EXPLICIT FORM OF THE HILBERT SYMBOL
FOR POLYNOMIAL FORMAL GROUPS

S. VOSTOKOV AND V. VOLKOV

Abstract. Let $K$ be a local field, $c$ a unit in $K$, and $F_c(X, Y) = X + Y + cXY$ a polynomial formal group that gives rise to a formal module $F_c(\mathfrak{m})$ on the maximal ideal in the ring of integers of $K$. Assume that $K$ contains the group $\mu_{F_c,n}$ of the roots of isogeny $[p^n]c(X)$. The natural Hilbert symbol $(\cdot, \cdot)_c: K^* \times F_c(\mathfrak{m}) \to \mu_{F_c,n}$ is defined over the module $F(\mathfrak{m})$. An explicit formula for $(\cdot, \cdot)_c$ is constructed.

§1. Introduction

The present paper continues the papers [5, 6], which were devoted to Hilbert pairing over the so-called polynomial formal groups. It is easy to show that the groups of the form $F_c = X + Y + cXY$ are the only formal groups defined by polynomials. We call such groups polynomial formal groups and investigate the Hilbert pairing over them. The case where the element $c$ belongs to the ring of Witte vectors, i.e., the case of polynomial Honda groups, was treated in [5]. There, the main results in the unramified case were formulated together with proof sketches. A similar pairing over the universal formal group $F_x = X + Y + xXY$ (where $x$ is an independent variable) was constructed and studied in [6].

Now we consider an arbitrary polynomial formal group $F_c = X + Y + cXY$, where $c$ is a unit in some local ring (finite extension of $\mathbb{Q}_p$) and find an explicit formula for the Hilbert symbol defined over the formal module of the group $F_c$. Similar formulas were constructed previously for the formal Lubin–Tate groups in [9, 10], for Honda groups in [11, 12, 13], and for the relative formal Lubin–Tate groups in [13]. The case considered in the present paper provides the first example of a formula for the Hilber symbol of groups whose ring of endomorphisms embeds in, but is not isomorphic to the ring where the group is defined.

We use the method suggested in [8] to derive the claimed explicit formula.

§2. Notation

We denote:

- $p \geq 3$ is a prime number;
- $\zeta$ is a certain fixed primitive root of unity of degree $p^n$;
- $K$ is a finite extension of the field $\mathbb{Q}_p$ that contains $\zeta$, with the ring of integers $\mathcal{O}_K$;
- $c$ is a unit of the local field $K$;
- $T$ is the inertia subfield of $K$, with the ring of integers $\mathcal{O} = \mathcal{O}_T$;
- $e$ is the ramification degree of $K/T$;
- $e_1 = e/(p - 1)$ is the relative ramification degree of $K/T(\zeta_1)$;
- $e_0 = e_1/p^{n-1}$;

2010 Mathematics Subject Classification. Primary 11S31; Secondary 14L05.

Key words and phrases. Polynomial formal groups, formal groups, Hilbert symbol, local rings.

Supported by RFBR (grant no. 14-01-00393).
Note that if we further define
\[ s = \frac{[p^n]c(X)}{c(X)} = \frac{\log(1 + cX)}{cX}, \]
then
\[ \lambda_c(X) = c^{-1}(1 + cX)(1 + cY) - 1, \]
whence \( \lambda_c(X) = c^{-1} \log(1 + cX) \) and \( \xi = c^{-1}(\xi - 1) \). We denote the completion of the maximal unramified \( p \)-extension of \( T \) by \( \tilde{T} \), and the Frobenius automorphism of the topological Galois group \( \text{Gal}(\tilde{T}/T) \) by \( \varphi \):

\[
\begin{array}{cccccc}
\mathbb{Q}_p & \Delta & T & T(\xi) & T(\xi, c) & K \\
\varphi & \varphi & \varphi & \varphi & \\
\tilde{T} & \tilde{T}(\xi) & \tilde{T}(\xi, c) & \tilde{T}K
\end{array}
\]

We fix certain series \( \zeta, \zeta_2 \), and \( \xi = c^{-1}(\xi - 1) \) in \( \mathcal{O}[[X]] \) such that \( \zeta(\pi) = c, \zeta(\pi) = \zeta, \) and \( \xi(\pi) = \xi \).

Consider the group \( \mathcal{H}_m = \mathcal{O}((X))^* \) and the formal \( \mathbb{Z}_p \)-module \( \mathcal{H}_c = X\mathcal{O}[[X]] \).

The structure of a \( \mathbb{Z}_p \)-module is defined on \( \mathcal{H}_c \) by the formal group \( F_c = X + Y + cXY \), which is an analog of the group \( F_c \), and the series \( \lambda_c = c^{-1} \log(1 + cX) \) is an analog of its logarithm.

