ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 122 (2007) 121–134

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Greenberg's conjecture and capitulation in $\mathbb{Z}_p^d$-extensions

Andrea Bandini [*,1]

Dipartimento di Matematica, Università della Calabria, Via P. Bucci, Cubo 30B, 87036 Arcavacata di Rende (CS), Italy

Received 10 September 2003; revised 26 January 2006

Available online 22 May 2006

Communicated by David Goss

Abstract

Let p be an odd prime. Let k be an algebraic number field and let $\tilde{k}$ be the compositum of all the $\mathbb{Z}_p$-extensions of k, so that $Gal(\tilde{k}/k) \simeq \mathbb{Z}_p^d$ for some finite d. We shall consider fields k with $Gal(k/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$. Building on known results for quadratic fields, we shall show that the Galois group of the maximal abelian unramified pro-p-extension of $\tilde{k}$ is pseudo-null for several such k's, thus confirming a conjecture of Greenberg. Moreover we shall see that pseudo-nullity can be achieved quite early, namely in a $\mathbb{Z}_p^2$-extension, and explain the consequences of this on the capitulation of ideals in such extensions.

Keywords: $\mathbb{Z}_p$-extensions; Iwasawa theory; Quadratic fields

1. Introduction

Let K be a $\mathbb{Z}_p^d$-extension of a number field k ($d \geqslant 1$). For any $n \geqslant 0$ let k_n be the subfield of K such that $Gal(k_n/k) \simeq (\mathbb{Z}/p^n\mathbb{Z})^d$. Let A_{k_n} be the p-part of the ideal class group of k_n. Let

$$N_{k_m/k_n} : k_m \to k_n \quad \text{and} \quad i_{k_n/k_m} : k_n \hookrightarrow k_m$$

* Address for correspondence: Via di Parigi 5/A, 56124 Pisa, Italy.
E-mail address: bandini@mail.dm.unipi.it.

1 Partially supported by a research grant from the University of Pisa.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2006.04.004

be the natural norm and inclusion for any $m \geqslant n \geqslant 0$. They induce the corresponding maps on ideal class groups. The A_{k_n} form a direct system with respect to the inclusion maps and a projective system with respect to the norms. Hence we can define

$$\varinjlim_n A_{k_n} \stackrel{\text{def}}{=} A_K \quad \text{and} \quad \varprojlim_n A_{k_n} \stackrel{\text{def}}{=} Y_K.$$

Let $\tau_1, \dots, \tau_d$ be independent topological generators of $Gal(K/k)$. Then the map $\tau_i \to T_i + 1$ for $i = 1, \dots, d$ defines a noncanonical isomorphism

$$\mathbb{Z}_p\left[\!\left[Gal(K/k)\right]\!\right] \simeq \mathbb{Z}_p[\![T_1, \dots, T_d]\!] \stackrel{\text{def}}{=} \Lambda_d,$$

see [17]. The group Y_K is canonically isomorphic to $Gal(L_K/K)$ where L_K is the maximal abelian unramified pro-p-extension of K. This isomorphism enables us to define an action of $Gal(K/k)$ on Y_K via conjugation and Y_K can be seen as a Λ_d-module. Greenberg, in [3], has proved that it is a finitely generated torsion Λ_d-module. A finitely generated Λ_d-torsion module M is called *pseudo-null* if it has at least two relatively prime annihilators. We shall write $M \sim_{\Lambda_d} 0$ to indicate that M is a pseudo-null Λ_d-module.

We will study the following:

Conjecture 1. [6, Conjecture 3.5] *Let $\tilde{k}$ be the compositum of all the $\mathbb{Z}_p$-extensions of k and let $Gal(\tilde{k}/k) \simeq \mathbb{Z}_p^n$. Then $Y_{\tilde{k}}$ is a pseudo-null Λ_n-module.*

This conjecture has been verified for many real quadratic fields (see [2,9] and the references there) and many imaginary quadratic fields (see [13]). Recently the case of certain cyclotomic fields has been studied in [11,12]. In [1], building on quadratic fields, we were able to prove Greenberg's conjecture for real fields with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$ and for some imaginary biquadratic fields. In that paper we had some restrictive hypothesis on the behaviour of the prime p in k, namely we did not want p to split completely. This limitation prevented us from building larger imaginary extensions. Now with our new Theorem 9 we are able to overcome this difficulty and to provide a large class of imaginary fields with Galois group $(\mathbb{Z}/2\mathbb{Z})^n$ for which the conjecture holds (Section 4).

Regarding capitulation of ideals, for a $\mathbb{Z}_p$-extension a Λ_1-module is pseudo-null if and only if it is finite. Using a well-known theorem of Iwasawa [8, Theorem 10], Greenberg proved that

$$Y_K \sim_{\Lambda_1} 0 \quad \Longleftrightarrow \quad A_K = 0$$

[4, Proposition 2]. In Section 2 we give a short proof for a partial generalization of such statement which can be applied to all the fields described above (see also [7]). We shall show that for a $\mathbb{Z}_p^d$-extension K/k, containing the cyclotomic $\mathbb{Z}_p$-extension of k,

$$Y_K \sim_{\Lambda_d} 0 \quad \Longrightarrow \quad A_K = 0.$$

The importance of this statement relies on the fact that it relates the pseudo-nullity of Y_K with capitulation of ideals in the extension K/k, which is an interesting but still quite mysterious phenomenon. Thus it provides further motivation for the study of Greenberg's conjecture.

Similar and more general results have been proved by Lannuzel and Nguyen Quang Do in [10] for nontotally real fields k and for $K = \tilde{k}$ with an additional hypothesis on the decomposition groups of the primes of k lying above p. Therefore we expect capitulation of ideals in $\tilde{k}$ but our examples in Section 4 will show how it is often possible to obtain capitulation at a lower (almost "minimal") level.

In the rest of the paper we will use the following notations. For any number field k let:

k_{cyc} the cyclotomic $\mathbb{Z}_p$-extension of k;

$\tilde{k}$ the compositum of all the $\mathbb{Z}_p$-extensions of k;

L_k the maximal abelian unramified p-extension of k;

$A_k \simeq Gal(L_k/k)$ the p-part of the ideal class group of k.

