suppose $a,b\in D(C)$ define non-trivial classes $[a],[b]\in\mathrm{H}^1(C,\mu_\ell)$. Choose $\alpha\in\overline{k(C)}$ with $\alpha^\ell=a$. Then $k(C)(\alpha)$ is the function field of an irreducible smooth projective curve C' over k. Write $\mathfrak{b}=\mathrm{div}_C(b)/\ell\in\mathrm{Div}(C)$. There is an element $\gamma\in k(C')$ such that $b=\mathrm{Norm}_{k(C')/k(C)}(\gamma)$. Let σ be a generator for the cyclic group $\mathrm{Gal}(k(C')/k(C))$ of order ℓ. There is a divisor $\mathfrak{c}\in\mathrm{Div}(C')$ such that*

$$\mathrm{div}_{C'}(\gamma)=\pi^*\mathfrak{b}+(1-\sigma)\cdot\mathfrak{c}$$

where $\pi : C' \to C$ is the morphism associated with the inclusion $k(C) \subset k(C')$. The element $\sigma(\alpha)/\alpha = \zeta$ lies in $\tilde{\mu}_\ell$. The cup product

$$[a] \cup [b] \in \mathrm{H}^2(C, \mu_\ell^{\otimes 2}) = \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell \tag{3.1}$$

is given by

$$[a] \cup [b] = \left([\mathrm{Norm}_{k(C')/k(C)}(\mathfrak{c})] + \frac{\ell}{2}[\mathfrak{b}] \right) \otimes \zeta \tag{3.2}$$

when we use the isomorphisms in Lemma 2.3, where $[\mathfrak{d}]$ is the class in $\mathrm{Pic}(C)$ of a divisor $\mathfrak{d}$. Suppose now that $t \in \mathrm{H}^1(C, \mathbb{Z}/\ell) = \mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}/\ell)$. The triple product

$$t \cup [a] \cup [b] \in \mathrm{H}^3(C, \mu_\ell^{\otimes 2}) = \tilde{\mu}_\ell$$

is given by

$$t \cup [a] \cup [b] = \zeta^{t([\mathrm{Norm}_{k(C')/k(C)}(\mathfrak{c})] + \frac{\ell}{2}[\mathfrak{b}])}. \tag{3.3}$$

To prove Theorem 3.1, we need a lemma. Using Remark 2.4, we have the following result from [8, Cor. II.3.3(b)].

Lemma 3.2. *The cup product pairing*

$$\mathrm{H}^1(C, \mathbb{Z}/\ell) \times \mathrm{H}^2(C, \mu_\ell) \to \mathrm{H}^3(C, \mu_\ell) = \mathbb{Z}/\ell \tag{3.4}$$

is a perfect duality between the groups $\mathrm{H}^1(C, \mathbb{Z}/\ell)$ and $\mathrm{H}^2(C, \mu_\ell)$.

Proof of Theorem 3.1. The expression (3.2) is shown by the argument of [5, Thm. 2.4], suitably adapted to the function field case. The formula (3.3) will now follow if we can show that the pairing (3.4) in Lemma 3.2 agrees with the natural evaluation pairing

$$\mathrm{Hom}(\mathrm{Pic}(C), \mathbb{Z}/\ell) \times (\mathrm{Pic}(C)/\ell \cdot \mathrm{Pic}(C)) \to \mathbb{Z}/\ell$$

when we use the identifications in Lemma 2.3. It will suffice to show that the cup product

$$\mathrm{H}^1(C, \mu_\ell) \times \mathrm{H}^2(C, \mu_\ell) \to \mathrm{H}^3(C, \mu_\ell^{\otimes 2}) = \tilde{\mu}_\ell \tag{3.5}$$

and the evaluation map

$$\mathrm{Hom}(\mathrm{Pic}(C), \tilde{\mu}_\ell) \times (\mathrm{Pic}(C)/\ell \cdot \mathrm{Pic}(C)) \to \tilde{\mu}_\ell \tag{3.6}$$

agree.

In [1, Cor. 5.3] it is shown that the Kummer sequence leads to an exact sequence

$$k(C)^*/(k(C)^*)^\ell \xrightarrow{\tau} J(k(C))/\left(U(k(C)) \cdot J(k(C))^\ell\right) \xrightarrow{\omega} \mathrm{H}^2(C, \mu_\ell) \to 1 \tag{3.7}$$

where $J(k(C))$ is the idele group of $k(C)$ and $U(k(C))$ is the group of unit ideles. The cokernel of τ is isomorphic to $\mathrm{Pic}(C)/\ell \cdot \mathrm{Pic}(C)$, and (3.7) agrees with our identification of $\mathrm{H}^2(C, \mu_\ell)$ with $\mathrm{Pic}(C)/\ell \cdot \mathrm{Pic}(C)$.

Let $[\beta]$ be the class of $\beta \in D(C)$ in $\mathrm{H}^1(C, \mu_\ell)$, and suppose $j \in J(C)$ defines a class $z(j) \in J(k(C))/\left(U(k(C)) \cdot J(k(C))^\ell\right)$ with class $\omega(z(j))$ in $\mathrm{H}^2(C, \mu_\ell)$ via (3.7). Let $k(C)^{\mathrm{ab}}$ be the maximal abelian extension of $k(C)$ in a separable closure of $k(C)$, and let $k(C)^{\mathrm{un}}$ be the maximal unramified extension of $k(C)$ in $k(C)^{\mathrm{ab}}$. It is shown in [1, Lemma 5.4] that the cup product $\omega(z(j)) \cup [\beta]$ in (3.5) is given by

$$\omega(z(j)) \cup [\beta] = \mathrm{Art}(j)(\beta^{1/\ell})/\beta^{1/\ell}. \tag{3.8}$$

where $\mathrm{Art} : J(C) \to \mathrm{Gal}(k(C)^{\mathrm{ab}}/k(C))$ is the idelic Artin map. We have identified $[\beta] \in \mathrm{H}^1(C, \mu_\ell) = \mathrm{Hom}(\pi_1(C, \eta), \mu_\ell)$ with an element f of $\mathrm{Hom}(\mathrm{Pic}(C), \mu_\ell)$ via the formula

$$f(c) = \mathrm{art}(c)(\beta^{1/\ell})/\beta^{1/\ell} \tag{3.9}$$

for $c \in \mathrm{Pic}(C)$, where $\mathrm{art} : \mathrm{Pic}(C) \to \mathrm{Gal}(k(C)^{\mathrm{un}}/k(C))$ is the unramified Artin map. Thus when $c \mod \ell \cdot \mathrm{Pic}(C)$ agrees with the image of $z(j)$ in the cokernel of τ in (3.7), the values (3.8) and (3.9) agree. This shows the cup product in (3.5) agrees with the evaluation map in (3.6). □

We next consider the connection to the Weil pairing of the restriction of the cup product map (1.4) that is given by (3.3).

Lemma 3.3. *There is a commutative diagram*

$$\begin{array}{ccccccc} \mathrm{H}^1(C,\mu_\ell) & \times & \mathrm{H}^1(C,\mu_\ell) & \longrightarrow & \mathrm{H}^2(C,\mu_\ell^{\otimes 2}) & = & \mathrm{Pic}(C)\otimes_{\mathbb{Z}}\tilde{\mu}_\ell \\ \downarrow & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \deg\otimes\mathrm{Id}} \\ \mathrm{H}^1(\overline{C},\mu_\ell) & \times & \mathrm{H}^1(\overline{C},\mu_\ell) & \longrightarrow & \mathrm{H}^2(\overline{C},\mu_\ell^{\otimes 2}) & = & \mathbb{Z}\otimes_{\mathbb{Z}}\tilde{\mu}_\ell \end{array} \tag{3.10}$$

produced by restriction from C to $\overline{C}$ in which both rows are the cup product pairings, and the bottom row is the Weil pairing when we identify $\mathrm{H}^1(\overline{C},\mu_\ell)$ with $\mathrm{Pic}(\overline{C})[\ell]$.

Proof. The statement about the bottom row being the Weil pairing is shown in [9, §20] and [3, Dualité §3]. The Kummer sequences for C and $\overline{C}$ show that the restriction map

$$\mathrm{H}^2(C,\mu_\ell) = \mathrm{Pic}(C)/\ell\cdot\mathrm{Pic}(C) \to \mathrm{H}^2(\overline{C},\mu_\ell) = \mathbb{Z}/\ell$$

is induced by the degree map. Since k contains $\tilde{\mu}_\ell$, it follows that the restriction map on the right side of (3.10) is induced by $\deg\otimes\mathrm{Id}$. □

In what follows we will use $\overline{c}$ to denote the image of $c\in\mathrm{H}^1(C,\mu_\ell)$ (resp. $c\in\mathrm{H}^1(C,\mathbb{Z}/\ell)$) under the restriction map to $\mathrm{H}^1(\overline{C},\mu_\ell)$ (resp. $\mathrm{H}^1(\overline{C},\mathbb{Z}/\ell)$).

Theorem 3.4. *The restriction of (1.4) to triples in which the third argument lies in $\mathrm{H}^1(k,\mu_\ell)$ can be computed in the following way. Suppose t, a and b are as in Theorem 3.1. Moreover, assume that $b\in k^*$, so $[b]\in\mathrm{H}^1(k,\mu_\ell)=k^*/(k^*)^\ell$. Then $b^{(q-1)/\ell}\in\tilde{\mu}_\ell$ and $w=t\otimes b^{(q-1)/\ell}\in\mathrm{H}^1(C,\mathbb{Z}/\ell)\otimes\tilde{\mu}_\ell=\mathrm{H}^1(C,\mu_\ell)$. One has*

$$t\cup[a]\cup[b] = \overline{w}\cup\overline{[a]} = \langle\overline{w},\overline{[a]}\rangle_{\mathrm{Weil}}\in\tilde{\mu}_\ell \tag{3.11}$$

where the second equality uses the identification of the Weil pairing in Lemma 3.3.

By the non-degeneracy of the Weil pairing, the following result is a consequence of Theorem 3.4.

Corollary 3.5. *The multilinear map*

$$\mathrm{H}^1(C,\mathbb{Z}/\ell)\times\mathrm{H}^1(C,\mu_\ell)\times\mathrm{H}^1(k,\mu_\ell)\to\tilde{\mu}_\ell$$

is induced by a multilinear map

$$\mathrm{H}^1(\overline{C},\mathbb{Z}/\ell)\times\mathrm{H}^1(\overline{C},\mu_\ell)\times\mathrm{H}^1(k,\mu_\ell)\to\tilde{\mu}_\ell \tag{3.12}$$

that is non-degenerate in the following sense. The map $\bar{t}\to\{\overline{[a]}\otimes[b]\to t\cup[a]\cup[b]\}$ identifies $\mathrm{H}^1(\overline{C},\mathbb{Z}/\ell)$ with $\mathrm{Hom}(\mathrm{H}^1(\overline{C},\mu_\ell)\otimes\mathrm{H}^1(k,\mu_\ell),\tilde{\mu}_\ell)$.

Proof of Theorem 3.4. With the notation of the theorem, we have elements $w=t\otimes b^{(q-1)/\ell}\in\mathrm{H}^1(C,\mathbb{Z}/\ell)\otimes_{\mathbb{Z}}\tilde{\mu}_\ell=\mathrm{H}^1(C,\mu_\ell)$ and $[a]\in\mathrm{H}^1(C,\mu_\ell)$ where $t\in\mathrm{H}^1(C,\mathbb{Z}/\ell)$, $b\in k^*$ and $[b]\in\mathrm{H}^1(k,\mu_\ell)=k^*/(k^*)^\ell$. Write

$$z = t\cup[a]\in\mathrm{H}^2(C,\mu_\ell)=\mathrm{Pic}(C)/\ell\cdot\mathrm{Pic}(C).$$

Then

$$\begin{aligned} w\cup[a] &= (t\otimes b^{(q-1)/\ell})\cup[a] = ([a]\cup(t\otimes b^{(q-1)/\ell}))^{-1} = (([a]\cup t)\otimes b^{(q-1)/\ell})^{-1} \\ &= ([a]\cup t)^{-1}\otimes b^{(q-1)/\ell} = z\otimes b^{(q-1)/\ell} \quad \text{in} \quad \mathrm{H}^2(C,\mu_\ell^{\otimes 2})=\mathrm{Pic}(C)\otimes_{\mathbb{Z}}\tilde{\mu}_\ell. \end{aligned}$$

The restriction map

$$\mathrm{H}^2(C,\mu_\ell)=\mathrm{Pic}(C)/\ell\cdot\mathrm{Pic}(C)\ \to\ \mathbb{Z}/\ell=\mathrm{H}^2(\overline{C},\mu_\ell)$$

is surjective and induced by the degree map $\deg:\mathrm{Pic}(C)\to\mathbb{Z}$. Let $d=\deg(z)\in\mathbb{Z}/\ell$. We obtain from diagram (3.10) of Lemma 3.3 that

$$\overline{w}\cup\overline{[a]} = d\otimes b^{(q-1)/\ell} = 1\otimes b^{d(q-1)/\ell}\in\mathbb{Z}/\ell\otimes\tilde{\mu}_\ell=\mathrm{H}^2(\overline{C},\mu_\ell)\otimes_{\mathbb{Z}}\tilde{\mu}_\ell=\mathrm{H}^2(\overline{C},\mu_\ell^{\otimes 2}). \tag{3.13}$$

On the other hand, the formula (3.9) in the proof of Theorem 3.1 shows that

$$t \cup [a] \cup [b] = \mathrm{art}(z)(b^{1/\ell})/b^{1/\ell}$$

when z is viewed as an element of $\mathrm{Pic}(C)/\ell \cdot \mathrm{Pic}(C)$ and art is the unramified Artin map. Since $b \in k^*$, we see that

$$\mathrm{art}(z)(b^{1/\ell}) = \Phi^d(b^{1/\ell})$$

when $\Phi = \Phi_{\overline{k}/k}$ is the Frobenius automorphism of $\overline{k}$ relative to k. Thus

$$t \cup [a] \cup [b] = b^{(q^d-1)/\ell}. \tag{3.14}$$

Therefore (3.13) and (3.14) are equal, as claimed in Theorem 3.4, because

$$(q^d-1)/\ell = (1+q+\cdots+q^{d-1}) \cdot (q-1)/\ell \equiv d \cdot (q-1)/\ell \mod \ell$$

since $q \equiv 1 \bmod \ell$. □

4. The arithmetic of covers

In this section we will prove various results necessary for analyzing the formula in Theorem 3.1.

Let C be a smooth projective curve with constant field $k = \mathbb{F}_q$ of order $q \equiv 1 \bmod \ell$ and function field $k(C)$. Define $\Phi_{\overline{k}/k}$ to be the arithmetic Frobenius on $\overline{k}$, so that $\Phi_{\overline{k}/k}$ is the q^{th} power map. Let $\langle \Phi_{\overline{k}/k} \rangle_\ell$ be the pro-ℓ completion of the cyclic group generated by $\Phi_{\overline{k}/k}$. Then $\langle \Phi_{\overline{k}/k} \rangle_\ell = \mathrm{Gal}(k^\dagger/k)$ when $k^\dagger$ is the maximal pro-ℓ extension of k in $\overline{k}$. Fix an algebraic closure $\overline{k(C)}$ of $k(C)$ containing $\overline{k}$.

