ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 31, Number 2, Summer 2001

SOME REMARKS ON THE THEORY OF CYCLOTOMIC FUNCTION FIELDS

PABLO LAM-ESTRADA AND GABRIEL DANIEL VILLA-SALVADOR

ABSTRACT. Let $\mathbf{F}_q$ be the finite field of q elements. First we calculate the Galois group of the extension $\mathbf{F}_q(T)(\Lambda_{P^\infty})/\mathbf{F}_q(T)$ obtained by adjoining all the Hayes' modules Λ_{P^n} with $n \to \infty$ and P an irreducible polynomial. Next we prove that for the class of cyclotomic function fields, an analogue of the Brauer-Siegel theorem holds. Finally we give examples of $\mathbf{Z}_p$-extensions in cyclotomic function fields which show that an analogue of a conjecture of Gross holds for some $\mathbf{Z}_p$-extensions, but not for all.

1. Introduction. There is a close analogy between algebraic number fields and algebraic function fields of one variable. This analogy is most pronounced for the class of congruence function fields, that is, when the field of constants is a finite field.

The class field theory of the field of rational numbers $\mathbf{Q}$ is "explicit" in the sense that one can write down a sequence of polynomials whose roots generate the maximal abelian extension of $\mathbf{Q}$. These polynomials define the cyclotomic extensions of $\mathbf{Q}$. The ring of integers in the ground field, $\mathbf{Q}$, $\mathbf{Z}$, acts on an algebraic closure of $\mathbf{Q}$. The maximal abelian extension of $\mathbf{Q}$ is obtained by adjoining the torsion points of that action.

Using the ideas of Carlitz [**1**], Hayes [**5**] developed a similar description for the class field theory of a rational function field over a finite field. The Carlitz-Hayes theory goes as follows: let k be the rational function field over the finite field $\mathbf{F}_q$ of q elements ($q = p^r$ with p a prime number and $r \geq 1$). Fix a generator T of k so that $k = \mathbf{F}_q(T)$, and let $R_T = \mathbf{F}_q[T]$. Let k^{ac} be an algebraic closure of k. Then k^{ac} is an R_T-module under the action. For $u \in k^{ac}$ and $M = M(T) \in R_T$, $u^M := M(\varphi + \mu)(u)$, where $\varphi : k^{ac} \to k^{ac}$ is

Key words and phrases. Congruence function fields, cyclotomic function fields, Carlitz-Hayes theory, class numbers, discriminants, Galois theory.
AMS *Mathematics Subject Classification.* 11R18, 11R29, 11R32, 11R58.
Received by the editors on April 5, 2000, and in revised form on May 12, 2000.
Research of the first author partially supported by COFFA-IPN and SNI-SEP.
Research of the second author partially supported by CONACyT.

the Frobenius automorphism, $\varphi(u) = u^q$ and $\mu : k^{ac} \to k^{ac}$ is multiplication by T, $\mu(u) = Tu$. Thus, u^M is a separable polynomial in u of degree q^d where $d = \deg(M)$, and Λ_M, the set of M-torsion points of k^{ac} under the given R_T-action, is a finite cyclic R_T-submodule of k^{ac} containing q^d elements. The field $k(\Lambda_M)$ is an abelian extension of k so that if λ is a generator of Λ_M as an R_T-module, the map $(R_T/(M))^* \to \mathrm{Gal}(k(\Lambda_M)/k)$ given by $A + (M) \mapsto \sigma_A$, where $\sigma_A(\lambda) = \lambda^A$, is an isomorphism of the group of units of $R_T/(M)$ onto the Galois group of the extension $k(\Lambda_M)/k$ ([**5**, Theorem 2.3]). This extension is a cyclotomic function field that is quite similar to the usual cyclotomic extensions $\mathbf{Q}(\zeta_m)$ of $\mathbf{Q}$.

We shall obtain the structure of $\mathrm{Gal}(k(\Lambda_{P^n})/k)$ with P an irreducible monic polynomial and $n \geq 1$. More generally, if $k(\Lambda_{P^\infty}) = \cup_{n\geq 1} k(\Lambda_{P^n})$, then we shall obtain the structure of $\mathrm{Gal}(k(\Lambda_{P^\infty})/k)$ and as a consequence the structure of $\mathrm{Gal}(k(\Lambda)/k)$, where $k(\Lambda) = \cup_{M\in R_T} k(\Lambda_M)$.

In [**6**] Inaba establishes a partial analogue of the Brauer-Siegel theorem for the class of all congruence function fields with a finite field of constants $\mathbf{F}_q$. More precisely, he proved that

$$\liminf_{g\to\infty} \frac{\ln h}{g \ln q} \geq 1,$$

where the limit is taken from the elements of the class of all congruence function fields over $\mathbf{F}_q$, g being the genus and h the class number. Further, Inaba proved that if we fix a positive integer m and we take the class of all congruence function fields K over $\mathbf{F}_q$ such that there exists $x \in K$ with $[K : \mathbf{F}_q(x)] \leq m$, then

$$\lim_{g\to\infty} \frac{\ln h}{g \ln q} = 1.$$

Madan and Madden [**9**] generalized this last result for the class of congruence function fields K over $\mathbf{F}_q$ for which there exists $x \in K$ with $[K : \mathbf{F}_q(x)] = m$ and $(m/g) \to 0$; this is

$$\lim_{(m/g)\to 0} \frac{\ln h}{g \ln q} = 1.$$

Using this last result, we prove that for the class of cyclotomic function fields $k(\Lambda_M)$, we have

