

# Index-class number formulas over global function fields

LINSHENG YIN\*

*Department of Mathematical Sciences, University of Tokyo, Tokyo 153, Japan*

*Current address: Dept. of Mathematics, Zhongshan University, Guangzhon 510275, P.R. China*

Received 8 August 1995; accepted in final form 13 May 1996

**Abstract.** In classical number theory, one has the famous theorem of Kummer–Sinnott giving the index of the cyclotomic units in the total unit group. Using the division values of sgn-normalized rank one Drinfeld modules, we construct the group of extended cyclotomic units for an abelian extension of a global function field and calculate its index in the whole unit group. The result could be regarded as an analogue and a generalization of Kummer–Sinnott’s.

**Key words:** sgn-normalized rank one Drinfeld modules, extended cyclotomic units, index-class number formula

## 0. Introduction

In the classical theory of numbers, one has the famous index-class number formula of Kummer–Sinnott [12], which says that in a cyclotomic number field the index of the cyclotomic units in the total unit group is equal to the class number of its maximal real subfield, up to a trivial factor. Galovich and Rosen [2] proved an analogue of this result for the rational function field over a finite field. In this paper, we extend this theory to an arbitrary global function field over a finite field. Our method is a generalization of that in [12] or [2]. The new ingredient is that the base field has non-trivial class group. Now we state our results more precisely.

Let  $k$  be the function field of a projective smooth curve over the finite field  $\mathbb{F}_q$  with  $q$  elements. Let  $\infty$  be a closed point in the curve with degree 1 and let  $k_\infty$  be the completion of  $k$  at  $\infty$ . Let  $\mathbb{A}$  be the Dedekind subring of  $k$  consisting of those functions having no pole other than  $\infty$  and let  $H_\infty$  be the Hilbert class field of  $(k, \infty)$ . For a ring  $R$ , let  $R^*$  denote the group of invertible elements. We fix, once for all, a sign function  $\text{sgn}: k_\infty^* \rightarrow \mathbb{F}_q^*$  (Def. 4.1, [7]). For a proper ideal  $\mathfrak{m}$  of  $\mathbb{A}$ , we denote  $K = K_\mathfrak{m}$  to be the ‘cyclotomic’ extension of the triple  $(k, \infty, \text{sgn})$  with conductor  $\mathfrak{m}$ , which arises in the theory of Drinfeld modules, and we set  $H = H_\mathfrak{m}$  to be the maximal real subfield of  $K$  such that  $\infty$  splits completely, which is the ray class field of  $(k, \infty)$  modulo  $\mathfrak{m}$  (Sect. 16, [8]). Let  $G_1 = \text{Gal}(H_\infty/k) \simeq \text{Pic}(\mathbb{A})$ . Let  $N = N_\mathfrak{m}$  denote the subgroup of  $G_1$  generated by the Artin symbols  $\tau_\mathfrak{p} = (\mathfrak{p}, H_\infty/k)$  for all primes  $\mathfrak{p} \mid \mathfrak{m}$ , and let  $e = [G_1 : N]$  be

\* The author was supported in part by Hitachi High-Soft Fellowship.

the index. Let  $C = C_m$  denote the cyclotomic unit group of  $K$  (Def. 1.1). We first obtain the rank of  $C$ .

**THEOREM A.**  $\text{rank } C = [H:k] - e$ .

This theorem answers a conjecture by D. Goss (2.7 Conjecture, [3]). Shu also proved the theorem in the case when the conductor  $m$  is a prime by a different method ([11], Thm. 5.2). Thus  $C$  does not have the maximal rank in the whole unit group of  $K$  unless  $m$  satisfies  $N_m = G_1$ . The reason is a shortage of unramified units in  $C$ . We extend  $C$  in a natural way to get the extended group  $\overline{C}$  of cyclotomic units with the maximal rank (Def. 1.6). We have  $C = \overline{C}$  if  $N_m = G_1$ . Our next theorem gives the index of  $\overline{C}$ . For any finite extension  $E/k$ , we denote by  $O_E$  the integral closure of  $\mathbb{A}$  in  $E$ ,  $O_E^*$  the unit group of  $O_E$ ,  $h(O_E)$  the ideal class number of  $E$ ,  $h(E)$  the divisor class number of  $E$  and  $R(E)$  the regulator of  $E$ . We abbreviate  $h = h(\mathbb{A}) = h(k)$ . Let  $s$  be the number of distinct prime divisors of  $m$ .

**THEOREM B.** *If  $s \geq 3$ , we assume  $(h, q-1) = 1$ . Then*

$$[O_K^* : \overline{C}] = (q-1)^a h(O_H),$$

where  $a = 0$  if  $s = 1$  and  $a = e(2^{s-2} - 1) - (s-2)$  if  $s > 1$ .

We conjecture that the restrictive hypothesis in Theorem B is unnecessary (see Sect. 6 for detail). When  $k = \mathbb{F}_q(T)$  and  $\infty = 1/T$ , then  $e = h = 1$ . The theorem gives Galovich and Rosen's formula (Thm., [2]). We mention that the elliptic units defined by Oukhaba (Def. 3.9, [9]) and by Hayes (Def. 1.3, [6]) are essentially our extended cyclotomic units. One part of Oukhaba's results (the part two in (Thm. 1, [9])) is a special case of  $s = 1$  in our Theorem B. Shu studied the cyclotomic units in the case when the conductor  $m$  is a prime ideal. She extended  $C$  in another way, and got an index formula which also includes the class number of a subfield of  $H_\infty$  (Main Thm. 2, [11]). In this paper, we also give a new method to compute an index appearing in the calculation of  $[O_K^* : \overline{C}]$ , which is much simpler than Galovich and Rosen's and Sinnott's when applying it to their cases.

## 1. Cyclotomic units and class number formula

In this section, we give the definitions of cyclotomic units and unramified elliptic units and recall their basic properties. We also recall the relation of them with the values for Artin  $L$ -function at zero. The main references for this section are Hayes' (Sect. 1, [6]), [7] and (Sect. 16, [8]) except for the definition of the extended group of cyclotomic units.

The notations are as above. A rank one Drinfeld  $\mathbb{A}$ -module  $\rho$  (of generic characteristic) is called *sgn-normalized* if  $\rho_x$  has all of its coefficients in  $H_\infty$  for all  $x \in \mathbb{A}$  and the coefficient of the highest order term of  $\rho_x$  is equal to  $\text{sgn}(x)$ . There is a

unique sgn-normalized rank one Drinfeld  $\mathbb{A}$ -module in each isomorphism class of rank one  $\mathbb{A}$ -modules (Thm. 2.3, [8]). Let  $X$  denote the set of these normalized  $\mathbb{A}$ -modules. Let  $\Omega$  be the completion of an algebraic closure of  $k_\infty$ . For  $\rho \in X$ , let  $\Lambda_m^\rho$  be the set of  $m$ -torsion points in  $\Omega$  associated to  $\rho$ , i.e.,  $\Lambda_m^\rho = \{\alpha \in \Omega \mid \rho_x(\alpha) = 0, x \in m\}$ , which is isomorphic to  $\mathbb{A}/m$  as an  $\mathbb{A}$ -submodule via  $\rho$  of  $\Omega$  (Sect. 16, [8]). Let  $\Lambda_m = \bigcup_{\rho \in X} \Lambda_m^\rho$ . Then  $K = H_\infty(\Lambda_m^\rho) = H_\infty(\Lambda_m)$  is abelian over  $k$  and is called the cyclotomic extension of  $k$  with conductor  $m$ .

**DEFINITION 1.1.** Let  $P = P_m$  be the subgroup of  $K^*$  generated by  $\Lambda_m^* = \Lambda_m - \{0\}$  and by  $\mathbb{F}_q^*$ . Let  $C = C_m = P \cap O_K^*$ . Call an element in  $P$  (resp. in  $C$ ) a cyclotomic number (resp. a cyclotomic unit) of  $K$ .

