PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 9, September 2008, Pages 3035–3039
S 0002-9939(08)09327-1
Article electronically published on April 30, 2008

AN ELEMENTARY PROOF OF THE LAW OF QUADRATIC RECIPROCITY OVER FUNCTION FIELDS

CHUN-GANG JI AND YAN XUE

(Communicated by Wen-Ching Winnie Li)

Abstract. Let P and Q be relatively prime monic irreducible polynomials in $\mathbb{F}_q[T]\,(2 \nmid q)$. In this paper, we give an elementary proof for the following law of quadratic reciprocity in $\mathbb{F}_q[T]$:

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{|P|-1}{2}\frac{|Q|-1}{2}},$$

where $\left(\frac{Q}{P}\right)$ is the Legendre symbol.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements; for the sake of clarity we assume q is an odd prime power. Let $\mathbb{F}_q[T]$ be the ring of polynomials in one variable over the finite field $\mathbb{F}_q$. Every element in $\mathbb{F}_q[T]$ has the form

$$f(T) = a_nT^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0.$$

If $a_n \neq 0$, we say that f has degree n, notationally $\deg(f) = n$. In this case, let $sgn(f) = a_n$ and call this element of $\mathbb{F}_q^*$ the sign of f. If $sgn(f) = 1$, we say that f is a monic polynomial. It is sometimes useful to define the sign of the zero polynomial to be 0 and its degree to be $-\infty$. Let $A \in \mathbb{F}_q[T]$. If $A \neq 0$, set $|A| = q^{\deg(A)}$. If $A = 0$, set $|A| = 0$.

Let P be a monic irreducible polynomial in $\mathbb{F}_q[T]$ and $A \in \mathbb{F}_q[T]$. We define the Legendre symbol as follows:

$$\left(\frac{A}{P}\right) = \begin{cases} 1 & \text{if } A \text{ is a nonzero quadratic residue modulo } P, \\ 0 & \text{if } P \text{ divides } A, \\ -1 & \text{if } A \text{ is a nonzero quadratic nonresidue modulo } P. \end{cases}$$

Theorem (Quadratic Reciprocity Law)**.** *Let P and Q be relatively prime monic irreducible polynomials in $\mathbb{F}_q[T]$. Then*

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{|P|-1}{2}\frac{|Q|-1}{2}}.$$

Received by the editors July 6, 2007.
2000 *Mathematics Subject Classification.* Primary 11R58; Secondary 11A15.
Key words and phrases. Rational function fields, Legendre symbol, quadratic reciprocity law.
The first author is partially supported by grants No. 10771103 and 10201013 from NNSF of China and Jiangsu planned projects for postdoctoral research funds.

Over the years, many authors have produced proofs of the law of quadratic reciprocity. In 1857, Dedekind [4] stated that quadratic reciprocity holds over function fields. This was proved later by Artin [1]. In [6], Merrill and Walling used their inversion formula of the polynomial theta function to give another proof. In [2], Carlitz proved a more general reciprocity law for function fields which includes Dedekind's quadratic law as a special case. In another paper [3], Carlitz used the Carlitz exponential map to re-prove the polynomial reciprocity law. In [5], Keqin Feng and Linsheng Yin gave an elementary proof of the law of quadratic reciprocity in $\mathbb{F}_q[T]$. In this paper our main motivation is to prove the law of quadratic reciprocity over function fields in a more simple and direct way than others. We use purely number-theoretic tools, such as the Chinese Remainder Theorem.

2. Some lemmas

Lemma 1. *Let $P \in \mathbb{F}_q[T]$ be a monic irreducible polynomial and $A \in \mathbb{F}_q[T]$ be a polynomial not divisible by P. Then*

$$A^{|P|-1} \equiv 1 (\operatorname{mod} P).$$

Proof. See M. Rosen [7, Corollary of Proposition 1.8]. □

Lemma 2. *Let $P \in \mathbb{F}_q[T]$ be a monic irreducible polynomial and $A \in \mathbb{F}_q[T]$ be a polynomial not divisible by P. The congruence $x^2 \equiv A (\operatorname{mod} P)$ is solvable if and only if*

$$A^{\frac{|P|-1}{2}} \equiv 1 (\operatorname{mod} P).$$

There are $(|P|-1)/2$ nonzero quadratic residues modulo P.

