COMPOSITIO MATHEMATICA

ALBERT A. CUOCO

Generalized Iwasawa invariants in a family

Compositio Mathematica, tome 51, nº 1 (1984), p. 89-103
<http://www.numdam.org/item?id=CM_1984__51_1_89_0>

Compositio Mathematica 51 (1984) 89–103

GENERALIZED IWASAWA INVARIANTS IN A FAMILY

Albert A. Cuoco

1. Introduction

Let k be a number field, p a rational prime, d a positive integer, and L a $\mathbf{Z}_p^d$-extension of k (L/k is an abelian extension such that $G(L/k)$ is topologically isomorphic with the additive group in $\mathbf{Z}_p^d$). Let $E = G(L/k)$ and $\Lambda_E = \mathbf{Z}_p[[E]]$, the complete group ring of E over $\mathbf{Z}_p$. If M_L is the maximal unramified pro-p extension of L, put $X_L \doteq G(M_L/L)$. X_L is a compact $\mathbf{Z}_p$-module, and the action of E on X_L by inner automorphisms makes X_L into a finitely generated torsion Λ_E-module, the "Iwasawa-Greenberg module" for L/k. Now, the Λ_E-module structure of X_L exerts a certain degree of control over the arithmetic of various subfields of L. In this paper we investigate this control by showing how various nontriviality properties of X_L can be translated into statements about generalized Iwasawa invariants for subfields of L.

We begin with a brief survey of known results. If e_n is the exact power of p that divides the class number of the fixed field of E^{p^n}, then there are non-negative integers $m_0 = m_0(L/k)$ and $l_0 = l_0(L/k)$ so that for all n,

$$e_n = \left(m_0 p^n + l_0 n + \mathrm{O}(1)\right) p^{(d-1)n}. \tag{1}$$

The invariants $m_0(L/k)$ and $l_0(L/k)$ are defined in terms of the Λ_E structure of X_L (more precisely, in terms of the characteristic power series of X_L, defined in §3); when $d = 1$, $m_0(L/k) = \mu(L/k)$ and $l_0(L/k) = \lambda(L/k)$ where μ and λ are Iwasawa's invariants. There are examples (cf. §5) where $m_0(L/k)$ is large, but there are no known examples when $d \geqslant 2$ and $l_0(L/k) \neq 0$.

If L/k is a $\mathbf{Z}_p^d$-extension, let S denote the set of finite extensions of k contained in L. If $k' \in S$, let $\mathfrak{S}(k')$ denote the set of $\mathbf{Z}_p$-extensions of k' contained in L; when $d \geqslant 2$, let $\mathfrak{S}'(k')$ denote the set of $\mathbf{Z}_p^{d-1}$ extensions of k' contained in L.

In [8], Paul Monsky proves the following two theorems:

THEOREM A: *There is a finite subset A of $\mathfrak{S}'(k)$ so that if $K \in \mathfrak{S}(k)$ and K is not contained in any element of A, $\mu(K/k) = m_0(L/k)$.*

THEOREM B: *If $d = 2$, then $l_0(L/k) = 0$ is equivalent to the boundedness of λ on $\mathfrak{S}(k)$.*

One consequence of Theorem A is that μ is bounded on $\mathfrak{S}(k)$. Also, because of Theorem B, a nonzero l_0 when $d=2$ would be of some importance in Iwasawa theory.

In §5 of this paper, we obtain further results of this type. Although the l_0 invariant is a generalization of λ, we find a relationship between l_0 and μ: under certain conditions, if $\mu=0$ almost everywhere on $\mathfrak{S}(k)$, then $l_0(L/k)=0$ (and if $l_0(L/k)$ is nonzero, $m_0(K/k)\neq 0$ for at least one K in $\mathfrak{S}'(k)$). We also show that the $l_0\neq 0$ problem for $d=2$ can be solved if one finds a $\mathbf{Z}_p^d$-extension L/k with $d\geqslant 3$ and $l_0(L/k)\neq 0$. From this it will follow that if L/k is an arbitrary $\mathbf{Z}_p^d$-extension ($d\geqslant 2$) so that $l_0(L/k)\neq 0$, then there exists a k' in S so that λ is unbounded on $\mathfrak{S}(k')$.

These results are concerned with the invariants $m_0(L/k)$ and $l_0(L/K)$, which, as mentioned above, are defined in terms of the Λ_E structure of X_L. In general, very little is known about the kinds of modules that can actually occur as Iwasawa-Greenberg modules for $\mathbf{Z}_p^d$-extensions. We will show that for a given d, if $p>2d+1$, there is a number field k and a $\mathbf{Z}_p^d$-extension L/k so that $m_0(L/k)\neq 0$ (and, in fact, by adjusting k and L, we can make $m_0(L/k)$ arbitrarily large). This will imply that the characteristic power series for X_L can be divisible by large powers of p (but this is unusual; we will give a simple and easily satisfied criterion to insure that $m_0=0$). However, there are no known examples of $\mathbf{Z}_p^d$-extensions L/k where the characteristic power series of X_L is not simply a power of p. We will show that such a characteristic power series would have an effect on the Iwasawa λ invariants of $\mathbf{Z}_p$-extensions contained in L: If the characteristic power series of X_L is not a power of p, then given any integer N, there exists k' in S and K' in $\mathfrak{S}(k')$ so that $\lambda(K'/k')>N$.

The proofs of these results make use of an iterative process that was first established in [3] for $d=2$ and is generalized to arbitrary d in §2-§4 of this paper. The process can be described as follows: Let L/k be a $\mathbf{Z}_p^d$-extension with $d\geqslant 2$. Choose K in $\mathfrak{S}'(k)$ and k_∞ in $\mathfrak{S}(k)$ so that $Kk_\infty=L$ and $K\cap k_\infty=k$. Let k_n be the unique subfield of k_∞ of degree p^n over k. Then $Kk_n\in\mathfrak{S}'(k_n)$, and hence we can speak of the invariants $m_0(Kk_n/k_n)=m_{0,n}$ and $l_0(Kk_n/k_n)=l_{0,n}$. We will establish the following result:

THEOREM 1: *There are constants m_1, l, c_1, and c so that for large n,*

$$m_{0,n}=m_0(L/k)p^n+m_1n+c_1 \qquad \textit{and},$$

$$l_{0,n}=lp^n+c.$$

Furthermore, $m_1\leqslant l_0(L/k)$.

The invariants m_1, l, c_1, and c appear at first glance to depend on L, K, k_∞, and k, but we will show that they are actually independent of k_∞, so that, fixing L and k, we can write $m_1(K)$, etc., and we can view m_1

and l as functions on $\mathcal{E}'(k)$. Furthermore, the m_1 invariant can be viewed as a "partial" l_0 invariant (details given below); this will be useful several times.

