Journal de Théorie des Nombres
de Bordeaux **16** (2004), 457–486

On Tate's refinement for a conjecture of Gross and its generalization

par Noboru AOKI

Résumé. Nous étudions un raffinement dù à Tate de la conjecture de Gross sur les valeurs de fonctions L abéliennes en $s = 0$ et formulons sa généralisation à une extension cyclique abitraire. Nous prouvons que notre conjecture généralisée est vraie dans le cas des corps de nombres. Cela entraine en particulier que le raffinement de Tate est vrai pour tout corps de nombres.

Abstract. We study Tate's refinement for a conjecture of Gross on the values of abelian L-function at $s = 0$ and formulate its generalization to arbitrary cyclic extensions. We prove that our generalized conjecture is true in the case of number fields. This in particular implies that Tate's refinement is true for any number field.

1. Introduction

In [9] Gross proposed a conjecture which predicts a relation between two arithmetic objects, the Stickelberger element and the Gross regulator, both of which are defined for any data $(K/k, S, T)$, where K/k is an abelian extension of global fields and S, T are finite, non-empty subsets of the places of k satisfying certain conditions. In the same paper, he proved the conjecture in the case of unramified extensions of number fields, and obtained a partial result when the extension is cyclic of prime degree. Since then the conjecture has been verified to be true in several cases (see Proposition 2.2 below), but yet it remains to be proved in general. Taking a close look at the conjecture, however, one can easily notice that it becomes trivial in some cases. For example, if S contains a place which completely splits in K, then both the Stickelberger element and the Gross regulator are zero, and the conjecture is trivially true. Besides such a trivial case, there are still some cases where the conjecture becomes trivial. As observed by Tate [22], this is the case if K/k is a cyclic extension whose degree is a power of a prime number l and if at least one place of S "almost splits completely"

Manuscrit reçu le 6 juin 2003.

in K/k (see Section 3 for the definition) and another place in S splits in K/k. He then proposed a refined conjecture in that case.

The purpose of this paper is to study Tate's refined conjecture from a cohomological view point and to generalize it to arbitrary cyclic extensions. (In a forthcoming paper [2], a further generalization of the conjecture will be given.) We will prove that a weak congruence holds for any cyclic l-extension (Theorem 3.3), which implies Tate's refined conjecture when k is a number field (Theorem 3.4). Piecing the congruences together for all primes l, we will also obtain a weak congruence for arbitrary cyclic extensions (Theorem 4.2), which is a partial result in the direction of our conjecture. In particular it shows that the generalized conjecture (and hence the Gross conjecture) is true for arbitrary cyclic extensions of number fields (Theorem 4.3 and Corollary 4.4). In the last section, using the results above, we will give a new proof of the Gross conjecture for arbitrary abelian extensions $K/\mathbb{Q}$ (Theorem 10.1), which simplifies our previous proof in [1].

The main idea of the proof consists of two ingredients: one is an interpretation of the Gross regulator map in terms of Galois cohomology, and the other is genus theory for cyclic extensions K/k. Here by genus theory we mean a formula (Theorem 7.1) for the (S,T)-ambiguous class number of K/k, and it will play an important role when we relate the Stickelberger element to the Gross regulator in the proof of Theorem 4.2. The idea to use genus theory can be already found in the paper of Gross [9], where he implicitly used it to prove a weak congruence in the case of cyclic extensions of prime degree. Thus our proof may be regarded as a natural generalization of his.

Acknowledgements I would like to thank Joongul Lee and Ki-Seng Tan for reading the manuscript very carefully and making a number of helpful suggestions. Especially I am considerably indebted to Lee for the treatment of the case "$m_0 > 0$" in Theorem 9.2. I am very grateful to David Burns for letting me know of recent work by himself [3] and by Anthony Hayward [11] both of which are closely related to this article. I also wish to express my gratitude to John Tate for many valuable comments and suggestions.

2. The Gross conjecture

In this section we briefly recall the Gross conjecture. Let k be a global field, and let S be any finite, non-empty set of places of k which contains all the archimedean places if k is a number field. Let $\mathscr{O}_S$ be the ring of S-integers of k and consider the S-zeta function

$$\zeta_S(s) = \sum_{\mathfrak{a} \subseteq \mathscr{O}_S} (N\mathfrak{a})^{-s},$$

where the summation is over the ideals $\mathfrak{a}$ of $\mathscr{O}_S$. It is well known that this series converges for $\Re(s) > 1$ and has a meromorphic continuation to the s-plane, with only a simple pole at $s = 1$. The analytic class number formula for k says that the Taylor expansion of $\zeta_S(s)$ at $s = 0$ begins:

$$\zeta_S(s) = -\frac{h_S R_S}{w_S} s^n + O(s^{n+1}),$$

where h_S is the class number of $\mathscr{O}_S$, R_S is the S-regulator, w_S is the number of root of unity in the S-unit group $U_S = \mathscr{O}_S^\times$ and $n = |S| - 1$. To achieve a formula with no denominator, following Gross, we introduce a slightly modified zeta function. Let T be a finite set of places of k which is disjoint from S, and define the (S,T)-zeta function

$$\zeta_{S,T}(s) = \prod_{v \in T} (1 - Nv^{1-s}) \cdot \zeta_S(s),$$

where Nv is the cardinality of the residue field of v. To describe the corresponding formula for $\zeta_{S,T}(s)$, we define the (S,T)-unit group of k by

$$U_{S,T} = \{u \in U_S \mid u \equiv 1 \pmod{v} \text{ for all } v \in T\}.$$

Clearly the index $(U_S : U_{S,T})$ is finite, and is a divisor of $\prod_{\mathfrak{q} \in T}(Nv - 1)$. Define the (S,T)-class number $h = h_{S,T}$ by the formula

$$h = h_S \cdot \frac{\prod_{v \in T}(Nv - 1)}{(U_S : U_{S,T})}. \tag{1}$$

Then the Taylor expansion of $\zeta_{S,T}(s)$ at $s = 0$ begins:

$$\zeta_{S,T}(s) = (-1)^{|T|-1} \frac{h R_{S,T}}{w} s^n + O(s^{n+1}), \tag{2}$$

where $R_{S,T}$ is the (S,T)-regulator (see below for the definition) and w is the number of root of unity in $U_{S,T}$. We henceforth assume that T is chosen so that $U_{S,T}$ is torsion-free. Then from (2) we obtain a formula without a denominator:

$$\zeta_{S,T}(s) = (-1)^{|T|-1} h R_{S,T} s^n + O(s^{n+1}). \tag{3}$$

To define the (S,T)-regulator, let Y_S be the free abelian group generated by the places of S and

$$X_S = \left\{ \sum_{v \in S} a_v \cdot v \in Y_S \;\middle|\; \sum_{v \in S} a_v = 0 \right\}$$

the subgroup of elements of degree zero in Y_S. Then $X_S \cong \mathbb{Z}^n$. Since we are assuming that $U_{S,T}$ is torsion-free, we have an isomorphism $U_{S,T} \cong \mathbb{Z}^n$.

Let $\langle u_1, \ldots, u_n \rangle$ and $\langle x_1, \ldots, x_n \rangle$ be $\mathbb{Z}$-bases of $U_{S,T}$ and X_S respectively. Let $\det_{\mathbb{R}}(\lambda)$ be the determinant of the map

$$\lambda_{\mathbb{R},S,T} : U_{S,T} \longrightarrow \mathbb{R} \otimes X_S, \qquad u \mapsto \sum_{v \in S} \log \|u\|_v \otimes v.$$

taken with respect to $\mathbb{Z}$-bases of $U_{S,T}$ and X_S chosen above. The (S,T)-regulator $R_{S,T}$ is by definition the absolute value of $\det_{\mathbb{R}}(\lambda)$. By (3) we have

$$\zeta_{S,T}(s) = \pm h \cdot \det_{\mathbb{R}}(\lambda) s^n + O(s^{n+1}), \tag{4}$$

where the sign of course depends on the choice of bases of $U_{S,T}$ and X_S.

The Gross conjecture predicts that there is an analogous congruence relation if we replace $\zeta_{S,T}(s)$ and $\det_{\mathbb{R}}(\lambda)$ in (4) by the Stickelberger element and the Gross regulator respectively. We give a brief review of the definition of these two objects.

First we define the Stickelberger element. Let K/k be a finite abelian extension which is unramified outside S and G the Galois group of K/k. For any complex valued character χ of G, we define the (S,T)-L function associated to χ to be the infinite product

$$L_{S,T}(\chi, s) = \prod_{v \in T} (1 - \chi(Fr_v) N(v)^{1-s}) \prod_{v \notin S} (1 - \chi(Fr_v) N(v)^{-s})^{-1},$$

where $Fr_v \in G$ denotes the Frobenius element at v. Then there exists a unique element $\theta_G = \theta_{G,S,T} \in \mathbb{C}[G]$ such that $\chi(\theta_G) = L_{S,T}(\chi, 0)$ for any χ. Gross [9] showed that θ_G is in $\mathbb{Z}[G]$ using integrality properties proved independently by Deligne-Ribet [7] and Barsky-Cassou-Noguès [5].

Next, to define the Gross regulator, consider the map

$$\lambda = \lambda_{G,S,T} : U_{S,T} \longrightarrow G \otimes X_S, \qquad u \mapsto \sum_{v \in S} r_v(u) \otimes v,$$

where $r_v : k_v^{\times} \longrightarrow G$ denotes the local reciprocity map. Let (g_{ij}) be the $n \times n$ matrix representing λ with respect to the bases $\{u_i\}$ and $\{x_j\}$ chosen above, namely:

$$\lambda(u_i) = \sum_{j=1}^{n} g_{ij} \otimes x_j \quad (i = 1, \ldots, n).$$

Let $\mathbb{Z}[G]$ be the integral group ring of G and I_G the augmentation ideal of $\mathbb{Z}[G]$. Then there is an isomorphism $G \cong I_G/I_G^2$, $g \mapsto g - 1$. Using this isomorphism we can view the matrix $(g_{ij} - 1)$ with entries in I_G/I_G^2 as a matrix representing λ. Define the Gross regulator by

$$\det_G(\lambda) = \sum_{\sigma} \operatorname{sgn}(\sigma)(g_{1,\sigma(1)} - 1) \cdots (g_{n,\sigma(n)} - 1) \quad \in I_G^n/I_G^{n+1},$$

where the sum is over the permutations σ of $\{1, \ldots, n\}$.

We are now in a position to state the conjecture of Gross.

Conjecture 2.1. *Let the notation be as above. Then $\theta_G \in I_G^n$ and the following congruence holds:*

$$\theta_G \equiv \pm h\mathrm{det}_G(\lambda) \pmod{I_G^{n+1}},$$

where the sign is chosen in a way consistent with (4).

In the following we have a list of the cases where Conjecture 2.1 is proved.

Proposition 2.2. *Conjecture 2.1 is true in the following cases:*

(i) $n = 0$.
(ii) k *is a number field and* S *is the set of the archimedean places.*
(iii) K *is a quadratic extension of* k.
(iv) k *is a function field and* $n = 1$.
(v) $k = \mathbb{Q}$.
(vi) K/k *is an abelian* p*-extension of function fields of characteristic* p.
(vii) K/k *is an abelian* l*-extension, where* l *is a prime number different from the characteristic of* k *and divides neither the class number of* k *nor the number of roots of unity in* K.
(viii) K/k *is an abelian extension of a rational function field* k *over a finite field and* $|S| \leq 3$.