We will use the same notations even for fields which have infinite degree over $\mathbb{Q}$, for example: if $k_{\text{cyc}} = \bigcup k_n$ then $L_{k_{\text{cyc}}} = \bigcup L_{k_n}$ and

$$A_{k_{\text{cyc}}} = \varinjlim_n A_{k_n}, \qquad Y_{k_{\text{cyc}}} = \varprojlim_n A_{k_n} \simeq Gal(L_{k_{\text{cyc}}}/k_{\text{cyc}}),$$

where the direct limit is taken on the inclusion maps and the projective limit is on the norms.

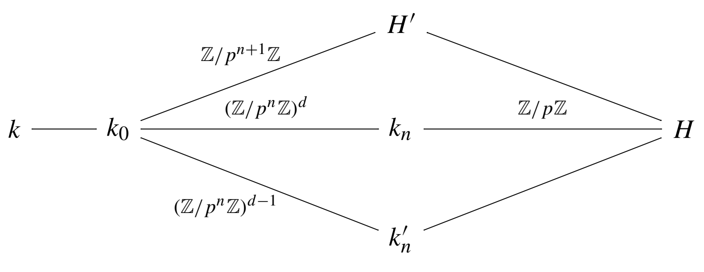
2. Pseudo-nullity and capitulation

Let k be a number field and let K/k be a $\mathbb{Z}_p^d$-extension with $d \geqslant 2$. In this section we briefly describe a relation between the pseudo-nullity of Y_K and the triviality of A_K.

Proposition 2. $Y_K \sim_{\Lambda_d} 0 \implies A_K \sim_{\Lambda_d} 0$.

Proof. Let k_0 be the maximal unramified extension of k contained in K, i.e., $k_0 = L_k \cap K$. Let k_n be such that $k_0 \subseteq k_n \subset K$ and $Gal(k_n/k_0) \simeq (\mathbb{Z}/p^n\mathbb{Z})^d$. Then $\bigcup k_n = K$ and obviously A_K is the direct limit of the A_{k_n}. We shall prove that there is no nontrivial unramified extension of k_n in K.

Fix an n and let H be any subfield of K such that $Gal(H/k_n) \simeq \mathbb{Z}/p\mathbb{Z}$. One can write $H = H'k'_n$, where $Gal(H'/k_0) \simeq \mathbb{Z}/p^{n+1}\mathbb{Z}$ and $Gal(k'_n/k_0) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{d-1}$. Consider a $\mathbb{Z}_p$-extension of k_0 containing H' and contained in K.



By the definition of k_0 there exists a prime $\mathfrak{p}$ in k_0 lying above p which totally ramifies in H'. Indeed some prime has to start ramification at k_0 and, in a $\mathbb{Z}_p$-extension, a prime is totally ramified from the level in which its ramification starts. Hence the inertia group of $\mathfrak{p}$ in $Gal(H'/k_0)$ is cyclic of order p^{n+1}. For the same prime $\mathfrak{p}$ the inertia group in $Gal(k'_n/k_0)$ is at most $(\mathbb{Z}/p^n\mathbb{Z})^{d-1}$ so $\mathfrak{p}$ has to be ramified in $H'k'_n/k_n$, i.e., in H/k_n.

Therefore, by class field theory, the norm maps $N_{k_m/k_n}: A_{k_m} \to A_{k_n}$ are surjective for all $m \geqslant n \geqslant 0$ and, taking the inverse limit, $N_{K/k_n}: Y_K \to A_{k_n}$ is surjective for all n. Hence the annihilators of Y_K annihilate A_{k_n} for any $n \geqslant 0$ and eventually they annihilate A_K as well. It immediately follows that

$$Y_K \sim_{\Lambda_d} 0 \quad \Longrightarrow \quad A_K \sim_{\Lambda_d} 0. \qquad \square$$

Let M_K be the maximal abelian pro-p-extension of K unramified outside p and let $X_K = Gal(M_K/K)$. Then we can define, via conjugation as usual, a Λ_d-module structure on X_K and we have the following theorem due to Greenberg.

Theorem 3. *If $K \supset k_{\mathrm{cyc}}$, the cyclotomic $\mathbb{Z}_p$-extension of k, then X_K contains no nontrivial pseudo-null Λ_d-submodules.*

Proof. See [5, Theorem 2] or, for a different approach, [14]. $\square$

Remark 4. In [5] the theorem is proved under the hypothesis of Leopoldt's conjecture for k. In all our examples in Section 4, k will be an abelian number field and Leopoldt's conjecture is known to hold for them. Anyway the hypothesis $k_{\mathrm{cyc}} \subset K$ used in [14] is, in general, more suitable for our purposes.

Let $\hat{A}_K = Hom(A_K, \mu_{p^\infty})$ be the Kummer dual of A_K and let χ be the cyclotomic character describing the action of $Gal(K/k)$ on μ_{p^∞}, i.e., $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for any $\sigma \in Gal(K/k)$ and $\zeta \in \mu_{p^\infty}$. Then $\hat{A}_K$ has a natural Λ_d-module structure defined by

$$\gamma\varphi(\cdot) = \gamma\big(\varphi\big(\gamma^{-1}\cdot\big)\big) = \big(\varphi\big(\gamma^{-1}\cdot\big)\big)^{\chi(\gamma)},$$

i.e., the natural action on μ_{p^∞} or, equivalently, the twist by χ of the trivial action on $\mathbb{Q}/\mathbb{Z}$.

Proposition 5. *Assume that $k \supset \mu_p$, the pth roots of unity, and that $K \supset k_{\mathrm{cyc}}$. Let $N_K = K(\{\sqrt[p^n]{\varepsilon}\colon\ n \geqslant 0,\ \varepsilon \text{ unit in } O_K\})$ where O_K is the ring of integers of K. Then $\hat{A}_K$ is isomorphic to $Gal(M_K/N_K)$ as Λ_d-module.*

Proof. The hypothesis yields $\mu_{p^\infty} \subset K$ and the proposition is a standard consequence of Kummer theory (see also [12]). Explicitly we can describe the isomorphism as follows. Let $\sqrt[p^n]{a}$ be a generator of M_K. Since $k_{\mathrm{cyc}} \subset K$, primes above p are ramified to an arbitrary high power in K/k. Thus the ideal (a) is the p^nth power of some ideal $\mathfrak{c}$ in O_K. Let c be the class in A_K representing $\mathfrak{c}$. We define $\eta : \hat{A}_K \to X_K$ by

$$\big(\eta(\varphi)\big)\big(\sqrt[p^n]{a}\big) = \varphi(c)\big(\sqrt[p^n]{a}\big).$$

It is not hard to check that $\operatorname{Im}\eta$ fixes N_K and that η provides the desired isomorphism of Λ_d-modules. $\square$

Theorem 6. *Let k be a number field and let K/k be a $\mathbb{Z}_p^d$-extension such that $k_{\mathrm{cyc}} \subset K$. Then $Y_K \sim_{\Lambda_d} 0 \Longrightarrow A_K = 0$.*

Proof. By Proposition 2 one has $A_K \sim_{\Lambda_d} 0$ and then $\hat{A}_K \sim_{\Lambda_d} 0$.

