Compositio Mathematica **106:** 247–266, 1997.

On Artin's conjecture for the Carlitz module

CHIH-NUNG HSU
Institute of Mathematics, National Taiwan Normal University, 88 Sec. 4 Ting-Chou Road, Taipei, Taiwan; e-mail: maco@math.ntnu.edu.tw

Received 28 April 1995; accepted in final form 17 October 1995

Mathematics Subject Classifications (1991): 12FXX, 04A20.

Key words: Kummer–Carlitz extensions, Artin's conjecture.

0. Introduction

A well-known conjecture of E. Artin [1] states that for any integers $a \neq \pm 1$ and a is not a perfect square, there are infinitely many prime integers p for which a is a primitive root (mod p). An analogue of this conjecture for function fields was attacked successfully by Bilharz [2] in 1937 using the Riemann hypothesis for curves over finite fields (subsequently proved by A. Weil). The original conjecture of Artin remains open, though it was shown to be true if one assumes the Generalized Riemann hypothesis by Hooley [7]. In recent years, this conjecture of Artin has also been formulated and studied for elliptic curves over global fields instead of just G_m (the original case) (see [11]).

Let $\mathcal{C}$ be a projective smooth algebraic curve defined over a finite field $\mathbb{F}_q$ (q, some power of a fixed prime number), and take a fixed place ∞ of $\mathcal{C}$. The Dedekind domain consisting of all functions on the curve $\mathcal{C}$ regular away from ∞ is denoted by $\mathbf{A}$. From the view point of class field theory, the Drinfeld $\mathbf{A}$-modules are the more interesting arithmetic objects over function fields. Their division points always generate very nice extension fields. In particular, the rank one Drinfeld $\mathbf{A}$-modules play a role entirely analogous to the important role played by G_m over number fields. This leads naturally to Artin's conjecture for Drinfeld $\mathbf{A}$-modules. The aim of this paper is to prove Artin's conjecture for the Carlitz module, i.e., the rank one Drinfeld $\mathbb{F}_q[t]$-module over the rational function field $\mathbb{F}_q(t)$.

In the following we always let $\mathcal{C} = \mathbb{P}^1$, and $\mathbf{A} = \mathbb{F}_q[t]$. Let $C = (\mathrm{G}_a, \phi)$ be a given Drinfeld $\mathbf{A}$-module defined over $\mathbf{A}$ where ϕ means an injective ring homomorphism from $\mathbf{A}$ to $\mathrm{End}_{\mathbf{A}}(\mathrm{G}_a)$. Let $\mathfrak{P}$ be a prime ideal of $\mathbf{A}$. The reduction of C mod $\mathfrak{P}$ makes $\mathbf{A}/\mathfrak{P}$ a finite $\mathbf{A}$-module denoted by $C(\mathbf{A}/\mathfrak{P})$. Given $0 \neq a \in \mathbf{A}$, we are interested in the set C_a consisting of prime ideals $\mathfrak{P}$ of $\mathbf{A}$ for which $\bar{a} = a + \mathfrak{P}$ is a generator of $C(\mathbf{A}/\mathfrak{P})$. Analogue of Artin's conjecture for C says that C_a always has a Dirichlet density $\delta(C_a)$ to be given by an infinite (Euler) product. Moreover

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

$\delta(C_a)$ should be positive in general, hence there are usually infinitely many prime ideals $\mathfrak{P}$ for which $\bar{a}$ is a generator of $C(\mathbf{A}/\mathfrak{P})$.

In this paper we deal with the Carlitz case. Hence ϕ is given by $\phi(t)(X) = tX + X^q$. In Section 4 Theorem 4.6, we prove that the density of C_a except in the case $q = 2$ is given by

$$\delta(C_a) = \prod_{\substack{\text{all monic irreducibles} \\ l(t) \text{ in } \mathbf{A}}} \left(1 - \frac{1}{N_{l(t)}}\right),$$

where $N_{l(t)}$ is the degree $[K_{l(t)} : \mathbb{F}_q(t)]$ and $K_{l(t)}$ is the Galois extension over $\mathbb{F}_q(t)$ obtained by adjoining roots of $\phi(l(t))(X) = 0$ and roots of $\phi(l(t))(X) = a$ to $\mathbb{F}_q(t)$. We also show that for given $a \neq 0$ in $\mathbf{A}$, $\delta(C_a) > 0$ except for the case that

$$q = 2 \text{ and } a \in \{1\} \cup \phi(t)(\mathbf{A}) \cup \phi(1+t)(\mathbf{A}).$$

This is analogous to the condition a is not perfect square and $a \neq \pm 1$ in the classical Artin's conjecture.

Let $k = \mathbb{F}_q(t), \Omega$ its algebraic closure, and $a \in \mathbf{A}$ a fixed nonzero polynomial in $\mathbf{A}$. Given monic irreducible $m \in \mathbf{A}$, we let $k_m = k(\Lambda_m)$ be the cyclotomic function fields over k (Λ_m consists of the roots of $\phi(m)(X) = 0$ in Ω). We are interested in the field extensions $K_m = k_m(\alpha)$, where α is a root of the equation $\phi(m)(X) - a = 0$ in Ω. These extensions K_m/k_m will be called Kummer–Carlitz extensions. They have very nice properties. Moreover, $\bar{a}$ is a generator of $C(\mathbf{A}/\mathfrak{P})$ if and only if $\mathfrak{P}$ does not split completely in any $K_{l(t)}$, $l(t)$ runs through all monic irreducibles of $\mathbf{A}$ (Theorem 1.3).

In Section 2, we shall estimate the growth of the discriminants $\Delta(K_m/k)$ by applying Newton Polygon method. In particular, we show that (Theorem 2.4)

$$\frac{\deg(\Delta(K_m/k))}{[K_m : k]} = O(\deg m).$$

In Section 3, we work out a generalized Artin problem for function fields by using an effective version of the Prime Number Theorem for function fields together with combinatorical techniques. Putting all these results together enables us to solve Artin's conjecture for Carlitz module in Section 4.

1. On Kummer–Carlitz extensions

Let $C = (\mathrm{G}_a, \phi)$ be the Carlitz $\mathbf{A}$-module given by $\phi(t)(X) = tX + X^q$. We shall use the notation X^m instead of $\phi(m)(X)$, hence for $\alpha \in \Omega$, and nonzero $m \in \mathbf{A}$, α^m means the value $\phi(m)(\alpha)$. We always consider Ω as $\mathbf{A}$-module under the Carlitz ϕ-action. For nonzero $m \in \mathbf{A}$, the m-torsion in Ω is denoted by Λ_m (i.e., Λ_m is the subset consisting of $\alpha \in \Omega$ such that $\phi(m)(\alpha) = 0$). Let $k_m = k(\Lambda_m)$. We shall also fix a nonzero polynomial $a \in \mathbf{A}$ in this section and let $K_m = k_m(\alpha)$, where $\alpha \in \Omega$ is a root of $X^m - a = 0$.

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

A prime ideal $\mathfrak{P}$ of $\mathbf{A}$ always has a monic irreducible polynomial in $\mathbf{A}$ as generator which will be denoted by $p(t)$. Given $b \in \mathbf{A}$, the canonical image of b in $\mathbf{A}/\mathfrak{P}$ is denoted by $\bar{b}$. We are particularly interested in the reduction of C modulo $\mathfrak{P}$. This is the action given by $\phi_{\mathfrak{P}}(t)(X) = \bar{t}X + X^q$ on $\mathbf{A}/\mathfrak{P}$ (as $\mathbf{A}$-algebra). Under this action, $\mathbf{A}/\mathfrak{P}$ acquires another $\mathbf{A}$-module structure which will be denoted by $C(\mathbf{A}/\mathfrak{P})$. It is not difficult to show that $C(\mathbf{A}/\mathfrak{P})$ is isomorphic to $\mathbf{A}/(p(t)-1)$, a cyclic finite $\mathbf{A}$-module (see [8]). We have

PROPOSITION 1.1. *Given $\mathfrak{P} \subset \mathbf{A}$ a prime ideal and nonzero $m \in \mathbf{A}$. Then $\mathfrak{P}$ splits completely in K_m if and only if $p(t) \equiv 1 \pmod{m}$ and $\phi_{\mathfrak{P}}(\frac{p(t)-1}{m})(\bar{a}) = 0$ (i.e., $a^{\frac{p(t)-1}{m}} \equiv 0 \pmod{p(t)}$).*

Proof. If $p(t) \equiv 1 \pmod{m}$, by [6, Theorem 7.1], $\mathfrak{P}$ splits completely in k_m. Let $\alpha \in \Omega$ be any root of $X^m - a$ (i.e., $\phi(m)(\alpha) - a = 0$). Since $X^{p(t)}$ is an Eisenstein polynomial,

$$\bar{\alpha}^{q^{\deg p(t)}} - \bar{\alpha} = \phi_{\mathfrak{P}}(p(t)-1)(\bar{\alpha}) = \phi_{\mathfrak{P}}(\frac{p(t)-1}{m})(\bar{a}) = 0.$$

We have $\bar{\alpha} \in \mathbf{A}/\mathfrak{P}$. The derivative of $\phi_{\mathfrak{P}}(m)(X) - \bar{a}$ is equal to $\overline{m}$ which is nonzero in $\mathbf{A}/\mathfrak{P}$ (since $p(t) \equiv 1 (\operatorname{mod} m)$). Combining these, it follows that the equation $\phi_{\mathfrak{P}}(m)(X) - \bar{a} = 0$ has exactly $q^{\deg m}$ different roots in $\mathbf{A}/\mathfrak{P}$. According to a principle of Dedekind, the prime ideal $\mathfrak{P}$ must split completely in the field $k(\alpha)$ over k. Hence $\mathfrak{P}$ splits completely also in K_m. Conversely, since $\mathfrak{P}$ splits completely in K_m, $p(t) \equiv 1 (\operatorname{mod} m)$ ([6], Theorem 7.1) and α is equivalent to some element $f \in \mathbf{A}$ modulo $\mathfrak{P}$. One has,

$$\phi_{\mathfrak{P}}(\frac{p(t)-1}{m})(\bar{a}) = \phi_{\mathfrak{P}}(p(t)-1)(\bar{\alpha}) = \phi_{\mathfrak{P}}(p(t)-1)(\bar{f}) = 0$$

(since $C(\mathbf{A}/\mathfrak{P}) \cong \mathbf{A}/(p(t)-1)$). This completes the proof.

