Relationships between conjectures on the structure of pro-p Galois groups unramified outside p

Romyar T. Sharifi*

1 Introduction

The fixed field Ω^* of the canonical representation $\phi\colon G_{\mathbf{Q}} \to \mathrm{Out}(\pi_1)$ with

$$\pi_1 = \pi_1^{\mathrm{pro}-p}(\mathbf{P}^1(\bar{\mathbf{Q}}) \setminus \{0, 1, \infty\})$$

is a pro-p extension of $\mathbf{Q}(\zeta_p)$ unramified outside p for any prime number p [I1]. We study, for odd primes p, the structure of $G = \mathrm{Gal}(\Omega^*/\mathbf{Q}(\zeta_{p^\infty}))$ and of a certain graded $\mathbf{Z}_p$-Lie algebra $\mathfrak{g}$ associated to ϕ and arising from a filtration of G. To that effect, this article can be viewed as an extension of the article of Ihara [I6] (esp., Lecture I).

Our primary insight comes from the examination of the relationship between elements of $\mathrm{Gal}(\Omega/\mathbf{Q}(\zeta_p))$, where Ω is the maximal pro-p extension of $\mathbf{Q}(\zeta_p)$ unramified outside p, and elements of $\mathrm{Gal}(\Omega/\mathbf{Q}(\zeta_{p^\infty}))$. More specifically, we construct elements $\sigma_m \in \mathrm{Gal}(\Omega/\mathbf{Q}(\zeta_{p^\infty}))$ restricting nontrivially to elements of the mth graded pieces $gr^m\mathfrak{g}$ for odd $m \geq 3$. The elements σ_m are obtained recursively starting from elements of $\mathrm{Gal}(\Omega/\mathbf{Q}(\zeta_p))$ which satisfy the property that their images in the maximal abelian quotient generate its odd eigenspaces under the action of $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. In fact, these elements of $\mathrm{Gal}(\Omega/\mathbf{Q}(\zeta_p))$ provide suitable σ_m for odd m with $3 \leq m \leq p$. In this way, we are able to employ knowledge of the Galois group of $\Omega/\mathbf{Q}(\zeta_p)$ in studying the structure of $\mathfrak{g}$. In particular, it will follow from a consequence of a conjecture of Greenberg's in multivariable Iwasawa theory [G2] that $\mathfrak{g}$ is not free on the restrictions of the σ_m for a large class of irregular primes.

Define Ω^*_{m-1} as the fixed field of the kernel of

$$\phi_m\colon G_K \to \mathrm{Out}(\pi_1/\pi_1(m+1)),$$

where $K = \mathbf{Q}(\zeta_{p^\infty})$ and $\pi_1(m+1)$ denotes the $(m+1)$st term in the lower central series of π_1. The graded $\mathbf{Z}_p$-Lie algebra $\mathfrak{g}$ is defined by setting $gr^m\mathfrak{g} = \mathrm{Gal}(\Omega^*_m/\Omega^*_{m-1})$

*The author would like to thank Yasutaka Ihara and Bill McCallum for many helpful discussions. Supported by NSF VIGRE grant 9977116.

for $m \geq 1$. Recall that, as a $\mathrm{Gal}(K/\mathbf{Q})$-module, $gr^m\mathfrak{g} \cong \mathbf{Z}_p(m)^{\oplus r_m}$ for some $r_m \geq 0$ [I1, I6].

Consider the filtration $F^mG = \mathrm{Gal}(\Omega^*/\Omega^*_{m-1})$ of G giving rise to $\mathfrak{g}$. For each odd integer $m \geq 3$, we let σ_m denote an element of F^mG with the property that $\kappa_m(\sigma_m)$ generates the image of the mth Soulé character κ_m on F^mG [So, I6]. In Section 2, we shall make a particular choice of the elements σ_m. By abuse of notation, the element of $gr^m\mathfrak{g}$ given by the restriction of σ_m to Ω^*_m will also be denoted by σ_m (and is nontrivial [I2, I6]). We remark that κ_m and κ_k induce the same character modulo p^n if $m \equiv k \bmod p^{n-1}(p-1)$.

Let S denote the free pro-p group on infinitely many generators s_m with m odd ≥ 3, and let $\mathfrak{s}$ denote the free graded $\mathbf{Z}_p$-Lie algebra with generators also denoted s_m in odd degree ≥ 3. Consider the homomorphisms $\Psi\colon S \to G$ and $\psi\colon \mathfrak{s} \to \mathfrak{g}$ determined by $s_m \mapsto \sigma_m$. Ihara attributes to Deligne the conjecture that $\psi \otimes \mathbf{Q}_p$ is an isomorphism [I2, I3, I6]. In fact, Hain and Matsumoto have recently shown $\psi \otimes \mathbf{Q}_p$ to be surjective [HM].

We will study the surjectivity, or lack thereof, of ψ itself. This appears to be a finer question, its answer depending upon arithmetic properties of the prime p. We shall show that the validity of certain conjectures would imply that the map ψ is not surjective exactly when p is an irregular prime. Without any assumptions, our results imply that ψ is not an isomorphism for a large class of irregular primes.

