Riv. Mat. Univ. Parma, Vol. **7** (2016), 181-192

Fabio Caldarola

Invariants and coinvariants of class groups in $\mathbb{Z}_p$-extensions and Greenberg's Conjecture

Abstract. Let K/k be a $\mathbb{Z}_p$-extension of a number field k, k_n its n-th layer and A_n the p-class group of k_n. In this paper we give two criteria, both based on the group of invariants B_n of A_n, which imply the finiteness of the Iwasawa module $X(K/k)$ and we discuss some of their consequences. The first criterion deals with stabilization and capitulation of the B_n, while the second one uses the nilpotency of the Galois group $\mathrm{Gal}(L(K)/k)$, where $L(K)$ is the maximal unramified abelian pro-p-extension of K.

Keywords. Iwasawa modules, $\mathbb{Z}_p$-extensions, class groups, capitulation of ideals, lower central series.

Mathematics Subject Classification (2010): 11R23, 11R29.

1 - Introduction

Let p be a prime number, k a number field and K/k any $\mathbb{Z}_p$-extension of k. We denote by $\Gamma = \overline{\langle\gamma\rangle} \simeq \mathbb{Z}_p$ the Galois group $\mathrm{Gal}(K/k)$ and by k_n the n-th layer of K/k, i.e., the unique subfield of K of degree p^n over k. Let $n_0(K/k)$ (or n_0 for short) be the minimal $n \geqslant 0$ such that every prime ideal which ramifies in the extension K/k_n, is totally ramified and let $s = s(K/k)$ be the number of ramified prime ideals in K/k_{n_0}.

We denote by $L = L(K)$ the maximal abelian unramified pro-p-extension of K in a fixed algebraic closure of $\mathbb{Q}$, and by $X = X(K)$ the Galois group $\mathrm{Gal}(L/K)$. Similarly, let $L_n = L(k_n)$ be the maximal abelian unramified p-extension of k_n and let $X_n = X(k_n)$ be the group $\mathrm{Gal}(L_n/k_n)$.

Received: January 4, 2016; accepted in revised form: February 23, 2016.

Let, moreover, A_n be the p-part of the ideal class group of k_n so, for all $n \in \mathbb{N}$, A_n is canonically isomorphic to X_n via the Artin map. For all $m \geqslant n \geqslant 0$, we denote by $i_{n,m} : A_n \to A_m$ the map induced by the extension of ideals. Put

$$(1) \qquad A := \varinjlim A_n \qquad \text{and denote by} \qquad i_n : A_n \to A$$

the natural inclusion map. In addition let $H_{n,m}$ be the kernel of $i_{n,m}$ and H_n be the kernel of i_n, i.e., $H_n = \bigcup_{m \geqslant n} H_{n,m}$. The $H_{n,m}$ and the H_n are often called *capitulation kernels* and are quite important in Iwasawa theory, for example because of their link with Greenberg's Conjecture (see [8, Proposition 2], [**10**, Proposition 1.B] or [**6**, Theorem 2]). For an extensive study of the properties of the $H_{n,m}$ and the H_n for $\mathbb{Z}_p$-extensions, see [**4**], in which the authors provide a detailed description in terms of the maximal finite submodule $D := D(K/k)$ of $X(K/k)$. For similar results on capitulation in connection with Greenberg's Generalized Conjecture in the case of multiple $\mathbb{Z}_p$-extensions see [**3**], [**2**] or [**9**]. We recall that Greenberg's Conjecture predicts the finiteness of $X(k_{cyc})$ when k is a totally real number field and k_{cyc} its cyclotomic $\mathbb{Z}_p$-extension; we will not deal with multiple $\mathbb{Z}_p$-extensions here, for a nice survey of the theory see [**7**] (it includes the statement of Greenberg's Generalized Conjecture as Conjecture 3.5).

Let $B_n := (A_n)^{\Gamma}$ be the invariant subgroup of A_n with respect to the action of Γ, i.e.,

$$B_n := \{b \in A_n \;:\; b^{\gamma} = b\}\,.$$

In Section 2, as preliminary result, we will show that the sequence of the orders of the B_n *stabilize*, i.e., becomes constant, at the very first layer $n \geqslant n_0$ for which $|B_n| = |B_{n+1}|$ (see Lemma 2.2 (**b**)). For similar results on stabilization of the A_n see [**6**] and [**1**], or for other Iwasawa modules like the capitulation kernels see [**4**] and, in a quite different context (non-abelian Iwasawa theory), [**5**]. Now, our first criterion can be stated as follows (cfr. Theorem 2.1)

Theorem 1.1. *Let K/k be any $\mathbb{Z}_p$-extension. Assume that $|B_n| = |B_{n+1}|$ and $B_n \subseteq H_{n,m}$ for some $m \geqslant n \geqslant n_0$, then $X \simeq A_m$.*

The previous theorem can be particularly useful in specific cases, for example when $|B_n| = |B_{n+1}|$ for a small n and B_n is generated by classes of totally ramified ideals or of ideals which totally split.

