Riv. Mat. Univ. Parma (7) **3*** (2004), 151-158

ANDREA BANDINI (*)

Greenberg's conjecture for multiple $\mathbb{Z}_p$-extensions (**)

1 - Introduction

Let k be a number field and let p be a prime. Let K be a $\mathbb{Z}_p^d$-extension of k, i.e. K/k is Galois and $Gal(K/k) \simeq \mathbb{Z}_p^d$. Then there exist number fields $k_n \subset K$ such that $Gal(k_n/k) \simeq (\mathbb{Z}/p^n\mathbb{Z})^d$ and $K = \cup k_n$. Let A_{k_n} be the p-part of the ideal class group of k_n. The A_{k_n}'s form an inverse system with respect to the natural norm maps so let Y_K be their inverse limit. By class field theory and infinite Galois theory one has $Y_K \simeq Gal(L_K/K)$ where L_K is the maximal abelian unramified pro-p-extension of K. Hence Y_K is a normal subgroup of $Gal(L_K/k)$ and it admits an action of $Gal(K/k)$ via conjugation. Thus Y_K is a $\mathbb{Z}_p[[Gal(K/k)]]$-module. In [**12**] Serre showed a noncanonical isomorphism between $\mathbb{Z}_p[[Gal(K/k)]]$ and $\mathbb{Z}_p[[T_1, \dots, T_d]] \overset{\text{def}}{=} \Lambda_d$ by sending topological generators τ_i to $T_i + 1$ for $1 \leqslant i \leqslant d$. In [**3**] Greenberg proved that Y_K is always a torsion Λ_d-module.

A torsion Λ_d-module M is said to be *pseudo-null* if it has at least two relatively prime annihilators, i.e. if $\mathrm{ht} Ann_{\Lambda_d}(M) \geqslant 2$. If this is the case we shall write $M \sim_{\Lambda_d} 0$. We shall study the following

Conjecture 1.1 ([**4**] Conjecture 3.5). *Let $\tilde{k}$ be the compositum of all the $\mathbb{Z}_p$-extensions of k and let $Gal(\tilde{k}/k) \simeq \mathbb{Z}_p^d$. Then $Y_{\tilde{k}} \sim_{\Lambda_d} 0$.*

This conjecture has been extensively studied for the case of real quadratic fields (see [**5**], [**6**], [**10**] and the references there) and imaginary quadratic fields

(*) Dipartimento di Matematica, Università di Pisa, via F. Buonarroti 2, 56127 Pisa, Italy; e-mail: bandini@mail.dm.unipi.it

(**) Received January 20th, 2004. AMS classification 11 R 23.

(see [**9**]) but very little in known in general (see [**8**] for the case of certain cyclotomic fields).

In the second section we shall show a technique which can be used to deduce the conjecture for a field k once one knows that it is true for some of its subfields. In the third section we shall use such technique in combination with the known results on quadratic fields to prove the conjecture for several fields with $Gal(k/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$.

We will assume Leopoldt's conjecture for all the fields involved so that $Gal(\tilde{k}/k) \simeq \mathbb{Z}_p^{r_2(k)+1}$ (see [**13**] Theorem 13.4, $r_2(k)$ is the number of pairs of conjugate complex embeddings of k).

2 - Lifting pseudo-nullity

Let k/F be a finite Galois extension of number fields and let F_∞/F be a $\mathbb{Z}_p^d$-extension. Let $G = Gal(k/F)$ and let $\widehat{G}$ be the group of characters of G. For any $\chi \in \widehat{G}$ let k^χ be the subfield of k fixed by $Ker\,\chi$. Then we have the following

Proposition 2.1. *If p does not divide the order of G then*

$$Y_{kF_\infty} \simeq \bigoplus_{\chi \in \widehat{G}} Y_{k^\chi F_\infty}.$$

Proof. The hypothesis on p yields $G \simeq Gal(kF_\infty/F_\infty)$ so one has an action of G on $Y_{kF_\infty} \simeq Gal(L_{kF_\infty}/kF_\infty)$ (notations as in the introduction). For any $\chi \in \widehat{G}$ let $Y^\chi_{kF_\infty}$ be the submodule of Y_{kF_∞} on which $Ker\,\chi$ acts trivially. One has a decomposition in eigenspaces

$$Y_{kF_\infty} \simeq \bigoplus_{\chi \in \widehat{G}} Y^\chi_{kF_\infty}.$$

Again using the hypothesis on p it is not hard to prove that $Y^\chi_{kF_\infty} \simeq Y_{k^\chi F_\infty}$ (see, for example, [**1**]) and the proposition follows. ∎

