Arch. Math. 108 (2017), 233–240

0003-889X/17/030233-8
published online October 20, 2016
DOI 10.1007/s00013-016-0990-3

Archiv der Mathematik

A rational reciprocity law over function fields

Yoshinori Hamahata

Abstract. In the classical case, reciprocity laws for power residue symbols are called rational, which means that the power residue symbols only assume the values ± 1 and have entries in $\mathbb{Z}$. We establish a rational reciprocity law over function fields.

Mathematics Subject Classification. Primary 11A15; Secondary 11R58.

Keywords. Power residues, Rational reciprocity law, Function fields.

1. Introduction. Let us recall the reciprocity laws for power residue symbols in $\mathbb{Z}$. For distinct odd primes p and q, let $\left(\frac{p}{q}\right)_k$ be the k-th power residue symbol. For the quadratic residue symbol, it is well known that

$$\left(\frac{p}{q}\right)_2 \left(\frac{q}{p}\right)_2 = (-1)^{(p-1)(q-1)/4}.$$

Next, let p and q be distinct primes such that $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 4$. For such primes, there exist integers a, b, A, and B such that

$$\begin{aligned} p &= a^2 + b^2, \quad a \equiv 1 \pmod 2, \quad b \equiv 0 \pmod 2, \\ q &= A^2 + B^2, \quad A \equiv 1 \pmod 2, \quad B \equiv 0 \pmod 2. \end{aligned}$$

Burde [3] proved that if $\left(\frac{p}{q}\right)_2 = \left(\frac{q}{p}\right)_2 = 1$, then

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^{\frac{q-1}{4}} \left(\frac{aB - bA}{q}\right)_2. \tag{1.1}$$

For another proof for Burde's reciprocity law, see [5,7,9,14].

Brown [2] posed the problem of finding an octic reciprocity law, which is analogous to Burde's reciprocity law, for distinct primes p and q such that

$p \equiv 1 \pmod 8$ and $q \equiv 1 \pmod 8$. It is known that for such primes, there exist integers c, d, C, and D such that

$$p = c^2 + 2d^2, \quad c \equiv 1 \pmod 2, \quad d \equiv 0 \pmod 2,$$
$$q = C^2 + 2D^2, \quad C \equiv 1 \pmod 2, \quad D \equiv 0 \pmod 2.$$

Williams [13] proved that if $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$, then

$$\left(\frac{p}{q}\right)_8 \left(\frac{q}{p}\right)_8 = \left(\frac{aB - bA}{q}\right)_4 \left(\frac{cD - dC}{q}\right)_2. \tag{1.2}$$

Note that Helou [5] gave another proof for Williams' reciprocity law. The reciprocity laws mentioned above are rational, which means that their power residue symbols only assume the values ± 1 and have entries in $\mathbb{Z}$. For a survey on rational reciprocity laws, we refer to Lehmer [8]. For other types of reciprocity laws, we refer to [10].

As in the classical case, we define the k-th power residue symbol in function fields. Artin [1] established the quadratic reciprocity law, which was stated by Dedekind [4]. Schmidt [12] proved a more general reciprocity law over function fields. For the details of reciprocity laws over function fields, we refer to [11]. We are interested in polynomial rational reciprocity laws, which means that their power residue symbols only assume the values ± 1 and have entries in $\mathbb{F}_q[T]$. Hsu [6] established a rational quartic reciprocity law, which is an analog of Burde's reciprocity law. In this paper, to generalize Hsu's result, we establish a rational reciprocity law for the 2^n-th power residue symbol in function fields. Our reciprocity law includes an analog of those of Burde and Williams.

The remainder of this paper is organized as follows. In Section 2, we review the results on power residue symbols in function fields. In Section 3, we state the main theorem (Theorem 3). Finally, in Section 4, we prove Theorem 3.