For the proof and some consequences of Theorem 1.1 see Subsection 2.2, in which we shall also explain how some results of [8] and [**6**] can be seen as particular cases of our Theorem 1.1.

Our second criterion, instead, relates the invariant subgroups B_n with the nilpotency of the group $\mathrm{Gal}(L(K)/k)$ as follows (cfr. Theorem 3.1)

Theorem 1.2. *Let K/k be any $\mathbb{Z}_p$-extension of a number field k. The following conditions are equivalent:*

(**a**) *the sequence $\{|B_n|\}_{n\in\mathbb{N}}$ is bounded and $\mathcal{G} := \mathrm{Gal}(L(K)/k)$ is nilpotent;*

(**b**) *$X = X(K/k)$ is finite.*

The previous theorem relies on methods very different from the ones used for Theorem 1.1. In particular it involves the lower central series and the nilpotency class of the group $\mathrm{Gal}(L(K)/k)$; similar tools are described and used in [**12**] and [**5**]. The final Section 3 of the present paper is devoted to the proof and some consequences of Theorem 1.2.

2 - The first criterion

In the first subsection we briefly describe some of the basic objects in Iwasawa theory we are going to work with: for more details and comprehensive references see [**14**, Chapter 7 and 13] or [**11**, Chapter 5].

2.1 - *Notations and preliminaries*

Let Γ be the Galois group $\mathrm{Gal}(K/k) \simeq \mathbb{Z}_p$ and choose a topological generator γ of Γ. We use Γ_n to denote Γ/Γ^{p^n}, which is canonically isomorphic to the cyclic group $\mathrm{Gal}(k_n/k)$ of order p^n.

We recall that $X = \mathrm{Gal}(L(K)/K)$ (called the *Iwasawa module*) is a module over the completed group ring $\mathbb{Z}_p[[\Gamma]] \simeq \varprojlim \mathbb{Z}_p[\mathrm{Gal}(k_n/k)]$ via the action of conjugation. The map $\gamma \to 1+T$ gives a noncanonical isomorphism between $\mathbb{Z}_p[[\Gamma]]$ (called the *Iwasawa algebra*) and $\Lambda := \mathbb{Z}_p[[T]]$, i.e., the formal power series ring in one variable over $\mathbb{Z}_p$. In the following we shall identify both with our symbol Λ. For any $n \geqslant n_0$ let Y_n be the Λ-submodule of X such that $A_n \simeq X/Y_n$, roughly speaking, Y_n is obtained by taking the closure of the module generated by the commutators and the inertia subgroups of $\mathrm{Gal}(L(K)/k_n)$. For any $m \geqslant n \geqslant n_0$ we have $Y_m = \nu_{n,m} Y_n$, where $\nu_{n,m} = \dfrac{\nu_m}{\nu_n} = \dfrac{(1+T)^{p^m}-1}{(1+T)^{p^n}-1} = 1 + (1+T)^{p^n} + \dots + \left((1+T)^{p^n}\right)^{p^{m-n}-1}$ is a distinguished polynomial which basically represents the map $i_{n,m}$ (in particular $H_{n,m} = \{x \in X/Y_n \,:\, \nu_{n,m}(x) \in Y_m\}$). Moreover, for any $m \geqslant n \geqslant 0$, the $\nu_{n,m}$ verify the following formula (see, e.g., [**6**, Lemma])

$$\nu_{n,m} = \frac{(((1+T)^{p^n}-1)+1)^{p^{m-n}}-1}{(1+T)^{p^n}-1} \equiv p^{m-n} \pmod{T\nu_n}\,. \tag{2}$$

A finitely generated Λ-module M is *pseudo-null* if it has at least two relatively prime annihilators. Being Λ-pseudo-null is equivalent to being finite, and we write $M \sim_\Lambda 0$ to denote a pseudo-null Λ-module M.

