UDC 511.22 Вестник СПбГУ. Сер. 1. Т. 3 (61). 2016. Вып. 1

DEGENERATION OF THE HILBERT PAIRING IN FORMAL GROUPS OVER LOCAL FIELDS*

S. V. Vostokov[1], *R. P. Vostokova*[2], *O. Yu. Podkopaeva*[1]

[1] St.Petersburg State University,
Universitetskaya nab., 7-9, St.Petersburg, 199034, Russian Federation
[2] Baltic State Technical University,
1st Krasnoarmeyskaya ul., 1, St.Petersburg, 190005, Russian Federation

For an arbitrary local field K (a finite extension of the field $\mathbb{Q}_p$) and an arbitrary formal group law F over K, we consider an analog c_F of the classical Hilbert pairing. A theorem by S. V. Vostokov and I. B. Fesenko says that if the pairing c_F has a certain fundamental symbol property for all Lubin—Tate formal groups, then $c_F = 0$. We generalize the theorem of Vostokov—Fesenko to a wider class of formal groups. Our first result concerns formal groups that are defined over the ring O_K of integers of K and have a fixed ring O_0 of endomorphisms, where O_0 is a subring of O_K. We prove that if the symbol c_F has the above-mentioned symbol property, then $c_F = 0$. Our second result strengthens the first one in the case of Honda formal groups. The paper consists of three sections. After a short introduction in Sec. 1, we recall basic definitions and facts concerning formal group laws in Sec. 2. In Sec. 3, we state and prove two main results of the paper (Theorems 1 and 2). Refs 8.

Keywords: formal group, isogeny, formal module, Hilbert pairing.

1. Introduction. Historically, local fields were introduced by Hensel to solve problems in number theory by methods borrowed from analysis. Recently, the theory of local fields has found successful applications in diverse areas ranging from non-commutative geometry and coding theory to the study of mesoscopic and nano systems (see, e. g., numerous articles published by A. Khrennikov relating p-adic analysis to various branches of physics, biology, neural networks, etc.). The present paper is devoted to some classical aspects of the theory of local fields. Let K be a local field, i. e., a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers, and let n be a positive integer. We assume that K contains the group μ_n of all nth roots of 1. It is well known (see, e. g., [1]) that the Hilbert norm residue symbol is a non-degenerate bilinear pairing $K^* \times K^* \to \mu_n$ such that

$$(\alpha, 1-\alpha) = 1 \text{ for all } \alpha \in K^*, \alpha \neq 1, \tag{1}$$

and every non-degenerate pairing $K^* \times K^* \to \mu_n$ satisfying relation (1) is a power of the Hilbert symbol. Moreover, for non-degenerate pairings, relation (1) is equivalent to the norm property of the Hilbert symbol. Using the reciprocity map of local class field theory, one can define an analog c_F of the Hilbert symbol for formal groups over local fields as in [2]. Let $\widehat{G}_m(X, Y)$ be the multiplicative formal group. In this case, the norm residue symbol gives rise to the Hilbert pairing $c_{\widehat{G}_m}$ on $K^* \times \widehat{G}_m(M)$ with values in

$$\mu_{p^n} - 1 = \{\theta - 1 \mid \theta \in \mu_{p^n}\},$$

where M is the maximal ideal of the ring of integers O_K of K, and relation (1) is equivalent to

$$c_{\widehat{G}_m}(\alpha, -\alpha) = 0 \text{ for all } \alpha \in M.$$

*Работа выполнена при финансовой поддержке РФФИ (грант №14-01-00393) и правительства РФ (грант 14.Z50.31.0016).

Based on the example of the formal group $\widehat{G}_m$, one might be tempted to guess (as was done by S. Lang in his book [3]) that the property

$$c_F(\alpha, -\alpha) = 0 \text{ for all } \alpha \in M \tag{2}$$

remains valid for every formal group F or at least for all formal groups from a certain class. However, S. Vostokov and I. Fesenko proved in [4] that if c_F satisfies property (2) for all Lubin–Tate formal groups F, then $c_F = 0$. More precisely, they proved the following statement.

