Invent. math. 172, 213–229 (2008)
DOI: 10.1007/s00222-007-0109-3

Inventiones mathematicae

Erratum

Surjectivity of p-adic regulators on K_2 of Tate curves*

Masanori Asakura

Graduate School of Mathematics, Kyushu University, Fukuoka 812-8581, Japan
(e-mail: asakura@math.kyushu-u.ac.jp)

Oblatum 11-VI-2007 & 5-XII-2007
Published online: 10 January 2008 – © Springer-Verlag 2008

Invent. math. (2006) Digital Object Identifier (DOI) 10.1007/s00222-005-0494-4
Published online: 1 February 2006 – © Springer-Verlag 2006

1. Mistake

There is a serious mistake in my paper [1] appeared in Invent. Math. **165** (2006), 267–324. The proof of the main theorem consists of three parts. The mistake is found in the Part III (Sect. 8.1 in loc. cit.). The proof there uses Jannsen's Hasse theorem ([7, Thm. 3 a)]). Though it is stated for cohomology with $\mathbf{Z}_p$-coefficients, I referred it as $\mathbf{Q}_p$-coefficients. That is my stupid but serious mistake. The argument in Sect. 8.1 now breaks down totally.

In the present paper, we correct the proof of the Part III (Theorem 2.1). The method is completely different from the previous one. The idea of it was given by Professor Kazuya Kato. I heartily thank him for the suggestion and for teaching me a lot about Iwasawa theory. Without his help, I could never overcome the mistake.

2. Correction

Let p be a prime number. $H^\bullet = H^\bullet_{\mathrm{cont}}$ denotes the continuous Galois cohomology.

* The online version of the original article can be found at http://dx.doi.org/10.1007/s00222-005-0494-4

Theorem 2.1. *Let K be a finite extension of $\mathbf{Q}_p$ which is contained in some cyclotomic extension $\mathbf{Q}_p(\zeta)$. Let $r \neq 1$ be an integer. Let*

$$\varinjlim_{F} H^1(F, \mathbf{Z}_p(r)) \longrightarrow H^1(K, \mathbf{Z}_p(r)) \tag{2.1}$$

be the natural map where F runs over all subfields of K which are finite abelian extensions of $\mathbf{Q}$ (i.e. F is a subfield of some cyclotomic extension of $\mathbf{Q}$).

(1) *Suppose $p \geq 3$. Then* (2.1) *is surjective.*
(2) *Suppose $p = 2$. If $\sqrt{-1} \in K$ then* (2.1) *is surjective. In general it has a finite cokernel.*

The Part III in [1] is the case $r = 2$ in the above.

2.1. Local units and cyclotomic units. Let H be a finite unramified extension of $\mathbf{Q}_p$ and O_H the ring of integers in H. We fix a generator $(\zeta_{p^n})_{n\geq 1}$ of $\mathbf{Z}_p(1)$. Put $G_n := \mathrm{Gal}(H(\zeta_{p^n})/H)$ and $G := \varprojlim G_n$. We denote by $O_H[[G]]$ the Iwasawa algebra of G:

$$O_H[[G]] := \varprojlim_{n} O_H[G_n].$$

Let $\chi : G \xrightarrow{\sim} \mathbf{Z}_p^\times$ be the cyclotomic character defined by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\chi(\sigma)}$. We write $\sigma_\alpha = \chi^{-1}(\alpha)$ for $\alpha \in \mathbf{Z}_p^\times$. We choose isomorphisms of topological O_H-algebras

$$\Phi : O_H[[G]] \xrightarrow{\cong} \overbrace{O_H[[T]] \times \cdots \times O_H[[T]]}^{p-1 \text{ times}} \tag{2.2}$$

which is uniquely determined by

$$\Phi(\sigma_{1+p}) = (T + 1 + p, \cdots, T + 1 + p),$$
$$\Phi(\sigma_\eta) = (\eta, \eta^2, \cdots, \eta^{p-1}) \quad \text{for } \eta^{p-1} = 1$$

for $p \geq 3$, and

$$\Phi : O_H[[G]] \xrightarrow{\cong} O_H[[T]][\sigma]/(\sigma^2 - 1) \tag{2.3}$$

determined by

$$\Phi(\sigma_5) = T + 5, \quad \Phi(\sigma_{-1}) = \sigma$$

for $p = 2$. We put

$$U' := \varprojlim_{n} O_H[\zeta_{p^n}]^\times, \quad V' := \varprojlim_{n} H(\zeta_{p^n})^\times,$$

where the limits are taken with respect to the norm maps. Let U and V be the p-adic completion of U' and V' respectively so that we have

$$V \cong \varprojlim_n H^1(H(\zeta_{p^n}), \mathbf{Z}_p(1)), \quad V \cong U \oplus \mathbf{Z}_p.$$

We note that $(0, 1) \in U \oplus \mathbf{Z}_p$ corresponds to $(1-\zeta_{p^n})_{n\geq 1} \in V$ in the second isomorphism. The group U (or V) is called the *local units* and it is known to be a finitely generated $\mathbf{Z}_p[[G]]$-module. For an integer r, one has a natural isomorphism

$$V(r-1) := V \otimes_{\mathbf{Z}_p} \mathbf{Z}_p(r-1) \cong \varprojlim_n H^1(H(\zeta_{p^n}), \mathbf{Z}_p(r)) \tag{2.4}$$

of $\mathbf{Z}_p[[G]]$-modules (G acts on the left hand side diagonally). If $r \neq 1$ and $p \geq 3$ (resp. $p = 2$) we also have

$$H^1(H(\zeta_{p^n}), \mathbf{Z}_p(r)) \cong V(r-1) \otimes_{\mathbf{Z}_p[[G]]} \mathbf{Z}_p[G_n] \tag{2.5}$$

for $n \geq 0$ (resp. $n \geq 2$). (When $p = 2$ and $n = 1$ there is a similar isomorphism if we neglect the torsion.)

Letting q_H be the order of the residue field of H, we denote the group of $(q_H - 1)$-th roots of unity in H by μ_H. Note that μ_H is equal to the group of all roots of unity in H if $p \geq 3$, but not equal if $p = 2$. Recall Coleman's exact sequence

$$0 \longrightarrow \mathbf{Z}_p(1) \oplus \mu_H \xrightarrow{i_1} U' \xrightarrow{l_\infty} O_H[[G]] \xrightarrow{i_2} \mathbf{Z}_p(1) \longrightarrow 0 \tag{2.6}$$

