Compositio Mathematica **138:** 157–163, 2003.

Stickelberger Elements for Cyclic Extensions and the Order of Vanishing of Abelian L-Functions at $s = 0$

JOONGUL LEE
School of Mathematics, Korea Institute for Advanced Study, 207-43 Cheongryangri-dong, Dongdaemun-gu, Seoul, Republic of Korea

(Received: 26 June 2001; accepted in final form: 8 April 2002)

Abstract. We study the Stickelberger element of a cyclic extension of global fields of prime power degree. Assuming that S contains an almost splitting place, we show that the Stickelberger element is contained in a power of the relative augmentation ideal whose exponent is at least as large as Gross's prediction. This generalizes the work of Tate (see Section 4) on a refinement of Gross's conjecture in the cyclic case. We also present an example for which Tate's prediction does not hold.

Mathematics Subject Classification (2002). 11S42.

Key words. class numbers, Gross's conjecture, special values of Abelian L-functions, Stickelberger elements.

1. Introduction

Suppose L/K is an Abelian extension of global fields with Galois group G. Let S be a finite nonempty set of places of K which contains all Archimedean places and places ramified in L, and make a suitable choice of a finite nonempty set T of places of K so that T is disjoint from S and that $U_{S,T}$, the collection of S-units in K that are congruent to 1 modulo v for all $v \in T$, is torsion free.

For a complex character $\chi \in \hat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$, the S-T modified L-function is defined as

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

where $g_v \in G$ is the Frobenius element for v and $\mathrm{Re}(s) > 1$. The Stickelberger element $\theta_{S,T}$ is the unique element in $\mathbb{C}[G]$ that satisfies

$$\chi(\theta_{S,T}) = L_{S,T}(0, \chi)$$

for all $\chi \in \hat{G}$, where χ is regarded as a $\mathbb{C}$-algebra homomorphism from $\mathbb{C}[G]$ to $\mathbb{C}$, extended by linearity. In [1], Deligne and Ribet proved that $\theta_{S,T}$ is in $\mathbb{Z}[G]$. From now on we will write θ for $\theta_{S,T}$ if no confusion arises.

Suppose H is a subgroup of G with fixed field E. We define the augmentation ideal I_H relative to H to be the kernel of the natural map $\mathbb{Z}[G] \to \mathbb{Z}[G/H]$. When $H = G$, $I := I_G$ is the usual augmentation ideal of $\mathbb{Z}[G]$, and in general I_H is the $\mathbb{Z}[G]$-ideal generated by the image of the augmentation ideal of $\mathbb{Z}[H]$ via the natural embedding $\mathbb{Z}[H] \hookrightarrow \mathbb{Z}[G]$.

PROPOSITION 1. *Suppose* $|S| \geqslant 2$. *Then, the following are equivalent.*

(1) $\theta \in I_H$.
(2) $\chi(\theta) = 0$ *for all characters* χ *of* G *whose kernels contain* H.
(3) *For each cyclic subextension* E'/K *of* E/K, *there is a place in* S *that splits completely in* E'.

Proof. Let r be the number of places in S that split completely in E. Then for each $\chi \in \hat{G}$ whose kernel is H, the order of zero of $L_{S,T}(s, \chi)$ at $s = 0$ is $r - 1$ or r depending on whether χ is trivial or not (see [3, Proposition I.3.4]). Also, the natural map $\mathbb{Z}[G] \to \mathbb{Z}[G/H]$ sends θ for the extension L/K to θ for the extension E/K (see [3, Proposition IV.1.8]). Therefore (3) is equivalent to $L_{S,T}(0, \chi) = 0$ for all characters χ of G/H (which is (2)), which in turn is equivalent to (1). □

From now on, we assume that $|S| \geqslant 2$ and that S contains a place v which splits completely in E. Let r be the number of places in S that split completely in E. In [2, p. 195], Gross makes a remark that he expects that θ always belongs to I_H^{r-1}, and that θ belongs to I_H^r if $|S| \geqslant r + 1$. The following proposition shows that enlarging S by unramified primes does not affect the truth of this conjecture.