$$\lim_{g\to\infty} \frac{\ln h}{g \ln q} = 1.$$

Next, we consider again a finite field $\mathbf{F}$ with q elements ($q = p^r$), a field K of algebraic functions of one variable with $\mathbf{F}$ as its exact field of constants. Let K_∞/K be a $\mathbf{Z}_p$-extension with Galois group $\Gamma = \mathrm{Gal}\,(K_\infty/K)$, and let S be the set of ramified primes of K in K_∞. We denote by $C_{\infty,S}(p)$ the p-primary part of the S-ideal class group of K_∞. The topological group Γ acts in a natural way on $C_{\infty,S}(p)$. Is the subgroup consisting of invariant classes finite? In the number field case, if K_∞/K_0 is the cyclotomic $\mathbf{Z}_p$-extension of fields of CM-type, Gross's conjecture states that the number of invariant S-classes under the action of Γ on the minus part of the p-class group of K_∞ is finite, if S is the set of ramified primes [**7**]. This conjecture has been verified for absolute abelian fields [**2**], [**3**]. Villa and Madan analyzed the finiteness of the group $C_S(p)^\Gamma$ in [**12**] for congruence function fields. Assume that for p an odd prime number, K_∞/K is either a purely constant extension or one with no new constants such that when no new constants are introduced, S is a finite set for which each prime divisor in S is fully ramified. If K_∞/K is a constant $\mathbf{Z}_p$-extension, then the group $C_{\infty,S}(p)^\Gamma$ is finite. When K_∞/K is a geometric $\mathbf{Z}_p$-extension, Villa and Madan use a formula of Witt [**13**] for the norm residue symbol in cyclic extensions of p-power degree of local fields of characteristic p, and they give necessary and sufficient conditions for the finiteness of the group $C_{\infty,S}(p)^\Gamma$ in terms of norms of S-units. These norm conditions are reflected in a certain square matrix C of order $|S|-1$ with coefficients in $\mathbf{Z}_p$ such that the nonsingularity of C implies the finiteness of $C_{\infty,S}(p)^\Gamma$. The converse holds if C has coefficients in $\mathbf{Q}$.

In the case of Carlitz-Hayes extensions, we give examples of $\mathbf{Z}_p$-extensions which show that the analogue of Gross's conjecture holds for some $\mathbf{Z}_p$-extensions, but not for all.

2. Galois groups of cyclotomic function fields. In this section we shall use the notation given in the introduction and in general in [**5**]. Furthermore, we shall assume that $M = P^n$ where P is a nonconstant monic irreducible polynomial in R_T of degree d and n is a positive integer. Also $q = p^r$ for some $r \geq 1$, where q is the number of elements of $\mathbf{F}_q$.

We shall determine the structure of the multiplicative group of units of R_T modulo P^{p^t} for any $t \geq 1$.

Proposition 1. *If $M = P^n$, then*

$$(R_T/(M))^* \cong H_M \oplus C_{q^d-1}, \tag{1}$$

where H_M is a p-group of order $q^{d(n-1)}$ and C_{q^d-1} is a cyclic group of order $q^d - 1$.

Proof. Let $\Phi(M)$ denote the order of $(R_T/(M))^*$. Then the statement is an immediate consequence of that $\Phi(M) = q^{d(n-1)}(q^d - 1)$, the natural map $\vartheta : (R_T/(M))^* \to (R_T/(P))^*$ is onto, and $(R_T/(P))^*$ is a cyclic group of order $q^d - 1$. □

Our objective is to give the structure of the abelian group H_M obtained in Proposition 1 for $M = P^{p^t}$ with $t \geq 0$. If $t = 0$, we have that $H_P = \{0\}$. Therefore we shall assume $t \geq 1$.

Thus, if $M = P^n$, then the Galois group of the extension $k(\Lambda_M)/k$ is a direct sum of a Sylow p-subgroup of order $q^{d(n-1)}$ and a cyclic subgroup of order $q^d - 1$, that is, $\mathrm{Gal}\,(k(\Lambda_M)/k) \cong (R_T/(M))^* = H_M \oplus C_{q^d-1}$ with $\mathrm{Gal}\,(k(\Lambda_M)/k(\Lambda_P)) \cong H_M$ and $\mathrm{Gal}\,(k(\Lambda_P)/k) \cong C_{q^d-1}$.

The proof of the following two lemmas is straightforward.

Lemma 1. *If $M = P^n$, then the elements of H_M are of the form*

$$1 + CP^s + (M),$$

where $1 \leq s \leq n$ and $(C, P) = 1$. Furthermore, for a fixed s, $1 \leq s \leq n-1$, H_M has

$$q^{d(n-s)} - q^{d(n-s-1)}$$

elements of the form $1 + CP^s + (M)$ with $(C, P) = 1$.

Lemma 2. *Let $M = P^n$ and let t be the positive integer satisfying $p^{t-1} < n \le p^t$. Let n_0 be the integral part of n/p^{t-1}. Then the elements in H_M of maximal order are exactly those of order p^t. Furthermore,*

(i) *if $n_0 = n/p^{t-1}$, then the number of elements of order p^t in H_M is*

$$q^{d(n-1)} - q^{d(n-n_0)};$$

(ii) *if $n_0 < n/p^{t-1}$, then the number of elements of order p^t in H_M is*

$$q^{d(n-1)} - q^{d(n-n_0-1)}.$$

Corollary 1. *With the notations of Lemma 2, let*

$$H_M \cong (\mathbf{Z}/p^t\mathbf{Z})^\alpha \times \mathbf{Z}/p^{n_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{n_s}\mathbf{Z}$$

with $t > n_1 \ge \cdots \ge n_s \ge 0$. Then

(i) *$\alpha = rd(n_0 - 1)$ if $n_0 = n/p^{t-1}$,*

(ii) *$\alpha = rdn_0$ if $n_0 < n/p^{t-1}$,*

where r is given by $q = p^r$. In particular, if $n = p^t$, then $\alpha = rd(p-1)$.

Proof. We have that H_M has $p^{\alpha t+m} - p^{\alpha(t-1)+m}$ elements of order p^t, where $m = n_1 + \cdots + n_s$. Thus the corollary follows immediately from Lemma 2. □

For each t positive integer, let $pH_{P^{p^t}}$ denote the subgroup of $H_{P^{p^t}}$ of all elements v^p with $v \in H_{P^{p^t}}$.

Proposition 2. *The map $\psi : H_{P^{p^{t-1}}} \to pH_{P^{p^t}}$, defined by*

$$\psi\Big(1 + CP^s + \Big(P^{p^{t-1}}\Big)\Big) = \Big(1 + CP^s + \Big(P^{p^t}\Big)\Big)^p,$$

with $(C, P) = 1$ and $1 \le s \le p^{t-1}$, is an isomorphism for every positive integer $t \ge 2$. □

The proof of the following theorem is easy.

