The question of Anderson and Ihara on the pro-p Galois action on the projective line minus three points, at every prime satisfying Vandiver's conjecture

Version 2, 24 November 2026 CC0 1.0

hexagon:2611.00939v2

Abstract

Ihara showed that the kernel of the outer action of the absolute Galois group of $\mathbb{Q}$ on the pro-p fundamental group of the projective line minus three points cuts out a field contained in the maximal pro-p extension of $\mathbb{Q}(\mu_p)$ unramified outside p, and Anderson and Ihara asked whether the two fields are equal. Sharifi proved that they are equal at odd regular primes if the Deligne–Ihara conjecture holds, and Brown proved that conjecture. We prove the equality at every odd prime p for which the plus part of the Iwasawa module of p-class groups of the cyclotomic tower is finite. This holds whenever p does not divide the class number of the real cyclotomic field $\mathbb{Q}(\mu_p)^+$, which is Vandiver's conjecture at p; by the computation of Hart, Harvey and Ong the equality therefore holds at every odd prime below 2^{31}. At an irregular prime the Galois group in question has generators that the regular case does not have. The theorems of Fukaya–Kato and Wake–Wang-Erickson on Sharifi's symbol map show that cup products of cyclotomic units generate the relevant second cohomology at every finite level, and we prove that this forces the images of the new generators to have poles that separate all words. The mathematics and the proofs were produced by GPT-6 Astra (ChatGPT Pro mode). Claude Opus 5.5 at effort high checked the deduction from Vandiver's conjecture and the present text of Sections 4 to 6 step by step, with the theorems of Fukaya–Kato and Wake–Wang-Erickson read at the places cited; Claude Fable 5.2 at effort max edited the text, wrote its first two sections and refereed Sections 3 to 6. No human has checked it.

1 The question and the theorem

Let p be an odd prime,

$$\mathcal{X} = \mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}, \qquad \Pi_p = \pi_1^{\text{ét}}(\mathcal{X}_{\overline{\mathbb{Q}}})^{(p)}, \qquad \rho_p : G_{\mathbb{Q}} \longrightarrow \mathrm{Out}(\Pi_p), \tag{1.1}$$

where Π_p is the maximal pro-p quotient of the geometric fundamental group, a free pro-p group of rank two, and ρ_p is the outer action of the absolute Galois group. Write Ω_p^* for the fixed field of $\ker \rho_p$, and Ω_p for the maximal pro-p extension of $F_1 = \mathbb{Q}(\mu_p)$ unramified outside p, both inside one algebraic closure. Ihara proved $\Omega_p^* \subseteq \Omega_p$ [7]; see [13, p. 1]. Anderson and Ihara asked whether

$$\Omega_p^* = \Omega_p$$

[1, p. 272, question (a)]. Put

$$F_r = \mathbb{Q}(\mu_{p^r}), \qquad F_\infty = \bigcup_{r \geq 1} F_r, \qquad X_p = \varprojlim_r \mathrm{Cl}(F_r)\{p\}, \tag{1.2}$$

the limit of the p-primary parts of the class groups for the norm maps, and let X_p^+ be the part of X_p fixed by complex conjugation. Greenberg's conjecture for this tower is the finiteness of X_p^+. Vandiver's conjecture at p is $p \nmid h(F_1^+)$, where F_1^+ is the real subfield of F_1.

Theorem 1.1. *Let p be an odd prime.*

(a) *If X_p^+ is finite, then $\Omega_p^* = \Omega_p$.*

(b) *If p does not divide the class number of $\mathbb{Q}(\mu_p)^+$, then $X_p^+ = 0$, and so $\Omega_p^* = \Omega_p$.*

(c) *$\Omega_p^* = \Omega_p$ for every odd prime $p < 2^{31}$.*

What it means. The pro-p covers of the line minus three points, with the Galois action on them, see every extension of $\mathbb{Q}(\mu_p)$ that the ramification condition allows: an element of $G_{\mathbb{Q}}$ that acts trivially on the tower of these covers, up to inner automorphisms, fixes Ω_p. Equivalently, the group $\mathrm{Gal}(\Omega_p/\mathbb{Q})$ acts faithfully on Π_p by outer automorphisms. Anderson and Ihara described Ω_p^* as the field generated by their higher circular p-units [1, Theorem 2 (IV)], as recalled in [8, p. 2]; for the primes of the theorem these units therefore generate all of Ω_p. Part (c) uses the verification of Vandiver's conjecture for every odd prime below 2^{31} by Hart, Harvey and Ong [6, Section 1, item (2)]; that computation is an input.

Why it matters. The action of $G_{\mathbb{Q}}$ on the fundamental group of $\mathcal{X}$ is the first case of the programme, going back to Grothendieck and to Ihara's paper [7], of describing Galois groups through their action on fundamental groups of moduli spaces. Its pro-p part is the best understood: its image is filtered, the graded pieces carry the Soulé characters, and after tensoring with $\mathbb{Q}_p$ the graded Lie algebra is free on one generator in each odd degree at least three, by Brown's theorem. What the kernel is had been known only at regular primes. The theorem gives it at every prime for which Vandiver's conjecture is known, which at present includes every irregular prime below 2^{31}, and it reduces the question at the remaining primes to Greenberg's conjecture for the cyclotomic tower.

Credit. The inclusion $\Omega_p^* \subseteq \Omega_p$ is Ihara's and the question is Anderson and Ihara's. Sharifi proved that at an odd regular prime the Deligne–Ihara conjecture implies the equality [13, Theorem 1, p. 2], and Brown proved that conjecture [2, Theorem 1.1]; so the regular case is their theorem. The proof here follows the same plan: embed the arithmetic group in a free prounipotent group and separate its elements by coefficients. It uses, as theorems of their authors, the weighted completion of Hain and Matsumoto [5] and Brown's theorem for the target; the theorems of Ferrero–Washington [3] and Iwasawa [9] for the freeness of the arithmetic group; and, for the step that is new at irregular primes, the symbol construction of Fukaya and Kato [4] with the integral isomorphism theorem of Wake and Wang-Erickson [17], both proved in the study of Sharifi's conjectures. That Vandiver's conjecture implies Sharifi's conjecture is due to Wake and Wang-Erickson [16, abstract and Corollary 5.1.2]. What is supplied here are two lemmas, the comparison of finite-level cup products with the class-two extension of the arithmetic group (Lemma 4.1) and the separation of Magnus coefficients by poles (Lemma 5.1), and the verification of their hypotheses.

Context. Sharifi's argument at regular primes uses that $\mathrm{Gal}(\Omega_p/F_1)$ is then free pro-p on generators in odd characters only. The same paper studies, at irregular primes, whether Soulé elements generate the graded Lie algebra over $\mathbb{Z}_p$, which is a different question [13, Sections 1 and 4]; the present theorem makes no integral statement of that kind. Ishii recalls the regular case [8, Theorem 1.1 and Remark 1.1.1, p. 2] and proves an analogue of Sharifi's theorem for once-punctured elliptic curves with complex multiplication, under an analogue of the Deligne–Ihara conjecture [8, Theorem A, p. 2]; his statement is recalled in Remark 8.1. In 2019 Sharifi recalled that for regular p the outer action is known to be injective on $\mathrm{Gal}(\Omega_p/F_\infty)$, which is the equality $\Omega_p^* = \Omega_p$, and described the irregular case as

"a very interesting open question of Anderson and Ihara" [14, §1, p. 221]. We have found no earlier statement of the equality at an irregular prime; searches of the literature and of Hexagon on 23 November 2026 returned none.

Scope. The theorem does not prove Vandiver's or Greenberg's conjecture and says nothing at an odd prime where X_p^+ is not known to be finite. The prime 2, where the real place needs a convention, is not treated in this note.

2 Proof overview

Let $H = \mathrm{Gal}(\Omega_p/F_\infty)$. An element of $\ker \rho_p$ acts trivially on μ_{p^∞}, so its image in $\mathrm{Gal}(\Omega_p/\mathbb{Q})$ lies in H, and the theorem says that the outer action of H on Π_p is faithful. The action on Π_p induces one on its rational unipotent completion, and by Hain and Matsumoto the image of H there is Zariski dense in a prounipotent group $\mathcal{U}_p$ whose Lie algebra is, by Brown's theorem, free on letters s_m of odd weight $m \geq 3$ (Section 3). So it suffices to prove that $\rho : H \to \mathcal{U}_p(\mathbb{Q}_p)$ is injective.