PROPOSITION 1.2. *The element $\bar{a}$ is a generator of $C(\mathbf{A}/\mathfrak{P})$ if and only if $\phi_{\mathfrak{P}}(\frac{p(t)-1}{l(t)})(\bar{a}) \neq 0$, for any monic irreducible $l(t)$ of $\mathbf{A}$ satisfying $p(t) \equiv 1 (\operatorname{mod} l(t))$.*

Proof. (⇒) If $\bar{a}$ is not a generator of $C(\mathbf{A}/\mathfrak{P})$, then there exists a monic irreducible $l(t)$ dividing $p(t)-1$, with degree less than $\deg \mathfrak{P}$ such that $\phi_{\mathfrak{P}}((p(t)-1)/l(t))(\bar{a}) = 0$ (since $C(\mathbf{A}/\mathfrak{P}) \cong \mathbf{A}/(p(t)-1)$ as $\mathbf{A}$-module). This contradicts the assumption.

For (⇐), if $\bar{a}$ is a generator of $C(\mathbf{A}/\mathfrak{P})$, then clearly $\phi_{\mathfrak{P}}((p(t)-1)/l(t))(\bar{a}) \neq 0$ for any monic irreducible $l(t) \in \mathbf{A}$ such that $p(t) \equiv 1 (\operatorname{mod} l(t))$.

Combining Propositions 1.1 and 1.2, we have the following basic.

THOEREM 1.3. *The element $\bar{a}$ is a generator of $C(\mathbf{A}/\mathfrak{P})$ if and only if the prime ideal $\mathfrak{P}$ does not split completely in any of the field $K_{l(t)}$, where $l(t)$ runs through monic irreducibles in $\mathbf{A}$ with $\deg l(t) \geqslant 1$.*

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

EXAMPLE. Let $\mathbf{A} = \mathbb{F}_2[t], a = 1$. Since $1^1 = 1, 1^t = 1 + t, 1^{t^n} = 1 + t$ for any positive integer n, this implies $a^f = 0, 1, t$ or $1 + t$. Thus $\bar{a} = \bar{1}$ is not a generator of $C(\mathbf{A}/\mathfrak{P})$ for all prime ideals $\mathfrak{P}$ in $\mathbb{F}_2[t]$ with $\deg p(t) \geqslant 3$. It is easy to check that $\bar{a} = \bar{1}$ is a generator of $C(\mathbf{A}/\mathfrak{P})$ for the remaining three prime ideals $\mathfrak{P} = (t), (1 + t)$ or $(1 + t + t^2)$.

LEMMA 1.4. *Let m, n be two nonzero monic relatively prime polynomials in $\mathbf{A}$. If the equations $X^m = a, Y^n = a$ have solutions in $\mathbf{A}$, then equation $Z^{mn} = a$ also has solutions in $\mathbf{A}$.*

Proof. Suppose that $X = \alpha$ (resp. $Y = \beta$) is a solution of $X^m = a$ (resp. $Y^n = a$) in $\mathbf{A}$, and $e, g \in \mathbf{A}$ such that $me + ng = 1$. Let $\gamma = \alpha^g + \beta^e \in \mathbf{A}$. Then $\gamma^{mn} = (\alpha^g + \beta^e)^{mn} = (\alpha^m)^{ng} + (\beta^n)^{me} = a^{me+ng} = a$. This completes the proof. □

The Galois group of k_m/k is naturally isomorphic to $(\mathbf{A}/(m))^\times$ ([6, Theorem 2.3]). This isomorphism is given by $\bar{f} \mapsto \sigma_{\bar{f}}$ such that $\sigma_{\bar{f}}(\xi) = \xi^f$ for all $\xi \in \Lambda_m$. If $\alpha \in K_m$ is a fixed root of $X^m = a$, then the roots of $X^m = a$ are necessarily of the form $\alpha + \xi$, for $\xi \in \Lambda_m$. Given $\psi \in \mathrm{Gal}(K_m/k_m)$, then one has $\psi(\alpha) = \alpha + \xi$, for some $\xi \in \Lambda_m$. We shall let ψ_ξ stand for this ψ. Thus we may view the Galois group of K_m/k_m as a subgroup of Λ_m, denoted by H_m. More precisely, we have an isomorphism $\psi\colon \mathrm{H}_m \to \mathrm{Gal}(K_m/k_m)$ given by $\psi_\xi(\alpha) = \alpha + \xi$.

Now $\mathrm{Gal}(k_m/k)$ can act on $\mathrm{Gal}(K_m/k_m)$ by conjugation. Identifying the group $\mathrm{Gal}(k_m/k)$ with $(\mathbf{A}/(m))^\times$, this action is explicitly given by the following.

PROPOSITION 1.5. *$\sigma_{\bar{f}} \cdot \psi_\xi = \psi_{\xi^f}$, for all $\bar{f} \in (\mathbf{A}/(m))^\times$, $\xi \in \mathrm{H}_m$, and $\sigma_{\bar{f}} \in \mathrm{Gal}(k_m/k)$ such that $\sigma_{\bar{f}}(\xi) = \xi^f$.*

Proof. Let $\sigma \in \mathrm{Gal}(K_m/k)$ such that $\sigma^{-1}(\alpha) = \alpha + \xi'$ (i.e., $\alpha = \sigma(\alpha + \xi')$), for some $\xi' \in \Lambda_m$ and the restriction of σ to k_m is equal to $\sigma_{\bar{f}}$. Then we have

$$\begin{aligned} \sigma_{\bar{f}} \cdot \psi_\xi(\alpha) &= \sigma \circ \psi_\xi \circ \sigma^{-1}(\alpha) \\ &= \sigma \circ \psi_\xi(\alpha + \xi') \\ &= \sigma(\alpha + \xi' + \xi) \\ &= \alpha + \xi^f. \end{aligned} \tag{1.1}$$

This completes the proof. □

The main point is to extend the action of $(\mathbf{A}/(m))^\times$ to an action of $\mathbf{A}/(m)$ on $\mathrm{Gal}(K_m/k_m)$. In the case $q \neq 2$ or $q = 2$ but $t(t + 1) \nmid m$, this is done in the following way. Given $f \in \mathbf{A}$, write f as a finite sum $f_1 + f_2 + \cdots + f_n$ such that

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

$(f_i, m) = 1$ for all i (This is possible by Chinese Remainder Theorem). Then we define, for $\xi \in \mathrm{H}_m$,

$$f \cdot \psi_\xi = \sum_i \sigma_{\bar{f}_i} \cdot \psi_\xi = \sum_i \psi_{\xi^{f_i}} = \psi_{\sum \xi^{f_i}}.$$

This is independent of the decomposition of f as $\sum f_i$. Hence our action is well-defined. Composing with the canonical map from $\mathbf{A}$ to $\mathbf{A}/(m)$, we can thus assign $\mathbf{A}$-module structure to $\mathrm{Gal}(K_m/k_m)$. This allow us to view $\mathrm{Gal}(K_m/k_m)$ as an $\mathbf{A}$-module from now on. We check these conditions in Proposition 1.6 below.

PROPOSITION 1.6. $\mathrm{Gal}(K_m/k_m)$ *(or* H_m*) is identified as a finite* **A**- *submodule of* Λ_m *except for the case:* $q = 2$ *and* $t(t+1) \mid m$.

Proof. To check that the action is independent of decomposition, suppose that $\xi \in \mathrm{H}_m \subset \Lambda_m, f \in \mathbf{A}$. If $f = \sum_i f_i = \sum_j g_j$ with $(f_i, m) = 1$, $(g_j, m) = 1$ for all i, j, then by Proposition 1.5

$$f \cdot \psi_\xi = \sum f_i \cdot \psi_\xi = \sum \psi_{\xi^{f_i}} = \psi_{\sum \xi^{f_i}} = \psi_{\sum \xi^{g_j}} = \sum \psi_{\xi^{g_j}} = \sum g_j \cdot \psi_\xi.$$

To check that H_m (or $\mathrm{Gal}(K_m/k_m)$) is an **A**-module under this action

(1) H_m is an abelian group.

(2) For $\xi_1, \xi_2 \in \mathrm{H}_m \subset \Lambda_m$,

$$\begin{aligned} f \cdot (\psi_{\xi_1} + \psi_{\xi_2}) &= f \cdot \psi_{\xi_1 + \xi_2} \\ &= \psi_{(\xi_1+\xi_2)^f} = \psi_{\xi_1^f} + \psi_{\xi_2^f} = f \cdot \psi_{\xi_1} + f \cdot \psi_{\xi_2}. \end{aligned}$$

(3) Let $f, g \in \mathbf{A}, \xi \in \mathrm{H}_m$ and let $f = \sum f_i, g = \sum g_j$, with $(f_i, m) = (g_j, m) = 1$ for all i, j. Then

$$\begin{aligned} (f \cdot g) \cdot \psi_\xi &= \left(\sum_{i,j} f_i \cdot g_j \right) \cdot \psi_\xi \\ &= \sum_{i,j} \psi_{\xi^{f_i \cdot g_j}} \, (\text{since } (f_i \cdot g_j, m) = 1). \end{aligned}$$

$$\begin{aligned} f \cdot (g \cdot \psi_\xi) &= f \cdot \left(\sum_j \psi_{\xi^{g_j}} \right) = \sum_i f_i \cdot \left(\sum_j \psi_{\xi^{g_j}} \right) \\ &= \sum_{i,j} \psi_{\xi^{f_i \cdot g_j}} = (f \cdot g) \cdot \psi_\xi. \end{aligned}$$

$$(f + g) \cdot \psi_\xi = \sum_i f_i \cdot \psi_\xi + \sum_j g_j \cdot \psi_\xi = f \cdot \psi_\xi + g \cdot \psi_\xi.$$

Thus H_m (or $\mathrm{Gal}(K_m/k_m)$) is an **A**-module under this action and we are done. □

We now have

THEOREM 1.7. *In the following, if $q = 2$, we assume $t(t+1) \nmid m$. Then we have*

(1) *The Galois group* $\mathrm{Gal}(K_m/k_m)$ *(or* H_m*) is isomorphic to* $\mathbf{A}/(z)$*, for some* $z \in \mathbf{A}$ *such that* $z|m$.

