

EULER SYSTEMS IN GLOBAL FUNCTION FIELDS

BY

FEI XU

*Morningside Center of Mathematics, Institute of Mathematics
Academia Sinica, Beijing 100080, P. R. China
e-mail: xufei@mcm01.mcm.ac.cn*

AND

JIANQIANG ZHAO

*Department of Mathematics, University of Pennsylvania
Philadelphia, PA 19104, USA
e-mail: iqz@math.upenn.edu*

ABSTRACT

In this paper, the construction of Euler systems of cyclotomic units in a general global function fields is explained. As an application, an analogue of Gras' conjecture in a global function field is proved.

1. Introduction and notations

Kolyvagin [7] introduced his remarkable Euler systems to prove important new results on ideal class groups of number fields. This method was further developed by Rubin in [10–12]. Using similar arguments, Feng and Xu [2] proved a result of the same type about abelian extensions of rational function fields. In this paper, we extend [2] to a general global function field.

Notation is standard if not explained. Specifically, k is a global function field with a finite constant field \mathbb{F}_q of q elements and ∞ is a fixed infinite prime in k of degree d_∞ . A denotes the ring of the functions in k which are holomorphic away from ∞ . \mathbf{M}_∞ is the set of integral ideals of A and \mathbf{P}_∞ is the set of prime ideals of A . \mathfrak{e} stands for the unit ideal of A . Let k_∞ be the completion of k at

Received April 25, 1995 and in revised form May 4, 2000

∞ and Ω the completion of the algebraic closure of k_∞ at ∞ . We also use \mathbb{F}_∞ for the constant field of k_∞ which is a finite extension over \mathbb{F}_q of degree d_∞ . Put $\Phi(\mathfrak{a}) = \#(A/\mathfrak{a})^\times$ and $N\mathfrak{a} = \#(A/\mathfrak{a})$ for any $\mathfrak{a} \in \mathbf{M}_\infty$.

For any finite abelian extension E/k , O_E stands for the integral closure of A in E and $\mu(E)$ for the multiplicative group of nonzero elements of the constant field of E .

Now we briefly review some facts from rank one elliptic modules (cf. [3, 5, 6]). Let $i: A \hookrightarrow \Omega$ be the inclusion map. An elliptic (Drinfeld) module over Ω is a nontrivial representation ρ of A as a ring of endomorphisms on the additive group scheme $\mathbb{G}_{a/\Omega} = \text{Spec}(\Omega[t])$ such that the induced representation on the tangent space at zero is i . The endomorphism ring of \mathbb{G}_a is isomorphic to the left twisted polynomial ring $\Omega\{\mathbf{F}\}$ in the Frobenius endomorphism \mathbf{F} on $\mathbb{G}_{a/\Omega}$. By the standard argument, it is clear that there is a positive integer n such that $q^{\deg \rho(x)} = (N(x))^n$ for all $x(\neq 0) \in A$. Such n is defined as the rank of ρ . In this paper we always assume that $n = 1$. Since the category of rank one A -lattices in Ω is equivalent to the category of rank one elliptic modules over Ω (see [3, §5]), there is a natural one-to-one correspondence between the set of isomorphic classes of rank one elliptic modules over Ω and the set of ideal class group $\text{Pic}(A)$ of A .

A sign function $s: k_\infty^\times \rightarrow \mathbb{F}_\infty^\times$ is a co-section of the inclusion morphism $\mathbb{F}_\infty^\times \hookrightarrow k_\infty^\times$ such that $s(u) = 1$ for all local principal units. An elliptic module ρ is called sign normalized with respect to s if the leading coefficient of $\rho(x)$ is in \mathbb{F}_∞^\times and equal to $s(x)$ twisted by a fixed element in $\text{Gal}(\mathbb{F}_\infty/\mathbb{F}_q)$ for all $x(\neq 0) \in A$. The field of definition K_ϵ of a sign normalized elliptic module (the normalizing field) only depends on the sign function (see [5, Def. 4.9]) and there is a sign normalized elliptic module $\rho_i (i = 1, \dots, \#\text{Pic}(A))$ in each isomorphism class over Ω (see [5, Prop. 4.6]). We always fix the sign function s in this paper.

Since the left ideal generated by $\{\rho(a) : a \in \mathfrak{m}\}$ in $\Omega\{\mathbf{F}\}$ for some elliptic module ρ is principal, we define $\rho_{\mathfrak{m}}(t)$ to be the polynomial in t obtained by letting the unique monic generator of this left ideal act on t ($\mathfrak{m} \in \mathbf{M}_\infty$). The \mathfrak{m} -torsion points of ρ are defined as the roots of $\rho_{\mathfrak{m}}(t)$, which form a cyclic A -module. Let $\Lambda_{\mathfrak{m}}^{(i)}$ be the \mathfrak{m} -torsion points of ρ_i for $i = 1, \dots, \#\text{Pic}(A)$. Then $K_{\mathfrak{m}} := K_\epsilon(\Lambda_{\mathfrak{m}}^{(i)})$ for all $1 \leq i \leq \#\text{Pic}(A)$ (see [5, §4]) is a cyclotomic function field over k . Let $H_{\mathfrak{m}}$ be the maximal “real” subfield of $K_{\mathfrak{m}}$ which is the fixed field of the decomposition group of ∞ .

2. Index formulas of cyclotomic units

The index formulas of cyclotomic units were established recently by efforts of Anderson, Hayes, Oukhaba, Shu and Yin (see [1], [4], [8], [15] and [18]). In this section, we review their results.

Let $F = H_m$ for some $m \in \mathbf{M}_\infty$, $G = \text{Gal}(F/k)$ and $d = [F : k]$. Fix a prime number l with $(l, dq(q^{d\infty} - 1)) = 1$. For any irreducible \mathbb{Z}_l -representation of G denoted by χ , write

$$e(\chi) = \frac{1}{d} \sum_{\sigma \in G} \text{Tr}(\chi(\sigma)) \sigma^{-1}.$$

If Y is a $\mathbb{Z}[G]$ -module, then $Y \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is a $\mathbb{Z}_l[G]$ -module in the natural way. Write $Y(\chi) = e(\chi)(Y \otimes_{\mathbb{Z}} \mathbb{Z}_l)$. Let $\omega_1, \dots, \omega_d$ denote all the primes of F above ∞ .