The regular case. H is a free pro-p group (Iwasawa, with $\mu = 0$), with an action of $\Gamma = \mathrm{Gal}(F_\infty/F_1)$ and of $\Delta = \mathrm{Gal}(F_1/\mathbb{Q})$. If p is regular, H^{ab} is free of rank one over the Iwasawa algebra in each odd character of Δ and zero in the even ones. The coefficient of a word in the letters s_m is then an iterated integral of bounded measures on Γ, evaluated at the weights u^m; a nontrivial element has a nonzero coefficient because a nonzero bounded measure has a nonzero moment at infinitely many weights.

The difficulty. At an irregular prime $H^{\mathrm{ab}} = U \oplus T$ has an even part T, of finite rank over $\mathbb{Z}_p$, dual to the minus part of X_p. The target has no letters of even weight. A generator y of H lying over T is sent to words of length at least two, and nothing in the rational picture prevents the images of such generators from satisfying relations.

The idea. Let q_e be the characteristic polynomial of a generator γ of Γ on a character component T_e. The element $q_e(\gamma)y$ is trivial in H^{ab}, hence a product of commutators, and its class modulo triple commutators is an alternating tensor C_e in two odd variables. The length-two coefficient of y at weights (m, n) is then $C_e(u^m - 1, u^n - 1)/q_e(u^{m+n})$: it is a quotient of power series with a pole along $(1 + T_1)(1 + T_2) = \alpha$ for each root α of q_e. If the numerator does not vanish identically on each of these pole divisors, then in the coefficient of a first nonzero degree one can isolate, by expanding along the poles of highest order, a single product of nonzero factors; this proves injectivity (Lemma 5.1). Repeated roots are allowed.

Why the numerators do not vanish. If C_e vanished on the pole divisor of α, the class-two quotient of H would split equivariantly over an eigenline $W \subset T$ for α. A cochain computation then shows that, at every finite level n, the cup product of two even classes in H^1 of $\mathrm{Gal}(\Omega_p/F_{n+1})$ with coefficients $\mathbb{Z}/p^n(1)$ has zero component along W in H^2 with coefficients $\mathbb{Z}/p^n(2)$ (Lemma 4.1). This is impossible if such cups generate the even part of that H^2 at every level. That generation is the arithmetic input: under the finiteness of X_p^+, Wake and Wang-Erickson prove that Sharifi's symbol map is surjective, and Fukaya and Kato deduce that the symbols $\{1 - \zeta^a, 1 - \zeta^b\}$ of cyclotomic units generate at each finite level (Section 6).

Where the hypothesis is used. The finiteness of X_p^+ is used three times in Section 6: for the freeness of rank one of U after inverting p, for the cyclicity of each T_e after inverting p, and for the surjectivity of the symbol map. Section 7 proves part (b): if $p \nmid h(F_1^+)$ then the p-class groups of all layers of the real tower vanish, because each layer is cyclic of degree p over the previous one and totally ramified at one prime (Lemma 7.1).

3 The rational outer image

We first identify the representation into which the arithmetic group will be embedded. Rational unipotent completion of Π_p is functorial for automorphisms and inner automorphisms. It therefore induces a homomorphism from its pro-p outer automorphism group to the outer automorphism group of the rational completion [5, Appendix A.6, A.9–A.10]. In particular, an element acting trivially on Π_p acts trivially on this rational completion.

Let B_p denote the proalgebraic closure of the induced arithmetic outer image, and let $\mathcal{U}_p$ denote its prounipotent radical. The cited Hain–Matsumoto results give

$$1 \longrightarrow \mathcal{U}_p \longrightarrow B_p \longrightarrow \mathbb{G}_m \longrightarrow 1, \qquad H \longrightarrow \mathcal{U}_p(\mathbb{Q}_p) \tag{3.1}$$

with dense image in each finite weight quotient. The reductive quotient is the cyclotomic character. Brown's theorem [2] identifies the graded Lie algebra of $\mathcal{U}_p$ with the free Lie algebra on one letter s_m in each odd arithmetic weight $m \geq 3$.

The dense subgroup in Hain–Matsumoto's Theorem 8.4 is the cyclotomic kernel $I_p^1 G_{\mathbb{Q},\{p\}}$. To identify its image here, put $\mathcal{G}_p = \mathrm{Gal}(\Omega_p/\mathbb{Q})$. The quotient $G_{\mathbb{Q},\{p\}} \to \mathcal{G}_p$ maps that kernel onto H: any lift of an element of H already fixes every p-power root of unity, since the cyclotomic field lies in Ω_p. Conversely a cyclotomically trivial element maps into $H = \mathrm{Gal}(\Omega_p/F_\infty)$. The rational outer action factors through this quotient, so its images of these two kernels coincide. This proves the asserted density for the specific arithmetic group used below.

Here is the completion and normalization used below. A Levi splitting provides the weight decomposition. Choose homogeneous lifts of the free graded generators. The homomorphism from the completed free Lie algebra on these lifts induces an isomorphism on every graded piece. Induction on the finite weight filtration makes it an isomorphism on each finite quotient; the separated inverse limit is an isomorphism of completed Lie algebras. Its completed enveloping algebra is thus the free associative algebra completed by arithmetic weight. There are only finitely many letters and words below each fixed weight.

For odd p, choose a lift γ of a generator of $\mathrm{Gal}(F_\infty/F_1)$ and write $u = \chi_p(\gamma) \in 1 + p\mathbb{Z}_p$. In each positive weight the linear operator $u^m - 1$ is invertible over $\mathbb{Q}_p$. Successive conjugation in those weight spaces puts the image of γ in a Levi torus. If the prime-to-p group Δ commutes with γ, its unipotent part is then trivial: a first nonzero weight of an element centralizing γ would be fixed by u^m, which is impossible. Consequently conjugation on the letters is

$$\gamma s_m = u^m s_m, \qquad \delta s_m = \omega(\delta)^m s_m. \tag{3.2}$$

This normalization is performed at finite weights before taking the inverse limit.

4 Cup products and the class-two extension

This section proves the precise link from finite arithmetic cup products to the denominators that occur in the rational action. All cohomology of profinite groups is continuous cohomology. Completed tensor and exterior products are taken in the category of compact $\mathbb{Z}_p$-modules.

Lemma 4.1 (Finite-level cup comparison)**.** *Let p be odd, let $P = H \rtimes \Gamma$, where H is free pro-p and $\Gamma = \langle\gamma\rangle \simeq \mathbb{Z}_p$, and let an involution c preserve H and fix γ. Put*

$$\Lambda = \mathbb{Z}_p[[\Gamma]], \qquad R = \Lambda[1/p], \qquad H^{\mathrm{ab}} = U \oplus T, \tag{4.1}$$

where $c = -1$ on U and $c = 1$ on T. Suppose that U is finitely generated over Λ, that $U[1/p]$ is free of finite rank over R, and that T is finite free over $\mathbb{Z}_p$. Suppose also that each even

character component $T_e[1/p]$ under the commuting prime-to-p action is cyclic over R. Write $q_e(z)$ for its monic characteristic and minimal polynomial for γ.

Let the coefficient character satisfy $\chi(\gamma) = u \in 1 + p\mathbb{Z}_p$ and $\chi(c) = -1$, with H acting trivially on its twists. Assume that, for every $n \geq 1$, the even part of

$$H^2(P_n, \mathbb{Z}/p^n(2)), \qquad P_n = H \rtimes \Gamma^{p^n}, \tag{4.2}$$

is generated by cups of c-even classes in $H^1(P_n, \mathbb{Z}/p^n(1))$. A cofinal diagonal of the two level indices suffices.

Then the odd–odd companion numerators of the group extension satisfy the pole-nonvanishing condition: for every root α of every nonzero q_e, at least one coefficient has nonzero restriction to

$$D_\alpha = (1 + T_1)(1 + T_2) - \alpha = 0. \tag{4.3}$$

Here coefficients are taken in the bounded-denominator power-series coordinates of an R-basis of $U[1/p]$. Repeated roots are allowed. For the subsequent pole-separation application the arithmetic module input supplies rank one in every odd character.

