THE PRODUCT OF SYMBOLS OF $p^n$TH POWER RESIDUES AS AN ABELIAN INTEGRAL

M. A. IVANOV

Abstract. In accordance with the Hilbert–Shafarevich ideology, the reciprocity law must be an analog of an integral theorem asserting that the Abelian integral of a differential form on a Riemann surface is equal to the sum of residues at singular points. In the present paper, it is shown that the product of the symbols of $p^n$th power residues is the integral of a certain function.

Introduction

The idea about an analogy between numbers and functions was conceived long ago, but it was most clearly stated by Leopold Kronecker who suggested that the prime ideals play the same role as the points of a Riemann surface in fields of algebraic functions, that prime divisors of the discriminant of a number field correspond to ramification points of a Riemann surface, and so on. David Hilbert was actually the first to study this idea in number fields, drawing analogy of his reciprocity law for the product of norm residue symbols and the Cauchy integral theorem (see [2, pp. 367–368]). Igor Shafarevich continued this line of investigation; from this point of view he studied the local norm residue symbol $\left( \frac{\alpha,\beta}{\wp} \right)$ as an analog of the Abelian differential $\alpha d\beta$ at the point $\wp$ (see [4]). In the paper [7], the classical reciprocity law for the product of power residue symbols in a cyclotomic field was examined as the product of finitely many local symbols of norm residues. In accordance with the ideology due to Hilbert and Shafarevich, this reciprocity law must be an analog of an integral theorem asserting that the Abelian integral of a differential form on a Riemann surface is equal to the sum of the residues of this form at singular points.

In the paper [7] it was shown that the right-hand side of the reciprocity law is a full analog of the sum of the residues of a function at singular points that are roots of unity. In the present paper, we show that the product of the symbols of $p^n$th power residues is the integral of a certain function. More precisely, let $K$ be a cyclotomic field of $p^n$th powers, $\zeta$ a primitive root of of unity of degree $p^n$, and $\pi = \zeta - 1$ a uniformizer. Then in our case the corresponding reciprocity law takes the form

\[
\left( \frac{\alpha}{\beta} \right) p^n \left( \frac{\beta}{\alpha} \right)^{-1} p^n = \left( \frac{\alpha,\beta}{\pi} \right).
\]

By the explicit Vostokov’s formula (see [5] or [2]), the right-hand side of (1) has the form

\[
\zeta^{\text{res}}_{\frac{\Phi_{\alpha}(X),\beta(X)}{\zeta(X)^{p^n} - 1}},
\]

2010 Mathematics Subject Classification. Primary 11A15.
Key words and phrases. Power residue symbol, Shnirel’man’s integral.
Supported by RFBR (grant no. 11-01-00588-a).

©2013 American Mathematical Society
where $\Phi$ is a certain function of $\alpha$ and $\beta$, calculated in explicit form, and $\zeta$ is a polynomial that becomes equal to $\zeta$ when the uniformizer is substituted in it. We show that the left-hand side of relation (1), i.e., the product of symbols of power residues, is the Shnirelman integral (see [3]) of the form

$$
\zeta \int_{0}^{\pi} \Phi(\alpha, \beta) \zeta pn - 1,
$$

where the inversion of $\zeta p n - 1$ occurs in the two-dimensional local ring, i.e., there exists a natural $k$ and a polynomial $V(X)$ such that

$$
V(X) X k \equiv p n 1 \zeta(X) pn - 1.
$$

Next, we verify that for the Eisenstein reciprocity law, such an integral can easily be computed.

§1. The Shnirelman integral and its properties

Let $p$ be a prime number and $k$ a local field of characteristic 0 (a finite extension of $\mathbb{Q}_p$); let $|\cdot|_p$ be the norm on $k$ and $r$ a nonzero element of $k$.

**Definition 1.** A sequence of polynomials $g_1(X), g_2(X), \ldots$ in $\mathbb{Z}[X]$ is said to be admissible if the following conditions are satisfied:

1. the $g_j(X)$ have no multiple roots;
2. if $g_j(X) = X^{n_j} + c_{j,1}X^{n_j-1} + \ldots + c_{j,\mu}X^{n_j-\mu} + c_0$, then $|n_j|_p = 1$, $|c_0|_p = 1$, and $n_j - n_{j,1} \to \infty$, $n_{j,\mu} \to \infty$.

