УДК 513.6

V. I. Nesteruk

ON THE KOLYVAGIN FORMULA FOR ELLIPTIC CURVES WITH GOOD REDUCTIONS OVER PSEUDOLOCAL FIELDS

V. I. Nesteruk. *On the Kolyvagin formula for elliptic curves with good reductions over pseudolocal fields*, Mat. Stud. **39** (2013), 16–20.

We consider the relationships between the local Artin map $\theta\colon K^* \to \mathrm{Gal}(K^{ab}/K)$ and the Hilbert symbol $(\cdot\,,\cdot)\colon K^*/K^{*m} \times K^*/K^{*m} \longrightarrow \mu_m$ for a general local field, as well as between the Tate pairing and the Weil pairing for elliptic curves with good reductions over pseudolocal fields (complete discretely valued fields with pseudofinite residue fields). It is known that the Weil pairing $\{\cdot\,,\cdot\}\colon \mathrm{E}(\overline{K})_m \times \mathrm{E}(\overline{K})_m \longrightarrow \mu_m$ and the Tate pairing $\langle\cdot\,,\cdot\rangle\colon \mathrm{E}(K)/m\mathrm{E}(K) \times \mathrm{H}^1(G_K, \mathrm{E}(\overline{K}))_m \longrightarrow \mathbb{Z}/m\mathbb{Z}$ satisfy $\zeta^{\langle c_1,c_2\rangle} = \{e_1, e_2\}$, where E is an elliptic curve with good reduction over local field and ζ an appropriate m^{th} root of 1. This is Kolyvagin's formula. It is proved that the same holds true for elliptic curves with good reductions over pseudolocal fields.

В. И. Нестерук. *О формуле Колывагина для эллиптических кривых с невырожденными редукциями над псевдолокальными полями* // Мат. Студії. – 2013. – Т.39, №1. – С.16–20.

Установлена связь между локальным отображением Артина $\theta\colon K^* \to \mathrm{Gal}(K^{ab}/K)$ и символом Гильберта $(\cdot\,,\cdot)\colon K^*/K^{*m} \times K^*/K^{*m} \longrightarrow \mu_m$ для общего локального поля, а также между спариванием Тэйта и спариванием Вейля для эллиптических кривых с невырожденными редукциями над псевдолокальными полями (полными дискретно нормированными полями с псевдоконечными полями вычетов). Известно, что спаривание Вейля $\{\cdot\,,\cdot\}\colon \mathrm{E}(\overline{K})_m \times \mathrm{E}(\overline{K})_m \longrightarrow \mu_m$ и спаривание Тэйта $\langle\cdot\,,\cdot\rangle\colon \mathrm{E}(K)/m\mathrm{E}(K) \times \mathrm{H}^1(G_K, \mathrm{E}(\overline{K}))_m \longrightarrow \mathbb{Z}/m\mathbb{Z}$ удовлетворяют $\zeta^{\langle c_1,c_2\rangle} = \{e_1, e_2\}$, где E — эллиптическая кривая с невырожденной редукцией над локальным полем и ζ — подходящий корень m-ой степени из 1. Это — формула Колывагина. Доказано, что это верно и для эллиптических кривых с невырожденными редукциями над псевдолокальными полями.

The Artin map was first introduced by E. Artin at the end of 20th and the bedinning of 30th of the previous century. This map allows to describe the Galois groups of abelian extensions in terms of objects, closely related to the basic field in local case and to the group of idele classes in global case. A significant contribution to its study was done by E. Noether, H. Hasse, R. Brauer, J.-P. Serre ([4]), I. Fesenko ([1]), J. Milne, M. Papikian. D. Hilbert has defined and investigated the norm residue symbol, which now is called the *Hilbert symbol*. The Hilbert symbol $(\cdot\,,\cdot)\colon K^*/K^{*m} \times K^*/K^{*m} \longrightarrow \mu_m$ is a pairing. Several pairings play an important role in mathematics and its applications, in particular, in cryptography. M. Papikian ([3]) described the connections between the Tate pairing and the Weil pairing for curves defined over local field. It is given by *Kolyvagin's formula* $\zeta^{\langle c_1,c_2\rangle} = \{e_1, e_2\}$.