(2) *Suppose that $p(t)$ is a monic irreducible in* **A**. *If $X^{p(t)} = a$ has one solution $X = c$ in* **A**, *then* $\mathrm{H}_{p(t)} = \{0\}$ *and $c|a$. Otherwise,* $\mathrm{H}_{p(t)} = \Lambda_{p(t)} \cong \mathbf{A}/(p(t))$.

(3) *Suppose that m, n are two monic square-free relatively prime polynomials in* **A**. *Then $K_{m\cdot n} = K_m \cdot K_n, K_m$ and K_n are linearly disjoint over base field k*

(4) *Suppose that m is monic and square-free in* **A**. *Let z be the largest divisor of m such that the equation $X^z = a$ has solution $X = b$ in* **A**. *Then the polynomial $X^{m/z} - b$ is irreducible over* **A**, *and* $\mathrm{H}_m \cong \mathbf{A}/(m/z)$.

(5) *The field of constants of K_m is $\mathbb{F}_q$.*

Proof. First, (1) follows directly from Proposition 1.6.

To prove (2), by (1) we have $\mathrm{H}_{p(t)} = \{0\}$ or $\mathrm{H}_{p(t)} = \Lambda_{p(t)} \cong \mathbf{A}/(p(t))$. If $X^{p(t)} = a$ has one solution $X = c$ in **A**, then all the roots of $X^{p(t)} = a$ belong to $k_{p(t)}$. This implies $\mathrm{H}_{p(t)} \cong \{0\}$. Also clearly $c|a$ (by the expansion of $X^{p(t)}$). Otherwise, if equation $X^{p(t)} = a$ has no solution in **A**, it suffices to show that $X^{p(t)} = a$ has no solution X in $k_{p(t)}$. Suppose that $X^{p(t)} = a$ has one solution $X = \alpha, \alpha \in k_{p(t)} - k$, then all solutions of $X^{p(t)} = a$ are in $k_{p(t)}$. Let us take $\beta = -\mathrm{Tr}_{k_{p(t)}/k}(\alpha)$, then one has $\beta^{p(t)} = -(q^{\deg p(t)} - 1)a = a$ and $\beta \in \mathbf{A}$. This contradicts the assumption and we are done.

To prove (3), given nonzero polynomial $d \in \mathbf{A}$, let us denote all the roots of $X^d = a$ in K_d by R_d. Suppose that $\alpha \in \mathrm{R}_m, \beta \in \mathrm{R}_n$, then $\alpha^m = a, \beta^n = a$. Let us take $e, f \in \mathbf{A}$ such that $me + nf = 1$, and let $\theta = \alpha^f + \beta^e \in K_m \cdot K_n$. Then $\theta^{m\cdot n} = (\alpha^m)^{nf} + (\beta^n)^{me} = a$. This implies that $\theta \in K_{m\cdot n}$, hence $K_m \cdot K_n \supseteq K_{m\cdot n}$ (since $K_{m\cdot n} = k_{m\cdot n}(\theta)$). Conversely, suppose that $\theta \in \mathrm{R}_{m\cdot n}$, then $\theta^n \in \mathrm{R}_m$, $\theta^m \in \mathrm{R}_n$. This implies that $K_m \cdot K_n \subseteq K_{m\cdot n}$.

To prove linearly disjointness, we suppose that $\theta \in \mathrm{R}_{m\cdot n}$, let $\alpha = \theta^n \in \mathrm{R}_m, \beta = \theta^m \in \mathrm{R}_n$. By (1), we have $\mathrm{H}_{m\cdot n} = \Lambda_z$ for some z dividing $m \cdot n$, and write Λ_z as a direct sum $\Lambda_{z_1} \oplus \Lambda_{z_2}$, where $z = z_1 z_2, z_1|m, z_2|n$. We contend that $\mathrm{H}_m = \Lambda_{z_1}$ and $\mathrm{H}_n = \Lambda_{z_2}$. Let $\sigma \in \mathrm{Gal}(K_{m\cdot n}/k_m)$ with $\sigma(\theta) = \theta + \xi_1 + \xi_2$, where $\xi_1 \in \Lambda_{z_1}, \xi_2 \in \Lambda_{z_2}$. Since $\alpha = \theta^n \in \mathrm{R}_m$ and ${\xi_2}^n = 0$, we have $\sigma(\alpha) = \sigma(\theta^n) = (\theta + \xi_1 + \xi_2)^n = \alpha + {\xi_1}^n$. This implies that ${\xi_1}^n \in \mathrm{H}_m$. Since $(m, n) = 1$, it follows that $\xi_1 \in \mathrm{H}_m$. We have $\Lambda_{z_1} \subset \mathrm{H}_m$. Conversely, suppose $\xi' \in \mathrm{H}_m$. Since $(m, n) = 1$, by ramification theory of k_{mn}, we know that K_m and k_{mn} are linearly disjoint over k_m. Then there exists $\sigma' \in \mathrm{Gal}(K_m k_{mn}/k_m)$ such that $\sigma' =$ identity on k_{mn} and $\sigma'(\alpha) = \alpha + \xi'$. We extend σ' to $\sigma \in \mathrm{Gal}(K_{mn}/k_{mn})$. Then we also have $\sigma(\alpha) = \alpha + \xi'$. Now if $\sigma(\theta) = \theta + \xi_1 + \xi_2$, where $\xi_1 \in \Lambda_{z_1}, \xi_2 \in \Lambda_{z_2}$, then

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

$\sigma(\alpha) = \sigma(\theta^n) = (\theta + \xi_1 + \xi_2)^n = \alpha + {\xi_1}^n$. Thus we have $\xi' = \xi_1^n \in \Lambda_{z_1}$; hence $\mathrm{H}_m \subset \Lambda_{z_1}$. Therefore, we have $\mathrm{H}_m = \Lambda_{z_1}$ and also $\mathrm{H}_n = \Lambda_{z_2}$. Since k_m and k_n are linearly disjoint over the base field k ([6, Theorem 2.3]), this shows that $[K_m : k] \cdot [K_n : k] = [K_m \cdot K_n : k]$, hence the the conclusion of (3).

To prove (4), let z be the largest divisor of m such that equation $X^z = a$ has solution $X = b$ in **A**. By (3), we have

$$[K_m : k_m] = \prod_{l(t)|m, l\nmid z} [K_{l(t)} : k_{l(t)}] = \deg(X^{m/z} - b).$$

Thus (4) follows from Lemma 1.4 and (2) of this theorem by degree considerations.

For the proof of (5), from [6], we know that the field of constants of k_m is $\mathbb{F}_q$. From (1) , we know that the field of constants of K_m is either $\mathbb{F}_q$ or $\mathbb{F}_{q^p}$ (since H_m is an elementary p-group). Suppose that the field of constants of K_m is $\mathbb{F}_{q^p}$. Then there are two Galois subextensions $k'_m/k_m, K'_m/k_m$ of K_m/k_m such that $k'_m \cong k_m \otimes_{\mathbb{F}_q} \mathbb{F}_{q^p}$, $K'_m \cap k'_m = k_m$, and $\mathrm{H}_m \cong \mathrm{Gal}(k'_m/k_m) \times \mathrm{Gal}(K'_m/k_m)$. Since $k'_m \cong k_m \otimes_{\mathbb{F}_q} \mathbb{F}_{q^p}$, the action of $\mathrm{Gal}(k_m/k)$ on $\mathrm{Gal}(k'_m/k_m)$ is trivial. By Proposition 1.5, this contradicts the action of $\mathrm{Gal}(k_m/k)$ on H_m. This completes the proof. □

In the case $q = 2$, the situation is more subtle.

EXAMPLE. Let $\mathbf{A} = \mathbb{F}_2[t]$, $k = \mathbb{F}_2(t)$. Then

(1) It may happen $K_t = K_{t+1}$. For example, if $a = t^2 + t + 1$, then $K_t = K_{t+1} = \mathbb{F}_4(t)$; if $a = t^3$, then $K_t = K_{t+1} \neq \mathbb{F}_4(t)$ and $[Kt :\ k] = 2$.
(2) $K_t = \mathbb{F}_4(t)$ (resp. $K_{t+1} = \mathbb{F}_4(t)$) if and only if $a = t^2(f^2 + f + 1)$ (resp. $a = (t+1)^2(f^2 + f + 1)$) for some $f \in k$.

2. Estimating discriminants

Let ∞ be the place at infinity of our rational function field $k = \mathbb{F}_q(t)$, with $\frac{1}{t}$ as its uniformizer. Let a be a nonzero element in **A** fixed throughout as before. We consider monic square-free nonzero polynomial m in **A**. Given m, we let $z = z(m, a)$ be the largest divisor of m such that the equation $X^z = a$ has solution $X = b$ in **A** (note that $b \neq 0$ because $a \neq 0$), and set $r = m/z$. The degree of the extension K_m over k will be denoted by N_m. In this section, our purpose is to get an upper bound for the totall degree d_m of the discriminant divisor $\Delta(K_m/k)$.

PROPOSITION 2.1. *Given monic square-free nonzero polynomial m in* **A**. *Then we have*

(1) $\Delta(k_m/k) | (\infty \cdot m)^{[k_m : k]}$.
(2) *The finite part of the discriminant $\Delta(K_m/k)$ divides $(m \cdot r)^{\mathrm{N}_m}$.*

Proof. To prove (1), let $\mathfrak{P}$ be a prime divisor of k, and let $e_{\mathfrak{P}}(k_m/k)$ denote the ramification index at $\mathfrak{P}$ of k_m/k. We know that every prime divisor of k except

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

∞ and the prime divisors $\mathfrak{P}$ dividing (m) is unramified in k_m. By [6, Thm 3.2], ramification index $e_\infty(k_m/k)$ is equal to $\Pi_{\mathfrak{P}|(m)}(q-1)$; by the discriminant formula in the case that (char.k, $e_\infty(k_m/k)$)=1, we have the ∞-part of $\Delta(k_m/k)$ is precisely equal to ∞^{d_1}, where

$$d_1 = \frac{e_\infty(k_m/k) - 1}{e_\infty(k_m/k)} \cdot [k_m : k].$$

For prime divisors $\mathfrak{P}$ dividing (m), the $\mathfrak{P}$-factor of $\Delta(k_m/k)$ is equal to $\mathfrak{P}^{d_2}$, where

$$d_2 = (q^{\deg \mathfrak{P}} - 2) \cdot [k_{\frac{m}{p(t)}} : k] = \frac{q^{\deg \mathfrak{P}} - 2}{q^{\deg \mathfrak{P}} - 1} \cdot [k_m : k]$$

(by [6], Theorem 4.1). Combining these, we obtain that the discriminant $\Delta(k_m/k)$ divides $(\infty \cdot m)^{[k_m:k]}$ (note that m is square-free).

