ON QUADRATIC RECIPROCITY OVER FUNCTION FIELDS

KATHY DONOVAN MERRILL AND LYNN WALLING
ON QUADRATIC RECIPROCITY OVER FUNCTION FIELDS

KATHY D. MERRILL AND LYNNE H. WALLING

A proof of quadratic reciprocity over function fields is given using the inversion formula of the theta function.

Over the years, many authors have produced proofs of the law of quadratic reciprocity. In 1857, Dedekind [2] stated that quadratic reciprocity holds over function fields; this was later proved by Artin [1]. One of the simplest proofs over the rational numbers relies on the functional equation of the classical theta function (see, for example, [3]); this technique was later generalized by Hecke [4] to number fields. In this note we use an analogous technique to give a simple and direct proof of quadratic reciprocity over rational function fields. We thank David Grant for suggesting this application of Theorem 2.3 of [6].

The reader is referred to [5] for a more complete discussion of the history of the Law of Quadratic Reciprocity.

Let \( F = F_\mathfrak{p} \) be a finite field with \( \mathfrak{p} \) elements; for the sake of clarity we assume \( \mathfrak{p} \) is an odd prime. Let \( T \) be an indeterminate, and set \( A = F[T] \). Then for \( \alpha, \beta \in A \) with \( \alpha \) irreducible, let

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

We will show that for \( \alpha, \beta \in A \) distinct monic irreducible polynomials,

\[
\left( \frac{\beta}{\alpha} \right) = \begin{cases} 
\left( \frac{-1}{\mathfrak{p}} \right) \left( \frac{\alpha}{\beta} \right) & \text{if } \deg \alpha, \deg \beta \text{ are both odd,} \\
\left( \frac{\alpha}{\beta} \right) & \text{otherwise.}
\end{cases}
\]

We require the following definitions.

Let \( K = F(T) \); let \( K_\infty \) denote the completion of \( K \) with respect to the “infinite” valuation \( | \cdot |_\infty \) given by \( |\alpha/\beta|_\infty = \mathfrak{p}^{\deg \alpha - \deg \beta} \) where \( \alpha, \beta \in A \). (We adopt the convention that \( \deg 0 = -\infty \), and hence \( |0|_\infty = 0 \).) One easily sees that \( K_\infty = F \left( \left( \frac{1}{T} \right) \right) \), formal Laurent series in \( \frac{1}{T} \); for \( x \in K_\infty \), we write \( x = \sum_{j=-\infty}^{n} x_j T^j \). The “unit ball” or “ring of integers” in \( K_\infty \) is
\( \mathcal{O}_\infty = \{ x \in K_\infty : |x|_\infty \leq 1 \} = F[[\frac{1}{T}]] \), formal Taylor series in \( \frac{1}{T} \). Set \( G = \text{PSL}_2(K_\infty) \); then the maximal compact subgroup of \( G \) (with respect to the standard topology induced on \( G \) by \( | \cdot |_\infty \)) is \( \text{PSL}_2(\mathcal{O}_\infty) \). Thus we set

\[ H = \text{PSL}_2(K_\infty)/\text{PSL}_2(\mathcal{O}_\infty). \]

We can view \( \text{PSL}_2(*) \) as a subgroup of \( \text{PGL}_2(*) \); so we consider a matrix of \( \text{PSL}_2(*) \) equivalent to every nonzero scalar multiple of the matrix. Then as shown in [6],

\[ \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} : y = T^{2m}, \ m \in \mathbb{Z}, \ x \in T^{2m+1}A \right\} \]

is a complete set of representatives for \( H \). For each \( z \equiv \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \in H \), set

\[ \theta(z) = \sum_{\delta \in A} \chi_{\mathcal{O}_\infty} ((T\delta)^2 y) e \{ (T\delta)^2 x \} \]

where \( e\{ \gamma \} = e \{ \sum_{j \geq 0} \gamma_j T^j \} = \exp(2\pi i \gamma_1/p) \) and \( \chi_{\mathcal{O}_\infty} \) is the characteristic function for \( \mathcal{O}_\infty \).

