JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Sören KLEINE

On pseudo-null Iwasawa modules

Tome 34, nº 2 (2022), p. 583-618.

https://doi.org/10.5802/jtnb.1218

Journal de Théorie des Nombres
de Bordeaux **34** (2022), 583–618

On pseudo-null Iwasawa modules

par Sören KLEINE

Résumé. Nous étudions les sous-modules pseudo-nuls maximaux de certains modules d'Iwasawa construits à partir des groupes de classes d'idéaux dans des $\mathbb{Z}_p^k$-extensions de corps de nombres. Nous décrivons quelques critères de la non-trivialité de ces modules, en nous concentrant sur les cas $k = 1$ et $k = 2$. De plus, nous en déduisons des applications à des formes faibles de la conjecture de Greenberg généralisée (GGC).

Abstract. We study the maximal pseudo-null submodules of Iwasawa modules arising from ideal class groups in $\mathbb{Z}_p^k$-extensions of number fields. We describe several sufficient criteria for the non-triviality of such modules, mainly in dimensions $k = 1$ and $k = 2$. This has applications to weak versions of Greenberg's Generalised Conjecture (GGC).

1. Introduction

Let p be a fixed rational prime. In this article, we study the maximal pseudo-null submodules of Iwasawa modules A attached to $\mathbb{Z}_p^k$-extensions of number fields. We denote by A° the maximal pseudo-null submodule of an Iwasawa module A (see Section 2 for the definitions). *Greenberg's Generalised Conjecture* (GGC) implies that pseudo-null Iwasawa modules appear quite naturally, in the following sense. Let $\mathbb{K}$ denote the composite of all $\mathbb{Z}_p$-extensions of a fixed number field K. Then $\mathbb{K}/K$ is a $\mathbb{Z}_p^d$-extension for some $d \in \mathbb{N}$ (if *Leopoldt's Conjecture* holds for K and p, then $d = r_2(K) + 1$, where $r_2(K)$ denotes the number of complex places of K). Let $A = A^{(\mathbb{K})}$ be the projective limit of p-Sylow subgroups of the ideal class groups of number fields contained in the extension $\mathbb{K}/K$. Greenberg's Generalised Conjecture (GGC) then states the following.

Conjecture (Greenberg; see [11, Conjecture (3.5)])**.** *The Iwasawa module $A = A^{(\mathbb{K})}$ is pseudo-null over the Iwasawa algebra $\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{K}/K)]\!]$, i.e. $A = A^\circ$.*

Only very few theoretical results are known concerning (GGC). We mention just some of them, without claiming to give an exhaustive overview. First, Nakayama's Lemma implies that (GGC) holds for K (and in fact

Manuscrit reçu le 26 février 2021, révisé le 2 juillet 2021, accepté le 11 novembre 2021.
2010 *Mathematics Subject Classification.* 11R23.
Mots-clefs. Greenberg's Generalised Conjecture, maximal pseudo-null submodules.

$A^{(\mathbb{K})} = \{0\}$) if K contains exactly one prime dividing p and the p-Sylow subgroup $A^{(K)}$ of the ideal class group of K is trivial. In fact, (GGC) for K holds if K contains exactly one prime $\mathfrak{p}$ dividing p and $A^{(K)}$ is cyclic, generated by the ideal class of $\mathfrak{p}$ or, more generally, if K is a finite normal p-ramified p-extension of such a number field (see [14, Theorem 4.6]).

It has been shown by McCallum and Sharifi (see [19, Corollary 10.5] and [30, Theorem 1.3]) that the conjecture is valid for $K = \mathbb{Q}(\zeta_p)$ for all $p < 1000$, and more generally if p is arbitrary, $A^{(K)}$ is cyclic and the restriction of a certain cup product to the cyclotomic p-units of K is non-trivial. Minardi proved in his thesis (see [20, Proposition 3.B]) that (GGC) holds if K is imaginary quadratic and $A^{(K)}$ is cyclic, generated by some power of a prime ideal of K dividing p (here p is allowed to split in K).

Finally, (GGC) for any number field K follows from [20, Proposition 4.B] if there exists a $\mathbb{Z}_p^2$-extension $\mathbb{L}$ of K such that $A^{(\mathbb{L})}$ is pseudo-null over the Iwasawa algebra $\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}/K)]\!]$ and only finitely many primes of $\mathbb{L}$ ramify in $\mathbb{K}$.

In more modern terms, pseudo-nullity can be phrased as the vanishing of the first Chern class of the Iwasawa module over the Iwasawa algebra; this geometric point of view has recently attained more and more attention (see for example [2]; this article promotes the study of higher Chern classes if (GGC) is known).

In [1], the following weaker conjecture has been introduced (in fact, the conjecture is stated in slightly different form there, namely for CM-fields K containing the p-th roots of unity; if p is totally split in $K/\mathbb{Q}$, then this formulation is equivalent to ours by [22, Lemme 2.1 and Lemme 2.2]).

Conjecture (Weak GGC)**.** *If* $A^{(\mathbb{K})} \neq \{0\}$*, then* $(A^{(\mathbb{K})})^\circ \neq \{0\}$.

It is obvious that (GGC) for K implies (Weak GGC) for K. Surprisingly, sometimes also the converse implication can be proved. In [1, Corollary 1.5], it is shown that (Weak GGC) actually is equivalent to (GGC) in the following situation: K is a CM-field containing a primitive p-th root of unity, Leopoldt's Conjecture and Iwasawa's μ-conjecture hold for K, and the characteristic power series of $\mathfrak{X}^{(L^+)}$ is irreducible, where L^+ denotes the cyclotomic $\mathbb{Z}_p$-extension of the maximal totally real subfield K^+ of K and where $\mathfrak{X}^{(L^+)}$ denotes the Galois group of the maximal abelian p-ramified pro-p-extension of L^+ over L^+.

Motivated by the (Weak GGC)-conjecture, we are interested in proving the non-triviality of the maximal pseudo-null submodules A° of Iwasawa modules. Actually very few results are known concerning the non-triviality of A°. The probably best-known result proves instead the triviality of such modules: if L denotes the cyclotomic $\mathbb{Z}_p$-extension of a CM-field K, $p \neq 2$, then the minus part $((A^{(L)})^\circ)^-$ of the maximal pseudo-null submodule is known to be trivial. Here the minus part is defined via the action of complex conjugation j on $A^{(L)}$: it consists of all elements a such that $j(a) = a^{-1}$. We will mention here just one known theoretical result proving the non-triviality of A° for some A: let K be a totally real number field in which the prime p is totally split, and suppose that Leopoldt's Conjecture holds for K, i.e. $\mathbb{K} = L$ is the cyclotomic $\mathbb{Z}_p$-extension of K. In [23], Ozaki proved that $(A^{(\mathbb{K})})^\circ \neq \{0\}$ if and only if the maximal p-ramified abelian pro-p-extension of $\mathbb{K}$ is strictly larger than the maximal subextension which is unramified over $\mathbb{K}$ (see also [6] for a slight generalisation of this result; the latter paper also describes reformulations of (GGC) and (Weak GGC) for totally real K in terms of *capitulation kernels*). In [4], Fujii proved an analogous result for imaginary quadratic number fields K in which the prime p splits.

In this article, we prove sufficient criteria for the non-triviality of A° for certain $\mathbb{Z}_p^k$-extensions. It will sometimes be advantageous to work with quotients $A^{\#} = A/D$ of A, where $D \subseteq A$ denotes the submodule generated by the ideal classes of primes which ramify in the given $\mathbb{Z}_p^k$-extension. In the literature (see, e.g., [12]) often the module $A' = A/B$ is considered, where B denotes the submodule generated by all primes above p (no matter whether these primes ramify in the $\mathbb{Z}_p^k$-extension or not). We have canonical surjections $A \twoheadrightarrow A^{\#} \twoheadrightarrow A'$, and $A' = A^{\#}$ if each prime above p is ramified in the $\mathbb{Z}_p^k$-extension under consideration (e.g. this is the case for the cyclotomic $\mathbb{Z}_p$-extension of any number field K).

First, we consider $\mathbb{Z}_p^1$-extensions L of K. In this case the pseudo-null Λ_1-submodules, $\Lambda_1 = \mathbb{Z}_p[\![T]\!]$, correspond to *finite* submodules. The main result of Section 3 (cf. Theorem 3.14 below) will imply the following

Theorem 1.1. *Let L/K be a $\mathbb{Z}_p$-extension, let $A = A^{(L)}$ and $A^{\#} = A/D$ be as above. We assume that each prime of K which ramifies in L is totally ramified. Let D_n denote the p-primary subgroup of the group of ideal classes of the n-th layer L_n of L/K which are generated by the primes of L_n ramifying in L (i.e. $D = \varprojlim D_n$).*

Then the following statements hold for every $n \in \mathbb{N}$.

(a) *If $|D_{n+2}|/|D_{n+1}| > |D_{n+1}|/|D_n|$, then $|A^\circ| \geq p^{n+1}$ or $|(A^{\#})^\circ| \geq p^{n+1}$ (possibly both inequalities are satisfied).*

(b) *If $\operatorname{rank}_p(D_{n+2}) > \operatorname{rank}_p(D_{n+1})$, then $|(A^{\#})^\circ| \geq p^{n+1}$.*

In order to illustrate the above theorem, we studied two lists of cubic number fields with signatures [3,0] and [1,1], each with 20000 elements (for more details, see Example 3.18). Letting $p = 2$, we have found about 200 (respectively, 900) examples satisfying the above conditions for the cyclotomic $\mathbb{Z}_p$-extension and $n = 0$. In particular, there happen to be more examples in the signature [1,1] situation. This is of interest because (GGC) for a totally real number field K actually predicts that $A = A^{(L)}$ should be finite for the cyclotomic $\mathbb{Z}_p$-extension L of K, whereas it need not be finite in the signature [1,1] case. One reason behind this observation may be that A is simply *trivial* very frequently in the totally real setting (in almost 75 % of our examples, compared to only 51 % in the signature [1,1] family).

Despite the much higher computational complexity, we have also found many examples satisfying the conditions from Theorem 1.1 for $p = 2$ and $n = 1$ and also for $p = 3$ and $n = 0$, thereby collecting some evidence suggesting that a non-trivial $(A^{\#})^\circ$ is not too uncommon. On the other hand, we will show that in the case of a CM-field K (and $p \neq 2$), the minus part of $(A^{\#})^\circ$ is trivial for the cyclotomic $\mathbb{Z}_p$-extension L of K (cf. Remark 3.4); as already mentioned above, it is well-known that also $(A^\circ)^- = \{0\}$ in this setting.

In Section 4, we generalise a result of Fujii ([3]) which concerns the non-triviality of $(A^{(\mathbb{L})})^\circ$ for some $\mathbb{Z}_p^2$-extensions $\mathbb{L}/K$ (see Theorem 4.2). This non-triviality follows from the existence of two suitable $\mathbb{Z}_p$-extensions L and M of K inside $\mathbb{L}$ such that $(A^{(L)})^\circ = \{0\}$ and $(A^{(M)})^\circ \neq \{0\}$.

We significantly generalise Fujii's result (see Theorem 4.3), in particular handling $\mathbb{Z}_p^k$-extensions $\mathbb{L}/K$ with arbitrary $k \geq 2$. For illustration, we formulate here a result in the special case that only one prime $\mathfrak{p}$ ramifies in $\mathbb{L}/K$.

Theorem 1.2. *Let $\mathbb{L}$ be a $\mathbb{Z}_p^k$-extension of a number field K, $k \geq 2$. We assume that exactly one prime $\mathfrak{p}$ of K ramifies in $\mathbb{L}$, and that $\mathfrak{p}$ is totally ramified.*

Suppose that there exist

(a) *a $\mathbb{Z}_p$-extension M/K contained in $\mathbb{L}$ such that $(A^{(M)})^\circ \neq \{0\}$, and*

(b) *a sequence of $\mathbb{Z}_p^i$-extensions $\mathbb{L}^{(i)}/K$, $1 \leq i \leq k-1$, contained in $\mathbb{L}$ such that $\mathbb{L}^{(1)} \subseteq \mathbb{L}^{(2)} \subseteq \cdots \subseteq \mathbb{L}^{(k-1)}$, $(M \cdot \mathbb{L}^{(i+1)})/(M \cdot \mathbb{L}^{(i)})$ is a $\mathbb{Z}_p$-extension and $\mathrm{pd}_{\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}^{(i)}/K)]\!]}(A^{(\mathbb{L}^{(i)})}) \leq 1$ for every i.*

Then $(A^{(\mathbb{L})})^\circ \neq \{0\}$.

Here pd denotes the projective dimension. Note: if

$$\mathrm{pd}_{\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}^{(i)}/K)]\!]}(A^{(\mathbb{L}^{(i)})}) \leq 1,$$

then $(A^{(\mathbb{L}^{(i)})})^\circ = \{0\}$; for $\mathbb{Z}_p^1$-extensions the converse is also true (see Lemma 4.1).

We then show how to deduce, under certain assumptions, that

$$A^{(\mathbb{L})} = (A^{(\mathbb{L})})^\circ$$

if $(A^{(\mathbb{L})})^\circ \neq \{0\}$ is already known. It is sometimes possible to check this condition via numerical computations. In view of Minardi's results mentioned above, this can be used in order to prove (GGC) for suitable number fields K (see Theorem 5.4 below).

In Section 5, we consider several applications. Suppose first that K contains exactly one prime above p. After proving several results concerning the non-triviality of $(A^{(M)})^\circ$ for suitable $\mathbb{Z}_p$-extensions M of K and deriving an application to (GGC), we give a proof of Theorem 1.2. In the second part of Section 5, we consider finite extensions K of an imaginary quadratic field k. We assume that p splits in k and that the primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of k dividing p do not split further in K/k. Let $\Bbbk$ denote the $\mathbb{Z}_p^2$-extension of k, $\mathbb{L} = \Bbbk \cdot K$, and let M and $\overline{M}$ be the $\mathbb{Z}_p$-extensions of K contained in $\mathbb{L}$ which are ramified at exactly one of the two primes of K dividing p. We assume that the prime $\mathfrak{p}_2$ which is unramified in M *does not split at all* in M/K (this is a technical assumption which is, however, crucial for our argument; it is known a priori only that the prime $\mathfrak{p}_2$ splits into finitely many primes in M).

In this setting we prove sufficient criteria for the non-triviality of pseudo-null submodules (see Theorem 5.9). We obtain infinite families of number fields to which our results apply.

Acknowledgement. I would like to thank Cornelius Greither, Martin Hofer and in particular Katharina Müller for making valuable comments concerning an earlier version of this article, and I am very grateful to Dominik Bullach for a fruitful discussion concerning Lemma 4.1. Finally, I thank the anonymous referee for the very thorough reading of the manuscript and for suggesting several valuable improvements of the contents and the exposition of the article.

2. Notation and basic facts

In what follows, we fix a rational prime p and a number field K. A $\mathbb{Z}_p^k$-*extension* of K is a normal extension $\mathbb{L}$ of K such that $\Gamma := \mathrm{Gal}(\mathbb{L}/K)$ is topologically isomorphic to $\mathbb{Z}_p^k$, where $\mathbb{Z}_p$ denotes the additive group of p-adic integers. Every $\mathbb{Z}_p^k$-extension $\mathbb{L}$ of K is the union of the intermediate fields $\mathbb{L}_n := \mathbb{L}^{\Gamma^{p^n}}$ fixed by Γ^{p^n}, $n \in \mathbb{N}$. Each $\mathbb{L}_n$ is abelian over K, and $\mathrm{Gal}(\mathbb{L}_n/K) \cong (\mathbb{Z}/p^n\mathbb{Z})^k$.

For any number field M, we denote by $A^{(M)}$ the p-primary subgroup of the ideal class group of M. For a $\mathbb{Z}_p^k$-extension $\mathbb{L}$ of K, $\mathbb{L} = \bigcup_n \mathbb{L}_n$, we write $A_n = A^{(\mathbb{L}_n)}$, and we study the projective limit $A = A^{(\mathbb{L})} := \varprojlim A_n$ with respect to the norm maps. Moreover, we consider certain quotients of A. For each $n \in \mathbb{N}$, let $D_n = D^{(\mathbb{L}_n)}$ denote the subgroup generated by the primes of $\mathbb{L}_n$ which ramify in $\mathbb{L}$ (note that the notion of $D_0 \subseteq A^{(K)}$ may depend on the chosen $\mathbb{Z}_p^k$-extension of K; if K contains only one prime above p, then the group $D^{(K)}$ is well-defined). Then we obtain projective limits $D = \varprojlim D_n$ and $A^{\#} = A/D = \varprojlim A_n^{\#}$, where $A_n^{\#} := A_n/D_n$, $n \in \mathbb{N}$.