Define $k^\dagger(C)$ to be the compositum of $k^\dagger$ and $k(C)$ in $\overline{k(C)}$. Define $L(C)$ to be the maximal abelian pro-ℓ unramified extension of $k^\dagger(C)$ in $\overline{k(C)}$. We then have canonical isomorphisms $\langle \Phi_{\overline{k}/k} \rangle_\ell = \mathrm{Gal}(k^\dagger(C)/k(C))$ and $T_\ell(C) = \mathrm{Gal}(L(C)/k^\dagger(C))$ when $T_\ell(C)$ is the ℓ-adic Tate module of C. Here $T_\ell(C)$ is isomorphic to $(\mathbb{Z}_\ell)^{2g(C)}$ when $g(C)$ is the genus of C over k. The conjugation action on $\mathrm{Gal}(L(C)/k^\dagger(C))$ of a lift $\tilde{\Phi}_{\overline{k}/k}$ of $\Phi_{\overline{k}/k}$ to $\mathrm{Gal}(L(C)/k(C))$ gives an automorphism $\Phi_{k,C}$ of $T_\ell(C)$ independent of the choice of $\tilde{\Phi}_{\overline{k}/k}$. The choice of $\tilde{\Phi}_{\overline{k}/k}$ gives an isomorphism

$$\mathrm{Gal}(L(C)/k(C)) = T_\ell(C) \rtimes \langle \Phi_{\overline{k}/k} \rangle_\ell. \tag{4.1}$$

Define $\mathrm{Pic}(C)_\ell$ to be the pro-ℓ completion of $\mathrm{Pic}(C)$. The Artin map then defines an isomorphism

$$\mathrm{art}_C : \mathrm{Pic}(C)_\ell \to \mathrm{Gal}(L(C)/k(C))^{\mathrm{ab}} = T_\ell(C)/(1-\Phi_{k,C})T_\ell(C) \times \langle \Phi_{\overline{k}/k} \rangle_\ell. \tag{4.2}$$

Let $\mathrm{Pic}^0(C)[\ell^\infty]$ be the Sylow ℓ-subgroup of $\mathrm{Pic}^0(C)$. The restriction of the Artin map defines an isomorphism

$$\mathrm{art}^0_C : \mathrm{Pic}^0(C)[\ell^\infty] \to \mathrm{Gal}(L(C)/k^\dagger(C)) = T_\ell(C)/(1-\Phi_{k,C})T_\ell(C). \tag{4.3}$$

Suppose now that $a \in k(C)^*$ is an element such that $\mathrm{div}_C(a)$ is a multiple of ℓ in $\mathrm{Div}(C)$ but a is not in $(k(C)^*)^\ell$. Then $k(C)(a^{1/\ell})$ is a cyclic degree ℓ unramified extension of $k(C)$ in $L(C)$. Let C' be the smooth projective curve associated to this extension, and let k' be the constant field of C'. Either $k = k'$ or k' is the unique cyclic degree ℓ extension of k in $\overline{k}$. In the latter case, $\Phi_{\overline{k}/k'} = \Phi^\ell_{\overline{k}/k}$. We have $k^\dagger(C) \subset k^\dagger(C')$ and $L(C) \subset L(C')$. We get a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L(C')/k'(C')) & = & T_\ell(C') \rtimes \langle \Phi_{\overline{k}/k'} \rangle_\ell \\ \downarrow & & \downarrow \pi_* \\ \mathrm{Gal}(L(C)/k(C)) & = & T_\ell(C) \rtimes \langle \Phi_{\overline{k}/k} \rangle_\ell \end{array} \tag{4.4}$$

in which the left vertical homomorphism results from restricting automorphisms of $L(C')$ to $L(C)$ and π_* is induced by the morphism $\pi : C' \to C$ associated to $k(C) \subset k'(C')$. By choosing compatible lifts of $\Phi_{\overline{k}/k'}$ and $\Phi_{\overline{k}/k}$, we can assume $\pi_*(\Phi_{\overline{k}/k'}) = \Phi^{[k':k]}_{\overline{k}/k}$. The restriction of π_* to $T_\ell(C')$ is the

natural projection to $T_\ell(C)$ induced by the morphism $\overline{k}\otimes_{k'} C' \to \overline{k}\otimes_k C$ resulting from $\pi : C' \to C$. For $y \in T_\ell(C')$ we have

$$\pi_*(\Phi_{k',C'}(y)) = \Phi_{k,C}^{[k':k]}(\pi_* y)$$

where $[k' : k] = 1$ or ℓ.

Taking maximal abelian quotients of the groups in this diagram gives a commutative diagram

$$\begin{array}{rcl} \mathrm{Gal}(L(C')/k'(C'))^{\mathrm{ab}} & = & T_\ell(C')/(1-\Phi_{k',C})T_\ell(C') \times \langle \Phi_{\overline{k}/k'}\rangle_\ell \xleftarrow{\mathrm{art}_{C'}} \mathrm{Pic}(C')_\ell \\ \mathcal{N}\downarrow & & \downarrow \mathrm{Norm}_{C'/C} \\ \mathrm{Gal}(L(C)/k(C))^{\mathrm{ab}} & = & T_\ell(C)/(1-\Phi_{k,C})T_\ell(C) \times \langle \Phi_{\overline{k}/k}\rangle_\ell \xleftarrow{\mathrm{art}_{C}} \mathrm{Pic}(C)_\ell \end{array} \tag{4.5}$$

Here $\mathcal{N}$ is induced by the previously described morphism π_* of diagram (4.4).

We must now analyze transfer maps. Recall that if H is a finite index subgroup of a group G, the transfer homomorphism $\mathrm{Ver} : G^{\mathrm{ab}} \to \mathrm{H}^{\mathrm{ab}}$ is defined in the following way. Let $\{x_i\}_i$ be a set of left coset representatives for H in G. For $\gamma \in G$, write $\gamma x_i = x_j h_i(\gamma)$ for some index j depending on i and γ and some $h_i(\gamma) \in H$. Then Ver sends the image $\overline{\gamma}$ of γ in G^{ab} to the image in H^{ab} of $\prod_i h_i(\gamma)$. We need to analyze this map when $G = \mathrm{Gal}(L(C')/k(C))$ and $H = \mathrm{Gal}(L(C')/k'(C'))$. Note that $G^{\mathrm{ab}} = \mathrm{Gal}(L(C)/k(C))^{\mathrm{ab}}$ in this case.

Definition 4.1. Suppose first that $k' \neq k$. Then $\overline{k}\otimes_{k'} C' = \overline{k}\otimes_k C$, which gives an identification $T_\ell(C') = T_\ell(C)$. With this identification, define $V : T_\ell(C) \to T_\ell(C') = T_\ell(C)$ by

$$V = \sum_{i=0}^{\ell-1} \Phi_{k,C}^i \tag{4.6}$$

when we write the group law of $T_\ell(C)$ additively.

Definition 4.2. Suppose now that $k' = k$. There is an exact sequence

$$1 \to \mathrm{Gal}(L(C')/k^\dagger(C')) \to \mathrm{Gal}(L(C')/k^\dagger(C)) \to \mathrm{Gal}(k^\dagger(C')/k^\dagger(C)) \to 1 \tag{4.7}$$

with canonical identifications

$$\mathrm{Gal}(L(C')/k^\dagger(C')) = T_\ell(C') \quad \text{and} \quad \mathrm{Gal}(L(C')/k^\dagger(C))^{\mathrm{ab}} = \mathrm{Gal}(L(C)/k^\dagger(C)) = T_\ell(C)$$

and in which $\mathrm{Gal}(k^\dagger(C')/k^\dagger(C))$ is cyclic of order ℓ. For $\sigma \in \mathrm{Gal}(k^\dagger(C')/k^\dagger(C))$, let $\tilde{\sigma}$ be a lift of σ to $\mathrm{Gal}(L(C')/k^\dagger(C))$. Let $s_\sigma : T_\ell(C') \to T_\ell(C')$ be the automorphism given by conjugation by $\tilde{\sigma}$. If $y \in T_\ell(C) = \mathrm{Gal}(L(C)/k^\dagger(C))$, let y' be any lift of y to $\mathrm{Gal}(L(C')/k^\dagger(C))$. Define $V : T_\ell(C) \to T_\ell(C')$ by

$$V(y) = \sum_{\sigma \in \mathrm{Gal}(k^\dagger(C')/k^\dagger(C))} s_\sigma(y') \quad \text{if} \quad y \in \mathrm{Gal}(L(C)/k^\dagger(C')) \quad \text{and} \quad V(y) = (y')^\ell \quad \text{otherwise.} \tag{4.8}$$

Lemma 4.3. *There is a commutative diagram*

$$\begin{array}{rcl} T_\ell(C) \longrightarrow \mathrm{Gal}(L(C)/k(C))^{\mathrm{ab}} & = & T_\ell(C)/(1-\Phi_{k,C})T_\ell(C) \times \langle \Phi_{\overline{k}/k}\rangle_\ell \xleftarrow{\mathrm{art}_{C}} \mathrm{Pic}(C)_\ell \\ V\downarrow \quad \mathrm{Ver}\downarrow & & \downarrow \pi^* \\ T_\ell(C') \longrightarrow \mathrm{Gal}(L(C')/k'(C'))^{\mathrm{ab}} & = & T_\ell(C')/(1-\Phi_{k',C'})T_\ell(C') \times \langle \Phi_{\overline{k}/k'}\rangle_\ell \xleftarrow{\mathrm{art}_{C'}} \mathrm{Pic}(C')_\ell \end{array} \tag{4.9}$$

in which Ver *is the transfer map, and V is as in Definitions 4.1 and 4.2.*

Proof. This is just a matter of unwinding the definitions when $G = \mathrm{Gal}(L(C')/k(C))$ and $H = \mathrm{Gal}(L(C')/k'(C'))$. If $k' \neq k$, we can choose the set of coset representatives for H in G to be $\{\Phi_{\overline{k}/k}^{-i}\}_{i=0}^{\ell-1}$. If $k' = k$, pick any $y_0 \in \mathrm{Gal}(L(C')/k^\dagger(C))$ that is non-trivial on $k^\dagger(C')$, and use the set of coset representatives $\{y_0^{-i}\}_{i=0}^{\ell-1}$. If $y \in \mathrm{Gal}(L(C)/k^\dagger(C'))$, the computation of $\mathrm{Ver}(y)$ with this set

of representatives leads to $V(y)$ as defined in (4.8). If $y \in \mathrm{Gal}(L(C)/k^\dagger(C))$ does not fix $k^\dagger(C')$, we just pick y_0 to be the lift y' of y chosen in Definition 4.2, and this leads to $V(y) = \mathrm{Ver}(y) = (y')^\ell$. $\square$

Corollary 4.4. *There is a commutative diagram*

$$\begin{array}{ccccc} T_\ell(C) & \longrightarrow & T_\ell(C)/(1-\Phi_{k,C})T_\ell(C) & \xleftarrow[\cong]{\mathrm{art}_C} & \mathrm{Pic}^0(C)[\ell^\infty] \\ \Big\downarrow{\scriptstyle V} & & & & \Big\downarrow{\scriptstyle \pi^*} \\ T_\ell(C') & \longrightarrow & T_\ell(C')/(1-\Phi_{k',C'})T_\ell(C') & \xleftarrow[\cong]{\mathrm{art}_{C'}} & \mathrm{Pic}^0(C')[\ell^\infty] \end{array} \tag{4.10}$$

If $k' \neq k$, then $T_\ell(C')$ is canonically identified with $T_\ell(C)$. With this identification, $V(1-\Phi_{k,C})T_\ell(C) = (1-\Phi_{k',C'})T_\ell(C)$ and both V and π^* are injective.

There is one further case which will be important later.

Lemma 4.5. *Suppose C has genus 1, 0_C is a point of C with residue field k and that $\mathrm{Pic}^0(C)[\ell]$ is not cyclic. Suppose $a \in D(C)$ is normalized at 0_C and represents a non-trivial class $[a] \in \mathrm{H}^1(C, \mu_\ell)_{0_C}$. Then 0_C splits in $k(C') = k(C)(a^{1/\ell})$ and C' is a genus 1 curve with constant field $k' = k$. Let Δ be the subgroup of of $\mathrm{Pic}^0(C')$ generated by divisors of degree 0 supported on $\pi^{-1}(0_C)$. Then Δ has order ℓ and is the image $\mathrm{Ver}(\mathrm{Pic}^0(C)[\ell])$ of the transfer map on the ℓ torsion of $\mathrm{Pic}^0(C)$.*

Proof. Since $a \in D(C)$ is normalized at 0_C, a is an ℓ-th power in the completion of $k(C)$ at 0_C. Since $[a]$ is non-trivial, it follows that 0_C splits in the cyclic degree ℓ unramified extension $k(C')$ of $k(C)$. Hence $k(C')$ has constant field $k' = k$, and the Hurwitz formula shows C' has genus 1. Choose a point $0'_{C'}$ of C' over 0_C. Then C and C' become elliptic curves with origins 0_C and $0'_C$, and $\pi : C' \to C$ is a cyclic isogeny of degree ℓ. The the maximal pro-ℓ unramified extension of $k^\dagger(C)$ has constant field $k^\dagger$ and results from a projective system of elliptic curves covering $k^\dagger \otimes_k C$. Therefore this extension is $L(C)$, so $L(C) = L(C')$. Hence the natural homomorphism

$$T_\ell(C') = \mathrm{Gal}(L(C')/k^\dagger(C')) = \mathrm{Gal}(L(C)/k^\dagger(C')) \to T_\ell(C) = \mathrm{Gal}(L(C)/k^\dagger(C))$$

is injective with cyclic cokernel of order ℓ. Viewing $T_\ell(C')$ in this way as an index ℓ subgroup of $T_\ell(C)$, the homomorphism $V : T_\ell(C) \to T_\ell(C')$ is induced by multiplication by ℓ on $T_\ell(C)$ because $L(C') = L(C)$ is abelian over $k^\dagger(C)$ in Definition 4.2. The action of $\mathrm{Gal}(C'/C)$ on C' is by translations by elements of a subgroup of $C'(k)$ of order ℓ. Thus the divisors of degree 0 on C' supported on $\pi^{-1}(0_C)$ form a subgroup Δ of order ℓ in $\mathrm{Pic}^0(C')$.

