SCIENCE CHINA
Mathematics

• ARTICLES •

September 2010 Vol. 53 No. 9: 2447–2462
doi: 10.1007/s11425-010-4070-z

Class numbers of cyclic 2-extensions and Gross conjecture over $\mathbb{Q}$

Dedicated to Professor Wang Yuan on the Occasion of his 80th Birthday

OUYANG Yi* & XUE Hang

Department of Mathematics, University of Science and Technology of China, Hefei 230026, China
Email: yiouyang@ustc.edu.cn, xuehang@math.columbia.edu

Received December 28, 2009; accepted June 28, 2010; published online August 6, 2010

Abstract The Gross conjecture over $\mathbb{Q}$ was first claimed by Aoki in 1991. However, the original proof contains too many mistakes and false claims to be considered as a serious proof. This paper is an attempt to find a sound proof of the Gross conjecture under the outline of Aoki. We reduce the conjecture to an elementary conjecture concerning the class numbers of cyclic 2-extensions of $\mathbb{Q}$.

Keywords Gross conjecture, class number, cyclic 2-extension

MSC(2000): Primary 11S40; Secondary 11R29, 11R37

Citation: Ouyang Y, Xue H. Class numbers of cyclic 2-extensions and Gross conjecture over $\mathbb{Q}$. Sci China Math, 2010, 53(9): 2447–2462, doi: 10.1007/s11425-010-4070-z

1 Introduction

1.1 A conjecture about class numbers of cyclic 2-extensions

Let $m \not\equiv 2 \pmod 4$ be a fixed positive integer which is not a prime power. Let $n \geqslant 2$ be the number of prime factors of m. By a standard way, we shall construct a subfield $L = L_m$ of $\mathbb{Q}(\mu_m)$ which is a maximal cyclic 2-extension of $\mathbb{Q}$ such that all prime factors of m are totally ramified. Moreover, $L/\mathbb{Q}$ is of order 2^t, where

$$t = \begin{cases} \min\{\mathrm{ord}_2(p_i - 1): \ 1 \leqslant i \leqslant n\}, & \text{if } 2 \nmid m; \\ 1, & \text{if } 4 \parallel m; \\ \min\{t_1 - 2, \mathrm{ord}_2(p_i - 1): \ 2 \leqslant i \leqslant n\}, & \text{if } 8 \mid m. \end{cases} \tag{1.1}$$

We decompose $L/\mathbb{Q}$ into a tower of cyclic extensions of order 2: $\mathbb{Q} = E_0 \subset E_1 \subset \cdots \subset E_t = L$. Let C_i be the 2-part of the narrow class group of E_i and let $h_i = |C_i|$ be the 2-part of narrow ideal class number. By the class field theory, $N_{i,i-1} : C_{i-1} \to C_i$ is surjective. Let $h_i^* = h_i/h_{i-1}$. We shall show that $2^{n-1} \mid h_i^*$.

Our conjecture is

Conjecture 1.1. *Assume $t \geqslant 2$, i.e., m odd or $16 \mid m$ and $p \equiv 1 \pmod 4$ for all odd prime $p \mid m$. The following three conditions are equivalent.*

(1) $h_1 = 2^{n-1}$;

(2) $h_i^* = 2^{n-1}$ *for some* i;

(3) $h_i^* = 2^{n-1}$ *for all* i.

*Corresponding author

1.2 The conjecture implies the Gross conjecture over $\mathbb{Q}$

Our main result in this paper is

Theorem 1.2. *If Conjecture* 1.1 *is true, then the Gross conjecture over* $\mathbb{Q}$ *is also true.*

Remark. (1) Readers who are familiar with the Gross conjecture certainly know that the case over $\mathbb{Q}$ was claimed by Aoki [1] in 1991. However, in that paper, there were numerous serious or small mistakes, and there were also many false claims. It is to understand Aoki's paper that makes the authors to work on a more complete proof. The readers can see that there are many ideas in this paper coming from Aoki's paper and the authors just tried to make them mathematically correct, but there are also many more which were obtained by our own research. We are not yet successful in giving a complete proof following this line of Aoki. The remaining obstacle is the above conjecture.

(2) Certainly new proofs of the Gross conjecture over $\mathbb{Q}$ has been achieved by Burns [3] and Aoki [2].

2 The Gross conjecture

2.1 General facts

Let k be a global field and K be an abelian extension of k with Galois group G. Let S be a finite set of places of k which contains all archimedean places and all places which are ramified in K/k. Let $n = \#S - 1$. By the Dirichlet unit theorem, U_S, the set of S-units over k, is a finitely generated abelian group of rank n. We choose T, a finite set of primes disjoint from S, such that

$$U_{S,T} = \{x \in U_S \mid x \equiv 1 \pmod{\mathfrak{q}} \text{ for every } \mathfrak{q} \in T\}$$

is a free abelian group of rank n. Let $\{\varepsilon_1, \ldots, \varepsilon_n\}$ be a set of $\mathbb{Z}$-basis of $U_{S,T}$. Let Y be the free abelian group generated by S and let $X = \ker(Y \xrightarrow{\deg} \mathbb{Z})$. Then X is also a free abelian group of rank n. Choose a basis $\{x_1, x_2, \ldots, x_n\}$ of X over $\mathbb{Z}$.

Let $I = I_G$ be the augmentation ideal $\ker(\deg : \mathbb{Z}[G] \to \mathbb{Z})$. We note that $G \to I_G/I_G^2 : g \mapsto g - 1$ is an isomorphism. The Gross regulator map λ_G is defined to be the $\mathbb{Z}$-linear map

$$\lambda : U_{S,T} \to I/I^2 \otimes X, \quad \varepsilon \mapsto \sum_{v \in S} (r_v(\varepsilon) - 1) \otimes v,$$

where r_v is the reciprocity map from $k_v^\times$ to G. Using the above chosen basis $\{\varepsilon_1, \ldots, \varepsilon_n\}$ and $\{x_1, x_2, \ldots, x_n\}$, we obtain an $n \times n$ matrix (η_{ij}) of λ_G with entries in I/I^2. Set

$$\det\nolimits_G \lambda = \det(\eta_{ij}) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \eta_{1\sigma(1)} \cdots \eta_{n\sigma(n)} \in I^n/I^{n+1}. \tag{2.1}$$

The element $\det_G \lambda$ is unique up to a sign depending on the basis chosen. However, if k is a number field, we always have

$$2 \det\nolimits_G \lambda \equiv 0 \pmod{I^{n+1}}. \tag{2.2}$$

Indeed, for an archimedean place v, $r_v(\varepsilon)$ is either trivial or of order 2, which means $2(r_v(\varepsilon) - 1) = -(r_v(\varepsilon) - 1)^2 \in I^2$.

On the other hand, let $\operatorname{Pic}(\mathcal{O}_S)$ be the group of invertible $\mathcal{O}_S$-modules and $\operatorname{Pic}(\mathcal{O}_S)_T$ be the group of invertible $\mathcal{O}_S$-modules together with a trivialization at T. Then one has the exact sequence

$$1 \to U_{S,T} \to U \to \prod_{\mathfrak{q} \in T} F_{\mathfrak{q}}^* \to \operatorname{Pic}(\mathcal{O}_S)_T \to \operatorname{Pic}(\mathcal{O}_S) \to 1.$$

Set $h_S = \#\operatorname{Pic}(\mathcal{O}_S)$ and

$$h_{S,T} = \#\operatorname{Pic}(\mathcal{O}_S)_T = h_S \cdot \frac{\prod_{\mathfrak{q} \in T}(N\mathfrak{q} - 1)}{(U_S : U_{S,T})}. \tag{2.3}$$

For $\chi \in G^\vee$, the group of complex characters of G, one defines the Hecke L-function

$$L_{S,T}(S,\chi) = \prod_{\mathfrak{q}\in T}(1-\chi(\mathrm{Frob}_\mathfrak{q})N\mathfrak{q}^{1-s})\prod_{\mathfrak{p}\notin S}(1-\chi(\mathrm{Frob}_\mathfrak{p})N\mathfrak{p}^{-s})^{-1},$$

where $\mathrm{Frob}_\mathfrak{q}$ is the Frobenius substitution of $\mathfrak{q}$ in G. Under the assumption that $U_{S,T}$ is free, one can show that there exists a unique element $\theta_G \in \mathbb{Z}[G]$ such that $\chi(\theta_G) = L_{S,T}(\chi, 0)$ for all $\chi \in G^\vee$.

Conjecture 2.1 [7, Conjecture 4.1]. *Assume the above assumptions, then*

$$\theta_G \equiv \pm h_{S,T} \det\nolimits_G(\lambda) \pmod{I^{n+1}}. \tag{2.4}$$

From now on, we denote the above conjecture as $\mathrm{Gr}(K/k,S,T)$. We list some known results about $\mathrm{Gr}(K/k,S,T)$ here.

Gross [7] first proved the following results:

Proposition 2.2. *The conjecture* $\mathrm{Gr}(K/k,S,T)$ *is true if one of the following holds*:

(1) *S contains a complex place, or S contains only archimedean places*;

(2) *K/k is a quadratic extension.*

We also have the following well-known results:

Proposition 2.3. *Let K/k, S, T be given as above. Then*

(1) *If $\mathfrak{p},\mathfrak{q} \notin S\cup T$, then* $\mathrm{Gr}(K/k,S,T)$ *implies* $\mathrm{Gr}(K/k,S\cup\{\mathfrak{p}\},T)$ *and* $\mathrm{Gr}(K/k,S,T\cup\{\mathfrak{q}\})$.

