

Greenberg's conjecture for \mathbb{Z}_p^d -extensions

by

ANDREA BANDINI (Pisa)

1. Introduction. Let k be a number field and let p be a prime. Let \tilde{k} be the compositum of all the \mathbb{Z}_p -extensions of k . Let $\text{Gal}(\tilde{k}/k) \simeq \mathbb{Z}_p^d$ and choose d independent topological generators τ_1, \dots, τ_d . There is a noncanonical isomorphism

$$\mathbb{Z}_p[[\text{Gal}(\tilde{k}/k)]] \simeq \mathbb{Z}_p[[T_1, \dots, T_d]] =: \Lambda_d$$

given by $\tau_i \rightarrow T_i + 1$ (see [Se]).

Let $\tilde{k} = \bigcup k_n$ where each k_n is a finite extension of k . Let A_{k_n} be the p -part of the ideal class group of k_n . The A_{k_n} 's form a projective system with respect to the natural norm maps N_{k_m/k_n} for any $m \geq n$. Taking their projective limit we get

$$\varprojlim_n A_{k_n} =: Y_{\tilde{k}} \simeq \text{Gal}(L_{\tilde{k}}/\tilde{k})$$

where $L_{\tilde{k}}$ is the maximal abelian unramified pro- p -extension of \tilde{k} . With this identification it is easy to see that $\text{Gal}(\tilde{k}/k)$ acts on $Y_{\tilde{k}}$ via conjugation. Then $Y_{\tilde{k}}$ can be viewed as a Λ_d -module and, in particular, it is a finitely generated torsion Λ_d -module (see [Gr1]).

We say that a torsion Λ_d -module is *pseudo-null* if it has at least two relatively prime annihilators. If this is the case we shall write $M \sim_{\Lambda_d} 0$.

We have the following

CONJECTURE 1.1 ([Gr3, Conjecture 3.5]). *With all notations as above, $Y_{\tilde{k}}$ is pseudo-null as a Λ_d -module.*

This conjecture has been extensively studied for the case of real quadratic fields (see [FT], [IS], [KS] and the references there) and imaginary quadratic fields ([Mi] or [Hu]) but very little is known in general (see [Ma] and [McC] for the case of certain cyclotomic fields).

In the second section of this paper we shall consider an odd prime p and a totally real field K which is a biquadratic extension of a number field k .

2000 *Mathematics Subject Classification*: 11R23, 11R11.

In this case $d = 1$, $\tilde{K} = K_{\text{cyc}}$, the cyclotomic \mathbb{Z}_p -extension of K , and a Λ_1 -module is pseudo-null if and only if it is finite. Thus the conjecture is equivalent to proving that the classical Iwasawa λ -invariant for K_{cyc}/K is zero (see [Iw]). Decomposing $Y_{\tilde{K}}$ in eigenspaces with respect to the action of the characters of $\text{Gal}(K/k)$ we prove the following

THEOREM 1.2. *Let F, E, H be the three quadratic extensions of k lying between K and k . Then*

$$Y_{\tilde{K}} \text{ is finite } \Leftrightarrow Y_{\tilde{k}}, Y_{\tilde{E}}, Y_{\tilde{F}}, Y_{\tilde{H}} \text{ are finite.}$$

The choice of biquadratic extensions is due to the fact that, to produce new examples, we have to rely on fields for which the conjecture is known to hold, i.e. only on quadratic fields up to now. Nevertheless the procedure of taking eigenspaces seems to work in general provided that p does not divide $[K : k]$.

In the third section with similar techniques and some more restrictive hypothesis we will see how the conjecture can be proved for some imaginary biquadratic fields.

Finally we shall give some numerical examples using as “base fields” the ones from the tables of [FT], [IS], [KS] and [Mi] for which the conjecture is known to hold.

In the rest of the paper we will use the following notations, for any number field k :

- 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 ;
- $A_k \simeq \text{Gal}(L_k/k)$ 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

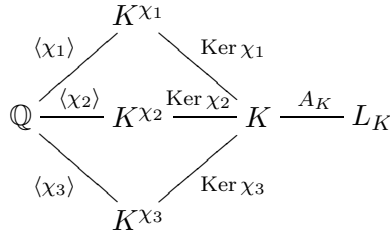
$$A_{k_{\text{cyc}}} = \varinjlim_n A_{k_n}, \quad Y_{k_{\text{cyc}}} = \varprojlim_n A_{k_n} \simeq \text{Gal}(L_{k_{\text{cyc}}}/k_{\text{cyc}})$$

where the direct limit is taken with respect to the inclusion maps and the projective limit is with respect to the norms.

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

Acknowledgements. This paper was mainly prepared while I was a guest at the University of Washington in Seattle. I would like to thank this institution for its hospitality. I am especially grateful to Ralph Greenberg and Adrian Iovita for being so friendly and helpful during the period I spent there.