We denote the roots of $g_j$ by $\alpha_1, \alpha_2, \ldots, \alpha_{n_j}$.

**Definition 2.** Let $U$ be a subset of $\mathbb{Q}_p^{alg}$, let $f(x) : U \to \mathbb{Q}_p^{alg}$, and let $g_j$ be an admissible sequence. The Shnirelman integral with center $x_0$ and radius $r$ is defined as

$$
\int_{x_0, r, g} f(x) = \lim_{j \to \infty} \sum_{g_j(\alpha_i) = 0} \frac{r \alpha_i}{n_j} f(x_0 + r \alpha_i),
$$

provided the values of $f(x)$ are well defined at the points $x_0 + r \alpha_i$ and the limit exists.

This definition is a discrete analog of the contour integral

$$
\int_{g(\frac{x}{r} - n_0)} f(z) dz.
$$

For this reason, it is natural to call the sequence $g_j$ the “contour” over which the integration proceeds.

Our aim in this section is to prove the following two statements.

**Proposition 1.** Let $P(X) \in k[[X]]$ be a power series convergent in the disk of radius $|r|_p$, and let $Q(X) \in k[[X]]$ be a polynomial that has no roots the norm of which is equal to $|r|_p$. Then the value of $\int_{x_0, r, g} \frac{P(x)}{Q(x)}$ does not depend on the choice of the sequence of polynomials $g_j$.

**Proposition 2.** Let $P(X) \in k[[X]]$ be a power series convergent in the disk of radius $|r|_p$, and let $Q(X) \in k[[X]]$ be a polynomial that has no roots the norm of which is equal to $|r|_p$. Then $\int_{x_0, r, g} \frac{P(x)}{Q(x)}$ is equal to the sum of residues of the function $\frac{P(x)}{Q(x)}$ over all poles inside the circle of radius $|r|_p$.

**Proof.** We may assume that $x_0 = 0$, because, obviously, the general case can be obtained from this one by parallel translation.
1. Let \( f(X) \in k[X] \) be a polynomial. Then
\[
\int_{0, r, g} f(x) = \lim_{j \to \infty} \sum_{\alpha_i=0}^r \frac{r\alpha_i}{g_j(\alpha_i)} f(r\alpha_i).
\]
The expression under the limit sign is a symmetric polynomial with respect to \( \alpha_1, \alpha_2, \ldots, \alpha_n \). Therefore, it can be expressed in terms of the basic symmetric polynomials with coefficients depending only on the coefficients of the polynomials \( f(X) \) and \( g_j(X) \) and on \( r \); this leads to the expression
\[
\lim_{j \to \infty} \left( \left( \sum \alpha_i \right) P_1 + \left( \sum \alpha_i \alpha_i \right) P_2 + \ldots + \left( \sum \alpha_i \alpha_i \ldots \alpha_i \right) P_k \right),
\]
where \( k = \deg f + 1 \). But this expression is equal to 0, because, by the definition of \( g_j \), all these symmetric polynomials are equal to 0 beginning with a certain place (when \( n_j - n_{j, 1} > k \)).

2. Let \( f(X) = \frac{P(X)}{X^n} \), where \( P(X) \in k[X] \) and \( |a|_p < |r|_p \), i.e., \( a \) “lies inside the contour”. Consider the identity
\[
\frac{1}{n_j} \sum_{i=1}^{n_j} \frac{1}{a - \alpha_i} = \frac{1}{g_j(\frac{a}{r})} \cdot \frac{g_j(\frac{a}{r})}{g_j(\frac{a}{r})} = 1,
\]
and this tends to zero in the norm \( \cdot \), because \( n_j, \mu \to \infty \) and \( \frac{a}{r} \to 0 \). Then
\[
\int_{0, r, g} \frac{1}{x - a} = \lim_{j \to \infty} \sum_{\alpha_i=0}^r \frac{\alpha_i}{g_j(\alpha_i)} = \lim_{j \to \infty} \sum_{\alpha_i=0}^r \frac{\alpha_i}{g_j(\alpha_i)} = \frac{1}{n_j} \sum_{\alpha_i=0}^r \left( \frac{a}{\alpha_i - a} \right).
\]
Now, representing \( P(X) \) in the form
\[
P(X) = P(a) + q(X)(X - a)
\]
and applying the Bézout theorem, we obtain
\[
\int_{0, r, g} \frac{P(x)}{x - a} = \int_{0, r, g} \left( \frac{P(a)}{x - a} + q(x) \right) = P(a) \int_{0, r, g} \frac{1}{x - a} = P(a) = \text{res}_a f(x).
\]
In the case where \( |a|_p > |r|_p \), i.e., when \( a \) “lies outside the contour”, the expression (1) has the limit \( \frac{1}{(\frac{a}{r})} \), whence the expression in (2) is equal to 0. The integral \( \int_{0, r, g} \frac{P(x)}{x - a} \) is equal to 0.

