On Artin’s Conjecture for Rank One Drinfeld Modules

Chih-Nung Hsu
Department of Mathematics, National Taiwan Normal University,
88 Sec. 4 Ting-Chou Road, Taipei, Taiwan
E-mail: maco@math.ntnu.edu.tw

and

Jing Yu
Institute of Mathematics, Academia Sinica, Nankang, Taipei, Taiwan;
and National Center for Theoretical Sciences, Hsinchu, Taiwan
E-mail: yu@math.sinica.edu.tw

Communicated by David Gross
Received March 7, 2000

Let \( k \) be a global function field with a chosen degree one prime divisor \( \infty \), and \( \mathcal{O} \subset k \) is the subring consisting of all functions regular away from \( \infty \). Let \( \phi \) be a \( \mathcal{O} \)-normalized rank one Drinfeld \( \mathcal{O} \)-module defined over \( \mathcal{O} \), the integral closure of \( \mathcal{O} \) in the Hilbert class field of \( \mathcal{O} \). We prove an analogue of the classical Artin’s primitive roots conjecture for \( \phi \). Given any \( a \neq 0 \) in \( \mathcal{O} \), we show that the density of the set consisting of all prime ideals \( \mathfrak{P} \) in \( \mathcal{O} \) such that \( a \equiv a \pmod{\mathfrak{P}} \) is a generator of \( \mathfrak{P}(\mathcal{O}/\mathfrak{P}) \) is always positive, provided the constant field of \( k \) has more than two elements.

Key Words: Artin’s conjecture; Drinfeld modules; function fields.

1. INTRODUCTION

In 1927, Artin hypothesized that for any given nonzero integer \( a \) other than \( 1, -1 \), or a perfect square, there exist infinitely many primes \( p \) for which \( a \) is a primitive root modulo \( p \). It was shown later by Hooley [5] that this conjecture is true under the generalized Riemann hypothesis. In 1976, Lang and Trotter [9] formulated an analog of Artin’s primitive roots conjecture for elliptic curves. In [8], we generalized this conjecture on primitive points to Drinfeld modules and proved it for the case of the Carlitz module. In this article we move on to general Drinfeld modules of rank one.
Let $X$ be a smooth projective and geometrically connected algebraic curve defined over finite field $\mathbb{F}_q$ with $q$ elements and let $k$ be its function field. Let $k_\infty$ be the completion of $k$ at $\infty$ and let $\Omega$ be a fixed algebraic closure of $k_\infty$ with respect to $\infty$. From the viewpoint of class field theory, the rank one Drinfeld $\mathcal{O}$-modules over $\Omega$ are the more interesting arithmetic objects over function fields. They play a role entirely parallel to the important role played by $\mathbb{G}_m$ over $\mathbb{Q}$. Since any Drinfeld $\mathcal{O}$-module of rank one over $\Omega$ is isomorphic to a sgn-normalized $\mathcal{O}$-module over $H$, where $H$ is the Hilbert class field of $\mathcal{O}$ embedded in $k$, we shall consider only the sgn-normalized $\mathcal{O}$-modules.

Recall that a sign function on $k_\infty$ is a group homomorphism $\text{sgn}: k_\infty^* \rightarrow \mathbb{F}_q^*$ which is the identity on $\mathbb{F}_q^*$. With pair $(X, \infty)$ given, a sign function shall be fixed. Let $\mathcal{O}$ be the integral closure of $\mathcal{O}$ in $H$ and let $\mathcal{O}\mathfrak{p}$ be a fixed algebraic closure of $k$ with respect to $\mathfrak{p}$. From the viewpoint of class field theory, the rank one Drinfeld $\mathcal{O}$-modules over $\mathfrak{p}$ are the more interesting arithmetic objects over function fields. They play a role entirely parallel to the important role played by $\mathbb{G}_m$ over $\mathbb{Q}$. Since any Drinfeld $\mathcal{O}$-module of rank one over $\mathfrak{p}$ is isomorphic to a sgn-normalized $\mathcal{O}$-module over $H$, where $H$ is the Hilbert class field of $\mathcal{O}$ embedded in $k$, we shall consider only the sgn-normalized $\mathcal{O}$-modules.

Given any commutative $\mathcal{O}$-algebra $K$, we let $\phi(K)$ denote the additive group of $K$ upon which $\mathcal{O}$ operates by the $\mathbb{F}_q$-linear ring homomorphism $\phi: \mathcal{O} \rightarrow \phi(\mathcal{O})$. Since $H$ is the Hilbert class field of $\mathcal{O}$, the ideal norm of any prime ideal $\mathfrak{p}$ of $\mathcal{O}$ is a principal ideal in $\mathcal{O}$, denoted by $N_{H/k}(\mathfrak{p}) = (p)$ where $p = p(\mathfrak{p})$ is the unique generator of $N_{H/k}(\mathfrak{p})$ with $\text{sgn}(p) = 1$. It is known that $\phi(\mathcal{O}/\mathfrak{p})$ is always a cyclic $\mathcal{O}$-module with Euler-Poincaré characteristic $p - 1$. Given $0 \neq a \in \mathcal{O}$, we are interested in the set $C_a$ consisting of prime ideals $\mathfrak{p}$ of $\mathcal{O}$ for which $a = a + \mathfrak{p}$ is a generator of $\phi(\mathcal{O}/\mathfrak{p})$. The analogue of Artin's conjecture for $\phi$ says that $C_a$ always has a density $\delta(C_a)$ which can be given explicitly by an infinite (Euler) product. If $q \neq 2$, we prove that this is indeed the case with $\delta(C_a)$ given in Theorem 4.6 by

$$\delta_a = \prod_{\text{prime } \mathfrak{p} \in \mathcal{O}} \left(1 - \frac{1}{N_{\mathfrak{p}}}\right) > 0,$$

where $N_{\mathfrak{p}}$ is the degree $[K_{\mathfrak{p}}: H]$ and $K_{\mathfrak{p}}$ is the Galois extension over $H$ obtained by adjoining $\mathfrak{p}$-division points and roots of equations $x^p = a$ (see Section 2) to $H$. In Section 2, we first show that $\tilde{a}$ is a generator of $\phi(\mathcal{O}/\mathfrak{p})$ if and only if the prime ideal $\mathfrak{p}$ does not split completely in any one of the fields $K_{\mathfrak{p}}$, where $\mathfrak{p}$ runs through prime ideals in $\mathcal{O}$. In order to solve our problem we study two families of Galois extensions $k_{\mathfrak{m}}$ and $K_{\mathfrak{m}}$ over $H$, where $\mathfrak{m}$ runs through squarefree ideals in $\mathcal{O}$. The field $k_{\mathfrak{m}}$ is the cyclotomic function field
obtained by adjoining \( \mathfrak{M} \)-division points to \( H \), while \( K_{\mathfrak{M}} \) is the Kummer-type extension obtained by adjoining roots of \( x^{\mathfrak{M}} = a \) to \( k_{\mathfrak{M}} \). It is known that \( \text{Gal}(k_{\mathfrak{M}}/H) \cong (\mathcal{O}/\mathfrak{M})^\times \). If \( q \neq 2 \), it becomes possible to extend the conjugation action of \( \text{Gal}(k_{\mathfrak{M}}/H) \) to an action of \( \mathcal{O}/\mathfrak{M} \) on \( \text{Gal}(K_{\mathfrak{M}}/k_{\mathfrak{M}}) \). This is a key to the structure of \( K_{\mathfrak{M}}/k_{\mathfrak{M}} \).

In Section 3, we continue the study of the Galois families, estimating the growth of the discriminant divisor \( 2(K_{\mathfrak{M}}H) \) as \( \deg \mathfrak{M} \) goes larger. Analytic theory of Drinfeld modules is used there for controlling ramifications over \( \infty \).

In Section 4, Artin’s conjecture for sgn-normalized rank one Drinfeld modules is reduced to a generalized Artin’s problem worked out already in Hsu [8, Theorem 3.1]. In addition, information collected in previous sections, a general version of the Brun–Titchmarsh theorem for function fields (cf. [7, Theorem 4.3]) and Poonen’s analogue of the Mordell–Weil theorem for Drinfeld modules also play roles for the deduction.

### 2. ON KUMMER’S THEORY OF SIGN NORMALIZED RANK ONE DRINFELD MODULES

In this section \( \mathbb{F}_q \) will be finite field of characteristic \( l \) with \( q \neq 2 \). Let \( \pi \in k \) be a local uniformizer at \( \infty \) fixed throughout. Since \( \infty \) is rational, we have \( k_{\infty} \cong \mathbb{F}_q((\pi)) \). Thus if \( f \in k_{\infty} \) with \( \text{ord}_f(f) = n \), then \( f \) can be written uniquely in the form

\[
    f = \sum_{i=0}^{n} a_i \pi^i, \quad a_i \in \mathbb{F}_q, a_n \neq 0.
\]

We define sign-function \( \text{sgn}: k_{\infty}^\times \to \mathbb{F}_q^\times \) by \( \text{sgn}(f) = a_n \). If \( \text{sgn}(f) = 1 \), then \( f \) is said to be a positive element in \( k_{\infty}^\times \).