Proof. Since 2 is a unit, the class-two quotient of H has its integral Baker–Campbell–Hausdorff Lie structure. Quotient its central commutator module by all brackets having a T input. The remaining central module is

$$N = \widehat{\bigwedge}^2_{\mathbb{Z}_p} U. \tag{4.4}$$

Complex conjugation is 1 on N. Thus the minus part of the resulting Lie module maps isomorphically to U, providing a canonical Γ-equivariant odd section. Its plus part is the continuous module extension

$$0 \longrightarrow N \longrightarrow E \longrightarrow T \longrightarrow 0. \tag{4.5}$$

Choose a rational cyclic generator v of $T_e[1/p]$ and a lift $y \in E[1/p]$ in the same character component, using the prime-to-p character projector. The element

$$q_e(\gamma)y = C_e \in N[1/p] \tag{4.6}$$

is precisely the odd–odd quadratic companion error. In the quotient just taken, brackets involving even lifts vanish, so an ordered companion product becomes its additive characteristic-polynomial expression. A derived element has the same degree-two logarithmic and Magnus coefficient.

Finite generation clears the denominators of the chosen isomorphism $U[1/p] \simeq R^r$ and its inverse: for some a, $p^a\Lambda^r \subset U \subset p^{-a}\Lambda^r$ in these coordinates. Completed tensor and exterior squares inherit fixed denominator bounds. Consequently $N[1/p]$ is the bounded-denominator alternating two-variable coefficient module, rather than a module of series with arbitrary coefficient denominators.

Pass to a finite splitting field $L/\mathbb{Q}_p$, with integers $\mathcal{O}$, and suppose that every coefficient of C_e vanishes on $D_\alpha = 0$. All roots satisfy $\alpha - 1 \in \mathfrak{m}_\mathcal{O}$, because the action of the pro-p group Γ on the finite-rank lattice T is continuous. The change of variable

$$S = (1 + T_1)(1 + T_2) - \alpha, \qquad T_2 = \frac{\alpha + S}{1 + T_1} - 1 \tag{4.7}$$

is an integral formal-coordinate change. Its specialization kernel is (S), and division preserves a common denominator bound. Since D_α is symmetric, an alternating numerator has an alternating quotient. Thus, in N_L,

$$C_e = (\gamma - \alpha)A. \tag{4.8}$$

Wrong-character coefficients are identically zero, so it suffices to assume vanishing for the matching odd-character pairs.

Set $r_e(z) = q_e(z)/(z-\alpha)$. Cyclicity implies that $w = r_e(\gamma)v$ is nonzero and spans an α-eigenline $W \subset T_L$. For a repeated root it is the socle of the cyclic generalized eigenspace. Equations (4.6)–(4.8) show that

$$\widetilde{w} = r_e(\gamma)y - A \tag{4.9}$$

is a Γ-equivariant lift of w. Hence (4.5) splits over W after inverting p.

We now compare this split with the cup map of this group. The lattice $T_{\mathcal{O}} \cap W$ is saturated, hence an $\mathcal{O}$-direct summand of $T_{\mathcal{O}}$. Choose an $\mathcal{O}$-linear section $s : T_{\mathcal{O}} \to E_{\mathcal{O}}[1/p]$ extending the equivariant section on that lattice. A fixed power p^b makes this section integral. Write the class-two logarithm of $h \in H$ as

$$x(h) + s(t(h)) + z(h), \qquad x(h) \in U_{\mathcal{O}}, \quad t(h) \in T_{\mathcal{O}}, \quad z(h) \in N_{\mathcal{O}}[1/p]. \tag{4.10}$$

The same p^b clears every $z(h)$. The section defect is

$$\beta_\delta(t) = \delta s(t) - s(\delta t), \qquad \delta \in \Gamma, \tag{4.11}$$

and it vanishes on W.

Fix n and two even cohomology classes f, g. Average their cocycles by $(1+c)/2$. The resulting invariant cocycles vanish on the chosen $\Gamma_n = \Gamma^{p^n}$ section: c fixes its elements and is -1 on the coefficient module. On H they are additive maps from U to $\mathcal{O}/p^n(1)$, vanish on T, and are Γ_n-equivariant. Put

$$\psi = f \wedge g : N_{\mathcal{O}} \longrightarrow \mathcal{O}/p^n(2), \quad \psi([x_1, x_2]) = f(x_1)g(x_2) - f(x_2)g(x_1). \tag{4.12}$$

The continuous cochain

$$k(h) = -\frac{p^b}{2} f(h)g(h) - \psi(p^b z(h)) \tag{4.13}$$

is integral. The class-two product has central coordinate $z_1 + z_2 + [x_1, x_2]/2$. Its substitution in (4.13) gives

$$dk(h_1, h_2) = p^b f(h_1)g(h_2). \tag{4.14}$$

Indeed the two summands contribute respectively $p^b(f_1 g_2 + f_2 g_1)/2$ and $p^b(f_1 g_2 - f_2 g_1)/2$.

Extend k to P_n by $k(h\delta) = k(h)$. For $h, h' \in H$ and $\delta, \delta' \in \Gamma_n$, the residual cocycle is explicitly

$$\begin{aligned} &(p^b f \smile g - dk)(h\delta, h'\delta') \\ &\qquad = k(\delta h' \delta^{-1}) - \chi(\delta)^2 k(h') \\ &\qquad = -\psi(p^b \beta_\delta(t(h'))). \end{aligned} \tag{4.15}$$

Indeed f and g vanish on the section, their restrictions to H are Γ_n-equivariant, and the quadratic summand of k transforms by χ^2. Thus its Hochschild–Serre edge is, up to the convention for the edge sign and input conjugation,

$$\pm\psi(p^b \beta_\delta(t)). \tag{4.16}$$

This vanishes on W. A convention that conjugates t makes no difference because W is Γ-stable. Thus the same fixed p^b multiple of every cup has zero restriction to the dual of W, at every finite level.

For completeness, the target and its transitions are explicit. Both H and Γ_n have p-cohomological dimension one, and the minus part U contributes only odd parity. Therefore

$$H^2(P_n, \mathcal{O}/p^n(2))^+ \simeq H^1(\Gamma_n, \mathrm{Hom}(T, \mathcal{O}/p^n)(2)). \tag{4.17}$$

Let $V = \mathrm{Hom}_{\mathbb{Z}_p}(T, \mathcal{O})(2)$, with γ operator B. Normalized cocycle evaluation identifies the right side with

$$V/(p^n V + (B^{p^n} - 1)V). \tag{4.18}$$

Corestriction for the procyclic index-p subgroup sends its generator value to the same value in the larger group's coinvariants. Thus the transitions are quotient maps, without an extra factor of p. Continuity implies $B^{p^n} - 1 \to 0$; the denominators in (4.18) are cofinal with the p-adic neighbourhoods. Their inverse limit is V.

Restriction to the primitive lattice in W gives, after inverting p, a nonzero quotient

$$V_L \longrightarrow W^*(2), \qquad \gamma|_{W^*(2)} = u^2/\alpha, \tag{4.19}$$

of character $\chi^2 e^{-1}$, or exponent $2 - e$ in cyclotomic character notation. The restriction maps on the integral Hom modules are surjective, and the corresponding finite coinvariant quotients form a separated inverse system. By (4.16) and the finite-level cup-surjectivity hypothesis, the image of $p^b V$ in every one of these quotients is zero. Its image in $W^*(2)$ must therefore be zero. This contradicts the nonzero torsionfree quotient. No compatible choice of finite-level cup expressions is needed, since b was fixed before their selection. The contradiction proves (4.3) for every root, including repeated ones. □

5 Separation in the completed Magnus algebra

The following lemma upgrades the nonzero quadratic restrictions to injectivity on the entire free pro-p group. Its coefficient ring is $\mathbb{Z}_p[[T]][1/p]$: each series has one common finite denominator. This bound permits evaluation at the cyclotomic weights and is preserved by all coordinate changes in a fixed assigned degree.

Lemma 5.1 (Separation of Magnus coefficients)**.** *Let p be odd and let H be a second-countable free pro-p group with commuting continuous actions of $\Gamma = \langle\gamma\rangle \simeq \mathbb{Z}_p$ and $\Delta \simeq \mathbb{F}_p^\times$. Let $c \in \Delta$ have order two, and put*

$$\Lambda = \mathbb{Z}_p[[\Gamma]], \qquad R = \Lambda[1/p], \qquad M = H^{\mathrm{ab}} = U \oplus T, \tag{5.1}$$

where $c = -1$ on U and $c = 1$ on T. Assume that M is finitely generated over Λ, that $U[1/p]$ is free of rank one over R in every odd Δ-character, and that T is finite free over $\mathbb{Z}_p$, with every nonzero $T_e[1/p]$ cyclic over R. Assume also that abelian eigenclasses have exact Δ-eigenlifts, including inside arbitrarily small Δ-stable neighbourhoods.

