

ON THE l -ADIC IWASAWA λ -INVARIANT IN A p -EXTENSION

EDUARDO FRIEDMAN AND JONATHAN W. SANDS
(WITH AN APPENDIX BY LAWRENCE C. WASHINGTON)

ABSTRACT. For distinct primes l and p , the Iwasawa invariant λ_l^- stabilizes in the cyclotomic \mathbb{Z}_p -tower over a complex abelian base field. We calculate this stable invariant for $p = 3$ and various l and K . Our motivation was to search for a formula of Riemann-Hurwitz type for λ_l^- that might hold in a p -extension. From our numerical results, it is clear that no formula of such a simple kind can hold. In the course of our calculations, we develop a method of computing λ_l^- for an arbitrary complex abelian field and, for $p = 3$, we make effective Washington's theorem on the stabilization of the l -part of the class group in the cyclotomic \mathbb{Z}_p -extension. A new proof of this theorem is given in the appendix.

INTRODUCTION

Our purpose here is to investigate the connection between a certain type of cyclotomic Iwasawa λ_l -invariant attached to a base field and the corresponding invariant attached to an extension field of degree prime to l . To simplify this investigation, the base field K will be a finite complex abelian Galois extension of the rational field \mathbb{Q} , and the prime number l will be odd. A \mathbb{Z}_l -extension of K is a field extension \mathfrak{K}/K such that $\text{Gal}(\mathfrak{K}/K)$ is topologically isomorphic to the additive group \mathbb{Z}_l of the l -adic integers. The cyclotomic \mathbb{Z}_l -extension $K_{l\infty}$ of K may be defined as the unique \mathbb{Z}_l -extension of K contained in the field obtained by adjoining all l -power roots of unity to K . Fix an embedding of $K_{l\infty}$ in the complex numbers \mathbb{C} , and let τ represent complex conjugation. Let K_{l^n} be the subfield of $K_{l\infty}$ having degree l^n over K , and let $A_l(K_{l^n})$ be the l -Sylow subgroup of the ideal class group of K_{l^n} . Complex conjugation acts on this group, and we let $A_l^-(K_{l^n})$ denote the subgroup consisting of elements c such that $c^\tau = c^{-1}$. The theorems of Iwasawa [12] and Ferrero and Washington [6] imply that there exist integers $N(K)$, $\lambda^- = \lambda_l^-(K)$ and $\nu^- = \nu_l^-(K)$ such that the order of $A_l^-(K_{l^n})$ is given by the formula

$$|A_l^-(K_{l^n})| = l^{n\lambda^- + \nu^-}$$

Received by the editor February 15, 1994 and, in revised form, August 23, 1994.

1991 *Mathematics Subject Classification.* Primary 11R23; Secondary 11R18.

Key words and phrases. Relative class number, \mathbb{Z}_l -extension, Iwasawa lambda invariant.

Research of the first author supported by Fondecyt grant 1168-92 and by the Max Planck Institut für Mathematik.

Research of the second author supported by National Security Agency Grant MDA904-89-H-2012 and the Deutsche Forschungsgemeinschaft.

for each $n \geq N(K)$. Iwasawa [13, p. 272] noted that $\lambda_l^-(K)$ depends only on K_{l^∞} , and not on the particular base field K . Thus, one could also denote the invariant $\lambda_l^-(K)$ by $\lambda_l^-(K_{l^\infty})$.

We now consider a finite normal extension L/K such that L is also a CM field. For simplicity, we even assume that L is abelian over \mathbb{Q} , and that $[L : K] = p$, a prime number.

When $p = l$, the invariants $\lambda_l^-(K)$ and $\lambda_l^-(L)$ are related by a formula proved by Gras [10], which is an analog of the Riemann–Hurwitz formula relating the genus of a curve to the genus of a covering curve. Kida [15] and Kuz'min [16] independently proved the formula without assuming that K and L are absolutely abelian, so we will refer to it as the Gras–Kida–Kuz'min formula. The reader will find a thorough survey of this formula in Jaulent and Michel's article [14]. In our examples, L will not contain the primitive l -th roots of unity, so let us make that assumption now and describe the Gras–Kida–Kuz'min formula in that case.

When w is a place of L_{l^∞} , denote the ramification index of w in $L_{l^\infty}/K_{l^\infty}$ by $e(w)$. Then

$$(*) \quad \lambda_l^-(L) = [L_{l^\infty} : K_{l^\infty}] \lambda_l^-(K) + \frac{1}{2} \sum_w (e(w) - 1),$$

with w running over all places of L_{l^∞} which do not lie above l and are not fixed by complex conjugation. This is the formula which motivates our investigation.

For the rest of this paper, l and p will be *distinct odd* primes (exception: in the appendix, l or p may be even). Iwasawa has pointed out that one cannot expect to find a formula like $(*)$ relating $\lambda_l^-(L)$ and $\lambda_l^-(K)$ in this case. Suppose, for instance, that $l = 2p + 1$, $K = \mathbb{Q}(\sqrt{-l}) \subset L = \mathbb{Q}(\zeta_l)$. Then the class number of K is less than l ; in particular, it is not divisible by l . The l -extension K_{l^n}/K has only one ramified prime, so that the class number of K_{l^n} is also not divisible by l (see [11]). Thus, $\lambda_l^-(K) = 0$. On the other hand, $\lambda_l^-(L)$ is the index of irregularity of l , at least for l less than 4 million (by [22, 4, 5], and [1]). This index of irregularity is a subtle invariant, for which no simple formula is anticipated.

Rather than simply consider $\lambda_l^-(L)$ and $\lambda_l^-(K)$, we will define similar invariants which also depend on p . Let K_{p^∞} denote the cyclotomic \mathbb{Z}_p -extension of K , and K_{p^m} denote the intermediate field of degree p^m over K . Let $A_l^-(K_{p^\infty})$ be the direct limit of the groups $A_l^-(K_{p^m})$ under the natural maps. Washington [25] has proved that there exists an integer $M(K)$ such that the inclusion maps induce isomorphisms $A_l^-(K_{p^m}) \cong A_l^-(K_{p^r})$ for all $r \geq m \geq M(K)$. Hence $A_l^-(K_{p^\infty})$ may be identified with any one of the finite groups $A_l^-(K_{p^m})$, for $m \geq M(K)$. In §2, we will make use of Washington's more effective proof of this result (see the appendix to this paper), which is obtained by modifying an alternative proof by Sinnott [21].

The stable λ_l^- -invariant which we will define arises from consideration of the fields $K_{l^n p^m}$. In keeping with our previous definitions, $K_{l^n p^m}$ denotes the field of relative degree $l^n p^m$ over K in the cyclotomic $\mathbb{Z}_l \times \mathbb{Z}_p$ -extension of K , and $K_{l^n p^\infty}$ will denote the union of such fields for all $m \geq 0$. Washington's theorem applies to K_{l^n} , and so there exists an integer $M(K_{l^n})$ such that $A_l^-(K_{l^n p^\infty}) \cong$

$A_l^-(K_{l^n p^m})$ for all $m \geq M(K_{l^n})$. A consequence of the main theorem of [7] is that in fact a single value $M(K_{l^n}) = M'$ works for all n . In §2, we will give a new, analytic proof of this fact. Thus, for each $m \geq M'$ and $n \geq N(K_{p^{M'}})$, we have

$$|A_l^-(K_{l^n p^m})| = |A_l^-(K_{l^n p^{M'}})| = l^{n\lambda_l^-(K_{p^{M'}}) + \nu_l^-(K_{p^{M'}})}.$$

This shows that $\lambda_l^-(K_{p^m}) = \lambda_l^-(K_{p^{M'}})$ and $\nu_l^-(K_{p^m}) = \nu_l^-(K_{p^{M'}})$ for each $m \geq M'$. We define the invariant $\lambda_l^-(K_{p^\infty}) = \lambda_l^-(K_{p^{M'}})$, which may then be considered as the p -stable version of $\lambda_l^-(K)$. Upon setting $\nu_l^-(K_{p^\infty}) = \nu_l^-(K_{p^{M'}})$, we see that the formula

$$|A_l^-(K_{l^n p^\infty})| = l^{n\lambda_l^-(K_{p^\infty}) + \nu_l^-(K_{p^\infty})}$$

holds for each $n \geq N(K_{p^{M'}})$.