We introduce an operator \( \Delta \) on the Laurent series ring:

\[ \Delta f(x) = \sum a_i^{\Delta} X^{pi}, \quad \text{where} \quad f(x) = \sum a_i X^i, \ a_i \in \mathcal{O}. \]

Next, we define the series

\[ s = [p^n]c(X) = \frac{\log(1 + cX)}{cX}; \]
\[ s_{n-1, c} = [p^{n-1}]c(\zeta); \]
\[ u_c = s_c/s_{n-1, c}. \]

Note that if we further define \( s = (\zeta^n - 1) \) and \( s_{n-1} = (\zeta^{p-1} - 1), \) where \( \zeta = 1 + c \cdot \zeta \), then

\[ u_c = s_c/s_{n-1, c} = s/s_{n-1} = u, \]

where \( s, s_{n-1}, \) and \( u \) are the same as in \( \mathbb{H} \ §3 \).

Consider the following functions \( E \) and \( \ell \):

\[ \ell(\alpha) = \frac{1}{p} \log \left( \frac{\alpha^p}{\alpha^c} \right), \quad \text{where} \quad \alpha \in \mathcal{H}_m, \]
\[ E(\beta) = \exp \left( 1 + \frac{\Delta}{p} + \frac{\Delta^2}{p^2} + \ldots \right) \beta, \quad \text{where} \quad \beta \in X\mathcal{O}[[X]] \]

(see \( \mathbb{H} \ §1 \)).
The definition given above agrees with that in [I §1], because for \( \beta \in XO[[X]] \) we have
\[
\ell(1 + \beta) = \frac{1}{p} \log \left( \frac{(1 + \beta)^p}{1 + \beta} \right) = \log(1 + \beta) - \frac{1}{p} \log(1 + \beta^\Delta) = \left( 1 - \frac{\Delta}{p} \right) \log(1 + \beta).
\]

Consider the analogs of these functions for the formal group \( F_\zeta \):
\[
\ell_c(\beta) = \zeta^{-1}\ell(1 + \zeta\beta), \quad \text{where} \quad \beta \in H_c,
\]
\[
E_c(\beta) = \zeta^{-1}(E(\zeta\beta) - 1), \quad \text{where} \quad \beta \in XO[[X]].
\]

The corresponding result on the functions \( \ell \) and \( E \) (see [I §1, Proposition 1]) implies the following statement.

**Proposition 1.** The functions \( \ell_c \) and \( E_c \) are mutually inverse isomorphims between the additive \( \mathbb{Z}_p \)-module \( XO[[X]] \) and the formal \( \mathbb{Z}_p \)-module \( H_c \).

In what follows, we use the notation \( F_c \) for the formal group \( F_\zeta \) and \( \lambda_c \) for its logarithm \( \lambda_\zeta \), since it is always clear whether we are currently dealing with numbers or formal series.

One can easily check the following relations:
\[
(1) \quad d\alpha^\Delta = pX^{-1}(Xd\alpha)^\Delta; \quad d\ell(\alpha) = \alpha^{-1}d\alpha - X^{-1}(X^{-1}d\alpha)^\Delta.
\]

We also recall the definition of the Hilbert symbol \( (\cdot, \cdot)_c \) of the formal group \( F_c \):
\[
(\alpha, \beta)_c = B^{\sigma(\alpha)} - F\alpha B,
\]
where \( \alpha \in K^*, \beta \in F_c(\mathbb{M}) \), \( B \) is the solution of the equation \([p^n]c(B) = \beta\), and \( \sigma: K^* \to \text{Gal}(K_{ab}/K) \) is the Artin–Frobenius automorphism.

### §3. Pairing over the formal \( \mathbb{Z}_p \)-module \( H_c \)

For \( \alpha \in K^* \) and \( \beta \in F_c(\mathbb{M}) \), we introduce the pairing
\[
\langle \cdot, \cdot \rangle_c : H_m \times H_c \to \mathcal{O}/p^n,
\]
\[
\alpha, \beta \mapsto \text{res}_X \Phi(\alpha, \beta)/s_c \mod p^n,
\]
where \( \Phi(\alpha, \beta) = \ell_c(\beta)\alpha^{-1}d\alpha - \ell(\alpha)\zeta^{-1}d\frac{\Delta}{p} \zeta \lambda_c(\beta) \).

**Proposition 2.** The pairing \( \langle \cdot, \cdot \rangle_c \) is \( \mathbb{Z}_p \)-linear, i.e.,
\[
\langle \alpha_1 \alpha_2, \beta \rangle_c = \langle \alpha_1, \beta \rangle_c + \langle \alpha_2, \beta \rangle_c; \quad \langle \alpha^a, \beta \rangle_c = a \langle \alpha, \beta \rangle_c,
\]
\[
\langle \alpha, \beta_1 + F_c \beta_2 \rangle_c = \langle \alpha, \beta_1 \rangle_c + \langle \alpha, \beta_2 \rangle_c; \quad \langle \alpha, [a]c(\beta) \rangle_c = a \langle \alpha, \beta \rangle_c.
\]

**Proof.** Linearity over the first argument follows from that of the logarithmic derivative and the function \( \ell(\alpha) \). Linearity over the second argument follows from that of the functions \( \ell_c \) and \( \lambda_c \).

