Functiones et Approximatio
56.2 (2017), 211–216
doi: 10.7169/facm/1606

GAUSS' LEMMA OVER FUNCTION FIELDS

Yoshinori Hamahata

Abstract: We generalize the function field analog of Gauss' lemma for the application of power residue symbols. We then provide another proof of the general reciprocity law for power residue symbols.

Keywords: power residues, reciprocity law, function fields.

1. Introduction

Let p and q be distinct odd primes. Then

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

where $\left(\frac{p}{q}\right)$ is the Legendre symbol. This result is called the *quadratic reciprocity law*. To prove this law, Gauss utilized *Gauss' lemma*, which is as follows. Let l be an integer that is not divisible by a prime p. Consider the least positive residues mod p of the following $(p-1)/2$ multiples of l: $l, 2l, 3l, \ldots, \frac{p-1}{2}l$. If m is the number of such residues that exceed $p/2$, then

$$\left(\frac{l}{p}\right) = (-1)^m.$$

The analogies between number fields and function fields have many interesting aspects. Artin [1] established a function field analog of the quadratic reciprocity law, which was stated by Dedekind [6]. Schmidt [12] proved a more general reciprocity law over function fields. Carlitz [3, 4, 5] gave another proof of the general reciprocity law using an analog of Gauss' lemma. For details of the general reciprocity law over function fields, we refer to [11, 14]. Further another proof of the reciprocity law over function fields can be found in [2, 7, 8, 9, 10].

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

2010 Mathematics Subject Classification: primary: 11T55; secondary: 11A15, 11G09

In this paper, we expand upon the work of Carlitz and generalize Gauss' lemma over function fields for the application of power residue symbols. We then provide another proof of the general reciprocity law for power residue symbols.

2. Gauss' lemma

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.

Let d be a positive divisor of $q-1$, and let $P \in A_+$ be an irreducible element of degree k. If P does not divide $a \in A$, let $\{\frac{a}{P}\}_d$ be the unique element of $\mathbb{F}_q^*$ (the unit groups of $\mathbb{F}_q$) such that

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

If P divides a, let $\{\frac{a}{P}\}_d = 0$. The symbol $\{\frac{a}{P}\}_d$ is called the *d-th power residue symbol*. When $d = 2$, this symbol is analogous to the Legendre symbol.

Let d be a positive divisor of $q-1$. Set

$$H_d = \{\epsilon^d \mid \epsilon \in \mathbb{F}_q^*\},$$

which is a subgroup of $\mathbb{F}_q^*$ of order $(q-1)/d$. Let R_d be a set of coset representatives of H_d in $\mathbb{F}_q^*$. Let $P \in A_+$ be an irreducible element of degree k. Set

$$S_{d,P} = \{b \in A \setminus \{0\} \mid \deg b < k, \operatorname{sgn}(b) \in H_d\},$$

where $\operatorname{sgn}(b)$ is the leading coefficient of b. The cardinality of $S_{d,P}$ is $(q^k-1)/d$.

We are going to establish Gauss's lemma. Take $a \in A$ that is not divisible by P. For any $b \in S_{d,P}$, there exist unique $b' \in S_{d,P}$ and $\zeta_b \in R_d$ such that $ab \equiv \zeta_b b' \pmod{P}$. The map $f : S_{d,P} \to S_{d,P}$ defined by $b \mapsto b'$ is bijective. Indeed, there exists $c \in A$ such that $ac \equiv 1 \pmod{P}$. For any $b' \in S_{d,P}$, there exist $b'' \in S_{d,P}$ and $\zeta_{b'} \in R_d$ such that $cb' \equiv \zeta_{b'} b'' \pmod{P}$. Then, $ab'' \equiv \zeta_{b'}^{-1} b' \pmod{P}$, which implies that f is surjective. Hence, f is also injective. Therefore, we have

$$\begin{aligned} a^{(q^k-1)/d} \prod_{b\in S_{d,P}} b &\equiv \prod_{b\in S_{d,P}} ab \equiv \prod_{b\in S_{d,P}} \zeta_b b' \equiv \left(\prod_{b\in S_{d,P}} \zeta_b\right)\left(\prod_{b\in S_{d,P}} b'\right) \pmod{P} \\ &\equiv \left(\prod_{b\in S_{d,P}} \zeta_b\right)\left(\prod_{b\in S_{d,P}} b\right) \pmod{P}. \end{aligned}$$

