1

Class number relation between type $(l, l, \cdots, l)$ function fields over $\mathbb{F}_q(T)$ and their subfields

Jianqiang Zhao†

Department of Mathematics, University of Science and Technology of China, Hefei, 230026, PRC

Current Address: Department of Mathematics, Brown University, Providence RI02912, USA

Abstract. Let $L/\mathbb{F}_q$ be a tame abelian extension of type $(l, l, \cdots, l)$. In this paper, we determine the ratios of the degree zero divisor class number and the ideal class number of L to the product of corresponding class numbers of all cyclic subfields of L.

keywords: function field, class number, prime decomposition, ζ-function.

Among the number theorists there are incessant efforts to clarify the class group structures and the class numbers of algebraic number fields, which have presented a large quantity of unsolved problems. In algebraic function fields a lot of work has been done concerning the same kind of problems. Around 1974, D.Hayes[1] successfully established the reciprocity law over $k = \mathbb{F}_q(T)$, the rational function field of one variable over finite constant field $\mathbb{F}_q$, where q is a power of a rational prime number p. He actually constructed the maximal abelian extension of k using the so called cyclotomic function fields. In this paper, our interest lies in a special type of abelian field L over k, whose Galois group $Gal(L/k) \cong (\mathbb{Z}/l\mathbb{Z})^n$ where l is a different prime from p. Such L over k is called n-fold of type $(l, l, \cdots, l)$. We first give the definitions of the class numbers. For any field extension L/k, let S be the set of infinite primes of K lying over the unique infinite prime $\infty = \left(\frac{1}{T}\right)$ of k. Let $\mathcal{D}_s$ be the group generated by the primes of K outside of S (thus D_s is the group of fractional ideals of K), $\mathcal{D}(K)$, $\mathcal{D}^0(K)$, $\mathcal{P}(K)$ and $\mathcal{P}_s$ the groups generated by the divisors of K, the degree zero divisors of K, the principal divisors of K and the finite parts of the principal divisors of K, respectively. Let $R = \mathbb{F}_q[T]$ and O_K be the integral closure of R in K. Conventionally we

*This work was done at the University of Science and Technology of China when the author was a visiting graduate student under a special program of Nankai University. The author thanks Prof. Keqin Feng and Prof. Xianke Zhang for their guidance and kindly help during his study at USTC

†jzhao@@math.brown.edu

call $h(K) = |\mathcal{D}^0(K)/\mathcal{P}(K)|$ the class number of degree zero divisors and $h(O_K) = |D_s/\mathcal{P}_s|$ the ideal class number. Finally we set

$$\mu(K) = g.c.d.\{\deg \mathfrak{p} : \mathfrak{p} \in S\} \tag{1}$$

and the regulator

$$R(K) = (\mathcal{D}^0(K) \cap \mathcal{D}(S) : \mathcal{P}(K) \cap D(S)) \tag{2}$$

where $\mathcal{D}(S)$ is the group generated by divisors in S. From the exact sequence

$$0 \longrightarrow \frac{\mathcal{D}^0(K) \cap \mathcal{D}(S)}{\mathcal{P}(K) \cap \mathcal{D}(S)} \longrightarrow \frac{\mathcal{D}^0(K)}{\mathcal{P}(K)} \xrightarrow{\text{fin. part}} \frac{\mathcal{D}_s}{\mathcal{P}_s} \xrightarrow{\deg} \frac{\mathbb{Z}}{\mu(K)\mathbb{Z}} \longrightarrow 0$$

we have

$$h(K)\mu(K) = h(O_K)R(K). \tag{3}$$

Now, let L/k be n-fold of type $(l, l, \cdots, l)$. When $n = 1$, the only cyclic subfields are L and k, so we assume $n \geq 2$ throughout this paper. Since constant field extensions are cyclic, it's easy to see that L/k is tame (i.e. all primes are tamely ramified) iff $l \neq p$ which we also assume except when we point out otherwise.

1. ζ-functions

It is well known[2] that for any finite extension K/k, the ζ-function defined by

$$\zeta(K, s) = \prod_{\mathfrak{P}:K\text{-prime}} (1 - N\mathfrak{P}^{-s})^{-1} \qquad (Re(s) > 1)$$

can be expressed by

$$\zeta(K, s) = \frac{F_K(u)}{(1-u)(1-qu)}, \tag{4}$$

where $u = q^{-s}$ and $F_K(u)$ is a polynomial in u such that $F_K(1) = h(K)$. So, to establish class number relations between L and its cyclic subfields, we begin by revealing a relation between their ζ-functions.