The strategy behind the proof of Theorem 1 is as follows: Just as the invariants $m_0(L/k)$ and $l_0(L/k)$ depend on the Λ_E structure of X_L, the invariants $m_{0,n}$ and $l_{0,n}$ are defined in terms of the Λ_G structure of X_{Kk_n}, where $G = G(Kk_n/k_n)$ (actually, we have some latitude in the choice of G, as we show in §4). Now, in §4, we show that the invariants of X_{Kk_n} can be realized as the invariants of a certain quotient module of X_L. In §3, we show that one can write down the Λ_G characteristic power series for this quotient module in terms of the Λ_E characteristic power series for X_L. This reduces the calculation of $m_{0,n}$ and $l_{0,n}$ to a calculation with power series. This calculation is carried out in §2.

Many of the ideas in this paper arose from thought provoking conversations with Ralph Greenberg and Paul Monsky. Thanks is also extended to Eduardo Friedman for his many stimulating letters.

2. Power series

Throughout, let W be the group of p-power roots of unity in the algebraic closure of $\mathbf{Q}_p$. If $\zeta \in W$, define $o(\zeta)$ by: $\zeta^{p^{o(\zeta)}} = 1$ and if $m < o(\zeta)$, $\zeta^{p^m} \neq 1$. If r is any integer and $\zeta = (\zeta_1, \dots, \zeta_r)$ is in W^r, we say that ζ is in $W^r(n)$ if $o(\zeta_i) \leqslant n$ for each i.

Let E be a multiplicative group isomorphic to the additive group in $\mathbf{Z}_p^d$, and put $\Lambda_E = \mathbf{Z}_p[[E]]$, the complete group ring of E over $\mathbf{Z}_p$. If we choose a basis $\{\sigma_1, \dots, \sigma_d\}$ for E, Λ_E can be viewed as the power series ring $\mathbf{Z}_p[[X_1, \dots, X_d]]$, by putting $X_i = \sigma_i - 1$; Λ_E is therefore a regular local ring.

Suppose f is in Λ_E, $f \neq 0$. We will define an integer $m_0(f)$, and a family of integers $l_G(f)$ where G ranges over the direct summands of E.

Let ord denote the p-adic exponential valuation on the algebraic closure of $\mathbf{Q}_p$ normalized so that ord $p = 1$. As in [7] we adopt the convention that ord $0 = 0$. Suppose $\zeta \in W$ and $\mathcal{O} = \mathbf{Z}_p[\zeta]$. We can define ord on $\Lambda_{E,\mathcal{O}} = \mathcal{O}[[X_1, \dots, X_d]]$ by putting ord g equal to the infimum of the p-orders of the coefficients of g. This allows us to view ord as a function on Λ_E, and if f is in Λ_E, $f \neq 0$, we see that ord f is simply the power to which p divides f. Comparing with the definition of $m_0(f)$ in [2], we have:

DEFINITION 2.1: If f is in Λ_E, $f \neq 0$, $m_0(f) = \operatorname{ord} f$.

Now, returning to the above situation, we let $\overline{\Lambda_{E,\mathcal{O}}}$ denote $\Lambda_{E,\mathcal{O}}/(\zeta - 1)\Lambda_{E,\mathcal{O}} \cong \mathbf{Z}_p[\zeta]/(\zeta - 1)[[X_1, \dots, X_d]]$. Note that $\overline{\Lambda_{E,\mathcal{O}}}$ is a unique factorization domain. If g is in $\Lambda_{E,\mathcal{O}}$, let $\bar{g}$ denote its image in $\overline{\Lambda_{E,\mathcal{O}}}$. Then if $\sigma \in E - E^p$, it is not hard to see that $\overline{\sigma - 1}$ is irreducible in $\overline{\Lambda_{E,\mathcal{O}}}$ and that if $\sigma \neq \sigma'$, $\overline{\sigma - 1} \neq \overline{\sigma' - 1}$. If $\mathcal{P}$ is any height one prime of $\overline{\Lambda_{E,\mathcal{O}}}$, let $\operatorname{ord}_{\mathcal{P}}$ denote the associated valuation on $\overline{\Lambda_{E,\mathcal{O}}}$.

DEFINITION 2.2: Suppose f is in $\Lambda_{E,\mathcal{O}}$, $f \neq 0$, and $f = (\zeta - 1)^m f_0$ where $\overline{f_0} \neq 0$. If G is any direct summand of E, put

$$l_G(f) = \sum \operatorname{ord}_{\mathcal{P}} \overline{f_0}$$

where $\mathcal{P}$ ranges over all the height one primes of $\overline{\Lambda_{E,\mathcal{O}}}$ of the form $\overline{\sigma - 1}$, $\sigma \in G - G^p$. Extend l_G to a function on all of $\Lambda_{E,\mathcal{O}}$ by putting $l_G(0) = 0$.

It is not hard to see that the function l_G is unchanged if we replace $\mathcal{O}$ by a larger cyclotomic ring. Also, if G is any direct summand of E and $f \in \Lambda_{G,\mathcal{O}}$, then $l_G(f) = l_E(f)$.

Comparing this definition with Monsky's definition of $l_0(f)$ in [8], we see that if f is in Λ_E, $l_0(f) = l_E(f)$. Also, it follows immediately that $l_G(f) \leqslant l_0(f)$ for every direct summand G of E, and $l_0(f) = 0 \Leftrightarrow l_G(f) = 0$ for every such G.

Let G' be a direct summand of E, and let $E = G' \oplus G$. Choose a basis $\{\sigma_1, \dots, \sigma_d\}$ for E so that G' is generated by $\sigma_1, \dots, \sigma_r$ and G is generated by $\sigma_{r+1}, \dots, \sigma_d$. Let $X_i = \sigma_{i-1}$, and identify Λ_E with $\mathbf{Z}_p[[X_1, \dots, X_d]]$. Suppose $f \in \Lambda_E$, $f \neq 0$. For each $\zeta = (\zeta_1, \dots, \zeta_r)$ in W^r, put $f_\zeta = f(\zeta_1 - 1, \dots, \zeta_r - 1, \quad X_{r+1}, \dots, X_d)$. Then if $\mathcal{O} = \mathbf{Z}_p[\zeta]$, $f_\zeta \in \mathcal{O}[[X_{r+1}, \dots, X_d]]$.