The completed group ring $\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}/K)]\!]$ acts on A and $A^{\#}$. This group ring is isomorphic to the ring $\Lambda_k := \mathbb{Z}_p[\![T_1, \dots, T_k]\!]$ of formal power series in k variables over $\mathbb{Z}_p$, the so-called *Iwasawa algebra* in k variables. We let $\Lambda := \Lambda_1 = \mathbb{Z}_p[\![T]\!]$. It is well-known that A is a finitely generated torsion $\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}/K)]\!]$-module (cf. [10, Theorem 1]; for more details concerning these and the following facts, see [31] and [21]).

In this paper, any finitely generated and torsion Λ_k-module will be called an *Iwasawa module*. An Iwasawa module N is called *pseudo-null* if the annihilator ideal of N is not contained in any prime ideal of height at most one (alternatively, if the localisation of N at any prime ideal of Λ_k of height at most one is trivial; cf. [21, Definition (5.1.4)]). This is equivalent to the fact that the annihilator ideal of N contains two coprime elements of the unique factorisation domain Λ_k. One can show that a Λ_1-module is pseudo-null if and only if it is finite (see [31, Lemmas 13.7 and 13.10]).

By a general structure theorem (see [21, Theorem (5.1.10)], each Iwasawa Λ_k-module A is pseudo-isomorphic to an *elementary* torsion Λ_k-module, i.e. a module of the form

$$E_A = \bigoplus_{i=1}^{s} \Lambda_k/(h_i)$$

with suitable elements $h_i \in \Lambda_k$ and $s \in \mathbb{N}$; here *pseudo-isomorphic* means that there exists a Λ_k-module homomorphism $\varphi\colon A \longrightarrow E_A$ such that the kernel and the cokernel of φ are pseudo-null.

The product $F_A := \prod_i h_i \in \Lambda_k$ is called the *characteristic power series* of A; it is unique up to units. In particular, if $k = 1$, then the Weierstraß Preparation Theorem (see [31, Theorem 7.3]) implies that $F_A \in \mathbb{Z}_p[\![T]\!]$ is associated to a power $p^{\mu(A)}$ of p times a so-called distinguished polynomial. We denote by $\lambda(A)$ the degree of this polynomial. The integers $\mu(A)$ and $\lambda(A)$ are called the *Iwasawa invariants* of A.

In this paper, we will usually denote $\mathbb{Z}_p = \mathbb{Z}_p^1$-extensions of K by L, $\widetilde{L}$ or M. $\mathbb{L}$ will usually denote a $\mathbb{Z}_p^k$-extension of K with $k \geq 2$, and $\mathbb{K}$ denotes the composite of *all* $\mathbb{Z}_p$-extensions of K.

If $A = \varprojlim A_n^{(L)}$ denotes the Iwasawa module of ideal class groups for some $\mathbb{Z}_p$-extension L/K, then a famous theorem of Iwasawa describes the asymptotic growth of $e_n = v_p(|A_n^{(L)}|)$ in terms of the Iwasawa invariants of A:

$$e_n = \mu(A) \cdot p^n + \lambda(A) \cdot n + \nu(A) \tag{2.1}$$

for some constant $\nu(A) \in \mathbb{Z}$ and each sufficiently large n. A similar formula holds for $A^{\#} = \varprojlim A_n^{\#}$.

Let now A be any Iwasawa Λ_k-module. The kernel of any pseudo-isomorphism

$$\varphi\colon A \longrightarrow E_A$$

will be denoted by A°. Note that $A^\circ \subseteq A$ is the maximal pseudo-null Λ_k-submodule, since E_A does not contain any non-trivial pseudo-null submodules. In particular, A° is independent of the choice of φ.

For any algebraic extension N of $\mathbb{Q}$, we let $H(N)$ denote the maximal abelian unramified pro-p-extension of N, and we denote by $H'(N)$ the maximal subfield of $H(N)$ in which each prime of N dividing p is totally split. By class field theory, there exists an isomorphism $A^{(N)} \cong \mathrm{Gal}(H(N)/N)$.

Recall that in a $\mathbb{Z}_p^1$-extension L/K only primes of K dividing p can ramify, and at least one of them has to. For each prime $\mathfrak{p}$ of K ramifying in L, there exists a unique index $n = n_{\mathfrak{p}}$ such that $\mathfrak{p}$ is unramified in L_n/K and totally ramified in L/L_n (here $L_n \subseteq L$ denotes the n-th layer, as above). Let $e := e(L/K)$ denote the maximum of the integers $n_{\mathfrak{p}}$ for the primes $\mathfrak{p}$ of K which ramify in L.

3. The finite torsion submodules of Iwasawa modules of $\mathbb{Z}_p$-extensions

We start by mentioning some

3.1. Known results. Let L/K be a $\mathbb{Z}_p$-extension. In this section, we study the maximal finite submodules of $A = \varprojlim A_n$ and $A^\# = \varprojlim A_n^\#$. Our arguments will exploit the Galois module structure of these Λ-modules.

Let $m, n \in \mathbb{N}$, $m \geq n$. Then $\mathrm{Gal}(L_m/L_n)$ acts on A_m. Moreover, the cardinality of the subgroup fixed by $\mathrm{Gal}(L_m/L_n)$ can be computed by using the following

Theorem 3.1 (Chevalley, Gras)**.** *Let M/K be a cyclic extension of number fields. Let $S = S_{\mathrm{ram}}(M/K)$ denote the set of primes of K ramifying in M, and let E_K and E_K^S denote the groups of units and S-units of K. Moreover, let $N_{M/K}\colon M^\times \longrightarrow K^\times$ denote the norm map, and write $r(M/K)$ and $f(M/K)$ for the products of the ramification indices and inertia degrees in M/K of all the primes in S. Then*

(i) $$|(A^{(M)})^{\mathrm{Gal}(M/K)}| = \frac{|A^{(K)}| \cdot r(M/K)}{[M:K] \cdot [E_K : (N_{M/K}(M^*) \cap E_K)]},$$

(ii) $$|((A^\#)^{(M)})^{\mathrm{Gal}(M/K)}| = \frac{|(A^\#)^{(K)}| \cdot r(M/K) \cdot f(M/K)}{[M:K] \cdot [E_K^S : (N_{M/K}(M^*) \cap E_K^S)]} \cdot$$

Proof. See [17, Lemma 4.1 in Chapter 13] for a proof of Chevalley's Theorem (i), and [9] for a proof of (ii). □

Lemma 3.2. *Let $L = \bigcup_n L_n$ be a $\mathbb{Z}_p$-extension of K, and let $m \geq n$. We consider the canonical homomorphism $i_{n,m} \colon A_n \longrightarrow A_m$ induced by the lifting of ideals, and we denote by $i_{n,m}^{\#} \colon A_n^{\#} \longrightarrow A_m^{\#}$ the induced map. Let $S = S_{\mathrm{ram}}(L_m/L_n)$ be the set of primes of L_n which ramify in L_m. Then*

$$[E_n^S : N_{m,n}(E_m^S)] = p^{(m-n)\cdot(|S|-1)} \cdot |\ker(i_{n,m}^{\#} \colon A_n^{\#} \longrightarrow A_m^{\#})|$$

and

$$[E_n : N_{m,n}(E_m)] = p^{s_{m,n}-(m-n)} \cdot |\ker(i_{n,m} \colon A_n \longrightarrow A_m)|,$$

where

$$\begin{aligned} p^{s_{m,n}} &= |P_{L_m}^{\mathrm{Gal}(L_m/L_n)}/(i_{n,m}(I_{L_n}) \cap P_{L_m}^{\mathrm{Gal}(L_m/L_n)})| \\ &= |(P_{L_m}^{\mathrm{Gal}(L_m/L_n)} + i_{n,m}(I_{L_n}))/i_{n,m}(I_{L_n})|. \end{aligned}$$

Here E_n and E_n^S denote the groups of units and S-units of L_n, I_{L_n} denotes the free group of fractional ideals of L_n, and P_{L_m} denotes the group of principal fractional ideals of L_m.

Proof. We first recall that

$$|\ker(i_{n,m}^{\#})| = |H^{-1}(\mathrm{Gal}(L_m/L_n), E_m^S)|$$

and

$$|\ker(i_{n,m})| \cdot p^{s_{m,n}} = |H^{-1}(\mathrm{Gal}(L_m/L_n), E_m)|;$$

here the first statement goes back to Iwasawa (see [12, Theorem 12]; Iwasawa considers the case where S contains *all* the primes above p). The second statement can be proved similarly (cf. [13, Corollary 3.81] and [29]).

The Herbrand quotients

$$q(\mathrm{Gal}(L_m/L_n), E_m) = p^{-(m-n)}$$

and

$$q(\mathrm{Gal}(L_m/L_n), E_m^S) = p^{(m-n)(|S|-1)}$$

can be computed as in [27]. □

Recall the notion of the Iwasawa invariant $\mu(A)$ from Section 2.

Lemma 3.3 (Grandet, Jaulent)**.** *Suppose that $\mu(A) = 0$. Then for sufficiently large n, the capitulation kernel* $\ker(i_{n,n+1} \colon A_n \longrightarrow A_{n+1})$ *is isomorphic to the group $A^\circ[p]$ of elements of A° which are annihilated by p.*

An analogous statement holds for the Iwasawa module $A^{\#}$.

Proof. The statement for A has been proved in [8]. The same proof goes through for $A^{\#}$. □

Let us finally briefly consider the special case of a CM-field K. It is well-known that the minus part of A° is trivial for the cyclotomic $\mathbb{Z}_p$-extension L of a CM-field K (see [31, Proposition 13.28]). In fact, the same holds for the minus part of $(A^{\#})^\circ$, by the following

Remark 3.4. Let K be a CM-field, and let L/K be the cyclotomic $\mathbb{Z}_p$-extension, $p \neq 2$. Suppose that $A^+ = \{0\}$. Then $(A^\#)^\circ$ is trivial.

Indeed, fix $m \geq n \geq e(L/K)$, and consider the exact sequence

$$0 \longrightarrow E_m \longrightarrow E_m^S \longrightarrow \mathbb{Z}^{j_m} \longrightarrow 0,$$

where j_m denotes the number of primes of L_m above p. In the induced exact sequence[1]

$$H^1(\mathrm{Gal}(L_m/L_n), E_m) \longrightarrow H^1(\mathrm{Gal}(L_m/L_n), E_m^S) \longrightarrow H^1(\mathrm{Gal}(L_m/L_n), \mathbb{Z}^{j_m}),$$

the last term $H^1(\mathrm{Gal}(L_m/L_n), \mathbb{Z}^{j_m}) = \mathrm{Hom}(\mathrm{Gal}(L_m/L_n), \mathbb{Z}^{j_m})$ is trivial. Therefore the triviality of $H^1(\mathrm{Gal}(L_m/L_n), E_m^-)$ (see [31, Lemma 13.27]) implies that $H^1(\mathrm{Gal}(L_m/L_n), (E_m^S)^-) = \{0\}$. This can be used in order to prove that $((A^\#)^\circ)^- = \{0\}$, as in the proof of [31, Proposition 13.28].

3.2. Comparing ranks of A° and $(A^\#)^\circ$. Let us introduce the following notation: for a Λ-module M, $\Lambda = \mathbb{Z}_p[\![T]\!]$, and any $\lambda \in \Lambda$ we define

$$\mathrm{rank}_\lambda(M) := v_p(|M/(\lambda \cdot M)|),$$

provided that the quotient is finite. For example,

$$\mathrm{rank}_T(A_m) = v_p(|A_m/(T \cdot A_m)|) = v_p(|A_m^{\mathrm{Gal}(L_m/K)}|),$$

since A_m is finite and $\mathrm{Gal}(L_m/K)$ is generated by $\gamma = T + 1$. Theorem 3.1 therefore can be regarded as a statement about the growth of T-ranks.

Lemma 3.5. *Suppose that $\mu(A) = 0$.*

(i) *Then $i_{k,k+1}(A_k) = p \cdot A_{k+1}$ for each sufficiently large $k \geq e(L/K)$ (the parameter $e(L/K)$ has been introduced at the end of Section 2).*

(ii) *For $\lambda \in \Lambda$ and $k \in \mathbb{N}$, we define $r_k^{(\lambda)} = \mathrm{rank}_\lambda(A_k) - \mathrm{rank}_\lambda(A_k^\#)$. Then $r_k^{(\lambda)} = v_p(|D_k/(\lambda A_k \cap D_k)|)$.*

(iii) *If k is as in* (i), *then $r_{k+1}^{(p)} = j_k - s_{k+1,k}$, where j_k denotes the number of primes of L_k which ramify in L_{k+1} and $s_{k+1,k}$ is defined as in Lemma 3.2.*

Proof. Statement (i) is [13, Lemma 3.72] and follows also from the results of [8]. For (ii), we just observe that

$$|D_k/(D_k \cap \lambda A_k)| = |(D_k + \lambda A_k)/(\lambda A_k)| = p^{r_k^{(\lambda)}}.$$

In order to prove (iii), we recall the notation introduced in Lemma 3.2. Let $J_{L_{k+1}} \subseteq I_{L_{k+1}}$ be the free subgroup generated by the ramified primes. Then

$$J_{L_{k+1}}/(i(I_{L_k}) \cap J_{L_{k+1}}) = J_{L_{k+1}}/pJ_{L_{k+1}}$$

[1] We thank the anonymous referee for suggesting this argument.

has order p^{j_k}, where we abbreviated $i_{k,k+1}$ to i. On the other hand, (ii) implies that $|D_{k+1}/(i(A_k) \cap D_{k+1})| = p^{r_{k+1}^{(p)}}$ for each k as in (i). The difference between these two quotients is given by the group

$$((P_{L_{k+1}} + i(I_{L_k})) \cap J_{L_{k+1}})/(i(I_{L_k}) \cap J_{L_{k+1}}).$$

Since

$$(P_{L_{k+1}} + i(I_{L_k})) \cap J_{L_{k+1}} = (P_{L_{k+1}}^{\mathrm{Gal}(L_{k+1}/L_k)} + i(I_{L_k})) \cap J_{L_{k+1}},$$

the latter group can be written as

$$((P_{L_{k+1}}^{\mathrm{Gal}(L_{k+1}/L_k)} + i(I_{L_k})) \cap J_{L_{k+1}})/(i(I_{L_k}) \cap J_{L_{k+1}}).$$

This quotient is isomorphic to

$$(P_{L_{k+1}}^{\mathrm{Gal}(L_{k+1}/L_k)} + i(I_{L_k}))/i(I_{L_k})$$

and therefore has order $p^{s_{k+1,k}}$. □

Now we prove an easy result relating the ranks of the maximal pseudo-null Λ-modules of A and of quotients A/B of A.

