Math. Ann. 305, 387–392 (1996)

Mathematische Annalen
© Springer-Verlag 1996

The Weil pairing and the Hilbert symbol

Everett W. Howe *

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA
(e-mail: however@math.lsa.umich.edu)

Received: 26 May 1995

Mathematics Subject Classifications (1991): 11G20, 11R37, 11R58, 14H25

1. Introduction and motivation

Let C be a geometrically irreducible curve over a field k, let $\overline{k}$ be an algebraic closure of k, and let m be any positive integer not divisible by the characteristic of k. The Jacobian variety J of C comes equipped with a principal polarization λ, which is in particular an isomorphism from J to its dual variety $\widehat{J}$. The polarization λ gives us an isomorphism between the m-torsion J_m of J and its Cartier dual, and this isomorphism turns the natural pairing $J_m \times \widehat{J}_m \longrightarrow \mu_m$ into the *Weil pairing* $e_m\colon J_m \times J_m \longrightarrow \mu_m$. Suppose D and E are $\overline{k}$-divisors on C whose mth powers are principal, say $mD = \operatorname{div} f$ and $mE = \operatorname{div} g$, where f and g are $\overline{k}$-functions on C. The following well-known theorem tells how the Weil pairing on the classes of D and E in $J_m(\overline{k})$ can be calculated.

Theorem 1. *Let $[D]$ and $[E]$ denote the classes of the divisors D and E in $J_m(\overline{k})$. Then we have*

$$e_m([D],[E]) = \prod_P (-1)^{m(\operatorname{ord}_P D)(\operatorname{ord}_P E)} \frac{g^{\operatorname{ord}_P D}}{f^{\operatorname{ord}_P E}}(P), \tag{1}$$

where P ranges over the geometric points of C.

Using Weil reciprocity one can easily show that to prove Theorem 1 it is enough to prove the theorem in the special case where the divisors D and E have disjoint supports, and in this case Eq. (1) can be written in the more familiar

* Supported in part by NSA grant number MDA904-95-H-1044.

form $e_m([D],[E]) = g(D)/f(E)$. This case of the theorem follows from results found in [2, Sect. 6.4], but as far as we know the theorem is not stated explicitly in the literature except in the case where the curve C has genus one. In this special case, our pairing e_m is the same as that defined in [1, Sect. 12.3] and in [7, Sect. 3.8], and Theorem 1 occurs as Remark 3.7 in [1, Sect. 12.3] and, with a sign error, as Exercise 16 in [7, Chap. 3].

Now suppose that k is a finite field that contains the mth roots of unity, let K be the function field of the curve C, and suppose g is an element of K such that $L = K(g^{1/m})$ has degree m over K and has constant field k. The Galois group of L over K is naturally isomorphic to the group of mth roots of unity in k, and for every prime $\mathfrak{p}$ of K local class field theory gives us a homomorphism, the Artin map, from the multiplicative group of the local field $K_\mathfrak{p}$ to $\mathrm{Gal}(L/K)$. This homomorphism, evaluated on an element $a \in K_\mathfrak{p}$, is *Hilbert's norm residue symbol* $(g,a)_\mathfrak{p}^*$. A result of Schmidt ([5], see also [6, Number VI.30]) gives an explicit formula for $(g,a)_\mathfrak{p}$: we have

$$(g,a)_\mathfrak{p} = \prod_P \left((-1)^{(\mathrm{ord}_P\, a)(\mathrm{ord}_P\, g)} \frac{g^{\mathrm{ord}_P\, a}}{a^{\mathrm{ord}_P\, g}}(P) \right)^{(q-1)/m}, \tag{2}$$

where $q = \#k$ and where the product is over the primes P of $K \otimes_k \bar{k}$ lying over $\mathfrak{p}$.

The typographical similarity between Eq. (1) and Eq. (2) is striking. Motivated by a desire to explain this similarity, we provide a new proof of Theorem 1. We begin in Sections 2 and 3 by proving the theorem in the special case where the base field k is finite. Our argument, which uses Kummer theory and class field theory to relate the Weil pairing to the Hilbert symbol, shows how Eq. (1) can be obtained from Eq. (2). In Section 4 we briefly indicate how the general theorem follows from the special case where k is finite.

2. The Weil pairing, Kummer theory, and class field theory

We begin by interpreting the Weil pairing in terms of Kummer theory. For the moment we make no assumptions on k.

