PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 125, Number 5, May 1997, Pages 1299–1303
S 0002-9939(97)03748-9

# A NOTE ON THE RELATIVE CLASS NUMBER IN FUNCTION FIELDS

MICHAEL ROSEN

(Communicated by William W. Adams)

Abstract. Let $F$ be a finite field, $A = F[T]$, and $k = F(T)$. Let $K_m = k(\Lambda_m)$ be the field extension of $k$ obtained by adjoining the $m$-torsion on the Carlitz module. The class number $h_m$ of $K_m$ can be written as a product $h_m = h_m^+ h_m^-$. The number $h_m^-$ is called the relative class number. In this paper a formula for $h_m^-$ is derived which is the analogue of the Maillet determinant formula for the relative class number of the cyclotomic field of $p$-th roots of unity. Some consequences of this formula are also derived.

Let $\mathbf{Q}$ denote the rational numbers and consider the cyclotomic field $K_p = \mathbf{Q}(\zeta_p)$ with class number $h_p$. It is well known that this class numbers factors as a product $h_p^+ h_p^-$ of two integers. The number $h_p^+$ is the class number of the maximal real subfield of $K_p$. The integer $h_p^-$ is called the relative class number. In [Ca] and [Ca-O] it is shown how the relative class number can be computed in terms of a certain classical determinant known as the Maillet determinant. A nice exposition of this is given in Chapter 3 of [L] (see Theorem 7.1).

In this note we will give an analogue of this material in the context of cyclotomic function fields. Let $F$ be a finite field with $q$ elements and $A = F[T]$ the polynomial ring over $F$. Let $k = F(T)$ be the quotient field of $A$. For an irreducible polynomial $m$ of degree $d$ we will denote by $\Lambda_m$ the $m$-torsion on the Carlitz module and let $K_m = k(\Lambda_m)$ be the "cyclotomic" function field obtained by adjoining the elements of $\Lambda_m$ to $k$. For the definition of the Carlitz module and its properties see [H] and [G-R]. The class number of $K_m$, $h_m$, factors as a product of two integers $h_m = h_m^+ h_m^-$, where $h_m^+$ is the class number of the "maximal real" subfield of $K_m$, i.e. the decomposition field of the prime at infinity of $k$ in $K_m$, and $h_m^-$ is called the relative class number. Our aim is to give an expression for $h_m^-$ as a product of certain easily computed determinants related to the classical Maillet determinant.

We begin by recalling the analytic class number formula for $h_m^-$ which follows immediately from Theorem 2 of [G-R]. A character $\chi$ of $(A/mA)^*$ is said to be *real* if its restriction to $F^*$ is the trivial character. Otherwise it is said to be *non-real* or *imaginary*. If $\chi$ is imaginary, define $S(\chi) = \sum_a \chi(a)$, where the sum is over all monic polynomials of degree less than $d$. Then,

$$h_m^- = \prod_{\chi \text{ imaginary}} S(\chi). \tag{1}$$

Received by the editors July 2, 1995 and, in revised form, November 15, 1995.
1991 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R58, 14H05.
This work was partially supported with a grant from the National Science Foundation.

Let $t = (q^d - 1)/(q-1)$. Then $t$ is the size of the set $\mathcal{M}$ of monic polynomials of degree less than $d$. We construct a $t \times t$ matrix $[c(a,b)]$ where $a, b \in \mathcal{M}$. Namely, for $a, b \in \mathcal{M}$ write $ab = sm + r$, where $s, r \in A$ and either $r = 0$ or $\deg(r) < d$. In fact, $r$ cannot be zero since we have assumed that $m$ is irreducible. Define $c(a,b)$ to be the leading coefficient of $r$. By construction, the matrix $[c(a,b)]$ has all its coefficients in $F^*$. Let $\lambda$ be a character of $F^*$ and define

$$d(\lambda) = \det[\lambda(c(a,b))].$$

**Theorem 1.**

$$h_m^- = \pm \prod_{\lambda \neq \lambda_o} d(\lambda)\,,$$

*where the product is over all the non-trivial characters $\lambda$ of $F^*$.*

*Proof.* The proof proceeds by a step by step rewriting of equation (1). Let $\lambda$ be any non-trivial character of $F^*$, and set