First we have the following lemma

LEMMA 2.1: *If χ is a nontrivial irreducible \mathbb{Z}_l -representation of G , then $O_F^\times(\chi)$ is a free rank one $e(\chi)\mathbb{Z}_l[G]$ -module.*

Proof: By assumption $(l, q^{d\infty} - 1) = 1$, thus $O_F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is a free \mathbb{Z}_l -module of rank $d - 1$ and

$$O_F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_l = \bigoplus_{\chi} O_F^\times(\chi)$$

where χ runs through all non-trivial irreducible \mathbb{Z}_l -representations of G .

On the other hand, since $\text{Pic}^0(F)$ is finite there is an $\varepsilon \in O_F^\times$ such that ε has a zero at ω_1 and a pole at ω_i for all $i = 2, \dots, d$. Therefore $\{\sigma(\varepsilon) : \sigma \in G \setminus \{1_G\}\}$ are linearly independent over \mathbb{Z} and $e(\chi)\varepsilon \neq 1$ for any nontrivial irreducible \mathbb{Z}_l -representation χ of G . Since $e(\chi)\mathbb{Z}_l[G]$ is isomorphic to the ring of integers of the unramified extension of \mathbb{Q}_l of degree $\dim(\chi)$, one concludes the lemma by considering the \mathbb{Z}_l -rank of $O_F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_l$. ■

The cyclotomic units of F consist of two parts. One is the ramified part and the other part is unramified.

(I) UNRAMIFIED UNITS. In order to get a nice index formula, one has to construct enough units in the Hilbert class field H of k . This was done by Hayes (see [4]) and Oukhaba (see [8] and [9]).

Let ρ be a sign normalized elliptic module of rank one and $\sigma \in \text{Gal}(H/k)$. For any $\mathfrak{p} \in \mathbf{P}_\infty$ with the Artin symbol $(\mathfrak{p}, H/k) = \sigma$, let λ be a nonzero root of $\rho_{\mathfrak{p}}(t)$. Let $U(\sigma, H)$ be the subgroup of $O_{K_c}^\times$ generated by $N_{K_{\mathfrak{p}}/K_c}(\rho_{\mathfrak{b}}(\lambda)/\lambda)$, where \mathfrak{b} runs over the set \mathbf{M}_∞ with $(\mathfrak{b}, \mathfrak{p}) = 1$. Then $U(\sigma, H)$ is independent of

the choice of ρ and \mathfrak{p} (see the proof of [9, Lemma 2] and [9, p. 304]). Then the unramified units of F are defined as

$$U = \prod_{\sigma \in \text{Gal}(H/k)} U(\sigma, H).$$

Remark 2.2: Since $[K_{\mathfrak{p}} : H_{\mathfrak{p}}K_{\mathfrak{e}}] = q - 1$, then $\mathbb{F}_{\infty}^{\times}U = \mathbb{F}_{\infty}^{\times}(\bar{E}_G)^{q-1}$ where \bar{E}_G is defined in [9, §1 and §2]. \bar{E}_G is also the same as \bar{E} defined in [18] (see remarks in [9, p. 299] and the introduction in [18]).

(II) **RAMIFIED UNITS.** The ramified units R are defined as the intersection with $O_{K_m}^{\times}$ of the subgroup of K_m^{\times} generated by $\mathbb{F}_{\infty}^{\times}$ and $\bigcup_{1 \leq i \leq \# \text{Pic}(A)} \Lambda_m^{(i)}$.

Definition 2.3: The cyclotomic units \mathcal{E}_F of F are defined as $\mathcal{E}_F = N_{K_m/F}(UR)$.

The following theorem is quoted from [18, Thm. 1] and [1].

THEOREM 2.4 (Hayes–Oukhaba–Shu–Yin–Anderson):

$$\#((O_F^{\times}/\mathcal{E}_F) \otimes_{\mathbb{Z}} \mathbb{Z}_l) = \#(\text{Pic}(O_F) \otimes_{\mathbb{Z}} \mathbb{Z}_l).$$

Proof: Since

$$((UR) \cap O_F^{\times})^{q^{d_{\infty}}-1} \subseteq \mathcal{E}_F \subseteq (UR) \cap O_F^{\times},$$

the theorem follows from $(l, q^{d_{\infty}} - 1) = 1$, the remark at the end of [18, §2] and Remark 2.2. ■

3. Euler systems

Let L be a power of l and

$$\text{Pic}(A) = \langle \bar{\mathfrak{a}}_1 \rangle \oplus \cdots \oplus \langle \bar{\mathfrak{a}}_h \rangle$$

be a decomposition into a direct sum of cyclic subgroups, where \mathfrak{a}_i is a fixed ideal of A and $\bar{\mathfrak{a}}_i$ is its class in $\text{Pic}(A)$ for $1 \leq i \leq h$. Write n_i for the order of $\bar{\mathfrak{a}}_i$ in $\text{Pic}(A)$ and fix a generator $a_i \in A$ of $\mathfrak{a}_i^{n_i}$ for $1 \leq i \leq h$. Let \mathcal{Q} be the subset of \mathbf{P}_{∞} whose elements \mathfrak{q} are prime to $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ and satisfy

- (i) \mathfrak{q} splits completely in F/k ,
- (ii) \mathfrak{q} splits completely in $k(a_1^{1/L}, \dots, a_h^{1/L})/k$,
- (iii) $L \mid \Phi(\mathfrak{q})$.

By Chebotarev's density theorem, \mathcal{Q} is infinite. Let S be the subset of \mathbf{M}_{∞} whose elements \mathfrak{s} are square-free and only divisible by primes in \mathcal{Q} .

