JOURNAL OF NUMBER THEORY 13, 363–375 (1981)

The Class Number of Cyclotomic Function Fields*

STEVEN GALOVICH

Department of Mathematics, Carleton College,
Northfield, Minnesota 55057

AND

MICHAEL ROSEN

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

Communicated by J. W. S. Cassels

Received January 11, 1980; revised March 4, 1980

Let k be a rational function field over a finite field. Carlitz and Hayes have described a family of extensions of k which are analogous to the collection of cyclotomic extensions $\{Q(\zeta_m) | \ m \geqslant 2\}$ of the rational field Q. We investigate arithmetic properties of these "cyclotomic function fields." We introduce the notion of the maximal real subfield of the cyclotomic function field and develop class number formulas for both the cyclotomic function field and its maximal real subfield. Our principal result is the analogue of a classical theorem of Kummer which for a prime p and positive integer n relates the class number of $Q(\zeta_{p^n} + \zeta_{p^n}^{-1})$, the maximal real subfield of $Q(\zeta_{p^n})$, to the index of the group of cyclotomic units in the full unit group of $Z[\zeta_{p^n}]$.

1. Introduction

On the basis of the work of Carlitz dating back to the 1930s [2, 3], Hayes [5] recently developed an "explicit" class field theory for a field of rational functions, k, over a finite field. Briefly, he describes a collection of finite abelian extensions of k with the property that any finite abelian extension of k is a subfield of one of the fields in the given collection. This result is a characteristic p analogue of the classical Kronecker–Weber theorem, which states that any abelian extension of the field of rational numbers, Q, is a subfield of a cyclotomic field $Q(w_n)$, w_n being a primitive nth root of unity.

* This work was completed while the authors were on sabbatical at the University of California, Berkeley. The second author was supported by a grant from the Vaughn Foundation.

0022-314X/81/030363–13$02.00/0

Thus we refer to the fields constructed by Carlitz and Hayes as "cyclotomic function fields."

In this paper we consider a certain class of cyclotomic function fields (described in Section 2). Within each field in this class, we distinguish a subfield which plays a role analogous to that played by the maximal real subfield of the classical cyclotomic field $Q(w_n)$. Our purpose is to study arithmetic properties of this "maximal real subfield." One highlight is the development of closed class number formulas for both the cyclotomic function field and its maximal real subfield. The class number of the latter field appears as a factor of the class number of the former, just as in the classical case the class number of the maximal real subfield divides the class number of the cyclotomic field itself via the plus–minus decomposition [6, Chap. 3]. Our other results are direct parallels of classical theorems, the principal one (Theorem 3) being that the class number of the ring of integers of the maximal real subfield equals the index in the unit group of this ring of the subgroup generated by roots of unity and by certain "cyclotomic units." The classical version of this theorem was proved by Kummer in the middle of the 19th century.

2. Cyclotomic Function Fields

We begin with a quick review of the work of Carlitz and Hayes. First we fix some notation. For a ring R, let R^* denote the unit group of R. If R is a Dedekind domain, then $C(R)$ will denote the divisor (ideal) class group. Let k be a field of rational functions over a finite field $\mathbb{F}_q$ with q elements. Fix a generator T of k so that $k = \mathbb{F}_q(T)$ and let $R_T = \mathbb{F}_q[T]$. Let ∞ denote the prime divisor of k corresponding to the pole of T. For example, note that for $g \in R_T$, $\text{ord}_\infty(g) = -\deg(g)$. The other prime divisors of k are in one-to-one correspondence with the monic prime polynomials of k. For such a prime polynomial Q, we let (Q) represent the corresponding prime divisor. We also write $\mathscr{M}_n$ for the set of monic polynomials in R_T of degree less than n. Finally let k^{ac} denote an algebraic closure of k.

Carlitz [2, 3] showed that k^{ac} becomes a module over R_T under the following action: For $u \in k^{ac}$ and $M = M(T) \in R_T$, define

$$u^M = M(\varphi + \mu)(u),$$

where $\varphi : k^{ac} \to k^{ac}$ is the Frobenius automorphism, $\varphi(u) = u^q$, and $\mu : k^{ac} \to k^{ac}$ is multiplication by T, $\mu(u) = Tu$. In particular, $u^T = u^q + Tu$. It is easy to check that $(M, u) \mapsto u^M$ endows k^{ac} with an R_T-module structure. Carlitz also established the following results.

(1) If $\deg(M)=d$, then

$$u^M=\sum_{i=0}^{d}\begin{bmatrix}M\\ i\end{bmatrix}u^{q^i},$$

where $[{}^{M}_{i}]$ is a polynomial in R_T of degree $(d-i)q^i$. In addition $[{}^{M}_{0}]=M$ and $[{}^{M}_{d}]$ is the leading coefficient of M.

