Product of p^n-power residues as an abelian integral*

S. V. Vostokov, M. A. Ivanov

June 13, 2010

Introduction

It was Leopold Kronecker who first understood that there is a deep relationship between algebraic numbers and algebraic functions. He stated that the prime ideals in the fields of algebraic functions play the same role as the points of Riemann surfaces, and that prime divisors of the discriminant of a number field correspond to the ramification points of a Riemann surface, etc. David Hilbert was the first who began investigate this idea in the fields of algebraic numbers. He noticed that his reciprocity law for the product of norm residue symbols, is an analog of Cauchy's integral theorem (see [2, p. 367–368]). Igor Shafarevich continued this investigation and studied from this point of view the local norm residue symbol $\left(\dfrac{\alpha, \beta}{\wp}\right)$ as an analog of the abelian differential $\alpha d\beta$ at the point $\wp$ (see [4, p. 114]). In the paper [7] we considered the classical reciprocity law for power residues in the cyclotomic field as a finite product of the local norm residue symbols. This reciprocity law, in the Gilbert–Shafarevich concept, should be an analog of the integral theorem stating that an abelian integral of a differential form on a Riemann surface is equal to the sum of residues of this form at the singular points.

It was shown in the paper [7] that the right-hand side of the reciprocity law is an analog of the sum of the function's residues in the singular points, which are roots of unity in our case. In the present paper we show that the product of the p^nth power residues is an integral of some function. More precisely, we consider cyclotomic field p^nth power. Let ζ be a primitive p^nth root of 1, and $\pi = \zeta - 1$ be a uniformizing element. Then the corresponding reciprocity law takes the form

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

According to Vostokov's explicit formula (see [5] or [6]), the r.h.s. of this equality becomes

$$\zeta^{\operatorname{res} \frac{\Phi(\underline{\alpha}(X), \underline{\beta}(X))}{\underline{\zeta}(X)^{p^n} - 1}},$$

where Φ is a function of α and β, which can be obtained in the explicit form, and $\underline{\zeta}$ is a polynomial such that $\underline{\zeta}(\pi) = \zeta$. We show that the left-hand side of (1), i. e. the product of power residue symbols, is Schnirelmann's integral (see [3]):

$$\zeta^{\int_{0,\pi} \frac{\Phi(\underline{\alpha}, \underline{\beta})}{\underline{\zeta}^{p^n} - 1}}$$

*Supported by Max-Planck-Institut für Mathematik

where the inverse of $\underline{\zeta}^{p^n} - 1$ is taken in the two dimension local ring, i. e. there exists integer number k and the polynomial $V(X)$ such that $\frac{V(X)}{X^k} \underset{p^n}{\equiv} \frac{1}{\underline{\zeta}(X)^{p^n}-1}$.

Finally we prove that this integral is simply calculated for Eisenstein's reciprocity law.

1 The Schnirelmann integral and its properties

Let p be a prime number and k be a local field of characteristic 0 (i.e. the finite extension of $\mathbb{Q}_p$).

Definition 1. *A polynomial sequence $g_1(X)$, $g_2(X)$, ... from $\mathbb{Z}[X]$ is called **permitted** if the following conditions hold:*

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

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

Definition 2. *Let U be a subset of $\overline{\mathbb{Q}_p^{alg}}$, $f(x) : U \to \overline{\mathbb{Q}_p^{alg}}$ and g_j be a permitted sequence. Define **the Schnirelmann integral** with the center x_0 and the radius r as*

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

if the function $f(x)$ is defined in the points $x_0 + r\alpha_i$, and the limit exists. This definition is the discrete analog of the contour integral

$$\oint_{g(\frac{z-z_0}{r})=0} f(z)dz.$$

Thus it is natural to say that the sequence g_j is the integration "contour".

The aim of this section is to prove the following proposition:

Proposition 1. *Suppose $P(X)$ is a power series which converges in the circle of the radius $|r|_p$, and $Q(X)$ is a polynomial which has no roots whose norm is $|r|_p$. Then $\int_{x_0,r,g} \frac{P(x)}{Q(x)}$ does not depend on the choice of the sequence g_j.*

Proposition 2. *Suppose $P(X)$ is a power series which converges in the circle of the radius $|r|_p$, and $Q(X)$ is a polynomial which has no roots whose norm is $|r|_p$. Then $\int_{x_0,r,g} \frac{P(x)}{Q(x)}$ is equal to the sum of the residues of $\frac{P(x)}{Q(x)}$ at the singular points in the circle of the radius $|r|_p$.*

Proof. Note that we can set $x_0 = 0$, since the general case can be obtained from this one by the parallel translation.