(2) *If L is a sub-extension of K/k corresponding to the subgroup H of G (i.e.,* $\mathrm{Gal}(L/k)=G/H$*), then $\theta_{G/H}$ and* $\det_{G/H}\lambda$ *are the images of θ_G and* $\det_G\lambda$ *under the natural homomorphism* $\mathbb{Z}[G]\to\mathbb{Z}[G/H]$ *respectively. In particular,* $\mathrm{Gr}(K/k,S,T)$ *implies* $\mathrm{Gr}(L/k,S,T)$.

This immediately gives the following

Corollary 2.4. *In order to prove the Gross conjecture for a fixed base field k, it suffices to prove* $\mathrm{Gr}(K_\mathfrak{f}/k,S,T_0)$ *for all S, $\mathfrak{f}$ and T_0, where $\mathfrak{f}$ is the cycle*

$$\mathfrak{f} = \prod_{v\mid\infty} v \prod_{\substack{v\in S\\ v\nmid\infty}} v^{n_v}, \quad n_v \in \mathbb{Z}_{>0},$$

$K_\mathfrak{f}$ is the ray class field of k modulo $\mathfrak{f}$ and T_0 is a minimal non-empty set of primes such that U_{S,T_0} is free.

2.2 The case $k=\mathbb{Q}$

This paper is an attempt to show the Gross conjecture over $\mathbb{Q}$, i.e., $\mathrm{Gr}(K/\mathbb{Q},S,T)$ for all possible K, S and T.

By [12], we have

Proposition 2.5. *The Gross conjecture is true for $k=\mathbb{Q}$ and $n=1$.*

By Corollary 2.4, to prove the Gross conjecture over $\mathbb{Q}$, since the ray class field of the cycle $m\infty$ of $\mathbb{Q}$ is nothing but $\mathbb{Q}(\mu_m)$, we only need to prove $\mathrm{Gr}(K_m/\mathbb{Q},S_m,T)$, where

$$K_m=\mathbb{Q}(\mu_m), \quad S=S_m=\{\infty,p_1,\dots,p_n : p_i \mid m\}, \quad T=\{q\},$$

for every m which is not a prime power and $\mathrm{ord}_2(m)\neq 1$ and every odd prime integer q not dividing m. In this case,

$$U := U_S = \langle -1,p_1,\dots,p_n\rangle, \quad U_T := U_{S,T} = \{x\in U : x\equiv 1 \pmod q\}, \quad h := h_{S,T} = \frac{q-1}{(U:U_T)}.$$

Under the canonical isomorphism $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ which associates $\sigma_a : \zeta_m \mapsto \zeta_m^a$ with a, we know that

$$\theta_G = (1-\mathrm{Frob}_q)\sum_{\substack{a=1\\(a,m)=1}}^{m-1}\left\{\frac{a}{m}-\frac{1}{2}\right\}\sigma_a = (1-\mathrm{Frob}_q)\cdot\theta_m^*, \tag{2.5}$$

where θ_m^* is the involution of the Stickelberger element

$$\theta_m = \sum_{\substack{a=1\\(a,m)=1}}^{m-1} \left\{\frac{a}{m} - \frac{1}{2}\right\} \sigma_a^{-1}. \tag{2.6}$$

It is well known (and easy to check) that $\sigma_{-1}\theta_m = -\theta_m$. Thus if $\theta_G \in I^n$, we have

$$2\theta_G = (1-\sigma_{-1})\theta_G \in I^{n+1}. \tag{2.7}$$

Therefore,

Proposition 2.6. *If K is a totally real abelian extension of $\mathbb{Q}$, then* $\mathrm{Gr}(K/Q,S,T)$ *is always true.*

Proof. By (2.2), we have $\det_G \lambda = 0 \in I^n/I^{n+1}$. Let $K_m = \mathbb{Q}(\zeta_m)$ be the minimal cyclotomic field containing K, then $\theta_{K/Q}$ is the restriction of $\theta_{K_m/\mathbb{Q}}$. By (2.7), it must be 0. □

2.3 A key lemma

Suppose $n \geqslant 2$. Let G be a finite abelian group with a decomposition $G = G_1 \times G_2 \times \cdots \times G_n$ such that $G_i = \langle\sigma_i\rangle$ is a cyclic group with a generator σ_i for $2 \leqslant i \leqslant n$, and G_1 is either:

(a) a cyclic group with a generator σ_1; or

(b) $G_{11} \times G_{12}$, where G_{1j} are cyclic groups with generators σ_{1j}.

We now regard G_i, G_{1j} and products of them as both subgroups and quotient groups of G. We denote by $\psi_{G/H}$ the restriction of $\mathbb{Z}[G]$ to $\mathbb{Z}[G/H]$. In particular for $H = G_i$, we simply write the restriction ψ_{G/G_i} as ψ_i. Moreover, for $J \subseteq [n] := \{1,\ldots,n\}$, we denote by $G_J = \prod_{i\in J} G_i$ and by ψ_J the corresponding restriction map ψ_{G/G_J}.

Lemma 2.7. *Assumptions as above. If $\alpha \in I_G \subset \mathbb{Z}[G]$ such that $\psi(\alpha) \in I_{G/G_i}^{n+1}$ for every $1 \leqslant i \leqslant n$, then*

(1) *In Case* (a) (*i.e.* G_1 *cyclic*), $\alpha \equiv c(\sigma_1-1)\cdots(\sigma_n-1) \pmod{I_G^{n+1}}$, *where* $0 \leqslant c < \gcd(|G_1|,\ldots,|G_n|)$.

(2) *In Case* (b), *if moreover* $\psi_{G/G_{12}}(\alpha) \in I_{G/G_{12}}^{n+1}$, *then* $\alpha \equiv c(\sigma_{12}-1)\cdots(\sigma_n-1) \pmod{I_G^{n+1}}$, *where* $0 \leqslant c < \gcd(|G_{12}|,|G_2|,\ldots,|G_n|)$.

Proof. We only prove (2), (1) follows similarly, or one can refer to [9].

Note that for $g = \prod_i g_i \in G$ ($g_i \in G_i$), $g-1$ is the linear combination of products of the form $\prod_{i\in J}(g_i-1)$ for J a subset of $[n] = \{1,\ldots,n\}$. Moreover, g_1-1 is the linear combination of $g_{11}-1$, $g_{12}-1$ and $(g_{11}-1)(g_{12}-1)$. Now if $g_i = \sigma_i^t$ (resp., $g_{1j} = \sigma_{1j}^t$), then $g_i - 1 \equiv t(\sigma_i-1) \pmod{I_{G_i}^2}$ (resp., $g_{1j}-1 \equiv t(\sigma_{1j}-1) \pmod{I_{G_{1j}}^2}$), thus any $\alpha \in I_G$ can be expressed as

$$\alpha \equiv \sum_{e\in E} c_e(\sigma_{11}-1)^{e_{11}}(\sigma_{12}-1)^{e_{12}}(\sigma_2-1)^{e_2}\cdots(\sigma_n-1)^{e_n} \pmod{I_G^{n+1}},$$

where

$$E = \{(e_{11},e_{12},e_2,\ldots,e_n) \in \mathbb{Z}_{\geqslant 0}^{n+1} \mid e_{11}+e_{12}+e_2+\cdots+e_n \leqslant n\}.$$

For $e \in E$, we define

$$\operatorname{Supp} e = \{i \mid e_i > 0 \text{ or } e_{11}+e_{12} > 0 \text{ if } i = 1\}.$$

We denote

$$T_e = (\sigma_{11}-1)^{e_{11}}(\sigma_{12}-1)^{e_{12}}(\sigma_2-1)^{e_2}\cdots(\sigma_n-1)^{e_n}.$$

Then for $J \subseteq [n]$,

$$\alpha_J = \psi_J(\alpha) \equiv \sum_{e:\,\operatorname{Supp} e\cap J=\emptyset} c_eT_e \pmod{I_{G/G_J}^{n+1}}.$$

By the assumption, if J is a non-empty proper subset of $[n]$, $\alpha_J \in I_{G/G_J}^{n+1} \subset I_G^{n+1}$. Then by the inclusion-exclusion principle,

$$\alpha = \alpha_\emptyset \equiv \sum_{J\neq\emptyset}(-1)^{|J|-1}\alpha_J \equiv (-1)^{n-1}\alpha_{[n]} \pmod{I_G^{n+1}}.$$

However, $e_1 = (1, 0, 1, \dots, 1)$ and $e_2 = (0, 1, 1, \dots, 1)$ are the only $e \in E$ with support $[n]$. Thus

$$\alpha_{[n]} \equiv c_1T_{e_1} + c_2T_{e_2} \pmod{I_G^{n+1}}.$$

By assumping $\psi_{G/G_{12}}(\alpha) \in I^{n+1}_{G/G_{12}}$, then $c_1T_{e_1} \in I_G^{n+1}$, thus

$$\alpha \equiv c(\sigma_{121} - 1)(\sigma_2 - 1)\cdots(\sigma_n - 1) \pmod{I_G^{n+1}}.$$

Let $m_i = |G_i|$ (or $|G_{12}|$ if $i = 1$), and $m_0 = \gcd\{m_i\}$, then there exist integers l_i such that $\sum l_im_i = m_0$. Thus

$$m_0T_{e_2} = \sum_i l_im_iT_{e_2}.$$

Note that $m_i(\sigma_i - 1) \in I^2_{G_i}$, each term in the summand is inside I_G^{n+1}. Hence $m_0T_{e_2} \in I_G^{n+1}$. This finishes the proof of (2). □

2.4 Reduction to the cyclic 2-extension case

We now construct explicitly the field $L = L_m$ which was mentioned in Subsection 1.1.