LEMMA 3.1: For any $\mathfrak{q} \in \mathcal{Q}$, there is a cyclic sub-extension $F_{\mathfrak{q}}/F$ of degree L of $F \cdot H_{\mathfrak{q}}/F$ which is totally ramified at all primes above \mathfrak{q} and unramified at all primes not dividing \mathfrak{q} .

Proof: Write $\text{Pic}(A, L, \mathfrak{q})$ for the quotient of the group of fractional ideals of A which are prime to \mathfrak{q} modulo the subgroup of the principal ideals having a generator which is an L -th power modulo \mathfrak{q} . Since $L \mid \Phi(\mathfrak{q})$ and $(L, q-1) = 1$, one has the exact sequence

$$0 \longrightarrow \mathbb{Z}/L\mathbb{Z} \longrightarrow \text{Pic}(A, L, \mathfrak{q}) \longrightarrow \text{Pic}(A) \longrightarrow 0.$$

By classfield theory (see [5, p. 230]), one has $\text{Gal}(H_{\epsilon}/k) \cong \text{Pic}(A)$ and there is a subfield H' between H_{ϵ} and $H_{\mathfrak{q}}$ such that $\text{Gal}(H'/k) \cong \text{Pic}(A, L, \mathfrak{q})$ via the Artin map. By the condition (ii) on \mathfrak{q} , \mathfrak{a}_i in $\text{Pic}(A, L, \mathfrak{q})$ has the same order as that in $\text{Pic}(A)$. This implies that the above exact sequence is split. Therefore, there is a subfield H'' of H' such that H''/k is a cyclic extension of degree L . By considering the ramification index, H''/k is totally ramified at \mathfrak{q} and unramified everywhere else. Since $F \cap H'' = k$ by condition (i) on \mathfrak{q} , FH'' is the desired extension. ■

For every $\mathfrak{q} \in \mathcal{Q}$, we fix the field $F_{\mathfrak{q}}$ constructed in Lemma 3.1. It is clear that ∞ splits completely in such $F_{\mathfrak{q}}$. If $\mathfrak{s} \in S$ with $\mathfrak{s} = \mathfrak{q}_1 \cdots \mathfrak{q}_j$, we write $F_{\mathfrak{s}} = F_{\mathfrak{q}_1} \cdots F_{\mathfrak{q}_j}$ and $G_{\mathfrak{s}} = \text{Gal}(F_{\mathfrak{s}}/F)$. For convenience we set $F_{\epsilon} = F$. Furthermore, we define the norm operator

$$N_{\mathfrak{s}} = \sum_{\tau \in G_{\mathfrak{s}}} \tau \in \mathbb{Z}[G_{\mathfrak{s}}].$$

Definition 3.2: An Euler system starting from $\eta \in \mathcal{E}_F$ is a map

$$\theta: S \longrightarrow \bigcup_{\mathfrak{s} \in S} F_{\mathfrak{s}}^{\times}$$

such that $\theta(\epsilon) = \eta$ and satisfying the following properties:

For any $\mathfrak{s} \in S$ and $\mathfrak{q} \mid \mathfrak{s}$ with $\mathfrak{q} \in \mathcal{Q}$,

AX 1. $\theta(\mathfrak{s})$ is a unit of $F_{\mathfrak{s}}$.

AX 2. $N_{\mathfrak{q}}\theta(\mathfrak{s}) = (\text{Fr}_{\mathfrak{q}} - 1)\theta(\mathfrak{s}/\mathfrak{q})$, where $\text{Fr}_{\mathfrak{q}}$ is the Frobenius of \mathfrak{q} .

AX 3. $\theta(\mathfrak{s}) \equiv \theta(\mathfrak{s}/\mathfrak{q})^{\Phi(\mathfrak{q})/L}$ modulo every prime above \mathfrak{q} .

One has the following result.

THEOREM 3.3: For any $\eta \in \mathcal{E}_F$, there is an Euler system starting from η .

Proof: Without loss of generality, we can assume that $\eta \in N_{K_m/F}(U)$ or $\eta \in N_{K_m/F}(R)$.

(I) $\eta \in N_{K_m/F}(U)$: Then η may be built up from the following elements:

$$N_{K_m/F} N_{K_q/K_\epsilon}(\rho_b(\lambda)/\lambda)$$

where $q \in \mathbf{P}_\infty$, $(q, s) = 1$ and λ is a nonzero root of ρ_q for some sign normalized elliptic module ρ by Section 2. Then $\theta(s)$ is obtained by replacing such elements by

$$(1) \quad N_{K_{mq_s}/F_s} \left(\frac{\rho_b(\lambda) - \sum_{p|s} \lambda(p)}{\lambda - \sum_{p|s} \lambda(p)} \right)$$

where $\lambda(p)$ is a fixed p -torsion generator of ρ .

In order to prove $\theta(s)$ satisfying AX 1, AX 2, and AX 3, one only need check that (1) satisfies these three properties.

AX 1 follows from [5, Corollary 4.13 or Thm. 4.17].

Suppose $\tau|s$ with $\tau \in \mathbf{P}_\infty$. Write $s = \tau s_1$. To prove AX 2, one notices

$$\begin{aligned} & N_\tau N_{K_{mq_s}/F_s}(\rho_b(\lambda) - \sum_{p|s} \lambda(p)) \\ &= N_{K_{mq_{s_1}}/F_{s_1}} \prod_{\sigma \in \text{Gal}(K_{mq_s}/K_{mq_{s_1}})} \sigma(\rho_b(\lambda) - \sum_{p|s} \lambda(p)) \\ &= N_{K_{mq_{s_1}}/F_{s_1}} \prod_{\sigma \in \text{Gal}(K_\tau/K_\epsilon)} (\rho_b(\lambda) - \sum_{p|s_1} \lambda(p) - \sigma\lambda(\tau)) \\ &= N_{K_{mq_{s_1}}/F_{s_1}} \left(\frac{\rho_\tau(\rho_b(\lambda) - \sum_{p|s_1} \lambda(p))}{\rho_b(\lambda) - \sum_{p|s_1} \lambda(p)} \right). \end{aligned}$$

The last equality holds by definition since $\{\sigma\lambda(\tau)\}$ are exactly the set of nonzero torsion points of ρ_τ . Therefore AX 2 follows from [5, Theorem 4.12] since $\rho_b(\lambda) - \sum_{p|s_1} \lambda(p)$ is in the set of qs_1 -torsions of ρ and $(\tau, qs_1) = 1$.

