CLASS GROUPS AND GALOIS COHOMOLOGY

SHILIN LAI

This is the notes for a talk given at the number theory working group. The aim is to study the cup product pairing $H^1(\mu_{p^n}) \otimes H^1(\mu_{p^n}) \to H^2(\mu_{p^n}^{\otimes 2})$ appearing in [MS03] and its relations to arithmetic.

1. Some Cohomology Computations

We fix the following notations for this section

– p is an odd prime.
– K is a number field with no real places.
– S is the set of places of K above p.
– K_S is the maximal unramified extension of K away from S.
– $G_{K,S} = \mathrm{Gal}(K_S/K)$.
– Given an extension L/K in K_S, $\mathcal{O}_{L,S} = \{x \in L : v(x) \geq 0 \text{ for all } v \notin S\}$.
– $\mathrm{Cl}(-)$ denotes the class group of a ring.

It follows that $\mathcal{O}_{L,S}^\times$ is the group of p-units in L, and $\mathrm{Cl}(\mathcal{O}_{L,S})$ is the ideal class group of $\mathcal{O}_L$ quotiented by the classes above p.

Furthermore, if A is an abelian group and n is an integer, then $A[n]$ is the kernel of multiplication by n, A_n is the cokernel. Let $A(p) = \bigcup_{i\geq 1} A[p^i]$ be the p-primary part of its torsion subgroup. If A has the action of complex conjugation c, then its plus part is $A^+ = A^{c=1}$ and minus part is $A^- = A^{c=-1}$.

1.1. Computation of $H^i(\mu_{p^n})$.

We start with a result on the cohomology of S-units.

Theorem 1.1. *Let $\mathcal{O}_S^\times = \mathcal{O}_{K_S,S}^\times$ be the group of S-units in K_S, then*

$$\begin{cases} H^0(G_{K,S}, \mathcal{O}_S^\times) = \mathcal{O}_{K,S}^\times \\ H^1(G_{K,S}, \mathcal{O}_S^\times) = \mathrm{Cl}(\mathcal{O}_{K,S}) \\ H^2(G_{K,S}, \mathcal{O}_S^\times)(p) = \bigoplus^0_{v\in S} \mathbf{Q}_p/\mathbf{Z}_p \\ H^i(G_{K,S}, \mathcal{O}_S^\times)(p) = 0 \text{ for } i \geq 3 \end{cases}$$

where $\bigoplus^0$ means the kernel of summation to $\mathbf{Q}_p/\mathbf{Z}_p$.

Proof. This is Proposition 8.3.11 of [NSW08]. For later use, we prove the statement about H^1 with explicit maps. Consider the short exact sequence

$$0 \to \mathcal{O}_S^\times \to K_S^\times \to K_S^\times/\mathcal{O}_S^\times \to 0$$

By Hilbert's theorem 90, this gives an identification

$$(K_S^\times/\mathcal{O}_S^\times)^{G_{K,S}}/K^\times \xrightarrow{\sim} H^1(G_{K,S}, \mathcal{O}_S^\times)$$

On the other hand, we have an injection $(K_S^\times/\mathcal{O}_S^\times)^{G_{K,S}} \to \prod_{v\notin S} \mathbf{Z}$ defined as follows: given $x \in K_S^\times$, let $L = K(x)$, then the v-component of the image of x is the valuation of x at any place w of L above v. It is surjective because every ideal of $\mathcal{O}_{K,S}$ becomes principal in a finite extension. Finally, observe that the image of $K^\times$ is the subgroup of principal ideals, so the quotient is $\mathrm{Cl}(\mathcal{O}_{K,S})$. □

The above theorem and the Kummer sequence imply

Proposition 1.2 (Proposition 5.1.5 of Sharifi's AWS notes)**.** *We have exact sequences*

$$0 \to \mathcal{O}_{K,S}^\times \otimes_{\mathbf{Z}} \mathbf{Z}/p^n\mathbf{Z} \to H^1(G_{K,S}, \mu_{p^n}) \to \mathrm{Cl}(\mathcal{O}_{K,S})[p^n] \to 0$$

$$0 \to \mathrm{Cl}(\mathcal{O}_{K,S}) \otimes_{\mathbf{Z}} \mathbf{Z}/p^n\mathbf{Z} \to H^2(G_{K,S}, \mu_{p^n}) \to \bigoplus_{v\in S}^0 \frac{1}{p^n}\mathbf{Z}_p/\mathbf{Z}_p \to 0$$