Proof. This is a special case of Proposition 1.10 in M. Rosen [7]. □

Lemma 3. *The Legendre symbol $\left(\frac{A}{P}\right)$ has the following properties:*

(1) If $A \equiv B (\operatorname{mod} P)$, then $\left(\frac{A}{P}\right) = \left(\frac{B}{P}\right)$;
(2) $\left(\frac{AB}{P}\right) = \left(\frac{A}{P}\right)\left(\frac{B}{P}\right)$;
(3) If $P \nmid A$, then $\left(\frac{A}{P}\right) \equiv A^{\frac{|P|-1}{2}} (\operatorname{mod} P)$;
(4) If $a \in \mathbb{F}_q^*$, then $\left(\frac{a}{P}\right) \equiv a^{\frac{|P|-1}{2}} (\operatorname{mod} P)$.

Proof. The first assertion follows immediately from the definition. The second and the third follow from the definition, Lemma 1, and Lemma 2. The fourth assertion is a special case of the third. □

Lemma 4. *Let $P \in \mathbb{F}_q[T]$ be a monic irreducible polynomial. Then*

$$\prod_{0 \le \deg(f) < \deg(P)} f \equiv -1 (\operatorname{mod} P).$$

Proof. See M. Rosen [7, Corollary 2 of Proposition 1.9]. □

3. The proof of the theorem

Let $A \in \mathbb{F}_q[T]$ be a monic polynomial of degree greater than 0. Set

$$\begin{aligned}\mu(A) &= \{B \in \mathbb{F}_q[T] \,|\, 0 \le \deg(B) < \deg(A)\},\\ \mu_1(A) &= \{B \in \mu(A) \,|\, sgn(B) \in \mathbb{F}_q^{*2}\},\\ \mu_2(A) &= \{B \in \mu(A) \,|\, sgn(B) \notin \mathbb{F}_q^{*2}\}.\end{aligned}$$

Then

$$\#\mu(A) = |A| - 1, \quad \#\mu_1(A) = \frac{1}{2}(|A| - 1), \quad \#\mu_2(A) = \frac{1}{2}(|A| - 1).$$

Let P and Q be relatively prime monic irreducible polynomials in $\mathbb{F}_q[T]$. For each pair $(M, N) \in \mu(P) \times \mu_1(Q)$, by the Chinese Remainder Theorem, there exists a unique $K_{MN} \in \mu(PQ)$ satisfying

$$\begin{cases} K_{MN} \equiv M (\operatorname{mod} P), \\ K_{MN} \equiv N (\operatorname{mod} Q). \end{cases}$$

In particular, $(K_{MN}, PQ) = 1$.

Let (M, N) and (M_1, N_1) lie in $\mu(P) \times \mu_1(Q)$. If $(M, N) \ne (M_1, N_1)$, then $K_{MN} \ne K_{M_1N_1}$ and $K_{MN} \ne gK_{M_1N_1}$, where g is a generator of $\mathbb{F}_q^*$. On the other hand, if $K_{MN} = gK_{M_1N_1}$, then $N \equiv gN_1 (\operatorname{mod} Q)$. By $\deg(N) = \deg(gN_1) < \deg(Q)$, we have $N = gN_1$, which is a contradiction to the fact that $N, N_1 \in \mu_1(Q)$.

If $M \in \mu(P)$, $N \in \mu_1(Q)$, set

$$K^*_{MN} = \begin{cases} K_{MN} & \text{if } sgn(K_{MN}) \in \mathbb{F}_q^{*2}, \\ gK_{MN} & \text{if } sgn(K_{MN}) \notin \mathbb{F}_q^{*2}. \end{cases}$$

Then $\{K^*_{MN} \,|\, M \in \mu(P), N \in \mu_1(Q)\}$ denotes the set of all polynomials in $\mu_1(PQ)$ which are relatively prime with PQ. So

$$\prod_{\substack{M \in \mu(P) \\ N \in \mu_1(Q)}} K^*_{MN} = \prod_{\substack{A \in \mu_1(PQ) \\ (A, PQ) = 1}} A. \tag{1}$$

Let r denote the number of K_{MN} which are in $\mu_2(PQ)$. Then

$$\prod_{\substack{M \in \mu(P) \\ N \in \mu_1(Q)}} K^*_{MN} = g^r \prod_{\substack{M \in \mu(P) \\ N \in \mu_1(Q)}} K_{MN}. \tag{2}$$

By (1) and (2), we have

$$\prod_{\substack{A \in \mu_1(PQ) \\ (A, PQ) = 1}} A = g^r \prod_{\substack{M \in \mu(P) \\ N \in \mu_1(Q)}} K_{MN}. \tag{3}$$