PROPOSITION 2. *Suppose* S *contains a non-Archimedean place* v *which is unramified in* L. *Let* $S_1 = S \backslash \{v\}$. *Then* $\theta_{S,T} \in \mathbb{Z}[G]\theta_{S_1,T}$, *and if* v *splits completely in* E, *then* $\theta_{S,T} \in I_H\theta_{S_1,T}$.

Proof. Let $g_v \in G$ be the Frobenius automorphism corresponding to v. Then $\theta_{S,T} = (1 - g_v)\theta_{S_1,T}$, and if v splits completely in E, then $g_v \in H$, hence $1 - g_v \in I_H$. □

In this paper, we consider the case when G is a cyclic group of order l^m where l is a prime number and $m \geqslant 2$, and H is a nontrivial subgroup of G. In this case, we say that a place v of K is an 'almost splitting' place if its decomposition group is of order l. Assuming S contains an almost splitting place, we prove that Gross's expectation holds. Furthermore we observe that there is an extra vanishing phenomenon which happens in many cases (see Theorem 6). This generalizes Tate's work on a refinement of Gross's conjecture under the present assumptions. Also using the techniques developed in Sections 2 and 3, we see that Tate's prediction may not hold if S does not contain a nonsplitting prime (see Section 5). Tate's work is described in Section 4 for the convenience of the reader.

2. The Cyclic Group Ring

Let G be a cyclic group of order l^m. Pick a generator σ of G and for each $i = 0, \dots, m$, set $G_i := \langle \sigma^{l^i} \rangle$. We have $[G : G_i] = l^i$, and $I_i := I_{G_i}$ is the principal ideal of $\mathbb{Z}[G]$ which is generated by $\sigma^{l^i} - 1$.

Let us choose a faithful character χ_m of G, and for each $i = 0, \dots, m-1$ we define $\chi_i := \chi_m^{l^{m-i}}$. Let $\zeta_i := \chi_i(\sigma)$ for $i = 1, \dots, m$ (so ζ_i is a primitive l^ith root of unity), and $\lambda_i := \zeta_i - 1 \in \mathbb{Z}[\zeta_i]$.

We may view $\mathbb{Z}[G]$ as a subring of $\prod_{i=0}^m \mathbb{Z}[\zeta_i]$ by identifying σ with $(1, \zeta_1, \zeta_2, \dots, \zeta_m)$. With respect to this embedding, the natural map $\mathbb{Z}[G] \to \mathbb{Z}[G/G_i]$ is the projection.

$$(\alpha_0, \dots, \alpha_m) \mapsto (\alpha_0, \dots, \alpha_i)$$

onto the first $i+1$ components. Therefore an element $\alpha = (\alpha_0, \dots, \alpha_m)$ is contained in I_i if and only if α is in the image of $\mathbb{Z}[G]$ and $\alpha_0 = \dots = \alpha_i = 0$.

Since the $\mathbb{Z}[G]$-ideal I_i is generated by $\sigma^{l^i} - 1$, the $\mathbb{Z}[G]$-ideal I_i^k is generated by $(\sigma^{l^i} - 1)^k$. Moreover, the following lemma holds.

LEMMA 3. *For each $i = 0, \dots, m-1$ and $k \geqslant 1$, the multiplication by $\sigma^{l^i} - 1$ defines an isomorphism from I_i^k to I_i^{k+1}.*

Proof. The multiplication by $\sigma^{l^i} - 1$ is clearly surjective. On the other hand, $\sigma^{l^i} - 1 = (0, \dots, 0, \lambda_1, \lambda_2, \dots, \lambda_{m-i})$ in $\prod_{i=0}^m \mathbb{Z}[\zeta_i]$. Now the injectivity follows as elements of I_i^k have their first $i+1$ components equal 0 and $\sigma^{l^i} - 1$ has its last $m-i$ components nonzero. □

The next theorem is the key for analyzing $\theta_{S,T}$ when S contains an almost splitting place.