Let $\rho : H \to \mathcal{U}(\mathbb{Q}_p)$ be continuous and $\Gamma \times \Delta$-equivariant, where $\mathcal{U}$ is the weight-completed free prounipotent group on letters s_m in all odd weights $m \geq 3$. Suppose its image is Zariski dense in every finite weight quotient and, after a Levi normalization,

$$\gamma s_m = u^m s_m, \qquad \delta s_m = \omega(\delta)^m s_m, \tag{5.2}$$

where u topologically generates $1 + p\mathbb{Z}_p$.

For each nonzero T_e, choose an integral multiple v_e of a rational cyclic generator, an exact eigenlift $y_e \in H$, and its conjugates $y_{e,j} = \gamma^j y_e \gamma^{-j}$. Let $q_e(z)$ be the characteristic polynomial of γ on T_e. In a rational R-basis of $U[1/p]$, let $C_{e;a,b}(T_1, T_2)$ be the odd–odd quadratic coefficients of the companion error formed from these conjugates. Suppose that for every root α of every q_e, there is a matching ordered odd pair (a, b) for which

$$C_{e;a,b}\left(T, \frac{\alpha}{1+T} - 1\right) \neq 0. \tag{5.3}$$

Then ρ is injective. All coefficient series here have a common finite denominator in each fixed assigned degree; no bound uniform over all degrees is required.

Proof. A compact free basis. A compact torsionfree $\mathbb{Z}_p$-module is a product of copies of $\mathbb{Z}_p$: its Pontryagin dual is a divisible p-primary group, hence a direct sum of copies of $\mathbb{Q}_p/\mathbb{Z}_p$. The abelianization of free H is torsionfree and metrizable. Using the integral character idempotents, choose pointed convergent $\mathbb{Z}_p$-bases in the U_a, and finite bases in the T_e. The open quotient map $H \to M$ permits lifts of the convergent basis vectors tending to 1. Apply the exact-eigenlift construction inside a nested sequence of Δ-stable open neighbourhoods; it preserves both the abelian classes and their convergence.

Let F be the free pro-p group on this pointed sequence and the finite even set. Its abelianization is the product module on those basis vectors, so the resulting map $F \to H$ is an isomorphism on abelianizations. Its compact image is Frattini-surjective and hence equals H. Indeed a proper closed subgroup of any pro-p group is contained in a proper open subgroup and then in an index-p subgroup, so cannot be Frattini-surjective. Since H is free, the surjection has a continuous section. The section is inverse on abelianizations; its closed image is Frattini-surjective in F and is all of F. Thus $F \simeq H$. This argument does not use an infinite-rank Hopficity assertion.

Give the odd Magnus variables X_i assigned degree 1, and the finite even variables Y_l assigned degree 2. This Magnus expansion is injective. To see this directly, kill a tail of the convergent free sequence. Every finite quotient kills such a tail, so H is the inverse limit of these finite-rank free groups. An ordinary finite-rank Magnus expansion detects every nonidentity element in some finite assigned degree. At each fixed degree the coefficient module is a finite sum of completed tensor products of U and T, using these assigned degrees.

Odd rational coordinates. Choose a character-preserving isomorphism

$$U[1/p] \simeq \bigoplus_{a \text{ odd}} Re_a. \tag{5.4}$$

Finite generation over Λ clears the denominators of this isomorphism and its inverse. Thus there are continuous integral maps between U and $\Lambda^{(p-1)/2}$ whose two compositions are multiplication by the same power of p. Their completed tensor powers have compositions equal to the corresponding powers of that scalar. The tensor modules are torsionfree: in the product bases they are products of copies of $\mathbb{Z}_p$. Hence the maps are injective and become inverse isomorphisms after inverting p. Every fixed degree therefore has coordinates in

$$\mathbb{Z}_p[[\Gamma^s]][1/p] = \mathbb{Z}_p[[T_1, \dots, T_s]][1/p], \tag{5.5}$$

for its singleton positions and their character types. These are the Amice transforms of bounded measures on Γ^s. The denominator bound may depend on the degree, which causes no problem at a first nonzero degree.

The target linear coefficient of weight m is a continuous additive map from M to $\mathbb{Q}_p$. Parity kills T, and character equivariance kills every U_a except $a \equiv m \pmod{p-1}$. On the remaining rank-one R-module, Γ-equivariance makes it a scalar multiple of evaluation at $T = u^m - 1$: check this on polynomials in γ and then pass to bounded series by continuity. The scalar is nonzero by Zariski density, since the weight-m abelian coordinate of the target cannot vanish on a dense image. Rescale s_m by this scalar. Such weightwise rescaling is an automorphism of the completed free Lie algebra, because each finite weight quotient has finitely many generators. The singleton kernel is now exactly evaluation at $u^m - 1$ in its matching type.

Even companion coordinates. Put $\lambda_e = \operatorname{rank}_{\mathbb{Z}_p} T_e$. The classes

$$v_e, \gamma v_e, \dots, \gamma^{\lambda_e - 1} v_e \tag{5.6}$$

are a rational basis, though they need not be an integral basis. The polynomial q_e is monic integral, has unit constant term, and reduces to $(z-1)^{\lambda_e}$ modulo p, since the image of Γ in $\mathrm{GL}(T_e/p)$ is a finite p-group. It is also the minimal polynomial, by rational cyclicity.

The group conjugates $y_{e,j}$ have assigned degree at least 2 and target generator length at least 2. Their assigned-degree-two parts have the form

$$Z_{e,j} = \sum_l b_{j,l} Y_{e,l} + A_{e,j}(X), \tag{5.7}$$

where b is a finite invertible rational matrix and $A_{e,j}$ is a completed quadratic odd tensor. Before the odd coordinate change these coefficients are integral; afterwards they retain bounded denominators. There are no other terms of assigned degree two. The quadratic tensor is alternating, by the commutator description or primitiveness of the first Magnus coefficient.

Replace the finite variables Y by Z. This is a homogeneous triangular automorphism of the completed coefficient algebra: it fixes X and its inverse is $Y = b^{-1}(Z - A(X))$. In each fixed degree only finitely many even variables occur, so both directions preserve a common finite denominator bound. In particular a first nonzero degree remains nonzero. This is a change in the rational tensor algebra, not a claim that the companion classes form an integral group basis.

By definition of $Z_{e,j}$, its leading target is the length-two part of the group element $y_{e,j}$. For an ordered target pair (m, n), put $z = u^{m+n}$. Its coefficient satisfies

$$B_{e,j;m,n} = z^j B_{e,0;m,n}. \tag{5.8}$$

Write $q_e(z) = z^{\lambda_e} - \sum_j c_{e,j} z^j$ and form

$$E_e = (\gamma^{\lambda_e} y_e \gamma^{-\lambda_e}) \left(\prod_j y_{e,j}^{c_{e,j}} \right)^{-1}. \tag{5.9}$$

Its abelian class is zero, so E_e is in the closed derived subgroup. Its assigned-degree-two part is the odd alternating tensor C_e. There are no target length-one terms in any even factor, so comparison of length two gives exactly

$$q_e(z) B_{e,0;m,n} = C_{e;a,b}(u^m - 1, u^n - 1), \qquad a \equiv m,\ b \equiv n \pmod{p-1}. \tag{5.10}$$

This is the companion class of the extension in Lemma 4.1. Exact eigenlifts make its assigned degree-two character e; hence wrong-character pairs have zero coefficient. One can also obtain this zero from (5.10) on the full residue grid and the successive analytic identity theorem.

Partial fractions and continuity. Pass to a finite splitting field L, with integers $\mathcal{O}$. All roots α satisfy $\alpha - 1 \in \mathfrak{m}_{\mathcal{O}}$. The finite-dimensional rational-function space with basis $z^j/q_e(z)$ has alternative basis

$$(z - \alpha)^{-k}, \qquad 1 \le k \le \mathrm{mult}_e(\alpha). \tag{5.11}$$

The corresponding constant invertible change in the finite Z variables preserves assigned degree and bounded denominators in every fixed degree. Its even letter (e, α, k) has kernel

$$\frac{C_{e;a,b}(T_1, T_2)}{((1+T_1)(1+T_2) - \alpha)^k}. \tag{5.12}$$

The numerator is common to all letters from the same companion component, even when roots repeat.

There are finitely many positive integers w such that u^w is a root of some q_e. Restrict all test weights to a sufficiently large ordinary tail, excluding every vanishing pair denominator. In each fixed odd residue class this still includes sequences $m_0 + (p-1)p^j$ with an interior p-adic accumulation point, for a sufficiently large fixed representative m_0.

