GREENBERG'S CONJECTURE AND CYCLOTOMIC TOWERS

DAVID C. MARSHALL

Abstract. We describe Greenberg's pseudo-null conjecture, and prove a result describing conditions under which the pseudo-null conjecture for a number field K implies the conjecture for finite extensions of K. We then apply the result to the cyclotomic $\mathbb{Z}_p$-tower above a cyclotomic field of prime roots of unity, verifying the conjecture for a large class of cyclotomic fields.

1. Greenberg's conjecture

In the late 1950's Iwasawa introduced a powerful technique for studying class groups and unit groups of number fields. Motivated by the theory of curves over finite fields, Iwasawa's theory of $\mathbb{Z}_p$-extensions has since become a widely used tool in algebraic number theory, Galois theory, and arithmetic geometry. We describe in this section a conjecture of Greenberg concerning the structure of a classical Iwasawa module, and we mention a Galois theoretic consequence concerning free pro-p-extensions of number fields.

Let K be an algebraic number field and p an odd prime. By a *multiple* $\mathbb{Z}_p$-*extension* K_∞/K we mean a Galois extension with Galois group $\Gamma \simeq \mathbb{Z}_p^d$ for some positive integer d. In what follows we will be particularly interested in two such extensions of K for which we reserve the following notation:

- K^{cyc}/K denotes the *cyclotomic* $\mathbb{Z}_p$-extension of K.
- $\widetilde{K}/K$ denotes the compositum of all $\mathbb{Z}_p$-extensions of K.

Let F be a finite extension of K contained in K_∞, and denote by $A(F)$ the Sylow p-subgroup of the ideal class group of F. The Galois group of F/K acts on $A(F)$ in the natural way, making $A(F)$ into a $\mathbb{Z}_p[\mathrm{Gal}(F/K)]$-module. As F varies over all finite subextensions the $A(F)$ form an inverse system (under norm maps) and we denote by A the inverse limit. The group A then carries a natural structure as a module over the Iwasawa algebra

$$\mathbb{Z}_p[[\Gamma]] := \varprojlim_{F} \mathbb{Z}_p[\mathrm{Gal}(F/K)].$$

It is common to study A by identifying the $A(F)$ with Galois groups as follows. By class field theory, the group $A(F)$ is isomorphic to the Galois group, X_F, of the maximal abelian unramified p-extension of F (the *p-Hilbert class field of* F).

Date: June 12, 2003.
2000 *Mathematics Subject Classification.* Primary 11R23; Secondary 11R18, 11R32.

The isomorphism respects the Galois module structure, the action of $\mathrm{Gal}(F/K)$ on X_F being inner automorphism. The X_F form an inverse system (the maps being given by restriction of automorphisms) and the limit X is the Galois group of the maximal abelian unramified pro-p-extension of K_∞. So $X \simeq A$.

The Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$ is non-canonically isomorphic to the power series ring

$$\Lambda := \mathbb{Z}_p[[T_1, T_2, \ldots, T_d]],$$

where topological generators γ_i of Γ are sent to $1 + T_i$. So the $\mathbb{Z}_p[[\Gamma]]$-module structure of A is studied via the Λ-module structure of X (noting that $T_i x = x^{\gamma_i - 1}$).

For K_∞/K any multiple $\mathbb{Z}_p$-extension Greenberg ([3], Theorem 1) has shown X to be a finitely generated torsion Λ-module. In particular, the annihilator of X, $\mathrm{Ann}_\Lambda(X)$, is non-trivial. Traditionally, annihilators of classical Iwasawa modules have been of much interest. The Main conjecture of Iwasawa theory gives the factors of the annihilator of X for the cyclotomic $\mathbb{Z}_p$-extension of a number field K as essentially the p-adic L-functions attached to K. There is also a two variable Main conjecture for certain $\mathbb{Z}_p^2$-extensions arising from the theory of elliptic curves.

Greenberg ([5], Conjecture 3.4) has conjectured that for the cyclotomic $\mathbb{Z}_p$-extension K^{cyc}/K of a totally real field K, the module X is finite. If a totally real field K satisfies Leopoldt's conjecture the extensions K^{cyc} and $\widetilde{K}$ coincide (i.e. K has only one $\mathbb{Z}_p$-extension). Furthermore, when $\Lambda = \mathbb{Z}_p[[T]]$ it can be shown that a module being finite is equivalent to having an annihilator of height at least 2. With this in mind the above conjecture is a special case of the more general conjecture ([5], Conjecture 3.5):

Conjecture 1. *Let K be any number field and $\widetilde{K}$ the compositum of all $\mathbb{Z}_p$-extensions of K. Then $\mathrm{Ann}_\Lambda(X)$ has height at least 2.*

A Λ-module whose annihilator has height at least 2 is said to be *pseudo-null*, and we will refer to Conjecture 1 above as *Greenberg's conjecture*, or just the *pseudo-null conjecture*.