Let  $G = \text{Gal}(K/k)$ . Since  $X$  is stable under the natural  $G$ -action,  $P$  and  $C$  are  $G$ -modules. Let  $\xi(m) \in \Omega$  be an invariant associated to the ideal  $m$ , which is characterized by the condition that the lattice ( $\mathbb{A}$ -submodule of  $\Omega$ )  $\xi(m)m$  corresponds to some  $\rho \in X$ . Thus  $\xi(m)$  is determined up to multiplication by  $\mathbb{F}_q^*$ . However, by Hayes' technique (Sect. 1, [6]) the ratio  $\xi(a)/\xi(b)$  for any fractional ideals  $a$  and  $b$  is determined uniquely, and by (P1, [6]) it is in  $H_\infty$ . Let  $e_m(x)$  be the exponential function associated to the lattice  $m$ . We have (Eqs. 5.4 and 5.5, [7]),  $\Lambda_m^\rho = \xi(m)e_m(\mathbb{A})$  and  $\lambda_m = \xi(m)e_m(1)$  is a generator of  $\Lambda_m^\rho$ . For a proper ideal  $f$  of  $\mathbb{A}$ , we set  $\lambda_f = \xi(f)e_f(1)$  and  $K_f = H_\infty(\Lambda_f)$ . Notice that  $\text{Gal}(K_f/H_\infty) \simeq (\mathbb{A}/f)^*$ . We regard  $\text{Gal}(K_f/k)$  as a quotient of  $G$  for  $f \mid m$ . By (Thm. 16.2, [8]), the  $G$ -conjugates of  $\lambda_f$  contain all generators of  $\Lambda_f^\rho$  for any  $\rho \in X$ . Let  $\epsilon$  denote the unit ideal. Thus we get

**LEMMA 1.2.** *As a  $G$ -module,  $P$  is generated by  $\mathbb{F}_q^*$  and by  $\lambda_f$  with  $f \mid m, f \neq \epsilon$ .*

Hayes studied the properties of the cyclotomic numbers and the invariants  $\xi(m)$ . In the following lemma, (1)–(2) are from (Thm. 4.17, [7]) and (3)–(4) from (Sect. 1 and Eq. 2.3, [6]).

**LEMMA 1.3.** *Let  $\lambda$  be a generator of  $\Lambda_m^\rho$  for  $\rho \in X$  and let  $\mathfrak{p}$  be a prime ideal of  $\mathbb{A}$ .*

- (1) *Assume  $m$  has at least two distinct prime divisors. Then  $\lambda$  is a unit.*
- (2) *Assume  $m = \mathfrak{p}^n$ . Let  $[\mathfrak{p}]$  be the product in  $O_K$  of the prime ideals dividing  $\mathfrak{p}$ . Then  $[\mathfrak{p}] = \lambda O_K$ .*
- (3)  *$N_{K_\mathfrak{p}/H_\infty}(\lambda_\mathfrak{p}) = \xi(\mathbb{A})/\xi(\mathfrak{p})$ , and it generates the ideal  $\mathfrak{p}O_{H_\infty}$  in  $O_{H_\infty}$ .*
- (4) *Let  $\mathfrak{a}, \mathfrak{b}$  be fractional ideals of  $\mathbb{A}$ . The Galois action is*

$$(\xi(\mathbb{A})/\xi(\mathfrak{a}))^{\tau_\mathfrak{b}} = \xi(\mathfrak{b}^{-1})/\xi(\mathfrak{a}\mathfrak{b}^{-1}),$$

where  $\tau_\mathfrak{b} = (\mathfrak{b}, H_\infty/k)$  is the Artin symbol.

We now recall the unramified elliptic units introduced by D. Hayes [6].

DEFINITION 1.4. Let  $Q_m$  be the  $G_1$ -submodule of  $H_\infty$  generated by  $\xi(\mathbb{A})/\xi(\mathfrak{p})$  with primes  $\mathfrak{p} \mid m$  and let  $E_m = Q_m \cap O_{H_\infty}^*$ . Call an element in  $Q_m$  (resp. in  $E_m$ ) an elliptic number (resp. an elliptic unit) of level  $m$ .

We remark that the definition of  $Q_m$  above is slightly different from Hayes'  $Q_{N_m}$  (Def. 1.3, [6]), but  $E_m$  is the same as his  $E_{N_m}$ . An element  $z \in k_\infty$  is called positive if  $\text{sgn } z = 1$  and  $z \in H_m$  is called totally positive if  $z^\sigma$  is positive for any  $\sigma \in G^+ = \text{Gal}(H_m/k)$ . By (Prop. 2.3, [6]),  $N_{K/H}(P) \cap Q_m$  consists of totally positive elements. Let  $M$  denote the set of positive elements in  $k$ . In Hayes' definition, the group of elliptic numbers of any level contains  $M$  as a subgroup. In our case, we have

LEMMA 1.5.  $Q_m \cap k = \{x \in M \mid \text{ord}_\mathfrak{p}(x) = 0 \text{ for } \mathfrak{p} \nmid m\}$ .

*Proof.* By Lemma 1.3(3), one sees the ' $\subseteq$ ' in the lemma. Now we show the ' $\supseteq$ '. Using the Galois action (Lemma 1.3(4)), we see that  $\xi(\mathfrak{a})/\xi(\mathfrak{b}) \in Q_m$  if  $\mathfrak{a}\mathfrak{b}^{-1} = \prod_{\mathfrak{p}_i \mid m} \mathfrak{p}_i^{e_i}$  by induction on  $\sum_i |e_i|$ . Thus by (Eq. 1.6, [6]), we have  $x = \xi(\mathbb{A})/\xi(x\mathbb{A}) \in Q_m$  if  $x \in M$  and if  $\text{ord}_\mathfrak{p}(x) = 0$  for  $\mathfrak{p} \nmid m$ . This completes the proof.  $\square$

When  $m$  satisfies  $N_m = G_1$ , we see that  $MQ_m$  is independent of such  $m$  by Lemma 1.5. Let  $Q = MQ_m$  and  $E = Q \cap O_{H_\infty}^*$  in this case. By (Prop. 3.7, [6]), each elliptic unit is a  $q - 1$ st power in  $H_\infty$ . We denote the group of  $q - 1$ st roots of the elements in  $E_m$  by  $\overline{E}_m$ , and write  $\overline{E} = E^{1/(q-1)}$ .

Let  $J = \text{Gal}(K/H) \simeq \mathbb{F}_q^*$ , which is both the decomposition group and the inertia subgroup at  $\infty$ . Let  $s(J) = \sum_{\sigma \in J} \sigma$ . Since  $J \subset \text{Gal}(K_\mathfrak{p}/H_\infty)$ , we have, by Lemma 1.3(3),

$$Q_m \subset P_m^{s(J)} \quad \text{and} \quad \overline{E}_m \subset C_m. \quad (1.1)$$

The second is deduced from the first and the fact  $\mathbb{F}_q^* P_m^{s(J)} = \mathbb{F}_q^* P_m^{q-1}$  (see (Eq. 4.13, [7])). In Section 3 we will show that  $\overline{E}_m$  is the intersection of  $\overline{E}$  and  $C_m$  (Prop. 4.4).

The Theorem A (we will show it in the next section) implies that the cyclotomic unit group  $C$  does not have the maximal rank in  $O_K^*$  unless  $N_m = G_1$ . Proposition 4.4 below shows that  $C$  does not contain enough unramified units. To get a unit subgroup with the maximal rank in  $O_K^*$ , we naturally extend  $C$  by adding all unramified elliptic units.

DEFINITION 1.6. Let  $\overline{C} = C \cdot \overline{E}$ . Call  $\overline{C}$  the extended group of cyclotomic units of  $K$ .

We will see that  $\overline{C}$  does have the maximal rank in  $O_K^*$  next section (Prop. 2.1).