**Proposition 3.** The pairing \( \langle \cdot, \cdot \rangle_c \) satisfies the following Steinberg relation:
\[
\langle \alpha, \zeta^{-n-1} \alpha \rangle_c = 0, \quad \text{where} \quad \alpha \in XO[[X]] \setminus \{0\}.
\]

**Proof.** First we prove the congruence
\[
(2) \quad \alpha^{mp} - \alpha^{m\Delta} \equiv m\alpha^{m\Delta} \mod (mp)^2, \quad \text{for} \quad \alpha \in \mathcal{O}[[X]]^*.
\]
By the definition of ℓ we have ℓ(α) = log(α^p/α^Δ)/p, i.e., mp·ℓ(α) = log α^{mp-mΔ}, whence
\[ α^{mp} - α^{mΔ} = α^{mΔ}(α^{mp-mΔ} - 1) = α^{mΔ}(\exp(\log α^{mp-mΔ}) - 1) \]
\[ = α^{mΔ}(\exp(mp·ℓ(α)) - 1) = α^{mΔ}\left(μpℓ(α) + \sum_{i≥2} (mp)^i/i! ℓ(α)^i\right) \]
\[ = α^{mΔ}μpℓ(α) + α^{mΔ}\sum_{i≥2} (mp)^i/i! ℓ(α)^i. \]

Note that if i ≥ 2 and p ≥ 3, then (mp)^i/i! ≡ 0 mod (mp)^2. Therefore, (2) is true.

The identities in (1) imply
\[ ψ_m = \frac{α^{pm} - α^{mΔ}}{pm}α^{-1}dα - ℓ(α) ≡ dχ_m, \]
(3) where χ_m = \frac{α^{pm} - α^{mΔ}}{(pm)^2} - \frac{α^{mΔ}}{pm} ℓ(α).

Moreover, the series χ_m has integral coefficients, in accordance with (2).

Any series β ∈ O[[x]] satisfies the congruence
\[ β^{p^n}m ≡ β^{p^n-1mΔ} mod p^n. \]
(4) Indeed, β^n ≡ β^Δ mod p, and easy induction shows that β^{p^n} ≡ β^{p^n-1Δ} mod p^n, yielding (4).

Now we calculate the series Φ(α, β^{p^n-1}). Directly from the definition, we deduce the relation
\[ Φ(α, β^{p^n-1}) = ℓ_c(β^{p^n-1}α)α^{-1}dα - ℓ(α)β^{-1}d(α^Δ β^{p^n-1}α). \]
(5)

Consider the first summand and apply the definition of ℓ_c to it:
\[ ℓ_c(β^{p^n-1}α)α^{-1}dα = ε^{-1}\left(1 - \frac{Δ}{p}\right)\log(1 + β^nα)α^{-1}dα \]
\[ = ε^{-1}\sum_{p|m} (-1)^{m-1}ε^{p^mαm}{m\choose αm}α^{-1}dα \]
\[ + ε^{-1}\sum_{m≥1} (-1)^{m-1}ε^{p^{m+1}αm}{m\choose pm}α^{p^m αm} - ε^{p^n αm}α^{p^m αm}α^{-1}dα. \]
(6)

It is easily seen that if p ∤ m, then
\[ ε^{p^m αm}{m\choose αm}α^{-1}dα \equiv d(ε^{p^m αm}{m\choose m^2}) mod p^n, \]
so that the first summand in (6) takes the form
\[ ε^{-1}\sum_{p|m} (-1)^{m-1}ε^{p^m αm}{m\choose αm}α^{-1}dα \equiv ε^{-1}dη mod p^n, \]
where η = \sum_{p|m} (-1)^{m-1}ε^{p^m αm}{m\choose m^2}.

Here the series η has integral coefficients. Finally, substituting this in (6) and taking (4) into account, we get
\[ ℓ_c(β^{p^n-1}α)α^{-1}dα = ε^{-1}dη + ε^{-1}\sum_{m≥1} (-1)^{m-1}ε^{p^{m+1}αm}{m\choose pm}α^{p^m αm}α^{-1}dα. \]
(7)
Now we consider the second summand in (5):

$$\ell(\alpha)c^{-1}d\frac{\Delta}{p}(g\lambda(g^{n-1}\alpha)) = \ell(\alpha)c^{-1}d\sum_{m \geq 1}(-1)^{m-1}\frac{g^{n+m}\alpha^m}{pm}.$$  

We use congruence (4) to get

$$\ell(\alpha)c^{-1}d\frac{\Delta}{p}(g\lambda(g^{n-1}\alpha)) \equiv \ell(\alpha)c^{-1}d\sum_{m \geq 1}(-1)^{m-1}\frac{g^{n+1+m}\alpha^m}{pm} \mod p^n.$$  