1. Let $f(X) \in k[X]$ be a polynomial. Then

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

This expression is a symmetric polynomial of $\alpha_1, \alpha_2, \ldots, \alpha_{n_j}$. Thus, it can be expressed via basic symmetric polynomials with coefficients which depend only on the coefficients of the polynomials $f(X)$, $g_j(X)$ and on r:

$$\lim_{j\to\infty}\Big((\sum \alpha_i)P_1 + (\sum \alpha_{i_1}\alpha_{i_2})P_2 + \cdots + (\sum \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k})P_k \Big),$$

where $k = degf + 1$. Hence, this expression is 0, since according to the definition of g_j all these symmetric polynomials are equal to 0 starting from some j (when $n_j - n_{j,1} > k$).

2. Let $f(X) = \frac{P(X)}{X-a}$, where $P(X) \in k[X]$, and $|a|_p < |r|_p$, i.e. a is "inside of the contour". Consider the identity

$$\begin{aligned}\frac{1}{n_j}\sum_{i=1}^{n_j}\frac{1}{\frac{a}{r}-\alpha_i} &= \frac{1}{n_j}\cdot\frac{g_j'(\frac{a}{r})}{g_j(\frac{a}{r})} = \\ &= \frac{1}{n_j}\cdot\frac{n_j(\frac{a}{r})^{n_j-1} + n_{j,1}c_{j,1}(\frac{a}{r})^{n_{j,1}-1} + \cdots + n_{j,\mu}c_{j,\mu}(\frac{a}{r})^{n_{j,\mu}-1}}{(\frac{a}{r})^{n_j} + c_{j,1}(\frac{a}{r})^{n_{j,1}} + \cdots + c_{j,\mu}(\frac{a}{r})^{n_{j,\mu}} + c_0} \\ &= \frac{1}{(\frac{a}{r})}\cdot\frac{(\frac{a}{r})^{n_j} + \frac{n_{j,1}}{n_j}c_{j,1}(\frac{a}{r})^{n_{j,1}} + \cdots + \frac{n_{j,\mu}}{n_j}c_{j,\mu}(\frac{a}{r})^{n_{j,\mu}}}{(\frac{a}{r})^{n_j} + c_{j,1}(\frac{a}{r})^{n_{j,1}} + \cdots + c_{j,\mu}(\frac{a}{r})^{n_{j,\mu}} + c_0}.\end{aligned} \tag{1}$$

The r.h.s. tends to zero in the norm $|\cdot|_p$, since $n_{j,\mu} \to \infty$ and $\left|\frac{a}{r}\right|_p < 1$.

Hence

$$\begin{aligned}\int_{0,r,g}\frac{1}{x-a} &= \lim_{j\to\infty}\sum_{g_j(\alpha_i)=0}\frac{r\alpha_i}{n_j}\frac{1}{r\alpha_i - a} = \lim_{j\to\infty}\frac{1}{n_j}\sum_{g_j(\alpha_i)=0}\frac{\alpha_i}{\alpha_i - \frac{a}{r}} \\ &= \lim_{j\to\infty}\frac{1}{n_j}\sum_{g_j(\alpha_i)=0}\left(1 + \frac{\frac{a}{r}}{\alpha_i - \frac{a}{r}}\right) \\ &= \lim_{j\to\infty}\left(1 - \frac{a}{r}\cdot\frac{1}{n_i}\sum_{g_j(\alpha_i)=0}\frac{1}{\frac{a}{r}-\alpha_i}\right) = 1.\end{aligned} \tag{2}$$

Using Bézout's theorem to represent $P(X) = P(a) + q(X)(X-a)$, we obtain

$$\int_{0,r,g}\frac{P(x)}{x-a} = \int_{0,r,g}\frac{P(a)}{x-a} + q(x) = P(a)\int_{0,r,g}\frac{1}{x-a} = P(a) = \operatorname{res}_a f(x).$$

In the case when $|a|_p > |r|_p$ (i.e. a is "outside of the contour") the expression in the r.h.s. of (1) has the limit $\frac{1}{(\frac{a}{r})}$, which yields that the l.h.s. of (2) is equal to 0. Thus, the integral $\int_{0,r,g}\frac{P(x)}{x-a}$ is 0.