The aim of this work is to prove the relation $\theta(b)(a^{1/m}) = (a,b)a^{1/m}$ between the Hilbert symbol $(\cdot\,,\cdot)\colon\ K^*/K^{*m} \times K^*/K^{*m} \longrightarrow \mu_m$ and the local Artin map $\theta\colon K^* \to \mathrm{Gal}(K^{ab}/K)$ in

2010 *Mathematics Subject Classification:* 12G99, 14H05, 14H52.
Keywords: pseudolocal field, general local field, elliptic curve, local Artin map, Hilbert symbol, Tate pairing, Weil pairing, Kolyvagin formula.

the case of a *general local field* (complete discretely valued field with quasifinite residue field) and the relations between Tate pairing in elliptic curves with good reductions and between Weil pairing in the case of such curves defined over a *pseudolocal field* (complete discretely valued field with pseudofinite residue field).

The proofs of formulas which describe these relations are based on the works of M. Papikian [3] and J. Milne [2]. The relationship between Hilbert's symbol and the local Artin map is given for a general local field. Using the work of M. Papikian [3], we prove the Kolyvagin formula for elliptic curves with good reductions over a pseudolocal field.

Let K be a general local field, and k be a residue field of K, $\overline{K}$ (resp. $\overline{k}$) be the algebraic closures of K (resp. k), K^* the multiplicative group of K, m a positive integer, $(m, \mathrm{char}(k)) = 1$, μ_m the group of m^{th} root of 1 in $\overline{K}$, $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K, $G_k = \mathrm{Gal}(\overline{k}/k)$ the absolute Galois group of k. Let $\mathrm{H}^2(G_K, \overline{K}^*)_m$ denote the subgroup of elements in $\mathrm{H}^2(G_K, \overline{K}^*)$, whose order divides m, $\widehat{\mathrm{H}}^n(.,.)$ the modified Tate cohomology groups for any $n \in \mathbb{Z}$. Fix $\sigma \in G_K$ and call σ the *Frobenius automorphism*, denote it $\mathrm{Frob}_{\overline{K}/K}$. Assume $\mu_m \subset K$. From the exact sequence of G_K-modules $0 \to \mu_m \to \overline{K}^* \xrightarrow{m} \overline{K}^* \to 0$ we get the exact sequence of cohomology groups $K^* \xrightarrow{m} K^* \to \mathrm{H}^1(G_K, \mu_m) \to \mathrm{H}^1(G_K, \overline{K}^*) \xrightarrow{m} \mathrm{H}^1(G_K, \overline{K}^*) \to \mathrm{H}^2(G_K, \mu_m) \to \mathrm{H}^2(G_K, \overline{K}^*) \xrightarrow{m} \mathrm{H}^2(G_K, \overline{K}^*) \to \dots$ Hence, $0 \to K^*/K^{*m} \to \mathrm{H}^1(G_K, \mu_m) \to \mathrm{H}^1(G_K, \overline{K}^*) \xrightarrow{m} \mathrm{H}^1(G_K, \overline{K}^*) \to \mathrm{H}^2(G_K, \mu_m) \to \mathrm{H}^2(G_K, \overline{K}^*)_m \to 0$. Hilbert's theorem 90 says that, $\mathrm{H}^1(G_K, \overline{K}^*) = 0$. Thus

$$K^*/K^{*m} \cong \mathrm{H}^1(G_K, \mu_m). \tag{1}$$

The pairing $\mathrm{H}^2(G_K, \mu_m) \times \mathrm{H}^0(G_K, \mu_m) \to \mathrm{H}^2(G_K, \mu_m \otimes \mu_m)$ defines the isomorphisms $\mathrm{H}^2(G_K, \mu_m) \times \mu_m \to \mathrm{H}^2(G_K, \mu_m \otimes \mu_m)$ and

$$\mathrm{H}^2(G_K, \mu_m \times \mu_m) \simeq \mathrm{H}^2(G_K, \mu_m) \otimes \mu_m \simeq (\mathbb{Z}/m\mathbb{Z}) \otimes \mu_m = \mu_m. \tag{2}$$