In the rest of this section, we recall the relation of the cyclotomic numbers with the values for Artin  $L$ -function at zero. Let  $\chi$  be a character of  $G$  with values in non-zero complex numbers  $\mathbb{C}^*$ . If  $\chi(J) = 1$ , it induces a character of  $G^+ = \text{Gal}(H/k) \simeq G/J$ , and we call it real. Let  $\mathfrak{f}_\chi$  be the conductor of  $\chi$ , which is an ideal of  $\mathbb{A}$ . Note  $\mathfrak{f}_\chi = \mathfrak{e}$  means that  $\chi$  induces a character of  $G_1$ . We always

denote by  $\chi$  its induced character. For a character  $\chi$  of  $G$  and an ideal  $\mathfrak{a}$  of  $\mathbb{A}$ , we define  $\chi(\mathfrak{a}) \in \mathbb{C}$  as follows. If  $(\mathfrak{a}, f_\chi) = \epsilon$ , let  $\sigma_{\mathfrak{a}}$  be the Artin  $k$ -automorphism of  $K_{f_\chi} = H_\infty(\Lambda_{f_\chi})$  corresponding to  $\mathfrak{a}$  and let  $\chi(\mathfrak{a}) = \chi(\sigma_{\mathfrak{a}})$ . If  $(\mathfrak{a}, f_\chi) \neq \epsilon$ , we put  $\chi(\mathfrak{a}) = 0$ .

From now on, we suppose that  $\chi$  is a non-trivial real character of  $G$ . Let  $L_k(s, \chi)$  be the Artin  $L$ -function associated to  $\chi$ , which is defined as the Euler products over the places of the field  $k$  where  $\chi$  is unramified. We have the well-known analytic class number formula

$$\prod_{\chi \neq 1, \text{real}} L_k(0, \chi) = \frac{h(H)}{h} \tag{1.2}$$

Let  $L_m(s, \chi)$  be the incomplete  $L$ -function of  $\chi$  relative to the prime divisors of  $m$  (Eq. 1.1, [7]). Let  $\alpha = \lambda_m^{s(J)} = -\lambda_m^{q-1} \in H^*$ . Hayes proved that, the last equality in [7],

$$\begin{aligned} L_m(0, \chi) &= \frac{1}{q-1} \sum_{\sigma \in G^+} \chi(\sigma) v_\infty(\alpha^\sigma) \\ &= \frac{1}{q-1} \sum_{\sigma \in G} \chi(\sigma) v_\infty(\lambda_m^\sigma), \end{aligned} \tag{1.3}$$

where  $v_\infty$  is the extension to  $\Omega$  of the normalized valuation of  $k_\infty$  at  $\infty$ . By the definitions we have the following formula which will be useful later

$$L_m(0, \chi) = \prod_{\mathfrak{p}|m} (1 - \chi(\mathfrak{p})) \cdot L_k(0, \chi). \tag{1.4}$$

## 2. The ranks

In this section, we compute the ranks of  $C$  and  $\overline{C}$  by using the logarithm map introduced below.

Let  $\widehat{G}$  denote the character group of  $G$ , and let  $\mathbb{C}[G]$  be the group ring of  $G$  over the complex number field  $\mathbb{C}$ . A character  $\chi \in \widehat{G}$  induces a ring homomorphism  $\mathbb{C}[G] \rightarrow \mathbb{C}$  in an obvious way. We denote it by the same symbol. Moreover these characters induce a natural isomorphism  $\mathbb{C}[G] \simeq \bigoplus_{\chi \in \widehat{G}} \mathbb{C}$ .

The logarithm map in function field case was first introduced by Galovich and Rosen [2] and was used by Hayes in [6]. It is an important device to study the cyclotomic units. We start this section by recalling its definition.

Let  $\mathbb{Q}[G]$  be the group ring of  $G$  over rational numbers  $\mathbb{Q}$ . The logarithm map  $l: K^* \rightarrow \mathbb{Q}[G]$  is defined for  $x \in K^*$  by

$$l(x) = \sum_{\sigma \in G} v_\infty(x^\sigma) \sigma^{-1}.$$

Clearly  $l$  is  $G$ -linear and  $\ker l \cap O_K^* = \mathbb{F}_q^*$ . We set  $l^* = (1 - e_1)l$ , where  $e_1 = (1/|G|) \sum_{\sigma \in G} \sigma^{-1}$  is the idempotent associated to the trivial character of  $G$ . Now we can show Theorem A.

*The Proof of Theorem A.* Let  $\mathfrak{m} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_s^{e_s}$  be the prime factorization and take prime ideal  $\mathfrak{R}_i$  of  $K$  lying above  $\mathfrak{p}_i$  for  $1 \leq i \leq s$ . By Lemma 1.3(1)–(2), there exists an exact sequence

$$0 \rightarrow C \rightarrow P \xrightarrow{v} \mathbb{Z}^s \rightarrow 0,$$

where  $v$  is the valuation map in  $K$ , i.e.,  $v(x) = (v_{\mathfrak{R}_1}(x), \dots, v_{\mathfrak{R}_s}(x))$  for  $x \in P$ . Again by Lemma 1.3(1)–(2), the action of  $G$  on  $P/C$  is trivial. We see that  $\mathbb{Q} \otimes l(C) \simeq \mathbb{Q} \otimes l^*(P)$ . Thus  $\text{rank } C = \dim_{\mathbb{C}} \mathbb{C} l^*(P)$ . Since  $\mathbb{C} l^*(P)$  is an ideal of  $\widehat{\mathbb{C}[G]}$ , we get

$$\text{rank } C = \#\{\chi \in \widehat{G} \mid \chi \neq 1, \chi(l(P)) \neq 0\},$$

where  $\#$  denotes the cardinality of a set. Since  $l(x) = l(x^\sigma) = \sigma l(x)$  for  $x \in P$  and  $\sigma \in J$ , when  $\chi$  is not real, we have  $\chi(l(P)) = 0$ . Now suppose that  $\chi$  is real. Let  $\mathfrak{f}$  be a divisor of  $\mathfrak{m}$  and  $\mathfrak{f} \neq \mathfrak{e}$ . If  $\mathfrak{f}_\chi \mid \mathfrak{f}$ , by (1.3) and (1.4), we have

$$\chi(l(\lambda_{\mathfrak{f}})) = a_{\mathfrak{f}} L_{\mathfrak{f}}(0, \bar{\chi}) = a_{\mathfrak{f}} \prod_{\mathfrak{p} \mid \mathfrak{f}} (1 - \bar{\chi}(\mathfrak{p})) \cdot L_k(0, \bar{\chi}) \tag{2.1}$$

where  $\bar{\chi}$  is the inverse of  $\chi$ , and  $a_{\mathfrak{f}} = (q - 1) \Phi(\mathfrak{m}) / \Phi(\mathfrak{f}) \neq 0$ . Here  $\Phi(\mathfrak{f}) = \#(\mathbb{A}/\mathfrak{f})^*$  denotes the Euler  $\Phi$ -function.

Hence if  $\chi$  is ramified, the  $\chi(l(\lambda_{\mathfrak{f}})) \neq 0$  for  $\mathfrak{f} = \mathfrak{f}_\chi$ . If  $\chi$  is unramified, then  $\chi(l(\lambda_{\mathfrak{f}})) \neq 0$  is equivalent to  $\chi(\mathfrak{p}) \neq 1$  for all  $\mathfrak{p} \mid \mathfrak{f}$ . Thus  $\{\chi \neq 1, \chi(l(P)) \neq 0\} = \widehat{G^+} - (\widehat{G_1/N})$ , which implies the theorem.  $\square$

Next we consider the rank of  $\overline{C}$ .

**PROPOSITION 2.1.**  $\text{rank } \overline{C} = [H : k] - 1$ .

*Proof.* By the proof of Theorem A, it is enough to show that  $\chi(l(Q)) \neq 0$  for real and unramified character  $\chi \neq 1$ . By Lemma 1.3(3), we have

$$\begin{aligned} \chi(l(\xi(\mathbb{A})/\xi(\mathfrak{p}))) &= \Phi(\mathfrak{p}) \chi(l(\lambda_{\mathfrak{p}})) = a_{\mathfrak{p}} \Phi(\mathfrak{p}) L_{\mathfrak{p}}(0, \bar{\chi}) \\ &= a_{\mathfrak{p}} \Phi(\mathfrak{p}) (1 - \bar{\chi}(\mathfrak{p})) L_k(0, \bar{\chi}) \end{aligned} \tag{2.2}$$

for unramified  $\chi$ . From the definition of  $Q$ , we conclude the proof.  $\square$

### 3. Outline of the proof of Theorem B

In this section, we explain an outline of the proof of Theorem B and calculate two simple indices appearing in the proof.