Now we show that AX 3 is satisfied too. By ramification considerations one has $K_{mq_{s_1}} \cap F_s = F_{s_1}$ and

$$\begin{aligned} [K_{mq_s} : K_{mq_{s_1}} F_s] &= [K_{mq_s} : K_{mq_{s_1}}] / [K_{mq_{s_1}} F_s : K_{mq_{s_1}}] \\ &= \Phi(\tau) / [F_s : F_{s_1}] = \Phi(\tau) / [F_\tau : F] \quad (\text{since } F_{s_1} \cap F_\tau = F) \\ &= \Phi(\tau) / L. \end{aligned}$$

Therefore AX 3 follows from [5, Theorem 4.17].

(II) $\eta \in N_{K_m/F}(R)$: Then η is built up from the following elements:

$$N_{K_m/F}(\lambda)$$

where λ is a nonzero m -torsion elements of some sign normalized elliptic module ρ . Then $\theta(\mathfrak{s})$ is obtained by replacing such elements by

$$N_{K_{m\mathfrak{s}}/F_{\mathfrak{s}}}(\lambda - \sum_{\mathfrak{p}|\mathfrak{s}} \lambda(\mathfrak{p}))$$

where $\mathfrak{p} \in \mathcal{Q}$ and $\lambda(\mathfrak{p})$ is a fixed generator of \mathfrak{p} -torsion of ρ . It is obvious that $\theta(\mathfrak{e}) = \eta$, which is a unit. If $\mathfrak{s} \neq \mathfrak{e}$, then

$$\lambda - \sum_{\mathfrak{p}|\mathfrak{s}} \lambda(\mathfrak{p})$$

is a unit by [5, Theorem 4.17]. Therefore AX 1 follows. AX 2 and AX 3 follow from the same arguments as those in case (I). ■

We next explain how to construct a sequence of elements of F^\times from an Euler system in the next two lemmas. Before doing this we further set some notation. For each $\mathfrak{q} \in \mathcal{Q}$ we fix a generator $\sigma_{\mathfrak{q}}$ of $\text{Gal}(F_{\mathfrak{q}}/F)$ and write

$$D_{\mathfrak{q}} = \sum_{i=1}^{L-1} i\sigma_{\mathfrak{q}}^i, \quad D_{\mathfrak{s}} = \prod_{\mathfrak{q}|\mathfrak{s}} D_{\mathfrak{q}}, \quad \forall \mathfrak{s} \in S.$$

LEMMA 3.4: For any $\mathfrak{s} \in S$, $D_{\mathfrak{s}}(\theta(\mathfrak{s})) \in [F_{\mathfrak{s}}^\times / (F_{\mathfrak{s}}^\times)^L]^{G_{\mathfrak{s}}}$.

Proof: If $\mathfrak{q}|\mathfrak{s}$, write $\mathfrak{s} = \mathfrak{q}\mathfrak{s}_1$; then

$$\begin{aligned} (\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{s}}(\theta(\mathfrak{s})) &= (L - N_{\mathfrak{q}})D_{\mathfrak{s}_1}(\theta(\mathfrak{s})) \\ &\equiv (1 - \text{Fr}_{\mathfrak{q}})D_{\mathfrak{s}_1}(\theta(\mathfrak{s}_1)) \pmod{(F_{\mathfrak{s}}^\times)^L}. \end{aligned}$$

Since $\text{Fr}_{\mathfrak{q}} \in G_{\mathfrak{s}_1}$, the lemma follows by induction. ■

LEMMA 3.5: For any $\mathfrak{s} \in S$, there is a $\kappa_{\mathfrak{s}} \in F^\times$ such that

$$\kappa_{\mathfrak{s}} \equiv D_{\mathfrak{s}}(\theta(\mathfrak{s})) \pmod{(F_{\mathfrak{s}}^\times)^L}.$$

Proof: Since ∞ splits completely in all $F_{\mathfrak{s}}$, $\mu(F_{\mathfrak{s}}) \subseteq \mathbb{F}_{\infty}^\times$. Thus $(\#\mu(F_{\mathfrak{s}}), L) = 1$. Hence by Lemma 3.4 the following 1-cocycle is well-defined:

$$\begin{aligned} c_{\mathfrak{s}}: G_{\mathfrak{s}} &\longrightarrow F_{\mathfrak{s}}^\times \\ \sigma &\longmapsto [(\sigma - 1)D_{\mathfrak{s}}(\theta(\mathfrak{s}))]^{1/L}. \end{aligned}$$

By Hilbert's Theorem 90, there is a $\beta_{\mathfrak{s}} \in F_{\mathfrak{s}}^\times$ such that $c_{\mathfrak{s}}(\sigma) = (\sigma - 1)\beta_{\mathfrak{s}}$ for all $\sigma \in G_{\mathfrak{s}}$. Put $\kappa_{\mathfrak{s}} = D_{\mathfrak{s}}(\theta(\mathfrak{s}))/\beta_{\mathfrak{s}}^L$ and we are done. ■

Let J denote the group of fractional ideals of F , $J_{\mathfrak{q}}$ the subgroup of J generated by the prime ideals above \mathfrak{q} , $[y]$ and $[y]_{\mathfrak{q}}$ the projections of principal ideal (y) in J/LJ and $J_{\mathfrak{q}}/LJ_{\mathfrak{q}}$, respectively. To look at the factorization of $\kappa_{\mathfrak{s}}$ in $J_{\mathfrak{q}}/LJ_{\mathfrak{q}}$ we need

LEMMA 3.6: *For each prime ideal $\mathfrak{q} \in S$, there is a unique $\text{Gal}(F/k)$ -equivariant homomorphism*

$$\varphi_{\mathfrak{q}}: (O_F/\mathfrak{q}O_F)^{\times} \longrightarrow J_{\mathfrak{q}}/LJ_{\mathfrak{q}}$$

such that the following diagram commutes:

$$\begin{array}{ccc} & F_{\mathfrak{q}}^{\times} & \\ \ell \swarrow & & \searrow r \\ (O_F/\mathfrak{q}O_F)^{\times}/((O_F/\mathfrak{q}O_F)^{\times})^L & \longrightarrow & J_{\mathfrak{q}}/LJ_{\mathfrak{q}} \end{array}$$

where for any $x \in F_{\mathfrak{q}}^{\times}$, $\ell(x) = [(1 - \sigma_{\mathfrak{q}})x]^{L/\Phi(\mathfrak{q})}$ and $r(x) = [N_{\mathfrak{q}}x]_{\mathfrak{q}}$.

