BULL. AUSTRAL. MATH. SOC. 11R60
VOL. 63 (2001) [21–34]

CLASS NUMBER OF (v, n, M)-EXTENSIONS

OSAMA ALKAM AND MEHPARE BILHAN

An analogue of cyclotomic number fields for function fields over the finite field $\mathbb{F}_q$ was investigated by L. Carlitz in 1935 and has been studied recently by D. Hayes, M. Rosen, S. Galovich and others. For each nonzero polynomial M in $\mathbb{F}_q[T]$, we denote by $k(\Lambda_M)$ the cyclotomic function field associated with M, where $k = \mathbb{F}_q(T)$. Replacing T by $1/T$ in k and considering the cyclotomic function field F_v that corresponds to $(1/T)^{v+1}$ gets us an extension of k, denoted by L_v, which is the fixed field of F_v modulo $\mathbb{F}_q^*$. We define a (v, n, M)-extension to be the composite $N = k_n k(\Lambda_m) L_v$ where k_n is the constant field of degree n over k. In this paper we give analytic class number formulas for (v, n, M)-extensions when M has a nonzero constant term.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field with $q = p^r$ elements, where p is a prime number, and let $k = \mathbb{F}_q(T)$ be the rational function field. To each nonzero polynomial $M(T)$ in $R_T = \mathbb{F}_q[T]$ one can associate a field extension $k(\Lambda_M)$, called the M^{th} cyclotomic function field. It has properties analogous to the classical number fields. Such extensions were investigated by Carlitz [2] and have been studied in recent years by Hayes, Rosen, Galovich, Goss and others. Hayes (in [4]) developed the theory of cyclotomic function fields in a modern language and constructed the maximal Abelian extension of k. We shall briefly review the relevant portions of Carlitz' and Hayes' theory. Let $\overline{k}$ be the algebraic closure of k and $\overline{k}^+$ be its underlying additive group. The Frobenius automorphsim Φ defined by $\Phi(u) = u^q$ and the multiplication map μ_T defined by $\mu_T(T) = Tu$ are $\mathbb{F}_q$-endomorphisms of $\overline{k}^+$. The substitution of $\Phi + \mu_T$ for T in every polynomial $M(T) \in R_T$ introduces a ring homomorphism from R_T into $\operatorname{End}\left(\overline{k}^+\right)$ which defines an R_T-module action on $\overline{k}$. The action of a polynomial $M(T) \in R_T$ on $u \in \overline{k}$ is denoted by u^M and given by

$$u^M = M(\Phi + \mu_t)(u).$$

Received 27th January, 2000

Copyright Clearance Centre, Inc. Serial-fee code: 0004-9727/01 $A2.00+0.00.

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

This action preserves the $\mathbb{F}_q$-algebra structure of $\overline{k}$, since $u^\beta = \beta u$ for $\beta \in \mathbb{F}_q$. Carlitz and Hayes 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 $\begin{bmatrix} M \\ i \end{bmatrix}$ is a polynomial in R_T of degree $(d-i)q^i$. Moreover $\begin{bmatrix} M \\ 0 \end{bmatrix} = M$ and $\begin{bmatrix} M \\ d \end{bmatrix}$ is the leading coefficient of M.

(2) u^M is a separable polynomial in u of degree q^d. If Λ_M denotes the set of roots of the polynomial u^M in $\overline{k}$ then Λ_M is an R_T-submodule of $\overline{k}$ which is cyclic and isomorphic to $R_T/\langle M\rangle$.

(3) The field $k(\Lambda_M)$, which is obtained by adjoining the elements of Λ_M to k, is a simple, Abelian extension of k with a Galois group isomorphic to $(R_T/\langle M\rangle)^*$. By $\Phi(M)$ we denote the order of the group $(R_T/\langle M\rangle)^*$.

(4) If $M \neq 0$ then the infinite prime divisor P_∞ of k splits into $\Phi(M)/(q-1)$ prime divisors of $k(\Lambda_M)$ with ramification index $e_\infty = q-1$ and residue degree $f_\infty = 1$.

Because of the presence of constant fields and wild ramification of the infinite prime P_∞, the above M^{th} cyclotomic function fields $k(\Lambda_M)$ are not sufficient to generate the maximal Abelian extension of k. To remedy this difficulty, Hayes constructed the fields F_v by applying Carlitz' theory with the generator $1/T$ instead of T and $(1/T)^{v+1}$ instead of M and considered the fixed field L_v of F_v under $\mathbb{F}_q^*$. Then the maximal Abelian extension A of k appears as the composite EK_TL_∞, where E is the composite of all constant field extensions of k, K_T is the composite of all cyclotomic function fields and L_∞ is the composite of all fields L_v. Thus we deduce an analogue of the Kronecker-Weber Theorem for rational function fields: Every finite Abelian extension K of k is contained in a composite of the type $N = k_n k(\Lambda_M) L_v$, where k_n is a constant field extension of degree n, M is a nonzero polynomial in R_T and v is a nonnegative integer. We call such extensions (v, n, M)-extensions.

In [3], Galovich and Rosen gave an analytic class number formula for the field $k(\Lambda_M)$ when $M = P^a$ for some prime polynomial $P \in \mathbb{F}_q[T]$. In this paper we give an analytic class number formula for (v, n, M)-extensions for any nonnegative integer v, positive integer n and any polynomial M in $\mathbb{F}_q[T]$ with a nonzero constant term.

Let $N = k_n k(\Lambda_M) L_v$ be such an extension. Then since $k \subseteq L_v$ and Λ_M is a cyclic R_T-module, say $\Lambda_M = \langle\lambda\rangle$, $N = \mathbb{F}_{q^n} L_v(\lambda)$. Hence the fields N and $L_v(\lambda)$ have the same genus. Moreover, the class number of N is divisible by the class number of $L_v(\lambda)$. We shall give explicit class number formulas for both $L_v(\lambda)$ and N. We begin by studying the decomposition of the infinite prime divisor P_∞ of k in $L_v(\lambda)$. Let $G_L = \mathrm{Gal}(L_v(\lambda)/k)$. Then G_L is isomorphic to the direct sum of $G_M = \mathrm{Gal}(k(\lambda)/k) \cong (R_T/\langle M\rangle)^*$ and $G_v = \mathrm{Gal}(L_v/k)$ [4].

