On Galois groups of unramified pro-p extensions

Romyar T. Sharifi

Abstract

Let p be an odd prime satisfying Vandiver's conjecture. We consider two objects, the Galois group X of the maximal unramified abelian pro-p extension of the compositum of all $\mathbf{Z}_p$-extensions of $\mathbf{Q}(\mu_p)$ and the Galois group $\mathfrak{G}$ of the maximal unramified pro-p extension of $\mathbf{Q}(\mu_{p^\infty})$. We give a lower bound for the height of the annihilator of X as an Iwasawa module. Under some mild assumptions on Bernoulli numbers, we provide a necessary and sufficient condition for $\mathfrak{G}$ to be abelian. The bound and the condition in the two results are given in terms of special values of a cup product pairing on cyclotomic p-units. We obtain in particular that, for $p < 1000$, Greenberg's conjecture that X is pseudo-null holds and $\mathfrak{G}$ is in fact abelian.

1 Introduction

Let L be a possibly infinite algebraic extension of $\mathbf{Q}$, and fix a prime p. We shall say that an algebraic extension of a number field is unramified if all of its finite subextensions are unramified at all places. The following are two frequently recurring questions in algebraic number theory.

1. What is the structure of the Galois group X_L of the maximal unramified abelian pro-p extension of L?
2. What is the structure of the Galois group $\mathfrak{G}_L$ of the maximal unramified pro-p extension of L?

If L is a number field, one sort of answer to the first question is found in class field theory. The maximal unramified abelian pro-p extension of L is finite and is known as the p-Hilbert class field, and X_L is isomorphic to the p-part A_L of the class group of L. As for the second question, the maximal unramified pro-p extension of L can be infinite, as Golod and Shafarevich demonstrated the existence of infinite Hilbert p-class field towers.

Consider next the cyclotomic $\mathbf{Z}_p$-extension K of a number field F. We let $\Gamma = \mathrm{Gal}(K/F)$ and set $\Lambda = \mathbf{Z}_p[[\Gamma]]$. Iwasawa showed that the group X_K is always finitely generated and torsion over Λ. Beyond that, if F is an abelian extension of $\mathbf{Q}$, the now-proven "main conjecture of Iwasawa theory" states the characteristic ideal of an odd eigenspace of X_K is determined by the p-adic L-function of a related even character. Wiles proved a similar result for abelian characters over totally real number fields.

In most instances, little is known about the structure of $\mathfrak{G}_K$ that cannot be obtained from the structure of X_K, its maximal abelian quotient. We consider the question of whether or not $\mathfrak{G}_K$ is abelian in the fundamental case that $F = \mathbf{Q}(\mu_p)$ for an odd prime p.

Theorem 1.1. *For $p < 1000$, the group $\mathfrak{G}_K$ is abelian. For $p = 1217$, 7069, and 9829, it is not.*

For the other 241 primes $p < 25{,}000$ such that the $\mathbf{Z}_p$-rank of X_K is at least 2, a conjecture of McCallum and the author's [MS, Conjecture 5.3] implies that $\mathfrak{G}_K$ is a free abelian pro-p group, so $\mathfrak{G}_K \cong X_K$. For the general result, see Theorem 5.2. Until recently, it was thought to be proven that $\mathfrak{G}_K$ is free pro-p under Vandiver's conjecture that p does not divide the class number of $\mathbf{Q}(\mu_p)^+$ [N, W], e.g., for $p < 12{,}000{,}000$. Now, it seems quite likely that $\mathfrak{G}_K$ is never free pro-p unless it is trivial or isomorphic to $\mathbf{Z}_p$.

For larger fields L, one can ask about the "size" of X_L. Early on, Greenberg proposed a conjecture in the abelian setting (see [G, Conjecture 3.5]). Let $\tilde{F}$ denote the compositum of all $\mathbf{Z}_p$-extensions of F, let $\tilde{\Gamma} = \mathrm{Gal}(\tilde{F}/F)$, and let $\tilde{\Lambda} = \mathbf{Z}_p[[\tilde{\Gamma}]]$. It follows from the analogous statement for K that $X_{\tilde{F}}$ is finitely generated and torsion as a $\tilde{\Lambda}$-module. To get slightly more information, we can pass to a family of $\tilde{\Lambda}$-modules that is in a definite sense one step smaller than the family of $\tilde{\Lambda}$-torsion modules. We say that a finitely generated $\tilde{\Lambda}$-module is pseudo-null if its annihilator has height at least 2.

Conjecture 1.2 (Greenberg)**.** *The Galois group $X_{\tilde{F}}$ of the maximal unramified abelian pro-p extension of $\tilde{F}$ is pseudo-null as a $\tilde{\Lambda}$-module.*

In Theorem 4.2, we give a lower bound on the height of the annihilator of $X_{\tilde{F}}$ for p satisfying Vandiver's conjecture. This implies the following weaker statement.