Consider the pairing $\mathrm{H}^1(G_K, \mu_m) \times \mathrm{H}^1(G_K, \mu_m) \to \mathrm{H}^2(G_K, \mu_m \times \mu_m)$. Using (1) and (2), we get the pairing $a, b \to (a, b)\colon K^*/K^{*m} \times K^*/K^{*m} \longrightarrow \mu_m$. This pairing is called the *Hilbert symbol*.

For the Hilbert symbol (a, b) over a general local field K the usual properties hold, in particular, the bi-multiplicativity, the skew-symmetry, and the nondegeneracy: $(a, b) = 1$ if and only if b is a norm from $K[a^{1/m}]$.

The proof of these properties of Hilbert's symbol is similar to the proofs in the case of a local basic field ([1]).

Lemma 1. *Let k be a field such that the group k^*/k^{*m} is finite, and K is complete discretely valued field with the residue field k. Then the group K^*/K^{*m} is finite.*

Proof. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{U}_K & \longrightarrow & K^* & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow m & & \downarrow m & & \downarrow m & & \\ 0 & \longrightarrow & \mathrm{U}_K & \longrightarrow & K^* & \longrightarrow & \mathbb{Z} & \longrightarrow & 0, \end{array} \tag{3}$$

where U_K is the group of units in K and K^* multiplicative group of K. Apply the snake lemma to commutative diagram (3). Then

$$0 \to \mathrm{U}_K/\mathrm{U}_K^m \to K^*/K^{*m} \to \mathbb{Z}/m\mathbb{Z} \to 0. \tag{4}$$

Let $\mathrm{U}_K^{(1)}$ be the group of units in K, congruent with 1 by modulo of prime element. Consider the filtration $\mathrm{U}_K \supset \mathrm{U}_K^{(1)} \supset \mathrm{U}_K^{(2)} \supset \mathrm{U}_K^{(3)} \supset \ldots \mathrm{U}_K^{(m)} \supset \ldots$ The commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{U}_K^{(1)} & \longrightarrow & \mathrm{U}_K & \longrightarrow & k^* & \longrightarrow & 0 \\ & & \downarrow m & & \downarrow m & & \downarrow m & & \\ 0 & \longrightarrow & \mathrm{U}_K^{(1)} & \longrightarrow & \mathrm{U}_K & \longrightarrow & k^* & \longrightarrow & 0, \end{array}$$

implies $0 \to \mathrm{U}_K^{(1)}/\mathrm{U}_K^{(1)m} \to \mathrm{U}_K/\mathrm{U}_K^m \to k^*/k^{*m} \to 0$. From Hensel's lemma we get that the group $\mathrm{U}_K^{(1)}/\mathrm{U}_K^{(1)m}$ is trivial. Finally, $\mathrm{U}_K/\mathrm{U}_K^m \cong k^*/k^{*m}$ and it follows from (4) that the group K^*/K^{*m} is finite. □

We summarize the properties of local the Artin map $\theta\colon K^* \to \mathrm{Gal}(K^{ab}/K)$ for general local field, which will be needed in the sequel.