2. Power residue symbols. Let q be a power of an odd prime, and let $\mathbb{F}_q$ be the finite field with q elements.

2.1. Power residue symbols. When discussing power residue symbols, we refer to [11]. Let r be a positive integer. Take a positive divisor d of $q^2 - 1$. First, we recall the definition of the d-th power residue symbol $\left(\frac{a}{P}\right)_{q^r,d}$. Let $P \in \mathbb{F}_{q^r}[T]$ be a monic irreducible element of degree $2k$, and let $a \in \mathbb{F}_{q^r}[T]$. If P does not divide a, then let $\left(\frac{a}{P}\right)_{q^r,d}$ be the unique element of $\mathbb{F}_{q^r} \setminus \{0\}$ such that

$$a^{\frac{q^{2k}-1}{d}} \equiv \left(\frac{a}{P}\right)_{q^r,d} \pmod P.$$

If P divides a, then let $\left(\frac{a}{P}\right)_{q^r,d} = 0$. When $d = 2$, this symbol is just like the Legendre symbol in the classical case. When $a \in \mathbb{F}_{q^r}$,

$$\left(\frac{a}{P}\right)_{q^r,d} = a^{\frac{q^r-1}{d} \deg P}. \tag{2.1}$$

For a non-zero $b = \beta Q_1^{e_1} Q_2^{e_2} \cdots Q_r^{e_r} \in \mathbb{F}_{q^r}[T]$ ($\beta \in \mathbb{F}_{q^r}$, $Q_1, Q_2, \ldots, Q_r \in \mathbb{F}_{q^r}[T]$ distinct monic irreducible polynomials), we define

$$\left(\frac{a}{b}\right)_{q^r,d} = \prod_{i=1}^{r} \left(\frac{a}{Q_i}\right)_{q^r,d}^{e_i}.$$

2.2. Representations of irreducible polynomials. Let P and Q be distinct monic irreducible polynomials in $\mathbb{F}_q[T]$ such that their degrees are even. Then P and Q decompose into the product of two distinct monic irreducible polynomials in $\mathbb{F}_{q^2}[T]$; in particular,

$$P = P_1 P_2, \quad P_1, P_2 \in \mathbb{F}_{q^2}[T], \quad \deg P_1 = \deg P_2 = \frac{1}{2}\deg P,$$
$$Q = Q_1 Q_2, \quad Q_1, Q_2 \in \mathbb{F}_{q^2}[T], \quad \deg Q_1 = \deg Q_2 = \frac{1}{2}\deg Q.$$

Let $\sigma \in \mathrm{Gal}\left(\mathbb{F}_{q^2}(T)/\mathbb{F}_q(T)\right)$ be the non-trivial automorphism. Set

$$A_1 = \frac{P_1 + P_2}{2}, \quad B_1 = \frac{P_1 - P_2}{\mathrm{sgn}(P_1 - P_2)}, \quad A_2 = \frac{Q_1 + Q_2}{2}, \quad B_2 = \frac{Q_1 - Q_2}{\mathrm{sgn}(Q_1 - Q_2)},$$

where $\mathrm{sgn}(P_1 - P_2)$ and $\mathrm{sgn}(Q_1 - Q_2)$ are the leading coefficients of $P_1 - P_2$ and $Q_1 - Q_2$, respectively. Because $\sigma(P_1 + P_2) = P_1 + P_2$, $\sigma(P_1 - P_2) = P_2 - P_1$, and $\sigma(\mathrm{sgn}(P_1 - P_2)) = \mathrm{sgn}(P_2 - P_1)$, A_1 and B_1 belong to $\mathbb{F}_q[T]$; similarly, A_2 and B_2 belong to $\mathbb{F}_q[T]$. Let $\alpha = \mathrm{sgn}(P_1 - P_2)/2$ and $\beta = \mathrm{sgn}(Q_1 - Q_2)/2$. Then it holds that $\alpha, \beta \in \mathbb{F}_{q^2} \backslash \{0\}$ and $\alpha^2, \beta^2 \in \mathbb{F}_q \backslash \mathbb{F}_q^2$, where $\mathbb{F}_q^2$ is the set of all square elements in $\mathbb{F}_q$. Using these notations, it follows that

$$P_1 = A_1 + \alpha B_1, \quad P_2 = A_1 - \alpha B_1, \quad \deg A_1 = \frac{1}{2}\deg P, \quad \deg B_1 < \frac{1}{2}\deg P, \tag{2.2}$$

$$Q_1 = A_2 + \beta B_2, \quad Q_2 = A_2 - \beta B_2, \quad \deg A_2 = \frac{1}{2}\deg Q, \quad \deg B_2 < \frac{1}{2}\deg Q. \tag{2.3}$$