To prove (2), let $f(X) = X^r - b$, and let α be a root of equation $f(X) = 0$ in K_m. Since $f'(\alpha) = r$, $\mathrm{Norm}_{K_m/k_m}(f'(\alpha)) \mid (r)^{q^{\deg r}}$, the finite part of discriminant $\Delta(K_m/k_m)$ divides $(r)^{q^{\deg r}}$. By transitivity of discriminants and (1) of this theorem, we obtain the finite part of the discriminant $\Delta(K_m/k)$ divides $((m)^{[k_m:k]})^{q^{\deg r}} \cdot \mathrm{Norm}_{k_m/k}((r)^{q^{\deg r}})$, which is equal to $(m \cdot r)^{\mathrm{N}_m}$. This completes the proof. □

PROPOSITION 2.2. *Let* $\mathrm{ord}_\infty(\cdot)$ *denote the normalized discrete valuation of* k *at* ∞ (*i.e.*, $\mathrm{ord}_\infty(\frac{1}{t}) = 1$), *and extended to* K_m *in the usual way. We have*

(1) *Suppose that* ∞_1 *is a prime divisor of* k_m *sitting over* ∞. *Then the ramification index* $e_{\infty_1}(K_m/k_m) \leqslant \max\{q \cdot \deg a,\ 1\} \leqslant q \cdot \deg a + 1$.

(2) *If* $\alpha \in K_m$ *is a root of* $X^r - b = 0$ (*note* $b \neq 0$ *here*), *then*

$$|\mathrm{ord}_\infty(\alpha)| \leqslant \deg r + \deg b \leqslant \deg m + \deg a.$$

(3) *If* $0 \neq \xi \in \Lambda_r$, *then* $-\frac{1}{q-1} \leqslant \mathrm{ord}_\infty(\xi) \leqslant \deg r$; *hence* $|\mathrm{ord}_\infty(\xi)| \leqslant \deg m$.

Proof. To prove (1), let $f(X) = X^r - b = -b + (\sum_{i=0}^{-1+\deg r} c_i X^{q^i}) + X^{q^{\deg r}}$, $f(\alpha) = 0$, where $c_i \in \mathbf{A}$ with $\deg c_i = (-i + \deg r) \cdot q^i$ and $c_0 = r$. To draw Newton polygon, we consider the following sequence of points in the real plane: $O = (0,0)$, $B_0 = (1, \mathrm{ord}_\infty(\frac{c_0}{b})), B_1 = (q^1, \mathrm{ord}_\infty(\frac{c_1}{b})), \ldots, B_i = (q^i, \mathrm{ord}_\infty(\frac{c_i}{b})), \ldots,\ B_{\deg r} = (q^{\deg r}, \mathrm{ord}_\infty(\frac{1}{b}))$, and computing these as $(0,0)$, $(1, \deg b - \deg r), (q^1, \deg b - (\deg r - 1)q^1)), \ldots, (q^i, \deg b - (\deg r - i)q^i)), \ldots,$ $(q^{\deg r}, \deg b)$. We have slopes: $s(O, B_0) = \deg b - \deg r, s(B_0, B_1) = 1 + \frac{1}{q-1} - \deg r, \ldots, s(B_{i-1}, B_i) = i + \frac{1}{q-1} - \deg r, \ldots, s(B_{\deg r - 1}, B_{\deg r}) = \frac{1}{q-1}$, and $s(O, B_0) = \deg b - \deg r, s(O, B_1) = \frac{\deg b}{q} + 1 - \deg r, \ldots, s(O, B_i) = \frac{\deg b}{q^i} + i - \deg r, \ldots, s(O, B_{\deg r}) = \frac{\deg b}{q^{\deg r}}$. Thus the slopes sequence $s(B_0, B_1), s(B_1, B_2), \ldots,$ $s(B_{i-1}, B_i), \ldots, s(B_{\deg r-1}, B_{\deg r})$ increases. Therefore if $\deg b = 0$, then we obtain that ∞_1 is unramified in K_m (by [6, Theorem 3.2], $s(O, B_0) = -\deg r$ and

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

the fact that the denominators of these slopes are $q-1$). Otherwise suppose that $q^{d-1} < \deg b \leqslant q^d$ for some integer d, and let $s(O, B_i) = \frac{\deg b}{q^i} + i - \deg r$ be the minimum slope of the convex hull of the Newton polygon of $f(X)$, then we have $i \leqslant d$. By considering the denominators of slopes of the convex hull, we have $e_{\infty_1}(K_m/k_m) \leqslant q^i \leqslant q \cdot \deg b$. Since $b^z = a$, by the expansion of X^z we must have $b|a$. Combine these with $\deg b \leqslant \deg a$, we obtain the inequality of (1).

To prove (2), if $\deg r \neq 0$, because these slopes $s(B_0, B_1), s(B_1, B_2), \ldots, s(B_{i-1}, B_i), \ldots, s(B_{\deg r-1}, B_{\deg r})$ and $s(O, B_0)$, $s(O, B_1), \ldots, s(O, B_i), \ldots, s(O,\ B_{\deg r})$ are all between $-(\deg r + \deg b)$ and $(\deg r + \deg b)$, then $|\mathrm{ord}_\infty(\alpha)| \leqslant \deg r + \deg b$. Otherwise, if $\deg r = 0$ (i.e., $r = 1 \in \mathbb{F}_q$), then

$$|\mathrm{ord}_\infty(\alpha)| = |\mathrm{ord}_\infty(b)| = \deg b \leqslant \deg r + \deg b.$$

To prove (3), consider the Newton polygon of polynomial X^r/X. Since $X^r/X = c_0 + (\sum_{i=1}^{-1+\deg r} c_i X^{q^i - 1}) + X^{q^{\deg r}-1}$, where $c_i \in \mathbf{A}$ with $\deg c_i = (-i + \deg r) \cdot q^i$ and $c_0 = r$. We consider the following points sequence: $B_1 = (q-1, \mathrm{ord}_\infty(c_1/c_0))$ $= (q-1, \deg r - (\deg r - 1) \cdot q)$, $B_2 = (q^2 - 1, \mathrm{ord}_\infty(c_2/c_0)) = (q^2 - 1, \deg r - (\deg r - 2) \cdot q^2)$, …, $B_i = (q^i - 1, \mathrm{ord}_\infty(c_i/c_0)) = (q^i - 1, \deg r - (\deg r - i) \cdot q^i)$, …, $B_{\deg r} = (q^{\deg r} - 1, \mathrm{ord}_\infty(\frac{c_{\deg r}}{c_0})) = (q^{\deg r} - 1, \deg r)$, and compute the slopes: $s(O, B_1) = 1 - \deg r + \frac{1}{q-1}, s(B_1, B_2) = 2 - \deg r + \frac{1}{q-1}, \ldots, s(B_{i-1}, B_i) = i - \deg r + \frac{1}{q-1}, \ldots, s(B_{\deg r-1}, B_{\deg r}) = \frac{1}{q-1}$. Since sequence $s(O, B_1), s(B_1, B_2), \ldots$, $s(B_{i-1}, B_i), \ldots, s(B_{\deg r-1}, B_{\deg r})$ increases and they are between $-\deg r$ and $\frac{1}{q-1}$, so we get the inequality of (3). □

Let $\mathcal{O} \subset k$ be the local ring at the place ∞, and let us denote the integral closure of $\mathcal{O}$ in K_m (resp. k_m) by $\mathcal{O}_a$ (resp. $\mathcal{O}_m$). Then we have

THEOREM 2.3. *The ∞-part of the discriminant $\Delta(K_m/k)$ divides*

$$\infty^{[1+2\deg m + \deg a + q \cdot \deg a \cdot (\deg a + 2\deg m)] \cdot \mathrm{N}_m}.$$

Proof. Let ∞_1 be a prime divisor of $\mathcal{O}_m$ lying over ∞. Let K_{∞_1} be the subextension of K_m/k_m such that K_{∞_1}/k_m is the maximal subextension of K_m/k_m unramified at prime divisor ∞_1. By Proposition 2.2 (1), we have $\mathrm{Gal}(K_m/K_{\infty_1}) \cong (Z/p\mathbb{Z})^d$ with $p^d \leqslant q \cdot \deg a + 1$. Let $\alpha \in K_m$ be a root of $X^r - a = 0$, and denote its monic minimal polynomial over K_{∞_1} by $f(X)$. We may assume $\mathrm{Gal}(K_m/k_m) \cong \Lambda_r$, $\mathrm{Gal}(K_m/K_{\infty_1}) \cong \mathrm{R}$, a subgroup of Λ_r with $\#(\mathrm{R}) = p^d$. Then we have

$$f(X) = \prod_{\xi \in R} (X - \alpha + \xi).$$

Since R is a d-dimensional vector space over $\mathbb{F}_p$, so we obtain that

$$f(X) = (X - \alpha)^{p^d} + \sum_{i=1}^{d} c_i (X - \alpha)^{p^{d-i}}$$

$$= X^{p^d} + \left(\sum_{i=1}^{d} c_i X^{p^{d-i}}\right) - \left(\alpha^{p^d} + \sum_{i=1}^{d} c_i \alpha^{p^{d-i}}\right),$$

where $c_i \in K_{\infty_1}$ and $c_d = \Pi_{\xi \in R-\{0\}}\xi$.