THEOREM 4. *Suppose $\alpha = (0, \dots, 0, \alpha_m)$ is an element of $\prod_{i=0}^m \mathbb{Z}[\zeta_i]$. Then for each integer $k \geqslant 1$ and $i = 0, \dots, m-1$, $\alpha \in I_i^k$ if and only if $\lambda_1 \lambda_{m-i}^{k-1} \mid \alpha_m$ in $\mathbb{Z}[\zeta_m]$.*

Proof. First we prove the equivalence for $k = 1$. In that case, the latter condition is independent of i, and $I_{m-1} = I_i \cap \{(\alpha_0, \dots, \alpha_m) \mid \alpha_j = 0 \text{ for } 0 \leqslant j \leqslant m-1\}$ which implies that the first condition is also independent of i. Therefore we may assume $i = m-1$.

I_{m-1} is generated by $\sigma^{l^{m-1}} - 1$ whose image in $\prod_{i=0}^m \mathbb{Z}[\zeta_i]$ is $(0, \dots, 0, \lambda_1)$. Therefore α is in I_{m-1} if and only if there exists an element $\beta = (\beta_0, \dots, \beta_m) \in \mathbb{Z}[G]$ that satisfies $\beta_m \lambda_1 = \alpha_m$. Now this condition is clearly equivalent to $\lambda_1 \mid \alpha_m$ as the map $\chi_m \colon \mathbb{Z}[G] \to \mathbb{Z}[\zeta_m]$ is surjective.

The case $k \geqslant 2$ follows easily from the case $k = 1$ together with Lemma 3. □

3. Comparison of the Zeta Functions

In this section, we investigate the case where L/K is an extension of global fields, with Galois group G as in Section 2. Suppose $S = \{v_0, \dots, v_n\}$. For each

$j = 0, \ldots, n$, let G_{v_j} be the decomposition group of v_j and let $l^{m_j} = [G : G_{v_j}]$. Without loss of generality, we may assume that $0 \leqslant m_0 \leqslant m_1 \leqslant \cdots \leqslant m_n$. When $m_n = m$, v_n splits completely in L and so $\theta = 0$. We consider the next case $m_n = m - 1$, in other words v_n is an almost splitting place.

Remark. If K is a number field, then $\theta = 0$ unless $l = 2$, K is totally real and L is totally complex, as the Archimedean places of S split in L if those conditions are not satisfied. If $\theta \neq 0$, then the Archimedean places of S almost split in L, hence in the number field case we may assume that S always contains an almost splitting place.

Theorem 4 can be translated in the style of [2, Lemma 6.1] to the following lemma.

LEMMA 5. *Assume $\theta \in I_{m-1}$. Then for $0 \leqslant i \leqslant m-1$ and for $k \geqslant 1$, the following are equivalent:*

(1) $\theta \in I_i^k$
(2) *the λ_m-valuation of $L_{S,T}(0, \chi_m)$ is greater than or equal to $l^{m-1} + (k-1)l^i$*
(3) *the l-valuation of $\prod_\chi L_{S,T}(0, \chi)$ is greater than or equal to $l^{m-1} + (k-1)l^i$, where the product is taken over the faithful characters of G.*

Proof. If we write $\theta = (0, \ldots, 0, \theta_m)$, then $\theta_m = \chi_m(\theta) = L_{S,T}(0, \chi_m)$. Therefore, $\prod_\chi L_{S,T}(0, \chi)$ is the norm of θ_m from $\mathbb{Q}(\zeta_m)$ to $\mathbb{Q}$.
l is totally ramified in $\mathbb{Z}[\zeta_m]$ and (λ_m) is the unique prime ideal of $\mathbb{Z}[\zeta_m]$ above l. Therefore the l-valuation of the norm of θ_m is equal to the (λ_m)-valuation of θ_m, and in $\mathbb{Z}[\zeta_m]$ the ideal (λ_{m-i}) is equal to $(\lambda_m^{[\mathbb{Q}(\zeta_m):\mathbb{Q}(\zeta_{m-i})]}) = (\lambda_m^{l^i})$, as it is totally ramified in $\mathbb{Q}(\zeta_m)$. Now the lemma follows from Theorem 4. □

Let F be the fixed field of G_{m-1}. The product in part (3) of Lemma 5 can be expressed as

$$\lim_{s \to 0} \left\{ \frac{\zeta_{L,S,T}(s)}{\zeta_{F,S,T}(s)} \right\}.$$

$\mathrm{Gal}(L/F)$ is cyclic of order l, and in that case Gross used the class number formula to prove that the above limit is divisible by $l^{|S(F)|-1}$ in [2, Section 6]. Note that $|S(F)| = |S(L)| = \sum_{j=0}^{n} l^{m_j}$.