Let $C_{\bar{k}}$ be the curve $C \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, \bar{k}$, so that the function field of $C_{\bar{k}}$ is $K \otimes_k \bar{k}$, which we will denote by K_∞. Let M_∞ be the maximal unramified abelian extension of K_∞ whose Galois group is killed by m, and let X be the corresponding curve over $\bar{k}$. Then we know that X fits into a Cartesian square

$$\begin{tikzcd} X \arrow[r] \arrow[d] & J_{\bar{k}} \arrow[d, "m"] \\ C_{\bar{k}} \arrow[r, "\psi"] & J_{\bar{k}} \end{tikzcd}$$

where the arrow on the right hand side is the multiplication-by-m map on the Jacobian of $C_{\bar{k}}$. This diagram provides an isomorphism between $J_m(\bar{k})$ and the Galois group of M_∞ over K_∞: translation by an m-torsion point on $J_{\bar{k}}$ gets pulled back to an automorphism of X, which gives an automorphism of M_∞/K_∞. On the other hand, there is also an isomorphism φ between $J_m(\bar{k})$ and $(K_\infty^* \cap M_\infty^{*m})/K_\infty^{*m}$ defined as follows: Suppose E is a $\bar{k}$-divisor of degree 0 whose image in $J(\bar{k})$ is an m-torsion point, so that mE is a principal divisor, say the divisor of g. Then g has an mth root in M_∞, and we define $\varphi([E]) = g/K_\infty^{*m}$. Kummer theory gives us a perfect pairing

$$\mathrm{Gal}(M_\infty/K_\infty) \times (K_\infty^* \cap M_\infty^{*m})/K_\infty^{*m} \to \boldsymbol{\mu}_m(\bar{k})$$

defined by $(\sigma, g) \mapsto \sigma(g^{1/m})/g^{1/m}$, and our isomorphisms $J_m(\bar{k}) \to \mathrm{Gal}(M_\infty/K_\infty)$ and φ turn the Kummer pairing into a pairing $J_m \times J_m \to \boldsymbol{\mu}_m$. This new pairing is none other than the Weil pairing; this can be seen by combining the explicit formula for the natural pairing of the m-torsion of an abelian variety with that of its dual (see [3, Sect. 16]) with the fact that the map $\psi: C \to J$ induces an isomorphism $\psi^*: \widehat{J} \to J$ that is equal to $-\lambda^{-1}$, where λ is the polarization of J that was used in the definition of the Weil pairing (see [4, Remark 6.10]).

Now let us assume that k is a finite field. By replacing k by a finite extension field, we may assume that the Cartesian diagram above can be defined over k, and that the m-torsion points of J are all defined over k. Replace the diagram above with the corresponding diagram of k-schemes, and let M be the function field of the curve X over k, so that K and M are both function fields over the finite field k. We are now in the right situation to use class field theory.

Let F be the Frobenius endomorphism of J/k and let Y be the pullback (via the map $\psi: C \to J$) of the covering $(F-1): J \to J$. The endomorphism $F-1$ is divisible by m in $\mathrm{End}\, J$ because the m-torsion points of J are defined over k, and we have a big diagram in which all rectangles are Cartesian:

$$\begin{tikzcd}
Y \arrow[r] \arrow[d] & J \arrow[d, "(F-1)/m"] \\
X \arrow[r] \arrow[d] & J \arrow[d, "m"] \\
C \arrow[r, "\psi"] & J .
\end{tikzcd}$$

Let N be the function field of the curve Y. Then N is a maximal unramified abelian extension of K with constant field k, and the diagram gives an isomorphism between $J(k) = \ker(F-1)$ and $\mathrm{Gal}(N/K)$. This isomorphism can be described by class field theory as follows.

Let I denote the geometric idèle group of C, so that $I = \prod'_P (K_\infty)_P^*$, where the restricted direct product is taken over all primes P of K_∞ (see [6, Number VI.29]). Let I^0 denote the group of idèles of degree 0. The Galois group G of K_∞/K, which is canonically isomorphic to $\mathrm{Gal}(\bar{k}/k)$, acts continuously on I^0. Let $I^0(k)$ denote the set of elements of I^0 that are fixed by G, and let U and $U(k)$ denote the subgroups of I^0 and $I^0(k)$ consisting of unit idèles. Note that the group $I^0/K_\infty^* U$ is isomorphic to the group $J(\bar{k})$ of geometric points of J, and that the group $I^0(k)/K^* U(k)$ is isomorphic to $J(k)$. Class field theory for curves (see [6, Sect. VI.6]) tells us that the Artin map from $I^0(k)$ to $\mathrm{Gal}(N/K)$ induces the isomorphism from $J(k)$ to $\mathrm{Gal}(N/K)$ given in the preceding paragraph.