The point of this note is two-fold. First, we prove a "going-up" theorem for the pseudo-null conjecture. Namely, if K is a number field, and F is a finite extension of K in $\widetilde{K}$, we give conditions under which Greenberg's conjecture for K implies Greenberg's conjecture for F (Theorem 6). The result is an exercise in utilizing several equivalent formulations of the conjecture. Versions of these formulations have appeared in Lannuzel and Nguyen-Quang-Do ([9], Theorem 4.4) as well as work of McCallum [11] and this author [10]. Secondly, as an application of the result, we consider the example $K = \mathbb{Q}(\zeta_p)$ and $F = \mathbb{Q}(\zeta_{p^n})$. We verify the conjecture for a certain class of such K's, implying the conjecture for each field in the corresponding $\mathbb{Z}_p$-tower.

The key argument in both results is reduced to a capitulation problem, namely the need for a set of ideals, or ideal classes, to become principal when extended to an appropriate field. For the "going-up" result, the resolution of this problem is provided by an equivalent form of the conjecture, stating that all ideal classes capitulate in $\widetilde{K}$. In verifying the conjecture for $\mathbb{Q}(\zeta_p)$ capitulation is obtained by more direct means. We state our second result here.

Let $K = \mathbb{Q}(\zeta_p)$, $E = \mathcal{O}_K^\times$ and $U = \mathcal{O}_{K_\pi}^\times$, where π is the unique prime of K above p. Denote by $\overline{E}$ the closure of E in U. We denote by λ_p the Iwasawa lambda invariant of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\zeta_p)$. Let v_p denote the p-adic valuation. In Section 4 we prove

Theorem 1. *Suppose $K = \mathbb{Q}(\zeta_p)$ satisfies the following conditions:*

(1) *Vandiver's conjecture*
(2) $\lambda_p = 1$.
(3) $v_p(|(U/\overline{E})[p^\infty]|) \leq v_p(|A(K)|)$.

Then for all $n \geq 1$ the pseudo-null conjecture holds for $\mathbb{Q}(\zeta_{p^n})$.

We mention here one Galois theoretic consequence of the pseudo-null conjecture for cyclotomic fields. The existence of free pro-p-extensions (Galois extensions with Galois group a free pro-p-group) has been the subject of much study. See for example the list of known results in [15]. Let $K = \mathbb{Q}(\zeta_{p^n})$ for some $n > 0$, and let Ω_K denote the maximal pro-p extension of K which is unramified at all primes not dividing p. Let $\mathcal{G}_K$ denote the Galois group.

Since free pro-p-extensions are unramified outside p, such extensions of K are contained in Ω_K. We will see that $\mathcal{G}_K$ is a free pro-p group exactly when p is a regular prime (since the number of relations defining $\mathcal{G}_K$ is equal to the p-rank of the class group of K). When p is an irregular prime the group $\mathcal{G}_K$ is not free, but we may look for free pro-p quotients. Let r_2 denote the number of complex places of K. Then Leopoldt's conjecture predicts $r_2 + 1$ independent $\mathbb{Z}_p$-extensions of K, and so the maximal rank of a free pro-p-extension of K is bounded above by $r_2 + 1$. The following is proved in [9], as well as [11]:

Theorem 2. *Suppose that $K = \mathbb{Q}(\zeta_{p^n})$ satisfies Greenberg's conjecture. Then $\mathcal{G}_K$ has a free pro-p-quotient of rank $r_2 + 1$ if and only if p is regular.*

We give here a brief outline of the paper. In Section 2, we introduce several auxiliary Λ-modules and Galois groups needed for the later study. Theorem 3 and Lemma 1 are the key results of this section, implying a sufficient condition for a standard Iwasawa module to be torsion free (Corollary 1). In Section 3 we recall and provide several equivalent formulations of Greenberg's pseudo-null conjecture, and we state and prove one of our main results (the "going-up" theorem). Finally, in Section 4 we turn to the example furnished by cyclotomic fields, proving Theorem 1 above.

Acknowledgements This work is an outgrowth of the authors Ph.D. thesis and he would like to thank his advisor Bill McCallum, as well as Ralph Greenberg and Manfred Kolster for useful conversations and comments. This work was partially supported by NSF VIGRE grant 9977116.

2. Auxiliary modules

For a number field K and a prime number p, we call a field extension of K *p-ramified* if it is unramified at all primes of K not dividing p. We fix the following notation:
The fields:

Ω_K	the maximal pro-p, p-ramified extension of K
$\widetilde{K}$	the compositum of all $\mathbb{Z}_p$-extensions of K
L_∞	the maximal abelian unramified pro-p-extension of $\widetilde{K}$
M_∞	the maximal abelian p-ramified pro-p-extension of $\widetilde{K}$
N_∞	the extension of $\widetilde{K}$ generated by p-power roots of p-units of $\widetilde{K}$

The Galois groups:

$\mathcal{G}_K$	the Galois group of Ω_K/K
Γ	the Galois group of $\widetilde{K}/K$
X	the Galois group of $L_\infty/\widetilde{K}$
Y	the Galois group of $M_\infty/\widetilde{K}$
Y'	the Galois group of $N_\infty/\widetilde{K}$

The Galois groups Y and Y' carry an action of Γ via conjugation, just as X, making them into Λ-modules. We shall see that for certain base fields K, the pseudo-null conjecture may be formulated in terms of the Λ-module structure of Y (in particular, that Y is Λ-torsion free). The module Y is known to be finitely generated, and, for $K/\mathbb{Q}$ abelian, have Λ-rank equal to r_2, where r_2 denotes the number of complex places of K ([4]). For a Λ-module M we write $\mathrm{Tor}_\Lambda(M)$ for the Λ-torsion submodule. The following result is due to McCallum.