Since a finite sum of pseudo-null modules is pseudo-null one immediately has the following

Corollary 2.2. *If p does not divide the order of G then*

$$Y_{kF_\infty} \sim_{\Lambda_d} 0 \Leftrightarrow Y_{k^\chi F_\infty} \sim_{\Lambda_d} 0 \text{ for any } \chi \in \widehat{G}.$$

This corollary enables us to prove pseudo-nullity for Y_{kF_∞} once we know it for some subfields k^χ but, in general, this is not enough to prove the conjecture for k

even if $F_\infty = \tilde{F}$, the compositum of all the $\mathbb{Z}_p$-extensions of F. For example let k be an imaginary biquadratic field with $F = \mathbb{Q}$ and $\tilde{F} = F_{cyc}$, the cyclotomic $\mathbb{Z}_p$-extension of F. Then $k^\chi \tilde{F} = k_{cyc}^\chi$ and $Y_{k_{cyc}^\chi} \sim_{\Lambda_1} 0$ for all χ's yields $Y_{k_{cyc}} \sim_{\Lambda_1} 0$. But $\tilde{k}/k$ is a $\mathbb{Z}_p^3$-extension containing k_{cyc} and, to prove the conjecture, we have to lift the condition of pseudo-nullity from $Y_{k_{cyc}} \sim_{\Lambda_1} 0$ to $Y_{\tilde{k}} \sim_{\Lambda_3} 0$. In some cases this can be achieved via the following

Proposition 2.3. *Let M be a finitely generated torsion Λ_d-module. If the quotient $M/T_d M$ is pseudo-null over Λ_{d-1} then M is pseudo-null over Λ_d.*

Proof. See [11] Lemme 2. ∎

Theorem 2.4. *Let K/k be a $\mathbb{Z}_p^d$-extension with $d \geq 2$. 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 ≥ 2;*

2) $Y_K \sim_{\Lambda_d} 0$.

Then Conjecture 1.1 *holds for k.*

Proof. Let $\tau_{d+1}, \ldots, \tau_{r_2(k)+1}$ be some independent topological generators of $Gal(\tilde{k}/K)$ corresponding to the variables $T_{d+1}, \ldots, T_{r_2(k)+1}$ in $\Lambda_{r_2(k)+1}$. Then

$$Y_{\tilde{k}}/(T_{d+1}, \ldots, T_{r_2(k)+1})\, Y_{\tilde{k}} \simeq Gal(L_0/\tilde{k})$$

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 $Gal(\tilde{k}/K)$. 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 $\mathfrak{p}_K$. The group $D(\mathfrak{p})$ 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. Independent topological generators of $D(\mathfrak{p})$ give rise to relatively prime annihilators of $I(\mathfrak{p}_K)$ so, by hypothesis 1), $I(\mathfrak{p}_K)$ is pseudo-null. This holds for any $\mathfrak{p}_K | \mathfrak{p}$ and, since the number of $\mathfrak{p}$'s is finite, 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,

$$Gal(L_0/\tilde{k}) \simeq Y_{\tilde{k}}/(T_{d+1}, \dots, T_{r_2(k)+1})\, Y_{\tilde{k}} \sim_{\Lambda_d} 0\,.$$

Applying repeatedly Proposition 2.3 one gets $Y_{\tilde{k}} \sim_{\Lambda_{r_2(k)+1}} 0$. ∎

3 - Applications

The case of totally real fields is quite easy because they have only one $\mathbb{Z}_p$-extension, namely the cyclotomic one, which is canonically obtained by composition with the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. If k/F is a Galois extension of totally real number fields one has $\tilde{k} = k_{cyc} = k\mathbb{Q}_{cyc} = kF_{cyc}$. Hence, assuming $p \nmid [k : F]$, by Corollary 2.2

$$Y_{\tilde{k}} = Y_{kF_{cyc}} \sim_{\Lambda_1} 0 \Leftrightarrow Y_{k^\chi F_{cyc}} = Y_{\widetilde{k^\chi}} \sim_{\Lambda_1} 0 \text{ for any } \chi \in \widehat{G}\,,$$