Proposition 1. *Let L/k be a tame n-fold of type $(l, l, \cdots, l)$ and $\{K_v : v \in \Phi\}$ the set of cyclic subfields of L, then we have*

$$\frac{\zeta(L, s)}{\zeta(k, s)} = \prod_{v \in \Phi} \frac{\zeta(K_v, s)}{\zeta(k, s)}.$$

To prove this proposition, we need a complete description of the decomposition of every prime in L/k, which we will obtain in the next section.

2. Prime Decomposition in L/k

Let ξ be a primitive l-th root of unity and γ a fixed generator of $\mathbb{F}_q{}^{\times}$. If $\xi \in \mathbb{F}_q$, then there exist $m_1, \cdots, m_n \in R = \mathbb{F}_q[T]$ such that $L = k(\sqrt[l]{m_1}, \cdots, \sqrt[l]{m_n})$. Let $R_1 = \{a \in R \setminus \{0\} : a$

has no l-th power factor in $R \setminus \mathbb{F}_q$ and the leading coefficient of a is γ^i for some i such that $0 \le i \le l-1\}$. Then we can assume $m_i \in R_1$ without loss of generality. Define

$$\Omega_n = \{(e_1, \cdots, e_n) : 0 \le e_i \le l-1\}, \tag{5}$$

and an equivalence relation in $\Omega_n^\times = \Omega_n \setminus \{(0, \cdots, 0)\}$ as follows: for any $(e_1, \cdots, e_n)$ and $(f_1, \cdots, f_n) \in \Omega_n^\times$,

$$(e_1, \cdots, e_n) \sim (f_1, \cdots, f_n) \Longleftrightarrow$$
$$\exists i \in \{1, \cdots, l-1\} \text{ such that } e_j \equiv i f_j \pmod{l} \text{ for all } 1 \le j \le n.$$

We define the projective space of Ω_n by

$$P(\Omega_n) = \Omega_n^\times / \sim . \tag{6}$$

For any $v = (e_1, \cdots, e_n) \in \Omega_n^\times$, we select the unique element $m_v \in R_1$ so that

$$b^l m_v = \prod_{i=1}^{n} m_i^{e_i} \qquad \text{for some } b \in R. \tag{7}$$

For any k-prime P, we define a symbol $\left(\frac{}{P}\right)$ as follows:

$$\left(\frac{m}{P}\right) = \begin{cases} 1 & \text{if } P \text{ splits in } k(\sqrt[l]{m}), \\ 0 & \text{if } P \text{ ramifies in } k(\sqrt[l]{m}), \\ \eta^i & \text{if } \varrho(m) \in \eta^i H; 1 \le i \le l-1, \end{cases}$$

where $\varrho : R \longrightarrow (R/(P)) = G$ is canonical map, η is a generator of $G^\times$ and $H = \{g^l : g \in G^\times\}$ (if $P = \left(\frac{1}{T}\right)$ is the infinite prime, we set $G = \mathbb{F}_q$, $\eta = \gamma$ and $\varrho(m)$ the leading coefficient of m). It is elementary to prove that $\left(\frac{}{P}\right)$ is multiplicative and, there exist $v_1, \cdots, v_n \in \Omega_n$ such that $L = k(\sqrt[l]{m_{v_1}}, \cdots, \sqrt[l]{m_{v_n}})$ with $\left(\left(\frac{m_{v_1}}{P}\right), \cdots, \left(\frac{m_{v_n}}{P}\right)\right)$ being one of the following four types

$$C^0 : (1, 1, \cdots, 1); C^1 : (\eta, 1, \cdots, 1); C^2 : (0, 1, \cdots, 1); C^3 : (0, \eta, 1, \cdots, 1).$$

If $v_1, \cdots, v_n \in \Omega_n$ have been chosen as above, then we say $L = k(\sqrt[l]{m_{v_1}}, \cdots, \sqrt[l]{m_{v_n}})$ is standard. If there are exactly a (respectively b, c) cyclic subfields of L such that P splits (respectively is inert, ramifies) in them, then we condense this information by writing $\mathrm{Sp}(L, P) = 1^a \eta^b 0^c$.