The invariant $\lambda_l^-(K_{p^\infty})$ is our principal object of study. We will consider the relation between $\lambda_l^-(K_{p^\infty})$ and $\lambda_l^-(L_{p^\infty})$. In other words, we will consider the p -stable λ_l^- -invariant in a p -extension L/K . The main reason for passing from L/K to $L_{p^\infty}/K_{p^\infty}$ is that the behavior of the places in the p -extension $L_{p^\infty}/K_{p^\infty}$ is particularly simple: all places other than those above p must either ramify or split completely. However, as our numerical calculations show, this does not suffice to make a formula of Riemann-Hurwitz type hold.

We emphasize that the Gras-Kida-Kuz'min formula (*) assumes L/K to be a Galois l -extension. Gold and Madan [9], following Rück's work [18] on the Hasse-Witt invariant, dealt with certain non-Galois l -extensions L/K of CM fields. They proved a formula relating $\lambda_l^-(L)$ and $\lambda_l^-(K)$ which is not of Riemann-Hurwitz type. It seems then that the Hasse-Witt invariant, rather than the genus, is the closer geometric analogue in characteristic l of the Iwasawa λ_l^- -invariant. For one thing, neither the λ_l^- nor the Hasse-Witt invariant assigns a special role to wild ramification in the known analogues of the Riemann-Hurwitz formula. Even more germane to this paper, for neither invariant is there yet any idea of how it changes in an extension of degree prime to l .

1. STABILIZATION OF THE RELATIVE l -CLASS NUMBER IN THE \mathbb{Z}_p -TOWER

Let K be a totally imaginary abelian number field and let K_{p^m} be the m -th layer of the cyclotomic \mathbb{Z}_p -extension of K as in the introduction. Let $K_{p^m}^+$ be the maximal totally real subfield of K_{p^m} . We denote the class numbers of these fields by h_m^+ and h_m , respectively. The relative class number of K_{p^m} is the integer $h_m^- = h_m/h_m^+$. Let v_l be the usual valuation at the prime l , and for any rational number g , let $(g)_l = l^{v_l(g)}$. Then $|A_l^-(K_{p^m})| = (h_m^-)_l$, and this is what we wish to investigate further when l and p are distinct odd primes. For simplicity, assume from now on that p^2 does not divide the conductor of K . (Lemma 1 of [24] shows that there is no loss of generality in doing so.) This implies that p^{m+1} exactly divides the conductor of K_{p^m} for $m \geq 1$. When χ is a character of $\Delta = \text{Gal}(K/\mathbb{Q})$, with conductor f_χ , the associated primitive Dirichlet character modulo f_χ will also be denoted by χ , and will be called a character corresponding to K . For a nontrivial Dirichlet character θ modulo

f , the generalized Bernoulli number $B_{1, \theta}$ is defined as

$$B_{1, \theta} = \frac{1}{f} \sum_{b=1}^f \theta(b)b.$$

Fix a nonzero multiple a of the exponent of Δ . Let $\zeta_a = e^{2\pi i/a}$ and $F = \mathbb{Q}(\zeta_a)$, so that F contains the values of each character χ of Δ . Given a positive integer m , we pick any prime l above l in $F(\zeta_{p^m})$ and let v_l be the valuation at l extending v_l .

(1.1) **Lemma.** *If $m \geq 1$, then $v_l(h_m^-/h_{m-1}^-) \geq 0$. Furthermore, if $v_l(h_m^-/h_{m-1}^-) > 0$, then $v_l(B_{1, \chi\psi}) > 0$ for some odd character χ corresponding to K and some Dirichlet character ψ of order p^m and conductor p^{m+1} .*

Proof. The lemma follows easily from the analytic class number formula and the known integrality properties of $B_{1, \chi\psi}$ (cf. [17] and [26, Chap. 7 exercises]). \square

We apply the lemma as follows. Fix a value

$$(**) \quad c \geq c' := v_p(l^{p-1} - 1) + \max \left(\{v_p(r - 1) : r \text{ prime, } r \neq l, r|a\}, v_p(a) - 1, 0 \right).$$

If l is a fixed prime above l in $F(\zeta_{p^c})$, this choice of c ensures that l remains inert in $F(\zeta_{p^d})$ for $d > c$, so we may also denote the prime over l in $F(\zeta_{p^d})$ by l . To see that l remains inert, note that we may assume $l \nmid a$. Otherwise we may just remove all factors of l from a , which leaves c' and the relevant residue degree unchanged. Since $c' \geq 1$, we may also assume that $p|a$. Otherwise we just replace a with pa . Let $a = \prod r_i^{e_i}$ be the factorization of a into prime powers, and let t be the exponent of the group $(\mathbb{Z}/a\mathbb{Z})^\times \cong \prod (\mathbb{Z}/r_i^{e_i}\mathbb{Z})^\times \cong \prod \mathbb{Z}/(r_i - 1)r_i^{e_i - 1}\mathbb{Z}$. Thus, $p - 1 \mid t$ and

$$k := v_p(t) = \max \left(\{v_p(r_i - 1)\}, v_p(a) - 1 \right).$$

Writing $t = (p - 1) \cdot p^k \cdot s$, we have

$$v_p(l^t - 1) = v_p((l^{p-1})^{p^k s} - 1) = v_p((l^{p-1})^{p^k} - 1) = v_p(l^{p-1} - 1) + k = c'.$$

Hence, $l^t \equiv 1 \pmod{a}$ and $l^t \equiv 1 \pmod{p^{c'}}$ but $l^t \not\equiv 1 \pmod{p^{c'+1}}$. This implies that l is inert in $F(\zeta_{p^{c'+1}})/F(\zeta_{p^{c'}})$, and hence in $F(\zeta_{p^d})/F(\zeta_{p^c})$.

For the rest of this section, we take $p = 3$. For each character χ of Δ , put $m_\chi = f_\chi/(f_\chi)_3$. For each integer y , define a polynomial

$$G_{y, \chi}(T) = \sum_{i=0}^{m_\chi - 1} \chi(y + 3^c i) T^i \in F[T].$$

(1.2) **Proposition.** *Let c, l and χ be as above. If $d \geq \max\{2c - 1, 2\}$, if ψ is a character of order 3^d with conductor 3^{d+1} , and if $v_l(B_{1, \chi\psi}) > 0$, then for each $y \equiv 1 \pmod{3}$, $0 < y < 3^c$, there exists a primitive 3^{d-c+1} -th root of unity ζ such that $G_{y, \chi}(\zeta) \equiv 0 \pmod{l}$.*

Proof. Assume that $v_l(B_{1,\chi\psi}) > 0$. Now we use the rational function $f_y(T)$ defined in (A.0) of the appendix by

$$f_y(T) = \left(\sum_{\substack{b \equiv y \pmod{3^c} \\ 0 < b < m_\chi 3^c}} \chi(b) T^b \right) / (T^{m_\chi 3^c} - 1).$$