We first fix some notations. For a prime ideal  $\mathfrak{p}$  of  $\mathbb{A}$ , let  $T_{\mathfrak{p}}$  be the inertia group of  $\mathfrak{p}$  in  $G$  and let  $F_{\mathfrak{p}} \in G$  be any Frobenius automorphism for  $\mathfrak{p}$ , which is the well defined modulo  $T_{\mathfrak{p}}$ . For a subset  $B$  of  $G$ , write  $s(B) = \sum_{\sigma \in B} \sigma \in R = \mathbb{Z}[G]$ , the group ring of  $G$  over rational integers  $\mathbb{Z}$ . We set  $\bar{\sigma}_{\mathfrak{p}} = F_{\mathfrak{p}}^{-1}s(T_{\mathfrak{p}})/|T_{\mathfrak{p}}|$ . One can see that  $\chi(\bar{\sigma}_{\mathfrak{p}}) = \bar{\chi}(\mathfrak{p})$  for any  $\chi \in \hat{G}$ .

Let  $I_{\mathfrak{f}} = \text{Gal}(K/K_{\mathfrak{f}})$  for  $\mathfrak{f} | \mathfrak{m}$ ,  $\mathfrak{f} \neq \mathfrak{e}$  and let  $I_{\mathfrak{e}} = \text{Gal}(K/H_{\infty}) \simeq (\mathbb{A}/\mathfrak{m})^*$ . Let  $V$  be the  $R$ -submodule of  $\mathbb{Q}[G]$  generated by

$$\alpha_{\mathfrak{f}} = s(I_{\mathfrak{f}}) \prod_{\mathfrak{p} | \mathfrak{f}} (1 - \bar{\sigma}_{\mathfrak{p}})$$

with  $\mathfrak{f} | \mathfrak{m}$ ,  $\mathfrak{f} \neq \mathfrak{e}$ . We also set  $U = V + s(I_{\mathfrak{e}})R$  and  $U' = (q - 1)V + s(I_{\mathfrak{e}})R$ . Here  $U$  is the  $R$ -module generated by  $\alpha_{\mathfrak{f}}$  with all  $\mathfrak{f} | \mathfrak{m}$ .

For any  $R$ -module  $T$ , we denote by  $T_0$  the submodule of elements killed by  $s(G)$  and for a subset  $B$  of  $G$ , denote by  $T^B$  the set of elements of  $T$  fixed by  $B$ . It is easy to see  $V_0 = V$ ,  $U_0 = V + s(I_{\mathfrak{e}})R_0$  and  $U'_0 = (q - 1)V + s(I_{\mathfrak{e}})R_0$ .

Let  $e^+ = (1/(q - 1))s(J)$ . Clearly  $U, e^+V$  and  $e^+U$  are free abelian subgroups of  $\mathbb{Q}[G]$ . Since  $\chi(\bar{\sigma}_{\mathfrak{p}}) = \bar{\chi}(\mathfrak{p})$  for any  $\chi \in \hat{G}$ , using the method in the proof of Theorem A, one can calculate their ranks. We leave the proof of the following lemma to the reader.

LEMMA 3.1.

$$\begin{aligned} \text{rank } U &= \text{rank } U' = [K : k], \\ \text{rank } e^+U_0 &= \text{rank } e^+U'_0 = [H : k] - 1, \\ \text{rank } e^+V &= [H : k] - e. \end{aligned}$$

Let  $Y = (1 - e_1)e^+\mathbb{Q}[G]$ . It is a  $\mathbb{Q}$ -subspace of  $\mathbb{Q}[G]$  with dimension  $r = [H : k] - 1$ . A lattice in  $Y$  is a finitely generated subgroup of  $Y$  with the maximal rank. Let  $L$  and  $L'$  be two lattices in  $Y$ . Sinnott defined the index  $(L : L')$  in [12] and described some basic properties of the index (Lemmas 1.1 and 6.1, [12]). We will freely use these properties.

Obviously  $e^+R_0$  is a lattice in  $Y$  and by the Dirichlet unit theorem,  $l(O_K^*)$  is a lattice in  $Y$ . Previous lemma implies that  $e^+U_0$  and  $e^+U'_0$  are lattices in  $Y$ .

Let  $\mathfrak{m}'$  be a proper ideal of  $\mathbb{A}$  coprime to  $\mathfrak{m}$  such that  $N_{\mathfrak{m}\mathfrak{m}'} = G_1$ . By Lemma 1.3(3),  $E = Q_{\mathfrak{m}\mathfrak{m}'} \cap O_{H_{\infty}}^* = E_{\mathfrak{m}}E_{\mathfrak{m}'}$ . We put  $P' = \mathbb{F}_q^* P^{q-1} Q_{\mathfrak{m}'}$  and  $C' = P' \cap O_K^*$ . Then by (1.1) and Lemma 1.3(1-3)

$$C' = \mathbb{F}_q^* C^{q-1} E_{\mathfrak{m}'} = \mathbb{F}_q^* \bar{C}^{q-1}.$$

The proofs of Theorem A and Proposition 2.1 show that  $l^*(P')$  and  $l(C')$  are also lattices in  $Y$ . Since  $\ker l \cap O_K^* = \ker l \cap C' = \mathbb{F}_q^*$ , we have, by the equality above,

$$[O_K^* : \bar{C}] = (q - 1)^{-r} [O_K^* : C'] = (q - 1)^{-r} [l(O_K^*) : l(C')]$$

$$\begin{aligned}
 &= (q - 1)^{-r} (l(O_K^*): e^+ R_0) (e^+ R_0: e^+ U_0) (e^+ U_0: e^+ U_0') \\
 &\quad \times (e^+ U_0': l^*(P')) (l^*(P'): l(C')).
 \end{aligned}
 \tag{3.1}$$

To prove Theorem B, we need to calculate the five indices in the right-hand of (3.1). In the last three sections, we will prove the following three equalities respectively. (Notice that we need a restrictive hypothesis on the third equality. See Sect. 6 for detail.)

$$\begin{aligned}
 (e^+ U_0': l^*(P')) &= (q - 1)^r h(H)/h, \\
 (l^*(P'): l(C')) &= (q - 1)^{-s} \Phi(\mathfrak{m})h, \\
 (e^+ R_0: e^+ U_0) &= \begin{cases} (q - 1)^e / \Phi(\mathfrak{m}) & \text{if } s = 1, \\ (q - 1)^{e2^{s-2}} / \Phi(\mathfrak{m}) & \text{if } s > 1, \end{cases}
 \end{aligned}
 \tag{3.1a}$$

and in the rest of this section we compute the indices  $(l(O_K^*): e^+ R_0)$  and  $(e^+ U_0: e^+ U_0')$ .

By the definition of the regulator, we have  $R(K) = (e^+ R_0: l(O_K^*))$ . Let  $Q_0 = [O_K^*: O_H^*]$ . Using the argument of (Prop. 1.14, [2]), we see that  $Q_0 = 1$  if  $s = 1$  and  $Q_0 = q - 1$  if  $s > 1$ . Moreover by (Prop. 1.15, [2]), we have  $R(K) = ((q - 1)^r / Q_0) R(H)$ . Thus

$$(l(O_K^*): e^+ R_0) = 1/R(K) = Q_0 / (R(H)(q - 1)^r).
 \tag{3.1b}$$

To compute  $(e^+ U_0: e^+ U_0')$ , we need a lemma. Let  $J_N$  be the ideal of  $R_1 = \mathbb{Z}[G_1]$  generated by  $\{\tau - 1 \mid \tau \in N\}$ . We identify  $R_1$  with  $s(I_\epsilon)R$  by  $\tau \mapsto \sum_{\sigma \mapsto \tau} \sigma$ .