2. The real case. Let p be an odd prime. Let K be a totally real bi-quadratic number field with $\Delta = \text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Let $\chi_0 = 1, \chi_1, \chi_2, \chi_3$ be the characters of Δ and, for any i , let K^{χ_i} be the fixed field of $\text{Ker } \chi_i$, for example $K^{\chi_0} = \mathbb{Q}$.

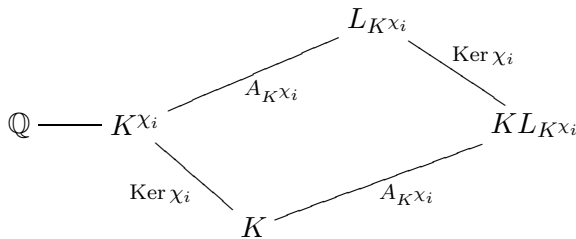


LEMMA 2.1. $A_K \simeq \bigoplus_{i=1}^3 A_{K^{\chi_i}}$.

Proof. Δ acts on A_K via conjugation so if we define $A_K^{\chi_i}$ to be the submodule of A_K on which $\text{Ker } \chi_i$ acts trivially we obtain a decomposition

$$A_K \simeq \bigoplus_{i=0}^3 A_K^{\chi_i}.$$

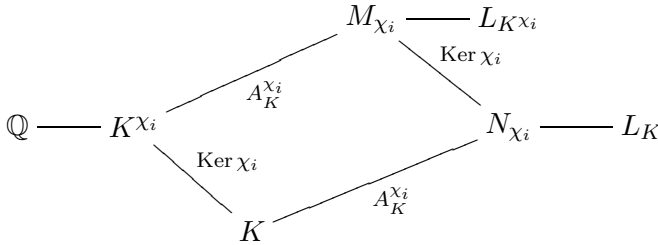
For any i let $L_{K^{\chi_i}}$ be the maximal abelian unramified p -extension of K^{χ_i} , so $\text{Gal}(L_{K^{\chi_i}}/K^{\chi_i}) \simeq A_{K^{\chi_i}}$. Then, since p is odd, $L_{K^{\chi_i}} \cap K = K^{\chi_i}$ and $L_{K^{\chi_i}}K/K$ is still an abelian unramified extension with $\text{Gal}(L_{K^{\chi_i}}K/K) \simeq A_{K^{\chi_i}}$. With this identification one can easily check that $\text{Gal}(K/K^{\chi_i}) \simeq \text{Ker } \chi_i$ acts trivially on $A_{K^{\chi_i}}$, i.e. $A_{K^{\chi_i}} \subseteq A_K^{\chi_i}$ by the definition of $A_K^{\chi_i}$.



$A_K^{\chi_i}$ is also a quotient of A_K so we have a sequence of fields $\mathbb{Q} \subseteq K^{\chi_i} \subset K \subseteq N_{\chi_i}$ such that $\text{Gal}(N_{\chi_i}/K) \simeq A_K^{\chi_i}$ and N_{χ_i} is an abelian unramified p -extension of K . By definition $\text{Gal}(K/K^{\chi_i}) \simeq \text{Ker } \chi_i$ acts trivially on $A_K^{\chi_i}$ so N_{χ_i} is abelian over K^{χ_i} as well. Hence there exists an abelian unramified p -extension of K^{χ_i} , call it M_{χ_i} , such that

$$\begin{aligned} \text{Gal}(M_{\chi_i}/K^{\chi_i}) &\simeq A_K^{\chi_i}, \\ \text{Gal}(N_{\chi_i}/M_{\chi_i}) &\simeq \text{Ker } \chi_i. \end{aligned}$$

This clearly implies $M_{\chi_i} \subseteq L_{K^{\chi_i}}$ and $A_K^{\chi_i} \subseteq A_{K^{\chi_i}}$.



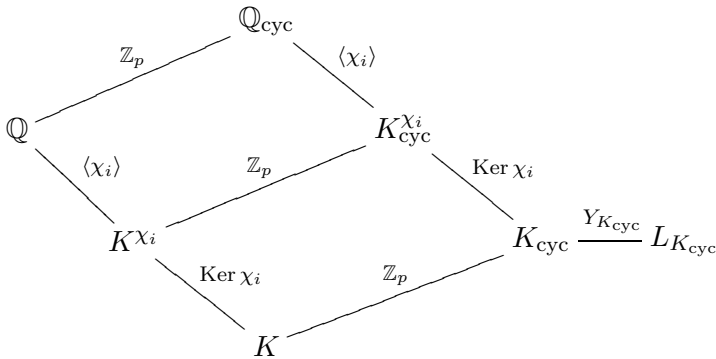
The two inclusions give equalities for any $i = 0, \dots, 3$ and it suffices to notice that $A_K^{\chi_0} = A_{K^{\chi_0}} = A_{\mathbb{Q}} = 0$ to complete the proof with the decomposition formula given above. ■

For any number field k let k_{cyc} be its cyclotomic \mathbb{Z}_p -extension. We can use the construction of the previous lemma for k_{cyc} and $Y_{k_{\text{cyc}}}$ which is isomorphic to the Galois group of the maximal abelian unramified pro- p -extension of k_{cyc} .