Theorem 1 ([1, 2, 4])**.** *Let K be a general local field, K^{ab} be the maximal abelian extension of K. Then there is a homomorphism $\theta\colon K^* \to \mathrm{Gal}(K^{ab}/K)$ with the following properties:*

a) for any prime element π of K and any finite unramified extension L of K one has $\theta(\pi)|_L = \mathrm{Frob}_{L/K}$;

b) for any finite abelian extension L K, $N_{L/K}(L^*)$ contained in the kernel of the map $a \to \theta(a)|_L$ and θ induces an isomorphism $\theta_{L/K}\colon K^*/N_{L/K} \to \mathrm{Gal}(L/K)$;

c) a subgroup N of K^* is of the form $N_{L/K}(L^*)$ for some finite abelian extension L of K, $([L:K], \mathrm{char}(k)) = 1$, if and only if it is of finite index and open.

The homomorphism θ in Theorem 1 is called the *local Artin map*. The next lemma is an auxiliary lemma to establish the connection between Hilbert's symbol and the local Artin map.

Lemma 2 ([4])**.** *Let G be a finite group, B be a G-module and $f\colon G \to B$ a 1-cocycle, $\overline{f} \in \mathrm{H}^1(G, B)$ its cohomology class, $\overline{g} \in \widehat{\mathrm{H}}^{-2}(G, \mathbb{Z})$, $f(s) \in B$ such that $Nf(s) = 0$. Then for every $g \in G$, $\overline{gf} = \overline{f(s)}_0 \in \widehat{\mathrm{H}}^{-1}(G, B)$, where $\overline{f(s)}_0$ is the canonical image of an element $f(s) \in B$ in $\widehat{\mathrm{H}}^{-1}(G, B)$.*

A field *extension L/K is of exponent m*, if it is Galois and its Galois group is of exponent m ($g^m = e$ for every $g \in \mathrm{Gal}(L/K)$). The next theorem will be used in the case, where the field K is a general local field.

Theorem 2 ([5])**.** *Let K be any field and m an integer, $(m, \mathrm{char}K) = 1$, and assume that all the m^{th} roots of unity are in K. Let B be a subgroup of K^* such that $K^{*m} \subset B$, $K_B = K(B^{1/m})$. Then K_B is a Kummer extension (abelian extension of exponent m) and we define the bilinear map*

$$(\cdot,\cdot)\colon \mathrm{Gal}(K_B/K) \times B \to \mu_m; (g, a) = \frac{g\alpha}{\alpha},\ \text{where}\ \alpha^m = a,\ g \in \mathrm{Gal}(K_B/K),\ a \in B.$$

The left kernel of this pairing is 1 and the right kernel is K^{*m}, and the extension K_B/K is finite if and only if $[B : K^{*m}]$ is finite. In that case, $B/K^{*m} \cong \mathrm{Hom}(\mathrm{Gal}(K_B/K), \mu_m)$.

There exists the so-called *inv-isomorphism* of local class theory for general local fields ([1, 4]) $\mathrm{inv}\colon \mathrm{H}^2(G, K_s^*) \to \mathbb{Q}/\mathbb{Z}$, $\mathrm{inv}\colon \mathrm{H}^2(G, \mu_m) \cong \mathrm{H}^2(G, \overline{K}^*)_m \to \mathbb{Z}/m\mathbb{Z}$, where K_s^* is the separable closure of K. The image of an element $\beta \in \mathrm{H}^2(G, K_s^*)$ under the map inv is called the *invariant* of β.

As in the case of a local ground field, the Hilbert symbol satisfies the equality $\theta(b)(a^{1/m}) = (a, b)a^{1/m}$.