Theorem 1. *We have*

(i) $H_{P^p} \cong (\mathbf{Z}/p\mathbf{Z})^{\alpha_1}$ *where* $\alpha_1 = rd(p-1)$;

(ii) *For each positive integer* $t \geq 2$,

$$H_{P^{p^t}} \cong \prod_{i=1}^{t} (\mathbf{Z}/p^i\mathbf{Z})^{\alpha_i},$$

where $\alpha_i = rdp^{t-i-1}(p-1)^2$ *if* $1 \leq i \leq t-1$ *and* $\alpha_t = rd(p-1)$.

Theorem 2. *If* P *is an irreducible polynomial of degree* d *in* R_T *and* C_{q^d-1} *is a cyclic group of order* $q^d - 1$, *then*

(i) $\mathrm{Gal}\,(k(\Lambda_{P^p})/k) \cong (\mathbf{Z}/p\mathbf{Z})^{\alpha_1} \times C_{q^d-1}$ *with* $\alpha_1 = rd(p-1)$;

(ii) *For each positive integer* $t \geq 2$,

$$\mathrm{Gal}\,(k(\Lambda_{P^{p^t}})/k) \cong \prod_{i=1}^{t} (\mathbf{Z}/p^i\mathbf{Z})^{\alpha_i} \times C_{q^d-1},$$

where $\alpha_i = rdp^{t-i-1}(p-1)^2$ *if* $1 \leq i \leq t-1$ *and* $\alpha_t = rd(p-1)$.

Proof. It follows immediately from Proposition 1 and Theorem 1. □

We have that $\Lambda_P \subseteq \Lambda_{P^2} \subseteq \cdots \subseteq \Lambda_{P^n} \subseteq \cdots$, so that $k \subseteq k(\Lambda_P) \subseteq k(\Lambda_{P^2}) \subseteq \cdots \subseteq k(\Lambda_{P^n}) \subseteq \cdots$ is a tower of field extensions. In particular, for each $n \geq 1$, there exists $t \geq 1$ such that $k(\Lambda_{P^n}) \subseteq k(\Lambda_{P^{p^t}})$. We denote by $k(\Lambda_{P^\infty})$ the union of the fields $k(\Lambda_{P^n})$, $n \geq 1$.

Theorem 3. *With the previous notation, we have*

$$\mathrm{Gal}\,(k(\Lambda_{P^\infty})/k(\Lambda_P)) \cong \varprojlim H_{P^{p^t}} \cong \varprojlim \left(\prod_{i=1}^{t} (\mathbf{Z}/p^i\mathbf{Z})^{\alpha_i} \right),$$

where $\alpha_i = rdp^{t-i-1}(p-1)^2$ *if* $1 \leq i \leq t-1$ *and* $\alpha_t = rd(p-1)$.

Proof. For $t \geq 2$, let Ψ_t be the composition of the homomorphism

$$\begin{aligned} H_{P^{p^t}} &\to pH_{P^{p^t}} \to H_{P^{p^{t-1}}} \\ 1 + CP^s + \left(P^{p^t}\right) &\mapsto \left(1 + CP^s + \left(P^{p^t}\right)\right)^p \mapsto 1 + CP^s + \left(P^{p^{t-1}}\right). \end{aligned}$$

Let λ be a generator of $\Lambda_{P^{p^t}}$. Then $\lambda^{P^{(p^t - p^{t-1})}}$ is a generator of $\Lambda_{P^{p^{t-1}}}$. Let $\sigma \in H_{P^{p^t}}$ and $A \in R_T$ be such that $(A, P) = 1$ and $\sigma(\lambda) = \lambda^A$. We have that $\sigma(\lambda^{P^{(p^t-p^{t-1})}}) = (\lambda^{P^{(p^t-p^{t-1})}})^A$. Therefore, Ψ_t is the homomorphism

$$\begin{aligned} H_{P^{p^t}} &\to H_{P^{p^{t-1}}} \\ \sigma &\mapsto \sigma|_{k(\Lambda_{P^{p^{t-1}}})}. \end{aligned}$$

Hence, the homomorphisms Ψ_t, $t \geq 2$, induce the projective system of the groups $\mathrm{Gal}\,(k(\Lambda_{P^{p^t}})/k(\Lambda_P))$, and consequently

$$\mathrm{Gal}\,(k(\Lambda_{P^\infty})/k(\Lambda_P)) = \varprojlim \mathrm{Gal}\,(k(\Lambda_{P^{p^t}})/k(\Lambda_P)) \cong \varprojlim H_{P^{p^t}}.$$

The second isomorphism follows from Theorem 1. □

As a corollary to Theorem 3, we have

Theorem 4. *If C_{q^d-1} is a cyclic group of order $q^d - 1$, then*

$$\begin{aligned} \mathrm{Gal}\,(k(\Lambda_{P^\infty})/k) &\cong \varprojlim \mathrm{Gal}\,(k(\Lambda_{P^{p^t}})/k(\Lambda_P)) \times C_{q^d-1} \\ &\cong \varprojlim \left(\prod_{i=1}^{t} (\mathbf{Z}/p^i\mathbf{Z})^{\alpha_i}\right) \times C_{q^d-1} \\ &\cong \mathbf{Z}_p^\infty \times C_{q^d-1}, \end{aligned}$$

where $\alpha_i = rdp^{t-i-1}(p-1)^2$ if $1 \leq i \leq t-1$, $\alpha_t = rd(p-1)$ and $\mathbf{Z}_p^\infty$ denotes direct product of a denumerable number of copies of the ring of p-adic integers $\mathbf{Z}_p$.

We denote by K_{R_T} to the composite of the cyclotomic function fields $k(\Lambda_M)$ in the algebraic closure k^{ac} of k, with $M \in R_T$. We have that the Galois group of the extension K_{R_T}/k is the inverse limit of the multiplicative groups $(R_T/(M))^*$.