THEOREM 2.2. $Y_{K_{\text{cyc}}} \simeq \bigoplus_{i=1}^3 Y_{K_{\text{cyc}}^{\chi_i}}$.

Proof. For any real field $K_{\text{cyc}} = K\mathbb{Q}_{\text{cyc}}$. Moreover p odd implies that for any $i = 0, \dots, 3$ we have isomorphisms

$$\begin{aligned} \text{Gal}(K_{\text{cyc}}/\mathbb{Q}_{\text{cyc}}) &\simeq \text{Gal}(K/\mathbb{Q}), & \text{Gal}(K_{\text{cyc}}^{\chi_i}/\mathbb{Q}_{\text{cyc}}) &\simeq \text{Gal}(K^{\chi_i}/\mathbb{Q}), \\ \text{Gal}(K_{\text{cyc}}/K_{\text{cyc}}^{\chi_i}) &\simeq \text{Gal}(K/K^{\chi_i}). \end{aligned}$$



Hence we can consider the action of Δ via conjugation on $Y_{K_{\text{cyc}}}$ and obtain a decomposition similar to the one of the previous lemma

$$Y_{K_{\text{cyc}}} \simeq \bigoplus_{i=0}^3 Y_{K_{\text{cyc}}}^{\chi_i}$$

where $Y_{K_{\text{cyc}}}^{\chi_i}$ denotes the submodule of $Y_{K_{\text{cyc}}}$ on which $\text{Ker } \chi_i$ acts trivially. Using the same proof of Lemma 2.1 but with the cyclotomic \mathbb{Z}_p -extensions

instead of the number fields we see that $Y_{K_{\text{cyc}}}^{\chi_i} = Y_{K_{\text{cyc}}^{\chi_i}}$ for any i . Moreover it is well known that $Y_{\mathbb{Q}_{\text{cyc}}} = 0$ so the decomposition formula above proves the theorem. ■

COROLLARY 2.3. *Greenberg's conjecture holds for $K \Leftrightarrow$ it holds for any K^{χ_i} , $i = 1, 2, 3$.*

Proof. The conjecture in the real case states that $Y_{K_{\text{cyc}}}$ is finite so the corollary immediately follows from the theorem. ■

Now let k be a totally real number field and let K be a totally real Galois biquadratic extension of k with $\text{Gal}(K/k) = \Delta$. Let $\chi_0 = 1, \chi_1, \chi_2, \chi_3$ be the characters of Δ . Then, with notations as above, we have the following

THEOREM 2.4. *$Y_{K_{\text{cyc}}}$ is finite $\Leftrightarrow Y_{K_{\text{cyc}}^{\chi_i}}$ is finite for any $i = 0, \dots, 3$.*

Proof. The proof relies again on the decomposition formula

$$Y_{K_{\text{cyc}}} \simeq \bigoplus_{i=0}^3 Y_{K_{\text{cyc}}}^{\chi_i}$$

which still holds with “base field” k instead of \mathbb{Q} .

Following the same path of Lemma 2.1 and Theorem 2.2 we can prove that this is the same as

$$Y_{K_{\text{cyc}}} \simeq \bigoplus_{i=0}^3 Y_{K_{\text{cyc}}^{\chi_i}}$$

and the theorem follows. ■

REMARK 2.5. (1) In the last theorem $K^{\chi_0} = k$ so $Y_{K_{\text{cyc}}}^{\chi_0} \simeq Y_{K_{\text{cyc}}^{\chi_0}} \simeq Y_{k_{\text{cyc}}}$ and we need to assume that it is finite because we do not have it “for free” as in the previous case where $k = \mathbb{Q}$.

(2) Note that we have no restrictive hypothesis on the degree of k , the orders of the p -ideal class groups of the number fields involved and the factorization of p in k or in K . We will need this kind of hypothesis in the next section.

3. The complex case. Now let K be a totally complex quadratic extension of a totally real quadratic field H . Let $\text{Gal}(K/\mathbb{Q}) = \Delta$, and with the usual notation let $K^{\chi_0} = \mathbb{Q}$, $K^{\chi_1} = F$, $K^{\chi_2} = E$ and $K^{\chi_3} = H$. Assume again $p \neq 2$.

We mention a result which will be useful in what follows.