DEFINITION 2.3: Notation as above, we define for each integer n,

(a) $\Sigma_{n,G}(f) = \Sigma \operatorname{ord} f_\iota$ and

(b) $\Theta_{n,G}(f) = \Sigma l_G(f_\zeta)$,

the sum extending over all ζ in $W^r(n)$.

Specialize now to the case $r = 1$. Then $G' = \{\sigma_1\}$ and $G = \{\sigma_2, \dots, \sigma_d\}$. Also, if $\zeta \in W, f_\zeta = f(\zeta - 1, X_2, \dots, X_d)$, so it is not hard to see that $f_\zeta = 0$ for only finitely many values of ρ. The main object of this section is to prove the following theorem:

THEOREM 2.4: *Suppose f is in $\Lambda_E, f \neq 0$. Then there exist integers l, c_1, and c so that for large n,*

(a) $\Sigma_{n,G} = m_0(f)p^n + l_{G'}(f)n + c_1$ *and,*

(b) $\Theta_{n,G} = lp^n + c$.

PROOF: Suppose $m_0(f) = m_0$ and $l_{G'}(f) = a$. Then we can write f in the following way:

$$f = p^{m_0}\big(X_1^a\big(h_0(X_2,\dots,X_d) + h_1(X_2,\dots,X_d)X_1 + \dots\big)$$
$$+ p^s g(X_1,\dots,X_d)\big).$$

Here $h_i(X_2,\dots,X_d) \in \Lambda_G$, $g(X_1,\dots,X_d) \in \Lambda_E$, ord $h_i =$ ord $g = 0$, and $h_0 \neq 0$. Choose n_0 so that if $o(\zeta) = n > n_0$, $f_\zeta \neq 0$ and ord $(\zeta - 1)^a < s$. Then for $o(\zeta) = n > n_0$, ord $f_\zeta = m_0 + \operatorname{ord}(\zeta - 1)^a$, so $\Sigma_{n,G} = m_0(p^n - p^{n_0}) + \Sigma' \operatorname{ord}(\zeta - 1)^a + d$ where Σ' means the summation is over all ζ in $W(n)$ so that $o(\zeta) > n_0$ and d is a constant independent of n. So,

$$\Sigma_{n,G}(f) = m_0(p^n - p^{n_0}) + a(n - n_0) + d$$
$$= m_0(f)p^n + l_{G'}(f)n + c_1,$$

giving (a). For (b) we argue similarly:

$$\Theta_{n,G}(f) = \Sigma' l_G(f_\rho) + d = \Sigma' l_0(h_0) + d$$
$$= \Sigma' l + d = l(p^n - p^{n_0}) + d = lp^n + c.$$

Remark: Using the deeper techniques of [7], one can extend theorem 2.1 (a) to the case when G' is a direct summand of E of rank r. In this case we have:

$$\Sigma_{n,G}(f) = \big(m_0(f)p^n + l_{G'}(f)n + O(1)\big)p^{(r-1)n}.$$

The proof of this fact follows along the lines of the argument used to prove Theorem 1.7 in [2].

3. Λ_E-modules

As in §2, E is a multiplicative group isomorphic to the additive group in $\mathbf{Z}_p^d$. We recall briefly what we need of the structure theorem for finitely generated Λ_E-modules. For more details, see [1] or [2]. Since Λ_E identifies with a ring of formal power series over $\mathbf{Z}_p$, we will refer to elements of Λ_E as "power series". Suppose X is a finitely generated torsion Λ_E-module. Take a presentation of X:

$$\Lambda_E^s \to \Lambda_E^r \to X \to 0$$

where $r \leqslant s$. Let f be a generator for the g.c.d. of all $r \times r$ minors of this presentation. Then f is well defined up to multiplication by a unit and is independent of the presentation chosen; f is called the *characteristic* *power series* of X. X is *pseudonull* if its characteristic power series is 1 (in other words, if the annihilator of X is not contained in any height 1 prime of Λ_E).

If X and X' are finitely generated torsion Λ_E-modules, a Λ_E-homorphism $\pi: X \to X'$ is called a pseudoisomorphism if both the kernel and cokernel of π are pseudonull. Pseudoisomorphic modules have the same characteristic power series. If X is a finitely generated torsion Λ_E-module, there is a unique elementary module Z (that is, Z is a direct sum of cyclic modules $\Lambda_E/\mathfrak{p}_i^{e_i}$ where the $\mathfrak{p}_i$ are height one primes in Λ_E) and a pseudoisomorphism $\pi: Z \to X$. Such a π must be an injection, so we can consider Z as a submodule of X where X/Z is pseudonull. The characteristic power series for Z (and hence for X) is $\Pi \mathfrak{p}_i^{e_i}$.

If X is a finitely generated torsion Λ_E-module with characteristic power series f, we define $m_0(X)$ as $m_0(f)$. Similarly, if G is a direct summand of E, we put $l_G(X) = l_G(f)$.

Let $\{N_j\}$ be a finite family of pseudo-null Λ_E-modules. Thanks to Lemma 2 of [5], there are infinitely many direct summands G of E so that $E/G \cong \mathbf{Z}_p$ and each N_j is a finitely generated torsion Λ_G-module. Indeed, let f_j be an annihilator of N_j with $\bar{f}_j \neq 0$. If $\{\sigma_1, \dots, \sigma_d\}$ is a basis for E, one can find infinitely many sequences of integers $r_2 \leqslant \dots \leqslant r_d$ so that if $\sigma_i' = \sigma_1^{p^{r_i}}\sigma_i$, $\{\sigma_1, \sigma_2', \dots, \sigma_d'\}$ is a basis for Λ_E with the property that f_j, when viewed as a power series in $X_1, X_2', \dots, X_d'$ ($X_1 = \sigma_1 - 1$, $X_i' = \sigma_i' - 1$), is regular in X_1; that is, f_j contains a term of the form uX_1^λ for some unit u in $\mathbf{Z}_p$. It follows easily that each N_j is a finitely generated torsion Λ_G-module, where $G = \{\sigma_2', \dots, \sigma_d'\}$. In other words, we have:

LEMMA 3.1: *Suppose $\sigma_1 \in E - E^p$ and $G' = \{\sigma_1\}$. Let $\{N_j\}$ be a finite family of pseudo-null Λ_E-modules, and, for each j, let f_j be an annihilator of N_j with $\bar{f}_j \neq 0$. There are infinitely many direct summands G of E so that $E = G \oplus G'$ and, when viewed as an element of $\Lambda_G[[G']]$, f_j is regular in $X_1 = \sigma_1 - 1$. For such G, each N_j is a finitely generated torsion Λ_G-module.*

For the rest of this section, let $\{\sigma_1, \dots, \sigma_d\}$ be a fixed basis for E, $G' = \{\sigma_1\}$ and $G = \{\sigma_2, \dots, \sigma_d\}$. If n_0 is any positive integer, and $n > n_0$, we put $\alpha_{n,n_0} = (\sigma_1^{p^n} - 1)/(\sigma_1^{p^{n_0}} - 1)$. Often, we write α_n for α_{n,n_0}. Note that $\alpha_{n+1,n}$ is irreducible in Λ_E.