Theorem 1.3. *For $p < 1000$, Greenberg's conjecture holds for p and $F = \mathbf{Q}(\mu_p)$.*

We can ask a similar question for the class of strongly admissible p-adic Lie extensions L of F. As in [HS], we say that L/F is strongly admissible if it is ramified at only finitely many places of F, L contains K, and $Q = \mathrm{Gal}(L/F)$ is pro-p, has dimension at least 2, and contains no elements of order p.

We define a finitely generated $\Lambda(Q) = \mathbf{Z}_p[[Q]]$-module M to be pseudo-null if

$$\mathrm{Ext}^i_{\Lambda(Q)}(M, \Lambda(Q)) = 0$$

for $i = 0, 1$. Note that Q contains a normal subgroup $G = \mathrm{Gal}(L/K)$ with quotient Γ. If M is finitely generated over $\Lambda(G)$, then M is $\Lambda(Q)$-pseudo-null if and only if M is $\Lambda(G)$-torsion [HS, Lemma 3.1]. Under Iwasawa's conjecture on the triviality of the μ-invariant of X_K, the finite generation of X_L over $\Lambda(G)$ would always hold for L/F strongly admissible [HS, Lemma 3.4]. The question is then to determine the L as above for which X_L is $\Lambda(G)$-torsion. In particular, we use this in showing the following.

Theorem 1.4. *Let $F = \mathbf{Q}(\mu_p)$ for some $p < 1000$, and suppose that L is a strongly admissible p-adic Lie extension of F that contains a $\mathbf{Z}_p$-extension of K that is unramified outside p and contains a pth root of p. Then X_L is $\Lambda(Q)$-pseudo-null.*

2 Growth of Iwasawa modules

For simplicity of the description, let us assume that either p is odd or our number field F is purely imaginary. We use S to denote a set of primes of F containing those above p, and for any algebraic extension E of F, we let S_E denote the set of primes of E above those in S. We use $\mathfrak{X}_{E,S}$ to denote the Galois group of the maximal abelian pro-p unramified outside S_E extension of E. For $v \in S_E$, we let G_{E_v} (resp., I_{E_v}) denote the absolute Galois group (resp., inertia subgroup) of the completion E_v, and we let $\mathcal{V}_E$ (resp., $\mathcal{U}_E$) denote the inverse limit under norm maps of the p-completions of the unit groups (resp., p-unit groups) of number fields in E. Let

$$\mathcal{W}_E = \varprojlim_{F' \subset E} \bigoplus_{v \in S_{F'}} H_1(I_{F'_v}, \mathbf{Z}_p)_{G_{F'_v}},$$

where F' runs over the finite extensions of F in E. We have the following proposition.

Proposition 2.1. *Let E be an algebraic extension of F, and let $L \subsetneq M$ be pro-p p-adic Lie extensions of E such that $G = \mathrm{Gal}(M/E)$ has no p-torsion. Let $H = \mathrm{Gal}(M/L)$. Let S be the set of primes of F consisting of those above p and those that ramify in M/F.*

a. *Suppose that the set of primes of S_L that ramify in M/L is finite and that there exists a $\mathbf{Z}_p$-extension E' of E contained in L such that X_L is finitely generated over $\Lambda(\mathrm{Gal}(L/E'))$. Then X_M is finitely generated and torsion over $\Lambda(G)$.*

b. *Suppose that there exists exactly one prime in S_L that ramifies in M/L and that M/L is totally ramified at that prime. Then $(X_M)_H \cong X_L$ via restriction.*

Proof. We consider the natural commutative diagram

$$\begin{array}{ccccccccc} \mathcal{V}_M & \longrightarrow & \mathcal{W}_M & \longrightarrow & \mathfrak{X}_{M,S} & \longrightarrow & X_M & \longrightarrow & 0 \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle d} & & \\ \mathcal{V}_L & \longrightarrow & \mathcal{W}_L & \longrightarrow & \mathfrak{X}_{L,S} & \longrightarrow & X_L & \longrightarrow & 0. \end{array}$$

Let b_H, c_H and d_H denote the maps induced by b, c and d, respectively, on H-coinvariants of the domains. A straightforward diagram chase yields an isomorphism

$$\operatorname{coker}(\ker c_H \to \ker d_H) \cong \frac{\ker(\operatorname{coker} b \to \operatorname{coker} c)}{\operatorname{image}(\operatorname{coker} a \to \operatorname{coker} b)}. \tag{1}$$

By the Hochschild-Serre spectral sequence, we have that $\ker c_H$ is isomorphic to a quotient of $H_2(H, \mathbf{Z}_p)$, which is finitely generated over $\mathbf{Z}_p$. Since we have assumed that the set of primes of S_L at which M/L ramifies is finite, we have that

$$\operatorname{coker} b \cong \bigoplus_{v \in S_L} J_v,$$

where J_v is the inertia subgroup of the abelianization of the decomposition group at v in H. Thus $\operatorname{coker} b$ is finitely generated over $\mathbf{Z}_p$. It follows that $\ker d_H$ is also finitely generated over $\mathbf{Z}_p$. Since, by assumption, X_L is finitely generated over $\Lambda(\mathrm{Gal}(L/E'))$, the same must hold for $(X_M)_H$. By [BH, Section 3], we then have that X_M is finitely generated over $\Lambda(\mathrm{Gal}(M/E'))$, and by [CFKSV, Proposition 2.3], we may conclude that X_M is a torsion $\Lambda(G)$-module, proving part a.