The main result in this section is

Theorem 5. *Let $\mathcal{M}$ be the set of all monic irreducible polynomials in R_T. Then*

$$\mathrm{Gal}\,(K_{R_T}/k) \cong \mathbf{Z}_p^{\infty} \times \prod_{P\in\mathcal{M}} C_{q^{d_P-1}},$$

where $C_{q^{d_P-1}}$ is a cyclic group of order q^{d_P-1} with $d_P = \deg(P)$ for each $P \in \mathcal{M}$.

Proof. Let $M \in R_T$ be a nonconstant polynomial with $M = \alpha P_1^{n_1} \cdots P_r^{n_r}$ its factorization into powers of monic irreducible polynomials. We have that $k(\Lambda_M) = k(\Lambda_{P_1^{n_1}}, \dots, \Lambda_{P_r^{n_r}})$. Therefore K_{R_T} is the composite, in the algebraic closure k^{ac} of k, of the fields $k(\Lambda_{P^\infty})$ with $P \in R_T$ monic irreducible polynomial. Furthermore, for each $P \in R_T$ monic irreducible polynomial, P is fully ramified in the extension $k(\Lambda_{P^\infty})/k$ and unramified in the extension $k(\Lambda_{Q^\infty})/k$ for all $Q \in R_T$ monic irreducible polynomial with $Q \neq P$. Thus, if P and Q are distinct monic irreducible polynomials in R_T, the extensions $k(\Lambda_{P^\infty})/k$ and $k(\Lambda_{Q^\infty})/k$ are linearly disjoint. Then the result follows immediately from this. □

3. Zeta functions and an analogue of the Brauer-Siegel theorem. We shall denote by $\mathbf{F} = \mathbf{F}_q$ the finite field of q elements and by K a function field of one variable with constant field $\mathbf{F}$. It is well known that the divisor class group of $K/\mathbf{F}$ of degree zero is finite. We denote the order of this group by h which is called the *class number* of $K/\mathbf{F}$. The *genus* of $K/\mathbf{F}$ is denoted by g.

We first prove that the analogue of the Brauer-Siegel theorem holds for the class of cyclotomic function fields.

Theorem 6 (Madan and Madden [**9**, Theorem 2]). *Let $\mathcal{C}$ be a class of congruence function fields over the finite field of constants $\mathbf{F}$. For each field K in $\mathcal{C}$, let m be the least integer such that there exists x in K with $[K : \mathbf{F}(x)] = m$. If $\lim_{g\to\infty} m/g = 0$, then*

$$\lim_{g\to\infty} \frac{\ln h}{g \ln q} = 1,$$

where h is the class number and g is the genus of $K/\mathbf{F}$.

We shall prove that in the class of cyclotomic function fields over the finite field of constants $\mathbf{F}_q$

$$\lim_{g\to\infty} \frac{\Phi(M)}{g} = 0.$$

Therefore, in this class of function fields, the conditions of Theorem 6 are satisfied and

$$\lim_{g\to\infty} \frac{\ln h}{g \ln q} = 1.$$

Let $M = \prod_{i=1}^{t} P_i^{n_i}$ be the factorization of $M \in R_T \backslash \mathbf{F}_q$ into powers of irreducible polynomials with $n_i \geq 1$ and $d_i = \deg(P_i) \geq 1$, $i = 1, \dots, t$. Let g_M be the genus of $k(\Lambda_M)$. Then from [**5**] it follows that

$$g_M = \frac{\Phi(M)}{2}\left(\sum_{i=1}^{t}\left(n_i d_i - \frac{d_i}{q^{d_i}-1}\right) - \frac{q}{q-1}\right) + 1. \tag{2}$$

Now, if $d = \deg(M)$, we have

$$\begin{aligned} g_M &\leq \Phi(M)d + 1 = d\prod_{i=1}^{t} q^{d_i(n_i-1)}(q^{d_i}-1) + 1 \\ &\leq d\prod_{i=1}^{t} q^{d_i n_i} + 1 = dq^q + 1. \end{aligned}$$

Suppose that d is sufficiently large, $d \geq 4q/(q-1)$. If $n_i = d_i = 1$ for some $i \in \{1, \dots, t\}$, we have

$$\Phi(M) = (q-1)\prod_{\substack{j=1\\ j\neq i}}^{t} \Phi(P_j^{n_j}).$$

Since we want to estimate the quotient $\Phi(M)/g_M$ when g_M is sufficiently large and the number of irreducible polynomials of degree one in R_T is finite, let us assume that $n_i \geq 2$ or $d_i \geq 2$ for $i = 1, \dots, t$. Hence for $i = 1, \dots, t$, we have that $n_i(q^{d_i} - 1) \geq 2$. Therefore,

$$n_i d_i - \frac{d_i}{q^{d_i} - 1} \geq \frac{n_i d_i}{2} \tag{3}$$

for $i = 1, \dots, t$.

From (2) and (3), we obtain

$$\begin{aligned} g_M \geq \frac{g_M}{\Phi(M)} &\geq \frac{1}{2}\left(\sum_{i=1}^{t}\left(n_i d_i - \frac{d_i}{q^{d_i - 1}}\right) - \frac{q}{q-1}\right) \\ &\geq \frac{1}{2}\left(\sum_{i=1}^{t}\frac{n_i d_i}{2} - \frac{q}{q-1}\right) = \frac{1}{2}\left(\frac{d}{2} - \frac{q}{q-1}\right) \geq \frac{d}{8}. \end{aligned}$$

Therefore we have the following

Proposition 3. *In the class of cyclotomic function fields $k(\Lambda_M)$ over the finite field of constants $\mathbf{F}_q$, we have*

$$g_M \to \infty \Leftrightarrow d \to \infty$$

where $M \in R_T \setminus \mathbf{F}_q$, $d = \deg(M)$ and g_M is the genus of $k(\Lambda_M)$. Furthermore,

$$\lim_{g_M \to \infty} \frac{\Phi(M)}{g_M} = 0.$$

Corollary 2. *In the class of cyclotomic function fields $k(\Lambda_M)$ over the finite field of constants $\mathbf{F}_q$,*

$$\lim_{g_M \to \infty} \frac{\ln h_M}{g_M \ln q} = 1,$$

where h_M is the class number of $k(\Lambda_M)/\mathbf{F}_q$.