When $q \equiv 3 \pmod 4$, $-\alpha^2$ and $-\beta^2$ are square elements in $\mathbb{F}_q$. Hence, there exist $\gamma, \delta \in \mathbb{F}_q$ such that $-\alpha^2 = \gamma^2$ and $-\beta^2 = \delta^2$. Let $C_1 = A_1, D_1 = \gamma B_1, C_2 = A_2$, and $D_2 = \delta B_2$. Then P and Q can be written as

$$P = C_1^2 + D_1^2, \quad Q = C_2^2 + D_2^2, \tag{2.4}$$

where $C_1, D_1, C_2, D_2 \in \mathbb{F}_q[T]$ with $\deg C_1 = \deg P/2$, $\deg D_1 < \deg P/2$, $\deg C_2 = \deg Q/2$, and $\deg D_2 < \deg Q/2$.

2.3. The rational quartic reciprocity law. We assume that $\left(\frac{P}{Q}\right)_{q,2} = 1$. Then the quartic residue symbol $\left(\frac{P}{Q}\right)_{q,4}$ is 1 or -1 depending on if $x^4 \equiv P \pmod Q$ is or is not solvable in $x \in \mathbb{F}_q[T]$. Hsu [6] proved an analog of Burde's reciprocity law (1.1).

Theorem 1 (The rational quartic reciprocity law [6]). *Let P and Q be distinct monic irreducible polynomials in $\mathbb{F}_q[T]$ of even degrees, and assume that $\left(\frac{P}{Q}\right)_{q,2} = \left(\frac{Q}{P}\right)_{q,2} = 1$.*

1. *If $q \equiv 1 \pmod 4$, then*
$$\left(\frac{P}{Q}\right)_{q,4}\left(\frac{Q}{P}\right)_{q,4} = 1.$$
2. *If $q \equiv 3 \pmod 4$, we express P and Q as in (2.4). Then*
$$\left(\frac{P}{Q}\right)_{q,4}\left(\frac{Q}{P}\right)_{q,4} = \left(\frac{\pm C_1D_2 \pm C_2D_1}{P}\right)_{q,2} = \left(\frac{\pm C_2D_1 \pm C_1D_2}{Q}\right)_{q,2}.$$

3. The main theorem. Let $n \geq 2$ and assume that q^2-1 is divisible by 2^n. Let P and Q be distinct monic irreducible polynomials in $\mathbb{F}_q[T]$ of even degrees. Furthermore, we assume that $\left(\frac{P}{Q}\right)_{q,2^{n-1}} = 1$. Then the 2^n-th power residue symbol $\left(\frac{P}{Q}\right)_{q,2^n}$ is 1 or -1 according to whether $x^{2^n} \equiv P \pmod Q$ is or is not solvable in $x \in \mathbb{F}_q[T]$.

To state the main theorem, we first need the following lemma.

Lemma 2. *Decompose P and Q into the product of two distinct monic irreducible polynomials in $\mathbb{F}_{q^2}[T]$ as follows:*
$$P = P_1P_2, \quad P_1, P_2 \in \mathbb{F}_{q^2}[T], \quad \deg P_1 = \deg P_2 = \frac{1}{2}\deg P,$$
$$Q = Q_1Q_2, \quad Q_1, Q_2 \in \mathbb{F}_{q^2}[T], \quad \deg Q_1 = \deg Q_2 = \frac{1}{2}\deg Q.$$
Then there exist $E_1, F_1, E_2, F_2 \in \mathbb{F}_q[T]$, and $\alpha \in \mathbb{F}_{q^2}\backslash\{0\}$ such that $\alpha^2 \in \mathbb{F}_q\backslash\mathbb{F}_q^2$,
$$P_1 = E_1 + \alpha F_1, \quad P_2 = E_1 - \alpha F_1, \quad \deg E_1 = \frac{1}{2}\deg P, \quad \deg F_1 < \frac{1}{2}\deg P, \tag{3.1}$$
$$Q_1 = E_2 + \alpha F_2, \quad Q_2 = E_2 - \alpha F_2, \quad \deg E_2 = \frac{1}{2}\deg Q, \quad \deg F_2 < \frac{1}{2}\deg Q. \tag{3.2}$$