Lemma 1. *Let L be the same as in Proposition 1, $L' = L(\xi)$ and $k' = k(\xi)$. For any k-prime P, let $\mathfrak{p}$ be a k'-prime lying over P. We further take $m_1, \cdots, m_n \in \mathbb{F}_q(\xi)[T]$ such that $L' = k'(\sqrt[l]{m_1}, \cdots, \sqrt[l]{m_n})$ is standard. Then according to the decomposition of P in L, L can be divided into four classes as shown in the following table:*

Type	$\left(\left(\frac{m_1}{\mathfrak{p}}\right), \cdots, \left(\frac{m_n}{\mathfrak{p}}\right)\right)$	*Sp*$(L, P) =$ *Sp*$(L', \mathfrak{p})$	$\log_l(g, e, f,)$
C^0	$(1, 1, \cdots, 1)$	1^{τ_n}	$(\ n\ , 0, 0)$
C^1	$(\eta, 1, \cdots, 1)$	$1^{\tau_{n-1}} \eta^{l^{n-1}}$	$(n-1, 1, 0)$
C^2	$(0, 1, \cdots, 1)$	$1^{\tau_{n-1}} 0^{l^{n-1}}$	$(n-1, 0, 1)$
C^3	$(0, \eta, 1, \cdots, 1)$	$1^{\tau_{n-1}} \eta^{l^{n-2}} 0^{l^{n-2}}$	$(n-2, 1, 1)$

where $\tau_i = (l^i - 1)/(l-1)$, g, e and f denote the splitting degree, the ramification index and the residue class degree respectively.

Proof. If the l-th root of unity $\xi \notin k$, then $\xi \in \mathbb{F}_{q^{l-1}}^{\times}$ by Fermat's little theorem. Thus $[k' : k]$ divides $l-1$ which is prime to l. Hence $\mathrm{Sp}(L,P) = \mathrm{Sp}(L',\mathfrak{p})$ since all of g, e and f are powers of l. Moreover we have: for any L-prime $\mathfrak{P}$ and L'-prime $\mathfrak{P}'$ over P and $\mathfrak{p}$ respectively, $g(\mathfrak{P}/P) = g(\mathfrak{P}'/\mathfrak{p})$, $f(\mathfrak{P}/P) = (\mathfrak{P}'/\mathfrak{p})$ and $e(\mathfrak{P}/P) = e(\mathfrak{P}'/\mathfrak{p})$. Thus, to prove the lemma, we can assume $\xi \in k$ without loss of generality. The rest of the proof is easy and the readers may refer to ref. [3] and its references. This concludes our proof of the lemma. □

Proof of Proposition 1. We only need to check the Euler factors for any k-prime P. Let $u = q^{-s}$, $d = \deg P$, then we have:

$$\frac{\prod_{\mathfrak{P}|P}(1-N\mathfrak{P}^{-s})}{(1-NP^{-s})} = \begin{cases} (1-u^d)^{l^n-1} & \text{if } (L,P)\in C^0, \\ \dfrac{(1-u^{dl})^{l^{n-1}}}{1-u^d} & \text{if } (L,P)\in C^1, \\ (1-u^d)^{l^{n-1}-1} & \text{if } (L,P)\in C^2, \\ \dfrac{(1-u^{dl})^{l^{n-2}}}{1-u^d} & \text{if } (L,P)\in C^3, \end{cases}$$

where $\mathfrak{P}$ is L-prime over P. And using the preceding Lemma we can compute

$$\prod_{v\in\Phi}\frac{\prod_{\mathfrak{p}_v|\mathfrak{p}}(1-N\mathfrak{P}_v^{-s})}{1-NP^{-s}} = \begin{cases} (1-u^d)^{(l-1)\cdot\tau_n} = (1-u^d)^{l^n-1} & \text{if } (L,P)\in C^0, \\ (1-u^d)^{(l-1)\cdot\tau_{n-1}}\cdot\left(\dfrac{1-u^{dl}}{1-u^d}\right)^{l^{n-1}} = \dfrac{(1-u^{dl})^{l^{n-1}}}{1-u^d} & \text{if } (L,P)\in C^1, \\ (1-u^d)^{(l-1)\cdot\tau_{n-1}} = (1-u^d)^{l^{n-1}-1} & \text{if } (L,P)\in C^2, \\ (1-u^d)^{(l-1)\cdot\tau_{n-2}}\cdot\left(\dfrac{1-u^{dl}}{1-u^d}\right)^{l^{n-2}} = \dfrac{(1-u^{dl})^{l^{n-2}}}{1-u^d} & \text{if } (L,P)\in C^3, \end{cases}$$