We have assumed that

$$\mathrm{Pic}^0(C)[\ell] = \frac{T_\ell(C)}{\ell T_\ell(C) + (\Phi_{k,C} - 1)T_\ell(C)}$$

is not cyclic. Since $T_\ell(C)$ has rank two as a $\mathbb{Z}_\ell$-module, it follows that $(\Phi_{k,C} - 1)T_\ell(C) \subset \ell T_\ell(C)$. Therefore there is an endomorphism $A : T_\ell(C) \to T_\ell(C)$ such that $\Phi_{k,C} = 1 + \ell A$. Furthermore $\Phi_{k',C'}$ is the restriction of $\Phi_{k,C}$ to $T_\ell(C') \subset T_\ell(C)$. Hence the diagram (4.10) becomes

$$\begin{array}{ccccc} T_\ell(C) & \longrightarrow & T_\ell(C)/\ell A T_\ell(C) & \xleftarrow[\cong]{\mathrm{art}_C} & \mathrm{Pic}^0(C)[\ell^\infty] \\ \Big\downarrow{\scriptstyle V=\cdot\ell} & & & & \Big\downarrow{\scriptstyle \pi^*} \\ T_\ell(C') & \longrightarrow & T_\ell(C')/\ell A T_\ell(C') & \xleftarrow[\cong]{\mathrm{art}_{C'}} & \mathrm{Pic}^0(C')[\ell^\infty] \end{array} \tag{4.11}$$

This identifies $\mathrm{Pic}^0(C)[\ell]$ with $AT_\ell(C)/\ell AT_\ell(C)$ and $V(\mathrm{Pic}^0(C)[\ell])$ with $\ell AT_\ell(C)/\ell AT_\ell(C')$. Since $T_\ell(C')$ has index ℓ in $T_\ell(C)$, this implies $V(\mathrm{Pic}^0(C)[\ell])$ has order ℓ. Furthermore, an element of $\mathrm{Pic}^0(C')[\ell^\infty]$ is in $V(\mathrm{Pic}^0(C)[\ell])$ if and only if it has trivial image under the homomorphism

$$\mathrm{Pic}^0(C')[\ell^\infty] = \frac{T_\ell(C')}{\ell AT_\ell(C')} \to \frac{T_\ell(C)}{\ell AT_\ell(C)} = \mathrm{Pic}^0(C)[\ell^\infty] \tag{4.12}$$

induced by $\pi : C' \to C$. This homomorphism is $\pi_* : \mathrm{Pic}^0(C')[\ell^\infty] \to \mathrm{Pic}^0(C)[\ell^\infty]$ by (4.4). Since π_* sends divisors of degree 0 supported on $\pi^{-1}(0_C)$ to zero, we conclude that $\Delta \subset V(\mathrm{Pic}^0(C)[\ell])$. Because these groups both have order ℓ, they are equal. □

5. Arithmetic Frobenius and Legendre derivatives

In this section, we consider restrictions of the cup product maps (1.4) and (1.3) that are connected to the derivative of the arithmetic Frobenius. We will use the notation of §4.

Proposition 5.1. *There is a unique automorphism A of $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(C)$ such that $\Phi_{k,C} = 1 + \ell A$. Multiplication by A^{-1} defines a homomorphism*

$$d\mathcal{L} : \mathrm{Pic}^0(C)[\ell] = \frac{T_\ell(C) \cap AT_\ell(C)}{\ell AT_\ell(C)} \to \frac{T_\ell(C)}{\ell T_\ell(C) + \ell AT_\ell(C)} = \mathrm{Pic}^0(C)/\ell \cdot \mathrm{Pic}^0(C) \tag{5.1}$$

which we will call the Legendre derivative of Frobenius.

Proof. By (4.10) we have an isomorphism

$$\mathrm{Pic}^0(C)[\ell^\infty] \to \frac{T_\ell(C)}{(1 - \Phi_{k,C})T_\ell(C)} = \frac{T_\ell(C)}{\ell AT_\ell(C)}.$$

Since this group is finite and $T_\ell(C)$ is a rank $2g(C)$ free $\mathbb{Z}_\ell$-submodule of $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(C)$, this implies A is an automorphism of $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(C)$. We have isomorphisms

$$\mathrm{Pic}^0(C)/\ell \cdot \mathrm{Pic}^0(C) = \mathrm{Pic}^0(C)[\ell^\infty]/\ell \cdot \mathrm{Pic}^0(C)[\ell^\infty] = \frac{T_\ell(C)}{\ell T_\ell(C) + \ell AT_\ell(C)}$$

and

$$\mathrm{Pic}^0(C)[\ell] = \frac{T_\ell(C) \cap AT_\ell(C)}{\ell AT_\ell(C)}$$

from which the proposition is clear. □

Remark 5.2. The groups $\mathrm{Pic}^0(C)[\ell]$ and $\mathrm{Pic}^0(C)/\ell \cdot \mathrm{Pic}^0(C)$ have the same order, but $d\mathcal{L}$ is not in general an isomorphism. For example, suppose C is an elliptic curve with affine equation $y^2 = x^3 - 3$ over $k = \mathbb{Z}/7$. Then C has an automorphism ζ of order 3 over k fixing y and sending x to $2x$, so C has complex multiplication by $\mathbb{Z}[\zeta]$. One finds $\#C(k) = 3$. This implies that if $\ell = 3$, $T_\ell(C)$ must be a free rank one $\mathbb{Z}_\ell[\zeta]$-module, and $\Phi_k - 1$ acts as multiplication by a uniformizing parameter in $\mathbb{Z}_\ell[\zeta]$. Since $\mathbb{Z}_\ell[\zeta]$ is quadratically ramified over $\mathbb{Z}_\ell$, it follows that A^{-1} acts by multiplication by a uniformizer in $\mathbb{Z}_\ell[\zeta]$. This forces $d\mathcal{L}$ to be the zero homomorphism. On the other hand, if C is any curve such that $\mathrm{Pic}^0(C)[\ell]$ is isomorphic to $(\mathbb{Z}/\ell)^{2g(C)}$, then A defines an automorphism of $T_\ell(C)$, and $d\mathcal{L}$ is an isomorphism. The reason for the terminology is that in the classical theory of convexity, the derivative of the Legendre transform of a differentiable function is the inverse of the derivative of the function; see [10]. It would be interesting to develop a counterpart of this theory over finite fields.

Theorem 5.3. *The restrictions of (1.4) and (1.3) in which the second argument lies in $\mathrm{H}^1(k, \mu_\ell)$ can be computed in the following way. Suppose t, a and b are as in Theorem 3.1, and $a \in k^*$, so $[a] \in \mathrm{H}^1(k, \mu_\ell) = k^*/(k^*)^\ell$. Let $[\mathfrak{b}]$ be the class in $\mathrm{Pic}^0(C)[\ell]$ of the divisor $\mathfrak{b} = \mathrm{div}_C(b)/\ell$. One has*

$$[a] \cup [b] = d\mathcal{L}([\mathfrak{b}]) \otimes a^{\frac{q-1}{\ell}} \in \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell = \mathrm{H}^2(C, \mu_\ell^{\otimes 2}) \tag{5.2}$$

and

$$t \cup [a] \cup [b] = a^{t(d\mathcal{L}([\mathfrak{b}])) \cdot (q-1)/\ell} \in \tilde{\mu}_\ell = \mathrm{H}^3(C, \mu_\ell^{\otimes 2}). \tag{5.3}$$

Moreover, $t \cup [a] \cup [b]$ depends only on the restriction of t to $\mathrm{Pic}^0(C)$.

Remark 5.4. In Theorem 5.3, it is important that the automorphism $\Phi_{k,C}$ of $T_\ell(C)$ used to define $d\mathcal{L}$ is the one arising from the arithmetic Frobenius $1_{C/k} \otimes \Phi_{\overline{k}/k}$ of $\overline{C} = C \otimes_k \overline{k}$. The geometric Frobenius endomorphism $F_{C/k} \otimes 1_{\overline{k}}$ of $\overline{C} = C \otimes_k \overline{k}$ over $\overline{k}$ is the identity map on the underlying topological space of C and that is the q^{th} power map on $\mathcal{O}_C$. In particular, $F_{C/k} \otimes 1_{\overline{k}}$ acts on $\overline{C}(\overline{k})$ by raising the coordinates of any point to the q^{th} power (see [7, p. 186 and p. 291-292]). The action of $F_{C/k} \otimes 1_{\overline{k}}$ on $T_\ell(C)$ is the inverse of the action of $\Phi_{k,C}$. In particular, if one writes the action of $\Phi_{k,C}$ on $T_\ell(C)$ as $1 + \ell A$ as in Proposition 5.1, then $F_{C/k} \otimes 1_{\overline{k}}$ acts as $(1 + \ell A)^{-1}$.

Proof of Theorem 5.3. By Theorem 3.1, formulas for the cup products (5.2) and (5.3) are obtained as follows. Choose $\alpha \in \overline{k}$ with $\alpha^\ell = a \in k^*$. Then $k' = k(\alpha)$ is the unique degree ℓ extension of k in $\overline{k}$, since by assumption, a defines a non-trivial element of $D(C)/(k(C)^*)^\ell$. The field $k(C)(\alpha)$ is the function field of a curve $C' = C \otimes_k k'$ over k'.

We have defined $\mathfrak{b} = \text{div}_C(b)/\ell \in \text{Div}(C)$. There is an element $\gamma \in k(C')$ such that $b = \text{Norm}_{k(C')/k(C)}(\gamma)$ since $k(C') = k(C) \otimes_k k'$ is a cyclic unramified (constant field) extension of $k(C)$. Let ψ_k be the automorphism of $k(C') = k(C) \otimes_k k'$ which is the identity on $k(C) \otimes 1$ and which is the Frobenius automorphism $\Phi_{k'/k}$ on $1 \otimes k' = k'$. Let $\pi : C' \to C$ be the morphism associated with the inclusion $k(C) \subset k(C')$. There is a divisor $\mathfrak{c} \in \text{Div}(C')$ such that

$$\text{div}_{C'}(\gamma) = \pi^*\mathfrak{b} + (1 - \psi_k) \cdot \mathfrak{c} \tag{5.4}$$

since $C' \to C$ is cyclic and unramified and the norm of the divisor on the right side of (5.4) is trivial. The element $\psi_k(\alpha)/\alpha = \alpha^{q-1} = a^{(q-1)/\ell}$ lies in $\tilde{\mu}_\ell$.

We obtain that the cup product

$$[a] \cup [b] \in \text{H}^2(C, \mu_\ell^{\otimes 2}) = \text{H}^2(C, \mu_\ell) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell = \text{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell$$

is given by

$$[a] \cup [b] = \left([\text{Norm}_{k(C')/k(C)}(\mathfrak{c})] + \frac{\ell}{2}[\mathfrak{b}] \right) \otimes a^{(q-1)/\ell} \tag{5.5}$$

where $[\mathfrak{d}]$ is the class in $\text{Pic}(C)$ of a divisor $\mathfrak{d}$. For $t \in \text{H}^1(C, \mathbb{Z}/\ell) = \text{Hom}(\text{Pic}(C), \mathbb{Z}/\ell)$, the triple product

$$t \cup [a] \cup [b] \in \text{H}^3(C, \mu_\ell^{\otimes 2}) = \tilde{\mu}_\ell$$

is given by

$$t \cup [a] \cup [b] = a^{t([\text{Norm}_{k(C')/k(C)}(\mathfrak{c})] + \frac{\ell}{2}[\mathfrak{b}]) \cdot (q-1)/\ell}. \tag{5.6}$$

Since the class $[\mathfrak{b}]$ lies in $\text{Pic}^0(C)[\ell]$, (5.4) shows

$$\pi^*[\mathfrak{b}] = (\psi_k - 1)[\mathfrak{c}] \quad \text{in} \quad \text{Pic}^0(C')[\ell]. \tag{5.7}$$

We now use diagram (4.9)

$$\begin{array}{ccccc} T_\ell(C) & \longrightarrow & T_\ell(C)/(1 - \Phi_{k,C})T_\ell(C) & \xleftarrow[\cong]{\text{art}_C} & \text{Pic}^0(C)[\ell^\infty] \\ {\scriptstyle V}\downarrow & & & & \downarrow{\scriptstyle \pi^*} \\ T_\ell(C) & \longrightarrow & T_\ell(C)/(1 - \Phi_{k',C})T_\ell(C) & \xleftarrow[\cong]{\text{art}_{C'}} & \text{Pic}^0(C')[\ell^\infty] \end{array} \tag{5.8}$$

of Corollary 4.4. Here since $C' = k' \otimes_k C$, and $[k' : k] = \ell$, $\Phi_{k,C}$ is the automorphism of the Tate module $T_\ell(C) = T_\ell(C')$ induced by $\psi_k = 1_C \otimes \Phi_{\overline{k}/k}$, and $\Phi_{k',C} = \Phi_{k,C}^\ell$. Write $\Phi_{k,C} = 1 + \ell A$ as in Proposition 5.1. The endomorphism $V : T_\ell(C) \to T_\ell(C)$ is

$$V = \sum_{i=0}^{\ell-1} \Phi_{k,C}^k = \sum_{i=0}^{\ell-1} (1 + \ell A)^i.$$

From (4.9) we have isomorphisms

$$\text{art}_C : \text{Pic}^0(C)[\ell^\infty] \xrightarrow{\cong} T_\ell(C)/(1 - \Phi_{k,C}) = T_\ell(C)/\ell A T_\ell(C)$$

and

$$\mathrm{art}_C : \mathrm{Pic}^0(C)[\ell] \xrightarrow{\cong} (T_\ell(C) \cap AT_\ell(C))/\ell AT_\ell(C).$$

Hence $\mathrm{art}_C([\mathfrak{b}]) = [AE]$ in $(T_\ell(C) \cap AT_\ell(C))/\ell AT_\ell(C)$ for some $E \in T_\ell(C)$ such that $AE \in T_\ell(C)$. Therefore (4.9) shows

$$\mathrm{art}_{C'} : \pi^*([\mathfrak{b}]) = [VAE] \quad \text{in} \quad T_\ell(C)/(1-\Phi_{k',C})T_\ell(C) = T_\ell(C)/(1-(1+\ell A)^\ell)T_\ell(C).$$

Here

$$VA = AV = A\sum_{i=0}^{\ell-1}(1+\ell A)^i = A\sum_{i=0}^{\ell-1}\sum_{j=0}^{i}\left(\begin{array}{c} i \\ j \end{array}\right)(\ell A)^j = \ell AU \tag{5.9}$$

where

$$U = 1 + A\sum_{i=1}^{\ell-1}\sum_{j=1}^{i}\left(\begin{array}{c} i \\ j \end{array}\right)(\ell A)^{j-1}. \tag{5.10}$$

The element $D = UE$ of $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(C)$ lies in $T_\ell(C)$ since E and AE are both in $T_\ell(C)$. We have

$$\mathrm{art}_{C'}(\pi^*[\mathfrak{b}]) = [VAE] = [\ell AUE] = [\ell AD] = (\Phi_{k,C} - 1)[D] \tag{5.11}$$

where on the right $[D]$ means the class of D in $T_\ell(C)/(1-\Phi_{k',C})T_\ell(C) = \mathrm{Pic}^0(C')[\ell^\infty]$.

The action of $\Phi_{k,C}$ on $T_\ell(C)$ gives the action of ψ_k on $\mathrm{Pic}^0(C')[\ell^\infty]$. When we let $\mathfrak{c} \in \mathrm{Div}(C')$ be as in (5.4), we have

$$[\pi^*\mathfrak{b}] = (\psi_k - 1)[\mathfrak{c}] \quad \text{in} \quad \mathrm{Pic}^0(C').$$

This and (5.11) now show

$$[\mathfrak{c}] - [D] \in \mathrm{Pic}^0(C')^G \tag{5.12}$$

when $G = \mathrm{Gal}(C'/C)$ is the cyclic group of over ℓ generated by ψ_k.

