PACIFIC JOURNAL OF MATHEMATICS
Vol. 173, No. 1, 1996

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 $\mathbf{F} = \mathbf{F}_p$ be a finite field with p elements; for the sake of clarity we assume p is an odd prime. Let T be an indeterminate, and set $\mathbf{A} = \mathbf{F}[T]$. Then for $\alpha, \beta \in \mathbf{A}$ with α 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 $\alpha, \beta \in \mathbf{A}$ distinct monic irreducible polynomials,

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

We require the following definitions.

Let $\mathbf{K} = \mathbf{F}(T)$; let $\mathbf{K}_\infty$ denote the completion of $\mathbf{K}$ with respect to the "infinite" valuation $|\cdot|_\infty$ given by $|\alpha/\beta|_\infty = p^{\deg\alpha - \deg\beta}$ where $\alpha, \beta \in \mathbf{A}$. (We adopt the convention that $\deg 0 = -\infty$, and hence $|0|_\infty = 0$.) One easily sees that $\mathbf{K}_\infty = \mathbf{F}\left(\left(\frac{1}{T}\right)\right)$, formal Laurent series in $\frac{1}{T}$; for $x \in \mathbf{K}_\infty$, we write $x = \sum_{j=-\infty}^{n} x_j T^j$. The "unit ball" or "ring of integers" in $\mathbf{K}_\infty$ is

$\mathcal{O}_\infty = \{x \in \mathbf{K}_\infty : |x|_\infty \le 1\} = \mathbf{F}\left[\left[\frac{1}{T}\right]\right]$, formal Taylor series in $\frac{1}{T}$. Set $G = PSL_2(\mathbf{K}_\infty)$; then the maximal compact subgroup of G (with respect to the standard topology induced on G by $|\cdot|_\infty$) is $PSL_2(\mathcal{O}_\infty)$. Thus we set

$$\mathbf{H} = PSL_2(\mathbf{K}_\infty)/PSL_2(\mathcal{O}_\infty).$$

We can view $PSL_2(*)$ as a subgroup of $PGL_2(*)$; so we consider a matrix of $PSL_2(*)$ equivalent to every nonzero scalar multiple of the matrix. Then as shown in [**6**],

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

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

$$\theta(z) = \sum_{\delta \in \mathbf{A}} \chi_{\mathcal{O}_\infty}\left((T\delta)^2 y\right) e\left\{(T\delta)^2 x\right\}$$

where $e\{\gamma\} = e\left\{\sum_{j \ge N} \gamma_j T^j\right\} = \exp(2\pi i \gamma_1/p)$ 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 $\alpha, \beta \in \mathbf{A}$ with α irreducible and α not dividing β, define the Gauss sum $G_\alpha(\beta)$ to be $G_\alpha(\beta) = \sum_{\delta \in \mathbf{A}/\alpha\mathbf{A}} e\left\{\beta\delta^2 T^2/\alpha\right\}$.

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

Proof. We have

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

and for $\beta' \in \mathbf{A}$ such that $\beta\beta' \equiv 1 \pmod{\alpha}$

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

□

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

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

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

$\square$

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

Lemma 3. *For any $\gamma \in \mathbf{A}$, $G_\gamma(1) = p^{\frac{d}{2}}\left(\frac{\gamma_d}{p}\right)^d\sqrt{\left(\frac{-1}{p}\right)^d}$ where $d = \deg\gamma$ and γ_d denotes the coefficient of T^d in γ.*

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

$$G_\gamma(1) = \sum_{\delta\in\mathbf{A}} \chi_{\mathcal{O}_\infty}\left((T\delta)^2T^{-2d}\right) e\{(T\delta)^2/\gamma\}.$$

Letting $z = \begin{pmatrix} T^{-2d} & \frac{1}{\gamma} \\ 0 & 1 \end{pmatrix}$, 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 $-\frac{1}{z} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z \equiv \begin{pmatrix} 1 & -\gamma \\ 0 & 1 \end{pmatrix}$. Since the only $\delta \in \mathbf{A}$ satisfying $\chi_{\mathcal{O}_\infty}((T\delta)^2) = 1$ is $\delta = 0$, $\theta(-\frac{1}{z}) = 1$. $\square$

These Lemmata easily imply the following

Theorem. *Let α, β 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

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

In particular, when α and β 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

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

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

[3] H. Dym and H.P. McKean, *Fourier Series and Integrals*, Academic Press, New York, 1972.

[4] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer-Verlag, New York-Heidelberg-Berlin, 1981.

[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York-Berlin-Heidelberg-London-Paris-Tokyo-Hong Kong, 1990.

[6] K.D. Merrill and L.H. Walling, *Sums of squares over function fields*, Duke Math. J., **71(3)** (1993), 665-684.

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