The following theorem will result from our definition of the elements σ_m, but holds for any choice of σ_m.

Theorem 1.1. *Let p be an odd regular prime. Then the homomorphism Ψ is surjective. If Deligne's conjecture holds for p, then ψ and Ψ are isomorphisms and $\Omega = \Omega^*$.*

Additionally, we shall obtain a refinement of this in the form of an extension of Theorem I-2(ii) of [I6]. It will also follow from our methods that if p is regular and $\Omega = \Omega^*$, then the map Ψ is injective. Furthermore, we shall show that injectivity of Ψ together with surjectivity of ψ forces ψ to be injective. Hence, we obtain the following result.

Theorem 1.2. *Let p be an odd regular prime. If $\Omega = \Omega^*$ and ψ is surjective, then Deligne's conjecture holds for p.*

For any number field F, Greenberg has a conjecture regarding the structure of the Galois group of a large pro-p extension of F unramified outside primes above p [G2] (see also [G1]). Let F_∞ denote the compositum of all $\mathbf{Z}_p$-extensions of F (which is necessarily unramified outside p), and let L_∞ denote the maximal abelian unramified pro-p extension of F_∞. Greenberg's conjecture states that $X = \mathrm{Gal}(L_\infty/F_\infty)$ has annihilator of height at least 2 as a module over the multivariable Iwasawa algebra $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$ [G2]. By class field theory, X is seen to be isomorphic to the

inverse limit A_∞ of the p-parts of the ideal class groups of finite subextensions of F in F_∞.

We consider Greenberg's conjecture for the field $F = \mathbf{Q}(\zeta_p)$, which we refer to as Greenberg's conjecture for the prime p. Since $A_\infty = 0$ if p is regular, Greenberg's conjecture holds trivially for regular primes. Let M_∞ denote the maximal abelian pro-p extension of F_∞ unramified outside p. Greenberg's conjecture for p is equivalent to $\mathrm{Gal}(M_\infty/F_\infty)$ having no torsion as a module over Λ [Mc, LN]. In particular, Greenberg's conjecture for an irregular prime p implies that $\mathrm{Gal}(\Omega/F)$ has no free pro-p quotient on $(p+1)/2$ generators [Mc] (see also [LN]). The absence of such a free pro-p quotient is the key to the following theorem.

Theorem 1.3. *Let p be an irregular prime. If Greenberg's conjecture holds for p, then ψ and Ψ are not isomorphisms. In particular, if Deligne's conjecture also holds for p, then ψ and Ψ are not surjective.*

McCallum has proven Greenberg's conjecture for a large class of irregular primes [Mc]. These are exactly those primes p for which both the p-part A of the ideal class group of $\mathbf{Q}(\zeta_p)$ and $(U/\bar{E})[p^\infty]$ are of order p, where U denotes the unit group of $\mathbf{Q}_p(\zeta_p)$ and $\bar{E}$ denotes the closure of the image of $\mathbf{Z}[\zeta_p]^*$ in U (see [Mc, Ma] for equivalent conditions). David Marshall has extended this result to a class of primes p for which A which may be cyclic of any positive p-power order [Ma]. Currently, there are no known examples in which A is cyclic of order greater than p. On the other hand, there are plenty of primes for which A is not cyclic, for instance $p = 157$ and 691.

2 Construction of the elements

Choose any element $\tau \in \mathrm{Gal}(\Omega/\mathbf{Q})$ that restricts to a generator of $\mathrm{Gal}(K/\mathbf{Q})$. Let $\delta = \lim_{i\to\infty} \tau^{p^i}$, an element of order $p-1$ restricting to a generator of $\mathrm{Gal}(F/\mathbf{Q})$, and let $\gamma = \tau^{p-1}$, which commutes with δ and restricts to a topological generator of $\mathrm{Gal}(K/F) \cong \mathbf{Z}_p$. By abuse of notation, we also denote by δ and γ the restrictions to subfields Galois over $\mathbf{Q}$. For any $m \in \mathbf{Z}$, let $\epsilon_m \in \mathbf{Z}_p[\mathrm{Gal}(\Omega/\mathbf{Q})]$ be the element

$$\epsilon_m = \frac{1}{p-1} \sum_{i=0}^{p-2} \chi(\delta^i)^{-m} \delta^i,$$

where $\chi\colon G_\mathbf{Q} \to \mathbf{Z}_p^*$ denotes the cyclotomic character.

