C. R. Math. Rep. Acad. Sci. Canada Vol. **39** (2) 2017, pp. 60–66

Polynomial Power Residue Symbols and q-resultants

Yoshinori Hamahata

Presented by Pierre Milman, FRSC

Abstract. We establish a relation between polynomial power residue symbols and q-resultants of $\mathbb{F}_q$-linear polynomials. We then establish the $q-1$-st power reciprocity law.

Résumé. On établit une relation entre le symbole de résidu de puissances en caractéristique p et le q-résultant de deux $\mathbb{F}_q$-polynômes linéaire. Alors on démontre la loi de réciprocité des puissances $q-1$-èmes.

1. **Introduction** The law of quadratic reciprocity, which was first proved by Gauss, states that for distinct odd primes p and q,

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

where $\left(\frac{p}{q}\right)$ is the Legendre symbol. Artin [1] established a polynomial analog of the quadratic reciprocity law, which was stated by Dedekind [5]. Schmidt [11] proved a more general reciprocity law over function fields. Carlitz [2] rediscovered this reciprocity law. He then gave another proof in [3, 4]. For details of the general reciprocity law over function fields, we refer to [10, 12]. Schmidt [11], Ore [9], and Hsu [7] established a relation between polynomial residue symbols and the resultants of polynomials over finite fields, and then proved the general reciprocity law. In this paper, we establish a relation between polynomial power residue symbols and q-resultants of $\mathbb{F}_q$-linear polynomials. We then establish the $q-1$-st power reciprocity law.

2. **Preliminaries** Let $A = \mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$, which denotes a finite field with q elements. Let $K = \mathbb{F}_q(T)$ denote the quotient field of A, and let $K_\infty = \mathbb{F}_q((1/T))$ be the completion of K at $\infty = (1/T)$. We write C_∞ for the completion of an algebraic closure of K_∞. Let A_+ denote the set of all monic elements of A. We remark that the number $q-1$, which is the order of the unit group of A, is analogous to 2, which is the order of the unit group of the integer ring $\mathbb{Z}$.

Received by the editors on March 17, 2016; revised May 22, 2016.
AMS Subject Classification: Primary: 11T55; secondary: 11A15, 11G09.
Keywords: Power residues, reciprocity law, function fields.

2.1. We recall the definition of the power residue symbol $\left\{\frac{a}{P}\right\}_d$. Take a positive divisor d of $q-1$. Let $P \in A$ be a monic irreducible element of degree k, and let $a \in A$. Then, if P does not divide a, then let $\left\{\frac{a}{P}\right\}_d$ be the unique element of $\mathbb{F}_q \setminus \{0\}$ such that

$$a^{\frac{q^k-1}{d}} \equiv \left\{\frac{a}{P}\right\}_d \pmod{P}.$$

If P divides a, then let $\left\{\frac{a}{P}\right\}_d = 0$. Let $b = \epsilon Q_1 \cdots Q_s \in A \setminus \{0\}$ ($\epsilon \in \mathbb{F}_q \setminus \{0\}, Q_1, \ldots, Q_s \in A_+$) be the irreducible decomposition of b. If $a \in A$, then let

$$\left\{\frac{a}{b}\right\}_d = \prod_{j=1}^{s} \left\{\frac{a}{Q_j}\right\}_d.$$

2.2. Let F be a field including $\mathbb{F}_q$. For $w_1, \ldots, w_n \in F$, the determinant

$$\Delta(w_1, \ldots, w_n) := \begin{vmatrix} w_1 & \cdots & w_n \\ w_1^q & \cdots & w_n^q \\ \vdots & & \vdots \\ w_1^{q^{n-1}} & \cdots & w_n^{q^{n-1}} \end{vmatrix}$$

