Peter BRUIN

The Tate pairing for Abelian varieties over finite fields


<http://jtnb.cedram.org/item?id=JTNB_2011__23_2_323_0>
The Tate pairing for Abelian varieties over finite fields

par Peter BRUIN

Résumé. Nous décrivons un accouplement arithmétique associé à une isogenie entre variétés abéliennes sur un corps fini. Nous montrons qu’il généralise l’accouplement de Frey et Rück, donnant ainsi une démonstration brève de la perfection de ce dernier.

Abstract. In this expository note, we describe an arithmetic pairing associated to an isogeny between Abelian varieties over a finite field. We show that it generalises the Frey–Rück pairing, thereby giving a short proof of the perfectness of the latter.

1. Introduction

Throughout this note, \( k \) denotes a finite field of \( q \) elements, and \( \bar{k} \) denotes an algebraic closure of \( k \). If \( n \) is a positive integer, then \( \mu_n \) denotes the group of \( n \)-th roots of unity in \( \bar{k}^\times \).

Let \( C \) be a complete, smooth, geometrically connected curve over \( k \), let \( J \) be the Jacobian variety of \( C \), and let \( n \) be a divisor of \( q - 1 \). In [1], Frey and Rück defined a perfect pairing

\[
\{ D, E \}_{\text{mod } nJ(k)} : J[n](k) \times J(k)/nJ(k) \to \mu_n(k)
\]

as follows: if \( D \) and \( E \) are divisors on \( C \) with disjoint supports and \( f \) is a non-zero rational function with divisor \( nD \), then

\[
\{ [D], [E] \mod nJ(k) \}_n = f(E)^{(q-1)/n},
\]

where

\[
f(E) = \prod_{x \in C(k)} f(x)^{n_x} \quad \text{if } E = \sum_{x \in C(k)} n_x x.
\]

Remark. We have composed the map as defined in [1] with the isomorphism \( k^\times/(k^\times)^n \to \mu_n(k) \) that raises elements to the power \( (q - 1)/n \).
To prove the perfectness of \( \{ , \} \), Frey and Rück used a pairing introduced by Tate [10], which relates certain cohomology groups of an Abelian variety over a \( p \)-adic field, and an alternative description of this pairing given by Lichtenbaum [6] in the case of the Jacobian of a curve over a \( p \)-adic field. The names ‘Tate pairing’ and ‘Tate–Lichtenbaum pairing’ are therefore often used for what we call the Frey–Rück pairing.

There are now several proofs of the non-degeneracy of the Frey–Rück pairing that no longer use the cited results of Tate and Lichtenbaum; see Heß [2] and Schaefer [8]. In this note, we consider a separable isogeny \( \phi: A \to B \) between Abelian varieties over \( k \) such that \( \ker \phi \) is annihilated by \( q - 1 \). We define a pairing

\[
[ , ]_\phi: \ker \hat{\phi}(k) \times \coker(\phi(k)) \to k^\times
\]

between the groups

\[
\ker \hat{\phi}(k) = \{ b \in B(k) \mid \hat{\phi}(b) = 0 \}
\]

and

\[
\coker(\phi(k)) = B(k)/\phi(A(k)).
\]

We show that this pairing is perfect in the sense that it induces isomorphisms

\[
\ker \hat{\phi}(k) \cong \Hom(\coker(\phi(k)), k^\times)
\]

and

\[
\coker(\phi(k)) \cong \Hom(\ker \hat{\phi}(k), k^\times).
\]

Furthermore, we show that the Frey–Rück pairing is the special case of multiplication by \( n \) on the Jacobian of a curve over \( k \). The more general pairing appears to be known, but has not to my knowledge appeared in the literature. In any case, I do not make any claim to originality. It seems appropriate to call \([ , ]_\phi\) the Tate pairing associated to \( \phi \).

Remark. The condition that \( \ker \phi \) be annihilated by \( q - 1 \) can be relaxed somewhat. Let \( m \) be the exponent of \( \ker \phi \) and let \( d \) be the order of \( q \) in \((\mathbb{Z}/m\mathbb{Z})^\times\). If \( m \) and \( d \) are coprime, then one can pass to an extension of degree \( d \) of \( k \) and consider appropriate eigenspaces for the Frobenius action. This reproduces a result of Frey and Rück [1, Proposition 2.5].

2. Preliminaries

By a pairing we mean a bilinear map

\[
A \times B \to C
\]

between Abelian groups. It is called perfect if the induced group homomorphisms

\[
A \to \Hom(B, C) \quad \text{and} \quad B \to \Hom(A, C)
\]

are isomorphisms.
The Galois group $G_k = \text{Gal}(\bar{k}/k)$ is canonically isomorphic to the profinite group $\hat{\mathbb{Z}}$, with the element 1 of $\hat{\mathbb{Z}}$ corresponding to the $q$-power Frobenius automorphism $\sigma$. The only actions of $G_k$ that we consider are continuous actions on Abelian groups with the discrete topology. An Abelian group equipped with such an action of $G_k$ is called a $G_k$-module.