Let I_Γ be the augmentation ideal of Λ (which correspond to $T\Lambda$ in the isomorphism $\gamma \leftrightarrow 1+T$ above) and let $C_n := (A_n)_\Gamma$ be the coinvariants of A_n with respect to the same action of Γ, i.e.,

$$C_n := A_n/I_\Gamma A_n = A_n/\{a^{\gamma-1} \,:\, a \in A_n\}\,. \tag{3}$$

In terms of Galois groups C_n is isomorphic to Gal(k'_n/k_n), where k'_n is the genus p-class field of k_n over k (i.e., the largest abelian extension of k contained in L_n), and B_n corresponds through the Artin map to Gal(L_n/L'_n), where L'_n is the smallest extension of k_n contained in L_n such that Γ_n acts trivially on Gal(L_n/L'_n). Moreover for all $m \geqslant n \geqslant 0$ we denote by $N_{m,n} : A_m \to A_n$ the norm map between the p-class groups.

Lemma 2.1. *For every $n \geqslant 0$ we have*

(a) $N_{n+1,n}(B_{n+1}) \subseteq B_n$ *and* $i_{n,n+1}(B_n) \subseteq B_{n+1}$*;*

(b) $N_{n+1,n}(I_\Gamma A_{n+1}) \subseteq I_\Gamma A_n$ *and* $i_{n,n+1}(I_\Gamma A_n) \subseteq I_\Gamma A_{n+1}$*.*

Proof. All statements can be easily derived from the commutativity of the following two diagrams

$$\begin{array}{ccc} A_{n+1} & \xrightarrow{\gamma-1} & A_{n+1} \\ \downarrow{\scriptstyle N_{n+1,n}} & & \downarrow{\scriptstyle N_{n+1,n}} \\ A_n & \xrightarrow{\gamma-1} & A_n \end{array} \qquad\qquad \begin{array}{ccc} A_n & \xrightarrow{\gamma-1} & A_n \\ \downarrow{\scriptstyle i_{n+1,n}} & & \downarrow{\scriptstyle i_{n+1,n}} \\ A_{n+1} & \xrightarrow{\gamma-1} & A_{n+1} \end{array}$$

□

Therefore inclusions and norms induce well defined maps on B_n and C_n as well, and we will still denote them with $i_{n,m}$ and $N_{m,n}$. We also put

$$B = B(K/k) := \varinjlim B_n \qquad \text{and} \qquad i_n : B_n \to B$$

(notation analogous to that in (1)). We introduce a final piece of notation: we let $\xi_T : X \to X$ represent multiplication by T and this implies that, in terms of Λ-modules, we write

$$\begin{aligned} B_n &= A_n^\Gamma \simeq (X/Y_n)^\Gamma \\ &= \{x \in X \,:\, \gamma x \equiv x \pmod{Y_n}\} \\ &= \{x \in X \,:\, Tx \in Y_n\} =: \xi_T^{-1}(Y_n)\,. \end{aligned}$$

So our ξ_T avoids using a possibly misleading T^{-1}.

2.2 - *The modules B_n and the pseudo-nullity of X*

In this subsection we give the proof of Theorem 1.1 together with some related results and consequences. We begin with the following stabilization lemma

Lemma 2.2. *Let K/k be any $\mathbb{Z}_p$-extension. Then*

(a) *the sequence $\{|B_n|\}_n$ is non decreasing for $n \geqslant n_0$;*

(b) *if $|B_n| = |B_{n+1}|$ for some $n \geqslant n_0$, then $|B_m| = |B_n|$ for every $m \geqslant n$.*

Proof. **(a)** Notice that B_n and C_n appear in the exact sequence

$$0 \longrightarrow B_n \longrightarrow A_n \xrightarrow{\gamma-1} A_n \longrightarrow C_n \longrightarrow 0$$

hence they have the same cardinality for every $n \geqslant 0$. But for $n \geqslant n_0$ we have $C_n \simeq X/TX + Y_n$, so the sequences $\{|C_n|\}_n$ and $\{|B_n|\}_n$ are non decreasing for $n \geqslant n_0$.