Suppose X is a finitely generated torsion Λ_E-module. Then if f is any annihilator of X, α_n and f are relatively prime in Λ_F for $n > n_0 \gg 0$. It follows that $\Lambda_E/(f, \alpha_n)$ is pseudo-null for $n > n_0$, and since α_n is regular in X_1, $\Lambda_E/(f, \alpha_n)$ is finitely generated and torsion over Λ_G, by Lemma 3.1. This implies that for $n_0 \gg 0$ and $n > n_0$, $X/\alpha_n X$ is a finitely generated torsion Λ_G-module, and hence we can speak of the Λ_G-invariants $m_0^G(X/\alpha_n X)$ and $l_0^G(X/\alpha_n X)$. The goal of this section is to investigate the growth of these invariants with n.

We will need the following technical definition. Suppose Z is the elementary module associated with X and f is the characteristic power series of M. Choose an annihilator f_1 of X/Z so that $(f_1, f)=1$, and choose another annihilator g of X/Z so that $(f_1, g)=1$. Then the modules $\Lambda_E/(f, f_1)$ and $\Lambda_E/(f_1, g)$ are pseudo-null. We say that G is "adapted to X" if these two modules are finitely generated torsion Λ_G-modules.

THEOREM 3.2: *Suppose X is a finitely generated torsion Λ_E-module, and n_0 is chosen so large that for $n > n_0$, $X/\alpha_n X$ is a finitely generated torsion Λ_G-module. Suppose further that G is adapted to X. Then*
(a) There exists a constant c_1 so that for $n \gg n_0$,

$$m_0^G(X/\alpha_n X) = m_0(X)p^n + l_{G'}(X)n + c_1$$

(b) There exist constants l and c so that for $n \gg n_0$,

$$l_0^G(X/\alpha_n X) = lp^n + c.$$

In the course of the proof of this result, we will have to enlarge n_0 a finite number of times. To see that this will not affect the result, consider, for example, the m_0^G invariant: If $n > n_0' > n_0$, we have

$$m_0^G(X/\alpha_{n,n_0'}X) = m_0^G(X/\alpha_{n,n_0}X) - m_0^G(\alpha_{n,n_0'}X/\alpha_{n,n_0}X).$$

But it is easy to see that the $m_0^G(\alpha_{n,n_0'}X/\alpha_{n,n_0}X)$ eventually stabalize.

The proof of Theorem 3.2 will use the more or less standard arguments for results of this type. If Z is the elementary module associated with X, we will prove our theorem for Z by appealing to Theorem 2.1. Then, we will show that for large n, the invariants of $X/\alpha_n X$ differ from those of $Z/\alpha_n Z$ by constants which are independent of n.

First, we handle the elementary case:

LEMMA 3.3: *Theorem 3.2 holds if X is elementary.*

PROOF: It is enough to prove the result when $X = \Lambda_F/f$ where f is in Λ_E, $f \neq 0$. For $n > n_0$, put $U_n = \Lambda_E/\alpha_n$, so that U_n is a free finitely generated Λ_G-module on which X_1 acts as a linear mapping. The eigenvalues of this mapping form the set $\{\zeta - 1 \mid n_0 < o(\zeta) \leqslant n\}$. Similarly, f acts on U_n with eigenvalues $\{f(\zeta - 1) \mid n_0 < o(\zeta) \leqslant n\}$. Viewing f as a linear mapping on U_n, we see that its cokernel is precisely $X/\alpha_n X$. For each n, we can take the determinant of this mapping, $\det_n f$, and obtain an element of Λ_G; in fact, $\det_n f = \Pi' f(\zeta - 1, X_2, \dots, X_d) = \Pi' f_\zeta$, where Π' means the product is over all ζ with $n_0 < o(\zeta) \leqslant n$. Since $X/\alpha_n X$ is a torsion Λ_G-module, $f_\zeta \neq 0$ for all ζ in this range, and it is shown in [1] that the ideal generated by $\det_n f$ in Λ_G is the characteristic power series of $X/\alpha_n X$ as a

Λ_G-module. So, $m_0^G(K/\alpha_n X) = m_0(\det_n f) = m_0(\Pi' f_\xi) = \Sigma' \operatorname{ord} f_\xi = \Sigma_{n,G}(f) + d$, and $l_0^G(M/\alpha_n X) = l_G(\det_n f) = l_G(\Pi' f_\xi) = \Sigma' l_G(f_\xi) = \Theta_{n,G}(f) + d'$. Now apply Theorem 2.1, noting that $m_0(X) = m_0(f)$ and $l_{G'}(X) = l_{G'}(f)$.

Note that in the case X is elementary, G is automatically adapted to X.

LEMMA 3.4. *Suppose N is a Λ_E-module which is finitely generated and torsion over Λ_G. Then the invariants $m_0^G(N/\alpha_n N)$ and $l_0^G(N/\alpha_n N)$ eventually stabalize.*

PROOF: It is easy to see that the sequences $m_0^G(N/\alpha_n N)$ and $l_0^G(N/\alpha_n N)$ are increasing with n. But $m_0^G(N/\alpha_n N) \leqslant m_0^G(N)$ and $l_0^G(N/\alpha_n N) \leqslant l_0^G(N)$.

We can now prove Theorem 3.2. Recall that X is an arbitrary finitely generated torsion Λ_E-module (with associated elementary module Z), and G is adapted to X. Let f be the characteristic power series of X, and suppose f_1 and g are two relatively prime annihilators of X/Z so that $(f_1, f) = 1$.

We have, for each n, a map induced by inclusion: $Z/\alpha_n Z \to X/\alpha_n X$. The kernel of this map is $B_n = (\alpha_n X \cap Z)/\alpha_n Z$, and the cokernel is $X/(Z + \alpha_n Z) \approx (X/Z)/[\alpha_n(X/Z)]$. Since G is adapted to X, $\Lambda_E/(f_1, g)$ is finitely generated and torsion over Λ_G. It follows that X/Z is also a finitely generated torsion Λ_G-module, so by lemma 3.4, the invariants of the cokernel eventually stabalize. For the kernel, we argue as follows: Multiplication by f_1 induces a Λ_E-homomorphism $f_{1,n}: Z/\alpha_n Z \to Z/\alpha_n Z$, and $B_n \subset \ker f_{1,n}$. So the invariants of B_n are bounded by the invariants of $\ker f_{1,n}$. But $\ker f_{1,n} \simeq \operatorname{coker} f_{1,n} \simeq Z/(\alpha_n Z + f_1 Z)$. Now there is a surjective homomorphism $(\Lambda_E/(f, f_1, \alpha_n))^u \to Z/(\alpha_n Z + f_1 Z)$ (u is independent of n), and since G is adapted to X, the invariants of $\Lambda_E/(f, f_1, \alpha_n)$ eventually stabalize by Lemma 3.4.

