THE CLASSICAL RECIPROCITY LAW FOR POWER RESIDUES AS AN ANALOG OF THE ABELIAN INTEGRAL THEOREM

S. V. VOSTOKOV

ABSTRACT. A formula for power residue symbols is deduced, which can be treated as an analog of the Abelian integral theorem for number fields.

§0. 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: the ramification points of a Riemann surface correspond to prime divisors of the discriminant of a number field, etc. The theory of Abelian integrals is the most studied part of the theory of algebraic functions. David Hilbert was apparently the first who initiated an analog of this theory in the fields of algebraic numbers. In particular, he noticed that his reciprocity law for the product of norm residue symbols (Hilbert symbols),

$$(1) \quad \prod_{\mathfrak{p}} \left(\frac{\alpha, \beta}{\mathfrak{p}} \right) = 1,$$

is an analog of Cauchy's integral theorem (see [6, pp. 367–368]). Igor Shafarevich corrected him: Hilbert's reciprocity law is an analog of the corollary to Cauchy's integral theorem that says that the sum of residues of an Abelian differential $\alpha d\beta$ at all points of a Riemann surface is zero. From this point of view the local norm residue symbol $\left(\frac{\alpha, \beta}{\mathfrak{p}} \right)$ is an analog of the Abelian differential $\alpha d\beta$ at $\mathfrak{p}$ (see [3, p. 114]).

To clarify the analogy with a Riemann surface, we consider the field of algebraic functions $\mathbb{C}(t)$ and a point P on a Riemann surface lying over the extended complex plane $\overline{\mathbb{C}}$. Let t be a local parameter. There are two simple operations in the field $\mathbb{C}(t)$: taking the derivative $\partial = d/dt$ and the residue $\text{res}(\sum \alpha_i t^i) = \alpha_{-1}$. Then the meromorphic differential $\omega = f dt$ defined in the vicinity of P has a finite number of poles, and we have

$$(1') \quad \text{res}(\omega) = 0.$$

On the other hand, only finitely many prime ideals ramify in an algebraic number field, and thus, only finitely many local norm residue symbols are different from 1. Therefore, the product in (1) is well defined, and relation (1) is an analog of relation (1') (for the details, see the book “The way” by Alexei Parshin, [2, Chapter 1]). Of course, our shallow explanation does not clarify the essence of this. To make the analogy more transparent, we consider the classical reciprocity law for power residues, which relates the product of power residues to a finite product of local norm residue symbols. It is well known

---

2000 *Mathematics Subject Classification*. Primary 11R37.

Key words and phrases. Power residue symbol, reciprocity law.

Supported by INTAS, SFB-478 “Algebraische Strukturen”, and RFBR (grant no. 08-01-00777-a).

that the main problem in the classical reciprocity law is to find an explicit formula for the product of power residue symbols. Class field theory relates this product to a finite product of local norm residue symbols:

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{p}|n, \infty} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n$$

(see [5]). This equation is 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 the residues of this form at the singular points. In the present paper, we find an explicit formula for the product of power residues in a cyclotomic field and show that this formula is an analog of the Abelian integral theorem.

NOTATION

- $\zeta := \zeta_n$ is a primitive n th root of 1;
- $K = \mathbb{Q}(\zeta)$ is a cyclotomic field;
- $n = \prod_{i=1}^r p_i^{m_i}$, $n_i = n/p_i^{m_i}$, $a_i n_i + b_i p_i^{m_i} = 1$, $a_i, b_i \in \mathbb{Z}$;
- $\zeta_i = \zeta_{p_i^{m_i}}$, $\pi_i = \zeta_i - 1$;
- $\{\pi_1^{\alpha_1} \cdots \pi_r^{\alpha_r}, 0 \leq \alpha_i < \phi(p_i^{m_i})\}$ is a basis of the ring $\mathbb{Z}[\zeta]$ over $\mathbb{Z}$;
- $X_1, \dots, X_r$ is a set of variables.