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

If $\sigma \in \mathrm{Gal}(L_v(\lambda)/L_v)$ then $\sigma_{\mathrm{res.to.}k(\lambda)} \in G_M$. Notice that $\sigma 1_{\mathrm{res.to.}k(\lambda)} = \sigma 2_{\mathrm{res.to.}k(\lambda)}$ implies that $\sigma_1 = \sigma_2$ since $\sigma 1_{\mathrm{res.to.}L_v} = \sigma 2_{\mathrm{res.to.}L_v} =$ identity automorphsim. Moreover $\left|\mathrm{Gal}(L_v(\lambda)/L_v)\right| = |G_M| = \Phi(M)$. Hence $\mathrm{Gal}(L_v(\lambda)/L_v) \cong G_M \cong (R_T/\langle M\rangle)^*$.

Consider the following diagrams of field extensions and prime divisors

with $\mathfrak{R}$ being a prime divisor of $L_v(\lambda)$ lying over the prime divisors $\mathfrak{I}$ and ℓ of the fields L_v and $k(\lambda)$ respectively, and P being a prime divisior of k lying under both $\mathfrak{I}$ and ℓ.

Restricting automorphisms in $\mathrm{Gal}(L_v(\lambda)/L_v)$ to $k(\lambda)$ makes an isomorphism between the decomposition groups $D(\mathfrak{R}/\mathfrak{I})$ and $D(\ell/P)$. It is an isomorphism between the intertia groups $I(\mathfrak{R}/\mathfrak{I})$ and $I(\ell/P)$ as well. Thus $e(\ell/P)$ and $f(\mathfrak{R}/\mathfrak{I})$ equal $f(\ell/P)$. Therefore we can easily see the following.

PROPOSITION 1. *Let $\mathfrak{R}$ be a prime divisor of $L_v(\lambda)$ lying over the infinite prime divisor P_∞ of k. Then*

(i) $e(\mathfrak{R}/P_\infty) = (q-1)q^v$
(ii) $f(\mathfrak{R}/P_\infty) = 1$
(iii) $g(\mathfrak{R}/P_\infty) = \Phi(M)/(q-1)$
(iv) $N\mathfrak{R} = q$.

Since the only finite prime divisors of k that ramify in $k(\lambda)$ are the divisors of M and no finite prime divisor of k ramifies in L_v, the only prime diviors of k that ramify in $L_v(\lambda)$ are the prime polynomials that divide M.

2. Analytic class number formulas

In this section we develop class number formulas for the fields $L_v(\lambda)$ and N by studying their L-functions and zeta functions. For the rest of this section the constant term of the polynomial M is assumed to be nonzero.

THE FIELD $L_v(\lambda)$. Let χ be a character of $G_L = \mathrm{Gal}(L_v(\lambda)/k)$. Then the L-functions of $L_v(\lambda)/k$ are given by

$$L(s, \chi, L_v(\lambda)/k) = \prod_{\varphi}\left(1 - \frac{\chi(\varphi)}{N\varphi^s}\right)^{-1}, \qquad \mathrm{Re}(s) > 1$$

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

where φ runs over all prime divsors of k, and

$$L^*(s,\chi,L_v(\lambda)/k)=\prod_P\left(1-\frac{\chi(P)}{NP^s}\right)^{-1},\qquad \mathrm{Re}(s)>1$$

where P runs over all finite prime divisors of k. Thus

$$\begin{aligned}L^*(s,\chi_0,L_v(\lambda)/k)&=\prod_P\left(1-\frac{1}{q^{s\deg P}}\right)^{-1}\\&=\zeta(s,R_T)\\&=(1-q^{1-s})^{-1}.\end{aligned}$$

If $\chi\neq\chi_0$ is a character in $\widehat{G}_L$ then

$$L^*(s,\chi,L_v(\lambda)/k)=\prod_{\substack{Q\in\mathbb{F}_q[T],\text{prime}\\ Q\nmid M}}\left(1-\frac{\chi(Q)}{NQ^s}\right)^{-1},\quad \mathrm{Re}(s)>1.$$

By $\chi(Q)$ we mean the value of the character χ at the Frobenius substitution of $L_v(\lambda)/k$ at Q. Therefore

$$\chi(Q)=\chi\left(Q+\langle M\rangle,\ \overline{Q}+\left\langle\left(\frac{1}{T}\right)^{v+1}\right\rangle\right),\quad \text{where } \overline{Q}=\frac{Q}{T^{\deg Q}}.$$

Hence

$$L^*(s,\chi,L_v(\lambda)/k)=\sum_{\substack{A\in\mathbb{F}_q[T],\text{monic}\\(A,M)=1}}\frac{\chi\left(A+\langle M\rangle,\overline{A}+\langle(1/T)^{v+1}\rangle\right)}{NA^s},\qquad \mathrm{Re}(s)>1$$

where $\overline{A}=A/T^{\deg A}$.