Theorem 3 ([11], Theorem 3)**.** *Suppose there is only one prime of K above p, and $\widetilde{K}$ contains all p-power roots of unity. Then* $\mathrm{Tor}_\Lambda(Y') = 0$.

Remark 1: The proof of this result involves a detailed analysis of the filtration

$$E_F^u \subset E_F^n \subset E_F^{\mathrm{loc}} \subset E_F,$$

where E_F denotes the units $\mathcal{O}_F[1/p]^\times$ of a finite extension F of K in $\widetilde{K}$, and the superscripts denote certain classes of universal norms (see Section 4 of [11] for the precise definitions). The torsion submodule of Y' is contained in the kernel of a surjective map of Galois groups. The Pontryagin dual of this kernel is $\varinjlim_F (E_F/E_F^u) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, and is shown to be zero by considering each graded factor from the filtration.

Remark 2: In particular, the result tells us $\mathrm{Tor}_\Lambda(Y)$ fixes the field N_∞. This observation, combined with Lemma 1 below, gives our approach to verifying the pseudo-null conjecture.

The group $\mathcal{G}_K$ has a minimal free presentation

$$1 \longrightarrow R \longrightarrow F_g \longrightarrow \mathcal{G}_K \longrightarrow 1,$$

where F_g is the free pro-p-group on g generators and R is the normal closure of a finitely generated subgroup (the group of relations for $\mathcal{G}_K$). Denote by s the minimal number of (topological) generators of R. The numbers g and s are equal to the $\mathbb{F}_p$-dimensions of $H^i(\mathcal{G}_K, \mathbb{Z}/p\mathbb{Z})$, $i = 1, 2$ respectively (see Chapter 4 of [13]).

Let $\mathcal{G}_K^{ab}$ denote the maximal abelian quotient of $\mathcal{G}_K$, and M_K the maximal abelian p-ramified pro-p-extension of K (so $\mathcal{G}_K^{ab} = \mathrm{Gal}(M_K/K)$). The field M_K is an abelian, p-ramified extension of $\widetilde{K}$ (the Galois group of $M_K/\widetilde{K}$ is just the torsion subgroup of $\mathcal{G}_K^{ab}$), and so is contained in the field M_∞. Hence we have a natural map from Y to $\mathcal{G}_K^{ab}$ given by restriction of automorphisms. We refer the reader to [11] for a proof of the following.

Lemma 1 ([11], Lemma 24). *Suppose K satisfies Leopoldt's conjecture. If $\mathcal{G}_K$ is a one-relator group (i.e. $s = 1$), then the map*

$$\mathrm{Tor}_\Lambda(Y) \longrightarrow \mathcal{G}_K^{ab}$$

is the zero map if and only if $\mathrm{Tor}_\Lambda(Y) = 0$.

The following is an immediate consequence of Theorem 3 and Lemma 1:

Corollary 1. *If K is a number field satisfying the hypotheses of Theorem 3 and Lemma 1, then*

$$M_K \subset N_\infty \textit{ implies } \mathrm{Tor}_\Lambda(Y) = 0. \tag{1}$$

3. Equivalent formulations

We have introduced the natural Iwasawa modules X and Y in the last section. The Galois action on each of the X_F is also compatible with regard to extensions of ideal classes, so we may form the Λ-module $\varinjlim_F X_F$ as well. Recall the groups $\mathrm{Ext}^i_\Lambda(\cdot, \Lambda)$ are the right derived functors of $\mathrm{Hom}_\Lambda(\cdot, \Lambda)$.

Theorem 4. *Let p be an odd prime and let K be a number field with a unique prime above p. Then $\mathrm{Ext}^1_\Lambda(X, \Lambda)$ is the Pontryagin dual of $\varinjlim_F X_F$, where the F vary over the finite extensions of K in $\widetilde{K}$.*

Proof: Let $\mathfrak{m}$ denote the unique maximal ideal of $\Lambda = \mathbb{Z}_p[[T_1, \ldots, T_r]]$, and define

$$\omega_n(T_i) = (1+T_i)^{p^n} - 1.$$

The result is obtained by establishing the isomorphism

$$H^r_{\mathfrak{m}}(X) \simeq \varinjlim_F X_F, \tag{2}$$

where $H^i_{\mathfrak{m}}(X)$ denotes Grothendieck's local cohomology relative to the $\mathfrak{m}$-primary sequences

$$\mathbf{x}_n = (p^n, \omega_n(T_1), \ldots, \omega_n(T_r)).$$

The desired result is then a consequence of (a version of) Grothendieck's local duality; namely

$$\mathrm{Ext}^{N-i}_\Lambda(X, \Lambda) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(H^i_{\mathfrak{m}}(X), \mathbb{Q}/\mathbb{Z}),$$

where N denotes the length of the $\mathfrak{m}$-primary sequence. A good reference for this material is Chapter 3 of [1].