Proof. It follows immediately from Theorem 6 and Proposition 3. □

As a consequence of Corollary 2, we may rewrite Inaba's result [**6**] as follows.

Theorem 7. *In the class of the congruence function fields over the finite field of constants* $\mathbf{F}_q$*, we have*

$$\liminf_{g\to\infty} \frac{\ln h}{g \ln q} = 1.$$

Now we establish an equivalent form of the analogue of the Brauer-Siegel theorem.

The number of integer divisors in a given class of divisors C of $K/\mathbf{F}$ equals

$$\frac{q^{\dim(C)} - 1}{q-1}.$$

Thus, if A_n denotes the number of integer divisors of $K/\mathbf{F}$ of degree n, we have

$$A_n = \sum_{\deg(C)=n} \frac{q^{\dim(C)} - 1}{q-1}.$$

In particular,

$$A_n = h\left(\frac{q^{n-g+1} - 1}{q-1}\right), \tag{4}$$

for $n \geq 2g-1$.

With the substitution $u = q^{-s}$, the zeta function of the function field $K/\mathbf{F}$ is given by

$$Z(u) = \frac{L(u)}{(1-u)(1-qu)},$$

where $L(u) = a_0 + a_1 u + \cdots + a_{2g} u^{2g}$ is a polynomial with rational coefficients.

If $k = \mathbf{F}(x)$ is the rational function field over $\mathbf{F}$, we denote the zeta function of $k/\mathbf{F}$ by $\zeta_0(s)$ and $Z_0(u)$. We have in this case $g = 0$, $h = 1$ and

$$\zeta_0(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}, \qquad Z_0(u) = \frac{1}{(1-u)(1-qu)}.$$

For $\mathrm{Re}\,(s) > 1$, $|u| > q^{-1}$, we have

$$\zeta(s) = \prod_{\mathcal{P}} \frac{1}{1 - N(\mathcal{P})^{-s}} = \prod_{\mathcal{P}} \frac{1}{1 - u^{\deg(\mathcal{P})}} \tag{5}$$

where $\mathcal{P}$ runs over the prime divisors of $K/\mathbf{F}$ and the product converges absolutely.

Theorem 8. *Let N_i be the number of prime divisors of degree i in $K/\mathbf{F}$. Then*

$$A_n = \sum_{\substack{r_1 + 2r_2 + \cdots + nr_n = n \\ r_i \geq 0}} \prod_{i=1}^{n} \binom{r_i + N_i - 1}{r_i},$$

where the sum runs over the partitions of n, that is, over the elements $(r_1, \dots, r_n) \in \mathbf{Z}^n$ with $r_i \geq 0$, and

$$\sum_{i=1}^{n} ir_i = n.$$

Proof. We have

$$\frac{1}{(1-x)^p} = \sum_{n=0}^{\infty} \binom{n+p-1}{p-1} x^n \quad \text{for } |x| < 1.$$

Now for $s \in \mathbf{C}$ with $\mathrm{Re}\,(s) > 1$ and $u = q^{-s}$, we have

$$\begin{aligned}
\zeta(s) &= \prod_{\mathcal{P}} \left(1 - \frac{1}{N(\mathcal{P})^s}\right)^{-1} = \prod_{n=1}^{\infty} \left(1 - \frac{1}{q^{ns}}\right)^{-N_n} \\
&= \prod_{n=1}^{\infty} \left(\frac{1}{1-u^n}\right)^{N_n} = \prod_{n=1}^{\infty} \left(\sum_{r_n=0}^{\infty} \binom{r_n + N_n - 1}{r_n} u^{nr_n} \right) \\
&= 1 + \sum_{n=1}^{\infty} \left(\sum_{\substack{r_1 + 2r_2 + \cdots + nr_n = n \\ r_i \geq 0}} \prod_{i=1}^{n} \binom{r_i + N_i - 1}{r_i} \right) u^n,
\end{aligned}$$

where $\mathcal{P}$ runs over all the prime divisors of $K/\mathbf{F}$ and N_n is the number of prime divisors of degree n in $K/\mathbf{F}$. That is,

$$\sum_{n=0}^{\infty} A_n u^n = Z(u) = 1+\sum_{n=1}^{\infty}\Bigg(\sum_{\substack{r_1+2r_2+\cdots+nr_n=n\\ r_i\geq 0}}\prod_{i=1}^{n}\binom{r_i+N_i-1}{r_i}\Bigg)u^n.$$

Comparing coefficients in the series above, we obtain the theorem. □

Now for $n \geq 2g-1$, we have

$$A_n = h\bigg(\frac{q^{n-g+1}-1}{q-1}\bigg) = \sum_{p(n)}\prod_{i=1}^{n}\binom{r_i+N_i-1}{r_i},$$

where $p(n)$ is the set of partitions of n. For $n = 2g-1$, we obtain

$$h\bigg(\frac{q^g-1}{q-1}\bigg) = \sum_{p(2g-1)}\prod_{i=1}^{2g-1}\binom{r_i+N_i-1}{r_i}.$$

Let

$$M = \max_{p(2g-1)}\prod_{i=1}^{2g-1}\binom{r_i+N_i-1}{r_i}.$$

Then

$$M \leq h\bigg(\frac{q^g-1}{q-1}\bigg) \leq |p(2g-1)|M.$$

It is well known that $|p(2g-1)| < \exp(T\sqrt{2g-1})$ with $T = \pi\sqrt{2/3}$. Thus we have

$$M \leq h\bigg(\frac{q^g-1}{q-1}\bigg) \leq \exp(T\sqrt{2g-1})M.$$

Therefore,

$$\text{(6)}\qquad \frac{\ln M}{g\ln q} \leq \frac{\ln h}{g\ln q} + \frac{\ln(q^g-1)-\ln(q-1)}{g\ln q} \leq \frac{T\sqrt{2g-1}}{g\ln q} + \frac{\ln M}{g\ln q}.$$