where $\mathfrak{p}_v$ is K_v-prime over P. Thus

$$\frac{\prod_{\mathfrak{P}|P}(1-N\mathfrak{P}^{-s})}{1-NP^{-s}} = \prod_{v\in\Phi}\frac{\prod_{\mathfrak{p}_v|\mathfrak{p}}(1-N\mathfrak{P}_v^{-s})}{1-NP^{-s}}$$

for any k-prime P, and Proposition 1 follows at once. □

Remark 1. For any finite set S of k-primes viewed as infinite primes, let $S(K)$ be the set of K-primes over S for any finite extension K/k. Define

$$\zeta(O_K,s) = \prod_{\mathfrak{P}\notin S(K)}(1-N\mathfrak{P}^{-s})^{-1} \qquad (Re(s)>1).$$

By the proof of Proposition 1, we also have

$$\frac{\zeta(O_L,s)}{\zeta(O_k,s)} = \prod_{v\in\Phi}\frac{\zeta(O_{K_v},s)}{\zeta(O_k,s)}.$$

3. Main Results

For any finite extension K/k, let $V(K)$ be the free part of the group of unit of K.

Proposition 2. *Let L/k be n-fold of type $(l, l, \cdots, l)$ (here we allow $l = p$). Let $Q = \left(V(L) : \prod_{v\in\Phi} V(K_v)\right)$ be the unit index, then*

$$Q | l^{(n-1)(g(\infty)-1)}$$

where $g(\infty)$ is the splitting degree of $\infty = \left(\frac{1}{T}\right)$ in L.

Proof. If $n = 1$, then we have nothing to prove since $Q = 1$. Suppose $n \geq 2$, and $\sigma_1, \sigma_2 \in Gal(L/k)$ such that $\langle\sigma_1, \sigma_2\rangle \cong (\mathbb{Z}/l\mathbb{Z})^2$. Let L_l and L_i $(1 \leq i \leq l-1)$ be the fixed fields of σ_1 and $\sigma_1^i\sigma_2$ respectively and E_i the group of units of L_i $(1 \leq i \leq l)$. For any units η of L, we have

$$\eta^l = \frac{\eta^{\sum_{i=0}^{l-1}\sum_{j=0}^{l-1}(\sigma_1^i\sigma_2)^j}}{\eta^{\sum_{i=0}^{l-1}\sum_{j=1}^{l-1}(\sigma_1^i\sigma_2)^j}} = \frac{\prod_{i=0}^{l-1}\left(\eta^{\sum_{j=0}^{l-1}(\sigma_1^i\sigma_2)^j}\right)}{\eta^{\sum_{i=0}^{l-1}\sum_{j=1}^{l-1}(\sigma_1^i\sigma_2)^j}}.$$

Clearly, $\eta^{\sum_{j=0}^{l-1}(\sigma_1^i\sigma_2)^j} \in E_i$ for $0 \leq i \leq l-1$ since they are fixed by $\sigma_1^i\sigma_2$. For any fixed i and j such that $0 \leq i \leq l-1$ and $1 \leq j \leq l-1$, there exists a unique i' with $0 \leq i' \leq l-1$ such that

$$ij + 1 \equiv i'j \pmod{l},$$

thus

$$\eta^{\sum_{i=0}^{l-1}\sum_{j=1}^{l-1}(\sigma_1^i\sigma_2)^j} = \sigma_1\left(\eta^{\sum_{i=0}^{l-1}\sum_{j=1}^{l-1}(\sigma_1^i\sigma_2)^j}\right) \in E_l$$

and consequently $\eta^l \in \prod_{i=0}^{l} E_i$. When $n = 2$, $\{L_i : 0 \leq i \leq l\}$ is the set of cyclic subfields of L. By Dirichlet Unit Theorem $V(L) \cong \mathbb{Z}^{g(\infty)-1}$ and Proposition 2 is true in this case.

Now assume that if L is $(n-1)$-fold of type $(l, l, \cdots, l)$ then $\eta^{l^{n-2}} \in \prod_{v\in\Phi} V(K_v)$ for any $\eta \in V(L)$. Let L/k be an extension of n-fold of type $(l, l, \cdots, l)$, then $\{L_i : 0 \leq i \leq l)$ are the set of subextensions of $(n-1)$-fold of type $(l, l, \cdots, l)$, and we have shown that $\eta^l \in \prod_{i=0}^{l} E_i$ for any unit η of L. By inductive assumption, we have

$$\eta^{l^{n-1}} = (\eta^l)^{l^{n-2}} \in \prod_{v\in\Phi} V(K_v).$$

Thus, Proposition 2 follows from the Dirichlet Unit Theorem. ◻

Remark 2. The above result is also true when L is n-fold of type $(l, l, \cdots, l)$ over rational number field $\mathbb{Q}$. To prove this, one can follow our proof word for word.