of G-modules. (See [4, Theorem 1] or [5, Theorem 3.5.1] where it is proved in the case $H = \mathbf{Q}_p$. However one can check that the same proof works for arbitrary H.) The map i_1 sends $((\zeta_{p^n})_n, \eta)$ to $(\eta^{1/p^n}\zeta_{p^n})_n$ if $p \geq 3$ (resp. $(-\eta^{1/2^n}\zeta_{2^n})_n$ if $p = 2$) where $\eta^{1/p^n} \in \mu_H$ denotes the unique element whose p^n-th power is equal to η. The map i_2 is the composition of the trace map $\mathrm{Tr}_{H/\mathbf{Q}_p} : O_H[[G]] \to \mathbf{Z}_p[[G]]$ with the $\mathbf{Z}_p$-linear map $\mathbf{Z}_p[[G]] \to \mathbf{Z}_p(1)$ such that $\sigma_\alpha \mapsto (\zeta_{p^n}^\alpha)_{n\geq 1}$. The map l_∞ is an important map in Iwasawa theory which is described in the following way. Let Fr_p be the Frobenius on H. We also denote by Fr_p the endomorphism on $O_H[[X]]$ given by $aX^i \mapsto \mathrm{Fr}_p(a)X^i$. Let $\varphi : O_H[[X]] \to O_H[[X]]$ be the endomorphism given by $a(X+1)^i \mapsto \mathrm{Fr}_p(a)(X+1)^{ip}$. Let $\psi : U' \to O_H[[X]]^\times$ be the Coleman power series which is characterized by $\mathrm{Fr}_p^{-n}(\psi(u))|_{X=\zeta_{p^n}-1} = u_n$ for $u = (u_n)_n \in U'$ ([2, Theorem A]). Let $\log^{(p)} : O_H[[X]]^\times \to O_H[[X]]$ be the homomorphism defined by

$$\log^{(p)}(f) := \frac{1}{p}\log\left(\frac{f^p}{\varphi(f)}\right).$$

Let $i : O_H[[G]] \to O_H[[X]]$ be the continuous O_H-linear map such that $\sigma_\alpha \mapsto (1+X)^\alpha$. Note that i is injective. Then l_∞ is defined as the unique

$\mathbf{Z}_p[[G]]$-linear map which makes the following diagram commutative:

$$\begin{array}{ccc} U' & \xrightarrow{l_\infty} & O_H[[G]] \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle i} \\ O_H[[X]]^\times & \xrightarrow{\log^{(p)}} & O_H[[X]]. \end{array}$$

If we replace U' with U, we get an exact sequence

$$0 \longrightarrow \mathbf{Z}_p(1) \xrightarrow{i_1} U \xrightarrow{l_\infty} O_H[[G]] \xrightarrow{i_2} \mathbf{Z}_p(1) \longrightarrow 0 \tag{2.7}$$

of $\mathbf{Z}_p[[G]]$-modules. In particular we have an isomorphism

$$l_\infty(U) \xrightarrow[\cong]{\Phi} (O_H^0 + TO_H[[T]]) \times O_H[[T]] \times \cdots \times O_H[[T]] \tag{2.8}$$

$$\Big(\text{resp. } l_\infty(U) \xrightarrow[\cong]{\Phi} \big\{ f(T) + g(T)\sigma \in O_H[[T]][\sigma]/(\sigma^2 - 1) \;\big|\; f(0) - g(0) \in O_H^0 \big\}\Big) \tag{2.9}$$

of $\mathbf{Z}_p[[G]]$-modules for $p \geq 3$ (resp. $p = 2$) where $O_H^0 := \ker(\mathrm{Tr}_{H/\mathbf{Q}_p} : O_H \to \mathbf{Z}_p)$.

For $\eta \in \mu_H$ we put

$$C(\eta) := \big(1 - \eta^{1/p^n} \zeta_{p^n}\big)_{n \geq 1} \in V \tag{2.10}$$

and call it the *cyclotomic unit*. The Coleman power series $\psi(C(\eta))$ is $1 - \eta(X + 1)$. Note that $C(1)$ is a generator of $V/U \cong \mathbf{Z}_p$ and if $\eta \neq 1$ then $C(\eta) \in U$. We also put

$$C_r(\eta) := C(\eta) \otimes \big(\zeta_{p^n}^{\otimes r-1}\big)_{n \geq 1} = \big(\big(1 - \eta^{1/p^n} \zeta_{p^n}\big) \otimes \zeta_{p^n}^{\otimes r-1}\big)_{n \geq 1} \in V(r-1)$$

for an integer r. We define a $\mathbf{Z}_p[[G]]$-submodule $V(r-1)_{\mathrm{cycl}} \subset V(r-1)$ in the following way. Let $L/\mathbf{Q}_p$ be a finite unramified extension such that $L \supset H$, and V_L the p-adic completion of $\varinjlim L(\zeta_{p^n})^\times$. The norm map for L/H induces a map $N_{L/H} : V_L(r-1) \to V(r-1)$. For $\eta_L \in \mu_L$, we have the cyclotomic unit $C_r(\eta_L) \in V_L(r-1)$ and hence $N_{L/H} C_r(\eta_L) = N_{L/H} C(\eta_L) \otimes (\zeta_{p^n})^{\otimes r-1} \in V(r-1)$. We define

$$V(r-1)_{\mathrm{cycl}} := \mathbf{Z}_p(r) + \Big(\sum_{L, \eta_L} \mathbf{Z}_p[[G]] \cdot N_{L/H} C_r(\eta_L) \Big) \subset V(r-1)\,,$$

where the summation runs over all L and η_L as above. We put $U(r-1)_{\mathrm{cycl}} := U(r-1) \cap V(r-1)_{\mathrm{cycl}}$. We simply write $V_{\mathrm{cycl}} = V(0)_{\mathrm{cycle}}$ and $U_{\mathrm{cycl}} = U(0)_{\mathrm{cycle}}$. Obviously we have $V(r-1)_{\mathrm{cycl}} \cong V_{\mathrm{cycl}} \otimes \mathbf{Z}_p(r-1)$ and $U(r-1)_{\mathrm{cycl}} \cong U_{\mathrm{cycl}} \otimes \mathbf{Z}_p(r-1)$.

The following is the key result.

Theorem 2.2. $V_{\mathrm{cycl}} = V$.

We shall prove Theorem 2.2 in Sects. 2.4 and 2.5.

Remark 2.3. Let us explain Thoerem 2.2 from the viewpoint of p-adic L-functions. Let

$$\Phi l_\infty(C(\eta)) = \left(F_\eta^{(1)}(T), \cdots, F_\eta^{(p-1)}(T)\right) \in \prod O_H[[T]].$$

As we shall see later (cf. (2.20) below), they correspond to the p-adic polylogarithms in the following way:

$$F_\eta^{(i)}((1+p)^r - (1+p)) = -l_{1-r}^{(p)}(\eta) \quad \text{for } r \equiv i \bmod p-1. \tag{2.11}$$

Then Theorem 2.2 can be stated as

$$\sum_{L,\eta_L} \mathbf{Z}_p[[T]]\mathrm{Tr}_{L/H} F_{\eta_L}^{(i)}(T) = \begin{cases} O_H[[T]] & 2 \le i \le p-1 \\ O_H^0 + TO_H[[T]] & i = 1. \end{cases} \tag{2.12}$$

Let $L_p(s, \chi)$ denote the p-adic L-function which is characterized as a p-adic analytic function on $\mathbf{Z}_p$ such that

$$L_p(1-r, \chi\omega^r) = (1 - \chi(p)p^{r-1})L(1-r, \chi), \quad r > 0 \tag{2.13}$$

where $L(s, \chi)$ is the Dirichlet L-function and $\omega : (\mathbf{Z}/p)^\times \to \mathbf{Z}_p^\times$ is the Teichmüller character. Due to Iwasawa's theorem, for each $1 \le i \le p-1$ there is a $G_\chi^{(i)}(T) \in \mathrm{Frac}\, O_H[\mathrm{Image}\chi][[T]]$ such that

$$G_\chi^{(i)}((1+p)^r - (1+p)) = -L_p(1-r, \chi\omega^i) \quad \text{for } r \equiv i \bmod p-1. \tag{2.14}$$