It follows

Theorem 9. *Let $\mathcal{C}$ be a class of congruence function fields over the finite field of constants* $\mathbf{F}$. *Then in the class* $\mathcal{C}$

$$\lim_{g\to\infty} \frac{\ln h}{g \ln q} = 1 \Longleftrightarrow \lim_{g\to\infty} \frac{\ln M}{g \ln q} = 2,$$

where

$$M = \max_{p(2g-1)} \prod_{i=1}^{2g-1} \binom{r_i + N_i - 1}{r_i}.$$

4. Analogue of a conjecture of Gross in function fields. We first fix the notation for this section, which is given in [**12**]. Let $\mathbf{F}_q$ denote the finite field of q elements, $q = p^r$, $p > 2$ a prime number. Let K_0 be a field of algebraic functions of one variable with field of constants $\mathbf{F}_q$. For each $n \geq 1$, let K_n/K_0 be a cyclic extension of degree p^n such that

(i) $K_n \subset K_{n+1}$ with $[K_{n+1} : K_n] = p$ for each $n \geq 1$;

(ii) The field of constants of K_n is $\mathbf{F}_q$;

(iii) $K_\infty = \cup_{n=1}^{\infty} K_n$,

and if S is the set of ramified primes in the extension K_n/K_0, then these are fully ramified. Let $s = |S|$. We have that K_∞/K_0 is a $\mathbf{Z}_p$-extension, that is, $\Gamma = \mathrm{Gal}\,(K_\infty/K_0) \cong \mathbf{Z}_p$. The S-classes group $C_{\infty,S}$ of the extension K_∞/K_0 is defined by

$$C_{\infty,S} = \varinjlim C_{n,S},$$

where $C_{n,S}$ is the S-class group of the extension K_n/K_0. In this situation, the p-primary part of the S-class group of K_∞ is given by

$$C_{\infty,S}(p) = \varinjlim C_{n,s}(p).$$

The topological group Γ acts in a natural way on $C_{\infty,S}(p)$.

Remark 1. If we consider a cyclic extension L/K of local fields of degree p^n determined by the Witt vector $(\beta_0, \beta_1, \dots, \beta_{n-1})$, then

K is isomorphic to a "Laurent series" field $k'((T))$, k' a finite field. Let $\alpha \in K$. Let F be the unramified extension of $\mathbf{Q}_p$ such that $\mathcal{O}_F/\mathcal{M}_F \cong k'$, where $\mathcal{O}_F$ is the ring of integers of F and $\mathcal{M}_F$ is the maximal ideal of $\mathcal{O}_F$. Choose $A, B_0, B_1, \dots, B_i, \dots, B_{n-1}$ in $\mathcal{O}_F((T))$ such that $A \equiv \alpha \bmod \mathcal{M}_F$, $B_i \equiv \beta_i \bmod \mathcal{M}_F$, $0 \le i \le n-1$, where the congruence is defined coefficientwise. From the Grunwald-Hasse-Wang theorem ([**10**, Theorem 5]), there exists a normal extension $E/\mathbf{Q}$ with $\mathrm{Gal}(E/\mathbf{Q}) \cong \mathrm{Gal}(F/\mathbf{Q}_p)$, that is, p is inert in $E/\mathbf{Q}$. Also, $\mathcal{O}_E/\mathcal{M}_E \cong \mathcal{O}_F/\mathcal{M}_F$ ([**4**, p. 143]) and $\mathcal{O}_E \subset \mathcal{O}_F$. Hence we may assume that the elements $A, B_0, B_1, \dots, B_{n-1}$ are chosen in $\mathcal{O}_E((T))$.

Let $S = \{P_1, P_2, \dots, P_s\}$ be the set of ramified prime divisors in the $\mathbf{Z}_p$-extension K_∞/K_0. We consider integers a_i, b_i, h_i such that the divisor

$$\left(\frac{P_i^{a_i}}{P_s^{b_i}}\right)$$

is of degree zero and $(P_i^{a_i}/P_s^{b_i})^{h_i} = (\delta_i)$ is principal in K_0. Let $\pi_{j,i}$ be a representative in characteristic 0 of δ_j when we complete at P_i, $1 \le i,\ j \le s-1$, as in Remark 1. Also, if K_∞/K_0 is determined by the Witt vector $(\beta_0, \beta_1, \dots, \beta_{n-1}, \dots)$, let $B_{n,i}$ be a representative in characteristic 0 of β_n when we complete at P_i, $i = 1, \dots, s-1$, $n = 0, 1, \dots$. Then we define

$$a_{j,i}^{(n,m)} = \mathrm{Tr}\,\mathrm{Res}\left[\left(\frac{d\pi_{j,i}}{\pi_{j,i}}\right) \cdot B_{n,i}^{p^m}\right] \in \mathbf{Z}_{(p)} \quad 1 \le i, j \le s-1.$$

Let

$$C_n = \begin{pmatrix} c_{1,1}^{(n)} & c_{2,1}^{(n)} & \cdots & c_{s-1,1}^{(n)} \\ c_{1,2}^{(n)} & c_{2,2}^{(n)} & \cdots & c_{s-1,2}^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1,s-1}^{(n)} & c_{2,s-1}^{(n)} & \cdots & c_{s-1,s-1}^{(n)} \end{pmatrix} \in M_{(s-1,s-1)}(\mathbf{Z}_{(p)}),$$

where

$$c_{j,i}^{(n)} = \sum_{t=0}^{n-1} p^t a_{j,i}^{(t,n-t-1)} \quad n \ge 1.$$

We have

$$c_{j,i}^{(n+1)} \equiv c_{j,i}^{(n)} + p^n a_{j,i}^{(n,0)} \bmod p^n. \tag{7}$$

Therefore, the sequence $\{C_n\}_{n=1}^{\infty}$ is Cauchy in $M_{(s-1,s-1)}(\mathbf{Z}_p)$. Let $C = \lim C_n$.

Proposition 4 [**12**, Proposition 3]. *If C is invertible, then the analogue of the conjecture of Gross holds.*

Proposition 5 [**12**, Proposition 5]. *If C has rational coordinates, then the analogue of the conjecture of Gross holds if and only if C is invertible.*

The following examples show that, in the class of cyclotomic extensions of Carlitz-Hayes, there exists $\mathbf{Z}_p$-extensions for which the analogue of the conjecture of Gross holds and $\mathbf{Z}_p$-extensions for which it does not.