Suppose $m = p_1^{t_1}\cdots p_n^{t_n}$ $(n \geqslant 2)$ and without loss of generality, we assume p_1 is minimal. We let G_i be the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_{p_i^{t_i}})/Q)$. Then $G_i \cong (\mathbb{Z}/p_i^{t_i}\mathbb{Z})^\times$ and $G = \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ is canonically isomorphic to $G_1 \times \cdots \times G_n$. For our purpose, we treat m in the following three cases.

(1) $2 \nmid m$, i.e. $p_1 > 2$;

(2) $4 \parallel m$, i.e. $p_1 = 2$, $t_1 = 2$;

(3) $8 \mid m$, i.e. $p_1 = 2$, $t_1 > 2$.

In Cases (1) and (2), G_i are cyclic and G satisfies Case (a) in Subsection 2.3; in Case (3), letting $G_{11} = \mathrm{Gal}(\mathbb{Q}(\mu_4)/\mathbb{Q})$ and $G_{12} = \mathrm{Gal}(\mathbb{Q}(\mu_{2^{t_1}})^+/\mathbb{Q}) \cong \mathbb{Z}/2^{t_1-2}\mathbb{Z}$, then G satisfies Case (b) in Subsection 2.3. Recall that

$$t = \begin{cases} \min\{\mathrm{ord}_2(p_i - 1):\ 1 \leqslant i \leqslant n\}, & \text{if } 2 \nmid m;\\ 1, & \text{if } 4 \parallel m;\\ \min\{t_1 - 2, \mathrm{ord}_2(p_i - 1):\ 2 \leqslant i \leqslant n\}, & \text{if } 8 \mid m.\end{cases}$$

Note that $|G_i| = p^{t_i-1}(p_i - 1)$ if $p_i \neq 2$ and $|G_1| = 2^{t_1-1}$, $G_{11} = 2$ and $G_{12} = 2^{t_1-2}$ if $p_1 = 2$. Then

$$\gcd(|G_1|, |G_2|, \dots, |G_n|) = \begin{cases} 2^tm', & \text{if } 2 \nmid m;\\ 2, & \text{if } 4 \parallel m,\end{cases} \tag{2.8}$$

where m' is an odd integer, and

$$\gcd(|G_{12}|, |G_2|, \dots, |G_n|) = 2^tm', \quad \text{if } 8 \mid m. \tag{2.9}$$

Pick a generator σ_i (or σ_{1j}) for every cyclic groups mentioned here. Let H and H' be the subgroups of G given by

$$H = \langle \sigma_i^{2^t},\ \sigma_i\sigma_{i'}^{-1} \mid 1 \leqslant i, i' \leqslant n\rangle, \quad H' = \langle \sigma_i^{2^tm'},\ \sigma_i\sigma_{i'}^{-1} \mid 1 \leqslant i, i' \leqslant n\rangle$$

if $2 \nmid m$, and by

$$H = H' = \langle \sigma_{11}, \sigma_{12}^{2^t}, \sigma_i^{2^t},\ \sigma_i\sigma_{i'}^{-1}, \sigma_i\sigma_{12}^{-1} \mid 1 \leqslant i, i' \leqslant n\rangle$$

if $4 \mid m$. Let $L = L_m$ (resp., $L' = L'_m$) be the corresponding field extension of H (resp., H') by Galois theory. Then $\mathrm{Gal}(L/\mathbb{Q}) = G/H$ (resp., $\mathrm{Gal}(L'/\mathbb{Q}) = G/H'$) is a cyclic subgroup of order 2^t (resp., $2^tm'$ with m' odd or $= 1$) with a generator σ (resp., σ') which is the image of all σ_i or σ_{12}. Moreover, the composite maps $G_i \to G \to G/H$ (resp., $G_{12} \to G \to G/H$) are all surjective, which means that

Lemma 2.8. *The finite primes p_i are totally ramified in $L_m/\mathbb{Q}$.*

Proof. Note that G_i is the inertia subgroup of p_i in $K/\mathbb{Q}$. Now the lemma follows from a more general fact:

If $K/L/k$ are Galois extensions, suppose that $\mathfrak{P}$ is a prime ideal in K and $\mathfrak{P} \cap \mathcal{O}_k = \mathfrak{p}$. If the inertia group $I(\mathfrak{P}/\mathfrak{p})$ maps to $\mathrm{Gal}(L/k)$ surjectively, then $\mathfrak{p}$ is totally ramified in L/k.

It is easy to see that L is a maximal cyclic 2-extension inside $K_m = \mathbb{Q}(\mu_m)$ such that all prime factors of m are totally ramified. □

Proposition 2.9. *To show the Gross conjecture for the base field* $\mathbb{Q}$*, it suffices to show the Gross conjecture* $\mathrm{Gr}(L_m/\mathbb{Q}, S_m, \{q\})$ *for all* L_m*.*

Proof. We need to show $\mathrm{Gr}(K_m/\mathbb{Q}, S_m, \{q\})$ for every $m \geqslant 3$ and $\mathrm{ord}_2(m) \neq 1$. We prove it by induction on m.

If $m = 3$, $\mathbb{Q}(\mu_3)/\mathbb{Q}$ is a quadratic extension, $\mathrm{Gr}(K_3/\mathbb{Q}, S_3, \{q\})$ is true by Gross (Proposition 2.2). Suppose $\mathrm{Gr}(K_{m_0}/\mathbb{Q}, S_{m_0}, \{q\})$ is true for all $m_0 < m$. Then for $\mathrm{Gr}(K_m)/\mathbb{Q}, S_m, \{q\})$, let $\alpha = \theta_G - h\det_G \lambda$. The case $n = 1$ is true by [12] (see Proposition 2.5). In other cases, by inductive hypothesis, $\psi_{G/G_i}(\alpha)$ (resp., $\psi_{G/G_{12}}(\alpha)$) satisfy the assumptions of the key Lemma 2.7, therefore,

$$\alpha \equiv c(\sigma_1 - 1) \cdots (\sigma_n - 1) \text{ (resp., } c(\sigma_{12} - 1) \cdots (\sigma_n - 1)) \pmod{I_G^{n+1}}$$

for some $0 \leqslant c < 2^t m'$. Then $\alpha_{L'} = \psi_{G/H'}(\alpha) = c(\sigma' - 1)^n \pmod{I_{G/H'}^{n+1}}$. Since both θ_G and $\det_G \lambda$ are killed by 2, $2\alpha_{L'} = 2c(\sigma' - 1)^n \in I_{G/H'}^{n+1}$. Note that G/H' is cyclic of order $2^t m'$, and $I_{G/H'}^n / I_{G/H'}^{n+1}$ is also cyclic of order $2^t m'$ generated by $(\sigma' - 1)^n$, which means either $c = 0$ or $c = 2^{t-1} m'$. Therefore, that $\mathrm{Gr}(L_m/\mathbb{Q}, S_m, \{q\})$ is true implies that $\alpha_L = \psi_{H/H'}(\alpha_{L'}) \equiv c(\sigma - 1)^n \in I_{G/H}^{n+1}$. Since $I_{G/H}^n / I_{G/H}^{n+1}$ is cyclic of order 2^t generated by $(\sigma - 1)^n$, c must be 0, which in turn implies that $\mathrm{Gr}(K_m/\mathbb{Q}, S_m, \{q\})$. □

Now by Proposition 2.2, the cases that $L_m/\mathbb{Q}$ is quadratic or L_m is totally real are automatically true. Thus we only need to consider that $t \geqslant 2$ and L is imaginary.

The rest of this paper is dedicate to the proof of the following theorem, which finishes the proof of our main Theorem 1.2.

Theorem 2.10. *If* $t \geqslant 2$ *and* L *is imaginary, then under Conjecture* 1.1, $\mathrm{Gr}(L/\mathbb{Q}, S_m, \{q\})$ *is always true.*

From now on, we drop the subscript m from our notations.

3 Class numbers and Gross regulators of cyclic 2-extensions

3.1 Class numbers of cyclic l-extensions

Suppose that l is a prime number. We start by reviewing some results of [6]. Suppose that K/F is a cyclic extension of order l. Let $G = \mathrm{Gal}(K/F) = \langle \sigma \rangle$ with σ a generator of G. Let $F' = F(\mu_l)$ and $K' = K(\mu_l)$. This is indicated in the following diagram.

$$\begin{tikzcd}
 & K' \arrow[d, no head] \\
K \arrow[ur, no head] \arrow[d, no head, "\langle\sigma\rangle"'] & F' \\
F \arrow[ur, no head] &
\end{tikzcd}$$

Let $I(K)$ be the group of fractional ideals of K and $\mathfrak{Cl}(K)$ be the *narrow* ideal class group of K. For a G-submodule C of $\mathfrak{Cl}(K)$, we take a G-submodule D of $I(K)$ satisfying the condition:

D generates C in $\mathfrak{Cl}(K)$, and $D \cap I(K) = D^{\sigma - 1}$.

