On the Generalized Gross-Tate Conjecture for Elementary Abelian 2-Extensions

by

Noboru Aoki

(Received September 18, 2003)

1. Introduction

Let \( k \) be a global field, namely \( k \) is either a number field of finite degree or a function field of one-variable over a finite field of characteristic \( p \). In [6] Gross proposed a conjecture which predicts that a congruence relation holds for the Stickelberger elements related to abelian extensions of \( k \). The conjecture is an analogy and a refinement of the class number formula for \( k \). For the progress of the conjecture, see [1], [2], [3], [5], [7], [8], [9], [10], [11], [12], [13], [14] and [17].

As can be easily seen, the conjecture is reduced to a trivial relation in some cases. Regarding this, Tate [16] introduced a refined conjecture in the case of cyclic extensions of prime power degree under certain assumptions. Tate’s refined conjecture is strictly stronger than the Gross conjecture in some cases. However, it shuld be remarked that the Tate conjecture is no longer true in general if one removes the assumptions Tate made (see [10]). In the previous paper [2], the author proved the Tate conjecture for number fields, and Tan [14] proved it for cyclic \( p \)-extensions of function fields. Based on those works, in [3] Lee, Tan and the author formulated a general conjecture which includes the Tate conjecture as a special case and implies the Gross conjecture in general cases. This is what we called “the generalized Gross-Tate conjecture” in the title of this paper. The precise statement of the conjecture will be recalled in Section 2 (cf. Conjecture 2.2).

The purpose of this paper is to prove the generalized conjecture in the case of elementary abelian 2-extensions under some assumptions (cf. Theorem 2.3). As a corollary we prove the original Gross conjecture for elementary abelian 2-extensions under the same assumptions (cf. Corollary 2.7). The result is not entirely contained in the work of Lee [9] because he proved the Gross conjecture for elementary abelian \( l \)-extensions assuming that \( l \) does not divide \( pw \), where \( w \) denotes the number of the roots of unity in \( k \), while \( l = 2 \) in our case and \( w \) is even unless \( p = 2 \).

2. Conjectures and results

Let \( k \) be a global field and \( S \) a finite, non-empty subset of places of \( k \) which contains the archimedean places if \( k \) is a number field. Let \( K \) be a finite abelian extension of \( k \) which is unramified outside \( S \). We denote by \( G \) the Galois group of the extension \( K/k \).
Let \( T \) be a finite, non-empty subset of places of \( k \) such that \( S \cap T = \emptyset \). For any character \( \chi \in \hat{G} \), we define a modified \( L \)-function

\[
L_{S,T}(s, \chi) = \prod_{v \in T} \left( 1 - \chi(\varphi_v)N(v)^{1-s} \right) \prod_{v \not\in S} \left( 1 - \chi(\varphi_v)N(v)^{-s} \right)^{-1},
\]

where for any finite place \( v \) of \( k \), \( \varphi_v \in G \) denotes the Frobenius element in \( G \) at \( v \). The Stickelberger element \( \theta_G = \theta_{G,S,T} \) is defined to be a unique element of the group ring \( \mathbb{C}[G] \) such that

\[
\chi(\theta_G) = L_{S,T}(0, \chi)
\]

for any character \( \chi \) of \( G \). It is then known [6] that \( \theta_G \) is in \( \mathbb{Z}[G] \).

For any intermediate field \( M \) of \( K/k \), we denote by \( U_{M,S} \) the \( S(M) \)-units group of \( k \), where \( S(M) \) is the set of places of \( M \) lying above the places in \( S \). We further define

\[
U_{M,S,T} = \left\{ u \in U_{M,S} \mid u \equiv 1 \pmod{q} \ (\forall q \in T(M)) \right\}.
\]

If a triple \((K/k, S, T)\) satisfy the conditions above and if \( U_{K,S,T} \) is torsion-free, then we call the triple an admissible data.

We will henceforth assume that \((K/k, S, T)\) is an admissible data. In this case, \( U_{M,S,T} \) is also torsion-free for any intermediate field \( M \) of \( K/k \). Let \( n = \#S - 1 \). Then \( U_{S,T} \cong \mathbb{Z}^n \) by Dirichlet’s unit theorem. Choose and fix a basis \( \{u_1, \ldots, u_n\} \) of \( U_{S,T} \).