Here we regard $f_y(T)$ as having coefficients in F . For the case of $p = 3$, it is proved in (A.2) of the appendix that if $v_l(B_{1,\chi\psi}) > 0$, then $f_y(\zeta_\psi^{y^{-1}}) \equiv 0 \pmod{l}$, where ζ_ψ is a primitive 3^{d+1} -th root of unity independent of y , the exponent y^{-1} is taken 3-adically, and y is as in (1.2). From the definition of $f_y(T)$, we then see that

$$0 < v_l(f_y(\zeta_\psi^{y^{-1}})) = v_l\left(\sum_b \chi(b) \zeta_\psi^{y^{-1}b}\right) - v_l(\zeta_\psi^{y^{-1}m_\chi 3^c} - 1).$$

Hence,

$$\sum_b \chi(b) \zeta_\psi^{y^{-1}b} \equiv 0 \pmod{l}.$$

Writing $b = y + 3^c i$ allows us to sum instead over i from 0 to $m_\chi - 1$, yielding

$$0 \equiv \sum_{i=0}^{m_\chi-1} \chi(y + 3^c i) \zeta_\psi^{y^{-1}3^c i} \zeta_\psi = G_{y,\chi}(\zeta) \zeta_\psi \pmod{l},$$

upon setting $\zeta = \zeta_\psi^{y^{-1}3^c}$. Since ζ_ψ is a primitive 3^{d+1} -th root of unity and $d > c$, ζ is a primitive 3^{d-c+1} -th root of unity. The proposition follows. \square

As a consequence, we obtain the following effective versions of Washington's theorem for the case of $p = 3$.

(1.3) **Proposition.** *Let K be a complex abelian number field with conductor not divisible by 9 and let a be a multiple of the exponent of $\Delta = \text{Gal}(K/\mathbb{Q})$. Define $F = \mathbb{Q}(\zeta_a)$, fix c as in (**), and choose a prime l of $F(\zeta_{3^c})$ above l , where $l \neq 3$ is an odd prime number. Let \mathcal{O} denote the ring of integers of $F(\zeta_{3^c})$. For each character χ of Δ and each integer y , let $\overline{G}_{y,\chi}(T)$ be the image of $G_{y,\chi}(T) = \sum_{i=0}^{m_\chi-1} \chi(y + 3^c i) T^i$ in $(\mathcal{O}/l)[T]$.*

Suppose that $d \geq \max\{2c - 1, 2\}$, let h_d^- denote the relative class number of K_{3^d} and suppose that for every odd character χ corresponding to K , there exists an integer $y \equiv 1 \pmod{3}$, $0 < y < 3^c$, such that for each primitive 3^c -th root of unity $\bar{\tau}$ in \mathcal{O}/l , we have that $T^{3^{d-2c+1}} - \bar{\tau}$ does not divide $\overline{G}_{y,\chi}(T)$ in $(\mathcal{O}/l)[T]$. Then $v_l\left(\frac{h_d^-}{h_{d-1}^-}\right) = 0$.

Proof. The proof is by contradiction. If $v_l\left(\frac{h_d^-}{h_{d-1}^-}\right) > 0$, then $v_l(B_{1,\chi\psi}) > 0$ for some odd character χ corresponding to K and some character ψ of order 3^d and conductor 3^{d+1} , by (1.1). Let \mathcal{O}' be the ring of integers of $F(\zeta_{3^{d-c+1}})$, so that $\mathcal{O} \subset \mathcal{O}'$, and recall that we can also regard l as a prime of \mathcal{O}' . Fix an arbitrary $y \equiv 1 \pmod{3}$ in the range from 0 to 3^c . Applying (1.2), we see that $\overline{G}_{y,\chi}(\bar{\zeta}) = 0$ in \mathcal{O}'/l , for some primitive 3^{d-c+1} -th root of unity $\bar{\zeta}$ in \mathcal{O}' with

image $\bar{\zeta}$ in \mathcal{O}'/l . Since l is inert from \mathcal{O} to \mathcal{O}' , the corresponding residue field extension is of degree 3^{d-2c+1} , and is generated by $\bar{\zeta}$. Now $\bar{\zeta}$ satisfies the polynomial $T^{3^{d-2c+1}} - \bar{r} \in \mathcal{O}'[[T]]$ for some primitive 3^c root of unity \bar{r} in \mathcal{O} . Because it is monic of the correct degree, this must be the minimal polynomial of $\bar{\zeta}$. We conclude that $T^{3^{d-2c+1}} - \bar{r} \mid \bar{G}_{y,\chi}(T)$. Since y was arbitrary, this completes the proof by contradiction. \square

(1.4) **Corollary.** *Let K and c and $p = 3$ be as in (1.3). If $3^{d-2c+1} \geq m_\chi$ for each odd character χ of Δ , then $v_l \left(\frac{h_d^-}{h_{d-1}^-} \right) = 0$.*

Proof. The condition $(T^{3^{d-2c+1}} - \bar{r}) \nmid \bar{G}_{1,\chi}(T)$ of Theorem (1.3) holds for each χ , because our assumption means that the degree of the first polynomial is greater than the degree of the second. Note that $\bar{G}_{1,\chi}$ is not the zero polynomial because the constant term is $\chi(1) = 1$. \square

2. STABILIZATION OF λ_l^- IN THE CYCLOTOMIC \mathbb{Z}_p -TOWER

As before, we let p and l be distinct odd primes, and let K be a complex abelian field. We also assume that neither l^2 nor p^2 divides the conductor of K . Again there is no loss of generality in doing so. We assume known an M such that

$$(2.0) \quad |A_l^-(K_{p^m})| = |A_l^-(K_{p^M})|$$

for all $m > M$. Equivalently, as we saw in §1,

$$(2.1) \quad B_{1,\theta} \not\equiv 0 \pmod{l},$$

where $\theta = \chi\psi_{p^m}$, χ is any odd Dirichlet character of K , ψ_{p^m} is any primitive Dirichlet character of conductor p^{m+1} and order p^m , $m > M$, and l is any prime above l in $\mathbb{Q}(\theta)$.

We now show how l -adic L -functions allow us to pass from K_{p^m} to $K_{p^m/n}$ in (2.0). Denote the l -adic Teichmüller character by ω_l and let $L_l(s, \theta\omega_l)$ be the l -adic L -function satisfying (see [26, p. 57])

$$(2.2) \quad L_l(0, \theta\omega_l) = -(1 - \theta(l))B_{1,\theta}.$$

Let $\mathcal{G}(T, \theta\omega_l)$ be the Iwasawa power series associated with $\theta\omega_l$, as in [26, p. 123]. Then

$$(2.3) \quad L_l(s, \theta\omega_l) = \mathcal{G}(u^s - 1, \theta\omega_l),$$

where $u = u_\theta \equiv 1 \pmod{l}$, $u \not\equiv 1 \pmod{l^2}$.

If ψ_{l^n} is a primitive Dirichlet character of conductor l^{n+1} and order l^n ($n \geq 1$), then

$$(2.4) \quad L_l(s, \theta\psi_{l^n}\omega_l) = \mathcal{G}(\zeta_{l^n}u^s - 1, \theta\omega_l),$$

where $\zeta_{l^n} = \psi_{l^n}(u)^{-1}$ is an l^n -th root of unity. By possibly increasing M to an M' that depends only on K , l , and p , we can obtain

$$1 - \theta(l) = 1 - \chi\psi_{p^m}(l) \not\equiv 0 \pmod{l}$$

for $m > M'$. For such m , it is clear from (2.2)–(2.4) that $B_{1,\theta} \not\equiv 0 \pmod{l}$ is equivalent to $B_{1,\theta\psi_{l^n}} \not\equiv 0 \pmod{l'}$ for all $n \geq 0$, where l' is the unique prime

above l in $\mathbb{Q}(\theta, \psi_{l^n})$. Hence, $|A_l^-(K_{p^m l^n})| = |A_l^-(K_{p^{m'} l^n})|$ for $m \geq m'$ and $n \geq 0$. It follows that $\lambda_l^-(K_{p^\infty}) = \lambda_l^-(K_{p^{m'}})$.