Hence,

$$\left\{\frac{a}{P}\right\}_d \equiv a^{(q^k-1)/d} \equiv \prod_{b\in S_{d,P}} \zeta_b \pmod{P}.$$

Because $\left\{\frac{a}{P}\right\}_d$ and $\prod_{b\in S_{d,P}} \zeta_b$ are included in $\mathbb{F}_q^*$,

$$\left\{\frac{a}{P}\right\}_d = \prod_{b\in S_{d,P}} \zeta_b.$$

This establishes the following generalized Gauss's lemma.

Theorem 1 (Generalized Gauss' lemma). *Let $P \in A_+$ be an irreducible element. For $a \in A$ that is not divisible by P,*

$$\left\{\frac{a}{P}\right\}_d = \prod_{b\in S_{d,P}} \zeta_b.$$

Note that Carlitz [3] proved this theorem in the case when $d = q - 1$.

Example 2. Let $q = 5$. Then, $P = T + 1$ and $Q = T^2 + 2$ are monic irreducible elements in A.

(1) Let $d = 4$. Then, $H_4 = \{1\}$ and we can take $R_4 = \{1, 2, 3, 4\}$. We see that $S_{4,P} = \{1\}$ and $S_{4,Q} = \{T, T + 1, T + 2, T + 3, T + 4, 1\}$. Because $Q \cdot 1 \equiv 3 \cdot 1 \pmod P$, we have $\left\{\frac{Q}{P}\right\}_4 = 3$. Because

$$\begin{aligned} PT &\equiv 1(T + 3) \pmod Q, & P(T + 1) &\equiv 2(T + 2) \pmod Q,\\ P(T + 2) &\equiv 3T \pmod Q, & P(T + 3) &\equiv 4(T + 4) \pmod Q,\\ P(T + 4) &\equiv 2 \cdot 1 \pmod Q, & P \cdot 1 &\equiv 1(T + 1) \pmod Q, \end{aligned}$$

we have $\left\{\frac{P}{Q}\right\}_4 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 2 \cdot 1 = 3$.

(2) Let $d = 2$. Then, $H_2 = \{1, 4\}$ and we can take $R_2 = \{1, 3\}$. We see that $S_{2,P} = \{1, 4\}$ and $S_{2,Q} = \{T, T + 1, T + 2, T + 3, T + 4, 4T, 4T + 1, 4T + 2, 4T + 3, 4T + 4, 1, 4\}$. Because $Q \cdot 1 \equiv 3 \cdot 1 \pmod P$ and $Q \cdot 4 \equiv 3 \cdot 4 \pmod P$, we have $\left\{\frac{Q}{P}\right\}_2 = 3 \cdot 3 = 4$. Because

$$\begin{aligned} PT &\equiv 1(T + 3) \pmod Q, & P(T + 1) &\equiv 3(4T + 3) \pmod Q,\\ P(T + 2) &\equiv 3 \cdot 4T \pmod Q, & P(T + 3) &\equiv 1(4T + 1) \pmod Q,\\ P(T + 4) &\equiv 3 \cdot 4 \pmod Q, & P \cdot 1 &\equiv 1(T + 1) \pmod Q,\\ P \cdot 4T &\equiv 1(4T + 2) \pmod Q, & P(4T + 1) &\equiv 3 \cdot 1 \pmod Q,\\ P(4T + 2) &\equiv 1(T + 4) \pmod Q, & P(4T + 3) &\equiv 3T \pmod Q,\\ P(4T + 4) &\equiv 3(T + 4) \pmod Q, & P \cdot 4 &\equiv 1(4T + 4) \pmod Q, \end{aligned}$$

we have $\left\{\frac{P}{Q}\right\}_2 = 1 \cdot 3 \cdot 3 \cdot 1 \cdot 3 \cdot 1 \cdot 1 \cdot 3 \cdot 1 \cdot 3 \cdot 3 \cdot 1 = 4$.