3. By the same way as for ordinary complex integral we can prove that

$$\int_{x_0,r,g}\frac{h(x)}{(x-a)} = h(a)$$

implies

$$\int_{x_0,r,g}\frac{h(x)}{(x-a)^n} = \frac{1}{(n-1)!}h^{(n-1)}(a).$$

This yields that we obtain for $f(X) = \frac{P(X)}{(X-a)^n}$, where $P(X) \in k[X]$ and $|a|_p < |r|_p$

$$\int_{0,r,g}\frac{P(x)}{(x-a)^n} = \frac{1}{(n-1)!}P^{(n-1)}(a) = \operatorname{res}_a f(x).$$

4. Suppose $f(X)=\frac{P(X)}{(X-a)^n}$, where $P(X)\in k[[X]]$, and $|a|_p<|r|_p$. Let $P_m(X)\in k[X]$ be a truncation of $P(X)$ such that $\frac{P_m(x)}{(x-a)^n}\underset{p^m}{\equiv}\frac{P(x)}{(x-a)^n}$ for $|x|_p=|r|_p$. By the above arguments we have

$$\int_{0,r,g}\frac{P(x)}{(x-a)^n}\underset{p^m}{\equiv}\int_{0,r,g}\frac{P_m(x)}{(x-a)^n}=$$
$$=\frac{1}{(n-1)!}P_m^{(n-1)}(a)=\frac{1}{(n-1)!}P^{(n-1)}(a)=\mathrm{res}_a\,f(x).$$

Setting $m\to\infty$ we obtain the required statement.

It is easy to see that in the case $|a|_p<|r|_p$ in the **3.** and **4.** we get $\int_{0,r,g}f(x)=0$.

5. Let now $f(X)=\frac{P(X)}{Q(X)}$, where $Q(X)$ is an arbitrary polynomial. We will reduce this case to the previous one, i.e. to the case $Q(X)=(x-a)^n$. The polynomial $Q(X)$ can be decomposed on the linear multipliers at $\mathbb{Q}_p^{alg}$. To simplify formulas below we assume that $Q(X)$ has only two different roots, i.e. $Q(X)=(x-a)^n(x-b)^m$. Then there exist polynomials $q(X)$ and $s(X)$ such that $(x-a)^nq(x)+(x-b)^ms(X)=1$. This yields

$$\begin{aligned}\int_{0,r,g}\frac{P(x)}{(x-a)^n(x-b)^m}&=\int_{0,r,g}\frac{P(x)((x-a)^nq(x)+(x-b)^ms(x))}{(x-a)^n(x-b)^m}\\&=\int_{0,r,g}\frac{P(x)q(x)}{(x-b)^m}+\int_{0,r,g}\frac{P(x)s(x)}{(x-a)^n}.\end{aligned}\tag{3}$$

If b is outside of the contour, then $\int_{0,r,g}\frac{P(x)q(x)}{(x-b)^m}=0$. If b is inside of the contour, then we have

$$\begin{aligned}\int_{0,r,g}\frac{P(x)q(x)}{(x-b)^m}&=\mathrm{res}_b\frac{P(x)q(x)}{(x-b)^m}=\mathrm{res}_b\frac{P(x)\left(\frac{1-s(x)(x-b)^m}{(x-a)^n}\right)}{(x-b)^m}\\&=\mathrm{res}_b\frac{P(x)}{(x-a)^n(x-b)^m}-\mathrm{res}_b\frac{P(x)s(x)(x-b)^m}{(x-a)^n(x-b)^m}\\&=\mathrm{res}_b\frac{P(x)}{(x-a)^n(x-b)^m}-\mathrm{res}_b\frac{P(x)s(x)}{(x-a)^n}\\&=\mathrm{res}_b\frac{P(x)}{(x-a)^n(x-b)^m}.\end{aligned}$$

The second addition in (3) can be computed similarly. Thus, the theorems are proved. □

We will omit the index g in the integral below and assume that $g_j=X^{n_j}-1$ with $(n_j,p)=1$.