In short, an explicit form of Washington's theorem (i.e., knowing M in (2.0)) and some elementary number theory (to ensure that $1 - \chi \psi_{p^m}(l) \not\equiv 0 \pmod{l}$) give an explicit level $K_{p^{m'}}$ at which the λ_l^- -invariant stabilizes. Moreover, the same technique would apply to any CM-field K for which the l -class numbers were known to stabilize in the cyclotomic \mathbb{Z}_p -extension of K .

In our numerical examples, in which $p = 3$, we will take advantage of our computation of $G_{y, \chi}$ (see §1) to obtain the stabilization of λ_l^- in a somewhat different manner (see §4).

3. COMPUTATION OF λ_l^- FOR A COMPLEX ABELIAN FIELD

We assume that l is an odd prime and that k is a totally imaginary abelian number field of conductor not divisible by l^2 . The invariant $\lambda_l^-(k)$ will be computed via its connections with l -adic L -functions, as in [3].

Let ω_l be the l -adic Teichmüller character modulo l , and let $u = \exp_l(l) = 1 + l + l^2/2! + \dots$ in \mathbb{Z}_l . Suppose $\chi \neq \omega_l^{-1}$ is an odd character associated with k . By our assumption on the conductor of k , the l -adic L -function $L_l(s, \chi \omega_l)$, defined for $s \in \mathbb{Z}_l$, has a unique associated power series

$$\mathcal{G}(T, \chi \omega_l) = \sum_{i=0}^{\infty} a_i T^i,$$

with coefficients in the ring $\mathcal{O}_\chi = \mathcal{O}_{\chi \omega_l}$ obtained by adjoining the values of χ to \mathbb{Z}_l , such that $L_l(s, \chi \omega_l) = G(u^s - 1, \chi \omega_l)$. The power series $\mathcal{G}(T, \chi \omega_l)$ has a λ_l -invariant, which may be defined to be the least i such that a_i does not lie in the maximal ideal of \mathcal{O}_χ . Such an i exists by the theorem of Ferrero and Washington [6]. Set

$$\lambda_l(\chi \omega_l) = \lambda_l(\mathcal{G}(T, \chi \omega_l)).$$

Then, again by virtue of our assumption on the conductor of k ,

$$(***) \quad \lambda_l^-(k) = \sum_{\chi \neq \omega_l^{-1}} \lambda_l(\chi \omega_l),$$

where χ runs through all odd characters associated with k (except ω_l^{-1} in the event that it is associated with k).

Our computation of $\lambda_l(\chi \omega_l) = \lambda_l(\mathcal{G}(T, \chi \omega_l))$ is based on the following result. We will use the convention that \log_l on \mathbb{Z}_l^\times is defined by the power series for $\log(1+x)$ when $i \equiv 1 \pmod{l}$ and $\log_l(i) = \log_l(i/\omega_l(i))$ in general. For each positive integer n , let $w_{l^n}(T) = (1+T)^{l^n} - 1$, and define the integer-valued function $L_{l^n}(i)$ by

$$0 \geq L_{l^n}(i) > -l^n, \quad L_{l^n}(i) \equiv \log_l(i)/l \pmod{l^n}.$$

(3.1) **Proposition.** *If $\chi \omega_l$ is a nontrivial primitive Dirichlet character with conductor $f = f_0$ or $f = f_0 l$, $l \nmid f_0$, then*

$$-f_0 \mathcal{G}(T, \chi \omega_l) \equiv \sum_{i=1}^{l^{n+1} f_0 - 1} \sum_{j=0}^{f_0 - 1} j \cdot \chi(i + j l^{n+1}) (1+T)^{-L_{l^n}(i)} \pmod{w_{l^n}(T)}.$$

Proof. This may be derived from the formula immediately preceding the state-

ment of Theorem (1.2) in [3, p. 103]. Simply multiply both sides of that formula by $(1 + T)^k$ and sum over k . \square

(3.2) **Corollary.** *Let χ be an odd character satisfying the conditions of (3.1), and let n be a positive integer. Then*

$$-f_0 \mathcal{E}(T, \chi \omega_l) \equiv 2 \sum_{i=1}^{(l^{n+1}-1)/2} \left(\sum_{j=0}^{f_0-1} j \cdot \chi(i + jl^{n+1}) \right) (1+T)^{-L_l(i)} \pmod{w_{l^n}(T)}.$$

Proof. The sum $\sum_{j=0}^{f_0-1} (f_0-1)\chi(i + jl^{n+1})$ vanishes for each i because $i + jl^{n+1}$ runs through a complete residue system modulo f_0 which is constant modulo l , and χ may be factored as a nontrivial character modulo f_0 times a character modulo l . Setting $j' = f_0-1-j$ and $i' = l^{n+1}-i$, we observe that $\chi(i + jl^{n+1}) = -\chi(i' + j'l^{n+1})$. Thus, the inner sum in (3.1) is the same for i (summing over j) and for i' (summing over j' , which is equivalent). Now $L(i) = L(i')$, so we see that the same term in the outer sum in (3.1) is obtained for both i and $i' = l^{n+1} - i$, implying the result. \square

4. THE ALGORITHM

The algorithm for computing $\lambda_l^-(K_{p^\infty})$ may now be described in full. We assume that $p = 3$, that $l \geq 5$ is a prime, and that K is a complex abelian number field with conductor not divisible by l^2 nor by $p^2 = 9$.

Corollary (1.4) and Proposition (1.3) provide the basis for determining an M such that

$$|A_l^-(K_{3^M})| = |A_l^-(K_{3^\infty})|.$$

This is the first step mentioned in the introduction. First we calculate c' as in (**) in §1 and choose $c = c'$. Thus, if F is the field of character values of $\Delta = \text{Gal}(K/\mathbb{Q})$, then each prime l above l in $F(\zeta_{3^c})$ remains inert in $F(\zeta_{3^d})$ for $d \geq c$. Then we determine the smallest d such that $3^{d-2c+1} \geq \max_\chi \{m_\chi\}$, where $m_\chi = f_\chi / (f_\chi)_3$, and $d \geq \max(2c - 1, 2)$. By (1.4), we may take $M = d - 1$. If $M = d - 1 \geq \max(2d - 1, 2)$, we try to reduce this choice of M by using Proposition (1.3) as follows. For each odd character χ , we set $y = 1$ in Proposition (3.1) and verify that

$$(T^{3^{M-2c+1}} - \bar{y}) \nmid \bar{G}_{y,\chi}(T)$$

for each \bar{y} of order 3^c in $(\mathcal{O}/l)^\times$. If we succeed, then (1.3) shows that M can be reduced to $M - 1$. In this case, as long as the new value of M is still greater than or equal to $\max(2c - 1, 2)$, we use (1.3) again to try to further reduce M . If the verification fails, we try another value of $y \equiv 1 \pmod{3^c}$. This is repeated until there are no y 's left to try, and we can reduce M no further.