Hence, recalling (7), we see that

$$\Phi(\alpha, g^{n-1}\alpha) \equiv c^{-1}\left(d\eta + \sum_{m \geq 1}(-1)^{m-1}g^{n+1+m}d\chi_m\right) \mod p^n,$$

and the series $\varphi$ and $\chi_m$ have integral coefficients. Thus,

$$\langle \alpha, g^{n-1}\alpha \rangle = \text{res}_X \Phi(\alpha, g^{n-1}\alpha)/s_c \equiv \text{res}_X \left(d\eta + \sum_{m \geq 1}g^{n+1+m}d\chi_m\right)/s \equiv 0 \mod p^n,$$

because $s_c = c^{-1}s$ and $d(1/s) \equiv 0 \mod p^n$. This proves the Steinberg relation is question. 

\begin{section}{Primary elements}

In the multiplicative case, the $p^n$-primary elements in the field $K$ were constructed and investigated in \[1\]. Recall that an element $\omega \in K^*$ is said to be $p^n$-primary if the extension $K(\sqrt[n]{\omega})/K$ is unramified. Two types of primary elements were defined in \[1\].

The first type will be called the Hasse type; we construct it in the following way. Let $a \in \mathcal{O}$ and $A \in \mathcal{O}_p$ be elements such that $A^n - a = 0$. Then the element $H(a) = E(p^nA\ell(\xi))|_{X = \pi}$ is $p^n$-primary, and for the Hilbert symbol $(\cdot, \cdot): K^* \times K^* \to \langle \zeta \rangle$ in the field $K$ we have $(\pi, H(a)) = \zeta^{ra}$ (see \[1\] §4, Lemma 8).

The second type of $p^n$-primary elements, as constructed in \[1\], has the form $\omega(a) = E(a(\sqrt[n]{\zeta} - 1))|_{X = \pi}$; it is related to $H(a)$ by $\omega(a) \equiv H(a) \mod (K^*)p^n$ (see \[1\] §4, item 3). The main difference between these types is that in the construction of the second type only elements of initial field $K$ are used.

Denote $H'(a) = \sqrt[n]{H(a)}$, $\omega'(a) = \sqrt[n]{\omega(a)}$. Then $H'(a)$ and $\omega'(a)$ lie in the finite unramified extension of the field $T(\zeta)$.

Now we define primary elements in the formal module $F_c(\mathfrak{M})$. An element $\omega_c \in F_c(\mathfrak{M})$ is said to be $p^n$-primary if the extension $K(\sqrt[n]{\mathfrak{M}}\omega_c)/K$ is unramified. Define

$$H_c(a) = c^{-1}(H(a) - 1) = E_c(p^nA\ell_c(\xi))|_{X = \pi};$$

$$\omega_c(a) = c^{-1}(\omega(a) - 1) = E_c(as_c(X))|_{X = \pi}.$$  

It is clear that $H_c(a), \omega_c(a) \in T(\zeta, c)$, and the elements $H'_c(a) = \sqrt[n]{H_c(a)}, \omega'_c(a) = \sqrt[n]{\omega_c(a)}$ lie in the unramified extension of the field $T(\zeta, c) = T(\xi, c)$.

\begin{Theorem} $H'_c(a)^p = H'_c(a) + F_c[a_\varphi](\xi)$, where $A^p - A = a_\varphi \in \mathbb{Z}_p$. \end{Theorem}
Proposition 5. Let a similar statement is true for the multiplicative case (see [1] §4, proof of Lemma 8), and $c^\varphi = c$, we have
\[
H'_c(a)^\varphi = c^{-1}(H'(a)^\varphi - 1) = c^{-1}(H'(a)c^\varphi - 1)
\]
\[
= c^{-1}(E(A\ell(\zeta))|_{X=\pi} \cdot c^\varphi - 1)
\]
\[
= c^{-1}((1 + cE_c(Ac^{-1}\ell(\zeta))|_{X=\pi}) \cdot c^\varphi - 1)
\]
\[
= c^{-1}((1 + cH'_c(a)) \cdot c^\varphi - 1) = H'_c(a) + F_c [a_\varphi](\xi).
\]

\[\Box\]

Remark 1. In our case $\varphi = \Delta^f$ with $f = (T : \mathbb{Q}_p)$, whence $A^\varphi - A = \text{tr} a \Rightarrow a_\varphi = \text{tr} a$.

Corollary. $(\pi, H_c(a))_c = [\text{tr} a]_c(\xi)$.