Now, suppose that the assumption of part b holds. Let w denote the unique prime of L at which M/L is totally ramified, and let I_w denote the inertia group of w in H. The existence of such a prime forces $\operatorname{coker} d = 0$ automatically. Since $I_w = H$, we also have that the map $\operatorname{coker} b \to \operatorname{coker} c$ is an isomorphism. Furthermore, $\ker b_H$ is canonically isomorphic to a quotient of $H_2(I_w, \mathbf{Z}_p)$, and $H_2(I_w, \mathbf{Z}_p) \to H_2(H, \mathbf{Z}_p)$ is an isomorphism since $I_w = H$. Thus the map $\ker b_H \to \ker c_H$ is surjective, and this forces the map $\ker c_H \to \ker d_H$ to be zero. By (1), we therefore have that $\ker d_H = 0$, proving part b. □

Next, consider the following lemma from commutative algebra.

Lemma 2.2. *Let $n \geq m \geq 0$, and consider the power series ring $R_n = \mathbf{Z}_p[[T_1, \ldots, T_n]]$ in n independent variables. Suppose that A is an R_n-module that is finitely generated over R_m. Let h denote the height of the annihilator of A in R_m. Then the height of the annihilator of A in R_n is at least $h + n - m$.*

Proof. Let I_m (resp., I_n) denote the annihilator of A in R_m (resp., R_n). Suppose that A is nonzero and generated over R_m by a given finite set of elements. For d with $m < d \leq n$, we may consider any characteristic polynomial $f_d \in R_m[X]$ of T_d acting on A with respect to this generating set. Now, if $\mathfrak{p}$ is a prime ideal containing I_n, then it contains I_m. Let $\mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_h$ be a chain of distinct nonzero primes of R_m contained in $\mathfrak{p} \cap R_m$. For d as above, set $i = d + h - m$, and define $\mathfrak{q}_i = \mathfrak{p} \cap R_d$. Then $f_d(T_d) \in \mathfrak{q}_i$, but $f_d(T_d) \notin \mathfrak{q}_{i-1} R_d$ since f_d is monic. Let $\mathfrak{p}_i = \mathfrak{q}_i R_n$ for all i with $1 \leq i \leq h + n - m$. Then the $\mathfrak{p}_i$ are prime, distinct, and contained in $\mathfrak{p}$, so the height of I_n is at least $h + n - m$. □

The following corollary will be useful to us later.

Corollary 2.3. *Let $L \subseteq M$ be abelian extensions of F containing the cyclotomic $\mathbf{Z}_p$-extension K of F with $\mathrm{Gal}(M/F) \cong \mathbf{Z}_p^n$ and $\mathrm{Gal}(L/F) \cong \mathbf{Z}_p^m$ for some $n \geq m \geq 1$. If X_L is finitely generated over $\mathbf{Z}_p$, then the height of the annihilator of X_M is at least m as a $\Lambda(\mathrm{Gal}(M/F))$-module.*

Proof. Since M/F is necessarily unramified outside p and there are only finitely many primes above p in L, the assumptions of Proposition 2.1a are satisfied, so X_M is a finitely generated, torsion $\Lambda(\Gamma \times \mathrm{Gal}(M/L))$-module. The result is then immediate from Lemma 2.2. □

3 Iwasawa modules over Kummer extensions

For the rest of this paper, we will focus on the case that $F = \mathbf{Q}(\mu_p)$ for an odd prime p. The key to the results in this paper is the use of cup products to control the growth of the Galois groups of the maximal unramified abelian pro-p extensions of Kummer extensions of $K = \mathbf{Q}(\mu_{p^\infty})$. These cup products were first studied in [MS] and later in [S]. Let us briefly review the material we will need.

Let $\mathcal{B}_F$ denote the p-completion of the group of elements of $F^\times$ whose pth roots generate unramified outside p extensions of F. Given an element of the p-completion $\mathcal{K}$ of $K^\times$, we may also speak of the extension of K its p-power roots generate, and we let $\mathcal{B}_K$

denote the subgroup of those elements whose p-power roots generate unramified outside p extensions. (Although $\mathcal{B}_F$ is not a subgroup of $\mathcal{B}_K$, there is a canonical map from the p-completion of $F^\times$ to $\mathcal{K}$ with kernel μ_p through which we will consider elements of $\mathcal{B}_F$ as elements of $\mathcal{K}$ by abuse of notation.)