Proof. In the case of (i) Conjecture 2.1 is an immediate consequence of (4). In both cases (ii) and (iii) the conjecture was proved by Gross in [9]. Case (iv) is a consequence of the work of Hayes [10] proving a refined version of the Stark conjecture. Case (v) was treated in our previous paper [1]. In the cases (vi), (vii) and (viii) the conjecture was proved by Tan [19], Lee [15] and Reid [16], respectively. □

As mentioned in the introduction, Gross [9] proved a weak congruence when K/k is a cyclic extension of a prime degree. Here we give the precise statement because our main results (Theorem 3.3 and Theorem 4.2) may be viewed as a generalization of it to arbitrary cyclic extensions.

Proposition 2.3. *Suppose K/k is a cyclic extension of prime degree l. Then there is a constant $c \in (\mathbb{Z}/l\mathbb{Z})^\times$ such that*

$$\theta_G \equiv c \cdot h\mathrm{det}_G(\lambda) \pmod{I_G^{n+1}}.$$

Proof. See [9, Proposition 6.15]. □

3. Tate's refinement for the Gross conjecture

In this section we give the precise statement of Tate's refinement for the Gross conjecture.

First, we assume that G is an arbitrary finite abelian group. Choose and fix a place $v_0 \in S$ and set $S_1 = S \setminus \{v_0\} = \{v_1, \dots, v_n\}$. Then, as a $\mathbb{Z}$-basis of X_S, we can take $\{v_1 - v_0, \dots, v_n - v_0\}$. In this case we have

$$\lambda(u) = \sum_{j=1}^{n} r_{v_j}(u) \otimes (v_j - v_0).$$

Choosing a $\mathbb{Z}$-basis $\{u_1, \dots, u_n\}$ of $U_{S,T}$, we define

$$\mathcal{R}_G = \mathcal{R}_{G,S,T} := \det\left(r_{v_i}(u_j) - 1\right)_{1 \le i,j \le n} \in \mathbb{Z}[G].$$

It is clear from the definition that $\mathcal{R}_G \in I_G^n$ and $\mathcal{R}_G \equiv \det_G(\lambda) \pmod{I_G^{n+1}}$.

Now, suppose that G is a cyclic group of degree l^m, a power of a prime number l. For each $v \in S$, let G_v denote the decomposition group of v in G. We fix the ordering of the elements of $S = \{v_0, v_1, \dots, v_n\}$ so that

$$G_{v_0} \supseteq G_{v_1} \supseteq \cdots \supseteq G_{v_n}.$$

Let $l^{m_i} = (G : G_{v_i})$ for $i = 0, \dots, n$. Thus $m_0 \le m_1 \le \ldots \le m_n \le m$. Let

$$N = l^{m_0} + \cdots + l^{m_{n-1}} = |S(K)| - l^{m_n}.$$

Clearly $N \ge n$, and $N = n$ if and only if $m_0 = \cdots = m_{n-1} = 0$.

If $m_n = m$, that is, v_n splits completely in K/k, then $\theta_G = \mathcal{R}_G = 0$. Hence Conjecture 2.1 trivially holds. Let us consider the second simplest case $m_n = m - 1$. Following Tate, we say that the place v_n *almost splits completely in* K if $m_n = m - 1$. Tate [22] proved the following.

Theorem 3.1. *Assume that $m_n = m - 1$. Then $\theta_G \in I_G^N$ and $\mathcal{R}_G \in I_G^{N - l^{m_0}+1}$. Moreover, the image of $\mathcal{R}_G$ in $I_G^{N-l^{m_0}+1}/I_G^{N-l^{m_0}+2}$ is, up to the sign, independent of the choice of the basis of $U_{S,T}$ and the choice of v_0.*

Since $N \ge n$, this theorem, in particular, shows that $\theta_G \in I_G^n$. Let us consider the case where $m_0 > 0$. In this case we have $N > n$ and hence Theorem 3.1 also shows that $\theta_G \in I_G^{n+1}$. Moreover, one can show that $h\mathcal{R}_G \equiv 0 \pmod{I_G^{n+1}}$ (see Theorem 9.2, (i)). Therefore Conjecture 2.1 is trivially true if $m_0 > 0$. On the other hand, if $m_0 = 0$, then both θ_G and $\mathcal{R}_G$ are in the same ideal I_G^N. Therefore it is meaningful to compare them in the quotient group I_G^N/I_G^{N+1}. Based on these facts, Tate [22] proposed a refinement for the Gross conjecture.

Conjecture 3.2. *Assume that $m_0 = 0$ and $m_n = m - 1$. Then*

$$\theta_G \equiv \pm h\mathcal{R}_G \pmod{I_G^{N+1}},$$

where the sign is chosen in a way consistent with (4).

Obviously Conjecture 3.2 implies Conjecture 2.1 since $N \ge n$ and

$$\det_G(\lambda_{S,T}) \equiv \mathcal{R}_G \pmod{I_G^{n+1}}.$$

Now, we can state one of our main results.

Theorem 3.3. *Let the notation and assumptions be as in Conjecture 3.2. Then there exists an integer c prime to l such that*

$$\theta_G \equiv c \cdot h\mathcal{R}_G \pmod{I_G^{N+1}}.$$

In particular, if $l = 2$, then Conjecture 3.2 is true.

We will give the proof of this theorem (more precisely, of Theorem 9.1 which is equivalent to Theorem 3.3) in Section 9. Here we only note that the last assertion immediately follows from the first one. To see this we have only to observe that $I_G^N/I_G^{N+1} \cong \mathbb{Z}/|G|\mathbb{Z}$ since G is a cyclic group and that both θ_G and $\mathcal{R}_G$ are killed by l in I_G^N/I_G^{N+1} under the condition that $m_n = m - 1$ (see Proposition 5.4). Therefore, if $l = 2$, then $ch\mathcal{R}_G \equiv h\mathcal{R}_G \pmod{I_G^{N+1}}$. Thus Conjecture 3.2 is true.

As a special case of Theorem 3.3 we have the following.

Corollary 3.4. *If K/k is a cyclic l-extension of number fields, then Conjecture 3.2 is true.*

Proof. Actually, Conjecture 3.2 is non-trivial only when $l = 2$ in the number field case since I_G^N/I_G^{N+1} is an l-group and both θ_G and $\mathcal{R}_G$ are killed by 2 in I_G^N/I_G^{N+1}. Thus Corollary 3.4 is a direct consequence of Theorem 3.3. □

Remark 3.5. As remarked by Lee [14], one can not drop the condition $m_0 = 0$ from the conditions in Conjecture 3.2. Indeed, he showed that there are infinitely many cyclic l-extensions K/k for which $\theta_G \notin I_G^{N+1}$ but $h\mathrm{det}_G(\lambda) \in I_G^{N+1}$. In the next section, we will generalize Conjecture 3.2 to arbitrary cyclic extensions in order to remove the restriction on m_0.

4. A generalization of Tate's conjecture

In this section G will be an arbitrary cyclic group. For any $v \in S$, let

$$I_G(v) = \mathrm{Ker}(\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G/G_v])$$

be the kernel of the canonical surjection $\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G/G_v]$. Let us choose and fix a place $v_0 \in S$. Let $S_1 = S \setminus \{v_0\}$ and consider the ideal

$$I_G(S_1) = \prod_{i=1}^{n} I_G(v_i)$$

in $\mathbb{Z}[G]$. If σ is a generator of G, then G_{v_i} is generated by $\sigma_{v_i} := \sigma^{(G:G_{v_i})}$ and $I_G(S_1)$ is a principal ideal generated by $(\sigma_{v_1} - 1) \cdots (\sigma_{v_n} - 1)$. Since the entries of the i-th row of the matrix $(r_{v_i}(u_j) - 1)_{i,j}$ are in the ideal $I_G(v_i)$, its determinant $\mathcal{R}_G$ belongs to the ideal $I_G(S_1)$. Moreover, the image of $\mathcal{R}_G$ in the quotient group $I_G(S_1)/I_G I_G(S_1)$ is, up to the sign, independent of the choice of the basis of $U_{S,T}$.

Given a finite abelian extension K/k of global fields and finite sets S, T of places of k such that $S \cap T = \emptyset$, we call the triple $(K/k, S, T)$ an *admissible data* if the following conditions are satisfied:

(i) S contains the places of k ramifying in K and the archimedean places of k.
(ii) $U_{K,S,T}$ is torsion-free.

In [9] Gross gave a sufficient condition for $U_{S,T}$ to be torsion-free:

- In the function field case $U_{S,T}$ is torsion-free if T is non-empty.
- In the number field case $U_{S,T}$ is torsion-free if T contains either primes of different residue characteristics or a prime v whose absolute ramification index e_v is strictly less than $p-1$, where p is the characteristic of $\mathbb{F}_v$.

It is worthwhile to note that each condition above also ensures that $U_{K,S,T}$ is torsion-free for any finite abelian extension unramified outside S.

We propose the following conjecture which will turn out to be equivalent to Tate's refinement when K/k is a cyclic l-extension such that $m_0 = 0$ and $m_n = m - 1$.

Conjecture 4.1. *Let $(K/k, S, T)$ be an admissible data such that $G = \mathrm{Gal}(K/k)$ is a cyclic group. Then*

$$\theta_G \equiv \pm h\mathcal{R}_G \pmod{I_G I_G(S_1)},$$

where the sign is chosen in a way consistent with (4).

It is very likely that the congruence in the conjecture holds for any finite abelian extension K/k. In a forthcoming paper [2], this will be discussed in some detail and some evidence will be given.

If l is a prime number dividing $|G|$, we denote by G_l the l-Sylow subgroup of G. For each $v \in S$, let G_v be the decomposition group of v in G, and put $G_{v,l} = G_v \cap G_l$. Thus $G_{v,l}$ is the l-Sylow subgroup of G_v. Now, consider the following condition:

$$\text{(5)} \qquad \begin{cases} \text{There exists a place } v_n \in S_1 \text{ such that } |G_{v_n,l}| \leq l \\ \text{for any prime divisor } l \text{ of } |G|. \end{cases}$$

In other words, this requires that there exists a place v_n in S which either splits completely or almost splits completely in the maximal l-extension of k contained in K for each prime divisor l of $|G|$. Although this condition is very restrictive in the function field case, it is always satisfied in the number field case since $|G_v| = 1$ or 2 for any archimedean place v of k.

Now, we can state our main result, which may be viewed as a partial answer to Conjecture 4.1.

Theorem 4.2. *Suppose condition (5) holds. Then θ_G belongs to $I_G(S_1)$ and there exists an integer c prime to $|G|$ such that*

$$\theta_G \equiv c \cdot h\mathcal{R}_G \pmod{I_G I_G(S_1)}.$$

In the next section we will see that in order to prove Theorem 4.2 it suffices to prove it when G is a cyclic group of a prime power order.

In the case of number fields, Theorem 4.2 gives a complete answer to Conjecture 4.1.