If k contains μ_p then, by Proposition 5, $\hat{A}_K$ embeds in X_K which, by Theorem 3, contains no nontrivial pseudo-null submodules. Therefore $\hat{A}_K \sim_{\Lambda_d} 0 \implies \hat{A}_K = 0$ and eventually $A_K = 0$.

If k does not contain μ_p, consider the $\mathbb{Z}_p^d$-extension $K(\mu_p)/k(\mu_p)$. As above one gets an injection $\hat{A}_{K(\mu_p)} \hookrightarrow X_{K(\mu_p)}$.

Let k_n be finite subextensions of K such that $\bigcup k_n = K$. All extensions $k_n(\mu_p)/k_n$ have the same Galois group and are totally ramified at primes lying above p so, by class field theory, the norms $N : A_{k_n(\mu_p)} \to A_{k_n}$ are surjective. Taking the direct limit one gets a surjection $N : A_{K(\mu_p)} \to A_K$. This, by duality, yields an injection $\hat{A}_K \hookrightarrow \hat{A}_{K(\mu_p)}$. Therefore $\hat{A}_K$ embeds in $X_{K(\mu_p)}$ and, using Theorem 3 as in the previous case, this implies $A_K = 0$. □

3. Main theorems

Greenberg's Conjecture 1 and our Theorem 6 tell us to expect capitulation in $\tilde{k}$, with no additional hypothesis on k or $\tilde{k}$, but this is not the only case.

For a nontrivial example we can look at biquadratic imaginary fields. Let $Gal(k/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Let F, E, H be the three quadratic subextensions of k and assume that H is the real one. We recall that for abelian number fields $Gal(\tilde{k}/k) \simeq \mathbb{Z}_p^{r_2+1}$ where r_2 is the number of pairs of complex embeddings of k (this is true in general assuming Leopoldt's conjecture for k, see [18, Theorem 13.4]).

Assume $p \neq 2$. In [1] we proved the following theorems (Theorem 3.2 and Theorem 3.3 there):

Theorem 7. *Assume that*:

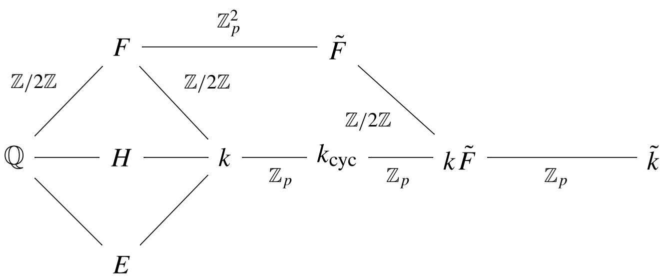
(1) *p does not split in k*;
(2) *Conjecture* 1 *holds for F and H, i.e., $Y_{\tilde{F}} \sim_{\Lambda_2} 0$ and $Y_{H_{\mathrm{cyc}}} \sim_{\Lambda_1} 0$*;
(3) *$Y_{E_{\mathrm{cyc}}} \sim_{\Lambda_1} 0$.*

Then $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$.

Theorem 8. *Assume that*:

(1) *$\tilde{F}/F_{\mathrm{cyc}}$ is unramified*;
(2) *Conjecture* 1 *holds for F and H, i.e., $Y_{\tilde{F}} \sim_{\Lambda_2} 0$ and $Y_{H_{\mathrm{cyc}}} \sim_{\Lambda_1} 0$*;
(3) *$Y_{E_{\mathrm{cyc}}} \sim_{\Lambda_1} 0$.*

Then $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$.



Proof. (*Sketch*) The action of $Gal(k/F)$ on $Y_{k\tilde{F}}$ gives a decomposition

$$Y_{k\tilde{F}} \simeq Y^+_{k\tilde{F}} \oplus Y^-_{k\tilde{F}}.$$

It is easy to see that $Y^+_{k\tilde{F}} \simeq Y_{\tilde{F}}$ so this is pseudo-null. For the minus part one can prove that

$$Y^-_{k\tilde{F}}/T_2 Y^-_{k\tilde{F}} \simeq Gal(L_{k_{\mathrm{cyc}}}/L_{k_{\mathrm{cyc}}} \cap k\tilde{F})^- \hookrightarrow Y_{H_{\mathrm{cyc}}} \oplus Y_{E_{\mathrm{cyc}}} \quad \text{(Theorem 7)}, \quad \text{or}$$

$$Y^-_{k\tilde{F}}/T_2 Y^-_{k\tilde{F}} \simeq Gal(L_{k_{\mathrm{cyc}}}/k\tilde{F})^- \hookrightarrow Y_{H_{\mathrm{cyc}}} \oplus Y_{E_{\mathrm{cyc}}} \quad \text{(Theorem 8)}.$$

In both cases $Y^-_{k\tilde{F}}/T_2 Y^-_{k\tilde{F}}$ is finite, i.e., a pseudo-null Λ_1-module. By [16, Lemme 2] (see also [1, Proposition 3.1]) this yields $Y^-_{k\tilde{F}} \sim_{\Lambda_2} 0$ and eventually $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$. □

Note that $Gal(\tilde{k}/k) \simeq \mathbb{Z}_p^3$ and $Gal(\tilde{F}/F) \simeq \mathbb{Z}_p^2$. Hence $Gal(k\tilde{F}/k) \simeq \mathbb{Z}_p^2$ and we obtain pseudo-nullity and capitulation at a level which is lower than the expected one.