The details establishing (2) can be found in Theorem 8 of [11], where McCallum proves a similar result for the Galois group X' of the maximal abelian unramified pro-p-extension of $\widetilde{K}$ in which all primes dividing p are completely decomposed. The proof translates easily to this case, simply replacing the decomposition group with inertia. □

Let μ_n denote the group of n-th roots of unity. As above, we let X'_F denote the Galois group of the maximal abelian unramified extension of F in which all primes dividing p are completely decomposed. We write X' for $X'_{\widetilde{K}}$.

Theorem 5. *Let $p > 5$ be a prime and suppose μ_p is in K. If K has a unique prime ideal $\wp$ dividing p, then the following are equivalent:*
(a) X is pseudo-null
(b) X' is pseudo-null
(c) $\mathrm{Tor}_\Lambda(Y) = 0$
(d) $\varinjlim_F X'_F = 0$
(e) $\varinjlim_F X_F = 0$,
where the fields F vary over all finite extensions of K in $\widetilde{K}$.

Proof: $(a) \Leftrightarrow (b)$. Recall $\Gamma = \mathrm{Gal}(\widetilde{K}/K)$. We let $\Gamma_\wp$ denote the decomposition group of $\wp$ in Γ, and let $\Lambda_\wp = \mathbb{Z}_p[[\Gamma/\Gamma_\wp]]$. There is a natural surjection $X \to X'$ whose kernel is generated as a $\mathbb{Z}_p$-module by the Frobenius automorphisms corresponding to the primes above p, and therefore is finitely generated as a module over $\Lambda_\wp$. As a Λ-module, the annihilator of $\Lambda_\wp$ has height equal to the $\mathbb{Z}_p$-rank of $\Gamma_\wp$ (this is just the augmentation ideal in $\mathbb{Z}_p[[\Gamma_p]]$). Since there is only one prime of K above p, its decomposition group has finite index in Γ, and therefore our assumption on p makes $\Lambda_\wp$ pseudo-null. Therefore the kernel of the surjection $X \to X'$ is pseudo-null, and X and X' are pseudo-isomorphic.

$(a) \Leftrightarrow (c)$. This follows from a duality due to Jannsen ([8], Theorem 5.4) relating the Λ-modules X' and Y, together with a structure theorem for Y due to Nguyen-Quang-Do (Corollary 14 of [11] or Theorem 4.4 of [9]).

$(c) \Leftrightarrow (d)$. In proving the results cited in the previous case, one shows, in particular, that

$$\mathrm{Tor}_\Lambda(Y) \simeq \mathrm{Ext}^1_\Lambda(X', \Lambda)$$

([11], Theorem 9). But $\mathrm{Ext}^1_\Lambda(X', \Lambda)$ is known to be the Pontryagin dual of $\varinjlim_F X'_F$ ([11], Theorem 8). The result then follows.

$(c) \Leftrightarrow (e)$. Grothendieck's local duality can be used to show that a torsion Λ-module is pseudo-null if and only if Ext^1_Λ vanishes ([11], Lemma 6). This implies, in particular, that $\mathrm{Ext}^1_\Lambda(X, \Lambda)$ and $\mathrm{Ext}^1_\Lambda(X', \Lambda)$ are isomorphic, yielding

$$\mathrm{Tor}_\Lambda(Y) \simeq \mathrm{Ext}^1_\Lambda(X, \Lambda)$$

as well. Theorem 4 then finishes the proof. □

Remark: Various forms of these equivalences have certainly appeared elsewhere. In [9], Lannuzel and Nguyen-Quang-Do prove the equivalence of (a), (c), and (e) under slightly different hypotheses. Namely, no restriction is made on the number of primes of K dividing p, but rather it is assumed that all finite extensions of K in $\widetilde{K}$ satisfy Leopoldt's conjecture. Formulation (c) has been used by McCallum [11] and this author [10] to verify Greenberg's conjecture for certain classes of cyclotomic fields.

The following theorem provides sufficient conditions for when the pseudo-null conjecture for a number field K implies the conjecture for a finite extension of K in $\widetilde{K}$. We apply this to the cyclotomic tower in Section 4.

Theorem 6. *Let $p \geq 5$ be a prime and suppose μ_p is contained in K. Suppose K has a unique prime $\wp$ dividing p. Then, if $F \subset \widetilde{K}$ is a finite extension of K satisfying*

(1) *$\wp$ is non-split in F/K*
(2) $\dim_{\mathbb{F}_p} H^2(\mathcal{G}_F, \mathbb{Z}/p\mathbb{Z}) \leq 1$
(3) *Leopoldt's conjecture,*

then Greenberg's conjecture for K implies Greenberg's conjecture for F.

Proof: Let K and F be number fields satisfying the above hypotheses, and assume the pseudo-null conjecture holds for K. We apply the notation introduced in Section 2 to the field F (so we have Ω_F, $\mathcal{G}_F$, M_F, etc.) If the $\mathbb{F}_p$-dimension of $H^2(\mathcal{G}_F, \mathbb{Z}/p\mathbb{Z})$ is 0, then $\mathcal{G}_F$ is a free pro-p-group. A structure theorem for Y due to Nguyen Quang Do ([12], Proposition 1.7) then implies $\mathrm{Tor}_\Lambda(Y) = 0$. Hence by formulation (c) of Theorem 5 Greenberg's conjecture holds for F.