We apply this to a few cases of interest

Corollary 1.3. *Let $K = \mathbf{Q}(\mu_p)$, then*

(1) $H^2(G_{K,S}, \mu_p) \simeq \mathrm{Cl}(\mathbf{Z}[\mu_p])_p$.
(2) *Let* $D_S = \{x \in K^\times : p|v(x) \text{ for all } v \notin S\} = (K_S^\times)^p \cap K^\times$, *then* $H^1(G_{K,S}, \mu_p) \simeq D_S/(K^\times)^p$.

Proof. For the first part, we need to observe that there is a unique prime above p in $\mathbf{Q}(\mu_p)$, and it is principal. For the second part, use the diagram

$$\begin{tikzcd} & H^0(G_K, \bar{K}^\times)_p \arrow[r] \arrow[d, "\simeq"] & H^0(G_{K_S}, \bar{K}^\times)_p \arrow[d, "\simeq"] \\ 0 \arrow[r] & H^1(G_{K,S}, \mu_p) \arrow[r] & H^1(G_K, \mu_p) \arrow[r] & H^1(G_{K_S}, \mu_p) \end{tikzcd}$$

where the bottom row is the inflation-restriction sequence and the vertical arrows are boundary maps from Kummer theory. □

Remark 1.4. Let $K = \mathbf{Q}(\mu_p)$. Using the identification in Corollary 1.3, the map $H^1(G_{K,S}, \mu_p) \to \mathrm{Cl}(\mathcal{O}_{K,S})$ in Proposition 1.2 sends $x \in D_S$ to the class of ideals $\mathfrak{a}$ such that $\mathfrak{a}^p = x$.

Corollary 1.5. *There is an isomorphism*

$$H^1(G_{K,S}, \mathbf{Z}_p(1)) \simeq \mathcal{O}_{K,S}^\times \otimes_{\mathbf{Z}} \mathbf{Z}_p$$

and an exact sequence

$$0 \to \mathrm{Cl}(\mathcal{O}_{K,S}) \otimes_{\mathbf{Z}} \mathbf{Z}_p \to H^2(G_{K,S}, \mathbf{Z}_p(1)) \to \bigoplus_{v\in S}^{0} \mathbf{Z}_p \to 0$$

Proof. In Proposition 1.2, take inverse limit in n. We need to use the finiteness of $\mathrm{Cl}(\mathcal{O}_{K,S})$, and also observe that the Mittag-Leffler condition holds for the left most terms of each exact sequence. □

1.2. **Some Iwasawa theory.** Let $K_n = \mathbf{Q}(\mu_{p^{n+1}})$ and $K_\infty = \bigcup_{n\geq 0} K_n$. The cyclotomic character induces an isomorphism $\chi : \Gamma = \mathrm{Gal}(K_\infty/K_0) \xrightarrow{\sim} 1 + p\mathbf{Z}_p$. Let $\Lambda = \mathbf{Z}_p[[\Gamma]]$, with the canonical action of $G_{\mathbf{Q}(\mu_p),S}$. Fix a topological generator γ of Γ, then there is an isomorphism $\Lambda \simeq \mathbf{Z}_p[[T]]$ sending γ to $1 + T$.

Let M be a complete topological $\mathbf{Z}_p$-module with a continuous $G_{\mathbf{Q}(\mu_p),S}$-action, e.g. a $\mathbf{Q}_p$-representation or a lattice in one. In this setting, the Iwasawa cohomology is defined by

$$H^i_{\mathrm{Iw}}(G_{\mathbf{Q}(\mu_p),S}, M) := H^i(G_{\mathbf{Q}(\mu_p),S}, M \otimes \Lambda)$$

This should be seen as an interpolation of the various $H^i(M(k))$ for $k \in \mathbf{Z}$. In fact, we have an isomorphism

$$H^2_{\mathrm{Iw}}(G_{\mathbf{Q}(\mu_p),S}, M) \otimes_\Lambda \Lambda/(\gamma - \chi(\gamma)^k)\Lambda \simeq H^2(G_{\mathbf{Q}(\mu_p),S}, M(k))$$