Let \( \Omega' = \text{End}_{\mathcal{O}}(\mathbb{G}_a^{\mathfrak{M}}) \) be the twisted polynomial ring over \( \mathcal{O} \) in the \( q \)th power Frobenius map \( \tau \). A rank one Drinfeld \( \mathcal{O} \)-module \( \phi \) over \( \mathcal{O} \) is an \( \mathbb{F}_q \)-linear ring homomorphism from \( \mathcal{O} \) into \( \Omega' \), \( b \mapsto \phi_b \), such that the constant coefficient of \( \phi_b \) is equal to \( b \) and \( \text{deg}_\mathcal{O} \phi_b = -\text{ord}_\mathcal{O}(b) \) for all \( b \in \mathcal{O} \). It is known that any Drinfeld \( \mathcal{O} \)-module of rank one over \( \mathcal{O} \) is isomorphic to a sgn-normalized \( \mathcal{O} \)-module \( \phi \) over \( H \), where \( H \) is the Hilbert class field of \( \mathcal{O} \), i.e., the maximal abelian unramified extension of \( k \) which splits completely over \( \infty \). In fact, sgn-normalized \( \mathcal{O} \)-modules \( \phi \) are always defined over \( \mathcal{O}' \subset H \) (cf. [2, Lemma 7.4.5]). From now on, \( \phi \) will denote a given rank one sgn-normalized \( \mathcal{O} \)-module over \( \mathcal{O}' \), in other words, an \( \mathbb{F}_q \)-linear homomorphism of \( \mathcal{O} \) into \( \mathcal{O}' \).

Given \( b \in \mathcal{O} \), the additive polynomial in \( x \) resulted from substituting \( \tau \) by \( x^b \) in the twisted polynomial \( \phi_b \) will be denoted by \( \phi_b(x) \). We shall also use the more suggestive notation \( x^b \) instead of \( \phi_b(x) \). For any nonzero ideal \( \mathfrak{M} \)
in \( \mathcal{O} \), we let \( \phi_m \) be the monic generator of the left ideal of \( H[\tau] \) generated by \( \phi_m \) for all \( m \in \mathfrak{M} \). Note that \( \phi_m \) actually lies in \( \mathcal{O}'[\tau] \) as \( \phi \) is sgn-normalized. The notation \( x^{**} \) instead of \( \phi_m(x) \) for the additive polynomial of \( \phi_m \) will be used too.

We are particularly interested in the finite \( \mathcal{O} \)-modules \( \phi(\mathcal{O}'/\mathfrak{P}) \), where \( \mathfrak{P} \) runs through prime ideals in \( \mathcal{O}' \). Since \( H \) is the Hilbert class field of \( \mathcal{O} \), the ideal norm \( N_{\mathcal{O}H}(\mathfrak{P}) \) is always principal in \( \mathcal{O} \), say \( N_{\mathcal{O}H}(\mathfrak{P}) = (p) \), for some positive element \( p = p(\mathfrak{P}) \in \mathcal{O} \). As an analogue of the little Fermat theorem, one has

**Proposition 2.1.** The module \( \phi(\mathcal{O}'/\mathfrak{P}) \) is a finite cyclic \( \mathcal{O} \)-module with Euler–Poincaré characteristic \( p(\mathfrak{P}) - 1 \), i.e., as \( \mathcal{O} \)-module

\[
\phi(\mathcal{O}'/\mathfrak{P}) \cong \mathcal{O}/(p(\mathfrak{P}) - 1).
\]

**Proof.** Since \( \phi \) is a rank one Drinfeld \( \mathcal{O} \)-module, the torsion \( \mathcal{O} \)-module \( \phi(\mathcal{O}'/\mathfrak{P}) \) has to be cyclic. Let \( \mathfrak{P} = \mathfrak{P}' \cap \mathcal{O} \). By [4, Proposition 11.4], we know that the congruence \( \phi_{\mathfrak{P}'}(x) \equiv x^{a+\mathfrak{P}'} \pmod{\mathfrak{P}'} \) holds. Since \( (p(\mathfrak{P}')) = \mathfrak{P}^{\deg \mathfrak{P}'}/\deg \mathfrak{P} ', \) we deduce that \( \phi_{p(\mathfrak{P}')}(b) \equiv b \pmod{\mathfrak{P}'} \), for all \( b \in \mathcal{O}' \). This completes the proof.

Given \( b \in \mathcal{O}' \), the canonical image of \( b \) in \( \phi(\mathcal{O}'/\mathfrak{P}) \) is denoted by \( \bar{b} \).

**Proposition 2.2.** Suppose that \( a \in \mathcal{O}' \), \( \mathfrak{P} \) is a prime ideal in \( \mathcal{O}' \), and \( N_{\mathcal{O}H}(\mathfrak{P}) = (p) \) for positive element \( p \in \mathcal{O} \). Then the element \( \bar{a} \) is a generator of \( \phi(\mathcal{O}'/\mathfrak{P}) \) if and only if \( \phi(p^{-1}a)(\bar{a}) \neq 0 \) for all prime ideal \( \mathfrak{P} \notin \mathcal{O} \) such that \( \mathfrak{P} \) divides \( p - 1 \).

**Proof.** This follows immediately from Proposition 2.1.

Given nonzero ideal \( \mathfrak{M} \) in \( \mathcal{O} \), we denote by \( A_{\mathfrak{M}} \) the set consisting of \( \lambda \in \Omega \) such that \( \phi_m(\lambda) = 0 \) for all \( m \in \mathfrak{M} \) and set \( k_{\mathfrak{M}} = H(A_{\mathfrak{M}}) \). These \( k_{\mathfrak{M}} \) are the analogues of cyclotomic fields for the base field \( k \). Since \( \phi \) is of rank one, the finite \( \mathcal{O} \)-module \( A_{\mathfrak{M}} \) is isomorphic to \( \mathcal{O}/\mathfrak{M} \) and \( \text{Gal}(k_{\mathfrak{M}}/H) \) is isomorphic to \( (\mathcal{O}/\mathfrak{M})^* \). It follows that all \( a \neq 0 \in \phi(\mathcal{O}') \) are nontorsion if \( q 
eq 2 \). The extension \( k_{\mathfrak{M}}/k \) is always abelian and is unramified at prime ideals \( \mathfrak{P} \) of \( \mathcal{O} \) not dividing \( \mathfrak{M} \) (cf. [2, Section 7]). Moreover, the Artin symbol \( \sigma_{\mathfrak{M}} \in \text{Gal}(k_{\mathfrak{M}}/k) \) at these prime ideals \( \mathfrak{P} \) can be described explicitly by:

\[
\sigma_{\mathfrak{M}}(\lambda) = \lambda^\mathfrak{M} = \phi_{\mathfrak{M}}(\lambda), \quad \text{for all } \lambda \in A_{\mathfrak{M}}.
\]

From now on we fix a given \( a \neq 0 \in \mathcal{O}' \). Let \( \mathfrak{M} \subset \mathcal{O} \) be a nonzero ideal. We are also interested in the Kummer-type extensions \( K_{\mathfrak{M}} = k_{\mathfrak{M}}(x) \), where \( x \in \Omega \) is a root of \( \lambda^{**} - a = \phi_{\mathfrak{M}}(x) - a = 0 \). We have
Proposition 2.3. Let $\mathfrak{p}$ be a prime ideal in $\mathfrak{C}$, and let $\mathfrak{P'}$ be a prime ideal in $\mathfrak{C'}$ with $N_{H\mathfrak{C}H}(\mathfrak{P'}) = (p)$ for some positive $p \in \mathfrak{C}$. Then $\mathfrak{P'}$ splits completely in $K_{\mathfrak{P}}$ if and only if $\mathfrak{P} | (p - 1)$ and $\phi_{(p - 1)}(\bar{a}) = 0$.

Proof. Suppose that $\mathfrak{P'}$ splits completely in $K_{\mathfrak{P}}$. Since $N_{H\mathfrak{C}H}(\mathfrak{P'}) = (p)$, the Artin symbol $\sigma_{(p)}$ is the identity in $\text{Gal}(k_{\mathfrak{P}}/k)$. Thus we have $\sigma_{(p)}(\lambda) = \lambda^p = \lambda$, i.e., $\lambda^{p - 1} = 0$, for all $\lambda \in A_{\mathfrak{P}}$. This implies that $\mathfrak{P}$ divides the principal ideal $(p - 1)$ in $\mathfrak{C}$. Since $\mathfrak{P'}$ splits completely in $K_{\mathfrak{P}}$, there is a root $\bar{x}$ of $x^{\mathfrak{P}} \equiv a \pmod{\mathfrak{P}'}$ in $\phi(\mathfrak{C'}/\mathfrak{P}')$. We obtain from Proposition 2.1 that $\phi_{(p - 1)}(\bar{a}) = \bar{x}^{p - 1} = 0$ in $\phi(\mathfrak{C'}/\mathfrak{P}')$.