We have an exact sequence

$$1 \to (k')^* \to k(C')^* \to \mathrm{Div}(C') \to \mathrm{Pic}(C') \to 1 \tag{5.13}$$

in which k' is the field of constants of $k(C')$ and the map $k(C')^* \to \mathrm{Div}(C')$ is induced by taking divisors. Splitting this into two short exact sequences and using that $\mathrm{H}^1(G, k(C')^*) = 0$ by Hilbert's theorem 90, we get exact sequences

$$\mathrm{Div}(C')^G \to \mathrm{Pic}(C')^G \to \mathrm{H}^1(G, k(C')^*/(k')^*) \to 0 \tag{5.14}$$

and

$$0 \to \mathrm{H}^1(G, k(C')^*/(k')^*) \to \mathrm{H}^2(G, (k')^*) \to \mathrm{H}^2(G, k(C')^*). \tag{5.15}$$

Since in (5.15), k'/k is a finite Galois extension with cyclic Galois group G, we have $\mathrm{H}^2(G, (k')^*) = \hat{H}^0(G, (k')^*) = 0$. We conclude from (5.14) that the map $\mathrm{Div}(C')^G \to \mathrm{Pic}(C')^G$ is surjective. However, $C' \to C$ is a cyclic unramified G-extension, so $\mathrm{Div}(C')^G = \pi^*\mathrm{Div}(C)$. Using this in (5.12) shows that there is a divisor $\mathfrak{e}$ on C such that

$$[\mathfrak{c}] = [D] + \pi^*[\mathfrak{e}]. \tag{5.16}$$

We now have

$$\begin{aligned} \mathrm{Norm}_{k(C')/k(C)}[\mathfrak{c}] &= \mathrm{Norm}_{k(C')/k(C)}([D]) + \mathrm{Norm}_{k(C')/k(C)}\pi^*[\mathfrak{e}] \\ &= \mathrm{Norm}_{k(C')/k(C)}([D]) + \ell \cdot [\mathfrak{e}]. \end{aligned} \tag{5.17}$$

Recall now that $D \in T_\ell(C)$ has the property that

$$\mathrm{art}_{C'}(\pi^*[\mathfrak{b}]) = [\ell AD] \quad \text{in} \quad T_\ell(C)/(1-\Phi_{k',C})T_\ell(C) = \mathrm{Pic}^0(C')[\ell^\infty].$$

By diagram (4.5),

$$\mathrm{Norm}_{C'/C}([D]) = [D] \quad \text{in} \quad T_\ell(C)/(1-\Phi_{k,C})T_\ell(C) = \mathrm{Pic}^0(C)[\ell^\infty]. \tag{5.18}$$

Formula (5.5) together with (5.17) and (5.18) now give

$$[a] \cup [b] = (\mathrm{Norm}_{k(C')/k(C)}[\mathfrak{c}] + \frac{\ell}{2}[\mathfrak{b}]) \otimes a^{(q-1)/\ell} = ([D] + \frac{\ell}{2}[\mathfrak{b}]) \otimes a^{(q-1)/\ell} \tag{5.19}$$

since $\ell \cdot [\mathfrak{c}] \otimes a^{(q-1)/\ell} = \ell \cdot ([\mathfrak{c}] \otimes a^{(q-1)/\ell})$ is trivial. On the right side of (5.19), $[D]$ and $[\mathfrak{b}]$ are classes in $T_\ell(C)/(1 - \Phi_{k,C})T_\ell(C) = \mathrm{Pic}^0(C)[\ell^\infty]$. We need to show that

$$([D] + \frac{\ell}{2}[\mathfrak{b}]) = d\mathcal{L}([\mathfrak{b}]) \quad \text{in} \quad T_\ell(C)/(\ell T_\ell(C) + \ell A T_\ell(C)) = \mathrm{Pic}^0(C)/\ell \cdot \mathrm{Pic}^0(C). \tag{5.20}$$

Recall that we chose $E \in T_\ell(C)$ so that $AE \in T_\ell(C)$ and

$$\mathrm{art}_C([\mathfrak{b}]) = [AE].$$

The definition of $d\mathcal{L}$ then shows that

$$d\mathcal{L}([\mathfrak{b}]) = [E] \quad \text{in} \quad T_\ell(C)/(\ell T_\ell(C) + \ell A T_\ell(C)) = \mathrm{Pic}^0(C)/\ell \cdot \mathrm{Pic}^0(C). \tag{5.21}$$

Concerning the left side of (5.20), $D = UE$ when U is as in (5.10). If $\ell > 2$ then $\frac{\ell}{2}[\mathfrak{b}] = 0$ in $\mathrm{Pic}^0(C)/\ell \cdot \mathrm{Pic}^0(C)$ since 2 is then invertible mod ℓ. So (5.20) for $\ell > 2$ is equivalent to

$$[UE] - [E] = 0 \quad \text{in} \quad \frac{T_\ell(C)}{\ell T_\ell(C) + \ell A T_\ell(C)} \quad \text{when} \quad \ell > 2. \tag{5.22}$$

We have

$$U - 1 = A \sum_{i=1}^{\ell-1} \sum_{j=1}^{i} \left(\begin{array}{c} i \\ j \end{array} \right) (\ell A)^{j-1} = A \frac{\ell(\ell-1)}{2} + (\sum_{i=1}^{\ell-1} \sum_{j=2}^{i} (\ell A)^{j-1}) A.$$

So

$$[UE] - [E] = \frac{\ell(\ell-1)}{2}[AE] + (\sum_{i=1}^{\ell-1} \sum_{j=2}^{i} (\ell A)^{j-1})[AE] = 0 \quad \text{in} \quad \frac{T_\ell(C)}{\ell T_\ell(C) + \ell A T_\ell(C)} \quad \text{when} \quad \ell > 2$$

as required since $2|(\ell - 1)$, $AE \in T_\ell(C)$, $E \in T_\ell(C)$ and ℓA is an endomorphism of $T_\ell(C)$. Suppose now that $\ell = 2$. Then (5.20) is equivalent to

$$[UE] + [AE] - [E] = 0 \quad \text{in} \quad \frac{T_\ell(C)}{\ell T_\ell(C) + \ell A T_\ell(C)} \quad \text{when} \quad \ell = 2. \tag{5.23}$$

We have

$$U + A - 1 = U - 1 + A = 2A = \ell A \quad \text{when} \quad \ell = 2$$

from which (5.23) is clear because $E \in T_\ell(C)$. □

6. The genus 1 case

In this section, we focus on the genus one case. We will use the following additional hypotheses and notations throughout this section.

Notation 6.1. The curve C is a curve over k of genus 1, and 0_C is a closed point of C having residue field degree $d(0_C)$ prime to ℓ. Suppose $a, b \in D(C)$ define non-trivial classes $[a], [b] \in \mathrm{H}^1(C, \mu_\ell)$. Define $\mathfrak{a} = \mathrm{div}_C(a)/\ell$ and $\mathfrak{b} = \mathrm{div}_C(b)/\ell$ in $\mathrm{Div}(C)$. Fix a uniformizing parameter π_{0_C} at 0_C. Let $r, s \in k^*$ be constants such that the leading term in the Laurent expansions of $\tilde{a} = a/r$ and $\tilde{b} = b/s$ with respect to π_{0_C} at 0_C lie in $(k^*)^\ell$. Let $d\mathcal{L} : \mathrm{Pic}^0(C)[\ell] \to \mathrm{Pic}^0(C)/\ell \cdot \mathrm{Pic}^0(C)$ be the arithmetic Legendre derivative from Proposition 5.1. Let $\langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} \in \tilde{\mu}_\ell$ be the value of the Weil pairing on the divisor classes $[\mathfrak{a}], [\mathfrak{b}] \in \mathrm{Pic}^0(C)[\ell]$. Define $[0_C]$ to be the class in $\mathrm{Pic}(C)$ of the divisor of degree $d(0_C)$ defined by the origin.

Theorem 6.2. *Suppose $\ell > 2$. The cup product $[a] \cup [b]$ in $\mathrm{H}^2(C, \mu_\ell^{\otimes 2}) = \mathrm{Pic}(C) \otimes \tilde{\mu}_\ell$ is given by*

$$\begin{aligned} [a] \cup [b] &= [\tilde{a}] \cup [\tilde{b}] + [r] \cup [\tilde{b}] + [\tilde{a}] \cup [s] \\ &= \frac{1}{d(0_C)} \cdot ([0_C] \otimes \langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}}) + d\mathcal{L}([\mathfrak{b}]) \otimes r^{\frac{q-1}{\ell}} - d\mathcal{L}(([\mathfrak{a}])) \otimes s^{\frac{q-1}{\ell}} \end{aligned} \tag{6.1}$$

Remark 6.3. Miller's algorithm in [6] computes $\langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\text{Weil}}$ using normalized functions $\tilde{a}$ and $\tilde{b}$ for which $\mathfrak{a} = \text{div}_C(\tilde{a})/\ell$ and $\mathfrak{b} = \text{div}_C(\tilde{b})/\ell$. For $\ell > 2$, Theorem 6.2 shows that computing the cup product $[\tilde{a}] \cup [\tilde{b}] = [0_C] \otimes \langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\text{Weil}}$ in $\text{Pic}(C) \otimes \tilde{\mu}_\ell$ over the finite field k is no more difficult than computing the Weil pairing value $\langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\text{Weil}}$. In particular, Miller's algorithm shows $[\tilde{a}] \cup [\tilde{b}]$ can be computed in polynomial time. We do not know whether the Legendre transform terms in Theorem 6.2 can be determined in polynomial time when a and b are not normalized.

The analogous result for $\ell = 2$ turns out to be more complicated.

Theorem 6.4. *Suppose $\ell = 2$.*

i. *Suppose one of $[\mathfrak{a}]$ or $[\mathfrak{b}]$ is trivial in $\text{Pic}^0(C)[\ell]$. The let $\zeta = \zeta'' = 1$.*
ii. *Suppose $[\mathfrak{a}] \neq 0 \neq [\mathfrak{b}]$ and $\langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\text{Weil}} = 1$. Then let $\zeta = (-1)^{(q-1)/2}$ and $\zeta'' = -1$.*
iii. *Suppose $\langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\text{Weil}} \neq 1$. Then let $\zeta'' = 1$. There are unique $\zeta, \zeta' \in \tilde{\mu}_2 = \{\pm 1\}$ such that in the group $\text{Pic}^0(C)/2 \otimes \tilde{\mu}_2$ we have*

$$d\mathcal{L}([\mathfrak{a}]) \otimes \zeta + d\mathcal{L}([\mathfrak{b}]) \otimes \zeta' = ([\mathfrak{a}] - [\mathfrak{b}]) \otimes (-1). \tag{6.2}$$

In all cases, we obtain

$$\begin{aligned} [a] \cup [b] &= [\tilde{a}] \cup [\tilde{b}] + [r] \cup [\tilde{b}] + [\tilde{a}] \cup [s] \\ &= \left(\frac{1}{d(0_C)} [0_C] + [\mathfrak{b}] \right) \otimes \langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\text{Weil}} + [\mathfrak{a}] \otimes \zeta'' + d\mathcal{L}([\mathfrak{b}]) \otimes r^{\frac{q-1}{\ell}} - d\mathcal{L}([\mathfrak{a}]) \otimes \zeta^{-1} s^{\frac{q-1}{\ell}}. \end{aligned} \tag{6.3}$$

Remark 6.5. In (6.3), the term $[\mathfrak{a}] \otimes \zeta''$ is non-zero only in case (ii) and only when $[\mathfrak{a}] \in \text{Pic}^0(C)[2]$ is not trivial in $\text{Pic}(C)/2 \cdot \text{Pic}(C)$.

Proof of Theorems 6.2 and 6.4. The first equality in each of (6.1) and (6.3) is clear from the bilinearity of cup products, since $[r] \cup [s]$ is trivial by Corollary 2.7.

Because cup products of elements in $\text{H}^1(C, \mu_\ell)$ are anti-commutative, Theorem 5.3 implies that to complete the proof of (6.1) and (6.3), it will suffice to show the following equalities:

$$[\tilde{a}] \cup [\tilde{b}] = \frac{1}{d(0_C)} [0_C] \otimes \langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\text{Weil}} \quad \text{if} \quad \ell > 2. \tag{6.4}$$

$$[\tilde{a}] \cup [\tilde{b}] = \left(\frac{1}{d(0_C)} [0_C] + [\mathfrak{b}] \right) \otimes \langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\text{Weil}} + [\mathfrak{a}] \otimes \zeta'' + d\mathcal{L}([\mathfrak{a}]) \otimes \zeta \quad \text{if} \quad \ell = 2. \tag{6.5}$$

We first show that we can reduce to the case $d(0_C) = 1$. Let $C' = k(0_C) \otimes_k C$ and let $\pi : C' \to C$ be the base change morphism. Let $0_{C'}$ be a point of C' over 0_C. Then $\text{Norm}_{C'/C}(0_{C'}) = 0_C$ since 0_C splits from C to C', and $0_{C'}$ has degree 1 over the constant field $k(0_C)$ of C'. Suppose the counterparts of (6.4) and (6.5) hold for the pullbacks of $[\tilde{a}], [\tilde{b}]$ from C to C'. We will use $d\mathcal{L}_C$ for the Legendre derivative over C, and $d\mathcal{L}_{C'}$ for the Legendre derivative over C'. Let $[\mathfrak{a}]' \in \text{Pic}^0(C')$ be the image of $[\mathfrak{a}] \in \text{Pic}^0(C)$ under the natural pullback map $\text{Pic}^0(C) \to \text{Pic}^0(C')$. We need to compare $\text{Norm}(\mathcal{L}_{C'}[\mathfrak{a}]')$ with $\mathcal{L}_C[\mathfrak{a}]$. One way to do this is to pick $\psi \in k^*$ such that $\psi^{\frac{q-1}{\ell}} = \gamma$ generates $\tilde{\mu}_\ell$. Then

$$d\mathcal{L}_C([\mathfrak{a}]) \otimes \gamma = d\mathcal{L}_C([\mathfrak{a}]) \otimes \psi^{\frac{q-1}{\ell}} = \psi \cup [a]$$

by Theorem 5.3. Similarly, on C' we have

$$d\mathcal{L}_{C'}([\mathfrak{a}']) \otimes \psi^{(q^{d(0_C)}-1)/\ell} = \psi \cup [a]'.$$

Here

$$\frac{q^{d(0_C)} - 1}{\ell} = \frac{q-1}{\ell} \cdot (1 + q + \cdots q^{d(0_C)-1}) \equiv \frac{q-1}{\ell} \cdot d(0_C) \mod \ell$$

since $q \equiv 1 \bmod \ell$. Therefore

$$\psi^{(q^{d(0_C)}-1)/\ell} = \gamma^{d(0_C)}$$

so on C' one has

$$d\mathcal{L}_{C'}([\mathfrak{a}'] \otimes \gamma^{d(0_C)} = \psi \cup [a]'.$$

The pullback of $\psi \cup [a]$ from C to C' is just $\psi \cup [a]'$, and the composition of this pullback with $\mathrm{Norm} \otimes \mathrm{Id}$ is multiplication by $d(0_C)$. Combining the above computations now shows

$$\mathrm{Norm}(d\mathcal{L}_{C'}([\mathfrak{a}']) \otimes \gamma = \frac{1}{d(0_C)} \cdot (\mathrm{Norm} \otimes \mathrm{Id})(\psi \cup [a]') = d\mathcal{L}_C([\mathfrak{a}]) \otimes \gamma.$$

This forces

$$\mathrm{Norm}(d\mathcal{L}_{C'}([\mathfrak{a}']) = d\mathcal{L}_C([\mathfrak{a}]).$$

We now find from this and Theorem 2.9 that the validity of (6.4) and (6.5) for the pullbacks of $[\tilde{a}], [\tilde{b}]$ from C to C' implies that these formulas hold for $[\tilde{a}], [\tilde{b}]$ over C. Thus we can assume from now on that $d(0_C) = 1$.