$$h_\lambda = \prod_{\chi|_{F^*} = \lambda} S(\chi).$$

From equation (1) we see that

$$h_m^- = \prod_{\lambda \neq \lambda_o} h_\lambda. \tag{2}$$

Let $\phi$ be a fixed character whose restriction to $F^*$ is $\lambda$. Then all the characters whose restriction to $F^*$ is $\lambda$ can be written $\phi\chi'$, where $\chi'$ is a real character. Note that a real character can also be thought of as a character of the group $G = (A/mA)^*/F^*$. We'll come back to this in a moment.

Starting with a non-trivial character $\lambda$ on $F^*$ we construct a function $\tilde{\lambda}$ on $(A/mA)^*$ as follows. Let $a$ be a polynomial prime to $m$. Write $a = sm + r$ with $s, r \in A$ and $\deg(r) < d$. Define $\tilde{\lambda}(a)$ to be $\lambda$ evaluated on the inverse of the leading coefficient of $r$. Then $\tilde{\lambda}$ is a well defined function on $(A/mA)^*$.

We rewrite $h_\lambda$ using the quantities just defined:

$$h_\lambda = \prod_{\chi|_{F^*} = \lambda} \sum_{a \text{ monic, } \deg(a) < d} \chi(a)$$

$$= \prod_{\chi'} \sum_{a \text{ monic, } \deg(a) < d} \chi'(a)\phi(a)\tilde{\lambda}(a).$$

Observe that the function $\phi(a)\tilde{\lambda}(a)$ is unchanged if we replace $a$ by $\alpha a$ where $\alpha$ is a constant. It is also unchanged if we replace $a$ by anything in the congruence class of $a$ modulo $m$. Thus the summation in the above sum can be rewritten as a summation over all the elements of the group $G = (A/mA)^*/F^*$. We obtain

$$h_\lambda = \prod_{\chi'} \sum_{a \in G} \chi'(a) \left[\phi(a)\tilde{\lambda}(a)\right].$$

We apply the Dedekind determinant formula (see [L], Theorem 6.1) to derive

$$h_\lambda = \det \left[\phi(b^{-1}a)\tilde{\lambda}(b^{-1}a)\right].$$

Here, $a$ and $b$ vary over the elements of the group $G$. Replacing $b^{-1}$ by $b$ merely permutes the rows of the matrix, and so,

$$h_\lambda = \pm \det \left[\phi(b)\phi(a)\tilde{\lambda}(ba)\right]. \tag{3}$$

We have used the fact that $\phi$ is a character. Each element of the $b'$th row of the determinant in equation (3) contains $\phi(b)$ as a factor. Similarly, each element of the $a'$th column contains $\phi(a)$ as a factor. By elementary properties of determinants, it follows that

$$h_\lambda = \pm\, \phi(\prod_{a\in G} a)^2 \det \left[\tilde{\lambda}(ab)\right].$$

The product of all the elements in an abelian group is equal to the product of all the elements of order two. Thus,

$$\phi(\prod_{a\in G} a)^2 = (\pm 1)^2 = 1,$$

and so,

$$h_\lambda = \pm \det \left[\tilde{\lambda}(ab)\right] = \pm d(\lambda^{-1}). \tag{4}$$

The last equality is obtained by letting $a$ and $b$ once again run through all the monic polynomials of degree less than $d$ and simply using the definition of $\tilde{\lambda}$. From equations (2) and (4) the proof of the theorem is immediate. □

I would like to thank David Goss for suggesting that the following result should hold.

**Theorem 2.** *Let $[c(a,b)]$ be the matrix introduced in the remarks preceding Theorem 1. Then, the relative class number $h_m^-$ is divisible by $p$, the characteristic of $F$, if and only if there is an integer $i$, $1 \le i \le q-2$, such that* $\det[c(a,b)^i] = 0$ .

*Proof.* We have to reinterpret equation (2) first $p$-adically and then, after reduction mod $p$, as an equality in the ring $A/mA$.