Conversely, let $\psi_{\mathfrak{P}}$ be the Artin symbol in $\text{Gal}(k_{\mathfrak{P}}/H)$. Since $N_{H\mathfrak{C}H}(\mathfrak{P'})(p)$, $\sigma_{\mathfrak{P}} = \sigma_{(p)}$. It follows from $\mathfrak{P} | (p - 1)$ that $\sigma_{\mathfrak{P}}(\lambda) = \sigma_{(p)}(\lambda) = \lambda^{p - 1} + \lambda = \lambda$ for all $\lambda \in A_{\mathfrak{P}}$; i.e., $\mathfrak{P}$ splits completely in $k_{\mathfrak{P}}$. To show that $\mathfrak{P'}$ splits completely in $k_{\mathfrak{P}}$, it is enough to find the solution of $x^{\mathfrak{P}} = a$ in $\mathfrak{C'}/\mathfrak{P}'$. Let $\beta$ be any root of $x^{\mathfrak{P}} = a$ inside an algebraic closure of $\mathfrak{C'}/\mathfrak{P}'$. We have $\beta^{p - 1} = a^{p - 1} \equiv \phi(\mathfrak{C'}/\mathfrak{P}')$; i.e., $\beta^p = \beta$. On the other hand the polynomial $x^{\mathfrak{P}}$ is Eisenstein at $\mathfrak{P}'$, hence $x^{\mathfrak{P}} \equiv x^{a^{p - 1}} \pmod{\mathfrak{P}'}$, so that $x^{\mathfrak{P}} \equiv x^{a^{p - 1}} \pmod{\mathfrak{P}'}$ always holds. Thus we obtain $\beta^{a^{p - 1}} = \beta$ which gives $\beta \in \mathfrak{C'}/\mathfrak{P}'$.

Combining Propositions 2.2 and 2.3, we have the following basic

Theorem 2.4. The element $\bar{a}$ is a generator of $\phi(\mathfrak{C'}/\mathfrak{P}')$ if and only if the prime ideal $\mathfrak{P'}$ does not split completely in any of the field $K_{\mathfrak{P}}$, where $\mathfrak{P}$ runs through prime ideals in $\mathfrak{C}$.

In what follows $\mathfrak{M}$ shall always denote squarefree ideal in $\mathfrak{C}$. Let $f \in \mathfrak{C}$ be a positive element prime to $\mathfrak{M}$. Let $\sigma_{f} \in \text{Gal}(k_{\mathfrak{M}}/k)$ be the Artin symbol of principal ideal $(f)$ in $\mathfrak{C}$. Then $\sigma_{f}(\lambda) = \lambda^{f}$ for all $\lambda \in A_{\mathfrak{M}}$. To study the Galois group $\text{Gal}(K_{\mathfrak{M}}/k_{\mathfrak{M}})$, let us fix $\alpha \in \mathfrak{M}$ satisfying $x^{\mathfrak{M}} = \alpha$. Let $\psi \in \text{Gal}(K_{\mathfrak{M}}/k_{\mathfrak{M}})$. Then we must have $\psi(\alpha) = \alpha + \lambda$ for some $\lambda \in A_{\mathfrak{M}}$. We denote the map $\psi$ by $\psi_{\lambda}$. Hence there exists a subgroup $A_{\mathfrak{M}}$ of $A_{\mathfrak{M}}$ such that the map $\psi: A_{\mathfrak{M}} \to \text{Gal}(K_{\mathfrak{M}}/k_{\mathfrak{M}})$ given by $\psi(\lambda) = \psi_{\lambda}$ is a group isomorphism. Since $K_{\mathfrak{M}}/H$ is a Galois extension and $\text{Gal}(K_{\mathfrak{M}}/k_{\mathfrak{M}})$ is abelian, the action of $\text{Gal}(K_{\mathfrak{M}}/H)$ on $\text{Gal}(K_{\mathfrak{M}}/k_{\mathfrak{M}})$ by conjugation, $\psi_{\lambda} \mapsto \sigma_{f} \cdot \psi_{\lambda} \cdot \sigma_{f}^{-1}$, can be explicitly given in

Proposition 2.5. Suppose that $f$ is a positive element in $\mathfrak{C}$ prime to $\mathfrak{M}$ and $\lambda \in A_{\mathfrak{M}}$. Then we have $\sigma_{f} \cdot \psi_{\lambda} = \psi_{\lambda f}$.

Since $(\mathfrak{C}, \mathfrak{M})^* \cong \text{Gal}(k_{\mathfrak{M}}/H)$ and every class in $(\mathfrak{C}, \mathfrak{M})^*$ can be represented by a positive element, from Proposition 2.5, we obtain an action of $(\mathfrak{C}, \mathfrak{M})^*$ on the abelian group $\text{Gal}(K_{\mathfrak{M}}/k_{\mathfrak{M}}) \cong A_{\mathfrak{M}}$. We then want to
extend this action of \((\mathcal{O}/\mathfrak{M})^*\) to an action of \(\mathcal{O}/\mathfrak{M}\) on \(A_{\mathfrak{a},\mathfrak{M}}\). For this purpose, the condition \(q \neq 2\) is needed. By an approximation lemma (cf. \cite[Chap. 1]{12}), for any \(f \in \mathcal{O}\) there exist \(f_1, f_2 \in \mathcal{O}\) such that \(f \equiv f_1 + f_2 \pmod{\mathfrak{M}}\), and the \(f_i\) are either positive and prime to \(\mathfrak{M}\) or 0. Thus for any \(x \in A_{\mathfrak{a},\mathfrak{M}}\) and \(f \in \mathcal{O}/\mathfrak{M}\), we define the action of \(\mathcal{O}/\mathfrak{M}\) on \(\text{Gal}(K_{\mathfrak{M}}/k_{\mathfrak{M}})\) by
\[
\tilde{f} \cdot \psi_j = \sigma_{f_1} \cdot \psi_j = \psi_{j + i_1} + \psi_{j + i_2} = \psi_{j}.\]

This is clearly well defined (independent of the decomposition of \(f\)) and \(\text{Gal}(K_{\mathfrak{M}}/k_{\mathfrak{M}})\) becomes a \(\mathcal{O}/\mathfrak{M}\)-module under this action. We have

**Theorem 2.6.** Let the assumptions and notation be as above. Then

1. The Galois group \(\text{Gal}(K_{\mathfrak{M}}/k_{\mathfrak{M}})\) is isomorphic to \(\mathcal{O}/\mathfrak{M}\), or \(A_{\mathfrak{a},\mathfrak{M}} = \lambda_{\mathfrak{a},\mathfrak{M}}\), for some ideal \(\mathfrak{a}\) dividing \(\mathfrak{M}\).

2. Suppose that \(\mathfrak{q}\) is a prime ideal in \(\mathcal{O}\). If \(x^\mathfrak{q} = a\) has one solution \(x = c\) in \(\mathcal{O}'\), then \(A_{\mathfrak{a},\mathfrak{q}} = \{0\}\) and \((a)\) as ideals in \(\mathcal{O}'\). Otherwise, \(A_{\mathfrak{a},\mathfrak{q}} = A_{\mathfrak{q}}\).

3. Suppose that \(\mathfrak{M}, \mathfrak{R}\) are two square-free relatively prime ideals in \(\mathcal{O}\). Then \(K_{\mathfrak{M}} \subset K_{\mathfrak{R}} \subset K_{\mathfrak{M}} \cdot K_{\mathfrak{R}}\) are linearly disjoint over \(H\).

4. Suppose that \(\mathfrak{M}\) is a square-free ideal in \(\mathcal{O}\). Let \(\mathfrak{D}\) be the largest ideal factor of \(\mathfrak{M}\) such that the equation \(x^\mathfrak{q} = a\) has solution \(x = b\) in \(\mathcal{O}'\). Then the polynomial \(x^\mathfrak{M}_{\mathfrak{M}^{-1}} - b\) is irreducible over \(\mathcal{O}'\), and \(A_{\mathfrak{a},\mathfrak{R}} = A_{\mathfrak{M}^{-1}}\).

5. The field of constants of \(K_{\mathfrak{M}}\) is still \(\mathcal{O}/\mathfrak{q}\).

**Proof.** (1) follows at once from the above discussion.

To prove (2), by (1) we have \(A_{\mathfrak{a},\mathfrak{q}} = \{0\}\) or \(A_{\mathfrak{a},\mathfrak{q}} = A_{\mathfrak{q}}\). If the equation \(x^\mathfrak{q} = a\) has one solution \(x = c\) in \(\mathcal{O}'\), then all the roots of \(x^\mathfrak{q} = a\) belong to \(k_{\mathfrak{q}}\). This implies that \(A_{\mathfrak{a},\mathfrak{q}} = \{0\}\). Also, \((a)\) clearly divides \((a)\) in \(\mathcal{O}'\) (by the expansion of \(x^\mathfrak{q}\)). Otherwise, if the equation \(x^\mathfrak{q} = a\) has no solution in \(\mathcal{O}'\), it suffices to show that \(x^\mathfrak{q} = a\) has no solution \(x\) in \(k_{\mathfrak{q}}\). Suppose that \(x^\mathfrak{q} = a\) has one solution \(x = a, x \in k_{\mathfrak{q}} - k\); then all solutions of \(x^\mathfrak{q} = a\) are in \(k_{\mathfrak{q}}\). Let us take \(\beta = -\text{Tr}_{k_{\mathfrak{q}}/k}(3)\); then one has \(\beta^\mathfrak{q} = -(q^\mathfrak{q} \beta - 1)a = a\) (because \(\text{Gal}(k_{\mathfrak{q}}/H) \cong (\mathcal{O}/\mathfrak{I})^*\) and \(\beta \in \mathcal{O}'\)). This contradicts the assumption.

