A cup product in the Galois cohomology of number fields

William G. McCallum and Romyar T. Sharifi

1 Introduction

This paper is devoted to the consideration of a certain cup product in the Galois cohomology of an algebraic number field with restricted ramification. Let n be a positive integer, let K be a number field containing the group μ_n of nth roots of unity, and let S be a finite set of primes including those above n and all real archimedean places. Let $G_{K,S}$ denote the Galois group of the maximal extension of K unramified outside S (inside a fixed algebraic closure of K). We consider the cup product

$$H^1(G_{K,S}, \mu_n) \otimes H^1(G_{K,S}, \mu_n) \to H^2(G_{K,S}, \mu_n^{\otimes 2}). \tag{1}$$

When the localization map

$$H^2(G_{K,S}, \mu_n^{\otimes 2}) \to \bigoplus_{v \in S} H^2(G_v, \mu_n^{\otimes 2}) \tag{2}$$

for the local absolute Galois groups G_v is injective, the cup product is a direct sum over primes in S of the corresponding local cup products, each of which may be expressed as the nth norm residue symbol on the completion of K at that prime. However, we are interested in a situation that is inherently non-local: that is, in which the cup product of two elements lies in the kernel of the localization map. This kernel is isomorphic to $C_{K,S}/nC_{K,S}$, where $C_{K,S}$ denotes the S-class group of K. In Section 2, we develop a formula for the cup product in this case in terms of ideals in a Kummer extension of K (Theorem 2.4).

Using Kummer theory, we can identify $H^1(G_{K,S}, \mu_n)$ with a subgroup of $K^\times/K^{\times n}$ containing the image of the units of the S-integers $\mathcal{O}_{K,S}$, and hence we have an induced pairing

$$\mathcal{O}_{K,S}^\times \times \mathcal{O}_{K,S}^\times \to H^2(G_{K,S}, \mu_n^{\otimes 2}).$$

Like the norm residue symbol, this pairing has the property that a and b pair trivially if $a + b = 1$. Thus, we obtain a relationship between the cup product and the K-theory of $\mathcal{O}_{K,S}$, which is described in Section 3 and discussed further in Section 5 (see Conjecture 5.3).

When $n = p$, a prime number, the cup product yields information on the form of relations in the maximal pro-p quotient $\mathcal{G} = G_{K,S}^{(p)}$ of $G_{K,S}$. It is well-known that $\mathcal{G}$ has a presentation

$$0 \to \mathcal{R} \to \mathcal{F} \to \mathcal{G} \to 0, \tag{3}$$

where $\mathcal{F}$ is a free pro-p group on a finite set X of generators and $\mathcal{R}$ is the smallest closed normal subgroup containing a finite set R of relations in $\mathcal{F}$. Choosing X and R of minimal order, we have

$$|X| = \dim_{\mathbb{Z}/p\mathbb{Z}} H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \quad \text{and} \quad |R| = \dim_{\mathbb{Z}/p\mathbb{Z}} H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}).$$

When the localization map (2) is injective, the relations can be understood in terms of relations in decomposition groups. On the other hand, it is quite difficult to say anything about relations corresponding to the kernel of the localization map.

Let us quickly review the precise relationship between $H^i(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$, $i = 1, 2$, and the generators and relations for $\mathcal{G}$, as detailed in [Lab67] or [NSW00, Section III.9]. Let $\mathrm{gr}^{\cdot}(\mathcal{F})$ denote the sequence of graded quotients associated with the descending p-central series on $\mathcal{F}$. The image of X in $\mathrm{gr}^1(\mathcal{F}) = \mathcal{F}/\mathcal{F}^p[\mathcal{F}, \mathcal{F}]$ forms a basis, which we also denote by X. With the choice of a linear ordering on X, the set

$$\{px, [x, x'] \colon x, x' \in X,\ x < x'\}$$

forms a basis for $\mathrm{gr}^2(\mathcal{F})$, where $p : \mathrm{gr}^1(\mathcal{F}) \to \mathrm{gr}^2(\mathcal{F})$ is induced by the pth power map and $[x, x']$ is (the image of) the commutator $xx'x^{-1}(x')^{-1}$. Now, any relation $\rho \in R$ has zero image in $\mathrm{gr}^1(\mathcal{F})$, and its image in $\mathrm{gr}^2(\mathcal{F})/p\mathrm{gr}^1(\mathcal{F})$ is

$$\sum_{x < x' \in X} a^{\rho}_{x,x'}[x, x'], \quad a^{\rho}_{x,x'} \in \mathbb{Z}/p\mathbb{Z}. \tag{4}$$

The quotient $\mathrm{gr}^1(\mathcal{F})$ and $H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \simeq H^1(\mathcal{F}, \mathbb{Z}/p\mathbb{Z})$ are dual as vector spaces over $\mathbb{F}_p$, allowing us to define a basis X^* of $H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$ dual to X. Similarly, R may be regarded as a basis for the dual to $H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$ via the transgression isomorphism $H^1(\mathcal{R}, \mathbb{Z}/p\mathbb{Z})^{\mathcal{G}} \simeq H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$. With these identifications, the numbers $a^{\rho}_{x,x'}$ in (4) are given by

$$a^{\rho}_{x,x'} = -\rho(x^* \cup x'^*), \quad x < x', \tag{5}$$

where the cup refers to the cup product pairing

$$H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \times H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \to H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}). \tag{6}$$

Since K contains μ_p, we have natural isomorphisms

$$H^i(G_{K,S}, \mu_p^{\otimes j}) \simeq H^i(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \otimes \mu_p^{\otimes j}$$

for any i and j, and so the cup product (6) is just (1) after a choice of isomorphism $\mu_p \simeq \mathbb{Z}/p\mathbb{Z}$.

Our primary focus in Sections 4–6 is a case in which the localization map (2) is zero: $n = p$, with p an odd prime, $K = \mathbb{Q}(\mu_p)$, and S consisting of the unique prime above p. In this case there is a natural conjugation action of $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{gr}^i(\mathcal{F})$; let us suppose that generators and relations have been chosen so that each x and each ρ is an eigenvector for this action. Define $a^{\rho}_{x,x'}$ by equation (5) for any $x, x' \in X$. Suppose further that p satisfies Vandiver's conjecture. Then

$H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})^-$, the subspace on which Δ acts by an odd character, is trivial, and therefore the matrix $A^\rho = (a^\rho_{x,x'})$ decomposes into blocks

$$A^\rho = \begin{pmatrix} A^{\rho+} & 0 \\ 0 & A^{\rho-} \end{pmatrix}$$

where $A^{\rho\pm}$ contains all entries $a^\rho_{x,x'}$ corresponding to $x, x' \in \mathrm{gr}^1(\mathcal{F})^\pm$. The matrix $A^{\rho+}$ is related to the p-adic zeta-function (see Sect. 4) and can be shown to be nonzero when Vandiver's conjecture holds and the λ-invariant of the p-part of the class group in the cyclotomic tower is equal to its index of irregularity (Proposition 4.2), in particular for $p < 12{,}000{,}000$ [BCE+01].

The question of when $A^{\rho-}$ is non-zero is more mysterious. In Section 5, we present a method for imposing linear conditions on $A^{\rho-}$. The relations $\rho \in R$ correspond to nontrivial eigenspaces of the p-part of the class group of K. For all such eigenspaces for p with $p < 10{,}000$, the method specifies $A^{\rho-}$ up to a scalar multiple (Theorem 5.1). Since the method works by imposing linear conditions, it is not capable of showing that

$$A^{\rho-} \neq 0. \tag{7}$$

In Sections 6 and 7, we consider conditions for the nontriviality in (7). In Section 6, we describe the relation between this nontriviality and the structure of class groups of Kummer extensions of K. In Section 7, we determine a formula for a certain projection of the cup product when it can be expressed as the corestriction of a cup product in an unramified Kummer extension L of K (Theorem 7.2). We then describe a computer calculation that uses this formula to verify the nontriviality of $A^{\rho-}$ for $p = 37$ (Theorem 7.5).

In Section 8, we describe, in detail, the relations in $\mathcal{G}$ that result from the nontriviality in (7) (Theorem 8.2) and, in particular, the explicit relation for $p = 37$. In Section 9, we use this description to exhibit relations in a graded $\mathbb{Z}_p$-Lie algebra $\mathfrak{g}$ associated with the action of the absolute Galois group on the pro-p fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$ (Theorem 9.1). For $p = 691$, we explain how a conjecture of Ihara on the relationship between the structure of $\mathfrak{g}$ and a certain Lie algebra of derivations implies (7) and, conversely, our calculations confirm Ihara's conjecture in this case if (7) is satisfied (Theorem 9.11).

In Section 10, we consider an Iwasawa-theoretic consequence of the nontriviality in (7), namely, Greenberg's pseudo-null conjecture in the case that the p-part of the class group of K has order p (Theorem 10.4).

Acknowledgments. The authors would like to thank Ralph Greenberg, Yasutaka Ihara, and Barry Mazur for their support, encouragement, and useful comments, Robert Bond and Michael Reid for some corrections, John Cremona for his invaluable assistance with C++ (used to prove Theorem 5.1 up to 6500), Claus Fieker for determining the structure of the maximal order of a degree 37 number field as part of the computation for $p = 37$ of Section 7, William Stein for his substantial contribution to this computation, and Kay Wingberg for his suggestion of the approach in Section 7. The first author was supported by NSF grant DMS-9624219 and by an AMS Bicentennial Fellowship and the second author by NSF VIGRE grant 9977116 and by an NSF Postdoctoral Research Fellowship.

2 A formula for the cup product

We consider the general setting for the cup product (1) of the introduction. First, we describe the groups $H^i(G_{K,S}, \mu_n)$, $i = 1, 2$. Let K_S denote the maximal extension of K unramified outside S. From the inflation-restriction exact sequence, $H^1(G_{K,S}, \mu_n)$ is the kernel of the restriction map from $H^1(K, \mu_n)$ to $H^1(K_S, \mu_n)$ and hence may be identified using Kummer theory with the kernel of $K^\times/K^{\times n} \to K_S^\times/K_S^{\times n}$. Thus

$$H^1(G_{K,S}, \mu_n) \simeq D_K/K^{\times n},$$

where

$$D_K = K_S^{\times n} \cap K^\times = \{x \in K^\times : n \mid \mathrm{ord}_{\mathfrak{q}}(x) \text{ for all } \mathfrak{q} \notin S\}.$$

The description of $H^2(G_{K,S}, \mu_n)$ involves the S-ideal class group $C_{K,S}$ of K. For an extension F/K, denote by $\mathcal{O}_{F,S}$ the ring of S-integers in F. For brevity, we set $\mathcal{O}_S = \mathcal{O}_{K_S,S}$. Since K_S contains the Hilbert class field of K, any nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_{K,S}$ becomes principal in $\mathcal{O}_S$—say $\mathfrak{a} = (\alpha)$ for $\alpha \in K_S^\times$. Furthermore, since $\mathfrak{a}$ is fixed by $G_{K,S}$, we have $\alpha^\sigma/\alpha \in \mathcal{O}_S^\times$ for $\sigma \in G_{K,S}$, and thus we can associate with $\mathfrak{a}$ an element of $H^1(G_{K,S}, \mathcal{O}_S^\times)$. Using Hilbert's Theorem 90 and the exact sequence

$$1 \to \mathcal{O}_S^\times \to K_S^\times \to P_S \to 1,$$

where P_S is the group of principal ideals of $\mathcal{O}_S$, it is easy to see that this induces an isomorphism

$$C_{K,S} \simeq H^1(G_{K,S}, \mathcal{O}_S^\times).$$

Also, if I_S is the group of fractional ideals of $\mathcal{O}_S$, then, since K_S contains the Hilbert class field of any of its subfields, I_S/P_S is trivial. Hence, since I_S is a direct sum of induced modules, we have

$$H^i(G_{K,S}, P_S) \simeq H^i(G_{K,S}, I_S) = 0, \quad i \geq 1.$$

It follows that $H^2(G_{K,S}, \mathcal{O}_S^\times)$ is isomorphic to $H^2(G_{K,S}, K_S^\times)$, the p-part of which, for those p dividing n, may be identified with the p-part of the subgroup of the Brauer group of K consisting of elements with zero invariant at all valuations $\nu \notin S$ [NSW00, Proposition 8.3.10]. As S contains all primes dividing n, the sequence

$$1 \to \mu_n \to \mathcal{O}_S^\times \xrightarrow{n} \mathcal{O}_S^\times \to 1 \tag{8}$$

is exact. Taking its cohomology and tensoring with μ_n, we obtain an exact sequence

$$1 \to C_{K,S}/nC_{K,S} \otimes \mu_n \to H^2(G_{K,S}, \mu_n^{\otimes 2}) \xrightarrow{\pi} \bigoplus_{\nu \in S} \mu_n \xrightarrow{\Pi} \mu_n \to 1, \tag{9}$$

where π is the twist by μ_n of the direct sum of the invariant maps. For future reference, we record that if the ideal $\mathfrak{a}$ represents an element of $C_{K,S}/nC_{K,S}$, the corresponding element of $H^2(G_{K,S}, \mu_n)$ is the coboundary $H^1(G_{K,S}, \mathcal{O}_S^\times) \to H^2(G_{K,S}, \mu_n)$ of the cocycle α^σ/α, where $\mathfrak{a}\mathcal{O}_S = (\alpha)$.

Now we consider the pairing

$$(\ ,\ )_S = (\ ,\ )_{n,K,S} \colon D_K \times D_K \to H^2(G_{K,S}, \mu_n^{\otimes 2})$$

induced by the cup product. Let $a, b \in D_K$. The image of $(a, b)_S$ under π as in (9) is given by the direct sum of the Hilbert pairings $(a, b)_v$ at $v \in S$. We determine a formula for $(a, b)_S$ with $a, b \in D_K$ in the case that $\pi(a, b)_S$ is trivial, obtaining an element of $C_{K,S}/nC_{K,S} \otimes \mu_n$.

Fix a primitive nth root of unity ζ. Let $\alpha \in K_S^\times$ with $\alpha^n = a$, and for $\sigma \in G_{K,S}$, let m_σ denote the smallest nonnegative integer such that $\sigma\alpha = \zeta^{m_\sigma}\alpha$. We start with a general cohomological lemma.

Lemma 2.1 Consider the homomorphism $G_{K,S} \to \mathbb{Z}/n\mathbb{Z}$ associated with a via Kummer theory and the isomorphism $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$ given by $\zeta \mapsto 1$. Let ϵ denote its coboundary in the cohomology sequence of

$$1 \to \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n^2\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 1.$$

Then

$$(a, a)_S = \frac{n(n-1)}{2}\epsilon \otimes \zeta^{\otimes 2}.$$

Proof. This is antisymmetry of the cup product if n is odd, since in that case both sides are zero. For n even, one can check directly that the difference of cocycles

$$(\sigma, \tau) \mapsto m_\sigma m_\tau - (m_\sigma + m_\tau - m_{\sigma\tau})/2 \pmod n$$

is the coboundary of

$$\sigma \mapsto -m_\sigma(1 + m_\sigma)/2 \pmod n.$$

(See also [NSW00, Section III.9].) ∎

We proceed by considering the exact sequence of $G_{K,S}$-modules

$$1 \to \mu_n \to SL_n(K_S) \to PSL_n(K_S) \to 1. \tag{10}$$

We define a $G_{K,S}$-cocycle with values in $PSL_n(K_S)$, the coboundary of which, when computed in two different ways, yields the formula. (The choice of this cocycle was motivated by consideration of the cyclic algebra associated with a and b.)