Proposition. *Let L be a field obtained by adjoining the roots κ_n of the isogeny $[\pi^n]$ to K, where π is a prime of K. Let $c_F : L^* \times F(M_L) \to \kappa_n$ be a symbol, where M_L is the maximal ideal of the ring of integers of L. If c_F satisfies property* (2) *for all $\alpha \in M_L$ and all Lubin–Tate formal groups, then $c_F(\alpha, \beta) = 0$ for all $\alpha \in L^*$ and $\beta \in F(M_L)$.*

In the present paper, we prove two new results. First, we generalize the Vostokov—Fesenko theorem to some other class of formal groups (Theorem 1). Secondly, we show that, in the case of Honda formal groups, Theorem 1 can be strengthened (Theorem 2).

2. Formal groups. ***2.1. Definition and basic properties.*** We recall some basic definitions and facts concerning formal group laws (for more details, see, e. g., [5, 6]). Let R be a commutative associative ring with identity element. A one-dimensional formal group law over R (or, simply a formal group) is a formal power series in $R[[X, Y]]$ satisfying the following conditions:

a) $F(X, F(Y, Z)) = F(F(X, Y), Z)$;

b) $F(X, 0) = X$, $F(0, Y) = Y$.

It can easily be proved that if $F(X, Y)$ is a formal group law over a ring R, then $F(X, Y) = X + Y \pmod{\deg 2}$. Moreover, there exists a formal series $i(X)$ in $R[[X]]$ such that $F(X, i(X)) = 0$ and $F(i(X), X) = 0$. It is well known that if R does not have nonzero elements that are $\mathbb{Z}$-torsion and nilpotent, then $F(X, Y)$ is commutative, i. e., satisfies the relation $F(X, Y) = F(Y, X)$. The standard examples of formal groups are $\widehat{G}_a(X, Y) = X + Y$ and $\widehat{G}_m(X, Y) = X + Y + XY$, called the additive and the multiplicative group law, respectively. Let $F(X, Y)$ and $G(X, Y)$ be formal group laws over R. A homomorphism $f : F \to G$ from $F(X, Y)$ to $G(X, Y)$ is a formal series $f(X) \in R[[X]]$ such that $f(0) = 0$ and $f(F(X, Y)) = G(f(X), f(Y))$. A homomorphism f is called an isomorphism if it has an inverse, i. e., if there exists a homomorphism $g : G \to F$ such that $f(g(X)) = g(f(X)) = X$. A homomorphism f is an isomorphism if and only if $f'(0)$ is invertible in R. An isomorphism f is called strict if $f'(0) = 1$. Homomorphisms from F to itself are called endomorphisms. We denote by $\mathrm{Hom}(F, G)$ the set of all homomorphisms from F to G and by $\mathrm{End}(F)$ the set of all endomorphisms of F.

For each F, there is a unique ring homomorphism from $\mathbb{Z}$ to $\mathrm{End}_R(F)$. We denote by $[n]_F(T)$ the image of $n \in \mathbb{Z}$ in $\mathrm{End}_R(F)$. Thus, $[1]_F(X) = X$, $[-1]_F = i_F$, $[n]_F(X) = F(X, [n-1]_F(X))$, and $[-n]_F(X) = i_F([n](X))$. It is easy to check by induction that $[n]_F(X) = nX \pmod{\deg 2}$. It follows that $[n]_F$ is an isomorphism if and only if n is invertible in R.

For $f, g \in \mathrm{Hom}(F, G)$, we define the sum $(\varphi +_G \psi)$ by the relation $(\varphi +_G \psi)(X) = G(\varphi(X), \psi(X))$. If G is commutative, then $\mathrm{Hom}(F, G)$ is an Abelian group. If we define the multiplication in $\mathrm{End}(F)$ as the composition of endomorphisms, then $\mathrm{End}(F)$ becomes a ring with 1.

For a commutative group law F over R, we have a homomorphism $c : \mathrm{End}(F) \to R$ that sends each $f \in \mathrm{End}(F)$ to $f'(0)$. Let R be of characteristic 0. Then c is an embedding. If $a \in c(\mathrm{End}(F))$, then we put $[a]_F = c^{-1}(a)$. Let C be a subring of R such that $C \subset c(\mathrm{End}(F))$. Then each element $a \in C$ gives rise to an endomorphism of F. In this case, we say that the formal group F has a structure of a formal C-module. If formal group laws F and G are formal C-modules and $f \in \mathrm{Hom}(F, G)$, then $f([a]_F) = [a]_G(f)$ for all $a \in C$.