(2) u^M is a separable polynomial in u of degree q^d. Thus Λ_M, the set of roots of $u^M=0$ or, equivalently, the set of M-torsion points of k^{ac} under the given R_T-action, contains q^d elements. Moreover, as an R_T-module, $\Lambda_M=R_T/(M)$.

(3) The field $k(\Lambda_M)$ obtained by adding the points of Λ_M to k is an abelian extension of k whose Galois group is isomorphic to $(R_T/(M))^*$. Let $\Phi(M)$ denote the order of $(R_T/(M))^*$.

(4) Let $M=P^n$, where P is a monic prime polynomial of degree d and n is a positive integer. In the extension $K=k(\Lambda_M)$ every prime divisor except (P) and ∞ is unramified. The ramification number of (P) is $\Phi(M)=q^{nd}-q^{(n-1)d}$.

Hayes [5] gives an exposition in modern language of these results of Carlitz. Hayes also determines the decomposition of ∞:

(5) Let M be as in (4). The prime divisor ∞ is tamely ramified in $K=k(\Lambda_M)$. In fact ∞ splits into $\Phi(M)/(q-1)$ prime divisors each of degree one; the ramification number at each such prime is $q-1$.

Finally Hayes establishes the following beautiful converse of (4).

(6) Any finite abelian extension of k in which ∞ is tamely ramified is a constant field extension of $k(\Lambda_M)$ for some polynomial $M\in R_T$.

Hayes actually determines the maximal abelian extension of k. However, we will deal only with the fields $k(\Lambda_M)$. Motivated by the analogy with the classical case, we name these fields *cyclotomic function fields*.

In the rest of this section we assume that $M=P^n$ as in (4). Hayes [5, Proposition 2.4] shows that $f_n(u)=u^{P^n}/u^{P^{n-1}}$ is an Eisenstein polynomial at P in R_T. The roots of $f_n(u)=0$ are precisely the generators of the R_T-module Λ_M. Suppose λ is a root of $f_n(u)=0$. Then

$$f_n(u)=\prod_A(u-\lambda^A),$$

where A runs through a set of representatives of $(R_T/(M))^*$. We identify $(R_T/(M))^*$ with the Galois group G of $K=k(\Lambda_M)$ over k by the correspondence $A\mapsto\sigma_A$, where $\sigma_A(\lambda)=\lambda^A$ for each $\lambda\in\Lambda_M$. Note that if $A=a\in\mathbb{F}_q^*\subseteq(R_T/(M))^*$, then $\sigma_A(\lambda)=\sigma_a(\lambda)=a\lambda$. Let $G_0=\{\sigma_A\in G\,|\,A=a\in\mathbb{F}_q^*\}$.

LEMMA 1. *Let $\mathscr{P}$ be any prime divisor of K lying over ∞. Then G_0 is the inertia group of $\mathscr{P}$. Let $F = K^{G_0}$ be the fixed field of G_0. Then $[K:F] = q-1$ and ∞ splits completely in F into $\Phi(M)/q-1$ prime divisors.*

Proof. Since $G \cong (R_T/(M))^*$, G is isomorphic to a direct product of a cyclic group of order $q^d - 1$ and a p-group. In particular G contains a unique subgroup of order $q-1$ which must be $\mathbb{F}_q^*$. Let $K_{\not{p}}$ and k_∞ be the completions of K and k at $\not{p}$ and ∞, respectively. By (5), $K_{\not{p}}$ is a cyclic extension of k_∞ of degree $q-1$. Hence $\mathrm{Gal}(K_{\not{p}}|k_\infty) = G_0$. Thus G_0 is the decomposition group of $\not{p}$. However, since the residue field of $K_{\not{p}}$ at $\not{p}$ equals that of k_∞ at ∞ (namely, $\mathbb{F}_q$), G_0 is also the inertia group of $\not{p}$. The last assertion of the lemma follows from (5).

Because F is the maximal subfield of K in which ∞ splits completely, we call F the *maximal real subfield* of K, in obvious analogy with the maximal real subfield of a cyclotomic extension of Q.

Let $\mathscr{S} = \{\not{p}_1, \ldots, \not{p}_{\Phi(M)/q-1}\}$ and $S = \{P'_1, \ldots, P'_{\Phi(M)/q-1}\}$ denote the sets of prime divisors of K and F, respectively, lying over ∞. We refer to elements of $\mathscr{S}$ and S as infinite primes. Let O_K and O_F denote the integral closures of R_T in K and F, respectively. The rings O_K and O_F are Dedekind domains whose ideal class groups are finite and whose unit groups are finitely generated. To illustrate the similarity between cyclotomic function fields and cyclotomic number fields, we prove two results that are direct analogues of classical theorems about cyclotomic number fields.