Main Theorem. *Let L be a tame Galois extension of k with Galois group $G(L/k) \cong (\mathbb{Z}/l\mathbb{Z})^n$. Let $\{K_v : v \in \Phi\}$ be the set of all cyclic subfields of L. Then we have*

$$h(L) = \prod_{v\in\Phi} h(K_v), \tag{8}$$

$$h(O_L) = Ql^{-t}\prod_{v\in\Phi} h(O_{K_v}), \tag{9}$$

where $t = \frac{1}{2}\left[\left(\frac{1}{l-1} + 2n - \lambda - 1\right)(l^\lambda - 1) - \lambda\right]$, $\lambda = \log_l(g(\infty))$, Q and $g(\infty)$ are the same as in Proposition 2.

Proof. By (4) and Proposition 1 we get

$$\frac{F_L(u)}{F_k(u)} = \prod_{v\in\Phi} \frac{F_{K_v}(u)}{F_k(u)}.$$

Since $F_k(1) = 1$ and $F_K(1) = h(K)$ for any finite extension of K/k, (8) follows immediately. By (3), this gives rise to

$$h(O_L) = \mu(L)R(L)^{-1} \prod_{v\in\Phi} \big(h(O_{K_v})\mu(K_v)^{-1}R(K_v)\big). \tag{10}$$

As in Lemma 1, let $L' = k'(\sqrt[l]{m_1}, \cdots, \sqrt[l]{m_n})$ be standard for some k'-prime $\mathfrak{p}$ over ∞. Reversing the order of $m_1, \cdots, m_n$ we may assume that the splitting field of $\mathfrak{p}$ in L' is $L'^+ = k'(\sqrt[l]{m_1}, \cdots, \sqrt[l]{m_\lambda})$, where $\lambda = \log_l(g(\infty))$ and $g(\infty)$ as in Proposition 2. Let $r = l^\lambda$, $r_0 = \frac{r-1}{l-1}$, $r_1 = r-1$, $L^+ = L'^+ \cap L$, Ω_λ and $P(\Omega_\lambda)$ defined as (5) and (6) respectively. We may choose $v_1, \ldots, v_{r_0}$ in Ω_λ as a set of representatives of the projective space $P(\Omega_\lambda)$ such that $v_i = (0, \cdots, 0, 1, 0, \cdots, 0)$ with 1 at the i-th coordinate for $1 \le i \le \lambda$. In what follows we view $P_\lambda = \{v_i \in P(\Omega_\lambda) : 1 \le i \le r_0\}$ as an ordered set. For any $\alpha \in \mathfrak{S} = \{1, \cdots, l-1\}$ and $v = (e_1, \cdots, e_\lambda) \in \Omega_\lambda$, we define $\alpha v = (e_1', \cdots, e_\lambda') \in \Omega_\lambda$ such that $e_i' \equiv \alpha e_i \pmod{l}$ for $1 \le i \le \lambda$. Next, we define two more ordered sets Ω^1 and Ω^2 as follows:

$\Omega^1 = \Omega^1_\lambda$: Put v_i in order where i runs from 1 to r_0, then after each v_i insert $l-2$ elements jv_i where j runs from 2 to $l-2$.

$\Omega^2 = \Omega^2_\lambda$: Put v_i in order, after each v_i insert $l-2$ elements $j^{-1}v_i$ where j runs from 2 to $l-2$. Here by j^{-1} we mean the unique number in $\mathfrak{S}$ such that $j^{-1}j \equiv 1 \pmod{l}$.

Note that $\Omega^1 = \Omega^2 = \Omega^\times_\lambda$ as sets, but they may be different as ordered sets.