PROPOSITION 3.1. *Let M be a finitely generated torsion $\mathbb{Z}_p[[T_1, \dots, T_d]]$ -module. If $M/T_d M$ is pseudo-null over $\mathbb{Z}_p[[T_1, \dots, T_{d-1}]]$ then M is pseudo-null over $\mathbb{Z}_p[[T_1, \dots, T_d]]$.*

Proof. See [Mi] or [Hu]; original proof in [PR, Lemme 2]. ■

The following two theorems give the basis to prove the conjecture in some special cases. We will not prove the conjecture for all the fields K as above, nevertheless Theorems 3.2, 3.3 and 3.6 provide a lot of explicit examples as we will show in Section 4.

THEOREM 3.2. *Assume that:*

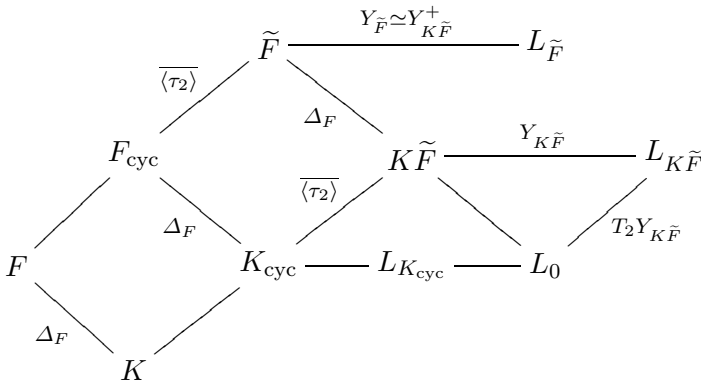
- (1) p does not split in K ;
- (2) the conjecture holds for F and H , i.e. $Y_{\tilde{F}} \sim_{\Lambda_2} 0$ and $Y_{H_{\text{cyc}}} \sim_{\Lambda_1} 0$;
- (3) $Y_{E_{\text{cyc}}} \sim_{\Lambda_1} 0$.

Then $Y_{K\tilde{F}}$ is pseudo-null as a module over $\Lambda_2 \simeq \mathbb{Z}_p[[\text{Gal}(K\tilde{F}/K)]]$.

Proof. With the previous method we obtain

$$Y_{K_{\text{cyc}}} \simeq \bigoplus_{i=1}^3 Y_{K_{\text{cyc}}^{\chi_i}} = Y_{F_{\text{cyc}}} \oplus Y_{E_{\text{cyc}}} \oplus Y_{H_{\text{cyc}}}.$$

Let $\Delta_F = \text{Gal}(K/F) \simeq \text{Gal}(K\tilde{F}/\tilde{F})$. Then this group acts via conjugation on $Y_{K\tilde{F}}$. Let $Y_{K\tilde{F}}^+$ (resp. $Y_{K\tilde{F}}^-$) be the submodule of $Y_{K\tilde{F}}$ on which Δ_F acts trivially (resp. nontrivially). Then $Y_{K\tilde{F}} = Y_{K\tilde{F}}^+ \oplus Y_{K\tilde{F}}^-$.



It is easy to see that $Y_{K\tilde{F}}^+ \simeq Y_{\tilde{F}}$ so, by hypothesis, it is pseudo-null over Λ_2 and we are left with $Y_{K\tilde{F}}^-$.

Let $\text{Gal}(K\tilde{F}/K_{\text{cyc}}) \simeq \text{Gal}(\tilde{F}/F_{\text{cyc}}) = \overline{\langle \tau_2 \rangle}$ and consider the quotient

$$Y_{K\tilde{F}}/(\tau_2 - 1)Y_{K\tilde{F}} \simeq Y_{K\tilde{F}}/T_2 Y_{K\tilde{F}}.$$

This quotient is isomorphic to $\text{Gal}(L_0/K\tilde{F})$ where L_0 is the maximal abelian extension of K_{cyc} contained in $L_{K\tilde{F}}$. By (1) there is only one prime in K_{cyc} above p . So one has $L_0 = K\tilde{F}L_{K_{\text{cyc}}}$ and, via restriction, one gets

$$Y_{K\tilde{F}}/T_2 Y_{K\tilde{F}} \simeq \text{Gal}(L_0/K\tilde{F}) \simeq \text{Gal}(L_{K_{\text{cyc}}}/L_{K_{\text{cyc}}} \cap K\tilde{F}).$$

Taking the minus part with respect to the action of Δ_F we see that

$$(Y_{K\tilde{F}}/T_2Y_{K\tilde{F}})^- \simeq Y_{K\tilde{F}}^-/T_2Y_{K\tilde{F}}^- \simeq \text{Gal}(L_{K_{\text{cyc}}}/L_{K_{\text{cyc}}} \cap K\tilde{F})^-$$

is a submodule of $Y_{K_{\text{cyc}}}^-$.