For such data $(K/F, C, D)$, we define a subgroup Λ of $F^\times$ by

$$\Lambda = \{x \in F^\times : x \text{ is totally positive and } (x) = x\mathcal{O}_F \in N_{K/F}(D)\}.$$

Let $\mathrm{Ram}(K/F) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ be the set of prime ideals of F ramified in K. Assume $\mathfrak{p}_i$ is unramified in F'. Let $Y_0(K/F)$ be the free abelian group generated by $\mathrm{Ram}(K/F)$. For each place v of F, choose a place v' of F' lying above v. Then for any $x, y \in F'_{v'}$, the Hilbert norm residue symbol $(x, y)_{v'}$ is independent of the choice of v', thus we denote it by $(x, y)_v$ in the following. Now we define the *Gras map* ρ *with respect to* $(K/F, C, D)$ as follows:

$$\rho : \Lambda/\Lambda^l \longrightarrow \mu_l \otimes Y_0(K/F), \qquad x \longmapsto \sum_{i=1}^{r} (a, x)_{\mathfrak{p}_i} \otimes \mathfrak{p}_i,$$

where μ_l is the group of l-th roots of unity in F'.

Lemma 3.1. *Viewing* $\mu_l \otimes Y_0(K/F)$ *as an* r*-dimensional vector space over* $\mathbb{F}_l$, *then* $\dim_{\mathbb{F}_l} \mathrm{im}\rho \leqslant r - 1$.

Proof. Let x be an element of Λ. Then for infinite places v', $(a, x) = 1$ since $x \gg 0$. For the inert prime $\mathfrak{p}$, if $x \in \mathfrak{p}$, we have $x \in \mathfrak{p}^l$ since $(x) \in N_{K/F}(D)$. Thus $l \mid v_{\mathfrak{p}}(x)$. Since $K'_{\mathfrak{P}'}/F'_{\mathfrak{p}'}$ is unramified, we have $r_{\mathfrak{p}'}(x) = \mathrm{Frob}^{v_{\mathfrak{p}'}(x)}$, where Frob is the Frobenius substitution in $\mathrm{Gal}(K'_{\mathfrak{P}'}/F'_{\mathfrak{p}'})$. The fact $l \mid v_{\mathfrak{p}}(x)$ then means that $r_{\mathfrak{p}'}(x)$ is trivial, hence $(a, x)_{\mathfrak{p}_i} = (\sqrt[l]{a})^{r_{\mathfrak{p}'}(x) - 1} = 1$. If $\mathfrak{p}$ splits, we have $K'_{\mathfrak{P}'} = F'_{\mathfrak{p}'}$. Note that $K' = F'(\sqrt[l]{a})$, we conclude that $r_{\mathfrak{p}'}(x)$ is trivial. Hence $(a, x)_{\mathfrak{p}} = 1$. Thus by the product formula, we have

$$\prod_{i=1}^{r} (a, x)_{\mathfrak{p}_i}^{\delta_i} = 1, \tag{3.1}$$

where δ_i is the number of prime ideals of F' lying above $\mathfrak{p}_i$. Since δ_i is a divisor of $l - 1$, it is relatively prime to l. Thus (3.1) gives a nontrivial relation on the image of ρ. Hence the result follows. □

Theorem 3.2. *Notations being as above, let* $\widetilde{C} = \{\mathfrak{P} \in \mathfrak{Cl}(K) : \mathfrak{P}^{\sigma - 1} \in C\}$. *Then we have*

$$|\widetilde{C}/C| = \frac{|\mathfrak{Cl}(F)|}{|N_{K/F}C|} \cdot l^{r - 1 - \dim_{\mathbb{F}_l} \mathrm{im}\rho}.$$

Proof. For the proof, see [6, Theorem 4.3]. □

In the following, we shall assume that $N_{K/F}(D)$ contains all $\mathfrak{p}_i$. Denote

$$U_0 := \{x \in F^{\times} : x \gg 0 \text{ and } \mathrm{ord}_{\mathfrak{p}}(x) = 0 \text{ for any } \mathfrak{p} \notin \mathrm{Ram}(K/F)\}.$$

Under the above assumption, U_0 is a subgroup of Λ. Let $S = \mathrm{Ram}(K/F) \cup M_{F,\infty}$, where $M_{F,\infty}$ is the set of infinite places of F. Let U be the group of S-units of F. Then we can consider the Gross regulator map λ_G. Define the *finite part* of λ_G as follows,

$$\begin{aligned} \lambda_{G,0} : U_0 &\longrightarrow G \otimes Y_0(K/F) \\ u &\longmapsto \sum_{i=1}^{r} r_{\mathfrak{p}_i}(u) \otimes \mathfrak{p}_i. \end{aligned}$$

Now we have a diagram

$$\begin{tikzcd} U_0 \arrow[r, "\lambda_{G,0}"] \arrow[d] & G \otimes Y_0(K/F) \arrow[d, "\xi"] \\ \Lambda/\Lambda^l \arrow[r, "\rho"] & \mu_l \otimes Y_0(K/F). \end{tikzcd}$$

The left vertical arrow is induced by the inclusion $U_0 \hookrightarrow \Lambda$, and the right is an isomorphism

$$\xi : G \otimes Y_0(K/F) \rightarrow \mu_l \otimes Y_0(K/F)$$

given by

$$\sum_{i=1}^{r} \sigma_i \otimes \mathfrak{p}_i \longmapsto \sum_{i=1}^{r} (\sqrt[l]{a}^{\,\sigma_i - 1})^{(l-1)/\delta_i} \otimes \mathfrak{p}_i.$$

Lemma 3.3. *The diagram above is commutative.*

Proof. Take an element u of U_0. Then the composition of $\lambda_{G,0}$ and ξ send it to

$$\sum_{i=1}^{r}(\sqrt[l]{a}^{\,r_{\mathfrak{p}_i}(u)-1})^{(l-1)/\delta_i}\otimes\mathfrak{p}_i,$$

and ρ sends it to $\sum_{i=1}^{r}(\sqrt[l]{a}^{\,r_{\mathfrak{p}'_i}(u)-1})\otimes\mathfrak{p}_i$. Class field theory gives us the following commutative diagram,

$$\begin{tikzcd}
F'_{\mathfrak{p}'_i} \arrow[r, hook] \arrow[d, "\text{norm}"] & J_{F'} \arrow[r] \arrow[d, "\text{norm}"] & \mathrm{Gal}(K'/F') \arrow[d, "\text{res}"] \\
F_{\mathfrak{p}} \arrow[r, hook] & J_F \arrow[r] & \mathrm{Gal}(K/F).
\end{tikzcd}$$

Therefore, $r_{\mathfrak{p}'_i}(u)=r_{\mathfrak{p}_i}(u)^{(l-1)/\delta_i}$. To simplify notations we denote $x=\sqrt[l]{a}$, $\sigma=r_{\mathfrak{p}_i}(u)$, $\zeta=x^{\sigma}/x$ for the moment. Note that ζ is a root of unity in $F'_{\mathfrak{p}}$, hence is σ-invariant. So one deduces $x^{\sigma^n}=\zeta^n x$ via elementary calculations. The result then follows. □

We shall need the following proposition.

Proposition 3.4. *Let D be the subgroup of $I(K)$ generated by $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$ and V be its image in $\mathfrak{Cl}(K)$. Suppose $N_{K/F}(V)$ equals the l-part of $\mathfrak{Cl}(F)$. Then V equals the l-part of $\mathfrak{Cl}(K)$ if and only if $\dim_{\mathbb{F}_l}\mathrm{im}\rho=r-1$, where ρ is the Gras map with respect to $(K/F,V,D)$.*

To prove this proposition, we need a lemma.

Lemma 3.5. *Let Γ be a cyclic group of order l with a generator γ. Let M be an abelian l-group with the structure of Γ-module, and let N be a Γ-submodule of M of finite index. Let $\widetilde{N}=\{x\in M: x^{\gamma-1}\in M\}$. Then $\widetilde{N}=N$ if and only if $M=N$.*

Proof. By definition we have $\widetilde{N}/N=(M/N)^{\Gamma}=\{x\in(M/N): x^{\gamma}=x \text{ for all } \gamma\in\Gamma\}$. If $M\neq N$, then M/N is an l-set with an action of Γ. The length of its Γ-orbit is either l or 1, thus the number of orbits of length 1, which is nothing but the order of $\widetilde{N}/N$, must be a multiple of l. In particular, $\widetilde{N}\neq N$. □

Proof of Proposition 3.4. By Theorem 3.2, we have

$$|\widetilde{V}/V|=l^{r-1-\dim_{\mathbb{F}_l}\mathrm{im}\rho}.$$

Therefore, $\widetilde{V}=V$ if and only if $\dim_{\mathbb{F}_l}\mathrm{im}\rho=r-1$. Now the result follows from the above lemma. □

3.2 Class numbers of cyclic 2-extensions over $\mathbb{Q}$

What we need for the Gross conjecture is the case $l=2$, $K=\mathbb{Q}$. We have $U=\langle -1,p_1,\ldots,p_n\rangle$, $U_0=\langle p_1,\ldots,p_n\rangle$. Recall that we have constructed a cyclic extension L of $\mathbb{Q}$ with Galois group $G=\mathbb{Z}/2^t\mathbb{Z}$ and all primes in $S=\{p_1,\ldots,p_n\}$ totally ramified. We can decompose the extension $L/\mathbb{Q}$ into a tower of cyclic extensions of order 2:

$$E_0(=\mathbb{Q})\subset E_1\subset\cdots\subset E_{t-1}\subset E_t\,(=L).$$

Moreover, since $t\geqslant 2$ and L is imaginary, we have $E_{t-1}=L^+$, the maximal real subfield of L and $E_1=\mathbb{Q}(\sqrt{m^*})$, where

$$m^*=\prod_{p\mid m}p=p_1\cdots p_n.$$

Let $G_i=\mathrm{Gal}(E_i/\mathbb{Q})$, $G_i=\mathbb{Z}/2^i\mathbb{Z}$. Denote the 2-part of the narrow class group of E_i by C_i. Since the prime $p\in S$ is totally ramified in L, by the class field theory we have C_{i+1} maps onto C_i, and the dual group $C_i^{\vee}$ embeds in $C_{i+1}^{\vee}$.