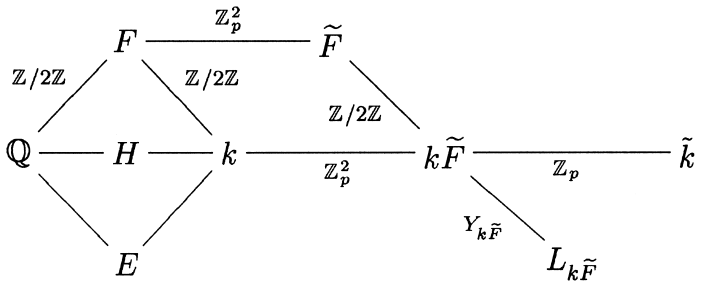
i.e. the conjecture holds for k if and only if it holds for any k^χ. In particular, for small primes like $p = 3, 5, 7$, with $F = \mathbb{Q}$ one can use the known results on fields like $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{l})$, $\mathbb{Q}(\sqrt{dl})$ to prove the conjecture for several biquadratic fields $\mathbb{Q}(\sqrt{d}, \sqrt{l})$. Then, with F a quadratic field, using the biquadratic fields, we can prove Conjecture 1.1 for fields of degree 8 and so on. In general the knowledge of the conjecture on real quadratic fields enables us to prove it for real fields like $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}, \dots)$.

The case of imaginary fields is more involved. We shall need to lift pseudo-nullity and, to apply Theorem 2.4, we need at last a $\mathbb{Z}_p^2$-extension so the cyclotomic one is not enough. The role that $\mathbb{Q}$ and $\mathbb{Q}_{cyc}$ had for real fields can be played by any imaginary quadratic field F and its $\mathbb{Z}_p^2$-extension $\tilde{F}$.

Proposition 3.1. *Let F be an imaginary quadratic field. Let k/F be a finite extension such that $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$. Then $Y_{\tilde{k}} \sim_{\Lambda_{r_2(k)+1}} 0$, i.e. the conjecture holds for k.*

Proof. Hypothesis 1) in Theorem 2.4 is known to hold for the extension $\tilde{F}/F$ so it holds for $k\tilde{F}/k$ as well and we can apply the theorem to prove this proposition. ∎

To find some examples we look at biquadratic imaginary fields and assume $p \neq 2$.



Let F and E be quadratic imaginary fields and let H be the real subfield of k. On $Y_{k\tilde{F}}$ one can prove the following theorems

Theorem 3.2. *Assume that*:

1) *p does not split in k*;

2) *Conjecture* 1.1 *holds for F and H i.e. $Y_{\tilde{F}} \sim_{\Lambda_2} 0$ and $Y_{H_{cyc}} \sim_{\Lambda_1} 0$*;

3) $Y_{E_{cyc}} \sim_{\Lambda_1} 0$.

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

Theorem 3.3. *Assume that*:

1) *$\widetilde{F}/F_{cyc}$ is unramified (this happens, for example, when p splits in F)*;

2) *Conjecture* 1.1 *holds for F and H*;

3) $Y_{E_{cyc}} \sim_{\Lambda_1} 0$.

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

Theorem 3.4. *Assume that*:

1) *p totally splits in k*;

2) *Conjecture* 1.1 *holds for H*;

3) $Y_{F_{cyc}} \simeq Y_{E_{cyc}} \simeq \mathbb{Z}_p$.

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

Proof. (Details in [1] and [2]) For Theorems 3.2 and 3.3 one considers the action of $Gal(k\widetilde{F}/\widetilde{F})$ on $Y_{k\tilde{F}}$ and gets a decomposition in eigenspaces $Y_{k\tilde{F}} = Y_{k\tilde{F}}^{+} \oplus Y_{k\tilde{F}}^{-}$ where $Y_{k\tilde{F}}^{+}$ (resp. $Y_{k\tilde{F}}^{-}$) is the submodule on which $Gal(k\widetilde{F}/\widetilde{F})$ acts trivially (resp. nontrivially). It is easy to see that $Y_{k\tilde{F}}^{+} \simeq Y_{\tilde{F}}$ so it is pseudo-null. Let T_2 be the variable in Λ_2 corresponding to a topological generator of $Gal(k\widetilde{F}/k_{cyc})$,

then one finds an injection

$$Y_{k\tilde{F}}/T_2 Y_{k\tilde{F}} \hookrightarrow Y_{E_{cyc}} \oplus Y_{H_{cyc}} \qquad (\sim_{\Lambda_1} 0 \text{ by hypothesis}).$$

Therefore, by Proposition 2.3, one gets $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$ and, eventually, $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$.