(b) The hypothesis $|B_n| = |B_{n+1}|$ gives $|C_n| = |C_{n+1}|$, hence we obtain $|X/TX + Y_n| = |X/TX + Y_{n+1}|$ which means $TX + Y_n = TX + Y_{n+1}$ for some $n \geqslant n_0$. Now considering the quotient module $TX + Y_n/TX$ we have $\nu_{n,n+1}(TX + Y_n/TX) = TX + Y_n/TX$, and from Nakayama's Lemma we obtain $TX + Y_n/TX = 0$. But this yields $Y_n \subseteq TX$, and $C_m \simeq X/TX$ for all $m \geqslant n$. □

Remark 2.1. Recall that the norm $N_{n+1,n}$ is surjective on class groups for $n \geqslant n_0$, hence the induced map on the C_n is surjective as well. From the proof of the previous lemma, the equality $|B_n| = |B_{n+1}|$ yields $|B_m| = |B_n|$ and $C_m \simeq C_n$ (for all $m \geqslant n$), but not $B_m \simeq B_n$. Moreover if the sequence $\{|A_n|\}_{n \geqslant n_0}$ stabilizes at m, then $\{|B_n|\}_{n \geqslant n_0}$ stabilizes at most at m as well. More precisely: if $N_{n+1,n} : A_{n+1} \to A_n$ is an isomorphism for some $n \geqslant n_0$, then it maps isomorphically B_{n+1} onto B_n as well. On the contrary, if we assume that B_{n+1} is isomorphic to B_n, we cannot deduce anything on the A_n unless we know that the isomorphism is given by the norm map (i.e., if $N_{n+1,n} : B_{n+1} \to B_n$ is an isomorphism, then $N_{n+1,n} : A_{n+1} \to A_n$ is an isomorphism too, see Proposition 2.1 below).

Now we state and prove the first criterion.

Theorem 2.1. *If $|B_n| = |B_{n+1}|$ and $B_n \subseteq H_{n,m}$ for some $m \geqslant n \geqslant n_0$, then $X \simeq A_m$.*

Proof. The hypothesis on the capitulation of B_n means that $\nu_{n,m}\, \xi_T^{-1}(Y_n)$ is contained in Y_m, so $T\nu_{n,m}\, \xi_T^{-1}(Y_n) \subseteq TY_m$ (recall the correspondence between the maps $i_{n,m}$ and the polynomials $\nu_{n,m}$). As we have already seen in the proof of Lemma 2.2, $|B_n| = |B_{n+1}|$ implies $Y_n \subseteq TX$, i.e., Y_n is contained in the image of ξ_T. Thus $T\nu_{n,m}\,\xi_T^{-1}(Y_n) = \nu_{n,m}Y_n = Y_m$ and $Y_m = TY_m$. Nakayama's Lemma yields $Y_m = 0$ and since $A_m \simeq X/Y_m$, we conclude that $X \simeq A_m$. □

The following is a straightforward consequence which reproves (and slightly generalizes) [8, Theorem 1] and the first statement of [6, Theorem 2].

Corollary 2.1. *If $s(K/k) = 1$, $n_0(K/k) = 0$ and $A_0 = H_{0,n}$ for some $n \geqslant 0$, then $X \sim_\Lambda 0$.*

Proof. The hypothesis on the unique totally ramified prime yields $|B_n| = |A_0|$ for any n. □

Furthermore it is also possible to generalize some results obtained in [4], using Theorem 2.1 in a very similar way. Recall that D is the maximal finite submodule of X and let $r = r(K/k) := \min\{z \geqslant n_0 \text{ s.t. } D \cap Y_n = 0\}$ (for the origin of this parameter and its meaning see [4, Definition 3.1 and Remark 3.8]). Another application of the criterion is given by the following

Corollary 2.2. *We have*

$$B = 0 \Leftrightarrow X \sim_\Lambda 0\,.$$

Proof. The $\Leftarrow$ direction is obvious. For the other direction if $B = 0$, then $i_{r+1}(B_{r+1}) = 0$ and this means that B_{r+1} is contained in H_{r+1}, i.e., in terms of Iwasawa modules, $\xi_T^{-1}(Y_{r+1}) \subseteq Y_{r+1} + D$ (see [4, Proposition 3.3]). It is easy to see that $\xi_T^{-1}(Y_{r+1}) = Y_{r+1} + D[T]$, thus

$$B_{r+1} \simeq D[T] + Y_{r+1}/Y_{r+1} \simeq D[T]$$

(the last isomorphism depends on the fact that $D[T] \cap Y_{r+1} = 0$, which comes from our definition of $r = r(K/k)$). Now consider B_r which, by hypothesis, is contained in H_r: repeating the previous argument we find $B_r \simeq D[T]$. Therefore $B_r = B_{r+1}$ and we can apply the criterion given by Theorem 2.1 to obtain the pseudo-nullity of X. □

Remark 2.2. For completeness we also give a direct proof of $B = 0 \Rightarrow A = 0$ (the fact that $A = 0 \Rightarrow X \sim_\Lambda 0$ is well known).