This is proven by considering the short exact sequence $0 \to \Lambda \to \Lambda \to \mathbf{Z}_p(k) \to 0$ and observing that H^3 vanishes. There is also a canonical isomorphism of Λ-modules

$$H^i_{\mathrm{Iw}}(G_{\mathbf{Q}(\mu_p),S}, M) = \varprojlim_n H^i(G_{K_n,S}, M(k))(-k)$$

induced from Shapiro's lemma, where the transition maps are corestrictions and k is any integer. In particular, Tate twists can be taken out of cohomology.

Taking inverse limit of the previous corollary gives

Corollary 1.6.

$$H^i_{\mathrm{Iw}}(G_{\mathbf{Q}(\mu_p),S}, \mathbf{Z}_p(1)) = \begin{cases} \mathcal{E}_\infty = \varprojlim \mathcal{O}^\times_{\mathbf{Q}(\mu_{p^n}),S} & i = 1 \\ X_\infty = \varprojlim \mathrm{Cl}(\mathbf{Z}[\mu_{p^n}])(p) & i = 2 \\ 0 & \textit{otherwise} \end{cases}$$

Remark 1.7. (1) The group $\mathcal{E}_\infty$ is independent of the choice of S as long as it contains p.
(2) It follows that $H^2_{\mathrm{Iw}}(G_{\mathbf{Q}(\mu_p),S}, \mathbf{Z}_p(2)) = X_\infty(1)$.
(3) Commutative algebra and the finiteness of class number shows that X_∞ is a torsion Λ-module.

(4) This should be compared with the definition of X_∞ using the dual of H^1 with p-divisible coefficients, cf. [Gre94] or Skinner's CMI notes. Note in particular that the component with character ω differs, which shows that we need an H^1, cf. the algebraic p-adic L-function of Perrin-Riou [PR95].

There is a natural action of $\Delta = \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ on the objects studied in this section. Let $\omega : \Delta \to \mathbf{Z}_p^\times$ be the restriction of the cyclotomic character. The group ring $\mathbf{Z}_p[\Delta]$ has idempotents

$$e_k = \frac{1}{p-1}\sum_{\sigma\in\Delta}\omega(\sigma)^{-k}\sigma, \quad k \in \mathbf{Z}$$

Given an $\mathbf{Z}_p[\Delta]$-module M, let $M^{(k)} = e_k M$, then $\sigma|_{M^{(k)}} = \omega(\sigma)^k$ for all $\sigma \in \Delta$, and $M = \bigoplus_{k=0}^{p-1} M^{(k)}$. The plus part of M is the direct sum of $M^{(k)}$ over all even k. We apply this decomposition to X_∞ to get $p-1$ torsion Λ-modules $X_\infty^{(k)}$. Let $f^{(k)} \in \Lambda$ be a characteristic power series of $X_\infty^{(k)}$, then the Iwasawa main conjecture states that if k is odd, then $f^{(k)}$ is a p-adic L-function interpolating the values of Dirichlet L-functions. Details of the interpolation property can be found in Chapter 13 of [Was97].

On the cohomological side, the action appears naturally if one restricts to $\mathbf{Q}$ using Shapiro's lemma:

$$H^i(G_{\mathbf{Q}(\mu_p),S}, M) = H^i(G_{\mathbf{Q},S}, M \otimes \mathbf{Z}_p[\Delta])$$

Each eigenspace is then of the form $H^i(G_{\mathbf{Q},S}, M \otimes \omega^k)$. One consequence of the control theorem and the Iwasawa main conjecture is that

$$\# H^2(G_{\mathbf{Q},S}, \mathbf{Z}_p(1+k)) = \#\mathbf{Z}_p/\zeta(-k)\mathbf{Z}_p$$

if $k > 0$ is odd and $p-1 \nmid k+1$. This is in agreement with Lichtenbaum's conjecture.