Lemma 3.6. *Suppose that $A/(\lambda \cdot A)$ is finite for some $\lambda \in \Lambda$, let $B \subseteq A$ be any Λ-submodule and let $r^{(\lambda)} = \mathrm{rank}_\lambda(A) - \mathrm{rank}_\lambda(A/B)$. Then*

$$\mathrm{rank}_\lambda((A/B)^\circ) + r^{(\lambda)} = \mathrm{rank}_\lambda(A^\circ) + \mathrm{rank}_\lambda(B) - \mathrm{rank}_\lambda(B^\circ).$$

Proof. By [13, Proposition 3.58], $\mathrm{rank}_\lambda(A) = \mathrm{rank}_\lambda(E_A) + \mathrm{rank}_\lambda(A^\circ)$; analogous equations hold for A/B and B. Since the characteristic polynomials satisfy the equation

$$F_A(T) = F_B(T) \cdot F_{A/B}(T),$$

it follows that

$$\mathrm{rank}_\lambda(E_A) = \mathrm{rank}_\lambda(E_{A/B}) + \mathrm{rank}_\lambda(E_B). \tag{3.1}$$

Indeed, suppose that $f, g \in \Lambda$ are elements which are relatively prime with λ, i.e. such that the quotient $\Lambda/(\lambda, fg)$ is finite. We will prove[2] that

$$\mathrm{rank}_\lambda(\Lambda/(fg)) = \mathrm{rank}_\lambda(\Lambda/(f)) + \mathrm{rank}_\lambda(\Lambda/(g)). \tag{3.2}$$

To this purpose, we first note that

$$[\Lambda : (\lambda, fg)] = [\Lambda : (\lambda, f)] \cdot [(\lambda, f) : (\lambda, fg)].$$

Now we consider the canonical map $\Lambda/(\lambda, g) \longrightarrow (\lambda, f)/(\lambda, fg)$ induced by the multiplication by f. This map is well-defined and surjective. In order to show that it is also injective, we let $x \in \Lambda$ be an element such that $fx \in (\lambda, fg)$. Then there exist $a, b \in \Lambda$ such that $fx = a\lambda + bfg$. This means that $f(x - bg) = a\lambda$ is divisible by λ in the UFD Λ. But f and λ are relatively prime. Therefore $x - bg \in (\lambda)$ and thus $x \in (\lambda, g)$.

[2] We thank the anonymous referee for suggesting this strategy of proof.

We have shown that multiplication by f induces a canonical isomorphism

$$\Lambda/(\lambda, g) \xrightarrow{\sim} (\lambda, f)/(\lambda, fg).$$

Therefore

$$[\Lambda : (\lambda, fg)] = [\Lambda : (\lambda, f)] \cdot [\Lambda : (\lambda, g)],$$

proving (3.2). This means that for any finitely generated torsion Λ-module M with elementary Λ-module E_M and every $\lambda \in \Lambda$ which is coprime with the characteristic polynomial $F_M(T)$, we have

$$\mathrm{rank}_\lambda(E_M) = \mathrm{rank}_\lambda(\Lambda/(F_M)).$$

By the multiplicativity of characteristic polynomials, we obtain (3.1). Rearranging terms proves the lemma. □

Corollary 3.7. *Suppose that* $\mathrm{rank}_\lambda(A) < \infty$*, and let*

$$r^{(\lambda)} = \mathrm{rank}_\lambda(A) - \mathrm{rank}_\lambda(A/B).$$

- *If* $r^{(\lambda)} > \mathrm{rank}_\lambda(B) - \mathrm{rank}_\lambda(B^\circ) - \mathrm{rank}_\lambda((A/B)^\circ)$*, then* $A^\circ \neq \{0\}$.
- *If* $r^{(\lambda)} < \mathrm{rank}_\lambda(B) - \mathrm{rank}_\lambda((B)^\circ) + \mathrm{rank}_\lambda(A^\circ)$*, then* $(A/B)^\circ \neq \{0\}$.

Note: if $\lambda = p$ or $\lambda = T$, then $\mathrm{rank}_\lambda(B^\circ) \leq \mathrm{rank}_\lambda(A^\circ)$. In particular, the corollary yields that $(A/B)^\circ \neq \{0\}$ if $r^{(\lambda)} < \mathrm{rank}_\lambda(B)$ in these cases.

In the next lemma, we show that the constant

$$r^{(\lambda)} = \mathrm{rank}_\lambda(A) - \mathrm{rank}_\lambda(A/B),$$

$\lambda \in \Lambda$, often can be determined efficiently by consideration of some finite layers of L/K. We consider the case of $A/B = A^\#$, i.e. we divide out ideal classes generated by ramified primes. Recall the notion of $e(L/K)$ which has been introduced at the end of Section 2.

Lemma 3.8. *Suppose that L/K is a $\mathbb{Z}_p$-extension such that $A^{(L)}/(\lambda \cdot A^{(L)})$ is finite for some $\lambda \in \Lambda$. Let $r_n^{(\lambda)} = \mathrm{rank}_\lambda(A_n) - \mathrm{rank}_\lambda(A_n^\#)$, $n \in \mathbb{N}$. Then $r^{(\lambda)} = r_n^{(\lambda)}$ for each $n \geq e(L/K)$ such that $\mathrm{rank}_\lambda(A_n) = \mathrm{rank}_\lambda(A_{n+1})$. In other words, if $\mathrm{rank}_\lambda(A_n)$ stabilises at layer n, then also $\mathrm{rank}_\lambda(A_n^\#)$ stabilises.*

Proof. The norm maps induce homomorphisms

$$\overline{N}_{n+1,n} \colon D_{n+1}/(\lambda A_{n+1} \cap D_{n+1}) \longrightarrow D_n/(\lambda A_n \cap D_n)$$

for each $n \in \mathbb{N}$. Since $N_{n+1,n}(\lambda A_{n+1}) \subseteq \lambda A_n$, these maps are well-defined. For each $n \geq e(L/K)$, the extension L_{n+1}/L_n is ramified; therefore $\overline{N}_{n+1,n}$ is surjective for each such n. We will show that it is also injective if $\mathrm{rank}_\lambda(A_{n+1}) = \mathrm{rank}_\lambda(A_n)$. If $x \in D_{n+1}$ satisfies $\overline{N}_{n+1,n}(\bar{x}) = \bar{0}$, i.e. $N_{n+1,n}(x) \in \lambda A_n$, then there exists some $y \in A_{n+1}$ such that

$$N_{n+1,n}(x) = \lambda \cdot N_{n+1,n}(y) = N_{n+1,n}(\lambda \cdot y).$$

Moreover, the assumption that $\mathrm{rank}_\lambda(A_{n+1}) = \mathrm{rank}_\lambda(A_n)$ implies that the kernel of $N_{n+1,n}$ is contained in $\lambda \cdot A_{n+1}$. In other words,

$$x \equiv \lambda \cdot y \pmod{\ker(N_{n+1,n})}$$

implies that $x \in \lambda \cdot A_{n+1}$.

Since

$$|D_n/(\lambda A_n \cap D_n)| = p^{r_n^{(\lambda)}}$$

for each $n \in \mathbb{N}$ by Lemma 3.5 (ii), this shows that $r_n^{(\lambda)} = r_{n+1}^{(\lambda)}$ whenever $n \geq e(L/K)$ satisfies

$$\mathrm{rank}_\lambda(A_n) = \mathrm{rank}_\lambda(A_{n+1}).$$

The lemma now follows by induction. □

Now we consider the special case $\lambda = p$. Suppose that $\mathrm{rank}_p(A) < \infty$ (equivalently, $\mu(A) = 0$). Then Lemma 3.6 yields

$$\mathrm{rank}_p((A^{\#})^\circ) + r^{(p)} = \mathrm{rank}_p(A^\circ) + \mathrm{rank}_{\mathbb{Z}_p}(D). \tag{3.3}$$

Of course this special instance of Lemma 3.6 can be derived also more directly from the equality

$$\mathrm{rank}_{\mathbb{Z}_p}(A) = \mathrm{rank}_{\mathbb{Z}_p}(D) + \mathrm{rank}_{\mathbb{Z}_p}(A^{\#})$$

of $\mathbb{Z}_p$-modules, since $\mathrm{rank}_{\mathbb{Z}_p}(A) = \mathrm{rank}_p(A) - \mathrm{rank}_p(A^\circ)$.

Example 3.9. Let K be the number field defined by the polynomial $g = x^4 + 231$. We consider the cyclotomic $\mathbb{Z}_p$-extension L of K, $p = 3$. Since the ramification index of p in $K/\mathbb{Q}$ is equal to 4, we have $e(L/K) = 0$. A computation using PARI [26] yields $A^{(K)} \cong \mathbb{Z}/3\mathbb{Z}$, $A_1 \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $A_2 \cong \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. Moreover, $D_0 = D_1 = D_2 = \{0\}$. Since $\mathrm{rank}_3(A_1^{(L)}) = \mathrm{rank}_3(A_2^{(L)}) = 2$, we may conclude that $r^{(3)} = 0$ by Lemma 3.8. This implies that $D^{(L)} \subseteq 3 \cdot A^{(L)}$. Moreover, since K contains exactly one prime dividing $p = 3$, we know that $\mathrm{rank}_{\mathbb{Z}_3}(D^{(L)}) = 0$. Therefore $\mathrm{rank}_3((A^{\#})^\circ) = \mathrm{rank}_3(A^\circ)$ by (3.3).

For a $\mathbb{Z}_p$-extension L/K, $A = A^{(L)}$, we define

$$s = s(A) := \mathrm{rank}_{\mathbb{Z}_p}(A/(T \cdot A)).$$

Then there exist integers $N_0 \in \mathbb{N}$ and $c \in \mathbb{Z}$ such that

$$\mathrm{rank}_T(A_n) = s \cdot n + c$$

for each $n \geq N_0$, since the difference $v_p(|A_n/(T \cdot A_n)|) - v_p(|A/((T, p^n) \cdot A)|)$ is bounded uniformly in n. Similarly, we define $s^{\#} := \mathrm{rank}_{\mathbb{Z}_p}(A^{\#}/(T \cdot A^{\#}))$. If $L = K_\infty^{\mathrm{cyc}}$ is the cyclotomic $\mathbb{Z}_p$-extension of K, then the conjecture of Gross and Kuz'min predicts that $s^{\#} = 0$, i.e. that $A^{\#}/(T \cdot A^{\#})$ should be finite.

Lemma 3.10. *Let L/K be a $\mathbb{Z}_p$-extension such that $e(L/K) = 0$. Then*

$$s \geq \mathrm{rank}_{\mathbb{Z}_p}(D).$$

Proof. Since the primes generating $D^{(L_0)}$ are totally ramified in L by assumption, we have $|D^{(L_n)}| \leq |A_n^\Gamma| = |A_n/(T \cdot A_n)|$ for each $n \in \mathbb{N}$. Letting n tend to infinity, we obtain an inequality

$$\mathrm{rank}_{\mathbb{Z}_p}(D) \leq \mathrm{rank}_{\mathbb{Z}_p}(A^{\mathrm{Gal}(L/K)}) = \mathrm{rank}_{\mathbb{Z}_p}(A/(T \cdot A)) = s.$$

This proves the lemma. □

Remark 3.11. In [10], Greenberg introduced a topology on the set of $\mathbb{Z}_p$-extensions of K. An open neighbourhood U of L with respect to this topology typically consists of all $\mathbb{Z}_p$-extensions of K which coincide with L up to a fixed layer L_n, $n \in \mathbb{N}$. It follows from [16, Theorem 2.2] that $\mathrm{rank}_{\mathbb{Z}_p}(A^{(M)}/(T \cdot A^{(M)})) \leq s$ for all $M \in U$, provided that each prime of K ramifies in L and n is large enough. Therefore Lemma 3.10 yields a bound for each $\mathrm{rank}_{\mathbb{Z}_p}(D^{(M)})$ in this case. We refer to [15] for more information about the arithmetic of $\mathbb{Z}_p$-extensions with respect to Greenberg's topology.

In the next theorem, we will derive upper bounds for $\mathrm{rank}_p((A^\#)^\circ)$. We need an auxiliary result which generalises Lemma 3.3.

Lemma 3.12. *Let L/K be a $\mathbb{Z}_p$-extension. Then*

$$\mathrm{rank}_p(A^\circ) \leq \mathrm{rank}_p(\ker(i_{k,k+1}))$$

and

$$\mathrm{rank}_p((A^\#)^\circ) \leq \mathrm{rank}_p(\ker(i_{k,k+1}^\#))$$

for each sufficiently large $k \in \mathbb{N}$.

Proof. We concentrate on the module A°, and we use a similar argument as in the proof of [31, Proposition 13.28]. Let $A^\circ[p] \subseteq A^\circ$ denote the subgroup of elements of order at most p. Choose an $\mathbb{F}_p$-basis $b^{(1)}, \ldots, b^{(r)}$ of $A^\circ[p]$, where $r = \mathrm{rank}_p(A^\circ[p]) = \mathrm{rank}_p(A^\circ)$. We write $b^{(i)} = (b_n^{(i)})_n \in A = \varprojlim A_n$. Let γ be a topological generator of $\mathrm{Gal}(L/K) \cong \mathbb{Z}_p$, and choose $k \in \mathbb{N}$ large enough to ensure that

- γ^{p^k} acts trivially on $A^\circ[p]$, and
- $\langle b_k^{(i)} \rangle_{1 \leq i \leq r}$ is a subgroup of A_k of rank r.

Then

$$(1 + \gamma^{p^k} + \gamma^{2p^k} + \cdots + \gamma^{(p-1)p^k}) \cdot b_{k+1}^{(i)} = p \cdot b_{k+1}^{(i)} = 0$$

for each $i \in \{1, \ldots, r\}$. On the other hand, the element on the left hand side is equal to

$$i_{k,k+1}(N_{k+1,k}(b_{k+1}^{(i)})) = i_{k,k+1}(b_k^{(i)}).$$

This shows that $\mathrm{rank}_p(\ker(i_{k,k+1})) \geq \mathrm{rank}_p(\langle b_k^{(i)} \rangle_{1 \leq i \leq r}) = r$. □

Theorem 3.13. *Let L/K be a $\mathbb{Z}_p$-extension such that each prime of K above p ramifies in L and $e(L/K) = 0$. Choose $k \in \mathbb{N}$ large enough to make both statements of Lemma 3.12 hold. We define*

$$N_k = v_p([(E_k \cap N_{k+1,k}(L_{k+1}^*)) : N_{k+1,k}(E_{k+1})])$$

and

$$N_k^\# := v_p([(E_k^S \cap N_{k+1,k}(L_{k+1}^*)) : N_{k+1,k}(E_{k+1}^S)]).$$

Then

$$\mathrm{rank}_p((A^\#)^\circ) + s^\# \leq N_k^\#.$$

If moreover $\mu(A) = 0$, then also

$$\mathrm{rank}_p((A^\#)^\circ) \leq N_k.$$

Proof. It follows from Chevalley's Theorem 3.1 (ii) and Lemma 3.2 that

$$|(A_{k+1}^\#)^{\mathrm{Gal}(L_{k+1}/L_k)}| = \frac{|A_k^\#| \cdot p^{j_k - 1}}{[E_k^S : N_{k+1,k}(E_{k+1}^S)]} \cdot p^{N_k^\#} = |A_k^\#| \cdot \frac{p^{N_k^\#}}{|\ker(i_{k,k+1}^\#)|},$$

where j_k denotes the number of primes of L_k above p. Since

$$\frac{|(A_{k+1}^\#)^{\mathrm{Gal}(L_{k+1}/L_k)}|}{|A_k^\#|} \geq p^{s^\#}$$

for each $k \in \mathbb{N}$ (see [16, Theorem 2.2]), the first statement of the theorem follows from Lemma 3.12.

Now suppose that $\mu(A) = 0$. Then Theorem 3.1 (i) implies that

$$|A_{k+1}^{\mathrm{Gal}(L_{k+1}/L_k)}| = \frac{|A_k| \cdot p^{j_k - 1}}{[E_k : N_{k+1,k}(E_{k+1})]} \cdot p^{N_k}.$$

Moreover, Lemma 3.2 and Lemma 3.5 (iii) imply that

$$\begin{aligned} v_p([E_k : N_{k+1,k}(E_{k+1})]) &= s_{k+1,k} - 1 + v_p(|\ker(i_{k,k+1})|) \\ &= j_k - r_{k+1}^{(p)} - 1 + v_p(|\ker(i_{k,k+1})|). \end{aligned}$$

Therefore

$$|A_{k+1}^{\mathrm{Gal}(L_{k+1}/L_k)}| = \frac{|A_k| \cdot p^{r_{k+1}^{(p)}}}{|\ker(i_{k,k+1})|} \cdot p^{N_k}. \tag{3.4}$$

It follows from Lemma 3.5 (ii) and from the proof of Lemma 3.8 that

$$r_{k+1}^{(p)} \leq \mathrm{rank}_p(A) - \mathrm{rank}_p(A^\#). \tag{3.5}$$

By [16, Theorem 2.2], we have

$$v_p(|A_{k+1}^{\mathrm{Gal}(L_{k+1}/L_k)}|) - v_p(|A_k|) \geq s \tag{3.6}$$

for every $k \in \mathbb{N}$. We may conclude that for sufficiently large k,

$$\begin{aligned}\operatorname{rank}_p(A^\circ) + s &\overset{3.12}{\leq} \operatorname{rank}_p(\ker(i_{k,k+1})) + s \\ &\overset{(3.6)}{\leq} \operatorname{rank}_p(\ker(i_{k,k+1})) + v_p(|A_{k+1}^{\mathrm{Gal}(L_{k+1}/L_k)}|) - v_p(|A_k|) \\ &\overset{(3.4)}{=} N_k + r_{k+1}^{(p)} \\ &\overset{(3.5)}{\leq} N_k + \operatorname{rank}_p(A) - \operatorname{rank}_p(A^{\#}).\end{aligned}$$

In view of (3.3) and Lemma 3.10, we obtain

$$s + \operatorname{rank}_p((A^{\#})^\circ) \leq N_k + \operatorname{rank}_{\mathbb{Z}_p}(D) \leq N_k + s,$$

and therefore $\operatorname{rank}_p((A^{\#})^\circ) \leq N_k$, as claimed. □

3.3. Non-trivial finite torsion submodules. In this subsection, we prove Theorem 1.1 from the Introduction. The following approach for proving the non-triviality of A° for a $\mathbb{Z}_p$-extension L of K is based on a simple idea: if

$$\operatorname{rank}_{\mathbb{Z}_p}(D^{(L)}) < \operatorname{rank}_p(D^{(L)}),$$

then actually $(D^{(L)})^\circ \neq \{0\}$. The next result can be used for bounding $\operatorname{rank}_{\mathbb{Z}_p}(D^{(L)})$ from the above by computation of only finitely many layers of L. Moreover, it is possible to make completely explicit how many layers have to be computed.