Having finished the first step of the algorithm, we have obtained a value of c and, for each odd character χ of K , an $M \geq \max(2c - 1, 2) - 1$, and a $y \equiv 1 \pmod{3}$, $0 < y < 3^c$, such that

$$G_{y,\chi}(\zeta) \not\equiv 0 \pmod{l}$$

for any primitive 3^{d-c+1} -th root of unity ζ , where $d > M$. Suppose we now replace χ by $\chi\psi_{l^n}$, where ψ_{l^n} is a primitive Dirichlet character of conductor l^{n+1} and order l^n , $n \geq 1$. One checks that c' in (**) is unchanged. There is a unique (totally ramified) prime l' above l in the new field of character values.

We now make the further assumption that 3 does not divide the conductor of K . Thus, $m_\chi = f_\chi$. Since the values of ψ_{l^n} are congruent to 1 modulo l' , we have

$$\begin{aligned} G_{y, \chi \psi_{l^n}}(T) &\equiv \sum_{i=0}^{l^{n+1} f_\chi - 1} \chi(y + 3^c i) T^i \\ &\equiv \sum_{i=0}^{f_\chi - 1} \sum_{k=0}^{l^{n+1} - 1} \chi(y + 3^c(i + k f_\chi)) T^{i+k f_\chi} \\ &= G_{y, \chi}(T)(T^{f_\chi l^{n+1}} - 1)/(T^{f_\chi} - 1) \pmod{l'}. \end{aligned}$$

As $3 \nmid f_\chi l^{n+1}$, we have $G_{y, \chi \psi_{l^n}}(\zeta) \not\equiv 0 \pmod{l'}$ whenever $G_{y, \chi}(\zeta) \not\equiv 0 \pmod{l'}$ and ζ has 3-power order. Applying Proposition (1.2) to K_{l^n} , we see that

$$|A_l^-(K_{3^d l^n})| = |A_l^-(K_{3^M l^n})|$$

for any $d \geq M, n \geq 0$, where M is as determined above for K . We conclude that if neither l^2 nor 3 divides the conductor of K , then $\lambda_l^-(K_{3^\infty}) = \lambda_l^-(K_{3^M})$, where M has been determined in step 1 (we take an M that works for all odd characters χ of K). This completes the second step.

Our third and final step is the computation of $\lambda_l^-(K_{3^M})$. First we invoke (***) with $F = K_{3^M}$, so that

$$\lambda_l^-(K_{p^{M'}}) = \sum_{\chi \neq \omega_l^{-1}} \lambda_l(\chi \omega_l),$$

where χ runs through all odd characters associated with K_{3^M} . Then (3.2) allows us to compute $\lambda_l(\chi \omega_l)$. Since $\omega_l = (1 + T)^l - 1 \in (T^l, l)$, we may take $n = 1$ and determine $\lambda_l(\chi \omega_l) = \lambda_l(G(T, \chi \omega_l))$ as the lowest power of T in the sum in (3.2) whose coefficient does not lie in the maximal ideal of \mathcal{O}_χ , as long as this answer is less than l . Otherwise, we determine $\lambda_l(G(T, \chi \omega_l))$ by choosing larger values of n as necessary. This completes the algorithm.

5. COMPUTATIONS

Computations were performed using Mathematica on the Silicon Graphics Iris 4D/480 at the Computer Facility of the University of Vermont Division of Engineering, Mathematics, and Business Administration. Steps one and three are easily reduced to testing the divisibility of various integral elements in a cyclotomic field $\mathbb{Q}(\zeta_c)$ by a prime above l . We represent such an element by a polynomial $q(\zeta_c)$ in ζ_c , and let $\Phi_c(x)$ be the minimal monic polynomial of ζ_c over \mathbb{Q} . In $(\mathbb{Z}/l\mathbb{Z})[x]$, an irreducible factor $\overline{C}_c(x)$ of $\overline{\Phi}_c(x)$ corresponds to a prime of $\mathbb{Z}[\zeta_c]$ above l , namely $\mathfrak{l} = (l, C_c(\zeta_c))$, where $C_c(x)$ is any lifting of $\overline{C}_c(x)$ to $\mathbb{Z}[x]$. Then $q(\zeta_c)$ lies in \mathfrak{l} if and only if $\overline{C}_c(x)$ divides $\overline{q}(x)$ in $\mathbb{Z}/l\mathbb{Z}[x]$. This condition may be tested in Mathematica by taking the greatest common divisor of $C_c(x)$ and $q(x)$ modulo l to see if it is different from 1.

In order to check our program, we used it to compute some invariants which could be verified independently. First we computed λ_3^- for three fields, each of which is a composite of an imaginary quadratic field and a cyclic cubic field. Namely, we took the composite of $\mathbb{Q}(\sqrt{-11})$ with the cubic subfield of $\mathbb{Q}(\zeta_7)$, the composite of $\mathbb{Q}(\sqrt{-19})$ with the cubic subfield of $\mathbb{Q}(\zeta_7)$, and the composite of $\mathbb{Q}(\sqrt{-13})$ with the cubic subfield of $\mathbb{Q}(\zeta_{19})$. We obtained the values 3, 2 and

6, respectively. These are in agreement with what one obtains by applying the Gras-Kida-Kuz'min formula (*) for an extension of degree 3 over an imaginary quadratic field. The invariants for these imaginary quadratic fields are found in Gold [8]. We computed $\lambda_7^-(\mathbb{Q}(\zeta_{19})) = 7$, in accord with Childress [2], and verified the values 1 and 2 of λ_5 for two individual characters (the product of the 5-adic Teichmüller character and the quadratic characters of conductor 37 and 53) considered by Ernvall and Metsänkylä [5].

TABLE OF RESULTS: Computations when $p = 3$, $K = \mathbb{Q}(\sqrt{-D})$ and L is the relative cubic extension of K contained in $K(\zeta_r)$. "Jump" denotes the difference in the two preceding columns after subtracting the contribution due to trivial zeros.

| l | D | r | $\lambda_l^-(K)$ | $\lambda_l^-(L)$ | $\lambda_l^-(K_{3^\infty})$ | $\lambda_l^-(L_{3^\infty})$ | Jump |
|-----|-----|-----|------------------|------------------|-----------------------------|-----------------------------|------|
| 5 | 4 | 7 | 1 | 1 | 1 | 3 | 0 |
| 5 | 4 | 13 | 1 | 3 | 1 | 3 | 0 |
| 5 | 4 | 19 | 1 | 1 | 1 | 3 | 0 |
| 5 | 7 | 7 | 0 | 0 | 0 | 0 | 0 |
| 5 | 7 | 13 | 0 | 0 | 0 | 0 | 0 |
| 5 | 7 | 19 | 0 | 0 | 0 | 0 | 0 |
| 5 | 11 | 7 | 2 | 2 | 2 | 4 | 0 |
| 5 | 11 | 13 | 2 | 4 | 2 | 4 | 0 |
| 5 | 11 | 19 | 2 | 4 | 2 | 4 | 0 |
| 5 | 19 | 7 | 1 | 1 | 1 | 3 | 0 |
| 5 | 19 | 13 | 1 | 3 | 1 | 3 | 0 |
| 5 | 19 | 19 | 1 | 1 | 1 | 3 | 0 |
| 5 | 31 | 7 | 1 | 1 | 1 | 3 | 0 |
| 5 | 31 | 13 | 1 | 3 | 1 | 3 | 0 |
| 5 | 31 | 19 | 1 | 1 | 1 | 3 | 0 |
| 5 | 210 | 7 | 0 | 2 | 0 | 4 | 4 |
| 7 | 3 | 7 | 1 | 1 | 1 | 1 | 0 |
| 7 | 3 | 13 | 1 | 1 | 1 | 3 | 0 |
| 7 | 3 | 19 | 1 | 3 | 1 | 3 | 0 |
| 7 | 19 | 7 | 1 | 1 | 1 | 1 | 0 |
| 7 | 19 | 13 | 1 | 1 | 1 | 3 | 0 |
| 7 | 19 | 19 | 1 | 7 | 1 | 9 | 6 |
| 7 | 31 | 7 | 1 | 1 | 1 | 1 | 0 |
| 7 | 31 | 13 | 1 | 1 | 1 | 3 | 0 |
| 7 | 31 | 19 | 1 | 3 | 1 | 4 | 1 |
| 7 | 143 | 7 | 3 | 3 | 5 | 6 | 1 |
| 7 | 143 | 13 | 3 | 3 | 5 | 9 | 2 |
| 7 | 143 | 19 | 3 | 6 | 5 | 8 | 1 |
| 11 | 7 | 7 | 1 | 1 | 1 | 3 | 0 |
| 11 | 7 | 13 | 1 | 1 | 1 | 3 | 0 |
| 11 | 7 | 19 | 1 | 3 | 1 | 3 | 0 |
| 11 | 8 | 7 | 1 | 1 | 1 | 3 | 0 |
| 11 | 8 | 13 | 1 | 1 | 1 | 3 | 0 |
| 11 | 8 | 19 | 1 | 3 | 1 | 3 | 0 |
| 11 | 19 | 7 | 2 | 2 | 2 | 4 | 0 |
| 11 | 19 | 13 | 2 | 2 | 2 | 4 | 0 |
| 11 | 19 | 19 | 2 | 4 | 2 | 4 | 0 |