Substitution is legitimate at every finite arithmetic-weight cutoff. In the compact free basis, truncate its convergent sequence and apply finite-rank Magnus substitution. These truncations converge to the identity on H, since every finite group quotient kills a tail. The image of H in the finite target quotient is compact, so its coefficient functions are bounded and continuous. Passing to the limit therefore gives the completed tensor substitution. The bounded rational coordinate changes preserve this statement in each fixed degree. In (5.5) it is equivalently integration against bounded measures and the finite Fubini rule. We do not invoke a free pro-p universal property for a noncompact rational group.

Separation of a first nonzero degree. Suppose $g \neq 1$ and $\rho(g) = 1$, and let d be its first nonzero assigned degree after these invertible changes. A larger source degree cannot contribute to target length d. Its coefficient is a finite sum over ordered tilings of d positions by singleton odd types and pairs labelled (e, α, k):

$$\sum_{\mathcal{P}} A_{\mathcal{P}}(T_i : \ i \text{ singleton}) \prod_{(j,e,\alpha,k)\in\mathcal{P}} \frac{C_{e;a_j,a_{j+1}}(T_j, T_{j+1})}{D_{j,\alpha}^{k}} = 0, \qquad D_{j,\alpha} = (1+T_j)(1+T_{j+1}) - \alpha. \tag{5.13}$$

Every $A_{\mathcal{P}}$ has a common bounded denominator. Clear the finitely many denominators. Vanishing on the Cartesian grid of large odd test weights and the successive one-variable identity theorem make (5.13) an identity in the fraction field of $\mathcal{O}[[T_1, \dots, T_d]][1/p]$.

Select a nonzero pattern with the largest number of pairs. Fix its pair positions J and its roots and even characters, and among nonzero patterns with those data choose a componentwise maximal pole-order vector (k_j). At each selected pair choose the ordered odd types in (5.3), and at each singleton its source type. These choices are independent because the pairs are disjoint.

Set $S_j = D_{j,\alpha_j}$ for $j \in J$. Retain as base variables the singleton variables and the left variable in each selected pair. The substitutions

$$T_{j+1} = \frac{\alpha_j + S_j}{1 + T_j} - 1 \tag{5.14}$$

are automorphisms of the complete integral power-series ring. Let K_0 be the fraction field of the bounded-denominator base ring. The identity embeds in $K_0[[S_j : j \in J]][S_j^{-1} : j \in J]$, with finite lower bounds on exponents. All other denominators are units in $K_0[[S_j]]$: a different root at the same position has nonzero constant root difference; a different pair position joins two distinct selected blocks, whose surviving variables are independent, so its product is not identically a prescribed root. Wrong even characters have already vanished.

Take the coefficient of $\prod_{j\in J} S_j^{-k_j}$. A pattern missing a selected position or using a different root there has no negative exponent in that variable. A pattern containing all selected pairs and an extra pair has zero coefficient by the first maximality choice. Among remaining patterns, a contribution requires all pole orders to dominate k_j; the componentwise maximal choice excludes strict domination and an incomparable vector fails in at least one variable. Singleton types must match. Thus exactly one coefficient remains:

$$A_{\mathcal{P}}(T_i : \ i \text{ singleton}) \prod_{j\in J} C_{e_j;a_j,b_j}\left(T_j, \frac{\alpha_j}{1+T_j} - 1\right). \tag{5.15}$$

The first factor is nonzero and its coefficient ring injects into K_0; every other factor is nonzero by (5.3). Their product is nonzero in a field, a contradiction. If J is empty, the same argument is the ordinary singleton moment identity. This proves injectivity of ρ. □

6 The arithmetic consequence of Greenberg's hypothesis

We now verify all hypotheses of the two preceding lemmas for the cyclotomic Galois group. The following comparison puts the finite-level symbol theorem in the group-cohomological form required there.

Lemma 6.1 (Low-degree étale comparison)**.** *Let S be a connected normal affine scheme, let $G = \pi_1^{\text{ét}}(S)$, and let P be its maximal pro-p quotient. For a finite p-primary local coefficient module A whose action factors through P, the natural maps give*

$$H^1(P, A) \simeq H^1_{\text{ét}}(S, A), \qquad H^2(P, A) \hookrightarrow H^2_{\text{ét}}(S, A). \tag{6.1}$$

They are compatible with cup products and with finite external automorphisms. Consequently generation of a character summand of the target H^2 by cups of H^1 classes gives the same generation in group cohomology and makes the displayed injection an isomorphism on that summand.

Proof. Put $N = \ker(G \to P)$. An element of $H^1(N, A)^P$ is a continuous P-equivariant homomorphism $N \to A$, since N acts trivially on A. If its image were nonzero, its kernel would be G-normal and the quotient of G by that kernel would be an extension of P by a nonzero finite p-group. This is a pro-p quotient: every finite quotient has p-power order. It would be strictly larger than the maximal pro-p quotient, a contradiction. Thus $H^1(N, A)^P = 0$. The five-term Hochschild–Serre sequence gives

$$H^1(P, A) \simeq H^1(G, A), \qquad H^2(P, A) \hookrightarrow H^2(G, A). \tag{6.2}$$

No finite-generation hypothesis on N was used.

The full universal finite étale tower over S has zero H^1 with finite locally constant coefficients: after trivializing the coefficients, an H^1 torsor is finite étale and becomes trivial at a later stage of the same tower. Finite étale objects and torsors descend under these affine limits. The Cartan–Leray spectral sequence for the tower therefore gives

$$H^1(G, A) \simeq H^1_{\text{ét}}(S, A), \qquad H^2(G, A) \hookrightarrow H^2_{\text{ét}}(S, A). \tag{6.3}$$

This is only its low-degree consequence, and asserts no vanishing of the higher rows. The sequence, the profinite-tower passage and the simply connected H^1 vanishing are given explicitly in [11, Theorem 14.9, Remark 14.10, Example 14.11 and Proposition 14.13, pp. 96–98]. All comparison maps are natural and respect cups. Lift each cup generator using the H^1 isomorphism and add its group cups; this proves surjectivity onto the asserted summand. Injectivity then identifies every group class in that summand with the lifted sum. □

Proof of the odd-prime assertion of Theorem 1.1. At $p = 3$, Sharifi's theorem [13, Theorem 1, p. 2] and Brown's theorem apply, since 3 is regular. Hence assume $p \geq 5$. Put

$$P = \mathrm{Gal}(\Omega_p/F_1), \quad H = \mathrm{Gal}(\Omega_p/F_\infty), \quad \Gamma = \mathrm{Gal}(F_\infty/F_1), \quad M = H^{\mathrm{ab}} = U \oplus T. \tag{6.4}$$

Choose the finite Δ lift by the coprime complement theorem. The fibre over a generator of Γ is a Δ-stable H-torsor because the cyclotomic quotient is abelian. The coprime identity $H^1(\Delta, H) = 1$, obtained from the finite complement theorem and compactness, gives a Δ-fixed lift γ. Its procyclic closure maps isomorphically to Γ and supplies the commuting section used above. Ferrero–Washington gives $\mu = 0$ for this abelian cyclotomic tower [3]. Iwasawa's Theorem 2 then states that H is free pro-p [9, p. 273]. The maximal extension in that theorem is the extension Ω_p used here: a finite p-extension over F_∞ descends to a finite cyclotomic layer, and the normal closure of its descended p-extension over F_1 is

again a p-extension unramified outside p. The finite-level Kummer sequence makes $H^1(P, \mathbb{F}_p)$ finite dimensional, so P is finitely generated and H is second-countable. Adjust a finite generating set of P by powers of the chosen Γ section to obtain elements of H. Together with γ they generate P; their closed normal closure is H, since the remaining quotient is the given procyclic quotient. Their abelian classes therefore generate M over $\Lambda = \mathbb{Z}_p[[\Gamma]]$. Section 3 gives the continuous dense rational representation and its Levi normalization as required in Lemma 5.1. The exact eigenlift construction is [13, Lemma 4, p. 3]; performing it inside stable neighbourhoods preserves convergence. We verify the module and cup hypotheses.

Rational odd module. The ring $R = \Lambda[1/p]$ is a PID. Indeed Λ is a two-dimensional regular local UFD, and its only height-two prime contains p. Thus R is a one-dimensional noetherian UFD and hence a PID. It remains the ring of bounded-denominator series, not $\mathbb{Q}_p[[T]]$.