Let S now denote the set consisting of the unique prime above p in F, and for any algebraic extension E of F, let $G_{E,S}$ denote the Galois group of the maximal unramified outside S_E extension of E. The cup product on $H^1(G_{F,S}, \mu_p)$ induces a pairing

$$(\,\cdot\,,\,\cdot\,)_{p,F,S} \colon \mathcal{B}_F \times \mathcal{B}_F \to A_F \otimes \mu_p,$$

where A_F again denotes the p-part of the class group of F, and the inverse limit of similar pairings arising from the cup products on the groups $H^1(G_{\mathbf{Q}(\mu_{p^n}),S}, \mu_{p^n})$ induces a pairing

$$(\,\cdot\,,\,\cdot\,)_{K,S} \colon \mathcal{B}_K \times \mathcal{U}_K \to X_K(1)$$

(see, for instance, [S, Section 4]).

Fix a primitive pth root of unity ζ_p in F. Let $\mathcal{E}_F$ denote the p-completion of the p-units in F. Let $\mathcal{C}_F$ denote the subgroup of $\mathcal{E}_F$ consisting of the p-completion of the cyclotomic p-units, i.e., those generated by the $1-\zeta_p^i$ with $1 \le i \le p-1$. For a finite extension E of F, let $A_{E/F}$ denote the image of the norm map $A_E \to A_F$. For an algebraic extension L/K, let $X_{L/K}$ denote the image of restriction $X_L \to X_K$, and let Y_L denote the maximal quotient of X_L in which all primes above p split completely. For a p-adic Lie group G, let I_G denote the augmentation ideal in $\Lambda(G)$. It will be useful to recall the following result.

Lemma 3.1. *Let $b \in \mathcal{B}_K$, and suppose that its p-power roots generate a $\mathbf{Z}_p$-extension L of K with Galois group G. We have that*

$$(b, \mathcal{U}_K)_{K,S} = X_{L/K}(1) \tag{2}$$

if and only if $I_G Y_L = 0$. If $ba^{-1} \in \mathcal{K}^p$ for some $a \in \mathcal{B}_F$, then (2) *follows from*

$$(a, \mathcal{C}_F)_{p,F,S} = A_{F(a^{1/p})/F} \otimes \mu_p. \tag{3}$$

Moreover, if Vandiver's conjecture holds at p, then (2) *implies* (3) *for some a with $ba^{-1} \in \mathcal{K}^p$.*

Proof. We remark that the containment of the pairing values in $X_{L/K}(1)$ (resp., in $A_{F(a^{1/p})/F} \otimes \mu_p$) in the statement holds for any $b \in \mathcal{B}_K$ (resp., $a \in \mathcal{B}_F$), as follows for example from [MS, Theorem 2.4]. The first part is a direct consequence of [S, Theorem 4.3], noting that there is a unique prime over p in K. Now, we know that the image of $(b, \mathcal{U}_K)_{K,S}$ under the natural map $X_K(1) \to A_F \otimes \mu_p$ contains $(a, \mathcal{C}_F)_{p,F,S}$ and is equal to it under Vandiver's conjecture at p, since every element of $\mathcal{C}_F$ is a universal norm from K and these are all the universal norms under Vandiver. Since we have as well that the image of $X_{L/K}(1)$ is contained in $A_{F(a^{1/p})/F} \otimes \mu_p$ and is equal to it when a is chosen properly (multiplying a by an element of μ_p to make $F(a^{1/p})/F$ unramified if possible), the second statement follows. □

We next recall [S, Corollary 5.9].

Theorem 3.2. *For $p < 1000$, we have $(p, \mathcal{C}_F)_{p,F,S} = A_F \otimes \mu_p$.*

We now obtain the following useful result.

Proposition 3.3. *Suppose that $a \in \mathcal{B}_F$ is such that (3) holds. Let L be a $\mathbf{Z}_p$-extension of K with Galois group G that is unramified outside p but not unramified and contains a pth root of a. Then X_L is finitely generated over $\mathbf{Z}_p$, and we have $Y_L \cong X_{L/K}$ via restriction.*

Proof. The field L is defined over K by the p-power roots of an element $b \in \mathcal{B}_K$ such that $ba^{-1} \in \mathcal{B}_K^p$. We have $I_G Y_L = 0$ by Lemma 3.1. It follows that $Y_L \cong (Y_L)_G$, and $(Y_L)_G \cong X_{L/K}$ is easily seen since L/K is a $\mathbf{Z}_p$-extension with a unique prime over p in K. In addition, we know that $(Y_L)_G = (X_L)_G$, so $I_G X_L$ is generated by the decomposition groups above p in X_L. Such decomposition groups are attached to the primes above p in L, of which there are finitely many since L/K is not unramified, and any such decomposition group is a quotient of $\mathbf{Z}_p$. Therefore, X_L is a finitely generated $\mathbf{Z}_p$-module. □

Noting the remarks preceding it in the introduction, Theorem 1.4 now follows from Theorem 3.2, Proposition 3.3, and Proposition 2.1a.