Theorem 3. *Let K be a general local field. Then $\theta(b)(a^{1/m}) = (a, b)a^{1/m}$.*

Proof. We follow the method used by M. Papikian ([3]) for the local field case. Let L/K be a maximal abelian m-extension with group G, $a \in K^*$. By Lemma 1, K^*/K^{*m} is a finite group. Then G is finite, hence $G \cong K^*/K^{*m}$. Let $a \in K^*$. Then using Theorem 2, define $\chi \in \mathrm{Hom}(G, \mu_m)$ by

$$\chi(g) = \frac{g(a^{1/m})}{a^{1/m}}. \tag{5}$$

The formula $\theta(b)(a^{1/m}) = (a, b)a^{1/m}$, using (5) at $g = \theta(b)$, can be written in the form $(a, b) = \chi(\theta(b))$. Let $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, $\overline{\alpha} \in \widehat{\mathrm{H}}^0(G, L^*)$ be the image of element $\alpha \in K^*$, $\delta_\chi \in \mathrm{H}^2(G, \mathbb{Z})$ be the image of character χ under the coboundary map $\delta\colon \mathrm{H}^1(G, \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^2(G, \mathbb{Z})$. The $\cup$-product $\overline{\alpha}\delta_\chi \in \mathrm{H}^2(G, L^*)$ and $\chi(\theta(b)) = \mathrm{inv}(\overline{\alpha}\delta_\chi)$ ([4]). Therefore it suffices to prove $\chi(\theta(b)) = \mathrm{inv}(\overline{\alpha}\delta_\chi)$.

Consider the isomorphism $\theta_{L/K}^{-1}\colon G \to K^*/N_{L/K}(L^*)$. Then by definition $\theta_{L/K}^{-1}$, $\theta(b) \cdot u_{L/K} = \overline{\alpha} \in \widehat{\mathrm{H}}^0(G, L^*)$ and $\overline{\alpha} \cdot \delta_\chi = \theta(b) \cdot u_{L/K} \cdot \delta_\chi$. Using the associativity of $\cup$-products, we obtain $\overline{\alpha} \cdot \delta_\chi = u_{L/K} \cdot (\theta(b) \cdot \delta_\chi) = u_{L/K} \cdot \delta(\theta(b) \cdot \chi)$, where $\theta(b) \cdot \chi \in \widehat{\mathrm{H}}^{-1}(G, \mathbb{Q}/\mathbb{Z})$. The group $\widehat{\mathrm{H}}^{-1}(G, \mathbb{Q}/\mathbb{Z})$ identifies with the group $\mathbb{Z}/n\mathbb{Z}$, under the condition that $[L : K] = n$, and the group $\widehat{\mathrm{H}}^{-2}(G, \mathbb{Z})$ identifies with G under the condition that equality is $\theta(b) \cdot \chi = \chi(\theta(b))$ (Lemma 2).

Consider $\delta\colon \widehat{\mathrm{H}}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \to \widehat{\mathrm{H}}^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$. Let $\theta(b) \cdot \chi = r/n$, where $r \in \mathbb{Z}$. Then $\delta(r/n) \in \widehat{\mathrm{H}}^0(G, \mathbb{Z})$, and $\delta(r/n) = r$,

$$\mathrm{inv}(\overline{\alpha} \cdot \delta_\chi) = \mathrm{inv}(u_{L/K} \cdot (\theta(b) \cdot \delta_\chi)) = \mathrm{inv}(u_{L/K} \cdot \delta(\theta(b) \cdot \chi)) = \mathrm{inv}(u_{L/K} \cdot r) = r/n = \chi(\theta(b)),$$

where $u_{L/K}$ is the fundamental class of $\mathrm{H}^2(G, L^*)$. □

From now on, the field K is a pseudolocal field (a complete discretely valued field with a pseudofinite residue field k).

Let E be an elliptic curve with good reduction over a pseudolocal field K, $\mathrm{E}_m(K)$ is the group of m-torsion. For all $0 \le i \le 2$ the groups $\mathrm{H}^i(G_K, \mathrm{E}_m(\overline{K}))$ are finite. There are alternating, nondegenerate pairings $\mathrm{H}^i(G_K, \mathrm{E}_m(\overline{K})) \times \mathrm{H}^{2-i}(G_K, \mathrm{E}_m(\overline{K})) \longrightarrow \mathbb{Z}/m\mathbb{Z}$, induced by the $\cup$-product, Weil pairing and the invariant map of the class field theory. These pairing induce the nondegenerate pairing $\langle \cdot, \cdot \rangle\colon \mathrm{E}(K)/m\mathrm{E}(K) \times \mathrm{H}^1(G_K, \mathrm{E}(\overline{K}))_m \longrightarrow \mathbb{Z}/m\mathbb{Z}$ ([6]), which is called the *Tate pairing*.