Consider the narrow genus group $\mathfrak{G}_+(E_i/\mathbb{Q})$ of $E_i/\mathbb{Q}$. Let $V_i = \mathfrak{G}_+(E_i/\mathbb{Q})^\vee$. Denote by $\phi(E_i/\mathbb{Q})$ the character group of $\mathrm{Gal}(E_i/\mathbb{Q})$ or of $C(\mathbb{Q})/N_{E_i/\mathbb{Q}}(C(E_i))$, and by $\phi_+^*(E_i/\mathbb{Q})$ the group

$$\phi_+^*(E_i/\mathbb{Q}) = \{\phi \in C(\mathbb{Q})^+ : N_{E_i/\mathbb{Q}}^\vee \phi \text{ is unramified at all finite primes}\},$$

where $C(\mathbb{Q})^+$ is torsion subgroup of $C(\mathbb{Q})^\vee$. Then V_i fits into an exact sequence (cf. [4, p. 15])

$$0 \longrightarrow \phi(E_i/\mathbb{Q}) \longrightarrow \phi_+^*(E_i/\mathbb{Q}) \longrightarrow V_i \longrightarrow 0. \tag{3.2}$$

By the genus theory, we have $\phi(E_i/\mathbb{Q}) \simeq \mathbb{Z}/2^i\mathbb{Z}$ and $\phi_+^*(E_i/\mathbb{Q}) \simeq (\mathbb{Z}/2^i\mathbb{Z})^n$. For each i, we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/2^{i-1}\mathbb{Z} \arrow[r] \arrow[d, "\times l"] & (\mathbb{Z}/2^{i-1}\mathbb{Z})^n \arrow[r] \arrow[d, "\times l"] & V_{i-1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{Z}/2^i\mathbb{Z} \arrow[r] & (\mathbb{Z}/2^i\mathbb{Z})^n \arrow[r] & V_i \arrow[r] & 0,
\end{tikzcd}$$

which shows that $V_i/V_{i-1} \simeq (\mathbb{Z}/2\mathbb{Z})^{n-1}$.

Let $h_i^* = \left|C_i^\vee/C_{i-1}^\vee\right| = |C_i|\,/\,|C_{i-1}|$. In particular, $h_t^* = h_L^- = h_L/h_L^+$. We have

Proposition 3.6. $2^{n-1} \mid h_i^*$ *for any* i, *and* $h_i^* = 2^{n-1}$ *if and only if* $V_iC_{i-1}^\vee = C_i^\vee$.

Proof. We first have $C_i^\vee \supset V_iC_{i-1}^\vee$, and

$$V_iC_{i-1}^\vee/C_{i-1}^\vee \simeq V_i/V_i \cap C_{i-1}^\vee = V_i/V_{i-1} \simeq (\mathbb{Z}/2\mathbb{Z})^{n-1}.$$

The result then follows. □

One natural question is whether h_i^* is divisible by a higher power of 2. The following proposition shows that h_1^* plays a deciding role in the divisibility of h_i^* by a high power of 2. For each $i = 1, \dots, t$, let D_i be the subgroup of $I(E_i)$ generated by the prime ideals of E_i dividing m and $\mathcal{C}_i$ be the image of D_i in $\mathfrak{Cl}(E_i)$. Let θ_i be the composition of obvious maps $\mathcal{C}_i \to C_i \to \mathfrak{G}_i$. Then we have

Proposition 3.7. *If* $h_1^* = 2^{n-1}$, *then* $h_i^* = 2^{n-1}$, *and the composite* θ_i *is an isomorphism for all* i.

In order to prove this proposition, we need some preparation. First note that for each $i = 0, \dots, t-1$, $N_{E_i/E_{i-1}}(D_i)$ contains all primes in $\mathrm{Ram}(E_i/E_{i-1})$. Let

$$\Lambda_i = \{x \in E_i^\times : x \gg 0 \text{ and } \mathrm{ord}_\mathfrak{p}(x) = 0 \text{ for any } \mathfrak{p} \notin \mathrm{Ram}(E_i/E_{i-1})\}.$$

It is obvious that $U_0 = \Lambda_0$. Let $\rho_i : \Lambda_{i-1}/\Lambda_{i-1}^l \longrightarrow \langle\pm1\rangle \otimes Y_0(E_i/E_{i-1})$ be the Gras map with respect to $(E_i/E_{i-1}, \mathcal{C}_i, D_i)$.

Lemma 3.8. *Let* $r_i = \dim_{\mathbb{F}_2} \mathrm{im}\rho_i$. *Then* $r_1 \leqslant r_2 \leqslant \cdots \leqslant r_t \leqslant n-1$. *In particular, if* $r_1 = n-1$, *then* $r_i = n-1$ *for* $i = 1, \dots, t$.

Proof. We first study the generator of E_i over E_{i-1}. We have $E_t = E_{t-1}(\sqrt{a})$ for some $a \in E_{t-1} \setminus E_{t-1}^2$. One can see that $E_t = \mathbb{Q}(\sqrt{a})$. In fact, $\{E_i : i = 0, \dots, t-1\}$ are the only proper subfields of L. If $E_i = \mathbb{Q}(\sqrt{a})$ for some $i \in \{i = 1, \dots, t-1\}$, we must have $a \in E_{t-1}$, a contradiction to the choice of a.

Let $a_i = N_{E_{t-1}/E_i(a)}$ for all i, we claim that $E_{i+1} = E_i(\sqrt{a_i})$. For $i = t-2$, $\mathrm{Gal}(E_t/E_{t-2}) = \{1, \tau, \tau^2, \tau^3\}, \mathrm{Gal}(E_t/E_{t-1}) = \{1, \tau^2\}$ and $\mathrm{Gal}(E_{t-1}/E_{t-2}) = \{1, \tau|_{E_{t-1}}\}$. We have $N_{E_{t-1}/E_{t-2}}(a) = a^{1+\tau} \in E_{t-2}$. Thus $(E_{t-2}(\sqrt{a}^{1+\tau}) : E_{t-2}) = 1$ or 2. If $\sqrt{a}^{1+\tau} \in E_{t-2}$, we have $(\sqrt{a}^{1+\tau})^\tau = \sqrt{a}^{1+\tau}$, which shows that $\sqrt{a} = \sqrt{a}^{\tau^2}$, so $\sqrt{a} \in E_{t-1}$. A contradiction. Thus $E_{t-1} = E_{t-2}(\sqrt{a_{t-2}})$. For general $i < t$, our claim follows from a simple induction.

For a fixed i, let $\mathfrak{p}$ (resp., $\mathfrak{P}$) denote the unique prime ideal of E_i (resp., E_{i+1}) above a prime factor of m. We have $(x, y)_\mathfrak{P} = (N_{E_{i+1}/E_i}(x), y)_\mathfrak{p}$ for any $x \in E_{i+1}$ and $y \in E_i$. This induces the following commutative diagram,

$$\begin{tikzcd}
\Lambda_{i-1}/\Lambda_{i-1}^2 \arrow[r, "\rho_i"] \arrow[d] & \langle\pm1\rangle \otimes Y_0(E_i/E_{i-1}) \arrow[d, "1\otimes f_i"] \\
\Lambda_i/\Lambda_i^2 \arrow[r, "\rho_{i+1}"] & \langle\pm1\rangle \otimes Y_0(E_{i+1}/E_i),
\end{tikzcd}$$

where the left vertical map is the natural one and f_i is the inverse of the isomorphism induced by the norm map from E_i to E_{i-1}. The equality $r_i \leqslant r_{i+1}$ is clear from the above commutative diagram. □

Proof of Proposition 3.7. First note that $E_1/\mathbb{Q}$ is quadratic, therefore, $|\mathcal{C}_1| = 2^{n-1}$ is always true (Theorem 39 and its corollary of [5]). By Proposition 3.6, if $h_1^* = 2^{n-1}$, then $|C_1| = 2^{n-1}$ and $V_1 = C_1^{\vee}$. Thus $C_1 \simeq \mathfrak{G}_1 \simeq \mathcal{C}_1$. Then by Proposition 3.4, $r_1 = n-1$. Thus by the previous lemma, we have $r_i = n-1$ for all i. Hence $\mathcal{C}_i = C_i$ for all i by Proposition 3.4 once more. By definition, $\mathfrak{G}_i = C_i/C_i^{1-\sigma_i}$. However, $\mathcal{C}_i = C_i$ is σ_i-invariant. Therefore, $\mathcal{C}_i = \mathfrak{G}_i$ and the result follows from Proposition 3.6. □

Now Conjecture 1.1 is just a generalization of Proposition 3.7, which claims that under our assumption of m, the divisibility of h_1 is equivalent to that of h_i^* for $L = L_m$.