PROPOSITION 1. $O_K^* = O_F^*$, i.e., *every unit in O_K is a real unit.*

Proof. Let $\varepsilon \in O_K^*$. First we show that $\varepsilon^{q-1} \in F$. Let $\sigma_a \in G_0$ and consider $u = \varepsilon/\sigma_a(\varepsilon)$. Clearly $u \in O_K^*$. Moreover, $\mathrm{ord}_{\not{p}}(u) = 0$ for each $\not{p} \in \mathscr{S}$ since $\sigma_a \in G_0$, the inertia group of $\not{p}$. Thus u is a unit at each prime divisor of K, whence $u \in \mathbb{F}_q^*$. Therefore $\varepsilon^{q-1} \in F$ and $F(\varepsilon)$ is an extension of F contained in K which is not ramified at the prime divisor of F that lies above (P). Therefore $F(\varepsilon) = F$ and $\varepsilon \in O_F^*$.

The classical result is that every unit of $Z[w_n]$ is a root of unity times a real unit. However, in this case each root of unity (i.e., each element of $\mathbf{F}_q^*$) lies in F; hence Proposition 1 is the direct analogue of the number field result.

THEOREM 1. *The natural homomorphism $C(O_F) \to C(O_K)$ is an injection.*

Proof. Let I be an ideal (divisor) of O_F that becomes principal in $O_K : I = (y)$, where $y \in O_K$. For each $\sigma \in G_0$, $I^\sigma = I$, implying that $(\sigma(y)) = (y)$; hence $\sigma(y) = u_\sigma y$, where $u_\sigma \in O_K^* = O_F^*$. Moreover $u_{\sigma\tau} = u_\sigma u_\tau$, which means that $\{u_\sigma | \sigma \in G_0\}$ is a cyclic subgroup of O_F^* and thus is contained in $\mathbf{F}_q^*$. It follows that $y^{q-1} \in O_F$. Let n be the least integer such that $y_0 = y^n \in F$. Then n divides $q-1$ and $I^n = (y^n) = (y_0)$. Therefore the extension $F(y) = F(\sqrt[n]{y_0})$ is unramified at all finite primes of F. Hence $F(y) = F$, $y \in F$, and $I = (y)$ is principal in O_F.

Although the next result is not, strictly speaking, necessary for the remainder of the paper, it is of heuristic value in Section 4 and is of interest for its own sake.

LEMMA 2. *Suppose $M = P^n$ as in* (4). *Let λ be a generator of Λ_M. Let N_1 and N_2 denote, respectively, the divisor of zeroes and the divisor of poles of λ. Then*

$$\begin{aligned} \deg N_1 = \deg N_2 &= q^{d-1} && \textit{if} \quad n = 1 \\ &= q^{(n-1)d-1}(q^d - 1) && \textit{if} \quad n > 1. \end{aligned}$$

Proof. Recall that $f_n(u) = u^{P^n}/u^{P^{n-1}}$ is an irreducible polynomial in u with coefficients in R_T. Regard $f_n(u)$ as a polynomial in the variable T with coefficients in $\mathbf{F}_q[u]$. Let $g_n(T, u)$ denote this polynomial and let $h_n(Z) = g_n(Z, \lambda)$. From (1) it follows that h_n has degree q^{d-1} if $n = 1$ and degree $q^{(n-1)d-1}(q^d - 1)$ if $n > 1$. Moreover the irreducibility of $f_n(u)$ implies that h_n is irreducible as a polynomial in Z over $F_q[\lambda]$. Note that T is a root of $h_n(Z) = 0$. Let $L = F_q(\lambda)$. Then $K = L(T)$ and $[K:L] = \deg h_n$. However, by [4, p. 25], $[K:L] = \deg N_1 = \deg N_2$, which proves the lemma.

3. CLASS NUMBER FORMULAS

In this section we summarize relevant facts concerning the zeta functions and L-functions of algebraic function fields and their rings of integers. We then apply these results to obtain class number formulas.

Let R be a Dedekind domain with quotient field L. Suppose that for every nonzero ideal I of R, the residue class ring R/I is finite with, say, $N(I)$ elements. We define the zeta function $\zeta(s, R)$ of R by

$$\zeta(s, R) = \sum_I \frac{1}{N(I)^s},$$

where $s \in C$, the field of complex numbers, and the sum ranges over the nonzero ideals I of R. (In the absence of convergence, we regard the sum as a formal expression. However, in our setting the sum will converge for $\operatorname{Re}(s) > 1$.) From the unique factorization of ideals in R, one obtains the Euler product representation,

$$\zeta(s, R) = \prod_Q \left(1 - \frac{1}{N(Q)^s}\right)^{-1},$$

where Q ranges over the nonzero prime ideals of R.