Let E denote a pro-p extension of F (unramified outside p) which is also Galois over $\mathbf{Q}$. If E/F is nonabelian, we cannot in general define an action of the idempotent ϵ_m on $\mathrm{Gal}(E/F)$. However, the following provides something of a substitute. For $g \in \mathrm{Gal}(E/F)$, we define

$$g^{\epsilon_m} = (g \cdot \delta g^{\chi(\delta)^{-m}} \delta^{-1} \cdot \delta^2 g^{\chi(\delta^2)^{-m}} \delta^{-2} \cdots \delta^{p-2} g^{\chi(\delta^{p-2})^{-m}} \delta^{-p+2})^{1/(p-1)}. \qquad (2.1)$$

Note that $g^{\epsilon_m} = g^{\epsilon_{m'}}$ whenever $m \equiv m' \bmod p-1$. We also define $g^{\epsilon_m^i}$ to be the ith iterate $(\dots(g^{\epsilon_m})^{\epsilon_m}\dots)^{\epsilon_m}$. Although $\epsilon_m^2 = \epsilon_m$, we do not necessarily have $g^{\epsilon_m^2} = g^{\epsilon_m}$. Instead, we have the following lemma.

Lemma 2.1. *For any $g \in \mathrm{Gal}(E/F)$, the element*

$$g^{(m)} = \lim_{i\to\infty} g^{\epsilon_m^i}$$

is well-defined and satisfies

$$\delta g^{(m)} \delta^{-1} = (g^{(m)})^{\chi(\delta)^m}. \tag{2.2}$$

Proof. Set $N = \mathrm{Gal}(E/F)$. Let $x \in N$, and let B denote the normal closure in $\mathrm{Gal}(E/\mathbf{Q})$ of the subgroup generated by the elements $[x, \delta^j x \delta^{-j}]$ with $1 \le j \le p-2$. We begin by proving the claim that

$$\delta x^{\epsilon_m} \delta^{-1} (x^{\epsilon_m})^{-\chi(\delta)^m} \in B.$$

To see this, note that by definition (2.1) we have

$$\delta x^{\epsilon_m} \delta^{-1} = (\delta x \delta^{-1} \cdot \delta^2 x^{\chi(\delta)^{-m}} \delta^{-2} \cdots \delta^{p-2} x^{\chi(\delta^{p-3})^{-m}} \delta^{-p+2} \cdot x^{\chi(\delta)^m})^{1/(p-1)}. \tag{2.3}$$

In N/B, the terms of (2.3) commute, and the right-hand side of equation (2.3) equals

$$(x^{\chi(\delta)^m})^{\epsilon_m} = (x^{\epsilon_m})^{\chi(\delta)^m},$$

which proves the claim.

Let $N(i)$ denote the ith term in the lower central series of N. We now show inductively that for $i \ge 0$ and $1 \le j \le p-2$ we have

$$a_{i,j} = \delta^j g^{\epsilon_m^i} \delta^{-j} (g^{\epsilon_m^i})^{-\chi(\delta^j)^m} \in N(i+1). \tag{2.4}$$

Note that $a_{0,j} \in N = N(1)$, and assume that $a_{i-1,j} \in N(i)$ for each j and some $i \ge 1$. Our earlier claim implies that the element $a_{i,j}$ is contained in the normal closure $C(i+1)$ in $\mathrm{Gal}(E/\mathbf{Q})$ of the group generated by the commutators

$$b_{i,l} = [g^{\epsilon_m^{i-1}}, \delta^l g^{\epsilon_m^{i-1}} \delta^{-l}] = [g^{\epsilon_m^{i-1}}, a_{i-1,l}]$$

with $1 \le l \le p-2$. Hence $b_{i,l} \in N(i+1)$ for each l and therefore $a_{i,j} \in N(i+1)$.

Similarly, we have that

$$c_i = g^{\epsilon_m^i} (g^{\epsilon_m^{i-1}})^{-1} \in C(i+1) \triangleleft N(i+1). \tag{2.5}$$

As $\cap_{i=1}^{\infty} N(i) = \{1\}$, we have that $g^{(m)}$ is well-defined by (2.5). Furthermore, (2.2) holds by (2.4) with $j = 1$. □

We shall now make our choice of the elements σ_m described in the introduction. First, for odd m with $3 \leq m \leq p$, we choose any element $t_m \in \mathrm{Gal}(\Omega^*/K)$ such that $\kappa_m(t_m)$ generates $\kappa_m(\mathrm{Gal}(\Omega^*/K))$, and we set $g_m = t_m^{(m)}$, which also has maximal image. For such m, set $\sigma_m = g_m$. We recursively define the other elements g_m and σ_m by

$$g_{m+p-1} = \gamma g_m \gamma^{-1} g_m^{-\chi(\gamma)^m} \tag{2.6}$$

and

$$\sigma_{m+p-1} = (\gamma \sigma_m \gamma^{-1} \sigma_m^{-\chi(\gamma)^m})^{(m)} \tag{2.7}$$

for any odd $m \geq 3$.

(We remark that it is not necessary to take the limit element in (2.7); a finite iteration

$$(\gamma \sigma_m \gamma^{-1} \sigma_m^{-\chi(\gamma)^m})^{\epsilon_m^i}$$

would work as an element σ_{m+p-1}, in fact with $i \leq 1$ if $m \geq p-2$.)

Let L^* denote the maximal abelian extension of K in Ω^*.