It is worth noting that in the first and second lines of the table, the value of $\lambda_5^-(L_{3^\infty})$ is the same even though the splitting behavior of the ramified primes is different in each case. In the first case, there is a unique ramified prime, which is inert from the maximal totally real subfield, while in the second there are two ramified primes which have split from the maximal totally real subfield.

The increase $\lambda_l^-(L_{3^\infty}) - \lambda_l^-(K_{3^\infty}) = 2$ in all but one of the tabulated examples for $l = 5$ and $l = 11$ is exactly accounted for by the trivial zeros of the additional 5-adic L -functions which one must consider when passing from K_{3^∞} to L_{3^∞} . Following a suggestion of L. Washington, we sought an example with a nontrivial contribution to the increase by choosing fields K and L such that the 5-rank of the ideal class group was greater for L than for K . He provided the example of $D = 210$ and $r = 7$, in which these ranks are 2 and 0, respectively, while no trivial zeros of the associated 5-adic L -functions occur. This forces $\lambda_5^-(L)$ to be at least 2. In fact, we found a conjugate pair of 5-adic L -functions associated with L which had nontrivial simple zeros, showing that $\lambda_5^-(L) = 2$, while $\lambda_5^-(K) = 0$. To our surprise, when passing to L_{3^∞} , we found a second conjugate pair of L -functions with simple nontrivial zeros. Consequently, $\lambda_l^-(L_{3^\infty}) = 4$, while $\lambda_l^-(K_{3^\infty}) = 0$. In this example, the conductors involved are divisible by 3, which makes for minor modifications in the algorithm described in the previous section.

The tabulated examples for $l = 7$ also reflect the occurrence of some nontrivial and higher-order zeros modulo a prime above l , as seen in the positive entries in the column labeled "Jump."

APPENDIX (BY LAWRENCE C. WASHINGTON)

The purpose of this appendix is to prove the congruence needed for the proof of Proposition (1.2). However, from this congruence it is possible to give a fairly quick proof of the main result of [25], so we include it:

Theorem. *Let ℓ and p be distinct primes, and let L be an abelian extension of \mathbb{Q} . Let L_{p^∞}/L be the cyclotomic \mathbb{Z}_p -extension of L . Let ℓ^{e_n} be the exact power of ℓ dividing the class number of the n -th intermediate field L_{p^n} . Then e_n is bounded as $n \rightarrow \infty$.*

The proof we give is basically a variation of that given by Sinnott [21], though we avoid the use of p -adic measures. In a sense, we work in the style of [27].

First, we need some notation. Let ℓ and p be distinct primes. Let $q = p$ if p is odd, $q = 4$ if $p = 2$. Any primitive odd Dirichlet character can be written in the form $\chi\psi_n$, where χ is a Dirichlet character with $\chi(-1) = -1$ such that pq does not divide the conductor f of χ , and ψ_n has p -power order and conductor qp^n for some n , or is trivial. Let

$$B_{1, \chi\psi_n} = \frac{1}{qp^n} \sum_{b=1}^{qp^n} b \chi\psi_n(b)$$

be the generalized Bernoulli number. Let $\mathcal{O}_\chi = \mathbb{Z}_\ell[\chi(1), \chi(2), \dots]$, let \mathcal{F} be the field of fractions of \mathcal{O}_χ , and let ζ_{p^n} be a primitive p^n -th root of unity in the algebraic closure $\overline{\mathcal{F}}$ of \mathcal{F} . Let $\bar{\ell}$ be the prime of $\overline{\mathcal{F}}$. As explained in

[24], to prove the theorem it suffices to prove that, for each such χ ,

$$\frac{1}{2}B_{1, \chi \psi_n} \not\equiv 0 \pmod{\bar{\ell}}$$

for all n sufficiently large. For the proof of Proposition (1.2), we need to make “sufficiently large” effective, at least in the case $p = 3$.

Fix $c \geq 1$ large enough that the extension $\mathcal{F}(\zeta_{p^n})/\mathcal{F}(\zeta_{p^c})$ has degree p^{n-c} whenever $n \geq c$. This is possible since a prime above ℓ cannot split completely in a global cyclotomic \mathbb{Z}_p -extension, hence must be inert starting at a certain level; the present situation lies in the completion of such a situation. In the following, we assume that $n \geq \max(2c - 1, 2)$, hence $n > c$.

Let $m_\chi = f$ if $(f, q) = 1$ and $m_\chi = f/q$ otherwise. Let $q_n = m_\chi qp^n$. Let ζ be a primitive qp^n -th root of unity. For $y \in \mathbb{Z}$, define $A_y(\zeta) \in \overline{\mathcal{F}}$ by

$$A_y(\zeta) = \sum_{\substack{b \equiv y \pmod{p^c} \\ b \pmod{q_n}}} \left\{ \frac{b}{q_n} \right\} \chi(b) \zeta^b,$$

where $\{x\}$ denotes the fractional part of x (so $0 \leq \{x\} < 1$). Then

$$\begin{aligned} (\zeta^{q_{c-1}} - 1)A_y(\zeta) &= \sum_b \left(\left\{ \frac{b - q_{c-1}}{q_n} \right\} - \left\{ \frac{b}{q_n} \right\} \right) \chi(b) \zeta^b \\ &= \sum_{\substack{b \equiv y \pmod{p^c} \\ 0 < b < q_{c-1}}} \chi(b) \zeta^b - \frac{q_{c-1}}{q_n} \sum_{\substack{b \equiv y \pmod{p^c} \\ 0 < b < q_n}} \chi(b) \zeta^b. \end{aligned}$$

Multiplication by $\zeta^{q_{c-1}} - 1 \neq 0$ kills the second sum, so it must be 0. Therefore,

$$A_y(\zeta) = f_y(\zeta),$$

where $f_y(T) \in \mathcal{F}(T)$ is given by

$$(A.0) \quad f_y(T) = \left(\sum_{\substack{b \equiv y \pmod{p^c} \\ 0 < b < q_{c-1}}} \chi(b) T^b \right) / (T^{q_{c-1}} - 1).$$

Since χ is odd, $f_{-y}(T^{-1}) = f_y(T)$.