Assume that $B = 0$ and that there exists $n \geqslant 0$ such that $H_n \neq A_n$. Consider the action of Γ_n on A_n/H_n: from the class orbit formula we have that there exists

$[\mathfrak{a}] \in A_n - H_n$ such that $[\mathfrak{a}]H_n$ is fixed by γ. Hence $[\mathfrak{a}]^{\gamma-1} \in H_n$, i.e., there exists $m \geqslant n$ such that $i_{n,m}([\mathfrak{a}]) \in B_m$. By hypothesis $B_m \subseteq H_m$ and we have a contradiction. Therefore $H_n = A_n$ for every $n \geqslant 0$, hence $A = 0$ and X is pseudo-null.

We want to point out the following fact about the B_n, in connection with the kernel of the norm maps.

Proposition 2.1. *Suppose that $B_{n+1} \cap \mathrm{Ker}(N_{n+1,n}) = 0$ for some $n \geqslant n_0$, then $X \simeq A_n$.*

Proof. By hypothesis $N_{n+1,n} : B_{n+1} \to B_n$ is injective. Thus it has to be surjective too and then $|B_{n+1}| = |B_n|$. But this means $\xi_T^{-1}(Y_{n+1}) + Y_n = \xi_T^{-1}(Y_n)$ and, as we have seen in the proof of Lemma 2.2, Y_n is contained in the image of ξ_T. Therefore $Y_{n+1} + TY_n = Y_n$, i.e., $(\nu_{n,n+1}, T)Y_n = Y_n$. By Nakayama's Lemma $Y_n = 0$ and $X \simeq A_n$. □

Remark 2.3. The proof of Proposition 2.1 follows the lines of the rest of our results, but we can also provide a more group theoretic proof. Consider the action of Γ_{n+1} on $\mathrm{Ker}(N_{n+1,n})/\mathrm{Ker}(N_{n+1,n}) \cap B_{n+1}$ which, by hypothesis, is isomorphic to $\mathrm{Ker}(N_{n+1,n})$. Now, since $\mathrm{Ker}(N_{n+1,n})/\mathrm{Ker}(N_{n+1,n}) \cap B_{n+1}$ has no fixed points, by the class orbit formula we have that $\mathrm{Ker}(N_{n+1,n})$ is trivial: hence $X \simeq A_{n+1} \simeq A_n$.

We conclude this section drawing attention on how the capitulation of $B_n \cap H_n$ depends basically on the exponent of the torsion module $D[T]$.

Proposition 2.2. *For any $n \geqslant r$, $B_n \cap H_n$ capitulates exactly in $B_{n+\zeta}$, where p^ζ is the exponent of $D[T]$.*

Proof. In terms of Λ-modules

$$B_n \cap H_n \simeq (\xi_T^{-1}(Y_n)/Y_n) \cap (D + Y_n/Y_n) = \xi_T^{-1}(Y_n) \cap (D + Y_n)/Y_n \ ,$$

so, using the modular law, we get

$$B_n \cap H_n \simeq (\xi_T^{-1}(Y_n) \cap Y_n) + (\xi_T^{-1}(Y_n) \cap D)/Y_n = Y_n + (\xi_T^{-1}(Y_n) \cap D)/Y_n \,.$$

Since $n \geqslant r$, one has that $Y_n + (\xi_T^{-1}(Y_n) \cap D)/Y_n$ is isomorphic to $\xi_T^{-1}(Y_n) \cap D = D[T]$. Hence we obtain $B_n \cap H_n \simeq D[T] + Y_n/Y_n$ and, using (2), we get

$$\nu_{n,n+\zeta}(Y_n + D[T]) = Y_{n+\zeta} + \nu_{n,n+\zeta}D[T] \subseteq Y_{n+\zeta} + p^\zeta D[T] + T\nu_n QD[T] = Y_{n+\zeta} \,,$$

for some $Q \in \Lambda$. This means that $B_n \cap H_n$ capitulates in $B_{n+\zeta}$ for all $n \geqslant r$. Now assume that there exists some $m \geqslant r$ such that $B_m \cap H_m$ capitulates in $B_{m+\zeta-1}$. Working as before, one finds $\nu_{m,m+\zeta-1}(Y_m + D[T]) = Y_{m+\zeta-1}$ and, in particular, $\nu_{m,m+\zeta-1}D[T] \subseteq D \cap Y_{m+\zeta-1} = 0$. Using (2) again, we find $p^{\zeta-1}D[T] = 0$: a contradiction. □

Recall that X is pseudo-null if and only if $A_n = H_n$ for every $n \geqslant 0$ (see [8, Proposition 2]). Then, an immediate consequence of Proposition 2.2 is that, if X is pseudo-null, then B_n capitulates exactly in $A_{n+\zeta}$ for every value of $n \geqslant r$.