Lemma 2.2. *The elements σ_m and g_m have the same restriction to L^* for all odd $m \geq 3$.*

Proof. For $3 \leq m \leq p$, the statement is trivially true. Note that ϵ_m defines an idempotent endomorphism of $G^{\mathrm{ab}} = \mathrm{Gal}(L^*/K)$. Also, ϵ_m commutes with conjugation by γ on G^{ab}. Hence we have

$$\begin{aligned} \sigma_{m+p-1}|_{L^*} = (\gamma \sigma_m \gamma^{-1} \sigma_m^{-\chi(\gamma)^m})^{\epsilon_m}|_{L^*} &= \gamma \sigma_m^{\epsilon_m} \gamma^{-1} (\sigma_m^{\epsilon_m})^{-\chi(\gamma)^m}|_{L^*} \\ &= \gamma \sigma_m \gamma^{-1} \sigma_m^{-\chi(\gamma)^m}|_{L^*}. \end{aligned}$$

The statement now follows immediately by induction. □

Let v_p denote the p-adic valuation on $\mathbf{Z}_p$.

Proposition 2.3. *Let m denote an odd integer with $m \geq 3$. The element σ_m fixes Ω^*_{m-1}, and its image under κ_m generates $\kappa_m(F^m G)$. Furthermore, if $m = k + j(p-1)$ for some integers $k \geq 3$ and $j \geq 0$, then*

$$v_p(\kappa_m(\sigma_m)) = v_p((jp)!) + v_p(\kappa_m(\sigma_k)).$$

Proof. We first show that σ_m fixes Ω^*_{m-1} inductively. Set $\Omega^*_k = K$ for $k < 0$. Assume that σ_m fixes Ω^*_{m-p+1}. Once we show that σ_m fixes Ω^*_{m-1}, then $\gamma \sigma_m \gamma^{-1} \sigma_m^{-\chi(\gamma)^m}$ will fix Ω^*_m, as $gr^m \mathfrak{g}$ has Tate twist m.

We prove the claim that if x fixes Ω^*_{m-p+1} then $y = x^{(m)}$ fixes Ω^*_{m-1}. Note first that y fixes Ω^*_{m-p+1}, so we assume inductively that it fixes Ω^*_{k-1} with $m-p+2 \leq k \leq m-1$. As Ω^*_k is abelian over Ω^*_{k-1} and $\mathfrak{g}_k$ has Tate twist k, we see that

$$\delta y \delta^{-1}|_{\Omega^*_k} = y^{\chi(\delta)^k}|_{\Omega^*_k}.$$

From Lemma 2.1, we therefore have that y will fix Ω^*_k, since $k \not\equiv m \bmod p-1$. We conclude that y fixes Ω^*_{m-1}. The first statement of the proposition now follows.

Note that

$$\kappa_m(\gamma t \gamma^{-1}) = \chi(\gamma)^m \kappa_m(t) \tag{2.8}$$

for any $t \in G$. Therefore, we see that

$$v_p(\kappa_m(\gamma t \gamma^{-1} t^{-\chi(\gamma)^l})) = v_p((m-l)p) + v_p(\kappa_m(t)) \tag{2.9}$$

for any $t \in G$. The last statement of the proposition now follows from the recursive definition (2.6) of g_m and (2.9).

By Lemma 2.2, the element g_m has the same image under κ_m as σ_m. Let $\tilde{L}$ denote the abelian subextension of Ω generated by roots of cyclotomic p-units, and note that κ_m can be considered as a homomorphism of $A = \mathrm{Gal}(\tilde{L}/K)$ [I6]. To prove the second statement of the proposition, it suffices to show that $\kappa_m(g_m)$ generates $\kappa_m(\mathrm{Gal}(\tilde{L}/\tilde{L} \cap \Omega^*_{m-1}))$.

Let i denote the unique integer with $3 \leq i \leq p$ and $m \equiv i \bmod p-1$. Let $A_i = A^{\epsilon_i}$, $B = \mathrm{Gal}(\tilde{L}/F)$, and $B_i = (B^{\mathrm{ab}})^{\epsilon_i}$. Let h_i denote an element of A_i restricting to a generator of the procyclic group B_i [W, Ch. 8,13]. Then h_i topologically generates A_i as a normal subgroup of B.

Let $\tilde{x}$ denote the restriction of an element $x \in \mathrm{Gal}(\Omega/F)$ to $\tilde{L}$. We claim that A_i is also the normal closure in B of the procyclic subgroup generated by $\tilde{g_i}$. If not, then since $\tilde{g_i} \in A_i$, we must have

$$\tilde{g_i} = x^p[\gamma, y]$$

for some $x, y \in A_i$. Clearly, we would then have

$$v_p(\kappa_i(g_i)) > v_p(\kappa_i(h_i)),$$

contradicting the definition of g_i.