For an odd character $a \neq \omega, \omega^{-1}$, apply the full duality calculation in Wake–Wang-Erickson's Proposition 2.2.6 with $\theta = \omega a^{-1}$. It gives

$$\mathrm{Ext}^1_\Lambda(M_a^\#(1), \Lambda) = X_\theta, \qquad \mathrm{Ext}^2_\Lambda(M_a^\#(1), \Lambda) = 0. \tag{6.5}$$

Here M is their p-ramified module $\mathfrak{X}$, whereas X on the right is unramified. Since θ is even, Greenberg makes the right-hand side zero after inverting p. Ext commutes with this localization for finitely generated modules. Over a PID, the Ext group into the ring of a finitely generated torsion summand is nonzero unless that summand is zero. Thus $M_a[1/p]$ is free. Its rank is one by the local/global unit exact sequence in the same proof: local units have rank one in this character, global minus units contribute only roots of unity, and the unramified quotient is torsion. The inversion $\#$ and Tate twist transport the ring by automorphisms, so undoing them preserves freeness [16, Proposition 2.2.6 and proof, pp. 3–4].

The two excluded characters can be calculated directly. Coleman's exact sequence at tame level one is

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow U_{\mathrm{loc}} \longrightarrow \mathbb{Z}_p[[\Delta \times \Gamma]] \longrightarrow \mathbb{Z}_p(1) \longrightarrow 0 \tag{6.6}$$

[15, Theorem 5.5.31, p. 148; Proposition 6.1.1, pp. 151–152]. Global minus units are exactly the root-of-unity term, and Stickelberger gives $X_\omega = X_{\omega^{-1}} = 0$; the latter exceptional statement is explicitly recorded in [16, proof of Lemma 5.2.7, p. 13]. The ω^{-1} component of M is consequently free of rank one. In the ω component, quotienting the local units by their root-of-unity kernel identifies M_ω with

$$\ker(\Lambda \longrightarrow \mathbb{Z}_p(1)) = (\gamma - u)\Lambda, \tag{6.7}$$

again free of rank one. The two characters are distinct for $p \geq 5$. The valuation direction at the unique prime above p is even and does not affect this calculation. We have therefore proved the required rational freeness for every odd character.

Rational even module. Kummer duality identifies $T = M^+$ up to finite kernel and cokernel with $(X^-)^\iota(1)$ [15, Proposition 3.4.7 and Corollary 3.4.8, p. 92]. Ferrero–Washington makes it finitely generated over $\mathbb{Z}_p$, and freeness of H excludes $\mathbb{Z}_p$-torsion. Thus T is finite free. Greenberg implies that X^- is pseudocyclic character by character, by the exact local/global unit sequence and Iwasawa adjunction in [17, Corollary 2.1.3 and Conjecture 2.1.5 with the following explanation, p. 8]. Finite kernels and cokernels vanish after inverting p, so every $T_e[1/p]$ is cyclic. This allows repeated roots; it does not assert integral cyclicity without Vandiver.

Integral symbol surjectivity under Greenberg. Fix an even character $\theta \neq 1, \omega^2$ and put $\chi = \omega^{-1}\theta$. Wake–Wang-Erickson's Corollary 8.1.3(2) assumes exactly

$$\begin{gathered} X_\chi(1)[1/p] \text{ cyclic over } (\Lambda/\xi_\chi)[1/p], \\ X_\theta \otimes_\Lambda (\Lambda/\xi_\chi)[1/p] = 0. \end{gathered} \tag{6.8}$$

The localization in the second condition is essential. Both conditions follow from the just stated consequences of Greenberg. The conclusion is an integral isomorphism

$$\varpi : (\mathcal{H}_\theta^- / I_\theta \mathcal{H}_\theta^-)/(p\text{-primary torsion}) \xrightarrow{\sim} X_\chi(1), \tag{6.9}$$

so the original ϖ is surjective [17, Corollary 8.1.3 and complete proof, pp. 48–49]. The source proves this with repeated roots: the derivative identity makes the error nilpotent in each cyclic local factor, rather than requiring the derivative to be invertible. Thus (6.9) does not insert a simple-root hypothesis.

Fukaya–Kato, §7.1.10, deduce from this surjectivity that for every $r \geq 1$ the finite-level θ component is generated by the symbols

$$\{1 - \zeta_{p^r}^a, 1 - \zeta_{p^r}^b\}. \tag{6.10}$$

Their §7.1.9 identifies its reduction modulo p^r with the corresponding class-group quotient, and their §6.1.5 shows that at tame level one the only excluded even characters are $1, \omega^2$ [4, §6.1.5, p. 76; §§7.1.8–7.1.10, p. 86]. Those excluded characters correspond to the unramified components $X_{\omega^{-1}}$ and X_ω, which are zero. Norm projections from X^- onto each finite minus class group are surjective, so the omitted finite targets are zero as well [15, Proposition 3.4.1 and proof, pp. 90–91]. Components with unit characteristic power series are also zero: the source's X^- is p-torsionfree, and a finite such module must vanish. We apply the nonunit running assumption of the modular source only to the nonzero components. Hence every even target is covered.

All finite group levels and coefficient conventions. Let

$$P_n = H \rtimes \Gamma^{p^n}, \qquad S_n = \operatorname{Spec} \mathcal{O}_{F_{n+1}}[1/p]. \tag{6.11}$$

The maximal pro-p quotient of $\pi_1(S_n)$ is exactly P_n. Indeed the normal closure over F_1 of any finite Galois p-extension of F_{n+1} unramified outside p remains a p-extension: its conjugate compositum over F_{n+1} has p-group Galois group, and F_{n+1}/F_1 has p-power degree. Thus it lies in the fixed field Ω_p used throughout.

At F_{n+1}, the finite-level symbol theorem gives generation with coefficients p^{n+1}. Reduction gives generation with coefficients p^n, exactly as in Lemma 4.1. The class-group quotient description in FK §7.1.9 makes this reduction explicit. The Brauer contribution is zero: these fields have no real places, and only one finite prime is omitted, so the global invariant condition forces its lone possible local invariant to vanish.

For a p-unit v, the quotient $v/c(v)$ is a global unit of absolute value one at every embedding and hence is a root of unity. Consequently the negative c part of the p-unit group modulo p^n is cyclic. Its alternating self-cup is zero because 2 is a unit; mixed-parity cups lie in the odd target. Thus the even target is generated by cups of c-even unit classes. This argument does not identify the whole of H^1 with units and does not use Vandiver.

Apply Lemma 6.1. Each Kummer class has a unique lift to $H^1(P_n, \mathbb{Z}/p^n(1))$, and group H^2 injects into étale H^2. Lifting the even symbol generators makes this injection surjective on the even part and gives precisely

$$H^2(P_n, \mathbb{Z}/p^n(2))^+ = \langle f \smile g \mid f, g \in H^1(P_n, \mathbb{Z}/p^n(1))^+ \rangle. \tag{6.12}$$

This treats every $n \geq 1$; no compatibility of expressions as sums of cups is needed. Scalar extension to the integers of a finite splitting field preserves the assertion, since that ring is finite free over $\mathbb{Z}_p$.

Lemma 4.1 now gives the nonzero companion restriction (5.3) for every root of every even component, including repeated roots. Its dual root is u^2/α and its dual character is ω^{2-e}, so

the inversion and both Tate twists match the symbol target. Lemma 5.1 proves injectivity on the entire H.

Finally an element in the kernel of the original pro-p tripod action is cyclotomically trivial, hence lies in H. Functorial rational completion sends it to 1 under ρ, and the proved injectivity makes it trivial. This is exactly $\Omega_p^* = \Omega_p$. □

7 Vandiver and the verified finite range

We prove directly that Vandiver supplies the Iwasawa hypothesis in Theorem 1.1.

Lemma 7.1. *Let L/K be cyclic of odd prime degree p, ramified at precisely one finite prime, which is totally ramified. If $\mathrm{Cl}(K)\{p\} = 0$, then $\mathrm{Cl}(L)\{p\} = 0$.*

Proof. Let E/L be the Hilbert p-class field. Its uniqueness makes E/K Galois, and $G = \mathrm{Gal}(E/K)$ is a finite p-group. The inertia group I above the ramified prime has order p, since E/L is unramified. Let N be its normal closure in G. All other inertia groups at that prime are conjugate, and every other prime is unramified; an odd-degree extension introduces no infinite-place ramification. Thus E^N/K is everywhere unramified. If G/N were nontrivial, it would have a cyclic quotient of order p, contradicting class field theory and the hypothesis on K. Hence $N = G$. The Frattini quotient of G is consequently generated by the image of one generator of I, so G is cyclic. Its subgroup I is then normal, whence $G = N = I$ and $E = L$. □

At every step F_{r+1}^+/F_r^+ the sole ramified finite prime is the prime above p, and it is totally ramified. Lemma 7.1 therefore gives $\mathrm{Cl}(F_r^+)\{p\} = 0$ at all layers when Vandiver holds at F_1. Extension and norm of ideals identify $\mathrm{Cl}(F_r^+)\{p\}$ with $\mathrm{Cl}(F_r)\{p\}^+$: their composites are multiplication by 2 and $1 + c$, and 2 is invertible on a p-group. Taking norm limits gives $X_p^+ = 0$. The odd-prime assertion already proved now establishes the Vandiver part of Theorem 1.1.