In [1] we thought that this might depend on condition (3), i.e., $Y_{E_{\mathrm{cyc}}} \sim_{\Lambda_1} 0$ which implies the conjecture for E but it is not equivalent to it. If p splits in E, (3) does not hold so, in [1], we did not consider the case in which p splits completely in k. But now we are able to prove a theorem which applies to that case and which will allow us to go further in the verification of the conjecture for larger fields (see Section 4 for some examples).

Theorem 9. *Assume that*:

(1) *p totally splits in k*;
(2) $Y_{F_{\mathrm{cyc}}} \simeq Y_{E_{\mathrm{cyc}}} \simeq \mathbb{Z}_p$;
(3) *Conjecture* 1 *holds for H, i.e.,* $Y_{H_{\mathrm{cyc}}} \sim_{\Lambda_1} 0$.

Then $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$.

Proof. Let $Gal(\tilde{k}/k\tilde{F}) \simeq \overline{\langle \tau_3 \rangle}$ and $Gal(k\tilde{F}/k_{\mathrm{cyc}}) \simeq \overline{\langle \tau_2 \rangle}$ with $\tau_i - 1 \to T_i$ in the isomorphism $\Lambda_3 \simeq \mathbb{Z}_p[\![Gal(\tilde{k}/k)]\!]$.

Then

$$Y_{\tilde{k}}/(T_2, T_3)Y_{\tilde{k}} \simeq Gal(L_0/\tilde{k}),$$

where L_0 is the maximal abelian extension of k_{cyc} contained in $L_{\tilde{k}}$, the maximal abelian unramified pro-p-extension of $\tilde{k}$ (see the notations at the end of the introduction).

As in [1, Theorem 2.2] one can prove that

$$Y_{k_{\mathrm{cyc}}} \simeq Y_{F_{\mathrm{cyc}}} \oplus Y_{H_{\mathrm{cyc}}} \oplus Y_{E_{\mathrm{cyc}}}.$$

Hence, by hypothesis (2),

$$Y_{k_{\mathrm{cyc}}} \simeq \mathbb{Z}_p^2 \oplus Y_{H_{\mathrm{cyc}}}.$$

Since $\tilde{F}/F_{\text{cyc}}$ and $\tilde{E}/E_{\text{cyc}}$ are unramified one has that $\tilde{k}/k_{\text{cyc}}$ is unramified as well. Therefore $L_{\tilde{k}}/\tilde{k}$ unramified $\Longrightarrow L_0/k_{\text{cyc}}$ is abelian and unramified, i.e., $L_0 = L_{k_{\text{cyc}}}$.

Since $Gal(\tilde{k}/k_{\text{cyc}}) \simeq \mathbb{Z}_p^2$ one has

$$Y_{\tilde{k}}/(T_2, T_3)Y_{\tilde{k}} \simeq Gal(L_{k_{\text{cyc}}}/\tilde{k}) \simeq Y_{H_{\text{cyc}}}$$

which, by hypothesis (3), is finite.

This, by [16, Lemme 2], yields

$$Y_{\tilde{k}}/T_3 Y_{\tilde{k}} \sim_{\Lambda_2} 0.$$

Moreover

$$Y_{\tilde{k}}/T_3 Y_{\tilde{k}} \simeq Gal(L_1/\tilde{k}),$$

where L_1 is the maximal abelian extension of $k\tilde{F}$ contained in $L_{\tilde{k}}$. But again since $\tilde{k}/k\tilde{F}$ is unramified one has $L_1 = L_{k\tilde{F}}$. Hence one has an exact sequence

$$0 \to Gal(L_{k\tilde{F}}/\tilde{k}) \to Gal(L_{k\tilde{F}}/k\tilde{F}) \to Gal(\tilde{k}/k\tilde{F}) \to 0,$$

i.e.,

$$0 \to Y_{\tilde{k}}/T_3 Y_{\tilde{k}} \to Y_{k\tilde{F}} \to \mathbb{Z}_p \to 0.$$

Since the elements on the left and on the right are pseudo-null as Λ_2-modules one gets $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$. □

Remark 10. In the classical language of Iwasawa λ-invariants for $\mathbb{Z}_p$-extensions our hypothesis (2) simply means $\lambda(F_{\text{cyc}}/F) = \lambda(E_{\text{cyc}}/E) = 1$ and it yields the conjecture for F and E. Indeed let T_2 correspond to a topological generator of $Gal(\tilde{F}/F_{\text{cyc}})$ (respectively $Gal(\tilde{E}/E_{\text{cyc}})$). Then, as in Theorem 9,

$$Y_{\tilde{F}}/T_2 Y_{\tilde{F}} \simeq Gal(L_{F_{\text{cyc}}}/\tilde{F}) = 0 \quad \big(\text{respectively } Y_{\tilde{E}}/T_2 Y_{\tilde{E}} \simeq Gal(L_{E_{\text{cyc}}}/\tilde{E}) = 0\big),$$

by hypothesis (2). Hence Nakayama's Lemma yields $Y_{\tilde{F}} = 0$ (respectively $Y_{\tilde{E}} = 0$).

Remark 11. One way to check hypothesis (2) for an imaginary quadratic field F is the following. Let O_F be the ring of integers of F and let $pO_F = \mathfrak{p}\bar{\mathfrak{p}}$. Let h_F be the class number of F and let $\bar{\mathfrak{p}}^{h_F} = (\alpha)$ for some $\alpha \in O_F$. Then

$$\lambda(F_{\text{cyc}}/F) = 1 \quad \Longleftrightarrow \quad \alpha \notin \left(\mathbb{Q}_p^*\right)^p$$

(see [13, Lemma 3.4]).

The following theorem and its corollary will be the main tools for the verification of the conjecture for several biquadratic fields and even for larger fields.

Theorem 12. *Let $Gal(\tilde{k}/k) \simeq \mathbb{Z}_p^n$ and let $K \subset \tilde{k}$ be such that $Gal(K/k) \simeq \mathbb{Z}_p^d$ for some $2 \leqslant d < n$. Assume that*:

(1) *for any prime $\mathfrak{p}$ of k dividing p the decomposition group $D(\mathfrak{p})$ of $\mathfrak{p}$ in $Gal(K/k)$ has $\mathbb{Z}_p$-rank at least* 2;
(2) $Y_K \sim_{\Lambda_d} 0$.