3 - The second criterion and Greenberg's Conjecture

This section is devoted to proving our second criterion, which in the case of a totally real field for which Leopold's Conjecture holds, links the nilpotency of the Galois group $\mathrm{Gal}(L(K)/k)$ with Greenberg's Conjecture (see Corollary 3.1).

If H is a group, for all $a, b \in H$, we put $a^b = b^{-1}ab$ and $[a, b] = a^{-1}b^{-1}ab$. If H_1, H_2 are subgroups of H we denote the *commutator group* of H_1 and H_2 by

$$[H_1, H_2] := \langle [h_1, h_2] \, : \, h_1 \in H_1, \, h_2 \in H_2 \rangle \, .$$

When H is a topological group we refer to $\overline{[H_1, H_2]}$ (the topological closure of $[H_1, H_2]$) as the *topological commutator group* of H_1 and H_2. Moreover we let

$$C_1(H) := H \quad \text{and} \quad C_i(H) := \overline{[H, C_{i-1}(H)]} \quad (\text{for any } i \geqslant 2)$$

denote the *lower central series* of H. If H is an abstract group, $C_i(H)$ has the obvious meaning. The group H is called *nilpotent* if there exists an integer i such that $C_{i+1}(H) = 1$ and the least integer i such that $C_{i+1}(H) = 1$ is called the *nilpotency class* of H. We use also the notation $H \leq_c G$ (resp. $H \leq_o G$) to indicate that H is a closed (resp. open) subgroup of a topological group G.

We begin with a simple observation: if a group G has a normal subgroup N such that $G/N \simeq \mathbb{Z}$, then there exists a subgroup H of G isomorphic to $\mathbb{Z}$ such that $G = N \rtimes H$. The following lemma deals with the case of a topological group.

Lemma 3.1. *Let G be a profinite group and N a closed normal subgroup such that G/N is a torsion-free procyclic group. Then there exists a procyclic subgroup H of G such that G is the topological semidirect product of H acting on N.*

Proof. Let $\alpha_1 \in G$ be a representative of a topological generator of G/N and let $H_1 := \overline{\langle \alpha_1 \rangle} \leq_c G$. Note that H_1N/N, being a subgroup of G/N, is torsion-free. By the canonical isomorphism (which is also an homeomorphism, because N is compact) between H_1N/N and $H_1/N \cap H_1$, we obtain that the last is torsion-free too. Hence (see, for example, [**13**, Section 2.7]) there exist disjoint sets of primes $S_1,\ S_2,\ S_3$ and an isomorphism

$$\phi : H_1 \xrightarrow{\simeq} \prod_{p\in S_1} \mathbb{Z}_p \times \prod_{p\in S_2} \mathbb{Z}_p \times \prod_{p\in S_3} \mathbb{Z}_p/p^{n(p)}\mathbb{Z}_p$$

(where $n(p)$ is a positive integer for every $p \in S_3$) such that

$$\phi(H_1 \cap N) = \prod_{p\in S_2} \mathbb{Z}_p \times \prod_{p\in S_3} \mathbb{Z}_p/p^{n(p)}\mathbb{Z}_p\ .$$

Define $H := \phi^{-1}(\prod_{p\in S_1} \mathbb{Z}_p)$ and let α be a topological generator of H: since $H \cap (H_1 \cap N) = 0$, it follows immediately that $H \cap N = 0$.

