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>
1. Introduction

Let $k$ be a number field, $p$ a rational prime, $d$ a positive integer, and $L$ a $\mathbb{Z}_p^d$-extension of $k$ ($L/k$ is an abelian extension such that $G(L/k)$ is topologically isomorphic with the additive group in $\mathbb{Z}_p^d$). Let $E = G(L/k)$ and $\Lambda_E = \mathbb{Z}_p[[E]]$, the complete group ring of $E$ over $\mathbb{Z}_p$. If $M_L$ is the maximal unramified pro-$p$ extension of $L$, put $X_L = G(M_L/L)$. $X_L$ is a compact $\mathbb{Z}_p$-module, and the action of $E$ on $X_L$ by inner automorphisms makes $X_L$ into a finitely generated torsion $\Lambda_E$-module, the “Iwasawa-Greenberg module” for $L/k$. Now, the $\Lambda_E$-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 $n$,

$$e_n = (m_0 p^n + l_0 n + O(1)) p^{(d-1)n}.$$  \hspace{1cm} (1)

The invariants $m_0(L/k)$ and $l_0(L/k)$ are defined in terms of the $\Lambda_E$ 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 $\mu$ and $\lambda$ are Iwasawa’s invariants. There are examples (cf. §5) where $m_0(L/k)$ is large, but there are no known examples when $d \geq 2$ and $l_0(L/k) = 0$.

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

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

**Theorem A:** There is a finite subset $A$ of $\mathcal{S}'(k)$ so that if $K \in \mathcal{S}(k)$ 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 $\lambda$ on $\mathcal{S}(k)$. 

89
One consequence of Theorem A is that $\mu$ is bounded on $\mathcal{E}(k)$. 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 $\lambda$, we find a relationship between $l_0$ and $\mu$: under certain conditions, if $\mu = 0$ almost everywhere on $\mathcal{E}(k)$, 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 $\mathcal{E}'(k)$). We also show that the $l_0 = 0$ problem for $d = 2$ can be solved if one finds a $\mathbb{Z}_p^d$-extension $L/k$ with $d \geq 3$ and $l_0(L/k) \neq 0$. From this it will follow that if $L/k$ is an arbitrary $\mathbb{Z}_p^d$-extension ($d \geq 2$) so that $l_0(L/k) = 0$, then there exists a $k'$ in $\mathcal{S}$ so that $\lambda$ is unbounded on $\mathcal{E}(k')$.

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 $\Lambda_{\mathcal{E}}$-structure of $X_L$. In general, very little is known about the kinds of modules that can actually occur as Iwasawa-Greenberg modules for $\mathbb{Z}_p^d$-extensions. We will show that for a given $d$, if $p > 2d + 1$, there is a number field $k$ and a $\mathbb{Z}_p^d$-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 $\mathbb{Z}_p^d$-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 $\lambda$ invariants of $\mathbb{Z}_p$-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 $\mathcal{S}$ and $K'$ in $\mathcal{E}(k')$ 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 $\mathbb{Z}_p^d$-extension with $d \geq 2$. Choose $K$ in $\mathcal{E}'(k)$ and $k_\infty$ in $\mathcal{E}(k)$ so that $KK_\infty = L$ and $K \cap k_\infty = k$. Let $k_n$ be the unique subfield of $k_\infty$ of degree $p^n$ over $k$. Then $KK_n \in \mathcal{E}'(k_n)$, 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 $n$,