Then the conjecture holds for k.

Proof. Let $\tau_{d+1}, \ldots, \tau_n$ be independent topological generators of $Gal(\tilde{k}/K)$ corresponding to the variables $T_{d+1}, \ldots, T_n$ in Λ_n. Then

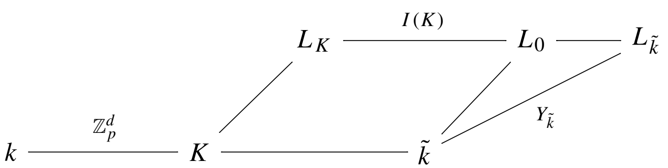
$$Y_{\tilde{k}}/(T_{d+1}, \ldots, T_n)Y_{\tilde{k}} \simeq Gal(L_0/\tilde{k}),$$

where L_0 is the maximal abelian extension of K contained in $L_{\tilde{k}}$.

Let $\mathfrak{p}_K$ be a prime of K lying above p and let $I(\mathfrak{p}_K)$ be its inertia group in $Gal(L_0/K)$. Since $L_0/\tilde{k}$ is unramified $I(\mathfrak{p}_K)$ embeds in $Gal(\tilde{k}/K)$ and it is isomorphic to $\mathbb{Z}_p^l$ for some $0 \leqslant l \leqslant n-d$. Moreover let

$$I(K) = \sum_{\mathfrak{p}_K | p} I(\mathfrak{p}_K),$$

then the fixed field of $I(K)$ is the maximal unramified extension of K contained in L_0, i.e., $Fix\, I(K) = L_K$.



Let $\mathfrak{p}$ be a prime of k lying below $\mathfrak{p}_K$ and let $\nu_1(\mathfrak{p})$, $\nu_2(\mathfrak{p})$ be two independent elements of its decomposition group $D(\mathfrak{p}) \subseteq Gal(K/k)$. The group $D(\mathfrak{p})$ fixes $\mathfrak{p}_K$ hence it acts via conjugation on $I(\mathfrak{p}_K)$ and it acts trivially because $I(\mathfrak{p}_K)$ embeds in $Gal(\tilde{k}/K)$ and $Gal(\tilde{k}/k)$ is abelian. Therefore $\nu_1(\mathfrak{p}) - 1$ and $\nu_2(\mathfrak{p}) - 1$ correspond to two relatively prime elements of Λ_d which annihilate $I(\mathfrak{p}_K)$. The same holds for all primes of K dividing $\mathfrak{p}$. Hence one has

$$\sum_{\mathfrak{p}_K | \mathfrak{p}} I(\mathfrak{p}_K) \sim_{\Lambda_d} 0.$$

Finally, since a finite sum of pseudo-null modules is pseudo-null, we have

$$I(K) = \sum_{\mathfrak{p}_K | p} I(\mathfrak{p}_K) = \sum_{\mathfrak{p} | p} \sum_{\mathfrak{p}_K | \mathfrak{p}} I(\mathfrak{p}_K) \sim_{\Lambda_d} 0.$$

By Galois theory there is an exact sequence

$$0 \to Gal(L_0/L_K) \to Gal(L_0/K) \to Gal(L_K/K) \to 0$$

which corresponds to

$$0 \to I(K) \to Gal(L_0/K) \to Y_K \to 0.$$

Thus $Gal(L_0/K) \sim_{\Lambda_d} 0$ and, in particular,

$$Gal(L_0/\tilde{k}) \simeq Y_{\tilde{k}}/(T_{d+1}, \dots, T_n)Y_{\tilde{k}} \sim_{\Lambda_d} 0.$$

Applying repeatedly Lemme 2 of [16] one eventually gets $Y_{\tilde{k}} \sim_{\Lambda_n} 0$. □

Corollary 13. *Let F be a quadratic imaginary field and let k/F be a field extension. Let $Gal(\tilde{k}/k) \simeq \mathbb{Z}_p^n$. If $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$ then $Y_{\tilde{k}} \sim_{\Lambda_n} 0$.*

Proof. It is a well-known fact that in $\tilde{F}/F$ the hypothesis on the decomposition group is verified. So it is verified in $k\tilde{F}/k$ as well and the previous theorem applies with $K = k\tilde{F}$. □

Remark 14. The three theorems on biquadratic fields apply to the cases in which p does not split in k (Theorem 7), p splits in F but not in H or E (Theorem 8) and p splits completely in k (Theorem 9). In all the cases described by the theorems we can prove Greenberg's conjecture using Theorem 12.

Remark 15. Hypothesis (1) in Theorem 12 holds for $K = \tilde{k}$ if $k \supset \mu_p$ or if k contains an imaginary Galois extension of $\mathbb{Q}$ (see [10, Théorème 3.2]).

3.1. Examples

Many examples for Theorems 7 and 8 can be found in [1]. We give examples for Theorem 9 with $p = 3$, $F = \mathbb{Q}(\sqrt{-d})$ and $E = \mathbb{Q}(\sqrt{-l})$. The hypothesis on $H = \mathbb{Q}(\sqrt{ld})$ has been verified in several papers (see [2,9,15]). When 3 divides the class number hypothesis (2) has been checked in [13] and we are taking our values of l and d from [13, Table 6.1]. In the range $2 \leqslant l, d \leqslant 500$ we can take l and d within the following set of numbers: 23, 26, 29, 38, 53, 59, 83, 89, 110, 170, 182, 233, 293, 335, 431, 434, 473, 491, 497.

If 3 does not divide the class number we can use direct computations as in Remark 11.