Since $NA=q^{\deg A}$ for each monic polynomial A in $\mathbb{F}_q[T]$, we can write

$$L^*(s,\chi,L_v(\lambda)/k)=\sum_{i=0}^{\infty}\frac{S_i(\chi)}{q^{si}},\qquad \mathrm{Re}(s)>1$$

where

$$S_i(\chi)=\sum_{\substack{A\in\mathbb{F}_q[T],\text{monic}\\(A,M)=1\\ \deg A=i}}\chi\left(A+\langle M\rangle,\ \overline{A}+\left\langle\left(\frac{1}{T}\right)^{v+1}\right\rangle\right).$$

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

THEOREM 1. *Let M be a polynomial in $\mathbb{F}_q[T]$ with a nonzero constant term. If $\deg M = m \geqslant 1$ and $\chi \neq \chi_0$ in $\widehat{G}_L$ then $S_i(\chi) = 0$ for all $i \geqslant m + v + 2$.*

PROOF: Let $i \geqslant m + v + 2$ and $S_i = \Big\{\Big(A + \langle M\rangle,\ \overline{A} + \langle(1/T)^{v+1}\rangle\Big) : A \in \mathbb{F}_q[T],$ monic of degree i with $(A, M) = 1\Big\}$. Define $\Theta : S_i \to G_L = \mathrm{Gal}\big(L_v(\lambda)/k\big)$ to be the map which sends $\Big(A + \langle M\rangle,\ \overline{A} + \langle(1/T)^{v+1}\rangle\Big)$ to $\Big(R_A + \langle M\rangle,\ \overline{A} + \langle(1/T)^{v+1}\rangle\Big)$ where R_A is the unique polynomial in $\mathbb{F}_q[T]$ such that $A = M^*Q_A + R_A$, $\deg R_A < \deg M$. Clearly Θ is well-defined. We show that Θ is onto.

Suppose that $R = \sum_{j=0}^{i} r_j T^j$ (with $r_j = 0$ when $j > \deg R$), $M = \sum_{j=0}^{m} d_j T^j$, and $h = \sum_{j=0}^{v} a_j (1/T)^{v-j}$ with $a_v = 1$ and allowing to have some of the a_j's to equal zero. Then, with the convention that $r_j = 0$ for all j such that $\deg R < j < v$, when $\deg R < v$ the system

$$\begin{bmatrix} d_0 & 0 & 0 & \dots & 0 \\ d_1 & d_0 & 0 & \dots & 0 \\ d_2 & d_1 & d_0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ d_v & d_{v-1} & d_{v-2} & \dots & d_0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_v \end{bmatrix} \begin{bmatrix} a_0 - r_0 \\ a_1 - r_1 \\ a_2 - r_2 \\ \vdots \\ 1 - r_v \end{bmatrix}$$

has a unique solution since the constant term d_0 of M is nonzero. Let $x_0 = q_0$, $x_1 = q_1, \dots, x_v = q_v$ be the solution of that system and consider $Q = \sum_{j=0}^{i-m} q_j T^j$ with $q_{v+1}, q_{v+2}, \dots, q_{i-m-1}$ chosen arbitrarily and $q_{i-m} = d_m^{-1}$. (Thus we have $q^{i-m-v-2}$ distinct choices for Q.) Take $A = M^*Q + R$. Then since $(R, M) = 1$, we have $(A, M) = 1$. Moreover A is monic, $\deg A = i$ and

$$\Theta\left(A + \langle M\rangle,\ \overline{A} + \left\langle\left(\frac{1}{T}\right)^{v+1}\right\rangle\right) = \left(R + \langle M\rangle,\ h + \left\langle\left(\frac{1}{T}\right)^{v+1}\right\rangle\right).$$

This shows that Θ is onto.

Now each $g \in G_L$ corresponds to $q^{i-m-v-2}$ distinct choices of A. Moreover, if $A_1 = M^*Q_1 + R_1$, $A_2 = M^*Q_2 + R_2$ then

$$\left(A_1 + \langle M\rangle,\ \overline{A_1} + \left\langle\left(\frac{1}{T}\right)^{v+1}\right\rangle\right) = \left(A_2 + \langle M\rangle,\ \overline{A_2} + \left\langle\left(\frac{1}{T}\right)^{v+1}\right\rangle\right).$$

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

Therefore

$$\begin{aligned} S_i(\chi) &= \sum_{\substack{A\in\mathbb{F}_q[T],\text{monic}\\ (A,M)=1\\ \deg A=i}} \chi\left(A+\langle M\rangle,\ \overline{A}+\left\langle\left(\frac{1}{T}\right)^{v+1}\right\rangle\right)\\ &= q^{i-m-v-2}\sum_{g\in G_L}\chi(g)\\ &= 0. \end{aligned}$$

This completes the proof of the theorem. ∎

The previous Theorem tells us that the L-function $L^*(s,\chi,L_v(\lambda)/k)$ is a polynomial in q^{-s} with degree at most $m+v+1$ whenever $\chi\neq\chi_0$. We may consider $\mathbb{F}_q^*$ to be a subgroup of $\mathrm{Gal}(k(\lambda)/k)$ via identifying each $a\in\mathbb{F}_q^*$ with $\sigma_a\in\mathrm{Gal}(k(\lambda)/k)$ which maps λ to $a\lambda$. If we let $S=\{(\sigma_a,\tau):\ a\in\mathbb{F}_q^*,\ \tau\in G_v=\mathrm{Gal}(L_v/k)\}$ then S is a subgroup of $G_L=\mathrm{Gal}(L_v(\lambda)/k)$. Moreover, $|S|=(q-1)q^v$. The subgroup S is the decomposition group of the point at infinity.

DEFINITION 1: A character χ of $\mathrm{Gal}(k(\lambda)/k)$ is said to be real if $\chi(a)=1$ for all $a\in\mathbb{F}_q^*$, while a character χ of $\mathrm{Gal}(L_v(\lambda)/k)$ is said to be real if $\chi(s)=1$ for all $s\in S$. Clearly there are $(\Phi(M)/(q-1))-1$ nontrivial real characters of each Galois group. Moreover, for any nontrivial real character χ of $\mathrm{Gal}(k(\lambda)/k)$, $L^*(0,\chi,k(\lambda)/k)=0$ [3].