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

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

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

The invariants $m_1$, $l$, $c_1$, and $c$ appear at first glance to depend on $L$, $K$, $k_\infty$, and $k$, but we will show that they are actually independent of $k_\infty$, so that, fixing $L$ and $k$, we can write $m_1(K)$, etc., and we can view $m_1$
and $l$ as functions on $\mathcal{O}'(k)$. 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 $\Lambda_E$ structure of $X_L$, the invariants $m_{0,n}$ and $l_{0,n}$ are defined in terms of the $\Lambda_G$ structure of $X_{K_k,n}$, where $G = G(K_{k,n}/k_n)$ (actually, we have some latitude in the choice of $G$, as we show in §4). Now, in §4, we show that the invariants of $X_{K_k,n}$ can be realized as the invariants of a certain quotient module of $X_L$. In §3, we show that one can write down the $\Lambda_G$ characteristic power series for this quotient module in terms of the $\Lambda_E$ 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 $\mathbb{Q}_p$. If $\xi \in W$, define $\varrho(\xi)$ by: $\xi^{p^m} = 1$ and if $m < \varrho(\xi)$, $\xi^{p^m} \neq 1$. If $r$ is any integer and $\xi = (\xi_1, \ldots, \xi_r)$ is in $W^r$, we say that $\xi$ is in $W^r(n)$ if $\varrho(\xi_i) \leq n$ for each $i$.

Let $E$ be a multiplicative group isomorphic to the additive group in $\mathbb{Z}_p$, and put $\Lambda_E = \mathbb{Z}_p[[E]]$, the complete group ring of $E$ over $\mathbb{Z}_p$. If we choose a basis $\{\zeta_1, \ldots, \zeta_d\}$ for $E$, $\Lambda_E$ can be viewed as the power series ring $\mathbb{Z}_p[[X_1, \ldots, X_d]]$, by putting $X_i = \zeta_i - 1$; $\Lambda_E$ is therefore a regular local ring.

Suppose $f$ is in $\Lambda_E$, $f \neq 0$. 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 $\operatorname{ord}$ denote the $p$-adic exponential valuation on the algebraic closure of $\mathbb{Q}_p$. If $\xi \in W$, define $\varrho(\xi)$ by: $\xi^{p^m} = 1$ and if $m < \varrho(\xi)$, $\xi^{p^m} \neq 1$. If $r$ is any integer and $\xi = (\xi_1, \ldots, \xi_r)$ is in $W^r$, we say that $\xi$ is in $W^r(n)$ if $\varrho(\xi_i) \leq n$ for each $i$.

Let $\operatorname{ord}$ denote the $p$-adic exponential valuation on the algebraic closure of $\mathbb{Q}_p$ normalized so that $\operatorname{ord} p = 1$. As in [7] we adopt the convention that $\operatorname{ord} 0 = 0$. Suppose $\xi \in W$ and $\emptyset = \mathbb{Z}_p[\xi]$. We can define $\operatorname{ord}$ on $\Lambda_{E,\emptyset} = \emptyset[[X_1, \ldots, X_d]]$ by putting $\operatorname{ord} g$ equal to the infimum of the $p$-orders of the coefficients of $g$. This allows us to view $\operatorname{ord}$ as a function on $\Lambda_{E}$, and if $f$ is in $\Lambda_{E}$, $f \neq 0$, we see that $\operatorname{ord} f$ 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 $\Lambda_{E}$, $f \neq 0$, $m_0(f) = \operatorname{ord} f$.

Now, returning to the above situation, we let $\overline{\Lambda_{E,\emptyset}}$ denote $\Lambda_{E,\emptyset}/(\xi - 1)\Lambda_{E,\emptyset} = \mathbb{Z}_p[\xi]/(\xi - 1)[[X_1, \ldots, X_d]]$. Note that $\overline{\Lambda_{E,\emptyset}}$ is a unique factorization domain. If $g$ is in $\Lambda_{E,\emptyset}$, let $\bar{g}$ denote its image in $\overline{\Lambda_{E,\emptyset}}$. Then
if $\sigma \in E - E^p$, it is not hard to see that $\sigma^{-1}$ is irreducible in $\Lambda_{E,0}$ and that if $\sigma = \sigma'$, $\sigma^{-1} = \sigma'^{-1}$. If $\mathfrak{P}$ is any height one prime of $\Lambda_{E,0}$, let $\text{ord}_{\mathfrak{P}} \sigma$ denote the associated valuation on $\Lambda_{E,0}$.