According to Proposition 2.2 (2), $\mathrm{ord}_\infty((1/t)^{\deg m+\deg a} \cdot \alpha) \geqslant 0$; this implies that $(1/t)^{\deg m+\deg a} \cdot \alpha \in \mathcal{O}_a$. Let $\mathcal{O}_{\infty_1}$ be the integral closure of $\mathcal{O}$ in K_{∞_1}. Let $g(X) = (1/t)^{p^d\cdot(\deg m+\deg a)} \cdot f(t^{\deg m+\deg a} \cdot X)$. Then $g(X)$ is the monic minimal polynomial of $(1/t)^{\deg m+\deg a} \cdot \alpha$ over K_{∞_1} and $g(X) \in \mathcal{O}_{\infty_1}[X]$. Since $g'((1/t)^{\deg m+\deg a} \cdot \alpha)$ is equal to $(1/t)^{p^d\cdot(\deg m+\deg a)} \cdot c_d$, so the ∞_1-part of $\Delta(\mathcal{O}_a/\mathcal{O}_m)$ divides (by transitivity of discriminants)

$$\begin{aligned}&\mathrm{Norm}_{K_{\infty_1}/k_m}(\mathrm{Norm}_{K_m/K_{\infty_1}}((1/t)^{p^d\cdot(\deg m+\deg a)} \cdot c_d))\\ &\quad = \mathrm{Norm}_{K_{\infty_1}/k_m}((1/t)^{p^d\cdot(\deg m+\deg a)} \cdot c_d)^{p^d},\end{aligned}$$

which is equal to $(1/t)^{p^d\cdot(\deg m+\deg a)\cdot[K_m:k_m]} \cdot (c_d)^{[K_m:k_m]}$. By Proposition 2.2 (3), the ∞_1-part of $\Delta(\mathcal{O}_a/\mathcal{O}_m)$ divides

$$(1/t)^{p^d\cdot(\deg m+\deg a)\cdot[K_m:k_m]} \cdot (1/t)^{p^d\cdot\deg m\cdot[K_m:k_m]},$$

which is equal to $(1/t)^{p^d\cdot(2\deg m+\deg a)\cdot[K_m:k_m]}$. Changing all places ∞_1 of $\mathcal{O}_m$ sitting over ∞, we obtain $\Delta(\mathcal{O}_a/\mathcal{O}_m)$ divides $(1/t)^{p^d\cdot(2\deg m+\deg a)\cdot[K_m:k_m]}$ (because $\mathcal{O}$ is the local ring at place ∞). Using the transitivity of discriminants and Proposition 2.1 (1), we obtain that the ∞-part of the discriminant $\Delta(K_m/k)$ divides

$$\mathrm{Norm}_{k_m/k}((1/t)^{p^d\cdot(2\deg m+\deg a)\cdot[K_m:k_m]}) \cdot ((1/t)^{[k_m:k]})^{[K_m:k_m]},$$

which is equal to $\infty^{(1+p^d\cdot(2\deg m+\deg a))\cdot \mathrm{N}_m}$. Since $p^d \leqslant q \cdot \deg a + 1$, we complete the proof.

Our main theorem in this section is

THEOREM 2.4. *The discriminant* $\Delta(K_m/k)$ *divides*

$$(m)^{2\mathrm{N}_m} \cdot \infty^{[1+2\deg m+\deg a+q\cdot\deg a\cdot(\deg a+2\deg m)]\cdot\mathrm{N}_m}.$$

Moreover, we have $\frac{\mathrm{d}_m}{\mathrm{N}_m} = O(\deg m)$, *as* $\deg m \to \infty$.

Proof. It follows from Proposition 2.1 (2), Theorem 2.3 and $r|m$.

3. A generalized Artin's problem for function fields

In this section we work out a generalized Artin's problem for function fields. We will make use of an effective version of the Prime Number Theorem, see [10].

Let L, K be two fixed function fields over k, and the field of constants of K is $\mathbb{F}_q$. Let S_L be a set of prime divisors of L. For each prime divisor $\mathfrak{L} \in \mathrm{S}_L$, let $K_{\mathfrak{L}}$ be a fixed finite Galois extension of K. Our generalized Artin’s problem is to determine the density of the set of prime divisors in K which do not split completely in any $K_{\mathfrak{L}}$ for $\mathfrak{L} \in \mathrm{S}_L$.

Let S_L^* be the set of all square free divisors (including 1) composed from all the prime divisors in S_L (i.e., $\flat \in \mathrm{S}_L^*$ if and only if $\flat = 1$ or $\flat$ can be written as a finite product of distinct prime divisors in S_L). On S_L^*, we have a natural partial order ‘$\leqslant$’ defined as follows: $\flat_1, \flat_2 \in \mathrm{S}_L^*, \flat_1 \leqslant \flat_2$ if and only if $\flat_1 | \flat_2$. Under this partial ordering we view S_L^* as a (Boolean) lattice. Given divisor $\flat \in \mathrm{S}_L^*$, let $K_\flat = \prod_{\mathfrak{L}|\flat} K_{\mathfrak{L}}$ (set $K_1 = K$), $\mathrm{N}_\flat = [K_\flat : K]$, and $\mathrm{d}_\flat = \deg \Delta(K_\flat/k)$. Let $f_\flat$ be the degree of the field of constants of $K_\flat$ over $\mathbb{F}_q$. These ideas follow [12] in their context and construction.

Given positive integer x, let $f(x, K)$ be the number of prime divisors $\mathfrak{P}$ of K such that $\deg \mathfrak{P} = x$, and $\mathfrak{P}$ does not split completely in any $K_{\mathfrak{L}}$ for all $\mathfrak{L} \in \mathrm{S}_L$. Also set

$$\delta_{\mathrm{S}_L} = \sum_{\flat \in \mathrm{S}_L^*} \frac{\mu(\flat)}{\mathrm{N}_\flat},$$

where μ is the möbius function defined by $\mu(\flat) = (-1)^n$, if $\flat = \prod_{i=1}^n \mathfrak{L}_i$. Then we have

THEOREM 3.1. *Suppose that* $\Sigma_{\flat \in \mathrm{S}_L^*}(1/\mathrm{N}_\flat) < \infty$, *and for each prime divisor* $\mathfrak{P}$ *of* K, *the number of* $\mathfrak{L} \in \mathrm{S}_L$ *such that* $\mathfrak{P}$ *splits completely in* $K_{\mathfrak{L}}$ *is finite. Also suppose that the following three conditions are true*

(a) $f_\flat = 1$ *for all* $\flat \in \mathrm{S}_L^*$.

(b) *As* $\deg \flat \to \infty$, $(\mathrm{d}_\flat/\mathrm{N}_\flat = O(\deg \flat)$, *and* $\mathrm{N}_\flat = O(q^{e \cdot \deg \flat})$ *for some constant* $e > 0$.

(c) *There exists a real number* $\nu(\nu > (1/\ln q))$ *such that: The number of prime divisors* $\mathfrak{P}$ *of* K *with* $\deg \mathfrak{P} = x$, *and* $\mathfrak{P}$ *splits completely in some* $K_{\mathfrak{L}}$, $\deg \mathfrak{L} > x/2 - \nu \ln x$ *is* $o(q^x/x)$.

Then we have

$$f(x, K) = \delta_{\mathrm{S}_L} \cdot \frac{q^x}{x} + o\left(\frac{q^x}{x}\right).$$

Proof. For each prime divisor $\mathfrak{P}$ in K, we let $c_{\mathfrak{P}}$ be the product of all prime divisors $\mathfrak{L} \in \mathrm{S}_L$ such that $\mathfrak{P}$ splits completely in $K_{\mathfrak{L}}$.

Given positive integer x and $\flat \in \mathrm{S}_L^*$. We denote the number of prime divisors $\mathfrak{P}$ of K such that $\deg \mathfrak{P} = x$ and $c_{\mathfrak{P}} = \flat$ by $f(x, \flat)$, and denote the number of prime divisors $\mathfrak{P}$ of K such that $\deg \mathfrak{P} = x$ and $\flat | c_{\mathfrak{P}}$ by $\pi_1(x, \flat)$. Then we have

$$\pi_1(x, \flat') = \sum_{\flat \in \mathrm{S}_L^*, \flat' | \flat} f(x, \flat).$$

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

Applying Möbius inversion formula ([12], Corollaries of Proposition 5), we obtain that

$$f(x,\flat') = \sum_{\flat\in \mathrm{S}_L^*,\flat'|\flat} \mu(\flat/\flat')\pi_1(x,\flat).$$

If $\flat' = 1$, then we get that

$$f(x,K) = f(x,1) = \sum_{\flat\in \mathrm{S}_L^*} \mu(\flat)\pi_1(x,\flat).$$

Given positive integer d, let $\mathrm{S}_{L,d}$ be the set of $\mathfrak{L} \in \mathrm{S}_L$ with $\deg \mathfrak{L} \leqslant d$, and let $n(x,d)$ denote the number of prime divisors $\mathfrak{P}$ of K with $\deg \mathfrak{P} = x$ and $\mathfrak{P}$ does not split completely in any $K_{\mathfrak{L}}$, $\mathfrak{L} \in \mathrm{S}_{L,d}$. By inclusion-exclusion principle, we have

$$n(x,d) = \sum_{\flat\in \mathrm{S}_{L,d}^*} \mu(\flat)\pi_1(x,\flat), \tag{3.1}$$

where $\mathrm{S}_{L,d}^*$ is defined in the same way as S_L^*. By definition, we also have

$$f(x,K) \leqslant n(x,d). \tag{3.2}$$

Given positive integers d_1, d_2, let $m(x,d_1,d_2)$ be the number of prime divisors $\mathfrak{P}$ in K with $\deg \mathfrak{P} = x$ and $\mathfrak{P}$ splits completely in some $K_{\mathfrak{L}}$, $\mathfrak{L} \in \mathrm{S}_L, d_1 < \deg \mathfrak{L} \leqslant d_2$. Let $g(x)$ be the largest number n such that there exists prime divisor $\mathfrak{P}$ in K with $\deg \mathfrak{P} = x$, $\mathfrak{P}$ splits completely in some $K_\flat$ ($\flat \in \mathrm{S}_L^*$) with $\deg \flat = n$. This implies

$$f(x,K) \geqslant n(x,d) - m(x,d,g(x)). \tag{3.3}$$

We write

$$m(x,d,g(x)) \leqslant \left\{ \sum_{\substack{\mathfrak{L}\in \mathrm{S}_L \\ d<\deg \mathfrak{L} \leqslant (1/2)x-\nu \ln x}} \pi_1(x,\mathfrak{L}) \right\} + m(x,(1/2)x-\nu \ln x, g(x)). \tag{3.4}$$