To prove (3), given ideal \(\mathfrak{D} \subset \mathcal{O}\), let us denote all the roots of \(x^\mathfrak{D} = a\) in \(K_{\mathfrak{D}}\) by \(R_{\mathfrak{D}}\). Suppose that \(x \in R_{\mathfrak{D}}, \beta \in R_{\mathfrak{M}}\); then \(x^\mathfrak{M} = a, \beta^\mathfrak{M} = a\). Since \(\mathfrak{M}, \mathfrak{R}\) are relatively prime, let us take positive elements \(m \in \mathfrak{M}, n \in \mathfrak{R}\) such that \(n - m = 1\), and let \(\theta = x^{(m)n^{-1}} - \beta^{(m)n^{-1}} \in K_{\mathfrak{M}} \cdot K_{\mathfrak{R}}\). Then \(\theta^\mathfrak{M} = (x^\mathfrak{M})^n - (\beta^\mathfrak{M})^n = a^n - a = a\). This implies that \(\theta \in R_{\mathfrak{M}, \mathfrak{R}}\); hence \(K_{\mathfrak{M}} \cdot K_{\mathfrak{R}} \supseteq R_{\mathfrak{M}, \mathfrak{R}}\) (because \(K_{\mathfrak{M}} \cdot K_{\mathfrak{R}} \supseteq K_{\mathfrak{M}, \mathfrak{R}}\)). Conversely, suppose that \(\theta \in R_{\mathfrak{M}, \mathfrak{R}}\), then \(\theta^\mathfrak{M} \in K_{\mathfrak{M}}, \theta^\mathfrak{R} \in R_{\mathfrak{R}}\). This implies that \(K_{\mathfrak{M}} \cdot K_{\mathfrak{R}} \supseteq K_{\mathfrak{M}, \mathfrak{R}}\).

To prove disjointness linearly, we suppose that \(\theta \in R_{\mathfrak{M}, \mathfrak{R}}\) and let \(x = \theta^\mathfrak{M} \in R_{\mathfrak{M}, \mathfrak{R}}, \beta = \theta^\mathfrak{R} \in R_{\mathfrak{R}}\). By (1), we have \(A_{\mathfrak{a},\mathfrak{R}} = A_{\mathfrak{D}}\) for some ideal \(\mathfrak{D}\) dividing
constants of $\kappa$ and write $A_2$ as a direct sum $A_\mathfrak{D} \oplus A_\mathfrak{D}$, where $\mathfrak{D} = \mathfrak{D}_1 \mathfrak{D}_2$, $\mathfrak{D}_1 \mid \mathfrak{P}$, $\mathfrak{D}_2 \mid \mathfrak{R}$. We claim that $A_{\mathfrak{D}'} = A_\mathfrak{D}$ and $A_{\mathfrak{D}'} = A_\mathfrak{D}$. Let $\sigma \in \text{Gal}(K_{\mathfrak{P}1}/k_{\mathfrak{P}1})$ with $\sigma(\theta) = \theta + \lambda_1 + \lambda_2$, where $\lambda_1 \in A_{\mathfrak{D}'}$, $\lambda_2 \in A_{\mathfrak{D}'}$. Since $\alpha = \theta^{\mathfrak{P}1} \in R_{\mathfrak{P}1}$ and $\lambda_2^{\mathfrak{P}1} = 0$, we have $\sigma(\alpha) = \sigma(\theta^{\mathfrak{P}1}) = (\theta + \lambda_1 + \lambda_2)^{\mathfrak{P}1} = \alpha + \lambda_1^{\mathfrak{P}1}$. This implies that $\lambda_1^{\mathfrak{P}1} \in A_{\mathfrak{D}'}$. Since $(\mathfrak{P}, \mathfrak{R}) = 1$, it follows that $\lambda_1 \in A_{\mathfrak{D}'}$. We have $A_{\mathfrak{D}'} \subset A_{\mathfrak{D}'}$.

Conversely, suppose $\lambda' \in A_{\mathfrak{D}'}$. Since $[k_{\mathfrak{P}1}/k_{\mathfrak{D}1}] = [k_{\mathfrak{D}1}/H]$ and $[k_{\mathfrak{D}1}/k_{\mathfrak{R}1}]$ are relatively prime (because $\mathfrak{P}$, $\mathfrak{R}$ are squarefree ideals in $\mathfrak{D}$), $K_{\mathfrak{P}1}$ and $K_{\mathfrak{R}1}$ are linearly disjoint over $k_{\mathfrak{D}1}$. Then there exists $\sigma' \in \text{Gal}(K_{\mathfrak{P}1}k_{\mathfrak{P}1}/k_{\mathfrak{R}1})$ such that $\sigma' = \text{identity}$ on $k_{\mathfrak{P}1}$ and $\sigma'(a) = a + \lambda'$. We extend $\sigma'$ to $\sigma \in \text{Gal}(K_{\mathfrak{P}1}k_{\mathfrak{P}1}/k_{\mathfrak{R}1})$. Then we also have $\sigma(\alpha) = \alpha + \lambda'$. Now if $\sigma(\theta) = \theta + \lambda_1 + \lambda_2$, where $\lambda_1 \in A_{\mathfrak{D}'}$, $\lambda_2 \in A_{\mathfrak{D}'}$, then $\sigma(\theta)^{\mathfrak{P}1} = \sigma(\alpha)^{\mathfrak{P}1} = \alpha + \lambda_1^{\mathfrak{P}1}$. Thus we have $\lambda' = \lambda_1^{\mathfrak{P}1} \in A_{\mathfrak{D}'}$; hence $A_{\mathfrak{D}'} \subset A_{\mathfrak{D}'}$. Therefore, we have $A_{\mathfrak{D}'} = A_\mathfrak{D}$ and also $A_{\mathfrak{D}'} = A_\mathfrak{D}$. Since $k_{\mathfrak{P}1}$ and $k_{\mathfrak{R}1}$ are linearly disjoint over the Hilbert class field $H$ (cf. [2, Chap. 7]), this shows that $[K_{\mathfrak{P}1}:H] \cdot [K_{\mathfrak{R}1}:H] = [K_{\mathfrak{P}1}:H]$. Combining these, assertion (3) is proved.

To prove (4), we first deduce from (3) that

$$[K_{\mathfrak{P}1}:k_{\mathfrak{D}1}] = \prod_{\text{prime } \mathfrak{P} \mid \mathfrak{D}} [K_{\mathfrak{P}1}:k_{\mathfrak{D}1}] = \text{deg}(x^{\mathfrak{D}1} - b).$$

Then (4) follows from (2) by degree considerations.

For the proof of (5), by [2, Lemma 7.5.11], the field of constants of $k_{\mathfrak{P}1}$ is $\overline{\mathbb{F}_q}$. From (1), we know that the field of constants of $k_{\mathfrak{R}1}$ is either $\overline{\mathbb{F}_q}$ or $\overline{\mathbb{F}_{q^p}}$ (since $A_{\mathfrak{P}1}$ is an elementary $l$-group). Suppose that the field of constants of $k_{\mathfrak{R}1}$ is $\overline{\mathbb{F}_q}$. Then there are two Galois subextensions $k_{\mathfrak{P}1}/k_{\mathfrak{R}1}$, $k_{\mathfrak{R}1}/k_{\mathfrak{P}1}$ of $K_{\mathfrak{P}1}/k_{\mathfrak{R}1}$ such that $k_{\mathfrak{P}1} \cong k_{\mathfrak{R}1} \oplus \overline{\mathbb{F}_q}$, $k_{\mathfrak{R}1} \cap k_{\mathfrak{P}1} = k_{\mathfrak{R}1}$, and $A_{\mathfrak{P}1} \cong \text{Gal}(k_{\mathfrak{P}1}/k_{\mathfrak{R}1}) \times \text{Gal}(k_{\mathfrak{R}1}/k_{\mathfrak{P}1})$. The action of $\text{Gal}(k_{\mathfrak{R}1}/H)$ on $\text{Gal}(k_{\mathfrak{P}1}/k_{\mathfrak{R}1})$ has to be trivial. On the other hand, the action of $\text{Gal}(k_{\mathfrak{R}1}/H)$ on $A_{\mathfrak{P}1}$ does not fix any nonzero subgroup. This gives a contradiction. $