Theorem 4.3. *If K/k is a cyclic extension of number fields, then we have*

$$\theta_G \equiv h\mathcal{R}_G \pmod{I_G I_G(S_1)}.$$

Proof. As we have remarked above, condition (5) is always satisfied in the number field case. As is well known, if k is not totally real or K is not a totally imaginary, then Conjecture 2.1 is trivial. Suppose K is a totally imaginary extension of a totally real field k. Then, as we will see later (see Proposition 5.4), the quotient group $I_G/I_G I_G(S_1)$ is a cyclic group of order 2. Thus Theorem 4.3 immediately follows from Theorem 4.2. □

Since Conjecture 3.2 implies Conjecture 2.1, Theorem 4.3 proves the following.

Corollary 4.4. *If K/k is a cyclic extension of number fields, then Conjecture 2.1 is true.*

5. Stickelberger elements for cyclic l-extensions

Throughout this section we will assume that G is a cyclic l-group and that $(K/k, S, T)$ is an admissible data. In particular $U_{K,S,T}$ is torsion-free. In order to state Theorem 5.1 below, let F be the intermediate field of K/k with $[K : F] = l$ and put

$$h^*_{K,S,T} = h_{K,S,T}/h_{F,S,T}.$$

If at least one place in S does not split completely in K/k, then $h^*_{K,S,T}$ is an integer by [17, Lemma 3.4]. In particular, if $m_n = m - 1$, then $h^*_{K,S,T}$ is an integer.

Theorem 5.1. *Suppose $m_n = m - 1$. Then*

$$\theta_G \equiv 0 \pmod{I_G(S_1)}.$$

Moreover, the following assertions hold.

(i) *If $m_0 > 0$, then $\theta_G \equiv 0 \pmod{I_G I_G(S_1)}$.*
(ii) *If $m_0 = 0$, then $\theta_G \equiv 0 \pmod{I_G I_G(S_1)}$ if and only if $h^*_{K,S,T} \equiv 0 \pmod{l}$.*

Although both the first statement and (i) of the second statement follows from Tate's theorem (Theorem 3.1) in view of Proposition 5.4, we will give a proof for the completeness. We begin with a lemma.

Lemma 5.2. *Let M be an intermediate field of K/k such that $|S(K)| = |S(M)|$. Then $U_{K,S,T} = U_{M,S,T}$.*

Proof. Let u be any element of $U_{K,S,T}$. For any $\sigma \in G$, $u^{\sigma-1}$ is also an element of $U_{K,S,T}$ since $U_{K,S,T}$ is G-stable. Moreover the following argument shows that $u^{\sigma-1}$ is a root of unity. Indeed, the assumption of the lemma implies that $U_{K,S,T}/U_{M,S,T}$ is a finite group. It follows that there exists a positive integer m such that $u^m \in U_{M,S,T}$. Therefore $(u^{\sigma-1})^m = (u^m)^{\sigma-1} = 1$. Thus $u^{\sigma-1}$ is an m-th root of unity. However, since $U_{K,S,T}$ is torsion-free, this shows that $u^{\sigma-1} = 1$ for any $\sigma \in \mathrm{Gal}(K/M)$, hence $u \in M^\times$. The assertion of the lemma then follows from the fact that $U_{K,S,T} \cap M^\times = U_{M,S,T}$. □

Proposition 5.3. *Assume that $m_n = m - 1$. Then*

$$\prod_\chi \chi(\theta_G) = \pm l^{|S(K)|-1} h^*_{K,S,T},$$

where χ runs through the faithful characters of G.

Proof. Let F be as above. Then the assumption on G_v's implies that $|S(K)| = |S(F)|$. This, in particular, implies that

$$\mathrm{ord}_{s=0}\zeta_{K,S,T}(s) = \mathrm{ord}_{s=0}\zeta_{F,S,T}(s).$$

Further we have

$$\lim_{s\to 0} \frac{\zeta_{K,S,T}(s)}{\zeta_{F,S,T}(s)} = \prod_\chi L_{S,T}(\chi, 0) = \prod_\chi \chi(\theta_G), \tag{6}$$

where χ runs through the faithful characters of G. On the other hand, by (3), we have

$$\lim_{s\to 0} \frac{\zeta_{K,S,T}(s)}{\zeta_{F,S,T}(s)} = \pm \frac{h_{K,S,T} R_{K,S,T}}{h_{F,S,T} R_{F,S,T}}. \tag{7}$$

Gross [9, (6.4), (6.5)] showed that

$$\frac{R_{K,S,T}}{R_{F,S,T}} = \frac{l^{|S(K)|-1}}{(U_{K,S,T} : U_{F,S,T})}.$$

The denominator of the right hand side is 1 by Lemma 5.2, hence

$$\frac{R_{K,S,T}}{R_{F,S,T}} = l^{|S(K)|-1}.$$

The assertion of the proposition then immediately follows from (6) and (7). □

Proposition 5.4. *Assume that $m_n = m - 1$. Let ρ be an element of G of order l. Then we have an equality*

$$I_G(S_1) = I_G^{N-l^{m_0}+1} \cap (\rho - 1)\mathbb{Z}[G] \tag{8}$$

and an isomorophism

$$I_G(S_1)/I_G I_G(S_1) \cong \mathbb{Z}/l\mathbb{Z}. \tag{9}$$

Proof. See [22]. □

Corollary 5.5. *If K/k is a cyclic l-extension such that $m_0 = 0$ and $m_n = m - 1$, then Conjecture 3.2 is equivalent to Conjecture 4.1*

Proof. If $m_0 = 0$, then from (8) we have

$$I_G(S_1) = I_G^N \cap (\rho - 1)\mathbb{Z}[G],$$
$$I_G I_G(S_1) = I_G^{N+1} \cap (\rho - 1)\mathbb{Z}[G].$$

Since both θ_G and $\mathcal{R}_G$ belong to $(\rho - 1)\mathbb{Z}[G]$, this shows that Conjecture 3.2 is equivalent to Conjecture 4.1. □

Proof of Theorem 5.1. Let $N_{\mathbb{Q}(\zeta_{l^m})/\mathbb{Q}}$ denote the norm map from $\mathbb{Q}(\zeta_{l^m})$ to $\mathbb{Q}$. Then by Proposition 5.3 we have

$$\mathrm{ord}_l\left(N_{\mathbb{Q}(\zeta_{l^m})/\mathbb{Q}}(\chi(\theta_G))\right) = |S(K)| - 1 + \nu,$$

where $\nu = \mathrm{ord}_l(h^*_{K,S,T})$. Since l completely ramifies in $\mathbb{Q}(\zeta_{l^m})$, it follows from this that

$$\mathrm{ord}_{\mathfrak{l}}(\chi(\theta_G)) = |S(K)| - 1 + \nu.$$

Since $|S(K)| - 1 = N + l^{m-1} - 1$ and $\theta_G \in (\rho - 1)\mathbb{Z}[G]$, from Proposition 5.3 and the lemma of [22] we deduce that

$$\theta_G \in I_G^{N+\nu} \setminus I_G^{N+\nu+1}. \tag{10}$$

Thus $\theta_G \in I_G(S_1)$ by Proposition 5.4. This proves the first statement.

If $m_0 > 0$, then $l^{m_0} > 1$, whence

$$I_G I_G(S_1) \supseteq I_G^N \cap (\rho - 1)\mathbb{Z}[G]$$

by Proposition 5.4. Therefore $\theta_G \in I_G I_G(S_1)$ by Theorem 3.1. If $m_0 = 0$, then by the same proposition we have

$$I_G I_G(S_1) = I_G^{N+1} \cap (\rho - 1)\mathbb{Z}[G]. \tag{11}$$

Therefore from (10) and (11) we deduce that $\theta_G \in I_G I_G(S_1)$ if and only if $h^*_{K,S,T} \equiv 0 \pmod{l}$. This completes the proof. □

6. Reduction to cyclic l-extensions

We wish to reduce Theorem 4.2 to the case of cyclic l-extensions. For that purpose we consider the ring homomorphism $\Psi_l : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G_l]$ induced from the canonical surjection $G \longrightarrow G_l$. Let

$$\Psi = \oplus\Psi_l : \mathbb{Z}[G] \longrightarrow \bigoplus_l \mathbb{Z}[G_l],$$

where l runs through the prime numbers dividing $|G|$. For any place $v \in S_1$, we have $\Psi_l(I_G(v)) = I_{G_l}(v)$ and hence $\Psi_l(I_G(S_1)) = I_{G_l}(S_1)$. If $*$ denotes either v or S_1, then we define the map

$$\Psi_* : I_G(*) \longrightarrow \bigoplus_l I_{G_l}(*)$$

to be the restriction of Ψ to $I_G(*)$.

Proposition 6.1. *The following assertions hold for the maps Ψ_v and Ψ_{S_1}.*

(i) *Both Ψ_v and Ψ_{S_1} are surjective.*
(ii) $\mathrm{Ker}(\Psi_v) = \mathrm{Ker}(\Psi_{S_1})$.
(iii) *The maps Ψ_v and Ψ_{S_1} respectively induce isomorphisms*

$$I_G(v)/I_G(S_1) \cong \bigoplus_l I_{G_l}(v)/I_{G_l}(S_1),$$

$$I_G(S_1)/I_G I_G(S_1) \cong \bigoplus_l I_{G_l}(S_1)/I_{G_l} I_{G_l}(S_1),$$

where l runs through the prime numbers dividing $|G|$.

Before giving the proof of this proposition, we show how the proof of Theorem 4.2 can be reduced to the case of cyclic l-extensions. We continue to use the notation above and assume that condition (5) holds. Then θ_G belongs to $I_G(v_n)$. Suppose that Theorem 6.1 is true for any G_l, that is, for each prime divisor l of $|G|$, θ_{G_l} belongs to $I_{G_l}(S_1)$ and we have a congruence

$$\theta_{G_l} \equiv c_l \cdot h\mathcal{R}_{G_l} \pmod{I_{G_l} I_{G_l}(S_1)} \tag{12}$$

for some integer c_l prime to l. Since $\Psi_l(\theta_G) = \theta_{G_l}$, Proposition 6.1, (iii) shows that θ_G belongs to $I_G(S_1)$. Let c be an integer such that $c \equiv c_l \pmod{l}$ for any prime l dividing $|G|$. By Proposition 5.4, $I_{G_l}(S_1)/I_{G_l} I_{G_l}(S_1)$ is trivial or isomorphic to $\mathbb{Z}/l\mathbb{Z}$ according as $|G_{v,l}| = 1$ or l. It follows that

$$\Psi_l(c \cdot h\mathcal{R}_G) \equiv c_l \cdot h\mathcal{R}_{G_l} \pmod{I_{G_l} I_{G_l}(S_1)}$$

for all l dividing $|G|$. Then Proposition 6.1, (iv) and (12) shows that

$$\theta_G \equiv c \cdot h\mathcal{R}_G \pmod{I_G I_G(S_1)},$$

as desired. □

To state the following lemma, for any subgroup H of G, we denote by I_H the kernel of the natural surjection $\mathbb{Z}[G] \to \mathbb{Z}[G/H]$.

Lemma 6.2. *Let G a finite abelian group and G_1, G_2 subgroups of G such that* $\mathrm{GCD}(|G_1|, |G_2|) = 1$. *Then*

$$I_{G_1} I_{G_2} \subseteq I_{G_1}^t I_{G_2} + I_{G_1} I_{G_2}^t.$$

for any positive integer t.