Proof. $H_c(a) \in T(\zeta, c)$, $H'_c(a) \in \mathcal{T}(\zeta, c)$. By the definition of the Hilbert symbol, we get
\[
(\pi, H_c(a))_c = H'_c(a)^\varphi - F_c H'_c(a) = [\text{tr} a]_c(\xi).
\]

\[\Box\]

Proposition 4. $\omega_c(a) \equiv H_c(a) \text{ mod } [p^n]_c(F_c(\mathfrak{M})).$

Proof. A similar proposition for the multiplicative case (see [1] §4 or [3] Chapter V, item 4) gives $\omega(a) = H(a) \cdot \varepsilon_\pi^n$, where $\varepsilon$ is some unit in $\mathcal{O}_K$ such that $\varepsilon \equiv 1 \text{ mod } \pi$. Thus,
\[
\omega(a) = H(a) \cdot \varepsilon_\pi^n = (1 + cH_c(a)) \cdot (1 + c[p^n]_c(c^{-1}(\varepsilon - 1))).
\]

Now, since $\omega_c(a) = c^{-1}(\omega(a) - 1)$, we get
\[
\omega_c(a) = c^{-1}((1 + cH_c(a)) \cdot (1 + c[p^n]_c(c^{-1}(\varepsilon - 1)))) - 1
\]
\[
= H_c(a) + F_c [p^n]_c(c^{-1}(\varepsilon - 1)).
\]

\[\Box\]

Proposition 5. Let $\zeta - 1 = \gamma_0 \pi^{e_0} + \ldots$, where $\gamma_0 \in \mathcal{O}$. Then
\[
\omega_c(a) \equiv H_c(a) \equiv c^{-1}a^\gamma \gamma_0^{p^n} \pi^{pe_1} \mod (\pi^{pe_1+1}, [p^n]_c(F_c(\mathfrak{M}))).
\]

Proof. It is known that
\[
H(a) = E(p^n A\ell(\zeta))|_{X=\pi} \equiv 1 + a^{p^n-1} \gamma_0^{p^n} \pi^{pe_1} \mod \pi^{pe_1+1}
\]
(see [2] p. 121, (14)). Now the definition of $H_c(a)$ directly implies the formula
\[
H_c(a) = c^{-1}(H(a) - 1) \equiv c^{-1}a^{p^n-1} \gamma_0^{p^n} \pi^{pe_1} \mod \pi^{pe_1+1}.
\]
The final result follows from Proposition 4.

\[\Box\]

Proposition 6. The primary element $\omega_c(a) \mod [p^n]_c(F_c(\mathfrak{M}))$ does not depend on the choice of the prime element $\pi$ and the form of the series expansion for the root $\xi$ of the kernel $[p^n]_c(x)$.

Proof. The proof is much similar to that in the multiplicative case (see [3] Chapter V, item 4).

\[\Box\]

§5. Main lemma

First, we prove some preliminary assertions.

Lemma 1. For $\psi \in X\mathcal{O}[[X]]$, the following congruence holds true:
\[
\left( \frac{\Delta}{p} \log(1 + c \psi) \right) / s \equiv \left( \frac{\Delta}{p} \log(1 + p \psi) \right) / s \text{ mod } (p^n, \text{deg } 1).
\]

(9)
Proof. For series $u$ and $s$, we have
\[
\frac{u^r}{rp}/s \equiv \frac{p^{r-1}}{r}/s \mod (p^n, \deg 0), \quad \text{where } r \geq 1
\]
(see [4, proof of Lemma 4]). Multiplying both sides of this congruence by $(-1)^{r-1}(\zeta u)^r$ and summing over $r$, we arrive at (9). □

Lemma 2. For $\psi \in \mathcal{O}[[X]]$, the following congruence holds true:
\[
(10) \quad \log(1 + \zeta w\psi)/s \equiv \frac{1}{p} \log(1 + pg\psi)/s_{n-1} \mod \deg 1.
\]
Proof. We use the congruence $u^r/s \equiv p^{r-1}/s_{n-1} \mod \deg 0$, where $r \geq 1$ (see [4, proof of Lemma 3]). Multiplying by $(-1)^{r-1}(\zeta u)^r$ and summing over $r$, we complete the proof. □

Corollary.
\[
(11) \quad \Delta (\log(1 + \zeta w\psi)/s) \equiv \left(\frac{\Delta}{p} \log(1 + p\zeta\psi)\right)/s \mod (p^n, \deg 1).
\]
Proof. It suffices to apply the operator $\Delta$ to both sides of (10) and to recall that $1/s_{n-1}\equiv 1/s_{n}\mod p^n$ (see [3, Chapter VI, item 3]). □