3. ESTIMATING DISCRIMINANTS

Let $a$ be a nonzero element in $\mathfrak{C}$ fixed throughout as before. The degree of the Galois extensions $K_{\mathfrak{R}1}$ over $H$ will be denoted by $N_{\mathfrak{R}1}$. Our purpose in this section is to obtain an upper bound for the total degree $d_{\mathfrak{R}1}$ of the discriminant divisor $A(K_{\mathfrak{R}1}/H)$ as $\mathfrak{R}$ running through squarefree ideals of $\mathfrak{C}$. All divisors of function fields will be written multiplicatively. Prime divisors of $H$ which are not lying above $\infty$ are identified as prime ideals in $\mathfrak{C}$. The divisor of $H$ which is the product of all prime divisors lying above $\infty$ (resp. $\mathfrak{P}$) will also be denoted by $\infty$ (resp. $\mathfrak{P}$) in this section.
Proposition 3.1. Let \( \mathfrak{P} \) be a prime ideal of \( \mathcal{O} \). We have

1. The discriminant \( \Delta(k_{\mathfrak{P}}/H) \) divides \( (\infty \cdot \mathfrak{P})^{(k_{\mathfrak{P}}/H)} \).

2. The finite part of \( \Delta(k_{\mathfrak{P}}/H) \) divides \( (\mathfrak{P})^{2N_{k_{\mathfrak{P}}/H}} \).

Proof. To prove (1), let \( e_{\mathfrak{P}}(k_{\mathfrak{P}}/k) \) (resp. \( e_{\infty}(k_{\mathfrak{P}}/k) \)) denote the ramification index at \( \mathfrak{P} \) (resp. \( k_{\mathfrak{P}}/k \)). We know that every prime divisor of \( k_{\mathfrak{P}} \) except \( \infty \) and the one that corresponds to \( \mathfrak{P} \) is unramified in \( k_{\mathfrak{P}} \). By [2, Proposition 7.5.8], the ramification index \( e_{\infty}(k_{\mathfrak{P}}/k) \) is equal to \( (q-1) \). Hence the \( -r \)-part of \( \Delta(k_{\mathfrak{P}}/H) \) is precisely \( (d_{1}) \), where

\[
d_{1} = \frac{e_{\infty}(k_{\mathfrak{P}}/k) - 1}{e_{\infty}(k_{\mathfrak{P}}/k)} \cdot [k_{\mathfrak{P}} : H].
\]

Similarly, by [2, Proposition 7.5.18], the part of the discriminant \( \Delta(k_{\mathfrak{P}}/H) \) over \( \mathfrak{P} \) is equal to \( (\mathfrak{P})^{(k_{\mathfrak{P}}/H)} \). Combining these, we obtain that \( \Delta(k_{\mathfrak{P}}/H) \) divides \( (\mathfrak{P})^{2N_{k_{\mathfrak{P}}/H}} \).

To prove (2), let \( f(x) = x^\mathfrak{P} - a \), and let \( \sigma \) be a root of equation \( f(x) = 0 \) in \( K_{\mathfrak{P}} \). By the principal ideal theorem (cf. [2, Theorem 7.6.10]), the ideal \( (f'(\sigma)) \) in \( \mathcal{O} \) is equal to \( (\mathfrak{P})^{(k_{\mathfrak{P}}/H)} \). Thus \( N_{k_{\mathfrak{P}}/k}(f'(\sigma)) \) divides \( (\mathfrak{P})^{(k_{\mathfrak{P}}/H)} \), and also the finite part of the discriminant \( \Delta(k_{\mathfrak{P}}/k_{\mathfrak{P}}) \) divides \( (\mathfrak{P})^{(k_{\mathfrak{P}}/H)} \). By transitivity of discriminants, we obtain from (1) that the finite part of \( \Delta(k_{\mathfrak{P}}/H) \) divides \( (\mathfrak{P})^{(k_{\mathfrak{P}}/H)} \), which is equal to \( (\mathfrak{P})^{2N_{k_{\mathfrak{P}}/H}} \). This completes the proof.

In order to understand the ramifications of the Kummer-type extension \( K_{\mathfrak{P}}/k_{\mathfrak{P}} \) at infinite places, we make use of the analytic theory of Drinfeld modules. A rank one \( \mathcal{O} \)-lattice is a discrete \( \mathcal{O} \)-submodule \( \mathfrak{L} \) of \( \mathcal{O} \) such that \( k_{\mathfrak{L}} \) is a 1-dimensional vector space over \( k \). Given such a \( \mathfrak{L} \subset \mathcal{O} \), there exists an ideal \( \mathfrak{D} \subset \mathcal{O} \) and a nonzero element \( \xi \in \Omega \) such that \( \mathfrak{L} = \mathfrak{D}\xi \). The exponential function associated to the \( \mathcal{O} \)-lattice \( \mathfrak{L} \) is the function \( e_{\mathfrak{L}}(z) \) defined for \( z \in \Omega \) by the infinite product

\[
e_{\mathfrak{L}}(z) = \prod_{0 \ne \nu \in \mathfrak{L}} \left( 1 - \frac{z}{\nu} \right).
\]

This function \( e_{\mathfrak{L}}(z) \) is a \( \mathbb{F}_{q} \)-linear entire function of \( \Omega \) onto \( \Omega \) such that \( e_{\mathfrak{L}}(z) \) is periodic with \( \mathfrak{L} \) as a group of periods. It is well known (analytic uniformization theorem, cf. [2, Theorem 4.6.9]) that, associated to any sgn-normalized rank one Drinfeld \( \mathcal{O} \)-module \( \phi \) defined over \( H \), there exists a rank one \( \mathcal{O} \)-lattice \( \mathfrak{L} \) such that the associated exponential function has expansion

\[
e_{\mathfrak{L}}(z) = \sum_{i=1}^{\infty} a_{i}z^{q^{i}}
\]
with \( a_i \in H \) and satisfies \( \phi_b(e_T(z)) = e_T(bz) \) for all \( b \in C \). This also gives the analytic description \( A_{\mathfrak{m}} = e_T(\mathfrak{M}^{-1}U) \subset \Omega \), for all ideals \( \mathfrak{M} \subset C \), and the cyclotomic function fields \( k_{\mathfrak{m}} \) are taken as subfields of \( \Omega \).

In the following proposition, the valuation \( \text{ord}_{\infty} \) is extended from \( k_{\infty} \) to \( \Omega \) in the usual way (note that \( \text{ord}_{\infty}(\pi) = 1 \)).

**Proposition 3.2.** Let \( \mathfrak{M} \) run through nonzero ideals in \( C \). Then

1. There exists constant \( C_0 \) (may be negative) which depends only on \( k \) and on the sgn-normalized Drinfeld module \( \phi \) such that \( \text{ord}_{\infty}(\lambda) \geq C_0 \), for any \( 0 \neq \lambda \in A_{\mathfrak{m}} \).

2. We have

\[
\text{ord}_{\infty}(\lambda) = O(\deg \mathfrak{M}),
\]
for any \( 0 \neq \lambda \in A_{\mathfrak{m}} \), where the implied constant depends only on \( k \) and on \( \phi \).

3. There exists constant \( C_1 \) (may be negative), which depends only on \( \phi \) and \( a \) such that if \( \pi \in \Omega \) is any root of \( x^\mathfrak{M} - a = 0 \), then

\[
\text{ord}_{\infty}(\pi) \geq C_1.
\]

4. Suppose that \( \infty \) is any prime divisor of \( k_{\mathfrak{m}} \) sitting over \( \infty \). Then the ramification index \( e_{\infty}(K_{\mathfrak{m}}/k) = O(1) \), where the implied constant depends only on \( \phi \) and \( a \).

**Proof.** Suppose that \( \mathfrak{M}^k = (p) \) for some positive element \( p \in C \), where \( h \) is the class number of \( C \). We shall show that \( \text{ord}_{\infty}(\lambda) \geq C_0 \), for any \( 0 \neq \lambda \in A_{(p)} \). Note (1) follows because \( A_{\mathfrak{m}} \subset A_{(p)} \).

By the analytic theory the sgn-normalized Drinfeld module \( \phi \) corresponds to lattice \( \Lambda = \mathfrak{D} \zeta \). Given \( \lambda \in A \) there exists \( d \in \mathfrak{D} \) such that \( \lambda = e_T(d\zeta/p) \). Applying the Riemann–Roch theorem we can always find element \( d' \in \mathfrak{D} \) such that \( d' \equiv d \pmod{p \mathfrak{D}} \) and \( \text{ord}_{\infty}(d') \geq \text{ord}_{\infty}(p) - \deg \mathfrak{D} - 2g + 1 \). This implies that there exists \( \beta = d'/p \in \Omega \) such that \( \lambda = e_T(\beta) \) and \( \text{ord}_{\infty}(\beta) \geq C_1 \). Applying the exponential function to \( \beta \), we obtain \( \text{ord}_{\infty}(\lambda) \geq C_0 \).