Hart–Harvey–Ong verify Vandiver for every odd prime below 2^{31} [6, Section 1, item (2)]. Their computation proves the stated numerical corollary. No assertion about an unverified prime is needed for that finite range.

Remark 7.2 (The groups $K_{4k}(\mathbb{Z})$)**.** Vandiver's conjecture at p can be read in the algebraic K-theory of $\mathbb{Z}$. Let ω be the Teichmüller character of $\mathrm{Gal}(F_1/\mathbb{Q})$. For an odd prime p and an integer $k \geq 1$,

$$K_{4k}(\mathbb{Z})/p \;\cong\; H^2_{\text{ét}}(\mathbb{Z}[1/p], \mu_p^{\otimes(2k+1)}) \;\cong\; (\mathrm{Cl}(F_1)/p)(\omega^{-2k}), \tag{7.1}$$

where the last group is the part of $\mathrm{Cl}(F_1)/p$ on which $\mathrm{Gal}(F_1/\mathbb{Q})$ acts through ω^{-2k}. The first isomorphism is [18, Chapter VI, Corollary 8.3], which rests on the norm residue isomorphism theorem. The second is Kummer theory over $\mathbb{Z}[\mu_p, 1/p]$, where the prime above p is principal and the Brauer group contributes nothing, as in Section 6. Since $K_{4k}(\mathbb{Z})$ is finite, it has no p-torsion if and only if the ω^{-2k}-part of $\mathrm{Cl}(F_1)\{p\}$ vanishes. The characters ω^{-2k} with $1 \leq k \leq (p-3)/2$ are the nontrivial even characters, and the part of $\mathrm{Cl}(F_1)\{p\}$ for the trivial character is zero, because the class group of $\mathbb{Q}$ is trivial. Vandiver's conjecture at p is the vanishing of the even parts, by the identification made before this remark. It is therefore equivalent to the absence of p-torsion in $K_{4k}(\mathbb{Z})$ for $1 \leq k \leq (p-3)/2$. This is Kurihara's theorem [10], in the form of [18, Chapter VI, Theorem 10.9].

Mok and Zheng state that $K_{4m}(\mathbb{Z}) = 0$ for every integer $1 \leq m \leq 30$ [12, Theorem 1]. The cases $m = 1$ and $m = 2$ are theorems of Rognes and of Dutour Sikirić, Elbaz-Vincent, Kupers and Martinet. For $3 \leq m \leq 30$ their argument uses the computation of Hart, Harvey and

Ong at the odd primes below 2^{31} and, at the larger primes, a bound for a Selmer group taken from the Lean files that accompany Alpöge's announcement of November 2026, together with exact computations of Hecke determinants. Their text was posted on 24 November 2026 and has not been refereed. We have read its statement, its introduction and its second section, and we have not checked its proof. If their theorem holds, then by (7.1) the ω^{-2m}-part of $\mathrm{Cl}(F_1)\{p\}$ vanishes for $1 \le m \le 30$ at every odd prime p. For $p \le 61$ these are all the parts that Vandiver's conjecture concerns, and the conjecture was already known there; for larger p they are 30 of the $(p-3)/2$ such parts. Theorem 1.1 needs the whole of X_p^+ to be finite, so their theorem adds no prime to it, and nothing in this note depends on it.

8 What remains open

The theorem determines the kernel field at every prime for which its arithmetic hypothesis has been established. For an odd prime with X_p^+ finite, the proof passes through the following specific maps: the modular symbol map to the cyclotomic class module; its projections to finite-level cup products; the edge map for $1 \to H \to H \rtimes \Gamma^{p^n} \to \Gamma^{p^n} \to 1$; and the coefficients of the induced rational outer representation. The two Tate twists in the edge map send an eigenvalue α to u^2/α. This identifies the arithmetic direction tested by each pole, including generalized eigenspaces for repeated roots.

To establish the same conclusion for every prime by this argument one must establish the required arithmetic module structure and cup nonvanishing beyond the finiteness hypothesis. The proof here does not provide that step. Vanishing of a particular quadratic coefficient would also require further analysis: a group element can have a nonzero image at higher generator length. Thus no converse to the criterion is asserted.

There is a related integral question concerning generation of the weight-graded Lie algebra by specified Soulé elements. The map from a group to its weight-graded Lie algebra, followed by tensoring with $\mathbb{Q}_p$, can discard integral indices. Our separation argument uses nonzero rational leading coefficients; it never proves that those coefficients are p-adic units. Accordingly the kernel-field theorem makes no integral generation assertion. Sharifi treats the maps from free integral generators to the filtered group and graded Lie algebra explicitly in [13, Sections 1 and 4].

Remark 8.1 (Elliptic curves with complex multiplication)**.** Ishii proves an analogue of Sharifi's theorem for a once-punctured elliptic curve [8, Theorem A, p. 2, which is Theorem 2.14, p. 11]. Let K be an imaginary quadratic field of class number one, E an elliptic curve over K with complex multiplication by the ring of integers of K, with origin O, and $X = E \setminus \{O\}$. For $n \ge 0$ let $K(p^n)$ be the ray class field of K of conductor p^n. Let $p \ge 5$ be a prime that splits in K, and assume that

(1) p does not divide the class number of $K(p)$;

(2) exactly two primes of $K(p^2)$ lie above p;

(3) his analogue of the Deligne–Ihara conjecture holds [8, Conjecture 2.3, p. 6]: a graded Lie algebra over $\mathbb{Q}_p$ attached to the pro-p outer Galois action on the fundamental group of X is freely generated by one element in each degree of an explicit set of pairs of positive integers.

Then the fixed field of the kernel of the pro-p outer Galois representation of X is the compositum of $K(E[p])$ and the maximal pro-p extension of $K(p)$ unramified outside p. Ishii notes that assumption (1) implies that p is regular [8, Remark 1.1.2 (3), p. 3]. His theorem is thus the analogue of the regular case, and its assumption (3) is a conjecture, whereas for

the line minus three points the corresponding statement is Brown's theorem. We have read the introduction of the preprint and the statements of its second section, and we have not checked its proofs. The present note removes the regularity hypothesis for the line minus three points by means of theorems on Sharifi's conjecture for the cyclotomic tower. Whether assumptions (1) and (2) can be weakened in a similar way for $X = E \setminus \{O\}$ is a question that this note does not examine.

Provenance and checks

The mathematics, and the text of Sections 3 to 8 apart from Remarks 7.2 and 8.1, are the work of GPT-6 Astra (ChatGPT Pro mode), in research runs of November 2026; the same model reread its proofs and its applications of the cited theorems. Sections 1 and 2 and this note were written by Claude (Claude Fable 5.2 at effort max), as editor, who also removed the treatment of the prime 2 from the text and changed it in no other mathematical respect.

Claude Opus 5.5 at effort high checked every step of Lemma 7.1 and of the deduction of $X_p^+ = 0$ from it (23 November). On 21 and 22 November, before this note was written, it had checked the separation lemma (Lemma 5.1) and the deduction of the theorem at primes satisfying Vandiver's conjecture, in the text that the research run had written by then. On 23 November it then checked Sections 4 to 6 step by step, in the text of version 1 of this note, with [16, Proposition 2.2.6], [17, Corollary 2.1.3, Conjecture 2.1.5 and Corollary 8.1.3(2)] and [4, §6.1.5 and §§7.1.9–7.1.10] opened at those places, and found no mathematical error; the statements cited from [11], [15] and [9] were not opened again. The editor, Claude Fable 5.2 at effort max, then refereed Sections 3 to 6 against the cited theorems of Hain–Matsumoto, Wake–Wang-Erickson and Fukaya–Kato and found no error. Claude Opus 5.5 at effort max read the whole note and checked Section 7 in full. No human has checked the proofs or this text.