Proof: Suppose \mathfrak{P} is a prime ideal of $F_{\mathfrak{q}}$ above \mathfrak{q} and take $\pi \in \mathfrak{P} - \mathfrak{P}^2$. Then the homomorphism

$$\text{Gal}(F_{\mathfrak{q}}/F) \longrightarrow (O_{F_{\mathfrak{q}}}/\mathfrak{P})^{\times}, \quad \sigma \longrightarrow (1 - \sigma)\pi$$

is injective. So the order of $(1 - \sigma_{\mathfrak{q}})\pi$ in $(O_{F_{\mathfrak{q}}}/\mathfrak{P})^{\times} \cong (A/\mathfrak{q})^{\times}$ is L . Hence ℓ is surjective by the Chinese Remainder Theorem and $\ker(\ell)$ consists of the elements of $F_{\mathfrak{q}}^{\times}$ which have order divisible by L at all primes above \mathfrak{q} . Then the lemma follows from the surjectivity of r and $\ker(\ell) = \ker(r)$. ■

For $\mathfrak{q} \in S$ we will also write $\varphi_{\mathfrak{q}}$ for the induced homomorphism

$$\varphi_{\mathfrak{q}}: \{y \in F^{\times}/(F^{\times})^L : [y]_{\mathfrak{q}} = 0\} \longrightarrow J_{\mathfrak{q}}/LJ_{\mathfrak{q}}.$$

LEMMA 3.7: *Suppose $\mathfrak{s} \in S$ with $\mathfrak{s} \neq \mathfrak{e}$ and $\mathfrak{q} \in \mathbf{P}_{\infty}$. Then*

$$[\kappa_{\mathfrak{s}}]_{\mathfrak{q}} = \begin{cases} 0 & \text{if } (\mathfrak{q}, \mathfrak{s}) = 1, \\ \varphi_{\mathfrak{q}}(\kappa_{\mathfrak{s}/\mathfrak{q}}) & \text{if } \mathfrak{q}|\mathfrak{s}. \end{cases}$$

Proof: By Lemma 3.5, $\kappa_{\mathfrak{s}} = D_{\mathfrak{s}}(\theta(\mathfrak{s}))/\beta_{\mathfrak{s}}^L$.

(i) If $(\mathfrak{q}, \mathfrak{s}) = 1$, all primes above \mathfrak{q} are unramified in $F_{\mathfrak{s}}/F$. So $[\kappa_{\mathfrak{s}}]_{\mathfrak{q}} = 0$ by AX 1.

(ii) If $\mathfrak{q}|\mathfrak{s}$, write $\mathfrak{s} = \mathfrak{q}\mathfrak{t}$ and $\kappa_{\mathfrak{t}} = D_{\mathfrak{t}}(\theta(\mathfrak{t}))/\beta_{\mathfrak{t}}^L$ with $\beta_{\mathfrak{t}} \in F_{\mathfrak{t}}^{\times}$. Then

$$(\sigma - 1)\beta_{\mathfrak{s}} = [(\sigma - 1)D_{\mathfrak{s}}(\theta(\mathfrak{s}))]^{1/L}$$

for all $\sigma \in G_{\mathfrak{s}}$ and

$$(\sigma' - 1)\beta_{\mathfrak{t}} = [(\sigma' - 1)D_{\mathfrak{t}}(\theta(\mathfrak{t}))]^{1/L}$$

for all $\sigma' \in G_{\mathfrak{t}}$. By (i), one can also assume that $\beta_{\mathfrak{t}}$ is prime to \mathfrak{q} . Since $(\beta_{\mathfrak{s}}^L) = (\kappa_{\mathfrak{s}}^{-1})$ as a fractional ideal in $F_{\mathfrak{s}}$ and all primes above \mathfrak{q} are unramified in $F_{\mathfrak{s}}/F_{\mathfrak{q}}$, there is a $\gamma \in F_{\mathfrak{q}}$ such that $\beta_{\mathfrak{s}}\gamma$ is a unit at all primes above \mathfrak{q} . So $[N_{\mathfrak{q}}\gamma]_{\mathfrak{q}} = [\kappa_{\mathfrak{s}}]_{\mathfrak{q}}$. Consider

$$\begin{aligned} (1 - \sigma_{\mathfrak{q}})\gamma &\equiv (\sigma_{\mathfrak{q}} - 1)\beta_{\mathfrak{s}} = [(\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{s}}(\theta(\mathfrak{s}))]^{1/L} \\ &= [(L - N_{\mathfrak{q}})D_{\mathfrak{t}}(\theta(\mathfrak{s}))]^{1/L} \\ &= D_{\mathfrak{t}}(\theta(\mathfrak{s}))/[N_{\mathfrak{q}}D_{\mathfrak{t}}(\theta(\mathfrak{s}))]^{1/L} \\ &= D_{\mathfrak{t}}(\theta(\mathfrak{s}))/[D_{\mathfrak{t}}(\text{Fr}_{\mathfrak{q}} - 1)(\theta(\mathfrak{t}))]^{1/L} \quad (\text{by AX 2}) \\ &\equiv [D_{\mathfrak{t}}(\theta(\mathfrak{t}))]^{\Phi(\mathfrak{q})/L}/(\text{Fr}_{\mathfrak{q}} - 1)\beta_{\mathfrak{t}} \quad (\text{by AX 3}) \\ &\equiv [D_{\mathfrak{t}}(\theta(\mathfrak{t}))]^{\Phi(\mathfrak{q})/L}/\beta_{\mathfrak{t}}^{\Phi(\mathfrak{q})} \\ &= (D_{\mathfrak{t}}(\theta(\mathfrak{t}))/\beta_{\mathfrak{t}}^L)^{\Phi(\mathfrak{q})/L} \end{aligned}$$

modulo any prime above \mathfrak{q} . The lemma now follows from Lemma 3.6. \blacksquare