1.3. **Cup product.** From now until the end, let $n = 1$, $K = \mathbf{Q}(\mu_p)$, and $A = \mathrm{Cl}(\mathbf{Z}[\mu_p])$. The cup product in cohomology

$$\smile : H^1(G_{K,S}, \mu_p) \times H^1(G_{K,S}, \mu_p) \to H^2(G_{K,S}, \mu_p^{\otimes 2})$$

gives a bilinear pairing

$$(\cdot,\cdot) : D_S \times D_S \to A_p \otimes \mu_p$$

using Corollary 1.3. Recall that D_S is the set of $a \in K^\times$ such that $K(a^{1/p})/K$ is unramified outside of p. We begin with two easy properties.

Proposition 1.8. *(1) $(a,b) = -(b,a)$.*
(2) Let $a, b \in \mathcal{O}_{K,S}^\times$. If b is a norm from the S-units of $K(a^{1/p})$ to K, then $(a,b) = 0$.
(3) If $a, 1-a \in \mathcal{O}_{K,S}^\times$, then $(a, 1-a) = 0$.

Proof. The first is the graded commutativity of cup product. For the second part, let $L = K(a^{1/p})$. Given $x \in D_S$, let $[x] \in H^1(G_{K,S}, \mu_p)$ be its associated class. This sends $\mathbf{N}_{L/K}$ to corestriction from $G_{L,S}$ to $G_{K,S}$, so $[b] = \mathrm{Cor}(\beta)$ for some $\beta \in H^1(G_{L,S}, \mu_p)$. Also, a becomes a p-th power in L, so $\mathrm{Res}([a]) = 0$, so

$$(a,b) = [a] \smile \mathrm{Cor}(\beta) = \mathrm{Cor}(\mathrm{Res}([a]) \smile \beta = 0$$

The final property is a consequence of this relation, since $1 - a = \mathbf{N}_{L/K}(1 - a^{1/p})$. □

For later applications, we also need the following formula of McCallum–Sharifi.

Theorem 1.9 (Theorem 2.4 of [MS03]). *Let $a, b \in D_S$. Let*

– $\alpha^p = a$, $L = K(\alpha)$.
– *σ be a generator of* $\mathrm{Gal}(L/K)$.
– *$\mathfrak{b}$ be the image of b in $A[p]$, i.e. $\mathfrak{b}^p = b$.*

Suppose that $a, b \notin D_S^p$ and $(a,b)_p = 0$, then there exists $\gamma \in L^\times$ such that $b = \mathbf{N}_{L/K}\gamma$, and we can find a fractional ideal $\mathfrak{c}$ of $\mathcal{O}_{L,S}$ such that $\gamma\mathcal{O}_{L,S} = \mathfrak{b}\mathfrak{c}^{1-\sigma}$, then

$$(a,b) = \mathbf{N}_{L/K}\mathfrak{c} \otimes \alpha^{\sigma-1}$$

Proof. We explain why γ and $\mathfrak{c}$ can be found. By the definition of the norm residue symbol (or the perfectness of local duality), b is a local norm at p. Away from p, the extension is unramified and the valuation of b is a multiple of p, so it is also a local norm. Since L/K is cyclic, the Hasse norm principle implies that b is a global norm.

For $\mathfrak{c}$, it is equivalent to showing that $H^1(L/K, I_{L,S}) = 0$, where $I_{L,S}$ is the group of fractaional ideals of L. This can be computed using Shapiro's lemma and the explicit description of H^1 of a cyclic group. $\square$

Continuing the theme of Kummer extensions, the cup product can also be interpreted as a boundary homomorphism. In the following two results, we *do not* keep track of the $\mathrm{Gal}(K/\mathbf{Q})$-action.

Proposition 1.10. *Let L/K a Kummer extension of degree p. Let $G = \mathrm{Gal}(L/K) \simeq \mathbf{Z}/p\mathbf{Z}$, viewed as a trivial $G_{K,S}$-module. Let $I_G = \ker((\mathbf{Z}/p\mathbf{Z})[G] \to \mathbf{Z}/p\mathbf{Z})$ be the augmentation ideal. We have a short exact sequence*

$$0 \to G \to (\mathbf{Z}/p\mathbf{Z})[G]/I_G^2 \to \mathbf{Z}/p\mathbf{Z} \to 0$$

where the first map is $g \mapsto g-1$. Let

$$\Psi : H^1(G_{K,S}, \mu_p) \to H^2(G_{K,S}, \mu_p) \otimes G$$

be the boundary map of the long exact sequence, then $\Psi(b) = \pi \smile b$, where $\pi : G_{K,S} \to G$ is the projection.