The natural projection $\pi : G \to G/N$ is a closed map since G is profinite and N is compact. Hence the equality $\alpha_1 N = \alpha N$ yields

$$G/N = \overline{\langle \alpha_1 N\rangle} = \overline{\langle \alpha N\rangle} = \overline{\langle \pi(\alpha)\rangle} = \overline{\pi(\langle \alpha\rangle)} = \pi(\overline{\langle \alpha\rangle}) = \pi(H)\ .$$

Therefore $G = HN$ and we have an isomorphism of groups between G and $N \rtimes H$. It is easy to check that the map

$$\theta : N \times H \longrightarrow G$$

given by $\theta(n,h) = nh$, is also a homeomorphism of topological spaces. □

Lemma 3.2. *Let G be a group and let $A \trianglelefteq G$, $B \le G$ be abelian subgroups such that $G = A \rtimes B$. Then*

$$C_i(G) = [A,{}_{i-1}B]$$

for all $i \geqslant 2$ (where $[A,{}_{i-1}B] = [[\dots[[A,B],B]\dots],B]$ with B appearing $i-1$ times).

Proof. We use induction on $i \geqslant 2$. Let $i = 2$ and $a,\ a_1 \in A, b,\ b_1 \in B$. A simple computation shows that

$$[ab, a_1b_1] = [a^b, b_1][(a_1^{-1})^{b_1}, b] \in [A,B]\,,$$

so $C_2(G) = [A,B]$.

Now assume the statement true for some $i \geqslant 2$ and observe that, if E is a normal subgroup of G contained in A, then $[E,G] = [E,B]$. Thus, since $C_i(G)$ is a normal subgroup of G contained in A,

$$C_{i+1}(G) = [C_i(G), G] = [[A,{}_{i-1}B], G] = [[A,{}_{i-1}B], B] = [A,{}_iB]\ .$$

□

Now we are ready to state and prove our second criterion for the finiteness of the Iwasawa module $X(K/k)$.

Theorem 3.1. *Let K/k be a $\mathbb{Z}_p$-extension of a number field k. The following conditions are equivalent:*

(a) $X = X(K/k)$ *is finite;*

(b) *the sequence $\{|B_n|\}_{n\in\mathbb{N}}$ is bounded and $\mathcal{G} := \mathrm{Gal}(L(K)/k)$ is nilpotent.*

Proof. By Lemma 3.1, we can write $\mathcal{G}$ as a semidirect product $\mathcal{G} = X \rtimes \Gamma$ (where Γ is isomorphic to $\mathbb{Z}_p$). We claim that $C_{i+1}(\mathcal{G}) = T^i X$ for every $i \geqslant 1$ and prove it with an induction argument on i.

If $i = 1$ the claim is true by, for example, [**14**, Lemma 13.14], so we assume that it holds for some $i \geqslant 1$. We have

$$C_{i+2}(\mathcal{G}) = \overline{[C_{i+1}(\mathcal{G}), \mathcal{G}]} = \overline{[T^i X, \mathcal{G}]}$$

and, applying Lemma 3.2, we obtain

$$C_{i+2}(\mathcal{G}) = \overline{[T^i X, \Gamma]}\,.$$

It is easy to show that $[T^i X, \Gamma] = T^{i+1}X$ and $T^{i+1}X$ is closed (since it is the image of a compact set). Thus $C_{i+2}(\mathcal{G}) = T^{i+1}X$ and the claim is proved.

(b) $\Rightarrow$ **(a)** Let $j \in \mathbb{N}$ be the nilpotency class of $\mathcal{G}$ (i.e., the least t such that $C_{t+1}(\mathcal{G}) = 1$): the previous claim yields $X = X[T^j]$. Now, since $\{|B_n|\}_{n\in\mathbb{N}}$ is bounded, we have $C_m \simeq X/TX$ (for every $m \gg n$, see the proof of Lemma 2.2) and in particular this means that X/TX is finite. Hence T does not divide the characteristic polynomial f_X of $X(K/k)$ (for a definition see, e.g., [**14**, Section 15.4]) and we conclude that T^j and $p^\eta f_X$ are two relatively prime annihilators of X for suitable $j, \eta \in \mathbb{N}$.

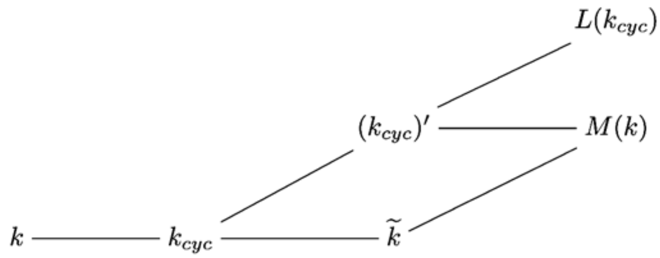
(a) $\Rightarrow$ **(b)** The boundedness of the orders of the B_n comes from the bound for the X_n. Since X is finite, there exists a $j \in \mathbb{N}$ such that $T^j X = 0$ which yields $C_{j+1}(\mathcal{G}) = 1$. □

Observe that in the previous theorem we can substitute, whenever convenient for applications, the hypothesis on the boundedness of the sequence $\{|B_n|\}_{n\in\mathbb{N}}$ with the one on $\{|C_n|\}_{n\in\mathbb{N}}$.