Fix i in $\{0, \ldots, m-1\}$, and let r be the number of places of S whose decomposition group is contained in G_i. In other words, r is the number of places v_j in S that satisfies $m_j \geqslant i$. We also define N to be the largest integer less than or equal to $1 + l^{-i}(|S(F)| - 1 - l^{m-1}) = 1 - l^{-i} + \sum_{j=0}^{n-1} l^{m_j - i}$. We obtain the following theorem as a simple consequence of Lemma 5.

https://doi.org/10.1023/A:1026128923148 Published online by Cambridge University Press

THEOREM 6. *In the situation described above, θ is contained in I_i^N. Moreover, $N = r - 1$ if and only if the decomposition group of each place of S other than the almost splitting place is G_i, and otherwise $N \geqslant r$.*

4. Tate's Refinement of Gross's Conjecture

We present Tate's work in this section—this section is a summary of [4]. We continue to assume that G is cyclic of order l^m and that S contains an almost splitting place. Consider the case $H = G$, or equivalently $i = 0$. Pick a faithful character χ of G, and as in Section 2, set $\lambda_i := \chi(\sigma^{l^{m-i}}) - 1$, and $\lambda := \lambda_m$. In that case $I = I_0$ is the usual augmentation ideal, and as we have shown in Section 3,

(1) if α is in I_{m-1}, then α is in I^k if and only if the λ-valuation of $\chi(\alpha)$ is greater than or equal to $l^{m-1} + k - 1$
(2) $\theta \in I^N$, where $N = \sum_{j=0}^{n-1} l^{m_j} = \sum_{v \in S}[G : G_v] - l^{m-1}$.

Gross's conjecture implies $\theta \in I^n$, and we have $N \geqslant n$ with equality if and only if the n places in S other than the almost splitting place do not split at all.

Tate's idea is that there should be a congruence

$$\theta \equiv \pm hR \pmod{I^{N+1}}$$

where h is the S-T class number of K, R is the determinant of an $(n \times n)$-matrix, and the sign is determined by the analogous classical formula as in [2]. He takes $R := \det_{1 \leqslant i,j \leqslant n}(f_j(u_i) - 1)$, where $f_j : K_{v_j}^* \longrightarrow G_{v_j}$ is the local reciprocity law homomorphism, and where $\{u_i\}$ is a $\mathbb{Z}$-basis for the group $U_{S,T}$ of S-T units of K.

For each i, there are integers a_{ij}, determined mod l^{m-m_j}, hence mod l, such that $f_j(u_i) = \sigma^{l^{m_j} a_{ij}}$. Then $\chi(f_j(u_i)) = (1 + \lambda_{m_j})^{a_{ij}} \equiv 1 + a_{ij}\lambda_{m_j} \pmod{\lambda^{l^{m_j}+1}}$ and hence $\chi(R) \equiv (\det a_{ij})\lambda^M \pmod{\lambda^{M+1}}$, where $M = \sum_{j=1}^n l^{m_j} = N + l^{m-1} - l^{m_0}$. From this it is easy to see that $\chi(R) (\mathrm{mod}\, \lambda^{M+1})$ is independent of the choice of basis for $U_{S,T}$ and of the choice of place $v_0 \in S$ with the least splitting in L.

Tate makes a remark that if $m_0 = 0$ (so that $R \in I^N$), then he has obtained a fair amount of numerical evidence for his conjectural congruence relation, which is stronger than Gross's in general. On the other hand, when $m_0 > 0$, the congruence relation boils down to the statement: $m_0 > 0$ implies $\theta \in I^{N+1}$, as l^{m_0} divides h in that case. He asks if this statement is always true. In the next section we construct an example in which $m_0 > 0$ and $\theta \notin I^{N+1}$, providing a negative answer to Tate's question.