The submodule of $Y_{K_{\text{cyc}}}^-$ on which Δ_F acts via -1 is $Y_{E_{\text{cyc}}} \oplus Y_{H_{\text{cyc}}}$, which is finite by our hypothesis. Then $Y_{K\tilde{F}}^-/T_2Y_{K\tilde{F}}^-$ is finite, i.e. pseudo-null over $\Lambda_1 = \mathbb{Z}_p[[T_1]] \simeq \mathbb{Z}_p[[\text{Gal}(K_{\text{cyc}}/K)]]$.

Using Proposition 3.1 with $M = Y_{K\tilde{F}}^-$ and $d = 2$ we get $Y_{K\tilde{F}}^- \sim_{\Lambda_2} 0$ and eventually

$$Y_{K\tilde{F}} = Y_{K\tilde{F}}^+ \oplus Y_{K\tilde{F}}^- \sim_{\Lambda_2} 0. \blacksquare$$

THEOREM 3.3. *Assume that:*

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

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

Proof. Keeping the notations of the previous theorem we again reduce ourselves to showing that $Y_{K\tilde{F}}^- \sim_{\Lambda_2} 0$.

Let again $Y_{K\tilde{F}}/T_2Y_{K\tilde{F}} \simeq \text{Gal}(L_0/K\tilde{F})$. Obviously $L_{K_{\text{cyc}}} \subseteq L_0$ and we claim that they are equal. By definition $L_0/K\tilde{F}$ is unramified and, by hypothesis (1), $K\tilde{F}/K_{\text{cyc}}$ is unramified as well. Therefore L_0/K_{cyc} is abelian and unramified so $L_0 \subseteq L_{K_{\text{cyc}}}$ and the equality is proved.

Taking the minus part in the isomorphism above one has

$$Y_{K\tilde{F}}^-/T_2Y_{K\tilde{F}}^- \simeq \text{Gal}(L_{K_{\text{cyc}}}/K\tilde{F})^-.$$

The latter is a submodule of

$$\text{Gal}(L_{K_{\text{cyc}}}/K_{\text{cyc}})^- \simeq Y_{K_{\text{cyc}}}^- \simeq Y_{H_{\text{cyc}}} \oplus Y_{E_{\text{cyc}}},$$

which is finite by hypothesis. Therefore, by Proposition 3.1,

$$Y_{K\tilde{F}}^-/T_2Y_{K\tilde{F}}^- \sim_{\Lambda_1} 0 \Rightarrow Y_{K\tilde{F}}^- \sim_{\Lambda_2} 0$$

and eventually $Y_{K\tilde{F}} \sim_{\Lambda_2} 0$. \blacksquare

An immediate application is the following

COROLLARY 3.4. *Assume that:*

- (1) p does not split in E and does not divide the class number of E ;
- (2) p does not split in H and $Y_{H_{\text{cyc}}} \sim_{\Lambda_1} 0$;
- (3) $Y_{\tilde{F}} \sim_{\Lambda_2} 0$.

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

Proof. It is well known that hypothesis (1) yields $Y_{E_{\text{cyc}}} = 0$ so if p does not split in F , we can apply Theorem 3.2. If p splits in \tilde{F} it is easy to see that $L_{F_{\text{cyc}}} \supseteq \tilde{F}$, i.e. \tilde{F}/F_{cyc} is unramified and Theorem 3.3 applies. ■

REMARK 3.5. 1. The results of the theorems are “improvements” of the conjecture because \tilde{K}/K is a \mathbb{Z}_p^3 -extension while $K\tilde{F}/K$ is only a \mathbb{Z}_p^2 -extension. It has been conjectured (and proved in some cases, see [Ba], [Gr2] and [LN]) that for a general \mathbb{Z}_p^d -extension k_∞/k ,

$$\varinjlim_n A_{k_n} = Y_{k_\infty} \sim_{\Lambda_d} 0 \Rightarrow \varinjlim_n A_{k_n} =: A_{k_\infty} = 0.$$

Moreover the triviality of A_{k_∞} is strictly related with capitulation of ideals in the extension k_∞/k , which is an interesting but still quite mysterious phenomenon. Therefore it is important to find the “minimal” extension in \tilde{k} which ideals capitulate. Conjecture 1.1 tells us to expect capitulation in \tilde{k} and our theorems provide examples of pseudo-nullity and capitulation at a “lower level”.

2. To find some explicit examples we need $Y_{E_{\text{cyc}}}$ to be finite, i.e. pseudo-null over Λ_1 . We know that this is false for complex quadratic fields E in which p splits, but for fields with just one prime above p , $Y_{E_{\text{cyc}}}$ might be finite. In the corollary we decided to use the more restrictive hypothesis (1) to find some numerical examples (see next section) because the original one needs the calculation of $\#Y_{E_{\text{cyc}}}$, which is not easy at all.

In our situation the theorems imply the conjecture for K .