Let

$$M_b = \begin{bmatrix} 0 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 \\ b & 0 & \dots & 0 \end{bmatrix}.$$

Note that $M_b^n = b$, and choose $\beta \in K_S^\times$ such that

$$\beta^n = \det M_b = (-1)^{n-1} b.$$

We define a cochain with values in $SL_n(K_S)$ by

$$C_\sigma^{a,b} = (\beta^{-1} M_b)^{m_\sigma}, \quad \sigma \in G_{K,S}.$$

The images of the $C_\sigma^{a,b}$ in $PSL_n(K_S)$ define a cocycle, as each is fixed by $G_{K,S}$ and has order dividing n. We denote the class of this cocycle by $C^{a,b}$.

Lemma 2.2 Let δ denote the coboundary in cohomology associated with (10). Then

$$\delta(C^{a,b}) \otimes \zeta = (a, -ab)_S.$$

Proof. Let n_σ be the smallest nonnegative integer such that $\sigma\beta = \zeta^{n_\sigma}\beta$. The coboundary of $C^{a,b}$ in $H^2(G_{K,S}, \mu_n)$ is represented by the 2-cocycle

$$\begin{aligned}(\sigma,\tau) \quad \mapsto \quad & (\beta^{-1}M_b)^{m_\sigma}(\beta^{-1}M_b)^{m_\tau\sigma}(\beta^{-1}M_b)^{-m_{\sigma\tau}} \\ & = \beta^{-(\sigma-1)m_\tau}(\beta^{-1}M_b)^{m_\sigma+m_\tau-m_{\sigma\tau}} \\ & = \zeta^{-n_\sigma m_\tau}(-1)^{(n-1)(m_\sigma+m_\tau-m_{\sigma\tau})/n},\end{aligned}$$

which, upon tensoring with ζ and applying Lemma 2.1, yields

$$-((-1)^{n-1}b, a)_S + (a, a)_S = (a, -ab)_S.$$

■

The following lemma is applicable to the case of interest that $\pi(a, b)_S$ is trivial.

Lemma 2.3 Let B be the class of a $G_{K,S}$-cocycle B_σ with values in $PSL_n(K_S)$ such that $\pi(\delta(B) \otimes \zeta) = 0$. Then there exists an $A \in GL_n(K_S)$ such that

$$A^\sigma A^{-1} \equiv B_\sigma \pmod{K_S^\times}.$$

For any such A, there is a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_{K,S}$ such that

$$\det(A)\mathcal{O}_S \equiv \mathfrak{a}\mathcal{O}_S \pmod{nI_S}$$

and

$$\delta(B) = -\mathfrak{a} \pmod{nC_{K,S}}.$$

Proof. Consider the commutative diagram

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_n & \longrightarrow & SL_n(K_S) & \longrightarrow & PSL_n(K_S) & \longrightarrow & 1 \\
 & & \downarrow f & & \downarrow & & \downarrow g & & \\
1 & \longrightarrow & K_S^\times & \longrightarrow & GL_n(K_S) & \longrightarrow & PGL_n(K_S) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow \det & & \downarrow & & \\
1 & \longrightarrow & K_S^{\times n} & \longrightarrow & K_S^\times & \longrightarrow & K_S^\times/K_S^{\times n} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

We use δ (resp., δ') to denote any coboundary in a long exact sequence of cohomology groups arising from a horizontal (resp., vertical) short exact sequence in this diagram. The map $f_* \otimes \mu_n$, with

$$f_* : H^2(G_{K,S}, \mu_n) \to H^2(G_{K,S}, K_S^\times),$$

can be identified with π, so our assumption on B is equivalent to $f_*(\delta(B)) = 0$. Note that we have $\delta(g_*(B)) = f_*(\delta(B))$, where g_* denotes the map

$$g_* \colon H^1(G_{K,S}, PSL_n(K_S)) \to H^1(G_{K,S}, PGL_n(K_S)).$$

Since $H^1(G_{K,S}, GL_n(K_S)) = 0$, this implies $g_*(B) = 0$. Hence, there exist an element $y \in (K_S^\times / K_S^{\times n})^{G_{K,S}}$ such that $B = \delta'(y)$ and so, by definition of δ', an $A \in GL_n(K_S)$ satisfying both the first statement of the lemma and

$$y = \det(A) \pmod{K_S^{\times n}}. \tag{11}$$

(Note that it suffices to check the remainder of the lemma for this choice of A.)

Since the coboundaries δ and δ' anticommute,

$$\delta(B) = \delta(\delta'(y)) = -\delta'(\delta(y)).$$

Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_{K,S}$ such that

$$\mathfrak{a}\mathcal{O}_S \equiv y\mathcal{O}_S \pmod{nI_S}. \tag{12}$$

Choose $\eta \in K_S^\times$ such that $\eta\mathcal{O}_S = \mathfrak{a}\mathcal{O}_S$, and observe that $y = \eta \pmod{K_S^{\times n}}$. Thus, $\delta(y)$ is the image of the cocycle associated to η under the map

$$H^1(G_{K,S}, \mathcal{O}_S^\times) \to H^1(G_{K,S}, K_S^{\times n}),$$

so $\delta'(\delta(y))$ can be computed using the Kummer sequence (8). Hence, by the discussion following (9), $\delta'(\delta(y))$ is the class modulo n of $\mathfrak{a}$, which, by (11) and (12), satisfies the conditions of the lemma. ∎

Let $N_{L/K}$ denote the norm map for an extension L of K. We denote the image of a (fractional) ideal $\mathfrak{a}$ in $C_{K,S}/nC_{K,S}$ by $[\mathfrak{a}]$. We remark that $(n/2)[\mathfrak{a}]$ is always trivial if n is odd. We now state our formula for the pairing.

Theorem 2.4 Let $a, b \in D_K$ be such that the Hilbert pairing $(a, b)_v$ is trivial for all valuations $v \in S$. Choose $\alpha \in K_S^\times$ such that $\alpha^n = a$, let $L = K(\alpha)$, and set $d = [L : K]$. Let $\mathfrak{b}$ be the fractional ideal of $\mathcal{O}_{K,S}$ such that $b\mathcal{O}_{K,S} = \mathfrak{b}^n$. Write $b = N_{L/K}\gamma$ for some γ, and write

$$\gamma\mathcal{O}_{L,S} = \mathfrak{c}^{1-\sigma}\mathfrak{b}^{n/d}, \tag{13}$$

for some fractional ideal $\mathfrak{c}$ of $\mathcal{O}_{L,S}$ and $\sigma \in \mathrm{Gal}(L/K)$. Let $\xi \in \mu_n$ be such that $\sigma\alpha = \xi\alpha$. Then

$$(a, b)_S = ([N_{L/K}(\mathfrak{c})] + \frac{n}{2}[\mathfrak{b}]) \otimes \xi.$$

Proof. We have that b is a norm from L_v for all v, since the Hilbert pairing $(a,b)_v$ is trivial for $v \in S$ by assumption and for $v \notin S$ by definition of D_K. Since, in a cyclic extension, an element that is a local norm everywhere is a global norm, we have $b = N_{L/K}\gamma$ with $\gamma \in L^\times$. It is easy to see that γ has a decomposition as in (13). Without loss of generality, L/K has degree n, and ξ is the primitive nth root of unity ζ chosen in the construction of the cohomology class $C^{a,b}$.

We use γ to construct a matrix A as in Lemma 2.3. Let G be the diagonal matrix with $\gamma\gamma^\sigma \dots \gamma^{\sigma^{i-1}}$ in the (i,i) position. Let $x_1, \dots, x_n$ be any K-basis for L, and let X be the matrix with $x_j^{\sigma^{i-1}}$ in the (i,j) position. Let $A = GX$, so that

$$A_{i,j} = \gamma\gamma^\sigma \dots \gamma^{\sigma^{i-1}} x_j^{\sigma^{i-1}},$$

and thus

$$\gamma A_{i,j}^\sigma = \begin{cases} A_{i+1,j} & i < n \\ bA_{1,j} & i = n. \end{cases}$$

From this, we see that $\gamma A^\sigma = M_b A$, that is,

$$A^\sigma A^{-1} \equiv C_\sigma^{a,b} \pmod{K_S^\times}.$$

This induces an equality of cocycles, as σ generates $\mathrm{Gal}(L/K)$. Since

$$\gamma\gamma^\sigma \dots \gamma^{\sigma^{i-1}} \mathcal{O}_{L,S} = \mathfrak{c}\mathfrak{c}^{-\sigma^i}\mathfrak{b}^i,$$

we have

$$\det(G)\mathcal{O}_{L,S} = \mathfrak{c}^n (N_{L/K}\mathfrak{c})^{-1} \mathfrak{b}^{n(n+1)/2}.$$

Thus, reducing exponents modulo n and using Lemmas 2.2 and 2.3, we find

$$(a, -ab)_S = \delta C^{a,b} \otimes \zeta = ([N_{L/K}\mathfrak{c}] + \frac{n}{2}[\mathfrak{b}] - [\det(X)\mathcal{O}_{K,S}]) \otimes \zeta, \tag{14}$$

where, by a slight abuse of notation, $\det(X)\mathcal{O}_{K,S}$ denotes the ideal of $\mathcal{O}_{K,S}$ whose extension to $\mathcal{O}_S$ is $\det(X)\mathcal{O}_S$, which exists because $\det(X)^\sigma = \pm\det(X)$. As a special case, we take $b = 1$, so $\mathfrak{c} = \mathfrak{b} = 1$ and

$$(a, -a)_S = -[\det(X)\mathcal{O}_{K,S}] \otimes \zeta.$$

Subtracting this from (14), we obtain the theorem. ■

We have the following corollaries (which are also easy to prove directly).

Corollary 2.5 If $a, b \in \mathcal{O}_{K,S}^\times$, and if b is the norm of an element of $\mathcal{O}_{L,S}^\times$, then $(a,b)_S = 1$.

Corollary 2.6 If $a \in \mathcal{O}_{K,S}^\times$ is such that $1 - a \in \mathcal{O}_{K,S}^\times$, then $(a, 1-a)_S = 1$.

3 The cup product and K-theory

Corollary 2.6 may be rephrased in terms of K-theory. Recall the definition of the Milnor K_2-group of a commutative ring R:

$$K_2^M(R) = (R^\times \otimes R^\times)/\langle a \otimes (1-a) \colon a, 1-a \in R^\times \rangle.$$

Then Corollary 2.6 says that the restriction of the cup product to the S-units induces a map

$$u \colon K_2^M(\mathcal{O}_{K,S})/n \to H^2(G_{K,S}, \mu_n^{\otimes 2}).$$

On the other hand, since $\mu_n \subset K$, the exact sequence of Tate [Tat76, Theorem 6.2] and (9) yield a (noncanonical) isomorphism

$$c \colon K_2(\mathcal{O}_{K,S})/n \xrightarrow{\sim} H^2(G_{K,S}, \mu_n^{\otimes 2})$$

(see [Sou79], [DF85] and [Keu89] for generalizations). In [Sou79], a particular choice of the map c is described as a Chern class map (for n a power of a prime p). The two versions of K_2 are related by a map

$$\kappa \colon K_2^M(\mathcal{O}_{K,S}) \to K_2(\mathcal{O}_{K,S}), \tag{15}$$

which is constructed as follows. First, we may identify $K_2^M(K)$ with $K_2(K)$ by a classical result of Matsumoto. The group $K_2(\mathcal{O}_{K,S})$ may then be defined via the exact localization sequence

$$0 \to K_2(\mathcal{O}_{K,S}) \to K_2(K) \xrightarrow{t} \bigoplus_{\mathfrak{q} \notin S} k_{\mathfrak{q}}^\times \to 0, \tag{16}$$

where $k_{\mathfrak{q}}$ denotes the residue field of K at $\mathfrak{q}$, and the map t is given by tame symbols. Since two S-units pair trivially under the tame symbols, the sequence (16) yields the map κ of (15). Let κ_n denote the map induced by κ on K-groups modulo n.

Proposition 3.1 The maps u, c, and κ are related by the commutative diagram

$$\begin{array}{ccc} K_2^M(\mathcal{O}_{K,S})/n & \xrightarrow{\kappa_n} & K_2(\mathcal{O}_{K,S})/n \\ & \searrow^{u} & \simeq \downarrow -c \\ & & H^2(G_{K,S}, \mu_n^{\otimes 2}). \end{array}$$

Proof. This is a special case of [Sou79, Theorem 1] for n a prime power, and the general case follows easily. ■

Thus, the question of whether the pairing $(\ ,\ )_S$ is surjective on S-units is the question of surjectivity of κ_n. In Section 5, we make a conjecture on the surjectivity of κ_p (Conjecture 5.3) for the ring of p-integers in $\mathbb{Q}(\mu_p)$. In order for this conjecture to hold, κ_p will often have to be injective as well. We now describe a necessary, general condition for this injectivity.

The Steinberg symbol $\{a, b\}$, for $a, b \in R^\times$, is defined to be the image of $a \otimes b$ in $K_2^M(R)$. For any field F, the group $K_2^M(F)$ has the property that the Steinberg symbols are antisymmetric. This need not be true in an arbitrary ring R. On the other hand, in order that κ_n be injective, it is necessary that antisymmetry hold in $K_2^M(\mathcal{O}_{K,S})/n$, since $K_2(\mathcal{O}_{K,S}) \subset K_2^M(K)$. We now present one sufficient condition for this antisymmetry.

Lemma 3.2 Fix $\varepsilon \in \mathbb{Z}$ relatively prime to n. Assume that $R^\times/R^{\times n}$ has a generating set with a set of representatives $S \subseteq R^\times$ such that

$$\{1 - st^\varepsilon : s \in S,\ t \in S \cup \{1\},\ s \neq t\} \subset R^\times. \tag{17}$$

Then $\{a, b\} + \{b, a\} \equiv 0 \pmod{n}$ for any $a, b \in R^\times$.

Proof. Let $s \in S$ and $t \in S^\varepsilon \cup \{1\}$ with $s \neq t$, and set $x = st$. By definition of $K_2^M(R)$, we have

$$\{x, -x\} = -\left\{x, -\frac{1}{x}\right\} = -\left\{x, \frac{x-1}{x}\right\} = \left\{\frac{1}{x}, \frac{x-1}{x}\right\} = 0.$$

Then

$$\{s, t\} + \{t, s\} = \{s, -st\} + \{t, -st\} = \{st, -st\} = 0.$$

In general, if $a = x^n \prod_{i=1}^M a_i$ and $b = y^n \prod_{j=1}^N b_j$ with $a_i, b_j \in S \cup S^{-1}$ and $x, y \in R^\times$, then

$$\{a, b\} + \{b, a\} \equiv \sum_{i=1}^M \sum_{j=1}^N (\{a_i, b_j\} + \{b_j, a_i\}) \equiv 0 \pmod{n}.$$

■

4 Pairing with a pth root of unity

We now focus on the case $n = p$, an odd prime, $K = \mathbb{Q}(\mu_p)$ and $S = \{(1 - \zeta)\}$. Here, and for the remainder of the paper, we fix a choice ζ of a primitive pth root of unity. In this section, we will show that the cup product we are considering is nontrivial for many p. We assume Vandiver's conjecture holds at p, i.e., that p does not divide the class number of $\mathbb{Q}(\zeta + \zeta^{-1})$. Let $\mathcal{C}$ denote the group of cyclotomic p-units.