For a number α in $\mathbb{Z}[\zeta]$, we denote by

- $\underline{\alpha} := \underline{\alpha}(X_1, \dots, X_r) \in \mathbb{Z}[X_1, \dots, X_r]$ the polynomial obtained from the expansion of α with respect to the basis of $\mathbb{Z}[\zeta]$. Thus,

$$\underline{\alpha}(\pi_1, \dots, \pi_r) = \alpha.$$

If $(\alpha, n) = 1$, then we assume that the free term of the polynomial $\underline{\alpha}$ is prime to n . As usual,

- $\text{res}_i := \text{res}_{X_i}$ is the residue at X_i .

§1. STATEMENT OF THE MAIN THEOREM

1.1. The definition of the function l_Δ . We fix a prime p and denote by $A_{(p)}$ (respectively, by A_p) the polynomial ring $\mathbb{Z}_{(p)}[X_1, \dots, X_{r-1}]$ (respectively, $\mathbb{Z}_p[X_1, \dots, X_{r-1}]$), where $\mathbb{Z}_{(p)}$ is the ring of p -adic integers. Let Δ be the operator acting on the Laurent series ring $A_{(p)}((X))$ as follows:

$$\begin{aligned} \Delta a &= a^\Delta = a, \quad a \in \mathbb{Z}_{(p)}; \\ \Delta X &= X^\Delta := X^p; \\ \Delta X_k &= X_k^\Delta := (1 + X_k)^p - 1, \quad 1 \leq k \leq r-1. \end{aligned}$$

Remark 1. The definition of the action of Δ on X_k is dictated by the fact that the Frobenius operator σ in the unramified extension $\mathbb{Q}_p(\zeta_k)/\mathbb{Q}_p$ acts on the prime π_k of this extension as follows: $\pi_k^\sigma = (1 + \pi_k)^p - 1$. Replacing π_k by the variable X_k , we obtain the action of Δ .

Let M_p be the multiplicative monoid of series in $A_{(p)}((X))$:

$$M_p = \{f_m X^m + f_{m+1} X^{m+1} + \dots; m \in \mathbb{Z}, f_{m+i} \in A_{(p)}, f_m(0, 0, \dots, 0) \in \mathbb{Z}_{(p)}^*\}.$$

We define a function l_Δ on M_p as follows:

$$l_\Delta(f) = \frac{1}{p} \log \frac{f^p}{f^\Delta}, \quad f \in M_p.$$

Proposition 1. *The function l_Δ is well defined and gives rise to a homomorphism from the multiplicative monoid M_p to the additive group of $A_p[[X]]$.*

Proof. Let

$$f = f_m X^m + f_{m+1} X^{m+1} + \cdots \in M_p.$$

Then $c = f_m(0, 0, \dots, 0)$ is invertible in $\mathbb{Z}_{(p)}$, $f_m = c(1 + g)$, and the free term of the polynomial g belonging to $A_{(p)}$ is zero. Therefore,

$$f = cX^m(1 + g + g_1X + g_2X^2 + \cdots),$$

where

$$g_i = c^{-1}f_{m+i} \in A_{(p)}.$$

This fact and the definition of l_Δ show that

$$l_\Delta(f) = l_\Delta(c) + l_\Delta(X^m) + l_\Delta(1 + h),$$

where $h = g + g_1X + \cdots \in A_{(p)}[[X]]$ and the free term of g is zero. Next, $l_\Delta(c) = \frac{1}{p} \log c^{p-1} \in \mathbb{Z}_p$, because $c^{p-1} = 1 + pc'$ and $c' \in \mathbb{Z}_{(p)}$. Moreover, $l_\Delta(X^m) = 0$. The proof of the statement about the series $l_\Delta(1 + h)$ can be obtained in the same way as the proof of Lemma 2 in [1]. $\square$