4 Iwasawa modules over multiple $\mathbf{Z}_p$-extensions

In this section, we turn to the study of the structure of the Galois group $X_{\tilde{F}}$ of the maximal unramified abelian pro-p extension of the compositum $\tilde{F}$ of all $\mathbf{Z}_p$-extensions of the pth cyclotomic field F. Proposition 3.3 allows us to immediately give a criterion for the verification of Greenberg's pseudo-nullity conjecture (Conjecture 1.2) for F.

Proposition 4.1. *Suppose that there exists $a \in \mathcal{C}_F$ satisfying* (3)*. Then Greenberg's conjecture holds for F and p.*

Proof. Since $(\zeta, \mathcal{C}_F)_{p,F,S} = 0$ for $\zeta \in \mu_p$, we may assume without loss of generality that a is not a root of unity times a pth power in $\mathcal{E}_F$. Since $a \in \mathcal{C}_F$, there exists a $\mathbf{Z}_p$-extension E of F containing a pth root of a. By assumption, E is not contained in K. Setting $L = EK$, we have that X_L is finitely generated over $\mathbf{Z}_p$ by Proposition 3.3, and since $L \subseteq \tilde{F}$, that Greenberg's conjecture holds by Proposition 2.1a, noting [HS, Lemma 3.4] (or [V, Proposition 5.4]). □

In particular, as stated in Theorem 1.3, Greenberg's conjecture holds for $\mathbf{Q}(\mu_p)$ for $p < 1000$. We remark that Theorem 1.3 was already known for those $p < 1000$ with A_F cyclic by [MS, Corollary 10.5] and Theorem 3.2. An inductive version of the above argument is due to Greenberg in the case that $X_K \cong \mathbf{Z}_p$, but unlike the argument of [MS], it works easily without this restriction. We thank Ralph Greenberg for communicating his argument to us.

One may ask if the pseudo-nullity of $X_{\tilde{F}}$ is the best one can do. That is, can one give a stronger lower bound on the height of the annihilator of $X_{\tilde{F}}$? In fact, the answer is yes, as we now show.

Let us say that k is irregular for p if (p, k) is an irregular pair, i.e., k is positive and even, $k \leq p - 3$, and p divides the kth Bernoulli number B_k. Let $\Delta = \mathrm{Gal}(F/\mathbf{Q})$. For a $\mathbf{Z}_p[\Delta]$-module A and $i \in \mathbf{Z}$, let $A^{(i)}$ denote the ω^i-eigenspace of A, where ω denotes the Teichmüller character. Then (p, k) is irregular if and only if $A_F^{(1-k)} \neq 0$. For any odd integer i, let η_i denote the projection of $(1 - \zeta_p)^{p-1}$ to $\mathcal{C}_F^{(1-i)}$.

Theorem 4.2. *Suppose that Vandiver's conjecture holds at p. Consider the following subsets of $\mathbf{Z}/(p-1)\mathbf{Z}$:*

$$R = \{k \mid (p, k) \text{ irregular}\}$$

and

$$I = \{i \mid i \text{ odd}, (\eta_i, \eta_{k-i})_{p,F,S} \neq 0 \text{ for all } k \text{ irregular for } p\}.$$

The height of the annihilator of $X_{\tilde{F}}$ as a $\tilde{\Lambda}$-module is at least one more than the maximal number of disjoint translates $i + R$ with $i \in I$.

Proof. Since we have assumed Vandiver's conjecture, $A_F^{(1-k)}$ is cyclic for all irregular k for p, and all other eigenspaces of A_F are trivial. Therefore, the condition that $i \in I$ is equivalent to that of (3) holding for $a = \eta_i$, along with the extension of F defined by a pth root of η_i being totally ramified above p (i.e., $i \neq p - k'$ for all k' irregular for p

[MS, Section 5]). Let L_i denote the unique $\mathbf{Z}_p$-extension of K Galois over $\mathbf{Q}$ and abelian over F that contains a pth root of η_i. Then Proposition 3.3 yields that $Y_{L_i} \cong X_K$ via restriction.

Let $i_1, i_2, \ldots, i_d \in I$ be such that the translates $i_s + R$ are all disjoint as s runs over $1 \le s \le d$, let $M_s = L_{i_1} \cdots L_{i_s}$ for any such s, and set $M_0 = K$. Suppose by induction on d that $Y_{M_{d-1}} \cong X_K$ via restriction. Again, the assumption that $i \in I$ implies that L_i/K is totally ramified at p. Since the $\mathrm{Gal}(L_i/K)$ have Δ-actions given by distinct powers of the Teichmüller character, M_d has a unique prime above p, and that prime is totally ramified over F.