Theorem 3.14. *Let L/K be a $\mathbb{Z}_p$-extension satisfying $e(L/K) = 0$. We write $A = A^{(L)}$, $A^{\#} = (A^{\#})^{(L)}$ and $D = D^{(L)} = \varprojlim D_n$ for brevity.*

(a) *If $A^{\#} = (A^{\#})^\circ$ is finite, then*

$$\operatorname{rank}_{\mathbb{Z}_p}(D) \leq v_p(|D_{n+1}|) - v_p(|D_n|)$$

for each n such that $|A_n^{\#}| = |A_{n+1}^{\#}|$.

(b) *If $(A^{\#})^\circ = \{0\}$, then*

$$\operatorname{rank}_{\mathbb{Z}_p}(D) \leq v_p(|D_{n+1}|) - v_p(|D_n|)$$

for every $n \in \mathbb{N}$.

(c) *Let $\nu_{n,0}(T) := \frac{(T+1)^{p^n}-1}{T}$ for each $n \in \mathbb{N}$. If*

$$\nu_{k,0}(T) \cdot A^\circ = \{0\} = \nu_{k,0}(T) \cdot (A^{\#})^\circ \tag{3.7}$$

for some $k \in \mathbb{N}$, then

$$\operatorname{rank}_{\mathbb{Z}_p}(D) \leq v_p(|D_{n+1}|) - v_p(|D_n|)$$

for every $n \geq k$.

In fact, if n is as in (a), (b) *or* (c), *then*

$$v_p(|D_{m+1}|) - v_p(|D_m|) \leq v_p(|D_{n+1}|) - v_p(|D_n|)$$

for every $m \geq n$. If $|D_{n+1}| = |D_n|$ for any such n, then $|D| = |D_n|$.

Proof. For any Λ-submodule $B = \varprojlim B_n$ of $A = \varprojlim A_n$ and each $n \in \mathbb{N}$ we denote by $Y_n^{(B)}$ the kernel of the canonical map $\mathrm{pr}_n \colon B \longrightarrow B_n$. As $e(L/K) = 0$, $Y_{n+1}^{(A)} = \nu_{n+1,n}(T) \cdot Y_n^{(A)}$ for each $n \in \mathbb{N}$, where

$$\nu_{n+1,n}(T) = \frac{(T+1)^{p^{n+1}} - 1}{(T+1)^{p^n} - 1} \in \mathbb{Z}_p[T],$$

$n \in \mathbb{N}$ (cf. [31, Theorem 13.15]). In particular, if $\nu_{n,0}(T) = \frac{(T+1)^{p^n}-1}{T}$ is defined as in assertion (c), then $\nu_{n,0}(T) = \prod_{i=1}^n \nu_{i,i-1}(T)$ and

$$Y_n^{(A)} = \nu_{n,0}(T) \cdot Y_0^{(A)}.$$

We will investigate whether also $Y_{n+1}^{(D)} = \nu_{n+1,n}(T) \cdot Y_n^{(D)}$ for all sufficiently large n. Note: since $T \cdot D = \{0\}$ because $e(L/K) = 0$, we have $\nu_{n+1,n}(T) \cdot Y_n^{(D)} = p \cdot Y_n^{(D)}$ for each n. In other words, we study whether

$$Y_{n+1}^{(D)} = p \cdot Y_n^{(D)} \tag{3.8}$$

for each sufficiently large n. It is obvious (and in fact true for each submodule D of A) that

$$\nu_{n+1,n}(T) \cdot (Y_n^{(A)} \cap D) \subseteq \nu_{n+1,n}(T) \cdot Y_n^{(A)} \cap D = Y_{n+1}^{(A)} \cap D = Y_{n+1}^{(D)}.$$

In order to deal with the reverse inclusion, we consider the three cases separately, starting with

Case (a): $A^{\#} = (A^{\#})^{\circ}$ is finite.
This means that we can choose $k \in \mathbb{N}$ such that $|A_k^{\#}| = |A_{k+1}^{\#}| (= |A^{\#}|)$. Then

$$Y_k^{(A)} + D = Y_{k+1}^{(A)} + D = \nu_{k+1,k}(T) \cdot Y_k^{(A)} + D,$$

and Nakayama's Lemma implies that $Y_k^{(A)} \subseteq D$. Therefore $Y_n^{(A)} \subseteq D$ (and thus $Y_n^{(D)} = Y_n^{(A)}$) for each $n \geq k$, and (3.8) holds for each $n \geq k$. This means that

$$v_p(|D_{n+1}|) - v_p(|D_n|) = v_p(|Y_n^{(D)}/(p \cdot Y_n^{(D)})|)$$

for every $n \geq k$, and similarly

$$v_p(|D_{n+j+1}|) - v_p(|D_{n+j}|) = v_p(|(p^j \cdot Y_n^{(D)})/(p^{j+1} \cdot Y_n^{(D)})|)$$

for each $j \in \mathbb{N}$. Therefore $v_p(|D_{n+r}|) - v_p(|D_n|) \leq r \cdot (v_p(|D_{n+1}|) - v_p(|D_n|))$ for every $r \in \mathbb{N}$ and $n \geq k$. This proves the assertion of the theorem in this case.

Case (b): $(A^{\#})^\circ = \{0\}$.
Suppose that $x = \nu_{n+1,n}(T) \cdot y \in D$ for some $y \in Y_n^{(A)}$. We want to show that $y \in D$. Since $(A^{\#})^\circ = \{0\}$, it follows that $A^{\#}$ can be embedded into its elementary Λ-module, and therefore multiplication by $\nu_{n+1,n}(T)$ is injective on $A^{\#}$, since $\nu_{n+1,n}(T)$ is coprime with the characteristic polynomial of $A^{\#}$ (which divides the characteristic polynomial of A) by the proof of [28, Proposition 2.1]. Therefore (3.8) follows, and we may proceed as above.

Case (c): $\nu_{k,0}(T) \cdot A^\circ = \{0\} = \nu_{k,0}(T) \cdot (A^{\#})^\circ$.
We want to show first that the cardinality of

$$Z_n := (\nu_{n,0}(T) \cdot Y_0^{(A)} \cap D)/\nu_{n,0}(T) \cdot (Y_0^{(A)} \cap D)$$

stabilises for $n \geq k$. Indeed, letting $Y^{\#} = Y_0^{(A)}/(D \cap Y_0^{(A)}) \subseteq A^{\#}$, we have an exact sequence

$$0 \longrightarrow Y_0^{(A)}[\nu_{n,0}(T)]/(D \cap Y_0^{(A)}[\nu_{n,0}(T)]) \longrightarrow Y^{\#}[\nu_{n,0}(T)] \xrightarrow{\alpha} Z_n \longrightarrow 0$$

for every $n \in \mathbb{N}$, where α maps a coset $\bar{y} \in Y^{\#}[\nu_{n,0}(T)]$ to the coset of $\nu_{n,0}(T) \cdot y$ in Z_n (this does not depend on the choice of $y \in \bar{y}$).

As in the above special case (b), multiplication by $\nu_{n,0}(T)$ is injective on the elementary Λ-module attached to $Y^{\#} \subseteq A^{\#}$, and therefore $Y^{\#}[\nu_{n,0}(T)] \subseteq (Y^{\#})^\circ$. On the other hand, $(Y^{\#})^\circ \subseteq (A^{\#})^\circ$ is annihilated by $\nu_{n,0}(T)$ for every $n \geq k$ (by assumption), and therefore

$$Y^{\#}[\nu_{n,0}(T)] = (Y^{\#})^\circ$$

for each $n \geq k$.

Now we study the kernel of α. Again, since multiplication by $\nu_{n,0}(T)$ is injective on the elementary Λ-module attached to $Y_0^{(A)} \subseteq A$, the kernel of multiplication by $\nu_{n,0}(T)$ is contained in $(Y_0^{(A)})^\circ$. In fact,

$$(Y_0^{(A)})^\circ = Y_0^{(A)}[\nu_{n,0}(T)]$$

because by our assumptions, $(Y_0^{(A)})^\circ \subseteq A^\circ$ is also annihilated by $\nu_{n,0}(T)$ if $n \geq k$. It follows that $\ker(\alpha) = (Y_0^{(A)})^\circ/(D \cap (Y_0^{(A)})^\circ)$ for each $n \geq k$.

We have therefore shown that there exists some $X \in \mathbb{N}$ such that $v_p(|Z_n|) = X$ for every $n \geq k$. Note that

$$Z_n = (Y_n^{(A)} \cap D)/\nu_{n,0}(T) \cdot (Y_0^{(A)} \cap D) = Y_n^{(D)}/\nu_{n,0}(T) \cdot Y_0^{(D)}.$$

Since $T \cdot D = \{0\}$, we can write this as

$$Z_n = Y_n^{(D)}/p^n \cdot Y_0^{(D)}.$$

We have shown that

$$v_p(|D_n|) - v_p(|D_0|) = v_p(|Y_0^{(D)}/Y_n^{(D)}|) = v_p(|Y_0^{(D)}/p^n Y_0^{(D)}|) - X$$

for every $n \geq k$. Therefore

$$\begin{aligned} v_p(|D_{k+j+1}|) - v_p(|D_{k+j}|) &= v_p(|p^{k+j} Y_0^{(D)} / p^{k+j+1} Y_0^{(D)}|) \\ &\leq v_p(|p^k Y_0^{(D)} / p^{k+1} Y_0^{(D)}|) \end{aligned}$$

for every $j \in \mathbb{N}$. In particular,

$$\operatorname{rank}_{\mathbb{Z}_p}(D) \leq v_p(|D_{n+1}|) - v_p(|D_n|)$$

for every $n \geq k$.

Finally, the last assertion of the theorem concerns a special case: if $|D_{n+1}| = |D_n|$ in the above setting, then $|D_{n+r}| = |D_n|$ for every $r \in \mathbb{N}$. □

Example 3.15. Let $K = \mathbb{Q}(\zeta_{11})$, $p = 3$. Then p is inert in the maximal real subfield K^+ of K and splits into two primes in K/K^+. Let L be the cyclotomic $\mathbb{Z}_3$-extension of K. Then $\mu(A) = 0$ by the Theorem of Ferrero-Washington, because $K/\mathbb{Q}$ is abelian. Since $A^{(K^+)} = \{0\}$, we know from Remark 3.4 that $(A^{(L)})^\circ = \{0\}$ and $((A^\#)^{(L)})^\circ = \{0\}$. Since $A_1^{(L)} = D_1^{(L)} = \mathbb{Z}/3\mathbb{Z}$, Theorem 3.14 implies that $\operatorname{rank}_{\mathbb{Z}_p}(D^{(L)}) \leq 1$.

Note that $(A^\#)^{(L)} = \{0\}$, because $(A_0^\#)^{(L)} = (A_1^\#)^{(L)} = \{0\}$. But $A^{(L)} \neq \{0\}$, and formula (3.3) implies that $\operatorname{rank}_{\mathbb{Z}_p}(D^{(L)}) = 1$. It follows that $\operatorname{rank}_p(A^{(L)}) = 1$ and $\operatorname{rank}_{\mathbb{Z}_p}(A^{(L)}/(T \cdot A^{(L)})) = 1$, i.e. $A^{(L)} \cong \Lambda/(T)$ as Λ-modules.

Example 3.16. Consider the number field K which is defined by the polynomial $x^3 + 36x^2 + 122x + 42$. Then K is totally real, and the prime $p = 3$ is totally split in $K/\mathbb{Q}$. Using PARI, we computed that $A^{(K)} \cong \mathbb{Z}/3\mathbb{Z}$, $(A^\#)^{(K)} = \{0\} = (A_1^\#)^{(L)}$, and $A_1^{(L)} \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ for the cyclotomic $\mathbb{Z}_3$-extension L of K.

Therefore $(A^\#)^{(L)} = \{0\}$ by [15, Theorem 2.5 and Remark 3.14], and thus $A^{(L)} = D^{(L)}$. Theorem 3.14 implies that $\lambda(A^{(L)}) = \operatorname{rank}_{\mathbb{Z}_3}(D^{(L)}) \leq 2$.

Note: since $p = 3$ is totally split in $K/\mathbb{Q}$, the composite $\mathbb{K}$ of all $\mathbb{Z}_3$-extensions of K is unramified over L, and therefore

$$\operatorname{rank}_{\mathbb{Z}_3}(A^{(L)}/(T \cdot A^{(L)})) = \delta(K)$$

equals the Leopoldt defect of K, as K is totally real. Since $T \cdot D^{(L)} = \{0\}$, we actually have $\operatorname{rank}_{\mathbb{Z}_3}(A^{(L)}/(T \cdot A^{(L)})) = \operatorname{rank}_{\mathbb{Z}_3}(D^{(L)}) = \lambda(A^{(L)})$. This shows that Theorem 3.14 can be used in order to bound the Leopoldt defect of a number field K.

Remark 3.17.

(1) If $\mu(A) = 0$, then Iwasawa's class number formula (2.1) implies that

$$\operatorname{rank}_{\mathbb{Z}_p}(D) \leq \lambda(A) = v_p(|A_{n+1}|) - v_p(|A_n|)$$

for each sufficiently large n. Using the property (3.8) of D, one can deduce an Iwasawa-type asymptotic formula for the orders $|D_n|$ for sufficiently large n; $\operatorname{rank}_{\mathbb{Z}_p}(D)$ then corresponds to $\lambda(D)$. Note that the statement of Theorem 3.14 gives more information because it includes an explicit description of what "sufficiently large" means in this context. An analogous concrete bound for the Iwasawa module A is not known in general.

(2) We are really using $T \cdot D = \{0\}$ here; for general Iwasawa modules, the same approach only yields only bounds for the growth of $\operatorname{rank}_T(A_n)$. We also remark that $v_p(|D_{n+1}|) - v_p(|D_n|)$ will often be smaller than $v_p(|A_{n+1}|) - v_p(|A_n|)$.

Note: in case (a) of the theorem we automatically have $\mu(A) = 0$, because D is a finitely generated $\mathbb{Z}_p$-module. In cases (b) and (c) we do not presume that $\mu(A) = 0$.

(3) It follows from [28, Corollary 2.5] that $\mu(A) = 0$ and

$$\lambda(A) \leq v_p(|A_{n+1}|) - v_p(|A_n|)$$

if the right hand side is smaller than $p^{n+1} - p^n$. If $|A^{\#}_{n+1}| = |A^{\#}_n|$, then $v_p(|D_{n+1}|) - v_p(|D_n|) = v_p(|A_{n+1}|) - v_p(|A_n|)$. Using Theorem 3.14, we obtain a bound on $\lambda(A) = \operatorname{rank}_{\mathbb{Z}_p}(D)$ even if this difference is greater than or equal to $p^{n+1} - p^n$ (note that this is indeed the case in Example 3.16). Also the case of $(A^{\#})^\circ = \{0\}$ is interesting, since $v_p(|D_{n+1}|) - v_p(|D_n|)$ can be much smaller than $v_p(|A_{n+1}|) - v_p(|A_n|)$.