is called the *Moore determinant*. Let $\tau = x^q$ and let $F\{\tau\}$ be the non-commutative ring in τ with the commutation rule $c^q\tau = \tau c$ ($c \in F$). For each $\mathbb{F}_q$-linear polynomial $P(x) = \sum_{i=0}^{n} a_i x^{q^i} \in F[x]$, we define $P(\tau) := \sum_{i=0}^{n} a_i \tau^i$, which is called the *$\tau$-polynomial* and belongs to $F\{\tau\}$. If $a_n \neq 0$, then we write $\deg_\tau P(\tau) = n$. For $f(\tau), g(\tau) \in F\{\tau\}$ with $\deg_\tau f(\tau) = n > 0$ and $\deg_\tau g(\tau) = m > 0$, let $\{w_1, \ldots, w_n\}$ and $\{\psi_1, \ldots, \psi_m\}$ be the $\mathbb{F}_q$-bases of the roots of $f(x)$ and $g(x)$, respectively. Then,

$$R_\tau(f(\tau), g(\tau)) := \frac{\Delta(w_1, \ldots, w_n, \psi_1, \ldots, \psi_m)}{\Delta(w_1, \ldots, w_n)\Delta(\psi_1, \ldots, \psi_m)}$$

is called the *q-resultant* of $f(\tau)$ and $g(\tau)$. This is the τ-analog of the resultant of polynomials (see [6, 8, 12] for further details). It holds that

$$R_\tau\left(f(\tau), g(\tau)\right) = (-1)^{mn} R_\tau\left(g(\tau), f(\tau)\right), \tag{2.1}$$

$$R_\tau\left(f(\tau), g(\tau)\right) = \frac{\Delta(f(\psi_1), \ldots, f(\psi_m))}{\Delta(\psi_1, \ldots, \psi_m)} = (-1)^{mn} \frac{\Delta(g(w_1), \ldots, g(w_n))}{\Delta(w_1, \ldots, w_n)}. \tag{2.2}$$

Note that for non-zero $f(\tau), g(\tau) \in F\{\tau\}$ with $\deg_\tau f(\tau) = 0$ and $\deg_\tau g(\tau) = m > 0$, $R_\tau\left(f(\tau), g(\tau)\right)$ can be defined as

$$R_\tau\left(f(\tau),g(\tau)\right)=R_\tau\left(g(\tau),f(\tau)\right)=\frac{\Delta(f(\psi_1),\dots,f(\psi_m))}{\Delta(\psi_1,\dots,\psi_m)}. \tag{2.3}$$

2.3. Let $D_0=1$ and $D_n=[n][n-1]^q\cdots[1]^{q^{n-1}}$ for $n>0$, where $[n]=T^{q^n}-T$. Let $e(z)$ be the *Carlitz exponential function* defined by

$$e(x)=\sum_{n=0}^{\infty}\frac{x^{q^n}}{D_n},$$

which is entire over C_∞. By definition, it holds that $de(x)/dx=e'(x)=1$. The map $e:C_\infty\to C_\infty$ is $\mathbb{F}_q$-linear and surjective. The kernel $L:=\mathrm{Ker}(e)$ is a free A-module of rank one. It is easy to see that $e(x)$ is L-periodic; that is, $e(x+l)=e(x)$ for $l\in L$. Let $\overline{\pi}$ denote a generator of L. For each $a\in A$, there exists a unique $\mathbb{F}_q$-polynomial $\rho_a(x)$ such that $\rho_a(e(x))=e(ax)$. The map $\rho:A\to C_\infty\{\tau\}$ $(a\mapsto\rho_a(\tau))$, which is an $\mathbb{F}_q$-linear ring homomorphism, is called the *Carlitz module*. It is known that $\rho_T(x)=Tx+x^q$. Hence, $\rho(A)$ is included in $K\{\tau\}$. For $a\in A$, $\deg_\tau\rho_a(\tau)$ is equal to the degree $\deg(a)$ of a.

3. The Main Theorem

The following is the main theorem of this paper.