Proof. We have only to show that

$$(g_1 - 1)(g_2 - 1) \in I_{G_1}^t I_{G_2} + I_{G_1} I_{G_2}^t \tag{13}$$

for any $g_i \in G_i$ and any positive integer t. First we note that $|G_i|(g_i - 1) \in I_{G_i}^2$ for $i = 1, 2$. By induction on t one can easily see that $|G_i|^t (g_i - 1) \in I_{G_i}^{t+1}$ for any positive integer t. Since $\mathrm{GCD}(|G_1|, |G_2|) = 1$, there exist integers a_1, a_2 such that $a_1 |G_1|^t + a_2 |G_2|^t = 1$. Then the identity

$$(g_1 - 1)(g_2 - 1) = a_1 |G_1|^t (g_1 - 1)(g_2 - 1) + a_2 |G_2|^t (g_1 - 1)(g_2 - 1)$$

shows that equation (13) holds, completing the proof. □

Proof of Proposition 6.1. It is clear from the definition that

$$\Psi_l(I_{G_{v,l}}) = I_{G_l}(v) \tag{14}$$

for any $v \in S$ and for any prime l dividing $|G|$. Since $I_G(v)$ is generated by $I_{G_{v,l}}$ as l ranges over the prime divisors of $|G|$, it follows from (14) that Ψ_v is surjective. From (14) and the definition of Ψ_l we also deduce that

$$\Psi_l \left(\prod_{v \in S} I_{G_{v,l'}} \right) = \begin{cases} I_{G_l}(S_1) & \text{if } l = l', \\ 0 & \text{otherwise.} \end{cases}$$

Since $I_G(S_1)$ contains $\prod_{v \in S_1} I_{G_{v,l}}$ for all l, we conclude that the map Ψ_{S_1} is also surjective.

To prove (ii) note that the ideal $\mathrm{Ker}(\Psi_v)$ is generated by the products $I_{G_{v,l}} I_{G_{v,l'}}$ of two ideals $I_{G_{v,l}}$ and $I_{G_{v,l'}}$ as l, l' runs through distinct prime divisors of $|G|$. By Lemma 6.2 we have an inclusion

$$I_{G_{v,l}} I_{G_{v,l'}} \subseteq I_{G_{v,l}}^t I_{G_{v,l'}} + I_{G_{v,l}} I_{G_{v,l'}}^t$$

for any positive integer t. Since $I_{G_{v,l}}^t \subseteq I_G(S_1)$ for any $t \geq n$, this shows that $I_{G_{v,l}} I_{G_{v,l'}} \subseteq I_G(S_1)$. Therefore $\mathrm{Ker}(\Psi_v) \subseteq I_G(S_1)$, whence $\mathrm{Ker}(\Psi_{S_1}) = \mathrm{Ker}(\Psi_v)$.

To prove the first isomorphism of (iii), for $* = v$ or S_1 let

$$P_G(*) = \bigoplus_l I_{G_l}(*).$$

Since $P_G(v)/P_G(S_1)$ is isomorphic to $\bigoplus_l I_{G_l}(v)/I_{G_l}(S_1)$, Ψ_v induces a map

$$\overline{\Psi}_v : I_G(v)/I_G(S_1) \longrightarrow P_G(v)/P_G(S_1).$$

We have to show that $\overline{\Psi}_v$ is an isomorphism. To this end, consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_G(S_1) & \longrightarrow & I_G(v) & \longrightarrow & I_G(v)/I_G(S_1) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \Psi_{S_1}} & & \downarrow{\scriptstyle \Psi_v} & & \downarrow{\scriptstyle \overline{\Psi}_v} & & \\ 0 & \longrightarrow & P_G(S_1) & \longrightarrow & P_G(v) & \longrightarrow & P_G(v)/P_G(S_1) & \longrightarrow & 0. \end{array}$$

Since both Ψ_{S_1} and Ψ_v are surjective, this diagram shows that $\overline{\Psi}_v$ is also surjective. Moreover by the snake lemma we have an exact sequence

$$0 \longrightarrow \mathrm{Ker}(\Psi_{S_1}) \longrightarrow \mathrm{Ker}(\Psi_v) \longrightarrow \mathrm{Ker}(\overline{\Psi}_v) \longrightarrow 0.$$

Then the equality $\mathrm{Ker}(\Psi_{S_1}) = \mathrm{Ker}(\Psi_v)$ shows that $\mathrm{Ker}(\overline{\Psi}_v) = 0$, whence $\overline{\Psi}_v$ is an isomorphism.

In order to prove the second isomorphism of (iii), let

$$Q_G(S_1) = \bigoplus_l I_{G_l} I_{G_l}(S_1).$$

Then $Q_G(S_1)$ is a subgroup of $P_G(S_1)$ and $P_G(S_1)/Q_G(S_1)$ is isomorphic to $\bigoplus_l I_{G_l}(S_1)/I_{G_l}I_{G_l}(S_1)$. Hence Ψ_{S_1} induces a map

$$\overline{\Psi}_{S_1} : I_G(S_1)/I_G I_G(S_1) \longrightarrow P_G(S_1)/Q_G(S_1).$$

To show that $\overline{\Psi}_{S_1}$ is an isomorphism, we consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_G I_G(S_1) & \longrightarrow & I_G(S_1) & \longrightarrow & I_G(S_1)/I_G I_G(S_1) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_{S_1}} & & \downarrow{\scriptstyle \Psi_{S_1}} & & \downarrow{\scriptstyle \overline{\Psi}_{S_1}} & & \\ 0 & \longrightarrow & Q_G(S_1) & \longrightarrow & P_G(S_1) & \longrightarrow & P_G(S_1)/Q_G(S_1) & \longrightarrow & 0, \end{array}$$

where φ_{S_1} denotes the restriction of Ψ_{S_1} to $I_G I_G(S_1)$. As we have seen above, Ψ_{S_1} is surjective. Moreover, quite similarly as in the proof of the surjectivity of Ψ_{S_1}, one can prove that φ_{S_1} is also surjective. Hence, by the snake lemma again, $\overline{\Psi}_{S_1}$ is also surjective and we obtain an exact sequence

$$0 \longrightarrow \mathrm{Ker}(\varphi_{S_1}) \longrightarrow \mathrm{Ker}(\Psi_{S_1}) \longrightarrow \mathrm{Ker}(\overline{\Psi}_{S_1}) \longrightarrow 0. \tag{15}$$

We wish to show that $\mathrm{Ker}(\overline{\Psi}_{S_1}) = 0$. To see this note that in the proof of (i) we have actually proved that $\mathrm{Ker}(\Psi_v)$ is contained in the ideal $I_G I_G(S_1)$. Therefore $\mathrm{Ker}(\Psi_{S_1})$ is also contained in the same ideal, whence $\mathrm{Ker}(\Psi_{S_1}) = \mathrm{Ker}(\varphi_{S_1})$. Thus from (15) we deduce that $\mathrm{Ker}(\overline{\Psi}_{S_1}) = 0$, as desired. This completes the proof of Proposition 6.1. □

7. The (S, T)-ambiguous class number

Let S, T be any finite sets of places of k such that $S \cap T = \emptyset$. (We do not impose any other condition on S and T.) Let J_k be the idèle group of k. If v is a place of k, then we denote by k_v and $\mathscr{O}_v$ the completion of k and the integer ring of k at v, respectively. We define the (S,T)-idèle group $J_{S,T} = J_{k,S,T}$ of k to be the subgroup

$$J_{S,T} = \prod_{v \in S} k_v^\times \times \prod_{v \in T} \mathscr{O}_{v,1}^\times \times \prod_{v \notin S \cup T} \mathscr{O}_v^\times$$

of J_k, where for $v \in T$ we put $\mathscr{O}_{v,1}^\times = \{u \in \mathscr{O}_v^\times \mid u \equiv 1 \pmod{v}\}$. Clearly we have

$$U_{S,T} = k^\times \cap J_{S,T}. \tag{16}$$

The (S,T)-idèle class group $C_{S,T} = C_{k,S,T}$ is defined to be the quotient group

$$C_{S,T} = J_{S,T}/U_{S,T}.$$

Let $C_k = J_k/k^\times$ be the idèle class group of k. It follows from (16) that the inclusion $J_{S,T} \hookrightarrow J_k$ induces an injective map $C_{S,T} \hookrightarrow C_k$. We define the (S,T)-ideal class group $Cl_{S,T} = Cl_{k,S,T}$ of k by

$$Cl_{S,T} = C_k/C_{S,T}.$$

Then $Cl_{S,T}$ is isomorphic to the ray class group $J_k/k^\times J_{S,T}$ corresponding to the subgroup $k^\times J_{S,T}$ of J_k. To see this, note that

$$\mathrm{Ker}(J_k/k^\times \longrightarrow J_k/k^\times J_{S,T}) = k^\times J_{S,T}/k^\times.$$

By (16) we have an isomorphism $k^\times J_{S,T}/k^\times \cong J_{S,T}/U_{S,T}$, whence

$$J_k/k^\times J_{S,T} \cong \frac{J_k/k^\times}{J_{S,T}/U_{S,T}} \cong C_k/C_{S,T} = Cl_{S,T}.$$

Let h be the (S,T)-class number defined in (1). This naming will be justified if we show that $h = |Cl_{S,T}|$. To show this, note that we have an exact sequence

$$0 \longrightarrow U_{S,T} \longrightarrow J_{S,T} \longrightarrow C_k \longrightarrow Cl_{S,T} \longrightarrow 0. \tag{17}$$

For simplicity we let $Cl_S := Cl_{S,\emptyset}$ (the S-ideal class group of k) and $J_S = J_{S,\emptyset}$ (the S-idèle group of k), respectively. Then, as a special case of (17), we have an exact sequence

$$0 \longrightarrow U_S \longrightarrow J_S \longrightarrow C_k \longrightarrow Cl_S \longrightarrow 0. \tag{18}$$

For any $v \in T$, let $\mathbb{F}_v$ be the residue field of v. Then two exact sequences (17) and (18) fit into the following commutative diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & U_{S,T} & & U_S & & \prod_{v\in T}\mathbb{F}_v^\times & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & J_{S,T} & \longrightarrow & J_S & \longrightarrow & \prod_{v\in T}\mathbb{F}_v^\times & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C_k & \longrightarrow & C_k & \longrightarrow & 0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & Cl_{S,T} & & Cl_S & & 0 & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

Applying the snake lemma to this diagram, we obtain an exact sequence

$$0 \longrightarrow U_{S,T} \longrightarrow U_S \longrightarrow \prod_{v\in T}\mathbb{F}_v^\times \longrightarrow Cl_{S,T} \longrightarrow Cl_S \longrightarrow 0.$$

Since $h_S = |Cl_S|$, it follows that

$$|Cl_{S,T}| = h_S \cdot \frac{\prod_{v\in T}(Nv-1)}{(U_S : U_{S,T})}.$$

Therefore $h = |Cl_{S,T}|$, as desired.