Let A_m denote the largest normal subgroup of A_i fixing $\Omega^*_{m-1} \cap \tilde{L}$. We have $\kappa_m(F^m G) = \kappa_m(A_m)$, and so we need only show that A_m is the normal closure in B of the procyclic subgroup generated by $\tilde{g}_m$. Inductively assuming this is true for k, we prove it for $k+p-1$. If $x \in A_k$, then since A is abelian, $x \in A_k$ is a product of conjugates of $\tilde{g}_k$ by powers of $\tilde{\gamma}$. From equation (2.8), we see that

$$\kappa_k(\prod \gamma^j g_k^{a_j} \gamma^{-j}) = 0$$

if and only if

$$\sum a_j \chi(\gamma)^{kj} = 0.$$

Observing (2.6), we see that any such element is a product of conjugates of $\tilde{g}_{k+p-1}$ by powers of $\tilde{\gamma}$. □

Proposition 2.3 has an interesting application to the study of the stable derivation algebra $\mathcal{D}$ over $\mathbf{Z}$ considered by Ihara [I4, I5, I6]. Ihara has shown that there is a canonical embedding of graded $\mathbf{Z}_p$-Lie algebras

$$\iota\colon \mathfrak{g} \hookrightarrow \mathcal{D} \otimes \mathbf{Z}_p$$

and has conjectured that $gr^m\iota$ is an isomorphism for (at least) $m < p$. There is also a canonical map

$$\lambda_m\colon gr^m\mathcal{D} \to \mathbf{Z}$$

(denoted $gr^m(c)$ in [I6]) which, after extending $\mathbf{Z}_p$-linearly, we may compose with $gr^m\iota$ to obtain a map $\lambda_m^{(p)}$. The latter map is related to the Soulé character κ_m by the formula [I2, I6]

$$\kappa_m = (p^{m-1} - 1)(m-1)!\lambda_m^{(p)} \tag{2.10}$$

on F^mG. Let N_m denote the positive generator of the image ideal of λ_m.

Corollary 2.4. *Let p denote an odd prime satisfying Vandiver's conjecture. Let $m \geq 3$ be an odd positive integer, and let k denote the largest integer less than or equal to $(m-3)/(p-1)$. Then*

$$v_p(N_m) \leq v_p((kp)!) - v_p((m-1)!), \tag{2.11}$$

with equality if $gr^m\iota$ is an isomorphism.

Proof. Since $\lambda_m^{(p)}(F^mG) \subseteq N_m\mathbf{Z}_p$, this follows directly from (2.10), the surjectivity of $\kappa_{m-k(p-1)}$ under Vandiver's conjecture [IS] and the last statement of Proposition 2.3. □

3 Proofs of the main results

Before proving any theorems regarding ψ and Ψ, we make the following general points.

Lemma 3.1. *Fix $r \geq 1$, and consider a pro-p group $\mathcal{F}$ topologically generated by elements y and x_i with $1 \leq i \leq r$. For each $1 \leq i \leq r$, define $x_{i,1} = x_i$ and*

$$x_{i,j+1} = yx_{i,j}y^{-1}x_{i,j}^{-1+pa_{i,j}} = [y, x_{i,j}]x_{i,j}^{pa_{i,j}} \tag{3.1}$$

for some $a_{i,j} \in \mathbf{Z}_p$ for each $j \geq 1$. Let H denote the normal closure of the pro-p subgroup of $\mathcal{F}$ generated by the x_i with $1 \leq i \leq r$. Then:

a. *The elements $x_{i,j}$ with $1 \le i \le r$ and $j \ge 1$ topologically generate H.*

b. *If $\mathcal{F}$ is a free pro-p group on the elements y and x_i with $1 \le i \le r$, then H is a free pro-p group on the elements $x_{i,j}$.*

c. *Assume H is a free pro-p group on the elements $x_{i,j}$ with $1 \le i \le r$ and $j \ge 1$. If $y^{p^n} \notin H$ for all n, then $\mathcal{F}$ is a free pro-p group on the elements y and x_i with $1 \le i \le r$.*

Proof. To prove part (a), we need only show that, for each $k \ge 0$, the element $y^k x_i y^{-k}$ is contained in the pro-p subgroup generated by the elements $x_{i,j}$. This follows easily from the fact that the group generated by $x_{i,j+1}$ and $x_{i,j}$ contains $yx_{i,j}y^{-1}$.

For any pro-p group N, let $N[j]$ denote the jth term in its descending central p-series, and set $\bar{N} = N/N[2]$. Now assume $\mathcal{F}$ is free pro-p on y and the x_i. Note that H is a free pro-p group as a closed subgroup of a free pro-p group. Hence it is free on the $x_{i,j}$ if and only if the images of the $x_{i,j}$ form a minimal generating set of $\bar{H}$.

Fix i, and let $D = D_i$ denote the free pro-p subgroup of $\mathcal{F}$ generated by x_i and y. Let $C = C_i$ denote the normal closure in D of the pro-p subgroup generated by x_i. By freeness of $\mathcal{F}$, we have

$$\bar{H} \cong \bigoplus_{k=1}^{r} \bar{C}_k.$$

Hence we are reduced to showing that the images of the $x_{i,j}$ form a minimal generating set of $\bar{C}$. As $\bar{C}$ is elementary abelian, we have an injection

$$\bar{C} \hookrightarrow \bigoplus_{j \ge 0} (C \cap D[j])/(C \cap D[j+1]).$$

Finally, as $x_{i,j} \in D[j] \setminus D[j+1]$, we obtain minimality, proving part (b).