Let $\pi^\flat(x)$ denote the number of prime divisors $\mathfrak{P}_\flat$ in $K_\flat$ with $\deg \mathfrak{P}_\flat = x$. One has $\pi_1(x,\flat) \leqslant \pi^\flat(x)/\mathrm{N}_\flat$. By [10, p. 55], we have $|\pi^\flat(x) - q^x/x| \leqslant 6.5 \cdot q^{x/2} \cdot \mathrm{d}_\flat$. Hence

$$\pi_1(x,\flat) \leqslant \frac{1}{\mathrm{N}_\flat} \cdot \frac{q^x}{x} + 6.5 \cdot q^{x/2} \cdot \frac{\mathrm{d}_\flat}{\mathrm{N}_\flat}. \tag{3.5}$$

$$\begin{aligned}&\sum_{\substack{\mathfrak{L}\in \mathrm{S}_L\\ d<\deg\,\mathfrak{L}\leqslant(1/2)x-\nu\ln x}} \pi_1(x,\mathfrak{L})\\ &\leqslant \sum_{\substack{\mathfrak{L}\in \mathrm{S}_L\\ d<\deg\mathfrak{L}\leqslant(1/2)x-\nu\ln x}} \left\{\frac{1}{\mathrm{N}_{\mathfrak{L}}}\cdot\frac{q^x}{x}+6.5q^{x/2}\cdot\frac{\mathrm{d}_{\mathfrak{L}}}{\mathrm{N}_{\mathfrak{L}}}\right\}.\end{aligned}\tag{3.6}$$

By condition (b) and the hypothesis $\nu > \frac{1}{\ln q}$, we have

$$\sum_{\substack{\mathfrak{L}\in \mathrm{S}_L\\ d<\deg\,\mathfrak{L}\leqslant(1/2)x-\nu\ln x}} 6.5\cdot q^{x/2}\cdot\frac{\mathrm{d}_{\mathfrak{L}}}{\mathrm{N}_{\mathfrak{L}}} \ll q^{x/2} \sum_{\substack{\mathfrak{L}\in \mathrm{S}_L\\ d<\deg\,\mathfrak{L}\leqslant(1/2)x-\nu\ln x}} \deg\mathfrak{L} = o\left(\frac{q^x}{x}\right).\tag{3.7}$$

We may assume that d (depends on x) goes to infinity (as $x\to\infty$). Using the assumption that $\Sigma_{\mathfrak{b}\in \mathrm{S}_L^*} 1/\mathrm{N}_{\mathfrak{b}} < \infty$, we obtain

$$\sum_{\substack{\mathfrak{L}\in \mathrm{S}_L\\ d<\deg\mathfrak{L}\leqslant(1/2)x-\nu\ln x}} \frac{1}{\mathrm{N}_{\mathfrak{L}}}\cdot\frac{q^x}{x} = o(\frac{q^x}{x}),\quad \text{as } x\to\infty.\tag{3.8}$$

Combine equations (3.6), (3.7) and (3.8), we obtain that

$$\sum_{\substack{\mathfrak{L}\in \mathrm{S}_L\\ d<\deg\mathfrak{L}\leqslant(1/2)x-\nu\ln x}} \pi_1(x,\mathfrak{L}) = o\left(\frac{q^x}{x}\right).\tag{3.9}$$

Combine equations (3.2), (3.3), (3.4), (3.9) and condition (c), we obtain that

$$f(x,K) = n(x,d) + o\left(\frac{q^x}{x}\right).\tag{3.10}$$

Again by [10, p. 55], $f_{\mathfrak{b}} = 1$ (condition (a)) and consider the Galois field extension $K_{\mathfrak{b}}/K$, we have $|\pi_1(x,\mathfrak{b}) - (1/\mathrm{N}_{\mathfrak{b}})\cdot(q^x/x)| \leqslant 6.5\cdot \mathrm{N}_{\mathfrak{b}}\cdot q^{x/2}\cdot \mathrm{d}_{\mathfrak{b}}$. Applying this and equation (3.1), we obtain that

$$\begin{aligned} n(x,d) &= \sum_{\mathfrak{b}\in \mathrm{S}_{L,d}^*} \mu(\mathfrak{b})\pi_1(x,\mathfrak{b})\\ &= \left(\sum_{\mathfrak{b}\in \mathrm{S}_{L,d}^*}\frac{\mu(\mathfrak{b})}{\mathrm{N}_{\mathfrak{b}}}\right)\cdot\frac{q^x}{x} + O\left(q^{x/2}\cdot\sum_{\mathfrak{b}\in \mathrm{S}_{L,d}^*}\mathrm{N}_{\mathfrak{b}}{}^2\cdot\deg\mathfrak{b}\right)\\ &\quad(\text{by condition (b)}).\end{aligned}$$

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

Since $\#(\mathrm{S}_{L,d}) \leqslant c \cdot q^d/d$ for some $c > 0$, $\#(\mathrm{S}^*_{L,d}) \leqslant 2^{c\cdot(q^d/d)}$ and $\deg \flat \leqslant c \cdot q^d$ for $\flat \in \mathrm{S}^*_{L,d}$. Thus we obtain that

$$\begin{aligned} n(x,d) &= \left(\sum_{\flat \in \mathrm{S}^*_{L,d}} \frac{\mu(\flat)}{\mathrm{N}_\flat} \right) \cdot \frac{q^x}{x} \\ &\quad + O(q^{x/2} \cdot 2^{c\cdot(q^d/d)} \cdot q^{2\cdot e \cdot c \cdot q^d} \cdot c \cdot q^d) \text{ (by condition (b))} \\ &= \left(\sum_{\flat \in \mathrm{S}^*_{L,d}} \frac{\mu(\flat)}{\mathrm{N}_\flat} \right) \cdot \frac{q^x}{x} + O(q^{x/2} \cdot q^{n_0 \cdot q^d}), \text{ for some } n_0 > 0. \end{aligned}$$

If we take $d = (\ln x - \ln 3n_0)/\ln q$, then $d \to \infty$ (as $x \to \infty$), and $q^{x/2} \cdot q^{n_0 \cdot q^d} = q^{(x/2)+(x/3)} = o(q^x/x)$. Thus we have

$$n(x,d) = \delta_{\mathrm{S}_L} \cdot \frac{q^x}{x} + o\left(\frac{q^x}{x}\right).$$

Combine this with (3.10) gives what we want. □

4. Artin’s conjecture for the Carlitz module

In this Section, let function fields K, L in Section 3 be the rational function field $\mathbb{F}_q(t)$, let $\mathrm{S} = \mathrm{S}_L$ be the set of all the prime ideals $\mathfrak{L}$ in $\mathbf{A} = \mathbb{F}_q[t]$. As before we use $l(t)$ to denote the monic irreducible generator of the ideal $\mathfrak{L} \in \mathrm{S}_L$. We let $k = \mathbb{F}_q(t), k_\mathfrak{L} = k_{l(t)} = k(\Lambda_{l(t)})$, $K_\mathfrak{L} = k_\mathfrak{L}(\alpha)$, where $\alpha \in \Omega$ satisfies $\alpha^{l(t)} = a, a$ is a fixed nonzero polynomial in $\mathbf{A}$ and let $\mathrm{N}_\mathfrak{L} = \mathrm{N}_{l(t)} = [K_\mathfrak{L} : k]$.

LEMMA 4.1. *Suppose that* $\mathrm{Z} = \{r \in \mathbb{F}_q[t] | r^m = 0$ *for some* $0 \neq m \in \mathbb{F}_q[t]\}$. *Then*

$$\mathrm{Z} = \begin{cases} \{0\} & \text{if } q \neq 2 \\ \{0, 1, t, 1+t\} & \text{if } q = 2 \end{cases}.$$

Moreover, suppose that $a \neq 0$ *in* $\mathbf{A}$ *and* $a \neq 0, 1, t, 1+t$ *if* $\mathbf{A} = \mathbb{F}_2[t]$. *Then we have* $a^m \neq 0$ *for* $0 \neq m \in \mathbf{A}$.

Proof. It is clear that $\mathrm{Z} = \Lambda_m$ for some $0 \neq m \in \mathbf{A}$. Since $k(\Lambda_m) = k$, so $\#((\mathbf{A}/(m))^\times) = 1$. If $q \neq 2$, then $m \in \mathbb{F}_q^\times$; i.e., $\mathrm{Z} = \Lambda_m = \{0\}$. If $q = 2$, then $m = 1, t, 1+t$, or $t(1+t)$; this implies that $\mathrm{Z} = \Lambda_{t(1+t)} = \{0, 1, t, 1+t\}$. This completes the proof.