THEOREM 1. *Let d be a positive divisor of $q-1$. For $a,b\in A\setminus\{0\}$,*

$$\left\{\frac{a}{b}\right\}_d=\mathrm{sgn}_d(b)^{-\deg(a)}\left(R_\tau\left(\rho_b(\tau),\rho_a(\tau)\right)\right)^{\frac{q-1}{d}},$$

where $\mathrm{sgn}_d(b)$ is the $(q-1)/d$ power of the leading coefficient $\mathrm{sgn}(b)$ of b.

This theorem yields the following reciprocity law.

THEOREM 2 ($q-1$-st power reciprocity law). *Let d be a positive divisor of $q-1$. For relatively prime $a,b\in A\setminus\{0\}$, it holds that*

$$\left\{\frac{a}{b}\right\}_d\left\{\frac{b}{a}\right\}_d^{-1}=(-1)^{\frac{q-1}{d}\deg(a)\deg(b)}\mathrm{sgn}_d(a)^{\deg(b)}\mathrm{sgn}_d(b)^{-\deg(a)}.$$

PROOF. Using (2.1), we have

$$\begin{aligned}\mathrm{sgn}_d(b)^{\deg(a)}\left\{\frac{a}{b}\right\}_d &= \left(R_\tau\left(\rho_b(\tau),\rho_a(\tau)\right)\right)^{\frac{q-1}{d}}\\ &= (-1)^{\frac{q-1}{d}\deg(a)\deg(b)}\left(R_\tau\left(\rho_a(\tau),\rho_b(\tau)\right)\right)^{\frac{q-1}{d}}\\ &= (-1)^{\frac{q-1}{d}\deg(a)\deg(b)}\mathrm{sgn}_d(a)^{\deg(b)}\left\{\frac{b}{a}\right\}_d.\end{aligned}$$

□

4. **Proof of Theorem 1** Let $\left\{\frac{a}{b}\right\} = \left\{\frac{a}{b}\right\}_{q-1}$. Because $\left\{\frac{a}{b}\right\}_d = \left\{\frac{a}{b}\right\}^{(q-1)/d}$, it suffices to prove that

$$\left\{\frac{a}{b}\right\} = \mathrm{sgn}(b)^{-\deg(a)} R_\tau\left(\rho_b(\tau), \rho_a(\tau)\right). \tag{4.1}$$

Let $\left(\frac{a}{b}\right)$ denote the right-hand side of (4.1).

4.1. First, we prove that if $a_1, a_2, b \in A \setminus \{0\}$, it holds that

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right). \tag{4.2}$$

When $a_1 a_2$ and b are not relatively prime, let P be an irreducible element of A such that P divides $a_1 a_2$ and b. We take an $\mathbb{F}_q$-basis $\eta_1, \ldots, \eta_l$ of the roots of $\rho_P(x)$, and extend this to generate the $\mathbb{F}_q$-bases $w_1, \ldots, w_n$ and $\psi_1, \ldots, \psi_m$ of the roots of $\rho_b(x)$ and $\rho_{a_1 a_2}(x)$, respectively. Then, by definition, we have $R_\tau(\rho_b(\tau), \rho_{a_1 a_2}(\tau)) = 0$, which implies that $\left(\frac{a_1 a_2}{b}\right) = 0$. Because P divides a_1 or a_2, a similar argument yields that $\left(\frac{a_1}{b}\right) = 0$ or $\left(\frac{a_2}{b}\right) = 0$. When $a_1 a_2$ and b are relatively prime, let $w_1, \ldots, w_n$ be an $\mathbb{F}_q$-basis of the roots of $\rho_b(x)$. Then, $\rho_{a_2}(w_1), \ldots, \rho_{a_2}(w_n)$ is also an $\mathbb{F}_q$-basis of the roots of $\rho_b(x)$. Then, using (2.2), we have