If the $\mathbb{F}_p$-dimension of $H^2(\mathcal{G}_F, \mathbb{Z}/p\mathbb{Z})$ is 1, then such an F satisfies the hypotheses of Theorem 3 and Lemma 1, and so Corollary 1 applies. Namely, Greenberg's pseudo-null conjecture will hold for F provided $M_F \subset N_\infty$, and hence it will suffice to show the extension $M_F/\widetilde{F}$ is generated by p-power roots of p-units of $\widetilde{F}$.

We consider the field $F^{cyc} = FK^{cyc}$, the cyclotomic $\mathbb{Z}_p$-extension of F. By assumption, this field contains all p-power roots of unity. Recall the group $\mathcal{G}_F^{ab} = \mathrm{Gal}(M_F/F)$. The subgroup $\mathrm{Gal}(M_F/F^{cyc})$ has the same torsion subgroup (which is just $\mathrm{Gal}(M_F/\widetilde{F})$) and $\mathbb{Z}_p$-rank 1 less. In particular, we have a non-canonical isomorphism

$$\mathrm{Gal}(M_F/F^{cyc}) \simeq \mathrm{Gal}(\widetilde{F}/F^{cyc}) \times \mathrm{Gal}(M_F/\widetilde{F}).$$

We let L denote the fixed field of the first factor (so $M_F = \widetilde{F}L$.)

The Galois group $\mathrm{Gal}(L/F^{cyc})$ is isomorphic to the torsion subgroup of $\mathcal{G}_F^{ab}$, and hence is a finite p-group. Since F^{cyc} contains all p-power roots of unity, the extension L/F^{cyc} is just a Kummer extension, generated by p-power roots of elements of F^{cyc},

$$L = F^{cyc}(x_1^{1/p^{m_1}}, x_2^{1/p^{m_2}}, \ldots, x_n^{1/p^{m_n}}).$$

Further, the ideals (x_i) are p^{m_i}-th powers of ideals of F^{cyc}, say $(x_i) = \mathsf{J}_i^{p^{m_i}}$.

The extension $M_F/\widetilde{F}$ is also generated by the $x_i^{1/p^{m_i}}$, and the ideals (x_i) are the p^{m_i}-th powers of the ideals J_i extended to $\widetilde{F}$. But here is the key: the ideal classes $[\mathsf{J}_i]$ become *principal classes* when extended to $\widetilde{F}$. This follows from the fact that $F^{cyc} \subset \widetilde{K}$ and, having assumed the pseudo-null conjecture holds for K (using formulation (e) of Theorem 5), the fact that all ideal classes become principal in $\widetilde{K}$.

For a generator $x_i^{1/p^{m_i}}$ of $M_F/\widetilde{F}$ we now know the ideal (x_i) is the p^{m_i}-th power of a principal ideal, say

$$(x_i) = (y_i)^{p^{m_i}}.$$

The elements x_i and $y_i^{p^{m_i}}$ must differ by a unit, say $x_i = uy_i^{p^{m_i}}$. But clearly, an extension generated by a p^{m_i}-th root of x_i is also generated by a p^{m_i}-th root of $x_i/(y_i^{p^{m_i}}) = u$, and so the extension $M_F/\widetilde{F}$ is generated by p-power roots of units on $\widetilde{F}$. This implies $M_F \subset N_\infty$ which, by Corollary 1 and Theorem 5, implies Greenberg's conjecture for F. □

4. Cyclotomic Fields

We fix p a prime number and consider more closely the case of the cyclotomic fields $K = \mathbb{Q}(\zeta_{p^n})$. Recall the group $\mathcal{G}_K$ has a minimal presentation as a pro-p-group with g generators and s relations, where g and s are equal to the $\mathbb{F}_p$-dimensions of $H^1(\mathcal{G}_K, \mathbb{Z}/p\mathbb{Z})$ and $H^2(\mathcal{G}_K, \mathbb{Z}/p\mathbb{Z})$ respectively.

Lemma 2. *Let p be a prime and let $K = \mathbb{Q}(\zeta_{p^n})$ for some natural number n. Let α denote the $\mathbb{Z}/p\mathbb{Z}$-rank of the p-class group of K. Then*

$$g = \frac{p^n + p^{n-1} + 2}{2} + \alpha$$
$$s = \alpha.$$

Proof: These computations are not new, and we give here just a sketch. Let Ω'_K be the maximal p-ramified extension of K with Galois group $\mathcal{G}'_K$. Since K contains the group μ_p, and $\mathcal{G}_K$ is the maximal pro-p quotient of $\mathcal{G}'_K$, we have

$$H^i(\mathcal{G}_K, \mathbb{Z}/p\mathbb{Z}) \simeq H^i(\mathcal{G}'_K, \mu_p).$$

The $\mathbb{Z}/p\mathbb{Z}$-dimensions of the latter groups can be obtained by considering the sequence

$$1 \longrightarrow \mu_p \longrightarrow \mathcal{O}_{\Omega'_K}[1/p]^\times \xrightarrow{p} \mathcal{O}_{\Omega'_K}[1/p]^\times \longrightarrow 1.$$

The p-power map on $\mathcal{O}_{\Omega'_K}[1/p]^\times$ is surjective by the maximality of Ω'_K over K (since p-th roots of p-units generate p-ramified extensions). Taking cohomology of the sequence with respect to the Galois group $\mathcal{G}'_K$ yields a long exact sequence which may be broken into the following pair of short exact sequences.