Lemma 4.1 The symbol $\{\zeta, x\} \in K_2^M(\mathcal{O}_{K,S})$ is zero for all $x \in \mathcal{O}_{K,S}^\times$. In particular, ζ pairs trivially with $\mathcal{O}_{K,S}^\times$ under the cup product.

Proof. This follows immediately from the properties of the symbol, since the elements $1 - \zeta^i$ with $1 \leq i \leq p-1$ generate $\mathcal{C}$, which, by a well-known consequence of Vandiver's conjecture, has index prime to p in $\mathcal{O}_{K,S}^\times$. ■

Let A_K denote the p-part of the class group C_K of K. (Note that $C_K = C_{K,S}$.) We have an exact sequence

$$0 \to \mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times p} \to H^1(G_{K,S}, \mu_p) \to A_K[p] \to 0,$$

in which the map on the right is induced by $a \mapsto \mathfrak{a}$, where $a\mathcal{O}_{K,S} = \mathfrak{a}^p$. By Lemma 4.1, the map $a \mapsto (\zeta, a)_S$ factors through a map

$$\psi\colon A_K[p] \to A_K \otimes \mu_p.$$

Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension, and let A_∞ be the inverse limit of the p-parts of the ideal class groups under norm maps up the cyclotomic tower. The abelian group A_∞ breaks up into eigenspaces $A_\infty(\omega^i)$, on which Gal$(K/\mathbb{Q})$ acts by the ith power of the Teichmüller character $\omega\colon \Delta \to \mathbb{Z}_p^\times$. Let Λ be the Iwasawa algebra. Fix a topological generator γ of Gal(K_∞/K) such that γ acts on μ_{p^2} by raising to the $(1+p)$th power, and let $T = \gamma - 1$ be the corresponding variable in the Iwasawa algebra, so $\Lambda \simeq \mathbb{Z}_p[[T]]$. Since p satisfies Vandiver's conjecture, $A_\infty(\omega^i) \simeq \Lambda/(f_i)$, where f_i is a characteristic power series [Was97].

We consider an i for which $A_K(\omega^i)$ is nontrivial. We often abuse notation by using the same symbol to denote both a (fractional) ideal and its ideal class.

Proposition 4.2 Let $\mathfrak{a} \in A_K[p](\omega^i)$, and choose $\mathfrak{a}_0 \in A_K(\omega^i)$ with $\mathfrak{a}_0^{f_i(0)/p} = \mathfrak{a}$. Then

$$\psi(\mathfrak{a}) = \mathfrak{a}_0^{-f_i'(0)} \otimes \zeta.$$

Proof. Let $L = K(\mu_{p^2})$, set $f = f_i$ and $N = N_{L/K}$, and let $\mathfrak{a}_1$ be an ideal of $\mathcal{O}_{L,S}$ with norm $\mathfrak{a}_0$. The ideal $\mathfrak{a}_1^{f(T)}$ is principal, generated by an element y, and

$$(Ny)\mathcal{O}_{K,S} = N\mathfrak{a}_1^{f(0)} = \mathfrak{a}^p = a\mathcal{O}_{K,S} \tag{18}$$

for some $a \in D_K$. Since ζ pairs trivially with p-units by Lemma 4.1, we may assume that y is the element we use to calculate $(\zeta, a)_S$ in Theorem 2.4. In particular, we have that

$$y\mathcal{O}_{L,S} = \mathfrak{a}_1^{f(T)} = \mathfrak{a}\mathfrak{b}^T \tag{19}$$

for $\mathfrak{b}$ such that

$$(\zeta, a)_S = N\mathfrak{b}^{-1} \otimes \zeta.$$

Let us make the identification

$$A_L(\omega^i) \simeq \mathbb{Z}_p[[T]]/(f(T), (1+T)^p - 1)$$

by mapping $\mathfrak{a}_1$ to 1. Then, using (18) and (19) and that $N = ((1+T)^p - 1)/T$, we see that $\mathfrak{b}$ may be identified with

$$\frac{1}{T}\left(f(T) - \frac{(1+T)^p - 1}{pT} f(0)\right) \equiv f'(0) \pmod{(p, T)},$$

and hence

$$N\mathfrak{b} \equiv \mathfrak{a}_0{}^{f'(0)} \pmod{pA_K}.$$

■

Thus if $f_i'(0)$ is nonzero modulo p, which is equivalent to saying that the λ-invariant of $A_\infty(\omega^i)$ is 1, then the pairing $(\ ,\ )_S$ is nontrivial. This occurs for all irregular primes less than 12,000,000 [BCE+01]. (We remark that for many purposes in this article, such as Proposition 4.2, the cyclicity of $A_K(\omega^i)$ would be a sufficient assumption [Kur93], but we are content to assume the stronger condition of Vandiver's conjecture.)

5 Restriction of the pairing to the cyclotomic p-units

We continue to assume $K = \mathbb{Q}(\mu_p)$, $S = \{(1-\zeta)\}$ and $n = p$, an odd prime satisfying Vandiver's conjecture. We consider the restriction of the pairing $(\ ,\ )_S$ to the subgroup $\mathcal{C}$ of cyclotomic p-units.

A pair (p, r), with r even and $2 \le r \le p-3$, is called irregular if p divides the numerator of the rth Bernoulli number B_r, that is, if the eigenspace $A_K(\omega^{p-r})$ is nontrivial. Given such a pair, we choose an isomorphism

$$A_K(\omega^{p-r}) \otimes \mu_p \simeq \mathbb{Z}/p\mathbb{Z}(2-r). \tag{20}$$

(We shall view the underlying group structure of $A(i)$ for a given $G_{K,S}$-module A and twist $i \in \mathbb{Z}$ as being canonically identified with that of A.) Let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$, and consider the Δ-equivariant pairing

$$\langle\ ,\ \rangle_r : D_K \times D_K \to \mathbb{Z}/p\mathbb{Z}(2-r)$$

arising via (20) from composition of $(\ ,\ )_S$ with projection onto $A_K(\omega^{p-r}) \otimes \mu_p$.

We consider the restriction of $\langle\ ,\ \rangle_r$ to $\mathcal{C} \times \mathcal{C}$. In fact, since $\mathcal{C} = \langle -\zeta \rangle \oplus \mathcal{C}^+$, we can by Lemma 4.1 focus attention on the restriction of the pairing to elements of $\mathcal{C}^+$. Eigenspace considerations put some restrictions on the elements that can pair nontrivially. For any integer i, consider the usual idempotent

$$\epsilon_i = \frac{1}{p-1} \sum_{\sigma \in \Delta} \omega(\sigma)^{-i} \sigma,$$

and choose $\eta_i \in \mathcal{C}$ with

$$\eta_i \equiv (1-\zeta)^{\epsilon_{p-i}} \pmod{\mathcal{C}^p}.$$

Then $\mathcal{C}^+$ is generated by $\{\eta_i : i \text{ odd}, 1 \le i \le p-2\}$. Since Δ acts on $(\eta_i, \eta_j)_S$ via ω^{2-i-j}, we have

$$\langle \eta_i, \eta_j \rangle_r = 0 \text{ if } i + j \not\equiv r \pmod{p-1}.$$

Let

$$e_{i,r} = \langle \eta_i, \eta_{r-i} \rangle_r, \quad i \text{ odd}, 1 \le i \le p-2.$$

We now impose many linear relations on the $e_{i,r}$ and, in the process, get bounds on the order of $K_2^M(\mathcal{O}_{K,S})/p$. Lemma 4.1 and Corollary 2.6 imply that if η is a cyclotomic unit and $1-\eta = \zeta^j\eta'$ for some j and cyclotomic unit η', then $\{\eta,\eta'\} = 0$ in $K_2^M(\mathcal{O}_{K,S})$, and hence $(\eta,\eta')_S = 1$. Applying this observation to

$$\eta = \rho_a = \sum_{j=0}^{a-1} (-\zeta)^j,$$

we get

$$\{\rho_a, \rho_{a-1}\} = 0, \qquad 3 \le a \le p-1.$$

Note that, if a is even,

$$\rho_a = \frac{1-\zeta^a}{1+\zeta} = \frac{(1-\zeta^a)(1-\zeta)}{1-\zeta^2}, \quad \rho_{a-1} = \frac{1+\zeta^{a-1}}{1+\zeta} = \frac{(1-\zeta^{2a-2})(1-\zeta)}{(1-\zeta^{a-1})(1-\zeta^2)}.$$

If $\sigma \in \Delta$ satisfies $\sigma\zeta = \zeta^a$, then $\omega(\sigma) \equiv a \pmod{p}$. Thus

$$(1-\zeta^a)^{\epsilon_{p-i}} \equiv \eta_i^{a^{p-i}} \pmod{\mathcal{C}^p}.$$

Hence, the $e_{i,r}$ must be solutions $x_i = e_{i,r}$ over $\mathbb{Z}/p\mathbb{Z}$ to

$$\sum_{\substack{i \text{ odd} \\ 1\le i\le p-2}} (1+a^{p-i}-2^{p-i})(1-2^{p-r+i})(1-(a-1)^{p-r+i})x_i = 0 \tag{21}$$

for every even a with $4 \le a \le p-1$. (These relations also hold for odd a with $3 \le a \le p-2$, but we will not use those.)

Theorem 5.1 For all irregular pairs (p,r) with $p < 10{,}000$, there exists a nontrivial, Galois equivariant, skew-symmetric pairing

$$\langle\ ,\ \rangle \colon \mathcal{C} \times \mathcal{C} \to \mathbb{Z}/p\mathbb{Z}(2-r)$$

satisfying (21) with $x_i = \langle \eta_i, \eta_{r-i}\rangle$. Furthermore, these properties uniquely define the pairing up to a scalar multiple.

Sketch of Proof. The relations (21) and the antisymmetry relations, $x_i + x_{r-i} = 0$, put constraints on possible values of the pairing. We used a computer to calculate the nullspace of the matrix of coefficients in these relations. ■

We have computed the pairing of Theorem 5.1 for all (p,r) with $p < 10{,}000$. A table of the pairings and Magma routines that perform the computation are available at `www.math.harvard.edu/~sharifi` and `www.math.arizona.edu/~wmc`. The pairing $\langle\ ,\ \rangle_r$ must be a (possibly zero) scalar multiple of the computed pairing.

Corollary 5.2 For all irregular pairs (p,r) with $p < 10{,}000$, one has

$$|(K_2^M(\mathcal{O}_{K,S})/p)(\omega^{2-r})| \le p.$$

Proof. The only point at issue here is whether the symbols in $K_2^M(\mathcal{O}_{K,S})/p$ satisfy the skew-symmetry that was used in the proof of Theorem 5.1, as the other relations used in Theorem 5.1 arise directly from relations in $K_2^M(\mathcal{O}_{K,S})$ and eigenspace considerations. Since $\mathcal{C}$ has index prime to p in $\mathcal{O}_{K,S}^\times$, we need only remark that the set S of generators of $\mathcal{C}$ given by $1-\zeta^i$ with $1 \le i \le p-1$ has the property (17) for $\varepsilon = -1$. Then, by Lemma 3.2, the image of $a \otimes b + b \otimes a$ is trivial in $K_2^M(\mathcal{O}_{K,S}) \otimes \mathbb{Z}_p$ for any $a, b \in \mathcal{O}_{K,S}^\times$. ■

In fact, by performing modulo p^2 the same computations as in the proof of Theorem 5.1, we have verified that

$$|(K_2^M(\mathcal{O}_{K,S}) \otimes \mathbb{Z}_p)(\omega^{2-r})| \le p$$

for all irregular pairs with $p < 3000$. The authors suspect that the uniqueness in Theorem 5.1 fails for the irregular pair given by $p = 89209$ and $r = (p+3)/2$, as the values $x_1 = -x_{(p+1)/2} = 1$ and $x_i = 0$ for $i \neq 1, (p+1)/2$ provide a solution to the equations in this case, since $2^{p-r+1} \equiv 1 \pmod{p}$. Corollary 5.2 may or may not still hold for this p, since we did not use all of the defining relations of $K_2^M(\mathcal{O}_{K,S})$ in its proof. We do, however, conjecture that the pairing $\langle\ ,\ \rangle_r$ is nontrivial. Since the eigenspaces of $K_2(\mathcal{O}_{K,S})/p$ corresponding to regular pairs are trivial, this may be rephrased as follows.

Conjecture 5.3 Let p be an odd prime satisfying Vandiver's conjecture. Let $K = \mathbb{Q}(\mu_p)$ and let $\mathcal{O}_{K,S}$ denote the ring of p-integers in K. The natural map

$$K_2^M(\mathcal{O}_{K,S}) \otimes \mathbb{Z}_p \to K_2(\mathcal{O}_{K,S}) \otimes \mathbb{Z}_p$$

is surjective.

In Section 7, we verify this conjecture in the case $p = 37$. In general, we have constructed many other relations similar to those of (21), and their solutions are consistent with the values of the calculated pairing of Theorem 5.1 in those cases that we have tested. As the example with $p = 89209$ illustrates (or consider the regular pair $(73, 38)$), we have no convincing evidence regarding whether or not the map in Conjecture 5.3 is always injective.

As further circumstantial evidence for the conjecture, we note that the nontrivial pairing of Theorem 5.1 has a property not obviously encoded in the relations above, namely that $x_{p-r} = 0$. The cup product pairing $\langle\ ,\ \rangle_r$ must itself satisfy this relation, since η_{p-r} provides a Kummer generator for the unramified extension of K whose Galois group corresponds to $(A_K/pA_K)(\omega^{p-r})$ with respect to the Artin map. Thus the norm of an ideal from this extension always has trivial projection to the ω^{p-r} eigenspace of A_K/pA_K, and hence the pairing must be trivial by Theorem 2.4.

6 Relationship with the ideal class group

Let K be a number field and S a set of primes of K that contains all real places of K. For a finite extension F of K, we denote by $I_{F,S}$, $P_{F,S}$, and $C_{F,S}$ the ideals, principal ideals, and ideal class group, respectively, of the S-integers $\mathcal{O}_{F,S}$, and by $H_{F,S}$ the maximal unramified abelian extension of F in which all primes above S split completely.

First we review some genus theory. Let L/K be a cyclic extension, unramified outside S, with Galois group G generated by an element σ.

Lemma 6.1 The norm map $N_{L/K} : C_{L,S} \to C_{K,S}$ induces a map

$$C_{L,S}/(\sigma - 1)C_{L,S} \to C_{K,S},$$

which is a surjection if and only if $L \cap H_{K,S} = K$, and is an injection if there is at most one prime in S that does not split completely in L/K.