(4) We can generalise condition (a) from Theorem 3.14: if $A^{\#}/(\lambda \cdot A^{\#})$ is finite for some $\lambda \in \Lambda$, and if $\lambda A \cap D = \lambda D$, then we obtain an equation (3.8) for the module $D/(\lambda \cdot D)$. In particular, if

$$\operatorname{rank}_\lambda(A^{\#}_{n+1}) = \operatorname{rank}_\lambda(A^{\#}_n)$$

for some n in this case, and if $\operatorname{rank}_\lambda(D_m) = \operatorname{rank}_\lambda(D_{m+1})$ for some $m \geq n$, then $\operatorname{rank}_\lambda(D) = \operatorname{rank}_\lambda(D_m)$. In other words: if two consecutive ranks of the $A^{\#}_n$ and the D_n coincide, then also the ranks of the A_n stabilise; this is kind of a converse of Lemma 3.8.

Proof of Theorem 1.1. First note that both parts of condition (3.7) are automatically satisfied as soon as $|A^\circ| \leq p^k$ and $|(A^{\#})^\circ| \leq p^k$. Therefore

$$v_p(|D_{m+1}|) - v_p(|D_m|) \leq v_p(|D_{k+1}|) - v_p(|D_k|)$$

for every $m \geq k$; we obtain the first part of Theorem 1.1.

Now suppose that $|(A^{\#})^\circ| \leq p^k$. For every coset in $(A^{\#})^\circ$, we choose a representative in A under the canonical map $\pi \colon A \twoheadrightarrow A^{\#}$, and we let

$$\widetilde{A} := A/(D + \pi^{-1}((A^{\#})^\circ)).$$

Note that the two Λ-modules D and $\widetilde{D} := D + \pi^{-1}((A^{\#})^{\circ})$ have the same finite $\mathbb{Z}_p$-rank. Since $\widetilde{A}^{\circ} = \{0\}$ by construction, the proof of Theorem 3.14 (b) implies that $Y_{n+1}^{(\tilde{D})} = \nu_{n+1,n}(T) \cdot Y_n^{(\tilde{D})}$, $n \in \mathbb{N}$, holds for the submodule $\widetilde{D} \subseteq A$.

Since $\nu_{k,0}(T) \cdot (A^{\#})^{\circ} = \{0\}$ by assumption, $\nu_{k,0}(T) \cdot \widetilde{D} \subseteq D$. Therefore

$$Y_{k+1}^{(\tilde{D})} = \nu_{k+1,0}(T) \cdot Y_0^{(\tilde{D})} = \nu_{k+1,k}(T) \cdot \nu_{k,0}(T) \cdot Y_0^{(\tilde{D})} \subseteq p \cdot D$$

since $T \cdot D = \{0\}$. As $D \subseteq \widetilde{D}$, we may conclude that $Y_{k+1}^{(D)} \subseteq Y_{k+1}^{(\tilde{D})}$ is contained in $p \cdot D$, and therefore

$$\mathrm{rank}_p(D_{k+1}) = v_p(|D/(Y_{k+1}^{(D)} + p \cdot D)|) = v_p(|D/(p \cdot D))|) = \mathrm{rank}_p(D),$$

i.e. $\mathrm{rank}_p(D_n) = \mathrm{rank}_p(D_{k+1})$ for every $n \geq k+1$. □

Example 3.18. In order to illustrate the above results, we choose $p = 2$ and we consider two sets of each 20000 number fields with discriminant as small as possible and of signatures [3,0] and [1,1], respectively. These families, ordered by discriminant, have been obtained from the LMFDB database [18]. All the computations have been done using PARI [26].

In all what follows, we consider the cyclotomic $\mathbb{Z}_p$-extensions L of the corresponding number fields K. First we search for examples L/K such that

$$v_p(|D_2|) - v_p(|D_1|) > v_p(|D_1|) - v_p(|D_0|)$$

or

$$\mathrm{rank}_p(D_2) > \mathrm{rank}_p(D_1)$$

(i.e. satisfying one of the two conditions (a) and (b) for $n = 0$ in Theorem 1.1). In these cases the theorem implies that $|A^{\circ}| \cdot |(A^{\#})^{\circ}| \geq 2$, respectively $|(A^{\#})^{\circ}| \geq 2$. We found around 900 such examples in the list of number fields with signature [1,1], and around 200 totally real examples. Note that in both cases there exist number fields for which exactly one of the two conditions (a) and (b) is satisfied, although the majority of examples (more than 90 %) satisfies both conditions.

Moreover, looking for a field which satisfies one of the above conditions for $n = 1$ yields 94 examples among the first 4000 cubic extensions in the above signature [1,1] list. Theorem 1.1 implies that $|A^{\circ}| \geq 4$ or $|(A^{\#})^{\circ}| \geq 4$ in each of these examples.

Finally, we searched for number fields verifying one of the conditions for $p = 3$ (and $n = 0$). To this purpose, we took from [18] a list of 1000 real cubic number fields with small discriminant (up to 23612), obtaining 18 examples (here the two criteria gave exactly the same matches). Note that Theorem 1.1 (b) implies that $|(A^{\#})^{\circ}| \geq 3$ in each of these cases. Interestingly, in 10 of the 18 examples, the number field K contains exactly one prime above $p = 3$ – in the examples for $p = 2$ computed before, we have not found a single number field containing only one prime above $p = 2$ which verified one of the conditions.

Let us state one further

Theorem 3.19. *Let L/K be a $\mathbb{Z}_p$-extension satisfying $e(L/K) = 0$. We assume that* $\operatorname{rank}_p(A_1) = \operatorname{rank}_p(A_0)$*. Then*

$$\operatorname{rank}_p((A^{\#})^\circ) \geq \operatorname{rank}_p(D) - \operatorname{rank}_p(D_0).$$

Proof. Lemma 3.6 implies that

$$\operatorname{rank}_p((A^{\#})^\circ) \geq \operatorname{rank}_p(D) - \operatorname{rank}_p(A) + \operatorname{rank}_p(A^{\#}).$$

In view of Lemma 3.5 (ii), we can write

$$\operatorname{rank}_p(A) - \operatorname{rank}_p(A^{\#}) = v_p(|D/(p \cdot A \cap D)|).$$

On the other hand, $\operatorname{rank}_p(D) - \operatorname{rank}_p(D_0) = v_p(|(Y_0^{(D)} + p \cdot D)/(p \cdot D)|)$. Since $\operatorname{rank}_p(A_1) = \operatorname{rank}_p(A_0)$ by assumption, the canonical map

$$\mathrm{pr}_0 \colon A \longrightarrow A_0$$

induces an isomorphism

$$A/(p \cdot A) \xrightarrow{\sim} A_0/(p \cdot A_0).$$

Therefore $Y_0^{(D)} \subseteq D \cap p \cdot A$. Summarising,

$$\begin{aligned} \operatorname{rank}_p(D) - \operatorname{rank}_p(D_0) &\leq v_p(|(p \cdot A \cap D)/(p \cdot D)|) \\ &= v_p(|D/(p \cdot D)|) - v_p(|D/(p \cdot A \cap D)|) \\ &\leq \operatorname{rank}_p((A^{\#})^\circ). \end{aligned}$$

□

Remark 3.20. Ozaki has shown in [25] that for any finite Λ-module M, there exists a suitable totally real number field K such that

$$A^{(L)} = (A^{(L)})^\circ \cong M,$$

where L denotes the cyclotomic $\mathbb{Z}_p$-extension of K. It seems not known whether something similar is true also for $A^{\#}$.

4. Pseudo-null submodules of $\mathbb{Z}_p^k$-extensions

In this section, we will prove results concerning the non-triviality of the maximal pseudo-null submodule of the Iwasawa module attached to suitable $\mathbb{Z}_p^k$-extensions $\mathbb{L}/K$. We will also explain that the statement $(A^{(\mathbb{L})})^\circ \neq \{0\}$ sometimes can be used in order to deduce that in fact $A^{(\mathbb{L})} = (A^{(\mathbb{L})})^\circ$ is pseudo-null. In view of a result of Minardi (see [20, Proposition 4.B]), this can imply (GGC) for K.

First we discuss a characterisation of the maximal pseudo-null submodule of an Iwasawa module A which depends on the projective dimension of A.

Lemma 4.1. *Let $1 \leq k \in \mathbb{N}$, and let A be an Iwasawa-Λ_k-module.*

(i) *If $k = 1$, then $A^\circ = \{0\}$ if and only if $\mathrm{pd}_{\Lambda_k}(A) \leq 1$.*

(ii) *If $k > 1$, then $\mathrm{pd}_{\Lambda_k}(A) \leq 1$ implies that $A^\circ = \{0\}$. The reverse statement, however, is not true in general.*

Proof. The statement for $k = 1$ is well-known (see [21, Proposition 5.3.19]). Suppose now that $k > 1$ and that $A^\circ \neq \{0\}$. Then there exists an element $0 \neq x \in A$ such that the height of the ideal $\mathrm{Ann}(x) \subseteq \Lambda_k$ annihilating x is at least two. But then

$$\mathrm{depth}_{\Lambda_k}(A) \leq \dim(\Lambda_k/\mathrm{Ann}(x)) \leq \dim(\Lambda_k) - 2 = k + 1 - 2 = k - 1$$

and therefore $\mathrm{pd}_{\Lambda_k}(A) \geq 2$ by the Auslander–Buchsbaum Theorem.

The following example shows that the reverse conclusion does not hold in general. Suppose that $k = 2$, and let $A = (T_1, T_2, p)/(T_1)$. Then $A \subseteq \Lambda_2/(T_1)$ does not contain any non-trivial pseudo-null Λ_2-submodules. We will compute the depth of A. Since multiplication by T_2 is injective on A,

$$\mathrm{depth}_{\Lambda_2}(A) = 1 + \mathrm{depth}_{\Lambda_1}(A/(T_2 \cdot A)),$$

where we let $\Lambda_1 = \mathbb{Z}_p[\![T_1]\!] \cong \Lambda_2/(T_2)$. Now

$$A/(T_2 \cdot A) = (T_1, T_2, p)/(T_1, T_2^2, T_2 p)$$

contains the pseudo-null $\mathbb{Z}_p[\![T_2]\!]$-submodule

$$(T_1, T_2)/(T_1, T_2^2, T_2 p) \cong \mathbb{Z}_p[\![T_2]\!]/(T_2, p).$$

Therefore $\mathrm{pd}_{\Lambda_1}(A/(T_2 \cdot A)) = 2$ and $\mathrm{depth}_{\Lambda_2}(A) = 1 + 0 = 1$. This proves that $\mathrm{pd}_{\Lambda_2}(A) = 2$. □

The starting point of our investigations concerning the non-triviality of A° is the following result due to Fujii.

Theorem 4.2 (Fujii)**.** *Let K be a number field, let L denote the cyclotomic $\mathbb{Z}_p$-extension of K, and let $M \neq L$ denote a $\mathbb{Z}_p$-extension of K such that each prime of K dividing p ramifies in M. We assume that either K contains exactly one prime above p, and $e(L/K) = 0$, or that p is totally split in K. Let $\mathbb{L} := L \cdot M$, so that $\mathbb{L}/K$ is a $\mathbb{Z}_p^2$-extension. Let $T_1 = \gamma_1 - 1$ for some generator γ_1 of $\mathrm{Gal}(\mathbb{L}/M) \cong \mathbb{Z}_p$.*

If $(A^L)^\circ = \{0\}$ and $(A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})}))^\circ \neq \{0\}$, then $A^{(\mathbb{L})}$ contains a non-trivial pseudo-null $\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}/K)]\!]$-submodule.

Proof. See [3, Proposition 2.1 and Corollary 2.1]. □

We generalise this result to $\mathbb{Z}_p^k$-extensions $\mathbb{L}/K$, $k \geq 2$ arbitrary. Moreover, we consider more general number fields K, and we will not be limited to $\mathbb{Z}_p$-extensions of K in which all the primes of K dividing p ramify.

Theorem 4.3. *Let K be an arbitrary number field, let L and M denote two different $\mathbb{Z}_p^{k-1}$-extensions of K such that $\mathbb{L} := L \cdot M$ is a $\mathbb{Z}_p^k$-extension of K. Let γ_1 and γ_2 denote generators of* $\mathrm{Gal}(\mathbb{L}/M)$ *and* $\mathrm{Gal}(\mathbb{L}/L)$*, and write $T_1 = \gamma_1 - 1$ and $T_2 = \gamma_2 - 1$. Suppose that*

(i) *$A^{(\mathbb{L})}/(T_2 \cdot A^{(\mathbb{L})})$ is a torsion $\mathbb{Z}_p[\![\mathrm{Gal}(L/K)]\!] \cong \mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}/K)]\!]/(T_2)$-module such that*

$$\mathrm{pd}_{\mathbb{Z}_p[\![\mathrm{Gal}(L/K)]\!]}(A^{(\mathbb{L})}/(T_2 \cdot A^{(\mathbb{L})})) \le 1$$

and that

(ii) *the kernel $(A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})}))[T_2]$ of multiplication by T_2 contains a non-trivial torsion $\mathbb{Z}_p[\![\mathrm{Gal}((L \cap M)/K)]\!]$-submodule, and only finitely many primes of M ramify in $\mathbb{L}/M$.*

Then $(A^{(\mathbb{L})})^\circ \neq \{0\}$. In fact, $(A^{(\mathbb{L})})^\circ[T_2]$ is non-trivial.

Remark 4.4. In view of Lemma 4.1 (i), Theorem 4.2 of Fujii is a special case of Theorem 4.3. Indeed, the hypotheses in Theorem 4.2 imply that we have an injection

$$A^{(\mathbb{L})}/(T_2 \cdot A^{(\mathbb{L})}) \hookrightarrow A^{(L)}, \tag{4.1}$$

see Lemma 4.6 below; therefore $(A^{(\mathbb{L})}/(T_2 \cdot A^{(\mathbb{L})}))^\circ \subseteq (A^{(L)})^\circ = \{0\}$. Moreover, hypothesis (ii) from Theorem 4.3 is satisfied in view of Lemma 4.7.

Proof of Theorem 4.3. First note that $A^{(\mathbb{L})} \neq \{0\}$ by (ii). Let

$$\Lambda_k := \mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}/K)]\!],$$

and let E denote an elementary torsion Λ_k-module attached to $A^{(\mathbb{L})}$. Fix a pseudo-isomorphism $\varphi : A^{(\mathbb{L})} \longrightarrow E$.

Let $\Lambda_{k-1}^{(1)} := \mathbb{Z}_p[\![\mathrm{Gal}(L/K)]\!] = \mathbb{Z}_p[\![T_1, T_3, \ldots, T_k]\!]$. Since $A^{(\mathbb{L})}/(T_2 \cdot A^{(\mathbb{L})})$ is a torsion $\Lambda_{k-1}^{(1)}$-module by (i), it follows that T_2 does not divide the characteristic power series $F_{A^{(\mathbb{L})}} \in \Lambda_k$. Now suppose that $A^{(\mathbb{L})}[T_2]$ does *not* contain any non-trivial pseudo-null Λ_k-submodules. Then $\varphi|_{A^{(\mathbb{L})}[T_2]}$ is in fact injective, and it follows that multiplication by T_2 is injective on $A^{(\mathbb{L})}$.

On the other hand, the hypothesis $\mathrm{pd}_{\Lambda_{k-1}^{(1)}}(A^{(\mathbb{L})}/(T_2 \cdot A^{(\mathbb{L})})) = 1$ implies that the depth over $\Lambda_{k-1}^{(1)}$ of $A^{(\mathbb{L})}/(T_2 \cdot A^{(\mathbb{L})})$ is $k-1$. This means that $\mathrm{depth}_{\Lambda_k}(A^{(\mathbb{L})}) = k$, and therefore $\mathrm{pd}_{\Lambda_k}(A^{(\mathbb{L})}) = 1$ by the Auslander–Buchsbaum Theorem.