Now, fix a place \( v_0 \in S \) and put \( S_1 = S \setminus \{v_0\} = \{v_1, \ldots, v_n\} \). Taking the trivial character for \( \chi \) in the definition of the modified \( L \)-function (1), we obtain a modified Dedekind zeta function \( \zeta_{k,S,T}(s) \).

Let \( h_S \) be the class number of the ring of \( S \)-integers of \( k \) and put

\[
h_{S,T} = h_S \cdot \#\text{Coker} (U_{S,T} \to \prod_{v \in T} \mathbb{Z}_{v}),
\]

where \( \mathbb{Z}_v \) denotes the residue field of \( v \). We define a modified regulator \( R_{S,T} \) by

\[
R_{S,T} = \det (\log |u_j|_{v_i})_{1 \leq i, j \leq n}.
\]

Then the class number formula for \( \zeta_{k,S,T}(s) \) shows that

\[
\zeta_{k,S,T}(s) = mR_{S,T}s^n + O(s^{n+1}) \quad (s \to 0),
\]

where \( m \) is an integer such that \( m = \pm h_{S,T} \).

To describe the Gross conjecture, we define

\[
R_G = \mathcal{R}_{G,S,T} := \det (r_{v_i}(u_j) - 1)_{1 \leq i, j \leq n},
\]

where \( r_v : k_v^* \to G \) is the local Artin map. Clearly \( \mathcal{R}_G \) is an element of \( \mathbb{Z}[G] \), the integral group ring of \( G \). Moreover, it is clear from the definition that \( \mathcal{R}_G \in I_G^0 \), where

\[
I_G = \text{Ker}(\mathbb{Z}[G] \to \mathbb{Z})
\]

is the augmentation ideal of \( \mathbb{Z}[G] \). Then the Gross conjecture asserts that \( \theta_G \) and \( \mathcal{R}_G \) satisfy a congruence relation which is analogous to the class number formula (2).
CONJECTURE 2.1 (Gross). Let \( m \) be the integer appeared in the formula (2). Then

\[ \theta_G \equiv mR_G \pmod{I_G^{n+1}}. \]

To state the generalized Gross-Tate conjecture, we need some notation. For any subgroup \( H \) of \( G \), let \( I_H \) be the kernel of the natural surjection \( \mathbb{Z}[G] \rightarrow \mathbb{Z}[G/H] \). For each \( v \in S \), let \( G_v \) be the decomposition group of \( v \) in \( G \) and consider an ideal

\[ I_G(S_1) = \prod_{v \in S_1} I_{G_v} \]

of \( \mathbb{Z}[G] \). It immediately follows from the definition that \( R_G \) is an element of \( I_G(S_1) \).

CONJECTURE 2.2. Let the notation be as above. Then

\[ \theta_G \equiv mR_G \pmod{I_GI_G(S_1)}. \]

In particular, \( \theta_G \in I_G(S_1) \).

Therefore Conjecture 2.2 implies Conjecture 2.1.

In [2] we proved Conjecture 2.2 for cyclic extensions of number fields, and Tan [14] proved it for cyclic \( p \)-extensions of function fields of characteristic \( p \). For more general cases, see [3]. We should remark that Burns [4] (see also [7]) formulated a similar conjecture in a more general context.

In this paper, we treat a horizontal case, that is, the case of elementary abelian 2-extensions. To state our result, we need some notation. If \( k \) is a number field, then we denote by \( S_2 \) the set of places of \( k \) lying above 2. Moreover, let \( \mathcal{O}_k^\times \) be the unit group of \( k \) and \( \mathcal{O}_{k,\text{pos}}^\times \) the subgroup of \( \mathcal{O}_k^\times \) consisting of the totally positive units of \( k \). For any \( v \in S \), we denote by \( \mathcal{O}_v^\times \) the local units in the completion of \( k \) at \( v \).

THEOREM 2.3. Let \( (K/k, S, T) \) be an admissible data such that \( G \) is an elementary 2-abelian group. We assume that the class number of \( k \) is odd. If \( k \) is a number field, we assume, in addition, that the following conditions hold.

(i) \( S \cap S_2 = \emptyset \).

(ii) If \( \mu_k \) denotes the group of roots of unity in \( k \), then \( \mathcal{O}_k^\times = \mu_k \cdot \mathcal{O}_{k,\text{pos}}^\times \), and \( \mathcal{O}_{k,\text{pos}}^\times \subseteq \mathcal{O}_v^\times \) for all \( v \in S \setminus S_\infty \).