The p-adic polylogarithms are expressed as a linear combination of the p-adic L-functions and vice versa. More precisely, for $p \nmid N$ and a primitive N-th root ζ_N of unity one has

$$l_{1-r}^{(p)}\left(\zeta_N^l\right) = \sum_{dN_0=N} \sum_{k,\chi} \varphi(N_0)^{-1} d^{r-1} \chi(k) \zeta_N^{lkd} L_p(1-r, \chi\omega^r), \quad l \not\equiv 0 \bmod N \tag{2.15}$$

where $k \in (\mathbf{Z}/N_0)^\times$ and χ runs over all characters modulo N_0. Let $N = q_H - 1$. Then (2.11), (2.14) and (2.15) imply

$$F_\eta^{(i)}(T) = \sum_{dN_0=N} \sum_{k,\chi} \varphi(N_0)^{-1} d^{r-1} \chi(k) \eta^{kd} G_\chi^{(i)}(T), \quad \eta \in \mu_H - \{1\}. \tag{2.16}$$

Therefore we have from (2.12) that

$$\sum_{L,\chi} \mathbf{Z}_p[\mathrm{Image}\chi][[T]]\mathrm{Tr}_{L/H} G_\chi^{(i)}(T) \supset \begin{cases} O_H[[T]] & 2 \le i \le p-1 \\ O_H^0 + TO_H[[T]] & i = 1 \end{cases}$$

where L/H is an unramified extension and χ runs over all characters modulo $q_L - 1$.

2.2. Proof of Theorem 2.2 $\Rightarrow$ Theorem 2.1. We first assume $K = H(\zeta_{p^n})$ where $n \geq 0$ and H is a finite unramified extension of $\mathbf{Q}_p$. It follows from Theorem 2.2 that $V(r-1) = V_{\mathrm{cycl}} \otimes \mathbf{Z}_p(r-1)$ is generated by $\mathbf{Z}_p(r)$ and $\{N_{L/H} C_r(\eta_L)\}_{L,\eta_L}$. Clearly the cyclotomic unit $C_r(\eta_L)$ comes from $\varprojlim H^1(\mathbf{Q}(\mu_L, \zeta_{p^n}), \mathbf{Z}_p(r))$. It implies that $N_{L/H} C_r(\eta_L)$ comes from $\varprojlim H^1(F_L(\zeta_{p^n}), \mathbf{Z}_p(r))$ where $F_L := \mathbf{Q}(\mu_L) \cap H$. Therefore

$$\bigoplus_L \left(\varprojlim_n H^1(F_L(\zeta_{p^n}), \mathbf{Z}_p(r)) \right) \longrightarrow \varprojlim_n H^1(H(\zeta_{p^n}), \mathbf{Z}_p(r)) \cong V(r-1)$$

is surjective where the second isomorphism is due to the isomorphism (2.4). Consider a commutative diagram

$$\begin{array}{ccc} \bigoplus_L \varprojlim_n H^1(F_L(\zeta_{p^n}), \mathbf{Z}_p(r)) & \longrightarrow & \varprojlim_n H^1(H(\zeta_{p^n}), \mathbf{Z}_p(r)) \\ \downarrow & & \downarrow \\ \bigoplus_L H^1(F_L(\zeta_{p^n}), \mathbf{Z}_p(r)) & \longrightarrow & H^1(H(\zeta_{p^n}), \mathbf{Z}_p(r)) \end{array}$$

with the surjective top arrow. Due to the isomorphism (2.5), the right vertical arrow is surjective if $r \neq 1$ and $p \geq 3$. In case $p = 2$ it is also surjective (resp. surjective modulo torsion) if $r \neq 1$ and $n \geq 2$ (resp. $n = 1$). Therefore so is the bottom arrow in each case. This completes the proof in the case $K = H(\zeta_{p^n})$.

Let $K \subset \mathbf{Q}_p(\zeta)$ be a general one. Let $H \subset K$ be the maximal unramified extension of $\mathbf{Q}_p$. There is $n \geq 0$ such that $K \subset H(\zeta_{p^n})$. Note $\mathrm{Gal}(H(\zeta_{p^n})/K) \to \mathrm{Gal}(H(\zeta_{p^n})/H) \cong (\mathbf{Z}/p^n)^\times$ is injective. Then one can easily check that the norm map $H^1(H(\zeta_{p^n}), \mathbf{Z}_p(r)) \to H^1(K, \mathbf{Z}_p(r))$ is surjective if $p \geq 3$ and $r \neq 1$ or $p = 2$, $r \neq 1$ and $n \geq 2$. In case $p = 2$ and $n = 1$, it is also surjective modulo torsion. Therefore one can deduce the assertion to the case $H(\zeta_{p^n})$. This completes the proof of Theorem 2.1.

2.3. p-adic polylogarithm. Let $\mathbf{C}_p$ be the completion of the algebraic closure $\overline{\mathbf{Q}}_p$. We denote the p-adic valuation by $|\cdot|_p$. Let $O_{\mathbf{C}_p} = \{z \in \mathbf{C}_p; |z|_p \leq 1\}$ be the valuation ring.

Coleman defined the *i-th p-adic polylogarithm* $l_i(z)$ for each $i \in \mathbf{Z}$ which are the analytic functions on $\mathbf{C}_p - \{1\}$ and has the Taylor expansion

$$l_i(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^i}$$

for $|z|_p < 1$ ([3] VI). When $i = 1$, $l_1(z) = -\log(1-z)$ is the Iwasawa logarithm and when $i \leq 0$, $l_i(z)$ are rational functions which are explicitly given by

$$l_0(z) = \frac{z}{1-z}, \quad l_{-i}(z) = \left(z \frac{d}{dz} \right)^i l_0(z), \quad i \geq 1.$$

Let

$$l_i^{(p)}(z) := l_i(z) - p^{-i} l_i(z^p) = \sum_{\substack{n \geq 1 \\ (p,n)=1}} \frac{z^n}{n^i}.$$

If $|z|_p \leq 1$ and $|z-1|_p = 1$, then it follows from [3] Lemma 7.2 that one has the following congruence relations

$$l_i^{(p)}(z) = \int_{\mathbf{Z}_p^\times} x^{-i} d\mu_z(x) \equiv \frac{1}{1-z^{p^m}} \sum_{\substack{1 \leq n \leq p^m - 1 \\ (p,n)=1}} \frac{z^n}{n^i} \mod p^m O_{\mathbf{C}_p}, \quad m \geq 1 \tag{2.17}$$

on noting $\mu_z(a + p^m \mathbf{Z}_p) = z^a/(1-z^{p^m})$ (see also [6, (3.2.3)]). Note also

$$l_0^{(p)}(z) = \frac{z}{1-z} - \frac{z^p}{1-z^p}, \quad l_{-i}^{(p)}(z) = \left(z\frac{d}{dz}\right)^i l_0^{(p)}(z), \quad i \geq 1.$$

The relationship between l_∞ and $l_i^{(p)}(z)$ is described as follows.