Now, let K/k be a finite Galois extension with the Galois group G. We define $U_{K,S,T}, J_{K,S,T}, C_{K,S,T}$, etc. similarly as above. Then, taking $H^\cdot(G,-)$ of the exact sequence

$$0 \longrightarrow U_{K,S,T} \xrightarrow{\alpha} J_{K,S,T} \xrightarrow{\beta} C_{K,S,T} \longrightarrow 0 \tag{19}$$

of G-modules, we obtain the long exact sequence

(20)

$$\begin{aligned}
0 \longrightarrow\ & U_{S,T} \xrightarrow{\alpha_0} J_{S,T} \xrightarrow{\beta_0} {C_{K,S,T}}^G \\
\longrightarrow\ & H^1(G,U_{K,S,T}) \xrightarrow{\alpha_1} H^1(G,J_{K,S,T}) \xrightarrow{\beta_1} H^1(G,C_{K,S,T}) \\
\longrightarrow\ & H^2(G,U_{K,S,T}) \xrightarrow{\alpha_2} H^2(G,J_{K,S,T}) \xrightarrow{\beta_2} H^2(G,C_{K,S,T}) \\
\longrightarrow\ & \cdots .
\end{aligned}$$

The next formula will play a key role in the proof of Theorem 4.2.

Theorem 7.1. *Suppose G is cyclic. Then*

$$\left|Cl_{K,S,T}{}^{G}\right| = \frac{h|\mathrm{Coker}(\alpha_2)|}{|G|}.$$

Proof. Since $H^1(G, C_K) = 0$, taking cohomology of the short exact sequence

$$0 \longrightarrow C_{K,S,T} \longrightarrow C_K \longrightarrow Cl_{K,S,T} \longrightarrow 0$$

yields the exact sequence

$$0 \longrightarrow C_{K,S,T}{}^{G} \longrightarrow C_K^G \longrightarrow Cl_{K,S,T}{}^{G} \longrightarrow H^1(G, C_{K,S,T}) \longrightarrow 0.$$

Noticing that $C_K^G = C_k$, we obtain

$$|Cl_{K,S,T}{}^{G}| = |H^1(G, C_{K,S,T})| \cdot |C_k/C_{K,S,T}{}^{G}|. \tag{21}$$

For any G-module M, let $Q(M)$ denote the Herbrand quotient:

$$Q(M) = \frac{|H^2(G, M)|}{|H^1(G, M)|}.$$

From the exact sequence (20) we deduce that

$$\frac{Q(J_{K,S,T})}{Q(U_{K,S,T})} \cdot |H^1(G, C_{K,S,T})| = |C_{K,S,T}{}^{G}/C_{S,T}| \cdot |\mathrm{Coker}(\alpha_2)|. \tag{22}$$

By class field theory we know that $Q(C_K) = |G|$. Moreover, we have $Q(Cl_{K,S,T}) = 1$ since $Cl_{K,S,T}$ is a finite group. Therefore, from the exact sequence

$$0 \longrightarrow C_{K,S,T} \longrightarrow C_K \longrightarrow Cl_{K,S,T} \longrightarrow 0$$

we obtain $Q(C_{K,S,T}) = |G|$. Since $Q(J_{K,S,T}) = Q(U_{K,S,T})Q(C_{K,S,T})$, it follows that $Q(J_{K,S,T})/Q(U_{K,S,T}) = |G|$. Therefore by (22) we have

$$|H^1(G, C_{K,S,T})| = \frac{|C_{K,S,T}{}^{G}/C_{S,T}| \cdot |\mathrm{Coker}(\alpha_2)|}{|G|}.$$

Substituting this into (21), we obtain

$$\begin{aligned} |Cl_{K,S,T}{}^{G}| &= \frac{|C_k/C_{K,S,T}{}^{G}| \cdot |C_{K,S,T}{}^{G}/C_{S,T}| \cdot |\mathrm{Coker}(\alpha_2)|}{|G|} \\ &= \frac{|C_k/C_{S,T}| \cdot |\mathrm{Coker}(\alpha_2)|}{|G|}. \end{aligned}$$

Since $|C_k/C_{S,T}| = |Cl_{S,T}| = h$, this proves the theorem. □

Remark 7.2. If S is the set of archimedean places S_∞ and $T = \emptyset$, then h is the usual class number h_k of k and Theorem 7.1 reduces to a well known formula for the ambiguous class number for the cyclic extension K/k:

$$|Cl_K{}^{G}| = \frac{h_k e(K/k)}{|G|(E_k : N_{K/k}K^\times \cap E_k)}, \tag{23}$$

where $h_k = |Cl_k|$, $e(K/k)$ and E_k denote the class number of k, the product of ramification indices in K/k of the places of k and the unit group of k, respectively. For this formula we refer the reader to [12, Lemma 4.1]. We should also remark that Federer [8] obtained a similar formula for $|{Cl_{K,S}}^G|$ when S is arbitrary. Thus our formula may be viewed as a generalization of those formulae. To see that (23) is a special case of Theorem 7.1, it suffices to prove the formula

$$|\mathrm{Coker}(\alpha_2)| = \frac{e(K/k)}{(E_k : N_{K/k}K^\times \cap E_k)} \tag{24}$$

in the case of $S = S_\infty, T = \emptyset$. To prove this note that

$$H^2(G, J_{K,S_\infty}) \cong \prod_v \mathscr{O}_v^\times / N_{K_w/k_v}(\mathscr{O}_w^\times) \cong \prod_v \mathbb{Z}/e_v\mathbb{Z},$$

where v runs through the places of k. Hence $|H^2(G, J_{K,S_\infty})| = e(K/k)$. Moreover, we have $H^2(G, U_{K,S_\infty}) \cong E_k/N_{K/k}E_K$, where $E_K = U_{K,S_\infty}$ is the unit group of K. Therefore (24) follows if we prove the formula

$$\mathrm{Ker}(\alpha_2) = \frac{N_{K/k}K^\times \cap E_k}{N_{K/k}E_K}.$$

But this is an easy consequence of the Hasse's norm theorem asserting the injectivity of the natural map

$$k^\times / N_{K/k}K^\times \longrightarrow \prod_v k_v^\times / N_{K_w/k_v}K_w^\times.$$

8. Cohomological interpretation of λ

Throughout this section we will assume that $(K/k, S, T)$ is an admissible data such that $G = \mathrm{Gal}(K/k)$ is a finite cyclic extension. In Section 1 we have defined λ to be a map from $U_{S,T}$ to $G \otimes X_S$. However, in order to give a cohomological interpretation of λ, it seems natural to replace the target group $G \otimes X_S$ with a subgroup $X_{G,S}$ defined below. To begin with, we let

$$Y_{G,S} = \bigoplus_{v \in S} G_v.$$

We will regard $Y_{G,S}$ as a subgroup of $G \otimes Y_S$ via the natural injection sending $(\ldots, g_v, \ldots)_{v\in S}$ to $\sum_{v\in S} g_v \otimes v$. Next we define a subgroup $X_{G,S}$ of $Y_{G,S}$ by the exact sequence

$$0 \longrightarrow X_{G,S} \longrightarrow Y_{G,S} \longrightarrow D_S \longrightarrow 0,$$

where D_S is the subgroup of G generated by G_v for all $v \in S$ and the map $Y_{G,S} \longrightarrow D_S$ is defined by sending $(\ldots, g_v, \ldots)_{v\in S}$ to $\prod_{v\in S} g_v$. Then the image of λ is contained in $X_{G,S}$. We will hereafter regard λ as a map

$$\lambda : U_{S,T} \longrightarrow X_{G,S}.$$

For example $\mathrm{Coker}(\lambda)$ will stand for the quotient group $X_{G,S}/\mathrm{Im}(\lambda)$.

We now wish to reveal a connection between the Gross regulator map λ and the (S,T)-ambiguous class number formula (Theorem 7.1). To this end, we start with studying $H^2(G, J_{K,S,T})$. For each place v of k, choose, once and for all, a place w of K lying above v. Then by Schapiro's lemma we have an isomorphism

$$H^2(G, J_K) \cong \bigoplus_v H^2(G_v, K_w^\times), \tag{25}$$

where v runs through the places of k. Let

$$\mathrm{pr}_S : H^2(G, J_K) \longrightarrow \bigoplus_{v\in S} H^2(G_v, K_w^\times).$$

be the projection to the S-part in the right hand side of (25). Similarly we have an isomorphism

$$H^2(G, J_{K,S,T}) \cong \bigoplus_{v\in S} H^2(G_v, K_w^\times) \oplus \bigoplus_{v\in T} H^2(G_v, \mathscr{O}_{w,1}^\times) \oplus \bigoplus_{v\notin S\cup T} H^2(G_v, \mathscr{O}_w^\times).$$

Lemma 8.1. *Both $H^2(G_v, \mathscr{O}_w^\times)$ and $H^2(G_v, \mathscr{O}_{w,1}^\times)$ vanish whenever $v \notin S$.*

Proof. First, for any v we have $H^2(G_v, \mathscr{O}_w^\times) \cong \mathbb{Z}/e_v\mathbb{Z}$, where e_v denotes the ramification index of v in the extension K/k. Therefore, if $v \notin S$, then K/k is unramified at v, and so $H^2(G_v, \mathscr{O}_w^\times) = 0$. Next, to see that $H^2(G_v, \mathscr{O}_{w,1}^\times)$ also vanishes for any $v \notin S$, we consider the long exact sequence

$$\cdots \longrightarrow H^1(G_v, \mathbb{F}_w^\times) \longrightarrow H^2(G_v, \mathscr{O}_{w,1}^\times) \longrightarrow H^2(G_v, \mathscr{O}_w^\times) \longrightarrow \cdots \tag{26}$$

obtained from the short exact sequence

$$0 \longrightarrow \mathscr{O}_{w,1}^\times \longrightarrow \mathscr{O}_w^\times \longrightarrow \mathbb{F}_w^\times \longrightarrow 0.$$

By Hilbert's theorem 90 we have $H^1(G_v, \mathbb{F}_w^\times) = 0$. From this and (26) it follows that $H^2(G_v, \mathscr{O}_{w,1}^\times) = 0$ for any $v \notin S$. This completes the proof. □

By this lemma we may view $H^2(G, J_{K,S,T})$ as a subgroup of $H^2(G, J_K)$. Thus, restricting the map pr_S to $H^2(G, J_{K,S,T})$, we obtain an isomorphism

$$\mathrm{pr}_S : H^2(G, J_{K,S,T}) \longrightarrow \bigoplus_{v\in S} H^2(G_v, K_w^\times).$$

Recall that the local invariant map

$$\mathrm{inv}_v : H^2(G_v, K_w^\times) \longrightarrow \frac{1}{|G_v|}\mathbb{Z}/\mathbb{Z}$$

is an isomorphism for any place v. Let

$$\mathscr{Y}_{G,S} = \bigoplus_{v\in S} \frac{1}{|G_v|}\mathbb{Z}/\mathbb{Z}.$$

Then the map

$$\mathrm{inv}_S := (\oplus_{v\in S}\mathrm{inv}_v)\circ \mathrm{pr}_S : H^2(G, J_{K,S,T}) \longrightarrow \mathscr{Y}_{G,S}$$

is an isomorphism. In order to study the image of $\mathrm{Im}(\alpha_2) \subseteq H^2(G, J_{K,S,T})$ under the map inv_S, let

$$s : \mathscr{Y}_{G,S} \longrightarrow \mathbb{Q}/\mathbb{Z}, \qquad (\ldots, y_v, \ldots)_{v\in S} \mapsto \sum_{v\in S} y_v$$

be the summation map. If we denote by D_S the subgroup of G generated by G_v for all $v \in S$, then $\mathrm{Im}(s) = \frac{1}{|D_S|}\mathbb{Z}/\mathbb{Z}$. We define $\mathscr{X}_{G,S}$ by the exact sequence

$$0 \longrightarrow \mathscr{X}_{G,S} \longrightarrow \mathscr{Y}_{G,S} \xrightarrow{s} \tfrac{1}{|D_S|}\mathbb{Z}/\mathbb{Z} \longrightarrow 0. \tag{27}$$

Lemma 8.2. $\mathrm{inv}_S(\mathrm{Im}(\alpha_2)) \subseteq \mathscr{X}_{G,S}$.