Let $\zeta$ be a complex primitive $(q^d-1)$st root of unity and set $E = \mathbf{Q}(\zeta)$. Let $\mathcal{O}$ be the ring of integers in $E$. $E$ is unramified at all primes above $p$. Let $\mathcal{P}$ be a fixed such prime and let $\hat{\mathcal{O}}$ be the completion of $\mathcal{O}$ at $\mathcal{P}$. Using the natural imbedding of $\mathcal{O}$ in $\hat{\mathcal{O}}$ we can (and do) interpret equation (2) as holding in $\hat{\mathcal{O}}$. Now, the residue class field, $\kappa$, of $\hat{\mathcal{O}}$ is a finite field with $q^d$ elements and so is isomorphic to $A/mA$. Let $\rho : \kappa \to A/mA$ be such an isomorphism. Finally, let $r$ denote reduction modulo $\hat{\mathcal{P}}$ on $\hat{\mathcal{O}}$. Applying the composed map $\rho \circ r$ to both sides of equation (2), we see that $p$ divides $h_m^-$ if and only if $\rho \circ r(h_\lambda) = 0$ in $A/mA$ for some complex character $\lambda$ of $F^*$.

Let $\lambda$ be any complex character of $F^*$, and define $\tilde{\lambda} = \rho \circ r \circ \lambda$. Then $\tilde{\lambda}$ is a character on $F^*$ with values in the $(q-1)$st roots of unity in $(A/mA)^*$, i.e. in $F^*$. It is easy to see that the multiplicative maps from $F^*$ to itself consist of precisely the powers of the identity map under pointwise product. Now, apply the homomorphism $\rho \circ r$ to both sides of equation (4). We find

$$\rho \circ r(h_\lambda) = \pm d(\rho \circ r \circ \lambda^{-1}) = \pm \det(c(a,b)^i),$$

where $i$ is some index between 1 and $q-2$. This proves the theorem. □

*Remark 1.* It is undoubtedly true that Theorem 2 can be refined so that the vanishing of $\det[c(a,b)^i]$ can be related to the $p$-divisibility of the order of the "$i$th piece" of the class group. See [G-S] for an explanation of how to decompose the class group into pieces corresponding to powers of the Teichmüller character. We shall not enter into this here.

As in [Ca], [Ca-O], and [L], it is possible to use Theorem 1 to give an upper bound for $h_m^-$.

**Theorem 3.** *As above, let $m \in A$ be an irreducible polynomial of degree $d$ and define $t = q^d - 1/(q-1)$. We have*

$$h_m^- \leq \sqrt{t}^{\,t\,(q-2)} < (2q)^{\frac{d-1}{2}q^d}. \tag{5}$$

*Proof.* We apply the Hadamard determinant inequality which states that the absolute value of the determinant of a complex square matrix is less than or equal to the product of the lengths of the row vectors which compose the matrix. Since all the entries of $[\lambda(c(a,b))]$ have absolute value 1, we find that $|d(\lambda)| \leq \sqrt{t}^{\,t}$. The first inequality follows from this and equation (2). As for the second inequality, note that the exponent $t(q-2) < q^d - 1 < q^d$. Also, note that $t = q^{d-1} + q^{d-2} + \ldots + 1 < 2q^{d-1}$. These two observation yield the second inequality. □

It is interesting to compare the inequalities of Theorem 3 with those obtained from the congruence Riemann hypothesis. Recall that $h_m^- = h_m/h_m^+$. It follows from the theory of algebraic curves over finite fields and the congruence Riemann hypothesis that there are complex numbers $\pi_i$ of absolute value $\sqrt{q}$ such that

$$h_m^- = \prod_{i=1}^{2g-2g^+} (1 - \pi_i)\,. \tag{6}$$

Here, $g$, resp. $g^+$, is the genus of the field $K_m$, resp. $K_m^+$. The only primes of $k$ which ramify in $K_m$ are $(m)$ and $\infty$. The prime $(m)$ is totally ramified of degree $d$, whereas $\infty$ splits into $t$ primes each with ramification index $q-1$ and degree 1. By Riemann-Hurwitz one deduces that