It follows that there exists an exact sequence

$$0 \longrightarrow \Lambda_k^{\oplus r} \longrightarrow \Lambda_k^{\oplus r} \longrightarrow A^{(\mathbb{L})} \longrightarrow 0. \tag{4.2}$$

Here we note that each projective Λ_k-module is in fact free (cf. [21, Corollary 5.2.20]); the two free modules in the above sequence have the same rank because $A^{(\mathbb{L})}$ is Λ_k-torsion.

Taking $\mathrm{Gal}(\mathbb{L}/M)$-invariants and -coinvariants yields an exact sequence

$$0 \longrightarrow (A^{(\mathbb{L})})^{\mathrm{Gal}(\mathbb{L}/M)} \longrightarrow (\Lambda_{k-1}^{(2)})^{\oplus r} \longrightarrow (\Lambda_{k-1}^{(2)})^{\oplus r} \longrightarrow A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})}) \longrightarrow 0$$

of $\Lambda_{k-1}^{(2)}$-modules, where we let $\Lambda_{k-1}^{(2)} := \mathbb{Z}_p[\![\mathrm{Gal}(M/K)]\!]$.

We claim that $A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})})$ is a finitely generated torsion $\Lambda_{k-1}^{(2)}$-module. Then also $(A^{(\mathbb{L})})^{\mathrm{Gal}(\mathbb{L}/M)}$ is torsion and therefore $(A^{(\mathbb{L})})^{\mathrm{Gal}(\mathbb{L}/M)} = \{0\}$, since it can be embedded into $(\Lambda_{k-1}^{(2)})^{\oplus r}$. Taking $\mathrm{Gal}(M/(L \cap M))$-invariants and -coinvariants of the above sequence then yields an exact sequence

$$0 \longrightarrow (A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})}))^{\mathrm{Gal}(M/(L\cap M))} \longrightarrow \Lambda_{k-2}^{\oplus r} \longrightarrow \Lambda_{k-2}^{\oplus r}$$

of $\mathbb{Z}_p$-modules; here $\Lambda_{k-2} = \mathbb{Z}_p[\![T_3, \ldots, T_k]\!]$. Therefore

$$(A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})}))[T_2]$$

does not contain any non-trivial torsion Λ_{k-2}-submodules, in contradiction to (ii).

In order to prove the above claim, we note that

$$A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})}) \cong \mathrm{Gal}(H(\mathbb{L})^{\mathrm{ab}}/\mathbb{L}),$$

where $H(\mathbb{L})^{\mathrm{ab}}$ denotes the maximal subextension of $H(\mathbb{L})$ which is abelian over M; the notation $H(\mathbb{L})$ has been introduced in Section 2. Note that we have an exact sequence

$$0 \longrightarrow \textstyle\sum_{\mathfrak{p}} I_{\mathfrak{p}}(H(\mathbb{L})^{\mathrm{ab}}/M) \longrightarrow \mathrm{Gal}(H(\mathbb{L})^{\mathrm{ab}}/M) \longrightarrow A^{(M)} \longrightarrow 0,$$

where $I_{\mathfrak{p}}(H(\mathbb{L})^{\mathrm{ab}}/M) \subseteq \mathrm{Gal}(H(\mathbb{L})^{\mathrm{ab}}/M)$ denotes the inertia subgroup of a prime $\mathfrak{p}$ of M, and where the sum runs over the finitely many primes of M which ramify in $\mathbb{L}$. Each of the inertia groups can be identified with a subgroup of $\mathrm{Gal}(\mathbb{L}/M)$, because $H(\mathbb{L})^{\mathrm{ab}}/\mathbb{L}$ is unramified. This shows that $\sum_{\mathfrak{p}} I_{\mathfrak{p}}(H(\mathbb{L})^{\mathrm{ab}}/M)$ is a finitely generated free $\mathbb{Z}_p$-module and thus is $\Lambda_{k-1}^{(2)}$-torsion; therefore also $\mathrm{Gal}(H(\mathbb{L})^{\mathrm{ab}}/M)$ and

$$A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})}) \cong \mathrm{Gal}(H(\mathbb{L})^{\mathrm{ab}}/\mathbb{L})$$

are torsion $\Lambda_{k-1}^{(2)}$-modules. □

Remark 4.5. Analogous results (i.e. non-triviality of the maximal pseudo-null Λ_k-submodule) can also be proved for quotients A/B, dividing out the ideals generated from the primes above p, as long as none of these primes splits into infinitely many primes in M. In the proof, we just have to replace inertia groups by decomposition groups.

The following two lemmas describe situations in which hypotheses (i) and (ii) from Theorem 4.3 are valid.

Lemma 4.6. *Condition (i) from Theorem 4.3 holds, for example, if*

$$\mathrm{pd}_{\mathbb{Z}_p[\![\mathrm{Gal}(L/K)]\!]}(A^{(L)}) \le 1$$

and at most one prime of L ramifies in $\mathbb{L}$.

Proof. This follows from the proof of [24, Lemma 1] (cf. also the proof of the next lemma; the strategy of the two proofs is the same). □

Lemma 4.7. *In order to obtain a situation as in Theorem 4.3(ii), it suffices that $A^{(M)}$ contains a non-trivial* finite *$\mathbb{Z}_p[\![\mathrm{Gal}(M/K)]\!]$-submodule, and that there exists a map*

$$A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})}) \longrightarrow A^{(M)} \tag{4.3}$$

which is injective and has $\mathbb{Z}_p$-free cokernel. This can be achieved

1. *if $\mathbb{L}/M$ is unramified, or*
2. *if there exists exactly one prime of M dividing p which ramifies in $\mathbb{L}$, and this prime is totally ramified.*

Proof. We have an isomorphism

$$A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})}) \cong \mathrm{Gal}(N/\mathbb{L}),$$

where N denotes the maximal subfield of $H(\mathbb{L})$ which is abelian over M; condition (1) implies that actually $N = H(M)$. In this case, we therefore obtain an injective map

$$A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})}) \cong \mathrm{Gal}(H(M)/\mathbb{L}) \hookrightarrow \mathrm{Gal}(H(M)/M)$$

with $\mathbb{Z}_p$-free cokernel. In case (2), there exists a unique prime $\mathfrak{p}$ of M which ramifies in $\mathbb{L}$. We denote by $I_\mathfrak{p} \subseteq \mathrm{Gal}(N/M)$ the inertia subgroup. Then $N^{I_\mathfrak{p}} = H(M)$; since $I_\mathfrak{p} \cap \mathrm{Gal}(N/\mathbb{L}) = \{1\}$, it follows that $N = H(M) \cdot \mathbb{L}$, and therefore

$$A^{(\mathbb{L})}/(T_1 \cdot A^{(\mathbb{L})}) \cong \mathrm{Gal}(N/\mathbb{L}) = \mathrm{Gal}(H(M)/(\mathbb{L} \cap H(M))) \cong A^{(M)},$$

because $\mathbb{L} \cap H(M) = M$ by the second hypothesis in (2). □

Using the previous two lemmas, we can derive from Theorem 4.3 the following

Corollary 4.8. *Let $\mathbb{L}/K$ be a $\mathbb{Z}_p^2$-extension of a number field K; suppose that $L, M \subseteq \mathbb{L}$ denote two $\mathbb{Z}_p$-extensions of K such that*

(i) $(A^{(L)})^\circ = \{0\}$*, and at most one prime of L ramifies in $\mathbb{L}$, and*
(ii) $(A^{(M)})^\circ \neq \{0\}$*, and the extension $\mathbb{L}/M$ is unramified.*

Then $(A^{(\mathbb{L})})^\circ \neq \{0\}$.

The above approach will also be used in Section 5 (cf. the proofs of Theorem 1.2 and Theorem 5.9 below). Sometimes the existence of a nontrivial pseudo-null submodule of $(A^{(\mathbb{L})})^\circ$ can be proved more directly by considering a submodule $B^{(\mathbb{L})}$ of $A^{(\mathbb{L})}$ generated by some of the primes dividing p:

Remark 4.9. Suppose that $\mathbb{L}/K$ denotes a $\mathbb{Z}_p^k$-extension such that the decomposition groups $D_\mathfrak{p}(\mathbb{L}/K) \subseteq \mathrm{Gal}(\mathbb{L}/K)$ have $\mathbb{Z}_p$-ranks at least two for each prime $\mathfrak{p}$ of K dividing p. Then $B^{(\mathbb{L})} \subseteq A^{(\mathbb{L})}$ is pseudo-null, i.e. $B^{(\mathbb{L})} \subseteq (A^{(\mathbb{L})})^\circ$. Important special case: $\mathbb{L}/K$ is a $\mathbb{Z}_p^2$-extension such that there exist only finitely many primes of $\mathbb{L}$ dividing p.

We mention two example settings where the condition from the previous remark is satisfied. First, if K contains only one prime above p, then this prime is almost totally ramified in $\mathbb{L}/K$.

On the other hand, suppose that K is a CM-field, that $p \neq 2$ is totally split in $K/\mathbb{Q}$, $[K : \mathbb{Q}] \geq 4$ and that Leopoldt's conjecture holds for K and p. Then for each pair $\{\mathfrak{p}_i, \overline{\mathfrak{p}_i}\}$ of complex conjugate primes above p, there exists a unique $\mathbb{Z}_p$-extension $M^{(i)}$ of K such that the set of primes ramifying in $M^{(i)}$ equals $\{\mathfrak{p}_i, \overline{\mathfrak{p}_i}\}$ (cf. [13, Lemma 3.31]). In view of [5, Lemma 3], each prime of K dividing p is finitely split in $M^{(i)}/K$. Therefore $\mathrm{rank}_{\mathbb{Z}_p}(D_\mathfrak{p}(\mathbb{K}/K)) \geq 2$ for every prime $\mathfrak{p}$ above p, where $\mathbb{K}$ denotes the composite of all $\mathbb{Z}_p$-extensions of K. Note: in [5] a result concerning (GGC) is derived from this, see [5, Theorem 2].

Example 4.10. In [14], we studied a family of cubic non-normal extensions of $\mathbb{Q}$ each of which contained exactly one prime dividing $p = 3$. For example, the number field K defined by the polynomial $x^3 - 27x^2 + 18x - 21$ was contained in that family. Using PARI, we computed $A^{(K)} \cong \mathbb{Z}/9\mathbb{Z}$ and $(A^\#)^{(K)} \cong \mathbb{Z}/3\mathbb{Z}$, i.e. $D^{(K)} = 3 \cdot A^{(K)}$. If $\mathbb{K}$ denotes the composite of all $\mathbb{Z}_3$-extensions of K (which is a $\mathbb{Z}_3^2$-extension of K since K has exactly one real archimedean and one pair of complex primes and Leopoldt's Conjecture holds for K), then the results of [14] imply that $H(K) \cap \mathbb{K} = H'(K) \cap \mathbb{K}$. For the reader's convenience, we will briefly sketch the proof of this fact below. It then follows that $\{0\} \neq D^{(\mathbb{K})} \subseteq (A^{(\mathbb{K})})^\circ$. Indeed, $Z := H'(K) \cap \mathbb{K}$ equals the decomposition field of the unique prime $\mathfrak{p}$ above p in $\mathbb{K}/K$; if $\mathfrak{p}^{(Z)}$ denotes any prime of Z dividing $\mathfrak{p}$, then the order of $\mathfrak{p}^{(Z)}$ in $D^{(Z)}$ is at least $|D^{(K)}| = 3$, since $N_{Z/K}(\mathfrak{p}^{(Z)}) = \mathfrak{p}$. Moreover, $\mathfrak{p}^{(Z)}$ is totally ramified in $\mathbb{K}/Z$, and therefore the norm map $N \colon D^{(\mathbb{K})} \longrightarrow D^{(Z)}$ is surjective, i.e. $D^{(\mathbb{K})} \neq \{0\}$. We recall that $D^{(\mathbb{K})} = B^{(\mathbb{K})} \subseteq (A^{(\mathbb{K})})^\circ$ in view of the previous remark.

One can actually show more: if L denotes the cyclotomic $\mathbb{Z}_3$-extension of K, then it turns out that $A_1^{(L)} = A_2^{(L)} \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, and therefore

$A^{(L)} \cong A_1^{(L)}$ is finite by Fukuda's Theorem (cf. [7, Theorem 1]). Since L contains exactly one prime above $p = 3$, it follows from [14, Corollary 2.5] that $A^{(\mathbb{K})} = (A^{(\mathbb{K})})^\circ$, i.e. (GGC) holds for K and $p = 3$. Note that $A^{(\mathbb{K})} \neq \{0\}$ by the above.

Proof of the above claim. Class field theory implies that we have an exact sequence

$$0 \longrightarrow (\mathcal{O}_\mathfrak{p}^*/\overline{E_K})(3) \longrightarrow J_3(3) \xrightarrow{\text{cont}} A^{(K)} \longrightarrow 0.$$

Here $\mathfrak{p}$ denotes the unique prime of K dividing $p = 3$, $\mathcal{O}_\mathfrak{p}^* \subseteq K_\mathfrak{p}^*$ is the local unit group, $J_3 = (\prod_{v \nmid 3} K_v^*/\mathcal{O}_v^* \times K_\mathfrak{p}^*)/K^*$, and for any group G, $G(3)$ denotes the 3-pro-primary part of G. Note that $J_3(3)$ is isomorphic to the Galois group $\operatorname{Gal}(M_3(K)/K)$, where $M_3(K)$ denotes the maximal abelian pro-3-extension of K unramified outside $p = 3$.

If the above exact sequence splits, then $H(K) \cap \mathbb{K} = K$ (cf. [14, Claim 1 in Example 4.9]). More generally, suppose that there exists a map $s\colon D^{(K)} \to J_3(3)$ such that $\text{cont} \circ s = \text{id}_{D^{(K)}}$. Then

$$X := (\mathcal{O}_\mathfrak{p}^*/\overline{E_K})(3) \oplus s(D^{(K)}) \hookrightarrow J_3(3);$$

note that $X = \text{cont}^{-1}(D^{(K)})$, which is the subgroup

$$\operatorname{Fix}(H'(K)) \subseteq \operatorname{Gal}(M_3(K)/K) \cong J_3(3)$$

fixing $H'(K)$.

But then $H(K) \cap \mathbb{K} = H'(K) \cap \mathbb{K}$, since

$$\operatorname{Fix}(H'(K))/\operatorname{Fix}(H(K)) \cong s(D^{(K)})$$

is contained in the torsion subgroup of $\operatorname{Gal}(M_3(K)/K)$, which is $\operatorname{Fix}(\mathbb{K})$, and therefore

$$\operatorname{Fix}(H(K)) \cdot \operatorname{Fix}(\mathbb{K}) = \operatorname{Fix}(H'(K)) \cdot \operatorname{Fix}(\mathbb{K}).$$

It remains to construct a map $s\colon D^{(K)} \longrightarrow J_3(3)$. This can be done exactly as in [14, Example 4.9] (in fact, the family studied there was chosen such that this split exists, cf. [14, Claim 3]). □

We have now seen how to produce a non-trivial pseudo-null submodule of $A^{(\mathbb{L})}$ for a $\mathbb{Z}_p^k$-extension $\mathbb{L}$ of K. The following lemma can be used for deriving consequences concerning (GGC).