Let $b \in K^*$, $\phi_b \in \mathrm{Hom}(G, \mu_m)$, $\phi_b(g) = g(b^{1/m})/b^{1/m}$. Fix a generator element ξ of K^*/K^{*m}, which can be identified with the primitive m^{th} root of 1, and choose ζ as follows

$$\zeta = \frac{\sigma(\xi^{1/m})}{\xi^{1/m}}. \tag{6}$$

Consider the homomorphisms $\overline{\phi}_a, \overline{\phi}_b \colon G \to \mathbb{Z}/m\mathbb{Z}$, such that $\zeta^{\overline{\phi}_a(g)} = \phi_a(g)$, $\zeta^{\overline{\phi}_b(g)} = \phi_b(g)$. Define an element of in $\mathrm{H}^2(G, \mu_m)$ by the bilinear form $\mathrm{B}_{a,b}(g_1, g_2) = \zeta^{\overline{\phi}_a(g_1)\overline{\phi}_a(g_2)}$. Then the Hilbert symbol becomes $(a, b) = \zeta^{\operatorname{inv} \mathrm{B}_{a,b}}$. As in [3], we associate to elements $c_1 \in \mathrm{E}(K)/m\mathrm{E}(K)$ and $c_2 \in \mathrm{H}^1(G, \mathrm{E}(\overline{K}))_m$ the homomorphisms $\varphi_1 \colon \mu_m \to \mathrm{E}_m(K)$, and $\varphi_2 \colon \mu_m \to \mathrm{E}_m(K)$, by using $\mathrm{E}(K)/m\mathrm{E}(K) \simeq \mathrm{Hom}(\mu_m, \mathrm{E}_m(\overline{K}))$ and $\mathrm{H}^1(G, \mathrm{E}(\overline{K}))_m \simeq \mathrm{Hom}(\mu_m, \mathrm{E}_m(\overline{K}))$.

Finally, following the method, used by M. Papikian in the case of a local ground field K ([3]), we show that Kolyvagin's formula holds for elliptic curves with good reductions over pseudolocal fields.

Theorem 4. *Let ζ be the primitive root of 1 in K that is chosen in a proper way (6) and $\varphi_1(\pi) = e_1$, $\varphi_2(\xi) = e_2 \in \mathrm{E}_m(\overline{K})$. Then $\zeta^{\langle c_1, c_2 \rangle} = \{e_1, e_2\}$, where $\{e_1, e_2\}$ is the Weil pairing on $\mathrm{E}_m(\overline{K})$, and $\langle c_1, c_2 \rangle$ is the Tate pairing.*

Proof. Again we follow the argument from [3]. Consider the maps $\varphi_1 \colon K^*/K^{*m} \to \mathrm{E}_m(K)$ and $\varphi_2 \colon K^*/K^{*m} \to \mathrm{E}_m(K)$ that satisfy the following properties $\varphi_1(\pi) = e_1,\ \varphi_1(\xi) = 0,\ \varphi_2(\pi) = 0,\ \varphi_2(\xi) = e_2$. The $\cup$-product $\varphi_1 \cup \varphi_2 \in \mathrm{H}^2(G, \mu_m)$, used to evalute the Tate pairing is described by the bilinear form $\mathrm{B}_1 : K^*/K^{*m} \times K^*/K^{*m} \to \mu_m$, where $\mathrm{B}_1(a, b) = \{\varphi_1(a), \varphi_2(b)\}$ and $\mathrm{B}_1(\pi, \pi) = 1,\ \mathrm{B}_1(\pi, \xi) = \{e_1, e_2\},\ \mathrm{B}_1(\xi, \pi) = 1,\ \mathrm{B}_1(\xi, \xi) = 1$.