Proposition 2.4. *Let $\eta \in \mu_H - \{1\}$ and $C(\eta) \in U$ the cyclotomic unit as in* (2.10). *Then we have*

$$\begin{aligned} l_\infty(C(\eta)) &= \left(\frac{-1}{1-\eta^{p^m}} \sum_{\substack{1 \leq n \leq p^m - 1 \\ (p,n)=1}} \frac{\eta^n \sigma_n}{n} \right)_{m \geq 1} \in \varprojlim_m \left(O_H/p^m\right)[G_m] \\ &= O_H[[G]]. \end{aligned}$$

In particular letting i be an integer and $\theta_i : \mathcal{O}_H[[G]] \to O_H$ a homomorphism of O_H-algebra given by $\sigma_\alpha \mapsto \alpha^i$ we have

$$\theta_i l_\infty(C(\eta)) = -l_{1-i}^{(p)}(\eta).$$

Proof. Noting $\psi(C(\eta)) = 1 - \eta(X+1)$, the assertion is equivalent to

$$\varprojlim_m \left(\frac{-1}{1-\eta^{p^m}} \sum_{\substack{1 \leq n \leq p^m - 1 \\ (p,n)=1}} \frac{\eta^n (1+X)^n}{n} \right) = \log^{(p)}(1 - \eta(1+X)) \in O_H[[X]].$$

Let D be the differential operator on $O_H[[X]]$ given by $D(f) = (1+X)df/dX$. Noting $D(1+X)^n = n(1+X)^n$ and $D\log^{(p)}(1 - \eta(1+X)) = -\eta(1+X)/(1-\eta(1+X)) + \eta^p(1+X)^p/(1-\eta^p(1+X)^p)$, the assertion is equivalent to saying

$$\frac{-1}{1-\eta^{p^m}} \sum_{\substack{1 \leq n \leq p^m - 1 \\ (p,n)=1}} \eta^n (1+X)^n = \frac{-\eta(1+X)}{1-\eta(1+X)} - \frac{-\eta^p(1+X)^p}{1-\eta^p(1+X)^p}$$

in $O_H[[X]]/(p^m, (1+X)^{p^m}-1)$ and

$$\frac{-1}{1-\eta^{p^m}} \sum_{\substack{1\le n\le p^m-1 \\ (p,n)=1}} \frac{\eta^n}{n} = \log^{(p)}(1-\eta)$$

in $O_H/p^m O_H$ for all $m \geq 1$. However both follow from direct calculations (the details are left to the reader). □

Remark 2.5. We will not use $l_i(z)$ or even $l_i^{(p)}(z)$ as analytic function on $\mathbf{C}_p$ in the proof of Theorem 2.2, but use values $l_i^{(p)}(\eta)$.

2.4. Proof of Theorem 2.2: Case $p \geq 3$. Let the notations be as in Sect. 2.1. Suppose $p \geq 3$. We denote the residue field of H by k_H.

Since V/U is generated by $C(1) = (1-\zeta_{p^n})_{n\geq 1}$, it is enough to show $U = U_{\mathrm{cycl}}$ or equivalently $l_\infty(U_{\mathrm{cycl}}) = l_\infty(U)$. Let $J := (p, \sigma_{1+p}-1) \subset \mathbf{Z}_p[[G]]$ be the Jacobson radical. Since U is finitely generated over $\mathbf{Z}_p[[G]]$ it is enough to prove

$$l_\infty(U)/Jl_\infty(U) = l_\infty(U_{\mathrm{cycl}})/Jl_\infty(U_{\mathrm{cycl}}) \tag{2.18}$$

by Nakayama's lemma. The isomorphism (2.8) induces a commutative diagram

$$\begin{array}{ccc} l_\infty(U) & \xrightarrow[\cong]{\Phi} & \left(O_H^0 + TO_H[[T]]\right) \times O_H[[T]] \times \cdots \times O_H[[T]] \\ \downarrow & & \downarrow \\ l_\infty(U)/Jl_\infty(U) & \xrightarrow{\cong} & \left(k_H^0 \oplus k_H/k_H^0 T\right) \times k_H \times \cdots \times k_H, \end{array} \tag{2.19}$$

where we put $k_H^0 := \ker(\mathrm{Tr}_{k_H/\mathbf{F}_p} : k_H \to \mathbf{F}_p)$. We want to show that $\Phi l_\infty(U_{\mathrm{cycl}})$ is onto the right bottom corner of (2.19). Since the image of $\Phi l_\infty(U_{\mathrm{cycl}})$ is a $\mathbf{Z}_p[[G]]/J = \mathbf{F}_p \times \cdots \times \mathbf{F}_p$-module, it is enough to see it on each component. Namely we show the following.

(A) Let $p_i : O_H[[T]] \times \cdots \times O_H[[T]] \to O_H[[T]]$ be the i-th projection. For each $2 \leq i \leq p-1$, the composition

$$\Phi l_\infty(U_{\mathrm{cycl}}) \xrightarrow{\subset} \prod_{p-1} O_H[[T]] \xrightarrow{p_i} O_H[[T]] \longrightarrow k_H$$

is surjective.

(B) The image of the composition

$$\Phi l_\infty(U_{\mathrm{cycl}}) \xrightarrow{\subset} \prod_{p-1} O_H[[T]] \xrightarrow{p_1} O_H[[T]] \longrightarrow k_H \oplus k_H/k_H^0 T$$

is $k_H^0 \oplus k_H/k_H^0 T$.

2.4.1. Proof of **(A)**. Let $v_i : O_H[[T]] \to O_H$ be the O_H-linear map given by $T \mapsto (1+p)^i - (1+p)$. Then the composition

$$O_H[[G]] \xrightarrow{\Phi} O_H[[T]] \times \cdots \times O_H[[T]] \xrightarrow{p_i} O_H[[T]] \xrightarrow{v_{i+j(p-1)}} O_H$$

coincides with $\theta_{i+j(p-1)}$ in Proposition 2.4. Therefore we have

$$v_{i+j(p-1)} p_i \Phi l_\infty(C(\eta)) = \theta_{i+j(p-1)} l_\infty(C(\eta)) = -l^{(p)}_{1-i-j(p-1)}(\eta) \in O_H, \tag{2.20}$$

for $\eta \in \mu_H - \{1\}$, $1 \le i \le p-1$ and $j \in \mathbf{Z}$. In particular

$$p_i \Phi l_\infty(C(\eta)) \bmod J = v_i p_i \Phi l_\infty(C(\eta)) \bmod p = -l^{(p)}_{1-i}(\eta) \bmod p.$$

Thus the following finishes the proof of **(A)**.