Proof. By class field theory, $C_{L,S} = \mathrm{Gal}(H_{L,S}/L)$ and $C_{K,S} = \mathrm{Gal}(H_{K,S}/K)$. With these identifications, the norm map is restriction to $H_{K,S}$. Thus the image of the norm map is $\mathrm{Gal}(H_{K,S}/(L \cap H_{K,S}))$, which immediately implies the first assertion. The kernel of the norm map is generated by the commutator subgroup and the intersection between $\mathrm{Gal}(H_{L,S}/L)$ and the subgroup of $\mathrm{Gal}(H_{L,S}/K)$ generated by decomposition groups of primes in S. If there is exactly one nontrivial decomposition group, then its contribution is trivial, since it maps injectively to Gal(L/K). Furthermore, since G is cyclic the commutator subgroup of $\mathrm{Gal}(H_{L,S}/K)$ is $[\sigma, \mathrm{Gal}(H_{L,S}/L)] = (\sigma - 1)C_{L,S}$. ■

Compare the following proposition with Theorem 2.4.

Proposition 6.2 There is an isomorphism

$$C_{L,S}^{G}/\phi(C_{K,S}) \xrightarrow{\sim} (\mathcal{O}_{K,S}^{\times} \cap N_{L/K}L^{\times})/N_{L/K}\mathcal{O}_{L,S}^{\times}$$

given by taking the class of an ideal $\mathfrak{a}$ to an element $\mathfrak{b} \in \mathcal{O}_{K,S}^{\times}$ such that $\mathfrak{b} = N_{L/K}y$ with $y\mathcal{O}_{L,S} = \mathfrak{a}^{1-\sigma}$. If $H_{K,S} \cap L = K$ and there is at most one prime in S that does not split completely in L/K, the order of these groups is equal to the number of ideal classes in $C_{K,S}$ that define trivial classes in $C_{L,S}$.

Proof. Consider the exact sequence

$$0 \to P_{L,S} \to I_{L,S} \to C_{L,S} \to 0.$$

Since L/K is unramified outside S, $I_{L,S}$ is a direct sum of induced modules, so $\hat{H}^1(G, I_{L,S}) = 0$. Thus we have a surjection

$$\hat{H}^0(G, C_{L,S}) \to \hat{H}^{-1}(G, P_{L,S}),$$

which takes the class of an ideal $\mathfrak{a}$ to $(1 - \sigma)\mathfrak{a}$. Since the map $P_{L,S}^{G} \to I_{L,S}^{G} = I_{K,S}$ has cokernel equal to the image of $C_{K,S}$ under the obvious map $\phi\colon C_{K,S} \to C_{L,S}$, we therefore have an isomorphism

$$C_{L,S}^{G}/\phi(C_{K,S}) \simeq \hat{H}^{-1}(G, P_{L,S}).$$

Furthermore, using the exact sequence

$$0 \to \mathcal{O}_{L,S}^{\times} \to L^{\times} \to P_{L,S} \to 0$$

and the triviality of $\hat{H}^{-1}(G, L^{\times})$, we obtain

$$\hat{H}^{-1}(G, P_{L,S}) \simeq (\mathcal{O}_{K,S}^{\times} \cap N_{L/K}L^{\times})/N_{L/K}\mathcal{O}_{L,S}^{\times},$$

induced by $N_{L/K}$ on a generator of a representative principal ideal. This proves the first statement in the proposition.

Now, suppose that $H_{K,S} \cap L = K$ and that there is at most one prime in S that does not split completely in L/K. Then it follows from Lemma 6.1 that $\phi(C_{K,S}) = N_G(C_{L,S})$, where N_G is the norm element in the group ring $\mathbb{Z}[G]$. Thus

$$C_{L,S}^G/\phi(C_{K,S}) = \hat{H}^0(G, C_{L,S}).$$

Furthermore, since $C_{L,S}$ is finite, we have

$$|\hat{H}^0(G, C_{L,S})| = |\hat{H}^{-1}(G, C_{L,S})|.$$

Finally, using Lemma 6.1 again, we see that

$$\hat{H}^{-1}(G, C_{L,S}) \simeq \ker(C_{K,S} \to C_{L,S}).$$

This proves the second assertion of the proposition. ■

Now we return to the situation of Section 2, fixing n and letting K contain the nth roots of unity and S all primes above n and real archimedean places. Let $a \in D_K$ and $\alpha \in K_S^{\times}$ with $\alpha^n = a$ and take $L = K(\alpha)$. We let $d = [L : K]$.

Proposition 6.3 Suppose $a \in D_K$ is such that $H_{K,S} \cap L = K$ and there is at most one prime of S that does not split completely in L/K. Then the map $(n/d)N_{L/K} : C_{L,S} \to C_{K,S}$ induces an isomorphism

$$C_{L,S}^G/((d, \sigma - 1)C_{L,S})^G \otimes \mu_n \xrightarrow{\sim} (a, \mathcal{O}_{K,S}^{\times})_S \cap (C_{K,S} \otimes \mu_n), \tag{22}$$

the intersection being taken in $H^2(G_{K,S}, \mu_n) \otimes \mu_n$.

Proof. Given $\mathfrak{a} \in C_{L,S}^G$, we can find $b \in \mathcal{O}_{K,S}^{\times} \cap N_{L/K}L^{\times}$ associated with $\mathfrak{a}$ by the isomorphism in Proposition 6.2. Since b is a global norm it is a local norm everywhere, and Theorem 2.4 applies. Conversely, given $b \in \mathcal{O}_{K,S}^{\times}$ such that $(a, b)_v = 1$ for all $v \in S$, Theorem 2.4 supplies an ideal $\mathfrak{a}$ with class in $C_{L,S}^G$ such that $(a, b)_S = N_{L/K}\mathfrak{a} \otimes \xi$, with ξ a fixed generator of μ_d. Therefore, the map in (22) is surjective. By Lemma 6.1, the kernel of $N_{L/K}$ on $C_{L,S}$ is $(\sigma - 1)C_{L,S}$ and $N_{L/K}$ is surjective. Thus, the kernel of the map $C_{L,S} \to C_{K,S} \otimes \mu_n$ given by $\mathfrak{a} \mapsto N_{L/K}\mathfrak{a} \otimes \xi$ is $(d, \sigma - 1)C_{L,S}$. ■

This has, for instance, the following corollary in the case $n = p$, a prime number. Let $A_{F,S}$ denote the p-part of the S-class group of F for F/K finite.

Corollary 6.4 Assume that $|A_{K,S}| = p$ and S consists of a single (unique) prime above p. Let $a \in D_K$ be such that $[L : K] = p$. Then $(a, \mathcal{O}_{K,S}^{\times})_S \neq 0$ if and only if $|A_{L,S}| = p$.

Proof. If $L \subseteq H_{K,S}$, then since $A_{L,S}$ is the commutator subgroup of a p-group that has maximal abelian quotient $A_{K,S} \simeq \mathbb{Z}/p\mathbb{Z}$, we must have $A_{L,S} = 0$. Hence, we may assume $H_{K,S} \cap L = K$.

By Lemma 6.1, the order of the quotient $A_{L,S}/(\sigma - 1)A_{L,S}$ is p. By the assumption on S, the image of the pairing is contained in $C_{K,S} \otimes \mu_p$. Thus, using Proposition 6.3, we see that $A_{L,S}^G$ surjects onto the above quotient if and only if $(a, \mathcal{O}_{K,S}^{\times})_S$ is nonzero. On the other hand, $A_{L,S}^G$ surjects onto the quotient if and only if $(\sigma - 1)A_{L,S} = 0$. ■

Again, let us consider the case $n = p$ odd, $K = \mathbb{Q}(\mu_p)$ and $S = \{(1-\zeta)\}$. Assume Vandiver's conjecture, and let (p, r) be an irregular pair. Recall the pairing $\langle \ , \ \rangle_r$ of Section 5.

Lemma 6.5 The image of the pairing $\langle \ , \ \rangle_r$ is $\langle 1 - \zeta, \mathcal{C}^+ \rangle_r$.

Proof. The image of the pairing is generated by $\langle \eta_i, \eta_{r-i} \rangle_r$ for all odd i. Since $\langle \eta_i, \eta_j \rangle_r = 0$ for $j \not\equiv r - i \mod p - 1$, we have

$$\langle \eta_i, \eta_{r-i} \rangle_r = \langle \eta_i, \prod_{j=0}^{p-2} (1 - \zeta)^{e_j} \rangle_r = \langle \eta_i, 1 - \zeta \rangle_r.$$

■

Proposition 6.3 allows us to conclude the following.

Corollary 6.6 Let $\alpha^p = 1 - \zeta$ and $L = K(\alpha)$. Then the image of the pairing $\langle \ , \ \rangle_r$ is isomorphic to the ω^{p-r}-eigenspace of $A_L^G/((p, \sigma - 1)A_L)^G$, where A_L denotes the p-part of the class group of L.

7 Relationship with local pairings

We restrict ourselves to the case $n = p$ and K containing μ_p. We assume that S consists of a single, unique prime of K above p and, if $p = 2$, that K has no real places. In Theorem 7.2, we will derive a formula for (a projection of) the pairing $(a, b)_S$ as a norm residue symbol in a certain unramified cyclic extension L of K of degree p. The formula is similar to that of Theorem 2.4 in that its applicability amounts to the determination of an element $c \in L^{\times}$ such that $c^{\sigma-1}b \in L^{\times p}$, where σ generates $\mathrm{Gal}(L/K)$ (for a different field L). In this case, however, one must determine an embedding of c in the multiplicative group modulo pth powers of the completion at L at a prime above p, as opposed to determining the class modulo p of an ideal of $\mathcal{O}_{K,S}$ that c generates in L, again up to a pth power.

Let L/K be an unramified cyclic extension of degree p, and set $G = \mathrm{Gal}(L/K)$. Consider the following commutative diagram, in which (9) has been used to obtain the top row and in which we have identified $H^2(G_{K,S}, \mu_p)$ with $C_{K,S}/pC_{K,S}$ in the bottom row.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_{L,S}/pC_{L,S} & \longrightarrow & H^2(G_{L,S}, \mu_p) & \longrightarrow & \bigoplus^0_{\mathfrak{p}|p} H^2(L_{\mathfrak{p}}, \mu_p) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \mathrm{cor}} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & N_{L/K}C_{L,S}/pC_{K,S} & \longrightarrow & C_{K,S}/pC_{K,S} & \longrightarrow & C_{K,S}/N_{L/K}C_{L,S} & \longrightarrow & 0 \end{array}$$

Here, the superscript 0 on the direct sum indicates the kernel of the map

$$\sum_{\mathfrak{p}|p} \mathrm{inv}_{\mathfrak{p}} : \bigoplus_{\mathfrak{p}|p} H^2(L_{\mathfrak{p}}, \mu_p) \to \mathbb{Z}/p\mathbb{Z}$$

(under the obvious identification $\frac{1}{p}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z}$). By class field theory, there is a natural isomorphism $C_{K,S}/N_{L/K}C_{L,S} \simeq G$. Let σ be a generator of G. Choose a prime of L above p, say $\mathfrak{p}_0$, and for any other, let $k_{\mathfrak{p}} \in \mathbb{Z}/p\mathbb{Z}$ be such that $\mathfrak{p} = \sigma^{-k_{\mathfrak{p}}}\mathfrak{p}_0$. We need the following explicit description of the map f.

Lemma 7.1 The map

$$f : \bigoplus_{\mathfrak{p}|p}^{0} H^2(L_{\mathfrak{p}}, \mu_p) \to C_{K,S}/N_{L/K}C_{L,S}$$

is given by

$$f(c) = \sum_{\mathfrak{p}|p} k_{\mathfrak{p}}\, \mathrm{inv}_{\mathfrak{p}}(c) \cdot \mathfrak{c}$$

for some ideal class $\mathfrak{c}$ generating $C_{K,S}/N_{L/K}C_{L,S}$.

Proof. Corestriction is equivariant with respect to G, and hence so is the map f. Furthermore, $\bigoplus^0 H^2(L_{\mathfrak{p}}, \mu_p)$ is a cyclic $\mathbb{Z}_p[G]$-module, and $C_{K,S}/N_{L/K}C_{L,S} \simeq \mathbb{Z}/p\mathbb{Z}$, so there is only one non-zero map up to scalar multiple. Since $G_{K,S}$ has cohomological dimension at most 2 [NSW00, Proposition 8.3.17], corestriction is surjective by [NSW00, Proposition 3.3.8], and hence so is f. So all we need to do is verify that the formula we have given for f is equivariant with respect to G. Note that $k_{\sigma\mathfrak{p}} = k_{\mathfrak{p}} - 1$. Hence, since $\mathrm{inv}_{\mathfrak{p}}(\sigma c) = \mathrm{inv}_{\sigma^{-1}\mathfrak{p}}(c)$, we have

$$f(\sigma c) = f(c) - \sum_{\mathfrak{p}|p} \mathrm{inv}_{\mathfrak{p}}(c)\mathfrak{c} = f(c).$$

■

For a prime $\mathfrak{p}$ of L above p, denote by $(\ ,\ )_{\mathfrak{p}}$ the Hilbert pairing on $L_{\mathfrak{p}}^{\times}$ into μ_p. Let π_L denote the projection map

$$\pi_L \colon H^2(G_{K,S}, \mu_p^{\otimes 2}) \to C_{K,S}/N_{L/K}C_{L,S} \otimes \mu_p.$$

Theorem 7.2 Let $\mathfrak{p}_0$ be a prime of L above p, and let $\mathfrak{c}$ be as in Lemma 7.1. Let $a, b \in \mathcal{O}_{K,S}^\times$ and suppose that $b = N_{L/K} b'$ for some $b' \in \mathcal{O}_{L,S}^\times$. Then

$$\pi_L(a,b)_S = \mathfrak{c} \otimes (a, N'b')_{\mathfrak{p}_0}, \quad N' = \sum_{k=1}^{p-1} k\sigma^k. \tag{23}$$

Proof. As a standard property of the cup product, we have

$$(a,b)_S = \mathrm{cor}_{L/K}(\mathrm{res}_{L/K}\, a, b')_{L,S}.$$

We evaluate $\pi_L(a,b)_S$ by taking the image of $(a,b')_{L,S}$ in $\bigoplus_{\mathfrak{p}} H^2(L_{\mathfrak{p}}, \mu_p^{\otimes 2})$, namely $\bigoplus_{\mathfrak{p}} (a,b')_{\mathfrak{p}}$, and applying the map $f \otimes \mu_p$ to it. By Lemma 7.1, the result of this is

$$\pi_L(a,b)_S = \mathfrak{c} \otimes \sum_{\mathfrak{p}|p} (a,b')_{\mathfrak{p}}^{k_{\mathfrak{p}}}. \tag{24}$$

Now, $(\sigma x, \sigma y)_{\sigma\mathfrak{p}} = (x,y)_{\mathfrak{p}}$ for any $x, y \in L^\times$. Thus (23) follows from (24) and the facts that $\sigma a = a$ and $\sigma^{-k_{\mathfrak{p}}}\mathfrak{p}_0 = \mathfrak{p}$. ■

We make the following observation on the applicability of Theorem 7.2.