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

$$l_G(f) = \sum \text{ord}_{\mathfrak{P}} f_0$$

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

It is not hard to see that the function $l_G$ is unchanged if we replace $\mathfrak{P}$ by a larger cyclotomic ring. Also, if $G$ is any direct summand of $E$ and $f \in \Lambda_{G,0}$, 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 $\Lambda_E$, $l_0(f) = l_E(f)$. Also, it follows immediately that $l_G(f) \leq l_0(f)$ for every direct summand $G$ of $E$, and $l_0(f) = 0 \Rightarrow l_G(f) = 0$ for every such $G$.

Let $G'$ be a direct summand of $E$, and let $E = G' \oplus G$. Choose a basis $(\sigma_1, \ldots, \sigma_d)$ for $E$ so that $G'$ is generated by $\sigma_1, \ldots, \sigma_r$ and $G$ is generated by $\sigma_{r+1}, \ldots, \sigma_d$. Let $X_i = \sigma_{r-1}$, and identify $\Lambda_E$ with $\mathbb{Z}_p[[X_1, \ldots, X_d]]$. Suppose $f \in \Lambda_E$, $f \neq 0$. For each $\xi = (\xi_1, \ldots, \xi_r)$ in $W^r$, put $f_\xi = f(\xi_1 - 1, \ldots, \xi_r - 1, X_{r+1}, \ldots, X_d)$. Then if $\mathfrak{P} = \mathbb{Z}_p[\xi]$, $f_\xi \in \mathfrak{P}[[X_{r+1}, \ldots, X_d]]$.

**Definition 2.3**: Notation as above, we define for each integer $n$,

(a) $\Sigma_{n,G}(f) = \Sigma \text{ord}_i f_i$ and

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

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

Specialize now to the case $r = 1$. Then $G' = (\sigma_1)$ and $G = (\sigma_2, \ldots, \sigma_d)$. Also, if $\xi \in W$, $f_\xi = f(\xi - 1, X_2, \ldots, X_d)$, so it is not hard to see that $f_\xi = 0$ for only finitely many values of $\rho$. 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:

\[
f = p^{m_0}(X_1^a(h_0(X_2, \ldots, X_d) + h_1(X_2, \ldots, X_d)X_1 + \ldots)
\]

\[+ p^g(X_1, \ldots, X_d)).\]

Here \( h_i(X_2, \ldots, X_d) \in \Lambda_G, g(X_1, \ldots, X_d) \in \Lambda_E, \) \( \text{ord } h_i = \text{ord } g = 0 \), and \( h_0 \neq 0 \). Choose \( n_0 \) so that if \( o(\zeta) = n > n_0, f^{\xi} \neq 0 \) and \( \text{ord } (\zeta - 1)^a < s \). Then for \( o(\zeta) = n > n_0, \) \( \text{ord } f^{\xi} = m_0 + \text{ord } (\zeta - 1)^a \), so \( \Sigma_{n,G} = m_0(p^n - p^{n_0}) + \sum' \text{ord } (\zeta - 1)^a + d \) where \( \sum' \) means the summation is over all \( \zeta \) 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:

\[
\Theta_{n,G}(f) = \Sigma' l_G(f) + d = \Sigma' l_0(h_0) + d
\]

\[= \Sigma' l + d = l(p^n - p^{n_0}) + d = lp^n + c.
\]

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:

\[
\Sigma_{n,G}(f) = (m_0(f)p^n + l_G(f)n + O(1))p^{(r-1)n}.
\]

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

3. \( \Lambda_E \)-modules

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

\[
\Lambda_E^r \to \Lambda_E^r \to X \to 0
\]

where \( r \leq s \). 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 $\Lambda_E$).