3. The general reciprocity law

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

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

which is entire over C_∞. By definition, it holds that $de(z)/dz = e'(z) = 1$. 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 verify that $e(z)$ is L-periodic; that is, $e(z + l) = e(z)$ for $l \in L$. Let $\overline{\pi}$ be a generator of L.

In the classical case, for an integer l that is not divisible by a prime p,

$$\left(\frac{l}{p}\right) = \prod_{n=1}^{(p-1)/2} \frac{\sin 2\pi ln/p}{\sin 2\pi n/p}.$$

For the details of this result, see Serre [13]. This result has the following polynomial analog:

Theorem 3. *Let $P \in A_+$ be an irreducible element. For $a \in A$ that is not divisible by P,*

$$\left\{\frac{a}{P}\right\}_d = \prod_{b \in S_{d,P}} \frac{e\left(\overline{\pi}ab/P\right)}{e\left(\overline{\pi}b/P\right)}.$$

Proof. For any $b \in S_{d,P}$, there exist unique $b' \in S_{d,P}$ and $\zeta_b \in R_d$ such that $ab \equiv \zeta_b b' \pmod{P}$. Because P divides $ab - \zeta_b b'$, $e\left(\overline{\pi}(ab - \zeta_b b')/P\right) = 0$. Hence, $e\left(\overline{\pi}ab/P\right) = \zeta_b e\left(\overline{\pi}b'/P\right)$. Applying Theorem 1,

$$\left\{\frac{a}{P}\right\}_d = \prod_{b \in S_{d,P}} \frac{e\left(\overline{\pi}ab/P\right)}{e\left(\overline{\pi}b'/P\right)} = \prod_{b \in S_{d,P}} \frac{e\left(\overline{\pi}ab/P\right)}{e\left(\overline{\pi}b/P\right)}. \qquad \blacksquare$$

Note that Carlitz [5] proved this theorem in the case when $d = q - 1$. We will see that this theorem yields the following general reciprocity law.

Theorem 4 (The general reciprocity law). *Let P and Q be distinct irreducible element in A_+. Then it holds that*

$$\left\{\frac{Q}{P}\right\}_d = (-1)^{\frac{q-1}{d} \deg P \deg Q} \left\{\frac{P}{Q}\right\}_d.$$

Remark 5. Carlitz [3, 4, 5] proved Theorem 4 in the case when $d = q - 1$ and further proved Theorem 4 for any d by using the fact that $\left\{\frac{a}{P}\right\}_d = \left\{\frac{a}{P}\right\}_{q-1}^{(q-1)/d}$.

4. Proof of Theorem 4

To prove Theorem 4, we require the Carlitz module. Let $\overline{\pi}$ denote a generator of L. For each $a \in A$, there exists a unique $\mathbb{F}_q$-linear polynomial $\rho_a(z)$ such that

$$\rho_a(e(z)) = e(az). \tag{4.1}$$

Let $\tau = z^q$, and let $C_\infty\{\tau\}$ be the non-commutative ring in τ with the commutation rule $c^q\tau = \tau c$ $(c \in C_\infty)$. For each $\mathbb{F}_q$-linear polynomial $P(z) = \sum_{i=0}^{n} a_i z^{q^i} \in C_\infty[z]$, we define $P(\tau) := \sum_{i=0}^{n} a_i \tau^i$. 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 $\rho_T(z) = Tz + z^q$. Hence, for $a \in A \setminus \{0\}$, the degree of $\rho_a(z)$ is $q^{\deg a}$. Let $\deg P = k$ and $\deg Q = l$. From (4.1), we have

$$\rho_Q(z) = z \prod_{\substack{0 \neq c \in A \\ \deg c < l}} \left(z - e\left(\overline{\pi}c/Q\right)\right).$$

For this equality, refer to page 239 of Rosen [11]. Using $S_{d,Q}$ and R_d, $\rho_Q(z)$ can be written as

$$\rho_Q(z) = z \prod_{b \in S_{d,Q}} \prod_{\zeta \in R_d} \left(z - e\left(\overline{\pi}\zeta b/Q\right)\right) = z \prod_{b \in S_{d,Q}} \prod_{\zeta \in R_d} \left(z - \zeta \cdot e\left(\overline{\pi}b/Q\right)\right).$$