THEOREM 3.6. *With K as above,*

$$Y_{K\tilde{F}} \sim_{\Lambda_2} 0 \Rightarrow Y_{\tilde{K}} \sim_{\Lambda_3} 0.$$

Proof. Obviously $r_2(K) + 1 = 3$ so $\tilde{K}/K\tilde{F}$ is a \mathbb{Z}_p -extension.

Let $\text{Gal}(\tilde{K}/K\tilde{F}) = \langle \tau_3 \rangle$ and $\Lambda_3 = \mathbb{Z}_p[[T_1, T_2, T_3]]$ with $T_3 \sim \tau_3 - 1$. It is known that the primes of F above p are finitely decomposed in \tilde{F} , i.e. their decomposition groups in $\text{Gal}(\tilde{F}/F)$ have \mathbb{Z}_p -rank exactly 2. Hence the decomposition groups in $\text{Gal}(K\tilde{F}/K)$ of the primes of K lying above p have \mathbb{Z}_p -rank 2 as well.

Let L_0 be the fixed field of $T_3 Y_{\tilde{K}}$. Then L_0 is the maximal abelian extension of $K\tilde{F}$ contained in $L_{\tilde{K}}$. For any prime \mathfrak{p} of $K\tilde{F}$ lying above p let $I_{\mathfrak{p}}$ be its inertia group in $\text{Gal}(L_0/K\tilde{F})$. Since $L_{K\tilde{F}}$ is the maximal abelian unramified extension of $K\tilde{F}$ contained in L_0 we have

$$\text{Gal}(L_0/L_{K\tilde{F}}) \simeq \sum_{\mathfrak{p}|p} I_{\mathfrak{p}}.$$

Moreover the extension L_0/\tilde{K} is unramified so each inertia group embeds in

$\text{Gal}(\tilde{K}/K\tilde{F})$, which means that they are 0 or isomorphic to \mathbb{Z}_p .

$$\begin{array}{ccccc}
 & & L_{K\tilde{F}} & \xrightarrow{\sum_{\mathfrak{p}|p} I_{\mathfrak{p}}} & L_0 & \xrightarrow{T_3 Y_{\tilde{K}}} & L_{\tilde{K}} \\
 & \nearrow & & & \nearrow & & \\
 K & \text{---} & K\tilde{F} & \xrightarrow{\langle \tau_3 \rangle} & \tilde{K} & \xrightarrow{Y_{\tilde{K}}} & \\
 & & & & & &
 \end{array}$$

Let \mathfrak{p}_K be a prime of K lying below \mathfrak{p} , \mathfrak{p} in $K\tilde{F}$ as above. Let $\nu_1(\mathfrak{p}_K)$, $\nu_2(\mathfrak{p}_K)$ be two independent topological generators of its decomposition group $D_{\mathfrak{p}_K}$ in $\text{Gal}(K\tilde{F}/K)$. Since $D_{\mathfrak{p}_K}$ fixes \mathfrak{p} , it acts on $I_{\mathfrak{p}}$, and it acts trivially because $\text{Gal}(\tilde{K}/K)$ is abelian and $I_{\mathfrak{p}}$ embeds in $\text{Gal}(\tilde{K}/K\tilde{F})$. Therefore $\nu_1(\mathfrak{p}_K) - 1$ and $\nu_2(\mathfrak{p}_K) - 1$ correspond to two relatively prime elements of Λ_2 which annihilate $\sum_{\mathfrak{p}|\mathfrak{p}_K} I_{\mathfrak{p}}$. Hence $\sum_{\mathfrak{p}|\mathfrak{p}_K} I_{\mathfrak{p}} \sim_{\Lambda_2} 0$ and moreover

$$\sum_{\mathfrak{p}|p} I_{\mathfrak{p}} = \sum_{\mathfrak{p}_K|p} \sum_{\mathfrak{p}|\mathfrak{p}_K} I_{\mathfrak{p}} \sim_{\Lambda_2} 0$$

because the number of such \mathfrak{p} is finite.

We have an exact sequence

$$0 \rightarrow \text{Gal}(L_0/L_{K\tilde{F}}) \rightarrow \text{Gal}(L_0/K\tilde{F}) \rightarrow \text{Gal}(L_{K\tilde{F}}/K\tilde{F}) \rightarrow 0,$$

i.e.

$$0 \rightarrow \sum_{\mathfrak{p}|p} I_{\mathfrak{p}} \rightarrow \text{Gal}(L_0/K\tilde{F}) \rightarrow Y_{K\tilde{F}} \rightarrow 0.$$

This and the hypothesis yield $\text{Gal}(L_0/K\tilde{F}) \sim_{\Lambda_2} 0$. It immediately follows that $\text{Gal}(L_0/\tilde{K}) \simeq Y_{\tilde{K}}/T_3 Y_{\tilde{K}} \sim_{\Lambda_2} 0$. This implies $Y_{\tilde{K}} \sim_{\Lambda_3} 0$ again by Proposition 3.1. ■

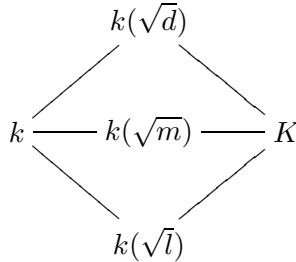
4. Numerical examples. We shall give some examples of real fields of degree 2^n over \mathbb{Q} , for some small n , for which Theorem 2.4 proves the conjecture, and some examples of biquadratic fields. In what follows we fix the prime $p = 3$.