As for part (c), consider a free presentation of $\mathcal{F}$ on generators $\tilde{x}_i$ and $\tilde{y}$ mapping to x_i and y:

$$1 \to R \to \tilde{\mathcal{F}} \to \mathcal{F} \to 1.$$

By parts (a) and (b), the group $\tilde{\mathcal{F}}$ has a free subgroup $\tilde{H}$ on elements $\tilde{x}_{i,j}$ defined as in (3.1). Since H is free on the $x_{i,j}$, the map $\tilde{H} \to H$ is an isomorphism. Hence $R \cap \tilde{H} = 0$. Thus R is isomorphic to $R\tilde{H}/\tilde{H}$, which is a subgroup of the group $\tilde{\mathcal{F}}/\tilde{H} \cong \mathbf{Z}_p$ generated by the image of $\tilde{y}$. Hence, if R is nontrivial, then $\tilde{y}^{p^n} \in R\tilde{H}$ for some $n \ge 0$. Therefore we have $y^{p^n} \in H$, a contradiction. Hence R is trivial, proving (c). □

We now prove Theorem 1.1.

Proof of Theorem 1.1. For p regular, it is well-known that $\mathrm{Gal}(\Omega/F)$ is free pro-p on the generators γ and g_m with $3 \le m \le p$ and m odd. By the construction (2.6) of

the g_m and parts (a) and (b) of Lemma 3.1, it follows that $H = \mathrm{Gal}(\Omega/K)$ is freely generated as a pro-p group by the g_m with m odd ≥ 3. As H is pronilpotent, and since by Lemma 2.2 the elements σ_m and g_m have the same image on the Galois group of the maximal abelian subextension of K in Ω, we have that H is also free on the σ_m. As $G = \mathrm{Gal}(\Omega^*/K)$ is a quotient of H, the map Ψ is surjective. (Note that the surjectivity of Ψ does not depend on the choice of elements σ_m.)

Assuming Deligne's conjecture, we have that ψ, and hence Ψ, is injective. Therefore, Ψ is an isomorphism and $\Omega = \Omega^*$. Finally, the injectivity of ψ plus the surjectivity of Ψ yield the surjectivity of ψ [I6, §III-I-2]. □

The following serves as a rough converse to the injectivity implies surjectivity theorem for $\psi \otimes \mathbf{Q}_p$ proven by Ihara [I6, Theorem I-1]. Recall that $\mathfrak{s}$ arises as the graded Lie algebra associated to a filtration $F^m S$ on S compatible with the filtration on G [I6].

Theorem 3.2. *If Ψ is injective and ψ is surjective, then ψ is injective.*

Proof. We begin by assuming merely that Ψ is injective and ψ is not. Then $\psi(\bar{x}) = 0$ for some nonzero $\bar{x} \in gr^m\mathfrak{s}$ and $m \geq 3$. Choose a lift $x_1 \in S$ of $\bar{x}$. Since Ψ is injective, the image element $g_1 = \Psi(x_1)$ is nontrivial. Let k_1 be maximal such that g_1 fixes $\Omega^*_{k_1-1}$. Let $\bar{g}_1$ be the image of g_1 in $gr^{k_1}\mathfrak{g}$. By [HM], we have that $\psi \otimes \mathbf{Q}_p$ is surjective, so there exists $\bar{y}_1 \in gr^{k_1}\mathfrak{s}$ such that $\psi(\bar{y}_1) = p^{n_1}\bar{g}_1$ for some minimum possible $n_1 \geq 0$. Set $x_2 = x_1^{p^{n_1}} y_1^{-1}$ for y_1 lifting $\bar{y}_1$. By construction and the injectivity of Ψ, there exists $k_2 > k_1$ maximal such that $g_2 = \Psi(x_2)$ fixes $\Omega^*_{k_2-1}$. By induction, we obtain a sequence of elements $x_i \in S$, each of which restricts to some multiple of $\bar{x} \in gr^m\mathfrak{s}$, and corresponding sequences of elements y_i and exponents n_i such that $x_{i+1} = x_i^{p^{n_i}} y_i^{-1}$.

If ψ is surjective, then each n_i is zero. Since the sequence of numbers k_i is increasing, the sequence x_i has a limit $x \in S$ which restricts to $\bar{x} \in gr^m\mathfrak{s}$. We see that $\Psi(x) = 0$, as $\Psi(x)$ will fix Ω^*_k for every k. This is a contradiction, proving the theorem. Note that, removing the assumption of the surjectivity of ψ, this argument yields that infinitely many of the n_i are non-zero. □

Theorem 1.2 now follows as a corollary to Theorem 3.2.

Proof of Theorem 1.2. If $\Omega = \Omega^*$, then since p is regular, Lemma 3.1b implies that G is free on the generators g_m with m odd ≥ 3 and hence is free on the σ_m by Lemma 2.2. That is, Ψ is an isomorphism. Since by assumption ψ is surjective, Theorem 3.2 implies that ψ is an isomorphism. □

Before proving Theorem 1.3, we make the following remark.