Suppose now that $\frac{1}{2}B_{1, \chi \psi_n} \equiv 0 \pmod{\bar{\ell}}$. Let $y \equiv 1 \pmod{p}$. Then (all congruences are mod $\bar{\ell}$)

$$\begin{aligned} 0 &\equiv \text{Trace}_{\mathcal{F}(\zeta_{p^n})/\mathcal{F}(\zeta_{p^c})} \left(\frac{1}{2} \psi_n(y)^{-1} \sum_{0 < b < q_n} \left\{ \frac{b}{q_n} \right\} \chi(b) \psi_n(b) \right) \\ &= \frac{1}{2} p^{n-c} \psi_n(y)^{-1} \sum_{\alpha} \sum_{\substack{b \equiv \alpha y \pmod{qp^{n-c}} \\ 0 < b < q_n}} \left\{ \frac{b}{q_n} \right\} \chi(b) \psi_n(b), \end{aligned}$$

where α runs through the $\phi(q)$ -th roots of unity in \mathbb{Z}_p . We have used the fact that $\psi_n(by^{-1})^{p^c} = 1 \Leftrightarrow (by^{-1})^{p^c} \equiv \alpha \pmod{qp^n}$ for some $\alpha \Leftrightarrow (by^{-1}\alpha^{-1})^{p^c} \equiv 1 \pmod{qp^n} \Leftrightarrow by^{-1}\alpha^{-1} \equiv 1 \pmod{qp^{n-c}}$.

Write $b \equiv \alpha y(1 + qp^{n-c}z) \pmod{qp^n}$. Then

$$\begin{aligned} \psi_n(b) &= \psi_n(y) \psi_n(1 + qp^{n-c}z) \quad (\text{since } n \geq 2c - 1) \\ &= \psi_n(y) \zeta_{\psi_n}^{zqp^{n-c}} = \psi_n(y) \zeta_{\psi_n}^{b(\alpha y)^{-1}-1}, \end{aligned}$$

where ζ_{ψ_n} is some primitive qp^n -th root of unity independent of y . Therefore,

$$0 \equiv \frac{1}{2} \sum_{\alpha} \sum_{\substack{b \equiv \alpha y \pmod{qp^{n-c}} \\ 0 < b < q_n}} \left\{ \frac{b}{q_n} \right\} \chi(b) \zeta_{\psi_n}^{b(\alpha y)^{-1}}.$$

Let $t \equiv 1 \pmod{p^c}$. Change y to ty , then apply $\sigma_t : \zeta_{\psi_n} \mapsto \zeta_{\psi_n}^t$. This is an automorphism of $\mathcal{F}(\zeta_{\psi_n})$ over $\mathcal{F}(\zeta_{p^c})$ by the choice of c , and the congruence mod $\bar{\ell}$ still holds. Summing over all such t modulo q_n , we obtain

$$0 \equiv \frac{1}{2} p^c \sum_{\alpha} \sum_{\substack{b \equiv \alpha y \pmod{p^c} \\ 0 < b < q_n}} \left\{ \frac{b}{q_n} \right\} \chi(b) \zeta_{\psi_n}^{b\alpha^{-1}y^{-1}} \equiv \frac{1}{2} p^c \sum_{\alpha} f_{\alpha y}(\zeta_{\psi_n}^{\alpha^{-1}y^{-1}}).$$

Fix once and for all a set R' of representatives for the set of roots of unity α modulo ± 1 . Since $f_{\alpha y}(\zeta_{\psi_n}^{\alpha^{-1}y^{-1}}) = f_{-\alpha y}(\zeta_{\psi_n}^{-\alpha^{-1}y^{-1}})$, the above condition becomes

$$(A.1) \quad 0 \equiv \sum_{\alpha \in R'} f_{\alpha y}(\zeta_{\psi_n}^{\alpha^{-1}y^{-1}}).$$

When $p = 3$, we have $\alpha = \pm 1$, hence $R' = \{1\}$, so we obtain

$$(A.2) \quad 0 \equiv f_y(\zeta_{\psi_n}^{y^{-1}}) \pmod{\bar{\ell}},$$

where ζ_{ψ_n} is a primitive 3^{n+1} -th root of unity independent of y , $y \equiv 1 \pmod{3}$, $0 < y < 3^c$, and $n \geq \max(2c - 1, 2)$. This is the formula needed in the proof of Proposition 1.2.

In the remainder of the proof of the present theorem, we only use (A.1) in the case $y = 1$. The following result is useful.

Lemma. *Let $t_1, \dots, t_s \in \mathbb{Z}_p$ be distinct mod p^M for some $M \geq 1$. Suppose there is a primitive p^n -th root of unity ζ_{p^n} , with $n \geq M + c$, and constants $c_1, \dots, c_s \in \mathcal{O}$ such that*

$$\sum_{i=1}^s c_i \zeta_{p^n}^{t_i} \equiv 0 \pmod{\bar{\ell}}.$$

Then $c_i \equiv 0 \pmod{\bar{\ell}}$ for all i .

Proof. The hypotheses imply that $\zeta_{p^n}^{t_i - t_j} \notin \mathcal{F}(\zeta_{p^c})$ for $i \neq j$. Therefore,

$$0 \equiv \text{Trace}_{\mathcal{F}(\zeta_{p^n})/\mathcal{F}(\zeta_{p^c})}(\zeta_{p^n}^{-t_j} \sum_i c_i \zeta_{p^n}^{t_i}) \equiv p^{n-c} c_j,$$

so $c_j \equiv 0$. \square

It is fairly easy to deduce Corollary (1.4) from this lemma. It is also possible to use this lemma for larger values of p to prove a version of Corollary (1.4)

for these primes as well. This is essentially what was done in the case of $p = 5$ in [23]. We show below how to use the lemma to obtain a proof of the theorem.

Let $k = \mathcal{O}/(\ell \cap \mathcal{O})$ be the residue field of \mathcal{O} and let \bar{k} be its algebraic closure. Let $\mu_{p^\infty} \subset \bar{k}$ be the set of p -power roots of unity and let F be the ring of functions from μ_{p^∞} to \bar{k} . Let U denote the function given by $U(x) = x$ for all $x \in \mu_{p^\infty}$. For $\beta \in \mathbb{Z}_p$, we have $U^\beta \in F$.

Let $\{a_1, \dots, a_r\}$ be a \mathbb{Z} -basis for $\mathbb{Z}[\{\alpha\}] = \mathbb{Z}[\zeta_{p-1}]$, regarded as a subset of \mathbb{Z}_p under some fixed embedding.

Corollary. *The functions U^{a_1}, \dots, U^{a_r} are algebraically independent over k .*

Proof. Suppose we have a relation

$$\sum_{(d)} c_{(d)} U^{\sum a_i d_i} = 0, \quad c_{(d)} \in k, \quad (d) = (d_1, \dots, d_r) \in \mathbb{Z}^r.$$

Since a_1, \dots, a_r are linearly independent over \mathbb{Z} , the exponents $\sum a_i d_i$ are distinct in \mathbb{Z}_p , hence incongruent mod p^M for some sufficiently large M . Take any $n \geq M + c$ and evaluate at any primitive p^n -th root of unity ζ_{p^n} . The lemma implies that $c_{(d)} = 0$ for all (d) . This proves the corollary. \square

A similar proof shows that the ring $k[\{U^\alpha\}] = k[U^{a_1}, U^{-a_1}, \dots, U^{a_r}, U^{-a_r}]$ is an integral domain, so we may form its field of fractions $k(\{U^{a_i}\})$.