If $X$ and $X'$ are finitely generated torsion $\Lambda_E$-modules, a $\Lambda_E$-homomorphism $\pi : X \to X'$ is called a pseudoisomorphism if both the kernel and cokernel of $\pi$ are pseudonull. Pseudoisomorphic modules have the same characteristic power series. If $X$ is a finitely generated torsion $\Lambda_E$-module, there is a unique elementary module $Z$ (that is, $Z$ is a direct sum of cyclic modules $\Lambda_E/\mathfrak{p}^r_i$ where the $\mathfrak{p}_i$ are height one primes in $\Lambda_E$) and a pseudoisomorphism $\pi : Z \to X$. Such a $\pi$ 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 $\Pi \mathfrak{p}_i^r$.

If $X$ is a finitely generated torsion $\Lambda_E$-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 $\Lambda_E$-modules. Thanks to Lemma 2 of [5], there are infinitely many direct summands $G$ of $E$ so that $E/G \cong \mathbb{Z}_p$ and each $N_j$ is a finitely generated torsion $\Lambda_G$-module. Indeed, let $f_j$ be an annihilator of $N_j$ with $\bar{f}_j \neq 0$. If $\{\sigma_1, \ldots, \sigma_d\}$ is a basis for $E$, one can find infinitely many sequences of integers $r_2 \leq \ldots \leq r_d$ so that if $\sigma'_i = \sigma_{i'}/\sigma_i$, $\{\sigma_1, \sigma'_2, \ldots, \sigma'_d\}$ is a basis for $\Lambda_E$ with the property that $f_j$, when viewed as a power series in $X_1, X_2', \ldots, X_d'$ ($X_1 = \sigma_1 - 1, X'_i = \sigma_i' - 1$), is regular in $X_1$; that is, $f_j$ contains a term of the form $uX_i^k$ for some unit $u$ in $\mathbb{Z}_p$. It follows easily that each $N_j$ is a finitely generated torsion $\Lambda_G$-module, where $G = \langle \sigma_2', \ldots, \sigma_d' \rangle$. In other words, we have:

**Lemma 3.1:** Suppose $\sigma_1 \in E - E^p$ and $G' = \langle \sigma_1 \rangle$. Let $\{N_j\}$ be a finite family of pseudo-null $\Lambda_E$-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 $\Lambda_G$-module.

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

Suppose $X$ is a finitely generated torsion $\Lambda_E$-module. Then if $f$ is any annihilator of $X$, $\alpha_n$ and $f$ are relatively prime in $\Lambda_F$ for $n > n_0 \gg 0$. It follows that $\Lambda_E/(f, \alpha_n)$ is pseudo-null for $n > n_0$, and since $\alpha_n$ is regular in $X_1$, $\Lambda_E/(f, \alpha_n)$ is finitely generated and torsion over $\Lambda_G$, 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 $\Lambda_G$-module, and hence we can speak of the $\Lambda_G$-invariants $m_G^G(X/\alpha_n X)$ and $l_G^G(X/\alpha_n X)$. 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 $\Lambda_G$-modules.

**Theorem 3.2:** Suppose $X$ is a finitely generated torsion $\Lambda_E$-module, and $n_0$ is chosen so large that for $n > n_0$, $X/\alpha_n X$ is a finitely generated torsion $\Lambda_G$-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 stabilize.

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 $X = \Lambda_E/f$ where $f$ is in $\Lambda_E$, $f \neq 0$. For $n > n_0$, put $U_n = \Lambda_E/\alpha_n$, so that $U_n$ is a free finitely generated $\Lambda_G$-module on which $X_1$ acts as a linear mapping. The eigenvalues of this mapping form the set $(\xi - 1)_{n_0 < \xi(\xi) \leq n}$. Similarly, $f$ acts on $U_n$ with eigenvalues $(f(\xi - 1)_{n_0 < \xi(\xi) \leq n})$. 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 $\Lambda_G$: in fact, $\det_n f = \Pi f((\xi - 1), X_2, \ldots, X_d) = \Pi' f$, where $\Pi'$ means the product is over all $\xi$ with $n_0 < \xi(\xi) \leq n$. Since $X/\alpha_n X$ is a torsion $\Lambda_G$-module, $f_\xi \neq 0$ for all $\xi$ in this range, and it is shown in [1] that the ideal generated by $\det_n f$ in $\Lambda_G$ is the characteristic power series of $X/\alpha_n X$ as a
$\Lambda_G$-module. So, $m_0^G(K/\alpha_nX) = m_0(\det_n f) = m_0(\Pi'_f) = \Sigma'\text{ord}_f = \Sigma_{n,G}(f) + d$, and $l_0^G(M/\alpha_nX) = l_G(\det_n f) = l_G(\Pi'_f) = \Theta_{n,G}(f) + d'$. 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 $\Lambda_E$-module which is finitely generated and torsion over $\Lambda_G$. Then the invariants $m_0^G(N/\alpha_nN)$ and $l_0^G(N/\alpha_nN)$ eventually stabilize.