$$0 \to \frac{\mathcal{O}_K[1/p]^\times}{(\mathcal{O}_K[1/p]^\times)^p} \to H^1(\mathcal{G}'_K, \mu_p) \to C(K)[p] \to 0$$

$$0 \to \frac{C(K)}{pC(K)} \to H^2(\mathcal{G}'_K, \mu_p) \to H^2(\mathcal{G}'_K, \mathcal{O}_{\Omega'_K}[1/p]^\times)[p] \to 0,$$

where $C(K)$ denotes the ideal class group of K. The group $H^2(\mathcal{G}'_K, \mathcal{O}_{\Omega'_K}[1/p]^\times)$ injects into the Brauer group $B(K)$, and can be shown to be 0 by considering its behavior in the exact sequence

$$0 \to B(K) \to \oplus_v B(K_v) \xrightarrow{\sum inv} \mathbb{Q}/\mathbb{Z} \to 0.$$

A simple dimension count then gives

$$g = r_2 + 1 + \alpha$$
$$s = \alpha$$

where $r_2 = (p^n + p^{n-1})/2$, as desired. □

If p is a regular prime, $\alpha = 0$ for $\mathbb{Q}(\zeta_{p^n})$, $n \geq 0$. Hence $s = 0$, implying $\mathrm{Tor}_\Lambda(Y) = 0$, establishing Greenberg's conjecture for each field in the cyclotomic tower.

The following corollary is an immediate consequence of Theorem 6 and Lemma 2.

Corollary 2. *Let p be an irregular prime. Let $n > 0$ be such that $\mathbb{Q}(\zeta_{p^n})$ has a cyclic p-class group. Then Greenberg's conjecture for $\mathbb{Q}(\zeta_p)$ implies Greenberg's conjecture for $\mathbb{Q}(\zeta_{p^n})$.*

Proof: In the notation of Theorem 6, with K as above, let $F = \mathbb{Q}(\zeta_{p^n})$ for some positive integer n satisfying the hypothesis. The field K has a unique prime π above p, and π is totally ramified in F/K, and hence non-split. The dimension of $H^2(\mathcal{G}_F, \mathbb{Z}/p\mathbb{Z})$ is less than or equal to 1 by our assumption of cyclic p-class groups. Since $F/\mathbb{Q}$ is abelian, implying Leopoldt's conjecture for F, the hypotheses of Theorem 6 are satisfied, as desired. □

Finally, we prove Theorem 1 by providing a class of cyclotomic fields $\mathbb{Q}(\zeta_p)$, satisfying the hypotheses of Corollary 2, for which the pseudo-null conjecture is true. A similar class was first given by McCallum ([11], Theorem 1). He considered such fields with p-class group isomorphic to $\mathbb{Z}/p\mathbb{Z}$. We provide here a slight generalization of that class, allowing for cyclic p-class groups of arbitrary p-power order, as well as apply Corollary 2 to extend the conjecture to all fields in the cyclotomic $\mathbb{Z}_p$-tower. We restate Theorem 1 here.

Theorem 7. *Suppose $K = \mathbb{Q}(\zeta_p)$ satisfies the following conditions:*

(1) *Vandiver's conjecture*
(2) $\lambda_p = 1$.
(3) $v_p(|(U/\overline{E})[p^\infty]|) \leq v_p(|A(K)|)$.

Then for all $n \geq 1$ the pseudo-null conjecture holds for $\mathbb{Q}(\zeta_{p^n})$.

Remark 1: Condition (2) is heuristically true for approximately 75% of all irregular primes and experimentally true for 75% of the irregular primes up to 12 million, according to [2] (for these primes, λ_p is just the index of irregularity of p).

Remark 2: Letting $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ and $A_n = A(K_n)$, the hypotheses of Vandiver's conjecture and $\lambda_p = 1$ imply

$$A_n \simeq X/((1+T)^{p^n}) - 1)X,$$

where $X = \mathbb{Z}_p[[T]]/(T + p^a)$ (see Theorem 10.16 and Proposition 13.22 of [14]). In particular this yields isomorphisms

$$A_n \simeq \mathbb{Z}/p^{a+n}\mathbb{Z}$$

for all $n \geq 0$, and so (3) is a condition on cyclic groups of p-power order.

Remark 3: Since $A(K)$ is cyclic, there is only one Bernoulli number B_i, $2 \leq i \leq p-3$, divisible by p. If B_{p-j} denotes this term (so $\varepsilon_j A(K)$ is the non-trivial term of the idempotent decomposition of $A(K)$),then $L_p(s, \omega^{1-j})$ is the only non-trivial p-adic L-function attached to K. It follows from Theorem 8.25 of [14] that

$$(U/\overline{E})[p^\infty] \simeq \mathbb{Z}/p^m\mathbb{Z},$$

where $m = v_p(L_p(1, \omega^{1-j}))$. This valuation may be computed in terms of the characteristic power series $f(T)$ of $\varprojlim_n A(K_n)$. Under the assumption $\lambda_p = 1$

this power series has the form $f(T) = (T + cp^a)u$, where u is a unit, p^a is the order of the cyclic group $A(K)$, and

$$f((1+p)^s - 1) = L_p(s, \omega^{1-j}).$$

So the valuation of L_p at $s = 1$ equals the valuation of $f(p) = (p + cp^a)u$.