Let $\tilde{R}$ be a localization of R with respect to the set of positive integers. A homomorphism from F to $\widehat{G}_a$ is called a logarithm of F. Every logarithm of F has the form al_F, where $a \in \tilde{R}$ and

$$l_F = \int_0^X \frac{dT}{F_X(0,T)}.$$

We have $F(X,Y) = l_F^{-1}(l_F(X) + l_F(Y))$.

If R has a prime characteristic p, then every nonzero endomorphism f of F has the form $f(X) = f_1(X^{p^h})$, where h is a nonnegative integer and $f_1'(0) \neq 0$. The number h is called the height of f. The height of the zero endomorphism is, by definition, ∞. The height of the endomorphism $[p]_F$ is called the height of the formal group law F.

Let B be a local commutative R-algebra, let M be the maximal ideal of B, and let B be complete with respect to the M-topology. For each formal group law $F(X,Y)$ over R, the power series $F(X,Y)$ and $i(X)$ converge for all $X, Y \in M$. We turn M into a group $F(M)$ by putting $x +_F y = F(x,y)$ and $-_F(x) = i_F(x)$ and call the group thus obtained the group of points of F over M. The same construction gives rise to a group structure on an arbitrary power M^n of M. We call the resulting group the group of points of F over M^n. If F has a structure of a formal C-module, then the Abelian group $F(M)$ has a structure of a C-module.

Let K be a discrete valuation field of characteristic 0 with ring of integers $R = O_K$ and residue field k of characteristic $p > 0$. For every formal group law F over O_K, we have $\mathbb{Z}_p \subset c(\mathrm{End}(F))$, and so F has a formal $\mathbb{Z}_p$-module structure. If π is a prime element of $\mathcal{O}_K$, then by the height of F we mean the height of the endomorphism $[\pi]$ reduced modulo π.

For a finite extension L/K of local fields and the maximal ideal M_L of L, we have the group $F(M_L)$. In the case of an infinite extension E/K, by $F(M_E)$ we mean the direct limit of $F(M_L)$ over the system of finite subextensions L/K of E/K. For a fixed algebraic closure $\bar{K}$ of K, we denote by $\bar{M}$ the maximal ideal of the ring of integers in $\bar{K}$ and by $F(\bar{M})$ the corresponding group. We say that an endomorphism of a formal group F over O_K is an isogeny if the corresponding group homomorphism is onto and has a finite kernel. It can be proved that an endomorphism f is an isogeny if and only if the height of f is finite. In this case the kernel of f has order p^h. Let f be an isogeny, and let $f^{(n)}$ be the n-fold composition of f with itself. Let $\kappa_{n,f}$ be the kernel of $f^{(n)}$. This is a finite subgroup of $F(\bar{M})$.

2.2. Symbols on formal groups. Let K be a local field. We recall that if K has characteristic zero, then there is an embedding $c : \mathrm{End}(F) \to O_K$ that sends each $f \in \mathrm{End}(F)$ to $f'(0)$. We denote by O_0 the image of $\mathrm{End}(F)$ in R. Let K_0 be the field of fractions of O_0. We consider an algebraic closure $\bar{K}_0$ of K_0 and the group $F(\bar{M})$ of points of F over $\bar{M}$, where $\bar{M}$ is the maximal ideal of the ring of integers in $\bar{K}_0$.

Let B be a topological O_0-module in which the addition and the action of the elements of O_0 is induced by the formal group F. A symbol on $F(M)$ is, by definition, a continuous

bilinear pairing

$$c_F : \bar{K}_0^* \times F(\bar{M}) \to B.$$

By bilinearity of c_F, we mean that the following conditions are valid:

$$\begin{aligned} &c_F(\alpha_1\alpha_2, \beta) = c_F(\alpha_1, \beta) +_F c_F(\alpha_2, \beta),\\ &c_F(\alpha, \beta_1 +_F \beta_2) = c_F(\alpha, \beta_1) +_F c_F(\alpha, \beta_2),\\ &c_F(\alpha, [a]\beta) = [a]c_F(\alpha, \beta), \end{aligned}$$

where $\alpha, \alpha_1, \alpha_2 \in \bar{K}_0^*$, $\beta, \beta_1, \beta_2 \in F(\bar{M})$, and $a \in O_0$. In a more general case, where we consider an entire class Φ of formal groups with the same group of points, the latter property assumes the following form:

$$c_G(\alpha, \phi(\beta)) = \phi(c_F(\alpha, \beta))$$

for all $F, G \in \Phi$ and every homomorphism $\phi : F \to G$.