By applying the Chebotarev Theorem, we can choose the desired $\mathfrak{s} \in S$. Letting C denote the l -part of $\text{Pic}(O_F)$, we have

PROPOSITION 3.8: *Let χ be a nontrivial irreducible \mathbb{Z}_l -representation of G and $C \in C$. Let W be a finite G -submodule of $(F^{\times}/(F^{\times})^L)(\chi)$, and*

$$\psi: W \longrightarrow (\mathbb{Z}/L\mathbb{Z})[G]$$

a G -equivariant map. Then there are infinitely many primes ϱ of F such that

- (i) $\varrho \in C$;
- (ii) $\mathfrak{q} \in S$, where $\mathfrak{q} = \varrho \cap A$;
- (iii) $[w]_{\mathfrak{q}} = 0$ for all $w \in W$, and there is a $u \in (\mathbb{Z}/L\mathbb{Z})^{\times}$ such that $\varphi_{\mathfrak{q}}(w) = u\psi(w)\varrho$ for all $w \in W$.

Proof: Suppose E is the maximal unramified abelian l -extension of F in which all infinite primes of F split completely. Then C is identified with $\text{Gal}(E/F)$ by the Artin map. Let $F' = \mathbb{F}_{q^{\mu}}F$ be a constant field extension of F with $L \mid (q^{\mu} - 1)$ and $\tilde{F} = F'(a_1^{1/L}, \dots, a_h^{1/L})$. Write τ for the Frobenius generator of $\text{Gal}(F'/F) \cong \text{Gal}(\mathbb{F}_{q^{\mu}}/\mathbb{F}_{\infty})$.

Step (1): $E \cap \tilde{F}(W^{1/L}) = F$

Since all infinite primes of F split completely in E/F , the constant field of E is the same as that of F . This implies that $F' \cap E = F$. Since

$\tilde{F}(W^{1/L})/F'$ is a Kummer extension, the action of τ on $\text{Gal}(\tilde{F}(W^{1/L})/F')$ is the q^{d_∞} -th power mapping. On the other hand, τ acts on $\text{Gal}(EF'/F')$ trivially. Thus $EF' \cap \tilde{F}(W^{1/L}) = F'$ since $(L, q^{d_\infty} - 1) = 1$. Hence $E \cap \tilde{F}(W^{1/L}) = F$ as desired.

Step (2): $(F^\times/(F^\times)^L)(\chi) \subseteq \tilde{F}^\times/(\tilde{F}^\times)^L$

If $a \in F^\times$ with $a = b^L$ for some $b \in F'^\times$, then there is $\varepsilon \in \mathbb{F}_{q^\mu}^\times$ such that $\tau(b) = \varepsilon b$. Let δ be a generator of $\mathbb{F}_{q^\mu}^\times$. Then $\varepsilon^{-1} = \delta^m$ for some integer m . Since $\varepsilon^L = 1$ and $(L, q^{d_\infty} - 1) = 1$, one has $(q^\mu - 1) | mL$ and $(q^{d_\infty} - 1) | m$. By the Chinese Remainder Theorem, there is an integer x such that

$$Lx \equiv 0 \pmod{q^\mu - 1} \quad \text{and} \quad (q^{d_\infty} - 1)x \equiv m \pmod{q^\mu - 1}.$$

Thus

$$\delta^x b \in F^\times \quad \text{and} \quad a = b^L = (\delta^x b)^L \in (F^\times)^L.$$

It follows that $F^\times/(F^\times)^L \subseteq F'^\times/(F'^\times)^L$.

Furthermore, take $e \in (F^\times/(F^\times)^L)(\chi)$ with $e \in (\tilde{F}^\times)^L$. Then e is in the group generated by a_1, \dots, a_h in $F'^\times/(F'^\times)^L$ by Kummer theory. So there are some rational integers c_1, \dots, c_h and $f \in F'^\times$ such that $e = a_1^{c_1} \cdots a_h^{c_h} f^L$. Since $F^\times/(F^\times)^L \subseteq F'^\times/(F'^\times)^L$, one can choose $f \in F^\times$. Because a_1, \dots, a_h are in k^\times and χ is nontrivial, the χ -component of the group generated by a_1, \dots, a_h in $F^\times/(F^\times)^L$ is trivial. It follows that $(F^\times/(F^\times)^L)(\chi) \subseteq \tilde{F}^\times/(\tilde{F}^\times)^L$.

Step (3): Construction of ϱ

By Kummer theory and Step (2), $\text{Gal}(\tilde{F}(W^{1/L})/\tilde{F}) \cong \text{Hom}(W, \mathbb{F}_{q^\mu}^\times)$. Fix a primitive L -th root of unity ζ_L and define a map $\iota: (\mathbb{Z}/L\mathbb{Z})[G] \rightarrow \mathbb{F}_{q^\mu}^\times$ by $\iota(1_G) = \zeta_L$ and $\iota(g) = 1$ for $g \in G$, $g \neq 1_G$. Then $\iota\psi \in \text{Hom}(W, \mathbb{F}_{q^\mu}^\times)$ and there is a $\gamma \in \text{Gal}(\tilde{F}(W^{1/L})/\tilde{F})$ such that $\iota\psi(w) = \gamma(w^{1/L})/w^{1/L}$ for all $w \in W$.