In particular, suppose $L = K(\alpha)$ with $\alpha^p = a \in D_S$. Let π_a be the map $G \to \mu_p$, $\sigma \mapsto \alpha^{\sigma-1}$, then

$$(a, b) = (1 \otimes \pi_a)\Psi(b)$$

Proof. Observe that π is the cocycle associated to the short exact sequence by a simple computation, so the boundary map $\partial : H^0(G_{K,S}, \mathbf{Z}/p\mathbf{Z}) \to H^1(G_{K,S}, G)$ sends 1 to π, so

$$\Psi(b) = \Psi(1 \smile b) = \partial(1) \smile b = \pi \smile b$$

The second claim follows from the fact that $\pi_a(\pi) = [a]$. $\square$

We have the following theorem of Sharifi about its image.

Theorem 1.11 (Corollay 5.1.20 of Sharifi's AWS Notes)**.** *Let L/K be a Kummer extension of degree p in K_S which is totally ramified at p. Let $A_{L,p} = \mathrm{Cl}(\mathcal{O}_{L,S})_p$, then*

$$\frac{A_{L,p}}{I_G A_{L,p}} \simeq A_p, \quad \frac{I_G A_{L,p}}{I_G^2 A_{L,p}} \simeq \frac{A_p \otimes G}{\Psi(\mathcal{O}_{K,S}^\times)}$$

where the first map is induced by norm.

2. Relation with arithmetics

Let p be an odd prime satisfying Vandiver's conjecture. In this section, let $K = \mathbf{Q}(\mu_p)$, $E = \mathcal{O}_{K,S}^\times$, and $A = \mathrm{Cl}(\mathcal{O}_{K,S})(p)$. We will study the relation between the cup product pairing defined earlier and the arithmetics of cyclotomic fields.

2.1. **Cyclotomic units.** Let ζ be a generator of μ_p. Inside the group of p-units E, we have a special subgroup generated by ζ and $1-\zeta^i$ for $1 \le i \le p-1$. This is the group of cyclotomic units, denoted by C.

Proposition 2.1. *(1) The free module C/C_{tor} has basis $1-\zeta^i$ for $1 \le i \le \frac{p-1}{2}$.*
(2) $[E : C] = h^+ := \#A/\#A^+$.

Proof. The listed elements generate since $1-\zeta^{p-r} = -\zeta^{-r}(1-\zeta^r)$. A regulator computation shows that they are independent. This and the analytic class number formula for $\mathbf{Q}(\mu_p)^+$ implies the second assertion. A closely related result is Theorem 8.2 of [Was97]. Note that E in [Was97] is $\mathcal{O}_K^\times$ in our notation. $\square$

2.2. **Eigenspaces and consequences of Vandiver's conjecture.** Recall that Vandiver's conjecture states that $p \nmid h_p^+ = \#A/\#A^+$. This is equivalent to saying

$$A = \bigoplus_{\substack{3 \le k \le p-2 \\ k \text{ odd}}} A^{(k)}$$

in the decomposition into Δ-eigenspaces. Here, we have also used the classical fact that $A^{(1)} = 0$. We record here some other arithmetic consequences of this conjecture.

The p-units of K is a direct sum of the roots of unities of K and a free part of rank $\frac{p-1}{2}$. The free part comes from $\mathbf{Q}(\mu_p)^+$, so

$$E_p = \mu_p \oplus \bigoplus_{\substack{1 \le i \le p-1 \\ i \text{ even}}} \epsilon_i E_p$$

with each $\epsilon_i E_p \simeq \mathbf{Z}/p\mathbf{Z}$ (this part does not need Vandiver's conjecture). Now, by the previous proposition, $p \nmid [E : C]$, so we also have $\epsilon_i C_p \simeq \mathbf{Z}/p\mathbf{Z}$ for the same range of i. In particular, for $1 \le k \le p-2$, k odd, there exists $\eta_k \in C$ such that

$$\eta_k \equiv (1-\zeta)^{\epsilon_{p-k}} \pmod{C^p}$$

They generate C^+.

