THE HEISENBERG COBOUNDARY EQUATION: APPENDIX TO *EXPLICIT CHABAUTY-KIM THEORY*

ISHAI DAN-COHEN AND STEFAN WEVERS

**Abstract.** Let $p$ be a regular prime number, let $G_{(p)}$ denote the Galois group of the maximal unramified away from $p$ extension of $\mathbb{Q}$, and let $H_{\text{ét}}$ denote the Heisenberg group over $\mathbb{Q}_p$ with $G_{(p)}$-action given by $H_{\text{ét}} = \mathbb{Q}_p(1)^2 \oplus \mathbb{Q}_p(2)$. Although Soulé vanishing guarantees that the map $H^1(G_{(p)}, H_{\text{ét}}) \rightarrow H^1(G_{(p)}, \mathbb{Q}_p(1)^2)$ is bijective, the problem of constructing an explicit lifting of an arbitrary cocycle in $H^1(G_{(p)}, \mathbb{Q}_p(1)^2)$ proves to be a challenge. We explain how we believe this problem should be analyzed, following an unpublished note by Romyar Sharifi, hereby making the original appendix to *Explicit Chabauty-Kim theory* available online in an arXiv-only note.

1. **The Context**

This brief note began its life as an appendix to *Explicit Chabauty-Kim theory for the thrice punctured line in depth two* [DCW], which received an appendectomy prior to publication. Let $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$, let

$$S = \{q_1, \ldots, q_s\}$$

denote a finite set of primes, let

$$S = \text{Spec} \mathbb{Z} \setminus S,$$

let $p$ denote a prime $\notin S$, and let $T = S \cup \{p\}$. Kim’s approach to the study of the set $X(S)$ of $S$-integral points of $X$ involves a certain tower of morphisms of affine finite-type $\mathbb{Q}_p$-varieties. As we explain in *Explicit Chabauty-Kim theory*, its first two steps look like so.

$$H^1_f(G_T, H_{\text{ét}}) \xrightarrow{h_2} \mathbb{A}^3_{\mathbb{Q}_p}$$

$$\cong \pi^*$$

$$H^1_f(G_T, \mathbb{Q}_p(1)^2) \xrightarrow{h_1} \mathbb{A}^2_{\mathbb{Q}_p}$$

Here $G_T$ denotes the Galois group of the maximal unramified outside of $T$ extension of $\mathbb{Q}$, $H_{\text{ét}}$ denotes the Heisenberg group object with $G_T$-action given simply by $H_{\text{ét}} = \mathbb{Q}_p(1)^2 \oplus \mathbb{Q}_p(2)$, and the $H^1_f$’s are certain subschemes of nonabelian cohomology varieties. The map induced by abelianization

$$\pi : H_{\text{ét}} \rightarrow \mathbb{Q}_p(1)^2$$

*Date: March 20, 2014.*
on the level of \( H^1_1 \)'s fits in a commuting square like so.

\[
\begin{array}{c}
H^1_1(G_T, H_{\text{et}}) \xrightarrow{\sim} H^1(G_T, H_{\text{et}}) \\
\xrightarrow{\pi_\ast} H^1_1(G_T, \mathbb{Q}_p(1)^2) \xrightarrow{\sim} H^1(G_T, \mathbb{Q}_p(1)^2) \\
\mathbb{Q}_p^S \xrightarrow{\pi_\ast} \mathbb{Q}_p^T
\end{array}
\]

Our main result in *Explicit Chabauty-Kim theory* is a complete computation of the map

\[
h_2 \circ \pi^{-1}_\ast : \mathbb{Q}_p^S \to \mathbb{Q}_p^T.
\]

Since our methods there where somewhat indirect, we document here our initial attempt to compute \( \pi^{-1}_\ast \) directly.

