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

ZHAO Jianqiang (赵健强)**

(Department of Mathematics, University of Science and Technology of China, Hefei 230026, China)

Received January 6, 1994

Abstract Let $L/\mathbb{F}_q(T)$ be a tame abelian extension of type $(l, l, \cdots l)$. The ratio of the degree zero divisor class number (as well as the ideal class number) of L to the product of corresponding class numbers of all cyclic subfields of L is clearly determined.

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

Among the number theorists, there are incessant efforts to clarify the class groups and the class numbers of the algebraic number fields, which have presented a large quantity of unsolved problems. In algebraic function fields, concerning the same sort of problems, a lot of work has been done. Around 1974, Hayes[1] successfully established the reciprocity law over $k=\mathbb{F}_q(T)$, the rational function field of one variable over finite constant fields $\mathbb{F}_q$, where q is a power of a prime number p. In fact, he 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 $\mathrm{Gal}(L/k)\cong(\mathbb{Z}/l\mathbb{Z})^n$, 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 $\mathscr{D}_s$ be the group generated by the primes of K outside of S (thus $\mathscr{D}_s$ is the group of fractional ideals of K), and let $\mathscr{D}(K)$ $\mathscr{D}^0(K)$, $\mathscr{P}(K)$ and $\mathscr{P}_s$ be the groups generated by the divisors of K, the degree zero divisors of K, the principal divisor 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. Then, conventionally, $h(K)=|\mathscr{D}^0(K)/\mathscr{P}(K)|$ and $h(O_K)=|\mathscr{D}_s/\mathscr{P}_s|$ are called the class number of degree zero divisors and the ideal class number, respectively. Finally, we set

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

and the regulator

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

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

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

* This work was done at USTC when the author was a graduate student in a special program of Nankai University.

** Current address: Department of Mathematics, Brown University, Providence RI02912, USA.

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 $n \geqslant 2$ throughout this paper. Since constant field extensions are cyclic, it is easy to see that L/k is tame (i. e. all primes are tamely ramified) iff $l \neq p$, which we also assume unless we point out otherwise.

1 ζ-functions

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

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

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 the 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 $(l, \cdots, l)$, and let $\{K_v; v\in\Phi\}$ be 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 decomposion 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 $m_1, \cdots, m_n \in \mathbb{R} = m_n \in R=\mathbb{F}_q[T]$, such that $L=k(\sqrt[l]{m_1}, \cdots, \sqrt[l]{m_n})$. Let $R_1=\{a\in R\backslash\{0\}$: a has no l-th power factor in $R\backslash\mathbb{F}_q$ and the leading coefficient of a is γ^i for some i such that $0\leqslant i\leqslant l-1\}$. Then we can assume $m_i\in R_1$ without loss of generality. Define

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

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

$$(e_1, \cdots, e_n)\sim(f_1, \cdots, f_n)$$
$$\Leftrightarrow \exists\, i\in\{1, \cdots, l-1\} \text{ such that } e_j=if_j \pmod l \text{ for all } 1\leqslant j\leqslant n.$$

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

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

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

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

where $\rho:R\to(R/(P))=G$ is a 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 $\rho(m)$ as 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:

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

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, ramified) in them, then we condense this information by $\mathrm{Sp}(L, P)=1^a\eta^b0^c$.

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

Table 1

Type	$\left(\left(\frac{m_1}{P}\right), \left(\frac{m_2}{P}\right), \cdots, \left(\frac{m_n}{P}\right)\right)$	$\mathrm{Sp}(L, P)=\mathrm{Sp}(L', \mathfrak{p})$	$\log_l(g, e, f)$
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	$(0, \eta, 1, \cdots, 1)$	$1^{\tau_{n-2}}\eta^{l^{n-2}}0^{l^{n-1}}$	$(n-2, 1, 1)$

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, $g(\mathfrak{P}/P)=g(\mathfrak{P}'/\mathfrak{p})$, $f(\mathfrak{P}/P)=f(\mathfrak{P}'/\mathfrak{p})$ 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

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

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

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

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

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

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

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

By the proof of Proposition 1, we also have

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

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 $Q=(V(L):\prod_{v\in\Phi}V(K_v))$ be the unit index. Then*

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

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

Proof. If $n=1$, then we have nothing to prove since $Q=1$. Suppose $n\geqslant 2$, and σ_1, $\alpha_2\in \mathrm{Gal}(L/k)$ such that $\langle\sigma_1, \sigma_2\rangle\cong(\mathbb{Z}/l\mathbb{Z})^2$. Let L_l and L_i $(1\leqslant i\leqslant l-1)$ be the fixed fields of σ_1 and $\sigma_1^i\sigma_2$, respectively, and let E_i be the group of units of L_i $(1\leqslant i\leqslant l)$. For any units η of L, we have

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

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

$$ij+1\equiv i'j \pmod l.$$

Thus

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

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

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 $\eta\in V(L)$. Now, let L/k be an extension of n-fold of type $(l, l, \cdots, l)$. Then $\{L_i\colon 0\leqslant i\leqslant 1\}$ 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 $\{K_v\colon v\in\Phi\}$ 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 eq. (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, eq. (8) follows immediately. By eq.(3) this gives rise to