For Theorem 3.4 let T_2 and T_3 be the variables in Λ_3 corresponding to topological generators of $Gal(\tilde{k}/k_{cyc})$. Using the fact that $\tilde{k}/k_{cyc}$ is unramified one finds an isomorphism

$$Y_{\tilde{k}}/(T_2, T_3) Y_{\tilde{k}} \simeq Y_{H_{cyc}} \qquad (\sim_{\Lambda_1} 0 \text{ by hypothesis}).$$

By Proposition 2.3 this yields $Y_{\tilde{k}}/T_3 Y_{\tilde{k}} \sim_{\Lambda_2} 0$. One has the exact sequence of Galois theory

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

which corresponds to

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

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

Remark 3.5. *The third hypothesis of each theorem is not known to hold in general. If p does not split in E (Theorems 3.2 and 3.3) then the hypothesis holds, for example, when p does not divide h_E (the order of the ideal class group of E). If $p = \mathfrak{p}\bar{\mathfrak{p}}$ in a quadratic imaginary field L (Theorem 3.4 with $L = E, F$) then $Y_{L_{cyc}} \simeq \mathbb{Z}_p$ if and only if $\bar{\mathfrak{p}}^{h_L} = (\alpha)$ with $\alpha \notin (\mathbb{Q}_p^*)^p$.*

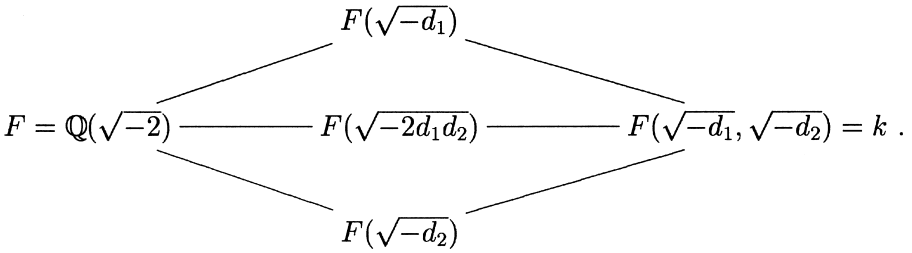
3.1 - *Example*

Take $F = \mathbb{Q}(\sqrt{-2})$ and $p = 3$. One has $Y_{F_{cyc}} \simeq \mathbb{Z}_3$, $\tilde{F}/F_{cyc}$ is unramified and $Y_{\tilde{F}} \sim_{\Lambda_2} 0$. Hence we can take $E = \mathbb{Q}(\sqrt{-d})$ with $d > 0$ and

(i) $d \equiv 0, 1 \pmod 3$ and $3 \nmid h_E$ for Theorem 3.3;

(ii) $d \equiv 2 \pmod 3$ and $Y_{E_{cyc}} \simeq \mathbb{Z}_3$ for Theorem 3.4,

to get $Y_{k\tilde{F}} \sim_{\Lambda_2} 0$ for $k = \mathbb{Q}(\sqrt{-2}, \sqrt{-d})$. After this first step consider



One has $Y_{k\tilde{F}} \simeq Y_{\tilde{F}} \oplus Y_{F(\sqrt{-d_1})\tilde{F}} \oplus Y_{F(\sqrt{-d_2})\tilde{F}} \oplus Y_{F(\sqrt{-2d_1d_2})\tilde{F}}$ so we can prove

$Y_{k\tilde{F}} \sim_{\Lambda_2} 0$ if we have such result for enough biquadratic fields. This process can obviously be iterated to fields of degree 16, 32 and so on (note that we need to use the theorems only in the first step).

$F(\sqrt{-d_1})$	$F(\sqrt{-2d_1d_2})$	$F(\sqrt{-d_2})$	k
$F(\sqrt{-3})$ thm 3.3	$F(\sqrt{-6})$ thm 3.3	$F(\sqrt{-1})$ thm 3.3	$F(\sqrt{-3}, \sqrt{-1})$
$F(\sqrt{-3})$ thm 3.3	$F(\sqrt{-30})$ thm 3.3	$F(\sqrt{-5})$ thm 3.4	$F(\sqrt{-3}, \sqrt{-5})$
$F(\sqrt{-3})$ thm 3.3	$F(\sqrt{-15})$ thm 3.3	$F(\sqrt{-10})$ thm 3.3	$F(\sqrt{-3}, \sqrt{5})$
$F(\sqrt{-3})$ thm 3.3	$F(\sqrt{-78})$ thm 3.3	$F(\sqrt{-13})$ thm 3.3	$F(\sqrt{-3}, \sqrt{-13})$
$F(\sqrt{-3})$ thm 3.3	$F(\sqrt{-39})$ thm 3.3	$F(\sqrt{-26})$ thm 3.4	$F(\sqrt{-3}, \sqrt{13})$
$F(\sqrt{-3})$ thm 3.3	$F(\sqrt{-390})$ thm 3.3	$F(\sqrt{-65})$ thm 3.4	$F(\sqrt{-3}, \sqrt{-65})$
$F(\sqrt{-3})$ thm 3.3	$F(\sqrt{-195})$ thm 3.3	$F(\sqrt{-130})$ thm 3.3	$F(\sqrt{-3}, \sqrt{65})$