LEMMA 3.2.

$$e^+ V \cap s(I_\epsilon)R = (q - 1)e^+ V \cap s(I_\epsilon)R = J_N.$$

*Proof.* Since  $J \cap I_f = \{1\}$  and  $J I_f \subseteq I_\epsilon$  for  $f \mid m, f \neq \epsilon$ , we see

$$e^+ V \cap s(I_\epsilon)R \supseteq (q - 1)e^+ V \cap s(I_\epsilon)R \supseteq J_N.$$

On the other hand,

$$\begin{aligned}
 e^+ V \cap s(I_\epsilon)R &\subseteq \mathbb{Q}e^+ V \cap s(I_\epsilon)R = \mathbb{Q}s(I_\epsilon)V \cap s(I_\epsilon)R \\
 &= \mathbb{Q}J_N \cap R_1 = J_N.
 \end{aligned}$$

The last equality follows from that  $R_1/J_N \simeq \mathbb{Z}[G_1/N]$  is torsion free. This completes the proof. □

COROLLARY 3.3.

$$[e^+ U_0: e^+ U_0'] = (q - 1)^{[H:k] - e}.$$

*Proof.* By the definitions of  $U$  and  $U'$ , we have  $e^+U_0 = e^+V + e^+s(I_\epsilon)R_0$  and  $e^+U'_0 = (q - 1)e^+V + e^+s(I_\epsilon)R_0$ . Hence by Lemma 3.2, there exists an isomorphism

$$e^+U_0/e^+U'_0 \simeq e^+V/(q - 1)e^+V.$$

By Lemma 3.1,  $e^+V$  is a free abelian subgroup of  $\mathbb{Q}[G]$  with rank  $[H:k] - e$ . Thus we get the index. □

By substituting (3.1a–3.1b) and Corollary 3.3 in (3.1), since  $h(H) = h(O_H)R(H)$ , the Theorem B follows at once.

#### 4. The image of cyclotomic numbers by logarithm

In this section, we calculate the index  $(e^+U'_0:l^*(P'))$ . To do this, we need compute the image of cyclotomic numbers under the logarithm. We also obtain the exact relation between the groups of cyclotomic units and the elliptic units in this section.

Let  $e_\chi = (1/|G|) \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}$  be the idempotent associated to  $\chi$  in  $\mathbb{C}[G]$ . We set

$$\omega = (q - 1) \sum_{\chi \neq 1, \text{ real}} L_k(0, \bar{\chi})e_\chi.$$

Note that  $\omega \in \mathbb{Q}[G]$ .

**PROPOSITION 4.1.**  $l^*(P) = \omega V$ .

*Proof.* By Lemma 1.2, it is enough to show

$$\chi(l(\lambda_f)) = \chi(\omega\alpha_f) = (q - 1)L_k(0, \bar{\chi})\chi(\alpha_f), \tag{4.1}$$

for any  $1 \neq \chi \in \widehat{G}$  and any  $f \mid m$ ,  $f \neq \epsilon$ . When  $\chi$  is non-real, we see that both sides of (4.1) are zeroes. Now suppose that  $\chi$  is real.

Assume  $f_\chi \nmid f$ . Since  $\text{Gal}(K_f/k) \simeq G/I_f$ , there exists  $\sigma \in I_f$  such that  $\chi(\sigma) \neq 1$  and  $\sigma l(\lambda_f) = l(\lambda_f^\sigma) = l(\lambda_f)$ . Hence  $\chi(l(\lambda_f)) = 0$ . If  $f_\chi \mid f$ , we have computed  $\chi(l(\lambda_f))$  in (2.1).

On the other hand,  $\chi(\bar{\sigma}_p) = \bar{\chi}(p)$  and  $\chi(s(I_f)) = \sum_{\sigma \in I_f} \chi(\sigma)$ , which equals 0 if  $f_\chi \nmid f$  and equals  $\Phi(m)/\Phi(f)$  if  $f_\chi \mid f$ . The equality (4.1) follows at once. □

**LEMMA 4.2.**  $l^*(Q_m) = \omega J_N$ .

*Proof.* For a prime  $p$  of  $\mathbb{A}$ , we see  $s(I_\epsilon)\bar{\sigma}_p = \tau_p^{-1}$ . By Lemma 1.3(3) and Equation (2.2)

$$l^*(\xi(\mathbb{A})/\xi(p)) = \omega(1 - \tau_p^{-1}).$$

This implies the lemma. □

Recall that  $P' = \mathbb{F}_q^* P^{q-1} Q_{m'} = \mathbb{F}_q^* P^{q-1} Q_{mm'}$  and  $U' = (q-1)V + s(I_\epsilon)R$ . Thus Proposition 4.1 and Lemma 4.2 imply

**COROLLARY 4.3.**  $l^*(P') = \omega U'_0$ .

Now we can calculate the index  $(e^+ U'_0 : l^*(P'))$ . Noting that  $\omega \in Y$ , we define a linear mapping  $A$  on  $Y$  by  $A(\alpha) = \omega \alpha$  for  $\alpha \in Y$ . Since  $l^*(P') = \omega U'_0 = \omega e^+ U'_0$ , we have  $A(e^+ U'_0) = l^*(P')$ . A standard calculation shows that

$$(e^+ U'_0 : l^*(P')) = \det A = \prod_{1 \neq \chi \in \widehat{G^+}} (q-1)L_k(0, \chi) = (q-1)^r \frac{h(H)}{h}.$$

In the rest of this section, we study the relation between the cyclotomic units and the unramified elliptic units. Since  $L(0, \chi) \neq 0$  for all non-trivial real characters  $\chi$ , the multiplication by  $\omega$  is an automorphism of  $e^+ \mathbb{C}[G]_0$ . Thus Lemma 3.2 gives us

$$\omega V \cap \omega s(I_\epsilon)R_0 = (q-1)\omega V \cap \omega s(I_\epsilon)R_0 = \omega J_N. \quad (4.2)$$

The following result gives the exact relation between the groups of cyclotomic units and elliptic units.

**PROPOSITION 4.4.**

$$P^{s(J)} \cap Q = Q_m \quad \text{and} \quad C \cap \overline{E} = \overline{E}_m.$$

*Proof.* First we show that the second equality follows from the first: Let  $u \in C \cap \overline{E}$ . We have  $u^{s(J)} = u^{q-1} \in P^{s(J)} \cap Q = Q_m$ . Thus  $u \in \overline{E}_m$ . By (1.1), the second one follows. Now we show the first one. By Proposition 2.1 and Lemma 2.2, the Equation (4.2) above implies

$$l^*(P^{q-1}) \cap l^*(Q) = l^*(P) \cap l^*(Q) = l^*(Q_m).$$

Thus for any  $x \in P^{s(J)} \cap Q$ , there exists  $y \in Q_m$  such that  $l^*(x) = l^*(y)$ . By considering  $xy^{-1}$ , it is reduced to the following

**LEMMA 4.5.**

$$\ker l^* \cap P^{s(J)} = k \cap Q_m.$$

*Proof.* Let  $x \in \ker l^* \cap P^{s(J)}$ . Then for  $\sigma \in G$ ,  $(\sigma-1)l^*(x) = l(x^{\sigma-1}) = 0$ . Hence  $x^{\sigma-1}$  is a positive root of 1 and is 1. Therefore  $x \in k^*$  and further by Lemma 1.5, we have  $x \in Q_m \cap k$ . The other inclusion is obvious.  $\square$

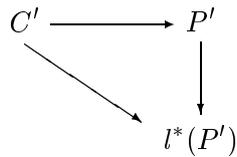
## 5. The index $[l^*(P') : l(C')]$

In this section, we compute the index  $[l^*(P') : l(C')]$ . Our method is much simpler than Galovich and Rosen's (Props. 4.1–4.7, [2]) and Sinnott's (Lemmas 4.1–4.3, [12]) when applied to their cases.