Choose $\tau \in \text{Gal}(E\tilde{F}(W^{1/L})/F)$ such that τ restricts to γ on $\tilde{F}(W^{1/L})$ and to the Artin symbol of \mathcal{C} on E . By the Chebotarev Theorem (see [17, p. 289, Theorem 12; p. 104, Corollary 2]), there are infinitely many degree one primes ϱ of F which are unramified in $E\tilde{F}(W^{1/L})/k$, and whose Frobenius class is the conjugacy class of τ . We will verify that ϱ satisfies (i)–(iii).

(i) follows from the Artin map.

Write $\mathfrak{q} = \varrho \cap A$. Then ϱ splits completely in \tilde{F} since τ is trivial on \tilde{F} . As ϱ has degree one and \mathfrak{q} is unramified, \mathfrak{q} splits completely in F/k , $k(a_1^{1/L}, \dots, a_h^{1/L})/k$ and $\mathbb{F}_{q^\mu}k/k$. Hence $\mathfrak{q} \in S$ and (ii) follows.

Since ϱ is unramified in $\tilde{F}(W^{1/L})/F$, $[w]_{\mathfrak{q}} = 0$ for all $w \in W$. By Lemma 3.6, $\text{ord}_{\varrho}(\varphi_{\mathfrak{q}}(w)) = 0$ if and only if w is an L -th power modulo ϱ .

On the other hand, since \mathfrak{q} splits completely in F/k ,

$$\text{ord}_{\varrho}(\psi(w)\varrho) = 0 \Leftrightarrow \iota\psi(w) = 1 \Leftrightarrow \gamma(w^{1/L}) = w^{1/L}.$$

By a simple computation,

$$\gamma(w^{1/L}) = w^{1/L} \Leftrightarrow \sigma\gamma\sigma^{-1}(w^{1/L}) = w^{1/L} \quad \forall \sigma \in \text{Gal}(\tilde{F}(W^{1/L})/F)$$

which is equivalent to w being an L -th power modulo ϱ . It follows that there is $u \in (\mathbb{Z}/L\mathbb{Z})^\times$ such that

$$\text{ord}_{\varrho}(\varphi_{\mathfrak{q}}(w)) = u(\text{ord}_{\varrho}(\psi(w)\varrho)) \quad \forall w \in W.$$

This proves (iii) since G acts on all primes above \mathfrak{q} transitively. ■

The following main result follows from the same arguments as those in [2, Theorem 4.3]. We repeat them for completeness.

THEOREM 3.9: *Let C be the l -part of $\text{Pic}(O_F)$. Then*

$$\sharp C(\chi) = \sharp(O_F^\times/\mathcal{E}_F)(\chi)$$

for every nontrivial irreducible \mathbb{Z}_l -representation χ of G .

Proof: Put $L = l^\sharp(O_F^\times/\mathcal{E}_F)(\chi)\sharp C(\chi)$. Since $(O_F^\times/(O_F^\times)^L)(\chi)$ is a cyclic $e(\chi)\mathbb{Z}_l[G]$ -module by Lemma 2.1 and $e(\chi)\mathbb{Z}_l[G]$ is isomorphic to the ring of integers of the unramified extension of \mathbb{Q}_l of degree $\dim(\chi)$, there is a divisor t of L such that

$$(O_F^\times/\mathcal{E}_F)(\chi) \cong e(\chi)(\mathbb{Z}/t\mathbb{Z})[G]$$

with $\sharp(O_F^\times/\mathcal{E}_F)(\chi) = t^{\dim(\chi)}$. Suppose η is a generator of $(O_F^\times/(O_F^\times)^L)(\chi)$ as an $e(\chi)\mathbb{Z}_l[G]$ -module, η has order L and $\eta^t \in (\mathcal{E}_F/(O_F^\times)^L)(\chi)$. Then there is an Euler system starting from η^t by Theorem 3.3. From now on we fix such an Euler system.

By induction, suppose $\mathcal{C}_1, \dots, \mathcal{C}_i$ are elements in $C(\chi)$ and one has chosen $\varrho_1, \dots, \varrho_i$ such that the class of ϱ_j in $C(\chi)$ is \mathcal{C}_j and $\mathfrak{q}_j = \varrho_j \cap A \in S$ for $1 \leq j \leq i$.

Writing $\mathfrak{s}_i = \prod_{j \leq i} \mathfrak{q}_j$ ($\mathfrak{s}_0 = \mathfrak{e}$) we have $\kappa_{\mathfrak{s}_i}$ by Lemma 3.5. Let m_i be the order of $e(\chi)\kappa_{\mathfrak{s}_i}$ in $F^\times/(F^\times)^L$, $t_i = L/m_i$ and W be the G -module generated by $e(\chi)\kappa_{\mathfrak{s}_i}$ in $(F^\times/(F^\times)^L)(\chi)$. Define a G -equivariant map $\psi: W \rightarrow (\mathbb{Z}/L\mathbb{Z})[G]$ by $\psi(e(\chi)\kappa_{\mathfrak{s}_i}) = t_i e(\chi)$ and choose $\mathcal{C}_{i+1} \in C(\chi) - \langle \mathcal{C}_1, \dots, \mathcal{C}_i \rangle$. By Proposition 3.8, one has a prime ϱ_{i+1} of F such that the class of ϱ_{i+1} in $C(\chi)$ is \mathcal{C}_{i+1} , $\mathfrak{q}_{i+1} = \varrho_{i+1} \cap A \in S$ and there is $u \in (\mathbb{Z}/L\mathbb{Z})^\times$ satisfying $\varphi_{\mathfrak{q}_{i+1}}(e(\chi)\kappa_{\mathfrak{s}_i}) = ut_i e(\chi)\varrho_{i+1}$.