Recall that Proposition 1.2 gives a short exact sequence $0 \to E_p \to D_S/(K^\times)^p \to A[p] \to 0$. The above discussion shows that this splits canonically as a $\mathbf{Z}_p[\Delta]$-module by eigenspace consideration. Since A has no plus part, the pairing $D_S \times D_S \to A_p(1)$ naturally decomposes into two blocks:

$$\begin{array}{cc} & \begin{array}{ccc} \mu_p & A[p] & C_p^+ \end{array} \\ \begin{array}{c} \mu_p \\ A[p] \\ C_p^+ \end{array} & \begin{pmatrix} 0 & - & 0 \\ - & - & 0 \\ 0 & 0 & + \end{pmatrix} \end{array}$$

To better understand the $C_p^+ \times C_p^+$ part, we need to know the finer structures of A, which is hard. However, Vandiver's conjecture drastically simplifies the situation.

Proposition 2.2. *Let k be an odd integer with $3 \le k \le p-2$, then*

(1) Each $A^{(k)}$ is cyclic, so by the Iwasawa main conjecture, $A^{(k)} \simeq \mathbf{Z}_p/L(0, \omega^{-k})\mathbf{Z}_p$.
(2) $X_\infty^{(k)} \simeq \Lambda/(f^{(k)})$.

Proof. We give an outline. The full details can be found in section 10.3 of [Was97].

The proof uses Kummer's reflection principle. The point is that Kummer theory and class field theory gives a perfect pairing between A_p and a subset B of $D_S/(K^\times)^p$, so $B \simeq A_p^*(1)$. But we also have a map $B \to A[p]$, made explicit in Remark 1.4. Its kernel is a subgroup of $\mathcal{O}^\times_{\mathbf{Q}(\mu_p),S} \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z}$, whose structure is well-understood under Vandiver's conjecture because of cyclotomic units. This gives a precise relation between the odd part and even parts of A. But the even part is trivial by Vandiver's conjecture. This is enough to prove part (1). The second part follows from Nakayama's lemma. $\square$

In particular, suppose $A_p^{(k)}$ is non-trivial, then it is isomorphic to $\mathbf{Z}/p\mathbf{Z}(k)$. We can consider the projection of the cup product to this component. Following the labelling in [MS03], for $2 \le r \le p-3$, r even, define the pairing

$$\langle \cdot, \cdot \rangle_r : D_S \times D_S \to A_p^{(p-r)} \otimes \mu_p \simeq \mathbf{Z}/p\mathbf{Z}(2-r)$$

By considering Δ-actions, we see that $\langle \eta_k, \eta_{k'} \rangle_r = 0$ unless $k + k' \equiv r \pmod{p-1}$. Define

$$e_{k,r} = \langle \eta_k, \eta_{r-k} \rangle_r \in A_p^{(p-r)} \otimes \mu_p$$

In Eric's talk, we saw that their vanishing is related to the vanishing modulo p of L-values of cusp forms via Sharifi's conjecture. We will later consider a different arithmetic application.

2.3. **Non-triviality of the $-$-part.** By the analysis in the previous section, we see that ζ pairs non-trivially only with $A[p]$. There is a relation between the non-triviality of this pairing and the λ-invariant of a p-adic L-function. Recall that if $f \in \Lambda$, we can associate to it a formal power series $\sum_i a_i T^i \in \mathbf{Z}_p[[T]]$ by sending a fixed topological generator γ to $1+T$, and the λ-invariant of f is the minimal i such that $a_i \in \mathbf{Z}_p^\times$. This is independent of the choice of γ.

In this section, we choose k odd such that $A_p^{(k)} \neq 0$. Let f_k be the characteristic ideal of $X_\infty^{(k)}$. By Vandiver's conjecture, $X_\infty^{(k)} \simeq \Lambda/(f_k)$ and $A^{(k)} \simeq \mathbf{Z}_p/f_k(0)\mathbf{Z}_p$. In particular, $p|f_k(0)$.