PROPOSITION 5.1. *Let  $s$  be the number of distinct prime divisors of  $m$ . Then*

$$[l^*(P'):l(C')] = (q - 1)^{-s} \Phi(m)h.$$

*Proof.* From the commutative diagram



we obtain an exact sequence

$$0 \rightarrow \mathbb{F}_q^* \rightarrow \ker l^* \cap P' \rightarrow P'/C' \rightarrow l^*(P')/l(C') \rightarrow 0.$$

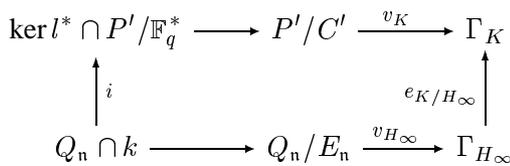
Regard  $(\ker l^* \cap P')/\mathbb{F}_q^*$  as a subgroup of  $P'/C'$ . Then

$$[l^*(P'):l(C')] = [P'/C':(\ker l^* \cap P')/\mathbb{F}_q^*]. \tag{5.1}$$

Write  $n = mm'$  for simplicity. Let  $m = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_s^{e_s}$  and  $m' = \mathfrak{p}_{s+1}^{e_{s+1}} \dots \mathfrak{p}_{s+t}^{e_{s+t}}$ . For  $1 \leq i \leq s + t$ , we take  $\wp_i$  to be a prime ideal in  $H_\infty$  lying above  $\mathfrak{p}_i$  and take  $\mathfrak{R}_i$  to be a prime ideal in  $K$  lying above  $\wp_i$ . Let  $\Gamma_K = \Gamma_{H_\infty} = \mathbb{Z}^{s+t}$  and let  $e_{K/H_\infty}: \Gamma_{H_\infty} \rightarrow \Gamma_K$  be the map multiplying the  $i$ th component by the ramification index  $e_{\mathfrak{R}_i/\wp_i}$  for  $1 \leq i \leq s + t$ . Define two valuation maps  $v_K$  and  $v_{H_\infty}$  by

$$v_K(x) = (v_{\mathfrak{R}_1}(x), \dots, v_{\mathfrak{R}_{s+t}}(x)) \quad \text{and} \quad v_{H_\infty}(y) = (v_{\wp_1}(y), \dots, v_{\wp_{s+t}}(y))$$

for  $x \in P'$  and  $y \in Q_n$ . We have the following commutative diagram



where  $i$  is induced by the inclusion. In fact by Lemma 4.5 it is an isomorphism. By Lemma 1.3(1–3), there exist two exact sequences

$$\begin{aligned} 0 \rightarrow C' \rightarrow P' &\xrightarrow{v_K} \Gamma_K, \\ 0 \rightarrow E_n \rightarrow Q_n &\xrightarrow{v_{H_\infty}} \Gamma_{H_\infty} \rightarrow 0, \end{aligned}$$

and  $\text{Im } v_K = (q - 1)\mathbb{Z}^s \oplus \mathbb{Z}^t$ . Thus

$$Q_n/E_n \simeq \Gamma_{H_\infty} \quad \text{and} \quad [\Gamma_K: \text{Im } v_K] = (q - 1)^s.$$

By (Thm. 4.17, [7]), the ramification index  $e_{\mathfrak{R}_i/\wp_i} = \Phi(\mathfrak{p}_i^{e_i})$  for  $1 \leq i \leq s$  and  $e_{\mathfrak{R}_i/\wp_i} = 1$  for  $s+1 \leq i \leq s+t$ . We have

$$[\Gamma_K: \text{Im}(e_{K/H_\infty})] = \prod_{i=1}^s \Phi(\mathfrak{p}_i^{e_i}) = \Phi(\mathfrak{m}).$$

By Equation (5.1) and the diagram (5.2), we have

$$[l^*(P'): l(C')] = (q-1)^{-s} \Phi(\mathfrak{m}) [Q_n/E_n: Q_n \cap k].$$

Finally we need to compute  $[Q_n/E_n: Q_n \cap k]$ . We will show

$$(Q_n/E_n)/Q_n \cap k \simeq G_1.$$

By (Prop. 1.7, [6]) recall that  $M$  is the set of positive elements in  $k$

$$G_1 \simeq MQ_n/ME_n.$$

Since  $Q_n \cap M = Q_n \cap k$ ,

$$MQ_n/ME_n \simeq Q_n/E_n(Q_n \cap M) \simeq (Q_n/E_n)/Q_n \cap k.$$

This completes the proof of the proposition. □

## 6. The index $(e^+R_0: e^+U_0)$

In this section, we calculate the index  $(e^+R_0: e^+U_0)$ . We follow Sinnott's arguments closely except for some modifications. First, we check that  $U$  has a nice property like in [2] and [12].

**PROPOSITION 6.1.** *Let  $U_{\mathfrak{p}}$  be the  $R$ -module generated in  $\mathbb{Q}[G]$  by  $s(T_{\mathfrak{p}})$  and  $1 - \bar{\sigma}_{\mathfrak{p}}$ . Then*

$$U = \prod_{\mathfrak{p}|\mathfrak{m}} U_{\mathfrak{p}}.$$

The proof is almost identical to that of (Prop. 5.1, [12]) with only one exception that  $I_{\mathfrak{c}} = \prod_{\mathfrak{p}|\mathfrak{m}} T_{\mathfrak{p}}$  in our case. Let  $\mathfrak{m} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$  and let  $S = \{1, \dots, s\}$ . For any subset  $I$  of  $S$ , let

$$U_I = \prod_{i \in I} U_{\mathfrak{p}_i} \quad \text{and} \quad T_I = \prod_{i \in I} T_{\mathfrak{p}_i}.$$

We put  $U_\phi = R, T_\phi = \{1\}$  for the empty set  $\phi$  by convention. Let  $I' = S - I$ . For  $0 \leq r \leq s$ , we put  $I_r = \{i \mid 1 \leq i \leq r\}$  and write  $U_r = U_{I_r}$  and  $T_r = T_{p_r}$  for simplicity. For  $t \geq 0$ , let

$$A_r^t = H^t(J, U_r^{T_{I_r'}})$$

be the  $t$ th cohomology of  $J$ -module  $U_r^{T_{I_r'}}$  induced by the  $G$ -action. They are  $G$ -modules. The proofs of the following two results are the same as those of (Lemmas 5.3 and 5.4, [12]) respectively. For convenience of the reader, we also copy the arguments of Sinnott's here.

LEMMA 6.2.  $I_c$  acts trivially on  $A_r^t$  and  $(q - 1)A_r^t = 0$ .

*Proof.* Since  $I_c = \prod_{i=1}^s T_i$ , it suffices to show that  $T_i$  acts trivially on  $A_r^t$  for  $1 \leq i \leq s$ . If  $i > r$ , then  $T_i \subseteq T_{I_r'}$  and  $T_i$  acts trivially on  $U_r^{T_{I_r'}}$ . Thus  $T_i$  acts trivially on  $A_r^t$ .

Now suppose that  $i \leq r$ . In the following proof, without loss of generality, we assume  $i = r$ . We have

$$U_r = U_{p_r} U_{r-1} = s(T_r)U_{r-1} + (1 - \bar{\sigma}_{p_r})U_{r-1}. \tag{6.1}$$

Let  $\sigma \in T_r$ . Since  $(\sigma - 1)s(T_r) = 0$ , we get  $(\sigma - 1)U_r \subseteq U_{r-1}$ . We can then make a commutative diagram of  $G$ -modules

$$\begin{array}{ccc} U_r & \xrightarrow{f} & U_{r-1} \\ & \searrow & \downarrow g \\ & & U_r, \end{array} \tag{6.2}$$

where  $f$  is the map induced by multiplication by  $\sigma - 1$ , and  $g$  is the map induced by multiplication by  $1 - \bar{\sigma}_{p_r}$ . Since  $(\sigma - 1)(1 - \bar{\sigma}_{p_i}) = \sigma - 1$ ,  $g \circ f$  is simply the endomorphism of  $U_r$  induced by multiplication by  $\sigma - 1$ . All of them are  $G$ -maps. Taking  $T_{I_r'}$ -invariants in (6.2) and applying  $H^t(J, \_)$ , we get the second commutative diagram

$$\begin{array}{ccc} A_r^t & \xrightarrow{f^*} & H^t(J, U_{r-1}^{T_{I_r'}}) \\ & \searrow & \downarrow g^* \\ & & A_r^t. \end{array}$$

However, by (Prop. 5.3, [12]),  $H^t(J, U_{r-1}^{T_{I_r'}}) = 0$ . Hence  $g^* \circ f^* = 0$ , i.e.,  $(\sigma - 1)A_r^t = 0$ . Thus  $T_r$  acts trivially on  $A_r^t$ . The result follows.  $\square$

Thus  $A_r^t$  are  $G/I_c = G_1$ -modules. The following result is important to the calculation of  $A_r^t$ .

