Algebra and Discrete Mathematics
Volume 16 **(2013)**. Number 1. pp. 103 – 106

RESEARCH ARTICLE

On the Tate pairing associated to an isogeny between abelian varieties over pseudofinite field

Volodymyr Nesteruk

Communicated by M. Ya. Komarnytskyj

Abstract. In this note, we consider the Tate pairing associated to an isogeny between abelian varieties over pseudofinite field. P. Bruin [1] defined this pairing over finite field k: $\ker\hat{\phi}(k) \times \operatorname{coker}(\phi(k)) \longrightarrow k^*$, and proved its perfectness over finite field. We prove perfectness of the Tate pairing associated to an isogeny between abelian varieties over pseudofinite field, with help of the method, used by P. Bruin in the case of finite ground field [1].

Introduction

P. Bruin [1] and E. Schaefer [7] shoved that the perfectness of the Tate pairing and of the Frey-Rück pairing follows from that of the Tate pairing associated to an isogeny between abelian varieties. The Tate pairing may be defined over pseudofinite fields [5]. Recall that a field k is called *pseudofinite* [2], if k is perfect, k has the unique extension of degree n for each natural number n and every nonempty absolutely irreducible variety over k, has a k-rational point.

The aim of this work is to prove that the Tate pairing $\ker\hat{\phi}(k) \times \operatorname{coker}(\phi(k)) \longrightarrow k^*$ associated to an isogeny ϕ of abelian varieties is perfect over pseudofinite field k.

2010 MSC: 12G99, 14H05, 14K02.

Key words and phrases: pseudofinite field, isogeny, Tate pairing associated to an isogeny.

1. Prerequisites

Let C be an absolutely irreducible projective curve defined over pseudofinite field k, and $\overline{k}$ be algebraic closure of k, k^* multiplicative group of k, n is a positive integer, $(n, \mathrm{char}(k)) = 1$ and $\mu_n(k)$ denotes the group of n-th roots of unity in $\overline{k}^*$, $\mathrm{J}(k)$ is the Jacobian of curve C over k, $\mathrm{J}[n](k)$ denotes the subgroup of elements in $\mathrm{J}(k)$ of order dividing n. For divisor classes $x \in \mathrm{J}[n](k)$ and $y \in \mathrm{J}(k)/n\mathrm{J}(k)$ there are coprime divisors D and R such that $x = [D]$ and $y = [R] + n\mathrm{J}(k)$, and there exists a function $f \in k(C)$ such that $(f) = nD$. The *Tate pairing* is the pairing $t_n(x, y)\colon\ \mathrm{J}[n](k) \times \mathrm{J}(k)/n\mathrm{J}(k) \longrightarrow k^*$, where $t_n(x, y) = f(R)$ [3].

Recall the concept of perfect pairing. Let A, B, C be abelian groups. A pairing $A \times B \to C$ is called *perfect* if the induced group homomorphisms $A \to \mathrm{Hom}(B, C)$ and $B \to \mathrm{Hom}(A, C)$ are isomorphisms.

Let A, B be abelian varieties, defined over a field k. A homomorphism $\phi : A \to B$ is called *isogeny* if it is surjective with finite kernel $\ker\phi$ [4, 8]. Recall that the degree $\deg\phi$ of isogeny $\phi : A \to B$ is the index $[k(A) : \phi\, k(B)]$, the degree of the corresponding function field extension $k(A)/k(B)$.

Clearly, the kernel $\ker\phi$ of an isogeny is a finite abelian group and satisfies the inequality $|\ker\phi| \leq \deg\phi$.

Recall some principal properties of isogenies which will be used later. For a homomorphisms $\phi : A \to B$ of abelian varieties A, B the following are equivalent: ϕ is an isogeny, $\dim A = \dim B$ and ϕ is surjective, $\dim A = \dim B$ and $\ker\phi$ is finite, ϕ is finite, flat, and surjective [4].

For any positive integer n, $(n, \mathrm{char} k) = 1$, we have $A_n(k) = \ker(n : A(k) \to A(k))$. Then if $n = \deg\phi$, so $\ker\phi \subseteq A_n(k)$.

2. The Tate pairing associated to an isogeny ϕ

Let G_k be absolute Galois group of k, and D finite G_k-module. The Cartier dual of D is the abelian group $D^\vee = \mathrm{Hom}(D, \overline{k}^*)$ with the G_k-action given by

$$(\sigma a)(x) = \sigma(a(\sigma^{-1}x)),$$

where $a \in D^\vee$, $\sigma \in G_k$ and $x \in D$. Let $\phi : A \to B$ be an isogeny. Then there is unique isogeny $\widehat{\phi} : B \to A$, $\widehat{\phi} \circ \phi = \deg\phi$ and $\widehat{\phi}$ is called the *dual isogeny.* Let ϵ_ϕ there canonical isomorphism from $\ker\hat{\phi}$ to the Cartier dual $(\ker\phi)^\vee$ of $\ker\phi$ and $\phi(k) : A(k) \to B(k)$ is homomorpfism induced by ϕ. For $x \in \ker\hat{\phi}(k) = \{b \in B(k) |\ \hat{\phi}(b) = 0\}$, $y \in \mathrm{coker}(\phi(k)) =$

$B(k)/\phi(A(k))$, we have $(x, y) \mapsto (\epsilon_\phi x)(\sigma a - a)$, where σ is the generator of absolute Galois group G_k and $a \in A(\overline{k})$, $(\phi(a) \mod \phi(A(k))) = y$.