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

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 $g(\infty)$ is as in Propositon 2. Let $r=l^\lambda$, $r_0=\dfrac{r-1}{l-1}$, $r_1=r-1$, $L^+=L'^+\cap L$, Ω_λ and $P(\Omega_\lambda)$ as defined in (5) and (6). We may choose $v_1,\cdots,v_\lambda$ in Ω_λ as a set of representatives of projective space $P(\Omega_\lambda)$ such that $v_i=(0,\cdots,0,1,0,\cdots,0)$ with 1 at the i-th coordinate of $1\leqslant i\leqslant\lambda$. In the following we view $P_\lambda=\{v_i\in P(\Omega_\lambda):\ 1\leqslant i\leqslant r_0\}$ as an orderd set. For any $\alpha\in\mathfrak{S}=\{1,\cdots,l-1\}$ and $v=(e_1,\cdots,e_n)\in\Omega_\lambda$, we define $\alpha v=(e_1',\cdots,e_\lambda')\in\Omega_\lambda$ such that $e_i'\equiv\alpha e_i \pmod l$ for $1\leqslant i\leqslant\lambda$. 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 $l-1$.

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

Note that $\Omega^1=\Omega^2=\Omega_\lambda^\times$ 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 $\mathbb{F}_q$, $k'=k'(\xi)$ and $L'=k'(\sqrt[l]{m_1},\cdots,\sqrt[l]{m_\lambda})$. Let $\sigma_i'\in\mathrm{Gal}(L'^+/k)$, $1\leqslant i\leqslant\lambda$, such that

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

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

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

Now we 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

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

For any m_v defined as eq.(7), we see that $\sigma_u'(\sqrt[l]{m_v})=\xi^{u\cdot v}(\sqrt[l]{m_v})$, and $\sigma_u'(\xi)=\xi$. Set $\sigma_v=\sigma_v'|L^+\in\mathrm{Gal}(L^+/k)$. Then it is easy to check that $\mathrm{Gal}(L^+/k)=\langle\sigma_1\rangle\times\cdots\times\langle\sigma_\lambda\rangle$, and for any $v, v'\in\Omega$ such that $v\cdot u=v'\cdot u$ we have

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

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

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

Let $\{\eta_v: v\in\Omega^2\}$ be a system of fundamental units of L, and let $\{K_v: v\in P_\lambda\}$ 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 ∞, dividing ∞_1, we have $e(\infty_1/\mathfrak{p}_u)=e$. Denote the additive valuations corresponding to $\sigma_u^{-1}(\infty_1)$ $\sigma_u^{-1}(\infty_1)$ 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 eq. (2)) we have

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

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

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

Let

$$\mathscr{M}=[v_u(\sigma_u\varepsilon_v)]_{v\in\Omega^1,\, u\in\Omega^2}. \tag{14}$$

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

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

where we get the equation by carrying out the following operations on the first determinant: 1st row$\times(-1)+$other rows. Since $N_{K_0/k}(\varepsilon_u)=1$, adding all rows but the first, we get a row

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

In obtaining eq. (16), we use the following elementary result which can be found in reference [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 eq. (16) to $l^\lambda\times$(1st row) we can get

$$\det\mathscr{M}=A=l^{-\lambda}\det\mathscr{B},\quad \mathscr{B}=[\mathscr{R}_u^v-\mathscr{R}_u^0]_{u\cdot v\in P_\lambda}, \tag{17}$$

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

$$[(1-\delta_{0,u\cdot v})(\mathscr{R}_u-\mathscr{R}_u^0)]_{v\in R_\lambda}.$$

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

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

where

$$\mathscr{A}=[\delta_{u\cdot v,1}]_{u\in\Omega_\lambda^2,\ v\in\Omega^\lambda}.$$

Set $\mathscr{A}\mathscr{A}^t=(b_{u,v})$, where $\mathscr{A}^t$ is the transposition of $\mathscr{A}$. Then

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

If $u=v$, then $b_{u,v}=l^{\lambda-1}$ from Lemma 2. If $u=jv$ for some $j\in\mathfrak{S}$ and $j\neq1$, then $b_{u,v}=0$. When $\lambda=1$, $b_{u,v}=0$ for $u\neq v$. When $\lambda\geqslant2$, 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 $1\leqslant i,\ j\leqslant\lambda$ such that $e_if_j\not\equiv e_jf_i \pmod l$, and therefore $b_{u,v}=l^{\lambda-2}$ by an easy computation. Thus

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

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

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

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

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

From eqs. (13)—(21), we have

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

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

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

From eq. (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 eqs. (8), (18)—(20), we can obtain desired equation (9) at last. This completes our proof of Main Theorem.

Remark 3. When $l=2$, our Main Theorem is stated as in the author's another paper (Th. 6 of Chap. IV)[1)].

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

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

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

References

1 Hayes, D., *Trans. Amer. Math. Soc.*, 1974, 189: 77.
2 Weil, A., *Basic Number Theory*, New York: Springer-Verlag, 1968.
3 Zhang, X., On number fields of type $(l, l, \cdots, l)$, *Scientia Sinica*, Ser. A, 1984, 27(10): 1018.
4 Hua, L.-K., *Introduction to Number Theory*, Berlin: Springer-Verlag, 1982.

1) Zhang, X., Doctoral thesis, University of Science and Technology of China (in Chinese), 1985.