1.2. Now, let p be a prime divisor of $n = p_1^{m_1} \cdots p_r^{m_r}$, say, $p = p_r$. Let $n = n_r p^m$, where $m := m_r$ and $(n_r, p) = 1$. We denote by $A_p\{\{X\}\}$ the following two-dimensional ring of series:

$$A_p\{\{X\}\} = \left\{ \sum_{k \in \mathbb{Z}} f_k X^k, f_k \in A_p, f_k \xrightarrow[k \rightarrow -\infty]{} 0 \text{ in the } p\text{-adic norm} \right\}.$$

Let $f(X)$ be a series from the ring $A_p[[X]]$, and let $g(X)$ be an invertible series from $A_p\{\{X\}\}$.

Lemma 1. *Let*

$$c(X_1, \dots, X_{r-1}) = \text{res}_X f(X)/g(X) \pmod{p^m A_p}.$$

Then $c(X_1, \dots, X_{r-1}) \in \mathbb{Z}[X_1, \dots, X_{r-1}]$, and the trace

$$\text{Tr}_r c(\pi_1, \dots, \pi_{r-1}) \in \mathbb{Z}$$

is well defined, where $\text{Tr}_r : \mathbb{Q}(\zeta_{n_r}) \rightarrow \mathbb{Q}$, $\pi_i = \zeta_{p_i}^{m_i} - 1$.

Proof. The residue $\text{res}_X f(X)/g(X)$ is a polynomial in $\mathbb{Z}_p[X_1, \dots, X_{r-1}]$. Therefore, $c(X_1, \dots, X_{r-1}) \in \mathbb{Z}[X_1, \dots, X_{r-1}]$, and we have $c(\pi_1, \dots, \pi_{r-1}) \in \mathbb{Z}[\zeta_{n_r}]$. $\square$

1.3. Let p_i be a prime divisor of n , and let $l_i := l_{\Delta_i}$ be a function as in Subsection 1.1 for the operator $\Delta = \Delta_i$ corresponding to the prime $p := p_i$, i.e.,

$$\Delta_i(X_k) = \begin{cases} X_i^p, & k = i, \\ (1 + X_k)^p - 1, & k \neq i, \end{cases}$$

$$l_i(f) := \frac{1}{p_i} \log f^{p_i} / f^{\Delta_i},$$

with values in the additive group of $A_{p_i}[[X_i]]$, where

$$A_{p_i} = \mathbb{Z}_{p_i}[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_r].$$

As before, we assume that for each element α of $\mathbb{Z}[\zeta]$ with $(\alpha, n) = 1$, a polynomial $\underline{\alpha} := \underline{\alpha}(X_1, \dots, X_r) \in \mathbb{Z}[X_1, \dots, X_r]$ is given such that $\underline{\alpha}(\pi_1, \dots, \pi_r) = \alpha$ and the free term of $\underline{\alpha}(0, \dots, 0)$ is prime to n .

For $\alpha, \beta \in \mathbb{Z}[\zeta]$, $(\alpha, n) = 1$, $(\beta, n) = 1$, we consider the series

$$(2) \quad \Phi_i(\underline{\alpha}, \underline{\beta}) = l_i(\underline{\alpha}) \frac{\partial}{\partial X_i} l_i(\underline{\beta}) - l_i(\underline{\alpha}) \underline{\beta}^{-1} \frac{\partial}{\partial X_i} \underline{\beta} + l_i(\underline{\beta}) \underline{\alpha}^{-1} \frac{\partial}{\partial X_i} (\underline{\alpha}).$$

By Proposition 1, the series $\Phi_i(\underline{\alpha}, \underline{\beta})$ belongs to $A_{p_i}[[X_i]]$.

Statement of the main theorem. Let $K = \mathbb{Q}(\zeta)$ be a cyclotomic field and $\zeta := \zeta_n$, where n is an odd integer, and let $\alpha, \beta \in \mathbb{Z}[\zeta]$ be relatively prime and prime to n . Then the n th power residue symbol $(\frac{\alpha}{\beta})_n$ is defined.