3.3 Gross regulators of 2-cyclic extensions

We define α_i by the following commutative diagram,

$$\begin{tikzcd}
U_0 \arrow[rr, "\lambda_{G,0}"] \arrow[dr] & & G_i \otimes X_0. \\
& U_0/U_0^{2^i} \arrow[ur, "\alpha_i"'] &
\end{tikzcd}$$

Proposition 3.9. *α_i is surjective for all i if and only if α_1 is surjective.*

Proof. Assume α_1 is surjective. We first have the following commutative diagram,

$$\begin{tikzcd}
0 \arrow[r] & \ker\alpha_i \arrow[r] \arrow[d] & U_0/U_0^{2^i} \arrow[r] \arrow[d] & \operatorname{im}\alpha_i \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \ker\alpha_1 \arrow[r] & U_0/U_0^{2} \arrow[r] & G_1 \otimes X_0 \arrow[r] & 0.
\end{tikzcd}$$

By adding the kernels and cokernels, we have a larger diagram,

$$\begin{tikzcd}
& 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
& A \arrow[r] \arrow[d] & (2\mathbb{Z}/2^i\mathbb{Z})^n \arrow[r] \arrow[d] & C \arrow[d] & \\
0 \arrow[r] & \ker\alpha_i \arrow[r] \arrow[d] & U_0/U_0^{2^i} \arrow[r] \arrow[d] & \operatorname{im}\alpha_i \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \ker\alpha_1 \arrow[r] \arrow[d] & U_0/U_0^{2} \arrow[r] \arrow[d] & G_1 \otimes X_0 \arrow[r] & 0. \\
& D \arrow[d] & 0 & & \\
& 0 & & &
\end{tikzcd}$$

By the snake lemma, we have

$$\dim A + \dim C = \dim D + (i-1)n. \tag{3.3}$$

Here by dim, we mean the 2-power of the order of each group. On the other hand, by the exactness of the left vertical sequence, we have

$$\dim A + \dim\ker\ \alpha_1 = \dim \alpha_i + \dim D. \tag{3.4}$$

Combining (3.3) and (3.4), we have

$$\dim C + \dim \ker \alpha_i = (i-1)n + 1. \tag{3.5}$$

By the exactness of the right vertical sequence, we also have

$$\dim C + (n-1) \geqslant \dim \operatorname{im} \alpha_i, \tag{3.6}$$

and the equality holds if and only if $\operatorname{im}\alpha_i$ maps onto $G_1 \otimes X_0$. Therefore, summarizing all above we have

$$in = \dim \ker \alpha_i + \dim \operatorname{im} \alpha_i \leqslant \dim \ker \alpha_i + \dim C + (n-1) = in,$$

which yields $\dim C + (n-1) = \dim \operatorname{im} \alpha_i$. Therefore, $\operatorname{im}\alpha_i$ maps onto $G_1 \otimes X_0$, which means that $\operatorname{im}\alpha_i \to G_i \otimes X_0 \to G_1 \otimes X_0$ is onto. This shows that for each $\mathbb{Z}/2^i\mathbb{Z}$-component of $G_i \otimes X_0$ (as a free $\mathbb{Z}/2^i\mathbb{Z}$-module of rank n), a generator of it is contained in $\operatorname{im}\alpha_i$. Therefore, $\operatorname{im}\alpha_i = G_i \otimes X_0$.

Proposition 3.10. *Assuming Conjecture* 1.1*, then $h_i^* = 2^{n-1}$ if and only if α_i is surjective.*

Proof. Because of Conjecture 1.1 and Proposition 3.9, it suffices to prove the case $i = 1$. We have the following commutative diagram,

$$\begin{tikzcd}
U_0/U_0^2 \arrow[r, "\alpha_1"] \arrow[d, equal] & G_1 \otimes X_0 \arrow[d, "\xi"] \\
\Lambda_0/\Lambda_0^2 \arrow[r, "\rho_1"] & \langle \pm 1 \rangle \otimes Y_0.
\end{tikzcd}$$

It follows that α_1 is surjective if and only if $\dim_{\mathbb{F}_2} \operatorname{im}\rho_1 = n-1$. This is equivalent to $V_1 = C_1^\vee$, hence $h_1^* = 2^{n-1}$.

Note that $U/U^{2^i} = \langle \pm 1 \rangle \times U_0/U_0^{2^i}$. We define $\widetilde{\alpha_i}$ by the following commutative diagram,

$$\begin{tikzcd}
U \arrow[rr, "\lambda_{G_i}"] \arrow[dr] & & G_i \otimes X. \\
& U/U^{2^i} \arrow[ur, "\widetilde{\alpha_i}"'] &
\end{tikzcd}$$

Note that $\lambda_{G_i}(-1) \neq 0$ by the local class field theory. The image of $\widetilde{\alpha_i}$ is contained in the group generated by $\lambda_{G_i}(-1)$ and $G_i \otimes X_0$ in $G_i \otimes X$. Denote this group by Γ_i. Note that the restriction of $\widetilde{\alpha_i}$ to $U_0/U_0^{2^i}$ is α_i. We have the following commutative diagram,

$$\begin{tikzcd}
1 \arrow[r] & U_0/U_0^{2^i} \arrow[r] \arrow[d, "\alpha_i"] & U/U^{2^i} \arrow[r] \arrow[d, "\widetilde{\alpha_i}"] & \langle \pm 1 \rangle \arrow[r] \arrow[d, "\simeq"] & 1 \\
1 \arrow[r] & G_i \otimes X_0 \arrow[r] & \Gamma_i \arrow[r] & \langle \lambda_{G_i}(-1) \rangle \arrow[r] & 1,
\end{tikzcd}$$

where the horizontal rows are exact. Then the surjectivity of $\widetilde{\alpha_i}$ is equivalent to that of α_i by the snake lemma. The following proposition is nothing but Proposition 3.10.

Proposition 3.11. *Assuming Conjecture* 1.1*, then h_i^* is exactly divisible by 2^{n-1} if and only if $\operatorname{im}(\widetilde{\alpha_i}) = \Gamma_i$.*

Take $T = \{q\}$ for q an odd prime number not in S and consider the following diagram,

$$\begin{tikzcd}
U_q/U_q^{2^i} \arrow[rr, "\gamma_i"] \arrow[dr, "\beta_i"'] & & U/U^{2^i} \arrow[r] \arrow[dl, "\widetilde{\alpha_i}"] & \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^{2^i}, \\
& \Gamma_i & &
\end{tikzcd} \tag{3.7}$$

where γ_i is induced by the inclusion $U_q \hookrightarrow U$ and $\beta_i = \widetilde{\alpha}_i \circ \gamma_i$. Note that the upper row of the diagram is exact. U_q is a free abelian group of rank n, hence $U_q/U_q^{2^i} \simeq (\mathbb{Z}/2^i\mathbb{Z})^n$. But Γ_i is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^i\mathbb{Z})^{n-1}$. Therefore, β_i can be regarded as an endomorphism of $(\mathbb{Z}/2^i\mathbb{Z})^n$ whose determinant is either 0 or 2^{i-1} and $\det \beta_i = 2^{i-1}$ exactly when β_i is surjective. We have the following commutative diagram,

$$\begin{tikzcd}
U_q \arrow[rr, "\lambda_G|_{U_q}"] \arrow[dr] & & \Gamma_i, \\
& U_q/U_q^{2^i} \arrow[ur, "\beta_i"'] &
\end{tikzcd}$$

hence the following proposition.

Proposition 3.12. $\det_{G_i} \lambda \neq 0$ *if and only if* β_i *is surjective.*

Recall $m^* = \prod_{p|m} p$ and $E_1 = \mathbb{Q}(\sqrt{m^*})$. The following proposition connects the relative class number of E_i and the Gross regulator.

Proposition 3.13. (1) *If* $(\frac{m^*}{q}) = 1$*, then* $\det_{G_i} \lambda = 0$.

(2) *If* $(\frac{m^*}{q}) = -1$*, assuming Conjecture* 1.1*, then* $\det_{G_i} \lambda \neq 0$ *if and only if* $2^{n-1} \parallel h_i^*$.

Proof. First of all we claim that

$$m^*U^2/U^2 \subset \ker \alpha_1. \tag{3.8}$$

For the quadratic field $E_1 = \mathbb{Q}(\sqrt{m^*})$, $r_v(u) = 1$ if and only if $(m^*, u)_v = 1$. If $p \neq 2$, then

$$(m^*, m^*)_p = (m^*, -1)_p = \left(\frac{-1}{p}\right) = 1;$$

if $p = 2$, then

$$(m^*, m^*)_2 = (-1)^{((m^*/2-1)/2)^2} = 1;$$

and $(m^*, m^*)_\infty = 1$ since m is positive. Thus we obtain (3.8).

For (1), first consider the case $i = 1$. We have to show that β_1 is not surjective. Note that $|U_q/U_q^2| = |\Gamma_1|$, it suffices to show that β_1 is not injective. By hypothesis, $(\frac{m^*}{q}) = 1$, hence $m^* \in (\mathbb{F}_q^\times)^2$. But the upper row of diagram (3.7) is exact, there is an element $x \neq 1$ of U_q/U_q^2, such that $\gamma_1(x) = m^*U^2/U^2$. This shows $\beta_1(x) = \alpha_1 \circ \gamma_1(x) = 1$. In particular β_1 is not injective.

For general i, consider the following commutative diagram,

$$\begin{tikzcd}
U_q/U_q^{2^i} \arrow[r] \arrow[d, "\beta_i"'] & U_q/U_q^2 \arrow[d, "\beta_1"] \\
\Gamma_i \arrow[r] & \Gamma_1,
\end{tikzcd}$$

where the upper and lower maps are surjective. Therefore, that β_1 is not surjective implies that β_i is not surjective, hence $\det_{G_i} \lambda = 0$.