3. By analogy with the usual complex integral, it can be proved that the formula
\[
\int_{x_0, r, g} h(x) \frac{h(x)}{(x - a)} = h(a)
\]
implies that
\[
\int_{x_0, r, g} h(x) \frac{h(x)}{(x - a)^n} = \frac{1}{(n - 1)!} h^{(n-1)}(a).
\]
For \( f(X) = \frac{P(X)}{(X-a)^n} \), where \( P(X) \in k[X] \) and \( |a|_p < |r|_p \), this yields the relation
\[
\int_{0,r,g} \frac{P(x)}{(x-a)^n} = \frac{1}{(n-1)!} P^{(n-1)}(a) = \text{res}_a f(x).
\]

4. Now, let \( f(X) = \frac{P(X)}{(X-c)^n} \), where \( P(X) \in k[[X]] \) and \( |a|_p < |r|_p \). Let \( P_m(X) \in k[X] \) be a polynomial obtained from the series \( P(X) \) by cutting at a certain place, so that \( P_m(x) = \frac{P(x)}{(x-a)^n} \) for \( |x|_p = |r|_p \). Then from the above we have
\[
\int_{0,r,g} \frac{P(x)}{(x-a)^n} = \frac{1}{(n-1)!} P^{(n-1)}(a) = \frac{1}{(n-1)!} P^{(n-1)}(a) = \text{res}_a f(x).
\]

Letting \( m \) tend to infinity, we obtain the required relation.

It is easily seen that if \( |a|_p > |r|_p \), then
\[
\int_{0,r,g} f(x) = 0
\]
in items 3 and 4.

5. Now let \( f(X) = \frac{Q(X)}{Q(X)} \), where \( Q(X) \) is an arbitrary polynomial. It expands in \( \mathbb{Q}_p^{alg} \) into linear factors. We reduce this case to the preceding item, i.e., to the case where the denominator has one root. For simplicity of computations, we assume that the denominator has two roots, i.e., \( Q(X) = (X-a)^n(X-b)^m \). Then there exist polynomials \( q(X) \) and \( s(X) \) such that \( (X-a)^n q(X) + (X-b)^m s(X) = 1 \). Then
\[
\int_{0,r,g} \frac{P(x)}{(x-b)^m} = \int_{0,r,g} \frac{P(x) q(x)(x-b)^m}{(x-a)^n(x-b)^m} + \int_{0,r,g} \frac{P(x) s(x)}{(x-a)^n}.
\]

If \( b \) lies outside the contour, then \( \int_{0,r,g} \frac{P(x) q(x)}{(x-b)^m} = 0 \), and if it lies inside the contour, we have
\[
\int_{0,r,g} \frac{P(x) q(x)}{(x-b)^m} = \text{res}_b \frac{P(x) q(x)}{(x-b)^m} = \text{res}_b \frac{P(x) (1-s(x)(x-b)^m)}{(x-b)^m} = \text{res}_b \frac{P(x)}{(x-a)^n(x-b)^m} = \text{res}_b \frac{P(x)}{(x-a)^n(x-b)^m} = \text{res}_b \frac{P(x)}{(x-a)^n(x-b)^m}.
\]

The second term in (3) is computed similarly. Thus, the claim is proved. \( \Box \)

In the sequel we omit the subscript \( g \) in the integral and assume that the sequence of polynomials (“contour”) is \( g_j = X^{n_j} - 1, (n_j, p) = 1 \).

§2. The main theorem

2.1. An explicit formula for the norm residue symbol.

We use the following notation:
\* \( K = \mathbb{Q}_p(\zeta_p^n) \) is a cyclotomic field with residue field of odd characteristic \( p \);
• $\pi$ is a prime element in $K$;
• $\mu_{p^n}$ is a group of roots of $1$;
• $\triangle$ is the Frobenius automorphism in $\mathbb{Q}_p$;
• $\overline{\alpha}(X) \in \mathbb{Z}_p((X))^*$ is such that $\overline{\alpha}(\pi) = \alpha$; $\overline{\beta}(X)$ and $\zeta(X)$ are defined similarly;
• $d = \frac{d}{dX}$.