On the other hand, we have

\[
\lambda = \frac{d' \zeta}{p} \prod_{0 \neq \epsilon \in \mathfrak{D}} \left( 1 - \frac{d' \zeta}{p \epsilon} \right) = d' \zeta \prod_{0 \neq \epsilon \in \mathfrak{D}} \left( 1 - \frac{d'}{p \epsilon} \right).
\]
Since \( \mathfrak{D} \) is discrete inside \( k_{\infty} \) and \( \text{ord}_{\infty}(p) = -h \deg \mathfrak{M} \). This implies

\[
\text{ord}_{\infty}(\lambda) \leq O(\deg \mathfrak{M}) + \text{ord}_{\infty} \left( \prod_{0 \neq \epsilon \in \mathfrak{D}, \text{ord}_{\infty}(d'/p \epsilon) = 0} \left( 1 - \frac{d'}{p \epsilon} \right) \right).
\]
There are only finitely many choices of $0 \neq c \in \mathfrak{D}$ with $\text{ord}_\infty(d'/pc) = 0$, because $\text{ord}_\infty(c) = \text{ord}_\infty(d') - \text{ord}_\infty(p) \geq C_2$. Moreover, the number of these $c$ has a bound depending only on $\mathfrak{D}$. For each of these $c$ we deduce

$$\text{ord}_\infty \left(1 - \frac{d'}{pc}\right) \leq \text{ord}_\infty \left(\frac{1}{pc}\right) \leq O(\deg \mathfrak{M}).$$

This completes the proof of (2).

To prove (3), we may assume $\text{ord}_\infty(x) < \text{ord}_\infty(\lambda)$, because of (1). Since

$$x^{\text{re}} = x \prod_{0 \neq \lambda \in A_{\mathfrak{M}}} (x - \lambda),$$

we have

$$\text{ord}_\infty(a) = \text{ord}_\infty(x) + \sum_{0 \neq \lambda \in A_{\mathfrak{M}}} \text{ord}_\infty(x - \lambda).$$

Using the fact that $\text{ord}_\infty(x - \lambda) = \min\{\text{ord}_\infty(x), \text{ord}_\infty(\lambda)\}$ always if $\text{ord}_\infty(x) \neq \text{ord}_\infty(\lambda)$, we obtain that $\text{ord}_\infty(x) = \text{ord}_\infty(a)/q^{\deg \mathfrak{M}} \geq C_1$. This yields (3).

To prove (4), let $b \in \mathcal{O}$ be a fixed positive element such that $\deg(b) \geq 1$ and let $x$ be a root of $x^a = a$. Since the exponential mapping $e_{\mathfrak{r}} : \mathfrak{M} \to \mathfrak{M}$ is surjective, we can choose an element $\eta \in \mathfrak{M}$ such that $e_{\mathfrak{r}}(\eta) = x$. It follows $e_{\mathfrak{r}}(\eta/p)^{\text{re}} = a$, where $(p) = \mathfrak{M}^a$ as above. This implies that

$$(e_{\mathfrak{r}}(\eta/p)^{\text{re}})^{\text{re}} = a.$$ 

Now $e_{\mathfrak{r}}(\eta/p)^{\text{re}}$ lies in the finite extension $k_{\mathfrak{M}}(\eta)/k_{\mathfrak{M}}$; it follows that all the roots of the equation $x^{\text{re}} = a$ can be found in the finite extension $k_{\mathfrak{M}}(\eta, \xi)/k_{\mathfrak{M}}$. Hence the ramification index $e_{\mathfrak{r}}(K_{\mathfrak{M}}/k)$ is always bounded by the ramification index of $k_{\infty}(\eta, \xi)/k_{\infty}$, which is independent of $\mathfrak{M}$.}

To estimate the $\infty$-part of the discriminant divisor, let $A \subset k$ be the local ring at the infinite place $\infty$, and let the integral closure of $A$ in $K_{\mathfrak{M}}$ (resp. $k_{\mathfrak{M}}$) be denoted by $A_{\infty, \mathfrak{M}}$ (resp. $A_{\infty}$).

**Proposition 3.3.** Let $\mathfrak{P}$ run through prime ideal in $\mathcal{O}$. The $\infty$-part of the discriminant $A(k_{\mathfrak{M}}/H)$ divides $\text{(\infty)}^{O(\deg \mathfrak{P})}_H$, where the implied constant depends only on $k, \phi$, and $a$.

**Proof.** Let $\infty$ be an infinite place of $A_{\mathfrak{M}}$. Let $K_{\infty, \mathfrak{M}} \subset K_{\mathfrak{M}}$ be the maximal subextension of $K_{\mathfrak{M}}/k_{\mathfrak{M}}$ unramified at $\infty$. By Proposition 3.2(4), we have $\text{Gal}(K_{\mathfrak{M}}/K_{\infty, \mathfrak{M}}) \cong (\mathbb{Z}/\mathfrak{P})^a$ with $\mathfrak{P} = O(1)$. Let $x \in K_{\mathfrak{M}}$ be a root of $x^a - a = 0,$
and denote its monic minimal polynomial over $K_{\infty}$ by $f(x)$. By Theorem 2.6(2), we may assume $\text{Gal}(K_{\wp}/K_{\infty}) \cong \mathbb{Z}$ and $\text{Gal}(K_{\wp}/K_{\infty}) \cong R \subset A_{\wp}$.

Since $R$ is a $d$-dimensional vector space over $F_1$, we obtain

$$f(x) = \prod_{x \in R} (x - \alpha + \lambda) = (x - \alpha)^d + \sum_{i=1}^{d} c_i(x - \alpha)^{d-i},$$

where $c_i \in K_{\infty}$ and $c_d = \prod_{x \in R \setminus \{0\}} \lambda$.

According to Proposition 3.2(3), $\text{ord}_\wp(c_d) = 0$ for some positive constant $C$. This implies that $\pi \cdot \alpha \in A_{\wp}$. Let $A_{\infty}$ be the integral closure of $A$ in $K_{\infty}$. Let $g(x) = \pi^{dC} \cdot f(-\pi \cdot \alpha)$. Then $g(x)$ is the monic minimal polynomial of $\pi \cdot \alpha$ over $K_{\infty}$ and $g(x) \in A_{\wp}[x]$. Since $g'(\pi \cdot \alpha)$ is equal to $\pi^{dC} \cdot c_d$, the $\infty_1$-part of the discriminant $\Delta(A_{\wp}/A_{\infty})$ divides

$$N_{\wp_{\infty}/k \wp_{\infty}}(N_{\wp_{\infty}/k \wp_{\infty}}(\pi^{dC} \cdot c_d)) = N_{\wp_{\infty}/k \wp_{\infty}}(\pi^{dC} \cdot c_d)^d,$$

which is equal to $\pi^{N_{k \infty}/k \wp_{\infty}}(\pi^{dC} \cdot c_d)$ by Proposition 3.2(2), this in turn divides

$$\pi^{dC} \cdot (k \wp_{\infty}/k \wp_{\infty}) \cdot \pi^{O(\deg \wp)} \cdot (k \wp_{\infty}/k \wp_{\infty}),$$

which is equal to $\pi^{dC} \cdot (k \wp_{\infty}/k \wp_{\infty})$. This implies that $\Delta(A_{\wp}/A_{\infty})$ divides $\pi^{dC} \cdot (k \wp_{\infty}/k \wp_{\infty})$ (because $A_{\wp}$ is the integral closure in $k \wp_{\infty}$ of the local ring at the infinite place $\infty$). Combining with Proposition 3.1(1), we obtain that the $\infty_1$-part of $\Delta(K_{\infty}/H)$ divides

$$N_{k \wp_{\infty}/k \wp_{\infty}}(\pi^{dC} \cdot (k \wp_{\infty}/k \wp_{\infty}) \cdot (k \wp_{\infty}/k \wp_{\infty})),$$

which is equal to $\pi^{dC} \cdot (k \wp_{\infty}/k \wp_{\infty})$. Since $\pi = O(1)$, this completes the proof.

Our main theorem in this section is

**Theorem 3.4.** Suppose that $\mathfrak{M}$ runs through the squarefree ideal in $\mathcal{O}$. Then the discriminant $\Delta(K_{\mathfrak{M}}/H)$ divides

$$\mathfrak{M}^{2N_{\mathfrak{M}}} \cdot \mathfrak{M}^{O(N_{\mathfrak{M}} \deg \mathfrak{M})},$$

where the implied constant depends only on $k, \wp, a_1$. Moreover, we have

$$\frac{d_{\mathfrak{M}}}{N_{\mathfrak{M}}} = O(\deg \mathfrak{M}),$$

as $\deg \mathfrak{M}$ goes to infinity.
Proof. This follows from Propositions 3.1(2) and 3.3 and the fact that \( K_N \) and \( K_{N'} \) are linearly disjoint over the class field \( H \) if squarefree ideals \( \mathfrak{m} \) and \( \mathfrak{m}' \) are relatively prime (Theorem 2.6(3)).