As an example for $F_1 = \mathbb{Q}(\sqrt{-35})$, $F_2 = \mathbb{Q}(\sqrt{-95})$ and $F_3 = \mathbb{Q}(\sqrt{-299})$ one has:

(i) $h_{F_1} = 2$, $h_{F_2} = h_{F_3} = 8$;
(ii) $3\mathcal{O}_{F_1} = (3, 1+\sqrt{-35})(3, 1-\sqrt{-35})$, $3\mathcal{O}_{F_2} = (3, 1+\sqrt{-95})(3, 1-\sqrt{-95})$ and $3\mathcal{O}_{F_3} = (3, 1+\sqrt{-299})(3, 1-\sqrt{-299})$;
(iii) $(3, 1-\sqrt{-35})^2 = (\frac{1-\sqrt{-35}}{2})$, $(3, 1-\sqrt{-95})^8 = (71+4\sqrt{-95})$ and $(3, 1-\sqrt{-299})^8 = (\frac{137-5\sqrt{-299}}{2})$;
(iv) $\sqrt{-35} = 1 + 3^2 + 2\cdot 3^3 + 2\cdot 3^5 + 3^6 + \cdots$, $\sqrt{-95} = 1 + 2\cdot 3 + 3^2 + 3^3 + 2\cdot 3^5 + 2\cdot 3^7 + 3^8 + \cdots$ and $\sqrt{-299} = 1 + 3 + 2\cdot 3^2 + 2\cdot 3^3 + 3^5 + 2\cdot 3^6 + 3^7 + 3^8 + \cdots$ in $\mathbb{Q}_3$.

Let v_3 be the 3-adic valuation. It is easy to check that

$$v_3\left(\frac{1-\sqrt{-35}}{2}\right) = 2 \quad \text{and} \quad v_3(71+4\sqrt{-95}) = v_3\left(\frac{137-5\sqrt{-299}}{2}\right) = 8.$$

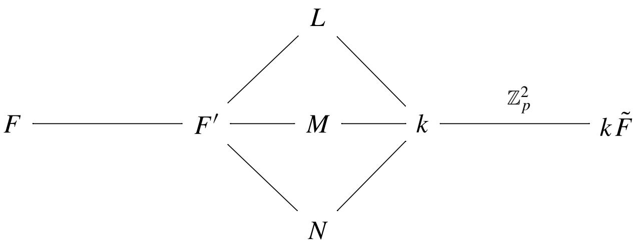
Hence these are not cubes in $\mathbb{Q}_3$ and this yields hypothesis (2) for F_1, F_2 and F_3.

In the same way one can prove hypothesis (2) for $\mathbb{Q}(\sqrt{-d})$, $d = 2, 5, 11, 14, 17$ (and many more, we are only mentioning the ones which are going to be used in the examples in Section 4).

Remark 16. In all these cases $Y_{k_{\mathrm{cyc}}}$ is not finite which yields $A_{k_{\mathrm{cyc}}} \neq 0$. So $k\tilde{F}$ is the "minimal" extension in which ideals capitulate. To our knowledge there are no known examples of imaginary biquadratic fields for which capitulation of ideals can be delayed further, i.e., examples in which $A_{k\tilde{F}} \neq 0$ and $A_{\tilde{k}} = 0$.

4. Application: fields with Galois group $(\mathbb{Z}/2\mathbb{Z})^n$

Iterating the application of the three theorems on biquadratic fields given in the previous section it is possible to build larger extensions for which Greenberg's conjecture holds. The general situation is the following:



where F is an imaginary quadratic field, F' is an extension of F, k is a biquadratic extension of F' and L, M, N are the three quadratic extensions lying between F' and k.

If p is odd then using the action of $Gal(k/F')$ on $Y_{k\tilde{F}}$ we obtain a decomposition

$$Y_{k\tilde{F}} \simeq \bigoplus_{i=0}^{3} Y_{k\tilde{F}}^{\chi_i},$$

where the χ_i are the characters of $Gal(k/F')$ and, for any i, $Y_{k\tilde{F}}^{\chi_i}$ is the submodule of $Y_{k\tilde{F}}$ on which $Gal(k/F')$ acts via χ_i or, equivalently, the submodule of $Y_{k\tilde{F}}$ on which $Ker\,\chi_i$ acts trivially. Working as in [1] it is not hard to prove that this decomposition corresponds to

$$Y_{k\tilde{F}} \simeq Y_{F'\tilde{F}} \oplus Y_{L\tilde{F}} \oplus Y_{M\tilde{F}} \oplus Y_{N\tilde{F}}.$$

Hence if all the four modules on the right are pseudo-null as Λ_2-modules one gets $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$ which has the following consequences:

1. by Corollary 13 it yields Greenberg's conjecture for k;
2. by Theorem 6 it yields $A_{k\tilde{F}} = 0$, i.e., ideals capitulate in the $\mathbb{Z}_p^2$-extension $k\tilde{F}$ which is, in general, much smaller than $\tilde{k}$.

4.1. Examples

In this section we consider $p = 3$ and give some examples of the procedure described above. We take $F = \mathbb{Q}(\sqrt{-2})$ as "base field." We start with $F' = F$ and take L, M, N among the biquadratic fields $F(\sqrt{-d})$ which can be found using Theorems 8 and 9. To apply those theorems we need:

(a) $d \equiv 0, 1 \pmod 3$ and 3 does not divide the class number of $\mathbb{Q}(\sqrt{-d})$ (this yields $Y_{\mathbb{Q}(\sqrt{-d})_{\text{cyc}}} = 0$), for Theorem 8;
(b) d among the values given in Section 3.1, for Theorem 9.

With this choice if we let H be any of the fields F', L, M, N and k listed in Table 1, we have $Y_{H\tilde{F}} \sim_{\Lambda_2} 0$ (note that $[k : \mathbb{Q}] = 8$). After the first step the iteration for fields of larger degree does not require the use of the theorems anymore and is straightforward. A first iteration provides fields k of degree 16 (Table 2), and a second one gives fields of degree 32 (Table 3). Starting with a different F the same results can be proved for many more fields. An example for $F = \mathbb{Q}(\sqrt{-23})$ (again ending with a field of degree 32) is provided in Tables 4, 5 and 6.

The class numbers of the fields involved in the tables can be found, for example, at the website http://tnt.math.metro-u.ac.jp.