Now set $G = \mathrm{Gal}(M_d/K)$, $H = \mathrm{Gal}(M_d/M_{d-1})$, and $T = \mathrm{Gal}(M_d/L_d)$. By Proposition 2.1b, we know that $(Y_{M_d})_T \cong Y_{L_d}$. We therefore have

$$0 = (I_H Y_{L_d})_H \cong (I_H (Y_{M_d})_T)_H \cong I_H Y_{M_d}/(I_T Y_{M_d} \cap I_H Y_{M_d} + I_H^2 Y_{M_d}). \tag{4}$$

By assumption, we have

$$I_T Y_{M_d}/(I_T Y_{M_d} \cap I_H Y_{M_d}) \cong I_T((Y_{M_d})_H) \cong I_T Y_{M_{d-1}} \cong I_T X_K = 0,$$

so we have

$$I_T Y_{M_d} = I_T Y_{M_d} \cap I_H Y_{M_d} \tag{5}$$

and therefore

$$I_T Y_{M_d} \subseteq I_H Y_{M_d}.$$

Consider for $N = H$ and $N = T$ the natural surjective $\mathbf{Z}_p[\Delta]$-homomorphisms

$$\pi_N \colon X_K \otimes_{\mathbf{Z}_p} N \to (I_N Y_{M_d})_G,$$

with

$$\pi_N(x \otimes \sigma) = (\sigma - 1)\tilde{x} \pmod{I_G I_N Y_{M_d}},$$

where $\tilde{x} \in Y_{M_d}$ restricts to x. Since the $\mathbf{Z}_p[\Delta]$-eigenspaces of $X_K \otimes_{\mathbf{Z}_p} N$ are nontrivial outside of those of the characters ω^{1-k+i_t} with k irregular for p and $t \le d-1$ if $N = T$ and $t = d$ if $N = H$, we have that $(I_N Y_{M_d})_G$ is also nontrivial at most in these eigenspaces. Since the $i_t + R$ are all disjoint, the canonical map

$$(I_T Y_{M_d})_G \to (I_H Y_{M_d})_G$$

is zero, and hence

$$I_T Y_{M_d} \subseteq I_G I_H Y_{M_d} = (I_T I_H + I_H^2) Y_{M_d}.$$

But (5) then forces

$$(I_T Y_{M_d} \cap I_H Y_{M_d}) + I_H^2 Y_{M_d} = I_G I_H Y_{M_d}.$$

Given this, (4) implies that $(I_H Y_{M_d})_G = 0$, that is,

$$Y_{M_d} \cong (Y_{M_d})_H \cong Y_{M_{d-1}},$$

and so $Y_{M_d} \cong X_K$ via restriction.

Since there exists a unique prime over p in M_d, the kernel of $X_{M_d} \to Y_{M_d}$ is a quotient of $\mathbf{Z}_p$, so X_{M_d} is finitely generated over $\mathbf{Z}_p$. By Corollary 2.3, the annihilator of $X_{\tilde{F}}$ then has height at least $d+1$ as a $\tilde{\Lambda}$-module. □

Corollary 4.3. *Suppose that Vandiver's conjecture holds at p, let r be the p-rank of A_F, and let s be the number of odd integers i with $1 \le i \le p-2$ such that $(\eta_i, \eta_{k-i})_{p,F,S} \neq 0$ for all k irregular for p. Then the height j of the annihilator of $X_{\tilde{F}}$ as a $\tilde{\Lambda}$-module satisfies*

$$j \geq \frac{s}{r^2 - r + 1} + 1.$$

Proof. Let R and I be as in Theorem 4.2. Suppose that we have t disjoint translates of R by elements of I. Each translate of R contains r elements and intersects at most r^2-r+1 of the s translates of R by elements of I. Therefore, so long at $t(r^2-r+1) < s$, there exists at least one other translate by an element of I that does not intersect any of the given translates. The result then follows from Theorem 4.2. □

We remark that, for $p < 1000$, one has $r \le 3$ and $\frac{p-1}{2} - s \in [2,6]$, $[6,8]$, and $[9,12]$ when $r = 1$, 2, and 3, respectively.

5 The maximal unramified pro-p extension

We now turn to the study of the structure of the Galois group $\mathfrak{G}_K$ of the maximal unramified pro-p extension of the field K of all p-power roots of unity.

Lemma 5.1. *Let M/L be an unramified abelian pro-p extension with torsion-free Galois group H, and assume that M and L are Galois extensions of F. Then there is a canonical exact sequence of $\Lambda(\mathrm{Gal}(L/F))$-modules,*

$$H \wedge_{\mathbf{Z}_p} H \to (X_M)_H \to X_L \to H \to 0.$$

Proof. This arises directly from the obvious exact sequence

$$1 \to \frac{[\mathfrak{G}_L, \mathfrak{G}_L]}{[\mathfrak{G}_M, \mathfrak{G}_L]} \to \frac{\mathfrak{G}_M}{[\mathfrak{G}_M, \mathfrak{G}_L]} \to \frac{\mathfrak{G}_L}{[\mathfrak{G}_L, \mathfrak{G}_L]} \to \frac{\mathfrak{G}_L}{\mathfrak{G}_M[\mathfrak{G}_L, \mathfrak{G}_L]} \to 1.$$

□

Moreover, we note that the sequences in Lemma 5.1 are natural in L and M (and thereby H) in the obvious sense. We have the following result on the structure of $\mathfrak{G}_K$.