The fact that $G_k$ is generated as a topological group by $\sigma$ implies that for any $G_k$-module $M$, the Galois cohomology group $H^1(G_k, M)$ has an easy description via the isomorphism

\begin{equation}
H^1(G_k, M) \sim \rightarrow M/(\sigma - 1)M
\end{equation}

of Abelian groups, where $[c]$ denotes the class of a cocycle $c: G_k \rightarrow M$; see Serre [9, XIII, §1, proposition 1].

If $F$ is a finite $G_k$-module, the Cartier dual of $F$ is the Abelian group

$$F^\vee = \text{Hom}(F, \bar{k}^\times)$$

with the $G_k$-action given by

$$(\sigma a)(x) = \sigma(a(\sigma^{-1}x)) \quad \text{for all } a \in F^\vee, \sigma \in G_k, x \in F.$$  

The subgroup $F^\vee(k)$ of $G_k$-invariants consists of the elements of $\text{Hom}(F, \bar{k}^\times)$ that are homomorphisms of $G_k$-modules.

**Lemma 2.1.** Let $F$ be a finite $G_k$-module annihilated by $q - 1$, and let $F^\vee$ be its Cartier dual. There is a perfect pairing

$$F^\vee(k) \times H^1(G_k, F) \rightarrow k^\times$$

sending $(a, [c])$ to $a(c(\sigma))$ for every $a \in F^\vee(k)$ and every cocycle $c: G_k \rightarrow F$.

**Proof.** By assumption, we can write

$$F^\vee(k) = \text{Hom}(F, \bar{k}^\times)^{G_k}$$

$$= \text{Hom}(F, k^\times)^{G_k}$$

$$= \text{Hom}(F/(\sigma - 1)F, k^\times).$$

Applying the isomorphism (2.1) with $M = F$, we get an isomorphism

$$F^\vee(k) \sim \rightarrow \text{Hom}(H^1(G_k, F), k^\times)$$

such that the induced bilinear map $F^\vee(k) \times H^1(G_k, F) \rightarrow k^\times$ is given by the formula in the statement of the lemma. Since $H^1(G_k, F)$ is annihilated by the order of $k^\times$, it is (non-canonically) isomorphic to $F^\vee(k)$. This implies that the map

$$H^1(G_k, F) \rightarrow \text{Hom}(F^\vee(k), k^\times)$$

is also an isomorphism, so the pairing is perfect. \qed
3. Definition of the Tate pairing

Let $\phi: A \to B$ be a separable isogeny between Abelian varieties over $k$ such that $\ker \phi$ is annihilated by $q - 1$. We write $\phi(k)$ for the homomorphism $A(k) \to B(k)$ induced by $\phi$. We note that

$$(\ker \phi)(k) = \ker(\phi(k)),$$

and we denote this group from now on by $\ker \phi(k)$. We also note that there is no similar equality for cokernels.

We start with the short exact sequence

$$0 \longrightarrow \ker \phi \longrightarrow A \longrightarrow B \longrightarrow 0$$

of commutative group varieties over $k$. Since $A$, $B$ and $\phi$ are defined over $k$, taking $\bar{k}$-points in this sequence gives a short exact sequence of $G_k$-modules. Taking Galois cohomology, we obtain a long exact sequence

$$0 \longrightarrow \ker \phi(k) \longrightarrow A(k) \overset{\phi(k)}{\longrightarrow} B(k) \overset{\delta}{\longrightarrow} H^1(G_k, \ker \phi(\bar{k})) \longrightarrow H^1(G_k, A(\bar{k})).$$

The connecting homomorphism $\delta$ is given by

$$\delta(b) = [\tau \mapsto \tau(a) - a],$$

where $a$ is any element of $A(\bar{k})$ such that $\phi(a) = b$. A theorem of Lang on Abelian varieties over finite fields [4, Theorem 3] implies that $H^1(G_k, A(\bar{k}))$ vanishes. This means that $\delta$ is surjective and hence gives an isomorphism

$$B(k)/\phi(A(k)) \overset{\sim}{\longrightarrow} H^1(G_k, \ker \phi(\bar{k})).$$

The pairing from Lemma 2.1 becomes a perfect pairing

$$(3.1) \quad (\ker \phi)^\vee(k) \times B(k)/\phi(A(k)) \longrightarrow k^\times$$

sending $(f, b \mod \phi(A(k)))$ to $f(\sigma(a) - a)$, with $a \in A(\bar{k})$ such that $\phi(a) = b$.