As in the classical setting, we will connect this theta series to quadratic reciprocity through Gauss sums. Accordingly, for \( \alpha, \beta \in A \) with \( \alpha \) irreducible and \( \alpha \) not dividing \( \beta \), define the Gauss sum \( G_\alpha(\beta) \) to be \( G_\alpha(\beta) = \sum_{\delta \in A/\alpha A} e \{ \beta \delta^2 T^2 / \alpha \} \).

**Lemma 1.** For \( \alpha, \beta \in A \) with \( \alpha \) irreducible and \( \alpha \nmid \beta \), \( \left( \frac{\beta}{\alpha} \right) = \frac{G_\alpha(\beta)}{G_\alpha(1)}. \)

**Proof.** We have

\[ G_\alpha(\beta) = \sum_{\delta \in A/\alpha A} \left( 1 + \left( \frac{\delta}{\alpha} \right) \right) e \{ \beta \delta^2 T^2 / \alpha \} = \sum_{\delta \in A} \left( \frac{\delta}{\alpha} \right) e \{ \beta \delta^2 T^2 / \alpha \} \]

and for \( \beta' \in A \) such that \( \beta \beta' \equiv 1 \pmod{\alpha} \)

\[ = \sum_{\delta \in A/\alpha A} \left( \frac{\delta \beta'}{\alpha} \right) e \{ \beta \delta \beta'T^2 / \alpha \} = \left( \frac{\beta'}{\alpha} \right) G_\alpha(1) = \left( \frac{\beta}{\alpha} \right) G_\alpha(1). \]

**Lemma 2.** For \( \alpha, \beta \) relatively prime irreducible polynomials, \( G_\alpha(\beta)G_\beta(\alpha) = G_{\alpha \beta}(1). \)

**Proof.** Notice that the map \( (\delta + \alpha \beta A, \ \gamma + \alpha \beta A) \mapsto \delta + \gamma + \alpha \beta A \) is an injective homomorphism from \( (\beta A/\alpha A) \times (\alpha A/\alpha \beta A) \) into \( A/\alpha \beta A \); since the cardinalities of the domain and the codomain are finite and equal, the map is an
isomorphism. Also notice that for $\delta \in \beta A$ and $\gamma \in \alpha A$, $e\{(\delta + \gamma)^2T^2/\alpha \beta\} = e\{\delta^2T^2/\alpha \beta\} e\{\gamma^2T^2/\alpha \beta\}$. Thus

$$G_{\alpha \beta}(1) = \sum_{\delta \in A/\alpha A} e\{(\beta \delta)^2T^2/\alpha \beta\} \sum_{\gamma \in A/\beta A} e\{(\alpha \delta)^2T^2/\alpha \beta\} = G_\alpha(\beta)G_\beta(\alpha).$$

Combining these two lemmata, we have that for $\alpha, \beta$ relatively prime irreducible polynomials, $(\frac{\alpha}{\beta}) (\frac{\beta}{\alpha}) = \frac{G_{\alpha \beta}(1)}{G_\alpha(1)G_\beta(1)}$. Thus for formulate the law of Quadratic Reciprocity, we need only evaluate $G_\gamma(1)$ for $\alpha \in A$. This is the content of our final lemma.

**Lemma 3.** For any $\gamma \in A$, $G_\gamma(1) = p^{d} \left( \frac{\gamma_d}{p} \right)^{d} \sqrt{\left( \frac{-1}{p} \right)^{d}}$ where $d = \deg \gamma$ and $\gamma_d$ denotes the coefficient of $T^d$ in $\gamma$.