4. ARTIN’S CONJECTURE FOR RANK ONE DRINFELD MODULES

We first recall a generalized Artin’s problem for function fields. We refer to [8, Theorem 3.1] for more details. Let \( L, H \) be two fixed function fields over \( k \) (finite extensions), and the field of constants of \( H \) is \( \mathbb{F}_q \). Let \( S \) be a set of prime divisors of \( L \). For each prime divisor \( \mathfrak{p} \in S \), let \( K_{\mathfrak{p}} \) be a fixed finite Galois extension of \( H \). Our generalized Artin’s problem is to determine the density of the set of prime divisors in \( H \) which do not split completely in any \( K_{\mathfrak{p}} \) for all \( \mathfrak{p} \in S \).

Let \( S^* \) be the set consisting of all square free divisors (including 1) composed from prime divisors in \( S \) (i.e., \( \mathfrak{m} \in S^* \) if and only if \( \mathfrak{m} = 1 \) or \( \mathfrak{m} \) can be written as a finite product of distinct prime divisors in \( S \)). On \( S^* \) divisibility gives a natural partial order. Under this partial ordering we view \( S^* \) as a (Boolean) lattice. Given divisor \( \mathfrak{m} \in S^* \), let \( K_{\mathfrak{m}} = \prod_{\mathfrak{p} \mid \mathfrak{m}} K_{\mathfrak{p}} \) (set \( K_1 = H \)), \( N_{\mathfrak{m}} = [K_{\mathfrak{m}} : H] \), and \( d_{\mathfrak{m}} = \deg(K_{\mathfrak{m}}/H) \). Also let \( f_{\mathfrak{m}} \) be the degree of the field of constants of \( K_{\mathfrak{m}} \) over \( \mathbb{F}_q \).

To positive integer \( x \), let \( f(x, H) \) denote the number of prime divisors \( \mathfrak{p} \) of \( H \) such that \( \deg(\mathfrak{p}) = x \), and \( \mathfrak{p} \) does not split completely in any \( K_{\mathfrak{p}} \) for all \( \mathfrak{p} \in S \). Also set

\[
\delta_S = \sum_{\mathfrak{m} \in S^*} \frac{\mu(\mathfrak{m})}{N_{\mathfrak{m}}},
\]

where \( \mu \) is the mobius function defined by \( \mu(\mathfrak{m}) = (-1)^n \), if \( \mathfrak{m} = \prod_{i=1}^n \mathfrak{p}_i \).

The fundamental theorem for our generalized Artin’s problem is

**Theorem 4.1.** Suppose that

\[
\sum_{\mathfrak{m} \in S^*} \frac{1}{N_{\mathfrak{m}}} < \infty,
\]

and for each prime divisor \( \mathfrak{p} \) of \( H \) the number of \( \mathfrak{p} \in S \) such that \( \mathfrak{p} \) splits completely in \( K_{\mathfrak{p}} \) is finite. Also suppose that the following three conditions are true:

(a) \( f_{\mathfrak{m}} = 1 \) for all \( \mathfrak{m} \in S^* \).

(b) As \( \deg(\mathfrak{m}) \to \infty \), \( d_{\mathfrak{m}}/N_{\mathfrak{m}} = O(\deg(\mathfrak{m})) \), and \( N_{\mathfrak{m}} = O(q^{e \deg(\mathfrak{m})}) \) for some constant \( e > 0 \).
There exists a real number $\alpha > 1/\ln q$ such that the number of prime divisors $\Psi'$ of $H$ with $\deg \Psi' = x$ and $\Psi'$ splits completely in some $K_{\Psi'}$, $\deg \Psi > x/2 - \alpha \ln x$, is $o(q^x/x)$.

Then we have

$$f(x, H) = \delta_S - \frac{q^x}{x} + o\left(\frac{q^x}{x}\right).$$

**Proof.** See [8, Section 3].

In this section we shall take $L = k$, with $H$ equals to the Hilbert class field of $\mathcal{O}$. The set $S$ is the set of all prime ideals in $\mathcal{O}$ identified as a set of prime divisors of $k$. Since one has one-to-one correspondence between prime divisors of $H$ not lying above $\infty$ and prime ideals of $\mathcal{O}$, we shall also replace prime divisors $\mathcal{P}$ by prime ideals of $\mathcal{O}$ in Theorem 4.1.

**Lemma 4.2.** Suppose that $a$ is not a torsion point in $\phi(\mathcal{O})$. Then the number of prime ideals $\Psi' \in \mathcal{O}$ such that $\deg \Psi' = x$ and $\Psi'$ splits completely in some $K_{\Psi'}(\Psi \in S)$, $x/2 + \ln x \leq \deg \Psi \leq x$, is $o(q^x/x)$.

**Proof.** We first note that the number of prime ideals $\Psi' \in \mathcal{O}$ of degree $x$ such that $N_{H_k}(\Psi')$ is not a prime ideal in $\mathcal{O}$ is $o(q^x/x)$. This follows from the fact that if $N_{H_k}(\Psi')$ is not a prime ideal, then the prime ideal of $\mathcal{O}$ containing $N_{H_k}(\Psi')$ will have degree at most $x/2$, together with the prime number theorem for $\mathcal{O}$. Thus in our counting of those prime ideals $\Psi'$ with $\deg \Psi' = x$ such that $\Psi'$ splits completely in some $K_{\Psi'}$, $x/2 + \ln x \leq \deg \Psi \leq x$, it is enough to assume that $N_{H_k}(\Psi')$ is prime. Write $N_{H_k}(\Psi') = (p)$ with positive $p \in \mathcal{O}$. By Proposition 2.3, $a^p \in \text{Hom}(\mathcal{O}, \mathcal{O})$. On the other hand, as $(p)$ now splits completely in $H$, $x = \deg \Psi' = \deg p = \deg(p - 1)$; therefore $0 \leq \deg((p - 1)^{-1}) \leq x/2 - \ln x$. Hence $\Psi'$ divides the ideal in $\mathcal{O}$ generated by

$$\prod_{\text{ideal } \mathfrak{m} \in \mathcal{O}} a^\mathfrak{m}.$$  

Since

$$a^\mathfrak{m} = \prod_{\lambda \neq \lambda_0} (a - \lambda) \neq 0,$$

we have, from Proposition 3.2(1),

$$\deg a^\mathfrak{m} = -\ord_\infty (a^\mathfrak{m}) \leq \deg a + \sum_{0 \neq \lambda \neq \lambda_0} \max\{\deg a, -\ord_\infty (\lambda)\}$$

$$\leq q^\deg \mathfrak{m}(\deg a + C),$$
where \( C \) is a positive constant. Thus the number of prime ideals \( \mathfrak{P}' \in \mathfrak{O}' \) such that \( \deg \mathfrak{P}' = x \) and \( \mathfrak{P}' \) splits completely in some \( K_{\mathfrak{P}}(\mathfrak{P} \in \mathcal{S}) \), \( x/2 + \ln x \leq \deg \mathfrak{P} \leq x \), is less than

\[
\deg \left( \prod_{\text{ideal } \mathfrak{M} \text{ in } \mathfrak{O}} \mathfrak{M} \right) \left| x + o(q^x/x) \right.
\]

Since the number of ideals \( \mathfrak{M} \) in \( \mathfrak{O} \) with \( \deg \mathfrak{M} = i \) is \( O(q^i) \) (e.g., as a consequence of the Riemann–Roch theorem), the number of the prime ideals \( \mathfrak{P} \in \mathfrak{O} \) which we are counting is dominated by

\[
O \left( \frac{x^2 - \ln x}{x^2} \right) / \ln x + o(q^x/x)
\]

This completes the proof. \( \square \)

Let \( \mathfrak{U} \) be an ideal in \( \mathfrak{O} \) and let \( b \) be an element in \( \mathfrak{O} \) such that \( b \in (\mathfrak{O}/\mathfrak{A})^\times \) (i.e., \( \mathfrak{U} \) and \( b \) are relatively prime ideals in \( \mathfrak{O} \)). We let \( \pi(N; b, \mathfrak{A}) \) denote the number of prime ideals \( \mathfrak{P}' \) in \( \mathfrak{O}' \) such that if \( N_{\mathfrak{P} \mathfrak{A}} \mathfrak{P}' = (p) \) for some positive element \( p \in \mathfrak{O} \), then \( p \equiv b \) (mod \( \mathfrak{U} \)) and \( \deg p = N \) (i.e., \( \deg \mathfrak{P}' = N \)). The following version of the Brun–Titchmarsh theorem for \( \mathfrak{O} \) will be needed:

**Theorem 4.3.** There exists effective constants \( C_1 \) and \( C_2 \), depending only on the genus \( g \) of \( k \) and the class number \( h = \left[ H : k \right] \), such that if \( N > \deg \mathfrak{A} + C_1 + C_2 \ln \deg \mathfrak{A} \), then we have

\[
\pi(N; b, \mathfrak{A}) \leq \frac{C_3 h q^N}{\phi(\mathfrak{A})(K_1 + 1 - 2g)};
\]

where \( \phi(\mathfrak{A}) \) is the order of \( (\mathfrak{O}/\mathfrak{A})^\times \), \( K_1 \) is equal to

\[
\min \left\{ \left[ \frac{N - 1}{h} \right], \left[ \frac{N - \deg \mathfrak{A} - C_1 - C_2 \ln \deg (\mathfrak{A} + 4g)}{2} \right] \right\},
\]

and \( C_3 \) is a positive effective constant depending only on \( k \).