Defining the action of the operator $\triangle$ on $\mathbb{Z}_p((X))$ as

$$\triangle \left( \sum a_i X^i \right) = \left( \sum a_i X^i \right) \triangle = \sum a_i \triangle X^i,$$

we construct the Artin–Hasse logarithm

$$\ell_m(\varphi) = \frac{1}{p} \log \left( \frac{\varphi^p}{\varphi \triangle} \right)$$

for any $\varphi(X) \in \mathbb{Z}_p((X))^*$. If $\varphi(X) \in 1 + X\mathbb{Z}_p[[X]]$, then this definition takes the more familiar form

$$\ell_m(\varphi) = \left( 1 - \frac{\triangle}{p} \right) \log(\varphi).$$

Now we can define the pairing

$$K^* \times K^* \to \mu_{p^n},$$

$$\langle \alpha, \beta \rangle = \zeta_{p^n} \frac{\Phi(\alpha, \beta)}{\zeta_{p^n} - 1},$$

where

$$\Phi(\alpha, \beta) = \ell_m(\beta) d(\ell_m(\alpha)) - \ell_m(\beta) \overline{\alpha}^{-1} d\overline{\alpha} - \ell_m(\alpha) \overline{\beta}^{-1} d\overline{\beta},$$

and the inversion in (4) is taken in the two-dimensional local ring $\mathbb{Z}_p\{\{X\}\}$, i.e.,

$$\left( \zeta_{p^n} - 1 \right)^{-1} = z^{-p^n} \left( 1 + \sum_{i=1}^{p^n-1} C_{p^n}^i z^{-i} \right)^{-1},$$

here we have denoted $z(X) = \zeta(X) - 1$ (for the details, see [5] §3 or [6, p. 208]); finally, res denotes the residue at the point 0.

In the paper we use the same notation for the pairing $\langle \alpha, \beta \rangle = \left( \frac{\Phi(\alpha, \beta)}{\zeta_{p^n} - 1} \right) \mod p^n$.

2.2. The main theorem. Our aim in this section is to represent the ratio of power residue symbols in a new form. In our case the reciprocity law, which was first proved by Hasse (see [11, p. 58]), has the form

$$\left( \frac{\alpha}{\beta} \right)_{p^n} \left( \frac{\beta}{\alpha} \right)^{-1}_{p^n} = \left( \frac{\alpha, \beta}{(\pi)} \right)_{p^n}.$$

This reduces the problem to studying the norm residue symbol, for which Vostokov obtained the explicit formula (see [5] or [6])

$$\left( \frac{\alpha, \beta}{(\pi)} \right)_{p^n} = \zeta^{\operatorname{res} \frac{\Phi(\alpha, \beta)}{\zeta_{p^n} - 1}},$$

in the notation of the previous section.

Now we can prove the main theorem.

**Theorem 1.** In the above notation, the following relation holds true:

$$\left( \frac{\alpha}{\beta} \right)_{p^n} \left( \frac{\beta}{\alpha} \right)^{-1}_{p^n} = \zeta_{0, \pi} \frac{\Phi(\alpha, \beta)}{\zeta_{p^n} - 1} = \zeta^{\operatorname{res} \frac{\Phi(\alpha, \beta)}{\zeta_{p^n} - 1}} = \left( \frac{\alpha, \beta}{(\pi)} \right)_{p^n},$$

where the division in the integral is in the two-dimensional local ring $\mathbb{Z}_p\{\{X\}\}.$
Proof. Using Proposition 2 about the properties of the Shnirelman integral, we obtain
\[
\int_{0, \pi} \Phi(\alpha, \beta) \frac{\zeta_{p^n} - 1}{\zeta_{p^n} - 1} = \text{res}_0 \frac{\Phi(\alpha, \beta)}{\zeta_{p^n} - 1} = \text{res}_0 \Phi(\alpha, \beta).
\]
Now, combining the said above, we get
\[
\left( \frac{\alpha}{\beta} \right)^{p^n} \left( \frac{\beta}{\alpha} \right)^{p^n} = \left( \frac{\alpha}{\beta} \right)^{p^n} \left( \frac{\beta}{\alpha} \right)^{p^n} = \zeta \text{res}_0 \frac{\Phi(\alpha, \beta)}{\zeta_{p^n} - 1} = \zeta \int_{0, \pi} \Phi(\alpha, \beta).
\]

§3. The Eisenstein reciprocity law

The classical Eisenstein reciprocity law yields conditions for equality of power residues in a cyclotomic field, provided that one of the arguments lies in the ground field. In the present paper, we want to prove this reciprocity law on the basis of the result obtained above.