$$2g - 2 = (d-1)q^d + 1 - 2d - t.$$

See [H] for more details and the case of general $m$. In $K_m^+$ only $(m)$ is ramified, and it is totally ramified. It follows that

$$2g^+ - 2 = (d-2)t - d.$$

Subtracting these equations, we find that

$$2g - 2g^+ = (d-1)q^d + O\left(q^{d-1}\right). \tag{7}$$

The error term is an explicit polynomial in $q$ whose leading term is $(1-d)q^{d-1}$, so for large $d$ the error term makes a negative contribution.

Combining equations (6) and (7) and using the very coarse inequality $\sqrt{q} + 1 < 2\sqrt{q}$, we deduce that

$$h_m^- < (\sqrt{q}+1)^{2g-2g^+} < (4q)^{g-g^+}. \tag{8}$$

Equations (7) and (8) yield

$$\log_q(h_m^-) < \left(1 + \frac{\log(4)}{\log q}\right)\frac{d-1}{2}q^d + O\left(q^{d-1}\right),$$

whereas the elementary methods used in proving Theorem 3 (see equation (5)) give the result

$$\log_q(h_m^-) < \left(1 + \frac{\log(2)}{\log(q)}\right) \frac{d-1}{2} q^d,$$

which is surprisingly good.

We conclude with two more remarks.

*Remark 2.* Throughout this paper we have been concerned with the class numbers associated to the fields $K_m$ and $K_m^+$. It is also of interest to consider the class numbers of the rings $\mathcal{O}_m$ and $\mathcal{O}_m^+$ which are the integral closures of $A$ in $K_m$ and $K_m^+$ respectively. Call these class numbers $h(\mathcal{O}_m)$ and $h(\mathcal{O}_m^+)$. It can be shown that the second of these numbers divides the first. Call the ratio $h(\mathcal{O}_m)^-$. This is the relative class number on the level of rings. The following relationship holds:

$$h(\mathcal{O}_m)^- = (q-1)^{1-t} h_m^-.$$

For a proof of this, in a more general setting, see [R].

The upshot is that Theorem 1 provides a formula for $h(\mathcal{O}_m)^-$ as well as $h_m^-$. Also, Theorem 2 gives a criterion for $p$-divisiblity of both of these numbers.

*Remark 3.* The "cyclotomic" construction of ray class fields of $k = F(T)$ due to Carlitz has been extended to arbitrary global function fields by V.G. Drinfeld and D.R. Hayes. Using Hayes' normalized rank one Drinfeld modules, L. Shu [S] has developed analytic class number formulas for the generalization of the relative class numbers $h_m^-$. Using these, she is has been able to extend Theorems 1 and 2 to this setting. Her paper is in preparation.

## References


[Ca] L. Carlitz, *A generalization of Maillet's determinant and a bound for the first factor of the class number*, Proc. AMS **12** (1961), 256–261. MR **22:**12093

[Ca-O] L. Carlitz and F.R. Olson, *Maillet's Determinant*, Proc. AMS **6** (1955), 265–269. MR **16:**999d

[G-R] S. Galovich and M. Rosen, *The Class Number of Cyclotomic Function Fields*, J. of Number Theory 13, No. 3 (1981), 363–375. MR **83m:**12022

[G-S] D. Goss and W. Sinnott, *Class-groups of Function Fields*, Duke Math. J. 52, No. 2 (1985), 507–516. MR **87b:**11118

[H] D. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91. MR **48:**8444

[L] S. Lang, *Cyclotomic Fields*, Springer Verlag, New York-Heidelberg-Berlin, GTM 59, 1978. MR **58:**5578

[R] M. Rosen, *The Hilbert class field in function fields*, Exposition. Math. **5** (1987), 365–378. MR **89b:**10094

[S] L. Shu, *Narrow ray class fields and partial zeta functions*, pre-print, 1995.



Department of Mathematics, Brown University, Providence, Rhode Island 02912-0001

*E-mail address*: ma408000@brownvm.brown.edu