Example 1. Let $\beta_0 = 1/(T-1)(T-2)$ and $\beta_i = 0$ for all $i \geq 1$. It is easy to see that $\beta_0 \notin \{\alpha^p - \alpha \mid \alpha \in K_0\}$ where $K_0 = \mathbf{F}_q(T)$. Therefore the Witt vector $(\beta_0, \beta_1, \dots, \beta_{n-1}, \dots)$ determines a $\mathbf{Z}_p$-extension K_∞/K_0 where the only ramified prime divisors are $P_1 = (T-1)$ and $P_2 = (T-2)$. Let $\tilde{K}_0$ be the completion of K_0 at P_1. Since $\deg(P_1) = 1$, we have that $\tilde{K}_0 \cong \mathbf{F}_q((x)) \cong \mathbf{F}_q((T-1))$. Let $\mathbf{F}/\mathbf{Q}_p$ be an unramified extension such that $\mathcal{O}_F/\mathcal{M}_F \cong \mathbf{F}_q$. Let $\delta_1 = (T-1)/(T-2)$, and let $\pi_{1,1}$, respectively $B_{n,1}$, be a representative of δ_1, respectively β_n, in characteristic 0 when we complete at P_1, $n = 0, 1, \dots$. We may take $B_{n,1} = 0$ for all $n \geq 1$. We have

$$\delta_1 = \frac{T-1}{T-2} = \frac{x}{x-1} = -x(1 + x + x^2 + \cdots).$$

Therefore,

$$\pi_{1,1} = -x(1 + x + x^2 + \cdots)\,.$$

Similarly we have

$$B_{0,1} = \frac{1}{(T-1)(T-2)} = \frac{1}{x(x-1)} = -\frac{1}{x}\,(1 + x + x^2 + \cdots)$$

and $B_{n,1} = 0$ for each $n \geq 1$.

The matrix C_n associated to each level K_n/K_0 of the $\mathbf{Z}_p$-extension K_∞/K_0 is of order 1×1 and its coefficient is given by

$$c_{1,1}^{(n)} = \sum_{t=0}^{n-1} p^t a_{1,1}^{(t,n-t-1)} \quad n \geq 1,$$

where

$$a_{1,1}^{(t,n-t-1)} = \operatorname{Tr}\operatorname{Res}\left[\frac{d\pi_{1,1}}{\pi_{1,1}} \cdot B_{t,1}^{p^{n-t-1}}\right].$$

If $t > 0$, then $a_{1,1}^{(t,n-t-1)} = 0$. Therefore

$$c_{1,1}^{(n)} = a_{1,1}^{(0,n-1)} = \operatorname{Tr}\operatorname{Res}\left[\frac{d\pi_{1,1}}{\pi_{1,1}} \cdot B_{0,1}^{p^{n-1}}\right].$$

Now

$$\begin{aligned}\frac{d\pi_{1,1}}{\pi_{1,1}} \cdot B_{0,1}^{p^{n-1}} &= \frac{1}{x(1-x)} \cdot b_{0,1}^{p^{n-1}}\, dx \\ &= -\frac{1}{x^{p^{n-1}+1}}\,(1 + x + x^2 + \cdots)^{p^{n-1}+1}\, dx.\end{aligned}$$

Hence,

$$\operatorname{Res}\left[\frac{d\pi_{1,1}}{\pi_{1,1}} \cdot B_{0,1}^{p^{n-1}}\right] \in \mathbf{Z} \setminus \{0\}.$$

Thus $c_{1,1}^{(n)} \in \mathbf{Z} \setminus \{0\}$. Since $C_n = (c_{1,1}^{(n)})$, we obtain the $C = \lim C_n$ is invertible, that is, the analogue of the conjecture of Gross holds.

We note that in this $\mathbf{Z}_p$-extension, the infinite prime is not ramified.

Example 2. Let $\beta_0 = (2T-1)/T(T-1) \in \mathbf{F}_q[T]$. We have that $\alpha^p - \alpha \neq \beta_0$ for all $\alpha \in K_0^*$. Let $P_1 = T-1$ and $P_2 = T$. Let $\tilde{K}_0$ be the completion of K_0 at P_1. As in Example 1, we obtain that $\tilde{K}_0 \cong \mathbf{F}_q((x))$ with $x = T-1$. Let $\delta_1 = (T-1)/T$ and let $\pi_{1,1}$, respectively $B_{0,1}$, be a representative of δ_1, respectively β_0, in characteristic 0 when we complete at P_1. We have that $\delta_1 = x/(x+1)$ so that $\pi_{1,1} = x/(x+1)$. Similarly, we have

$$B_{0,1} = \frac{2T-1}{T(T-1)} = \frac{2x+1}{x(x+1)}.$$

Therefore

$$\frac{d\pi_{1,1}}{\pi_{1,1}} \cdot B_{0,1} = \left(\frac{1}{x^2} - 1 + 2x - 3x^2 + \cdots \right) dx.$$

Hence

$$\operatorname{Res}\left(\frac{d\pi_{1,1}}{\pi_{1,1}} \cdot B_{0,1} \right) = 0.$$

Thus $c_{1,1}^{(1)} = a_{1,1}^{(0,0)} = 0$, that is, $C_1 = (0)$. Assume we have constructed $B_{0,1}, B_{1,1}, \dots, B_{n-1,1}$ such that $C_i \equiv 0 \bmod p^i$ for each $i = 1, 2, \dots, n$, where $C_i = (c_{1,1}^{(i)})$. From (7) and from the fact that $C_n \equiv 0 \bmod p^n$, it follows that $c_{1,1}^{n+1} = p^n(a_n + b_n)$ where $a_n = a_{1,1}^{(n,0)}$ and $b_n \in \mathbf{Z}_p$. We have

$$\begin{aligned} c_{1,1}^{(n+1)} \equiv 0 \bmod p^{n+1} &\iff d_n \in \mathbf{Z}_p \text{ exists s.t. } p^n(a_n + b_n) = p^{n+1} d_n \\ &\iff a_n + b_n = p d_n \\ &\iff a_n + b_n \equiv 0 \bmod p. \end{aligned}$$