Proof. By class field theory we have an isomorphism

$$\mathrm{inv}_{K/k} : H^2(G, C_K) \longrightarrow \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}.$$

Let $\mathrm{inv}_{K/k,S} : H^2(G, C_{K,S,T}) \longrightarrow \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$ be the composite map of inv_S and the natural map $H^2(G, C_{K,S,T}) \longrightarrow H^2(G, C_K)$. Then we have a commutative diagram

$$\begin{array}{ccccccc}
 & & H^2(G, U_{K,S,T}) & \xrightarrow{\alpha_2} & H^2(G, J_{K,S,T}) & \xrightarrow{\beta_2} & H^2(G, C_{K,S,T}) \\
 & & & & \downarrow \mathrm{inv}_S & & \downarrow \mathrm{inv}_{K/k,S} \\
0 & \longrightarrow & \mathscr{X}_{G,S} & \longrightarrow & \mathscr{Y}_{G,S} & \xrightarrow{s} & \tfrac{1}{|G|}\mathbb{Z}/\mathbb{Z},
\end{array}$$

from which the assertion of the lemma follows. □

Now, the connecting homomorphism

$$\delta : \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \longrightarrow H^2(G, \mathbb{Z})$$

obtained from the short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

is an isomorphism since $H^i(G, \mathbb{Q}) = 0$ for $i > 0$. For any G-module M we consider the cup product

$$\cup : H^0(G, M) \times H^2(G, \mathbb{Z}) \longrightarrow H^2(G, M).$$

Choose and fix a faithful additive character $\psi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ of G. Then $\delta(\psi) \in H^2(G, \mathbb{Z})$ defines an homomorphism

$$\cup\delta(\psi) : M^G = H^0(G, M) \longrightarrow H^2(G, M), \quad x \mapsto x \cup \delta(\psi).$$

Lemma 8.3. *If M is torsion free, then the map $\cup\delta(\psi)$ is surjective.*

Proof. By [18, Chap. IX, §8, Theorem 14], the cup product

$$\hat{H}^0(G,M)\times H^2(G,\mathbb{Z})\longrightarrow H^2(G,M)$$

is a non-degenerate pairing. Since $H^2(G,\mathbb{Z})$ is a cyclic group generated by $\delta(\psi)$, this induces an isomorphism $\hat{H}^0(G,M)\cong H^2(G,M)$. Therefore the composite map

$$\cup\delta(\psi): M^G \twoheadrightarrow \hat{H}^0(G,M)\xrightarrow{\cong} H^2(G,M)$$

is also surjective. □

We define a map

$$\mu_\psi : U_{S,T}\longrightarrow \mathscr{X}_{G,S}$$

to be the composite map

$$U_{S,T}\xrightarrow{\cup\delta(\psi)} H^2(G,U_{K,S,T})\xrightarrow{\mathrm{inv}_S\circ\alpha_2}\mathscr{X}_{G,S}.$$

Since ψ is a faithful additive character of G, it induces an isomorphism $G_v\cong\frac{1}{|G_v|}\mathbb{Z}/\mathbb{Z}$ for any $v\in S$. We denote the map

$$Y_{G,S}\longrightarrow\mathscr{Y}_{G,S},\quad (\ldots,g_v,\ldots)_{v\in S}\mapsto(\ldots,\psi(g_v),\ldots)_{v\in S}$$

by the same notation ψ. Clearly this map is also an isomorphism.

Proposition 8.4. *Notation being as above, we have*

$$\psi\circ\lambda=\mu_\psi.$$

In particular, we have $|\mathrm{Coker}(\lambda)|=|\mathrm{Coker}(\mu_\psi)|$.

Proof. For each $v\in S$ we denote by

$$\mu_v : U_{S,T}\longrightarrow\frac{1}{|G_v|}\mathbb{Z}/\mathbb{Z}$$

the v-component of the map μ_ψ. Similarly let

$$\alpha_{i,v}: H^i(G,U_{K,S,T})\xrightarrow{\alpha_i} H^i(G,J_{K,S,T})\xrightarrow{\mathrm{pr}_v} H^i(G,K_w^\times)$$

be the v-component of the map α_i. Then we have a commutative diagram

$$\begin{array}{ccccc} U_{S,T} & \xrightarrow{\alpha_{0,v}} & k_v^\times & \xrightarrow{r_v} & G_v \\ \downarrow{\scriptstyle\cup\delta(\psi)} & & \downarrow{\scriptstyle\cup\delta(\psi)} & & \downarrow{\scriptstyle\psi} \\ H^2(G,U_{K,S,T}) & \xrightarrow[\alpha_{2,v}]{} & H^2(G_v,K_w^\times) & \xrightarrow[\mathrm{inv}_v]{} & \frac{1}{|G_v|}\mathbb{Z}/\mathbb{Z}. \end{array}\tag{28}$$

Indeed, the left square commutes by the functorial property of the cup product. The right square commutes by [18, Chap. XI, §3, Proposition 2]. Let

$$r_S=\oplus_{v\in S}r_v : J_{S,T}\xrightarrow{\mathrm{pr}_S}\bigoplus\nolimits_{v\in S}k_v^\times\xrightarrow{\oplus_{v\in S}r_v} Y_{G,S}.$$

Then $\lambda = r_S \circ \alpha_0$. From (28) we obtain a commutative diagram

$$\begin{array}{ccccc} U_{S,T} & \xrightarrow{\alpha_0} & J_{S,T} & \xrightarrow{r_S} & Y_{G,S} \\ \downarrow{\scriptstyle \cup\delta(\psi)} & & \downarrow{\scriptstyle \cup\delta(\psi)} & & \downarrow{\scriptstyle \psi} \\ H^2(G, U_{K,S,T}) & \xrightarrow[\alpha_2]{} & H^2(G_v, J_{K,S,T}) & \xrightarrow[\mathrm{inv}_S]{} & \mathscr{Y}_{G,S}. \end{array}$$

It follows that $\mu_\psi = \mathrm{inv}_S \circ \alpha_2 \circ \cup\delta(\psi) = \psi \circ r_S \circ \alpha_0 = \psi \circ \lambda$. This proves the proposition. □

The following proposition, which is a corollary of Theorem 7.1, will be useful when we relate θ_G with $h\mathcal{R}_G$.

Proposition 8.5. *Notation being as above, we have*

$$|(Cl_{K,S,T})^G| = \frac{h|\mathrm{Coker}(\lambda)|}{|G/D_S|}.$$

Proof. Since $U_{K,S,T}$ is torsion-free, the map

$$\cup\delta(\psi) : U_{S,T} \longrightarrow H^2(G, U_{K,S,T})$$

is surjective by Lemma 8.3. Thus we have a commutative diagram

$$\begin{array}{ccccccccc} & & U_{S,T} & \xrightarrow{\alpha_2 \circ \cup\delta(\psi)} & H^2(G, J_{K,S,T}) & \longrightarrow & \mathrm{Coker}(\alpha_2) & \longrightarrow & 0 \\ & & {\scriptstyle\lambda}\downarrow & & \cong\downarrow{\scriptstyle \mathrm{inv}_S} & & & & \\ 0 & \longrightarrow & \mathscr{X}_{G,S} & \longrightarrow & \mathscr{Y}_{G,S} & \longrightarrow & \frac{1}{|D_S|}\mathbb{Z}/\mathbb{Z} & \longrightarrow & 0. \end{array}$$

From this we obtain an exact sequence

$$0 \longrightarrow \mathrm{Coker}(\lambda) \longrightarrow \mathrm{Coker}(\alpha_2) \longrightarrow \frac{1}{|D_S|}\mathbb{Z}/\mathbb{Z} \longrightarrow 0.$$

Hence

$$|\mathrm{Coker}(\alpha_2)| = |D_S| \cdot |\mathrm{Coker}(\lambda)|.$$

Substituting this into the right hand side of the formula in Theorem 7.1, we obtain the desired equality

$$\left|(Cl_{K,S,T})^G\right| = \frac{h|D_S||\mathrm{Coker}(\lambda)|}{|G|}.$$

This proves the proposition. □

9. Proof of Theorem 3.3

In this section we will prove the following theorem which is equivalent to Theorem 3.3 under the assumption that $m_0 = 0$ and $m_n = m - 1$ (see Corollary 5.5).

Theorem 9.1. *Assume that G is a cyclic l-group and $m_0 = 0, m_n = m-1$. Then there exists an integer c prime to l such that*

$$\theta_G \equiv c \cdot h\mathcal{R}_G \pmod{I_G I_G(S_1)}.$$

We start with the following theorem, which is a counter part of Theorem 5.1.

Theorem 9.2. *Assume that G is a cyclic l-group and $m_n = m - 1$. Then the following assertions hold.*

(i) *If $m_0 > 0$, then $h\mathcal{R}_G \equiv 0 \pmod{I_G I_G(S_1)}$.*
(ii) *If $m_0 = 0$, then $h\mathcal{R}_G \equiv 0 \pmod{I_G I_G(S_1)}$ if and only if $|Cl_{K,S,T}{}^G| \equiv 0 \pmod{l}$.*

Before begining the proof of this theorem we will prove the following lemma, which I learned from Lee and is stated in [14, §4] without proof.

Lemma 9.3. *Notation and assumptions being as above, the (S,T)-class number h is divisible by l^{m_0}.*

Proof. Let M be the subextension of K/k such that $[M : k] = l^{m_0}$. Then every place in S splits completely in M. Let $S(M)$ denote the set of places of M lying above a place in S. Let $\langle S\rangle$ and $\langle S(M)\rangle$ be the subgroup of Cl_k and Cl_M generated by the prime ideals in S and $S(M)$ respectively. Then we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \langle S(M)\rangle & \longrightarrow & Cl_M & \longrightarrow & Cl_{M,S} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{M/k}} & & \downarrow{\scriptstyle N_{M/k}} & & \downarrow{\scriptstyle N_{M/k}} & & \\ 0 & \longrightarrow & \langle S\rangle & \longrightarrow & Cl_k & \longrightarrow & Cl_{k,S} & \longrightarrow & 0, \end{array}$$

where $N_{M/k}$ denotes the norm map. Since every place in S splits completely in M, the left vertical map is surjective. Therefore we have an isomorphism

$$Cl_k/N_{M/k}(Cl_M) \cong Cl_{k,S}/N_{M/k}(Cl_{M,S})$$

Since M/k is unramified, $Cl_k/N_{M/k}(Cl_M)$ (and hence $Cl_{k,S}/N_{M/k}(Cl_{M,S})$) is isomorphic to $\mathbb{Z}/l^{m_0}\mathbb{Z}$. This, in particular, implies that $|Cl_{k,S}|$ is divisible by l^{m_0}. Since h is a multiple of $|Cl_{k,S}|$, it follows that h is also divisible by l^{m_0}. □

Proof of Theorem 9.1. Suppose first that $m_0 > 0$. Then $h \equiv 0 \pmod{l}$ by Lemma 9.3. But, since $I_G(S_1)/I_G I_G(S_1) \cong \mathbb{Z}/l\mathbb{Z}$, this implies that $h\mathcal{R}_G \equiv 0 \pmod{I_G I_G(S_1)}$. This proves (i).