3. Main results. In this section, we prove two theorems concerning the symbols satisfying condition (2). Let K be a local field and O_K be the ring of integers of K. Let L be an extension of K containing the kernel κ_n of the isogeny $[\pi_0^n]$, where π_0 is a prime element of the ring O_0. We denote by M_L the maximal ideal of the ring of integers of L.

Theorem 1. *If a symbol $c_F : L^* \times F(M_L) \to \kappa_n$ satisfies the relation $c_F(\alpha, -\alpha) = 0$ for every formal group F over O_K such that* $\mathrm{End}(F) \simeq O_0$ *and for all $\alpha \in M_L$, then $c_F(\alpha, \beta) = 0$ for all $\alpha \in L^*$ and $\beta \in F(M_L)$.*

Proof. We fix a formal group F satisfying the conditions of Theorem 1. Let $\phi(X) = X + a_2X^2 + \cdots +$ be a series with coefficients in O_K. We prove that there exists a formal group $G(X, Y) \in O_K[X, Y]$ such that the series $\phi(X)$ is a homomorphism from G to F and $\mathrm{End}(G) \simeq O_0$. To this end, it is necessary to prove that there exists a $G(X, Y) \in K[[X, Y]]$ such that

$$\phi(G(X, Y)) = F(\phi(X), \phi(Y)).$$

We let

$$G(X, Y) = \phi^{-1} \circ F \circ \phi,$$

where ϕ^{-1} is the inverse to ϕ with respect to the composition, and prove that $G(X, Y)$ is a required formal group. First, we prove that $G(X, Y)$ is a formal group. We have

$$G(X, 0) = \phi^{-1}(F(\phi(X), 0) = \phi^{-1}(\phi(X)) = X.$$

Similarly, $G(0, Y) = Y$. Finally,

$$\begin{aligned} G(X, G(Y, Z)) &= \phi^{-1}(F(\phi(X), \phi(G(Y, Z))) = \phi^{-1}(F(\phi(X), F(\phi(Y), \phi(Z)))) =\\ &= \phi^{-1}(F((\phi(X), F(\phi(Y)), \phi(Z))) = \phi^{-1}(F(\phi(G(X, Y)), \phi(Z))) = G(G(X, Y), Z). \end{aligned}$$

It remains to check the relation $\mathrm{End}(G) \simeq O_0$. However, this is obvious due to the fact that the homomorphism $\psi(a) = \phi^{-1} \circ a \circ \phi$ yields an isomorphism $\mathrm{End}(F) \simeq \mathrm{End}(G)$ of endomorphism rings.

From what have just been proved, it follows that the relation

$$c_F(\alpha, \phi(-\alpha)) = 0$$

is valid for all $\phi(X) \in O_K[[X]]$. Now we observe that $c(\theta, \beta) = 0$ if $\theta \in \mu_{q-1}$, where q is the number of elements in the residue field of K. This follows from the bilinearity of the symbol and the fact that the order of B is prime to $q-1$. Let π be a prime in O_L. Obviously, $c_G(\pi, -\theta\pi) = 0$ is valid for every formal group G satisfying the conditions of Theorem 1. Consequently, $c_F(\pi, \phi(-\theta\pi)) = 0$. For each $\beta \in F(M_L) \setminus F(M_L^2)$, there is a series $\phi(X) \in O_K[[X]]$ and $\theta \in \mu_{q-1}$ such that

$$\phi(-\theta\pi) = \beta.$$

Thus, we obtain that $c_F(\pi, \beta) = 0$ for all $\beta \in F(M_L) \setminus F(M_L^2)$. We see that if $\beta \in F(M_L^2)$, then $\beta +_F (-\pi) = \beta' \in F(M_L) \setminus F(M_L^2)$. Therefore,

$$c_F(\pi, \beta') = c_F(\pi, \beta) +_F c_F(\pi, -\pi) = 0,$$

which implies that $c_F(\pi, \beta) = 0$ for all $\beta \in F(M_L)$ and for all prime elements π of the ring of integers. It only remains to observe that the multiplicative group of a field is generated by its prime elements. This completes the proof of Theorem 1. ■

The condition imposed on the symbol in Theorem 1 is very strong. Namely, we assumed that property (2) is valid for all formal groups from a certain class of groups. Theorem 2, which is stated and proved below, establishes the degeneration of any symbol satisfying condition (2) for an individual formal group of certain type, namely, for a Honda formal group (for the definition of Honda groups, see [7, 8]).