If $a > 1$, $v_p(f(p)) = 1$, and condition (3) is satisfied. If, on the other hand, $a = 1$, $v_p(f(p))$ depends on the value of $c \pmod p$. The valuation will again be 1 provided $c \not\equiv -1 \pmod p$. This congruence has been checked for $p < 4000$ in [6], although tables are only given for $p < 400$ and $3600 < p < 4000$. For these values the congruence condition is satisfied.

Suppose $K = \mathbb{Q}(\zeta_p)$ satisfies (1)-(3) above. Since $A(K)$ is cyclic, say of order p^a, the group $\mathcal{G}$ is a one-relator group and Lemma 1 applies. We will utilize this lemma to show $\mathrm{Tor}_\Lambda(Y) = 0$. In light of Corollary 1, it suffices to show $M_K \subset N_\infty$, and so we consider the structure of $\mathcal{G}_K^{ab}$ in more detail.

Lemma 3. *Suppose K satisfies hypothesis (1) and (2) of Theorem 7. Then the torsion subgroup of $\mathcal{G}_K^{ab}$ is cyclic.*

Proof: Let J_K denote the idele group of K, with $K^\times$ embedded diagonally. Let U be the subgroup of ideles which are units at π (the prime of K above p) and 1 elsewhere, and let U' be the subgroup of ideles which are 1 at π and units elsewhere. Class field theory gives an isomorphism

$$\mathcal{G}_K^{ab} \simeq \text{pro-}p\text{-completion of } J_K/(\overline{K^\times U'}),$$

where the overline denotes the closure.

If we let $\overline{E}$ denote the closure of the embedding of the units of K in U, then in fact we have an exact sequence

$$0 \longrightarrow U_1/\overline{E}_1 \longrightarrow \mathcal{G}_K^{ab} \longrightarrow A(K) \longrightarrow 0,$$

where the subscript 1 indicates we are taking units congruent to 1 modulo π. Since U_1 has $\mathbb{Z}_p$-rank $[K : \mathbb{Q}] = p-1$ and $\overline{E_1}$ has $\mathbb{Z}_p$-rank $(p-3)/2$ (by Leopoldt's conjecture, which holds for K), the $\mathbb{Z}_p$-rank of $\mathcal{G}_K^{ab}$ is $(p+1)/2$ ($p \neq 2$ by the assumption $\lambda_p = 1$).

We claim the torsion in $\mathcal{G}_K^{ab}$ comes from $U_1/\overline{E}_1$, and show this by considering an idele (a_v) whose image in $\mathcal{G}_K^{ab}$ is a torsion element, say of order p^m. So

$$(a_v)^{p^m} \in \overline{K^\times U'},$$

say $(a_v)^{p^m} = \alpha(u_v)$ (where we abuse notation writing α for both the element of $K^\times$ as well as its diagonal image in J_K). This implies α is a p^m-th power in K_π, the π-adic completion of K. Let a then be the ideal of K such that $\mathsf{a}^{p^m} = (\alpha)$. We want to show the class of a is principal.

Let $K_{m-1} = \mathbb{Q}(\zeta_{p^m})$, so $K_{m-1}(\alpha^{1/p^m})$ is an unramified extension. Since the class of a lies in $A(K)^-$ (by Vandiver's conjecture), the Kummer pairing implies the Galois group of $K_{m-1}(\alpha^{1/p^m})/K_{m-1}$ is trivial. Hence α must be a p^m-th power in K_{m-1} as well, which means the ideal class of a is principal when extended to K_{m-1} (represented by a principal ideal generated by a p^m-th root of α). But the map from $A(K)$ to $A(K_{m-1})$ is injective ([14], Proposition 13.26), and so a must have represented a principal class in $A(K)$ as well. Hence the torsion in $\mathcal{G}_K^{ab}$ maps to 0 in $A(K)$.

We now just need to determine the torsion subgroup of $U_1/\overline{E}_1$. We may consider each factor of the idempotent decomposition separately. Since $\varepsilon_i E_1 = 0$ for $i = 0$ and for i odd, and each $\varepsilon_i U_1 \simeq \mathbb{Z}_p$, we obtain

$$U_1/\overline{E}_1 \simeq (\mathbb{Z}_p)^{(p+1)/2} \oplus \bigoplus_{i \text{ even}} \varepsilon_i U_1/\varepsilon_i \overline{E_1}.$$

For even i the terms $\varepsilon_i U_1/\varepsilon_i\overline{E_1}$ are equal to $\varepsilon_i U_1^+/\varepsilon_i\overline{E_1}^+$, where the superscript $+$ indicates we are looking at units in the local subfield fixed by the automorphism of order 2. Vandiver's conjecture implies the cyclotomic units C_1^+ have index prime to p in E_1^+ ([14], Theorem 8.2), and so it suffices to consider the quotients $\varepsilon_i U_1^+/\varepsilon_i\overline{C_1}^+$. But Theorem 8.25 of [14] states

$$[\varepsilon_i U_1^+ : \varepsilon_i \overline{C_1}^+] = p^{v_p(L_p(1,\omega^i))}.$$

Since $A(K)$ is cyclic there is only one non-trivial $L_p(s,\omega^i)$, and hence only one cyclic factor, say of order p^m, in the torsion subgroup of $U_1/\overline{E}_1$. □

Proof of Theorem 7: The field $\widetilde{K}$ is in fact the fixed field of the torsion subgroup of $\mathcal{G}_K^{ab}$, and so the extension $M_K/\widetilde{K}$ is a Kummer extension with $\mathrm{Gal}(M_K/\widetilde{K}) \simeq \mathbb{Z}/p^m\mathbb{Z}$. With $A(K) \simeq \mathbb{Z}/p^a\mathbb{Z}$, condition (3) of the Theorem just states $m \leq a$.