4.1. The real case. For real fields we can use Theorem 2.2 to find biquadratic fields for which the conjecture holds. It suffices to choose K^{χ_i} , $i = 1, 2, 3$, among the fields given in [FT], [KS] and [IS]. Note that these papers cover all the cases $\mathbb{Q}(\sqrt{d})$ with $d < 10000$ and $d \equiv 0, 2 \pmod{3}$ while there are some gaps in [FT] for $d \equiv 1 \pmod{3}$. René Schoof kindly informed me that he is able to fill these gaps with a method similar to the one used in [KS] but the paper is not published yet.

After that we can combine biquadratic fields, using a quadratic field as the k of Theorem 2.4, to obtain the conjecture for fields of degree 8 and so

on. This procedure could lead to the determination of the “largest” field for which the conjecture is proved to hold to date.

For an explicit example fix the diagram



where m is the squarefree part of dl .

Assume $k = \mathbb{Q}$. Then we can prove the conjecture for the following K 's:

d	l	K	d	l	K
2	3	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	2	21	$\mathbb{Q}(\sqrt{2}, \sqrt{21})$
2	5	$\mathbb{Q}(\sqrt{2}, \sqrt{5})$	2	35	$\mathbb{Q}(\sqrt{2}, \sqrt{35})$
2	7	$\mathbb{Q}(\sqrt{2}, \sqrt{7})$	2	105	$\mathbb{Q}(\sqrt{2}, \sqrt{105})$
2	15	$\mathbb{Q}(\sqrt{2}, \sqrt{15})$			

Now assume $k = \mathbb{Q}(\sqrt{2})$. Then we get

d	l	K	d	l	K
3	5	$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$	3	35	$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{35})$
3	7	$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{7})$			

Finally with $k = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $d = 5, l = 7$ we get $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$.

In the same way we can prove the conjecture for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11})$ or $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{13})$ (and many others). The only thing that stops the process is the fact that we are limiting ourselves to $d, l, m < 10000$.

4.2. The complex case. Let $F = \mathbb{Q}(\sqrt{-d}), E = \mathbb{Q}(\sqrt{-l})$ and $H = \mathbb{Q}(\sqrt{m})$ with $d, l > 0$ squarefree and m the squarefree part of dl . For any number field k let h_k be its class number.

In [Mi] the conjecture is proved in the following cases:

- (1) $(h_F, 3) = 1$;
- (2) $d \equiv 2 \pmod{3}$ and A_F is generated by powers of primes lying above p ;
- (3) $d = 31, 247, 283, 298$.

We consider the “nontrivial” cases of (2) and (3), i.e. the ones in which 3 divides h_F . Examples for case (1) can be found in a similar way.

Fix one of the four fields in (3). To build our biquadratic extension according to Corollary 3.4 we need $E = \mathbb{Q}(\sqrt{-l})$ with:

- (i) $l \equiv 0 \pmod{3}$, to avoid the splitting of 3 in E or H ;
- (ii) $(h_E, 3) = 1$.

We will limit ourselves to $0 < l < 500$ and $0 < m < 10000$. We shall give all the possible combinations in this range for the four fields above.

1. $F = \mathbb{Q}(\sqrt{-31})$: 38 fields. We distinguish two cases:

- (a) 31 does not divide l : then $31l = m < 10000$ implies $l < 323$. Together with conditions (i) and (ii) this gives 36 values, namely $l = 3, 6, 15, 21, 30, 33, 39, 42, 51, 57, 66, 69, 78, 102, 105, 111, 114, 123, 138, 141, 159, 165, 177, 183, 195, 210, 213, 219, 258, 267, 273, 282, 285, 291, 303, 321$;
- (b) 31 divides l : then $m = l/31$. Between 0 and 500 we find only two values $l = 93, 465$.

2. $F = \mathbb{Q}(\sqrt{-283})$: 6 fields. To have $m < 10000$ we need $l < 36$ and we find 6 values, namely $l = 3, 6, 15, 21, 30, 33$.