If $R = R_T = \mathbf{F}_q[T]$, then it follows easily that

$$\zeta(s, R_T) = \sum_A \frac{1}{q^{(\deg A)s}} = 1/(1 - q^{1-s}),$$

where A runs over monic polynomials in R_T. Let O_K again denote the integral closure of R_T in the field $k(\Lambda_M) = K$. In exact analogy with the zeta function of a cyclotomic number field, one has the product decomposition

$$\zeta(s, O_K) = \prod_\chi L(s, \chi),$$

where χ runs over the primitive Dirichlet characters of the group $(R_T/(M))^*$ and

$$L(s, \chi) = \prod_Q \left(1 - \frac{\chi(Q)}{N(Q)^s}\right)^{-1} = \sum_A \frac{\chi(A)}{q^{(\deg A)s}},$$

where in the product, Q runs over the nonzero prime ideals of R_T, and in the sum, A ranges over monic polynomials in R_T. Note that for the trivial character χ_0,

$$L(s, \chi_0) = \zeta(s, R_T) = 1/(1 - q^{1-s}).$$

LEMMA 3. *If χ is a nontrivial primitive character of $(R_T/(M))^*$, then $L(s, \chi)$ is a polynomial in $u = q^{-s}$ of degree at most deg$(M) - 1$.*

Proof. Letting A represent a monic polynomial, we have

$$\begin{aligned} L(s, \chi) &= \sum_A \frac{\chi(A)}{q^{(\deg A)s}} \\ &= \sum_{k=1}^{\infty} \frac{s_k(\chi)}{q^{sk}}, \end{aligned}$$

where $s_k(\chi) = \sum_{\deg A = k} \chi(A)$. Suppose that $\deg(A) = k \geqslant \deg(M)$ and that $(A, M) = 1$, i.e., that A and M are relatively prime. Then $A = Mf + r$, where f is monic with $\deg(f) = \deg(A) - \deg(M)$, $\deg(r) < \deg(M)$ and $(r, M) = I$. Moreover, for each A, f and r are uniquely determined. Thus

$$s_k(\chi) = q^{\deg(A) - \deg(M)} \sum_{r \in (R_T/(M))^*} \chi(r) = 0.$$

The proof is now complete.

For a finite separable extension L of $k = F_q(T)$, one defines the zeta function of L, $\zeta(s, L)$, via the formula

$$\zeta(s, L) = \prod_P \left(1 - \frac{1}{N(P)^s}\right)^{-1},$$

where P ranges over all the prime divisors of L, and $N(P)$ denotes the number of elements in the residue field of P. For instance, $\zeta(s, k) = 1/(1-q^{1-s})(1-q^{-s}) = \zeta(s, R_T)/(1-q^{-s})$, and if O_L is the integral closure of R_T in L and S is the set of infinite primes of L, then

$$\zeta(s, L) = \zeta(s, O_L) \prod_{P \in S} (1 - 1/N(P)^s)^{-1}.$$

In particular when $M = P^n$, $K = k(\Lambda_M)$ and F is the maximal real subfield of K, then

$$\zeta(s, F) = \zeta(s, O_F)(1-q^{-s})^{-\Phi(M)/(q-1)},$$
$$\zeta(s, K) = \zeta(s, O_K)(1-q^{-s})^{-\Phi(M)/(q-1)}.$$

It is well-known [8, p.130] that $\zeta(s, L)$ is actually a rational function of q^{-s} of the form

$$\zeta(s, L) = F(q^{-s}, L)/(1-q^{-s})(1-q^{1-s}),$$

where $F(q^{-s}, L)$ is a polynomial of degree $2g_L (g_L$ is the genus of $L)$ in the variable $u = q^{-s}$. Thus for $M = P^n$, $K = k(\Lambda_M)$,

$$F(u, K)/(1-u)(1-qu) = \zeta(s, O_K)(1-u)^{-\Phi(M)/(q-1)}$$
$$= (1-qu)^{-1}(1-u)^{-\Phi(M)/(q-1)} \prod_{\chi \neq \chi_0} f(u, \chi),$$

where $f(u, \chi) = L(s, \chi)$ for $u = q^{-s}$. If χ is a character on $(R_T/(M))^*$, then we call χ a *real character* if $\chi(a) = 1$ for all $a \in F_q^*$. Notice that there are $\Phi(M)/(q-1) - 1$ nontrivial real characters on $(R_T/(M))^*$. Thus we have

$$F(u, K) = \prod_{\substack{\chi \neq \chi_0 \\ \chi \text{ real}}} [f(u, \chi)/(1-u)] \prod_{\chi \text{ nonreal}} f(u, \chi).$$

Suppose that χ is a real character. Then

$$0 = \sum_{B \in (R_T/(M))^*} \chi(B) = (q-1) \sum_{\substack{A \in (R_T/(M))^* \\ A \text{ monic}}} \chi(A)$$
$$= (q-1) f(1, \chi)$$

implying $f(1,\chi)=0$. Using the well-known fact [8, p. 130] that $F(1,K)=h(K)$, the number of divisor classes of degree zero of K, and using l'Hôpital's rule to evaluate $\lim_{u\to 1}$ of the right side, we derive the following class number formulas.