From the fields k listed in the table one can get $Y_{L\tilde{F}} \sim_{\Lambda_2} 0$ for $L = F(\sqrt{-3}, \sqrt{-1}, \sqrt{-5})$, $F(\sqrt{-3}, \sqrt{-1}, \sqrt{-13})$, $F(\sqrt{-3}, \sqrt{-1}, \sqrt{65})$ and, finally, with this three fields we can prove the conjecture for $F(\sqrt{-3}, \sqrt{-1}, \sqrt{-5}, \sqrt{-13})$. More examples can be found in [**1**] and [**2**]. For an example of the computations needed to apply the theorems consider $\mathbb{Q}(\sqrt{-65})$ with $h_{\mathbb{Q}(\sqrt{-65})} = 8$ and $\overline{\mathfrak{p}} = (3, 1 - \sqrt{-65})$. One has $\overline{\mathfrak{p}}^8 = (49 + 8\sqrt{-65}) = (\alpha)$, $\sqrt{-65} = 1 + 3 + 3^4 + 3^6 + 2\cdot 3^8 + \ldots$ in $\mathbb{Q}_3$ and $v_3(\alpha) = 8$ so that $\alpha \notin (\mathbb{Q}_3^*)^3$ and we can use Theorem 3.4.

Remark 3.6. *There is a deep relation between the pseudo-nullity of Y_K and the behaviour of ideals in a $\mathbb{Z}_p^d$-extension K/k. When $k_{cyc} \subseteq K$ we can prove that if $Y_K \sim_{\Lambda_d} 0$ then ideals «capitulate» (i.e. become principal) in K (see* [**2**] *or, for other general results,* [**7**]*). Conjecture* 1.1 *tells us to expect capitulation in $\tilde{k}$ but our results give lots of examples in which capitulation is achieved at a lower level. We have always obtained capitulation in a $\mathbb{Z}_p^2$-extension $k\tilde{F}$ while $\tilde{k}$ are $\mathbb{Z}_p^3$, $\mathbb{Z}_p^5$, $\mathbb{Z}_p^9$ or $\mathbb{Z}_p^{17}$-extensions. It is easy to find examples of ideals not capitulating in a $\mathbb{Z}_p$-*

extension like the cyclotomic one but, up to now, there are no known examples in which capitulation can be delayed further.

References

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

[2] A. Bandini, *Greenberg's conjecture and capitulation in $\mathbb{Z}_p^d$-extensions*, in preparation.

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

[4] R. Greenberg, *Iwasawa theory - Past and present*, Adv. Stud. Pure Math. **30** (2001), 335-385.

[5] H. Ichimura and H. Sumida, *On the Iwasawa invariants of certain real abelian fields*, Tôhoku Math. J. **49** (1997), 203-215.

[6] J. S. Kraft and R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Comp. Math. **97** (1995), 135-155.

[7] 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.

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

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

[10] M. Paoluzi, *La congettura di Greenberg per campi reali quadratici*, Ph.D. Thesis, University of Tor Vergata, Rome 2002.

[11] B. Perrin-Riou, *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, Mém. Soc. Math. France, (N.S.) **17** (1984).

[12] J. P. Serre, *Classes des corpes cyclotomiques (d'après K. Iwasawa)*, Séminaire Bourbaki **174** (1958) in Séminaire Bourbaki **5** Soc. Math. France, Paris (1995), 83-93.

[13] L. C. Washington, *Introduction to cyclotomic fields*, Second edition, Springer-Verlag, New York 1997.

Abstract

Let $\tilde{k}$ be the compositum of all the $\mathbb{Z}_p$-extensions of a number field k. 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.

* * *