**Proof:** It is easy to see that the sequences $m_0^G(N/\alpha_nN)$ and $l_0^G(N/\alpha_nN)$ are increasing with $n$. But $m_0^G(N/\alpha_nN) \leq m_0^G(N)$ and $l_0^G(N/\alpha_nN) \leq l_0^G(N)$.

We can now prove Theorem 3.2. Recall that $X$ is an arbitrary finitely generated torsion $\Lambda_E$-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: $Z/\alpha_nZ \to X/\alpha_nX$. The kernel of this map is $B_n = (\alpha_n X \cap Z)/\alpha_nZ$, and the cokernel is $X/(Z + \alpha_nZ) \approx (X/Z)/(\alpha_n(X/Z))$. Since $G$ is adapted to $X$, $\Lambda_E/(f_1, g)$ is finitely generated and torsion over $\Lambda_G$. It follows that $X/Z$ is also a finitely generated torsion $\Lambda_G$-module, so by lemma 3.4, the invariants of the cokernel eventually stabilize. For the kernel, we argue as follows: Multiplication by $f_1$ induces a $\Lambda_E$-homomorphism $f_1,n : Z/\alpha_nZ \to Z/\alpha_nZ$, 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 $\ker f_1,n \approx \text{coker } f_1,n \approx Z/(\alpha_nZ + f_1Z)$. Now there is a surjective homomorphism $(\Lambda_E/(f, f_1, \alpha_n))^u \to Z/(\alpha_nZ + f_1Z)$ ($u$ is independent of $n$), and since $G$ is adapted to $X$, the invariants of $\Lambda_E/(f, f_1, \alpha_n)$ eventually stabilize by Lemma 3.4.

It follows that for $n \gg 0$, the invariants of $X/\alpha_nX$ and $Z/\alpha_nZ$ 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 $\mathbb{Z}_p^d$-extension of a number field $k$, $K$ is a $\mathbb{Z}_p^{d-1}$-extension of $k$ contained in $L$ and $k_\infty$ is a $\mathbb{Z}_p$-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 $E = (\sigma_1, \ldots, \sigma_d)$ where $G(L/K) = G' = (\sigma_1)$ and $G(L/k_\infty) = G = (\sigma_2, \ldots, \sigma_d)$. If $k_n$ is the unique subfield of $k_\infty$ of degree $p^n$ over $k$, $Kk_n/k_n$ is a $\mathbb{Z}_p^{d-1}$-extension and $G(Kk_n/k_n) = G$. [8]
We let $M$ (resp. $M_n$) denote the maximal unramified pro-$p$ extension of $L$ (resp. of $K_{k_n}$), and we let $X = G(M/L)$ (resp. $X_n = G(M_n/K_{k_n})$).

Now $E$ acts on $X$ by inner automorphisms; this makes $X$ into a finitely generated torsion $\Lambda^E_{G}$-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 $\Lambda^G_{G}$-module, and $m_{0,n} = m_0(K_{k_n}/k_{n}) = m_0^G(X_n)$; $l_{0,n} = l_0(K_{k_n}/k_{n}) = l_0^G(X_n)$.