It follows that for $n \gg 0$, the invariants of $X/\alpha_n X$ and $Z/\alpha_n Z$ differ by constants which are independent of n. Lemma 3.3 and the fact that $m_0(X) = m_0(Z)$ and $l_{G'}(X) = l_{G'}(Z)$ give the desired result.

REMARK: Theorem 3.2 a) can even be proved without the assumption that G is adapted to X.

4. Galois groups

The goal of this section is to prove Theorem 1. Recall that L is a $\mathbf{Z}_p^d$-extension of a number field k, K is a $\mathbf{Z}_p^{d-1}$-extension of k contained in L and k_∞ is a $\mathbf{Z}_p$-extension of k in L so that $k_\infty K = L$ and $k_\infty \cap K = k$. Suppose that $E = G(L/k)$ and that $E = \{\sigma_1, \dots, \sigma_d\}$ where $G(L/K) = G' = \{\sigma_1\}$ and $G(L/k_\infty) = G = \{\sigma_2, \dots, \sigma_d\}$. If k_n is the unique subfield of k_∞ of degree p^n over k, Kk_n/k_n is a $\mathbf{Z}_p^{d-1}$-extension and $G(Kk_n/k_n) \simeq G$.

We let M (resp. M_n) denote the maximal unramified pro-p extension of L (resp. of Kk_n), and we let $X = G(M/L)$ (resp. $X_n = G(M_n/Kk_n)$).

Now E acts on X by inner automorphisms; this makes X into a finitely generated torsion Λ_E-module ([4]). By definition, $m_0(L/k) = m_0(X)$ and $l_0(L/k) = l_0(X)$. Similarly, X_n is a finitely generated torsion Λ_G-module, and $m_{0,n} = m_0(Kk_n/k_n) = m_0^G(X_n)$; $l_{0,n} = l_0(Kk_n/k_n) = l_0^G(X_n)$.

Our first goal is to show that the invariants $m_{0,n}$ and $l_{0,n}$ are independent of k_∞; that is, we claim that if k'_∞ is a $\mathbf{Z}_p$-extension of k contained in L with intermediate fields k'_n so that $k'_\infty K = L$ and $k'_\infty \cap K = k$, then $m_0(Kk'_n/k'_n) = m_0(Kk_n/k_n)$ and $l_0(Kk'_n/k'_n) = l_0(Kk_n/k_n)$.

To see this, note first that Kk_n is just the fixed field of $\sigma_1^{p^n}$ in L, so it is independent of k_n (and hence of k_∞); let $Kk_n = K_n$. It follows that the fields M_n and the Iwasawa-Greenberg modules X_n are also independent of k_∞. It remains to show that the invariants of X_n as a Λ_G-module are the same as the invariants of X_n as a Λ_H-module where $H = G(L/k'_\infty)$. To this end, we need the following general lemma:

LEMMA 4.1: *Suppose L/k is a $\mathbf{Z}_p^d$-extension and $E = G(L/k)$. Let k_n denote the fixed field of E^{p^n}. Then, for any integer m,*

$$\text{(a) } m_0(L/k_m) = p^{dm} m_0(L/k) \qquad \textit{and,}$$

$$\text{(b) } l_0(L/k_m) = p^{(d-1)m} l_0(L/k).$$

PROOF: If $n > m$, $k_n = (k_m)_{n-m}$. From formula (1) of §1,

$$\big(m_0(L/k)p^n + l_0(L/k)n + \mathrm{O}(1)\big)p^{(d-1)n} = e_n =$$

$$\big(m_0(L/k_m)p^{n-m} + \lambda_0(L/k_m)(n-m) + \mathrm{O}(1)\big)p^{(d-1)(n-m)}.$$

Since this is valid for all $n > m$, Lemma 4.1 follows.

Returning to the comparison between the invariants of K_n/k_n and K_n/k'_n, note that for each n, the fixed field of $G(K_n/k_n)^{p^n}$ in K_n is the same as the fixed field of $G(K_n/k'_n)^{p^n}$ in K_n; this field is just the fixed field of E^{p^n} in L, call it $k_{n,n}$. Appling Lemma 4.1 to K_n/k_n and K_n/k'_n (with $m = n$), we find:

$$p^{(d-1)} m_{0,n} = m_0(K_n/k_{n,n}) = p^{(d-1)n} m'_{0,n} \qquad \text{and,}$$

$$p^{(d-2)} l_{0,n} = l_0(K_n/k_{n,n}) = p^{(d-2)n} l'_{0,n}$$

So, $m_{0,n} = m'_{0,n}$ and $l_{0,n} = l'_{0,n}$. We have proved:

LEMMA 4.2: *With the above notation, the invariants $m_{0,n}$ and $l_{0,n}$ are independent of k_∞.*

REMARK: The invariants $m_{0,n}$ and $l_{0,n}$ are determined by he Λ_H structure ($H = G(K/k)$) of the modules X_n. In this way we can view Theorem 1 as a result about $\mathbf{Z}_p$-extensions of algebraic number fields K, where, rather than assuming that $[K:\mathbf{Q}]$ is finite, we assume that K is a multiple $\mathbf{Z}_p$-extension of a finite extension of $\mathbf{Q}$.

Combining lemmas 3.1 and 4.2, we see that we can assume without loss of generality that G is adapted to X. We make this assumption for the rest of our discussion.

Let $\eta_n = \sigma_1^{p^n} - 1$, so that the commutator subgroup of $G(M/K_n)$ is $\eta_n X$. If we let J_n be the subgroup of $G(M/K_n)$ generated by $\eta_n X$ and all the inertia groups in $G(M/K_n)$, and we put $Y_n = J_n \cap X$, then we have:

LEMMA 4.3: *There is an integer n_0 so that for $n > n_0$, $X_n \simeq (X/Y_n) \oplus \mathbf{Z}_p^r$. Here, $r = 0$ or 1 and is independent of n. Also, for $n > n_0$, $Y_n = \alpha_n Y_{n_0}$.*

PROOF: This is just Proposition 3.1 of [3]. The proof given there is for $d = 2$, but the same proof goes through for arbitrary d.