Proposition 2.6. *Suppose* $(p-1) \nmid r$. *Then* $\{l^{(p)}_r(\eta)\ ;\ \eta \in k_H - \{0,1\}\}$ *span* k_H *as a* $\mathbf{F}_p$*-module.*

Proof. Set $S := \{l^{(p)}_r(\eta)\ ;\ \eta \in k_H - \{0,1\}\} \cup \{0\} \subset k_H$. It is enough to show that the cardinality $\sharp S$ is greater than p^{d-1} where $d := [H : \mathbf{Q}_p]$. Due to (2.17) we have

$$l^{(p)}_r(\eta) \equiv \frac{1}{1-\eta^p} \sum_{n=1}^{p-1} \frac{\eta^n}{n^r} \mod p$$

for $\eta \in k_H - \{0,1\}$. Letting $h(z) := \sum_{n=1}^{p-1} z^n/n^r$ be a polynomial with coefficients in $\mathbf{F}_p$, we have $h(1) = 0$ as $(p-1) \nmid r$. Therefore there is a polynomial $h^*(z)$ such that $h(z) = (1-z)h^*(z)$ and hence

$$l^{(p)}_r(\eta) \equiv \frac{h^*(\eta)}{(1-\eta)^{p-1}} \mod p.$$

Letting $g(z) := h^*(z)/(1-z)^{p-1}$ and viewing it as a map $g : k_H - \{1\} \to k_H$ of sets, we have $\mathrm{Image}(g) = S$. Since the degree of $h^*(z)$ is $(p-2)$ we have $\sharp g^{-1}(a) \le p-1$ for $a \ne 0 \in S$ and $\sharp g^{-1}(0) \le p-2$. Hence

$$p^d - 1 = \sum_{a \in S} \sharp g^{-1}(a) \le (p-1)(\sharp S - 1) + (p-2) = (p-1)(\sharp S) - 1$$

which implies $\sharp S > p^{d-1}$. □

2.4.2. Proof of **(B)**. Let $L/\mathbf{Q}_p$ be a finite unramified extension such that $L \supset H$. We denote the ring of integers by O_L and the residue field by k_L.

We use the same notations Φ, p_i etc. for L. Let

$$p_1\Phi l_\infty(C(\eta)) = Q_\eta(T) = q_0(\eta) + q_1(\eta)T + \cdots \in O_L^0 + TO_L[[T]]$$

for $\eta \in \mu_L - \{1\}$. Then

$$\begin{aligned} p_1\Phi l_\infty(N_{L/H}C(\eta)) &= \mathrm{Tr}_{L/H}(Q_\eta(T)) \\ &= \mathrm{Tr}_{L/H}q_0(\eta) + (\mathrm{Tr}_{L/H}q_1(\eta))T + \cdots . \end{aligned}$$

We want to show that the map

$$\begin{aligned} \Phi l_\infty(U_{\mathrm{cycl}}) &\longrightarrow k_H^0 \oplus k_H/k_H^0 T \cong k_H^0 \oplus \mathbf{F}_p, \\ \Phi l_\infty(N_{L/H}C(\eta)) &\longmapsto (\mathrm{Tr}_{L/H}q_0(\eta), \mathrm{Tr}_{L/\mathbf{Q}_p}q_1(\eta)) \end{aligned} \tag{2.21}$$

is surjective.

Lemma 2.7. *For $\eta \in \mu_L - \{1\}$ we have*

$$q_0(\eta) = \frac{-\eta}{1-\eta} - \frac{-\eta^p}{1-\eta^p} \in O_L, \tag{2.22}$$

$$q_0(\eta) - pq_1(\eta) \equiv -l_{1-p}^{(p)}(\eta) \mod p^2 O_L, \tag{2.23}$$

$$p\mathrm{Tr}_{L/\mathbf{Q}_p}q_1(\eta) \equiv \mathrm{Tr}_{L/\mathbf{Q}_p}l_{1-p}^{(p)}(\eta) \mod p^2\mathbf{Z}_p. \tag{2.24}$$

Proof. The last one follows from the above two due to the fact that $\mathrm{Tr}_{L/\mathbf{Q}_p}q_0(\eta) = 0$. We show (2.22) and (2.23). It follows from (2.20) for $i = 1$ that we have

$$\begin{aligned} v_{1+j(p-1)}p_1\Phi l_\infty(C(\eta)) &= Q_\eta((1+p)^{1+j(p-1)} - 1 - p) \\ &= -l_{-j(p-1)}^{(p)}(\eta) \in O_H \end{aligned}$$

for $j \in \mathbf{Z}$. We thus have

$$Q_\eta(0) = q_0(\eta) = -l_0^{(p)}(\eta) = \frac{-\eta}{1-\eta} - \frac{-\eta^p}{1-\eta^p}$$

and

$$\begin{aligned} Q_\eta((1+p)^p - (1+p)) &= q_0(\eta) + q_1(\eta)((1+p)^p - (1+p)) + \cdots \\ &= -l_{1-p}^{(p)}(\eta). \end{aligned}$$

They imply (2.22) and (2.23). □

Proposition 2.8. *Suppose $d := [L : \mathbf{Q}_p] \geq 2$. Then there are $\eta,\ \eta' \in \mu_L - \{1\}$ such that*

$$\left(\frac{\eta}{1-\eta} - \frac{\eta^p}{1-\eta^p}\right) \equiv \left(\frac{\eta'}{1-\eta'} - \frac{\eta'^p}{1-\eta'^p}\right) \mod pO_L \tag{2.25}$$

and

$$\mathrm{Tr}_{L/\mathbf{Q}_p}\big(l^{(p)}_{1-p}(\eta) - l^{(p)}_{1-p}(\eta')\big) = p \times (\textit{unit}). \tag{2.26}$$

Hence $q_0(\eta) \equiv q_0(\eta')$ *and* $\mathrm{Tr}_{L/\mathbf{Q}_p}(q_1(\eta) - q_1(\eta'))$ *is a unit by* (2.22) *and* (2.24).

Proposition 2.8 together with Lemma 2.7 finish the proof of **(B)**. In fact, it is straightforward from (2.22) that the composition

$$\Phi l_\infty(U_{\mathrm{cycl}}) \overset{(2.21)}{\longrightarrow} k_H^0 \oplus \mathbf{F}_p \longrightarrow k_H^0$$

is surjective. Moreover Proposition 2.8 implies that an element $\Phi l_\infty(N_{L/H}C(\eta) - N_{L/H}C(\eta'))$ goes to $(\mathrm{Tr}_{L/H}(q_0(\eta) - q_0(\eta')), \mathrm{Tr}_{L/\mathbf{Q}_p}(q_1(\eta) - q_1(\eta'))) = (0, *) \in k_H^0 \oplus \mathbf{F}_p$ with $* \neq 0$. Hence we have the surjectivity of (2.21).