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

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

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

(a) $m_0(L/k^m) = p^{dm}m_0(L/k)$ and,

(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,

$$m_0(L/k)p^n + l_0(L/k)n + O(1) = e_n =$$

$$m_0(L/k^m)p^{n-m} + l_0(L/k^m)(n-m) + O(1) = p^{(d-1)(n-m)}.$$

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 $E^p$ in $L$, call it $k_{n,n}$. Applying Lemma 4.1 to $K_{n}/k_n$ and $K_{n}/k'_{n}$ (with $m = n$), we find:

$$p^{(d-1)m_{0,n}} = m_0(K_{n}/k_{n,n}) = p^{(d-1)n}m'_{0,n}$$ 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 $k_{\infty}$. 


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

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 \(\eta_n = \sigma^n - 1\), 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 \(n > n_0\), \(X_n \cong (X/Y_n) \oplus \mathbb{Z}_p\). 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 \(\eta_{n_0}\), and, since \(X/Y_{n_0}\) is a torsion \(\Lambda_G\)-module, it is also annihilated by an element of \(\Lambda_G\). Hence, \(X/Y_{n_0}\) is a pseudo-null \(\Lambda_E\)-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 \(n \gg 0\),

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

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

For \(l_{0,n}\) we argue similarly:

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

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 \(\mathbb{Z}_p^d\)-extension, \(K_\infty \subset L\) is a \(\mathbb{Z}_p\)-extension of \(k\), and \(K \subset L\) is a \(\mathbb{Z}_p^{d-r}\)-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 $\mathbb{Z}_p^{d-r}$-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

$$m_{0,n} = (m_0(L/k)^{p^n} + m_1n + O(1))^{p(r-1)n}.$$  

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 $\xi_p$ be an element of $\mathcal{W}$ so that $o(\xi) = 1$, and suppose $F$ is a finite Galois extension of $\mathbb{Q}$ so that $\mathbb{Q}(\xi_p) \subseteq F$. Denote complex conjugation by $J$, and consider $J$ as an element of $G(F/\mathbb{Q})$. If $R$ is a $\mathbb{Z}_p$-extension of $F$ which is Galois over $\mathbb{Q}$, $J$ acts on $G(R/F)$ by conjugation.

**Lemma 5.1:** Notation as above, suppose $R^{(1)}, R^{(2)}, \ldots, R^{(d)}$ are $\mathbb{Z}_p$-extensions of $F$, Galois over $\mathbb{Q}$, so that $G(R^{(1)}/F)^{1+J} = 1$ and $R^{(i)} \cap R^{(j)} = F$ for $i \neq j$. Suppose $\wp_1, \wp_2, \ldots, \wp_r$ are primes in $F$ which split completely in each $R^{(i)}$. Find $a \in F$ so that $ord \wp_i = 1$ for each $i$, and let $k = F(\wp a), L = R^{(1)} \ldots R^{(d)}(\wp a)$. Then $m_0(L/k) > t - [F:\mathbb{Q}]$.

**Proof:** Induct on $d$; when $d = 1$, this is a theorem of Iwasawa ([6]). Suppose $d > 1$. To simplify notation, let $R = R^{(1)}, R' = R^{(2)} \ldots R^{(d)}$, and let $R_n$ be the intermediate fields of $R/F$. Let $k_\infty = R(\wp a), K = R'(\wp a)$, and let $k_n$ be the intermediate fields of $k_\infty/k$. Finally let $\wp$ denote one of the $\wp_i$ and let $G_{\wp(n)}$ be any prime of $R_n$ over $\wp$.