THEOREM 2. *For any nontrivial real character χ of $\mathrm{Gal}(L_v(\lambda)/k)$, $L^*(0,\chi,L_v(\lambda)/k)=0$.*

PROOF: Any nontrivial real character χ of $\mathrm{Gal}(L_v(\lambda)/k)$ can be viewed as a character of $\mathrm{Gal}(k(\lambda)/k)$ via defining $\chi(g)=\chi(\sigma,1_{G_v})$. Moreover, $L^*(s,\chi,L_v(\lambda)/k)=L^*(s,\chi,k(\lambda)/k)$. Hence $L^*(0,\chi,L_v(\lambda)/k)=0$ and the Theorem is proved. ∎

In light of the previous results, we may proceed to derive a class number formula for the field $L_v(\lambda)$. By Theorem 1 and Proposition 1 we may write the zeta function of $L_v(\lambda)$ as follows

$$\begin{aligned} \zeta(s,L_v(\lambda)) &= \left(1-q^{-s}\right)^{-\Phi(M)/(q-1)}\prod_{\chi\in\widehat{G}_L}L^*(s,\chi,L_v(\lambda)/k)\\ &= \left(1-q^{-s}\right)^{-\Phi(M)/(q-1)}\left(1-q^{1-s}\right)^{-1}\prod_{\substack{\chi\in\widehat{G}_L\\ \chi\neq\chi_0}}L^*(s,\chi,L_v(\lambda)/k). \end{aligned}$$

It is well known that

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

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

where $F(q^{-s}, L_v(\lambda))$ is a polynomial in $\mathbb{Z}[q^{-s}]$ of degree $2g$ (where g is the genus of $L_v(\lambda)$). Moreover, the class number of $L_v(\lambda)$ is $F(1, L_v(\lambda))$ [5]. Thus

$$\begin{aligned} F(q^{-s}, L_v(\lambda)) &= (1-q^{-s})^{(-\Phi(M)/(q-1))-1} \prod_{\substack{\chi\in\widehat{G}_L \\ \chi\neq\chi_0}} L^*(s,\chi,L_v(\lambda)/k) \\ &= \Bigg(\prod_{\substack{\chi\in\widehat{G}_L,\text{real} \\ \chi\neq\chi_0}} \frac{L^*(s,\chi,L_v(\lambda)/k)}{1-q^{-s}} \Bigg) \Bigg(\prod_{\substack{\chi\in\widehat{G}_L \\ \chi\,\text{nonreal}}} L^*(s,\chi,L_v(\lambda)/k) \Bigg) \\ &= \Bigg(\prod_{\substack{\chi\in\widehat{G}_L,\text{real} \\ \chi\neq\chi_0}} \frac{\sum_{i=0}^{m+v+1} S_i(\chi)/q^{si}}{1-q^{-s}} \Bigg) \Bigg(\prod_{\substack{\chi\in\widehat{G}_L \\ \chi\,\text{nonreal}}} \sum_{i=0}^{m+v+1} \frac{S_i(\chi)}{q^{si}} \Bigg). \end{aligned}$$

By Theorem 2, $L^*(0,\chi,L_v(\lambda)/k) = 0$ for each nontrivial character χ in $\widehat{G}_L$. Using L'Hopital's rule to evaluate the limit of the above equation's right-hand side as s tends to 0, we derive the following class number formula:

$$h(L_v(\lambda)) = F(1, L_v(\lambda)) = \Bigg(\prod_{\substack{\chi\in\widehat{G}_L,\text{real} \\ \chi\neq\chi_0}} \sum_{i=1}^{m+v+1} -iS_i(\chi) \Bigg) \Bigg(\prod_{\chi\in\widehat{G}_L,\text{nonreal}} \sum_{i=0}^{m+v+1} S_i(\chi) \Bigg).$$

THE FIELD $L_v(\lambda)\mathbb{F}_{q^n}$. Let $G_N = \mathrm{Gal}(N/k)$, $G_v = \mathrm{Gal}(L_v/k)$ and $G_M = \mathrm{Gal}(k(\lambda)/k)$. Then G_N essentially equals the direct sum of the groups G_M, G_v and the cyclic group $\mathbb{Z}_n$ [4]. We shall study the L-functions $L^*(s,\chi,N/k)$ for any nontrivial character χ of G_N. Let $\chi\neq\chi_0$ be a character in $\widehat{G}_N$. Then we have one of two cases:

CASE I. The restriction of χ to $G_M\oplus G_v = \mathrm{Gal}(L_v(\lambda)/k)$ is the trivial character. In this case we define the character Ψ on $\mathrm{Gal}(k\mathbb{F}_{q^n})$ by $\Psi(a) = \chi((1_{G_M}, 1_{G_v}, a))$. We identify the restriction of χ to $G_M\oplus G_v$ with the character χ_{res} of $G_M\oplus G_v$ which is defined by $\chi_{\text{res}}((\sigma,\tau)) = \chi((\sigma,\tau,0))$. Notice that $\chi((\sigma,\tau,a)) = \Psi(a)$ for each $(\sigma,\tau,a)\in G_N$ and that Ψ is nontrivial since χ_{res} is the trivial character. Moreover, Ψ can be viewed as a character of G_N via putting $\Psi((\sigma,\tau,a)) = \Psi(a)$. Hence $L^*(s,\Psi,N/k) = L^*(s,\Psi,k\mathbb{F}_{q^n}/k)$. That is, $L^*(s,\chi,N/k) = L^*(s,\Psi,k\mathbb{F}_{q^n}/k)$. Thus our problem of studying $L^*(s,\chi,N/k)$ is reduced to studying $L^*(s,\Psi,k\mathbb{F}_{q^n}/k)$ which equals $\sum_{f\in\mathbb{F}_q[T],\text{monic}} \Psi(f)/q^{s\deg f}$, $\mathrm{Re}(s) > 1$, where (see [1])

$$\Psi(f) = \Psi\left(\left[\frac{k\mathbb{F}_{q^n}/k}{f}\right]\right) = \Psi(\deg f \pmod n).$$

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

Let r_{d_f} be the unique integer such that $\deg f = c^*n + r_{d_f}$, $0 \leqslant r_{d_f} < n$. Then $\Psi(f) = \Psi\left(r_{d_f}\right)$ and

$$L^*(s, \Psi, k\mathbb{F}_{q^n}/k) = \sum_{f \in \mathbb{F}_q[T],\text{monic}} \frac{\Psi\left(r_{d_f}\right)}{q^{s \deg f}}, \qquad \operatorname{Re}(s) > 1$$

where $d_f = \deg f$.