2 The main theorem.

2.1 The explicit formula of the norm residue symbol

Notation

Let $K=\mathbb{Q}_p(\zeta_{p^n})$ be a cyclotomic field with the residue field of the odd characteristic p, and

- π is a uniformizing element in K,
- μ_{p^n} is the group of the nth roots of unity,
- $\triangle$ is the Frobenius automorphism in $\mathbb{Q}_p$,
- $\underline{\alpha}(X)\in\mathfrak{o}_T((X))^*$ such that $\underline{\alpha}(\pi')=\alpha$, similarly we define $\underline{\beta}(X)$ and $\underline{\zeta}(X)$,

• $d = \frac{d}{dX}$.

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

$$\triangle\left(\sum a_i X^i\right) = \left(\sum a_i X^i\right)^{\triangle} = \sum a_i^{\triangle} X^{pi}.$$

Construct the Artin–Hasse logarithm. Set

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

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

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

Now we can define the pairing as

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

$$\langle \alpha,\, \beta\rangle = \zeta^{\operatorname{Tr}\operatorname{res}\frac{\Phi(\underline{\alpha},\underline{\beta})}{\underline{\zeta}^{p^n}-1}} \tag{4}$$

with

$$\Phi(\underline{\alpha},\, \underline{\beta}) = \ell_m(\underline{\beta})\, d(\ell_m(\underline{\alpha})) - \ell_m(\underline{\beta})\underline{\alpha}^{-1}d\underline{\alpha} - \ell_m(\underline{\alpha})\underline{\beta}^{-1}d\underline{\beta}. \tag{5}$$

The inverse in (4) is taken in the two dimension local ring $\mathbb{Z}_p\{\{X\}\}$ i. e.

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

where we denote $z(X) = \underline{\zeta}(X) - 1$ (see [5, §3] for more details). The symbol res here is residue at 0.

We will use below the same notations for the pairing $\langle \underline{\alpha},\, \underline{\beta}\rangle = \operatorname{res}\frac{\Phi(\underline{\alpha},\underline{\beta})}{\underline{\zeta}^{p^n}-1} \bmod p^n$.

2.2 The main theorem

The aim of this subsection is to represent the ratio of the power residue symbols in the new form. The reciprocity law, which was proved first by Hasse (see [1, p. 58]), in our case has the form

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

This reduces the problem to the analysis of the norm residue symbol. For this symbol there is Vostokov's explicit formula (see [5] or [6])

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

Here we use the notations of the previous subsection.

The main theorem of this paper is

Theorem 1. *In the notations of the previous subsection we have*

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

where the inverse in the integral is taken in the two dimension local ring $\mathbb{Z}_p\{\{X\}\}$.

Proof. Using Theorem 2 we obtain

$$\int_{0,\pi} \frac{\Phi(\underline{\alpha},\underline{\beta})}{\underline{\zeta}^{p^n}-1} = \operatorname{res}_0 \frac{\Phi(\underline{\alpha},\underline{\beta})}{\underline{\zeta}^{p^n}-1} = \operatorname{res} \frac{\Phi(\underline{\alpha},\underline{\beta})}{\underline{\zeta}^{p^n}-1}.$$

Thus, according to the above arguments, we get

$$\left(\frac{\alpha}{\beta}\right)_{p^n}\left(\frac{\beta}{\alpha}\right)_{p^n}^{-1} = \left(\frac{\alpha,\beta}{(\pi)}\right)_{p^n} = \zeta^{\operatorname{res}_0 \frac{\Phi(\underline{\alpha},\underline{\beta})}{\underline{\zeta}^{p^n}-1}} = \zeta^{\int_{0,\pi} \frac{\Phi(\underline{\alpha},\underline{\beta})}{\underline{\zeta}^{p^n}-1}}.$$

□

3 The Eisenstein reciprocity law

The classical Eisenstein reciprocity law gives the conditions of the equality of the power residues in the cyclotomic field, when one of the arguments lies in the basic field. In the present paper we prove it using our result.

Theorem 2. *Let $K = \mathbb{Q}_p(\zeta_{p^n})$. Then we have for $a \in \mathbb{Z}_p^*$*

$$\left(\frac{a}{\beta}\right)_{p^n}\left(\frac{\beta}{a}\right)_{p^n}^{-1} = 1\ \forall\beta \Leftrightarrow \frac{a^{p-1}-1}{p} \equiv 0 \mod p^n.$$