To prove (ii), let σ_{v_i} a generator of G_{v_i}. First we will prove that there exists an integer c prime to $|G|$ such that

$$\mathcal{R}_G \equiv c \cdot |\mathrm{Coker}(\lambda)| \cdot \prod_{i=1}^{n} (\sigma_{v_i} - 1) \pmod{I_G I_G(S_1)}. \tag{29}$$

To prove this, define n^2 integers a_{ij} by $r_{v_i}(u_j) = \sigma_{v_i}^{a_{ij}}$. Since the map $U_{S,T} \to I_G(v_i)/I_G I_G(v_i)$ sending $u \mapsto r_v(u) - 1 \pmod{I_G(v)^2}$ is a homomorphism, we have

$$\mathcal{R}_G \equiv \det(a_{ij}) \cdot \prod_{i=1}^{n} (\sigma_{v_i} - 1) \pmod{I_G I_G(S_1)}. \tag{30}$$

On the other hand we have a congruence

$$\det(a_{ij}) \equiv c \cdot |\mathrm{Coker}(\lambda)| \pmod{l} \tag{31}$$

with an integer c prime to l. Then (29) follows from (30) and (31) .

Now, combining Proposition 8.4 with (29), we obtain a congruence relation

$$\mathcal{R}_G \equiv c \cdot |\mathrm{Coker}(\lambda)| \cdot \prod_{v \in S_1} (\sigma_v - 1) \pmod{I_G I_G(S_1)}. \tag{32}$$

Note that $D_S = G$ since we are assuming that $m_0 = 0$. It then follows from Proposition 8.5 that $|Cl_{K,S,T}{}^G| = h|\mathrm{Coker}(\lambda)|$. From this and (32) we deduce that

$$h\mathcal{R}_G \equiv c \cdot |Cl_{K,S,T}{}^G| \cdot \prod_{v \in S_1} (\sigma_v - 1) \pmod{I_G I_G(S_1)}.$$

Therefore, $h_{K,S,T}\mathcal{R}_G$ belongs to $I_G I_G(S_1)$ if and only if $|Cl_{K,S,T}{}^G| \equiv 0 \pmod{l}$. This proves (ii). □

We would like to prove Theorem 3.3 by relating Theorem 9.2 to Theorem 5.1. For this end we will prove two lemmas.

Lemma 9.4. *Let G be a cyclic l-group and A a finite abelian G-module. Let H be the subgroup of G with $|H| = l$, and put $\nu = \sum_{h \in H} h \in \mathbb{Z}[G]$. Then the following conditions are equivalent.*

(i) $|A| \equiv 0 \pmod{l}$.
(ii) $|A^G| \equiv 0 \pmod{l}$.
(iii) $|\mathrm{Ker}(\nu : A \longrightarrow A)| \equiv 0 \pmod{l}$.

Proof. Clearly it suffices to show the lemma in the case where A is an l-group. Both implications (ii)⇒(i) and (iii)⇒(i) are trivial. To prove the converse implications, assume that (i) holds, namely $A \neq 0$. This, in

particular, means that the multiplication-by-l map on A is not injective. Let σ be a generator of G. Then we have an identity

$$(\sigma-1)^{|G|} = -\sum_{i=1}^{|G|-1} \binom{|G|}{i} (\rho-1)^i. \tag{33}$$

Since G is an l-group, we have $\binom{|G|}{i} \equiv 0 \pmod{l}$ for any integer i with $0 < i < |G|$. It follows from (33) that the map $\sigma - 1 : A \to A$ is not injective. This means that $A^G \neq 0$, hence (i)⇒(ii).

To prove the implication (i)⇒(iii), note that we have an identity

$$\nu^2 = l\nu.$$

This implies that the map $\nu : A \to A$ is not injective, or equivalently, $\mathrm{Ker}(\nu : A \longrightarrow A) \neq 0$. This proves (iii), completing the proof. □

Lemma 9.5. *Let M be the intermediate field of K/k such that $|S(M)| = |S(K)|$. If $U_{K,S,T}$ is torsion-free, then the natural map $Cl_{M,S,T} \to Cl_{K,S,T}$ is injective.*

Proof. Let $H = \mathrm{Gal}(K/M)$. First we show that $H^1(H, U_{K,S,T}) = 0$. For this end note that $U_{K,S,T} = U_{M,S,T}$ by Lemma 5.2. Therefore

$$H^1(H, U_{K,S,T}) = H^1(H, U_{M,S,T}) = \mathrm{Hom}(H, U_{M,S,T}).$$

The last group is trivial since H is a finite group and $U_{M,S,T} (\subseteq U_{K,S,T})$ is torsion-free, so $H^1(H, U_{K,S,T}) = 0$. Thus, taking $H^{\cdot}(H, -)$ of the exact sequence (19), we obtain an exact sequence

$$0 \longrightarrow U_{M,S,T} \longrightarrow J_{M,S,T} \longrightarrow {C_{K,S,T}}^H \longrightarrow 0. \tag{34}$$

This implies that $C_{M,S,T} \cong {C_{K,S,T}}^H$.

Now, consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_{M,S,T} & \longrightarrow & C_M & \longrightarrow & Cl_{M,S,T} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & {C_{K,S,T}}^H & \longrightarrow & {C_K}^H & \longrightarrow & {Cl_{K,S,T}}^H, & & \end{array}$$

where the vertical maps are natural maps. It is well known that the middle vertical map $C_M \to {C_K}^H$ is an isomorphism. By what we have shown above, the left vertical map $C_{M,S,T} \to C^H_{K,S,T}$ is also an isomorphism. As a consequence the right vertical map $Cl_{M,S,T} \to {Cl_{K,S,T}}^H$ is injective, hence the map $Cl_{M,S,T} \to Cl_{K,S,T}$ is also injective. □

Proof of Theorem 3.3. One can easily see that Conjecture 3.2 for the data $(K/k, S, T)$ implies the conjecture for any data $(K/k, S', T)$ with $S' \supset S$. Therefore we have only to prove Theorem 3.3 in the case where S is the union of the places ramifying in K and the archemidean places. If $m_0 > 0$,

then Theorem 4.2 becomes the trivial congruence $0 \equiv 0 \pmod{I_G I_G(S_1)}$ by Theorem 5.1,(i) and Theorem 9.2,(i). Suppose $m_0 = 0$. In this case, by Theorem 5.1,(ii) and Theorem 9.2,(ii), Theorem 4.2 reduces to the equivalence

$$\left|(Cl_{K,S,T})^G\right| \equiv 0 \pmod{l} \Longleftrightarrow h^*_{K,S,T} \equiv 0 \pmod{l}.$$

To show this, let $\nu = 1 + \rho + \cdots + \rho^{l-1} \in \mathbb{Z}[G]$ and $N_{K/F}$ the norm map from K to F. Since $Cl_{F,S,T} \to Cl_{K,S,T}$ is injective by Lemma 9.5, we have

$$\mathrm{Ker}(\nu : Cl_{K,S,T} \longrightarrow Cl_{K,S,T}) = \mathrm{Ker}(N_{K/F} : Cl_{K,S,T} \longrightarrow Cl_{F,S,T}).$$

Therefore, in view of Lemma 9.4, we have only to show the equality

$$h^*_{K,S,T} = |\mathrm{Ker}(N_{K/F} : Cl_{K,S,T} \longrightarrow Cl_{K,S,T})|. \tag{35}$$

First, consider the commutative diagram

$$\begin{array}{ccc} Cl_K & \longrightarrow & Cl_{K,S} \\ \Big\downarrow{\scriptstyle N_{K/F}} & & \Big\downarrow{\scriptstyle N_{K/F}} \\ Cl_F & \longrightarrow & Cl_{F,S}, \end{array} \tag{36}$$

where the both horizontal maps are surjective and the vertical maps are norm maps. Since every finite place of S ramifies completely in K/F, the norm map $N_{K/F} : Cl_K \to Cl_F$ is surjective. Therefore (36) shows that the norm map $N_{K/F} : Cl_{K,S} \to Cl_{F,S}$ is also surjective.

Next, consider the commutative diagram

$$\begin{array}{ccccccc} \prod_{w\in T(K)} \mathbb{F}_w^\times & \longrightarrow & Cl_{K,S,T} & \longrightarrow & Cl_{K,S} & \longrightarrow & 0 \\ \Big\downarrow & & \Big\downarrow{\scriptstyle N_{K/F}} & & \Big\downarrow{\scriptstyle N_{K/F}} & & \\ \prod_{v\in T(F)} \mathbb{F}_v^\times & \longrightarrow & Cl_{F,S,T} & \longrightarrow & Cl_{F,S} & \longrightarrow & 0, \end{array}$$

where the left vertical map is the norm map, and is surjective. The right vertical map is also surjective as we have seen above. Therefore the middle vertical map is also surjective. It follows that

$$|\mathrm{Ker}(N_{K/F} : Cl_{K,S,T} \longrightarrow Cl_{F,S,T})| = \frac{|Cl_{K,S,T}|}{|Cl_{F,S,T}|} = h^*_{K,S,T}.$$

Thus (35) holds, as desired. □

10. The Gross conjecture for abelian extensions over $\mathbb{Q}$

As a consequence of Corollary 4.4 we can give a proof of the Gross conjecture for abelian extensions of $\mathbb{Q}$ which simplifies our previous one [1].

Theorem 10.1. *If $k = \mathbb{Q}$, then Conjecture 2.1 is true, that is, the congruence*

$$\theta_G \equiv h\mathrm{det}_G(\lambda) \pmod{I_G^{n+1}}$$

holds for any admissible data $(K/\mathbb{Q}, S, T)$.

Actually we will prove this in a more general setting. To state it we need some notation. Let G be a finite abelian group such that

$$G = G_1 \times \cdots \times G_r, \tag{37}$$

where $G_1, \ldots, G_r$ are non-trivial cyclic groups of prime power order. Then $r = r(G)$ is independent of the decomposition. Fix a number field k. If K/k is a finite abelian extension, we denote by $S_{ram}(K/k)$ the set of places of k which ramify in K and by S_∞ the archimedean places of k. Define two integers $r(K/k)$ and $n(K/k)$ by

$$r(K/k) = r(\mathrm{Gal}(K/k)), \quad n(K/k) = |S_{ram}(K/k) \cup S_\infty| - 1.$$

Let $\mathcal{K}_k$ be the set of finite abelian extensions K/k such that $r(K/k) \geq n(K/k)$. If $K/k \in \mathcal{K}_k$, then we put

$$\delta(K/k) = (n(K/k), r(K/k) - n(K/k)) \in \mathbb{Z}^2_{\geq 0},$$

where $\mathbb{Z}_{\geq 0}$ denotes the set of non-negative integers.