From

$$\prod_{\substack{A\in\mu_1(PQ)\\(A,PQ)=1}} A=\prod_{\substack{A\in\mu_1(PQ)\\(A,P)=1}} A/\prod_{\substack{B\in\mu_1(PQ)\\Q|B,\,(B,P)=1}} B,$$

$$\prod_{\substack{A\in\mu_1(PQ)\\(A,P)=1}} A\equiv\prod_{A\in\mu_1(P)} A\cdot\Big(\prod_{K\in\mu(P)} K\Big)^{\frac{|Q|-1}{2}}\equiv\prod_{A\in\mu_1(P)} A\cdot(-1)^{\frac{|Q|-1}{2}}\,(\operatorname{mod} P)$$

and

$$\prod_{\substack{B\in\mu_1(PQ)\\Q|B,\,(B,P)=1}} B\equiv\prod_{A\in\mu_1(P)}(QA)\equiv Q^{\frac{|P|-1}{2}}\prod_{A\in\mu_1(P)} A\equiv\left(\frac{Q}{P}\right)\prod_{A\in\mu_1(P)} A\,(\operatorname{mod} P),$$

we have

$$\prod_{\substack{A\in\mu_1(PQ)\\(A,PQ)=1}} A\equiv(-1)^{\frac{|Q|-1}{2}}\left(\frac{Q}{P}\right)(\operatorname{mod} P).\tag{4}$$

Similarly,

$$\prod_{\substack{A\in\mu_1(PQ)\\(A,PQ)=1}} A\equiv(-1)^{\frac{|P|-1}{2}}\left(\frac{P}{Q}\right)(\operatorname{mod} Q).\tag{5}$$

On the other hand,

$$g^r\prod_{\substack{M\in\mu(P)\\N\in\mu_1(Q)}} K_{MN}\equiv g^r\Big(\prod_{M\in\mu(P)} M\Big)^{\frac{|Q|-1}{2}}\equiv g^r(-1)^{\frac{|Q|-1}{2}}(\operatorname{mod} P),\tag{6}$$

$$\begin{aligned}g^r\prod_{\substack{M\in\mu(P)\\N\in\mu_1(Q)}} K_{MN}&\equiv g^r\Big(\Big(\prod_{N\in\mu_1(Q)} N\Big)^2\Big)^{\frac{|P|-1}{2}}\equiv g^r\Big(g^{-\frac{|Q|-1}{2}}\prod_{N\in\mu(Q)} N\Big)^{\frac{|P|-1}{2}}\\&\equiv g^r g^{-\frac{|Q|-1}{2}\frac{|P|-1}{2}}(-1)^{\frac{|P|-1}{2}}(\operatorname{mod} Q).\end{aligned}\tag{7}$$

From (3), (4), (6), we have

$$\left(\frac{Q}{P}\right)=g^r.$$

From (3), (5), (7), we have

$$\left(\frac{P}{Q}\right)=g^r g^{-\frac{|P|-1}{2}\frac{|Q|-1}{2}}.$$

Hence

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=g^{-\frac{|P|-1}{2}\frac{|Q|-1}{2}}=(-1)^{\frac{|P|-1}{2}\frac{|Q|-1}{2}}.$$

This completes the proof of the theorem.

References

[1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen, I, II*, Math. Z. **19** (1924), 153-246. MR1544651, MR1544652

[2] L. Carlitz, *The arithmetic of polynomials in a Galois field*, Amer. J. Math. **54** (1932), 39-50. MR1506871

[3] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1** (1935), 137-168. MR1545872

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

[5] Ke Qin Feng and Linsheng Yin, *An elementary proof of the law of quadratic reciprocity in* $\mathbb{F}_q(T)$, Sichuan Daxue Xuebao, Special Issue **26** (1989), 36-40. MR1059674 (91i:11178)

[6] K. D. Merrill and L. H. Walling, *On quadratic reciprocity over function fields*, Pacific J. Math. **173** (1996), 147-150. MR1387795 (97a:11011)

[7] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657 (2003d:11171)

Department of Mathematics, Nanjing Normal University, Nanjing 210097, People's Republic of China

E-mail address: cgji@njnu.edu.cn

Department of Mathematics, Nanjing Normal University, Nanjing 210097, People's Republic of China

E-mail address: xueyan1981521@163.com