Lemma 7.3 If $|A_{K,S}| = p$, then $N_{L/K}\mathcal{O}_{L,S}^\times = \mathcal{O}_{K,S}^\times$.

Proof. By Proposition 6.2, we must show that $A_{L,S}^G/\phi(A_{K,S}) = 0$ (where ϕ is the natural map). Since $A_{L,S}$ is finite and G is cyclic, we have

$$|A_{L,S}^G| = |A_{L,S}/(\sigma - 1)|,$$

and it follows from Lemma 6.1 that this latter group has order $|A_{K,S}|/p = 1$. ■

We now focus on our main interest: $K = \mathbb{Q}(\mu_p)$ and $S = \{(1-\zeta)\}$, with p an irregular prime satisfying Vandiver's conjecture. We consider the pairing $\langle\ ,\ \rangle_r$, where p divides B_r. Now let $\alpha_{p-r}^p = \eta_{p-r}$, and set $L = K(\alpha_{p-r})$, so that Δ acts on G with eigenvalue ω^{p-r}. Then π_L amounts to the application of the idempotent ϵ_{2-r}.

We can exploit the action of Δ to simplify the computation of $(N'b')_{\mathfrak{p}_0}$ as follows. Let $\iota_{\mathfrak{p}} : L \hookrightarrow K_p = \mathbb{Q}_p(\mu_p)$ be the embedding corresponding to $\mathfrak{p}$. Let Δ_0 be the inertia group of $\mathfrak{p}_0$, which we identify with $\mathrm{Gal}(K_p/\mathbb{Q}_p)$ via the projection onto $\mathrm{Gal}(K/\mathbb{Q})$.

Proposition 7.4 Let $3 \le i \le p-2$ be odd such that p does not divide B_{p-i}. Assume that $b = \eta_{r-i}$ is the norm of an S-unit $b' \in \mathcal{O}_{L,S}^\times$, and choose b' to have image in the ω^{p-r+i}-eigenspace of $\mathcal{O}_{L,S}^\times/\mathcal{O}_{L,S}^{\times p}$. Then $\langle \eta_i, \eta_{r-i}\rangle_r \neq 0$ if and only if $\iota_{\mathfrak{p}_0}(N'b') \notin K_p^{\times p}$.

Proof. Let $\delta \in \Delta_0$. We see that

$$\delta(N'b') = \prod_{k=1}^{p-1} \delta\sigma^k(b')^k = \prod_{k=1}^{p-1} \sigma^{k\omega^{p-r}(\delta)}\delta(b')^k.$$

Modulo $\mathcal{O}_{L,S}^{\times p}$, this is congruent to

$$\prod_{k=1}^{p-1} \sigma^{k\omega^{p-r}(\delta)}(b')^{k\omega^{p-r+i}(\delta)} \equiv \prod_{k=1}^{p-1} \sigma^{k}(b')^{k\omega^{i}(\delta)} \equiv (N'b')^{\omega^{i}(\delta)}.$$

Hence $N'b'$ has image in the ω^i-eigenspace of $\mathcal{O}_{L,S}^{\times}/\mathcal{O}_{L,S}^{\times p}$ under Δ_0.

By Theorem 7.2, $\langle \eta_i, \eta_{r-i} \rangle_r = 0$ if and only if $(\eta_i, N'b')_{\mathfrak{p}_0} = 1$. Since p does not divide B_{p-i}, the element η_i is not locally a pth power. Furthermore, we have seen that the elements η_i and $N'b'$ have image in the ω^{1-i} and ω^i eigenspaces of $K_p^{\times}/K_p^{\times p}$, respectively. These eigenspaces have dimension 1 since $i \not\equiv 0, 1 \pmod{p-1}$, and hence the result follows from the non-degeneracy and Galois equivariance of the norm residue symbol. ■

For $p = 37$, the condition of Proposition 7.4 is computationally verifiable.

Theorem 7.5 The pairing $\langle\ ,\ \rangle_{32}$ for $p = 37$ is nontrivial. Thus, Conjecture 5.3 is true for $p = 37$.

Sketch of Proof. Consider the fixed field F of Δ_0. This is generated by the trace x of a pth root α_{p-r} of (a choice of) η_{p-r}. With the help of William Stein, we determined a minimal polynomial for x by considering small primes l that are primitive roots modulo p, computing the minimal polynomial of the image of x in $\mathbb{F}_{l^{p-1}}[X]/(X^p - \eta_{p-r})$, and using the Chinese Remainder Theorem to find a $\mathbb{Q}$-polynomial that x satisfies. Given this polynomial, Claus Fieker used Magma routines to compute the maximal order of F and then a polynomial for F with smaller discriminant (by far the most time-intensive steps), which made it possible to compute the p-unit group of F (by first computing the class group to "sufficient precision"). Now F has two prime ideals above p, and the prime of F below $\mathfrak{p}_0$ embeds F into $\mathbb{Q}_p$. We chose a p-unit that generates this prime, and this provided an element b' as in Proposition 7.4 with $p = N_{L/K}b'$. We then computed the embeddings of x at the primes $\mathfrak{p}_k$ from the embeddings of α_{p-r}, which we obtained by factoring $X^p - \eta_{p-r}$ over $\mathbb{Q}_p(\zeta)$. Writing b' as a $\mathbb{Q}$-polynomial in x, we then computed the image

$$\iota_{\mathfrak{p}}(N'b') = \prod_{k=1}^{p-1} \iota_{\mathfrak{p}_k}(b')^k$$

to verify the condition of Proposition 7.4. The Magma code is currently available at `www.math.harvard.edu/~sharifi` and `www.math.arizona.edu/~wmc`. ■

Using the results of Section 6, we obtain the following corollary, which implies, for example, that $\mathbb{Q}(\sqrt[37]{37})$ has class number prime to 37, answering a question of Ralph Greenberg's.

Corollary 7.6 Let $p = 37$, and let L/K be a cyclic extension of degree 37 that is unramified outside 37. Then $|A_{L,S}| = 37$ if and only if L is not contained in $\mathbb{Q}(\zeta_{37^2}, \alpha_5, \alpha_{27})$, where $\alpha_i^{37} = \eta_i$ for any odd i.

Proof. The values of the pairing $\langle\ ,\ \rangle_{32}$ tell us that the subgroup of D_K consisting of elements that pair trivially with all 37-units of K is $Q = \langle \zeta, \eta_5, \eta_{27} \rangle \cdot D_K^{37}$. By Corollary 6.4, $|A_{L,S}| = 37$ if and only if $L = K(\alpha)$ with $\alpha^{37} \notin Q$. The result now follows via Kummer theory. ■

8 Relations in the Galois group

Let us return to the general situation and notation of the introduction with $n = p$, considering a free presentation (3) of $\mathcal{G} = G_{K,S}^{(p)}$. The image of an arbitrary relation $\rho \in R$ in $\mathrm{gr}^2(\mathcal{F})/p\,\mathrm{gr}^1(\mathcal{F})$ was given by (4). In $\mathrm{gr}^2(\mathcal{F})$ itself, the relation must have the form

$$\sum_{x \in X} a_x^{\rho} p x + \sum_{x < x' \in X} a_{x,x'}^{\rho} [x, x']. \tag{25}$$

To describe $a_x^{\rho} \in \mathbb{Z}/p\mathbb{Z}$, we use the Bockstein homomorphism

$$B \colon H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \to H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}),$$

which is the coboundary in the long exact cohomology sequence of

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{p} \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

For $x \in X$ and $\rho \in R$ we have [NSW00, Proposition 3.9.14]

$$a_x^{\rho} = -\rho(B(x^*)), \tag{26}$$

where $x^* \in X^*$ is the dual to x.

Lemma 8.1 Let K be a number field containing μ_p and S a set of primes containing those above p. For $a \in D_K$ the homomorphism $\Phi = B \otimes \mathrm{id}_{\mu_p}$ is given, abusing notation, by

$$\Phi(a) \otimes \zeta = \mathfrak{a} \otimes \zeta - (\zeta, a)_S,$$

where $\mathfrak{a}^p = a\mathcal{O}_{K,S}$.

Proof. By comparison with the Kummer sequence (8) for $n = p$, the coboundary map B^* in the cohomology of the short exact sequence

$$1 \to \mu_p \to \mu_{p^2} \xrightarrow{p} \mu_p \to 1,$$

is seen to be given by $B^*(a) = \mathfrak{a} \pmod{p}$. We compute $B - (B^* \otimes j)$, where j is the identity map on $\mu_p^{\otimes(-1)}$, in terms of cocycles.

On the one hand, for $f \in H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$, we have that $B(f)$ is the class of

$$(\sigma, \tau) \mapsto \frac{1}{p}(\tilde{f}(\tau) + \tilde{f}(\sigma) - \tilde{f}(\sigma\tau))$$

for an arbitrary lift of f to a map $\tilde{f} \colon \mathcal{G} \to \mathbb{Z}/p^2\mathbb{Z}$. On the other hand, $B^* \otimes j$ takes f to the class of

$$(\sigma, \tau) \mapsto \frac{1}{p}(\chi(\sigma)\tilde{f}(\tau) + \tilde{f}(\sigma) - \tilde{f}(\sigma\tau)),$$

where $\chi\colon \mathcal{G} \to (\mathbb{Z}/p^2\mathbb{Z})^\times$ is the cyclotomic character associated with a root of unity of order p^2. The difference of these cocycles is

$$(\sigma,\tau) \mapsto -\frac{\chi(\sigma)-1}{p} f(\tau),$$

and here $\sigma \mapsto \zeta^{(\chi(\sigma)-1)/p}$ is the Kummer character associated with ζ. By the well-known formula for the cup product of two homomorphisms as their product, we have the result. ■

Again, let us focus on $K = \mathbb{Q}(\zeta_p)$ and $S = \{(1-\zeta)\}$, with p satisfying Vandiver's conjecture. We describe a minimal generating set X of $\mathcal{G}$. Let M denote the set of integers m with $2 \le m \le p$ and either m odd or $(A_K/p)(\omega^{p-m})$ nontrivial. (We take the given interval, instead of $1 \le m \le p-1$, for compatibility with Section 9.) We let M_o and M_e denote the odd and even elements of M, respectively. For each $m \in M \cup \{0\}$, we choose an element $x_m \in \mathcal{G}$ with image generating the ω^m-eigenspace of $\mathrm{gr}^1(\mathcal{G})$, subject to the following normalizations. For $m \in M_o$, we assume that $x_m\alpha_m = \zeta\alpha_m$ for α_m a pth root of η_m, the cyclotomic unit defined in Section 5. For $m \in M_e$, let $\mathfrak{b}_m \in A_K(\omega^{p-m})$ be such that $\mathfrak{b}_m \otimes \zeta$ maps to 1 under the isomorphism (20) (chosen in defining the pairing $\langle\ ,\ \rangle_m$), and let f_{p-m} be the Iwasawa power series for $A_\infty(\omega^{p-m})$ with

$$f_{p-m}((1+p)^s - 1) = L_p(\omega^m, s),$$

for $s \in \mathbb{Z}_p$, where $L_p(\omega^m, s)$ is the p-adic L-function. Choose $b_m \in D_K$ with image in $(D_K/D_K^p)(\omega^{p-m})$ such that

$$b_m \mapsto \mathfrak{b}_m^{f_{p-m}(0)/p} \qquad \text{under } D_K \to A_K[p]. \tag{27}$$

Writing $b_m = \beta_m^p$, we require that $x_m(\beta_m) = \zeta\beta_m$. Finally, for $m = 0$, we let $x_0 = \gamma$ satisfy $\gamma(\xi) = \xi^{1+p}$ for all $\xi \in \mu_{p^\infty}$.

Let

$$X = \{x_m \colon m \in M \cup \{0\}\}.$$

Then X provides a dual basis to the basis of $H^1(\mathcal{G}, \mu_p)$ given by the elements η_m for $m \in M_o$, b_m for $m \in M_e$, and ζ (under the isomorphism $\mu_p \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}$ provided by ζ).

Now fix $r \in M_e$. Recall that $e_{i,r}$ was defined to be $\langle \eta_i, \eta_{r-i}\rangle_r$ for $i \in M_o$. If $i \in M_e$ and the least positive residue j of $r-i$ modulo $p-1$ is also in M_e (so that p divides B_i, B_j and B_r!) we then set $e_{i,r} = \langle b_i, b_j\rangle_r$.

Identify $1+T$ with the restriction of γ to $K_\infty = \mathbb{Q}(\mu_{p^\infty})$. Define $g_{p-r} \in \Lambda \simeq \mathbb{Z}_p[[T]]$ by the relation

$$g_{p-r}((1+p)^s - 1) = f_{p-r}((1+p)^{1-s} - 1) \tag{28}$$

for every $s \in \mathbb{Z}_p$.

Theorem 8.2 For $r \in M_e$ with p satisfying Vandiver's conjecture, there is a relation in $\mathrm{gr}^2(\mathcal{G})$ of the form

$$g_{p-r}(0)x_r + g'_{p-r}(0)[\gamma, x_r] + \sum_{\substack{i<j\in M \\ i+j\equiv r \pmod{p-1}}} e_{i,r}[x_i, x_j] = 0.$$

Proof. Choose a relation $\rho \in \mathcal{F}$ such that the map $H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z}$ corresponding to ρ factors through the negative of the isomorphism (20) used in defining $\langle\ ,\ \rangle_r$. By the expression (25) for ρ, the identities (5) and (26), and eigenspace considerations, we see that

$$\rho \equiv a^{\rho}_{x_r} p x_r + a^{\rho}_{\gamma,x_r}[\gamma, x_r] + \sum_{\substack{i<j\in M \\ i+j\equiv r \pmod{p-1}}} a^{\rho}_{x_i,x_j}[x_i, x_j] \pmod{\mathrm{Fil}^3\mathcal{F}},$$

with $a^{\rho}_{x_i,x_j} = e_{i,r}$.

Let $f = f_{p-r}$ and $g = g_{p-r}$. We claim that

$$a^{\rho}_{x_r} = g(0)/p \pmod{p} \quad \text{and} \quad a^{\rho}_{\gamma,x_r} = g'(0) \pmod{p}.$$

Recalling the notation and statement of (27), Proposition 4.2 and Lemma 8.1 imply that

$$B(x_r^*) \otimes \zeta = \mathfrak{b}_r^{f(0)/p+f'(0)} \quad \text{and} \quad (\zeta, \mathfrak{b}_r)_S = \mathfrak{b}_r^{-f'(0)} \otimes \zeta.$$

Applying $-\rho$, we obtain by (26) and (5) that

$$a^{\rho}_{x_r} = f(0)/p + f'(0) \pmod{p} \quad \text{and} \quad a^{\rho}_{\gamma,x_r} = -f'(0) \pmod{p}.$$

That these agree with $g(0)/p$ and $g'(0)$ follows from the definition (28) of g in terms of f. ■

From our table of the pairings and some basic Bernoulli number computations, we obtain the following corollary of Theorem 7.5 (for a particular choice of x_{32}).