Theorem 5.2. *Assume that Vandiver's conjecture holds at* p *and that* $X_K^{(1-k)} \cong \mathbf{Z}_p$ *for each irregular* k *for* p*. Assume also that for any irregular* $k' > k$ *for* p*, we have both that* $k + k' \not\equiv 2 \bmod p-1$ *and that* $j = k$ *whenever* $j' > j$ *are irregular for* p *with* $j + j' \equiv k + k' \bmod p-1$*. Then the group* $\mathfrak{G}_K$ *is abelian if and only if* $(\eta_{p-k}, \eta_{k+k'-1})_{p,F,S} \neq 0$ *for all irregular* $k' > k$ *for* p*.*

Proof. Under Vandiver's conjecture, X_K is p-torsion free, so $\mathfrak{G}_K$ is free pro-p and abelian if the $\mathbf{Z}_p$-rank of X_K is at most 1. Hence, we may assume that the $\mathbf{Z}_p$-rank of X_K is at least 2. Then, by assumption, X_K has at least two nontrivial $\mathbf{Z}_p[\Delta]$-eigenspaces, where $\Delta = \mathrm{Gal}(F/\mathbf{Q})$. Fix k irregular for p, and consider the unramified $\mathbf{Z}_p$-extension L/K defined by $H = X_K^{(1-k)}$.

We begin by showing that $X_L \cong (X_L)_H$. This is equivalent to showing that $(I_H X_L)_H$ is trivial. Note first that $(X_L)_H \cong (Y_L)_H$. Furthermore, we claim that

$$(I_H X_L)_H \cong (I_H Y_L)_H. \tag{6}$$

The image of a decomposition group above p in X_L must lie in the trivial $\mathbf{Z}_p[\Delta]$-eigenspace of $(I_H X_L)_H$. On the other hand, by the procyclicity of the eigenspaces of X_K and Vandiver's conjecture, $(I_H X_L)_H$ can only be nontrivial in its $(\omega^{2-k-k'})$-eigenspaces for k' irregular with $k' \neq k$, so the claim follows from our assumption that $k + k' \not\equiv 2 \bmod p-1$.

Note that the condition

$$(\eta_{p-k}, \eta_{k+k'-1})_{p,F,S} \neq 0 \tag{7}$$

for all irregular $k' \neq k$ is equivalent to the statement that

$$A_F^{(1-k')} \otimes \mu_p \subseteq (\eta_{p-k}, \mathcal{C}_F)_{p,F,S},$$

as the odd eigenspaces of A_F are cyclic and $\mathcal{C}_F^{(j)}$ is generated by η_{p-j} for each even j. Let E denote the extension of F by a pth root of η_{p-k}. Since E/F is unramified, we have

$$A_{E/F} \cong \bigoplus_{\substack{k' \neq k \\ (p,k') \text{ irregular}}} A_F^{(1-k')}.$$

We therefore have

$$(\eta_{p-k}, \mathcal{C}_F)_{p,F,S} = A_{E/F} \otimes \mu_p$$

exactly when (7) holds for any irregular k' for p not equal to k.

If (7) holds for all irregular $k' \neq k$, then Proposition 3.3 yields that $Y_L \cong X_{L/K}$ via restriction, i.e., that $(I_H Y_L)_H = 0$ and, therefore, $(I_H X_L)_H = 0$ by (6). On the other hand, if (7) fails for some k', then Lemma 3.1 implies that $I_H Y_L \neq 0$ and therefore that the restriction map $Y_L \to X_K$ is not injective, so in particular the restriction map $X_L \to X_K$ is not. Therefore, in this case, $\mathfrak{G}_K$ is not abelian.

We now suppose that (7) holds for all k and k' irregular for p with $k' > k$. We have shown that $(I_H X_L)_H = 0$ for the field L and Galois group H determined by k above, for each k. Since $H \wedge_{\mathbf{Z}_p} H = 0$, we have by Lemma 5.1 that X_L injects into X_K with cokernel H. Now let M be the maximal unramified abelian pro-p extension of K, and set $G = X_K = \mathrm{Gal}(M/K)$ and $N = X_L \cong \ker(G \to H)$. From Lemma 5.1, we obtain a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
N \wedge_{\mathbf{Z}_p} N & \longrightarrow & (X_M)_N & \longrightarrow & X_L & \xrightarrow{\sim} & N & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
G \wedge_{\mathbf{Z}_p} G & \longrightarrow & (X_M)_G & \longrightarrow & X_K & \xrightarrow{\sim} & G & \longrightarrow & 0.
\end{array}$$