Lemma 3. For $\psi \in \mathcal{O}[[X]]$, the following congruence holds true:
\[
(12) \quad \frac{\Delta}{p} \log(1 + \zeta w\psi) d(1/s) \equiv 0 \mod (p^n, \deg 0).
\]
Proof. Note that $d(1/s) \equiv 0 \mod p^n$ (see [3, Chapter VI, item 3]). Since the series $(1 - \frac{\Delta}{p}) \log(1 + \zeta w\psi)$ has integral coefficients, we have
\[
\left(1 - \frac{\Delta}{p}\right) \log(1 + \zeta w\psi) d(1/s) \equiv 0 \mod p^n.
\]
Now the claim is equivalent to the following congruence:
\[
(13) \quad \log(1 + \zeta w\psi) d(1/s) \equiv 0 \mod (p^n, \deg 0).
\]
The definition of the series $u$ (see [1, §3]) shows that
\[
u \in p\mathcal{O}[[X]] + X^e\mathcal{O}[[X]] \Rightarrow \zeta w\psi = pa + X^e b, \quad \text{where } a, b \in \mathcal{O}[[X]].
\]
Plugging this in the series for $\log(1 + X)$, we get
\[
(14) \quad \log(1 + \zeta w\psi) = pa_{-1} + a_0 X^e + a_1 \frac{X^e}{p} + a_2 \frac{X^{2e}}{p^2} + a_3 \frac{X^{3e}}{p^3} + \ldots,
\]
where $a_i \in \mathcal{O}[[X]]$. From the definition of $s$ and $\zeta$ and the properties of $\zeta$ (see [2, p. 121]) it follows that
\[
\zeta \in 1 + p\mathcal{O}[[X]] + X^{\varepsilon_0}\mathcal{O}[[X]] \Rightarrow s = pX^{-\varepsilon_0/2}\varepsilon_1(X) + X^{\varepsilon_0}\varepsilon_2(X),
\]
where $\varepsilon_1, \varepsilon_2 \in \mathcal{O}\{\{X\}\}^*$. This identity and the congruence $ds \equiv 0 \mod p^n$ (see [3, Chapter VI, item 3]) imply that
\[
(15) \quad d(1/s) = -ds/s^2 = p^n\left(b_0 X^{-2p^n\varepsilon_0} + b_1 X^{-2p^n\varepsilon_0 - e}p + b_2 X^{-2p^n\varepsilon_0 - 2e} p^2 + \ldots\right),
\]
where $b_i \in \mathcal{O}[[X]]$. The expansions (14) and (15) with the inequality $p^{ne} \geq -2p^n\varepsilon_0 + me$ for $m \geq 1$ prove the desired congruence (13). □

Lemma 4 (main lemma). For $\alpha \in \mathcal{H}_m$ and $\psi \in \mathcal{O}[[X]]$, the following congruence holds true:
\[
\langle \alpha, w\psi\rangle_c \equiv (1 - \Delta)d_0 \mod p^n, \quad \text{where } d_0 \in \mathcal{O}.
\]
Proposition 7. The elements 
\[ (\pi, \varepsilon_{i, \theta})_c = 0, \quad (\pi, \omega_c(a)) = [\text{tr} a]_c(\xi). \]

\[ \varepsilon_{i, \theta} = \theta c^{p^n-1} \pi^i, \quad \text{where } \theta \in \mathcal{R}, \quad p \nmid i, \quad \text{and} \quad \omega_c(a) \text{ with } a \in \mathcal{O} \]
Proof. The first part of the proposition is a simple generalization of the Hensel theorem (see [7, 2]) to the formal $\mathbb{Z}_p$-module $F_c(\mathfrak{M})$, with regard to the congruence (8).

Now we check the relation $(\pi, \varepsilon_i, \theta) = 0$. Indeed, Lemma 5 shows that

$$0 = (\theta \pi^i, c \theta^{-1}(\theta \pi^i)) = (\theta, c \theta^{-1}(\theta \pi^i)) + F_c [i]_c (\pi, c \theta^{-1}(\theta \pi^i)) = [i]_c (\pi, c \theta^{-1}(\theta \pi^i)),$$

because $\theta$ is a $p$-divisible element of the Teichmüller set $\mathfrak{R}$. Therefore, $(\pi, c \theta^{-1}(\theta \pi^i)) = 0$ whenever $p \mid i$. The second relation $(\pi, \omega_c(a)) = [\text{tr} a]_c (\xi)$ is proved in the corollary to Theorem 1 and Proposition 4.

**Proposition 8.** Let $\alpha \in \mathcal{H}_m$, $a \in \mathcal{O}$. Then

$$\langle \alpha, E_c(as_c(X)) \rangle_c \equiv \deg \alpha \cdot a \mod p^n.$$

**Proof.** First, we consider the case where $\alpha(X) = X$. By definition, we have

$$\langle X, E_c(as_c(X)) \rangle_c = \text{res}_X \ell_c (E_c(as_c(X))) X^{-1} \, dX/s_c = \text{res}_X as_c X^{-1}/s_c = a.$$

Since the pairing $\langle \cdot, \cdot \rangle_c$ is multiplicative in the first argument, it suffices to prove that for $\varepsilon(X) \in \mathcal{O}[[X]]^*$ we have

$$\langle \varepsilon(X), E_c(as_c(X)) \rangle_c = 0.$$  \hfill (18)

Using the definition, we get

$$\Phi(\varepsilon(X), E_c(as_c(X)))/s_c = a \varepsilon(X)^{-1} \, d\varepsilon(X) - \ell(\varepsilon(X)) \, d \frac{\Lambda}{p} \log (1 + \varepsilon E_c(as_c(X)))/s.$$

Trivially, we have $\varepsilon(X)^{-1} \, d\varepsilon(X) \in \mathcal{O}[[X]]$, so that the residue of this element is zero. Consider the second summand:

$$\ell(\varepsilon(X)) \, d \frac{\Lambda}{p} \log (1 + \varepsilon E_c(as_c(X)))/s = \ell(\varepsilon) \, d \frac{\Lambda}{p} \log (E(as))/s$$

$$= \ell(\varepsilon) \cdot (1/s) \, d \sum_{m \geq 1} \frac{(as)^n}{p^m} \equiv \ell(\varepsilon) \cdot (1/s) \cdot X^{-1} (X a \, ds)^n \equiv 0 \mod p^n.$$

The last congruence is valid because $ds \equiv 0 \mod p^n$ and all other factors have integral coefficients. This proves formula (18) and the lemma.