Proof of Proposition 2.8. One has

$$\frac{1}{p}\left(l^{(p)}_{1-p}(\eta) - \left(\frac{\eta}{1-\eta} - \frac{\eta^p}{1-\eta^p}\right)\right) \equiv \frac{1}{1-\eta^{p^2}} \sum_n \frac{n^{p-1}-1}{p}\eta^n \mod p$$

where n runs over the integers such that $1 \leq n \leq p^2 - 1$ and $(p, n) = 1$. Put

$$l^*(z) := \frac{1}{1-z^{p^2}} \sum_n \frac{n^{p-1}-1}{p} z^n \in \mathbf{F}_p[z, 1/(1-z)].$$

Then (2.26) is equivalent to

$$\mathrm{Tr}_{k_L/\mathbf{F}_p}(l^*(\eta)) \neq \mathrm{Tr}_{k_L/\mathbf{F}_p}(l^*(\eta')). \tag{2.27}$$

Letting

$$\begin{aligned} l(z) := -l^*(z^{-1}+1) &= \sum_n \frac{n^{p-1}-1}{p} z^{p^2-n}(z+1)^n \\ &= \sum_{i=1}^{p-1}\sum_{j=0}^{p-1} \frac{(i+jp)^{p-1}-1}{p} z^{p^2-i-jp}(z+1)^{i+jp} \\ &= \sum_{i=1}^{p-1}\sum_{j=0}^{p-1} \left(\frac{i^{p-1}-1}{p} - i^{p-2}j\right) z^{p^2-i-jp}(z+1)^{i+jp} \\ &= c_1 z + c_2 z^2 + \cdots + c_{p^2} z^{p^2} \in \mathbf{F}_p[z], \end{aligned}$$

(2.27) is written as

$$\mathrm{Tr}_{k_L/\mathbf{F}_p}\left(l\left(\frac{\eta^{-1}}{1-\eta^{-1}}\right)\right) \neq \mathrm{Tr}_{k_L/\mathbf{F}_p}\left(l\left(\frac{\eta'^{-1}}{1-\eta'^{-1}}\right)\right). \tag{2.28}$$

On the other hand (2.25) is equivalent to

$$\begin{aligned}\frac{\eta}{1-\eta}-\frac{\eta'}{1-\eta'} \equiv \frac{\eta^p}{1-\eta^p}-\frac{\eta'^p}{1-\eta'^p} \equiv \left(\frac{\eta}{1-\eta}-\frac{\eta'}{1-\eta'}\right)^p \in k_L \\ \Leftrightarrow \frac{\eta}{1-\eta}-\frac{\eta'}{1-\eta'} \in \mathbf{F}_p \Leftrightarrow \frac{1}{1-\eta}-\frac{1}{1-\eta'} \in \mathbf{F}_p \\ \Leftrightarrow \frac{\eta^{-1}}{1-\eta^{-1}}-\frac{\eta'^{-1}}{1-\eta'^{-1}} \in \mathbf{F}_p. \qquad (2.29)\end{aligned}$$

When η runs over all elements of $k_L - \{0, 1\}$, the element $\eta^{-1}/(1-\eta^{-1})$ runs over all elements of $k_L - \{0, -1\}$. Therefore Proposition 2.8 is equivalent to saying that

$$\mathrm{Tr}_{k_L/\mathbf{F}_p}(l(\nu)) \neq \mathrm{Tr}_{k_L/\mathbf{F}_p}(l(\nu+1)) \quad \text{for some } \nu \in k_L - \{0\}. \qquad (2.30)$$

Note that we do not need to exclude the case $\nu = -1$ because the both sides are zero if $\nu = -1$. The following lemma is the key to the proof.

Lemma 2.9. *$c_1 = c_{2p} = c_{2p+1} = \cdots = c_{p^2} = 0$ and $c_{2p-1} = -1$.*

Proof. By the definition we have

$$c_m = \sum_{i,j}\left(\frac{i^{p-1}-1}{p} - i^{p-2}j\right)\binom{i+jp}{m-p^2+i+jp} \in \mathbf{F}_p$$

where (i, j) runs over the pair of integers such that $1 \leq i \leq p-1$, $0 \leq j \leq p-1$ and $m - p^2 + i + jp \geq 0$. Noting

$$\binom{i+jp}{m-p^2+i+jp} = \binom{i+jp}{p^2-m}$$

and the right hand side is automatically zero if $m - p^2 + i + jp < 0$, one can write

$$c_m = \sum_{i=1}^{p-1}\sum_{j=0}^{p-1}\left(\frac{i^{p-1}-1}{p} - i^{p-2}j\right)\binom{i+jp}{p^2-m}. \qquad (2.31)$$

We have $c_1 = 0$ directly from (2.31). To show the rest we use the following formula.

Claim 2.10. For an indeterminate x and an integer $k \geq 1$ we put $\binom{x}{k} := x(x-1)\cdots(x-k+1)/k!$ and $\binom{x}{0} := 1$. Then we have

$$\binom{xp+i}{k} \equiv \binom{x}{r}\binom{i}{k-rp} \mod p\mathbf{Z}_{(p)}[x]$$

for $1 \leq i \leq p-1$, $0 \leq r \leq p-1$ and $rp \leq k \leq (r+1)p-1$.

Proof. Let $k = rp + j$. In the fraction

$$\binom{i+xp}{k} = \frac{(xp+i)(xp+i-1)\cdots(xp+i-k+1)}{k!}$$

the divisor p appears r-times in the denominator (note $r < p$). In the numerator, the divisor p appears r-times when $i \geq j$ and $(r+1)$-times when $i < j$. This completes the proof in the case $i < j$. Assume $i \geq j$. Write

$$k! = p^r r! \cdot \prod_{\substack{1\leq m\leq k\\(p,m)=1}} m,$$

$$(xp+i)(xp+i-1)\cdots(xp+i-k+1) = p^r x(x-1)\cdots(x-r+1)\cdot \prod_{\substack{i-k+1\leq \ell\leq i\\(p,\ell)=1}} (xp+\ell).$$

Therefore

$$\begin{aligned}\binom{i+xp}{k} &= \frac{x(x-1)\cdots(x-r+1)}{r!}\frac{\prod_\ell (xp+\ell)}{\prod_m m}\\ &\equiv \binom{x}{r}\frac{\prod_\ell \ell}{\prod_m m} \mod p\\ &\equiv \binom{x}{r}\binom{i}{j} \mod p.\end{aligned}$$

This completes the proof in the case $i \geq j$. □

Suppose $2p-1 \leq m \leq p^2$. Let r be the integer satisfying $rp \leq p^2 - m \leq (r+1)p - 1$. It implies $0 \leq r \leq p-2$. By Claim 2.10, we have

$$\begin{aligned}c_m &= \sum_{i=1}^{p-1}\sum_{j=0}^{p-1}\left(\frac{i^{p-1}-1}{p} - i^{p-2}j\right)\binom{j}{r}\binom{i}{p^2-m-rp}\\ &= \sum_{i=1}^{p-1}\sum_{j=0}^{p-1}\left(s_0(i) + s_1(i)j + s_2(i)j^2 + \cdots + s_{r+1}(i)j^{r+1}\right).\end{aligned}$$

(Note $\binom{j}{0} := 1$ by convention.) The above is zero when $r+1 < p-1$ due to the fact that $\sum_{j=0}^{p-1} j^\ell = 0$ for $0 \leq \ell \leq p-2$. If $r = p-2$, then $m = 2p$ or $2p-1$. We have

$$c_{2p} = \sum_{i=1}^{p-1}\sum_{j=0}^{p-1}\left(\frac{i^{p-1}-1}{p} - i^{p-2}j\right)\binom{j}{p-2} = \sum_{i=1}^{p-1} i^{p-2} = 0$$

and

$$\begin{aligned} c_{2p-1} &= \sum_{i=1}^{p-1}\sum_{j=0}^{p-1}\left(\frac{i^{p-1}-1}{p} - i^{p-2}j\right)\binom{j}{p-2}\binom{i}{1} \\ &= \sum_{i=1}^{p-1}\sum_{j=0}^{p-1}\left(\frac{i^{p}-i}{p} - j\right)\binom{j}{p-2} \\ &= -1. \end{aligned}$$