Corollary 8.3 For $p = 37$ and $r = 32$, there is a relation in $\mathrm{gr}^2(\mathcal{G})$ of the form

$$37y - 3[\gamma, y] - 11[x_3, x_{29}] - [x_7, x_{25}] + [x_9, x_{23}] - 2[x_{11}, x_{21}] - 6[x_{13}, x_{19}] \\ - 3[x_{15}, x_{17}] - [x_{31}, x_{37}] + 11[x_{33}, x_{35}] = 0$$

with $y = x_{32}^c$ for some $c \in (\mathbb{Z}/37\mathbb{Z})^\times$.

Proof. The coefficients of all but the first two terms are obtained from the table of calculated pairings. It is easy to check that (see the proof of [Was97, Corollary 10.17])

$$pf'_{p-r}(0) \equiv \frac{B_r}{r} - \frac{B_{r+p-1}}{r-1} \equiv 16p \pmod{p^2}$$

and

$$f_{p-r}(0) = \frac{r-2}{r}B_r - B_{r+p-1} \equiv 14p \pmod{p^2},$$

in order to compute the first two coefficients (up to a scalar relative to the others). ■

9 Relationship with pro-p fundamental groups

We consider the curve $V = \mathbb{P}^1 - \{0, 1, \infty\}$ over $\mathbb{Q}$, and let $\overline{V} = V \times_{\mathbb{Q}} \overline{\mathbb{Q}}$. The natural identification of the absolute Galois group $G_{\mathbb{Q}}$ with $\mathrm{Aut}(\overline{V}/V)$ induces a representation

$$\phi \colon G_{\mathbb{Q}} \to \mathrm{Out}(\pi_1^{(p)}(\overline{V}))$$

where $\pi_1^{(p)}(\overline{V})$ denotes the pro-p fundamental group. As before, let $K = \mathbb{Q}(\mu_p)$ and $S = \{(1-\zeta)\}$. Then ϕ factors through $\mathcal{G}$, and one can put a "weight" filtration $F^m\mathcal{G}$ on $\mathcal{G}$, consisting of the subgroups corresponding to the fixed fields of the various induced representations

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

where $\pi_1 = \pi_1^{(p)}(\overline{V})$ and $\pi_1(m+1)$ is the $(m+1)$th term in the descending central series of π_1. In particular, the fixed field of ϕ_1 is $K_\infty = \mathbb{Q}(\mu_{p^\infty})$. Consider the graded $\mathbb{Z}_p$-Lie algebra

$$\mathfrak{g} = \oplus_{m=1}^{\infty} \mathrm{gr}^m \mathfrak{g}, \quad \text{where} \quad \mathrm{gr}^m \mathfrak{g} = F^m\mathcal{G}/F^{m+1}\mathcal{G}.$$

Then $\mathrm{gr}^m\mathfrak{g}$ is torsion-free of finite $\mathbb{Z}_p$-rank, and $G_{\mathbb{Q}}$ acts on it by the mth power of the p-adic cyclotomic character [Iha86].

Let G denote the closed normal subgroup of $\mathcal{G}$ with fixed field K_∞. Note that $F^mG = F^m\mathcal{G}$ for $m \geq 1$. For odd $m \geq 1$, let $\kappa_m \colon G \to \mathbb{Z}_p(m)$ denote the $\mathrm{Gal}(K_\infty/\mathbb{Q})$-equivariant homomorphism dual to an appropriate sequence of cyclotomic p-units as defined in [Iha02] and known to be nontrivial by [Sou84]. Then κ_m induces a nontrivial map $\kappa_m \colon \mathrm{gr}^m\mathfrak{g} \to \mathbb{Z}_p$ for odd $m \geq 3$ [Iha89, Proposition 1]. Let $\tilde{\sigma}_m$ denote an element of F^mG such that $v_p(\kappa_m(\tilde{\sigma}_m))$ is minimal. Then $\tilde{\sigma}_m$ restricts to a nontrivial element $\sigma_m \in \mathrm{gr}^m\mathfrak{g}$.

Let $\mathfrak{h}$ denote the Lie subalgebra of $\mathfrak{g}$ generated by the σ_m. Hain and Matsumoto have proven a conjecture of Deligne that $\mathfrak{g} \subset \mathfrak{h} \otimes \mathbb{Q}_p$ [HM] (see also [Gon01, Section 3.7] for a description of motivic arguments of Beilinson and Deligne that lead to this result). Deligne has further conjectured that $\mathfrak{g} \otimes \mathbb{Q}_p$ is free on the σ_m. On the other hand, Sharifi [Sha02, Theorem 1.3] has shown that Greenberg's conjecture, as described in Section 10, implies that $\mathfrak{g}$ itself is not free on the σ_m if p is irregular. Deligne's conjecture would then imply that $\mathfrak{h} \neq \mathfrak{g}$. In this section, we describe relations in $\mathfrak{g}$, conjecturally nontrivial, in terms of the cup product $(\ ,\ )_S$ (Theorem 9.1). Taking $p = 691$ as an example, we see in Theorem 9.11 that the nontriviality of $\langle\ ,\ \rangle_{12}$ is, in fact, equivalent to $\mathrm{gr}^{12}\mathfrak{h} \neq \mathrm{gr}^{12}\mathfrak{g}$.

Let $\mathfrak{s}$ the free $\mathbb{Z}_p$-Lie algebra on generators s_i with $i \geq 3$ odd, and let $\psi \colon \mathfrak{s} \to \mathfrak{g}$ denote the map given by $s_i \mapsto \sigma_i$ for each i. Deligne's conjecture is equivalent to the statement that ψ is injective. We say that Deligne's conjecture holds in degree i if $\mathrm{gr}^i\psi$ is injective.

Assume p satisfies Vandiver's Conjecture for the remainder of the section. Recall the notation of Section 8. Let Δ be a choice of lift of $\mathrm{Gal}(K/\mathbb{Q})$ to a subgroup of $\mathcal{G}$ of order $p-1$. We may choose x_m for each $m \in M \cup \{0\}$ such that

$$\delta x_m \delta^{-1} = x_m^{\omega(\delta)^m}$$

for each $\delta \in \Delta$ by [Sha02, Lemma 2.1], which immediately forces $x_m \in F^m G$ for $m \in M$. Furthermore, for $m \in M_o$, we may take $\tilde{\sigma}_m = x_m$. For each $m \in M$, we let $\bar{x}_m$ denote the image of x_m in $\mathrm{gr}^m \mathfrak{g}$, which for even m may or may not be trivial.

Recall that $\mathrm{Fil}^k \mathcal{G}$ was defined as the descending p-central series of $\mathcal{G}$. We define the induced filtration on $\mathfrak{g}$:

$$\underline{\mathrm{Fil}}^k \mathfrak{g} = \bigoplus_{m=1}^{\infty} \frac{\mathrm{Fil}^k \mathcal{G} \cap F^m G}{\mathrm{Fil}^k \mathcal{G} \cap F^{m+1} G},$$

which differs from the descending central p-series on $\mathfrak{g}$.

Theorem 9.1 Let $m \in M_e$ for p satisfying Vandiver's conjecture. Then there is a relation in $\mathrm{gr}^m \mathfrak{g}$ of the form

$$B_m \bar{x}_m \equiv m \sum_{\substack{i<j \in M \\ i+j=m}} e_{i,m} [\bar{x}_i, \bar{x}_j] \pmod{\mathrm{gr}^m \underline{\mathrm{Fil}}^3 \mathfrak{g}}, \qquad (29)$$

where the $e_{i,m}$ are as defined in Section 8.

Proof. We note that for $x \in F^i G$, we have

$$x^{\gamma - 1} \equiv x^{(1+p)^i - 1} \bmod F^{i+1} G, \qquad (30)$$

since $\mathrm{gr}^i \mathfrak{g}$ has Tate twist i. Let $g = g_{p-m}$ be as in (28). Since

$$g((1+p)^m - 1) = L_p(\omega^m, 1-m) = (p^m - 1)\frac{B_m}{m},$$

applying (30), we obtain

$$x_m^{g(T)} \equiv x_m^{(p^m-1)B_m/m} \pmod{F^{m+1} G}.$$

The result now follows from Theorem 8.2 by reducing its relation modulo the image of $F^{m+1} G$ in $\mathrm{gr}^2(\mathcal{G})$. ■

We derive some consequences of this result regarding the freeness and generation of $\mathfrak{g}$. In order to do so, we must compare the filtration $\underline{\mathrm{Fil}}^{\cdot} \mathfrak{g}$ on $\mathfrak{g}$ with the descending central p-series on the simpler Lie algebra $\mathfrak{h}$. This will proceed in several steps. We begin with the following lemma.

Lemma 9.2 Let $\mathcal{H}$ be the pro-p subgroup of $\mathcal{G}$ generated by the x_i for $i \in M_o \cup \{0\}$. Let H be the pro-p subgroup of G generated by the $\tilde{\sigma}_i$ for odd $i \geq 3$. Then $\mathcal{H}$ and H are freely generated as pro-p groups on these sets of elements.

Proof. Hain and Matsumoto [HM, Theorems 7.3, 7.4] have demonstrated the existence of a filtration on G with graded quotient a $\mathbb{Z}_p$-Lie algebra that injects into a free graded $\mathbb{Q}_p$-Lie algebra on the images of the $\tilde{\sigma}_i$ in degree i. As remarked by Ihara [Iha02, Section 6], this implies that H must be free on the $\tilde{\sigma}_i$. By [Sha02, Lemma 3.1c] (as in the proof of Theorem 1.3 therein), this implies the desired freeness on the generators of $\mathcal{H}$. ■

For Z a pro-p group or $\mathbb{Z}_p$-Lie algebra, we let $Z(k)$ denote the kth term in its descending central series and $\mathrm{Fil}^k Z$ the kth term in its descending central p-series. Next, we compare $\mathrm{Fil}^{\cdot}\mathfrak{h}$ with the filtration induced on $\mathfrak{h}$ by $\mathrm{Fil}^{\cdot}H$. Note that we use H, as opposed to $\mathcal{H}$ (at this point), since the weight filtration is defined by a filtration on H.

Lemma 9.3 Let m and k be positive integers. If $\mathrm{gr}^m\psi$ is injective for $i < m$ then

$$\mathrm{gr}^m\mathfrak{h}(k) \simeq \frac{H(k) \cap F^m G}{H(k) \cap F^{m+1} G}$$

and

$$\mathrm{gr}^m \mathrm{Fil}^k \mathfrak{h} \simeq \frac{\mathrm{Fil}^k H \cap F^m G}{\mathrm{Fil}^k H \cap F^{m+1} G}.$$

Proof. By definition of $\mathfrak{h}$, we may lift any element of $\mathrm{gr}^m\mathfrak{h}(k)$ to an element of $H(k) \cap F^m G$. We must show that, conversely, an element of $H(k) \cap F^m G$ projects to an element of $\mathrm{gr}^m\mathfrak{h}(k)$. By the injectivity of $\mathrm{gr}^i\psi$ in weights $i < m$, the group $H/(H \cap F^m G)$ is isomorphic to the free pro-p subgroup on the $\tilde{\sigma}_i$ modulo the pro-p subgroup generated by commutators $[\tilde{\sigma}_{m_1}, \ldots [\tilde{\sigma}_{m_{j-1}}, \tilde{\sigma}_{m_j}] \ldots]$ with $\sum m_i \geq m$ [Iha02, Section 6]. Using the freeness of H in Lemma 9.2, $H(k) \cap F^m G$ is then the normal pro-p subgroup of H generated by those among the above commutators with $j = k$, which clearly project to elements of $\mathrm{gr}^m\mathfrak{h}(k)$. The same arguments hold with the descending central series terms replaced by descending central p-series terms. ■

Now we compare the filtration $\underline{\mathrm{Fil}}^{\cdot}\mathfrak{g}$ induced by $\mathrm{Fil}^{\cdot}\mathcal{G}$ with the filtration on $\mathfrak{h}$ induced by $\mathrm{Fil}^{\cdot}\mathcal{H}$, since $\mathcal{G}$ is more closely related to $\mathcal{H}$ than to H.

Lemma 9.4 Let m and k be positive integers with $m \leq p+r-2$, with r the minimal element of M_e. If $\mathrm{gr}^i\psi$ is surjective for $i \leq m$, then

$$\mathrm{gr}^m \underline{\mathrm{Fil}}^k \mathfrak{g} \simeq \frac{\mathrm{Fil}^k \mathcal{H} \cap F^m G}{\mathrm{Fil}^k \mathcal{H} \cap F^{m+1} G}.$$

Proof. We first show that $x_r \in [H, H] \cdot F^{m+1} G$ if $r \in M_e$ with $r \leq m$. Note that since r is even, $\mathrm{gr}^r\mathfrak{h} = \mathrm{gr}^r[\mathfrak{h}, \mathfrak{h}]$ by definition. Since $x_r \in F^r G$ and $\mathrm{gr}^r\psi$ is surjective, we have $\bar{x}_r \in \mathrm{gr}^r[\mathfrak{h}, \mathfrak{h}]$. Thus, we obtain $x_r \in [H, H] \cdot F^{r+1} G$. Now assume that $x_r \in [H, H] \cdot F^l G$ for some $l \not\equiv r \pmod{p-1}$ with $l \leq m$. We remark that

$$\frac{[H, H] \cdot F^l G}{[H, H] \cdot F^{l+1} G} \simeq \frac{F^l G}{([H, H] \cap F^l G) \cdot F^{l+1} G} \simeq \mathrm{gr}^l \mathfrak{h}^{ab},$$

and $\mathrm{Gal}(K_\infty/\mathbb{Q})$ acts on the latter group by the lth power of the cyclotomic character. On the other hand,

$$\delta x_r \delta^{-1} = x_r^{\omega(\delta)^r} \qquad \text{for } \delta \in \Delta,$$

and this forces $x_r \in [H, H] \cdot F^{l+1}G$. By recursion, since $m < r + p - 1$, we have $x_r \in [H, H] \cdot F^{m+1}G$.

For a tuple $\mathrm{m} = (m_1, \ldots, m_j)$ with $m_i \in M \cup \{0\}$ for each i, and $m_{j-1} < m_j$ if $j \geq 2$, let

$$x_{\mathrm{m}} = [x_{m_1}, \ldots, [x_{m_{j-1}}, x_{m_j}] \ldots].$$

Then $\mathrm{Fil}^k \mathcal{G}$ is generated as a normal subgroup by those elements of the form $p^{k-j} x_{\mathrm{m}}$, with m a tuple of length $j \leq k$. Since $x_r \in [H, H] \cdot F^{m+1}G$ for $r \in M_e$, the images of those elements $p^{k-j} x_{\mathrm{m}}$ with some $m_i \in M_e$ are redundant as elements of the induced generating set of $\mathrm{Fil}^k \mathcal{G} / (\mathrm{Fil}^k \mathcal{G} \cap F^{m+1}G)$, and hence $\mathrm{Fil}^k \mathcal{H}$ surjects onto the latter quotient, finishing the proof. ■

In the following proposition, we conclude our discussion of filtrations by filling in the intermediate comparison between the filtrations on $\mathfrak{h}$ induced by $\mathrm{Fil}^{\cdot} H$ and $\mathrm{Fil}^{\cdot} \mathcal{H}$. Note that these filtrations will always disagree in sufficiently large weight, since for each k, there exists i sufficiently large such that $\tilde{\sigma}_i \in \mathrm{Fil}^k \mathcal{H}$.