Suppose $n = p_i^{m_i} \cdots p_r^{m_r}$, $\zeta_i := \zeta_{p_i^{m_i}}$, $\pi_i = \zeta_i - 1$.

Theorem 1. *The product of power residue symbols obeys the following relation:*

$$(3) \quad \left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \zeta^{\sum_{i=1}^r \text{res}_i S_i},$$

where

$$S_i = n_i b_i \text{Tr}_i \left(\frac{\Phi_i(\underline{\alpha}, \underline{\beta})}{\zeta_i^{p_i^{m_i}} - 1} \right) \Big|_{X_k = \pi_k, k \neq i}$$

(for the notation, see §0).

Remark 2. Formula (3) is an analog of the Abelian integral theorem in number fields. The exponent on the right-hand side of this formula involves the sum of the residues of the differential forms Φ_i at the “singular” points, which are the denominators $\zeta_i^{p_i^{m_i}} - 1$, because $\zeta_i^{p_i^{m_i}} - 1 = 0$. The remaining problem is to properly define an analog of the integral, which should correspond to the product of power residue symbols

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1}.$$

If, for example,

$$n = p_1 \cdots p_r,$$

then, as will be shown below, the differential forms Φ_i turn into simple series, and the general differential form will be $\Phi = \log \underline{\beta} \log \underline{\alpha}$. Therefore, the left-hand side of (3) becomes

$$\int (\log \underline{\beta}) d \log \underline{\alpha} / (\zeta^n - 1).$$

Proposition 2. *All calculations in formula (3) are done in the field $K = \mathbb{Q}(\zeta)$, and the right-hand side is well defined.*

Proof. It is easily seen that

$$\text{res}_i S_i = n_i b_i \text{Tr}_i \left(\text{res}_i (\Phi_i(\underline{\alpha}, \underline{\beta}) / (\zeta_i^{p_i^{m_i}} - 1)) \right) \Big|_{X_k = \pi_k, k \neq i}.$$

Next, the polynomial $\zeta_i^{p_i^{m_i}} - 1$ is an invertible element of the ring $A_{p_i} \{\{X_i\}\}$. By Lemma 1, we have

$$a = \text{Tr}_i c(\pi_1, \dots, \pi_{i-1}, \pi_{i+1}, \dots, \pi_r) \in \mathbb{Z},$$

where $c(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_r) = \text{res}_i \Phi_i / (\zeta_i^{p_i^{m_i}} - 1) \pmod{p^{m_i} A_{p_i}}$, and so $\zeta^{n_i b_i a}$ is a $p_i^{m_i}$ th root of unity. Therefore, the i th factor on the right-hand side of formula (3) is well defined; it is $\zeta^{\text{res}_i S_i}$. Here the calculation is done in the field $K = \mathbb{Q}(\zeta)$. $\square$

§2. LOCAL SYMBOLS

2.1. Let $K = \mathbb{Q}(\zeta_n)$, let p be a prime divisor of n , and let $\mathfrak{p}$ be a prime ideal in K dividing (p) . Suppose $F = K_{\mathfrak{p}} = \mathbb{Q}_p(\zeta_n)$ is the completion of K with respect to the ideal $\mathfrak{p}$. Let $n = n_1 p^m$ and $T = \mathbb{Q}_p(\zeta_{n_1})$. Then F/T is a totally ramified extension and the extension $T/\mathbb{Q}_p$ is unramified.