**Proof.** See [7, Theorem 4.3]. \( \square \)

Now let \( SC_{x, y} \) be the number of prime ideals \( \mathfrak{P}' \) in \( \mathfrak{O}' \) such that \( \deg \mathfrak{P}' = x \) and \( \mathfrak{P}' \) splits completely in some \( K_{\mathfrak{P}}(\mathfrak{P} \in \mathcal{S}) \), \( \deg \mathfrak{P} > x/2 - y \cdot \ln x \). With our Brun–Titchmarsh theorem at hand, we can establish
Lemma 4.4. Suppose $v > 0$ and $a$ is not a torsion point in $\mathfrak{p}(C')$. As $x$ goes to infinity, we have

$$SC_{x,v} = o(q^v/x).$$

Proof. Let $m(x, d_1, d_2)$ be the number of prime divisors $\mathfrak{p}'$ in $C'$ with $\deg \mathfrak{p}' = x$ and $\mathfrak{p}'$ splits completely in some $K_{q'}$, $\mathfrak{p} \in S$, $d_1 < \deg \mathfrak{p} \leq d_2$. As in the proof of Lemma 4.2, it suffices to consider those prime ideals $\mathfrak{p}'$ in $C'$ such that $N_{H_k}(\mathfrak{p}') = (p)$ is a prime ideal in $C$. By Proposition 2.3, if $\mathfrak{p}'$ splits completely in some $K_{q'}$, then $\deg \mathfrak{p} \leq \deg (p-1) = \deg p = x$. In view of Lemma 4.2, this gives

$$SC_{x,v} \leq m(x, x/2 - v \cdot \ln x) + o(q^v/x).$$

Let us denote the number of prime ideals $\mathfrak{p}'$ in $C'$ such that $\deg \mathfrak{p}' = x$, $N_{H_k}(\mathfrak{p}') = (p)$ is prime, and $\mathfrak{p}'$ splits completely in $K_{q'}$, by $\pi_1(x, \mathfrak{p})$. Then we have

$$m(x, x/2 - v \cdot \ln x) \leq \sum_{\mathfrak{p} \in S} \pi_1(x, \mathfrak{p}) \leq \sum_{x/2 - v \cdot \ln x \leq \deg \mathfrak{p} \leq x/2 + \ln x} \pi_1(x, \mathfrak{p}).$$

By Proposition 2.3 and the assumption that $N_{H_k}(\mathfrak{p}') = (p)$ is prime, we have

$$\pi_1(x, \mathfrak{p}) \ll \pi(x; 1, \mathfrak{p}).$$

If $x/2 - v \cdot \ln x < \deg \mathfrak{p} \leq x/2 + \ln x$, then by our Brun–Titchmarsh theorem for $C$ (Theorem 4.3), there exists a constant $C > 0$ such that

$$\pi(x; 1, \mathfrak{p}) \leq C \cdot \frac{q^x}{q^{\deg \mathfrak{p}^2} x}.$$ 

It follows that

$$\sum_{\mathfrak{p} \in S} \pi_1(x, \mathfrak{p}) \ll \frac{q^x}{x} \cdot \sum_{\mathfrak{p} \in S} \frac{1}{q^{\deg \mathfrak{p}^2}}.$$
Combining this with Eqs. (2) and (3), and applying the prime number theorem for \( \mathcal{O} \), we arrive at

\[
SC_{x, x} \ll \frac{q^x}{x} \sum_{x/2 - \sqrt{x} \cdot \ln x < i \leq x/2 + \ln x} \frac{1}{i} = 0 \left( \frac{q^x}{x} \right).
\]

In order to study the solvability of equation \( x^p = a \) for various prime ideals \( \mathfrak{p} \) of \( \mathcal{O} \), we recall an analogue of the Mordell-Weil theorem for Drinfeld modules established by Poonen [10]: The \( \mathcal{O} \)-module \( \phi(H) \) is the direct sum of its torsion submodule, which is finite, with a free \( \mathcal{O} \)-module of countable rank (not finite). As a corollary, if \( a \) is nontorsion in \( \phi(H) \), it cannot be divisible by infinitely many distinct elements from \( \mathcal{O} \).

**Theorem 4.5.** Suppose that \( q \neq 2 \) and \( a \neq 0 \in \mathcal{O}' \). Then

1. Given prime ideal \( \mathfrak{p} \in \mathcal{O} \), we have \( \text{Gal}(K_{\mathfrak{p}}/K_{\mathfrak{p}^*}) \cong \mathcal{O}/\mathfrak{p} \) and \( N_{\mathfrak{p}} = (q^{\deg \mathfrak{p}} - 1) \cdot q^{\deg \mathfrak{p}} \) if \( \deg \mathfrak{p} \gg 0 \).
2. \[
\sum_{\mathfrak{p} \in S^*} \frac{1}{N_{\mathfrak{p}}} < \infty.
\]

**Proof.** First we note that \( q \neq 2 \) and \( a \neq 0 \in H \) implies that \( a \) is nontorsion. This follows from [2, Corollary 7.5.6]. To prove (1), suppose there are infinitely many prime ideals \( \mathfrak{p} \) in \( \mathcal{O} \) such that \( x^\mathfrak{p} = a \) has a solution in \( \mathcal{O}' \). We may assume these \( \mathfrak{p} \) are in the same ideal class. If \( h \) is the class number of \( \mathcal{O}' \), multiplying any \( h \) such prime ideals gives an element \( b \in \mathcal{O} \) with \( x^b = a \) solvable in \( \mathcal{O}' \). Since \( a \) is always nontorsion in \( \phi(H) \), this contradicts Poonen’s theorem. In view of Theorem 2.6(2), the proof of (1) is complete.

Using (1), and the prime number theorem for \( \mathcal{O} \), we then have

\[
\ln \left( \prod_{\mathfrak{p} \in S} \left( 1 + \frac{1}{N_{\mathfrak{p}}} \right) \right) \leq \sum_{\mathfrak{p} \in S} \frac{1}{N_{\mathfrak{p}}} \leq \sum_{i=1}^{\infty} \frac{1}{i(q^i - 1)} < \infty.
\]

By 2.6(3), this implies:

\[
\sum_{\mathfrak{p} \in S^*} \frac{1}{N_{\mathfrak{p}}} = \prod_{\mathfrak{p} \in S} \left( 1 + \frac{1}{N_{\mathfrak{p}}} \right) < \infty.
\]
Let $C_a(x)$ be the number of prime ideals $\mathfrak{p}'$ in $\mathcal{O}'$ with $\deg \mathfrak{p}' = x$ such that $\alpha$ is a generator of $\phi(\mathcal{O}'/\mathfrak{p}')$, and let

$$\delta_a = \sum_{\mathfrak{p}' \in S^*} \frac{\mu(\mathfrak{p}')}{N_{\mathfrak{p}' \mathfrak{p}}^N} < \infty.$$ 

The main theorem of this paper is

**Theorem 4.6.** Suppose that $q \neq 2$ and $a \neq 0 \in \mathcal{O}'$. Then

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

Moreover $\delta_a > 0$ always.

**Proof.** It suffices to check the conditions of Theorem 4.1. The condition

$$\sum_{\mathfrak{p}' \in S^*} 1/N_{\mathfrak{p}' \mathfrak{p}}^N < \infty$$

follows from Theorem 4.5(2). Let $\mathfrak{p}'$ be a prime ideal in $\mathcal{O}'$ and let $N_{\mathfrak{p}' \mathfrak{p}}(\mathfrak{p}') = (p(\mathfrak{p}'))$ for some positive element $p(\mathfrak{p}') \in \mathcal{O}$. Suppose that $\mathfrak{p}'$ splits completely in $K_\mathfrak{p}$. Then by Proposition 2.3, we have $\mathfrak{p}' \mid (p(\mathfrak{p}') - 1)$. Thus the number of $\mathfrak{p}' \in S$ such that $\mathfrak{p}'$ splits completely in $K_\mathfrak{p}$ is finite. The condition (a) of Theorem 4.1 follows from Theorem 2.6(5). The condition (b) of Theorem 4.1 follows from Theorem 3.4. The condition (c) of Theorem 4.1 follows from Lemma 4.4.

Since as $q \neq 2, a \in \phi(\mathcal{O}')$ is always nontorsion, one more application of Theorem 2.6(3) gives

$$\delta_a = \prod_{\mathfrak{p}' \in S^*} \left(1 - \frac{1}{N_{\mathfrak{p}' \mathfrak{p}}}\right) > 0.$$  

REFERENCES