We have

$$(\pi, \xi) = \frac{\theta(\pi)\xi^{1/m}}{\xi^{1/m}} = \frac{\sigma(\xi^{1/m})}{\xi^{1/m}} = \zeta,\ (\xi, \pi) = \zeta^{-1},\ (\pi, \pi) = 1,\ (\xi, \xi) = 1.$$

Therefore $\mathrm{B}_{\xi,\pi}(\pi, \pi) = \zeta^{\overline{\phi}_\xi(\pi)\overline{\phi}_\pi(\pi)} = \phi_\pi(\pi)^{\overline{\phi}_\xi(\pi)} = (\pi, \pi)^{\overline{\phi}_\xi(\pi)} = 1^{\overline{\phi}_\xi(\pi)} = 1$, $\mathrm{B}_{\xi,\pi}(\xi, \pi) = \zeta^{-1}$, $\mathrm{B}_{\xi,\pi}(\xi, \xi) = 1,\ \mathrm{B}_{\xi,\pi}(\pi, \xi) = 1$. Let $\{e_1, e_2\} = \zeta^x$. The bilinear forms B_1 and $\mathrm{B}_{\xi,\pi}$ are related $\mathrm{B}_1 = \mathrm{B}_{\xi,\pi}^{-x}$, as $\operatorname{inv} \mathrm{B}_1 = (-x) \operatorname{inv} \mathrm{B}_{\xi,\pi}$. For $\zeta^{\operatorname{inv} \mathrm{B}_1} = \zeta^{(-x) \operatorname{inv} \mathrm{B}_{\xi,\pi}}$ find $\zeta^{\operatorname{inv} \mathrm{B}_{\xi,\pi}} = (\xi, \pi) = \zeta^{-1}$. Then $\zeta^{(-x) \operatorname{inv} \mathrm{B}_{\xi,\pi}} = (\zeta^{\operatorname{inv} \mathrm{B}_{\xi,\pi}})^{-x} = (\zeta^{-1})^{-x} = \zeta^x$.

Thus, $\operatorname{inv} \mathrm{B}_1 = x$, since $\{e_1, e_2\} = \zeta^{\operatorname{inv} \mathrm{B}_1}$. Therefore, $\operatorname{inv} \mathrm{B}_1$ is the value of the Tate pairing, so $\zeta^{<c_1, c_2>} = \{e_1, e_2\}$ and the proof of Theorem 4 is finished. □

REFERENCES

1. Fesenko I.B., Vostokov S.V. Local Fields and Their Extensions. – Transl. Math. Monogr., Amer. Math. Soc., Second Edition, 2001, V.121. – 353 p.
2. Milne J.S. Class Field Theory. – Available at www.jmilne.org/math. – 2008. – 287 p.
3. Papikian M. On Tate Local Duality. Seminar "Kolyvagin's Application of Euler Systems to Elliptic curves", Massachusetts Institute of Technology – 2000, preprint.
4. Serre J.P. Corps locaux. – Paris: Hermann, 1968. – 246 p.
5. Lang S. Fundamentals of Diophantine Geometry. Springer-Verlag: Berlin-Heidelberg-New York-Tokyo, 1983. – 370 p.
6. Nesteruk V.I. *On nondegeneracy of Tate pairing for elliptic curves with good reduction over pseudolocal field*// Applied problems of mechanics and mathematics. – 2010. – V.8. – P. 37–40. (in Ukrainian)

Algebra and Logic Department
Ivan Franko National University of Lviv
volodymyr-nesteruk@rambler.ru

Received 28.11.2011