We can now prove Theorem 1. Note first that X/Y_{n_0} is annihilated by η_{n_0}, and, since X/Y_{n_0} is a torsion Λ_G-module, it is also annihilated by an element of Λ_G. Hence, X/Y_{n_0} is a pseudo-null Λ_E-module. Since m_0 and $l_{G'}$ depend only on the characteristic power series of a module, (that is, on a module's pseudo-isomorphism class), we see that $m_0(X) = m_0(Y_{n_0})$ and $l_{G'}(X) = l_{G'}(Y_{n_0})$. Also, since G is adapted to X, G is adapted to Y_{n_0}. Using Lemma 4.3 and Theorem 3.2, we find that for $n \gg 0$,

$$\begin{aligned} n_{0,n} &= m_0^G(X_n) = m_0^G(X/Y_n) = m_0^G(X/Y_{n_0}) + m_0^G(Y_{n_0}/Y_n) \\ &= d + m_0^G(Y_{n_0}/\alpha_n Y_{n_0}) = m_0(Y_{n_0})p^n + l_{G'}(Y_{n_0})n + c_1 \\ &= m_0(L/k)p^n + m_1 n + c_1. \end{aligned}$$

Note that $m_1 = l_{G'}(X) \leqslant l_0(X) = l_0(L/k)$.

For $l_{0,n}$ we argue similarly:

$$\begin{aligned} l_{0,n} &= l_0^G(X_n) = l_0^G(X/Y_n) = l_0^G(X/Y_{n_0}) + l_0^G(Y_{n_0}/Y_n) \\ &= d + l_0^G(Y_{n_0}/\alpha_n Y_{n_0}) = lp^n + c. \end{aligned}$$

Theorem 1 is proved.

The remark following the proof of Theorem 2.1 suggests that it may be possible to generalize Theorem 1 a) as follows: Suppose L/k is a $\mathbf{Z}_p^d$-extension, $K_\infty \subset L$ is a $\mathbf{Z}_p^r$-extension of k, and $K \subset L$ is a $\mathbf{Z}_p^{d-r}$-extension of k so that $K_\infty K = L$ and $K_\infty \cap K = k$. Let the fixed field of

$G(K/k)^{p^n}$ in K be k_n, so that Kk_n is a $\mathbf{Z}_p^{d-r}$-extension of k_n with m_0-invariant $m_{0,n}$.

Conjecture: With the above notation, there is a non-negative integer m_1 so that

$$m_{0,n} = \left(m_0(L/k)p^n + m_1 n + \mathrm{O}(1)\right)p^{(r-1)n}.$$

Of course, when $r = 1$, we have a weak form of Theorem 1 a). One can also consider formula (1) of §1 as a special case $(r = d)$ of this conjecture.

5. Examples and applications

In this section, we use Theorem 1 to obtain the results mentioned in §1.

We begin with a method for making m_0 large. Let ζ_p be an element of W so that $o(\zeta) = 1$, and suppose F is a finite Galois extension of $\mathbf{Q}$ so that $\mathbf{Q}(\zeta_p) \subset F$. Denote complex conjugation by J, and consider J as an element of $G(F/\mathbf{Q})$. If R is a $\mathbf{Z}_p$-extension of F which is Galois over $\mathbf{Q}$, J acts on $G(R/F)$ by conjugation.

LEMMA 5.1: *Notation as above, suppose $R^{(1)}, R^{(2)}, \dots, R^{(d)}$ are $\mathbf{Z}_p$-extensions of F, Galois over $\mathbf{Q}$, so that $G(R^{(i)}/F)^{1+J} = 1$ and $R^{(i)} \cap R^{(j)} = F$ for $i \neq j$. Suppose $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_t$ are primes in F which split completely in each $R^{(i)}$. Find $\alpha \in F$ so that ord $\mathfrak{p}_i = 1$ for each i, and let $k = F(\sqrt[p]{\alpha})$, $L = R^{(1)} \dots R^{(d)}(\sqrt[p]{\alpha})$. Then $m_0(L/k) > t - [F:\mathbf{Q}]$.*

PROOF: Induct on d; when $d = 1$, this is a theorem of Iwasawa ([6]). Suppose $d > 1$. To simplify notation, let $R = R^{(1)}$, $R' = R^{(2)} \dots R^{(d)}$, and let R_n be the intermediate fields of R/F. Let $k_\infty = R(\sqrt[p]{\alpha})$, $K = R'(\sqrt[p]{\alpha})$, and let k_n be the intermediate fields of k_∞/k. Finally let $\mathfrak{p}$ denote one of the $\mathfrak{p}_i$ and let $\mathfrak{P}^{(n)}$ be any prime of R_n over $\mathfrak{p}$.

Now, since $\mathfrak{p}$ splits completely in each $R^{(s)}$, $\mathfrak{P}^{(n)}$ splits completely in each $R^{(s)}R_n$ $(s = 2, \dots, d)$. Since $\mathrm{ord}_{\mathfrak{p}}\alpha = 1$, $\mathrm{ord}_{\mathfrak{P}(n)}\alpha = 1$ also. Applying the induction hypothesis to the fields R_n and $R^{(s)}R_n$ $(s = 2, \dots, d)$, we find that $m_0(Kk_n/k_n) > tp^n - [R_n:\mathbf{Q}] = (t - [F:\mathbf{Q}])p^n$. But $L = Kk_\infty$ and so, by Theorem 1, $m_0(L/k)p^n + m_1 n + c_1 > (t - [F:\mathbf{Q}])p^n$ for $n \gg 0$; Lemma 5.1 follows.

Now, suppose d is a positive integer and p is a prime so that $p > 2d + 1$. If $F = \mathbf{Q}(\zeta_p)$, there are d independent $\mathbf{Z}_p$-extensions of F that satisfy the hypotheses of Lemma 5.1. Furthermore, any prime in F which is inert from the maximal real subfield of F will split completely in each of these $\mathbf{Z}_p$-extensions. Since there are infinitely many such primes, we have:

THEOREM 5.2: *If d and N are positive integers and $p > 2d + 1$, then there exists a cyclic extension k of $F = \mathbf{Q}(\zeta_p)$ and a $\mathbf{Z}^d$-extension L of k so that $m_0(L/k) > N$.*

Next, we describe a condition that insures the vanishing of m_0. Let L/k be a $\mathbf{Z}_p^d$-extension and let F be a subfield of L containing k. We say that p is almost finitely decomposed in F if every prime of k that ramifies in L is finitely decomposed in F. Suppose $k' \in S$ and $k_\infty \in \mathfrak{S}(k)$. Then if p is almost finitely decomposed in k_∞, p is almost finitely decomposed in $k_\infty k'$. It follows (cf. [6]) that if $\mu(k_\infty/k) = 0$, then $\mu(k_\infty k'/k') = 0$ also.