Now, since $\wp$ splits completely in each $R^{(s)}$, $G_{\wp(n)}$ splits completely in each $R^{(s)}_n$ ($s = 2, \ldots, d$). Since $ord \wp a = 1$, $ord G_{\wp(n)} a = 1$ also. Applying the induction hypothesis to the fields $R_n$ and $R^{(s)}R_n$ ($s = 2, \ldots, d$), we find that $m_0(Kk_n/k_n) > t^{p^n} - [R_n:\mathbb{Q}] = (t - [F:\mathbb{Q}])p^n$. But $L = Kk_\infty$ and so, by Theorem 1, $m_0(L/k)^{p^n} + m_1n + c_1 > (t - [F:\mathbb{Q}])p^n$ 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 $F = \mathbb{Q}(\xi_p)$, there are $d$ independent $\mathbb{Z}_p$-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 $\mathbb{Z}_p$-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 \( F = \mathbb{Q}(\zeta_p) \) and a \( \mathbb{Z}^d \)-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 \( \mathbb{Z}_p^d \)-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 \( k_\infty \in \mathcal{S}(k) \). Then if \( p \) is almost finitely decomposed in \( k_\infty \), \( p \) 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 \( \mathbb{Z}_p^d \)-extension and \( k_\infty \in \mathcal{S}(k) \) has the property that \( \mu(k_\infty/k) = 0 \) and \( p \) is almost finitely decomposed in \( k_\infty \), 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 \( R \in \mathcal{S}(k) \) and \( K \in \mathcal{S}'(k) \) 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 \( \mathbb{Z}_p^d \)-extensions \( L/k \) where \( m_0(L/k) = 0 \) but \( \mu \) is greater than this generic value infinitely often on \( \mathcal{S}(k) \). It would be interesting to find examples where \( \mu(R/k) < m_0(L/k) \) for some \( R \in \mathcal{S}(k) \).

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

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

**Theorem 5.5.** Suppose \( d \geq 3 \) 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 \( \mathcal{S}(k) \).

**PROOF:** Suppose \( \mu = 0 \) except on a finite subset of \( \mathcal{S}(k) \). Let \( K \) be any element of \( \mathcal{S}'(k) \). Since \( d \geq 3 \), we can find a \( \mathbb{Z}_p \)-extension \( R/k \) so that \( R \subset K \) and \( \mu(R/k) = 0 \). If \( k_\infty \in \mathcal{S}(k) \) is such that \( k_\infty K = L \), 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 \( m_0(K) = 0 \); Lemma 5.4 gives the desired result.
Remark: A similar argument shows that if \(L/k\) is a \(\mathbb{Z}_p^2\)-extension in which \(p\) is finitely decomposed, then \(l_0(L/k) \neq 0\) implies \(\mu(R/k) \neq 0\) for some \(R \in \mathcal{S}(k)\) (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 \(\mathbb{Z}_p^d\)-extension in which \(p\) is finitely decomposed, then \(l_0(L/k) \neq 0\) implies \(m_0(K/k) \neq 0\) for some \(K \in \mathcal{S}(k)\).

**Proof:** Suppose \(m_0(K/k) = 0\) for every \(K \in \mathcal{S}(k)\). Then every such \(K\) contains an \(R \in \mathcal{S}(k)\) 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 \(\mathbb{Z}_p^d\)-extension (with no restriction on ramification). Suppose that \(E = G(L/k)\) and \(f\) is the characteristic power series for \(X_1\). If \(m = m_0(L/k)\), \(f = p^m f^0\) where \(f^0 \neq 0\). Suppose \(l_0(L/k) \neq 0\). Then there is an element \(\gamma\) in \(E - E^p\) so that \(\gamma - 1\) is a factor of \(f^0\). Let \(X_1 = \gamma - 1\), and choose \(X_2, \ldots, X_d\) so that \(\Delta_E \cong \mathbb{Z}_p[[X_1, \ldots, X_d]]\). Let \(\sigma = X_2 + 1\), and let \(K\) be the fixed field of \(\sigma\), so that \(K \in \mathcal{S}(k)\). Then, as in the proof of Theorem 2.1, we can write \(f\) in the following way:

\[
f = p^m \left( X_2 (h_0(X_1, X_3, \ldots, X_d) + h_1(X_1, X_3, \ldots, X_d) X_2 + \ldots) + p^g(X_1, X_2, \ldots, X_d) \right)
\]

where \(a = m_1(K)\). Now \(X_1 | f_0\) and so \(X_1 | h_0\). 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 \(K \in \mathcal{S}(k)\) so that \(l(K) \neq 0\).