§7. Pairing over the formal module $F_c(\mathfrak{M})$

Now we introduce the pairing $\langle \cdot, \cdot \rangle_c$ on numbers by using the pairing $\langle \cdot, \cdot \rangle_c$ on series.

**Definition 1.** Let

$$\{\cdot, \cdot\}_c : K^* \times F_c(\mathfrak{M}) \to (\xi),$$

$$\{\alpha, \beta\}_c = [\text{tr}(\alpha, \beta)]_c (\xi),$$

where $\alpha \in \mathcal{H}_m$ and $\beta \in \mathcal{H}_c$ are such that $\alpha(\pi) = \alpha$, $\beta(\pi) = \beta$.

In the following lemmas we check the consistency of this definition, i.e., the independence of the choice of the series $\alpha$ and $\beta$.

**Lemma 6.** Let series $\beta_1, \beta_2 \in \mathcal{H}_c$ be such that $\beta_1(\pi) = \beta_2(\pi)$. Then for any series $\alpha \in \mathcal{H}_m$ we have

$$[\text{tr}(\alpha, \beta_1)]_c (\xi) = [\text{tr}(\alpha, \beta_2)]_c (\xi).$$
Proof. Consider the series $\beta = \beta_1 - F, \beta_2$. By assumption, $\beta(\pi) = 0$. Hence (see \cite{11} Lemma 6), $\beta = \psi$ for some series $\psi \in \mathcal{O}[[X]]$. The main lemma (Lemma 4) implies that

$$\langle \alpha, \beta \rangle_c = 0 \Rightarrow [\text{tr} \langle \alpha, \beta \rangle_c] (\xi) = 0.$$  

Hence, by the linearity of the pairing $\langle \cdot, \cdot \rangle_c$, we get the claim. \qed

Lemma 7 (change of variables). Let $g(Y) \in \mathcal{O}[[Y]]$ be such that $\deg g = 1$, and let $g(\pi) = \pi'$ be the uniformizing parameter of $\mathcal{O}_K$. Then for any $\alpha \in \mathcal{H}_m$ and $\beta \in \mathcal{H}_c$ we have

$$\langle \alpha(X), \beta(X) \rangle_{c, X, \pi} = \langle \alpha(g(Y)), \beta(g(Y)) \rangle_{c, Y, \pi'}.$$

In the pairing on the right-hand side the series and residue are regarded with respect to the variable $Y$, and the corresponding series $s'_m$ and $u'$ are constructed with the help of expansions of $\xi, \zeta$, and $c$ in $\pi'$-series (for the prime element $\pi'$).

Proof. We denote by $c$ the $\pi'$-series expansions of the element $c$.

First, we consider the case where $\alpha(X) = X$. By Lemma 6 and Proposition 7, we may replace the series $\beta$ by the formal sum of the series $\theta \pi^{p-1} X^i$ and $E_c(\alpha c(X))$. By the linearity of pairings, it suffices to check that

$$\langle X, \theta \pi^{p-1} X^i \rangle_{c, X, \pi} = \langle g(Y), \theta \pi^{p-1} g(Y)^i \rangle_{c, Y, \pi'}, \quad \text{where } p \nmid i,$$

$$\langle X, E_c(\alpha c(X)) \rangle_{c, X, \pi} = \langle g(Y), E_c(\alpha c(Y)) \rangle_{c, Y, \pi'}.$$

The first congruence follows immediately from the Steinberg relation (Proposition 8), and the second from Proposition 8.

Now we address the case of $\alpha(X) = \varepsilon(X) \in \mathcal{O}[[X]]^*$. It suffices to check only this case, by multiplicativity in the first argument. We need to prove that

$$\langle \varepsilon(X), \beta(X) \rangle_{c, X, \pi} = \langle \varepsilon(g(Y)), \beta(g(Y)) \rangle_{c, Y, \pi'}.$$

Denoting $f(X) = X \varepsilon(X), \pi'' = f(\pi), Z = f(X)$, and $h(Y) = f(g(Y))$, we write

$$\langle \varepsilon(X), \beta(X) \rangle_{c, X, \pi} = \langle f(X), \beta(X) \rangle_{c, X, \pi} - \langle X, \beta(X) \rangle_{c, X, \pi},$$

$$\langle \varepsilon(g(Y)), \beta(g(Y)) \rangle_{c, Y, \pi'} = \langle f(g(Y)), \beta(g(Y)) \rangle_{c, Y, \pi'} - \langle g(Y), \beta(g(Y)) \rangle_{c, Y, \pi'}.$$