Now, let ξ be an l-th root of unity in the algebraic closure of $\mathbb{F}_q$, $k' = k(\xi)$, $L' = L(\xi)$ and $L'^+ = k'(\sqrt[l]{m_1}, \cdots, \sqrt[l]{m_\lambda})$. Let $\sigma_i' \in Gal(L'^+/k), 1 \le i \le \lambda$ such that

$$\sigma_i'(\xi) = \xi, \qquad \sigma_i'(\sqrt[l]{m_j}) = \xi^{\delta_{i,j}}(\sqrt[l]{m_j}) \quad 1 \le j \le \lambda,$$

where $\delta_{i,j}$ is the Kronecker symbol. Then for any $u = (e_1, \cdots, e_\lambda) \in \Omega_\lambda$ we write

$$\sigma_u' = \prod_{i=1}^{\lambda} (\sigma_i')^{e_i}.$$

We next give an inner product on Ω_λ with images in $\mathfrak{S} \cup \{0\}$: for any $u = (e_1, \cdots, e_\lambda)$, $v = (f_1, \cdots, f_\lambda) \in \Omega_\lambda$, define

$$\mathfrak{S} \cup \{0\} \ni u \cdot v \equiv \sum_{i=1}^{\lambda} e_i f_i \pmod{l}.$$

For any m_v defined as (7) we see that $\sigma_u'(\sqrt[l]{m_v}) = \xi^{u\cdot v}(\sqrt[l]{m_v})$ and $\sigma_u'(\xi) = \xi$. Set $\sigma_v = \sigma_v'|L^+ \in Gal(L^+/k)$, then it is easy to check that

$$Gal(L^+/k) = \langle \sigma_1 \rangle \times \cdots \times \langle \sigma_\lambda \rangle$$

and for any $v, v' \in \Omega_\lambda$ such that $v \cdot u = v' \cdot u$ we have

$$\sigma_{v'}\big|_{K_u} = \sigma_v\big|_{K_u} = \sigma_v'\big|_{K_u}, \tag{11}$$

where $K_u = k'(\sqrt[l]{m_u}) \cap L$. Also,

$$\sigma_v\big|_{K_u} = id \Longleftrightarrow u \cdot v = 0 \qquad \forall u, v \in \Omega_\lambda. \tag{12}$$

Let $\{\eta_v : v \in \Omega^2\}$ be a system of fundamental units of L, and $\{K_u : u \in P_\lambda\}$ be the set of real cyclic subfields of L (also of L^+). For each $v \in P_\lambda$, let $\{\varepsilon_{\alpha^{-1}v} : \alpha \in \mathfrak{S}\}$ be a system of fundamental units of K_v, and then put all of them into an ordered set $\{\varepsilon_v : v \in \Omega^2\}$. Let ∞_1 be an L-prime over ∞ and $e = e(\infty_1/\infty)$ the ramification index. Then for any K_u-prime $\mathfrak{p}_u$ over ∞ and dividing ∞_1, we have $e(\infty_1/\mathfrak{p}_u) = e$. Denote the additive valuations corresponding to $\sigma_u^{-1}(\infty_1)$ and $\mathfrak{p}_u$ by w'_u and w_u respectively, then by definition

$$Q = \left|\frac{\langle \eta_v : v \in \Omega^2\rangle}{\langle \varepsilon_v : v \in \Omega^2\rangle}\right| = \left|\frac{\det[w'_u(\varepsilon_v)]}{\det[w'_u(\eta_v)]}\right|.$$

By definition of the regulator (see formula (2)) we have

$$\begin{aligned} R(L) &= \big|\det[w'_u(\eta_v)]\big| = Q^{-1}\big|\det[w'_u(\varepsilon_v)]\big| \\ &= Q^{-1}\big|\det[\mathrm{ord}_{\infty_1}(\sigma_u\varepsilon_v)]\big| \\ &= Q^{-1}\big|\det[e\,\mathrm{ord}_{\mathfrak{p}_v}(\sigma_u\varepsilon_v)]\big| \\ &= Q^{-1}e^{r_1}\left|\det\left[w_v(\sigma_u\varepsilon_v)\right]_{u\in\Omega^1, v\in\Omega^2}\right| \\ &= Q^{-1}e^{r_1}\left|\det\left[w_u(\sigma_v\varepsilon_u)\right]_{v\in\Omega^1, u\in\Omega^2}\right|. \end{aligned} \tag{13}$$

For any $u \in P_\lambda$, set

$$\beta_u = \left[w_u(\varepsilon_{j^{-1}u})\right]_{j\in\mathfrak{S}}, \qquad \mathcal{R}_u^v = \left[w_u(\sigma_{iv}\varepsilon_{j^{-1}u})\right]_{i,j\in\mathfrak{S}} \quad .$$