Then Conjecture 2.2 is true for any choice of \( v_0 \in S \).

REMARK 2.4. Replacing Condition (i) with the following condition, one can similarly prove Conjecture 2.2:

(\( i' \)) Either \( \#(S \cap S_2) \leq 1 \) or the inertia group in \( G \) at \( v \) is cyclic for any \( v \in S \cap S_2 \). If \( \#(S \cap S_2) = 1 \), then one must take the unique element of \( S \cap S_2 \) for \( v_0 \). But we will not discuss it in this paper.
If \( k = \mathbb{Q} \), then the assumption and Condition (ii) in Theorem 2.3 always hold. Therefore from Theorem 2.3 we deduce the following.

**COROLLARY 2.5.** Let \( (K/\mathbb{Q}, S, T) \) be an admissible data such that \( K \) is an elementary abelian \( 2 \)-extension of \( \mathbb{Q} \) unramified outside \( 2 \). Then Conjecture 2.2 is true for any choice of \( v_0 \in S \).

**COROLLARY 2.6.** Let \( (K/k, S, T) \) be an admissible data such that \( K/k \) is an elementary abelian \( 2 \)-extension of function fields. If the class number of \( k \) is odd, then Conjecture 2.2 is true for any choice of \( v_0 \in S \).

As a corollary, we obtain the following.

**COROLLARY 2.7.** Let \( k \) be a global field whose class number is odd. Then the Gross conjecture is true for any admissible data \( (K/k, S, T) \) such that \( K/k \) is an elementary abelian \( 2 \)-extension and \( S \cap S_2 = \emptyset \).

Although, as is mentioned in the introduction, this is not entirely contained in Lee’s work [9], it is not a new result. Indeed a more general result is obtained in our previous paper [2, Theorem 10.2]. We remark however that the proof in this paper is more direct and simpler than that of [2], where genus theory and cohomological interpretation of the Gross regulator map were the key points in the proof.

### 3. Preliminaries

In what follows we will assume that \( k \) and \( S \) satisfy the conditions in Theorem 2.3. Let \( K \) be the maximal abelian \( 2 \)-extension of \( k \) which is unramified outside \( S \). We denote by \( G \) the Galois group of the extension \( G \). Thus \( G \) is an elementary abelian \( 2 \)-group. Fix a (finite or infinite) place \( v_0 \in S \) and let

\[
S_1 = S \setminus \{v_0\} = \{v_1, \ldots, v_n\}.
\]

Since the class number is assumed to be odd, there is no unramified extension of \( k \) of even degree. Therefore by class field theory there is a surjection

\[
\left( \prod_{i=0}^{n} \mathcal{O}_{v_i}^\times \right) / \mathcal{O}_k^\times \twoheadrightarrow G,
\]

where \( \mathcal{O}_k^\times \) is diagonally embedded in the direct product group \( \prod_{i=0}^{n} \mathcal{O}_{v_i}^\times \). By assumption, we have \( \mathcal{O}_{v_i}^\times = \mu_k \times \mathcal{O}_{k,\text{pos}}^\times \) and \( \mathcal{O}_{k,\text{pos}}^\times \subset \mathcal{O}_{v_i}^{\times 2} \) for all \( v \in S \setminus S_\infty \). Therefore the surjection above reduces to the isomorphism

\[
\left( \prod_{i=0}^{n} \mathcal{O}_{v_i}^\times / \mathcal{O}_{v_i}^{\times 2} \right) / (\mu_k/\mu_2^k) \cong G.
\]

The assumption that \( S_1 \cap S_2 = \emptyset \) implies that \( \mathcal{O}_{v_i}^\times / \mathcal{O}_{v_i}^{\times 2} \) is a cyclic group of order 2 for all \( i = 0, 1, \ldots, n \). Since \( \mu_k/\mu_2^k \) is also a cyclic group of order 2, we obtain an isomorphism
\[
\prod_{i=1}^{n} O_{v_i}^\times / O_{v_i}^{\times 2} \cong G
\]
such that the image \( C_i \) of \( O_{v_i}^\times \) in \( G \) under this isomorphism is the inertia group of \( v_i \) in \( G \). Thus we have a decomposition of \( G \) into a direct product of inertia groups:

\[
G = C_1 \times \cdots \times C_n.
\]