We can write $L^*(s, \Psi, k\mathbb{F}_{q^n}/k)$ as $\sum_{i=0}^{\infty} S_i(\Psi)/q^{si}$, $\operatorname{Re}(s) > 1$, where $S_i(\Psi) = \sum_{f \in \mathbb{F}_q[T],\text{monic}} \Psi(r_i)$.

Since we have q^i possible monic polynomials in $\mathbb{F}_q[T]$ of degree i, $S_i(\Psi) = q^i \Psi(r_i)$. Therefore

$$\begin{aligned} L^*(s, \Psi, k\mathbb{F}_{q^n}/k) &= \sum_{i=0}^{\infty} \frac{q^i \Psi(r_i)}{q^{si}}, \qquad \operatorname{Re}(s) > 1 \\ &= \sum_{i=0}^{\infty} \frac{\Psi(r_i)}{q^{i(s-1)}}, \qquad \operatorname{Re}(s) > 1 \\ &= \sum_{i=0}^{\infty} \frac{\Psi(i)}{q^{i(s-1)}}, \qquad \operatorname{Re}(s) > 1 \\ &= \sum_{i=0}^{\infty} \frac{\Psi(1)^i}{q^{i(s-1)}}, \qquad \operatorname{Re}(s) > 1 \\ &= \frac{1}{1 - \Psi(1) q^{1-s}}. \end{aligned}$$

Whence, if χ is a nontrivial character of G_N which is trivial on $G_M \oplus G_v$ and Ψ_χ is the character of $\mathbb{Z}_n$ defined by $\Psi_\chi(i) = \chi\left(\left(1_{G_M}, 1_{G_v}, i\right)\right)$ then

$$L^*(s, \chi, N/k) = \frac{1}{1 - \Psi_\chi(1) q^{1-s}}.$$

Case II. The restriction of χ to $G_M \oplus G_v$ is not the trivial character.

Again we let χ_{res} be the restriction of χ to $G_M \oplus G_v$, that is, $\chi_{\text{res}}\left((\sigma, \tau)\right) = \chi\left((\sigma, \tau, 0)\right)$. Then

$$L^*(s, \chi, N/k) = \sum_{\substack{A \in \mathbb{F}_q[T],\text{monic} \\ (A,M)=1}} \frac{\chi\left(\left(A + \langle M \rangle, \overline{A} + \left\langle (1/T)^{v+1} \right\rangle, r_{d_A}\right)\right)}{q^{s d_A}}, \qquad \operatorname{Re}(s) > 1,$$

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

where $d_A = \deg A$, $\overline{A} = A/T^{d_A}$ and r_{d_A} is the unique integer such that $d_A = c^* n + r_{d_A}$, $0 \leqslant r_{d_A} < n$, [1]. If

$$S_i(\chi) = \sum_{\substack{A \in \mathbb{F}_q[T], \text{monic} \\ (A,M)=1,\ d_A = i}} \chi\left(\left(A + \langle M \rangle, \overline{A} + \left\langle \left(\frac{1}{T}\right)^{v+1} \right\rangle, r_{d_A}\right)\right)$$

then

$$L^*(s, \chi, N/k) = \sum_{i=0}^{\infty} \frac{S_i(\chi)}{q^{si}}, \qquad \mathrm{Re}(s) > 1.$$

For each i,

$$S_i(\chi) = \sum_{\substack{A \in \mathbb{F}_q[T], \text{monic} \\ (A,M)=1,\ d_A = i}} \chi((1_{G_M}, 1_{G_v}, r_i))\chi\left(\left(A + \langle M \rangle, \overline{A} + \left\langle \left(\frac{1}{T}\right)^{v+1} \right\rangle, 0\right)\right).$$

Since $\chi((1_{G_M}, 1_{G_v}, r_i))$ is independent of the choice of A as long as $\deg A = i$, we have

$$S_i(\chi) = \chi((1_{G_M}, 1_{G_v}, r_i)) \sum_{\substack{A \in \mathbb{F}_q[T], \text{monic} \\ (A,M)=1,\ d_A = i}} \chi\left(\left(A + \langle M \rangle, \overline{A} + \left\langle \left(\frac{1}{T}\right)^{v+1} \right\rangle, 0\right)\right) = 0$$

because χ_{res} is nontrivial on $G_M \oplus G_v$. Therefore $S_i(\chi) = 0$ for all $i \geqslant d_M + v + 2$. Whence

$$L^*(s, \chi, N/k) = \sum_{i=0}^{d_M+v+1} \frac{S_i(\chi)}{q^{si}}.$$

To summarise we write

$$L^*(s, \chi, N/k) = \begin{cases} \dfrac{1}{1 - \Psi_\chi(1) q^{1-s}}, & \text{if } \chi_{\text{res}} \text{ is trivial on } G_M \oplus G_v \\ \displaystyle\sum_{i=0}^{d_M+v+1} \frac{S_i(\chi)}{q^{is}}, & \text{otherwise.} \end{cases}$$

DEFINITION 2: A character χ of $G_N = \mathrm{Gal}(N/k)$ is said to be real in $\widehat{G}_N$ if $\chi((\sigma_a, \tau, m)) = 1$ for any $a \in \mathbb{F}_q^*$, $\tau \in G_v$ and $m \in \mathbb{Z}_n$.

Clearly we have $(\Phi(M)/(q-1)) - 1$ nontrivial real characters in $\widehat{G}_N$.