Proof. First we need the following

lemma 1. *Let $a \in \mathbb{Z}_p^*$. Then the Artin-Hasse logarithm $\ell_m(a)$ can be represented in the form*

$$\ell_m(a) = \frac{a^{p-1}-1}{p}\, t$$

with some t such that

$$t \equiv 1 \mod p.$$

Proof. Since $\frac{a^{p-1}-1}{p} \in \mathbb{Z}_p$, we can write

$$\begin{aligned}\ell_m(a) = \frac{1}{p}\log\left(\frac{a^p}{a^{\triangle}}\right) = \frac{1}{p}\log(a^{p-1}) = \frac{1}{p}\log\left(1+\frac{a^{p-1}-1}{p}p\right) = \\ = \frac{a^{p-1}-1}{p}\underbrace{\left(1-\frac{1}{2}\frac{a^{p-1}-1}{p}p+\frac{1}{3}\left(\frac{a^{p-1}-1}{p}p\right)^2-\dots\right)}_{t} \underset{p}{\equiv} \frac{a^{p-1}-1}{p}\, t.\end{aligned}$$

□

Take $\pi = \zeta_{p^n} - 1$ as a prime in $\mathbb{Q}_p(\zeta_{p^n})$. According to Theorem 1, the statement of Theorem 2 is equivalent to

$$\int_{0,\pi} \frac{\Phi(a,\underline{\beta})}{\underline{\zeta}^{p^n}-1} \underset{p^n}{\equiv} 0\ \forall\beta \Leftrightarrow \frac{a^{p-1}-1}{p} \equiv 0 \mod p^n.$$

Substituting the expression of Φ (see (5)) and using that a in the basic field (i.e. $\underline{a}(X) = a$), we obtain

$$\int_{0,\pi} \frac{\Phi(a,\underline{\beta})}{\underline{\zeta}^{p^n}-1} = \int_{0,\pi} \frac{\ell_m(a)\underline{\beta}^{-1}d\underline{\beta}}{\underline{\zeta}^{p^n}-1} = \ell_m(a)\int_{0,\pi} \frac{\underline{\beta}^{-1}d\underline{\beta}}{\underline{\zeta}^{p^n}-1}.$$

We are left to find β such that $\int_{0,\pi} \frac{\underline{\beta}^{-1}d\underline{\beta}}{\underline{\zeta}^{p^n}-1} \not\equiv 0 \mod p$. Since $\zeta = 1+\pi$, we have $\underline{\zeta} = 1+X$. Thus, $\frac{1}{\underline{\zeta}^{p^n}-1} \underset{p}{\equiv} \frac{1}{X^{p^n}}$. Hence, substituting $\beta = 1-\pi$, we get

$$\int_{0,\pi} \frac{\underline{\beta}^{-1}d\underline{\beta}}{\underline{\zeta}^{p^n}-1} \underset{p}{\equiv} -\int_{0,\pi} \frac{1+X+X^2+X^3+\dots}{X^{p^n}} = -1.$$

Therefore, using the lemma, we obtain finally

$$\int_{0,\pi} \frac{\Phi(a,\underline{\beta})}{\underline{\zeta}^{p^n}-1} \underset{p^n}{\equiv} 0 \ \forall\beta \Leftrightarrow \ell_m(\underline{\alpha}) \underset{p^n}{\equiv} 0 \Leftrightarrow \frac{a^{p-1}-1}{p} \equiv 0 \mod p^n.$$

This completes the proof. □

References

[1] Helmut Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. II. Reziprozitätsgesetz, Leipzig–Berlin, 1930.

[2] David Hilbert, Gesammelte Abhandlungen. Bd. 1, Springer, Berlin , 1932

[3] L.G. Snirel'mann, Sur les fonctions dans les corps normés et algébriquement fermés, (Russian. French summary) Bull. Acad. Sci. URSS, Ser. Math. 1938, **2** 5–6, 487–498.

[4] I. R. Shafarevich, A general reciprocity law, Amer. Math. Soc. Transl. Ser. 2, **4** (1956) 73–106.

[5] S. V. Vostokov, Explicit form of the law of reciprocity, Izv. Akad. Nauk SSSR, Ser. Mat., **42** no. 6 (1978),1288–1321; English transl., Math. USSR-Izv. **13** (1979), 557–588.

[6] I. B. Fesenko, S. V. Vostokov, Local Fields and Their Extensions Second Edition, AMS, 2002, 345 pp

[7] S.V. Vostokov, The classical reciprocity law for power residues as an analog of an Abelian integral theorem, Algebra i Analiz, **20** (2008), no. 6, 108–118; English transl., St. Petersburg Math. J. **20** (2009), 929–936.