Suppose first that $\langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} = 1$ and that either $\ell > 2$ or $\ell = 2$ and one of $[\mathfrak{a}]$ or $[\mathfrak{b}]$ is trivial. We want to simply show that

$$[\tilde{a}] \cup [\tilde{b}] = 0. \tag{6.6}$$

Since the Weil pairing is non-degenerate, $[\mathfrak{a}]$ and $[\mathfrak{b}]$ together generate a cyclic subgroup of $\mathrm{Pic}^0(C)[\ell]$. Cup products are anti-commutative and bilinear. So it suffices to show (6.6) is true after replacing either a or b by a power of themselves that is prime to ℓ and after switching a and b if necessary. So we can reduce to two cases: (i) $[\mathfrak{b}]$ is 0, or (ii) $[\mathfrak{b}] = [\mathfrak{a}]$ in $\mathrm{Pic}^0(C)[\ell]$. Moreover, if $\ell = 2$ we need to consider only case (i). The cup product $[\tilde{a}] \cup [\tilde{b}]$ does not change if we multiply either a or b by the ℓ^{th} power of an element of $k(C)^*$. This means that the above cases reduce to (i) $\mathfrak{b} = 0$ or (ii) $\mathfrak{b} = \mathfrak{a}$ in $\mathrm{Div}(C)$. Since $\tilde{a}$ and $\tilde{b}$ are normalized, these cases reduce further to either (i) $[\tilde{b}] = 0$ or (ii) $[\tilde{b}] = [\tilde{a}]$ in $D(C)$. In case (i), we immediately obtain (6.6). In particular, we are done when $\ell = 2$. If $\ell > 2$, then cup products are alternating, which implies (6.6) also in case (ii).

Suppose now that $\langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} = 1$, $\ell = 2$ and $[\mathfrak{a}] \neq 0 \neq [\mathfrak{b}]$. Then the non-degeneracy of the Weil pairing implies $[\mathfrak{a}] = [\mathfrak{b}] \neq 0$. As in the previous paragraph, we can reduce to the case in which $\mathfrak{a} = \mathfrak{b}$ in $\mathrm{Div}(C)$. Hence $\mathrm{div}_C(\tilde{a}) = \mathrm{div}_C(\tilde{b}) = \ell\mathfrak{a} = \ell\mathfrak{b}$, so $\tilde{a} = \tilde{b}$ because $\tilde{a}$ and $\tilde{b}$ are normalized. Let C' be the smooth projective curve in Theorem 3.1 with function field $k(C') = k(C)(\tilde{a}^{1/\ell}) = k(C)(\tilde{a}^{1/2})$, and let $\pi : C' \to C$ be the morphism associated to the inclusion $k(C) \subset k(C')$. Here $k(C')$ is a quadratic extension of $k(C)$ since $[\mathfrak{a}] \neq 0$ in $\mathrm{Pic}^0(C)[2]$. The element $\gamma' = \tilde{a}^{1/2}$ of $k(C')$ has norm $b' = -\tilde{a}$ to $k(C)$. We have

$$2\ \mathrm{div}_{C'}(\gamma') - 2\ \pi^*(\mathfrak{b}) = \mathrm{div}_{C'}(\tilde{a}) - \pi^*(2\mathfrak{a}) = \mathrm{div}_{C'}(\tilde{a}) - \pi^*(\mathrm{div}_C(\tilde{a})) = 0.$$

Hence

$$\mathrm{div}_{C'}(\gamma') - \pi^*(\mathfrak{b}) = 0$$

and the formula of Theorem 3.1 shows

$$[\tilde{a}] \cup [b'] = [\mathfrak{b}] \otimes (-1) = [\mathfrak{a}] \otimes (-1).$$

However, $-b' = \tilde{a} = \tilde{b}$ so we conclude

$$[\tilde{a}] \cup [\tilde{b}] = [\tilde{a}] \cup [b' \cdot (-1)] = [\tilde{a}] \cup [b'] + [\tilde{a}] \cup [-1] = [\mathfrak{a}] \otimes (-1) - d\mathcal{L}([\mathfrak{a}]) \otimes (-1)^{(q-1)/2}$$

by Theorem 5.3 and the anticommutativity of cup products. This shows (6.5) since

$$d\mathcal{L}([\mathfrak{a}]) \otimes (-1)^{(q-1)/2} = -d\mathcal{L}([\mathfrak{a}]) \otimes (-1)^{(q-1)/2}.$$

For the rest of the proof we assume $\langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} \neq 1$. We again use the formula of Theorem 3.1 for $[\tilde{a}] \cup [\tilde{b}]$. Let C' be the smooth projective curve with function field $k(C') = k(C)(\tilde{a}^{1/\ell})$, and let $\pi : C' \to C$ be the morphism associated to the inclusion $k(C) \subset k(C')$. Let $\mathrm{Art}_{C'/C} : \mathrm{Pic}(C) \to \mathrm{Gal}(k(C')/k(C))$ be the Artin map, and let $\sigma_{\mathfrak{b}} = \mathrm{Art}_{C'/C}(\mathfrak{b})$. By [4, ?],

$$\langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} = \frac{\sigma_{\mathfrak{b}}(\tilde{a}^{1/\ell})}{\tilde{a}^{1/\ell}}. \tag{6.7}$$

Since this is non-trivial, we see that $\sigma_{\mathfrak{b}}$ is a generator of $\mathrm{Gal}(k(C')/k(C))$. As in Theorem 3.1, there is a $\gamma \in k(C')^*$ so that $\mathrm{Norm}_{k(C')/k(C)}(\gamma) = \tilde{b}$. Then the divisor $\mathrm{div}_{C'}(\gamma) - \pi^*(\mathfrak{b})$ has norm

$$\mathrm{div}_C(\mathrm{Norm}_{k(C')/k(C)}(\gamma)) - \ell \cdot \mathfrak{b} = \mathrm{div}_C(\tilde{b}) - \ell \cdot \mathfrak{b} = 0.$$

Since $k(C')/k(C)$ is cyclic degree ℓ and unramified,

$$\mathrm{div}_{C'}(\gamma) - \pi^*(\mathfrak{b}) = (1 - \sigma_{\mathfrak{b}}) \cdot \mathfrak{c}$$

for some divisor $\mathfrak{c}$ on C'. Theorem 3.1 and (6.7) show

$$[\tilde{a}] \cup [\tilde{b}] = \left[\mathrm{Norm}_{k(C')/k(C)}(\mathfrak{c}) + \frac{\ell}{2}\mathfrak{b}\right] \otimes \langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} \tag{6.8}$$

in $\mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell$.

The pullback map $\pi^* : \mathrm{Div}(C) \to \mathrm{Div}(C')$ induces the transfer homomorphism $\mathrm{Ver} : \mathrm{Pic}(C) \to \mathrm{Pic}(C')$. Therefore the class $[\pi^*(\mathfrak{b})]$ lies in $\mathrm{Ver}(\mathrm{Pic}^0(C)[\ell])$. By Lemma 4.5, there is a point $P \in \pi^{-1}(0_C)$ such that $[\pi^*\mathfrak{b}] = [P] - [0_{C'}]$ in $\mathrm{Pic}^0(C')$. Hence there is a function $\gamma' \in k(C')^*$ such that

$$\mathrm{div}_{C'}(\gamma') - \pi^*(\mathfrak{b}) = [0_{C'}] - [P] \quad \text{in} \quad \mathrm{Div}(C'). \tag{6.9}$$

Since $\pi(P) = \pi(0_{C'}) = 0_C$ and $\mathfrak{b} = \mathrm{div}_C(b)/\ell$ this gives

$$\mathrm{div}_C(\mathrm{Norm}_{k(C')/k(C)}(\gamma')) - \mathrm{div}_C(b) = \mathrm{Norm}_{C'/C}\left(\mathrm{div}_{C'}(\gamma') - \pi^*(\mathfrak{b})\right) = 0 \quad \text{in} \quad \mathrm{Div}(C).$$

Thus $b' = \mathrm{Norm}_{k(C')/k(C)}(\gamma')$ must equal $\tilde{b}z$ for some constant $z \in k^*$, since $b = s\tilde{b}$ for some $s \in k^*$. Because of (6.9), there is a divisor $\mathfrak{c}'$ supported on $\pi^{-1}(0_C)$ such that

$$\mathrm{div}_{C'}(\gamma') - \pi^*(\mathfrak{b}) = [0_{C'}] - [P] = (1 - \sigma_{\mathfrak{b}}) \cdot \mathfrak{c}'$$

since $\pi : C' \to C$ is unramified and 0_C splits in this cover. We now apply Theorem 3.1 with a and b replaced by $\tilde{a}$ and b', and with γ replaced by γ'. From (6.8) we find

$$[\tilde{a}] \cup [b'] = \left[\mathrm{Norm}_{k(C')/k(C)}(\mathfrak{c}') + \frac{\ell}{2}\mathfrak{b}\right] \otimes \langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} \tag{6.10}$$

since $\mathfrak{b}$ equals $\mathfrak{b}' = \mathrm{div}_C(b')/\ell$ as well as $\tilde{\mathfrak{b}} = \mathrm{div}_C(\tilde{b})/\ell$. Here $\mathrm{Norm}_{k(C')/k(C)}(\mathfrak{c}') = \tau \cdot [0_C]$ for some integer τ since $\mathfrak{c}'$ is supported on $\pi^{-1}(0_C)$. Because $b' = \tilde{b}z$ we conclude finally from Theorem 5.3 that

$$\begin{aligned} [\tilde{a}] \cup [\tilde{b}] &= [\tilde{a}] \cup [b'] - [\tilde{a}] \cup [z] \\ &= [\tilde{a}] \cup [b'] + [z] \cup [\tilde{a}] \\ &= \left(\tau \cdot [0_C] + \frac{\ell}{2}[\mathfrak{b}]\right) \otimes \langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} + d\mathcal{L}([\mathfrak{a}]) \otimes z^{\frac{q-1}{\ell}}. \end{aligned} \tag{6.11}$$

Applying $\deg_C \otimes \mathrm{Id}$ to (6.11) and using Lemma 3.3 shows $\tau \equiv 1 \bmod \ell$, since $\langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} \neq 1$ and the degrees of $[0_C]$, $\mathfrak{a}$ and $\mathfrak{b}$ are 1, 0 and 0, respectively. So we have

$$[\tilde{a}] \cup [\tilde{b}] = \left([0_C] + \frac{\ell}{2}[\mathfrak{b}]\right) \otimes \langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} + d\mathcal{L}([\mathfrak{a}]) \otimes z^{\frac{q-1}{\ell}}. \tag{6.12}$$

Reversing the roles of a and b in (6.12) and using the fact that cup products and the Weil pairing are both anti-commutative leads to a formula of the form

$$[\tilde{a}] \cup [\tilde{b}] = \left([0_C] + \frac{\ell}{2}[\mathfrak{a}]\right) \otimes \langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} - d\mathcal{L}([\mathfrak{b}]) \otimes (z')^{\frac{q-1}{\ell}} \tag{6.13}$$

for some $z' \in k^*$. Subtracting (6.13) from (6.12) leads to

$$d\mathcal{L}([\mathfrak{a}]) \otimes z^{\frac{q-1}{\ell}} + d\mathcal{L}([\mathfrak{b}]) \otimes (z')^{\frac{q-1}{\ell}} = \frac{\ell}{2}([\mathfrak{a}] - [\mathfrak{b}]) \otimes \langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}}. \tag{6.14}$$

We now use the fact that $[\mathfrak{a}]$ and $[\mathfrak{b}]$ generate independent order ℓ subgroups of $\mathrm{Pic}^0(C)[\ell]$ since $\langle [\mathfrak{a}], [\mathfrak{b}] \rangle_{\mathrm{Weil}} \neq 1$. Therefore, Remark 5.2 shows $d\mathcal{L} : \mathrm{Pic}^0(C)[\ell] \to \mathrm{Pic}^0(C)/\ell \cdot \mathrm{Pic}^0(C)$ is an isomorphism. Hence $d\mathcal{L}([\mathfrak{a}])$ and $d\mathcal{L}([\mathfrak{b}])$ must be a basis for the $\mathbb{Z}/\ell$ vector space $\mathrm{Pic}^0(C)/\ell \cdot \mathrm{Pic}^0(C)$.

It now follows from (6.14) that the elements $z^{\frac{q-1}{\ell}}$ and $(z')^{\frac{q-1}{\ell}}$ are uniquely determined by the element $\frac{\ell}{2}([\mathfrak{a}]-[\mathfrak{b}])\otimes\langle[\mathfrak{a}],[\mathfrak{b}]\rangle_{\mathrm{Weil}}$ in $\mathrm{Pic}^0(C)/\ell\cdot\mathrm{Pic}^0(C)\otimes_{\mathbb{Z}/\ell}\tilde{\mu}_\ell$. This element is trivial if $\ell>2$, and if $\ell=2$ we know $\langle[\mathfrak{a}],[\mathfrak{b}]\rangle_{\mathrm{Weil}}$ is non-trivial, so $\langle[\mathfrak{a}],[\mathfrak{b}]\rangle_{\mathrm{Weil}}=-1\in\tilde{\mu}_2$ in this case. This leads to (6.4) and (6.5). □

7. Cup products of normalized classes on curves of arbitrary positive genus

Throughout this section we will suppose that C is a smooth projective geometrically irreducible curve over the finite field k of genus $g\geq 1$. We suppose as before that $\tilde{\mu}_\ell\subset k^*$. Since C is geometrically irreducible over k, there is a divisor of C that has degree 1 by [11, Cor. 5, §VII.5], which implies there must a point 0_C for which $d(0_C)$ is prime to ℓ. The goal of this section is to prove the following result.