Theorem 2. Let \( K = \mathbb{Q}_p(\zeta_{p^n}) \). Then
\[
\left( \frac{a}{\beta} \right)^{p^n} \left( \frac{\beta}{a} \right)^{p^n} = 1 \quad \forall \beta \iff \frac{a^{p-1} - 1}{p} \equiv 0 \mod p^n.
\]
for \( a \in \mathbb{Z}_p^* \).

Proof.

Lemma 1. Let \( a \in \mathbb{Z}_p^* \). Then the Artin–Hasse logarithm \( \ell_m(a) \) can be represented in the form
\[
\frac{a^{p-1} - 1}{p} t
\]
for some \( t \); moreover, \( t \equiv 1 \mod p \).

Proof of Lemma. Since \( \frac{a^{p-1} - 1}{p} \in \mathbb{Z}_p \), we have
\[
\ell_m(a) = \frac{1}{p} \log \left( \frac{a^p}{a^a} \right) = \frac{1}{p} \log(a^{p-1}) = \frac{1}{p} \log \left( 1 + \frac{a^{p-1} - 1}{p} \right) = \frac{a^{p-1} - 1}{p} \left( 1 - \frac{1}{2} \frac{a^{p-1} - 1}{p} + \frac{1}{3} \left( \frac{a^{p-1} - 1}{p} \right)^2 - \ldots \right) \equiv \frac{a^{p-1} - 1}{p} t.
\]

As a prime element in \( \mathbb{Q}_p \), we take \( \pi = \zeta_{p^n} - 1 \). Theorem 1 implies that Theorem 2 is equivalent to the following assertion:
\[
\int_{0, \pi} \Phi(\alpha, \beta) \frac{\zeta_{p^n} - 1}{\zeta_{p^n} - 1} \equiv 0 \quad \forall \beta \iff \frac{a^{p-1} - 1}{p} \equiv 0 \mod p^n.
\]

Substituting the formula for \( \Phi \) (see (5)) and using the fact that \( a \) lies in the ground field (i.e., \( g(X) = a \)), we obtain
\[
\int_{0, \pi} \Phi(\alpha, \beta) \frac{\zeta_{p^n} - 1}{\zeta_{p^n} - 1} = \ell_m(a) \int_{0, \pi} \frac{\ell_{m}(\alpha)^{1-\delta}}{\zeta_{p^n} - 1} = \ell_m(a) \int_{0, \pi} \frac{\beta^{1-\delta}}{\zeta_{p^n} - 1}.
\]
It remains to find \( \beta \) such that
\[
\int_{0, \pi} \frac{\beta^{1-\delta}}{\zeta_{p^n} - 1} \not\equiv 0 \mod p.
\]
Since $\zeta_{p^n} = 1 + \pi$, we have $\zeta = 1 + X$, and then $\frac{1}{\zeta^{p^n} - 1} \equiv \frac{1}{X^{p^n}}$. Now, taking $\beta = 1 - \pi$, we get
\[
\int_{0,\pi} \frac{\beta^{-1} d\beta}{\zeta^{p^n} - 1} \equiv -\int_{0,\pi} \frac{1 + X + X^2 + X^3 + \ldots}{X^{p^n}} = -1.
\]
Thus, using the lemma, we finally have
\[
\int_{0,\pi} \Phi(a, \beta)^{p^n} \equiv 0 \quad \forall \beta \iff \ell_m(\alpha) \equiv 0 \Leftrightarrow \frac{a^{p-1} - 1}{p} \equiv 0 \pmod{p^n},
\]
which completes the proof. \hfill \Box

References


Department of Mathematics and Mechanics, St. Petersburg State University, Petrodvorets, St. Petersburg 198904, Russia

E-mail address: micliva@gmail.com

Received 25/MAR/2011

Translated by N. B. LEBEDINSKAYA