For each \( i = 1, \ldots, n \), we choose an element \( \phi_i \in G \) in the following manner. If \( v_i \) is a non-archimedean place, then \( \phi_i \) is the Frobenius element in \( G \) associated to \( v_i \) and if \( v_i \) is an archimedean place, then \( \phi_i \) is the complex conjugation with respect to the embedding \( v_i : K \to \mathbb{C} \). Then the decomposition group \( G_i \) of \( v_i \) in \( G \) is generated by \( \sigma_i \) and \( \phi_i \), hence

\[
I_G G_i = (\sigma_i - 1, \phi_i - 1).
\]

Therefore

\[
\xi_A := \prod_{i \in A^c} (1 - \phi_i) \cdot \prod_{i \in A} (1 - \sigma_i) \quad (A \subset \{1, \ldots, n\})
\]
generate the ideal \( I_G(S_1) \).

**Lemma 3.1.** For any \( \sigma \in G \) and any \( A \subset \{1, \ldots, n\} \), the element \( \frac{1 - \sigma}{2} \xi_A \) belongs to \( I_G(S_1) \).

**Proof.** Since \( \frac{1 + \sigma}{2} = \frac{1 - \sigma}{2} + \sigma \), it suffices to show that

\[
\frac{1 - \sigma}{2} \xi_A \in I_G(S_1)
\]
for any \( \sigma \in G \) and any \( A \subset \{1, \ldots, n\} \). We prove (3) by descending induction on the cardinality of \( A \).

First, suppose \( \#A = n \), that is, \( A = \{1, \ldots, n\} \). Then

\[
\xi_A = (1 - \sigma_1) \cdots (1 - \sigma_n).
\]
Let \( \sigma = \sigma_1^{a_1} \cdots \sigma_n^{a_n} \) with \( a_i = 0 \) or \( 1 \). Since \( a_i \xi = -\xi \) for all \( i \), we have

\[
\frac{1 - \sigma}{2} \xi_A = \frac{1 - (1 - a_1) + \cdots + a_n}{2} \xi_A,
\]
and this equals either \( \xi_A \) or \( 0 \) according as \( a_1 + \cdots + a_n \) is odd or even. Hence (3) holds in this case.

Next, let \( r \) be a positive integer such that \( r < n \), and suppose (3) holds for any \( A' \subset \{1, \cdots, n\} \) with \( \#A' > r \). Let \( A \) be any subset of \( \{1, \cdots, n\} \) such that \( \#A = r \). If \( \sigma = \sigma_1^{a_1} \cdots \sigma_n^{a_n} \) with \( a_i = 0 \) or \( 1 \), then

\[
1 - \sigma = (1 - \sigma_1^{a_1}) + \sigma_1^{a_1}(1 - \sigma_2^{a_2}) + \cdots + \sigma_1^{a_1} \cdots \sigma_{n-1}^{a_{n-1}}(1 - \sigma_n^{a_n})
\]
Therefore it suffices to show that \( \frac{1 - \sigma_i}{2} \xi_A \in I_G(S_1) \) for any \( i = 1, \ldots, n \). For this, note that \( (1 - \sigma_i)^2 = 2(1 - \sigma_i) \). Hence
\[
1 - \sigma_i \xi_A = \begin{cases} 
\xi_A & \text{if } i \in A, \\
\frac{1 - \varphi_i}{2} \xi_{A \cup \{i\}} & \text{if } i \notin A.
\end{cases}
\]

If \( i \notin A \), then \( \#(A \cup \{i\}) = r + 1 \), and \( \frac{1 - \varphi_i}{2} \xi_{A \cup \{i\}} \) belongs to \( I_G(S_1) \) by the inductive hypothesis. Consequently \( \frac{1 - \sigma_i}{2} \xi_A \) belongs to \( I_G(S_1) \), and (3) holds for any \( A \) with \( \#A = r \).

Thus (3) holds for any \( A \).

For each \( \chi \in \hat{G} \), let

\[
e_{\chi} = \frac{1}{\#G} \sum_{\sigma \in G} \chi(\sigma)\sigma
\]

be the idempotent corresponding to \( \chi \). If \( X \) is a submodule of \( \mathbb{Z}[G] \), then we have an inclusion

\[
X \subset \bigoplus_{\chi \in \hat{G}} X e_{\chi}
\]

in \( \mathbb{Q}[G] \). This inclusion map is defined by sending \( \alpha \in X \) to \( (\cdots, \chi(\alpha)e_{\chi}, \cdots)_{\chi \in \hat{G}} \). The right hand side of (4) is usually strictly larger than \( X \) since \( X e_{\chi} \) need not be contained in \( X \).