**PROPOSITION 6.3.** *There exists an exact sequence of  $G$ -modules*

$$0 \rightarrow A_{r-1}^t / (1 - F_{\mathfrak{p}_r}^{-1}) \rightarrow A_r^t \rightarrow (A_{r-1}^{t+1})^{F_{\mathfrak{p}_r}} \rightarrow 0, \tag{6.3}$$

where  $F_{\mathfrak{p}_r}$  is the Frobenius associated to  $\mathfrak{p}_r$  in  $G$ .

*Proof.* Since  $(1 - \bar{\sigma}_{\mathfrak{p}_r})U_{r-1} \subseteq U_r$ , there exists a  $G$ -map  $g: U_{r-1} \rightarrow U_r$  induced by multiplication by  $1 - \bar{\sigma}_{\mathfrak{p}_r}$ . Let  $e_{\mathfrak{p}} = s(T_{\mathfrak{p}})/|T_{\mathfrak{p}}|$  for prime  $\mathfrak{p}$  and let  $Y = (1 - e_{\mathfrak{p}_r})U_{r-1}$ . Since  $(1 - e_{\mathfrak{p}_r})e_{\mathfrak{p}_r} = 0$ , we also have  $Y = (1 - e_{\mathfrak{p}_r})U_r$  by (6.1). Consider the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_{r-1}^{T_r} & \longrightarrow & U_{r-1} & \longrightarrow & Y & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \longrightarrow & U_r^{T_r} & \longrightarrow & U_r & \longrightarrow & Y & \longrightarrow & 0, \end{array} \tag{6.4}$$

where  $f$  and  $h$  are the maps induced by  $g$ . Since  $\bar{\sigma}_{\mathfrak{p}_r} = e_{\mathfrak{p}_r}F_{\mathfrak{p}_r}^{-1}$ ,  $h$  is indeed the identity map. Notice that for any  $R$ -submodule  $B$  of  $\mathbb{Q}[G]$ ,  $a \in B^{T_{\mathfrak{p}}}$  if and only if  $(1 - e_{\mathfrak{p}})a = 0$ . Thus the two rows in (6.4) are exact sequences of  $R$ -modules. By (Prop. 5.2, [12]),  $U_{r-1}$  is free over  $T_r$  and hence  $U_r^{T_r} = U_{r-1}^{T_r}$  by (Lemma 5.2, [12]). We see  $f$  is the map induced by multiplication by  $1 - F_{\mathfrak{p}_r}^{-1}$ .

Again by (Prop. 5.2, [12]),  $U_r$  is free over  $T_{I'_r}$  and  $U_{r-1}$  is free over  $T_{I'_{r-1}}$ . Hence  $U_{r-1}^{T_r} (= U_r^{T_r})$  and  $Y$  are free over  $T_{I'_r}$ . Thus taking  $T_{I'_r}$ -invariants in (6.4) leaves the rows exact. We get the second commutative diagram of  $G$ -modules, with the exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_{r-1}^{T_{I'_{r-1}}} & \longrightarrow & U_{r-1}^{T_{I'_r}} & \longrightarrow & Y^{T_{I'_r}} & \longrightarrow & 0 \\ & & \downarrow 1 - F_{\mathfrak{p}_r}^{-1} & & \downarrow g & & \downarrow 1 & & \\ 0 & \longrightarrow & U_{r-1}^{T_{I'_r}} & \longrightarrow & U_r^{T_{I'_r}} & \longrightarrow & Y^{T_{I'_r}} & \longrightarrow & 0. \end{array} \tag{6.5}$$

Now by (Prop. 5.3, [12]),  $H^t(J, U_{r-1}^{T_{I'_r}}) = 0$  for any  $t > 0$ . Applying  $H^*(J, \_)$  to (6.5), we obtain in part the following commutative diagram of  $G$ -modules with exact rows

$$\begin{array}{ccccccccccc} H^{t-1}(J, Y^{T_{I'_r}}) & \longrightarrow & A_{r-1}^t & \longrightarrow & 0 & \longrightarrow & H^t(J, Y^{T_{I'_r}}) & \longrightarrow & A_{r-1}^{t+1} & \longrightarrow & 0 \\ \downarrow 1 & & \downarrow 1 - F_{\mathfrak{p}_r}^{-1} & & \downarrow & & \downarrow 1 & & \downarrow 1 - F_{\mathfrak{p}_r}^{-1} & & \\ H^{t-1}(J, Y^{T_{I'_r}}) & \xrightarrow{\alpha} & A_{r-1}^t & \xrightarrow{\beta} & A_r^t & \xrightarrow{\gamma} & H^t(J, Y^{T_{I'_r}}) & \xrightarrow{\delta} & A_{r-1}^{t+1}. \end{array}$$

Using the commutativity of the square on the far left, we see  $\text{Im } \alpha = (1 - F_{p_r}^{-1})A_{r-1}^t = \ker \beta$ . Similarly using the commutativity on the far right, we have  $\ker \delta = H^t(J, Y^{T_{I_r}})_{F_{p_r}^{-1}} = \text{Im } \gamma$ . Finally the top row then gives an isomorphism  $H^t(J, Y^{T_{I_r}}) \simeq A_{r-1}^{t+1}$ . The result follows at once.  $\square$

We compute  $A_r^t$  by inductively using Proposition 6.3. Let  $G_1^{(r)} = G_1 / \langle \tau_{p_1}, \dots, \tau_{p_r} \rangle$ , where  $\langle \tau_{p_1}, \dots, \tau_{p_r} \rangle$  is the subgroup of  $G_1$  generated by  $\tau_{p_1}, \dots, \tau_{p_r}$ . We have

**PROPOSITION 6.4.** *If  $r > 1$ , we assume  $(q - 1, h) = 1$ . Then for  $1 \leq r \leq s$  and  $t > 0$*

$$A_r^t \simeq (\mathbb{Z}/(q - 1)[G_1^{(r)}])^{2^{r-1}}.$$

*Remark.* Although we can not determine  $A_2^t$  in general case, we can get the order of  $A_2^t$  by taking  $r = 2$  in (6.3), i.e.

$$\#A_2^t = (q - 1)^{2\#G_1^{(2)}}. \tag{6.6}$$

It enables us to compute  $(e^+R_0: e^+U_0)$  when  $s = 2$ .

*Proof.* Since  $I_\epsilon$  acts trivially on  $A_{r-1}^t$  and  $s(I_\epsilon)F_{p_r} = \tau_{p_r}$ , we can replace  $F_{p_r}^{-1}$  and  $F_{p_r}$  in (6.3) by  $\tau_{p_r}$ . Recall  $R_1 = \mathbb{Z}[G_1] = s(I_\epsilon)R$ . Since  $R^{I_\epsilon} = s(I_\epsilon)R = R_1$ , we have

$$\begin{aligned} A_0^1 &= H^1(J, R^{I_\epsilon}) = 0, \\ A_0^2 &= H^2(J, R^{I_\epsilon}) \simeq \frac{R_1}{(q - 1)R_1} \simeq \frac{\mathbb{Z}}{(q - 1)}[G_1]. \end{aligned}$$

Since  $J$  is a cyclic group,  $A_0^t = 0$  if  $t$  is odd, and  $A_0^t \simeq \mathbb{Z}/(q - 1)[G_1]$  if  $t$  is even. Taking  $r = 1$  in (6.3), we get the assertion for  $r = 1$ . By the following lemma, the exact sequence (6.3) splits when  $(h, q - 1) = 1$ . Thus the cases of  $r > 1$  come from the case  $r = 1$  and (6.3) by the inductive arguments.  $\square$