THEOREM 2. *For $M=P^n$, where P is a prime polynomial of degree d, $K=k(\Lambda_M)$, and F is the maximal real subfield of K,*

$$h(K)=\prod_{\substack{\chi\neq\chi_0\\ \chi \text{ real}}}\left(\sum_{k=0}^{nd-1} -ks_k(\chi)\right)\prod_{\chi \text{ nonreal}}\left(\sum_{k=0}^{nd-1} s_k(\chi)\right)$$

and

$$h(F)=\prod_{\substack{\chi\neq\chi_0\\ \chi \text{ real}}}\left(\sum_{k=0}^{nd-1} -ks_k(\chi)\right).$$

In his thesis Artin [1] obtained similar formulas for the class number of a quadratic extension of k.

4. CLASS NUMBER–UNIT INDEX RELATION

In this section we assume $M=P^n$, where P is a monic prime polynomial of degree d, n is a positive integer, $K=k(\Lambda_M)$, and F is the maximal real subfield of K. Let λ be a generator of Λ_M and let $A\in\mathscr{M}_{dn}$ with $(A,P)=1$. (Note that there are $\Phi(M)/(q-1)$ such A.) Now (λ) is the unique prime ideal of O_K over (P) (see [5, (2.1)]). Thus $(\lambda^A)=(\lambda)$ for $A\in\mathscr{M}_{dn}$, $(A,P)=1$, and $\lambda^A/\lambda\in O_K^*=O_{\mathrm{F}}^*$. In the classical case $K=Q(w)$, where $w=w_{p^n}$ and p is prime and $O_K=Z[w]$, $(w-1)$ is the unique prime above p and the units $(w^g-1)/(w-1)$, $(g,p)=1$ are called cyclotomic units. Thus we call λ^A/λ for $A\in\mathscr{M}_{dn}$, $(A,P)=1$, a cyclotomic unit. A proof of the classical version of our next result (due to Kummer) can be found in [6, p. 88].

THEOREM 3. *Let $\mathscr{E}$ be the subgroup of O_F^* generated by F_q^* and the set of cyclotomic units*

$$\{\lambda^A/\lambda\,|\,A\in\mathscr{M}_{dn} \text{ and } (A,P)=1\}.$$

Then $h(O_F)=[O_F^*:\mathscr{E}]$.

Proof. We begin with a complete proof for the case $M=P$. While this case is conceptually identical to the general case $M=P^n$, $n>1$, the calculations involved are simpler; hence the proof is more transparent. We will then indicate how the proof must be modified when $M=P^n$, $n>1$.

We first rewrite the formula for $h(F)$ from Theorem 2 in a slightly different fashion. For a nontrivial real character χ on $(R_T/(P))^*$, the conjugate character $\bar{\chi}$ is also real. We write

$$h(\bar{\chi}) = \sum_{k=0}^{d-1} -ks_k(\bar{\chi}).$$

Since $\sum_{k=0}^{d-1} s_k(\bar{\chi}) = 0$,

$$h(\chi) = \sum_{k=0}^{d-1} (d-1-k)\, s_k(\bar{\chi}).$$

Therefore

$$\begin{aligned}(q-1)h(\bar{\chi}) &= \sum_{k=0}^{d-1} (q-1)(d-1-k)\, s_k(\bar{\chi}) \\ &= \sum_{k=0}^{d-1} [(q-1)(d-1-k)-1]\, s_k(\bar{\chi}) \\ &= \sum_{A \in \mathcal{M}_d} m(A)\, \bar{\chi}(A),\end{aligned}$$

where $m(A) = (d-1-k)(q-1)-1$ if A is monic of degree k. Therefore,

$$h(F) = (q-1)^{-\Phi(P)/(q-1)+1} \prod_{\substack{\chi \neq \chi_0 \\ \chi \text{ real}}} \left(\sum m(A)\bar{\chi}(A)\right).$$

The reason for writing $h(F)$ in this form will become apparent presently.

Next we turn to the unit index. Let $\mathcal{D}^0(S)$ denote the F-divisors of degree zero which are linear combinations of the primes in S. Let $\mathcal{P}(S)$ be the F-divisors of elements of O_F^* and let E be the F-divisors of the set of cyclotomic units $\mathcal{E}$. Clearly $E \subset \mathcal{P}(S) \subset \mathcal{D}^0(S)$. We first compute $[\mathcal{D}^0(S): E]$.