Theorem 2. *Let K be a local field, let O_K be the ring of integers in K with maximal ideal M_K. Let E be a subfield of K such that K/E is an unramified extension of local fields, and let O_E be the ring of integers of E. Let $F \in O_K[[X, Y]]$ be a formal group such that $\mathrm{End}(F) \simeq O_E$. Let π be a prime element of E, and let the height of $[\pi]$ be equal to 1. Let κ_n be the kernel of $[\pi^n]$, let $L = K(\kappa_n)$, and let M_L be the maximal ideal of the ring of integers in L. Finally, let $c_F : L^* \times M_L \to \kappa_n$ be a symbol such that $c_F(\alpha, -\alpha) = 0$ for all $\alpha \in M_L$. Then $c_F(\alpha, \beta) = 0$ for all $\alpha \in L^*$ and all $\beta \in M_L$.*

We need several lemmas.

Lemma 1. *Under the conditions of Theorem 2, the extension L/K is totally ramified.*

Proof. For each s, $1 \le s \le n$, let κ_s be the kernel of $[\pi^s]$, and let K_s be the field obtained by adjoining κ_s to K. First, we show that the extension K_1/K is totally ramified. It is sufficient to prove that each element $a \in \kappa_1$ is a root of some Eisenstein polynomial. We observe that a is a root of

$$[\pi](X) = \pi X + a_2 X^2 + \cdots + a_p X^p + \cdots .$$

We see that the coefficients of $[\pi](X)$ belong to O_K. Since the height of $[\pi]$ is equal to 1, we have $a_i \in M_K$ for $i \le p-1$ and $a_p \notin M_K$ (π is a prime in E; but K/E is unramified, consequently, π is a prime in K). By the Weierstrass preparation theorem, we have

$$[\pi](X) = (c_0 + \cdots + c_{p-1} X^{p-1} + X^p)(b_0 + b_1 X + \cdots), \tag{3}$$

where $b_i, c_i \in O_K$ and b_0 is invertible. We may slightly change Eq. (3) by assuming that $b_0 = 1$. Then the roots of $[\pi]$ are roots of the first factor in (3). Consequently, it remains

to prove that this factor is an Eisenstein polynomial, which is easy. Indeed, Eq. (3) with $b_0 = 1$ and the fact that $a_i \in M_K$ for $i \le p-1$ and $a_p \notin M_K$ imply that $c_1 = \pi$, $c_i \in M_K$ for $i \le p-1$, and $c_p \notin M_K$. Thus, each element of κ_1 is a root of an Eisenstein polynomial. Therefore, the extension K_1/K is totally ramified. Now, we prove by induction that the extension K_n/K is totally ramified. We remark that $\kappa_1 \subset \kappa_2 \subset \cdots \subset \kappa_n$ and prove that for each s, $1 < s \le n$, the extension K_s/K_{s-1} is totally ramified. For this, we must prove that each element of $K_s \setminus K_{s-1}$ is a root of an Eisenstein polynomial. Since

$$[\pi^s](X) = \pi^s X + \cdots + a_{p^s} X^{p^s} + \cdots,$$

we obtain that $c([\pi^s]) = \pi^s$, and the height of $[\pi^s]$ is s. In the same way as for the case $s = 1$, we obtain

$$[\pi^s](X) = P_s(X)(1 + b_1 X + \cdots), \tag{4}$$

where $P_s(X)$ is a polynomial of degree p^s. All elements of κ_s are roots of this polynomial, $P_s(0) = 0$, and $c(P_s(X)) = \pi^s$. From the Weierstrass preparation theorem, we obtain that all coefficients of the polynomials $P_s(X)$, except the leading ones, are divisible by π. Since $\kappa_s \supset \kappa_{s-1}$, the polynomial $P_s(X)$ is divisible by $P_{s-1}(X)$, and we have

$$P_s(X) = P_{s-1}(X)\left(\pi + a_1 X + \cdots + a_{p^s c - p^{s-1}} X^{p^s - p^{s-1}}\right). \tag{5}$$

It follows that all coefficients of the polynomial

$$\pi + a_1 X + \cdots + a_{p^s - p^{s-1}} X^{p^s - p^{s-1}}, \tag{6}$$

except the leading one, are divisible by π, which means that this polynomial is Eisenstein. Since the elements of K_s/K_{s-1} are roots of (6), the extension K_s/K_{s-1} is totally ramified. The lemma is proved. ■

Thus, we proved that the extension L/K is totally ramified. It follows that the residue fields of the fields L and K are isomorphic. Therefore, we can choose a common system of multiplicative representatives for L and K.