**LEMMA 6.5.** *Let  $G$  be a finite abelian group with a subgroup  $H$ . Let  $m$  be a positive integer coprime to  $|G|$ . Then any exact sequence of  $\mathbb{Z}/m[G]$ -modules*

$$0 \rightarrow (\mathbb{Z}/m[G/H])^a \xrightarrow{f} A \xrightarrow{g} (\mathbb{Z}/m[G/H])^b \rightarrow 0$$

*splits, where  $a, b$  are positive integers.*

*Proof.* It suffices to show that  $H$  acts trivially on  $A$ . Let  $e_1, \dots, e_b$  be a basis of  $\mathbb{Z}/m[G/H]^b$  as  $G$ -module. Let  $\tilde{e}_1, \dots, \tilde{e}_b \in A$  whose images are  $e_1, \dots, e_b$  respectively. It is enough to prove that  $\sigma(\tilde{e}_i) = \tilde{e}_i$  for all  $\sigma \in H$  and all  $i$ . Let

$$\sigma(\tilde{e}_i) - \tilde{e}_i = f_i(\sigma) \in \ker g = \text{Im } f.$$

Since  $f_i(\sigma\tau) = \sigma(f_i(\tau)) + f_i(\sigma) = f_i(\sigma) + f_i(\tau)$ , we see  $f_i: H \rightarrow \text{Im } f$  is a group homomorphism. For  $(|G|, m) = 1, f_i = 0$ .  $\square$

The calculation of  $A_r^t$  leans heavily on the splitting of the exact sequence (6.3). The lemma above shows that (6.3) splits under the hypothesis  $(q - 1, h) = 1$ . Does (6.3) split always? This is equivalent to the following problem.

**PROBLEM 6.6.** *Let  $1 \leq r \leq s$ . Does  $F_{p_i}$  or  $\tau_{p_i}$  act trivially on  $A_r^t$  for  $1 \leq i \leq r$ ?*

If this problem had an affirmative answer, the restrictive hypothesis in Proposition 6.4 and thus in Theorem B (see below) would be unnecessary.

After the preparation above, we can compute the index  $(e^+ R_0: e^+ U_0)$  under the assumption  $(h, q - 1) = 1$  when  $s \geq 3$ . Exactly as in ([12], Sect. 6), one shows that

$$(R: U) = \prod_{r=1}^s (U_{r-1}: U_r) = 1.$$

By ([12], Lemma 6.1) it follows that

$$1 = (R: U) = (R_0: U_0)(s(G)R: s(G)U) = \Phi(m)(R_0: U_0).$$

The last equality is from  $s(G)U = |I_c|s(G)\mathbb{Z}$ . Again by ([12], Lemma 6.1)

$$\frac{1}{\Phi(m)} = (R_0: U_0) = (e^+ R_0: e^+ U_0)(\ker(e^+)|_{R_0}: \ker(e^+)|_{U_0}).$$

However

$$\begin{aligned} (\ker(e^+)|_{R_0}: \ker(e^+)|_{U_0}) &= (\ker(e^+)|_R: \ker(e^+)|_U) \\ &= (\ker(e^+)|_R: (1 - j)U)((1 - j)U: \ker(e^+)|_U), \end{aligned}$$

where  $j$  is a generator of  $J$ , and

$$\ker(e^+)|_U/(1 - j)U \simeq H^{-1}(J, U) \simeq A_s^1.$$

Thus, by  $\ker(e^+)|_R = (1 - j)R$  and by Proposition 6.4 (or Eq. (6.6) when  $s = 2$ )

$$(e^+ R_0: e^+ U_0)((1 - j)R: (1 - j)U) = (q - 1)^{e^{2^s - 1}} / \Phi(m). \tag{6.7}$$

To calculate  $((1 - j)R: (1 - j)U)$ , note that

$$\begin{aligned} ((1 - j)R: (1 - j)U) &= \prod_{r=1}^s ((1 - j)U_{r-1}: (1 - j)U_r) \\ &= \prod_{r=1}^s ((1 - j)U_{r-1}^{T_r}: (1 - j)U_r^{T_r}). \end{aligned}$$

The second equality is from ([12], Lemma 6.1) and ([12], Eq. 5.2). Thus we are reduced to compute  $((1 - j)U_{r-1}^{T_r} : (1 - j)U_r^{T_r})$ . Let

$$B_{r-1} = (1 - j)U_{r-1}^{T_r} / s(T_r)(1 - j)U_r^{T_r}.$$

Then

$$((1 - j)U_{r-1}^{T_r} : (1 - j)U_r^{T_r}) = |B_{r-1} / (1 - F_{p_r}^{-1})|.$$

Exactly as in [12], one sees that

$$B_{r-1} \simeq H^1(T_r, U_{r-1}^J) \simeq H^1(J, U_{r-1}^{T_r}).$$

Assume  $s = 1$ . Then  $r = 1$  and  $B_0 = 0$ . Hence

$$((1 - j)R : (1 - j)U) = 1.$$

Suppose that  $s > 1$ . If  $r < s$ , we must have  $B_{r-1} = 0$  by (Prop. 5.3, [12]). If  $r = s$ , then  $B_{s-1} \simeq A_{s-1}^1 \simeq (\mathbb{Z}/(q - 1)[G_1^{(s-1)}])^{2^{s-2}}$  and

$$B_{s-1} / (1 - F_{p_s}^{-1}) = B_{s-1} / (1 - \tau_{p_s}) \simeq (\mathbb{Z}/(q - 1)[G_1^{(s)}])^{2^{s-2}}.$$

Hence

$$((1 - j)R : (1 - j)U) = (q - 1)^{e2^{s-2}}.$$

It follows from (6.7) that

$$(e^+R_0 : e^+U_0) = \begin{cases} (q - 1)^e / \Phi(\mathfrak{m}) & \text{if } s = 1, \\ (q - 1)^{e2^{s-2}} / \Phi(\mathfrak{m}) & \text{if } s > 1. \end{cases}$$

Thus we complete the proof of the Theorem B stated in the introduction.

### Acknowledgements

The author would like to express his sincere gratitude to his adviser Professor Takeshi Saito for many helpful suggestions. He also wants to express his thanks to Professors D. Goss and Y. Taguchi for their interest and encouragement. He thanks also the referees for their careful reading of the manuscript and suggestions on the writing of the paper.

### References

1. Drinfeld, V. G.: Elliptic modules, *English Trans. Math. USSR-Sb.* 23 (1974) 561–592.

2. Galovich, S. and Rosen, M.: Units and class group in cyclotomic function fields, *J. Number Theory* 14 (1982) 156–184.
3. Goss, D.: The  $\Gamma$ -ideal and special zeta-values, *Duke Math. J.* 47 (1980) 345–364.
4. Gross, B. and Rosen, M.: Fourier series and special values of  $L$ -functions, *Advances in Math.* 69 (1988) 1–31.
5. Hayes, D.: Analytic class number formula in function fields, *Invent. Math.* 65 (1981) 49–69.
6. Hayes, D.: Elliptic units in function fields, in *Number Theory Related to Fermat's Last Theorem*, D. Goldfeld (ed.), Birkhäuser, Boston, (1982) 321–340.
7. Hayes, D.: Stickelberger elements in function fields, *Compositio Math.* 55 (1985) 209–235.
8. Hayes, D.: A brief introduction to Drinfeld modules, in *The Arithmetic of Function Fields*, D. Goss, D. Hayes, and M. Rosen (eds), W. de Gruyter, Berlin, (1992) 1–32.
9. Oukhaba, H.: Groups of elliptic units in global function fields, in *The Arithmetic of Function Fields*, D. Goss, D. Hayes, and M. Rosen (eds), W. de Gruyter, Berlin, (1992) 87–102.
10. Rosen, M.: The Hilbert class field in function fields, *Exposition Math.* 5 (1987) 365–378.
11. Shu, L.: Class number formulas over global function fields, *J. Number Theory* 48 (1994) 133–161.
12. Sinnott, W.: On the Stickelberger ideal and the circular units of a cyclotomic field, *Ann. of Math.* 108 (1978) 107–134.