Let $B_{n,1} = r_n / rx(x+1)$ where $r_n \in \mathbf{Z}$ and $q = p^r$. We shall choose a suitable r_n. Since

$$a_n = a_{1,1}^{(n,0)} = \operatorname{Tr}\operatorname{Res}\left[\frac{d\pi_{1,1}}{\pi_{1,1}} \cdot B_{n,1} \right],$$

where

$$\begin{aligned} \frac{d\pi_{1,1}}{\pi_{1,1}} \cdot B_{n,1} &= \frac{1}{x(x+1)} \cdot \frac{r_n}{rx(x+1)}\, dx \\ &= \left(\frac{r_n}{rx^2} - \frac{2r_n}{rx} + \frac{3r_n}{r} - \cdots \right) dx, \end{aligned}$$

we have that $a_n = -2r_n$. Since p is odd, we can choose $r_n \in \mathbf{Z}$ such that $2r_n \equiv b_n \bmod p$.

Thus for this $\mathbf{Z}_p$-extension $C = \lim C_n = 0$, and therefore the analogue of the conjecture of Gross does not hold.

We note that in this $\mathbf{Z}_p$-extension, the only ramified prime divisors are P_1 and P_2.

Hayes gave an explicit description of the maximal abelian extension of the field of rational function $k = \mathbf{F}_q(T)$ over the finite field $\mathbf{F}_q$

in terms of cyclotomic function field extensions over k, constant field extensions of k and some extensions of k in which the infinite prime is wildly ramified. In cyclotomic function field extensions over k, the infinite prime is tamely ramified (see [**5**]).

A particular consequence of this construction is the following result.

Any finite abelian extension of k in which the infinite prime is tamely ramified is a subfield of a constant extension of $k(\Lambda_M)$ for some $M \in \mathbf{F}_q[T]$.

Therefore, if L/k is a geometric cyclic extension of degree p^n, that is, where there are not new constants, the infinite prime is not ramified, and if $P_1, \dots, P_s$ are the finite primes of k ramified in the extension L/K, then there exists a polynomial $M \in \mathbf{F}_q[T]$ such that $L \subset k(\Lambda_M)$. Since the finite primes of k ramified in the extension $k(\Lambda_M)/k$ are exactly the prime divisors corresponding to the monic irreducible polynomials dividing M (see [**5**]), we have that $P_i \mid M$ for each $i = 1, \dots, s$.

Assume that there exists a monic irreducible polynomial P such that P divides M and $P \neq P_1, \dots, P_s$. Let $N \in \mathbf{F}_q[T]$ be such that $M = NP^m$ with $(P, N) = 1$. Since the extension $k(\Lambda_N)/k$ is linearly disjoint from the extension $k(\Lambda_{P^m})/k$, we have that $L \subseteq k(\Lambda_N)$. Therefore, we may assume $P \mid M$ if and only if $P = P_i$ for some $i = 1, \dots, s$. Let $M_0 = P_1 \cdots P_s$. Then there exists $t \in \mathbf{N}$ such that $M \mid M_0^t$, and hence $L \subset k(\Lambda_{M_0^t})$.

Now, in particular, let $M_0 = T(T-1)(T-2)$ and let

$$k(\Lambda_{M_0^\infty}) = \bigcup_{t \geq 0} k(\Lambda_{M_0^T}).$$

Let $K_{\infty,1}/k$ and $K_{\infty,2}/k$ be the $\mathbf{Z}_p$-extensions obtained in Examples 1 and 2, respectively. We have

$$K_{\infty,i} \subset k(\Lambda_{M_0^\infty}) \quad i = 1, 2.$$

Therefore, in the cyclotomic extension $k(\Lambda_{M_0^\infty})/k$, there exist $\mathbf{Z}_p$-extensions for which the analogue of the conjecture of Gross holds and $\mathbf{Z}_p$-extensions for which it does not.

REFERENCES

1. L. Carlitz, *A class of polynomials*, Trans. Amer. Math. Soc. **43** (1938), 167–182.

2. R. Greenberg, *On a certain l-adic representation*, Invent. Math. **21** (1973), 117–124.

3. B. Gross, *p-adic L-series at $s = 0$*, J. Fac. Science Univ. Tokyo Sect. IA Math. **28** (1981), 979–994.

4. H. Hasse, *Number theory*, Grundlehren Math. Wiss. **229** Springer-Verlag, New York, 1980.

5. D.R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91.

6. E. Inaba, *Number of divisor classes in algebraic function fields*, Proc. Jap. Acad. Ser. A Math. Sci. **26** (1950), 1–4.

7. K. Iwasawa, *On cohomology groups of units for $\mathbf{Z}_p$-extensions*, Amer. J. Math. **105** (1983), 189–200.

8. M. Kida and N. Murabayashi, *Cyclotomic function fields with divisor class number one*, Tokyo J. Math. **14** (1991), 45–56.

9. M.L. Madan and D.J. Madden, *On the theory of congruence function fields*, Comm. Algebra **8** (1980), 1687–1697.

10. H. Miki, *On Grunwald-Hasse-Wang's theorem*, J. Math. Soc. Japan **30** (1978), 313–325.

11. H. Reichardt, *Der Primdivisorsatz für algebraische Funktionenkörper über einem endlichen Konstantenkörper*, Math. Z. **40** (1936), 713–719.

12. G.D. Villa-Salvador and M.L. Madan, *On an analogue of a conjecture of Gross*, Manuscripta Math. **61** (1988), 327–345.

13. E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n*, J. Reine Angew. Math. **176** (1936–1937), 126–140.

Departamento de Matemáticas, Escuela Superior de Física y Matemáticas del I.P.N., Edificio 9, Unidad Adolfo López Mateos, Zacatenco, 07300 México, D.F., México
E-mail address: plam@esfm.ipn.mx

Departamento de Matemáticas, Centro de Investigación y de Estudios Avanzados del I.P.N., Apartado Postal 14-740, 07000 México, D.F. México
E-mail address: villa@math.cinvestav.mx