Lemma 2. *Let $kn_1 + lp^m = 1$, $k, l \in \mathbb{Z}$, and let α, β be elements of F^* such that $(\alpha\beta, n) = 1$. Then, for the local norm residue symbol, we have*

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n = \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_{p^m}^k.$$

Proof. The basic properties of the norm residue symbol imply

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n = \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_{n_1}^l \cdot \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_{p^m}^k$$

(see, e.g., [7, Chapter IV, 5]). The first symbol on the right-hand side of the above relation is tame because $\mathfrak{p} \nmid n_1$. Therefore, the well-known formula for the tame symbol yields

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_{n_1} \equiv (-1)^{v(\alpha)v(\beta)} \alpha^{-v(\beta)} \beta^{v(\alpha)} \pmod{\mathfrak{p}},$$

where v is the valuation in F , and using the fact that α and β are units in F because $(\alpha\beta, n) = 1$ and $p \mid n$, we obtain $v(\alpha) = v(\beta) = 0$, whence $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_{n_1} = 1$. $\square$

Let $\pi = \zeta_n - 1$. For an element $\alpha \in F^*$, we write $\alpha := \alpha(X) \in \mathfrak{o}_T[[X]]$, where $\mathfrak{o}_T$ is the ring of integers of the field T , if

$$\alpha(\pi) = \alpha.$$

Let

$$(3') \quad l(\alpha) = \frac{1}{p} \log \alpha^p / \alpha^\Delta,$$

where $\alpha^\Delta := (\sum a_i X^i)^\Delta = \sum (\text{Frob } a_i) X^{p^i}$, $a_i \in \mathfrak{o}_T$, and Frob is the Frobenius automorphism in T (for the details, see [1]).

Lemma 3. *If $\alpha, \beta \in F^*$, $(\alpha\beta, n) = 1$, $p \mid n = n_1 p^m$, and $kn_1 + lp^m = 1$, then the following explicit formula is valid:*

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n = \zeta_n^{\text{Tr}(\text{res}_X \Phi(\alpha, \beta) / (\zeta_{p^m}^{p^m} - 1))},$$

where $\text{Tr} := \text{Tr}_{T/\mathbb{Q}_p}$ and

$$(4) \quad \Phi(\alpha, \beta) = l(\alpha) \frac{\partial}{\partial X} l(\beta) - l(\alpha) \beta^{-1} \frac{\partial}{\partial X} \beta + l(\beta) \alpha^{-1} \frac{\partial}{\partial X} (\alpha).$$

Corollary. *If in Lemma 3 we have $n = n_1 p$ and $(n_1, p) = 1$, then the series $\Phi(\alpha, \beta)$ for the units α and β has a simpler form:*

$$\Phi(\alpha, \beta) = \log \beta \frac{\partial}{\partial X} \log \alpha$$

(see [7, Chapter VII, 5]).

The proof of Lemma 3 follows from Lemma 2 and the explicit formula for the norm residue symbol (see [1, 4]).

2.2. Suppose $n = p_1^{m_1} \cdots p_r^{m_r}$, $\zeta_i := \zeta_{p_i^{m_i}}$, and $\pi_i = \zeta_i - 1$. We fix p with $p \mid n$, say, $p := p_1$. Then $n = n_1 p^m$, where $m = m_1$ and $(n_1, p) = 1$; the extension $T = \mathbb{Q}_p(\zeta_{n_1})$ is unramified over $\mathbb{Q}_p$, and the Frobenius automorphism σ in $T/\mathbb{Q}_p$ takes the root ζ_i to ζ_i^p ; thus, $\pi_i^\sigma = (1 + \pi_i)^p - 1$, $i = 2, 3, \dots, r$.

Let a be an element of the ring $\mathbb{Z}[\zeta_{n_1}]$, and let $\underline{a}(X_2, X_3, \dots, X_r)$ be a polynomial in $\mathbb{Z}[X_2, X_3, \dots, X_r]$ such that $\underline{a}(\pi_2, \pi_3, \dots, \pi_r) = a$. Let Δ_1 be the operator on the ring $\mathbb{Z}[X_2, X_3, \dots, X_r]$ acting as in Subsection 1.1, i.e.,