However, we have the following fact, which will play a key role in the proof of Theorem 2.3.

**Proposition 3.2.** Both \( I_G(S_1) \) and \( I_G I_G(S_1) \) are direct sums of the \( \chi \)-components, that is, we have

\[
I_G(S_1) = \bigoplus_{\chi \in \hat{G}} I_G(S_1)e_{\chi},
\]

\[
I_G I_G(S_1) = \bigoplus_{\chi \in \hat{G}} I_G I_G(S_1)e_{\chi}.
\]

**Proof.** It suffices to show that \( I_G(S_1)e_{\chi} \subset I_G(S_1) \) for any \( \chi \in \hat{G} \). To see this, note that

\[
e_{\chi} = \prod_{i=1}^{n} \frac{1 + \chi(\sigma_i)\sigma_i}{2}.
\]

Therefore we have only to show that \( \frac{1 + \chi}{\#G} I_G(S_1) \subset I_G(S_1) \) for any \( \sigma \in G \). But this follows from Lemma 3.1 since \( \xi_A \)'s generate the ideal \( I_G(S_1) \).

**Corollary 3.3.** The decomposition in Proposition 3.2 induces an injection

\[
I_G(S_1)/I_G I_G(S_1) \hookrightarrow \bigoplus_{\chi \in \hat{G}} \mathbb{Z}/2\mathbb{Z}.
\]

Moreover, given \( \alpha \in I_G(S_1) \), we have \( \alpha \in I_G I_G(S_1) \) if and only if \( \chi(\alpha) \in 2^{n+1}\mathbb{Z} \) for all \( \chi \in \hat{G} \).
Proof. For any $\chi \in \hat{G}$, we have $\chi(I_G(S_1))$ equals either $2^n\mathbb{Z}$ or 0, and accordingly $\chi(I_GI_G(S_1))$ equals either $2^{n+1}\mathbb{Z}$ or 0. Therefore the decomposition in Proposition 3.2 induces an injection

$$I_G(S_1)/I_GI_G(S_1) \hookrightarrow \bigoplus_{\chi \in \hat{G}} 2^n\mathbb{Z}/2^{n+1}\mathbb{Z}.$$  

Combining this with the natural isomorphism $2^n\mathbb{Z}/2^{n+1}\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$, we obtain the desired injection. The second assertion is clear from the definition of the inclusion map. □

4. An auxiliary ideal

In this section we study an auxiliary ideal $\mathfrak{A}$ of $\mathbb{Z}[G]$ which will be helpful in showing that $\theta_G \in I_G(S_1)$ in the next section. To define the ideal $\mathfrak{A}$, let

$$\omega = \prod_{i=1}^{n} \left( 1 - \varphi_i \cdot \frac{1 + \sigma_i}{2} \right) \in \mathbb{Q}[G].$$

For any $\chi \in \hat{G}$, we have $\frac{1 + \chi(\sigma_i)}{2} = 1$ or 0 according as $\chi(\sigma_i) = 1$ or $-1$. Therefore

$$\chi(\omega) = \prod_{i \notin A_\chi} (1 - \chi(\varphi_i)), \quad (6)$$

where $A_\chi := \{ i \in \{1, \ldots, n\} | \chi(\sigma_i) = -1 \}$. We then define $\mathfrak{A}$ by

$$\mathfrak{A} = \{ \alpha \in \omega \mathbb{Q}[G] \cap \mathbb{Z}[G] | \chi(\alpha) \equiv 0 \pmod{2^n} \quad (\forall \chi \in \hat{G}) \}. $$

We will show that $\mathfrak{A}$ is a subideal of $I_G(S_1)$ by specifying a $\mathbb{Z}$-basis of the module $\mathfrak{A}$.

For this end, let

$$\eta_\chi = \xi_{A_\chi} \cdot \prod_{i \notin A_\chi} \frac{1 + \sigma_i}{2} \quad (\chi \in \hat{G}).$$

We want to show that non-zero $\eta_\chi$’s form a $\mathbb{Z}$-basis of the module $\mathfrak{A}$.