Theorem 7.1. *Suppose $\ell>2$ or that $\ell=2$ and the normalized classes $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ do not have dimension 1. The following two conditions are equivalent:*

i. *The image of the cup product map $\mathrm{H}^1(C,\mu_\ell)\times\mathrm{H}^1(C,\mu_\ell)\to\mathrm{H}^2(C,\mu_\ell^{\otimes 2})$ on pairs of classes in $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ spans a $\mathbb{Z}/\ell$-subspace of $\mathrm{H}^2(C,\mu_\ell^{\otimes 2})$ of dimension at most one.*
ii. *For all classes $[a],[b]\in\mathrm{H}^1(C,\mu_\ell)_{0_C}$, the cup product $[a]\cup[b]$ in $\mathrm{H}^2(C,\mu_\ell^{\otimes 2})=\mathrm{Pic}(C)\otimes_{\mathbb{Z}}\tilde{\mu}_\ell$ equals $\frac{1}{d(0_C)}\cdot([0_C]\otimes\langle[a],[b]\rangle_{\mathrm{Weil}})$.*

Remark 7.2. In the next section, we will give an infinite family of curves of genus $g=2$ for which neither (i) nor (ii) of Theorem 7.1 hold when $\ell=3$.

Remark 7.3. Suppose C has genus 1. If $\ell>2$, the normalized classes $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ have dimension at most two, and the cup product pairing is alternating. Hence condition (i) of Theorem 7.1 holds.

Suppose now that $\ell=2$, so that q is odd. Let V be the subspace of $\mathrm{H}^2(C,\mu_\ell^{\otimes 2})$ spanned by cup products of elements of $\mathrm{H}^1(C,\mu_\ell)_{0_C}$. The dimension of $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ over $\mathbb{Z}/\ell=\mathbb{Z}/2$ is between 0 and 2, and $V=\{0\}$ if $\mathrm{H}^1(C,\mu_\ell)_{0_C}=\{0\}$.

Suppose $0\neq[a]\in\mathrm{H}^1(C,\mu_\ell)_{0_C}$. Then $\mathfrak{a}=\mathrm{div}_C(a)/\ell$ defines a non-trivial class $[\mathfrak{a}]\in\mathrm{Pic}^0(C)[\ell]$. Since the Weil pairing is alternating, Theorem 6.4 gives

$$[a]\cup[a]=[\mathfrak{a}]\otimes(-1)+d\mathcal{L}([\mathfrak{a}])\otimes(-1)^{(q-1)/2}\quad\text{in}\quad\mathrm{Pic}(C)\otimes_{\mathbb{Z}}\tilde{\mu}_\ell=\mathrm{H}^2(C,\mu_\ell^{\otimes 2}) \tag{7.1}$$

where $d\mathcal{L}:\mathrm{Pic}^0(C)[\ell]\to\mathrm{Pic}^0(C)/\ell\cdot\mathrm{Pic}^0(C)$ is the Legendre derivative defined in Proposition 5.1. If $q\equiv 1 \bmod 4$ then $(-1)^{(q-1)/2}=1$ and this formula shows $[a]\cup[a]$ is the class $[a]\otimes(-1)$. This shows that if $q\equiv 1 \bmod 4$, the span V_0 of all classes of the form $[a]\cup[a]$ with $[a]\in\mathrm{H}^0(C,\mu_\ell)_{0_C}$ is the image of the natural homomorphism

$$\iota:\quad\mathrm{Pic}^0(C)[\ell]\otimes_{\mathbb{Z}}\tilde{\mu}_\ell\to\mathrm{Pic}(C)\otimes_{\mathbb{Z}}\tilde{\mu}_\ell$$

induced by the inclusion $\mathrm{Pic}^0(C)\subset\mathrm{Pic}(C)$. If $q\equiv 3 \bmod 4$, a similar analysis shows V_0 is the image of the homomorphism

$$\iota+(d\mathcal{L}\otimes\mathrm{Id}):\quad\mathrm{Pic}^0(C)[\ell]\otimes_{\mathbb{Z}}\tilde{\mu}_\ell\to\mathrm{Pic}(C)\otimes_{\mathbb{Z}}\tilde{\mu}_\ell.$$

Note that in either case V_0 has trivial image under $\deg\otimes\mathrm{Id}:\mathrm{Pic}(C)\otimes\tilde{\mu}_\ell\to\tilde{\mu}_\ell$.

Suppose now that $[a]$ and $[b]$ are distinct non-zero elements of $\mathrm{H}^1(C,\mu_\ell)_{0_C}$. Such elements exist if and only if $\dim_{\mathbb{Z}/2}\mathrm{H}^1(C,\mu_\ell)_{0_C}=2$. All cup products $[a]\cup[b]$ arising from such pairs are congruent mod V_0, and they do not lie in V_0 because their image under $\deg\otimes\mathrm{Id}$ is the Weil pairing $\langle[\mathfrak{a}],[\mathfrak{b}]\rangle_{\mathrm{Weil}}=-1$. Thus $\dim_{\mathbb{Z}/\ell}(V)=\dim_{\mathbb{Z}/\ell}(V_0)+1$ if $\dim_{\mathbb{Z}/2}\mathrm{H}^1(C,\mu_\ell)_{0_C}=2$, and $V=V_0$ otherwise.

Proof of Theorem 7.1. It is clear that (ii) implies (i), so we now show that (i) implies (ii).

Suppose first that the normalized classes $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ have dimension at most 1. If $\ell>2$, both the cup product of elements of $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ and the Weil pairing are alternating, so condition (ii) holds. When $\ell=2$ our hypotheses force $\mathrm{H}^1(C,\mu_\ell)_{0_C}=\{0\}$ so (ii) again holds.

We suppose from now on that $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ has dimension greater than 1. The restriction map sends $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ isomorphically to $\mathrm{H}^1(\overline{C},\mu_\ell)$. Since the Weil pairing is non-degenerate, for each

non-trivial class $[a] \in \mathrm{H}^1(C,\mu_\ell)_{0_C}$, there is a class $[b] \in \mathrm{H}^1(C,\mu_\ell)_{0_C}$ such that the Weil pairing of $[a]$ and $[b]$ is non-trivial. Hence $[a]\cup[b]$ is non-trivial in $\mathrm{H}^2(C,\mu_\ell^{\otimes 2}) = \mathrm{Pic}(C)\otimes_{\mathbb{Z}}\tilde{\mu}_\ell$. Hence $[a]\cup[b] = [D]\otimes\zeta \neq 0$ for some class $[D]\in\mathrm{Pic}(C)$ and some non-trivial $\zeta\in\tilde{\mu}_\ell$. Since the map $\deg\otimes\mathrm{Id} : \mathrm{Pic}(C)\otimes_{\mathbb{Z}}\tilde{\mu}\to\tilde{\mu}$ takes $[a]\cup[b]$ to $\langle[a],[b]\rangle_{\mathrm{Weil}}$, we can assume D has degree $d(0_C)$ mod ℓ and that

$$(\deg\otimes\mathrm{Id})(D\otimes\zeta) = \zeta^{d(0_C)} = \langle[a],[b]\rangle_{\mathrm{Weil}} \neq 1.$$

To prove that (ii) holds, it will suffice to show

$$[D] = [0_C] \quad \text{in} \quad \mathrm{Pic}(C)/\ell\cdot\mathrm{Pic}(C) \tag{7.2}$$

since then

$$[a]\cup[b] = [0_C]\otimes\zeta = \frac{1}{d(0_C)}\left([0_C]\otimes\zeta^{d(0_C)}\right) = \frac{1}{d(0_C)}([0_C]\otimes\langle[a],[b]\rangle_{\mathrm{Weil}}).$$

Let $[a']\in\mathrm{H}^1(C,\mu_\ell)_{0_C}$ be arbitrary. Suppose first that $[a']\cup[a']$ is not zero, so $\ell = 2$ since the cup product is anti-commutative. Then $[a']\cup[a'] = [D']\otimes\zeta'$ for some divisor D' and some non-trivial $\zeta'\in\tilde{\mu}_\ell$. The Weil pairing is alternating (see, for example, [4, Theorem 1]). The degree of D' would have to be divisible by ℓ, since $\deg\otimes\mathrm{Id}$ sends $[a']\cup[a'] = [D']\otimes\zeta'$ to $\langle[a'],[a']\rangle_{\mathrm{Weil}} = 1$. But now $[a]\cup[b] = [D]\otimes\zeta$ and $[a']\cup[a'] = [D']\otimes\zeta'$ span a two dimensional subspace of $\mathrm{Pic}(C)\otimes\tilde{\mu}_\ell$, contradiction hypothesis (i). Hence $[a']\cup[a'] = 0$ for all $[a']\in\mathrm{H}^1(C,\mu_\ell)_{0_C}$.

For each non-trivial $[a']\in\mathrm{H}^1(C,\mu_\ell)_{0_C}$, we can pick a $[b']\in\mathrm{H}^1(C,\mu_\ell)_{0_C}$ so $[a']\cup[b']$ is non-trivial. Hypothesis (i) then implies that $[a']\cup[b']$ is a non-zero multiple of $[D]\otimes\zeta$. Since $[a']\cup[a']\cup[b'] = ([a']\cup[a'])\cup[b'] = 0\cup[b']$ is trivial, we conclude that $[a']\cup([D]\otimes\zeta)$ must be trivial in $\mathrm{H}^3(C,\mu_\ell^{\otimes 3})$ for all $[a']\in\mathrm{H}^1(C,\mu_\ell)_{0_C}$.

Now the class $[a']\in\mathrm{H}^1(C,\mu_\ell)_{0_C}$ defines a class $\alpha'\in\mathrm{H}^1(C,\mathbb{Z}/\ell)$ via a choice of isomorphism $\xi : \mathbb{Z}/\ell\to\tilde{\mu}_\ell$. Here $[a']$ is identified with the element of $\mathrm{Hom}(\pi_1(C),\mu_\ell) = \mathrm{H}^1(C,\mu_\ell)$ arising from Kummer theory via the map sending $\sigma\in\pi_1(C)$ to $\sigma((a')^{1/\ell})/(a')^{1/\ell}$. Thus α' is the element of $\mathrm{Hom}(\pi_1(C),\mathbb{Z}/\ell) = \mathrm{H}^1(C,\mathbb{Z}/\ell)$ arising from this Kummer map and the identification ξ. In particular, α' factors through the Galois group $\mathrm{Gal}(k(C)((a')^{1/\ell})/k(C))$, and 0_C splits in $k(C)((a')^{1/\ell})$ because a' is normalized at 0_C. Via class field theory, α' corresponds to an element of $\mathrm{Hom}(\mathrm{Pic}(C),\mathbb{Z}/\ell)$ which is trivial on the class $[0_C]\in\mathrm{Pic}(C)$, since the decomposition group of a place of $k(C)((a')^{1/\ell})$ over the place of $k(C)$ associated to 0_C is trivial.

We have shown that the cup product $[a']\cup([D]\otimes\zeta)$ is trivial in $\mathrm{H}^3(C,\mu_\ell^{\otimes 3})$. Since ζ is non-trivial, this implies that the cup product of $\alpha'\in\mathrm{H}^1(C,\mathbb{Z}/\ell)$ with $[D]\in\mathrm{H}^2(C,\mu_\ell) = \mathrm{Pic}(C)/\ell\cdot\mathrm{Pic}(C)$ is trivial in $\mathrm{H}^3(C,\mu_\ell) = \mathbb{Z}/\ell$. The identification of $\mathrm{H}^1(C,\mathbb{Z}/\ell)$ with $\mathrm{Hom}(\mathrm{Pic}(C),\mathrm{Z}/\ell)$ and $\mathrm{H}^2(C,\mu_\ell)$ with $\mathrm{Pic}(C)/\ell\cdot\mathrm{Pic}(C)$ makes the cup product

$$\mathrm{H}^1(C,\mathbb{Z}/\ell)\times\mathrm{H}^2(C,\mu_\ell)\to\mathrm{H}^3(C,\mu_\ell) = \mathbb{Z}/\ell \tag{7.3}$$

simply the evaluation homomorphism

$$\mathrm{Hom}(\mathrm{Pic}(C),\mathbb{Z}/\ell)\times\mathrm{Pic}(C)/\ell\cdot\mathrm{Pic}(C)\to\mathbb{Z}/\ell.$$

Hence the above arguments show

$$\alpha'\cup[0_C] = 0 = \alpha'\cup[D] \quad \text{in} \quad \mathrm{H}^3(C,\mu_\ell) \tag{7.4}$$

for all α' associated to normalized classes $[a']\in\mathrm{H}^1(C,\mu_\ell)_{0_C}$. However, the pairing (7.3) is non-degenerate, and $\mathrm{H}^1(C,\mu_\ell)_{0_C}$ is a codimension one subspace of $\mathrm{H}^1(C,\mu_\ell)$. Hence (7.4) forces $[D]$ and $[0_C]$ to lie in a common one-dimensional $\mathbb{Z}/\ell$-subspace of $\mathrm{Pic}(C)/\ell\cdot\mathrm{Pic}(C)$. Since both $[D]$ and $[0_C]$ have degree $d(0_C)$ mod ℓ, we conclude (7.2) holds and that (ii) is true. □

8. An infinite family of genus two examples

The goal of this section is to construct an infinite family of curves of genus $g = 2$ for which neither (i) nor (ii) of Theorem 7.1 hold when $\ell = 3$.

Let $\zeta\in\mathbb{C}$ be a primitive cube root of unity, and let $F = \mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$. Define E to be the elliptic curve over F defined by $y^2 = x^3 - 3$, and let $\pi : E\to\mathbb{P}^1_F$ be the morphism associated to the

inclusion of function fields $F(x) \subset F(E) = F(x)[y]/(y^2 - x^3 + 3)$. Let Y be the smooth projective curve with function field $F(E)(x^{1/2})$ and let $\eta : Y \to E$ be the natural morphism. Then η is of degree 2 and ramified over the points $Q_1 = (0, \sqrt{-3})$ and $Q_2 = (0, -\sqrt{-3})$ in (x, y) coordinates on E, so Y has genus 2 by the Hurwitz formula.

Letting $\tilde{y} = y/x^{3/2} \in F(Y)$ we see that the function field $F(x)[\tilde{y}]/(\tilde{y}^2 - 1 + 3x^{-3})$ of the elliptic curve $E' : \tilde{y}^2 = 1 - 3x^{-3}$ is contained in $F(Y)$. The morphism $\eta' : Y \to E'$ associated to the containment $F(E') \subset F(Y)$ is of degree 2. We see from this that $F(Y)$ is a biquadratic extension of $F(x)$ with intermediate fields $F(E)$, $F(x^{1/2})$ and $F(E')$. Let $\pi' : E' \to \mathbb{P}^1_F$ be associated to $F(x) \subset F(E')$. The point $x = \infty$ on $\mathbb{P}^1_F$ is a branch point of $\pi : E \to \mathbb{P}^1_F$ and splits under $\pi' : E' \to \mathbb{P}^1_F$. So there are two points 0_Y and $0'_Y$ of Y over $x = \infty$ on $\mathbb{P}^1_F$.

Lemma 8.1. *Let N be a number field containing F and let $Y_N = N \otimes_F Y$, $E_N = N \otimes_F E$ and $E'_N = N \otimes_F E'$. The direct image homomorphisms $\eta_* : \mathrm{Pic}^0(Y_N) \to \mathrm{Pic}^0(E_N)$ and $\eta'_* : \mathrm{Pic}^0(Y_N) \to \mathrm{Pic}^0(E'_N)$ give a homomorphism*

$$\eta_* \times \eta'_* : \mathrm{Pic}^0(Y_N) \to \mathrm{Pic}^0(E_N) \times \mathrm{Pic}^0(E'_N) \tag{8.1}$$

whose kernel and cokernel are finite groups annihilated by 2.