Proposition 9.5 Let m and k be positive integers with $m \leq p+1$. If $\mathrm{gr}^i \psi$ is bijective for $i \leq m$, then

$$\mathrm{gr}^m \underline{\mathrm{Fil}}^k \mathfrak{g} = \mathrm{gr}^m \mathrm{Fil}^k \mathfrak{h}.$$

Proof. By the second isomorphism in Lemma 9.3 and the isomorphism of Lemma 9.4, it suffices to show that

$$\frac{\mathrm{Fil}^k H \cap F^m G}{\mathrm{Fil}^k H \cap F^{m+1} G} \simeq \frac{\mathrm{Fil}^k \mathcal{H} \cap F^m G}{\mathrm{Fil}^k \mathcal{H} \cap F^{m+1} G}.$$

We clearly have that $\mathrm{Fil}^k H \subseteq \mathrm{Fil}^k \mathcal{H}$, and we are left to verify that

$$(\mathrm{Fil}^k \mathcal{H} \cap F^m G) \cdot F^{m+1} G \subseteq (\mathrm{Fil}^k H \cap F^m G) \cdot F^{m+1} G \tag{31}$$

From the generating set $\{x_i : i \in M_o \cup \{0\}\}$ of $\mathcal{H}$, we may define a generating set $\{x_{i,n} : i \in M_o,\ n \geq 0\}$ of H, taking $x_{i,0} = x_i$ and

$$x_{i,n+1} = \gamma x_{i,n} \gamma^{-1} x_{i,n}^{-(1+p)^{i+n(p-1)}}.$$

By [Sha02, Lemma 3.1b], the $x_{i,n}$ freely generate H as a pro-p group. Note that $x_{i,n} \in \mathrm{Fil}^{n+1} \mathcal{H} - \mathrm{Fil}^{n+2} \mathcal{H}$ by Lemma 9.2. Thus $H \cap \mathrm{Fil}^k \mathcal{H}$ is generated as a normal pro-p subgroup by those elements of the form

$$p^{k-J} [x_{m_1,n_1}, \ldots, [x_{m_{j-1},n_{j-1}}, x_{m_j,n_j}] \ldots]$$

with $m_t \in M_o$, $n_t \geq 0$, and $J = j + \sum n_t$ for $1 \leq t \leq j$. Furthermore, it follows as in [Sha02, Lemma 2.2], that the elements $\tilde{\sigma}_i$ with $i \geq 3$ odd may be chosen such that

$$x_{i,n} \tilde{\sigma}_{i+n(p-1)}^{-1} \in [H, H] \cap \mathrm{Fil}^{n+1} \mathcal{H}.$$

Therefore, $H \cap \mathrm{Fil}^k \mathcal{H}$ is generated as a normal pro-p subgroup by the elements

$$p^{k-J} [\tilde{\sigma}_{m_1+n_1(p-1)}, \ldots, [\tilde{\sigma}_{m_{j-1}+n_{j-1}(p-1)}, \tilde{\sigma}_{m_j+n_j(p-1)}] \ldots],$$

with m_t, n_t and J as before. Since $\tilde{\sigma}_{i+n(p-1)} \in F^{m+1}G$ if $n \geq 1$, to show (31), it suffices to verify that

$$p^{k-j}[\tilde{\sigma}_{m_1}, \ldots, [\tilde{\sigma}_{m_{j-1}}, \tilde{\sigma}_{m_j}] \ldots] \in \mathrm{Fil}^k H,$$

but this is true by definition. ■

Combining Proposition 9.5 with Theorem 9.1, we obtain the following.

Proposition 9.6 Assume that $e_{i,m}$ is nonzero for some $i \in M_o$ with $i < m/2$ and $m \in M_e$. Then $\mathfrak{g}$ is not freely generated by the elements σ_i. In fact, there is an $i \leq m$ for which $\mathrm{gr}^i\psi$ is not is an isomorphism.

Proof. Assume that $\mathrm{gr}^i\psi$ is bijective for all $i \leq m$, so the relation (29) holds modulo $\mathrm{gr}^m\mathrm{Fil}^3\mathfrak{h}$ by Proposition 9.5. Then $B_m\bar{x}_m \in p \cdot \mathrm{gr}^m\mathfrak{h}$ by the surjectivity of $\mathrm{gr}^m\psi$. Furthermore, for any $r \in M_e$ with $r < m$, we have $\bar{x}_r \in [\mathfrak{h}, \mathfrak{h}]$ by the surjectivity of $\mathrm{gr}^r\psi$, as in the proof of Lemma 9.4. Since some $e_{i,m} \neq 0$, reducing (29) modulo $p\mathfrak{h} + \mathfrak{h}(3)$ exhibits a contradiction of the injectivity of $\mathrm{gr}^m\psi$. ■

This can be improved as follows, when m is the smallest positive even integer such that p divides B_m.

Theorem 9.7 Let m be the minimal element of M_e for an irregular prime p satisfying Vandiver's conjecture. Assume that Deligne's conjecture holds in degrees $i \leq m$. Then $\mathrm{gr}^m\mathfrak{g} = \mathbb{Z}_p\bar{x}_m + \mathrm{gr}^m\mathfrak{h}$ and $\mathrm{gr}^m\mathfrak{g}^{\mathrm{ab}}$ is generated by the image of $\bar{x}_m$. Furthermore, if $e_{i,m}$ is nonzero for some $i \in M_o$ with $i < m/2$, then in fact $\mathrm{gr}^m\mathfrak{h} \subsetneq \mathrm{gr}^m\mathfrak{g}$ and $\mathrm{gr}^m\mathfrak{g}^{\mathrm{ab}}$ is nontrivial.

Proof. First, we remark that $\mathrm{gr}^i\psi$ is not only injective, but bijective in degrees $i < m$ by [Iha02, Theorem I.2(ii)]. From this, it is easy to see that $\bar{x}_m$ and $\mathrm{gr}^m\mathfrak{h}$ generate $\mathrm{gr}^m\mathfrak{g}$. That is, $\mathrm{gr}^m[\mathfrak{g}, \mathfrak{g}] = \mathrm{gr}^m[\mathfrak{h}, \mathfrak{h}]$ by the bijectivity in lower degrees, and $\mathrm{gr}^m\mathfrak{g}^{\mathrm{ab}}$ is generated by the image of $\bar{x}_m$ as shown, e.g, in the proof of [Sha02, Theorem 4.1]. By Proposition 9.6, we know that $\mathrm{gr}^m\psi$ is not bijective, hence not surjective, finishing the proof. ■

Let $\mathcal{D}$ denote Ihara's stable derivation algebra [Iha02], which is a graded Lie algebra over $\mathbb{Z}$. More specifically, it is a Lie algebra of derivations of the free graded Lie algebra $\mathcal{F}$ on two variables x and y over $\mathbb{Z}$ and consists of $D \in \mathrm{gr}^m\mathcal{D}$ such that $D(x) = 0$ and $D(y) = [y, f_D]$ with $f_D \in \mathrm{gr}^m\mathcal{F}$ satisfying certain relations.

Ihara has shown that there is an injection of graded $\mathbb{Z}_p$-Lie algebras [Iha89]

$$\iota\colon \mathfrak{g} \to \mathcal{D} \otimes \mathbb{Z}_p.$$

He has also made the following conjecture.

Conjecture 9.8 (Ihara) The map $\mathrm{gr}^m\iota$ is an isomorphism for $m < p$.

Consider the map

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

(denoted $\mathrm{gr}^m(c)$ in [Iha02]) given by

$$f_D \equiv \lambda_m(D)[x, [x, \dots [x, y] \dots]] \pmod{\text{terms of degree } \geq 2 \text{ in } y}.$$

We remark that $\lambda_m = 0$ if m is even or $m = 1$. Extending λ_m $\mathbb{Z}_p$-linearly, we may precompose with $\mathrm{gr}^m \iota$ to obtain a map $\lambda_m^{(p)}$ satisfying the formula [Iha89, Iha02]

$$\kappa_m = (p^{m-1} - 1)(m-1)!\lambda_m^{(p)} \tag{32}$$

for odd $m \geq 3$.

Lemma 9.9 For $m \in M_o$, there exists $D_m \in \mathrm{gr}^m \mathcal{D}$ such that $\lambda_m(D_m)$ is the positive generator of the image of λ_m and

$$D_m \equiv -(m-1)!\lambda_m(D_m)\iota(\sigma_m) \pmod{p\mathcal{D} \otimes \mathbb{Z}_p}. \tag{33}$$

Proof. We need only show that the two defining properties of D_m are consistent. If $m \leq p$, we have

$$\lambda_m^{(p)}(\sigma_m) \equiv -1/(m-1)! \pmod{p}$$

by equation (32), and consistency follows from applying λ_m to both sides of (33). ■

Ihara has conjectured the existence of p-torsion in the mth graded piece of $\mathcal{D}^{\mathrm{ab}}$ when p divides B_m [Iha02, Conjecture II.2]. We will focus on a case in which the stable derivation algebra has been calculated sufficiently to allow comparison with the relation in Theorem 9.1. That is, when $p = 691$ and $m = 12$, Ihara has exhibited a relation

$$691\delta = 2[D_3, D_9] - 27[D_5, D_7] \tag{34}$$

for some $\delta \in \mathrm{gr}^{12}\mathcal{D}$. On the other hand, Matsumoto has shown that $[D_3, D_9]$ and $[D_5, D_7]$ form a basis of $\mathrm{gr}^{12}\mathcal{D} \otimes \mathbb{Q}$ and generate $\mathrm{gr}^{12}[\mathcal{D}, \mathcal{D}]$ [Mat95, Appendix A], which implies that $\delta \notin [\mathcal{D}, \mathcal{D}]$. Furthermore, he has verified that the image of δ generates $\mathrm{gr}^{12}\mathcal{D}^{\mathrm{ab}}$.

Proposition 9.10 For $p = 691$, Conjecture 9.8 in degree $m = 12$ is equivalent to the statement that $\mathrm{gr}^{12}\mathfrak{h} \subsetneq \mathrm{gr}^{12}\mathfrak{g}$.

Proof. We remark that $\mathrm{gr}^i \psi$ is injective for $i \leq 11$, as follows directly from the main results of [Iha89]. By Theorem 9.7, the top row of the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{gr}^{12}[\mathfrak{h}, \mathfrak{h}] & \longrightarrow & \mathrm{gr}^{12}\mathfrak{g} & \longrightarrow & \mathrm{gr}^{12}\mathfrak{g}^{\mathrm{ab}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow {\scriptstyle \mathrm{gr}^{12}\iota} & & \downarrow & & \\
0 & \longrightarrow & \mathrm{gr}^{12}[\mathcal{D}, \mathcal{D}] \otimes \mathbb{Z}_{691} & \longrightarrow & \mathrm{gr}^{12}\mathcal{D} \otimes \mathbb{Z}_{691} & \longrightarrow & \mathrm{gr}^{12}(\mathcal{D} \otimes \mathbb{Z}_{691})^{\mathrm{ab}} & \longrightarrow & 0
\end{array}$$

is exact and $\mathrm{gr}^{12}\mathfrak{g}^{\mathrm{ab}}$ is nonzero if and only if $\mathrm{gr}^{12}\mathfrak{h} \subsetneq \mathrm{gr}^{12}\mathfrak{g}$. The bottom row is exact by definition. Since $\mathrm{gr}^{12}[\mathcal{D},\mathcal{D}]$ is generated by $[D_3, D_9]$ and $[D_5, D_7]$, Lemma 9.9 implies that the leftmost vertical arrow is a surjection. Since ι is injective, the rightmost vertical arrow is now forced to be an injection as well. Furthermore, noting (34) and Matsumoto's results discussed after it, we have that $\mathrm{gr}^{12}\mathcal{D}^{\mathrm{ab}}$ is cyclic of order 691. Therefore, $\mathrm{gr}^{12}\iota$ is an isomorphism if and only if $\mathrm{gr}^{12}\mathfrak{g}^{\mathrm{ab}}$ is nonzero, hence the result. ■

By Proposition 9.10, the following shows that Conjectures 5.3 and 9.8 are equivalent for the irregular pair $(691, 12)$.

Theorem 9.11 The pairing $\langle\ ,\ \rangle_{12}$ is nontrivial for $p = 691$ if and only if $\mathrm{gr}^{12}\mathfrak{h} \subsetneq \mathrm{gr}^{12}\mathfrak{g}$. In this case, there is a relation in $\mathrm{gr}^{12}\mathfrak{g}$,

$$[\sigma_3, \sigma_9] \equiv 50[\sigma_5, \sigma_7] \pmod{691}. \tag{35}$$

Proof. According to [Iha02], we have $\lambda_m(D_m) = 1, 2, 16, 144$ for $m = 3, 5, 7, 9$ respectively. If $\mathrm{gr}^{12}\mathfrak{h} \subsetneq \mathrm{gr}^{12}\mathfrak{g}$, then the injectivity of ι implies that δ is contained in $\iota(\mathrm{gr}^{12}\mathfrak{g})$. By Theorem 9.7 and Lemma 9.9, equation (34) becomes

$$691c \cdot \bar{x}_{12} \equiv 190[\sigma_3, \sigma_9] + 174[\sigma_5, \sigma_7] \pmod{691[\mathfrak{g}, \mathfrak{g}]} \tag{36}$$

in $\mathrm{gr}^{12}\mathfrak{g}$ for some $c \not\equiv 0 \pmod{691}$. This yields (35). By the linear independence of $[\sigma_3, \sigma_9]$ and $[\sigma_5, \sigma_7]$, this equation must agree with that of (29) (noting Proposition 9.5, and after multiplication by an appropriate scalar). Therefore, by Theorem 9.1, the pairing $\langle\ ,\ \rangle_{12}$ is nontrivial.

On the other hand, the coefficients in equation (36) of $[\sigma_i, \sigma_{12-i}]$ equal the values of the pairing $e_{i,12}$ up to a constant scalar multiple by the computation yielding Theorem 5.1. Hence, by Theorem 9.7, nontriviality of $\langle\ ,\ \rangle_{12}$ implies that $\mathrm{gr}^{12}\mathfrak{h} \subsetneq \mathrm{gr}^{12}\mathfrak{g}$. ■

In general, we expect that for m minimal such that p divides B_m, a determination of the structure of $\mathrm{gr}^i\mathcal{D}$ with $i \le m$, together with a computation of a unique possibility for the pairing $\langle\ ,\ \rangle_m$ on $\mathcal{C} \times \mathcal{C}$ up to possibly trivial scalar (to show $e_{i,m} \neq 0$ for some $i \in M_o$ with $i < m/2$ if $\langle \mathcal{C}, \mathcal{C} \rangle_m \neq 0$), would yield (in essence) that Conjectures 5.3, 9.8, and the statement that $\mathrm{gr}^m\mathfrak{g} \subsetneq \mathrm{gr}^m\mathfrak{h}$, are equivalent as well.