Table 1
$F = F' = \mathbb{Q}(\sqrt{-2})$

F'	L	M	N	k	F'	L	M	N	k
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-6})$ thm 8	$F(\sqrt{-1})$ thm 8	$F(\sqrt{-3}, \sqrt{-1})$	F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-57})$ thm 8	$F(\sqrt{-38})$ thm 9	$F(\sqrt{-3}, \sqrt{19})$
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-30})$ thm 8	$F(\sqrt{-5})$ thm 9	$F(\sqrt{-3}, \sqrt{-5})$	F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-138})$ thm 8	$F(\sqrt{-23})$ thm 9	$F(\sqrt{-3}, \sqrt{-23})$
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-15})$ thm 8	$F(\sqrt{-10})$ thm 8	$F(\sqrt{-3}, \sqrt{5})$	F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-69})$ thm 8	$F(\sqrt{-46})$ thm 8	$F(\sqrt{-3}, \sqrt{23})$
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-42})$ thm 8	$F(\sqrt{-7})$ thm 8	$F(\sqrt{-3}, \sqrt{-7})$	F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-210})$ thm 8	$F(\sqrt{-35})$ thm 9	$F(\sqrt{-3}, \sqrt{-35})$
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-21})$ thm 8	$F(\sqrt{-14})$ thm 9	$F(\sqrt{-3}, \sqrt{7})$	F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-105})$ thm 8	$F(\sqrt{-70})$ thm 8	$F(\sqrt{-3}, \sqrt{35})$
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-66})$ thm 8	$F(\sqrt{-11})$ thm 9	$F(\sqrt{-3}, \sqrt{-11})$	F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-330})$ thm 8	$F(\sqrt{-55})$ thm 8	$F(\sqrt{-3}, \sqrt{-55})$
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-33})$ thm 8	$F(\sqrt{-22})$ thm 8	$F(\sqrt{-3}, \sqrt{11})$	F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-165})$ thm 8	$F(\sqrt{-110})$ thm 9	$F(\sqrt{-3}, \sqrt{55})$
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-78})$ thm 8	$F(\sqrt{-13})$ thm 8	$F(\sqrt{-3}, \sqrt{-13})$	F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-570})$ thm 8	$F(\sqrt{-95})$ thm 9	$F(\sqrt{-3}, \sqrt{-95})$
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-39})$ thm 8	$F(\sqrt{-26})$ thm 9	$F(\sqrt{-3}, \sqrt{13})$	F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-285})$ thm 8	$F(\sqrt{-190})$ thm 8	$F(\sqrt{-3}, \sqrt{95})$
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-102})$ thm 8	$F(\sqrt{-17})$ thm 9	$F(\sqrt{-3}, \sqrt{-17})$	F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-627})$ thm 8	$F(\sqrt{-418})$ thm 8	$F(\sqrt{-3}, \sqrt{209})$
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-51})$ thm 8	$F(\sqrt{-34})$ thm 8	$F(\sqrt{-3}, \sqrt{17})$	F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-6270})$ thm 8	$F(\sqrt{-1045})$ thm 8	$F(\sqrt{-3}, \sqrt{-1045})$
F	$F(\sqrt{-3})$ thm 8	$F(\sqrt{-114})$ thm 8	$F(\sqrt{-19})$ thm 8	$F(\sqrt{-3}, \sqrt{-19})$					

Table 2
$F' = \mathbb{Q}(\sqrt{-2}, \sqrt{-3})$

F'	L	M	N	k
$F(\sqrt{-3})$	$F'(\sqrt{-5})$	$F'(\sqrt{5})$	$F'(\sqrt{-1})$	$F'(\sqrt{-5}, \sqrt{-1})$
$F(\sqrt{-3})$	$F'(\sqrt{-5})$	$F'(\sqrt{35})$	$F'(\sqrt{-7})$	$F'(\sqrt{-5}, \sqrt{-7})$
$F(\sqrt{-3})$	$F'(\sqrt{-5})$	$F'(\sqrt{7})$	$F'(\sqrt{-35})$	$F'(\sqrt{-5}, \sqrt{7})$
$F(\sqrt{-3})$	$F'(\sqrt{-5})$	$F'(\sqrt{55})$	$F'(\sqrt{-11})$	$F'(\sqrt{-5}, \sqrt{-11})$
$F(\sqrt{-3})$	$F'(\sqrt{-5})$	$F'(\sqrt{11})$	$F'(\sqrt{-55})$	$F'(\sqrt{-5}, \sqrt{11})$
$F(\sqrt{-3})$	$F'(\sqrt{-5})$	$F'(\sqrt{95})$	$F'(\sqrt{-19})$	$F'(\sqrt{-5}, \sqrt{-19})$
$F(\sqrt{-3})$	$F'(\sqrt{-5})$	$F'(\sqrt{19})$	$F'(\sqrt{-95})$	$F'(\sqrt{-5}, \sqrt{19})$
$F(\sqrt{-3})$	$F'(\sqrt{-5})$	$F'(\sqrt{209})$	$F'(\sqrt{-1045})$	$F'(\sqrt{-5}, \sqrt{209})$
$F(\sqrt{-3})$	$F'(\sqrt{-1})$	$F'(\sqrt{7})$	$F'(\sqrt{-7})$	$F'(\sqrt{-1}, \sqrt{-7})$
$F(\sqrt{-3})$	$F'(\sqrt{-1})$	$F'(\sqrt{11})$	$F'(\sqrt{-11})$	$F'(\sqrt{-1}, \sqrt{-11})$
$F(\sqrt{-3})$	$F'(\sqrt{-1})$	$F'(\sqrt{13})$	$F'(\sqrt{-13})$	$F'(\sqrt{-1}, \sqrt{-13})$
$F(\sqrt{-3})$	$F'(\sqrt{-1})$	$F'(\sqrt{17})$	$F'(\sqrt{-17})$	$F'(\sqrt{-1}, \sqrt{-17})$
$F(\sqrt{-3})$	$F'(\sqrt{-1})$	$F'(\sqrt{19})$	$F'(\sqrt{-19})$	$F'(\sqrt{-1}, \sqrt{-19})$
$F(\sqrt{-3})$	$F'(\sqrt{-1})$	$F'(\sqrt{23})$	$F'(\sqrt{-23})$	$F'(\sqrt{-1}, \sqrt{-23})$

Table 3
$F' = \mathbb{Q}(\sqrt{-2}, \sqrt{-3}, \sqrt{-5})$

F'	L	M	N	k
$F(\sqrt{-3}, \sqrt{-5})$	$F'(\sqrt{-1})$	$F'(\sqrt{7})$	$F'(\sqrt{-7})$	$F'(\sqrt{-1}, \sqrt{-7})$
$F(\sqrt{-3}, \sqrt{-5})$	$F'(\sqrt{-1})$	$F'(\sqrt{11})$	$F'(\sqrt{-11})$	$F'(\sqrt{-1}, \sqrt{-11})$
$F(\sqrt{-3}, \sqrt{-5})$	$F'(\sqrt{-1})$	$F'(\sqrt{19})$	$F'(\sqrt{-19})$	$F'(\sqrt{-1}, \sqrt{-19})$
$F(\sqrt{-3}, \sqrt{-5})$	$F'(\sqrt{-11})$	$F'(\sqrt{209})$	$F'(\sqrt{-19})$	$F'(\sqrt{-11}, \sqrt{-19})$