If $\mathfrak{p}$ is some fixed infinite prime of K, then any other infinite prime of K has the form $\sigma_A(\mathfrak{p}) = \mathfrak{p}_A$ for a unique polynomial $A \in \mathcal{M}_d$. Thus $\mathcal{S} = \{\mathfrak{p}_A | A \in \mathcal{M}_d\}$. Similarly $S = \{P'_A | A \in \mathcal{M}_d\}$, where $P' \in S$ lies under $\mathfrak{p}$. Now the divisor of λ in K has the form $(\lambda) + \sum_{A \in_{md}} m_A \mathfrak{p}_A$, where $m_A \in Z$. ((λ) is the unique prime divisor of K lying over (P).) For $1 \neq B \in \mathcal{M}_d$, the divisor of λ^B is $(\lambda) + \sum_A m_A \mathfrak{p}_{AB}$. Therefore the divisor of λ^B/λ is

$$\begin{aligned}\sum_A m_A(\mathfrak{p}_{AB} - \mathfrak{p}_A) &= \sum_A m_A(\mathfrak{p}_{AB} - \mathfrak{p}) - \sum_A m_A(\mathfrak{p}_A - \mathfrak{p}) \\ &= \sum_A (m_{AB^{-1}} - m_A)(\mathfrak{p}_A - \mathfrak{p}).\end{aligned}$$

Since $\lambda^B/\lambda \in F$, $q-1 \mid m_{AB^{-1}} - m_A$ for each $A \in \mathcal{M}_d$. Hence

$$\sum_{1\neq A\in\mathcal{M}_d} (m_{AB^{-1}} - m_A)(\wp_A - \wp) = \frac{1}{q-1} \sum_{1\neq A\in\mathcal{M}_d} (m_{AB^{-1}} - m_A)(P'_A - P').$$

Clearly $\mathscr{D}^0(S)$ is a free abelian group with basis $\{P'_A - P' \mid 1 \neq A \in \mathcal{M}_d\}$. Thus $[\mathscr{D}^0(S):E] < \infty$ if and only if $\det_{A,B\neq 1}(m_{AB^{-1}} - m_A) \neq 0$, in which case

$$[\mathscr{D}^0(S):E] = \left[\det_{A,B\neq 1}(m_{AB^{-1}} - m_A)\right] \Big/ (q-1)^{[\Phi(P)/(q-1)]-1}.$$

However, by [6, p. 90]

$$\det_{A,B\neq 1}(m_{AB^{-1}} - m_A) = \prod_{\substack{\chi\neq\chi_0 \\ \chi \text{ real}}} \left(\sum m_A \bar{\chi}(A)\right).$$

We next prove that relative to some choice of the fixed infinite prime $\wp$, $m_A = m(A)$. This fact will imply that

$$\begin{aligned} h(F) &= [\mathscr{D}^0(S):E] \\ &= [\mathscr{D}^0(S):\mathscr{P}(S)][\mathscr{P}(S):E] \\ &= (h(F)/h(O_F))[\mathscr{P}(S):E] \end{aligned}$$

(see [7, Proposition 1]) or that $h(O_F) = [\mathscr{P}(S):E]$. Now the homomorphism which assigns to each element of O_F^* its F-divisor induces a surjective homomorphism onto $\mathscr{P}(S)/E$ whose kernel is exactly $\mathscr{E}$. Hence the theorem will be proved in case $M = P$.

To show that $m_A = m(A)$ with respect to some choice of fixed infinite prime $\wp$, we must determine $\text{ord}_{\wp_A}(\lambda) = \text{ord}_{\wp}(\lambda^A)$ for each $A \in \mathcal{M}_d$. Recall that

$$\lambda^P/\lambda = \lambda^{q^d-1} + \begin{bmatrix} P \\ d-1 \end{bmatrix} \lambda^{q^d-1} + \cdots + \begin{bmatrix} P \\ 1 \end{bmatrix} \lambda^{q-1} + P = 0,$$

where $\left[\begin{smallmatrix} P \\ i \end{smallmatrix}\right] \in R_T$ has degree $(d-i)q^i$. Dividing by T^{q^d-1} one obtains

$$(\lambda/T)^{q^d-1} + g_{d-1}(1/T)(\lambda/T)^{q^{d-1}-1} + \cdots + g_1(1/T)(\lambda/T)^{q-1} + g_0(1/T) = 0,$$

where $g_i(1/T) \in \mathbf{F}_q[1/T]$ and $\text{ord}_\infty(g_{d-i}(1/T)) = q^d - (i+1)q^{d-i}$. Since $\text{ord}_\infty(g_{d-1}(1/T)) \leqslant \text{ord}_\infty(g_{d-i}(1/T))$ for $i \geqslant 2$, one notices that (since $\text{ord}_\wp(\lambda/T) \geqslant 0$)

$$\text{ord}_\wp[(\lambda/T)^{q^d-1}] \geqslant \text{ord}\ \ g_{d-1}(1/T) = (q-1)(q^d - 2q^{d-1}),$$

which forces

$$\operatorname{ord}_{\mathfrak{p}}(\lambda) \geqslant (q-1)(1-2q^{d-1})/(q^d-1) > -2.$$