Lemma 4.11 (Fujii). *Let $\mathbb{L}/K$ be a $\mathbb{Z}_p^k$-extension, $k \geq 2$, and suppose that there exists a $\mathbb{Z}_p^{k-1}$-extension $L \subseteq \mathbb{L}$ of K such that*

(i) $(A^{(L)})^\circ = \{0\}$,

(ii) *there exists an injection for L as in* (4.1)*, where we write $T_2 = \gamma_2 - 1$ for some generator γ_2 of* $\operatorname{Gal}(\mathbb{L}/L) \cong \mathbb{Z}_p$*, as in Theorem 4.3, and*

(iii) *the characteristic power series* $F_{A^{(L)}}(T) \in \mathbb{Z}_p[\![L]\!] \cong \Lambda_{k-1}$ *of* $A^{(L)}$ *is irreducible.*

Then the following holds: If $(A^{(\mathbb{L})})^\circ \neq \{0\}$*, then* $A^{(\mathbb{L})}$ *is pseudo-null over* $\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}/K)]\!] \cong \Lambda_k$*.*

Proof. This follows from the proof of [3, Proposition 3.1] (which is given for a $\mathbb{Z}_p^2$-extension). For the reader's convenience, we include a sketch here. (i) and (ii) imply that $A^{(\mathbb{L})}/(T_2 \cdot A^{(\mathbb{L})})$ is not pseudo-null, and therefore the characteristic power series of the quotient $A^{(\mathbb{L})}/(T_2 \cdot A^{(\mathbb{L})})$ is not a unit (note that $A^{(\mathbb{L})} \neq \{0\}$ since $(A^{(\mathbb{L})})^\circ \neq \{0\}$ by assumption). The assumptions (ii) and (iii) imply that the characteristic power series of $A^{(\mathbb{L})}/(T_2 \cdot A^{(\mathbb{L})})$ is irreducible. Since the quotient does not contain any non-trivial pseudo-null submodules by (i) and (ii), it follows that the characteristic ideal and the Fitting ideal of this $\mathbb{Z}_p[\![\mathrm{Gal}(L/K)]\!]$-module coincide. Lifting the characteristic polynomial to $\mathrm{Fitt}_{\Lambda_k}(A^{(\mathbb{L})})$, we obtain an *irreducible* annihilator g of $A^{(\mathbb{L})}$ contained in $\mathrm{Fitt}_{\Lambda_k}(A^{(\mathbb{L})})$ (note that the image of a non-unit of Λ_k yields also a non-unit in $\Lambda_k/(T_2)$). If $A^{(\mathbb{L})}$ was not pseudo-null over Λ_k, then the annihilator ideal $\mathrm{Ann}(A^{(\mathbb{L})})$ of $A^{(\mathbb{L})}$ would be contained in some prime ideal of height one, and we could conclude that

$$\mathrm{Fitt}_{\Lambda_k}(A^{(\mathbb{L})}) = \mathrm{Ann}_{\Lambda_k}(A^{(\mathbb{L})}) = (g)$$

was principal. But then $(A^{(\mathbb{L})})^\circ = \{0\}$, in contradiction to our assumptions. □

Remark 4.12. If the characteristic power series $F_{A^{(L)}}(T)$ is irreducible and $\mathbb{L}/L$ is unramified, then $F_{A^{(L)}}(T) = T$, and $A^{(\mathbb{L})} = \{0\}$ in view of Nakayama's Lemma. Therefore hypotheses (ii) and (iii) from Lemma 4.11 can yield a *non-trivial* pseudo-null $A^{(\mathbb{L})}$ only if a prime (e.g. exactly one) ramifies in $\mathbb{L}/L$.[3]

In the last result of this section, we will describe an efficient criterion for proving that the characteristic polynomial $F_{A^{(L)}}(T)$ of a $\mathbb{Z}_p$-extension L of K is irreducible (cf. condition (iii) of the above lemma).

Lemma 4.13. *Let* L/K *be a* $\mathbb{Z}_p$*-extension and suppose that*

$$|A_{n+1}/(\lambda \cdot A_{n+1})| = |A_n/(\lambda \cdot A_n)| \leq p$$

for some $\lambda \in (p, T) \subseteq \Lambda = \mathbb{Z}_p[\![\mathrm{Gal}(L/K)]\!]$ *and some* $n \geq e(L/K)$*.*

Then either $A^{(L)} = (A^{(L)})^\circ$ *is finite, or* $(A^{(L)})^\circ = \{0\}$ *and the characteristic polynomial* $F_{A^{(L)}}(T)$ *of* $A^{(L)}$ *in* $\mathbb{Z}_p[\![\mathrm{Gal}(L/K)]\!] = \Lambda$ *is irreducible.*

Proof. By [15, Theorem 2.5], the assumption implies that

$$|A^{(L)}/(\lambda \cdot A^{(L)})| \leq p.$$

[3] I thank the anonymous referee for pointing out this constraint to me.

If the cardinality is 1, then $A^{(L)} = \{0\}$ by Nakayama's Lemma, because λ is contained in the maximal ideal of Λ. Therefore suppose that the order of the quotient is p. Now

$$|A^{(L)}/(\lambda \cdot A^{(L)})| = |(A^{(L)})^\circ/(\lambda \cdot (A^{(L)})^\circ)| \cdot |E_A/(\lambda \cdot E_A)|,$$

where E_A denotes the elementary Λ-module attached to $A^{(L)}$, by [13, Proposition 3.58]. Therefore one of the two factors on the right hand side must vanish. Again, this means that either $(A^{(L)})^\circ = \{0\}$ or $E_A = \{0\}$. In the second case, $A^{(L)}$ is finite. Suppose therefore that $(A^{(L)})^\circ = \{0\}$ and $|E_A/(\lambda \cdot E_A)| = p$. It is easy to see that $F_{A^{(L)}}(T)$ has to be irreducible in this case (in fact, if $F_{A^{(L)}}(T) = g_1 \cdot \ldots \cdot g_t$ for suitable irreducible elements $g_1, \ldots, g_t \in \Lambda$, then $|E_A/(\lambda \cdot E_A)| = \sum_{i=1}^t |\Lambda/(\lambda, g_i)|$, and each summand is greater than or equal to p). □

5. Applications and further Examples

In this section, we apply the results from the preceding two sections to two different settings: first we describe situations where we can show certain finiteness results for Iwasawa modules for the cyclotomic $\mathbb{Z}_p$-extension of a number field K, with an eye towards (but not limited to) fields K which contain exactly one prime above p. In this subsection, we also give a proof of Theorem 1.2 from the Introduction. In the second part, we study a certain class of number fields containing exactly two primes above p.

5.1. One prime above p. In this subsection we prove Theorem 1.2. The following lemma might prove useful also in other interesting situations.

Lemma 5.1. *Let K be any number field, and let L/K be a $\mathbb{Z}_p$-extension such that*

(i) $e(L/K) = 0$,
(ii) $\operatorname{rank}_p(A_1^{(L)}) = \operatorname{rank}_p(A^{(K)})$, *and*
(iii) $\operatorname{rank}_p(A^{(K)}) < \operatorname{rank}_p((A^\#)^{(K)}) + \operatorname{rank}_p(D^{(L)})$.

Then $((A^\#)^{(L)})^\circ$ is non-trivial. If moreover $\operatorname{rank}_p((A^\#)^{(K)}) = 1$, *then $(A^\#)^{(L)}$ is finite and cyclic.*

Proof. It follows from (i) and (ii) that $\operatorname{rank}_p(A_n) = \operatorname{rank}_p(A^{(K)})$ for every $n \in \mathbb{N}$. Lemma 3.8 implies that

$$r^{(p)} = r_0^{(p)} = \operatorname{rank}_p(A^{(K)}) - \operatorname{rank}_p((A^\#)^{(K)}) \overset{\text{(iii)}}{<} \operatorname{rank}_p(D^{(L)}).$$

Therefore $((A^\#)^{(L)})^\circ \neq \{0\}$ by Corollary 3.7. Since

$$\operatorname{rank}_p(A_n^\#) = \operatorname{rank}_p((A^\#)^{(K)})$$

for every $n \in \mathbb{N}$ by Lemma 3.8, the additional hypothesis means that actually $(A^\#)^{(L)} = ((A^\#)^{(L)})^\circ$ is finite. □

Remark 5.2. The following special instance of Lemma 5.1 is well-known. Let L/K be a $\mathbb{Z}_p$-extension such that only one prime $\mathfrak{p}$ of K ramifies in L, and suppose that $\mathfrak{p}$ is totally ramified. If $A^{(K)} = A_0^{(L)}$ and $A_1^{(L)}$ both are cyclic and $\{0\} \neq D^{(L)}$, then $(A^{\#})^{(L)}$ is either trivial or finite cyclic (depending on whether $D^{(L)} \subseteq p \cdot A^{(L)}$ or not).

In fact, $D^{(L)}$ is contained in $(A^{(L)})^{\Gamma}$, $\Gamma = \mathrm{Gal}(L/K)$, and therefore it is finite by Chevalley's Theorem 3.1 (i) because only one prime ramifies in L/K. Since $\mathrm{rank}_p(A^{(L)}) = 1$ and $D^{(L)} \neq \{0\}$ by assumption, it follows that actually

$$A^{(L)} = (A^{(L)})^{\circ}$$

is finite cyclic.

The following variant of Lemma 5.1 will be used for the proof of Theorem 5.4. Recall that for any finitely generated torsion Λ-module X, we defined

$$\mathrm{rank}_T(X) = v_p(|X/(T \cdot X)|),$$

whenever this is finite.

Lemma 5.3. *Let K be any number field, and let L/K be a $\mathbb{Z}_p$-extension. We suppose that*

(i) $e(L/K) = 0$,
(ii) $\mathrm{rank}_T(A_1) = \mathrm{rank}_T(A^{(K)})$,
(iii) $|(A^{\#})^{(K)}| = p$, *and*
(iv) $|D_n^{(L)}| > |D_0^{(L)}| = |D^{(K)}|$ *for some* $n \in \mathbb{N}$.

Then $A^{(L)}$ is finite.

Proof. It follows from (i) and (ii) that $\mathrm{rank}_T(A_n) = \mathrm{rank}_T(A^{(K)})$ for every $n \in \mathbb{N}$; Lemma 3.8 implies that $\mathrm{rank}_T(A_n^{\#}) = \mathrm{rank}_T((A^{\#})^{(K)}) \overset{\text{(iii)}}{=} 1$ for each n. We claim that $((A^{\#})^{(L)})^{\circ} \neq \{0\}$; by the above, this will imply that $(A^{\#})^{(L)} = ((A^{\#})^{(L)})^{\circ}$ is actually finite. Indeed, as in the proof of Lemma 5.1 the claim is true by Corollary 3.7 and Lemma 3.8, since

$$r^{(T)} = r_0^{(T)} = \mathrm{rank}_T(A^{(K)}) - \mathrm{rank}_T((A^{\#})^{(K)}) = v_p(|D_0^{(L)}|),$$

and this is strictly smaller than $\mathrm{rank}_T((A^{(L)})^{\circ}) \geq v_p(|D^{(L)}|)$ by (iv).

Therefore $(A^{\#})^{(L)}$ is finite. But $D^{(L)} \subseteq A^{(L)}[T]$ is also finite, since $\mathrm{rank}_T(A^{(L)})$ is finite by (i) and (ii). □

Theorem 5.4. *Let K be a number field containing exactly one prime $\mathfrak{p}$ above p. Let $L = \bigcup_n L_n$ be a $\mathbb{Z}_p$-extension of K such that the prime $\mathfrak{p}$ is totally ramified in L/K. If $|(A^{\#})^{(K)}| = p$ and $|D^{(L)}| > |D^{(K)}|$, then (GGC) holds for K.*

Proof. If K contains only one prime above p, then Chevalley's Theorem 3.1 (i) implies that hypothesis (ii) in Lemma 5.3 is satisfied; the remaining assumptions from that lemma are also satisfied by assumption, and therefore $A^{(L)}$ is finite. (GGC) for K and p follows from [14, Corollary 2.5], because L contains exactly one prime above p. □

Example 5.5. We consider a list of 20000 real quadratic number fields with small discriminant, taken from the LMFDB database [18]. Among this family, 11669 fields K contain exactly one prime $\mathfrak{p}$ above $p = 2$ which is totally ramified in the cyclotomic $\mathbb{Z}_2$-extension of K, and 261 of these fields satisfy the conditions from Theorem 5.4.

Moreover, let us consider the family of 20000 cubic number fields of signature [1,1] which has been used already in Example 3.18. We checked the conditions from Theorem 5.4, for $p = 3$. It turned out that for 69 of the number fields K in this list the hypotheses in Theorem 5.4 are satisfied. For example, suppose that K is defined by the polynomial $x^3 + 6x - 50$. Then

$$A^{(K)} \cong \mathbb{Z}/3\mathbb{Z},\ D^{(K)} = \{0\},\ A_1^{(L)} \cong (\mathbb{Z}/3\mathbb{Z})^3 \text{ and } D_1^{(L)} \cong \mathbb{Z}/3\mathbb{Z}.$$

Now we turn to the

Proof of Theorem 1.2. Since exactly one prime of K ramifies in $\mathbb{L}$, and as it is totally ramified, we have

$$A^{(L^{(i)})}/(TA^{(L^{(i)})}) \cong A^{(L^{(i-1)})}$$

for every $\mathbb{Z}_p^i$-extension $L^{(i)} \subseteq \mathbb{L}$ of K and any $\mathbb{Z}_p^{i-1}$-subextension

$$L^{(i-1)} = (L^{(i)})^{\langle T+1\rangle}.$$

In view of Lemmas 4.6 and 4.7, hypotheses (i) and (ii) of Theorem 4.3 can be replaced by the conditions "$\mathrm{pd}_{\mathbb{Z}_p[\![\mathrm{Gal}(L/K)]\!]}(A^{(L)}) \leq 1$" and "$A^{(M)}[T_2]$ contains a non-trivial $\mathbb{Z}_p[\![\mathrm{Gal}((L \cap M)/K)]\!]$-torsion submodule" for the corresponding subextensions of $\mathbb{L}$, respectively.

We proceed by induction. Suppose first that there exist $\mathbb{Z}_p$-extensions $L, M \subseteq \mathbb{L}$ of K such that $(A^{(L)})^\circ = \{0\}$ and $(A^{(M)})^\circ \neq \{0\}$. Then Theorem 4.3 implies that $(A^{(\mathbb{M}^{(2)})})^\circ[T_2] \neq \{0\}$, where $\mathbb{M}^{(2)} := L \cdot M$ and $\langle T_2 + 1\rangle = \mathrm{Gal}(\mathbb{M}^{(2)}/L)$.

Suppose now that we are given $\mathbb{Z}_p^i$-extensions $\mathbb{L}^{(i)}, \mathbb{M}^{(i)} \subseteq \mathbb{L}$ of K, $2 \leq i < k$, such that $(\mathbb{L}^{(i)} \cap \mathbb{M}^{(i)})/K$ is a $\mathbb{Z}_p^{i-1}$-extension,

$$\mathrm{pd}_{\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}^{(i)}/K)]\!]}(A^{(\mathbb{L}^{(i)})}) \leq 1$$

and $(A^{(\mathbb{M}^{(i)})})^\circ[T_2] \neq \{0\}$, where $(\mathbb{M}^{(i)})^{\langle T_2+1\rangle} = \mathbb{L}^{(i)} \cap \mathbb{M}^{(i)}$. Then $A^{(\mathbb{M}^{(i)})}[T_2]$ contains a non-trivial torsion $\mathbb{Z}_p[\![\mathrm{Gal}((\mathbb{L}^{(i)} \cap \mathbb{M}^{(i)})/K)]\!]$-submodule. Let

$\mathbb{M}^{(i+1)} = \mathbb{M}^{(i)} \cdot \mathbb{L}^{(i)}$. Noting that

$$\mathrm{Gal}(\mathbb{M}^{(i+1)}/\mathbb{L}^{(i)}) \cong \mathrm{Gal}(\mathbb{M}^{(i)}/(\mathbb{L}^{(i)} \cap \mathbb{M}^{(i)})),$$

Theorem 4.3 then implies that $(A^{(\mathbb{M}^{(i+1)})})^\circ[T_2] \neq \{0\}$. □

Remark 5.6. Let again $\mathbb{L}/K$ be a $\mathbb{Z}_p^k$-extension such that only one prime $\mathfrak{p}$ of K ramifies in $\mathbb{L}$, and suppose that $\mathfrak{p}$ is totally ramified. Now we assume that

$$\mathrm{pd}_{\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}/K)]\!]}(A^{(\mathbb{L})}) \leq 1$$

(in particular, this implies that $(A^{(\mathbb{L})})^\circ = \{0\}$). Then

$$\mathrm{pd}_{\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}^{(i)}/K)]\!]}(A^{(\mathbb{L}^{(i)})}) \leq 1$$

for each $\mathbb{Z}_p^i$-extension $\mathbb{L}^{(i)}$ of K contained in $\mathbb{L}$.