THEOREM 3. *Let χ be a nontrivial real character in $\widehat{G}_N$. Then $L^*(0, \chi, N/k) = 0$.*

PROOF: The character χ_{res} is a nontrivial real character of $G_M \oplus G_v$. Hence

$$L^*(s, \chi, N/k) = \sum_{i=0}^{d_M+v+1} \frac{S_i(\chi)}{q^{si}}$$

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

where

$$S_i(\chi) = \chi\big((1_{G_M}, 1_{G_v}, r_i)\big) \sum_{\substack{A\in\mathbb{F}_q[T],\text{monic}\\ (A,M)=1,\ d_A=i}} \chi_{\text{res}}\left(\left(A+\langle M\rangle, \overline{A}+\left\langle\left(\frac{1}{T}\right)^{v+1}\right\rangle\right)\right).$$

Since χ is real, $\chi\big((1_{G_M}, 1_{G_v}, r_i)\big) = 1$. Thus $S_i(\chi) = S_i(\chi_{\text{res}})$. Therefore $L^*(s,\chi,N/k)$ $= L^*\big(s,\chi_{\text{res}}, L_v(\lambda)/k\big)$. The Theorem then follows from Theorem 2. □

Having studied the L-functions $L^*(s,\chi,N/k)$, one can give a class number formula for N via exploring the zeta function $\zeta(s,N)$. Let ℓ be a prime divisor of N lying over the infinite prime divisor P_∞ of k and let $\mathfrak{p}$ be a prime divisor of $L_v(\lambda)$ lying under ℓ and over P_∞. Then we deduce (from the theory of constant field extensions) that $g(\ell,\mathfrak{p}) = \big(d_{L_v(\lambda)}(\mathfrak{p}), n\big) = (1,n) = 1$. Thus, every prime divisor of $L_v(\lambda)$ which lies over the infinite prime divisor of k has a unique extension to a prime divisor of N. Moreover, as is well known from the theory of constant field extensions, no prime divisor of $L_v(\lambda)$ is ramified in N. Thus $e(\ell/\mathfrak{p}) = 1$. Hence $f(\ell/\mathfrak{p}) = n$. Therefore $N\ell = N\mathfrak{p}^{f(\ell/\mathfrak{p})} = q^n$. So

$$\zeta(s,N) = \big(1-q^{-ns}\big)^{-\Phi(M)/(q-1)}\big(1-q^{1-s}\big) \prod_{\substack{\chi\in\widehat{G}_N\\ \chi\neq\chi_0}} L^*(s,\chi,N/k).$$

Since the field of constants of N is $\mathbb{F}_{q^n}$ we get

$$\zeta(s,N) = \frac{F(q^{-ns},N)}{\big(1-q^{-ns}\big)\big(1-q^{n(1-s)}\big)}$$

where $F(q^{-ns},N) \in \mathbb{Z}[q^{-ns}]$ and $F(1,N) = h(N)$; the class number of N. Thus

$$\begin{aligned}
&F(q^{-ns},N)\\
&= \big(1-q^{-ns}\big)^{(-\Phi(M)/(q-1))+1}\Big(1-q^{n(1-s)}\Big)\big(1-q^{1-s}\big)^{-1} \prod_{\substack{\chi\in\widehat{G}_N\\ \chi\neq\chi_0}} L^*(s,\chi,N/k)\\
&= \Big(1-q^{n(1-s)}\Big)\big(1-q^{1-s}\big)^{-1}\Bigg(\prod_{\substack{\chi\in\widehat{G}_N,\text{real}\\ \chi\neq\chi_0}} \frac{L^*(s,\chi,N/k)}{1-q^{-ns}}\Bigg)\Bigg(\prod_{\chi\in\widehat{G}_N,\text{nonreal}} L^*(s,\chi,N/k)\Bigg)\\
&= \Big(1-q^{n(1-s)}\Big)\big(1-q^{1-s}\big)^{-1}\Bigg(\prod_{\substack{\chi\in\widehat{G}_N,\text{real}\\ \chi\neq\chi_0}} \frac{\sum_{i=0}^{d_M+v+1} S_i(\chi)/q^{is}}{1-q^{-ns}}\Bigg)\\
&\qquad\Bigg(\prod_{\substack{\chi\in\widehat{G}_N,\text{nonreal}\\ \chi_{\text{res}}\text{ nontrivial}}} \sum_{i=0}^{d_M+v+1} \frac{S_i(\chi)}{q^{is}}\Bigg)\Bigg(\prod_{\substack{\chi\in\widehat{G}_N,\text{nonreal}\\ \chi_{\text{res}}\text{ trivial}}} \frac{1}{1-\Psi_\chi(1)q^{(1-s)}}\Bigg)
\end{aligned}$$

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

$$= \Bigg(\prod_{\substack{\chi \in \widehat{G}_N, \text{real} \\ \chi \neq \chi_0}} \frac{\sum_{i=0}^{d_M+v+1} S_i(\chi)/q^{is}}{1 - q^{-ns}} \Bigg) \Bigg(\prod_{\substack{\chi \in \widehat{G}_N, \text{nonreal} \\ \chi_{\text{res}} \text{ nontrivial}}} \sum_{i=0}^{d_M+v+1} \frac{S_i(\chi)}{q^{is}} \Bigg) (1 - q^{n(1-s)}) \Bigg(\prod_{\Psi \in \widehat{\mathbb{Z}}_n} \frac{1}{1 - \Psi(1) q^{(1-s)}} \Bigg)$$

$$= \Bigg(\prod_{\substack{\chi \in \widehat{G}_N, \text{real} \\ \chi \neq \chi_0}} \frac{\sum_{i=0}^{d_M+v+1} S_i(\chi)/q^{is}}{1 - q^{-ns}} \Bigg) \Bigg(\prod_{\substack{\chi \in \widehat{G}_N, \text{nonreal} \\ \chi_{\text{res}} \text{ nontrivial}}} \sum_{i=0}^{d_M+v+1} \frac{S_i(\chi)}{q^{is}} \Bigg) (1 - q^{n(1-s)}) \Bigg(\prod_{i=0}^{n-1} \frac{1}{1 - \omega_i q^{(1-s)}} \Bigg),$$