Lemma 2. *Let $\Theta = \{\theta_k \mid 1 \le k \le q-1\}$ be a common system of multiplicative representatives for L and K, and let $\bar\pi$ be a prime element in L. Then $A = \{\theta_k \bar\pi^n \mid 1 \le k \le q-1, n \ge 1\}$ is a set of generators for M_L with respect to the operation $+_F$.*

Proof. Since $\bar\pi$ is a prime in L and the extension L/K is totally ramified, every $\alpha \in M_L$ can be represented in the form

$$\alpha = a_1 \bar\pi + \cdots + a_n \bar\pi^n + \cdots. \tag{7}$$

Now, we can successively approximate α by formal sums of elements of A. ■

The same reasoning can be used to prove the following statement.

Lemma 3. *If $A = \{a_{ij} \mid i \ge 1, 0 \le j \le q-1\}$ is a system of multiplicative representatives such that $a_{ij} \equiv \theta_j \bar\pi^i \pmod{\bar\pi^{i+1}}$, then A is a set of generators for M_L with respect to the operation $+_F$.*

Now we turn back to the proof of Theorem 2. Let $\bar{\pi}$ be a prime in O_L. We show that $c_F(\bar{\pi}, \beta) = 0$ for all $\beta \in M_n$. By Lemma 3, it is sufficient to prove that there exists a system $\{a_{ij} \mid i \geq 1, 0 \leq j \leq q-1\}$ of multiplicative representatives such that

$$a_{ij} \equiv \theta_j \bar{\pi}^i \pmod{\bar{\pi}^{i+1}} \text{ and } c_F(\bar{\pi}, a_{ij}) = 0 \text{ for all } i \text{ and } j. \tag{8}$$

By assumption, we have $c_F(\alpha, -\alpha) = 0$ for all $\alpha \in M_L$. Hence, $c_F(\alpha^m/\theta, -\alpha^m/\theta) = 0$, where $\theta \in \Theta$. It follows that

$$c_F(\alpha^m, -\alpha^m/\theta) = c_F(\alpha^m\theta, -\alpha^m/\theta) +_F c_F(\theta, -\alpha^m/\theta) = 0 \tag{9}$$

since $c_F(\theta, \beta) = 0$ for all $\theta \in \Theta$ and $\beta \in M_L$. If m is prime to p, then Eq. (9) implies that

$$c_F(\alpha, -\alpha^m/\theta) = 0. \tag{10}$$

Putting $\alpha = \bar{\pi}$ in Eq. (10), we obtain

$$c_F(\bar{\pi}, -\bar{\pi}^m/\theta) = 0. \tag{11}$$

If θ runs through a system of multiplicative representatives, then $-1/\theta$ runs through the same system of representatives. Therefore, it is sufficient to prove that relations (8) are valid for $i \equiv 0 \pmod{p}$. Assuming that relations (8) hold when $0 < i \leq ps - 1$ and $0 < j \leq q-1$, we prove that they are valid for $a_{ps,j}$. We consider separately two different cases: 1) $s < \frac{p^n}{p-1}$ and 2) $s > \frac{p^n}{p-1}$.

1) Since $c_F(\bar{\pi}, a_{sj}) = 0$, we have $[\pi](c_F(\bar{\pi}, a_{sj})) = c_F(\bar{\pi}, [\pi](a_{sj})) = 0$. Since the height of $[\pi]$ is 1, we have

$$[\pi](X) = \pi X + a_2 X^2 + \cdots + a_{p-1}X^{p-1} + a_p X^p + \cdots,$$

where $a_2, \ldots, a_{p-1}$ are divisible by π and a_p is not divisible by π. Since the extension K_n/K is totally ramified, we have $v(\pi) = p^n$. Consequently, $v([\pi](a_{sj})) = ps$. Since $v(a_p) = 0$, we see that if θ_j runs through the system of multiplicative representatives, $a_p\theta_j^p$ runs through the same system of representatives because p is prime to $q-1$. Therefore, for each i there is a j such that

$$[\pi](a_{sj}) \equiv \theta_i \bar{\pi}^{ps} \pmod{\bar{\pi}^{ps+1}},$$

and we can take $[\pi](a_{sj})$ as $a_{ps,i}$.