To show that M_K is contained in N_∞, we need to show that $M_K/\widetilde{K}$ is generated by a p-th power root of a unit of $\widetilde{K}$. The argument, as in the proof of Theorem 6, is reduced to a capitulation problem.

Consider the extension M_K/K_{m-1}. There is a non-canonical isomorphism

$$\mathrm{Gal}(M_K/K_{m-1}) \simeq \mathrm{Gal}(\widetilde{K}/K_{m-1}) \times \mathrm{Gal}(M_K/\widetilde{K}).$$

We let L denote the fixed field of the first factor. The extension L/K_{m-1} is a Kummer extension, and we may write

$$L = K_{m-1}(x^{1/p^m})$$

for some x in K_{m-1} where the ideal (x) is of the form $(x) = \mathsf{J}^{p^m}P$, where P is the principal ideal of K_{m-1} lying above p.

Since, in particular, J represents a class of order dividing p^m in $A(K_{m-1})$, condition (3) implies the class of J is an extension of a class from $A(K)$ (recall the map $A(K) \to A(K_{m-1})$ is just an injection $\mathbb{Z}/p^a\mathbb{Z} \hookrightarrow \mathbb{Z}/p^{a+m-1}\mathbb{Z}$). We let A be a representative ideal of the class that extends to the class of J.

Since the p-Hilbert class field of K is contained in $\widetilde{K}$, and the class of A, and therefore J, becomes principal in $\widetilde{K}$. The extension $M_K/\widetilde{K}$ is also generated by a p^m-th root of x, and the ideal (x) in $\widetilde{K}$ is now the p^m-th power of a *principal* ideal,

$$(x) = (y)^{p^m}.$$

The elements x and y^{p^m} then differ by a unit , i.e. $x = uy^{p^m}$. But clearly the extension M_K is also generated by the p^m-th root of $x/y^{p^m} = u$, and so the field M_K is contained in N_∞. $\square$

References

[1] W. Bruns and J. Herzog. *Cohen-Macaulay rings*, Cambridge studies in advanced mathematics **39**, Cambridge University Press, Cambridge, 1993.

[2] J. Buhler, R. Crandall, R. Ernvall, T. Metsankyla, and M. A. Shokrollahi. Irregular primes and cyclotomic invariants to 12 million. *J. Symbolic Comput.*, **31**: 89-96, 2001.

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

[4] R. Greenberg. On the structure of certain Galois groups. *Inventiones Math.*, **47**: 85-99, 1978.

[5] R. Greenberg. Iwasawa theory - past and present. *Class field theory - its centenary and prospect (Tokyo, 1998)*, Advanced Studies in Pure Math., Math. Soc. Japan, **30**: 335-385, 2001.

[6] K. Iwasawa and C. Sims. Computation of invariants in the theory of cyclotomic fields. *J. Math. Soc. Japan*, **18**: 86-96, 1965.

[7] U. Jannsen. On the structure of Galois groups as Galois modules. *Number Theory Noordwijkerhout*, Springer Lecture Notes, **1068**: 109-126, 1984.

[8] U. Jannsen. Iwasawa modules up to isomorphism. *Advanced Studies in Mathematics*, **17**: 171-207, Academic Press, Orlando, 1989.

[9] A. Lannuzel and T. Nguyen Quang Do. Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres. *Manuscripta Math.*, **102**: 187-209, 2000.

[10] D. Marshall. *Galois groups and Greenberg's conjecture.* Ph.D. thesis, University of Arizona, August 2000.

[11] W. McCallum. Greenberg's conjecture and units in multiple $\mathbb{Z}_p$-extensions. *Amer. J. Math.*, **123**: 909-930, 2001.

[12] T. Nguyen Quang Do. Formations de classes et modules d'Iwasawa. *Number Theory Noordwijkerhout*, Springer Lecture Notes, **1068**: 167-185, 1984.

[13] J. P. Serre. *Galois Cohomology*, Springer-Verlag: Berlin Heidelberg, 1997.

[14] L. Washington. *Introduction to Cyclotomic Fields*, Second Edition, Graduate Texts in Mathematics, Springer-Verlag, New York, 1997.

[15] M. Yamagishi. On free pro-p extensions of algebraic number fields. *Moduli Spaces, Galois Representations, and L-functions*, (Kyoto, 1993, 1994), **884**: 172-177, 1994.

Department of Mathematics, University of Texas at Austin, Austin, Texas 78712, USA

E-mail address: marshall@math.utexas.edu