Алгебра и анализ
Том 19 (2007), № 5

St. Petersburg Math. J.
Vol. 19 (2008), No. 5, Pages 719–722
S 1061-0022(08)01017-0
Article electronically published on June 25, 2008

VARIATIONS ON THE THEME OF D. K. FADDEEV'S PAPER "AN EXPLICIT FORM OF THE KUMMER–TAKAGI RECIPROCITY LAW"

S. V. VOSTOKOV

Dedicated to the centenary of the birth of my teacher Dmitriĭ Konstantinovich Faddeev

Abstract. The following form of the Eisenstein reciprocity law is established: in the cyclotomic field $\mathbb{Q}(\zeta)$, the relation $(\frac{\alpha}{a}) = (\frac{a}{\alpha})$ is equivalent to $\frac{a^{p-1}-1}{p} \cdot \underline{\alpha}'(1) \equiv 0 \mod p$.

Introduction

In volume 1 of "Zapiski Nauchnych Seminarov LOMI", four papers by Dmitriĭ Konstantinovich were published. One of those papers concerned explicit reciprocity laws and later compelled the author of the present paper to devote himself to this classical theme. In his paper, Dmitriĭ Konstantinovich gave an elegant "local" proof of the Kummer reciprocity law in a cyclotomic field. Using this proof, here we obtain necessary and sufficient conditions in the Eisenstein classical reciprocity law. Certainly, this result can be deduced from the explicit formula of general type obtained in [V], but we want to take an easier way.

The Eisenstein reciprocity law is stated as follows. Let $K = \mathbb{Q}(\zeta), \zeta = e^{2\pi i/p}$, be a cyclotomic field, where p is an odd prime. Let a be a rational integer relatively prime to p, and let α be a primary element of K, i.e., $\alpha \equiv b \mod (\zeta-1)^2$ for some rational integer b prime to p.

The Eisenstein classical reciprocity law.

$$\left(\frac{\alpha}{a}\right) = \left(\frac{a}{\alpha}\right), \tag{1}$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the pth power residue symbol in the field K (see [E]).

In the present paper, we find necessary and sufficient conditions under which the power residue symbols in (1) are equal. Let α be an element of $\mathbb{Z}[\zeta]$ with expansion

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$$

such that $a_0 + a_1 + \cdots + a_{p-2}$ is not divisible by p. We put $\underline{\alpha} := \underline{\alpha}(X) = a_0 + a_1X + \cdots + a_{p-2}X^{p-2}$. Then $\underline{\alpha}(\zeta) = \alpha$ and $\underline{\alpha}(1) \not\equiv 0 \mod p$.

Theorem 1. *In the cyclotomic field $\mathbb{Q}(\zeta)$, we have*

$$\left(\frac{\alpha}{a}\right) = \left(\frac{a}{\alpha}\right) \Longleftrightarrow \frac{a^{p-1}-1}{p} \cdot \underline{\alpha}'(1) \equiv 0 \mod p.$$

2000 *Mathematics Subject Classification.* Primary 11A15.
Key words and phrases. Reciprocity law, cyclotomic field.
Supported by INTAS.

1. Faddeev's formulas

Let $F = \mathbb{Q}_p(\zeta)$. It is well known that $F = \mathbb{Q}_p(\omega)$, where $\omega^{p-1} = -p$ and $\omega \equiv \zeta - 1 \mod \omega^2$ (see, e.g., [H, Chapter II, §15, 3, Proposition IV]).

As in [F], we consider the following basis of the multiplicative group F^*:

$$E_0 = \omega,\ E_1 = \zeta,\ E_k = \exp \omega^k, \quad 2 \le k \le p.$$

The basis $E_0, E_1, \dots, E_p$ is orthogonal with respect to the norm residue symbol $(,)$ in the field F:

$$\begin{aligned} (E_p, E_0) &= (E_0, E_p)^{-1} = \zeta, \\ (E_{p-k}, E_k) &= \zeta^k, \quad k = 1, 2, \dots, p-1, \\ (E_k, E_l) &= 1 \quad \text{if} \quad r + l \not\equiv 0 \mod p. \end{aligned} \tag{2}$$

Precisely this fact was proved by D. K. Faddeev in the paper [F]. Using the above relations, we prove Theorem 1.

2. Reduction of Theorem 1 to the norm residue symbol

We note that

$$\left(\frac{\alpha}{a}\right) = \left(\frac{a}{\alpha}\right) \Longleftrightarrow (a, \alpha) = 1. \tag{3}$$

This follows directly from the reciprocity law for the power residue symbols in the field $K = \mathbb{Q}(\zeta)$,

$$\left(\frac{\alpha}{a}\right)\left(\frac{a}{\alpha}\right)^{-1} = (a, \alpha).$$

Therefore, Theorem 1 reduces to the local situation, and we must find triviality conditions for the norm residue symbol (a, α).

3. Congruence for the first argument in (a, α)

Let a be a rational integer prime to p.