THEOREM 5.3: *If L/k is a $\mathbf{Z}_p^d$-extension and $k_\infty \in \mathfrak{S}(k)$ has the property that $\mu(k_\infty/k) = 0$ and p is almost finitely decomposed in k_∞, then $m_0(L/k) = 0$.*

PROOF: Induct on d. If $d = 1$, $L = k_\infty$ and there is nothing to prove. Suppose $d > 1$. Find $R \in \mathfrak{S}(k)$ and $K \in \mathfrak{S}'(k)$ so that $k_\infty \subset K$ and $R \cap K = k$. Let R_n be the intermediate fields of R. The above discussion shows that p is almost finitely decomposed in $k_\infty R_n/R_n$ and $\mu(k_\infty R_n/R_n) = 0$. So, by the induction hypothesis, $m_0(KR_n/R_n) = 0$ for all n. But for $n \gg 0$, $m_0(KR_n/R_n) = m_0(L/k)p^n + m_1 n + c_1$.

REMARK: Using Theorems 5.2 and 5.3, it is not hard to construct examples of $\mathbf{Z}_p^d$-extensions L/k where $m_0(L/k) = 0$ but μ is greater than this generic value infinitely often on $\mathfrak{S}(k)$. It would be interesting to find examples where $\mu(R/k) < m_0(L/k)$ for some $R \in \mathfrak{S}(k)$.

Returning to the previous notation, let L/k be a $\mathbf{Z}_p^d$-extension. We consider the relationship between $l_0(L/k)$ and the behavior of μ on $\mathfrak{S}(k)$. Because of Lemma 4.2, we can view the m_1 and l of Theorem 1 as functions on $\mathfrak{S}'(k)$; our results are based on the following observations: If $K \in \mathfrak{S}'(k)$, $m_1(K) = l_G(X_L)$ where $G = G(L/K)$. It follows that if $l_0(L/k) \neq 0$, then $m_1(K) \neq 0$ for some $K \in \varepsilon'(k)$. That is,

LEMMA 5.4. *It m_1 vanishes identically on $\mathfrak{S}'(k)$, $l_0(L/k) = 0$.*

THEOREM 5.5. *Suppose $d \geqslant 3$ and p is finitely decomposed in L. Then if $l_0(L/k) \neq 0$, $\mu(R/k) \neq 0$ for infinitely many R in $\mathfrak{S}(k)$.*

PROOF: Suppose $\mu = 0$ except on a finite subset of $\mathfrak{S}(k)$. Let K be any element of $\mathfrak{S}'(k)$. Since $\mathrm{d} \geqslant 3$, we can find a $\mathbf{Z}_\mathrm{p}$-extension R/k so that $R \subset K$ and $\mu(R/k) = 0$. If $k_\infty \in \mathfrak{S}(k)$ is such that $k_\infty K = L$ and $k_\infty \cap K = k$, then $\mu(Rk_n/k_n) = 0$ for all n, and hence, from Theorem 5.3, $m_0(Kk_n/k_n) = 0$. It follows that $m_1(K) = 0$; Lemma 5.4 gives the desired result.

REMARK: A similar argument shows that if L/k is a $\mathbf{Z}_p^2$-extension in which p is finitely decomposed, then $l_0(L/k) \neq 0$ implies $\mu(R/k) \neq 0$ for some $R \in \mathfrak{S}(k)$ (this could also be proved using one of the main results in [4]). More generally, we have:

THEOREM 5.6. *If L/k is a $\mathbf{Z}_p^d$-extension in which p is finitely decomposed, then $l_0(L/k) \neq 0$ implies $m_0(K/k) \neq 0$ for some $K \in \mathfrak{S}'(k)$.*

PROOF: Suppose $m_0(K/k) = 0$ for every $K \in \mathfrak{S}'(k)$. Then every such K contains an R in $\mathfrak{S}(k)$ so that $\mu(R/k) = 0$. Arguing as in Theorem 5.5, we find that $m_1(K) = 0$; now apply Lemma 5.4.

Return now to the case where L/k is an arbitrary $\mathbf{Z}_p^d$-extension (with no restriction on ramification). Suppose that $E = G(L/k)$ and f is the characteristic power series for X_L. If $m = m_0(L/k)$, $f = p^m f_0$ where $\bar{f}_0 \neq 0$. Suppose $l_0(L/k) \neq 0$. Then there is an element γ in $E - E^p$ so that $\overline{\gamma - 1}$ is a factor of $\bar{f}_0$. Let $X_1 = \gamma - 1$, and choose $X_2, \dots, X_d$ so that $\Lambda_E \cong \mathbf{Z}_p[[X_1, \dots, X_d]]$. Let $\sigma = X_2 + 1$, and let K be the fixed field of σ, so that $K \in \mathfrak{S}'(k)$. Then, as in the proof of Theorem 2.1. we can write f in the following way:

$$f = p^m\big(X_2^a (h_0(X_1, X_3, \dots, X_d) + h_1(X_1, X_3, \dots, X_d) X_2 + \dots)$$
$$+ p^s g(X_1, X_2, \dots, X_d)\big)$$

where $a = m_1(K)$. Now $\bar{X}_1 \mid \bar{f}_0$ and so $X_1 \mid \bar{h}_0$. This implies that $l_0(h_0) \neq 0$. But $l_0(h_0) = l(K)$, and we have the following result:

LEMMA 5.7. *If $l_0(L/k) \neq 0$, then there is some $K \in \mathfrak{S}'(k)$ so that $l(K) \neq 0$.*

THEOREM 5.8. *Let L/k be a $\mathbf{Z}_p^d$-extension with $d \geqslant 2$. If $l_0(L/k) \neq 0$, there exists a $k' \in S$ and $K' \in \mathfrak{S}'(k')$ so that $l_0(K'/k') \neq 0$.*

PROOF: Let $K \in \mathfrak{S}'(k)$ be so that $l(K) \neq 0$. If k_∞ is a $\mathbf{Z}_p$-extension of k so that $k_\infty K = L$ and $k_\infty \cap K = k$, then for $n \gg 0$, $l_0(Kk_n/k_n) = l(K)p^n + c$.