Theorem 2.3. *Let $\mathfrak{a} \in A[p]^{(k)}$. Choose $\mathfrak{a}_0 \in A^{(k)}$ such that $\mathfrak{a}_0^{f_k(0)/p} = \mathfrak{a}$, then for all $\zeta \in \mu_p$,*

$$(\zeta, \mathfrak{a}) = \mathfrak{a}_0^{-f_k'(0)} \otimes \zeta^{\frac{\chi_{\mathrm{cyc}}(\gamma)-1}{p}}$$

Proof. We use Theorem 1.9. Let $L = \mathbf{Q}(\mu_{p^2})$, ζ_{p^2} be a fixed p-th root of ζ, and a be a generator of $\mathfrak{a}^p$. A generator of $\mathrm{Gal}(L/K)$ is γ. Recall that there exists $\alpha \in L^\times$ such that $\mathbf{N}_{L/K}\alpha = a$ and fractional ideal $\mathfrak{c}$ of $\mathcal{O}_{L,S}$ such that $\alpha\mathcal{O}_{L,S} = \mathfrak{a}\mathfrak{c}^{1-\gamma}$. The result is then $\mathbf{N}_{L/K}\mathfrak{c} \otimes \zeta_{p^2}^{\gamma-1}$.

Classical Iwasawa theory gives an isomorphism

$$X_\infty/(\gamma^p - 1)X_\infty \xrightarrow{\sim} A_L := \mathrm{Cl}(\mathcal{O}_{L,S})(p)$$

This is Proposition 13.22 of [Was97], see also [Ser95]. The assumption required is that K_∞/K_0 is ramified at a unique prime, and it is totally ramified there, which holds here. Therefore, we have an isomorphism

$$\mathbf{Z}_p[[T]]/((1+T)^p - 1, f_k) \xrightarrow{\sim} A_L$$

With respect to this, $\mathbf{N}_{L/K} = \sum_{i=0}^{p-1} \gamma^i = \frac{1}{T}((1+T)^p - 1)$. Suppose $\mathfrak{a}_0$ maps to $u(T)$, then

$$\mathbf{N}_{L/K}\mathfrak{c} = -\frac{1}{T}\left(f_k(T) - \mathbf{N}_{L/K} \cdot \frac{f_k(0)}{p}\right)u(T) \equiv -f_k'(0)u(T) \pmod{(p, T)}$$

This implies the result. Note that all division makes sense since we have proven that α and $\mathfrak{c}$ exist, and the results do not depend on their choices. $\square$

Corollary 2.4. *The map $(\zeta, \cdot) : A[p] \to A_p \otimes \mu_p$ is non-trivial if $\lambda(f_k) = 1$.*

2.4. **Non-triviality of the $+$-part.** This is a more difficult question. We state without proof a theorem of McCallum and Sharifi, which gives a computable criterion for the non-vanishing of $e_{k,r}$ in some cases.

Fix r an irregular index for p, i.e. $A^{(p-r)} \neq 0$ or equivalently $p|B_r$. Let $L = K(\eta_{p-r}^{1/p})$. This is an unramified extension of K because the Δ-action on $\mathrm{Gal}(L/K)$ is via ω^{p-r} (by Kummer theory, cf. the proof of Proposition 2.2), and the corresponding eigenspace of A is non-trivial.

Theorem 2.5 (Proposition 7.4 of [MS03])**.** *Suppose $3 \le k \le p-2$, k odd, and $p \nmid B_{p-k}$. Assume that η_{r-k} is the norm of $\alpha \in \mathcal{O}_{L,S}^\times$. Modify α so that its image in $\mathcal{O}_{L,S}^\times \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z}$ lies in the ω^{p-r+k}-eigenspace. Then $e_{k,r} = \langle \eta_k, \eta_{r-k}\rangle_r \neq 0$ if and only if*

$$\sum_{i=1}^{p-1} \sigma^i (b')^i \notin (\mathbf{Q}_p(\mu_p)^\times)^p$$

for one (equivalently any) embedding of L into $\mathbf{Q}_p(\mu_p)$.

We end with two examples.

Example 2.6. Let $p = 37$, then $r = 32$ is the unique irregular index. In particular, $\#A = 37$.