This completes the proof of Lemma 2.9. □

We now prove Proposition 2.8, which is equivalent to (2.30). Put

$$Tl(z) := \sum c_i (z^i + z^{pi} + \cdots + z^{p^{d-1}i})$$

so that we have $\mathrm{Tr}_{k_L/\mathbf{F}_p}(l(\nu)) = Tl(\nu)$. Due to Lemma 2.9, i ranges only over $2 \leq i \leq 2p-1$. There is a canonical one-to-one correspondence between $\mathbf{F}_p[z]/(z^{p^d} - z)$ and the set of polynomials of degree $< p^d$. For a polynomial $f(z)$ we write by $[f(z)] \in \mathbf{F}_p[z]$ the corresponding polynomial of degree $< p^d$. We have

$$[Tl(z)] = \sum c_i [z^i + z^{pi} + \cdots + z^{p^{d-1}i}]$$

with

$$[z^i + z^{pi} + \cdots + z^{p^{d-1}i}] = \begin{cases} z^i + z^{pi} + \cdots + z^{p^{d-1}i} & 2 \leq i \leq p-1 \\ z + z^p + \cdots + z^{p^{d-1}} & i = p \\ z^i + z^{pi} + \cdots + z^{p^{d-2}i} + z^{1+(i-p)p^{d-1}} & p+1 \leq i \leq 2p-1. \end{cases}$$

In the above the maximal degree is $(1 + (p-1)p^{d-1})$ and it is only when $i = 2p-1$. Since $c_{2p-1} = -1$ (Lemma 2.9), $[Tl(z)]$ is a polynomial of degree $(1 + (p-1)p^{d-1})$. Suppose that $\mathrm{Tr}_{k_L/\mathbf{F}_p}(l(\nu)) = \mathrm{Tr}_{k_L/\mathbf{F}_p}(l(\nu+1))$ for all $\nu \in k_L - \{0\}$. It implies that $[Tl(z+1)] - [Tl(z)] = 0$ since the degree of $[Tl(z)]$ is less than $(p^d - 1)$. However we have

$$\begin{aligned} [Tl(z+1)] - [Tl(z)] &= -(z+1)^{1+(p-1)p^{d-1}} + z^{1+(p-1)p^{d-1}} + \cdots \\ &= -z^{(p-1)p^{d-1}} + \cdots \\ &\neq 0. \end{aligned}$$

This is a contradiction, which proves (2.30). This completes the proof of Proposition 2.8. □

We have completed the proof of **(B)** and hence Theorem 2.2 for $p \geq 3$.

2.5. Proof of Theorem 2.2: Case $p = 2$. Let L be a finite unramified extension of $\mathbf{Q}_2$ such that $L \supset H$. We denote by k_L the residue field of L. We put $O_L^0 := \ker(\mathrm{Tr}_{L/\mathbf{Q}_2} : O_L \to \mathbf{Z}_2)$ and $k_L^0 := \ker(\mathrm{Tr}_{k_L/\mathbf{F}_2} : k_L \to \mathbf{F}_2)$.

Recall from (2.9) the isomorphism

$$\Phi : l_\infty(U_L) \xrightarrow{\cong} \left\{ f(T) + g(T)\sigma \in O_L[[T]][\sigma]/(\sigma^2 - 1) \;\middle|\; f(0) - g(0) \in O_L^0 \right\} \quad (2.32)$$

of $\mathbf{Z}_2[[G]] = \mathbf{Z}_2[[T]][\sigma]/(\sigma^2 - 1)$-modules. Write

$$\Phi l_\infty(C(\eta)) = F_\eta(T) + G_\eta(T)\sigma$$
$$F_\eta(T) = f_0(\eta) + f_1(\eta)T + \cdots, \quad G_\eta(T) = g_0(\eta) + g_1(\eta)T + \cdots$$

for $\eta \in \mu_L - \{1\}$. Then

$$\Phi l_\infty(N_{L/H} C(\eta)) = \mathrm{Tr}_{L/H} F_\eta(T) + \mathrm{Tr}_{L/H} G_\eta(T)\sigma.$$

Let $\alpha_k \in \mathbf{Z}_2$ satisfy

$$5^{\alpha_k} = 1 + 4\alpha_k + \binom{\alpha_k}{2} 4^2 + \cdots = \begin{cases} k & \text{if } k \equiv 1 \mod 4 \\ -k & \text{if } k \equiv 3 \mod 4. \end{cases}$$

It follows from Proposition 2.4 and the definition of Φ that we have

$$F_\eta(T) \equiv \frac{-1}{1 - \eta^{2^m}} \sum_{k=1}^{2^{m-2}} \frac{\eta^{4k-3}}{4k-3} (T+5)^{\alpha_{4k-3}} \quad (2.33)$$

$$G_\eta(T) \equiv \frac{-1}{1 - \eta^{2^m}} \sum_{k=1}^{2^{m-2}} \frac{\eta^{4k-1}}{4k-1} (T+5)^{\alpha_{4k-1}} \quad (2.34)$$

modulo $(2^m, (T+5)^{2^{m-2}} - 1)$ for $m \geq 2$. We have

$$f_0(\eta) = \frac{-\eta}{1 - \eta^4}, \quad g_0(\eta) = \frac{-\eta^{-1}}{1 - \eta^{-4}}, \quad (2.35)$$

$$f_1(\eta) \equiv \frac{\eta^5}{1 - \eta^8}, \quad g_1(\eta) \equiv \frac{\eta^{-5}}{1 - \eta^{-8}} \mod 2 \quad (2.36)$$

in a similar way to the case $p \geq 3$ (cf. Lemma 2.7).

We now prove Theorem 2.2 for $p = 2$. We want to prove $l_\infty(U_{\mathrm{cycl}}) = l_\infty(U)$. Let $J = (2, T, \sigma - 1)$ be the maximal ideal of $\mathbf{Z}_2[[T]][\sigma]/(\sigma^2 - 1)$. It is enough to show

$$l_\infty(U_{\mathrm{cycl}})/J l_\infty(U_{\mathrm{cycl}}) = l_\infty(U)/J l_\infty(U) \quad (2.37)$$

by Nakayama's lemma. Let $\iota : O_L[[T]][\sigma]/(\sigma^2 - 1) \xrightarrow{\cong} O_L[[T]] \times O_L[[T]]$ be the isomorphism of $\mathbf{Z}_2[[T]][\sigma]/(\sigma^2 - 1)$-modules given by $f(T) + g(T)\sigma \mapsto (f(T) - g(T), g(T))$ where the action of σ on the target is given

by $\sigma(h_1, h_2) := (-h_1, h_1 + h_2)$. Due to (2.32) we have an isomorphism $\iota\Phi : l_\infty(U_L) \xrightarrow{\cong} (O_L^0 + TO_L[[T]]) \times O_L[[T]]$ and it induces a commutative diagram

$$\begin{array}{ccc} l_\infty(U_L) & \xrightarrow[\cong]{\iota\Phi} & \left(O_L^0 + TO_L[[T]]\right) \times O_H[[T]] \\ \downarrow & & \downarrow \\ l_\infty(U_L)/Jl_\infty(U_L) & \xrightarrow[\cong]{\phi} & k_L^0 \times k_L/k_L^0 \times k_L/k_L^0 \end{array}$$