Let $\bar{f}_\alpha(T) \in k(T)$ be the reduction of $f_\alpha(T)$ modulo $\bar{\ell}$. We claim that if the theorem fails, then

$$\sum_{\alpha \in R'} \bar{f}_\alpha(U^{\alpha^{-1}}) = 0$$

in $k(\{U^{a_i}\})$.

Let $\bar{Q}(T) = T^{q_{c-1}} - 1$ and $\bar{P}_\alpha(T) = \bar{Q}(T)\bar{f}_\alpha(T) \in k[T]$. Write

$$\begin{aligned} \prod_{\beta \in R'} \bar{Q}(U^{\beta^{-1}}) \sum_{\alpha \in R'} \bar{f}_\alpha(U^{\alpha^{-1}}) &= \sum_{\alpha \in R'} \left[\prod_{\beta \neq \alpha} \bar{Q}(U^{\beta^{-1}}) \right] \bar{P}_\alpha(U^{\alpha^{-1}}) \\ &= \sum_i c_i U^{t_i} \text{ for some } c_i \in k, \quad t_i \in \mathbb{Z}[\{\alpha\}]. \end{aligned}$$

Since $\prod_{\beta \in R'} \bar{Q}(U^{\beta^{-1}}) \neq 0$, it suffices to show that $c_i = 0$ for each i .

Evaluating the above at ζ_{ψ_n} , we have that

$$\sum_i c_i \zeta_{\psi_n}^{t_i} \equiv \prod_{\beta} \left(\zeta_{\psi_n}^{\beta^{-1} q_{c-1}} - 1 \right) \cdot \sum_{\alpha \in R'} f_\alpha(\zeta_{\psi_n}^{\alpha^{-1}}) \equiv 0 \pmod{\bar{\ell}},$$

by (A.1) with $y = 1$. If the theorem fails, then this congruence holds for an infinite set of integers n . The lemma implies that $c_i \equiv 0$ for all i . This proves the claim. We now need the following result.

Proposition (Sinnott [19]). *Let k be a field, let X_1, \dots, X_n, Z ($n \geq 1$) be indeterminates over k , and let Y_1, \dots, Y_m ($m \geq 1$) be nontrivial elements of the group $\prod_i X_i^{\mathbb{Z}}$ generated by X_1, \dots, X_n in $k(X_1, \dots, X_n)^\times$. Suppose that Y_1, \dots, Y_m are pairwise multiplicatively independent (that is, for $i \neq j$, and integers a and b , we have $Y_i^a = Y_j^b$ if and only if $a = b = 0$). Then a relation*

of the form

$$r_1(Y_1) + \cdots + r_m(Y_m) = 0$$

with $r_j \in k(Z)$ can occur only if $r_j(Z) \in k$ for all j .

We apply this result as follows. Let $X_i = U^{a_i}$ and $Y_\alpha = U^{\alpha^{-1}}$. Since $\alpha/\alpha' \notin \mathbb{Q}$ unless $\alpha = \pm\alpha'$, the elements Y_α for $\alpha \in R'$ are pairwise multiplicatively independent. Let $r_\alpha(Z) = f_\alpha(Z)$. We obtain $f_\alpha(Z) \equiv d_\alpha \pmod{\bar{\ell}}$ for some $d_\alpha \in \mathcal{O}$, for all α . Let $\alpha = 1$. The coefficient of Z in the numerator of $f_1(Z)$ is $\chi(1) = 1 \not\equiv 0$. Therefore, $f_\alpha(Z) \not\equiv \text{constant}$, so we have a contradiction. Therefore, $\frac{1}{2}B_{1, \chi \psi_n} \not\equiv 0 \pmod{\bar{\ell}}$ for all sufficiently large n . This completes the proof of the theorem.

ACKNOWLEDGMENT

We thank Warren Sinnott for some useful discussions and for running some of our computations through a check of predicted relative class numbers using his programs.

BIBLIOGRAPHY

1. J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä, *Irregular primes and cyclotomic invariants to four million*, Math. Comp. **61** (1993), 151–153.
2. N. Childress, *Examples of λ -invariants*, Manuscripta Math. **68** (1990), 447–453.
3. D. S. Dummit, D. Ford, H. Kisilevsky, and J. W. Sands, *Computation of Iwasawa lambda invariants for imaginary quadratic fields*, J. Number Theory **37** (1991), 100–121.
4. R. Ernvall and T. Metsänkylä, *Cyclotomic invariants for primes between 125000 and 150000*, Math. Comp. **56** (1991), 851–858.
5. ———, *Cyclotomic invariants for primes to one million*, Math. Comp. **59** (1992), 249–250.
6. B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), 377–395.
7. E. C. Friedman, *Ideal class groups in basic $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$ -extensions of abelian number fields*, Invent. Math. **65** (1982), 425–440.
8. R. Gold, *Examples of Iwasawa invariants, II*, Acta Arith. **26** (1975), 233–240.
9. R. Gold and M. Madan, *Kida's theorem for a class of non-normal extensions*, Proc. Amer. Math. Soc. **104** (1988), 55–60.
10. G. Gras, *Sur les invariants lambda d'Iwasawa des corps abéliennes*, Pub. Math. Fac. Sci. Bézangon (1978/79).
11. K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.
12. ———, *On Γ -extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226.
13. ———, *Riemann–Hurwitz formula and p -adic Galois representations for number fields*, Tôhoku Math. J. **33** (1981), 263–288.
14. J.-F. Jaulent and A. Michel, *Classes des corps surcirculaires et des corps de fonctions*, Séminaire de Théorie des Nombres Paris 1989-90, Birkhäuser, Boston, 1992, pp. 141–162.
15. Y. Kida, *l -extensions of CM-fields and cyclotomic invariants*, J. Number Theory **12** (1980), 519–528.
16. L. Kuz'min, *Some duality theorems for cyclotomic Γ -extensions over algebraic number fields of CM-type*, Math. USSR–Izv. **14** (1980), 441–498.
17. H. W. Leopoldt, *Eine Verallgemeinerung der Bernoullischen Zahlen*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 131–140.

18. H. G. Rück, *Hasse-Witt-invariants and dihedral extensions*, Math. Z. **191** (1986), 513–517.
19. W. Sinnott, *On the μ -invariant of the Γ -transform of a rational function*, Invent. Math. **75** (1984), 273–282.
20. ———, *On p -adic L -functions and the Riemann–Hurwitz genus formula*, Compositio Math. **53** (1984), 3–17.
21. ———, *On a theorem of L. Washington*, Astérisque **147-148** (1987), 209–224.
22. S. S. Wagstaff, Jr., *The irregular primes to 125000*, Math. Comp. **32** (1978), 583–591.
23. L. C. Washington, *The class number of the field of 5^n th roots of unity*, Proc. Amer. Math. Soc. **61** (1976), 205–208.
24. ———, *Class numbers and \mathbb{Z}_p -extensions*, Math. Ann. **214** (1975), 177–193.
25. ———, *The non- p -part of the class number in a cyclotomic \mathbb{Z}_p -extension*, Invent. Math. **49** (1978), 87–97.
26. ———, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982.
27. ———, *On Sinnott's proof on the vanishing of the Iwasawa invariant μ_p* , Algebraic Number Theory in honor of K. Iwasawa, Advanced Studies in Pure Math., vol. 17, Academic Press, Boston, 1990, pp. 457–462.

DEPARTAMENTO DE MATEMÁTICAS, FACULTAD DE CIENCIAS, UNIVERSIDAD DE CHILE, CASILLA 653, SANTIAGO, CHILE

E-mail address: `friedman@abello.seci.uchile.cl`

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF VERMONT, BURLINGTON, VERMONT 05405

E-mail address: `sands@math.uvm.edu`