LEMMA 4.2. *Suppose that a is a nonzero polynomial in* **A** *and $a \neq 1, t, 1+t$ if* $\mathbf{A} = \mathbb{F}_2[t]$. *Let* SC_x *be the number of prime ideals $\mathfrak{P}$ in* **A** *such that* $\deg \mathfrak{P} = x$, *and $\mathfrak{P}$ splits completely in some* $K_{\mathfrak{L}}(\mathfrak{L} \in \mathrm{S}), \frac{x}{2} + \ln x \leqslant \deg \mathfrak{L} \leqslant x$. *Then*

$$\mathrm{SC}_x = o\left(\frac{q^x}{x}\right), \quad \text{as } x \to \infty.$$

Proof. Suppose $\mathfrak{P}$ is a prime divisor in **A** with $\deg \mathfrak{P} = x$ such that $\mathfrak{P}$ splits completely in some $K_{\mathfrak{L}}(\mathfrak{L} \in \mathrm{S}), \frac{x}{2} + \ln x \leqslant \deg \mathfrak{L} \leqslant x$. By Proposition 1.1, $p(t) \equiv 1 (\mathrm{mod}\ l(t)), p(t) | a^{\frac{p(t)-1}{l(t)}}$ and $0 \leqslant \deg \frac{p(t)-1}{l(t)} \leqslant \frac{x}{2} - \ln x$. Hence

$$p(t) | \prod_{\substack{m \text{ monic in } A \\ 0 \leqslant \deg m \leqslant (x/2) - \ln x}} a^m.$$

If $\deg m = i$, then $\deg a^m \leqslant q^i \cdot (\deg a + 1)$ ([6], Prop. 1.1). By the assumption in a and Lemma 4.1, $a^m \neq 0$ for $0 \neq m \in \mathbf{A}$. Thus we have

$$\begin{aligned}
\mathrm{SC}_x &\leqslant \frac{\deg\left(\prod_{\substack{m \text{ monic in } A \\ 0 \leqslant \deg m \leqslant (x/2) - \ln x}} a^m\right)}{x} \\
&\leqslant \frac{\sum_{i=0}^{(x/2) - \ln x} q^i \cdot q^i \cdot (\deg a + 1)}{x} \\
&= O\left(\frac{\sum_{i=0}^{(x/2) - \ln x} q^{2 \cdot i}}{x}\right) \\
&= o\left(\frac{q^x}{x}\right), \quad \text{as } x \to \infty.
\end{aligned}$$

This completes the proof. □

THEOREM 4.3. *Suppose $\nu > 0$. Let $\mathrm{SC}_{x,\nu}$ be the number of prime ideals $\mathfrak{P}$ in* **A** *such that* $\deg \mathfrak{P} = x$, *and $\mathfrak{P}$ splits completely in some* $K_{\mathfrak{L}}(\mathfrak{L} \in \mathrm{S}), \deg \mathfrak{L} > \frac{x}{2} - \nu \cdot \ln x$. *Then*

$$\mathrm{SC}_{x,\nu} = o\left(\frac{q^x}{x}\right), \quad \text{as } x \to \infty.$$

Proof. Let $m(x, d_1, d_2)$ be the number of prime divisors $\mathfrak{P}$ in **A** with $\deg \mathfrak{P} = x$ and $\mathfrak{P}$ splits completely in some $K_{\mathfrak{L}}$, $\mathfrak{L} \in \mathrm{S}, d_1 < \deg \mathfrak{L} \leqslant d_2$. By Proposition 1.1, we have

$$\begin{aligned}
\mathrm{SC}_{x,\nu} &= m(x, \tfrac{1}{2}x - \nu \cdot \ln x, x) \\
&= m(x, \tfrac{1}{2}x - \nu \cdot \ln x, \frac{x}{2} + \ln x) + o\left(\frac{q^x}{x}\right) \quad (\text{by Lemma 4.2}). \quad (4.1)
\end{aligned}$$

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

Let us denote the number of prime divisors $\mathfrak{P}$ in $\mathbf{A}$ such that $\deg \mathfrak{P} = x$ and $\mathfrak{P}$ splits completely in $K_{\mathfrak{L}}$ by $\pi_1(x, \mathfrak{L})$. We have

$$m(x, \tfrac{1}{2}x - \nu \cdot \ln x, \tfrac{1}{2}x + \ln x) \leqslant \sum_{\substack{\mathfrak{L} \in \mathrm{S} \\ (x/2) - \nu \cdot \ln x < \deg g L \leqslant (x/2) + \ln x}} \pi_1(x, \mathfrak{L}). \tag{4.2}$$

Given integer $N \geqslant 0$, nonzero polynomials $a, b \in \mathbf{A}$ with $(a, b) = 1$. Let us denote by $\Pi(N; a, b)$ the number of monic irreducibles $f \in \mathbf{A}$ such that $\deg f = N$, f congruent to $b (\operatorname{mod} a)$. In [9, Theorem 4.3], we have worked out an analogue of the Brun–Titchmarsh Theorem for Arithmetic Progressions in $\mathbf{A}$ as follows

For any positive integer $N > \deg a$, we have

$$\Pi(N; a, b) \leqslant 2 \cdot \frac{q^N}{\phi(a) \cdot (N - \deg a + 1)},$$

where $\phi(a) = \#((\mathbf{A}/(a))^{\times})$.

Now let us go back to $\pi_1(x, \mathfrak{L})$. By Proposition 1.1, we have

$$\pi_1(x, \mathfrak{L}) \leqslant \pi(x; l(t), 1).$$

If $(x/2) - \nu \cdot \ln x < \deg l(t) \leqslant (x/2) + \ln x$, then by the Brun–Titchmarsh Theorem for arithmetic progressions in $\mathbf{A}$, there exists a constant $c > 0$ such that

$$\Pi(x; l(t), 1) \leqslant c \cdot \frac{q^x}{q^{\deg \mathfrak{L}} \cdot x}, \quad \text{for } \frac{x}{2} - \nu \cdot \ln x < \deg \mathfrak{L} \leqslant \frac{x}{2} + \ln x.$$

Thus we obtain that

$$\pi_1(x, \mathfrak{L}) \leqslant c \cdot \frac{1}{q^{\deg \mathfrak{L}}} \cdot \frac{q^x}{x}, \qquad \text{for} \frac{x}{2} - \nu \cdot \ln x < \deg \mathfrak{L} \leqslant \frac{x}{2} + \ln x.$$

Hence we obtain that

$$\sum_{\substack{\mathfrak{L} \in \mathrm{S} \\ (x/2) - \nu \cdot \ln x < \deg g L \leqslant (x/2) + \ln x}} \pi_1(x, \mathfrak{L}) \ll \frac{q^x}{x} \cdot \sum_{\substack{\mathfrak{L} \in \mathrm{S} \\ (x/2) - \nu \cdot \ln x < \deg \mathfrak{L} \leqslant (x/2) + \ln x}} \frac{1}{q^{\deg \mathfrak{L}}},$$

by Prime Number Theorem for polynomials

$$\ll \frac{q^x}{x} \cdot \sum_{(x/2) - \nu \cdot \ln x < i \leqslant (x/2) + \ln x} \frac{1}{i} = o\left(\frac{q^x}{x}\right).$$

Combining this with equations (4.1) and (4.2) gives the proof. □

PROPOSITION 4.4. *Given* $0 \neq a \in \mathbf{A}$, *and* $\mathfrak{L} \in \mathrm{S}$ *with* $\deg \mathfrak{L} = d$. *Then*

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

(1) *If* $q \neq 2$, *and* $d > 1 + (\ln(\deg a + 1)/\ln q)$, *then the equation* $X^{l(t)} = a$ *has no solution* X *in* $\mathbf{A}$(*i.e.*, $\mathrm{Gal}(K_{\mathfrak{L}}/k_{\mathfrak{L}}) \cong \mathbf{A}/\mathfrak{L}$, *and* $\mathrm{N}_{\mathfrak{L}} = (q^d - 1) \cdot q^d)$.

(2) *In the case* $q = 2$ *and* $a \neq 1, t$, *or* $1 + t$, *there exists a positive integer* d_a *(depends on* a*) such that if* $d > d_a$, *then the equation* $X^{l(t)} = a$ *has no solution* X *in* $\mathbf{A}$*(i.e.*, $\mathrm{Gal}(K_{\mathfrak{L}}/k_{\mathfrak{L}}) \cong \mathbf{A}/\mathfrak{L}$, *and* $\mathrm{N}_{\mathfrak{L}} = (2^d - 1) \cdot 2^d)$.

(3) *We have*

$$\sum_{\substack{\text{monic square-free} \\ m \in \mathbf{A}}} \frac{1}{\mathrm{N}_m} < \infty,$$

except in the special case that $\mathbf{A} = \mathbb{F}_2[t]$ *and* $a = 1, t$ *or* $1 + t$.

Proof. Consider the polynomial $f(X) = X^{l(t)} = X^{q^d} + \sum_{i=1}^{d} c_i X^{q^{d-i}}$, where $c_i \in \mathbf{A}$ with $\deg c_i = i \cdot q^{d-i}$. If $0 \neq b \in \mathbf{A}$, then we have $\deg b^{q^d} = \deg b \cdot q^d$, $\deg c_i \cdot b^{q^{d-i}} = (i + \deg b) \cdot q^{d-i}$.

To prove (1), if $\deg b \neq 0$, we have

$$\deg b^{q^d} > \deg c_1 \cdot b^{q^{d-1}} > \cdots > \deg c_i \cdot b^{q^{d-i}} > \cdots > \deg c_d \cdot b.$$

Otherwise ($\deg b = 0$)

$$\deg c_1 \cdot b^{q^{d-1}} > \cdots > \deg c_i \cdot b^{q^{d-i}} > \cdots > \deg c_d \cdot b.$$

Thus if $f(X) = a$ has a solution $X = b$ in $\mathbf{A}$, then we must have $\deg a = \deg b \cdot q^d (\deg b \neq 0), \deg a = q^{d-1} (\deg b = 0)$. Hence if $d > 1 + (\ln(1 + \deg a)/\ln q)$, then the equation $X^{l(t)} = a$ has no solution in $\mathbf{A}$ and by Theorem 1.7 (2), we have $\mathrm{Gal}(K_{\mathfrak{L}}/k_{\mathfrak{L}}) \cong \mathbf{A}/\mathfrak{L}$.

To prove (2), if $X^{l(t)} = a$ has a solution $X = b$ and $\deg b \geqslant 2$ in $\mathbf{A}$, then

$$\deg b^{2^d} > \deg c_1 \cdot b^{2^{d-1}} > \cdots > \deg c_i \cdot b^{2^{d-i}} > \cdots > \deg c_d \cdot b,$$

hence $\deg b^{2^d} = \deg a$. It follows there exists a positive integer d_a such that if $d > d_a$ then the equation $x^{l(t)} = a$ has no solution $X = b$ in $\mathbf{A}$ with $\deg b \geqslant 2$. Otherwise suppose the equation $x^{l(t)} = a$ has a solution $X = b$ in $\mathbf{A}$ with $\deg b \leqslant 1$ (i.e., $b = 1, t$, or $1+t$). In case $b = 1$, since $1^1 = 1, 1^t = 1+t, 1^{t^n} = 1+t$ for any positive integer n; this implies $1^f = 0, 1, t$ or $1 + t$ for any $f \in \mathbf{A}$. Thus $a = 1^{l(t)} = 0, 1, t$ or $1 + t$, this contradicts the assumption. In case $b = t$ (resp. $b = 1 + t$), since $t^1 = t, t^t = 0, t^{t^n} = 0$ (resp. $(1 + t)^1 = 1 + t, (1 + t)^{1+t} = 0$, $(1 + t)^{(1+t)^n} = 0$) for any positive integer n; this implies $t^f = 0$ or t (resp.$(1 + t)^f = 0$ or $1 + t$) for any $f \in \mathbf{A}$. Thus $a = t^{l(t)} = 0$ or t (resp. $a = (1 + t)^{l(t)} = 0$ or $1 + t$), this contradicts the assumption. Combine these and our assumptions give the proof.