$$\begin{aligned}
R_\tau(\rho_b(\tau), \rho_{a_1 a_2}(\tau)) &= (-1)^{\deg b \deg a_1 a_2} \frac{\Delta(\rho_{a_1 a_2}(w_1), \ldots, \rho_{a_1 a_2}(w_n))}{\Delta(w_1, \ldots, w_n)} \\
&= (-1)^{\deg b \deg a_1} \frac{\Delta(\rho_{a_1}(\rho_{a_2}(w_1)), \ldots, \rho_{a_1}(\rho_{a_2}(w_n)))}{\Delta(\rho_{a_2}(w_1), \ldots, \rho_{a_2}(w_n))} \\
&\quad \times (-1)^{\deg b \deg a_2} \frac{\Delta(\rho_{a_2}(w_1), \ldots, \rho_{a_2}(w_n))}{\Delta(w_1, \ldots, w_n)} \\
&= R_\tau(\rho_b(\tau), \rho_{a_1}(\tau)) R_\tau(\rho_b(\tau), \rho_{a_2}(\tau)).
\end{aligned}$$

By combining this with the fact that

$$\mathrm{sgn}(b)^{-\deg(a_1 a_2)} = \mathrm{sgn}(b)^{-\deg(a_1)} \mathrm{sgn}(b)^{-\deg(a_2)},$$

we obtain (4.2).

4.2. Next, we prove that if $a \in A \setminus \{0\}$ and if $b = \epsilon Q_1 \cdots Q_s \in A \setminus \{0\}$ ($\epsilon \in \mathbb{F}_q \setminus \{0\}$, $Q_1, \ldots, Q_s \in A_+$) is the irreducible decomposition of b, then

$$\left(\frac{a}{b}\right) = \prod_{j=1}^{s} \left(\frac{a}{Q_j}\right). \tag{4.3}$$

By combining (2.2) with the argument presented in Subsection 4.1, it holds for $a, b_1, b_2 \in A \setminus \{0\}$ that

$$\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right).$$

For $\epsilon \in \mathbb{F}_q \setminus \{0\}$, using (2.3) to obtain that

$$\left(\frac{a}{\epsilon}\right) = \mathrm{sgn}(\epsilon)^{-\deg(a)} \cdot \mathrm{sgn}(\epsilon)^{\deg(a)} = 1.$$

Thus, we have proved (4.3).

4.3. Finally, we prove that for distinct monic irreducible $P, Q \in A$,

$$\left\{\frac{P}{Q}\right\} = \left(\frac{P}{Q}\right). \tag{4.4}$$

To do so, we will require the following lemma.

LEMMA 3 ([6], Corollary 1.3.7). *It holds that*

$$\Delta(w_1, \dots, w_n) = \prod_{i=1}^{n} \prod_{\epsilon_1, \dots, \epsilon_{i-1} \in \mathbb{F}_q} (w_i + \epsilon_{i-1} w_{i-1} + \cdots + \epsilon_1 w_1).$$

Let

$$\{w_1 = e(\overline{\pi}/Q), w_2 = e(\overline{\pi}T/Q), \dots, w_n = e(\overline{\pi}T^{n-1}/Q)\}$$

and

$$\{\psi_1 = e(\overline{\pi}/P), \psi_2 = e(\overline{\pi}T/P), \dots, \psi_m = e(\overline{\pi}T^{m-1}/P)\}$$

be the $\mathbb{F}_q$-bases of the roots of $\rho_Q(x)$ and $\rho_P(x)$, respectively. Then, using Lemma 3, we have that $R_\tau(\rho_Q(\tau), \rho_P(\tau))$ can be written as