$$\Delta_1 X_i = X_i^{\Delta_1} := (1 + X_i)^p - 1, \quad i = 2, 3, \dots, r.$$

We obtain

$$\underline{a}(X_2, X_3, \dots, X_r)^{\Delta_1} \big|_{X_i=\pi_i} = a^\sigma.$$

Next, for an element α of $\mathbb{Z}[\zeta_n]$, we take an arbitrary series $\underline{\alpha} := \underline{\alpha}(X)$ in the ring $A_{(p)}((X))$, where $A_{(p)} = \mathbb{Z}_{(p)}[X_2, X_3, \dots, X_r]$, with the property

$$\underline{\alpha}(X) \big|_{X=\pi_1, X_i=\pi_i, 2 \leq i \leq r} = \alpha.$$

As in Subsection 1.3, we define an operator Δ_1 on the ring $A_{(p)}$ as follows: $\Delta_1 X := X^{\Delta_1} := X^p$, $\Delta_1 X_i = X_i^{\Delta_1} = (1 + X_i)^p - 1$, $2 \leq i \leq r$, and Δ_1 is the identity on $\mathbb{Z}_{(p)}$. Then $\underline{\alpha}(X)^{\Delta_1} \big|_{X_i=\pi_i, 2 \leq i \leq r} = \underline{\alpha}(X)^{\Delta} \big|_{X_i=\pi_i, 2 \leq i \leq r}$, where $\underline{\alpha}(X)$ is a series from Subsection 2.1 for α . Therefore, the function $l(\alpha)$ as in (3') coincides with the function

$$l_{\Delta_1}(\underline{\alpha}) \big|_{X_i=\pi_i, 2 \leq i \leq r},$$

and therefore, the series $\Phi(\alpha, \beta)$ occurring in (4) coincides with the series

$$\Phi_1(\underline{\alpha}, \underline{\beta}) \big|_{X_i=\pi_i, 2 \leq i \leq r}$$

occurring in (2).

2.3. Let Z be the decomposition field of the ideal (p) in $\mathbb{Q}(\zeta_n)$, where $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_d$ and $d = (Z : \mathbb{Q})$. Let $\mathfrak{P}_1, \dots, \mathfrak{P}_d$ be the prime ideals in $\mathbb{Q}(\zeta_n)$ lying over $\mathfrak{p}_1, \dots, \mathfrak{p}_d$, respectively,

$$\text{Gal}(Z/\mathbb{Q}) = \{\sigma_1 = \text{id}, \sigma_2, \dots, \sigma_d\}.$$

Let

$$\mathfrak{P}_i = \mathfrak{P}_1^{\sigma_i}, \quad 1 \leq i \leq d.$$

We have a tower of fields

$$\begin{array}{ccccccc} \mathbb{Q} & \longrightarrow & Z & \longrightarrow & \mathbb{Q}(\zeta_{n_1}) & \longrightarrow & \mathbb{Q}(\zeta_n) = K \\ & & \downarrow & & \downarrow & & \downarrow \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}_p & \longrightarrow & T = \mathbb{Q}_p(\zeta_{n_1}) & \longrightarrow & F = \mathbb{Q}_p(\zeta_n), \end{array}$$

where $\mathbb{Q}_p$ and T are the completions of Z and $\mathbb{Q}(\zeta_{n_1})$ with respect to any of the ideals $\mathfrak{p}_i$, $1 \leq i \leq d$, and F is the completion of K with respect to $\mathfrak{P}_i$ for any i . We have

$$\begin{aligned} \text{Gal}(F/\mathbb{Q}_p) &\cong \text{Gal}(K/Z), \\ \text{Gal}(F/T) &\cong \text{Gal}(K/\mathbb{Q}(\zeta_{n_1})), \\ \text{Gal}(T/\mathbb{Q}_p) &\cong \text{Gal}(\mathbb{Q}(\zeta_{n_1}))/Z. \end{aligned}$$

Let tr be the trace operator in $\mathbb{Q}(\zeta_{n_1})/Z$.