In other words $\operatorname{ord}_{\mathfrak{p}}(\lambda) \geqslant -1$, and if $\operatorname{ord}_{\mathfrak{p}}(\lambda) < 0$, then $\operatorname{ord}_{\mathfrak{p}}(\lambda) = -1$. Since the degree of the denominator is q^{d-1} (Lemma 2) we conclude that there are q^{d-1} infinite primes for which $\operatorname{ord}_{\mathfrak{p}}(\lambda) = -1$, or equivalently, for any fixed infinite prime $\mathfrak{p}$, there are q^{d-1} polynomials $A \in \mathcal{M}_d$ such that $\operatorname{ord}_{\mathfrak{p}}(\lambda^A) = -1$.

Observe that if $\operatorname{ord}_{\mathfrak{p}}(\lambda) \geqslant 0$, then $\operatorname{ord}_{\mathfrak{p}}(\lambda^T) = \operatorname{ord}_{\mathfrak{p}}(\lambda^q + T\lambda) = \operatorname{ord}_{\mathfrak{p}}(T\lambda) = \operatorname{ord}_{\mathfrak{p}}(\lambda) - (q-1)$. Thus the possible nonnegative values of $\operatorname{ord}_{\mathfrak{p}}(\lambda)$ are $i(q-1)-1$, where $i \geqslant 1$. This observation is amplified by the following result.

LEMMA 4. *If* $\operatorname{ord}_{\mathfrak{p}}(\lambda) = j(q-1)-1$ *with* $j > 0$, *and* $A \in R_T$ *is monic of degree* $i \leqslant j$, *then*

$$\operatorname{ord}_{\mathfrak{p}}(\lambda^A) = \operatorname{ord}_{\mathfrak{p}}(\lambda^T) = (j-i)(q-1)-1.$$

Proof. We prove the result by induction on i. For $i=1$, $\operatorname{ord}_{\mathfrak{p}}(\lambda^{T+a}) = \operatorname{ord}_{\mathfrak{p}}(\lambda^q + T\lambda + a\lambda) = \operatorname{ord}_{\mathfrak{p}}(T\lambda) = \operatorname{ord}_{\mathfrak{p}}(\lambda) - (q-1) = \operatorname{ord}_{\mathfrak{p}}(\lambda^T)$. If $A = T^i + \sum_{k<i} a_k T^k$, then

$$\begin{aligned} &\min(\operatorname{ord}_{\mathfrak{p}}(\lambda^{T^i}), \operatorname{ord}_{\mathfrak{p}}(\lambda^{\sum a_k T^k})) \\ &\quad = \min(\operatorname{ord}_{\mathfrak{p}}(\lambda^{T^i}), \operatorname{ord}_{\mathfrak{p}}(\lambda^{T^m})) && \text{for some } m < i \text{ by inductive hypothesis} \\ &\quad = \operatorname{ord}_{\mathfrak{p}}(\lambda^{T^i}) && \text{by the remarks preceding the lemma.} \end{aligned}$$

Therefore $\operatorname{ord}_{\mathfrak{p}}(\lambda^A) = \operatorname{ord}_{\mathfrak{p}}(\lambda^{T^i})$.

COROLLARY. *For each* $\mathfrak{p} \in \mathscr{S}$, $\operatorname{ord}_{\mathfrak{p}}(\lambda) = i(q-1)-1$ *for some integer* i, $0 \leqslant i \leqslant d-1$.

We claim that there exists an infinite prime $\mathfrak{p}$ for which $\operatorname{ord}_{\mathfrak{p}}(\lambda) = (d-1)(q-1)-1$. Once this fact is established, the lemma assures us that relative to this infinite prime, $m_A = m(A)$.

Suppose to the contrary that for every infinite prime $\mathfrak{p}$, $\operatorname{ord}_{\mathfrak{p}}(\lambda) \leqslant (d-2)(q-1)-1$; i.e., for any fixed infinite prime $\mathfrak{p}$ and for all $A \in \mathcal{M}_d$, $\operatorname{ord}_{\mathfrak{p}}(\lambda^A) \leqslant (d-2)(q-1)-1$. Again calling P' the unique prime of F lying below $\mathfrak{p}$, we have $\operatorname{ord}_{\mathfrak{p}}(\lambda^A) = \operatorname{ord}_{P'}(\lambda^{q-1})^A \leqslant (d-2)(q-1)-1$. Let $x = \sum_{A \in \mathcal{M}_d} 1/(\lambda^{q-1})^A$. Clearly $x \in k$ and $\operatorname{ord}_{P'}(x) = \operatorname{ord}_{\infty}(x) \geqslant 1-(d-2)(q-1)$. However, since

$$\lambda^P/\lambda = (\lambda^{q-1})^{(q^d-1)/(q-1)} + \cdots + \begin{bmatrix} P \\ 1 \end{bmatrix} (\lambda^{q-1}) + P = 0,$$