Theorem 10.2. *If $K/k \in \mathcal{K}_k$, then Conjecture 2.1 is true for any admissible data $(K/k, S, T)$.*

Proof. We consider the lexicographic order on the set $\mathbb{Z}^2_{\geq 0}$. Thus for any $(a, b), (a', b') \in \mathbb{Z}^2_{\geq 0}$, we have $(a, b) > (a', b')$ if and only if either $a > a'$ or $a = a'$ and $b > b'$. Clearly the minimal element of $\mathbb{Z}^2_{\geq 0}$ is $(0, 0)$. We will prove Conjecture 2.1 for any admissible data $(K/k, S_{ram} \cup S_\infty, T)$ with $K/k \in K_k$ by induction on $\delta(K/k)$. If $\delta(K/k) = (0, 0)$, then Conjecture 2.1 is true as we have remarked in Proposition 2.2. Suppose $\delta(K/k) = (n, r - n) > (0, 0)$ and assume that the conjecture holds for any $K'/k \in \mathcal{K}_k$ with $\delta(K'/k) < \delta(K/k)$. Let $G = \mathrm{Gal}(K/k)$. In the decomposition (37), for each $i = 1, \ldots, r$, we let

$$\pi_i : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G/G_i]$$

be the ring-homomorphism induced from the natural surjections $\pi_i : G \to G/G_i$. If we set $K_i = K^{G_i}$, then $K_i/k \in \mathcal{K}_k$ and $\delta(K_i/k) < \delta(K/k)$ for all i. By the inductive hypothesis we have

$$\pi_i(\theta_G - h\mathrm{det}_G(\lambda)) \equiv \theta_{G/G_i} - h\mathrm{det}_{G/G_i}(\lambda) \equiv 0 \pmod{I^{n+1}_{G/G_i}}$$

for all i.

Here we need a lemma.

Lemma 10.3. *Let σ_i be a generator of G_i. Then*

$$\bigcap_{i=1}^{r} \pi_i^{-1}\left(I^{n+1}_{G/G_i}\right) = (\sigma_1 - 1) \cdots (\sigma_r - 1)\mathbb{Z}[G] + I^{n+1}_G$$

Proof. We use Darmon's trick ([6, §8]). For any $\alpha = \sum_{\sigma\in G} c_\sigma \sigma \in \mathbb{Z}[G]$, we consider the element

$$\alpha' = \sum_{\sigma} c_\sigma (\sigma_1 - 1)\cdots(\sigma_r - 1) \quad \in (\sigma_1 - 1)\cdots(\sigma_r - 1)\mathbb{Z}[G],$$

where for each $\sigma \in G$ we write $\sigma = \sigma_1 \cdots \sigma_r$ with $\sigma_i \in G_i$ according as the decomposition (37) of G. For each subset J of $\{1, \ldots, r\}$, we regard $G_J = \prod_{j\in J} G_j$ as a subgroup of G and let

$$\pi_J : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G/G_J]$$

be the natural surjection. Then we have

$$\alpha' = \sum_{J\subseteq\{1,\ldots,r\}} (-1)^{|J|} i_J(\pi_J(\alpha)), \tag{38}$$

where $i_J : \mathbb{Z}[G/G_J] \longrightarrow \mathbb{Z}[G]$ denotes the injection induced by the inclusion map $G/G_J \hookrightarrow G$. Clearly we have $i_J(I_{G/G_J}^{n+1}) \subseteq I_G^{n+1}$. Now, suppose $\pi_i(\alpha) \in I_{G/G_i}^{n+1}$ for all $i = 1, \ldots, r$. Then $\pi_J(\alpha) \in I_{G/G_J}^{n+1}$ for any non-empty J. Therefore (38) shows that

$$\alpha = \alpha' - \sum_{\emptyset\neq J\subseteq\{1,\ldots,r\}} (-1)^{|J|} i_J(\pi_J(\alpha)) \quad \in (\sigma_1 - 1)\cdots(\sigma_r - 1)\mathbb{Z}[G] + I_G^{n+1}.$$

This proves the inclusion

$$\bigcap_{i=1}^{r} \pi_i^{-1}\left(I_{G/G_i}^{n+1}\right) \subseteq (\sigma_1 - 1)\cdots(\sigma_r - 1)\mathbb{Z}[G] + I_G^{n+1}.$$

Since the converse inclusion is clear, the lemma holds. □

By this lemma, we have

$$\theta_G - h\mathrm{det}_G(\lambda) \in (\sigma_1 - 1)\cdots(\sigma_r - 1)\mathbb{Z}[G] + I_G^{n+1}.$$

If $r > n$, then this shows that $\theta_G \equiv h\mathrm{det}_G(\lambda) \pmod{I_G^{n+1}}$. Suppose $r = n$. Then there exists an integer a such that

$$\theta_G - h\mathrm{det}_G(\lambda) \equiv a(\sigma_1 - 1)\cdots(\sigma_n - 1) \pmod{I_G^{n+1}}. \tag{39}$$

Let $\varphi : G \to \Gamma$ be the maximal cyclic quotient of G such that $\varphi(\sigma_i) = \gamma$ for all i, where γ is a generator of Γ. Then $|\Gamma| = \mathrm{GCD}(|G_1|, \ldots, |G_n|)$. By Corollary 3.4 we know that

$$\varphi(\theta_G - h\mathrm{det}_G(\lambda)) \equiv \theta_\Gamma - h\mathrm{det}_\Gamma(\lambda) \equiv 0 \pmod{I_\Gamma^{n+1}}.$$

Since $\varphi((\sigma_1 - 1)\cdots(\sigma_n - 1)) = (\gamma - 1)^n$, this shows that

$$a(\gamma - 1)^n \equiv 0 \pmod{I_\Gamma^{n+1}}.$$

Note that $(\gamma-1)^n$ is a generator of the quotient group $I_\Gamma^n/I_\Gamma^{n+1} \cong \mathbb{Z}/|\Gamma|\mathbb{Z}$, this shows that $a \equiv 0 \pmod{|\Gamma|}$. Thus, if we show that

$$|\Gamma|(\sigma_1-1)\cdots(\sigma_n-1) \equiv 0 \pmod{I_G^{n+1}}, \tag{40}$$

then (39) proves that Conjecture 2.1 holds for $(K/k, S_{ram}, T)$. To show (40) note that there exist integers $a_1, \ldots, a_n$ such that

$$a_1|G_1| + \cdots + a_n|G_n| = |\Gamma|$$

since $|\Gamma| = \mathrm{GCD}(|G_1|, \ldots, |G_n|)$. Then the fact $|G_i|(\sigma_i - 1) \in I_G^2$ proves (40), as desired. The proof of Theorem 10.2 is now complete. □

Proof of Theorem 10.1. It suffices to prove Conjecture 2.1 for any admissible data $(\mathbb{Q}(\zeta_m)/\mathbb{Q}, S_m, T)$ for all positive integers m, where ζ_m is a primitive m-th root of unity and $S_m = \{\infty\} \cup \{\text{primes dividing } m\}$. By Theorem 10.2 we have only to show that $\mathbb{Q}(\zeta_m) \in \mathcal{K}_\mathbb{Q}$. Let $m = m_1 \cdots m_n$ be the decomposition of m into the product of prime powers with $\mathrm{GCD}(m_i, m_j) = 1$ $(i \neq j)$ and let $G_i = \mathrm{Gal}(\mathbb{Q}(\zeta_{m_i})/\mathbb{Q})$. Then

$$G \cong G_1 \times \cdots \times G_n.$$

Note that if we regard G_i as a subgroup of G, then G_i coincides with the inertia group of the prime dividing m_i. Thus $\mathbb{Q}(\zeta_m) \in \mathcal{K}_\mathbb{Q}$, as desired. □

References

[1] N. Aoki, *Gross' conjecture on the special values of abelian L-functions at $s = 0$*. Comm. Math. Univ. Sancti Pauli **40** (1991), 101–124.

[2] N. Aoki, J. Lee, K.S. Tan, *A refinement for a conjecture of Gross*. In preparation.

[3] D. Burns, *On relations between derivatives of abelian L-functions at $s = 0$*. Preprint (2002).

[4] D. Burns, J. Lee, *On refined class number formula of Gross*. To appear in J. Number Theory.

[5] Pi. Cassou-Nogues, *Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques*. Inv. Math. **51** (1979), 29–59.

[6] H. Darmon, *Thaine's method for circular units and a conjecture of Gross*. Canadian J. Math. **47** (1995), 302–317.

[7] P. Deligne, K. Ribet, *Values of Abelian L-functions at negative integers over totally real fields*. Inv. Math. **59** (1980), 227–286.

[8] L.J. Federer, *p-adic L-functions, Regulators, and Iwasawa modules*. PhD thesis (1982), Princeton University.

[9] B. Gross, *On the values of abelian L-functions at $s = 0$*. J. Fac. Univ. Tokyo **35** (1988), 177–197.

[10] D. Hayes, *The refined p-adic abelian Stark conjecture in function fields*, Invent. Math. **94** (1988), 505–527.

[11] A. Hayward, *A class number formula for higher derivatives of abelian L-functions*, Compositio Math. **140** (2004), 99–120.

[12] S. Lang, *Cyclotomic fields II*. GTM 69, Springer-Verlag, New-York Heidelberg Berlin (1980).

[13] J. Lee, *On Gross's Refined Class Number Formula for Elementary Abelian Extensions*. J. Math. Sci. Univ. Tokyo **4** (1997), 373–383.

[14] J. Lee, *Stickelberger elements for cyclic extensions and the order of zero of abelian L-functions at $s = 0$*. Compositio. Math. **138** (2003), 157–163.

[15] J. Lee, *On the refined class number formula for global function fields*. To appear in Math. Res. Letters.
[16] M. Reid, *Gross' conjecture for extensions ramified over three points of* $\mathbb{P}^1$. J. Math. Sci. Univ. Tokyo **10** (2003), 119–138.
[17] K. Rubin, *A Stark conjecture "over* $\mathbb{Z}$*" for abelian L-functions with multiple zeros*. Ann. Inst. Fourier, Grenoble **46**, 1 (1996), 33–62.
[18] J.-P. Serre, *Local Fields*. GTM 67, Springer-Verlag.
[19] K.-S. Tan, *On the special values of abelian L-functions*. J. Math. Sci. Univ. Tokyo **1** (1994), 305–319.
[20] K.-S. Tan, *A note on the Stickelberger elements for cyclic p-extensions over global function fields of characteristic p*. To appear in Math. Res. Letters.
[21] J. Tate, *Les Conjectures de Stark sur les Fonctions L d'Artin en* $s = 0$. Progress in Math. **47**, Birkhäuser, Boston-Basel-Stuttgart (1984).
[22] J. Tate, *Refining Gross's conjecture on the values of abelian L-functions*. To appear in Contemporary Math.
[23] M. Yamagishi, *On a conjecture of Gross on special values of L-functions*. Math. Z. **201** (1989), 391–400.

Noboru Aoki
Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Toshima-ku
Tokyo 171-8501, Japan
E-mail : aoki@rkmath.rikkyo.ac.jp