where the right vertical arrow is the map induced from $(f(T), g(T)) \mapsto (f(0), f'(0), g(0))$. Let $\eta \in \mu_L - \{1\}$. It follows from (2.35) and (2.36) that we have

$$\begin{aligned} \phi l_\infty(C(\eta)) &= (f_0(\eta) - g_0(\eta), f_1(\eta) - g_1(\eta), g_0(\eta)) \\ &= \left(\frac{-\eta}{1-\eta^4} - \frac{-\eta^{-1}}{1-\eta^{-4}}, \frac{\eta^5}{1-\eta^8} - \frac{\eta^{-5}}{1-\eta^{-8}}, \frac{-\eta^{-1}}{1-\eta^{-4}}\right) \\ &= (\lambda + \lambda^2, \lambda + \lambda^2 + \lambda^3 + \lambda^4, (\lambda + \lambda^3)^2) \quad \left(\lambda := \frac{1}{1-\eta}\right) \\ &= (\lambda + \lambda^2, \lambda + \lambda^3, \lambda^4 + \lambda^5) \end{aligned}$$

in $k_L^0 \times k_L/k_L^0 \times k_L/k_L^0$. Hence

$$\phi l_\infty(N_{L/H} C(\eta)) = \left(\mathrm{Tr}_{k_L/k_H}(\lambda + \lambda^2), \mathrm{Tr}_{k_L/k_H}(\lambda + \lambda^3), \mathrm{Tr}_{k_L/k_H}(\lambda^4 + \lambda^5)\right) \tag{2.38}$$

in $k_H^0 \times k_H/k_H^0 \times k_H/k_H^0$. To show (2.37) it is enough to show that the elements (2.38) span $k_H^0 \times k_H/k_H^0 \times k_H/k_H^0$ when L and $\eta \in \mu_L - \{1\}$ run. When $\eta \in \mu_L - \{1\}$ runs, λ runs over all elements of $k_L - \{0\}$. Therefore it is enough to show the following:

Proposition 2.11. *Put*

$$l(\lambda) := (\lambda + \lambda^2, \lambda + \lambda^3, \lambda^4 + \lambda^5) \in k_L^0 \times k_L \times k_L$$

for $\lambda \in k_L$. Let W be the $\mathbf{F}_2$-submodule of $k_H^0 \times k_H \times k_H$ generated by $\{\mathrm{Tr}_{k_L/k_H} l(\lambda)\}_{k_L, \lambda}$ where k_L and λ run over all pairs such that $k_L \supset k_H$ and $\lambda \in k_L$. Then $W \to k_H^0 \times k_H/k_H^0 \times k_H/k_H^0$ is surjective.

Proof. Since the trace maps for finite fields are surjective, we may replace k_H with an arbitrary large extension of k_H. Thus we may assume $d = [k_H : \mathbf{F}_2] \geq 5$.

Claim 2.12. There is a $\lambda \in k_H^\times$ such that $\mathrm{Tr}_{k_H/\mathbf{F}_2}(\lambda^5) \neq 0$. Hence we have

$$l(\lambda) + l(\lambda\zeta) + \cdots + l(\lambda\zeta^4) = (0, 0, v) \in W \text{ with } \mathrm{Tr}_{k_H/\mathbf{F}_2}(v) \neq 0$$

where $\zeta = \zeta_5$ is a primitive 5th root of unity.

Proof. Put

$$T(z) := z^5 + z^{10} + \cdots + z^{5\cdot 2^{d-3}} + z^{2^{d-2}+1} + z^{2^{d-1}+2} \in k_H[z].$$

Then $\mathrm{Tr}_{k_H/\mathbf{F}_2}(\lambda^5) = T(\lambda)$. Since $T(z)$ is a non-zero polynomial of degree $5 \cdot 2^{d-3} < 2^d$ as $d \geq 5$, there is a $\lambda \in k_H^\times$ such that $T(\lambda) \neq 0$. □

Claim 2.13. There is a $\lambda \in k_H^\times$ such that $\mathrm{Tr}_{k_H/\mathbf{F}_2}(\lambda + \lambda^{-1}) \neq 0$. Hence

$$l(\lambda) + l(\lambda^{-1}) + l(\lambda + \lambda^{-1}) = (0, v, *) \in W \text{ with } \mathrm{Tr}_{k_H/\mathbf{F}_2}(v) \neq 0.$$

Proof. Put

$$\begin{aligned} T(z) := {} & z^{2^{d-1}} + z^{2^{d-2}} + \cdots + z^2 + z + z^{-1} + z^{-2} + \cdots + z^{-2^{d-1}} \\ & \in k_H[z, z^{-1}]. \end{aligned}$$

Then $\mathrm{Tr}_{k_H/\mathbf{F}_2}(\lambda + \lambda^{-1}) = T(\lambda)$. Suppose that $T(\lambda) = 0$ for all $\lambda \in k_H^\times$. Put

$$\begin{aligned} T^*(z) := {} & z + z^{2^{d-2}+2^{d-1}} + \cdots + z^{2+2^{d-1}} + z^{1+2^{d-1}} + z^{-1+2^{d-1}} \\ & + \cdots + z^{2^{d-1}-2^{d-2}} + 1. \end{aligned}$$

Then $T^*(\lambda) = 0$ for all $\lambda \in k_H^\times$. Since $T^*(z)$ is a non-zero polynomial of degree $2^{d-2} + 2^{d-1} < 2^d - 1$ as $d \geq 5$, it is impossible. □

Due to Claims 2.12 and 2.13 we have that the image of W contains $\{0\} \times k_H/k_H^0 \times k_H/k_H^0$. Therefore it is enough to show that the composition $W \to k_H^0 \times k_H/k_H^0 \times k_H/k_H^0 \to k_H^0$ is surjective. However it follows from the fact that $\{\lambda + \lambda^2\}_{\lambda \in k_H}$ span k_H^0. This completes the proof of Proposition 2.11. □

We have completed the proof of (2.37) and hence Theorem 2.2 for $p = 2$.

References

1. Asakura, M.: Surjectivity of p-adic regulators on K_2 of Tate curves. Invent. Math. **165**, 267–324 (2006)
2. Coleman, R.: Division values in local fields. Invent. Math. **53**(2), 91–116 (1979)
3. Coleman, R.: Dilogarithms, regulators and p-adic L-functions. Invent. Math. **69**(2), 171–208 (1982)
4. Coleman, R.: Local units modulo circular units. Proc. Amer. Math. Soc. **89**(1), 1–7 (1983)
5. Coates, J., Sujatha, R.: Cyclotomic Fields and Zeta Values. Springer Monographs in Mathematics. Springer, Berlin (2006)
6. Deligne, P.: Le groupe fondamental de la droite projective moins trois points. In: Galois Groups over **Q** (Berkeley, CA, 1987), pp. 79–297. Springer, New York (1989)
7. Jannsen, U.: On the l-adic cohomology of varieties over number fields and its Galois cohomology. In: Galois Groups over **Q** (Berkeley, 1987), pp. 315–360. Springer, New York (1989)