Proof. We have pullback maps $\eta^* : \mathrm{Pic}^0(E_N) \to \mathrm{Pic}^0(Y_N)$ and $\eta'^* : \mathrm{Pic}^0(E_N) \to \mathrm{Pic}^0(Y_N)$ such that $\eta_* \circ \eta^*$ and $\eta'_* \circ \eta'^*$ are multiplication by 2. Furthermore, $\eta'_* \circ \eta^* = \pi'^* \circ \pi_*$ and $\eta_* \circ \eta'^* = \pi^* \circ \pi'_*$ are trivial since $\mathrm{Pic}^0(\mathbb{P}^1_N)$ is trivial. Hence the composition

$$(\eta_* \times \eta'_*) \circ (\pi^* \times \pi'^*) : \mathrm{Pic}^0(E_N) \times \mathrm{Pic}^0(E'_N) \to \mathrm{Pic}^0(E_N) \times \mathrm{Pic}^0(E'_N)$$

is multiplication by 2. Since all the groups appearing in (8.1) are finitely generated abelian groups, it will suffice to show that the kernel $\mathcal{K}$ of $\eta_* \times \eta'_*$ is annihilated by 2. View Y_N as a Galois cover of $\mathbb{P}^1_N$ with Galois group G a Klein four group. The three intermediate quadratic covers are E, E' and the projective line over N with function field $N(x^{1/2})$. Since the latter projective line has trivial Jacobian, we see $\mathcal{K}$ is annihilated by the group ring element $1 + \sigma$ for each non-trivial $\sigma \in G$. The sum of these three group ring elements is $2 + \mathrm{Trace}_G$. Hence 2 annihilates $\mathcal{K}$ because the action of Trace_G on $\mathrm{Pic}^0(Y_N)$ factors through $\mathrm{Pic}^0(\mathbb{P}^1_N) = 0$. □

The following lemma is clear from the functorial properties of Jacobians.

Lemma 8.2. *Let X be a geometrically integral curve of genus 1 over a perfect field K, and suppose $\tilde{0}_X$ is an arbitrary point of $X(K)$. Then X becomes an elliptic curve with origin $\tilde{0}_X$ via the morphism from X to its Jacobian sending $\tilde{0}_X$ to the origin.*

i. *Suppose $1 \leq n \in \mathbb{Z}$. The n-torsion of $\mathrm{Pic}^0(X)$ will have order n^2 if and only if the set of elements $P \in X(K)$ such that $nP = \tilde{0}_X$ with respect to the group law on X has order n^2.*
ii. *Suppose $P_1, P_2 \in X(K)$. There is a class $D \in \mathrm{Pic}^0(X)$ such that $nD = [P_1] - [P_2]$ in $\mathrm{Pic}^0(X)$ if and only if there is a point $P \in X(K)$ such that in the group law on $X(K)$ one has $nP = P_1 - P_2$.*

We now return to our elliptic curves $E : y^2 = x^3 - 3$ and $E' : \tilde{y}^2 = 1 - 3x^{-3} = 1 - 3w^3$ over $F = \mathbb{Q}(\zeta)$ where $w = x^{-1}$ and ζ is a primitive third root of unity. We let ℓ be the prime 3.

Lemma 8.3. *Let N be a finite extension of F and define $E_N = N \otimes_F E$ and $E'_N = N \otimes_F E'$.*

i. *$\mathrm{Pic}^0(E_N)$ has 3-torsion of order 9 if and only if $F(12^{1/3}) \subset N$.*
ii. *$\mathrm{Pic}^0(E'_N)$ has 3-torsion of order 9 if and only if $F((4/3)^{1/3}) \subset N$.*
iii. *Let 0_Y and $0'_Y$ be the two points of Y defined just prior to the statement of Lemma 8.1. Then $\{0_Y, 0'_Y\}$ is the inverse image under $\eta : Y \to E$ of the point 0_E at infinity on the curve $E : y^2 = x^3 - 3$. We can label these points so that under $\eta' : Y \to E'$ one has $\eta'(0_Y) = (0, 1) = P_1$ and $\eta'(0'_Y) = (0, -1) = P_2$ relative to the $(w, \tilde{y})$ coordinates of $E' : \tilde{y}^2 = 1 - 3w^3$. The divisor class $[P_1] - [P_2]$ in $\mathrm{Pic}^0(E'_N)$ lies in $3 \cdot \mathrm{Pic}^0(E'_N)$ if and only if $F((4/3)^{1/3}, \zeta^{1/3}) \subset N$.*

Proof. The complex multiplication of $\zeta \in F$ on $E : y^2 = x^3 - 3$ is defined by $\zeta \cdot (x, y) = (\zeta x, y)$, while $-(x, y) = (x, -y)$ in the group law of E. Thus $(x, y) = (0, \sqrt{-3})$ and $(x, y) = (0, -\sqrt{-3})$ are fixed by ζ and therefore sent to 0 in the group law of E by $(\zeta - 1)$. Since $(\zeta^2 - 1)(\zeta - 1) = 3$ in F, these points are 3-torsion points of E over $\mathbb{Q}(\sqrt{-3}) = F$. To find the remaining 3-torsion points over $\overline{F}$, we just need a point $(x, y) \in E(\overline{F})$ such that $(\zeta^2 - 1)(x, y) = (0, \sqrt{-3})$. Here $\zeta^2(x, y) = (\zeta^2 x, y)$, $-(x, y) = (x, -y)$ and $-(0, \sqrt{-3}) = (0, -\sqrt{-3})$. So we are looking for a line of the form $cx + dy - e = 0$ containing three points of the form $(\zeta^2 x, y)$, $(x, -y)$ and $(0, -\sqrt{-3})$. Furthermore, one should not have $x = 0$, since such a solution leads to the previous points $(0, \sqrt{-3})$ and $(0, \sqrt{-3})$. Writing out the constraints on c, d and e we find $d(-\sqrt{-3}) = e$ and that there is a matrix equation

$$\begin{pmatrix} \zeta^2 x & y + \sqrt{-3} \\ x & -y + \sqrt{-3} \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{8.2}$$

Since c and d are not both 0 we find from this that

$$0 = \det \begin{pmatrix} \zeta^2 x & y + \sqrt{-3} \\ x & -y + \sqrt{-3} \end{pmatrix} = y(-\zeta^2 x - x) + \sqrt{-3}(\zeta^2 - 1)x. \tag{8.3}$$

Since $x \neq 0$ and $\zeta^2 + 1 = -\zeta$ we can divide by x to have

$$y = -\zeta^2 \sqrt{-3}(\zeta^2 - 1).$$

On squaring we get

$$x^3 - 3 = y^2 = -3\zeta(\zeta^2 - 1)^2 = -3\zeta(\zeta^4 - 2\zeta^2 + 1) = -3(\zeta^5 - 2\zeta^3 + \zeta) = -3(\zeta^2 - 2 + \zeta) = 9.$$

Thus

$$x^3 = 12 \quad \text{so} \quad x = 12^{1/3} \quad \text{and} \quad y = \pm 3.$$

This shows part (i) of the lemma.

For part (ii) we proceed similarly using the model $E' : \tilde{y}^2 = 1 - 3w^3$, with complex multiplication defined by $\zeta(w, \tilde{y}) = (\zeta w, \tilde{y})$ and $-(w, \tilde{y}) = (w, -\tilde{y})$. As the origin of E' we will use the point $\tilde{0}_{E'}$ at infinity relative to the above affine $(w, \tilde{y})$ model of E'. Note that this choice is different from the point $0_{E'}$ used in Lemma 8.1, but this does not make a difference as far as part (ii) of Lemma 8.3 is concerned because of Lemma 8.2. The points $(w, \tilde{y}) = (0, 1)$ and $(0, -1)$ are fixed by ζ and hence annihilated by $\zeta - 1$, so they are 3-torsion points. To find the remaining 3-torsion points, we look for a $(w_0, \tilde{y}_0)$ with $(\zeta^2 - 1) \cdot (w_0, \tilde{y}_0) = (0, 1)$. Thus we would need a line $cw_0 + d\tilde{y}_0 - e = 0$ containing the points $(\zeta^2 w_0, \tilde{y}_0)$, $(w_0, -\tilde{y}_0)$ and $-(0, 1) = (0, -1)$. This implies $-d - e = 0$ so $-e = d$ and

$$\begin{pmatrix} \zeta^2 w_0 & \tilde{y}_0 + 1 \\ w_0 & -\tilde{y}_0 + 1 \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{8.4}$$

Since c and d are not both 0, this gives

$$0 = \det \begin{pmatrix} \zeta^2 w_0 & \tilde{y}_0 + 1 \\ w_0 & -\tilde{y}_0 + 1 \end{pmatrix} = \tilde{y}_0(-\zeta^2 w_0 - w_0) + (\zeta^2 - 1)w_0. \tag{8.5}$$

The solution we are looking for does not have $w_0 = 0$, so we can divide by w_0 and then square to find

$$1 - 3w_0^3 = \tilde{y}_0^2 = \left(\frac{\zeta^2 - 1}{\zeta^2 + 1}\right)^2 = \zeta^{-2}(\zeta^4 - 2\zeta^2 + 1) = (\zeta^2 - 2 + \zeta) = -3. \tag{8.6}$$

Thus

$$w_0^3 = 4/3 \quad \text{and} \quad \tilde{y}_0 = \left(\frac{\zeta^2 - 1}{\zeta^2 + 1}\right) = -\sqrt{-3} \in F$$

where we set $\sqrt{-3} = 2\zeta + 1$, which leads to part (ii).

Finally, for part (iii), note that we have shown $P_1 = (0, 1)$ and $P_2 = (0, -1)$ are three torsion points on E' with $P_2 = -P_1$, so $P_1 - P_2 = 2P_1$ and $P_1 = 2 \cdot (2P_1)$. So in view of Lemma 8.2, it will suffice to determine the extension of F generated by the coordinates of a point Q with $3Q = P_1 = (0, 1)$ when the group law on E' is the one coming from the map to the Jacobian

which sends the point $\tilde{0}_{E'}$ at infinity on E' to the origin. We have found above a point $(w_0, \tilde{y}_0)$ with $(\zeta^2 - 1)(w_0, \tilde{y}_0) = (0, 1)$; this point has $w_0^3 = 4/3$ and $\tilde{y}_0$ a particular square root of -3 depending on ζ. So we now look for a point $Q = (w, \tilde{y})$ with $(\zeta - 1)(w, \tilde{y}) = (w_0, \tilde{y}_0)$; then $3Q = (\zeta^2 - 1)(\zeta - 1)(w, \tilde{y}) = (0, 1)$. Here $\zeta(w, \tilde{y}) = (\zeta w, \tilde{y})$ and $-(w, \tilde{y}) = (w, -\tilde{y})$ and $-(w_0, \tilde{y}_0) = (w_0, -\tilde{y}_0)$. So we are looking for a line

$$c(w - w_0) + d(\tilde{y} + \tilde{y}_0) - e = 0 \tag{8.7}$$

containing $(\zeta w, \tilde{y})$, $(w, -\tilde{y})$ and $(w_0, -\tilde{y}_0)$. Here if $w = w_0$ then $(w, \tilde{y}) = \pm(w_0, \tilde{y}_0)$ and

$$(\zeta - 1)(w, \tilde{y}) = \pm(\zeta - 1)(w_0, \tilde{y}_0) = \mp\zeta(\zeta^2 - 1)(w_0, \tilde{y}_0) = \mp\zeta(0, 1) = (0, \mp 1) \neq (w_0, \tilde{y}_0).$$

So we can assume $w \neq w_0$, and similarly we can assume $\zeta w \neq w_0$, so the three points $(\zeta w, \tilde{y})$, $(w, -\tilde{y})$ and $(w_0, -\tilde{y}_0)$ are distinct. In order for the point $(w_0, -\tilde{y}_0)$ to be on the line (8.7) we must have $-e = 0$. The remaining two points $(\zeta w, \tilde{y})$, $(w, -\tilde{y})$ are on the line if and only if

$$\begin{pmatrix} \zeta w - w_0 & \tilde{y} + \tilde{y}_0 \\ w - w_0 & -\tilde{y} + \tilde{y}_0 \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \tag{8.8}$$

Since c and d are not both 0, we conclude

$$\begin{aligned} 0 = \det \begin{pmatrix} \zeta w - w_0 & \tilde{y} + \tilde{y}_0 \\ w - w_0 & -\tilde{y} + \tilde{y}_0 \end{pmatrix} &= (\zeta w - w_0) \cdot (-\tilde{y} + \tilde{y}_0) - (\tilde{y} + \tilde{y}_0) \cdot (w - w_0) \\ &= \tilde{y}((-\zeta - 1)w + 2w_0) + (\zeta - 1)w\tilde{y}_0. \end{aligned}$$

Since $-\zeta - 1 = \zeta^2$ we get

$$\tilde{y}(\zeta^2 w + 2w_0) = (1 - \zeta)w\tilde{y}_0 \tag{8.9}$$

so on squaring this we find

$$(1 - 3w^3)(\zeta^2 w + 2w_0)^2 = (1 - \zeta)^2 w^2 (-3).$$

Writing $(\zeta^2 w + 2w_0)^2 = \zeta^4 w^2 + 4\zeta^2 w_0 w + 4w_0^2$ we end up with an equality

$$-3(\zeta^4 w^5 + 4\zeta^2 w_0 w^4 + 4w_0^2 w^3) + (\zeta^4 + 3(1 - \zeta)^2)w^2 + 4\zeta^2 w_0 w + 4w_0^2 = 0.$$

We know $w \neq w_0$ and $w \neq \zeta^{-1} w_0 = \zeta^2 w_0$, so we divide the left hand side by $(w - w_0)(w - \zeta^2 w_0) = w^2 - (1 + \zeta^2)w_0 w + \zeta^2 w_0^2 = w^2 + \zeta w_0 w + \zeta^2 w_0^2$. This gives

$$-3\zeta w^3 - 9\zeta^2 w_0 w^2 + 4\zeta = 0.$$

Dividing by -3ζ gives

$$w^3 + 3\zeta w_0 w^2 - 4/3 = 0. \tag{8.10}$$

We now write down the roots of this equation using Cardano's formulas. Write

$$a = 3\zeta w_0, \quad b = 0, \quad c = -4/3$$

so our equation is

$$w^3 + aw^2 + bw + c = 0.$$

Write

$$p = \frac{1}{3}(3b - a^2) = \frac{1}{3}(-9\zeta^2 w_0^2) = -3\zeta^2 w_0^2,$$

$$q = \frac{1}{27}(2a^3 - 9ab + 27c) = 2w_0^3 - 4/3 = 2(4/3) - 4/3 = 4/3,$$

$$D = -4p^3 - 27q^2 = -4(-27w_0^6) - 27(4/3)^2 = 4 \cdot 27 \cdot (4/3)^2 - 27 \cdot (4/3)^2 = 4^2 3^2,$$

$$A^3 = \frac{-27q}{2} + \frac{3}{2}\sqrt{-3D} = -\frac{27}{2} \cdot \frac{4}{3} + \frac{3}{2}\sqrt{-3^3 4^2} = 36\zeta,$$

$$B^3 = \frac{-27q}{2} - \frac{3}{2}\sqrt{-3D} = 36\zeta^2.$$

The roots w are then

$$\frac{A+B}{3};\quad \frac{\zeta^2 A+\zeta B}{3};\quad \frac{\zeta A+\zeta^2 B}{3}.$$