Proof. We prove that for $\alpha, \beta \in \mathbb{F}_{q^2}\backslash\{0\}$ in (2.2) and (2.3), there exists $\epsilon \in \mathbb{F}_q\backslash\{0\}$ such that $\beta = \epsilon\alpha$. Because $\alpha \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$, $\{1, \alpha\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^2}$. Hence, there exist $\eta, \epsilon \in \mathbb{F}_q$ such that $\beta = \eta + \epsilon\alpha$. Raise both sides to the second power. Noting that $\alpha^2, \beta^2 \in \mathbb{F}_q$, we conclude that $\eta = 0$.

Setting $E_1 = A_1$, $F_1 = B_1$, $E_2 = A_2$, and $F_2 = \epsilon B_2$ yields the desired result. □

We now state the main theorem that is a rational reciprocity law for the 2^n-th power residue symbol.

Theorem 3. *Let P and Q be distinct monic irreducible elements in $\mathbb{F}_q[T]$ such that their degrees are even, and assume that $\left(\frac{P}{Q}\right)_{q,2^{n-1}} = \left(\frac{Q}{P}\right)_{q,2^{n-1}} = 1$. Then using the notations in (3.1) and (3.2), we have*

$$\begin{aligned}\left(\frac{P}{Q}\right)_{q,2^n}\left(\frac{Q}{P}\right)_{q,2^n} &= \left(\frac{\pm E_1F_2 \pm E_2F_1}{P}\right)_{q,2^n}^{q-1}\left(\frac{F_1}{P}\right)_{q,2^n}^{q-1}\left(\frac{F_1}{P}\right)_{q,2^{n-1}}^{q-1}\cdots\left(\frac{F_1}{P}\right)_{q,2^2}^{q-1}\\ &= \left(\frac{\pm E_2F_1 \pm E_1F_2}{Q}\right)_{q,2^n}^{q-1}\left(\frac{F_2}{Q}\right)_{q,2^n}^{q-1}\left(\frac{F_2}{Q}\right)_{q,2^{n-1}}^{q-1}\cdots\left(\frac{F_2}{Q}\right)_{q,2^2}^{q-1}.\end{aligned}$$

When $q \equiv 3 \pmod 4$, $-\alpha^2$ is a square element in $\mathbb{F}_q$. Hence, there exists $\gamma \in \mathbb{F}_q$ such that $-\alpha^2 = \gamma^2$. Let $G_1 = E_1, H_1 = \gamma F_1, G_2 = E_2$, and $H_2 = \gamma F_2$. Then P and Q can be written as

$$P = G_1^2 + H_1^2, \quad Q = G_2^2 + H_2^2, \tag{3.3}$$

where $G_1, H_1, G_2, H_2 \in \mathbb{F}_q[T]$ with $\deg G_1 = \deg P/2$, $\deg H_1 < \deg P/2$, $\deg G_2 = \deg Q/2$, and $\deg H_2 < \deg Q/2$. Noting that $\pm G_1H_2 \pm G_2H_2 = \gamma(\pm E_1F_2 \pm E_2F_1)$ and $\left(\frac{\gamma}{P}\right)^{q-1} = \left(\frac{\gamma}{Q}\right)^{q-1} = 1$, we have the following theorem.