Proposition 3. Suppose $\alpha, \beta \in \mathbb{Z}[\zeta_n]$ and $(\alpha\beta, n) = 1$. Then

$$(5) \quad \left(\frac{\alpha, \beta}{\mathfrak{P}_1} \right)_{p^m} = \zeta_n^s,$$

where

$$s = \text{tr} \left(\text{res}_X \Phi_1(\underline{\alpha}, \underline{\beta}) / (\zeta_1^{p^m} - 1) \right) \Big|_{X_i = \pi_i, 2 \leq i \leq r}$$

(Φ_1 is as in (2)).

Proof. We use the formula from Lemma 2 for $n = p^m$ and observe that

$$\zeta_1^{p^m} - 1 = \zeta_1^{p^m} - 1 = (1 + X)^{p^m} - 1.$$

Then the above result (see Subsection 2.2) implies that the series

$$\Phi_1(\underline{\alpha}, \underline{\beta}) / (\zeta_1^{p^m} - 1) \Big|_{X_i = \pi_i, 2 \leq i \leq r}$$

coincides with the series

$$\Phi(\underline{\alpha}, \underline{\beta}) / (\zeta_1^{p^m} - 1),$$

whence

$$c = \left(\text{res}_X \Phi_1(\underline{\alpha}, \underline{\beta}) / (\zeta_1^{p^m} - 1) \right) \Big|_{X_i = \pi_i, 2 \leq i \leq r} = \text{res}_X \Phi_1(\underline{\alpha}, \underline{\beta}) / (\zeta_1^{p^m} - 1).$$

Since the element $c_m = c \pmod{p^m}$ belongs to the ring

$$\mathbb{Z}[\zeta_{n_1}] \hookrightarrow \mathbb{Z}_p[\zeta_{n_1}]$$

and $\text{Gal}(\mathbb{Q}(\zeta_{n_1})/\mathbb{Z}) \cong \text{Gal}(\mathbb{Q}_p(\zeta_{n_1})/\mathbb{Q}_p)$, we see that

$$\text{tr } c_m = \text{tr}_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Z}} c_m = \text{Tr}_{T/\mathbb{Q}_p} c_m,$$

and therefore, by Lemma 3, we obtain (5). $\square$

Proposition 4. As in the preceding proposition, let $c_m = c \pmod{p^m} \in \mathbb{Z}[\zeta_{n_1}]$, where

$$c = \left(\text{res}_X \Phi_1(\underline{\alpha}, \underline{\beta}) / (\zeta_1^{p^m} - 1) \right) \Big|_{X_i = \pi_i, 2 \leq i \leq r}, \quad \text{Tr} = \text{Tr}_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}}.$$

Then

$$\left(\frac{\alpha, \beta}{\mathfrak{P}_1} \right)_{p^m} \cdots \left(\frac{\alpha, \beta}{\mathfrak{P}_d} \right)_{p^m} = \zeta_1^{\text{Tr } c_m}.$$

Proof. The properties of the norm residue yield

$$\left(\frac{\alpha, \beta}{\mathfrak{P}_i} \right)_{p^m} = \left(\frac{\alpha, \beta}{\mathfrak{P}_1} \right)_{p^m}^{\sigma_i}, \quad 1 \leq i \leq d.$$

Consequently,

$$\prod_{i=1}^d \left(\frac{\alpha, \beta}{\mathfrak{P}_i} \right)_{p^m} = \zeta_1^{\sum_{i=1}^d (\text{tr } c_m)^{\sigma_i}}.$$

However,

$$\sum_{i=1}^d (\text{tr } c_m)^{\sigma_i} = \text{Tr}_{\mathbb{Z}/\mathbb{Q}}(\text{tr } c_m) = \text{Tr}_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}}(c_m) = \text{Tr } c_m. \quad \square$$