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

**Proof:** Let \(K \in \mathcal{S}(k)\) be so that \(l(K) \neq 0\). If \(k_\infty\) is a \(\mathbb{Z}_p\)-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 \(\mathbb{Z}_p^d\)-extension with \(l_0(L/k) \neq 0\), then there exists \(k' \in S\) and a \(\mathbb{Z}_p^d\)-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 \(\mathbb{Z}_p^d\)-extension with \(l_0(L/k) \neq 0\), then there exists \(k' \in S\) so that \(\lambda\) is unbounded on \(\mathcal{S}(k')\).
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 $\mathbb{Z}_p^d$-extension.

**LEMMA 5.11.** Suppose $L/k$ is a $\mathbb{Z}_p^d$-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 $S'(k')$ 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 $f \not\equiv (\sigma_1 - 1, p)$; identify $E$ with $\mathbb{Z}_p[[X_1, \ldots, X_d]]$ where $X_i = \sigma_i - 1$. Let $K$ be the fixed field for $\sigma_1$ and let $k_{\infty}$ be the fixed field for $G = \{\sigma_2, \ldots, \sigma_d\}$.

Choose $n_0 > 0$ so that if $\sigma \in W$ and $o(\sigma) \geq n_0$, then $f^e_0 \equiv 0$ (and ord $f = 0$), where, as in §2, $f^e_0 = f(\sigma - 1, X_2, \ldots, X_d)$.

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

$$X_n = G(M_{K/k_{n'}}/K_{k_{n'}}) \sim Y/\alpha_nY \oplus \mathbb{Z}_p^r.$$ 

Here $\sim$ means “pseudoisomorphic as $\Lambda_G$-modules”, $r = 0$ or 1 and is independent of $n$, and $k_{n'}$ is the $n$th layer of $k_{\infty}$. We will be done if we can find something other than $p$ in the support of $Y/\alpha_nY$ for some $n \gg 0$.

Now, since $X_L \sim Y$, there is a presentation of $Y$:

$$\Lambda_E^* \rightarrow \Lambda_E \rightarrow Y \rightarrow 0$$

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

$$(\Lambda_E/\alpha_n)^* \rightarrow (\Lambda_E/\alpha_n)^r \rightarrow Y/\alpha_nY \rightarrow 0$$

so that each $r \times r$ minor is divisible by $f$, where $f$ is the image of $f$ in $\Lambda_E/\alpha_n$. Now, $\Lambda_E/\alpha_n$ identifies with $\Lambda_G^{p^n - p^{n_0}}$ as $\Lambda_G$-modules. Under this identification $f$ 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 $\Lambda_G$). Using this, we get a presentation:

$$\Lambda_G^u \rightarrow \Lambda_G^v \rightarrow Y/\alpha_nY \rightarrow 0$$

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, $\det M = \prod_{n \geq \alpha(\xi) > n_0} f^n_\xi$, a non zero element of $\Lambda_G$ which is not a power of $p$.

**Theorem 5.12** Suppose that $L/k$ is a $\mathbb{Z}_p^d$-extension ($d \geq 2$) 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 $\mathcal{O}(k')$ 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

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

where $m = m_0(L/k)$, $S = \sigma - 1$, $T = \tau - 1$ and $E = \langle \sigma, \tau \rangle$. Furthermore the non zero coefficients of the $h_i$ are units in $\mathbb{Z}_p$, $h_0(T) \neq 0$ (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 $\sigma$, $l(K) \neq 0$. But if $k_\infty$ is the fixed field of $\xi$, then $\lambda(Kk_\infty/k_\infty) = l(K)p^n + c$ for large $n$, giving the desired results.

**References**


Mathematics Department
Woburn High School
Woburn, MA 01801
USA