1. If $k = 5$, then $L = K(\eta_5^{1/37})$ is unramified. By Theorem 1.9, $e_{5,32}$ is the projection to the ω^5-eigenspace of the norm of an ideal in L. But we have an Δ-equivariant isomorphism $\mathrm{Gal}(L/K) \simeq A_K/\mathbf{N}_{L/K}A_L$, so the norms are all trivial, which implies that $e_{5,32} = 0$. By anti-symmetry, $e_{27,5} = 0$. This in fact follows from the symbol relation, as explained in section 5 of [MS03].
2. Using the above theorem, McCallum and Sharifi verified that the pairing $\langle \cdot, \cdot \rangle_{32}$ is non-trivial. They have also verified that the symbol property defines this pairing uniquely up to scalar, so we can compute that $e_{k,32} \neq 0$ unless $k = 5, 27$.

   We give an arithmetic consequence. Let $L = K(a^{1/p})$ for some $a \in D_S$, so L/K is a Kummer extension unramified away from p. We want to understand A_L, the p-primary part of the ideal class group of L. We suppose that L/K is totally ramified at p, then the unique prime above p in L is principal, so $A_{L,S} = A_L$. Let $G = \mathrm{Gal}(L/K)$. Recall that in 1.10, we constructed a reciprocity map which can be specialized to $\Psi : \mathcal{O}_{K,S}^\times \to A_p \otimes G \simeq \mathbf{Z}/p\mathbf{Z}$. It has non-trivial image if and only if $(a, \cdot)$ is non-trivial on $\mathcal{O}_{K,S}^\times$. By Theorem 1.11, if Ψ is non-trivial, then $(A_{L,S})_G \simeq A$ and $I_G A_{L,S} = I_G^2 A_{L,S}$. The second statement implies that $A_{L,S} \simeq (A_{L,S})_G$ by Nakayama's lemma, so we have an isomorphism $A_L \simeq A$.

Let $a = 37$, then it is in the component generated by η_1 and not a p-th power, so by the above discussion, $\#\mathrm{Cl}(\mathbf{Q}(\mu_{37}, \sqrt[37]{37}))(p) = 37$. Furthermore, the norm map $(A_{L,S})_G \xrightarrow{\sim} A$ is Δ-equivariant, so the classes in $A_{L,S}$ does not descend to the field $\mathbf{Q}(\sqrt[37]{37})$. It follows that $\mathbf{Q}(\sqrt[37]{37})$ has class number coprime to 37, answering a question of Ralph Greenberg.[1]

Remark 2.7. Greenberg showed that this answer implies Greenberg's conjecture for $p = 37$. We briefly recall the conjecture. Let K be a number field, and let K_∞ be the compositum of all $\mathbf{Z}_p$-extensions of K, then $\mathrm{Gal}(K_\infty/K) \simeq \mathbf{Z}_p^{r_2+1+\delta}$, where δ is the Leopoldt defect, known to be 0 if $\mathrm{Gal}(K/\mathbf{Q})$ is abelian (Theorem 5.25 of [Was97]). Let X be the Galois group of the maximal abelian unramified extension of K_∞, then X naturally becomes a module over $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \simeq \mathbf{Z}_p[[T_1, \cdots, T_d]]$, and Greenberg conjectured that X is pseudo-null, i.e. $\mathrm{ht}\,\mathrm{Ann}_\Lambda(X) \geq 2$.

In section 10 of [MS03], it was proven directly that if the cup product pairing is non-trivial on cyclotomic units for a prime p, then Greenberg's conjecture holds for $\mathbf{Q}(\mu_p)$.

References

[Gre94] Ralph Greenberg. Iwasawa theory and p-adic deformations of motives. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 193–223. Amer. Math. Soc., Providence, RI, 1994.

[MS03] William G. McCallum and Romyar T. Sharifi. A cup product in the Galois cohomology of number fields. *Duke Math. J.*, 120(2):269–310, 2003.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[PR95] Bernadette Perrin-Riou. Fonctions L p-adiques des représentations p-adiques. *Astérisque*, (229):198, 1995.

[Ser95] Jean-Pierre Serre. Classes des corps cyclotomiques (d'après K. Iwasawa). In *Séminaire Bourbaki, Vol. 5*, pages Exp. No. 174, 83–93. Soc. Math. France, Paris, 1995.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[1]It is also amusing to observe that $\mathrm{disc}\,\mathbf{Q}(\sqrt[37]{37}) = 37^{73}$.