where $\omega_0, \omega_1, \ldots, \omega_{n-1}$ are the nth roots of unity,

$$= \Bigg(\prod_{\substack{\chi \in \widehat{G}_N, \text{real} \\ \chi \neq \chi_0}} \frac{\sum_{i=0}^{d_M+v+1} S_i(\chi)/q^{is}}{1 - q^{-ns}} \Bigg) \Bigg(\prod_{\substack{\chi \in \widehat{G}_N, \text{nonreal} \\ \chi_{\text{res}} \text{ nontrivial}}} \sum_{i=0}^{d_M+v+1} \frac{S_i(\chi)}{q^{is}} \Bigg).$$

By Theorem 3, $L^*(0, \chi, N/k) = 0$ for all nontrivial real characters $\chi \in \widehat{G}_N$. If we evaluate the limit of the right hand-side as s tends to 0 we get the following formula for the class number $h(N)$:

$$h(N) = \Bigg(\prod_{\substack{\chi \in \widehat{G}_N, \text{real} \\ \chi \neq \chi_0}} \frac{1}{n} \sum_{i=1}^{d_M+v+1} -i S_i(\chi) \Bigg) \Bigg(\prod_{\substack{\chi \in \widehat{G}_N, \text{nonreal} \\ \chi_{\text{res}} \text{ nontrivial}}} \sum_{i=0}^{d_M+v+1} S_i(\chi) \Bigg).$$

3. Examples

When we specialise our results to $N = \mathbb{F}_{q^n} L_v(\lambda)$ with $n = 1$ and $v = 0$ we get $N = k(\lambda)$ and

$$h(N) = \Bigg(\prod_{\substack{\chi \in \widehat{G}_N \text{ real} \\ \chi \neq \chi_0}} \Big(\sum_{i=1}^{m+1} -i S_i(\chi) \Big) \Bigg) \Bigg(\prod_{\chi \in \widehat{G}_N, \text{nonreal}} \Big(\sum_{i=0}^{m+1} S_i(\chi) \Big) \Bigg),$$

where $m = \deg M$ and $S_i(\chi) = \sum_{\substack{A \in \mathbb{F}_q[T], \text{monic} \\ \deg A = i}} \chi(a + \langle M \rangle)$.

That is exactly the result obtained by Galovich and Rosen [3]. In the following examples we apply the class number formula mentioned above for the special cases when $\mathbb{F}_q = \mathbb{Z}_2, \mathbb{F}_q = \mathbb{Z}_3$ and for specific prime polynomials $M(T) \in \mathbb{F}_q[T]$.

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

EXAMPLE 1.

Let $k=\mathbb{Z}_2(T)$ and $M(T)=T^3+T+1$. Then $[N:k]=\Phi(M)=2^3-1=7$. Thus $G_N \cong (\mathbb{Z}_2[T]/\langle T^3+T+1\rangle)^*$ is cyclic of order 7. Hence the character group $\widehat{G}_N$ is cyclic of the same order. The element $[T]$ in $(\mathbb{Z}_2[T]/\langle T^3+T+1\rangle)^*$ could be identified with a generator for G_N. Let χ be a generator for the group $\widehat{G}_N$ and assume that $\chi([T])=\zeta$, then ζ is a primitive 7^{th} root of unity. Since $\mathbb{F}_q^*=\mathbb{Z}_2^*=\langle 1\rangle$, any character of G_N is real. Moreover $S_4(\psi)=S_3(\psi)=0$ for each $\psi\in\widehat{G}_N$. Therefore

$$\begin{aligned} h(N) &= \prod_{\substack{\psi\neq\chi_0\\ \psi\in\widehat{G}_N}} \left(\sum_{i=1}^{2}(-iS_i(\psi))\right)\\ &= \prod_{n=1}^{6}\left(\sum_{i=1}^{2}(-iS_i(\chi^n))\right). \end{aligned}$$

Now

$$\begin{aligned} S_1(\chi^n) &= \chi^n([T])+\chi^n([T]^3)\\ &= \zeta+\zeta^{3n} \end{aligned}$$

and

$$\begin{aligned} S_2(\chi^n) &= \chi^n([T]^6)+\chi^n([T]^5)+\chi^n([T]^4)+\chi^n([T]^2)\\ &= \zeta^{6n}+\zeta^{5n}+\zeta^{4n}+\zeta^{2n}. \end{aligned}$$

The number ζ could be any primitive 7^{th} root of unity, in particular $e^{2\pi i/7}$. Substituting this value of ζ in the class number formula yields $h(N)=71$.

EXAMPLE 2. In this example we consider $k=\mathbb{Z}_3(T)$ and $M(T)=T^2+1$. Clearly $G_N=(\mathbb{Z}_2[T]/\langle T^2+1\rangle)^*$ is cyclic of order $\Phi(M)=3^2-1=8$. The element $[T+1]$ is a generator for G_N. Let χ be a generator for $\widehat{G}_N$. Then $\chi([T+1])$ is a primitive 8^{th} root of unity, let us say $\chi([T+1])=\zeta=e^{\pi i/4}$. A character χ^n is real if and only if $n\in\{0,2,4,6\}$. Therefore

$$h(N)=\left(\prod_{n=1}^{3}\sum_{i=1}^{3}-iS_i(\chi^{2n})\right)\left(\prod_{n=0}^{3}\sum_{i=0}^{3}S_i(\chi^{2n+1})\right).$$

If we compute $S_i(\chi^m)$ we find that $S_2(\chi^m)=S_3(\chi^m)=0$ for any m such that $1\leqslant m\leqslant 7$, and that

$$S_0(\chi^m)=\sum_{\substack{B\in\mathbb{Z}_3[T],\text{monic}\\ \deg B=0}}\chi^m([B])$$

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

$$
\begin{aligned}
&= \chi^m([1]) + \chi^m([2]) \\
&= \chi^m([1]) + \chi^m([T+1]^4) \\
&= 1 + \zeta^{4m} \\
&= 1 + e^{m\pi i}.
\end{aligned}
$$

Thus $S_0(\chi^m) = 0$ when m is odd.