2) In this case we have $ps = p^n + s_1$, where $s_1 > s$. Consequently, $ps_1 > p^n + s_1$. As in case 1), we obtain that

$$v([\pi](a_{s_1 j})) = p^n + s_1.$$

If $\pi \equiv a\bar{\pi}^{p^n} \pmod{\bar{\pi}^{p^n+1}}$ and a is not divisible by $\bar{\pi}$, then

$$[\pi](a_{s_1 j}) \equiv a\theta_j \bar{\pi}^{p^n+s_1} \pmod{\bar{\pi}^{p^n+s+1}}.$$

Since $v(a) = 0$, the elements $a\theta_j$ run through the same system of multiplicative representatives as θ_j do. This implies that the required elements $a_{p^n+s_1,i}$ exist, which completes the proof of Theorem 2. ■

References

1. Iwasawa K., *Local class field theory* (Oxford Univ. Press, 1986, 155 p.).
2. Fröhlich A., "Formal groups", *Lect. Notes in Math.* **74** (Heidelberg, Springer, 1968, 140 p.).

3. Lang S., *Cyclotomic fields* (Heidelberg, Springer, 1978, 253 p.).

4. Vostokov S. V., Fesenko I. B., "A certain property of the Hilbert pairing", *Math. Notes* **43**(3), 226–230 (1988).

5. Hazewinkel M., *Formal groups and application* (Academic Press, New York, 1978, 573 p.).

6. Kolyvagin V. A., "Formal groups and the norm residue symbol", *Math. USSR-Izv.* **15**(2), 289–348 (1980).

7. Honda T., "On the theory of commutative formal groups", *J. Math. Sci. Japan* **22**, 213–246 (1970).

8. Vostokov S. V., Demchenko O. V., "An explicit formula of the Hilbert pairing for Honda formal groups", *J. Math. Sci.* **116**(1), 2926–2952 (New York, 2003).

Статья поступила в редакцию 22 октября 2015 г.

Сведения об авторах

Востоков Сергей Владимирович — доктор физико-математических наук, профессор; s.vostokov@spbu.ru

Востокова Регина Петровна — доцент; rvostokova@yandex.ru

Подкопаева Оксана Юрьевна — кандидат физико-математических наук, научный сотрудник; o.podkopaeva@spbu.ru

ВЫРОЖДЕНИЕ СПАРИВАНИЯ ГИЛЬБЕРТА ДЛЯ ФОРМАЛЬНЫХ ГРУПП НАД ЛОКАЛЬНЫМИ ПОЛЯМИ

С. В. Востоков[1], *Р. П. Востокова*[2], *О. Ю. Подкопаева*[1]

[1] Санкт-Петербургский государственный университет, Российская Федерация, 199034, Санкт-Петербург, Университетская наб., 7-9; s.vostokov@spbu.ru, o.podkopaeva@spbu.ru

[2] Балтийский государственный технический университет «Военмех» им. Д. Ф. Устинова, Российская Федерация, 190005, Санкт-Петербург, 1-я Красноармейская ул., 1; rvostokova@yandex.ru

Для произвольного локального поля (конечного расширения поля $\mathbb{Q}_p$) и произвольной формальной группы над полем K мы рассматриваем аналог c_F классического символа Гильберта. Теорема Востокова—Фесенко утверждает, что если c_F удовлетворяет основному символьному свойству, то $c_F = 0$. Мы обобщаем теорему Востокова—Фесенко на более широкий класс формальных групп. Наш первый результат относится к формальным группам, определённым над кольцом целых O_K и имеющим в качестве кольца эндоморфизмов некоторое фиксированное подкольцо O_0 кольца O_K. Мы доказываем, что если c_F имеет вышеупомянутое символьное свойство, то $c_F = 0$. Наш второй результат усиливает первый в случае формальных групп Хонды. Статья состоит из трёх частей. После краткого введения (часть 1) мы напоминаем основные определения и факты о формальных групповых законах (часть 2). В последней части статьи мы формулируем и доказываем наши основные результаты (теоремы 1 и 2). Библиогр. 8 назв.

Ключевые слова: формальная группа, изогения, формальный модуль, спаривание Гильберта.