Lemma 3.3. *The state of Ψ being an isomorphism does not depend on the choice of elements σ_m.*

Proof. For each odd $m \geq 3$, let τ_m be an element of $F^m G$ with maximal possible image under κ_m. Let $\Psi' \colon S \to G$ be a homomorphism satisfying $\Psi'(s_m) = \tau_m$ for each odd $m \geq 3$. Assume that Ψ is an isomorphism. The surjectivity of Ψ forces that

$$\tau_m|_{L^*} = \prod_{\substack{k \geq m \\ k \text{ odd}}} \sigma_k^{a_{m,k}}|_{L^*}$$

for some $a_{m,m} \in \mathbf{Z}_p^*$ and $a_{m,k} \in \mathbf{Z}_p$ for odd $k > m$. Setting $a_{m,k} = 0$ for $k < m$, we find that the matrix formed by the $a_{m,k}$ with m and k odd ≥ 3 is upper triangular and invertible. Then the $\tau_m|_{L^*}$ form a minimal generating set of $G^{\mathrm{ab}} = \mathrm{Gal}(L^*/K)$, and hence the τ_m freely generate G, as G is a free pro-p group. □

We may now prove Theorem 1.3.

Proof of Theorem 1.3. The idea of the proof is to show that if ψ or Ψ is an isomorphism then $\mathcal{G} = \mathrm{Gal}(\Omega^*/F)$ is free, contradicting the corollary of Greenberg's conjecture that $\mathrm{Gal}(\Omega/F)$ has no free pro-p quotient of rank $(p+1)/2$. The state of ψ or Ψ being an isomorphism does not depend on the choice of generators σ_m by [I6, §III-6] and Lemma 3.3, so we use our previously defined generators from (2.7) (which is possible by Proposition 2.3).

If ψ is an isomorphism, then Ψ is as well [I6, §III-6]. Assume that Ψ is an isomorphism. This means that the σ_m freely generate G, so Lemma 2.2 implies that the g_m do as well. We clearly have that $\mathcal{G}$ is generated by γ and g_m with m odd and $3 \leq m \leq p$. As $\gamma^{p^n} \notin G$ for any n, it follows by Lemma 3.1c that $\mathcal{G}$ is freely generated by these elements, finishing the proof. □

4 The filtration on the Galois group

We now consider the question of where in the filtration of G the nonsurjectivity of Ψ may first occur. In this regard, we also have the following extension of Theorem I-2(ii) of [I6] which removes the assumption $m < p$. It can also be viewed as a more precise version of the contrapositive to Theorem 1.1 that if Ψ is not surjective, then p is irregular.

Let $G_m = \mathrm{Gal}(\Omega_m^*/K)$ and set $S_m = S/F^{m+1}S$ [I6]. We also recall the map $\Psi_m \colon S_m \to G_m$ with $\Psi_m(s_i) = \sigma_i$ for $3 \leq i \leq m$ and i odd.

Theorem 4.1. *Let p be an odd prime and assume that Ψ is not surjective. If m is minimal such that Ψ_m is not surjective, then Ω_m^* contains a nontrivial elementary abelian extension of F with Tate twist m which is linearly disjoint from the fixed field of the kernel of κ_m if m is odd. If m is even, then p divides B_m and $L^* \cap \Omega_m^*$ has a nontrivial even part. If m is odd, then p divides B_{p-m} and Vandiver's conjecture fails at p.*

Proof. We remark that the surjectivity, or lack thereof, of Ψ and Ψ_m is independent of the choice of the elements σ_k. Thus, Proposition 2.3 again allows us to use our choice of σ_k from (2.7).

Set $B = gr^m\mathfrak{g}$ if m is even, and let B denote the kernel of κ_m on $gr^m\mathfrak{g}$ if m is odd. Set $A = B/(B \cap G_m(2))$. Similarly to the proof of Theorem I-2(ii) of [I6], we have an isomorphism of abelian groups

$$G_m^{\mathrm{ab}} \cong \Psi(S_m)^{\mathrm{ab}} \times A.$$

We claim that $\Psi(S_m)^{\mathrm{ab}}$ is a $\mathbf{Z}_p^*$-submodule of G_m^{ab}. (Ihara points out that a similar group need not be $\mathbf{Z}_p^*$-stable.) In fact, we have by definition that

$$\delta\sigma_k\delta^{-1} = \sigma_k^{\chi(\delta)^k}$$

and

$$\gamma\sigma_k\gamma^{-1}|_{L^*} = \sigma_k^{\chi(\gamma)^i}\sigma_{k+p-1}|_{L^*}.$$

This proves the claim, so A is a direct summand of G_m^{ab} as a $\mathbf{Z}_p^*$-submodule.