Corollary 3.1. *Let k be a totally real number field for which Leopold's Conjecture holds. Then Greenberg's Conjecture is true for k if and only if $\mathrm{Gal}(L(k_{cyc})/k)$ is nilpotent.*

P r o o f. For any number field k let $M(k)$ be the maximal abelian p-ramified pro-p-extension ok k, $\tilde{k}$ be the compositum of all the $\mathbb{Z}_p$-extensions of k and, in analogy to the definition of k'_n (i.e., the genus p-class field of k_n/k), we denote by $(k_{cyc})'$ the maximal abelian extension of k contained in $L(k_{cyc})$.

Considering the following diagram



we notice that the degree $[M(k) : \tilde{k}]$ is finite for every number field k by class field theory (see for example the proof of [**14**, Theorem 13.4]). Since, in our case, k is a totally real number field for which Leopold's Conjecture holds, we have $\tilde{k} = k_{cyc}$ and consequently $(k_{cyc})'$ is a finite extension of k_{cyc}.

Now, the sequence $\{|C_n|\}_{n\in\mathbb{N}}$ is bounded if and only if $|X/TX|$ is finite (see the proof of Lemma 2.2) and this means $[(k_{cyc})' : k_{cyc}] < \infty$, so the condition on the sequence $\{|B_n|\}_{n\in\mathbb{N}}$ in Theorem 3.1 is automatically satisfied in the setting we are considering. □

The results of this section seem to suggest that it could be worthwhile to study the lower central series of the Galois group $\mathcal{G} := \mathrm{Gal}(L(K)/k)$. It is reasonable to expect that (at least in some cases) it could provide a different approach to results similar to those obtained in [**5**].

References

[1] A. Bandini, *A note on p-ranks of class groups in $\mathbb{Z}_p$-extensions*, JP J. Algebra Number Theory Appl. **9** (2007), 95-103.

[2] A. Bandini, *Greenberg's conjecture and capitulation in $\mathbb{Z}_p^d$-extensions*, J. Number Theory **122** (2007), 121-134.

[3] A. Bandini, *Greenberg's conjecture for $\mathbb{Z}_p^d$-extensions*, Acta Arith. **108** (2003), 357-368.

[4] A. Bandini and F. Caldarola, *Stabilization for Iwasawa modules in $\mathbb{Z}_p$-extensions*, Rend. Semin. Mat. Univ. Padova, to appear.

[5] A. Bandini and F. Caldarola, *Stabilization in non-abelian Iwasawa theory*, Acta Arith. **169** (2015), 319-329.

[**6**] T. FUKUDA, *Remarks on $\mathbb{Z}_p$-extensions of number fields*, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), 264-266.

[**7**] R. GREENBERG, *Iwasawa theory - past and present*, Adv. Stud. Pure Math., **30**, Math. Soc. Japan, Tokyo 2001, 335-385.

[**8**] R. GREENBERG, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263-284.

[**9**] A. LANNUZEL and T. NGUYEN QUANG DO, *Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres*, Manuscripta Math. **102** (2000), 187-209.

[**10**] J. V. MINARDI, *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, Ph.D. Thesis, University of Washington, 1986.

[**11**] J. NEUKIRCH, A. SCHMIDT and K. WINGBERG, *Cohomology of number fields*, 2nd edition, Grundlehren Math. Wiss., **323**, Springer-Verlag, Berlin 2008.

[**12**] M. OZAKI, *Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions*, J. Reine Angew. Math. **602** (2007), 59-94.

[**13**] L. RIBES and P. ZALESSKII, *Profinite groups*, 2nd edition, Ergeb. Math. Grenzgeb. (3), **40**, Spinger-Verlag, Berlin 2010.

[**14**] L. C. WASHINGTON, *Introduction to cyclotomic fields*, 2nd edition, Grad. Texts in Math., **83**, Springer-Verlag, New York 1997.

FABIO CALDAROLA
University of Calabria,
Department of Mathematics and Computer Science
Cubo 31/B, ponte Pietro Bucci
Arcavacata di Rende, 87036, Italy
e-mail: caldarola@mat.unical.it