It suffices to prove that

$$\langle f(X), \beta(X) \rangle_{c, X, \pi} = \langle f(g(Y)), \beta(g(Y)) \rangle_{c, Y, \pi'}.$$

The case considered above shows that

$$\langle f(X), \beta(X) \rangle_{c, X, \pi} = \langle Z, \beta(f^{-1}(Z)) \rangle_{c, Z, \pi''} = \langle h(Y), \beta(f^{-1}(h(Y))) \rangle_{c, Y, \pi'} = \langle f(g(Y)), \beta(g(Y)) \rangle_{c, Y, \pi'}.$$

The lemma is proved. \qed

Lemma 8. Let series $\alpha_1, \alpha_2 \in \mathcal{H}_m$ be such that $\alpha_1(\pi) = \alpha_2(\pi)$. Then for any series $\beta \in \mathcal{H}_c$ we have

$$[\text{tr} \langle \alpha_1, \beta \rangle_c] (\xi) = [\text{tr} \langle \alpha_2, \beta \rangle_c] (\xi).$$

Proof. By multiplicativity, it suffices to prove that

$$\langle \alpha_1/\alpha_2, \beta \rangle_c = 0.$$

Consider the series $g(X) = X \cdot (\alpha_1(X)/\alpha_2(X))$; since $g(\pi) = \pi$, Lemmas 6 and 7 show that

$$\langle X, \beta(X) \rangle_c = \langle g(X), \beta(g(X)) \rangle_c = \langle g(X), \beta(X) \rangle_c = \langle X \cdot (\alpha_1(X)/\alpha_2(X)), \beta(X) \rangle_c,$$

which immediately implies the claim. \qed
We unite and reshape these results as follows.

**Theorem 2.** The pairing \( \{ \cdot, \cdot \}_c \) is well defined, i.e., it does not depend of the choice of a uniformizing element \( \pi \in \mathcal{O}_K \) and the way of expansion of elements \( \alpha \in K^* \) and \( \beta \in F_c(\mathfrak{M}) \) in the \( \pi \)-series \( \alpha \in \mathcal{H}_m \) and \( \beta \in \mathcal{H}_c \). It is multiplicative in the first argument and linear in the second; moreover, it satisfies the Steinberg relation
\[
\{ \alpha, e^{\pi n} - 1 \alpha \}_c = 0, \quad \text{where} \quad \alpha \in F_c(\mathfrak{M}) \setminus \{0\}.
\]

\[\text{§8. Hilbert pairing}\]

**Theorem 3.** For any elements \( \alpha \in K^* \) and \( \beta \in F_c(\mathfrak{M}) \), the values of the pairings \( \{ \cdot, \cdot \}_c \) and \( (\cdot, \cdot)_c \) are equal:
\[
\{ \alpha, \beta \}_c = (\alpha, \beta)_c.
\]

**Proof.** First, we consider case of prime \( \alpha = \pi \). Expand \( \beta \) in Hensel generators. By linearity of the pairings with respect to the second argument, it suffices to prove the theorem in the cases where \( \beta = \varepsilon_i \theta, \beta = \omega_c(a) \) (see Proposition 7). The Steinberg relations immediately imply (see the proof of Proposition 7) that
\[
\{ \pi, \varepsilon_i \theta \}_c = (\pi, \varepsilon_i \theta)_c = 0.
\]

Propositions 7 and 8 also show that
\[
\{ \pi, \omega_c(a) \}_c = (\pi, \omega_c(a))_c = [\text{tr } a](\xi).
\]

The case of prime \( \alpha \) is proved. Now, an arbitrary unit of the field \( \varepsilon \in \mathcal{O}_K \) can be rewritten in the form \( \varepsilon = \tau/\pi \), where \( \tau \) and \( \pi \) are prime elements. Then
\[
\{ \varepsilon, \beta \}_c = \{ \tau, \beta \}_c - F_c \{ \pi, \beta \}_c = (\tau, \beta)_c - F_c (\pi, \beta)_c = (\varepsilon, \beta)_c.
\]

By multiplicativity in the first argument, we get the desired claim for arbitrary \( \alpha \in K^* \).

Thus, we have obtained an explicit formula for the symbol \( (\cdot, \cdot)_c \).

**References**


Mathematics and Mechanics Department, St. Petersburg State University, Universitetskii pr. 28, Petrodvorets, St. Petersburg 198504, Russia

E-mail address: sergei.vostokov@gmail.com

Mathematics and Mechanics Department, St. Petersburg State University, Universitetskii pr. 28, Petrodvorets, St. Petersburg 198504, Russia

E-mail address: vladvolkov239@gmail.com

Received 10/JAN/2014

Translated by V. VOLKOV