Now we show (2). The assumption $(\frac{m^*}{q}) = -1$ implies that there exist some $p \mid m^*$ such that $(\frac{p}{q}) = -1$. Let $U_q^+ = \{a \in U_q : a > 0\}$. Then $U_q^+ \neq U_q$, since $-p^{(q-1)/2} \in U_q \backslash U_q^+$. Take $a \in U_q$ which generates U_q/U_q^+. Let $\beta_i^+ := \beta \mid_{U_q^+/U_q^{2^i}}$. Then the following diagram shows that β_i being surjective is equivalent to β_i^+ being surjective.

$$\begin{tikzcd}
1 \arrow[r] & U_q^+/U_0^{2^i} \arrow[r] \arrow[d, "\beta_i^+"] & U_q/U_q^{2^i} \arrow[r] \arrow[d, "\beta"] & \langle a \rangle/\langle a^2 \rangle \arrow[r] \arrow[d, "\simeq"] & 1 \\
1 \arrow[r] & G_i \otimes X_0 \arrow[r] & \Gamma_i \arrow[r] & \langle \lambda_{G_i}(-1) \rangle \arrow[r] & 1.
\end{tikzcd}$$

We have the following commutative diagram,

$$\begin{tikzcd}
U_q^+/U_q^{2^i} \arrow[rr, "\gamma_i"] \arrow[dr, "\beta_i^+"'] & & U_0/U_0^{2^i} \arrow[dl, "\alpha_i"] \\
& G_i \otimes X_0. &
\end{tikzcd}$$

By Proposition 3.10, to show (2), it suffices to show that β_i^+ being surjective is equivalent to α_i being surjective. Obviously, β_i^+ being surjective implies that α_i is surjective. Conversely we first consider the case $i = 1$. This time γ_1 is injective, because

$$U_q^+ \cap U_0^2 = U_q^2. \tag{3.9}$$

In fact, if $x^2 \in U_q^+$, then $x^2 \equiv 1 \pmod q$, hence either x or $-x$ lies in U_q, which shows $U_q^+ \cap U_0^2 \subset U_q^2$. The reverse inclusion is obvious. Hence the identity (3.9) holds, and γ_1 is injective. Note that $m^* U^2/U^2 \in \ker \alpha_1$, $m^* \notin U_0^2$. But $\left|U_0/U_0^2\right| = 2^n$ and $|G_1 \otimes X_0| = 2^{n-1}$, $\ker \alpha_1$ contains only two elements because α_1 is surjective. Therefore, $\ker \alpha_1$ is generated by $m^* U^2/U^2$. Moreover, $(\frac{m^*}{q}) = -1$, $m^* \notin U_q^+$. Hence $\ker \alpha_1 \cap \operatorname{im} \gamma_1 = \{1\}$. Therefore, β_1^+ is surjective.

For general i, consider the following diagram,

$$\begin{tikzcd}
1 \arrow[r] & \ker \beta_i^+ \arrow[r] \arrow[d] & U_q^+/U_q^{2^i} \arrow[r] \arrow[d] & \operatorname{im} \beta_i^+ \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \ker \beta_1^+ \arrow[r] & U_q^+/U_q^2 \arrow[r] & G_1 \otimes X_0 \arrow[r] & 1.
\end{tikzcd}$$

By exactly the same method as in the proof of Proposition 3.9 one can show $\operatorname{im} \beta_i^+ = G_i \otimes X_0$, thus β_i^+ is also surjective. □

4 θ_G and class number

4.1 Sinnott's index formula

In this subsection, we review several results concerning the index formula of Sinnott about the Stickelberger ideal in an imaginary abelian field. The readers can refer to [10] for the proof.

Let K be an imaginary abelian field, $G = \mathrm{Gal}(K/\mathbb{Q})$, $R = \mathbb{Z}[G]$. Let τ be the complex conjugation in G and $e^- = (1-\tau)/2$. Let w be the number of roots of unity in K.

We first recall the definition and some properties of generalized index. Let V be a subspace of $\mathbb{Q}[G]$, A and B be two lattices in V of the same rank. Then there is a linear transformation ϕ of V, such that $\phi(A) = B$. Define

$$(A : B) = |\det(\phi)|. \tag{4.1}$$

We have a series of lemmas about the generalized index.

Lemma 4.1. *Let A, B, C be three lattices in V of the same rank. Then*

(1) $(A : C) = (A : B)(B : C)$;

(2) If $A \supset B$, then $(A : B) = [A : B]$.

Lemma 4.2. *Let $\alpha \in \mathbb{Q}[G]$, A be a lattice in V. The character $\chi \in G^\vee$ extends naturally to a ring homomorphism from $\mathbb{Q}[G]$ to $\mathbb{C}$. If $\chi(A) \neq 0$ for any character χ of G satisfying $\chi(\alpha) \neq 0$, then*

$$(A : \alpha A) = \left| \prod_{\chi(A) \neq 0} \chi(\alpha) \right|. \tag{4.2}$$

Lemma 4.3. *If A and B are two lattices in $e^-\mathbb{Q}[G]$, then*

$$(A : B) = (wA : wB). \tag{4.3}$$

Let S' be the abelian group generated by elements of the following form

$$\mathrm{cores}_{K/K\cap\mathbb{Q}(\mu_m)} \sum_{\substack{1\leqslant t<m\\ \gcd(t,m)=1}} \left\{\frac{at}{m}\right\}\left(\frac{K\cap\mathbb{Q}(\mu_m)/\mathbb{Q}}{t}\right)^{-1}, \qquad a\in\mathbb{Z}, m\in\mathbb{Z},$$

where $\{x\}$ stands for the fractional part of x. Define the Stickelberger ideal $S=S'\cap R$. We denote $-^*$ the involution of $\mathbb{Q}[G]$ sending g to g^{-1}. Let $\omega=\mathrm{res}_{\mathbb{Q}(\mu_m)/K}(\theta_m^*)$, where m is the minimal integer such that $K\subset\mathbb{Q}(\mu_m)$, and θ_m is defined in (2.6). Then by [10], we know that there is an R-submodule U of $\mathbb{Q}[G]$ such that $e^-S'=\omega U$. Let R^- and S^- be the minus part of R and S respectively, i.e.,

$$R^-=\{\alpha\in R:\tau\alpha=-\alpha\},\quad S^-=S\cap R^-.$$

Proposition 4.4. *S^- is a submodule of e^-S', and $[e^-S':S^-]=w$.*

Let h_K^- be the relative class number of K, Q_K be the unit index of K, i.e., $Q_K=[\mathcal{O}_K:\mu_K\mathcal{O}_{K^+}]$, where K^+ is the maximal real subfield of K. Sinnott's index formula is the following theorem:

Theorem 4.5. *S^- is of finite index in R^-, which is given by*

$$[R^-:S^-]=\frac{h_K^-}{Q_K}(e^-R:e^-U). \tag{4.4}$$

Theorem 4.6. *If G is cyclic, then $(e^-R:e^-U)=1$.*

Proposition 4.7. *If L is the cyclic extension constructed in Subsection 2.4, then $Q_L=1$.*

Proof. In this case the roots of unity $\mu_L=\{\pm1\}$. Thus we have the following embedding,

$$\phi:\mathcal{O}_L^\times/\mathcal{O}_{L^+}^\times\hookrightarrow\langle\pm1\rangle,\quad \varepsilon\mapsto\varepsilon/\bar{\varepsilon},$$

where $\bar{\varepsilon}$ is the complex conjugate of ε. If there is a unit $\varepsilon\in\mathcal{O}_L^\times$ such that $\bar{\varepsilon}=-\varepsilon$, since $\varepsilon^2\in L^+$, then $L=L^+(\varepsilon)$ and L/L^+ is unramified outside 2. But by our assumption, there are at least two primes ramified in L. The contradiction means that for any $\varepsilon\in\mathcal{O}_L^\times$ we have $\bar{\varepsilon}=\varepsilon$, i.e., $Q_L=1$. □

Corollary 4.8. *If L is defined as above, then $[R^-:S^-]=h_L^-$.*

4.2 θ_G and the class number

For any subgroup M of R, denote by M_2 the group $M\otimes\mathbb{Z}_2$. Let $A_i=I_2^i\cap R_2^-$. We have

Lemma 4.9. *Suppose $\theta_G\in I^i$ for some $i\geqslant1$. Then $\theta_G\notin I^{i+1}$ if and only if $\theta_GR_2=A_i$.*

Proof. This is just the special case $\alpha=\theta_G$ of the claim: if $t\geqslant2$ and $\alpha\in I_G^i\cap R^-$ such that αR is a subgroup in $I_G^i\cap R^-$ of the same rank, then $\alpha\notin I_G^{i+1}$ if and only if $(I_G^i\cap R^-:\alpha R)$ is odd.