5. An Example

Let us take K to be a rational function field $\mathbb{F}_q(t)$ with $q \not\equiv 1 \pmod{l}$, and take L to be the constant field extension of K of degree l^m. Then L/K is cyclic and unramified everywhere. We choose S and T so that all the places of S have degrees divisible by l, and that T only contains places whose residue fields do not contain a primitive lth root of 1. The assumption on S is equivalent to the condition $m_0 > 0$.

Pick a place v of degree 1, and set $S' = S \cup \{v\}$. We first prove that $\theta_{S',T} \notin I^{N'+1}$ where $N' = \sum_{v \in S'}[G : G_v] - l^{m-1}$. We remind the reader that F is the unique subextension of L/K with $[L : F] = l$. The discussion near the end of Section 3 shows that $\theta_{S',T}$ is in $I_G^{N'+1}$ if and only if the Stickelberger element $\theta_{S'(F),T(F)}$ for the extension L/F is in $I^{|S'|}$. Using Gross's result in [2, Section 6], we see that $\theta_{S'(F),T(F)}$ is not contained in $I^{|S'|}$ if

(1) the S'-class number of F and L are both prime to l
(2) F does not contain a primitive lth root of 1
(3) none of the residue fields of $T(L)$ contain a primitive lth root of 1.

As S' contains a place v of degree 1, $G_v = G$ and the S'-class number of F and L are both 1. Neither L (and hence F) nor the residue fields of $T(L)$ contain a primitive lth root of unity – the lth cyclotomic polynomial has degree $l - 1$, therefore if k_2/k_1 is a field extension of degree some power of l such that k_2 contains a primitive lth root of 1, then this root is in fact contained in k_1. So we conclude that $\theta_{S',T} \notin I^{N'+1}$.

One has $\theta_{S',T} = (1 - g_v)\theta_{S,T}$, and Lemma 3 implies that $\theta_{S,T} \in I^{N+1}$ if and only if $\theta_{S',T} \in I^{N'+1}$ where $N = \sum_{v \in S}[G : G_v] - l^{m-1} = N' - 1$. Therefore $\theta_{S,T} \notin I^{N+1}$, providing a negative answer to Tate's question.

Remarks. (1) When L/K is a constant field extension of global function fields, everything can be made explicit. Therefore, in the above example one can check that $\theta_{S,T}$ does not belong to I^{N+1} by direct computation.

(2) The above example suggests a possible remedy of Tate's refinement in the general case. Namely, pick a nonsplitting place v which is not in $S \cup T$ (possible by Tchebotarev density theorem), and set $S' = S \cup \{v\}$. By Lemma 3, there is a unique element $\kappa \in I^N/I^{N+1}$ such that $(1 - g_v)\kappa = h_{S',T}R_{S',T} \in I^{N+1}/I^{N+2}$, and κ is independent of the choice of the nonsplitting place v. The congruence relation $\theta_{S,T} \equiv \kappa (\mathrm{mod}\, I^{N+1})$ is equivalent to Tate's statement for $\theta_{S',T}$, and we may take it as a suitable generalization of Gross's conjecture.

Acknowledgements

This work was inspired by the work of Tate on a refinement of Gross's conjecture, and the author is very grateful to Tate for many insightful comments and warmest encouragements, and for granting permission to reproduce his work in this paper. This research was performed while the author was visiting Max-Planck Institut für Mathematik and the BK21 program of the Mathematics Department, Yonsei University, and he would like to thank them for their hospitality during his stay.

References

1. Deligne, P. and Ribet, K.: Values of Abelian L-functions at negative integers over totally real fields, *Invent. Math.* **59** (1980), 227–286.
2. Gross, B.: On the values of Abelian L-functions at $s=0$, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **35** (1988), 177–197.
3. Tate, J.: *Les conjectures de Stark sur les fonctions L d'Artin en* $s=0$, Birkhäuser, Basel-Boston, 1984.
4. Tate, J.: Private communication, 1997.