To prove (3), since

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

$$\ln\left(\prod_{\mathfrak{L}\in \mathrm{S}}\left(1+\frac{1}{\mathrm{N}_{\mathfrak{L}}}\right)\right) = \sum_{\mathfrak{L}\in \mathrm{S}}\ln\left(1+\frac{1}{\mathrm{N}_{\mathfrak{L}}}\right)$$
$$\leqslant \sum_{\mathfrak{L}\in \mathrm{S}}\frac{1}{\mathrm{N}_{\mathfrak{L}}},$$

By (3) of Theorem 1.7, this implies

$$\sum_{\substack{\text{monic square}-\text{free}\\ m\in\mathbf{A}}}\frac{1}{\mathrm{N}_m} = \prod_{\mathfrak{L}\in \mathrm{S}}\left(1+\frac{1}{\mathrm{N}_{\mathfrak{L}}}\right) < \infty.$$

This completes the proof of Proposition 4.4.

Let C_a be the set of prime ideals $\mathfrak{P}$ in $\mathbf{A}$ for which $\bar{a} = a + \mathfrak{P}$ is a generator of $C(\mathbf{A}/\mathfrak{P})$.

PROPOSITION 4.5. *In the special case* $\mathbf{A} = \mathbb{F}_2[t]$, $0 \neq a \in \mathbb{F}_2[t]$. *Then we have*

(1) $C_1 = \{(t), (1+t), (1+t+t^2)\}$.
(2) *If* $a = f^t$ *for some* $f \in \mathbf{A}$, *then*

$$C_a = \begin{cases} \{(t)\} & \text{if } t \nmid f \\ \emptyset & \text{if } t | f \end{cases}.$$

(3) If $a = f^{1+t}$ for some $f \in \mathbf{A}$, then

$$C_a = \begin{cases} \{(1+t)\} & \text{if } (1+t) \nmid f \\ \emptyset & \text{if } (1+t) | f \end{cases}.$$

(4) $C_t = \{(1+t)\}, C_{1+t} = \{(t)\}$.

Proof. To prove (1), from the proof of Proposition 4.4 (2), we have $1^f = 0, 1, t$, or $1+t$, for $f \in \mathbf{A}$; this implies $C_1 = \{(t), (1+t), (1+t+t^2)\}$.

To prove (2), let $\mathfrak{P}$ be a prime ideal in $\mathbf{A}$. If $\deg p(t) \geqslant 2$, then $p(t) \equiv 1(\operatorname{mod} t)$ and $a(p(t)-1)/t = f^{p(t)-1} \equiv 0(\operatorname{mod} \mathfrak{P})$ (since $C(\mathbf{A}/\mathfrak{P}) \cong \mathbf{A}/(p(t)-1)$). By Proposition 1.2, $\bar{a}$ is not a generator of $C(\mathbf{A}/\mathfrak{P})$.

If $p(t) = t$, since $C(\mathbf{A}/(t)) \cong \mathbf{A}/(t-1)$ (i.e. $h^{t-1} \equiv 0(\operatorname{mod}(t))$ for all $h \in \mathbf{A}$), then $a^g = f^{t\cdot g} \equiv f^g \equiv 0$ or $f(\operatorname{mod}(t))$ for all $g \in \mathbf{A}$. Thus if $t|f$, then $\bar{a}$ is not a generator of $C(\mathbf{A}/(t))$, otherwise ($t \nmid f$), $\bar{a}$ is a generator of $C(\mathbf{A}/(t))$.

If $p(t) = 1+t$, since $C(\mathbf{A}/(1+t)) \cong \mathbf{A}/(t)$, then $a^g = f^{t\cdot g} \equiv 0(\operatorname{mod}(1+t))$. This implies $\bar{a}$ is not a generator of $C(\mathbf{A}/(1+t))$.

The proof of (3) is the same as the proof of (2).

To prove (4), this follows from $t = t^{1+t}, 1+t = (1+t)^t$ and (2), (3) of this theorem.

Let $C_a(x)$ be the number of prime ideals $\mathfrak{P}$ in $\mathbf{A}$ with $\deg \mathfrak{P} = x$ such that $\bar{a}$ is a generator of $C(\mathbf{A}/\mathfrak{P})$, and let

$$\begin{aligned}\delta_a &= \sum_{\substack{\text{monic square-free}\\ \text{polynomials } m \text{ of } \mathbf{A}}} \frac{\mu(m)}{N_m}\\ &= \prod_{\mathfrak{L}\in \mathrm{S}_L}\left(1-\frac{1}{\mathrm{N}_{\mathfrak{L}}}\right), \quad \text{(by (3) of Theorem 1.7)},\end{aligned}$$

except for the special case $q = 2$ and $a = 1, t$, or $1 + t$. In the later cases we let $\delta_a = 0$.

Now the main theorem of this paper is

THEOREM 4.6. *Given nonzero polynomial $a \in \mathbf{A}$. Then if $q \neq 2$, then*

$$C_a(x) = \delta_a \cdot \frac{q^x}{x} + o\left(\frac{q^x}{x}\right).$$

Proof. We apply Theorem 3.1 with $K = L = k$ and let S be the set of all primes of $\mathbf{A}$. By (3) of Proposition 4.4, it suffices to check the three conditions in Theorem 3.1. Condition (a) follows from (5) of Theorem 1.7. Condition (b) follows from Theorem 2.4 and Theorem 1.7 (1). Finally Condition (c) follows from Theorem 4.3. The special case $q = 2$ and $a = 1, t$, or $1 + t$ follows from Proposition 4.5.

If $1 - 1/\mathrm{N}_{\mathfrak{L}} \neq 0$ (i.e., $1/\mathrm{N}_{\mathfrak{L}} \neq 1$) for all $\mathfrak{L} \in \mathrm{S}$, by the prime number theorem, Proposition 4.4 (3) and $\mathrm{N}_{\mathfrak{L}} \geqslant 2$, we have

$$\ln \delta_a \geqslant \sum_{\mathfrak{L}\in\mathrm{S}} -\frac{3}{\mathrm{N}_{\mathfrak{L}}}, \quad \text{converges}$$

except for the special case that $q = 2$ and $a = 1, t$, or $1 + t$. This implies $\delta_a > 0$. Otherwise, if $1/\mathrm{N}_{\mathfrak{L}} = 1$ for some $\mathfrak{L} \in \mathrm{S}$, then $[k_{\mathfrak{L}} : k] = 1$ and $[K_{\mathfrak{L}} : k_{\mathfrak{L}}] = 1$. This implies $k = \mathbb{F}_2(t), l(t) = t$ (or $1 + t$) and $X^t = a$ (or $X^{1+t} = a$) has a solution $X = f$ in $\mathbf{A}$. In these cases that $\delta_a = 0$. Our conclusion is therefore:

COROLLARY 4.7. *Given nonzero polynomial $a \in \mathbf{A} = \mathbb{F}_q[t]$. If $q \neq 2$, or if $q = 2$ and a is not of the form $1, f^t$, or f^{1+t} for some $f \in \mathbf{A}$, then the density of the set of prime ideals $\mathfrak{P}$ in $\mathbf{A}$ such that $\bar{a}$ is a generator of $C(\mathbf{A}/\mathfrak{P})$ is > 0. In particular, there are infinitely many prime ideals $\mathfrak{P}$ in $\mathbf{A}$ such that $\bar{a}$ is a generator of $C(\mathbf{A}/\mathfrak{P})$.*

Proof. Since $t = t^{1+t}, 1+t = (1+t)^t$ and the assumption, we have $a \neq 1, t, 1+t$ and a is not of the form f^t, or f^{1+t} for some $f \in \mathbf{A}$ in the case $q = 2$. The above discussions and the last example of Section 1 give $\delta_a > 0$.

Acknowledgment

I wish to thank my advisor Professor Jing Yu for useful suggestions.

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press

References

1. Artin, E.: *The collected papers of Emil Artin* (S. Lang and J. Tate, Eds.), Addison–Wesley (1965).
2. Bilharz, H.: Primdivisoren mit vorgegebener Primitivwurzel, *Math. Ann.* 114 (1937), 476–492.
3. Carlitz, L.: On certain functions connected with polynomials in a Galois field, *Duke Math.* 141 (1935), 137–168.
4. Drinfel'd, V. G.: Elliptic modules (Russian), *Math. USSR Sb.* 23 (1974), 561–592.
5. Goldstein, L. J.: Some remarks on arithmetic density questions in Proceedings symposium in pure mathematics, *Amer. Math. Soc.*, (1972).
6. Hayes, D. R.: Explicit class fields theory for rational function fields, *Trans. Amer. Math. Soc.* 189 (1974), 77–91.
7. Hooley, C.: On Artin's conjecture, *J. reine angew. Math.* 225 (1967), 209–220.
8. Hsu, C. -N.: *On Drinfeld Modules of Carlitz type*, Preprint (1994).
9. Hsu, C. -N.: *A Large Sieve Inequality for Rational Function Fields*, to appear in Journal of Number Theory (1996).
10. Ishibashi, M.: Effective version of the Tschebotareff density theorem in function fields, *Bull. London Math. Soc.* 24 (1992), 52–56.
11. Lang, S. and Trotter, H.: Primitive points on elliptic curves, *Bull. Amer. Math. Soc.* 83 (1977), 289–291.
12. Ram Murty, M.: On Artin's conjecture, *J. of Number* 16 (1983), 147–168.
13. Rota, G. C.: On the foundations of combinatorial theory I, Theory of mobius functions, *Z. Wahrsch. Verw. Gebiete* 2 (1964), 340–368.
14. Serre, J. -P.: *Local fields* (*GTM 67*), Springer-Verlag (1979).

https://doi.org/10.1023/A:1017932203320 Published online by Cambridge University Press