Lemma 4.1. For any $\chi \in \hat{G}$, $\eta_\chi$ belongs to $I_G(S_1)$. Moreover, $\eta_\chi = 2^{n_\chi} \omega e_\chi$ for any $\chi$. In particular, $\eta_\chi \neq 0$ if and only if $\chi(\omega) \neq 0$.

Proof. The first assertion immediately follows from Lemma 3.1. To prove the second assertion, note that

$$\eta_\chi = \prod_{i \notin A_\chi} (1 - \varphi_i) \prod_{i \in A_\chi} (1 - \sigma_i) \cdot \prod_{i \notin A_\chi} \frac{1 + \sigma_i}{2} \quad (7)$$

$$= \prod_{i \notin A_\chi} (1 - \varphi_i) \cdot 2^{n_\chi} \prod_{i=1}^{n_\chi} \frac{1 + \chi(\sigma_i)\varphi_i}{2}. $$

Therefore from (5) we obtain
\[ \eta_X = 2^{n_X} \prod_{i \not\in \Lambda_X} (1 - \psi_i) \cdot e_X = 2^{n_X} \prod_{i \not\in \Lambda_X} (1 - \chi(\varphi_i)) \cdot e_X. \]

It then follows from (6) that
\[ \eta_X = 2^{n_X} \chi(\omega) e_X = 2^{n_X} \omega e_X. \]

This proves the lemma. \( \square \)

To state the next proposition, let
\[ \hat{G}(\omega) = \{ \chi \in \hat{G} \mid \chi(\omega) \neq 0 \}. \]

Then it is clear from Lemma 4.1 that \( \eta_X \neq 0 \) if and only if \( \chi \in \hat{G}(\omega) \).

**Proposition 4.2.** The set \( \{ \eta_X \mid \chi \in \hat{G}(\omega) \} \) forms a \( \mathbb{Z} \)-basis of the module \( \mathfrak{A} \). In particular, \( \mathfrak{A} \subset I_G(S_1) \).

**Proof.** The second assertion follows from the first assertion and Lemma 4.1.

To prove the first assertion, let \( \alpha = \omega \beta \in \mathfrak{A} \) with \( \beta \in \mathbb{Q}[G] \). We write \( \beta \) as
\[ \beta = \sum_{\chi \in \hat{G}} b_\chi e_\chi. \]

Then \( \alpha \) may be written as
\[ \alpha = \sum_{\chi \in \hat{G}(\omega)} \omega b_\chi e_\chi = \sum_{\chi \in \hat{G}(\omega)} \chi(\omega) b_\chi e_\chi. \]

Since \( \chi(\omega) b_\chi = \chi(\alpha) \equiv 0 \pmod{2^n} \) and \( \chi(\omega) = 2^{n-n_X} \) for any \( \chi \in \hat{G}(\omega) \), we have
\[ b_\chi = \frac{\chi(\alpha)}{2^{n-n_X}} \in 2^{n_X} \mathbb{Z} \]
for any \( \chi \in \hat{G}(\omega) \). Thus \( b_\chi = 2^{n_X} c_\chi e_\chi \) with an integer \( c_\chi \). Since \( 2^{n_X} \omega e_X = \eta_X \) by Lemma 4.1, it follows that
\[ \alpha = \sum_{\chi \in \hat{G}(\omega)} c_\chi \eta_X. \]

This implies that \( \mathfrak{A} \) is contained in the submodule of \( \mathbb{Z}[G] \) generated by \( \eta_X \)'s. Conversely, we have \( \chi(\eta_X) = 2^n \) if \( \chi(\omega) \neq 0 \), and hence \( \eta_X \in \mathfrak{A} \). Therefore, \( \mathfrak{A} \) is coincides with the module generated by \( \eta_X \)'s. Since \( \eta_X \) is a multiple of the idempotent \( e_X \) for all \( \chi \in \hat{G} \), the elements \( \eta_X \)'s (\( \chi \in \hat{G}(\omega) \)) are clearly linear independent. Therefore the set \( \{ \eta_X \mid \chi \in \hat{G}(\omega) \} \) forms a \( \mathbb{Z} \)-basis of \( \mathfrak{A} \). This completes the proof. \( \square \)

5. **Proof of Theorem 2.3**

Let \( K,G \) be as in the previous section. For each character \( \chi \in \hat{G} \), let \( K_\chi \) be the fixed field of \( \text{Ker}(\chi) \). Then \( K_\chi \) is a quadratic extension of \( \mathbb{Q} \) unless \( \chi = 1 \). Let \( m_{K_\chi,S,T} \) (resp.
Let $\Lambda_{\chi}$ be as in the previous section and set $n_{\chi} = n_{A_{\chi}}$. Then, one can show that the assumption on the class number implies that $m_{\chi}$ is a 2-adic integer for any $\chi$.