Theorem 4. *Let P and Q be distinct monic irreducible elements in $\mathbb{F}_q[T]$ such that their degrees are even, and assume that $\left(\frac{P}{Q}\right)_{q,2^{n-1}} = \left(\frac{Q}{P}\right)_{q,2^{n-1}} = 1$. If $q \equiv 3 \pmod 4$, then, using the notations in (3.3), we have*

$$\begin{aligned}\left(\frac{P}{Q}\right)_{q,2^n}\left(\frac{Q}{P}\right)_{q,2^n} &= \left(\frac{\pm G_1H_2 \pm G_2H_1}{P}\right)_{q,2^n}^{q-1}\left(\frac{H_1}{P}\right)_{q,2^n}^{q-1}\left(\frac{H_1}{P}\right)_{q,2^{n-1}}^{q-1}\cdots\left(\frac{H_1}{P}\right)_{q,2^2}^{q-1}\\ &= \left(\frac{\pm G_2H_1 \pm G_1H_2}{Q}\right)_{q,2^n}^{q-1}\left(\frac{H_2}{Q}\right)_{q,2^n}^{q-1}\left(\frac{H_2}{Q}\right)_{q,2^{n-1}}^{q-1}\cdots\left(\frac{H_2}{Q}\right)_{q,2^2}^{q-1}.\end{aligned}$$

Remark 5.
1. We can derive Theorem 1 from the Theorems 3 and 4.
2. The case when $n = 3$ for Theorems 3 and 4 is an analog of Williams' reciprocity law (1.2).

4. Proof of Theorem 3. Because the finite field $\mathbb{F}_q[T]/(P)$ is isomorphic to $\mathbb{F}_{q^2}[T]/(P_i)$ via the map

$$\mathbb{F}_q[T]/(P) \to \mathbb{F}_{q^2}[T]/(P_i), \quad a \bmod P \mapsto a \bmod P_i,$$

we have $\left(\frac{Q}{P}\right)_{q,2^n} = \left(\frac{Q}{P_i}\right)_{q^2,2^n}$ $(i = 1, 2)$. Similarly, $\left(\frac{P}{Q}\right)_{q,2^n} = \left(\frac{P}{Q_i}\right)_{q^2,2^n}$ $(i = 1, 2)$. Hence, it holds that

$$\left(\frac{P}{Q}\right)_{q,2^n}\left(\frac{Q}{P}\right)_{q,2^n}=\left(\frac{P}{Q}\right)_{q,2^n}\left(\frac{Q}{P}\right)_{q,2^n}^{-1}=\left(\frac{P}{Q_1}\right)_{q^2,2^n}\left(\frac{Q}{P_1}\right)_{q^2,2^n}^{-1}$$
$$=\left(\frac{P_1}{Q_1}\right)_{q^2,2^n}\left(\frac{P_2}{Q_1}\right)_{q^2,2^n}\left(\frac{Q_1}{P_1}\right)_{q^2,2^n}^{-1}\left(\frac{Q_2}{P_1}\right)_{q^2,2^n}^{-1}$$
$$=\left(\frac{P_1}{Q_1}\right)_{q^2,2^n}\left(\frac{Q_1}{P_1}\right)_{q^2,2^n}^{-1}\left(\frac{P_2}{Q_1}\right)_{q^2,2^n}\left(\frac{Q_1}{P_2}\right)_{q^2,2^n}^{-1}$$
$$\left(\frac{Q_1}{P_2}\right)_{q^2,2^n}\left(\frac{Q_2}{P_1}\right)_{q^2,2^n}^{-1}.$$

We now use the following reciprocity law.

Theorem 6 (The d-th reciprocity law, cf. [11]). *Let d be a positive integer dividing q^2-1, and let P_1 and Q_1 be distinct monic irreducible polynomials in $\mathbb{F}_{q^2}[T]$. Then*

$$\left(\frac{P_1}{Q_1}\right)_{q^2,d}\left(\frac{Q_1}{P_1}\right)_{q^2,d}^{-1}=(-1)^{\frac{q^2-1}{d}\deg P_1\deg Q_1}.$$

Using Theorem 6,

$$\left(\frac{P}{Q}\right)_{q,2^n}\left(\frac{Q}{P}\right)_{q,2^n}=\left(\frac{Q_1}{P_2}\right)_{q^2,2^n}\left(\frac{Q_2}{P_1}\right)_{q^2,2^n}^{-1}=\left(\frac{Q_1}{\sigma(P_1)}\right)_{q^2,2^n}\left(\frac{\sigma(Q_1)}{P_1}\right)_{q^2,2^n}^{-1}.$$