10 Relationship with Greenberg's conjecture

Let K be a number field, K_∞ the compositum of all $\mathbb{Z}_p$-extensions of K, $\tilde{\Gamma} = \mathrm{Gal}(K_\infty/K)$ and $\tilde{\Lambda} = \mathbb{Z}_p[[\tilde{\Gamma}]]$. Let L_∞ be the maximal abelian unramified pro-p extension of K_∞, and let M_∞ be the maximal abelian p-ramified pro-p extension of K_∞. Then $X_\infty = \mathrm{Gal}(L_\infty/K_\infty)$ and $Y_\infty = \mathrm{Gal}(M_\infty/K_\infty)$ are $\tilde{\Lambda}$-modules. We say that a $\tilde{\Lambda}$-module is pseudo-null if its annihilator has height at least 2. Greenberg has made the following conjecture [Gre01, Conjecture 3.5].

Conjecture 10.1 (Greenberg) X_∞ is pseudo-null as a $\tilde{\Lambda}$-module.

For a prime ideal $\mathfrak{p}$ of K lying above p, let $r_{\mathfrak{p}}$ be the integer such that the decomposition group $\tilde{\Gamma}_{\mathfrak{p}} \subset \tilde{\Gamma}$ is isomorphic to $\mathbb{Z}_p^{r_{\mathfrak{p}}}$. In certain cases, Greenberg's conjecture has an equivalent form in terms of the torsion in Y_∞. For example, we have the following theorem, which is [McC01, Corollary 14] (see also [LNQD00]).

Theorem 10.2 (McCallum) Assume that $r_{\mathfrak{p}} \geq 2$ for all primes $\mathfrak{p}$ above p and that $\mu_{p^\infty} \subset K_\infty$. Then Greenberg's conjecture holds if and only if Y_∞ is $\tilde{\Lambda}$-torsion free.

Let $\mathcal{G}$ be the Galois group of the maximal p-ramified pro-p extension of K and let $\tilde{G} \subset \mathcal{G}$ be the Galois group of the same extension over K_∞. Let $I(\mathcal{G})$ denote the augmentation ideal of $\mathbb{Z}_p[[\mathcal{G}]]$. Then the module $Z = H_0(\tilde{G}, I(\mathcal{G}))$ has torsion subgroup isomorphic to that of Y_∞ (see [McC01, Theorem 10]).

Consider a free presentation of $\mathcal{G}$ as in (3) with minimal sets of generators and relations X and R as in Section 1. The presentation gives rise to an exact sequence [NQD84, McC01]

$$0 \to \tilde{\Lambda}^s \xrightarrow{\phi} \tilde{\Lambda}^g \to Z \to 0, \tag{37}$$

where $s = |R|$ and $g = |X|$. Let h denote the $\mathbb{Z}_p$-rank of $\tilde{\Gamma}$ (so $h \geq g - s$). Write $\tilde{\Lambda} = \mathbb{Z}_p[[T]]$, where $T = (T_1, \ldots, T_h)$ and $1 + T_i$ is the restriction of a generator $x_i \in X$. Furthermore, we choose the remaining elements $x_i \in X$ with $h + 1 \leq i \leq g$ such that the image of x_i in $\mathcal{G}^{\mathrm{ab}}$ is torsion. If

$$f = (f_1, \ldots, f_g) \in \tilde{\Lambda}^g,$$

we also use the notation

$$f = \sum_{i=1}^{g} f_i \, dx_i.$$

We briefly describe the map ϕ in (37) (see [NQD84] for details). Fox [Fox53] defines a derivative (extended to pro-p groups in [NQD84])

$$D \colon \mathbb{Z}_p[[\mathcal{F}]] \to I(\mathcal{F})$$

satisfying $D(x) = x - 1$ for $x \in X$ and a certain non-abelian Leibniz condition that yields, for example,

$$D[x, y] = (1 - xyx^{-1})(x - 1) + (x - [x, y])(y - 1)$$

and

$$Dx^q = \left(\sum_{i=0}^{q-1} x^i \right) (x - 1)$$

for q a power of p. We also have the map

$$\theta \colon I(\mathcal{F}) = \sum \mathbb{Z}_p[[\mathcal{F}]](x_i - 1) \to \sum \tilde{\Lambda} dx_i = \tilde{\Lambda}^g.$$

We remark that the map $\Phi = \theta \circ D$ factors through $\mathbb{Z}_p[[\mathcal{F}/\mathcal{F}'']]$ (where $N' = [N, N]$ for a group N). The map ϕ in the presentation (37) is then obtained on basis elements of $\tilde{\Lambda}^s$ by identifying them with elements of R, considering these as elements of $\mathcal{F}$ via the presentation (1), and then composing with Φ. Roughly speaking, the map ϕ is the Jacobian matrix of the relations.

We choose R such that each $r_k \in R$ has the form

$$r_k \equiv \left(\prod_{1 \le i < j \le g} [x_i, x_j]^{f^k_{i,j}} \right) \cdot x_k^{l_k} \pmod{\mathcal{F}''}, \tag{38}$$

with $g - s + 1 \le k \le g$, where l_k is a power of p for $k > h$ and $l_k = 0$ for $k \le h$ and where $f^k_{i,j} \in \mathbb{Z}_p[[\mathcal{F}^{\rm ab}]]$. Each $f^k_{i,j}$ may be chosen not to involve any x_a with $i < a < j$ in order to make the expression unique. Via the surjection $\mathbb{Z}_p[[\mathcal{F}^{\rm ab}]] \to \tilde{\Lambda}$, we obtain elements $f^k_{i,j}(T)$ of $\tilde{\Lambda}$, in which x_i is replaced by $1 + T_i$ if $1 \le i \le h$ and 1 otherwise. We find

$$\Phi(r_k) = \sum_{1 \le i < j \le h} f^k_{i,j}(T)(-T_j\,dx_i + T_i\,dx_j) + \sum_{1 \le i \le h < j \le g} f^k_{i,j}(T) T_i\,dx_j + l_k\,dx_k. \tag{39}$$

Let us assume from now on that p is odd. We require the following lemma.

Lemma 10.3 Let K be a number field containing μ_p, and let $\alpha \in K^\times$ be a universal norm from the extension $K(\mu_{p^\infty})/K$. Then the torsion in $\mathcal{G}^{\rm ab}$ acts trivially on any pth root of α.

Proof. We may assume that $\alpha \notin \mu_{p^\infty} \cdot K^{\times p}$. Let $K_n = K(\mu_{p^n})$, and let $\alpha_n \in K_n^\times$ be the elements of a norm-compatible sequence with $\alpha_1 = \alpha$. Set

$$\alpha'_n = \prod_{\sigma \in {\rm Gal}(K_n/K)} \sigma(\alpha_n)^{i_{\sigma,n}},$$

with $i_{\sigma,n}$ the minimal nonnegative integer satisfying $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{i_{\sigma,n}^{-1}}$. Then $\alpha'_1 = \alpha$, and

$$\alpha'_{n+1} {\alpha'_n}^{-1} \in K_{n+1}^{\times p^n}.$$

Since $\alpha \notin \mu_{p^\infty} \cdot K^{\times p}$, we have that $\alpha'_n \notin K(\mu_{p^\infty})^{\times p}$. By Kummer theory, the sequence (α'_n) defines a nontrivial element of $H^1(G, \varprojlim \mu_{p^n})$, with G as in Section 9, on which

$$\Gamma = {\rm Gal}(K(\mu_{p^\infty})/K)$$

acts by the cyclotomic character. Hence, by a choice of isomorphism

$$\lambda \colon \mathbb{Z}_p(1) \xrightarrow{\sim} \varprojlim \mu_{p^n}$$

of $\mathcal{G}$-modules and the fact that G acts trivially on $\mathbb{Z}_p(1)$, it defines an element of $H^1(G, \mathbb{Z}_p)^\Gamma$. Since Γ has cohomological dimension 1, this element is the image under restriction of an element $\kappa \in {\rm Hom}(\mathcal{G}, \mathbb{Z}_p)$. Furthermore, the map induced by the quotient $\mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$ takes κ to the Kummer character associated with α, viewed as an element of ${\rm Hom}(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$ via λ (as K contains μ_p). Since κ has torsion-free image, the lemma is proven. ■

We remark that all universal norms for the cyclotomic $\mathbb{Z}_p$-extension are p-units. We are now ready to prove the following consequence of nontriviality of the pairing.

Theorem 10.4 Let K be a number field containing μ_p for an odd prime p, and let S be the set of primes above p and any real archimedean places. Suppose that

$$\dim_{\mathbb{Z}/p\mathbb{Z}} H^2(G_{K,S}, \mathbb{Z}/p\mathbb{Z}) = 1.$$

If the pairing $(\alpha, \beta)_S$ is nontrivial on two universal norms α, β for the extension $K(\mu_{p^\infty})/K$, then Greenberg's conjecture holds for K.

Proof. By Lemma 10.3 and equation (5), the nontriviality of the cup product implies that

$$f^g_{a,b}(0) \not\equiv 0 \pmod{p},$$

with $f^g_{a,b}$ as in (38) for some a and b with $1 \le a < b \le h$. Set $\mathfrak{m} = (p, T)\tilde{\Lambda}$. From equation (39), we see that

$$\Phi(r_g) \equiv \sum_{1 \le i < j \le h} f^g_{i,j}(0)(-T_j\, dx_i + T_i\, dx_j) + \delta(l_g + \sum_{1 \le i \le g-1} f^g_{i,g}(0)T_i)dx_g \pmod{\mathfrak{m}^2}, \quad (40)$$

where $\delta = 1$ if $h = g-1$ and $\delta = 0$ if $h = g$. Equation (40) therefore shows that the coefficients of dx_a and dx_b in $\Phi(r_g)$ are both nontrivial modulo $\mathfrak{m}^2$, with only the latter involving a linear term in T_a that is nonzero modulo p. Hence, one cannot factor a non-unit polynomial out of $\Phi(r_g)$, and Z has no torsion. ∎

Let us specialize to the case $K = \mathbb{Q}(\mu_p)$ by way of example. Assume that A_K has order p. In [McC01, Theorem 1] (see also [Mar]), it is shown that Greenberg's conjecture holds if $f(0) \not\equiv -pf'(0) \pmod{p^2}$, where f denotes a characteristic power series of the p-part of the class group of $\mathbb{Q}(\mu_{p^\infty})$. Essentially, this is a condition on the last term in the expression (40). (By the discussion in Section 8, it is exactly that $l_g \not\equiv 0 \pmod{p^2}$.) Since that term involves only dx_g, the method of analysis in Theorem 10.4 seems incapable of giving an alternate proof of McCallum's result. On the other hand, since cyclotomic p-units are universal norms, we have the following variation on McCallum's result which replaces the condition on the characteristic power series with a condition on the pairing.

Corollary 10.5 Let $K = \mathbb{Q}(\mu_p)$, and assume that A_K is a cyclic group. If the restriction of $(\ ,\ )_S$ to the cyclotomic p-units is nontrivial, then Greenberg's conjecture holds for K.

Using Theorem 7.5, this gives another proof of Greenberg's conjecture for $\mathbb{Q}(\mu_{37})$.

References

[BCE+01] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and M. A. Shokrollahi, Irregular primes and cyclotomic invariants to 12 million, J. Symbolic Computation 31 (2001), 89–96.

[DF85] William Dwyer and Eric Friedlander, Algebraic and étale K-theory, Trans. Amer. Math. Soc. 292 (1985), no. 1, 247–280.

[Fox53] Ralph Fox, Free differential calculus. I. Derivation in the free group ring, Ann. of Math. 57 (1953), 547–560.

[Gon01] Alexander Goncharov, The dihedral Lie algebras and Galois symmetries of $\pi_1^{(l)}(\mathbb{P}^1 - (\{0,\infty\} \cup \mu_N))$, Duke Math. J. 110 (2001), no. 3, 397–487.

[Gre01] Ralph Greenberg, Iwasawa theory—past and present, Class Field Theory—Its Centenary and Prospect, Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 335–385.

[HM] Richard Hain and Makoto Matsumoto, Weighted completion of Galois groups and Galois actions on the fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$, to appear in Compositio Math., arXiv:math.AG/0006158, Aug. 11, 2001.

[Iha86] Yasutaka Ihara, Profinite braid groups, Galois representations and complex multiplications, Ann. of Math. 123 (1986), no. 1, 43–106.

[Iha89] ______, The Galois representation arising from $\mathbb{P}^1 - \{0, 1, \infty\}$ and Tate twists of even degree, Galois groups over $\mathbb{Q}$, Math. Sci. Res. Inst. Publ., vol. 16, Springer-Verlag, New York, 1989, pp. 299–313.

[Iha02] ______, Some arithmetic aspects of Galois actions of the pro-p fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$, Arithmetic fundamental groups and noncommutative algebra, Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, 2002.

[Keu89] Frans Keune, On the structure of the K_2 of the ring of integers in a number field, K-theory 2 (1989), no. 5, 625–645.

[Kur93] Masato Kurihara, Ideal class groups of cyclotomic fields and modular forms of level 1, J. Number Theory 45 (1993), 281–294.

[Lab67] John P. Labute, Classification of Demushkin groups, Canad. J. Math. 19 (1967), 106–132.

[LNQD00] Arthur Lannuzel and Thong Nguyen Quang Do, Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombers, Manuscripta Math. 102 (2000), no. 2, 187–209.

[Mar] David Marshall, Greenberg's conjecture and cyclotomic towers, preprint.

[Mat95] Makoto 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 Mathematics, vol. 186, Amer. Math. Soc., Providence, 1995, pp. 201–213.

[McC01] William McCallum, Greenberg's conjecture and units in multiple $\mathbb{Z}_p$-extensions, Amer. J. Math. 123 (2001), 909–930.

[NQD84] Thong Nguyen Quang Do, Formations de classe et modules d'Iwasawa, Number theory (Noordwijkerhout, Netherlands, 1983), Lecture Notes in Mathematics, vol. 1068, Springer-Verlag, Berlin, 1984, pp. 167–185.

[NSW00] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, Cohomology of number fields, Grundlehren Math. Wiss., vol. 323, Springer-Verlag, Berlin, 2000.

[Sha02] Romyar Sharifi, Relationships between conjectures on the structure of Galois groups unramified outside p, Arithmetic fundamental groups and noncommutative algebra, Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, 2002.

[Sou79] Christophe Soulé, K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale, Invent. Math. 55 (1979), no. 3, 251–295.

[Sou84] ______, On higher p-adic regulators, Algebraic K-theory, Evanston 1980, Lecture Notes in Mathematics, vol. 854, Springer-Verlag, Berlin-New York, 1984, pp. 372–401.

[Tat76] John Tate, Relations between K_2 and Galois cohomology, Invent. Math. 36 (1976), 257–274.

[Was97] Lawrence Washington, Introduction to cyclotomic fields, 2nd ed., Grad. Texts in Math., vol. 83, Springer-Verlag, New York, 1997.