The *Tate pairing associated to isogeny* ϕ is the pairing

$$\ker \hat{\phi}(k) \ \times \ \operatorname{coker}(\phi(k)) \longrightarrow k^*, \tag{1}$$

where $(x, y) \mapsto (\epsilon_\phi x)(\sigma a - a)$.

Lemma 1 ([6]). *Let D be finite G_k-module. Then*

$$|\mathrm{H}^0(G_k, D)| = |\mathrm{H}^1(G_k, D)|.$$

Applying the method, used by P. Bruin [1] in the case of finite ground field, we prove the next theorem for pseudofinite field.

Theorem 1. *Let ϕ be an isogeny between abelian varieties A, B over pseudofinite field k. Let m be order of* $\ker \phi$*. Suppose that k contains m-th roots of 1. Then the Tate pairing associated to ϕ is perfect.*

Proof. Consider of the exact sequence of G_k-modules

$$0 \to \ker\phi \to A(\overline{k}) \to B(\overline{k}) \to 0.$$

This exact sequence gives us the following long exact sequence of cohomology groups

$$\begin{aligned} 0 \to \mathrm{H}^0(G_k, \ker\phi) \to \mathrm{H}^0(G_k, A(\overline{k})) \to \mathrm{H}^0(G_k, B(\overline{k})) \\ \to \mathrm{H}^1(G_k, \ker\phi) \to \mathrm{H}^1(G_k, A(\overline{k})) \to \mathrm{H}^1(G_k, B(\overline{k})). \end{aligned}$$

Hence,

$$0 \to \ker\phi(k) \to A(k) \xrightarrow{\phi} B(k) \to \mathrm{H}^1(G_k, \ker\phi) \to 0. \tag{2}$$

It is known that the group $\mathrm{H}^1(G_k, A(\overline{k})) = \mathrm{H}^1(G_k, B(\overline{k})) = 0$, since k is a pseudofinite field [5]. From (2) we have that

$$B(k)/\phi(A(k)) \xrightarrow{\sim} \mathrm{H}^1(G_k, \ker\phi). \tag{3}$$

Thus (3), gives us the following description of $\operatorname{coker}(\phi(k))$,

$$\operatorname{coker}(\phi(k)) \xrightarrow{\sim} \mathrm{H}^1(G_k, \ker\phi).$$

The exact sequence analogous (2) and the Lemma 1 allow to define the perfect pairing

$$(\ker \phi)^\vee(k) \ \times \ \operatorname{coker}(\phi(k)) \to k^*.$$

Finally, taking into account the canonical isomorphism, ϵ_ϕ, we get that this perfect pairing coincides with (1). □

References

[1] P. Bruin, *The Tate pairing for abelian varieties over finite fields*, Journal de theorie des nombres de Bordeaux, 23(2), 2011, 323-328.

[2] M. Fried, M. Jarden, *Field arithmetic*. Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, 11. Springer-Verlag, Berlin, 2005.

[3] F. Hess, *A Note on the Tate Pairing of Curves over Finite Fields*, Archiv der Mathematik 82, N.**1**, 2004, 28-32.

[4] J. S. Milne, *Abelian Varieties*, available at www.jmilne.org/math/, 2008.

[5] V. Nesteruk, *On nondegeneracy of Tate product for curves over pseudofinite fields*, Visnyk of the Lviv Univ. Series Mechanics and Mathematics, Is. 72, 2010, 195-200 (in Ukrainian).

[6] V. Platonov, A. Rapinchuk, *Algebraic groups and number theory*, 1991 (in Russian).

[7] E. F. Schaefer, *A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field*. In: T. Shaska (editor), Computational Aspects of Algebraic Curves (Conference held at the University of Idaho). Lecture Notes Series in Computing 13. World Scientific Publishing, Hackensack, NJ, 2005, 1-12.

[8] J. H. Silverman, *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

Contact information

V. Nesteruk

Algebra and Logic Department, Mechanics and Mathematics Faculty, Ivan Franko National University of L'viv, 1, Universytetska str., Lviv, 79000, Ukraine
E-Mail: volodymyr-nesteruk@rambler.ru

Received by the editors: 13.02.2012
and in final form 30.03.2013.