$x = \genfrac{[}{]}{0pt}{}{P}{1}/P$. Therefore $\mathrm{ord}_\infty(x) = \mathrm{ord}_\infty \genfrac{[}{]}{0pt}{}{P}{1} - \mathrm{ord}_\infty P = d - q(d-1) = 1 - (d-1)(q-1)$. This contradiction establishes our claim and completes the proof of the theorem when $M = P$. (Hayes [5, Theorem 3.2] gives a proof of this claim using a Newton polygon argument.)

For the general case $M = P^n$, where $n > 1$, one again argues essentially as when $n = 1$. One obtains the formula

$$(q-1)\, h(\bar{\chi}) = \sum_{A \in \mathscr{M}_{dn}} m(A)\, \bar{\chi}(A),$$

where $m(A) = (nd - 1 - k)(q-1) - 1$ if $\deg A = k$.

The integers m_A are defined as in the previous case; to show that $m(A) = m_A$ for a suitable fixed infinite prime of K, one uses the equation $T^{-(q^{nd}-1)}(\lambda^{P^n}/\lambda) = 0$ to conclude that $\mathrm{ord}_{\mathfrak{p}}(\lambda) \geqslant -1$ for each infinite prime. One next shows that the only possible values for $\mathrm{ord}_{\mathfrak{p}}(\lambda)$ are $i(q-1) - 1$, where $0 \leqslant i \leqslant nd - 1$. Finally, to show that the maximum possible value of $\mathrm{ord}_{\mathfrak{p}}(\lambda)$ (namely, $(nd-1)(q-1) - 1$) is actually realized at some infinite spot $\mathfrak{p}$, one considers the equation $f_n(u) = u^{P^n}/u^{P^{n-1}}$. Since u^{P^n}/u and $u^{P^{n-1}}/u$ are polynomials in u^{q-1},

$$f_n(u) = (u^{q-1})^{\Phi(P^n)/(q-1)} + \cdots + a_1 u^{q-1} + a_0,$$

where $a_i \in k$. It follows (from (1), Section 2) that $a_0 = P$ and that $\mathrm{ord}_\infty(a_1) = -(q-1)\, nd - d + q$. Thus if $x = \sum_{A \in \mathscr{M}_{dn}} 1/(\lambda^{q-1})^A$, then $\mathrm{ord}_\infty(x) = 1 - (nd-1)(q-1)$. Hence there is at least one infinite prime divisor $\mathfrak{p}$ such that $\mathrm{ord}_{\mathfrak{p}}(\lambda) = (nd-1)\,(q-1) - 1$. The remainder of the argument for the case $M = P^n$ is identical to that for the case $M = P$.

The reader interested in pursuing the Carlitz module described here, and its generalizations, can consult papers by D. Goss ("von Staudt for $\mathbf{F}_q[T]$," *Duke Math. J.* **45** (1978) and "The Γ-Ideal and Special Zeta Values," *Duke Math. J.*, in press); V. Drinfel'd ("Elliptic Modules," *Mat. Sb.* **23** (1974)); and D. Hayes ("Explicit Class Field Theory in Global Function Fields," in *Studies in Algebra and Number Theory* (G.-C. Rota, Ed.), Academic Press, New York, 1979).

Acknowledgments

We would like to thank D. Goss for several very valuable discussions concerning this paper.

References

1. E. Artin, Quadratische Korper im Gebiet der höhern Kongruenzen I, II, *Math. Z.* **19** (1924), 153–246.

2. L. Carlitz, A class of polynomials, *Trans. Amer. Math. Soc.* **43** (1938), 167–182.
3. L. Carlitz, On certain functions connected with polynomials in a Galois field, *Duke Math. J.* **1** (1935), 137–168.
4. M. Deuring, "Lectures on the Theory of Algebraic Functions of One Variable," Lecture Notes in Mathematics No. 314, Springer–Verlag, New York/Berlin, 1973.
5. D. Hayes, Explicit class field theory for rational function fields, *Trans. Amer. Math. Soc.* **189** (1974), 77–91.
6. S. Lang, "Cyclotomic Fields," Graduate Texts in Mathematics No. 59, Springer–Verlag, New York/Berlin, 1978.
7. M. Rosen, S-units and S-class group in algebraic function fields, *J. Algebra* **26** (1973), 98–108.
8. A. Weil, "Basic Number Theory," Springer–Verlag, New York/Berlin, 1967.