**Proof.** First notice that by the Euclidean Algorithm, $\{\delta \in A : \deg \delta < d\}$ is a complete set of representatives for $A/\gamma A$. Thus

$$G_\gamma(1) = \sum_{\delta \in A} \chi_\delta ((T\delta)^2T^{-2d}) e\{((T\delta)^2/\gamma)\}.$$

Letting $z = \left( \begin{array}{cc} T^{-2d} & \frac{1}{\gamma} \\ 0 & 1 \end{array} \right)$, we see that $G_\gamma(1) = \theta(z)$ where $\theta(z)$ is as in [6]. By the Inversion Formula, we have $\theta(z) = p^{\frac{d}{2}} \left( \frac{\gamma_d}{p} \right)^{d} \sqrt{\left( \frac{-1}{p} \right)^{d}} \theta \left( \frac{-1}{z} \right)$ where $-\frac{1}{z} = \left( \begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right) z \equiv \left( \begin{array}{cc} 1 & -\gamma \\ 0 & 1 \end{array} \right)$. Since the only $\delta \in A$ satisfying $\chi_\delta ((T\delta)^2) = 1$ is $\delta = 0$, $\theta(-\frac{1}{z}) = 1$. □

These Lemmata easily imply the following

**Theorem.** Let $\alpha, \beta$ be relatively prime irreducible polynomials of degrees $d$ and $d'$ respectively. Then

$$\left( \frac{\alpha}{\beta} \right) = \epsilon \left( \frac{\alpha_d}{p} \right)^{d'} \left( \frac{\beta_{d'}}{p} \right)^{d} \left( \frac{\beta}{\alpha} \right)$$

where

$$\epsilon = \begin{cases} \left( \frac{-1}{p} \right) & \text{if } d, d' \text{ are both odd,} \\ 1 & \text{otherwise.} \end{cases}$$
In particular, when $\alpha$ and $\beta$ are distinct monic irreducible polynomials,

$$
\left( \frac{\alpha}{\beta} \right) = \begin{cases} 
\left( \frac{-1}{p} \right) \left( \frac{\beta}{\alpha} \right) & \text{if } d, d' \text{ are both odd}, \\
\left( \frac{\beta}{\alpha} \right) & \text{otherwise}.
\end{cases}
$$

References


Received September 27, 1993 and revised March 25, 1994. The second author was partially supported by NSF grant DMS 9103303.

COLORADO COLLEGE
COLORADO SPRINGS, CO 80903
*E-mail address*: merrill@cc.colorado.edu

AND

UNIVERSITY OF COLORADO
BOULDER, CO 80309-0426
*E-mail address*: walling@euclid.colorado.edu
Isometric immersions of $H^n_1$ into $H^{n+1}_1$

Kinetsu Abe

Rotationally symmetric hypersurfaces with prescribed mean curvature

Marie-Françoise Bidaut-Veron

The covers of a Noetherian module

Jian-Jun Chuai

On the odd primary cohomology of higher projective planes

Mark Foskey and Michael David Slack

Unit indices of some imaginary composite quadratic fields. II

Mikihiro Hirabayashi

Mixed automorphic vector bundles on Shimura varieties

Min Ho Lee

Trace ideal criteria for Toeplitz and Hankel operators on the weighted Bergman spaces with exponential type weights

Peng Lin and Richard Rochberg

On quadratic reciprocity over function fields

Kathy Donovan Merrill and Lynne Walling

$(A_2)$-conditions and Carleson inequalities in Bergman spaces

Takahiko Nakazi and Masahiro Yamada

A note on a paper of E. Boasso and A. Larotonda: “A spectral theory for solvable Lie algebras of operators”

C. Ott

Tensor products with anisotropic principal series representations of free groups

Carlo Pensavalle and Tim Steger

On Ricci deformation of a Riemannian metric on manifold with boundary

Ying Shen

The Weyl quantization of Poisson $SU(2)$

Albert Jeu-Liang Sheu

Weyl’s law for $SL(3, \mathbb{Z}) \setminus SL(3, \mathbb{R})/SO(3, \mathbb{R})$

Eric George Stade and Dorothy Irene Wallace (Andreoli)

Minimal hyperspheres in two-point homogeneous spaces

Per Tomter

Subalgebras of little Lipschitz algebras

Nikolai Isaac Weaver