Indeed, we proceed via induction, and we assume that $k \geq 2$. Let $\mathbb{L}^{(k-1)} \subseteq \mathbb{L}$ be a $\mathbb{Z}_p^{(k-1)}$-extension of K contained in $\mathbb{L}$, and write

$$\mathbb{L}^{(k-1)} = \mathbb{L}^{\langle T+1 \rangle}.$$

Then $A^{(\mathbb{L}^{(k-1)})} \cong A^{(\mathbb{L})}/(T \cdot A^{(\mathbb{L})})$ and therefore

$$\begin{aligned}\mathrm{pd}_{\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}^{(k-1)}/K)]\!]}(A^{(\mathbb{L}^{(k-1)})}) &= \mathrm{pd}_{\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}^{(k-1)}/K)]\!]}(A^{(\mathbb{L})}/T \cdot A^{(\mathbb{L})}) \\ &= \mathrm{pd}_{\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}/K)]\!]}(A^{(\mathbb{L})}) \leq 1.\end{aligned}$$

5.2. Two primes above p.

Let $\mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field in which the prime p splits, and let $K \supseteq \mathbb{Q}(\sqrt{-d})$ be a number field such that p does not split further in $K/\mathbb{Q}(\sqrt{-d})$. We denote the primes of K dividing p by $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Let L denote the cyclotomic $\mathbb{Z}_p$-extension of K, and let M be a $\mathbb{Z}_p$-extension of K in which exactly one of the two primes of K dividing p, let's say $\mathfrak{p}_1$, is ramified (take M to be the shift of one of the two corresponding well-known $\mathbb{Z}_p$-extensions of $\mathbb{Q}(\sqrt{-d})$). We assume that the prime $\mathfrak{p}_2$ of K, which is unramified in M, *does not split at all* in M/K, and we consider the $\mathbb{Z}_p^2$-extension $\mathbb{L} := L \cdot M$ of K (this is just the shift of the $\mathbb{Z}_p^2$-extension of $\mathbb{Q}(\sqrt{-d}) \subseteq K$).

Theorem 5.7. *If, under the above assumptions, $|(A_0^\#)^{(M)}| = 1$, then (GGC) holds for K.*

Proof. If $(A_0^\#)^{(M)} = \{0\}$, then $A^{(K)}$ is generated by the ideal class of $\mathfrak{p}_1$. Then also $(A^\#)^{(M)} = \{0\}$ by Theorem 3.1 (ii) (note: it does not matter here whether $e(M/K) = 0$ or not). Therefore $A^{(M)}$ is finite. Moreover, since only one prime ramifies in $\mathbb{L}/M$ (because $\mathfrak{p}_2$ does not split at all in M by assumption), it follows from [14, Corollary 2.5] that $A^{(\mathbb{L})}$ is pseudo-null over $\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{L}/K)]\!]$. Since $\mathbb{L}$ contains only finitely many primes dividing p, (GGC) for K follows from [14, Corollary 2.4]. □

Remark 5.8. Let $B^{(K)} \subseteq A^{(K)}$ be generated by both primes above p, and write $(A')^{(K)} = A^{(K)}/B^{(K)}$. If $K/\mathbb{Q}(\sqrt{-d})$ is *abelian*, $A^{(K)}$ is cyclic and $A'^{(K)} = \{0\}$, then the validity of (GGC) is already proved in [20, Proposition 3.B]. Note that the primes of $\mathbb{Q}(\sqrt{-d})$ dividing p are allowed to ramify in K; therefore it is possible that $B^{(K)} \supsetneq D_0^{(M)}$.

Now we prove a sufficient criterion for the existence of a non-trivial pseudo-null submodule of $A^{(\mathbb{L})}$.

Theorem 5.9. *Let $K/\mathbb{Q}(\sqrt{-d})$ be as above and let $\mathbb{L} = L \cdot M$ denote the shift of the $\mathbb{Z}_p^2$-extension of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ contained in K. We assume that $e(L/K) = 0$ and $(A^{(L)})^\circ = \{0\}$ for the cyclotomic $\mathbb{Z}_p$-extension L of K.*

If $[(H(K) \cap \mathbb{L}) : K]$ is smaller than the order of the ideal class of $\mathfrak{p}_1$ in $A^{(K)}$, then $(A^{(\mathbb{L})})^\circ \neq \{0\}$.

Proof. Let $N = M_{e(M/K)} = H(K) \cap M$. Since $e(L/K) = 0$, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ do not split at all in $\mathbb{L}/K$. It follows from our assumptions that the ideal class of $\mathfrak{p}_1 = \mathfrak{p}_1^{(N)}$ in $A^{(N)}$ is non-trivial. Therefore the prime of M dividing $\mathfrak{p}_1^{(N)}$ generates a non-trivial subgroup $D^{(M)}$ of $A^{(M)}$. But $\operatorname{rank}_T(A^{(M)}) < \infty$, since only one prime of K ramifies in M, and therefore $D^{(M)} \subseteq (A^{(M)})^{\mathrm{Gal}(M/K)}$ is finite.

Since $(A^{(M)})^\circ \neq \{0\}$, it follows from Theorem 4.3, Lemma 4.6 and Lemma 4.7 that $(A^{(\mathbb{L})})^\circ \neq \{0\}$, because both primes of K dividing p are finitely split in $\mathbb{L}$, the assumption $e(L/K) = 0$ implies that $e(\mathbb{L}/M) = 0$, and $\mathbb{L}/L$ is unramified. Note that only one prime ramifies in $\mathbb{L}/M$, since $\mathfrak{p}_2$ does not split at all in M by assumption. □

In the following example we show that there exist infinite families of number fields to which the above results can be applied.

Example 5.10. We choose $k = \mathbb{Q}(\sqrt{-107})$, $p = 3$, and we let $K = kK^+$, where K^+ denotes the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{17})$. Then $p = 3$ splits in $k/\mathbb{Q}$, $A^{(k)} = D^{(k)} \cong \mathbb{Z}/3\mathbb{Z}$ and it is known that $H(k)$ is disjoint from the $\mathbb{Z}_3^2$-extension of k (cf. Table 6.1 in [20]). Moreover, if we denote the two primes of k dividing $p = 3$ by $\mathfrak{p}$ and $\bar{\mathfrak{p}}$, and if k_∞ denotes the $\mathbb{Z}_3$-extension of k which is ramified at $\mathfrak{p}$ and unramified at $\bar{\mathfrak{p}}$, then $\bar{\mathfrak{p}}$ does not split at all in k_∞. Indeed, $\bar{\mathfrak{p}}$ splits in k_∞ if and only if the Frobenius homomorphism attached to $\bar{\mathfrak{p}}$ is a cube in $\mathrm{Gal}(k_\infty/k) \cong \mathbb{Z}_3$. Using an argument from class field theory similar to the approach used in Example 4.10, we therefore have to show that a uniformising element $\bar{\pi}$ of $\bar{\mathfrak{p}}$ is not a cube in $\mathcal{O}_{\mathfrak{p}} \cong \mathbb{Z}_3$. Since $28^2 \equiv -107 \pmod{81}$, we see that $x = 28$ approximates $\sqrt{-107}$ in $\mathbb{Z}_3$. Note that the polynomial generating k over $\mathbb{Q}$ can be written as $x^2 + 107 \equiv x^2 - 1 = (x-1)(x+1) \pmod 3$; we thus write

$\mathfrak{p} = (3, \sqrt{-107} - 1)$, $\bar{\mathfrak{p}} = (3, \sqrt{-107} + 1)$, and we approximate $\sqrt{-107} \in \mathbb{Z}_3$ by the element $x = 28$. Then $\overline{\pi}$ is approximated by $\sqrt{-107}+1 \equiv 28+1 = 29 \pmod{81}$. If $\overline{\pi}$ was a cube in $\mathcal{O}_{\mathfrak{p}}^* \cong \mathbb{Z}_3^*$, then 29 would be a cube modulo 81. But this is not the case.

Therefore $\bar{\mathfrak{p}}$ does not split at all in k_∞/k. Since 3 is a primitive root modulo 17, $p = 3$ is inert in $K^+/\mathbb{Q}$, and therefore K contains exactly two primes above p. Moreover, $A^{(K^+)} = \{0\}$ and therefore $(A^{(L)})^\circ = \{0\}$, because K^+ contains exactly one prime above p. Finally, we have

$$H(K) \cap \mathbb{L} = K,$$

because $H(k)$ is disjoint from $\mathbb{L}$ and $[K : k] = 8$ is coprime with p; by the same reason, the prime of K dividing $\bar{\mathfrak{p}}$ does not split at all in $M := k_\infty \cdot K$. But $D_0^{(M)} \cong \mathbb{Z}/3\mathbb{Z}$ is non-trivial, and therefore (the proof of) Theorem 5.9 implies that $(A^{(\mathbb{L})})^\circ \neq \{0\}$.

More generally, let K^+ be the maximal totally real subfield of $\mathbb{Q}(\zeta_{17^n})$ for any $n \in \mathbb{N}, n \geq 1$. Then again $p = 3$ is inert in K^+, $A^{(K^+)} = \{0\}$ and the composite field $K := kK^+$ has degree $[K : k] = 8 \cdot 17^{n-1}$ coprime with p. Therefore $H(K) \cap \mathbb{L} = K$, and $D^{(K)}$ is non-trivial, proving that $(A^{(\mathbb{L})})^\circ \neq \{0\}$.

The same works with the number field K^+ which is defined by the polynomial $x^3 + 3x^2 - 27x + 9$: K^+ is a non-normal totally real cubic number field such that $A^{(L^+)} = \{0\}$, where L^+ denotes the cyclotomic $\mathbb{Z}_3$-extension of K^+. Note that the two primes of $k = \mathbb{Q}(\sqrt{-107})$ dividing $p = 3$ are totally ramified in K/k, and therefore the prime of K dividing $\bar{\mathfrak{p}}$ does not split in the $\mathbb{Z}_p$-extension $M = k_\infty \cdot K$ of K:

$$\begin{tikzcd}
k_1 \arrow[r, dash, "\text{ram.}"] \arrow[d, dash, "\text{inert}"'] & M_1 = k_1 \cdot K \arrow[d, dash, "\text{inert}"] \\
k \arrow[r, dash, "\text{ram.}"'] & K
\end{tikzcd}$$

Since $e(L/K) = 0$ for the cyclotomic $\mathbb{Z}_3$-extension L of K, the prime of K dividing $\mathfrak{p}$ also does not split in M. Moreover, $A^{(K)} \cong \mathbb{Z}/9\mathbb{Z}$ is generated by each of the two primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of K dividing p, and $[(H(K) \cap M) : K] \leq 3$, because $H(k) \cap \mathbb{L} = k$. Therefore again

$$(A^{(\mathbb{L})})^\circ \neq \{0\}$$

by (the proof of) Theorem 5.9.

Note: since $A^{(K)}$ is generated by $\mathfrak{p}_2$, it follows from Theorem 5.7 that (GGC) holds for K.

References

[1] R. Badino & T. Nguyen Quang Do, "Sur les égalités du miroir et certaines formes faibles de la conjecture de Greenberg.", *Manuscr. Math.* **116** (2005), no. 3, p. 323-340.

[2] F. M. Bleher, T. Chinburg, R. Greenberg, M. Kakde, G. Pappas, R. T. Sharifi & M. J. Taylor, "Higher Chern classes in Iwasawa theory", *Am. J. Math.* **142** (2020), no. 2, p. 627-682.

[3] S. Fujii, "Pseudo-null submodules of the unramified Iwasawa module for $\mathbb{Z}_p^2$-extensions.", *Interdiscip. Inf. Sci.* **16** (2010), no. 1, p. 55-66.

[4] ———, "On restricted ramifications and pseudo-null submodules of Iwasawa modules for $\mathbb{Z}_p^2$-extensions.", *J. Ramanujan Math. Soc.* **29** (2014), no. 3, p. 295-305.

[5] ———, "On Greenberg's generalized conjecture for CM-fields", *J. Reine Angew. Math.* **731** (2017), p. 259-278.

[6] ———, "Some remarks on finite submodules of the unramified Iwasawa module of totally real fields", *Proc. Japan Acad., Ser. A* **96** (2020), no. 9, p. 83-85.

[7] T. Fukuda, "Remarks on $\mathbb{Z}_p$-extensions of number fields.", *Proc. Japan Acad., Ser. A* **70** (1994), no. 8, p. 264-266.

[8] M. Grandet & J.-F. Jaulent, "Sur la capitulation dans une $\mathbb{Z}_\ell$-extension.", *J. Reine Angew. Math.* **362** (1985), p. 213-217.

[9] G. Gras, "Classes généralisées invariantes.", *J. Math. Soc. Japan* **46** (1994), no. 3, p. 467-476.

[10] R. Greenberg, "The Iwasawa invariants of Γ-extensions of a fixed number field.", *Am. J. Math.* **95** (1973), p. 204-214.

[11] ———, "Iwasawa theory – past and present.", in *Class field theory – its centenary and prospect. Proceedings of the 7th MSJ International Research Institute of the Mathematical Society of Japan, Tokyo, Japan, June 3–12, 1998*, Mathematical Society of Japan, 2001, p. 335-385.

[12] K. Iwasawa, "On the μ-invariants of $\mathbb{Z}_\ell$-extensions.", in *Number theory, algebraic geometry and commutative algebra in honor of Yasuo Akizuki*, Kinokuniya Book-Store Co., 1973, p. 1-11.

[13] S. Kleine, "A new approach for the investigation of Iwasawa invariants.", PhD Thesis, University of Göttingen, 2015.

[14] ———, "Relative extensions of number fields and Greenberg's generalised conjecture.", *Acta Arith.* **174** (2016), no. 4, p. 367-392.

[15] ———, "Local behavior of Iwasawa's invariants.", *Int. J. Number Theory* **13** (2017), no. 4, p. 1013-1036.

[16] ———, "T-ranks of Iwasawa modules.", *J. Number Theory* **196** (2019), p. 61-86.

[17] S. Lang, *Cyclotomic fields. I and II. With an appendix by Karl Rubin: The main conjecture. Combined 2nd edition.*, New York etc.: Springer-Verlag, 1990, xvii + 433 pages.

[18] The LMFDB Collaboration, "The L-functions and Modular Forms Database", 2021, `http://www.lmfdb.org`.

[19] W. G. McCallum & R. T. Sharifi, "A cup product in the Galois cohomology of number fields.", *Duke Math. J.* **120** (2003), no. 2, p. 269-310.

[20] J. Minardi, "Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields.", PhD Thesis, University of Washington, 1986.

[21] J. Neukirch, A. Schmidt & K. Wingberg, *Cohomology of number fields. 2nd ed.*, Springer, 2008, xv + 825 pages.

[22] T. Nguyen Quang Do, "Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé.", *Int. J. Number Theory* **2** (2006), no. 1, p. 49-64.

[23] M. Ozaki, "The class group of $\mathbb{Z}_p$-extensions over totally real number fields.", *Tôhoku Math. J.* **49** (1997), no. 3, p. 431-435.

[24] ———, "Iwasawa invariants of $\mathbb{Z}_p$-extensions over an imaginary quadratic field.", in *Class field theory – its centenary and prospect. Proceedings of the 7th MSJ International Research Institute of the Mathematical Society of Japan, Tokyo, Japan, June 3–12, 1998*, Mathematical Society of Japan, 2001, p. 387-399.

[25] ———, “Construction of $\mathbb{Z}_p$-extensions with prescribed Iwasawa modules”, *J. Math. Soc. Japan* **56** (2004), no. 3, p. 787-801.

[26] The PARI Group, *PARI/GP version* `2.11.2`, 2021, available from `http://pari.math.u-bordeaux.fr/`.

[27] M. Rosen, “Two theorems on Galois cohomology.”, *Proc. Am. Math. Soc.* **17** (1966), p. 1183-1185.

[28] J. W. Sands, “On small Iwasawa invariants and imaginary quadratic fields.”, *Proc. Am. Math. Soc.* **112** (1991), no. 3, p. 671-684.

[29] B. Schmithals, “Kapitulation der Idealklassen und Einheitenstruktur in Zahlkörpern.”, *J. Reine Angew. Math.* **358** (1985), p. 43-60.

[30] R. T. Sharifi, “On Galois groups of unramified pro-p extensions”, *Math. Ann.* **342** (2008), no. 2, p. 297-308.

[31] L. C. Washington, *Introduction to cyclotomic fields. 2nd ed.*, Springer, 1997, xiv + 487 pages.

Sören Kleine
Institut für Theoretische Informatik, Mathematik und Operations Research
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
D-85577 Neubiberg, Germany
E-mail: `soeren.kleine@unibw.de`