Write $G=\langle\sigma\rangle$. Then $\sigma_{-1}=\sigma^{2^{t-1}}$. An element $a=\sum_{i=1}^{2^t}a_i\sigma^i\in R$ is contained in R^- if and only if $a_{i+2^{t-1}}=-a_i$, for every $i\in[1,2^{t-1}]$, or equivalently, a is contained in the ideal $(\sigma_{-1}-1)$ of R. Choose a primitive character $\chi:G\to C^*$ and extend it linearly to a ring homomorphism $R\to\mathcal{O}:=\mathbb{Z}[\zeta_{2^t}]$. Denote $\lambda=\chi(\sigma)$. The kernel of χ is the ideal $(\sigma_{-1}+1)$. Therefore, the restriction of χ to $(\sigma_{-1}-1)$ is injective, and it sends $(\sigma_{-1}-1)$ onto $(\lambda-1)^{2^{t-1}}$. From this we see that if $\alpha R\subset(\sigma_{-1}-1)$, then the index $((\sigma_{-1}-1):\alpha R)$ is finite. A lemma of Tate [8] says that χ induces an isomorphism

$$(\sigma_{-1}-1)\cap I_G^i/(\sigma_{-1}-1)\cap I_G^{i+1}\xrightarrow{\sim}(\lambda-1)^{i-1+2^{t-1}}/(\lambda-1)^{i+2^{t-1}}.$$

Now the claim is a direct consequence of this isomorphism. □

The next proposition connects θ_G and the class number.

Proposition 4.10. *Let L be constructed as before, $G=\mathrm{Gal}(L/\mathbb{Q})$. Then the following are equivalent for $n\geqslant2$.*

(1) $\theta_G\in I^n\backslash I^{n+1}$;

(2) $(\frac{m^*}{q}) = -1$ *and* $2^{n-1} \parallel h_L^-$.

Proof. First of all, $\theta_G \in I$. Take the largest i such that $\theta_G \in I^i$. We compute $[R_2^- : \theta_G R_2]$ in two ways. Note that $R_2^- \in I_2$, thus

$$[R_2^- : \theta_G R_2] = \prod_{k=1}^{i-1}[A_k : A_{k+1}][A_i : \theta_G R_2] = 2^{i-1}.$$

On the other hand, we have

$$[R_2^- : \theta_G R_2] = [R_2^- : \theta_G^* R_2] = [R_2^- : S_2^-][S_2^- : \theta^* R_2] = (\text{2-part of } h_L^-)[S_2^- : \theta^* R_2].$$

Since $2^{n-1} \mid h_L^-$, $i \geqslant n$. Therefore, $i = n$ if and only if $2^{n-1} \parallel h_L^-$ and $[S_2^- : \theta^* R_2] = 1$. Therefore, all we have to do is to show the following,

$$\left(\frac{m^*}{q}\right) = -1 \text{ if and only if } [S^- : \theta^* R] \text{ is odd.}$$

Since $\theta_G = \alpha\theta_m$, where $\alpha = 1 - q(\frac{L/\mathbb{Q}}{q})$. We have

$$\begin{aligned}[S^- : \theta^* R] &= [e^- S' : \alpha^* \omega R]/[e^- S' : S^-] \quad \text{(Lemma 4.1)}\\ &= \frac{1}{2}(e^- \omega U : e^- \alpha^* \omega R) \quad \text{(Proposition 4.4)}\\ &= \frac{1}{2}(e^- U : e^- \alpha^* R) \quad \text{(Lemma 4.3)}\\ &= \frac{1}{2}(e^- U : e^- R)[e^- R : e^- \alpha^* R] \quad \text{(Lemma 4.1)}\\ &= \frac{1}{2}[e^- R : e^- \alpha^* R] \quad \text{(Theorem 4.6).}\end{aligned}$$

Let $a = \mathrm{ord}_2[e^- R : e^- \alpha^* R]$. We have to show $(\frac{m^*}{q}) = -1$ if and only if $a = 1$. Take a primitive 2^t-th root of unity η. Suppose $(\frac{L/\mathbb{Q}}{q}) = \sigma^b$. Note that $G^\vee$ is generated by $\chi : \sigma \mapsto \eta$. By Lemma 4.3,

$$[e^- R : e^- \alpha^* R] = \left|\prod_{\chi \text{ odd}} (1 - q\chi(\sigma)^b)\right| = \left|\prod_{i \in (\mathbb{Z}/d\mathbb{Z})^\times} (1 - q\eta^{bi})\right|.$$

Suppose $b = 2^r b'$, where $2 \nmid b'$, $r < t - 1$. Then

$$\prod_{i \in (\mathbb{Z}/d\mathbb{Z})^\times} (1 - q\eta^{bi}) = N_{\mathbb{Q}(\mu_{2^{t-r}})/\mathbb{Q}}(1 - q\xi)^{2^r},$$

where ξ is a primitive 2^{t-r}-th root of unity. Note that by the definition of cyclotomic polynomial

$$N_{\mathbb{Q}(\mu_{2^{t-r}})/\mathbb{Q}}(1 - q\xi) = q^{2^{t-r}} \Phi_{2^{t-r}}\left(\frac{1}{q}\right).$$

It is well known that $\Phi_{2^{t-r}}(X) = X^{2^{t-r-1}} + 1$, hence

$$\prod_{i \in (\mathbb{Z}/d\mathbb{Z})^\times} (1 - q\eta^{bi}) = (q^{2^{t-r-1}} + 1)^{2^r}.$$

Since $r < t - 1$, $a = 1$ if and only if $r = 0$, i.e., b is odd.

On the other hand, $E_1 = \mathbb{Q}(\sqrt{m^*})$,

$$(-1)^b = \left(\frac{E_1/\mathbb{Q}}{q}\right) = \left(\frac{m^*}{q}\right).$$

Therefore, b is odd if and only if $(\frac{m^*}{q}) = -1$. This proves the proposition. □

4.3 End of the proof

We are to finish the proof of Theorem 2.10, and hence of Theorem 1.2.

Note that $h = (q-1)/[U : U_T]$. We have

Lemma 4.11. *If h is even, then* $(\frac{m^*}{q}) = 1$.

Proof. Define

$$Z = \operatorname{coker}(U \xrightarrow{\bmod q} \mathbb{F}_q^\times).$$

By definition, $h = |Z|$. We have the following exact sequence,

$$1 \longrightarrow U/U^dU_q \longrightarrow \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^d \longrightarrow Z/Z^d \longrightarrow 1.$$

Note that $|\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^d| = \gcd(q-1,d)/2$. If h is even, then $\left|Z/Z^d\right|$ is even, hence $\left|U/U^dU_q\right|$ divides $\gcd(q-1,d)/2$. Thus $m^{\gcd(q-1,d)/2} \in U^dU_q$, $m^{\gcd(q-1,d)/2} \pmod q \in (\mathbb{F}_q^\times)^d$. Take a primitive root g of q, suppose $m \equiv g^r \pmod q$. Then

$$g^{a\gcd(q-1,d)/2} \equiv m^{\gcd(q-1,d)/2} \in (\mathbb{F}_q^\times)^d.$$

Therefore a is even, which shows $(\frac{m^*}{q}) = 1$. □

Proof of Theorem 2.10. Take L and q. We shall show $\mathrm{Gr}(L/\mathbb{Q}, S, \{q\})$ under Conjecture 1.1. If $(\frac{m^*}{q}) = 1$, then by Propositions 3.13 and 4.10, $\theta_G \in I^{n+1}$, $\det_G \lambda = 0$. Thus $\mathrm{Gr}(L/\mathbb{Q}, S, \{q\})$ holds. If $(\frac{m^*}{q}) = -1$, then by Propositions 3.13 and 4.10, $\theta_G \notin I^{n+1}$ if and only if $\det_G \lambda \not\equiv 0 \pmod{I^{n+1}}$. Note that θ_G and $\det_G \lambda$ both lie in the cyclic group I^n/I^{n+1}, and $2\theta_G = 2\det_G \lambda = 0$. Thus $\theta_G \equiv \det_G \lambda \pmod{I^{n+1}}$. Then by Lemma 4.11, h is odd. Therefore, $\mathrm{Gr}(L/\mathbb{Q}, S, \{q\})$ also holds. This completes the proof of Theorem 2.10. □

Acknowledgements Research partially supported by National Natural Science Foundation of China (Grant No. 10871183) and Specialized Research Fund for the Doctoral Program of Higher Education (Grant No. 200803580047).

References

1 Aoki N. Gross conjecture on the special values at abelian L-functions at $s = 0$. Comm Math Univ Sancti Pauli, 1991, 40: 101–124

2 Aoki N. On Tate's refinement for a conjecture of Gross and its generalization. J Théor Nombres Bordeaux, 2004, 16: 457–486

3 Burns D. Equivariant Tamagawa numbers and refined Abelian Stark conjectures. J Math Sci Univ Tokyo, 2003, 10: 225–259

4 Fröhlich A. Central Extensions, Galois Groups and Ideal Class Groups of Number Fields. In: Contemp Math, vol. 24. Providence, RI: Amer Math Soc, 1983

5 Frölich A, Taylor M J. Algebraic Number Theory. Cambridge: Cambridge University Press, 1993

6 Gras G. Sur les l-classes d'ideaux dans les extensions cycliques relatives de degré premiere l. Ann Inst Fourier (Grenoble), 1973, 23: 1–48

7 Gross B. On the values of abelian L-functions at $s = 0$. J Fac Sci Univ Tokyo, 1988, 35: 177–197

8 Lee J. Stickelberger elements for cyclic extensions and the order of vanishing of abelian L-functions at $s = 0$. Compos Math, 2003, 138: 157–163

9 Ouyang Y. The Gross conjecture over rational function fields. Sci China Ser A, 2005, 48: 1609–1617

10 Sinnott W. On the Stickelberger ideal and the circular units of abelian field. Invent Math, 1980, 62: 181–234

11 Washington L C. Introduction to Cyclotomic Fields. In: Graduate Texts in Math, vol. 83. New York: Springer-Verlag, 1982

12 Yamagishi M. On a conjecture of Gross on special values of L-functions. Math Z, 1989, 201: 391–400