We conclude that the extension of F generated by w is $F((36\zeta)^{1/3})$. We have from (8.9) that

$$\tilde{y}/w = (1-\zeta)\tilde{y}_0/(\zeta^2 w + 2w_0).$$

Since $\tilde{y}_0 = \pm\sqrt{-3} \in F$, we conclude that w and $\tilde{y}$ generate over F the same extension as w and w_0. So the extension of F generated by w and $\tilde{y}$ is $F((36\zeta)^{1/3},(4/3)^{1/3}) = F(36^{1/3},\zeta^{1/3}) = F((4/3)^{1/3},\zeta^{1/3})$. This completes the proof of part (iii). □

Corollary 8.4. *Let $\mathcal{E}$, $\mathcal{E}'$ and $\mathcal{Y}$ be the projective curves over $\mathbb{Z}$ defined by the affine equations used to define E, E' and Y. For $\mathcal{C} = \mathcal{E}, \mathcal{E}'$ or $\mathcal{Y}$ let $\mathcal{C}_q$ be the reduction of $\mathcal{C}$ modulo the prime q. Suppose q splits in the field $N = F(4^{1/3}, 3^{1/3})$ but does not split in the extension $N(\zeta^{1/3})$.*

i. *The 3-torsion subgroup of $\mathrm{Pic}^0(\mathcal{Y}_q)$ is isomorphic to $(\mathbb{Z}/3)^4 = (\mathbb{Z}/3)^{2g(\mathcal{Y}_q)}$.*
ii. *The point $0_{\mathcal{E}_q}$ at infinity associated to the affine model $\mathcal{E}_q : y^2 = x^3 - 3$ splits into two points $0_{\mathcal{Y}_q}$ and $0'_{\mathcal{Y}_q}$ via the morphism $\mathcal{Y}_q \to \mathcal{E}_q$ associated to the field embedding $(\mathbb{Z}/q)(\mathcal{E}_q) \subset (\mathbb{Z}/q)(\mathcal{Y}_q)$.*
iii. *The divisor class $[0_{\mathcal{Y}_q}] - [0'_{\mathcal{Y}_q}]$ in $\mathrm{Pic}^0(\mathcal{Y}_q)$ does not lie in $3 \cdot \mathrm{Pic}(\mathcal{Y}_q)$.*

Proof. By Lemma 8.3, the 3-torsion on the general fibers of $\mathcal{E}$ and $\mathcal{E}'$ is defined over N, so these torsion points define sections of the natural morphisms $\mathcal{E}_N = \mathrm{Spec}(O_N) \otimes_{\mathbb{Z}} \mathcal{E} \to \mathrm{Spec}(O_N)$ and $\mathcal{E}'_N = \mathrm{Spec}(O_N) \otimes_{\mathbb{Z}} \mathcal{E}' \to \mathrm{Spec}(O_N)$. Since q must be larger than 3, these sections specialize to distinct 3-torsion points of the fibers of $\mathcal{E}_N$ and $\mathcal{E}'_N$ over a prime of O_N over q. Since q splits in O_N, these fibers are isomorphic to $\mathcal{E}_q$ and $\mathcal{E}'_q$, respectively. This shows (i) because the same arguments used in the proof of Lemma 8.1 show the natural direct image homomorphism $\mathrm{Pic}^0(\mathcal{Y}_q) \to \mathrm{Pic}^0(\mathcal{E}_q) \times \mathrm{Pic}^0(\mathcal{E}'_q)$ has kernel and cokernel equal to finite abelian groups annihilated by 2.

Part (ii) follows from the corresponding fact on the generic fibers of $\mathcal{Y}$ and $\mathcal{E}$. Finally, for (iii), it suffices to show that the image D of $[0_{\mathcal{Y}_q}] - [0'_{\mathcal{Y}_q}]$ in $\mathrm{Pic}^0(\mathcal{E}'_q)$ does not lie in $3 \cdot \mathrm{Pic}^0(\mathcal{E}'_q)$. Setting $w = x^{-1}$ defines the affine model $\mathcal{E}'_q : \tilde{y}^2 = 1 - 3w^3$ when $\tilde{y} = y/x^{3/2}$. Let $0_{\mathcal{E}'_q}$ be the point at infinity for this model. Then $D = [P_1] - [P_2]$ when $P_{1,q} = (0,1)$ and $P_{2,q} = (0,-1)$ in $(w,\tilde{y})$ coordinates. Here $[P_{2,q}] = -[P_{1,q}]$ in $\mathrm{Pic}^0(\mathcal{E}'_q)$ and $(\zeta - 1)[P_{1,q}] = 0$ relative to the complex multiplication action of $\mathbb{Z}[\zeta] = O_F$ on $\mathcal{E}'_q$ defined by $\zeta(w,\tilde{y}) = (\zeta w, \tilde{y})$. So $[P_{1,q}]$ is a three torsion point when we use $0_{\mathcal{E}'_q}$ as the origin of the group law of $\mathcal{E}'_q$. Lemma 8.2 shows that $D = [P_{1,q}] - [P_{2,q}]$ lies in $3 \cdot \mathrm{Pic}(\mathcal{E}'_q)$ if and only if $P_{1,q} - P_{2,q} = 2P_{1,q}$ lies in $3 \cdot \mathcal{E}'_q(\mathbb{Z}/q)$ relative the group law of $\mathcal{E}'_q(\mathbb{Z}/q)$. Since $P_{1,q}$ is a 3-torsion point, this will be true if and only if $P_{1,q}$ lies in $3 \cdot \mathcal{E}'_q(\mathbb{Z}/q)$. However, $P_{1,q}$ is the intersection of the fiber of $\mathcal{E}'_N$ over a chosen prime $\mathfrak{q}$ of O_N over q with the corresponding point P_1 on the general fiber of $\mathcal{E}'_N$, i.e. the point P_1 with $(w,\tilde{y})$ coordinates $(0,1)$. Multiplication by 3 defines an étale morphism of abelian schemes $\mathbb{Z}[\frac{1}{6}] \otimes \mathcal{E}'_N \to \mathbb{Z}[\frac{1}{6}] \otimes \mathcal{E}'_N$. The pullback of the section defined by P_1 is a divisor $\mathcal{P}$ on $\mathbb{Z}[\frac{1}{6}] \otimes \mathcal{E}'_N$ which is étale over this section. Therefore $\mathcal{P}$ must be a disjoint union of divisors of the form $\mathrm{Spec}(\mathcal{O})$ in which $\mathcal{O}$ is the integral closure of $\mathbb{Z}[\frac{1}{6}]$ in the residue field L of a closed point P' of E'_N such that $3 \cdot P' = P_1$. By Lemma 8.3, L must contain $N(\zeta^{1/3})$, and by construction $\mathfrak{q}$ is a prime of O_N inert to $N(\zeta^{1/3})$ which is prime to 6. Any point of the fiber of $\mathcal{E}'_N$ over $\mathfrak{q}$ which when multiplied by 3 gives $P_{1,q}$ must lie on the intersection of $\mathcal{P}$ with this fiber. Because $N(\zeta^{1/3}) \subset L$, there is no point of this intersection with residue field $O_N/\mathfrak{q} = \mathbb{Z}/q$. This implies (iii). □

Remark 8.5. By the Cebotarev density theorem, the set of rational primes q that have the properties in Corollary 8.4 has Dirichlet density $1/18 - 1/54 = 1/27$. The prime $q = 439$ is an example.

Theorem 8.6. *The conclusion of Theorem 6.2 need not hold if C is allowed to have genus greater than 1. More specifically, with the notations of Corollary 8.4, let C be the curve $\mathcal{Y}_q$ and let 0_C be either one of the points $0_{\mathcal{Y}_q}$ or $0'_{\mathcal{Y}_q}$. There are $a, b \in k(\mathcal{E}_q)^*$ that are normalized at $0_{\mathcal{E}_q}$ such that*

the associated classes $[a],[b] \in \mathrm{H}^1(\mathcal{E}_q,\mu_\ell)$ *have non-trivial Weil pairing. Let* $\eta : C = \mathcal{Y}_q \to \mathcal{E}_q$ *be the morphism associated to the construction of* $\mathcal{Y}_q$*. The pullbacks* $\eta^*[a],\eta^*[b] \in \mathrm{H}^1(C,\mu_\ell)$ *are normalized classes at* 0_C*, but the cup product of these classes is not equal to* $\frac{1}{d(0_C)}\left([0_C] \otimes \langle \eta^*[a],\eta^*[b]\rangle_{\mathrm{Weil}}\right)$ *in* $\mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_\ell$*.*

Proof. By Corollary 8.4, the $\ell = 3$ torsion of $\mathrm{Pic}(\mathcal{E}_q)$ is isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/3$. So there are $a,b \in k(\mathcal{E}_q)^*$ normalized at $0_{\mathcal{E}_q}$ such that $\langle [a],[b]\rangle_{Weil,\mathcal{E}_q} \neq 1$ with respect to the Weil pairing on $\mathcal{E}_q$. Here if $\overline{k}$ is an algebraic closure of k, $\langle [a],[b]\rangle_{Weil,\mathcal{E}_q}$ is the value of the cup product $\overline{[a]} \cup \overline{[b]} \in \mathrm{H}^2(\overline{k} \otimes_k \mathcal{E}_q, \mu_3^{\otimes 2}) = \tilde{\mu}_3$ when $\overline{[c]}$ is the image of $[c] \in \mathrm{H}^1(\mathcal{E}_q,\mu_3)$ under the restriction map $\mathrm{H}^1(\mathcal{E}_q,\mu_3) \to \mathrm{H}^1(\overline{k} \otimes_k \mathcal{E}_q,\mu_3)$. Cup products respect restrictions and pullbacks by η, so we find that

$$\langle \eta^*[a],\eta^*[b]\rangle_{\mathrm{Weil}} = \eta^*(\overline{[a]} \cup \overline{[b]}) \tag{8.11}$$

when η^* on the right is the pullback map

$$\eta^* : \mathrm{H}^2(\overline{k} \otimes_k \mathcal{E}_q, \mu_3^{\otimes 2}) \to \mathrm{H}^2(\overline{k} \otimes_k C, \mu_3^{\otimes 2}). \tag{8.12}$$

When we identify the domain and range of η^* in (8.12) with $\tilde{\mu}_3$, the map η^* becomes raising to the second power since $C \to \mathcal{E}_q$ is a degree two map of curves with constant field k. This and (8.11) imply $\langle \eta^*[a],\eta^*[b]\rangle_{\mathrm{Weil}}$ is a non-trivial third root of unity. Suppose now that in fact,

$$\eta^*[a] \cup \eta^*[b] = \frac{1}{d(0_C)}\left([0_C] \otimes \langle \eta^*[a],\eta^*[b]\rangle_{\mathrm{Weil}}\right) \quad \text{in} \quad \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_3 \tag{8.13}$$

where $d(0_C) = 1$. The action of the non-trivial automorphism σ of C over $\mathcal{E}_q$ fixes $\eta^*[a]$ and $\eta^*[b]$ and is equivariant with respect to cup products. The action of σ on $\mathrm{H}^2(C,\mu_3^{\otimes 2}) = \mathrm{H}^2(C,\mu_3) \otimes_{\mathbb{Z}} \tilde{\mu}_3 = \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \tilde{\mu}_3$ corresponds to $\sigma' \otimes \mathrm{Id}$ when σ' is the automorphism of $\mathrm{Pic}(C)$ induced by σ. Hence (8.13) would imply

$$\begin{aligned} \eta^*[a] \cup \eta^*[b] &= \sigma(\eta^*[a]) \cup \sigma(\eta^*[b]) = \sigma(\eta^*[a] \cup \eta^*[b]) = \sigma([0_C] \otimes \langle \eta^*[a],\eta^*[b]\rangle_{\mathrm{Weil}}) \\ &= [\sigma(0_C)] \otimes \langle \eta^*[a],\eta^*[b]\rangle_{\mathrm{Weil}}. \end{aligned} \tag{8.14}$$

Subtracting the right side of (8.14) from the right side of (8.13) we get

$$0 = ([0_C] - [\sigma(0_C)]) \otimes \langle \eta^*[a],\eta^*[b]\rangle_{\mathrm{Weil}} \quad \text{in} \quad \mathrm{Pic}(C) \otimes_{\mathbb{Z}} \mu_3.$$

Here $\langle \eta^*[a],\eta^*[b]\rangle_{\mathrm{Weil}}$ is a non-trivial third root of unity, so this would force $[0_C] - [\sigma(0_C)]$ to lie in $3 \cdot \mathrm{Pic}(C)$. However, $\{0_C,\sigma(0_C)\} = \{0_{\mathcal{Y}_q},0'_{\mathcal{Y}_q}\}$ and we have shown the difference $[0_{\mathcal{Y}_q}] - [0'_{\mathcal{Y}_q}]$ is not in $3 \cdot \mathrm{Pic}(C)$. So the contradiction shows that (8.13) cannot be true. □

References

[1] Bleher, F. M., Chinburg, T., Greenberg, R., Kakde, M., Pappas, G. and Taylor, M. J., Cup products in the étale cohomology of number fields, *New York J. Math.* 24 (2018), 514–542.

[2] Boneh, D. and Silverberg, A., Applications of multilinear forms to cryptography. *Contemporary Mathematics*, 324(1) (2003), 71–90.

[3] Deligne, P. (with Boutot, J.F., Grothendieck, A., Illusie, L. and Verdier, J. L.), Cohomologie Étale. Séminaire de Géometrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$, Lecture Notes in Mathematics, 569, Springer-Verlag, 1977.

[4] Howe, E.W., The Weil pairing and the Hilbert symbol. *Math. Ann.* 305 (1996), 387–392.

[5] McCallum, W. and Sharifi, R. A cup product in the Galois cohomology of number fields, *Duke Math. J.*, 120, no. 2 (2003), 269–310.

[6] Miller, V. S., The Weil pairing and its efficient calculation, *J. Cryptology* 17 (2004), 235–261.

[7] Milne, J., Étale cohomology. Princeton University Press, 1980.

[8] Milne, J., Arithmetic Duality Theorems, second edition. Academic Press, 2006.

[9] Mumford, J., Abelian Varieties. Oxford University Press, 1970.

[10] Simon, B., Convexity. An analytic viewpoint. Cambridge Tracts in Mathematics, 187, Cambridge University Press, 2011.

[11] Weil, A., Basic Number Theory, third edition Springer Verlag, 1974.

Frauke M. Bleher, Dept. of Mathematics, Univ. of Iowa, Iowa City, IA 52242, USA
Email address: frauke-bleher@uiowa.edu

Ted Chinburg, Dept. of Mathematics, Univ. of Pennsylvania, Philadelphia, PA 19104, USA
Email address: ted@math.upenn.edu