$$\begin{aligned}
&\prod_{i=1}^{n} \prod_{\substack{\epsilon_1, \dots, \epsilon_{i-1}, \zeta_1, \dots, \zeta_m \in \mathbb{F}_q \\ (\zeta_1, \dots, \zeta_m) \neq (0, \dots, 0)}} (w_i + \epsilon_{i-1} w_{i-1} + \cdots + \epsilon_1 w_1 + \zeta_1 \psi_1 + \cdots + \zeta_m \psi_m) \\
&\quad = \prod_{\substack{M \in A_+ \\ \deg M < n}} \prod_{\substack{N \in A \setminus \{0\} \\ \deg N < m}} \{e(\overline{\pi}M/Q) + e(\overline{\pi}N/P)\} \\
&\quad = \prod_{\substack{M \in A_+ \\ \deg M < n}} \prod_{\substack{N \in A_+ \\ \deg N < m}} \prod_{\epsilon \in \mathbb{F}_q \setminus \{0\}} \{e(\overline{\pi}M/Q) - \epsilon e(\overline{\pi}N/P)\} \\
&\quad = \prod_{\substack{M \in A_+ \\ \deg M < n}} \prod_{\substack{N \in A_+ \\ \deg N < m}} \left\{e(\overline{\pi}M/Q)^{q-1} - e(\overline{\pi}N/P)^{q-1}\right\}.
\end{aligned}$$

Now, we recall that

$$\begin{aligned}\rho_P(x) &= \prod_{\substack{N\in A\\ \deg N<m}} (x - e(\overline{\pi}N/P)) \\ &= x \prod_{\substack{N\in A_+\\ \deg N<m}} \prod_{\epsilon\in\mathbb{F}_q\setminus\{0\}} (x - \epsilon e(\overline{\pi}N/P)) \\ &= x \prod_{\substack{N\in A_+\\ \deg N<m}} \left(x^{q-1} - e(\overline{\pi}N/P)^{q-1}\right).\end{aligned}$$

By substituting $x = e(\overline{\pi}M/Q)$ into the above polynomial, we obtain that

$$R_\tau(\rho_Q(\tau), \rho_P(\tau)) = \prod_{\substack{M\in A_+\\ \deg M<n}} \frac{e(\overline{\pi}PM/Q)}{e(\overline{\pi}M/Q)}.$$

To complete the proof, we require the following lemma.

Lemma 4 (Carlitz [3], (10.04)). *For distinct irreducible $P, Q \in A_+$, it holds that*

$$\left\{\frac{P}{Q}\right\} = \prod_{\substack{M\in A_+\\ \deg M<n}} \frac{e(\overline{\pi}PM/Q)}{e(\overline{\pi}M/Q)}.$$

By applying Lemma 4, (4.4) is proved. □

Acknowledgements

The author would like to thank the referee for valuable comments. 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. L. Carlitz, The arithmetic of polynomials in a Galois field, Amer. J. Math. **54** (1932), 39–50.
3. L. Carlitz, On a theorem of higher reciprocity, Bull. Amer. Math. Soc. **39** (1933), 155–160.
4. L. Carlitz, On certain functions connected with polynomials in a Galois field, Duke Math. J. **1** (1935), 137–168.
5. R. Dedekind, Abriss einer Theorie der höheren Congruenzen in Bezug auf einer reellen Primzahl-Modulus, J. Reine Angew. Math. **54** (1857), 1–26.
6. D. Goss, Basic Structures of Function Field Arithmetic, Springer, 1998.
7. C.-H. Hsu, On polynomial reciprocity law, J. Number Theory **101** (2003), 13–31.
8. O. Ore, On a special class of polynomials, Trans. Amer. Math. Soc. **35** (1933), 559–584.

9. O. Ore, Contributions to the theory of finite fields, Trans. Amer. Math. Soc. **36** (1934), 243–274.
10. M. Rosen, Number Theory in Function Fields, Springer, 2002.
11. F.K. Schmidt, Zur Zahlentheorie in Körper von der Charakteristik p, Erlanger Sitzungsberichte, **58**–**59** (1928), 159–172.
12. D. Thakur, Function Field Arithmetic, World Scientific, 2004.

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