Now let notation be as in Theorem 1, and again replace k by a finite extension so that the divisors D and E are defined over k and the functions f and g are in K. By multiplying g by a constant if necessary, we may assume that g has an mth root in M, so that the field $L = K(g^{1/m})$ is contained in M. Kummer theory gives us a homomorphism $\mathrm{Gal}(L/K) \to \mu_m(k)$, and from our last diagram we obtain a commutative diagram

$$\begin{tikzcd}
I^0(k) \arrow[r] & J(k) \arrow[r, "\sim"] \arrow[d, "(F-1)/m"'] & \mathrm{Gal}(N/K) \arrow[d] & \\
& J_m(k) \arrow[r, "\sim"] & \mathrm{Gal}(M/K) \arrow[d] & \\
& & \mathrm{Gal}(L/K) \arrow[r] & \mu_m(k)
\end{tikzcd}$$

where the vertical arrows between the Galois groups are the natural restriction maps. Our comments on the Weil pairing at the start of this section show that the homomorphism $e_m(\,\cdot\,, [E]) : J_m(k) \to \mu_m(k)$ is equal to the composition $J_m(k) \cong \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K) \to \mu_m(k)$, and we know that the Artin map Ψ from $I^0(k)$ to $\mathrm{Gal}(L/K)$ is obtained by following the arrows from the upper left of the diagram to the lower right. We can calculate the Artin map by using Hilbert symbols, so the proof of Theorem 1 for finite fields is reduced to a calculation and a diagram chase.

3. A calculation

We introduce two auxiliary homomorphisms. Let $\Phi : I^0 \to \bar{k}^*$ be defined by

$$\Phi(a) = \prod_P (-1)^{(\mathrm{ord}_P\, a)(\mathrm{ord}_P\, g)} \frac{g^{\mathrm{ord}_P\, a}}{a^{\mathrm{ord}_P\, g}}(P)$$

and let $\Upsilon : (I^0)^m \to \bar{k}^*$ be defined by

$$\Upsilon(a) = \prod_P (-1)^{(\mathrm{ord}_P\, a)(\mathrm{ord}_P\, g)/m} \frac{g^{(\mathrm{ord}_P\, a)/m}}{a^{(\mathrm{ord}_P\, g)/m}}(P),$$

where the products are taken over the primes of K_∞. The next lemma summarizes the relevant properties of these functions.

Lemma 2. *We have the following:*
(1) *The functions Φ and Υ are G-equivariant.*
(2) *The functions Φ and Υ kill elements of $\bar{k}^*$.*
(3) *The function Φ kills elements of K_∞^*.*
(4) *For every $a \in I^0$ we have $\Phi(a) = \Upsilon(a^m)$.*

(5) *For every $a \in I^0(k)$ we have $\Psi(a) = \Phi(a)^{(q-1)/m}$.*

Proof Statements (1), (2), and (4) follow easily from the definitions of Φ and Υ. Statement (3) is Weil reciprocity (see the proof of [6, Number III.4, Prop. 6]). Finally, we note that the global Artin map Ψ is the product over the primes of K of the local Artin maps, each of which is given by the corresponding Hilbert symbol. Statement (5) then follows from Eq. (2).