The sources were opened by the run, which recorded for each the pages used; the locators in the text are its own. For version 1 of this note the editor read the abstracts of [13] and [8]; the literature check of 23 November opened [13], [14], [8], Sharifi's 2011 paper on his conjectures, [4] and both papers of Wake and Wang-Erickson at the source. What Section 1 says about [1] follows [8, p. 2], Ihara's inclusion follows [13, p. 1], and the sentences on the programme are the editor's summary.

Version 2 (24 November 2026). No statement and no proof of version 1 (23 November 2026) is changed, and the checks described above are checks of that text. In Sections 3 to 7 the changes are two locators in Section 6 and the new Remark 7.2. All the changes are these.

(i) Sharifi's paper [13] is cited throughout in the numbering of arXiv:math/0104116v2. Version 1 cited his theorem by its number in the author's version, Theorem 1.1, and his lemma by its number in the arXiv version.

(ii) The sentence of [14] cited in Section 1 is on p. 221, and the article occupies pp. 220–227. Version 1 gave p. 222 and pp. 221–228. The quoted words were compared with the source and are exact.

(iii) The account of the checks no longer speaks of earlier versions of the argument; it says which text each check read.

(iv) Remarks 7.2 and 8.1 are new, and the locators for [8] are more precise.

Points (i) to (iii) were raised in the review of 23 November and again in a reading of 24 November, both by Claude Opus 5.5 at effort high. The connection of Vandiver's conjecture

with the groups $K_{4k}(\mathbb{Z})$ and with [12] was pointed out by Claude Opus 5.5 at effort max. The editor, Claude Fable 5.2 at effort max, made the changes and wrote the two remarks with the sources open: [13], in the arXiv version and in the author's version, at the theorem and the lemma; [14] at the page; [8] at the statements cited; [12] at its Theorem 1, its introduction and its second section; and [18] at Theorem 8.2, Corollary 8.3 and Theorem 10.9 of Chapter VI. The page numbers in (ii) are the editor's correction. [10] was not opened. The two remarks report results of others. Claude Opus 5.5 at effort max read them before deposit and checked the deduction in Remark 7.2 from the statements cited, not the cited proofs. No human has checked version 2.

The records of the checks are at the permanent page of this work, WB-0006:

`https://github.com/KokunoYumeto/mathematics-workbenches/blob/main/works/WB-0006.md`.

This text is dedicated to the public domain (CC0 1.0).

References

[1] G. Anderson and Y. Ihara, *Pro-l branched coverings of* $\mathbb{P}^1$ *and higher circular l-units*, Ann. of Math. (2) **128** (1988), 271–293. `https://doi.org/10.2307/1971443`. The kernel question is on p. 272, question (a); its statement is also reproduced in [8, p. 2].

[2] F. Brown, *Mixed Tate motives over* $\mathbb{Z}$, Ann. of Math. **175** (2012), 949–976. `https://annals.math.princeton.edu/wp-content/uploads/annals-v175-n2-p10-p.pdf`.

[3] B. Ferrero and L. C. Washington, *The Iwasawa invariant* μ_p *vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), 377–395. `https://doi.org/10.2307/1971116`.

[4] T. Fukaya and K. Kato, *On conjectures of Sharifi*, author preprint, 15 August 2012, 121 pages. `https://www.math.ucla.edu/~sharifi/sharificonj.pdf`. Locators in this author version: §§6.1.4–6.1.8, pp. 76–77; §7.1.3, pp. 84–85; Conjecture 7.1.8 and §§7.1.9–7.1.10, p. 86; Theorem 7.2.8 and §§7.2.10–7.2.12, p. 89; Lemma 10.2.2 and §10.2.3, p. 107.

[5] R. Hain and M. Matsumoto, *Weighted completion of Galois groups and Galois actions on the fundamental group of* $\mathbb{P}^1 - \{0, 1, \infty\}$, arXiv:math/0006158v2, 11 August 2001. `https://arxiv.org/pdf/math/0006158`.

[6] W. B. Hart, D. Harvey and W. Ong, Irregular primes to two billion, *Math. Comp.* 86 (2017), 3031–3049. `https://doi.org/10.1090/mcom/3211`. Author preprint: `https://arxiv.org/abs/1605.02398`. Section 1, item (2), verifies Vandiver for every odd prime $\ell < 2^{31}$.

[7] Y. Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) **123** (1986), 43–106. `https://doi.org/10.2307/1971352`.

[8] S. Ishii, *On the kernels of the pro-p outer Galois representations associated to once-punctured CM elliptic curves*, arXiv:2312.04196v3, 6 January 2026, 30 pages. `https://arxiv.org/abs/2312.04196v3`. Locators in that version: Theorem 1.1, Remark 1.1.1 and Theorem A, p. 2; Remark 1.1.2, p. 3; Conjecture 2.3, p. 6; Theorem 2.14, p. 11.

[9] K. Iwasawa, *Riemann–Hurwitz formula and p-adic Galois representations for number fields*, Tohoku Math. J. **33** (1981), 263–288. `https://www.jstage.jst.go.jp/article/tmj1949/33/2/33_2_263/_pdf/-char/en`.

[10] M. Kurihara, *Some remarks on conjectures about cyclotomic fields and K-groups of* $\mathbb{Z}$, Compositio Math. **81** (1992), 223–236. Cited through [18, Chapter VI, Theorem 10.9].

[11] J. S. Milne, *Lectures on* Étale *Cohomology*, version 2.21, 22 March 2013, 202 pages. `https://www.jmilne.org/math/CourseNotes/LEC.pdf`. Theorem 14.9, Remark 14.10, Example 14.11 and Proposition 14.13, printed pp. 96–98.

[12] C. P. Mok and H. Zheng, *Vanishing of* $K_{4m}(\mathbb{Z})$ *through degree* 120, Hexagon 2611.00998, version 1, dated 23 November 2026 and posted 24 November 2026, 12 pages. `https://hexagonmath.org/2611.00998`. Theorem 1, p. 2; Section 2, pp. 2–3.

[13] R. T. Sharifi, *Relationships between conjectures on the structure of pro-p Galois groups unramified outside p*, Proc. Sympos. Pure Math. **70** (2002), 275–284. arXiv:math/0104116v2, 3 October 2001, 12 pages: `https://arxiv.org/abs/math/0104116v2`. Locators in this note are to that version: Ihara's inclusion, p. 1; Theorem 1, p. 2; Lemma 4, p. 3. In the author's 13-page version, `https://www.math.ucla.edu/~sharifi/publ/galstr.pdf`, the theorem is Theorem 1.1, p. 2, and the lemma is Lemma 2.1, p. 4.

[14] R. T. Sharifi, *Soulé characters in the work of Ihara*, RIMS Kôkyûroku **2120** (2019), 220–227. `https://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/pdf/2120-11.pdf`.

[15] R. T. Sharifi, *Iwasawa Theory*, author lecture notes, 184 pp., retrieved 23 November 2026. `https://www.math.ucla.edu/~sharifi/notes/iwasawa.pdf`. Locators: Propositions 3.4.1 and 3.4.7, Corollary 3.4.8, pp. 90–92; Theorem 5.5.31, p. 148; Proposition 6.1.1, pp. 151–152.

[16] P. Wake and C. Wang-Erickson, *Ordinary pseudorepresentations and modular forms*, Proc. Amer. Math. Soc. Ser. B **4** (2017), 53–71. `https://doi.org/10.1090/bproc/29`. Final author preprint arXiv:1510.01661v4, 30 January 2017: `https://arxiv.org/pdf/1510.01661v4`. Locators in that version: §2.1, pp. 2–3; Proposition 2.2.6, p. 4; Theorem 4.2.8, pp. 10–11; Corollaries 5.1.1–5.1.2, p. 11; Lemma 5.2.7, p. 13.

[17] P. Wake and C. Wang-Erickson, *Pseudo-modularity and Iwasawa theory*, Amer. J. Math. **140** (2018), no. 4, 977–1040. `https://doi.org/10.1353/ajm.2018.0022`. Author version: arXiv:1505.05128v3, 7 September 2017, 54 pages: `https://arxiv.org/pdf/1505.05128v3`. Locators in that version: Corollary 2.1.3 and Conjecture 2.1.5, p. 8; Corollaries 8.1.2–8.1.3, pp. 48–49; Theorem 8.2.3, pp. 50–51.

[18] C. A. Weibel, *The K-book: an introduction to algebraic K-theory*, Graduate Studies in Mathematics **145**, American Mathematical Society, 2013. Chapter VI, Theorem 8.2, Corollary 8.3 and Theorem 10.9, read in the author's online version of that chapter, pp. 47–48 and 65: `https://sites.math.rutgers.edu/~weibel/Kbook/Kbook.VI.pdf`.