**Lemma 5.1.** For each $\chi \in \hat{G}$, we have

$$\chi(\theta_G) = 2^{n_{\chi}} m_{\chi} \chi(\omega).$$

In particular, $\chi(\theta_G) \equiv 0 \pmod{2^n}$. Moreover, $m_{\chi}$ is an integer for any $\chi \in \hat{G}(\omega)$.

**Proof.** In view of (6) it suffices to show the equality

$$\chi(\theta_G) = 2^{n_{\chi}} m_{\chi} \prod_{i \notin \Lambda_{\chi}} \left(1 - \chi(\phi_i)\right)$$

assuming that $\chi$ is non-trivial. Then $K_{\chi}$ is a quadratic extension of $k$, hence

$$\chi(\theta_G) = \lim_{s \to 0} \frac{\xi_{K_{\chi},\mathbf{S},T}(s)}{\xi_{k,\mathbf{S},T}(s)} \cdot \frac{R_{K_{\chi},\mathbf{S},T}}{R_{k,\mathbf{S},T}} \cdot \prod_{i \notin \Lambda_{\chi}} \left(1 - \chi(\phi_i)\right).$$

If $\#S(K_{\chi}) = \#S$, then $R_{K_{\chi},\mathbf{S},T} = 2^{n_{\chi}} R_{k,\mathbf{S},T}$, and so (10) follows. If $\#S(K_{\chi}) > \#S$, then the both sides of (10) become zero since $\text{ord}_{s=0} \xi_{K_{\chi},\mathbf{S},T} > \text{ord}_{s=0} \xi_{k,\mathbf{S},T}$. Thus (10) holds.

The remainder assertions follow from (9) since $\chi(\omega) \in 2^{n_{\chi}-n_{\chi}} \mathbb{Z}$. This completes the proof.

**Proposition 5.2.** The Stickelberger element $\theta_G$ belongs to $I_G(S_1)$. More precisely, $\theta_G$ can be written as

$$\theta_G = \sum_{\chi \in \hat{G}(\omega)} m_{\chi} \eta_{\chi},$$

where $m_{\chi}$ is the integer defined in (8). In particular, $\theta_G$ is an element of $I_G(S_1)$.

**Proof.** From the identity $1 = \sum_{\chi} e_{\chi}$ it follows that

$$\theta_G = \sum_{\chi \in \hat{G}} \chi(\theta_G) e_{\chi}.$$ 

Then combining this with Lemma 9, we obtain

$$\theta_G = \sum_{\chi \in \hat{G}} 2^{n_{\chi}} m_{\chi} \chi(\omega) e_{\chi} = \sum_{\chi \in \hat{G}(\omega)} m_{\chi} \eta_{\chi}.$$ 

This proves the proposition.
Now we are in a position to prove Theorem 2.3.

Proof of Theorem 2.3. By functorial properties of the conjecture ([6]), it suffices to prove the theorem assuming that $K$ is the maximal abelian 2-extension of $k$ unramified outside $S$. By Corollary 3.3 and Proposition 5.2, it suffices to show the congruence

$$\chi(\theta_G) \equiv m \chi(\mathcal{R}_G) \pmod{2^{n+1}}$$

for all $\chi \in \hat{G}$. Let $K_\chi$ be the intermediate field of $K/k$ corresponding to $\chi$ and $G_\chi$ the Galois group of the extension $K_\chi/k$. Since $\chi(\theta_G) = \chi(\theta_{G_\chi})$, $\chi(\mathcal{R}_G) = \chi(\mathcal{R}_{G_\chi})$ and $\chi(I_n^{G_\chi}) = \chi(I_n^{G_\chi})$, (12) is equivalent to the congruence

$$\theta_{G_\chi} \equiv m \mathcal{R}_{G_\chi} \pmod{I_n^{G_\chi}}.$$

But this is the Gross conjecture for the quadratic extension $K_\chi/k$, which has been proved by Gross [6, Proposition 6.15]. The proof of Theorem 2.3 is now complete. □

References