Note that

$$\prod_{\substack{\alpha \in H_d \\ \zeta \in R_d}} (X - \zeta\alpha) = X^{q-1} - 1 = \prod_{\alpha \in H_d} (X^d - \alpha).$$

Hence, $\rho_Q(z) = z \prod_{b \in S_{d,Q}} \left(z^d - e\left(\overline{\pi}b/Q\right)^d\right)$. Using Theorem 3,

$$\begin{aligned}
\left\{\frac{Q}{P}\right\}_d &= \prod_{b \in S_{d,P}} \frac{\rho_Q\left(e\left(\overline{\pi}b/P\right)\right)}{e\left(\overline{\pi}b/P\right)} = \prod_{b \in S_{d,P}} \prod_{c \in S_{d,Q}} \left(e\left(\overline{\pi}b/P\right)^d - e\left(\overline{\pi}c/Q\right)^d\right) \\
&= (-1)^{(q^k-1)(q^l-1)/d^2} \prod_{c \in S_{d,Q}} \prod_{b \in S_{d,P}} \left(e\left(\overline{\pi}c/Q\right)^d - e\left(\overline{\pi}b/P\right)^d\right) \\
&= (-1)^{(q^k-1)(q^l-1)/d^2} \left\{\frac{P}{Q}\right\}_d.
\end{aligned}$$

If q is even, then $(-1)^{(q^k-1)(q^l-1)/d^2} = 1 = (-1)^{\frac{q-1}{d}kl}$. If q is odd, then

$$\begin{aligned}
\frac{q^k-1}{d} \cdot \frac{q^l-1}{d} &\equiv \left(\frac{q-1}{d}\right)^2 \left(1 + q + \cdots + q^{k-1}\right)\left(1 + q + \cdots + q^{l-1}\right) \pmod 2 \\
&\equiv \left(\frac{q-1}{d}\right)^2 kl \equiv \frac{q-1}{d} kl \pmod 2.
\end{aligned}$$

Hence,

$$(-1)^{(q^k-1)(q^l-1)/d^2} = (-1)^{\frac{q-1}{d}kl}.$$

This completes the proof of the theorem. ■

Acknowledgements. The author would like to thank the referee for some suggestions to improve the readability of the original manuscript.

References

[1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*, Math. Z. **19** (1924), 153–246.
[2] A. Blaszczok, *An elementary proof of the d-th power reciprocity law over function fields*, Ann. Math. Silesianae **25** (2011), 49–57.
[3] L. Carlitz, *The arithmetic of polynomials in a Galois field*, Amer. J. Math. **54** (1932), 39–50.
[4] L. Carlitz, *On a theorem of higher reciprocity*, Bull. Amer. Math. Soc. **39** (1933), 155–160.
[5] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1** (1935), 137–168.
[6] R. Dedekind, *Abriss einer Theorie der höheren Congruenzen in Bezug auf einer reellen Primzahl-Modulus*, J. Reine Angew. Math. **54** (1857), 1–26.
[7] C.-H. Hsu, *On polynomial reciprocity law*, J. Number Theory **101** (2003), 13–31.
[8] C.-G. Ji and Y. Xue, *An elementary proof of the law of quadratic reciprocity over function fields*, Proc. Amer. Math. Soc. **136** (2008), 3035–3039.
[9] K. Merrill and H. Walling, *On quadratic reciprocity over function fields*, Pacific J. Math. **173** (1996), 147–150.
[10] O. Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. **36** (1934), 243–274.
[11] M. Rosen, *Number Theory in Function Fields*, Springer, 2002.
[12] F.K. Schmidt, *Zur Zahlentheorie in Körper von der Charakteristik p*, Erlanger Sitzungsberichte, **58–59** (1928), 159–172.
[13] J.-P. Serre, *Cours d'arithmétique*, Presses Univ. France, 1967.
[14] D. Thakur, *Function Field Arithmetic*, World Scientific, 2004.

Address: 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: 13 May 2016; **revised:** 23 August 2016