Table 4
$F = F' = \mathbb{Q}(\sqrt{-23})$

F'	L	M	N	k
F	$F(\sqrt{-46})$ thm 8	$F(\sqrt{-2})$ thm 9	$F(\sqrt{-1})$ thm 8	$F(\sqrt{2}, \sqrt{-1})$
F	$F(\sqrt{-46})$ thm 8	$F(\sqrt{-6})$ thm 8	$F(\sqrt{-3})$ thm 8	$F(\sqrt{2}, \sqrt{-3})$
F	$F(\sqrt{-46})$ thm 8	$F(\sqrt{-138})$ thm 8	$F(\sqrt{-69})$ thm 8	$F(\sqrt{2}, \sqrt{3})$
F	$F(\sqrt{-46})$ thm 8	$F(\sqrt{-26})$ thm 9	$F(\sqrt{-13})$ thm 8	$F(\sqrt{2}, \sqrt{-13})$
F	$F(\sqrt{-46})$ thm 8	$F(\sqrt{-598})$ thm 8	$F(\sqrt{-299})$ thm 9	$F(\sqrt{2}, \sqrt{13})$
F	$F(\sqrt{-46})$ thm 8	$F(\sqrt{-78})$ thm 8	$F(\sqrt{-39})$ thm 8	$F(\sqrt{2}, \sqrt{-39})$
F	$F(\sqrt{-46})$ thm 8	$F(\sqrt{-1794})$ thm 8	$F(\sqrt{-897})$ thm 8	$F(\sqrt{2}, \sqrt{39})$

Table 5
$F' = \mathbb{Q}(\sqrt{-23}, \sqrt{2})$

F'	L	M	N	k
$F(\sqrt{2})$	$F'(\sqrt{-3})$	$F'(\sqrt{3})$	$F'(\sqrt{-1})$	$F'(\sqrt{-3}, \sqrt{-1})$
$F(\sqrt{2})$	$F'(\sqrt{-3})$	$F'(\sqrt{39})$	$F'(\sqrt{-13})$	$F'(\sqrt{-3}, \sqrt{-13})$
$F(\sqrt{2})$	$F'(\sqrt{-3})$	$F'(\sqrt{-39})$	$F'(\sqrt{13})$	$F'(\sqrt{-3}, \sqrt{13})$

Table 6
$F' = \mathbb{Q}(\sqrt{-23}, \sqrt{2}, \sqrt{-3})$

F'	L	M	N	k
$F(\sqrt{2}, \sqrt{-3})$	$F'(\sqrt{-1})$	$F'(\sqrt{13})$	$F'(\sqrt{-13})$	$F'(\sqrt{-1}, \sqrt{-13})$

Remark 17. Our new Theorem 9 is necessary for the iteration because we need a large amount of biquadratic fields to get extensions of degree 8, 16 and so on and, among these fields, one is bound to find some in which 3 (or p in general) totally splits.

Remark 18. For all the k's in Tables 1–6 we have proved that $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$ hence ideals capitulate in this $\mathbb{Z}_3^2$-extension. These fields have degree 8 (Tables 1, 4), 16 (Tables 2, 5) and 32 (Tables 3, 6). So in this setting capitulation comes quite early since $\tilde{k}/k$ is a $\mathbb{Z}_3^5$, $\mathbb{Z}_3^9$, $\mathbb{Z}_3^{17}$-extension, respectively.

References

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

[2] T. Fukuda, H. Taya, The Iwasawa λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields, Acta Arith. 69 (1995) 277–292.

[3] R. Greenberg, The Iwasawa invariants of Γ-extensions of a fixed number field, Amer. J. Math. 95 (1973) 204–214.

[4] R. Greenberg, On the Iwasawa invariants of totally real number fields, Amer. J. Math. 98 (1976) 263–284.

[5] R. Greenberg, On the structure of certain Galois groups, Invent. Math. 47 (1978) 85–99.

[6] R. Greenberg, Iwasawa theory—Past and present, Adv. Stud. Pure Math. 30 (2001) 335–385.

[7] D. Hubbard, The nonexistence of certain free pro-p-extensions and capitulation in a family of dihedral extensions of $\mathbb{Q}$, PhD thesis, University of Washington, 1996.

[8] K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields, Ann. of Math. 98 (1973) 246–326.

[9] J.S. Kraft, R. Schoof, Computing Iwasawa modules of real quadratic number fields, Compos. Math. 97 (1995) 135–155.

[10] A. Lannuzel, T. Nguyen Quang Do, Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres, Manuscripta Math. 102 (2000) 187–209.

[11] D.C. Marshall, Galois groups and Greenberg's conjecture, PhD thesis, University of Arizona, 2000.

[12] W.G. McCallum, Greenberg's conjecture and units in multiple $\mathbb{Z}_p$-extensions, Amer. J. Math. 123 (2001) 909–930.

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

[14] T. Nguyen Quang Do, Formations de classes et modules d'Iwasawa, in: Number Theory, Noordwijkerhout, 1983, in: Lecture Notes in Math., Springer, New York, 1984, pp. 167–185.

[15] M. Paoluzi, Greenberg's conjecture for real quadratic fields, PhD thesis, University of Rome, 2002.
[16] B. Perrin-Riou, Arithmétique des courbes elliptiques et théorie d'Iwasawa, Bull. Soc. Math. France Mém. (N.S.) 17 (1984).
[17] J.P. Serre, Classes des corpes cyclotomiques (d'après K. Iwasawa), Sém. Bourbaki Exposé 174 (1958); in: Sém. Bourbaki, vol. 5, Soc. de France, 1995, pp. 83–93.
[18] L.C. Washington, Introduction to Cyclotomic Fields, second ed., Grad. Texts in Math., vol. 83, Springer, 1997.