Lemma 1. *In the field $F = \mathbb{Q}_p(\zeta)$, we have the congruence*

$$a \equiv E_{p-1}^{(a^{p-1}-1)/p} \mod F^{*p}. \tag{4}$$

Proof. Clearly,

$$a = a^p - \frac{a^p - a}{p} \cdot p, \qquad a^p \cdot a^{p(p-2)} \equiv 1 \mod p^2. \tag{5}$$

Therefore,

$$a \equiv a^p\Big(1 - \frac{a^{p-1} - 1}{p} \cdot a^{(p-1)^2} \cdot p\Big) \equiv a^p\Big(1 - \frac{a^{p-1} - 1}{p} \cdot p\Big) \mod p^2. \tag{6}$$

The definition of the unit E_{p-1} and the equation $\omega^{p-1} = -p$ imply that

$$\begin{aligned} E_{p-1}^{(a^{p-1}-1)/p} &= (\exp \omega^{p-1})^{(a^{p-1}-1)/p)} \equiv 1 + \frac{a^{p-1} - 1}{p}\omega^{p-1} \\ &= 1 - \frac{a^{p-1} - 1}{p}p \mod p^2. \end{aligned}$$

Thus,

$$a \equiv a^p E_{p-1}^{(a^{p-1}-1)/p} \mod p^2. \tag{7}$$

Moreover, every principal unit ϵ in F such that $\epsilon \equiv 1 \mod p^2$ is a pth power. Combining this with (7), we obtain the congruence (4). □

4. Congruence for the second argument in (a, α)

Let

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \in \mathbb{Z}[\zeta], \tag{8}$$

where $a_i \in \mathbb{Z}$ and $\sum_{i=0}^{p-2} a_i \not\equiv 0 \mod p$. As above, we have $\underline{\alpha} := \underline{\alpha}(X) = a_0 + a_1X + \cdots + a_{p-2}X^{p-2}$.

Lemma 2. *In the field $F = \mathbb{Q}_p(\zeta)$, we have the congruence*

$$\alpha \equiv E_1^{c_1}E_2^{c_2}\dots E_p^{c_p} \mod F^{*^p}, \tag{9}$$

where $c_1 = \underline{\alpha}(1)^{p(p-2)} \cdot \underline{\alpha}'(1)$ and $c_2, c_3, \dots, c_p$ are integers.

Proof. We embed the ring $\mathbb{Z}[\zeta]$ in $\mathbb{Z}_p[\zeta]$ and, in the latter ring, consider the basis $1, \omega, \omega^2, \dots, \omega^{p-2}$, where $\omega^{p-1} = -p$. Then, taking into account the congruence $\omega \equiv \zeta - 1 \mod p$ and the expansion (8), we obtain the congruence

$$\alpha = b_0 + b_1\omega + b_2\omega^2 + \cdots + b_{p-2}\omega^{p-2}, \quad b_i \in \mathbb{Z}_p,$$

where $b_0 = \underline{\alpha}(1)$ and $b_1 = \underline{\alpha}'(1)$. As in Lemma 1 (see (6), (5)), we obtain the congruences

$$b_0 \equiv b_0^p\Big(1 + \frac{b_0^{p-1} - 1}{p}\omega^{p-1}\Big) \mod p^2,$$
$$b_i \equiv b_0^p(b_0^{p(p-2)}b_i) \mod p^2.$$

Consequently,

$$\alpha \equiv b_0^p\Big(1 + b_0^{p(p-2)}b_1\omega + \cdots + b_0^{p(p-2)}b_{p-2}\omega^{p-2} + \frac{b_0^{p-1} - 1}{p}\omega^{p-1}\Big) \mod p^2,$$

whence

$$\alpha = b_0^p(1 + b_0^{p(p-2)}b_1\omega)(1 + c\omega^2) \tag{10}$$

for some $c \in \mathbb{Z}_p[\omega]$.

From the congruence $\zeta \equiv 1 + \omega \mod \omega^2$, we easily deduce the relation

$$1 + b_0^{p(p-2)}b_1\omega \equiv \zeta^{b_0^{p(p-2)}b_1} = E_1^{b_0^{p(p-2)}b_1} \mod \omega^2.$$

Now, equation (10) yields the congruence

$$\alpha \equiv E_1^{c_1}E_2^{c_2}\dots E_p^{c_p} \mod F^{*p},$$

where $c_1 = b_0^{p(p-2)}b_1, c_2, \dots, c_p \in \mathbb{Z}$. To obtain (9), it remains to observe that $b_0 = \underline{\alpha}(1)$ and $b_1 = \underline{\alpha}'(1)$. □

5. Proof of Theorem 1

Using Lemmas 1 and 2 and Faddeev's relations (2), we obtain

$$(a, \alpha) = \zeta^d,$$

where $d = \frac{a^{p-1}-1}{p} \cdot \underline{\alpha}(1)^{p(p-2)}\underline{\alpha}'(1)$. By assumption, $\underline{\alpha}(1) \not\equiv 0 \mod p$. Therefore, the norm residue symbol (a, α) is trivial if and only if

$$\frac{a^{p-1} - 1}{p}\underline{\alpha}'(1) \equiv 0 \mod p.$$

Taking (3) into account, we complete the proof of Theorem 1. □

References

[E] G. Eisenstein, *Beweis des allgemeinsten Reziprozitaetsgesetze zwischen reellen und komplexen Zahlen*, Mathematische Werke. Band II, Chelsea, New York, 1975, pp. 189–198. MR0427030 (55:66b)

[F] D. K. Faddeev, *An explicit form of the Kummer–Takagi reciprocity law*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **1** (1966), 114–122; English transl., Sem. in Math. Steklov Math. Inst., Leningrad **1** (1968), 43–46. MR0219513 (36:2594)

[H] H. Hasse, *Zahlentheorie*, Akademie-Verlag, Berlin, 1963. MR0153659 (27:3621)

[V] S. V. Vostokov, *The reciprocity law in an algebraic number field*, Trudy Mat. Inst. Steklov. **148** (1978), 77–81; English transl. in Proc. Steklov Inst. Math. **1980**, no. 4 (148). MR0558942 (81a:12012)

Department of Mathematics and Mechanics, St. Petersburg State University, Universitetskiĭ Prospekt 28, Staryĭ Peterhof, St. Petersburg 198504, Russia

E-mail address: sergeivostokov@mail.ru

Received 23/MAY/2007

Translated by B. M. BEKKER