Applying Theorem 5.8 recursively, we obtain the following result:

COROLLARY 5.9. *If L/k is a $\mathbf{Z}_p^d$-extension with $l_0(L/k) \neq 0$, then there exists k' in S and a $\mathbf{Z}_p^2$-extension K' of k' with $l_0(K'/k') \neq 0$.*

Combining this with Theorem B, we have:

COROLLARY 5.10. *If L/k is a $\mathbf{Z}_p^d$-extension with $l_0(L/k) \neq 0$, then there exists k' in S so that λ is unbounded on $\mathfrak{S}(k')$.*

REMARK: Theorems 5.5, 5.6, and 5.8 can be viewed as giving necessary conditions for the non vanishing of l_0. However, it is not hard to construct module theoretic examples to show that these necessary conditions are not sufficient.

As a final application, we investigate the effect of a characteristic power series that is not a power of p on the subfields of a $\mathbf{Z}_p^d$-extension.

LEMMA 5.11. *Suppose L/k is a $\mathbf{Z}_p^d$-extension ($d \geq 2$), and suppose further that the characteristic power series for X_L is not a power of p. Then there exists k' in S and K' in $\mathfrak{S}'(k')$ with the property that the characteristic power series for the Iwasawa-Greenberg module for K'/k' is not a power of p.*

PROOF: Let f be an irreducible factor of the characteristic power series for X_L, $f \neq p$. Choose generators $\sigma_1, \ldots, \sigma_d$ for $E = G(L/k)$ so that $f \notin (\sigma_1 - 1, p)$; identify Λ_E with $\mathbf{Z}_p[[X_1, \ldots, X_d]]$ where $X_i = \sigma_i - 1$. Let K be the fixed field for σ_1 and let k_∞ be the fixed field for $G = \{\sigma_2, \ldots, \sigma_d\}$. Choose $n_0 > 0$ so that if $\sigma \in W$ and $o(\zeta) \geq n_0$, then $f_\zeta \neq 0$ (and ord $f_\zeta = 0$), where, as in §2, $f_\zeta = f(\zeta - 1, X_2, \ldots, X_d)$.

Using Lemma 4.3, we see that there is a submodule Y of X_L so that $X_L \sim Y$ (as Λ_E-modules), and for $n \gg 0$,

$$X_n = G\left(M_{Kk_n}/Kk_n\right) \sim Y/\alpha_n Y \oplus \mathbf{Z}_p^r.$$

Here $\sim$ means "pseudoisomorphic as Λ_G-modules", $r = 0$ or 1 and is independent of n, and k_n is the n^{th} layer of k_∞. We will be done if we can find something other than p in the support of $Y/\alpha_n Y$ for some $n \gg 0$. Now, since $X_L \sim Y$, there is a presentation of Y:

$$\Lambda_E^s \to \Lambda_E^r \to Y \to 0 \tag{1}$$

so that f divides each $r \times r$ minor. This presentation gives rise to an exact sequence:

$$\left(\Lambda_E/\alpha_n\right)^s \to \left(\Lambda_E/\alpha_n\right)^r \to Y/\alpha_n Y \to 0 \tag{2}$$

so that each $r \times r$ minor is divisible by $\hat{f}$, where $\hat{f}$ is the image of f in Λ_E/α_n. Now, Λ_E/α_n identifies with $\Lambda_G^{p^n - p^{n_0}}$ as Λ_G-modules. Under this identification $\hat{f}$ defines a linear mapping on $\Lambda_G^{p^n - p^{n_0}}$; let M denote this mapping (M is represented by a $p^n - p^{n_0} \times p^n - p^{n_0}$ matrix with entries in Λ_G). Using this, we get a presentation:

$$\Lambda_G^u \to \Lambda_G^v \to Y/\alpha_n Y \to 0 \tag{3}$$

where $u = s(p^n - p^{n_0})$ and $v = r(p^n - p^{n_0})$. Now, it is not hard to see that any $v \times v$ minor of this presentation is divisible by det M. But, as in §2, det $M = \prod_{n \geqslant o(\zeta) > n_0} f_\zeta$, a non zero element of Λ_G which is not a power of p.

THEOREM 5.12 *Suppose that L/k is a $\mathbf{Z}_p^d$-extension ($d \geqslant 2$) and that the characteristic power series for X_L is not a power of p. Then, given any integer N, there is a k' in S and K' in $\mathfrak{S}(k')$ so that $\lambda(K'/k') > N$.*

PROOF: From Lemma 5.11 we can assume $d = 2$. Furthermore, we can assume $l_0(L/k) = 0$ (otherwise, apply Corollary 5.10). Let f be the characteristic power series for X_L. As in Theorem 2.1, we can write

$$f = p^m\left(h_0(T) + h_1(T)S + \ldots + p^s g(S, T)\right)$$

where $m = m_0(L/k)$, $S = \sigma - 1$, $T = \tau - 1$ and $E = \{\sigma, \tau\}$. Furthermore the non zero coefficients of the h_i are units in $\mathbf{Z}_p$, $h_0(T) \neq 0$ (because $l_0(L/k) = 0$) and $h_0(0) = 0$ (otherwise, $h_0(0)$ is a unit, and f can be replaced by p^m contrary to the hypothesis of the theorem). Therefore $l_0(h_0) \neq 0$. Hence, if K is the fixed field of σ, $l(K) \neq 0$. But if k_∞ is the fixed field of ζ, then $\lambda(Kk_n/k_n) = l(K)p^n + c$ for large n, giving the desired results.

References

[1] BOURBAKI, N.: Chapter VII, *Commutative Algebra.* Addison Wesley (1972).
[2] CUOCO, A. and MONSKY, P.: Class numbers in $\mathbf{Z}_p^d$-extensions. *Math. Ann. 255* (1981) 235–258.
[3] CUOCO, A.: The growth of Iwasawa's invariants in a family. *Comp. Math. 41* (1980) 415–437.
[4] GREENBERG, R.: The Iwasawa invariants of Γ-extensions of a fixed number field. *Am. J. of Math. 95* (1973) 204–214.
[5] GREENBERG, R.: On the structure of certain Galois groups. *Inventiones Math. 47* (1978) 85–89.
[6] IWASAWA, K.: On the μ-invariants of $\mathbf{Z}_l$-extensions. Number theory, Algebraic Geometry, and Commulative Algebra, in honor of Y. Akizuki, Kinokuniya, Tokyo, 1-11 (1973).
[7] MONSKY, P.: On P-adic power series. *Math. Ann. 255* (1981) 217–227.
[8] MONSKY, P.: Some invariants of $\mathbf{Z}_p^d$-extensions. *Math. Ann. 255* (1981) 229–233.

(Oblatum 22-IX-1981 & 24-VIII-1982)

Mathematics Department
Woburn High School
Woburn, MA 01801
USA