3. $F = \mathbb{Q}(\sqrt{-298})$: 12 fields. We distinguish three cases:

- (a) $(298, l) = 1$: then $298l = m < 10000$ yields $l < 34$. There are 4 values, namely $l = 3, 15, 21, 33$;
- (b) $(298, l) = 2$: then $m = 298l/4 < 10000$ yields $l < 135$. There are 7 values, $l = 6, 30, 42, 66, 78, 102, 114$;
- (c) $(298, l) = 149$: between 0 and 500 we only get $l = 447$.

4. $F = \mathbb{Q}(\sqrt{-247})$: 16 fields. We distinguish three cases:

- (a) $(247, l) = 1$: $l < 40$. There are 6 values, namely $l = 3, 6, 15, 21, 30, 33$;
- (b) $(247, l) = 13$: then $m = 247l/169$ and between 0 and 500 we get $l = 39, 78, 195, 273, 390, 429$;
- (c) $(247, l) = 19$: in our range we have $l = 57, 114, 285, 399$.

The same thing can be done with the fields in (2) choosing E such that

- (i) $l \equiv 0, 1 \pmod{3}$, to avoid splitting in E or H ;
- (ii) $(h_E, 3) = 1$.

We give just one example:

5. $F = \mathbb{Q}(\sqrt{-23})$: 117 fields. We distinguish two cases:

- (a) $(23, l) = 1$: $l < 435$. There are 108 values, namely $l = 1, 3, 6, 7, 10, 13, 15, 19, 21, 22, 30, 33, 34, 37, 39, 42, 43, 51, 55, 57, 58, 66, 67, 70, 73, 78, 79, 82, 85, 91, 93, 94, 97, 102, 103, 105, 111, 114, 123, 127, 130, 133, 141, 142, 145, 151, 154, 159, 163, 165, 166, 177,$

- 178, 181, 183, 187, 190, 193, 195, 205, 210, 213, 217, 219, 223, 226, 229, 235, 238, 258, 259, 265, 267, 271, 273, 282, 285, 291, 295, 301, 303, 310, 313, 319, 321, 330, 337, 346, 349, 354, 355, 357, 373, 381, 382, 385, 390, 394, 399, 402, 403, 406, 409, 415, 418, 421, 427, 429;
- (b) 23 divides l : in our range we have $l = 46, 69, 115, 138, 253, 322, 345, 391, 483$.

References

- [Ba] A. Bandini, *Capitulation of ideals in \mathbb{Z}_p^d -extensions*, preprint, University of Pisa, 2002.
- [FT] T. Fukuda and H. Taya, *The Iwasawa λ -invariants of \mathbb{Z}_p -extensions of real quadratic fields*, Acta Arith. 69 (1995), 277–292.
- [Gr1] R. Greenberg, *The Iwasawa invariants of Γ -extensions of a fixed number field*, Amer. J. Math. 95 (1973), 204–214.
- [Gr2] —, *On the Iwasawa invariants of totally real number fields*, ibid. 98 (1976), 263–284.
- [Gr3] —, *Iwasawa theory—Past and present*, Adv. Stud. Pure Math. 30 (2001), 335–385.
- [Hu] D. Hubbard, *The nonexistence of certain free pro- p -extensions and capitulation in a family of dihedral extensions of \mathbb{Q}* , Ph.D. thesis, Univ. of Washington, 1996.
- [IS] H. Ichimura and H. Sumida, *On the Iwasawa invariants of certain real abelian fields*, Tohoku Math. J. 49 (1997), 203–215.
- [Iw] K. Iwasawa, *On \mathbb{Z}_l -extensions of algebraic number fields*, Ann. of Math. 98 (1973), 246–326.
- [KS] J. S. Kraft and R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. 97 (1995), 135–155.
- [LN] A. Lannuzel et T. Nguyen Quang Do, *Conjectures de Greenberg et extensions pro- p -libres d'un corps de nombres*, Manuscripta Math. 102 (2000), 187–209.
- [Ma] D. C. Marshall, *Galois groups and Greenberg's conjecture*, Ph.D. thesis, Univ. of Arizona, 2000.
- [McC] W. G. McCallum, *Greenberg's Conjecture and units in multiple \mathbb{Z}_p -extensions*, Amer. J. Math. 123 (2001), 909–930.
- [Mi] J. Minardi, *Iwasawa modules for \mathbb{Z}_p^d -extensions of algebraic number fields*, Ph.D. thesis, Univ. of Washington, 1986.
- [PR] B. Perrin-Riou, *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, Bull. Soc. Math. France Mém. 17 (1984).
- [Se] J. P. Serre, *Classes des corps cyclotomiques (d'après K. Iwasawa)*, Sémin. Bourbaki Exp. 174 (1958), in: Sémin. Bourbaki 5, Soc. Math. de France, 1995, 83–93.
- [Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

via I. Bargagna n. 42
56124 Pisa, Italy
E-mail: bandini@mail.dm.unipi.it

Received on 2.8.2001

(4089)