Now let $\hat{\phi}: \hat{B} \to \hat{A}$ denote the isogeny dual to $\phi$. The Cartier duality theorem for isogenies of Abelian varieties (see for example Mumford [7, §15, Theorem 1]) gives a canonical isomorphism

$$\epsilon_{\phi}: \ker \hat{\phi} \overset{\sim}{\longrightarrow} (\ker \phi)^\vee$$

of $G_k$-modules. Combining this with the pairing (3.1) gives a perfect pairing

$$(3.2) \quad [\ , \ ]_{\phi}: \ker \hat{\phi}(k) \times \coker(\phi(k)) \longrightarrow k^\times$$

$$(x, y) \mapsto (\epsilon_{\phi}x)(\sigma a - a),$$

where $a$ is any element of $A(\bar{k})$ with $(\phi(a) \mod \phi(A(k))) = y$. We call this pairing the Tate pairing associated to $\phi$. 

4. Comparison to the Frey–Rück pairing

We now take \( A = B = J \), where \( J \) is the Jacobian of a complete, smooth, geometrically connected curve \( C \) over \( k \), and we take \( \phi \) to be the multiplication by a positive integer \( n \) dividing \( q - 1 \). We identify \( J \) with its dual Abelian variety using the canonical principal polarisation. Then the Tate pairing (3.2) becomes a perfect pairing

\[
[\ , ]_n : J[n](k) \times J(k)/nJ(k) \to k^\times.
\]

Moreover, from the Cartier duality isomorphism \( \epsilon_n : \hat{J}[n] \sim J[n]^\vee \) and the identification of \( J[n] \) with \( \hat{J}[n] \) we obtain a perfect pairing

\[
e_n : J[n] \times J[n] \to \mu_n
\]

\[
(x, y) \mapsto (\epsilon_n y)(x) \quad \text{for all } x, y \in J[n](\overline{k}),
\]
called the Weil pairing. It can be computed as follows. Let \( D \) and \( E \) be two divisors of degree 0 on \( C_{\overline{k}} \) with disjoint supports and such that their classes \([D]\) and \([E]\) in \( J(k) \) are \( n \)-torsion points. Then there exist non-zero rational functions \( f \) and \( g \) on \( C_{\overline{k}} \) such that

\[
nD = \div f \quad \text{and} \quad nE = \div g,
\]

and we have

\[
e_n([D], [E]) = \frac{g(D)}{f(E)};
\]

see Howe [3]. The fact that this depends only on the linear equivalence classes of \( D \) and \( E \) comes down to Weil reciprocity: if \( f \) and \( g \) are two rational functions on \( C_{\overline{k}} \) whose divisors have disjoint supports, then

\[
f(\div g) = g(\div f).
\]

For a proof, we refer to Lang [5, Chapter VI, corollary to Theorem 10].

**Theorem 4.1.** The pairing \([\ , ]_n\) equals the Frey–Rück pairing \(\{\ , \}_n\).

**Proof.** Consider elements of \( J[n](k) \) and \( J(k)/nJ(k) \), represented by \( (k-) \)-rational divisors \( D \) and \( E \), respectively, such that the supports of \( D \) and \( E \) are disjoint. We choose a divisor \( E_0 \) on \( C_{\overline{k}} \) such that \( nE_0 \) is linearly equivalent to \( E \) and rational functions \( f \) on \( C \) and \( g \) on \( C_{\overline{k}} \) such that

\[
nD = \div f \quad \text{and} \quad nE_0 - E = \div g.
\]

Then we have

\[
\div(\sigma g / g) = n(\sigma E_0 - E_0).
\]
Using the definitions of the pairing $[\ , \ ]_n$ and of the Weil pairing $e_n$, the formula (4.1), the fact that $\sigma$ is the $q$-power map on $\bar{k}^\times$, and Weil reciprocity, we can compute $[\ , \ ]_n$ as follows:

$$[[D], [E] \mod nJ(k)]_n = (\epsilon_n[D])([\sigma E_0 - E_0])$$

$$= e_n([\sigma E_0 - E_0], [D])$$

$$= f(\sigma E_0 - E_0)$$

$$= (\sigma g/g)(D)$$

$$= \sigma(f(E_0)/f(E_0))$$

$$= (f(E_0)/g(D))^{q-1}$$

$$= (f(nE_0)/g(nD))^{(q-1)/n}$$

$$= (f(nE_0)/f(nE_0 - E))^{(q-1)/n}$$

$$= f(E)^{(q-1)/n}.$$ 

This equality is what we had to prove. □

References