Let

$$\mathcal{M} = \left[w_u(\sigma_v\varepsilon_u)\right]_{v\in\Omega^1, u\in\Omega^2} \quad . \tag{14}$$

In the above matrices, i and v are indices for rows, j and u are indices for columns. By (11), for every fixed u and any v such that $u \cdot v = 1$, $\mathcal{R}_u^v$ are all equal, which we denote by $\mathcal{R}_u$. By the definition of the regulator $R(K_u) = |\det \mathcal{R}_u|$. In what follows we will omit the symbols for absolute value and only consider the equations up to signs. In order to computer $\det \mathcal{M}$, we set

$$A := \begin{vmatrix} 1 & \beta_{v_1}\cdots\beta_{v_{r_0}} \\ 0 & \\ \vdots & \mathcal{M} \\ 0 & \end{vmatrix} = \begin{vmatrix} 1 & \beta_{v_1} \quad \cdots \quad \beta_{v_{r_0}} \\ -1 & \\ \vdots & \mathcal{B} = \left[\mathcal{R}_u^v - \mathcal{R}_u^0\right]_{u,v\in P_\lambda} \\ -1 & \end{vmatrix}, \tag{15}$$

where we get the equation by carrying out the following operations on the first determinant: 1-st row $\times\,(-1)$ + other rows. Since $N_{K_u/k}(\varepsilon_u) = 1$, adding all rows but the first we get a row

$$[1 - l^\lambda \qquad -l^\lambda\beta_{v_1} \quad \cdots \quad -l^\lambda\beta_{v_{r_0}}] \tag{16}$$

In obtaining (16), we use the following elementary result which can be found in ref. [4].

Lemma 2. *For any fixed $v \in \Omega_\lambda^\times$, $x \cdot v = 0$ has $l^{\lambda-1} - 1$ solutions in $\Omega_\lambda^\times$. If $\alpha \in \mathfrak{S}$, then $x \cdot v = \alpha$ has $l^{\lambda-1}$ solutions in $\Omega_\lambda^\times$.*

Adding (16) to $l^\lambda \times$ (1-st row) we can get

$$\det \mathcal{M} = A = l^{-\lambda} \det \mathcal{B}, \qquad \mathcal{B} = \left[\mathcal{R}_u^v - \mathcal{R}_u^0\right]_{u,v \in P_\lambda}, \tag{17}$$

where u is index of columns, v of rows. For each $u \in P_\lambda$, let $\mathcal{B}_u$ denote the $l-1$ columns of $\mathcal{B}$ corresponding to u. By (11) we can permute the rows of $\mathcal{B}_u$ so that the result is

$$\left[(1 - \delta_{0,u\cdot v})(\mathcal{R}_u - \mathcal{R}_u^0)\right]_{v \in P_\lambda}.$$

This operation on $\mathcal{B}$ is called u-trans. Under u-trans, the element of $\mathcal{B}$ at $(iv, j^{-1}u)$-th position remains fixed if $u \cdot v = 0$ or moves to the $(i(u\cdot v)v, j^{-1}u)$-th position by formulas (12) and (11). Now, view $\det(\mathcal{R}_u - \mathcal{R}_u^0)$ as an element, we can bring it outside of $\det \mathcal{B}$, and the element at the $(i(u\cdot v)v, j^{-1}u)$-th position of the remaining matrix is $\delta_{i(u\cdot v),j}$. Then, taking the inverse transformation of u-trans, we see that except for $l-1$ columns corresponding to $u \in P_\lambda$, other columns remain the same as before we take u-trans while the $(iv, j^{-1}u)$-th element becomes $\delta_{i(u\cdot v),j}$. Going through the above procedure for each $u \in P_\lambda$ we arrive at

$$\det \mathcal{B} = \det \mathcal{A} \prod_{u \in P_\lambda} \det(\mathcal{R}_u - \mathcal{R}_u^0) \tag{18}$$

where

$$\mathcal{A} = \left[\delta_{u\cdot v,1}\right]_{u \in \Omega^2, v \in \Omega^1}.$$

Set $\mathcal{A}\mathcal{A}^t = [b_{u,v}]$, where $\mathcal{A}^t$ is the transposition of $\mathcal{A}$, then

$$b_{u,v} = \sum_{w \in \Omega_\lambda^\times} \delta_{v\cdot w,1}\delta_{u\cdot w,1} = \sharp\{w \in \Omega_\lambda : u \cdot w = v \cdot w = 1\}.$$