Note that

$$\left(\frac{Q_1}{\sigma(P_1)}\right)_{q^2,2^n}=\sigma\Big(\left(\frac{\sigma(Q_1)}{P_1}\right)_{q^2,2^n}\Big)=\left(\frac{\sigma(Q_1)}{P_1}\right)_{q^2,2^n}^{q}.$$

Hence,

$$\left(\frac{P}{Q}\right)_{q,2^n}\left(\frac{Q}{P}\right)_{q,2^n}=\left(\frac{Q_2}{P_1}\right)_{q^2,2^n}^{q-1}.$$

Because

$$Q_2F_1\equiv(E_2-\alpha F_2)F_1\equiv E_1F_2+E_2F_1\pmod{P_1},$$

we have

$$\left(\frac{Q_2}{P_1}\right)_{q^2,2^n}=\left(\frac{Q_2F_1}{P_1}\right)_{q^2,2^n}\left(\frac{F_1^{2^n-1}}{P_1}\right)_{q^2,2^n}$$
$$=\left(\frac{E_1F_2+E_2F_1}{P}\right)_{q,2^n}\left(\frac{F_1}{P}\right)_{q,2^n}^{2^n-1}.$$

Noting that $2^n-1=1+2+\cdots+2^{n-1}$, we obtain

$$\left(\frac{Q_2}{P_1}\right)_{q^2,2^n}=\left(\frac{E_1F_2+E_2F_2}{P}\right)_{q,2^n}\left(\frac{F_1}{P}\right)_{q,2^n}\left(\frac{F_1}{P}\right)_{q,2^{n-1}}\cdots\left(\frac{F_1}{P}\right)_{q,2}.$$

Next, we prove the following lemma.

Lemma 7. *Let the assumptions be as in Theorem 3. For F_1 and F_2 in (3.1) and (3.2),*

$$\left(\frac{F_1}{P}\right)_{q,2} = \left(\frac{F_2}{Q}\right)_{q,2} = 1.$$

Proof. Let $c = \operatorname{sgn}(P_1 - P_2)$. Then

$$\begin{aligned}\left(\frac{F_1}{P}\right)_{q,2} &= \left(\frac{c}{P}\right)_{q^2,2}\left(\frac{P_1-P_2}{P}\right)_{q^2,2}\\ &= \left(\frac{c}{P}\right)_{q^2,2}\left(\frac{P_1-P_2}{P_1}\right)_{q^2,2}\left(\frac{P_1-P_2}{P_2}\right)_{q^2,2}\\ &= \left(\frac{c}{P}\right)_{q^2,2}\left(\frac{-1}{P}\right)_{q^2,2}\left(\frac{P_2}{P_1}\right)_{q^2,2}\left(\frac{P_1}{P_2}\right)_{q^2,2}.\end{aligned}$$

By (2.1) and Theorem 6, this becomes 1. Similarly, $\left(\frac{F_2}{Q}\right)_{q,2} = 1$. □

Using Lemma 7, it follows that

$$\left(\frac{P}{Q}\right)_{q,2^n}\left(\frac{Q}{P}\right)_{q,2^n} = \left(\frac{E_1F_2+E_2F_1}{P}\right)^{q-1}_{q,2^n}\left(\frac{F_1}{P}\right)^{q-1}_{q,2^n}\left(\frac{F_1}{P}\right)^{q-1}_{q,2^{n-1}}\cdots\left(\frac{F_1}{P}\right)^{q-1}_{q,2^2}. \tag{4.1}$$

Also, we have

$$\left(\frac{P}{Q}\right)_{q,2^n}\left(\frac{Q}{P}\right)_{q,2^n} = \left(\frac{P}{Q_2}\right)_{q^2,2^n}\left(\frac{Q}{P_1}\right)^{-1}_{q^2,2^n} = \left(\frac{Q_1}{P_1}\right)^{q-1}_{q^2,2^n}.$$