In the diagram, the leftmost horizontal arrows are surjective, the leftmost vertical arrow is the natural injection, and the second vertical arrow is the natural surjection. It follows that $N \wedge_{\mathbf{Z}_p} N \to (X_M)_G$ is surjective. Now $G \wedge_{\mathbf{Z}_p} G$ (resp., $N \wedge_{\mathbf{Z}_p} N$) is nontrivial only in its $(\omega^{2-j-j'})$-eigenspaces, where $j < j'$ are irregular for p (resp., are irregular for p and distinct from k). Since the $j + j' \pmod{p-1}$ with $j < j'$ are all distinct by assumption, we have that $(X_M)_G$ is trivial in its $\omega^{2-k-k'}$-eigenspaces for all k' irregular for p and distinct from k. Since this holds for all k, we have $(X_M)_G = 0$. This forces $[\mathfrak{G}_K, \mathfrak{G}_K]^{\mathrm{ab}} \cong X_M = 0$, so $\mathfrak{G}_K$ is abelian. □

Corollary 5.3. *For $p < 1000$, the group $\mathfrak{G}_K$ is abelian. For $p = 1217$, 7069, and 9829, it is nonabelian. For all other $p < 25{,}000$, it is abelian if $(\,\cdot\,,\cdot\,)_{p,F,S}$ is surjective.*

Proof. Vandiver's conjecture and the assumption that the nontrivial eigenspaces of X_K are procyclic are known for $p < 12{,}000{,}000$ [BCEMS]. Using Magma, we checked that the congruences assumed not to hold among irregular k for p are never satisfied for $p < 25{,}000$. We then checked the pairing values that appear in the tables mentioned in [MS, Theorem 5.1] (now completed for $p < 25{,}000$). That is, for each irregular k

and k' for p with $k < k'$, we checked the table value $b_{p,k,k'} \in \mathbf{Z}/p\mathbf{Z}$ that corresponds to $a_{p,k,k'} = (\eta_{p-k}, \eta_{k+k'-1})_{p,F,S}$ to see if it is zero. Since

$$a_{p,k,k'} = b_{p,k,k'} \cdot \mathfrak{c}_{p,k'}$$

for some $\mathfrak{c}_{p,k'}$ in $A_F^{(1-k')} \otimes \mu_p$, the triviality of $b_{p,k,k'}$ implies the triviality of $a_{p,k,k'}$. On the other hand, the converse holds whenever $(\,\cdot\,,\,\cdot\,)_{p,F,S}$ is surjective. We know this surjectivity to be the case for $p < 1000$ by Theorem 3.2.

The values $b_{p,k,k'}$ with $p <$ 25,000 are nonzero aside from three exceptions:

- $p = 1217$, $k = 784$, and $k' = 866$,
- $p = 7069$, $k = 1478$, and $k' = 2570$,
- $p = 9829$, $k = 4562$, and $k' = 7548$.

(We remark that the index of irregularity of p is 3 for $p = 1217$ and 2 for $p = 7069$ and $p = 9829$.) The result now follows from Theorem 5.2. □

We remark that McCallum and the author have conjectured that $(\,\cdot\,,\,\cdot)_{p,F,S}$ is surjective when Vandiver's conjecture holds at p [MS, Conjecture 5.3], so we expect $\mathfrak{G}_K$ to be abelian for all $p <$ 25,000 other than 1217, 7069, and 9829.

References

[BH] P. Balister, S. Howson, Note on Nakayama's Lemma for compact Λ-modules, *Asian Math. J.* **1** (1997), 224-229.

[BCEMS] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, M. A. Shokrollahi, Irregular primes and cyclotomic invariants to 12 million, *J. Symbolic Comput.* **31** (2001), 89–96.

[CFKSV] J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob, The GL_2 main conjecture for elliptic curves without complex multiplication. *Publ. Math. Inst. Hautes Études Sci.* **101** (2005), 163–208.

[G] R. Greenberg, Iwasawa theory–past and present, Class Field Theory: Its Centenary and Prospect, *Adv. Stud. Pure. Math.* **30**, Math. Soc. Japan, Tokyo, 2001, 335–385.

[HS] Y. Hachimori, R. Sharifi, On the failure of pseudo-nullity of Iwasawa modules, *J. Alg. Geom.* **14** (2005), 567–591.

[MS] W. McCallum, R. Sharifi, A cup product in the Galois cohomology of number fields, *Duke Math. J.* **120** (2003), 269–310.

[N] T. Nguyen Quang Do, K_3 et formules de Riemann-Hurwitz p-adiques, *K-theory* **7** (1993), 429–441.

[S] R. Sharifi, Iwasawa theory and the Eisenstein ideal, *Duke Math. J.* **120** (2003), 269–310.

[V] O. Venjakob, A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory, *J. reine angew. Math.* **559** (2003), 153–191.

[W] K. Wingberg, On the maximal unramified p-extension of an algebraic number field, *J. reine angew. Math.* **440** (1993), 129–156.

Romyar Sharifi
Department of Mathematics and Statistics
McMaster University
1280 Main Street West
Hamilton, Ontario L8S 4K1, Canada
e-mail address: `sharifi@math.mcmaster.ca`
web page: `http://www.math.mcmaster.ca/∼sharifi`