Proof of Theorem 1. Let $K = \mathbb{Q}(\zeta_n)$, where $n = p_1^{m_1} \cdots p_r^{m_r}$ is an odd integer. Let $n = n_i p_i^{m_i}$, and let $a_i n_i + b_i p_i^{m_i} = 1$. We assume that $\alpha, \beta \in \mathbb{Z}[\zeta_n]$ and α and β are relatively prime and prime to n . Consider the reciprocity law for n th power residues in K :

$$\left(\frac{\alpha}{\beta}\right)_n \cdot \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{P}|n} \left(\frac{\alpha, \beta}{\mathfrak{P}}\right)_n.$$

We split the right-hand side into r factors,

$$A_i = \prod_{\mathfrak{P}_{ij}|p_i} \left(\frac{\alpha, \beta}{\mathfrak{P}_{ij}}\right)_n, \quad 1 \leq i \leq r,$$

where $j = 1, 2, \dots, d_i$ and d_i is the degree of the decomposition field of the ideal (p_i) in $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$. By Lemma 2, we have

$$\left(\frac{\alpha, \beta}{\mathfrak{P}_{ij}}\right)_n = \left(\frac{\alpha, \beta}{\mathfrak{P}_{ij}}\right)_{p_i^{m_i}}^{a_i}.$$

Proposition 3 implies that

$$A_i = \zeta_{p_i^{m_i}}^{a_i \operatorname{Tr}_i c_{m_i}} = \zeta_n^{a_i n_i \operatorname{Tr}_i c_{m_i}},$$

where

$$c_{m_i} = \left(\operatorname{res}_{X_i} \Phi_i(\underline{\alpha}, \underline{\beta}) / (\zeta_{p_i^{m_i}}^{m_i} - 1) \right) \Big|_{X_k = \pi_k, k \neq i}$$

and $\operatorname{Tr}_i = \operatorname{Tr}_{\mathbb{Q}(\zeta_{n_i})/\mathbb{Q}}$. Now, to obtain formula (3) it remains to observe that the trace operator Tr_i commutes with res_{X_i} . $\square$

REFERENCES

- [1] S. V. Vostokov, *An explicit form of the reciprocity law*, Izv. Akad. Nauk SSSR Ser. Mat. **42** (1978), no. 6, 1288–1320; English transl., Math. USSR-Izv. **13** (1978), no. 3, 557–588 (1979). MR0522940 (80f:12014)
- [2] A. N. Parshin, *The way. Mathematics and other worlds*, Dobrosvet, Moscow, 2002. (Russian)
- [3] I. R. Shafarevich, *A general reciprocity law*, Mat. Sb. **26(68)** (1950), no. 1, 113–146; English transl., Amer. Math. Soc. Transl. Ser. 2, vol. 4, Amer. Math. Soc., Providence, RI, 1956, pp. 73–106. MR0031944 (11:230f)
- [4] H. Brückner, *Explizites Reziprozitätsgesetz und Anwendungen*, Vorlesungen Fachbereich Math. Univ. Essen, No. 2, Univ. Essen, Essen, 1979. MR0533354 (80m:12015)
- [5] H. Hasse, *Die Normenresttheorie relativ-Abelscher Zahlkörper als Klassenkörpertheorie im Kleinen*, J. Reine Angew. Math. **162** (1930), 145–168.
- [6] D. Hilbert, *Gesammelte Abhandlungen*. Bd. 1: Zahlentheorie, Springer, Berlin, 1932. MR0188046 (32:5489a)
- [7] I. Fesenko and S. Vostokov, *Local fields and their extensions*, Transl. Math. Monogr., vol. 121, Amer. Math. Soc., Providence, RI, 1993. MR1218392 (94d:11095)

DEPARTMENT OF MATHEMATICS AND MECHANICS, ST. PETERSBURG STATE UNIVERSITY, UNIVERSITETSKIĖ PROSPEKT 28, PETRODVORETS, 198504 ST. PETERSBURG, RUSSIA
E-mail address: sergei.vostokov@gmail.com

Received 14/APR/2008

Translated by B. M. BEKKER