Because

$$Q_1F_1 \equiv (E_2+\alpha F_2)F_1 \equiv E_2F_1 - E_1F_2 \pmod{P_1},$$

a similar computation yields

$$\left(\frac{P}{Q}\right)_{q,2^n}\left(\frac{Q}{P}\right)_{q,2^n} = \left(\frac{E_2F_1-E_1F_2}{P}\right)^{q-1}_{q,2^n}\left(\frac{F_1}{P}\right)^{q-1}_{q,2^n}\left(\frac{F_1}{P}\right)^{q-1}_{q,2^{n-1}}\cdots\left(\frac{F_1}{P}\right)^{q-1}_{q,2^2}. \tag{4.2}$$

Because $\left(\frac{-1}{P}\right)^{q-1}_{q,2^n} = 1$, using (4.1) and (4.2), we have

$$\left(\frac{P}{Q}\right)_{q,2^n}\left(\frac{Q}{P}\right)_{q,2^n} = \left(\frac{\pm E_1F_2 \pm E_2F_1}{P}\right)^{q-1}_{q,2^n}\left(\frac{F_1}{P}\right)^{q-1}_{q,2^n}\left(\frac{F_1}{P}\right)^{q-1}_{q,2^{n-1}}\cdots\left(\frac{F_1}{P}\right)^{q-1}_{q,2^2}.$$

By symmetry of P and Q,

$$\left(\frac{P}{Q}\right)_{q,2^n}\left(\frac{Q}{P}\right)_{q,2^n} = \left(\frac{\pm E_2F_1 \pm E_1F_2}{Q}\right)^{q-1}_{q,2^n}\left(\frac{F_2}{Q}\right)^{q-1}_{q,2^n}\left(\frac{F_2}{Q}\right)^{q-1}_{q,2^{n-1}}\cdots\left(\frac{F_2}{Q}\right)^{q-1}_{q,2^2}.$$

□

Acknowledgments. This work was supported by JSPS KAKENHI Grant Number 15K04801.

References

[1] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen, Math. Z. **19** (1924), 153–246.

[2] E. Brown, Quadratic forms and biquadratic reciprocity, J. Reine Angew. Math. **253** (1972), 214–220.

[3] K. Burde, Ein rationales biquadratisches Reziprozitätsgesetz, J. Reine Angew. Math. **235** (1969), 175–184.

[4] R. Dedekind, Abriß einer Theorie der höheren Congruenzen in Bezug auf einen reellen Primzahl-Modulus, J. Reine Angew. Math. **54** (1857), 1–26.

[5] C. Helou, On rational reciprocity, Proc. Amer. Math. Soc. **108** (1990), 861–866.

[6] C.-H. Hsu, On polynomial reciprocity law, J. Number Theory **101** (2003), 13–31.

[7] E. Lehmer, On the quadratic character of some quadratic surds, J. Reine Angew. Math. **250** (1971), 42–48.

[8] E. Lehmer, Rational reciprocity laws, Amer. Math. Monthly **85** (1978), 467–472.

[9] F. Lemmermeyer, Rational quartic reciprocity, Acta Arithmetica **67** (1994), 387–390.

[10] F. Lemmermeyer, Reciprocity Laws From Euler to Einstein, Springer, Berlin, 2000.

[11] M. Rosen, Number Theory in Function Fields, Springer, New York, 2002.

[12] F.K. Schmidt, Zur Zahlentheorie in Körpern von der Charakteristik p, Sitzungsberichte Erlangen **58–59** (1928), 159–172.

[13] K. Williams, A rational octic reciprocity law, Pacific J. Math. **63** (1976), 563–570.

[14] K. Williams, K. Hardy, and C. Friesen, On the evaluation of the Legendre symbol $\left(\frac{A+B\sqrt{m}}{p}\right)$, Acta Arithmetica **45** (1985), 255–272.

Yoshinori Hamahata
Department of Applied Mathematics,
Okayama University of Science,
Ridai-cho 1-1,
Okayama 700–0005,
Japan
e-mail: hamahata@xmath.ous.ac.jp

Received: 9 September 2016