Similarly we find that $S_1(\chi^m) = \zeta^{6m} + \zeta^m + \zeta^{7m} = e^{3m\pi i/2} + e^{m\pi i/4} + e^{-m\pi i/4}$. Substitution of these values in the class number formula gives that $h(N) = 9$.

General Treatment. Having treated very special cases in the examples above, one may wonder about the more general case when $\mathbf{F}_q = \mathbb{Z}_p$ and $M(T)$ is any prime polynomial in $\mathbb{Z}_p[T]$. Let $k = \mathbb{Z}_p(T)$ and let $M(T)$ be any prime polynomial in $\mathbb{Z}_p[T]$ of degree d. The extension $k(\Lambda_M)/k$ is of degree $\Phi(M) = p^d - 1$ and the Galois group $G = \mathrm{Gal}(k(\Lambda_M)/k)$ is isomorphic to $(\mathbb{Z}_p[T]/M(T))^*$ which is cyclic. We identify a generator of G with a generator $[A]$ of $(\mathbb{Z}_p[T]/M(T))^*$. The character group $\widehat{G}$ is cyclic as well. Moreover, if $\chi \neq \chi_0$ is a generator of $\widehat{G}$ then $\chi([A])$ is a primitive (p^d-1)st root of unity, say $\chi([A]) = \zeta = e^{2\pi i/(p^d-1)}$. Let H be the subgroup of $\widehat{G}$ consisting of all real characters, that is $H = \{\psi \in \widehat{G} : \Psi([a]) = 1 \text{ for each } a \in \mathbb{Z}_p^*\}$, then $|H| = |\widehat{G}|/|\mathbb{Z}_p^*| = (p^d-1)/(p-1)$ and H is cyclic generated by χ^{p-1}. Thus $H = \{\chi^{m(p-1)} : 0 \leqslant m \leqslant p^d/(p-1)\}$. If $\hbar = \{1, 2, \dots, p^d-2\}$ and $\hbar_d = \{m(p-1) \mid 1 \leqslant m \leqslant (p^d-1)/(p-1) - 1\}$, then a nontrivial character ψ is real if and only if $\psi = \chi^n$ for some $n \in \hbar_d$. The class number $h(k(\Lambda_M))$ of the field $k(\Lambda_M)$ is given by

$$
h(k(\Lambda_M)) = \Bigg(\prod_{\substack{\psi \neq \chi_0 \\ \psi \in H}} \sum_{i=1}^{d+1} -iS_i(\psi)\Bigg)\Bigg(\prod_{\psi \notin H} \sum_{i=0}^{d+1} S_i(\psi)\Bigg),
$$

where

$$
S_i(\psi) = \sum_{\substack{B \in \mathbb{Z}_p[T],\text{monic} \\ \deg B = i}} \psi([B]).
$$

Since G is cyclic, for any $B \in \mathbb{Z}_p[T]$ of degree i with $0 \leqslant i \leqslant d-1$ there is a unique nonnegative integer $n_{[B]}$ with $0 \leqslant n_{[B]} \leqslant p^d - 1$ such that $[B] = ([A])^{n_{[B]}}$. Thus,

$$
\begin{aligned}
S_i(\chi^m) &= \sum_{\substack{B \in \mathbb{Z}_p[T],\text{monic} \\ \deg B = i}} \chi^m([A]^{n_{[B]}}) \\
&= \sum_{\substack{B \in \mathbb{Z}_p[T],\text{monic} \\ \deg B = i}} \zeta^{mn_{[B]}}
\end{aligned}
$$

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press

Hence

$$h(k(\Lambda_M)) = \left(\prod_{n=1}^{((p^d-1)/(p-1))-1} \sum_{i=1}^{d+1} -iS\left(\chi^{n(p-1)}\right)\right)\left(\prod_{n\notin \hbar_d} \sum_{i=0}^{d+1} S_i(\chi^n)\right)$$

$$= \left(\prod_{n=1}^{((p^d-1)/(p-1))-1} \sum_{i=1}^{d+1} -i \sum_{\substack{B\in \mathbb{Z}_p[T],\text{monic} \\ \deg B=i}} \zeta^{n(p-1)n_{[B]}}\right)$$

$$\left(\prod_{n\notin \hbar_d} \sum_{i=0}^{d+1} \sum_{\substack{B\in \mathbb{Z}_p[T],\text{monic} \\ \deg B=i}} \zeta^{nn_{[B]}}\right).$$

Replacing ζ by $e^{2\pi i/(p^d-1)}$, $n_{[B]}$'s by their values and evaluating the expression above gets us the sought class number.

References

[1] M. Bilhan, 'Arithmetic progressions of polynomials over a finite field', in *Number theory and its applications (Ankara 1996)*, Lecture Notes in Pure and Applied Mathematics **204** (Dekker, New York, 1999), pp. 1–21.

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

[3] S. Galovich and M. Rosen, 'The class number of cyclotomic function fields', *J. Number Theory* **13** (1981), 363–375.

[4] D.R. Hayes, 'Explicit class field theory for rational functional fields', *Trans. Amer. Math. Soc.* **189** (1974), 77–91.

[5] A. Weil, *Basic number theory* (Springer-Verlag, Berlin, Heidelberg, New York, 1973).

Department of Mathematics
College of Science
University of Petra
Amman
Jordan

Department of Mathematics
Faculty of Science and Arts
Middle East Technical University
Ankara
Turkey

https://doi.org/10.1017/S0004972700019080 Published online by Cambridge University Press