Now let $a \in I^0(k)$ be an idèle whose associated divisor is the divisor D of Theorem 1, so that $a^m = fu$ for some unit idèle $u \in U(k)$. Let b be an element of $I^0(k)$ such that $((F-1)/m)[b] = [a]$, and let c be an element of I^0 such that $[b] = m[c]$ in $J(\bar{k})$, so that $[a] = (F-1)[c]$. If we translate these last two equalities into equalities in I^0, we find that there must exist functions $\alpha, \beta \in K_\infty^*$ and unit idèles $v, w \in U$ so that we have both $b = c^m \alpha v$ and $a = c^{\sigma-1}\beta w$, where σ denotes the qth-power automorphism of $\bar{k}$, which is a topological generator of G. Using the various statements in Lemma 2, we find that

$$\begin{aligned} e_m([D],[E]) &= \Psi(b) \\ &= \Phi(b)^{(q-1)/m} \\ &= \Phi(c)^{q-1}\ \Phi(v)^{(q-1)/m} \\ &= \Phi(c^{\sigma-1})\ \Upsilon(v^{\sigma-1}) \\ &= \Phi(aw^{-1})\ \Upsilon(v^{\sigma-1}) \\ &= \Upsilon(a^m w^{-m} v^{\sigma-1}) \\ &= \Upsilon(f)\ \Upsilon(uw^{-m}v^{\sigma-1}). \end{aligned}$$

However, we have

$$fu = a^m = c^{m(\sigma-1)}\beta^m w^m = b^{\sigma-1}\alpha^{1-\sigma}v^{1-\sigma}\beta^m w^m = \alpha^{1-\sigma}v^{1-\sigma}\beta^m w^m$$

so that

$$uw^{-m}v^{\sigma-1} = f^{-1}\alpha^{1-\sigma}\beta^m.$$

The left hand side of the last equality is a unit idèle, while the right hand side is a principal idèle. Thus $uw^{-m}v^{\sigma-1}$ is an element of $\bar{k}^*$, so that $\Upsilon(uw^{-m}v^{\sigma-1}) = 1$ by Lemma 2. This gives us $e_m([D],[E]) = \Upsilon(f)$, and by combining this with the equalities $mD = \operatorname{div} f$ and $mE = \operatorname{div} g$ we get Theorem 1. □

4. Proof of Theorem 1 for arbitrary base fields

We briefly indicate how Theorem 1 can be proven for arbitrary base fields. Suppose we are given a curve C, divisors D and E, and functions f and g as in Theorem 1. Choose a model for C, and let R be the subring of $\bar{k}$ generated as a ring by the coefficients of the defining equations of the chosen model of C, the coördinates of the points of the divisors D and E, the coefficients of f and g, and the mth roots of unity. If R is a finite field we are done, so assume R is not finite. Then the fact that R is finitely generated as a ring implies that it contains infinitely many maximal ideals, coprime to m, where the curve C and its Jacobian have good reduction. Choose such an ideal $\mathfrak{m}$. By reducing modulo $\mathfrak{m}$ we get corresponding objects C_0, D_0, E_0, f_0, and g_0 over the residue field $k_0 = R/\mathfrak{m}$. We know that $e_m([D],[E])$ specializes to $e_m([D_0],[E_0])$ and the right hand side of Eq. (1) specializes to the same expression with subscript zeros added. The field k_0 is finitely generated as a ring and is therefore finite, so the two specializations are equal to one another by the special case of Theorem 1 we have already proven. However, the left hand side of Eq. (1) is an mth root of unity by construction and the right hand side is an mth root of unity by Weil reciprocity. Since reduction modulo $\mathfrak{m}$ is injective on the mth roots of unity, we find that Eq. (1) must hold. □

References

1. Husemöller, D.: Elliptic curves (Grad. Texts Math., vol. 111) Berlin Heidelberg New York: Springer 1987
2. Lang, S.: Abelian varieties. New York: Interscience 1959
3. Milne, J. S.: Abelian varieties. In: Cornell, G., Silverman, J. H. (eds.): Arithmetic geometry (pp. 103–150) Berlin Heidelberg New York: Springer 1986
4. Milne, J. S.: Jacobian varieties. In: Cornell, G., Silverman, J. H. (eds.): Arithmetic geometry (pp. 167–212) Berlin Heidelberg New York: Springer 1986
5. Schmidt, H. L.: Über das Reziprozitätsgesatz in relativ-zyklischen algebraischen Funktionkörpern mit endlichem Konstantenkörper. Math. Z. 40, 94–109 (1936)
6. Serre, J.-P.: Algebraic groups and class fields (Grad. Texts Math., vol. 117) Berlin Heidelberg New York: Springer 1988
7. Silverman, J. H.: The arithmetic of elliptic curves (Grad. Texts Math., vol. 106) Berlin Heidelberg New York: Springer 1986

This article was processed by the author
using the Springer-Verlag TEX QPMZGHB macro package 1991.