Writing $\mathfrak{s}_{i+1} = \mathfrak{s}_i \mathfrak{q}_{i+1}$ we obtain $\kappa_{\mathfrak{s}_{i+1}}$ by Lemma 3.5. Let m_{i+1} be the order of $e(\chi)\kappa_{\mathfrak{s}_{i+1}}$ in $F^\times / (F^\times)^L$ and $t_{i+1} = L/m_{i+1}$. Then $e(\chi)\kappa_{\mathfrak{s}_{i+1}} = f^{t_{i+1}}$ for some $f \in F^\times$. By Lemma 3.7,

$$[e(\chi)\kappa_{\mathfrak{s}_{i+1}}] = \varphi_{\mathfrak{q}_{i+1}}(e(\chi)\kappa_{\mathfrak{s}_i}) + \sum_{j \leq i} [e(\chi)\kappa_{\mathfrak{s}_{i+1}}]_{\mathfrak{q}_j} \equiv ut_i e(\chi)\varrho_{i+1}$$

in $J/(LJ, J_{\mathfrak{q}_1}, \dots, J_{\mathfrak{q}_i})$. So $t_{i+1}|t_i$ and $t_{i+1}|t_0$ by induction. Since $\kappa_{\mathfrak{s}_0} = \kappa_\epsilon = \eta^t$ one has $t_0 = t$ and $(L/t_{i+1})C(\chi) = 0$. Now in $J/((L/t_{i+1})J, J_{\mathfrak{q}_1}, \dots, J_{\mathfrak{q}_i})$ one has

$$[f] \equiv u(t_i/t_{i+1})e(\chi)\varrho_{i+1}.$$

This implies that

$$(t_i/t_{i+1})\mathcal{C}_{i+1} \equiv 0$$

in $C(\chi)/\langle \mathcal{C}_1, \dots, \mathcal{C}_i \rangle$.

Continue this process until we obtain a set $\{\mathcal{C}_1, \dots, \mathcal{C}_k\}$ which generates $C(\chi)$ as an $e(\chi)\mathbb{Z}_l[G]$ -module. Then

$$[\langle \mathcal{C}_1, \dots, \mathcal{C}_{i+1} \rangle : \langle \mathcal{C}_1, \dots, \mathcal{C}_i \rangle] (t_i/t_{i+1})^{\dim(\chi)}$$

for $i = 0, 1, \dots, k-1$ and therefore

$$\#C(\chi) \prod_{i=1}^k (t_{i-1}/t_i)^{\dim(\chi)} = (t_0/t_k)^{\dim(\chi)}.$$

Thus

$$\#C(\chi)|t_0^{\dim(\chi)} = \#(O_F^\times/\mathcal{E}_F)(\chi).$$

The result follows from Theorem 2.4. \blacksquare

ACKNOWLEDGEMENT: We would like to thank the referee for pointing out several misprints and flaws in the original version of this paper. The work is partially supported by the Doctor Program Foundation of Higher Education of China.

References

- [1] G. W. Anderson, *A double complex for computing the sign-cohomology of the universal ordinary distribution*, Contemporary Mathematics **224** (1999), 1–27.
- [2] K. Feng and F. Xu, *Kolyvagin's "Euler Systems" in cyclotomic function fields*, Journal of Number Theory **57** (1996), 114–121.

- [3] D. Hayes, *Explicit class field theory in global function fields*, Studies in Algebra and Number Theory, Advances in Mathematics Supplementary Studies **6** (1979), 173–271.
- [4] D. Hayes, *Elliptic units in function fields*, in *Proceeding of a Conference Related to Fermat's Last Theorem* (D. Goldfeld, ed.), Birkhäuser, Boston, 1982, pp. 321–341.
- [5] D. Hayes, *Stickelberger elements in function fields*, *Compositio Mathematica* **55** (1985), 209–239.
- [6] D. Hayes, *A brief introduction to Drinfeld modules*, in *The Arithmetic of Function Fields* (D. Goss, D. Hayes and M. Rosen, eds.), Proceedings of a Workshop at the Ohio State University, de Gruyter, Berlin, 1991, pp. 1–32.
- [7] V. Kolyvagin, *Euler system*, in *Grothendieck Festschrift*, Vol. 2, Progress in Mathematics **87** (1990), 435–483.
- [8] H. Oukhaba, *Elliptic units in global function fields*, in *The Arithmetic of Function Fields* (D. Goss, D. Hayes and M. Rosen, eds.), Proceedings of a Workshop at the Ohio State University, de Gruyter, Berlin, 1991, pp. 87–102.
- [9] H. Oukhaba, *Groups of elliptic units and torsion points of Drinfeld modules*, in *Proceedings of the Workshop on Drinfeld Modules, Modular Schemes and Applications* (E.-U. Gekeler, M. van der Put, M. Reversat and J. Van Geel, eds.), World Science Publications, River Edge, NJ, 1997, pp. 298–310.
- [10] K. Rubin, *The Main Conjecture*, Appendix to *Cyclotomic Fields*, by S. Lang, GTM 121, Springer-Verlag, Berlin, 1990, pp. 397–419.
- [11] K. Rubin, *The “Main Conjecture” of Iwasawa theory for imaginary quadratic fields*, *Inventiones Mathematicae* **103** (1991), 2–68.
- [12] K. Rubin, *Kolyvagin's system of Gauss sums*, *Progress in Mathematics* **89** (1991), 309–324.
- [13] K. Rubin, *Stark units and Kolyvagin's “Euler Systems”*, *Journal für die reine und angewandte Mathematik* **425** (1992), 141–154.
- [14] K. Rubin, *On “Main Conjecture” of Iwasawa theory for imaginary quadratic fields*, CRM Proceedings and Lecture Notes **4** (1994), 23–28.
- [15] L. Shu, *Class number formulas over global function fields*, *Journal of Number Theory* **48** (1994), 133–161.
- [16] J. Tate, *Les conjectures de Stark sur les fonctions d'Artin en $s = 0$* , *Progress in Mathematics* **47**, Birkhäuser, Boston, 1984.
- [17] A. Weil, *Basic Number Theory*, Grundlehren der Mathematischen Wissenschaften 144, Springer, Berlin, 1974.
- [18] L. Yin, *On the index of cyclotomic units in characteristic p and its applications*, *Journal of Number Theory* **63** (1997), 302–324.