If $u = v$, then $b_{u,v} = l^{\lambda-1}$ from Lemma 2. If $u = jv$ for some $j \in \mathfrak{S}$ and $j \neq 1$, then $b_{u,v} = 0$. When $\lambda = 1$, $b_{u,v} = 0$ for $u \neq v$. When $\lambda \geq 2$, we set $u = (e_1, \cdots, e_\lambda)$ and $v = (f_1, \cdots, f_\lambda)$, then $u \neq jv$ for all $j \in \mathfrak{S}$ iff there exist $i \neq j$ and $1 \leq i, j \leq \lambda$ such that $e_i f_j \not\equiv e_j f_i \pmod{l}$, therefore $b_{u,v} = l^{\lambda-2}$ by an easy computation. Thus

$$\det \mathcal{A}^2 = \det \mathcal{A}\mathcal{A}^t = l^{r_1(\lambda-2)} \begin{vmatrix} lI & E & \cdots & E \\ E & lI & \cdots & E \\ \vdots & \vdots & & \vdots \\ lE & E & \cdots & lI \end{vmatrix}, \tag{19}$$

where I is the unit matrix of rank $l-1$, and each entry of E is 1. It is not difficult to compute $\det \mathcal{A}^2$ by elementary transformations and to find that

$$\det \mathcal{A}^2 = l^{r_1(\lambda - \frac{1}{l-1}) + \lambda}. \tag{20}$$

Since $N_{K_u/k}(\varepsilon_u) = 1$, we get

$$\det(\mathcal{R}_u - \mathcal{R}_u^0) = l \det(\mathcal{R}_u) = lR(K_u). \tag{21}$$

From formulas (13) to (21), we have

$$R(L) = Q^{-1} e^{r_1} l^{\frac{1}{2}[(\frac{1}{l-1}+\lambda-1)r_1-\lambda]} \prod_{u\in P(\Omega_\lambda)} R(K_u).$$

But for imaginary field K over k (i.e. ∞ does not split in K), $R(K) = 1$. So

$$R(L) = Q^{-1} e^{r_1} l^{\frac{1}{2}[(\frac{1}{l-1}+\lambda-1)r_1-\lambda]} \prod_{v\in \Phi} R(K_u). \tag{22}$$

From (1) and $e = e(\infty_1/\infty)$ we have

$$\mu(L)^{-1} \prod_{v\in\Phi} \mu(K_v) = \begin{cases} 1 & \text{if } (L,\infty) \in C^0 \cup C^2, \\ l^{r_1} & \text{if } (L,\infty) \in C^1 \cup C^3, \end{cases} \tag{23}$$

and

$$e^{r_1} = \begin{cases} 1 & \text{if } (L,\infty) \in C^0 \cup C^1, \\ l^{r_1} & \text{if } (L,\infty) \in C^2 \cup C^3. \end{cases} \tag{24}$$

Combining formulas (8), (10), (22), (23) and (24) we can obtain the desired equation (9) at last. This completes our proof of the Main theorem. □

Remark 3. When $l = 2$, our Main Theorem implies Th.6 in Chap.IV of ref. [5].

Corollary 1. *Let L/k be a tame abelian extension of type $(l, l, \cdots, l)$ where l is a prime. Let $\{K_v : v \in \Phi\}$ is the set of all cyclic subfields of L. Then the ratio $h(O_L)/\prod_{v\in\Phi} h(O_{K_v})$ is an l-power.*

Proof. We only need to show that Q is an l-power, which readily follows from Proposition 2. □

Added Note. There is a gap in the proof of the Main Theorem. If K/k has constant field extension, then we need to replace u by u^l in formula (4). But since constant field extension is cyclic, there is only one cyclic constant field subextension of L of degree l in the Main Theorem if L contains a constant field extension. Then it is easy to see that formula (8) is also true.

References

[1] Hayes, D., *Trans. Amer. Math. Soc.* **189**(1974), 77.

[2] Weil, A., *Basic Number Theory*, Springer-Verlag, New York, 1968.

[3] Zhang, X., *Scientia Sinica (Series A)* **27**(10)1984, 1018.

[4] Hua, L.K., *Introduction to Number Theory*, Springer-Verlag, Berlin, Heidelberger, New York, 1982.

[5] Zhang, X., *Doctoral Thesis, University of Science and Technology of China*, 1985. (Chinese)