Therefore, A gives rise to an abelian pro-p extension Σ of K unramified outside p with Tate twist m and satisfying $\Sigma \cap \tilde{L} = K$. The maximal elementary abelian subextension of Σ/K descends to the desired elementary abelian p-extension of F. $\square$

One may ask if the assumption $m < p$ in Ihara's result actually needs to be removed. That is, is the smallest m such that Ψ_m is not surjective also the smallest m such that p divides B_m? We shall briefly describe what an answer should involve.

Let us assume Vandiver's conjecture at p. That p divides B_m indicates the existence of a relation in $\mathcal{G}$. If m is any number such that Ψ_{m-1} is surjective, then the relation induced in G_m can be put in the form

$$h^{p^c} = \Psi_m(s)$$

for some $h \in G_m$, $c \geq 1$, and $s \in [S_m, S_m]$ which is not a pth power of a nontrivial element. The map Ψ_m is not surjective if and only if $\Psi_m(s) \neq 1$. The surjectivity of Ψ_m is therefore governed by both the structure of the relation in $\mathcal{G}$ and the form of the filtration on G, two objects about which we require more information.

For example, in the case $p = 691$ and $m = 12$ considered by Ihara [I6] we know that the commutators $[\sigma_3, \sigma_9]$ and $[\sigma_5, \sigma_7]$ are linearly independent in $gr^{12}\mathfrak{g} \otimes \mathbf{Q}_{691}$ [Mt], and so we have information about the filtration. However, to prove the nonsurjectivity of Ψ_{12} one still needs to demonstrate that the relation in $\mathcal{G}$ actually "involves" these commuators so that in G_{12} it reduces to a nontrivial relation of the form

$$h^{691} = [\sigma_3, \sigma_9]^a[\sigma_5, \sigma_7]^b.$$

This question will be discussed in further detail in [MS].

References

[G1] R. Greenberg, *On the structure of certain Galois groups.* Invent. Math. **47** (1978), 85–99.

[G2] R. Greenberg, *Iwasawa Theory - past and present.* Class Field Theory - It's Centenary and Prospect, Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 335–385.

[HM] R. Hain and M. Matsumoto, *Weighted completion of Galois groups and Galois actions on the fundamental group of* $\mathbf{P}^1 - \{0, 1, \infty\}$. arXiv:math.AG/0006158, Aug. 11, 2001.

[IS] H. Ichimura and K. Sakaguchi, *The non-vanishing of a certain Kummer character* χ_m *(after C. Soulé) and some related topics.* Galois Representations and arithmetic algebraic geometry, Adv. Stud. Pure Math., vol. 12, North-Holland, Amsterdam, 1987, pp. 53–64.

[I1] Y. Ihara, *Profinite braid froups, Galois representations and complex multiplications.* Ann. of Math. **123** (1986), 43–106.

[I2] Y. Ihara, *The Galois representation arising from* $\mathbf{P}^1 - \{0, 1, \infty\}$ *and Tate twists of even degree.* Galois groups over $\mathbf{Q}$, Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 299–313.

[I3] Y. Ihara, *Braids, Galois groups, and some arithmetic functions.* Proceedings of the International Congress of Mathematicians, Vol. I (Kyoto, 1990), Math Soc. Japan, Tokyo, 1991, pp. 99–120.

[I4] Y. Ihara, *Automorphisms of pure sphere braid groups and Galois representations.* The Grothendieck Festschrift, Vol. II, Prog. in Math., vol. 87, Birkhäuser, Boston, 1991, pp. 353–373.

[I5] Y. Ihara, *On the stable derivation algebra associated with some braid groups.* Israel J. Math. **80** (1992), 135–153.

[I6] Y. Ihara, *Some arithmetic aspects of Galois actions of the pro-p fundamental group of* $\mathbf{P}^1 - \{0, 1, \infty\}$. Proc. Symp. Pure Math. (this volume).

[LN] A. Lannuzel, T. Nguyen Quang Do, *Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres.* Manuscripta Math. **102** (2000), no. 2, 187–209.

[Ma] D. Marshall, *Greenberg's conjecture and cyclotomic towers.* UIUC Algebraic Number Theory Preprint Archives, no. 309, Sept. 25, 2001.

[Mt] M. Matsumoto, *On the Galois image in the derivation algebra of π_1 of the projective line minus three points.* Recent developments in the inverse Galois Problem, Contemporary Math., vol. 186, Amer. Math. Soc., Providence, RI, 1995, pp. 201–213.

[Mc] W. McCallum, *Greenberg's Conjecture and units in multiple $\mathbf{Z}_p$-extensions.* Amer. J. Math. **123** (2001), no. 5, 909–930.

[MS] W. McCallum and R. Sharifi, *A cup product in the Galois cohomology of number fields.* In preparation.

[So] C. Soulé, *On higher p-adic regulators.* Algebraic K-theory, Evanston 1980, Lecture Notes in Math., vol. 854, Springer, Berlin-New York, 1981, pp. 372–401.

[W] L. Washington, Introduction to Cyclotomic Fields, 2nd ed., Springer, New York, 1997.

Department of Mathematics
Harvard University
Cambridge, MA 02138
e-mail address: sharifi@math.harvard.edu
web page: http://www.math.harvard.edu/~sharifi