## 2. The Problem

2.1. By Corollary 6.2.3 of [DCW], an \( A \)-point of \( H^1_1(G_T, \mathbb{Q}_p(1)) \) may be written \( \kappa_x \), where

\[
x = q_1^{x_1} \cdots q_s^{x_s}
\]

is a formal product of powers, with \( x_1, \ldots, x_r \in A \). If

\[
y = q_1^{y_1} \cdots q_s^{y_s}
\]

denotes another point, the cup product \( \kappa_y \cup \kappa_x \) is an element of \( Z^1(G_T, A(2)) \). For simplicity, restrict attention to the case \( A = \mathbb{Q}_p \), and consider the cochain complex

\[
0 \to \mathcal{C}^0(\mathbb{Q}_p(2)) \to \mathcal{C}^1(\mathbb{Q}_p(2)) \to \mathcal{C}^2(\mathbb{Q}_p(2)) \to \mathcal{C}^3(\mathbb{Q}_p(2)) \to \cdots
\]

for the cohomology of \( G_T \) with coefficients in \( \mathbb{Q}_p(2) \). By the vanishing results

\[
H^1(G_T, \mathcal{O}_p(2)) = H^2(G_T, \mathcal{O}_p(2)) = 0,
\]

the equation

\[
\kappa_y \cup \kappa_x = d\alpha
\]

in \( \mathcal{C}^2 \) admits a solution \( \alpha \in \mathcal{C}^1 \), unique up to translation by the coboundary \( d\beta : \sigma \mapsto \beta - \sigma(\beta) \) of an element \( \beta \in \mathbb{Q}_p(2) \). Recalling the definition of the cup product and the second coboundary, we have

\[
\kappa_x(\sigma) \otimes \sigma \kappa_y(\tau) = \alpha(\sigma\tau) - \sigma\alpha(\tau) - \alpha(\sigma).
\]

Here, \( \sigma \) and \( \tau \) vary over \( G_T \). We call this the *Heisenberg coboundary equation*.

2.2. By §5 of [DCW], we have an exact sequence

\[
1 \longrightarrow \mathcal{O}_p(2) \longrightarrow H_{\text{et}} \xrightarrow{\Sigma} \mathcal{O}_p(1)^2 \longrightarrow 1
\]

of nonabelian \( G_T \)-modules, which is split if we identify \( H_{\text{et}} \) with its Lie algebra and forget the bracket. Fix a point \( (x, y) \in (\mathbb{Z}[S^{-1}] \otimes \mathcal{O}_p)^2 \) in the source of the unipotent \( p \)-adic Hodge morphism in depth one. We then have associated Kummer cocycles \( \kappa_x, \kappa_y : G_T \to \mathcal{O}_p(1) \), and by composing with \( \Sigma \), we obtain a candidate \( \Sigma(\kappa_x, \kappa_y) \in C^1(G_T, H_{\text{et}}) \) for a lifting of \( (\kappa_x, \kappa_y) \) to depth two. By segment 2.3.2 of [DCW], its failure to be a cocycle is measured by a solution \( \alpha \) of the Heisenberg coboundary equation. So if we set \( \kappa_{x,y} := \alpha^{-1} \Sigma(\kappa_x, \kappa_y) \), we obtain a representative for the element of \( H^1(G_T, H_{\text{et}}) \) which maps to \( (\kappa_x, \kappa_y) \) in \( H^1(G_T, \mathcal{O}_p(1)^2) \).

2.3. The problem then, is to make the solution \( \alpha \) of the Heisenberg coboundary equation in some way explicit.
3. Steps towards its solution

3.1. Soulé’s proof of the vanishing of $H^2(Q_p(2))$ is not well adapted to this application. A simpler proof is given by Romyar Sharifi in an unpublished note [Sha], for the case $p = 2$. As Sharifi points out, the essential property of the even prime which makes his proof possible is its regularity. Sharifi’s proof goes roughly as follows. Let $K_T$ denote the maximal unramified outside $T$ extension of $Q$. Let $G_{T,n}$ denote the Galois group of $K_T$ over $Q(\zeta_{p^n})$. Similarly, we let $G_{T,\infty}$ denote the Galois group of $K_T$ over $Q(\zeta_{p^\infty})$. Noting that the Galois group of $Q(\zeta_{p^n})/Q$ is $(Z/p^n)^*$, we have the following tower of fields and Galois groups for each $n$.

$$
\begin{array}{ccc}
K_T & \rightarrow & G_{T,n} \\
\downarrow & & \downarrow \\
Q(\zeta_{p^n}) & \rightarrow & G_T \\
& \downarrow & \\
(\mathbb{Z}/p^n)^* & \rightarrow & Q
\end{array}
$$

By direct computation applied to the low degree terms of the Hochschild-Serre spectral sequence, we obtain an isomorphism

$$(\ast) \quad H^1(G_T, Q_p(2)) \cong H^1(G_{T,\infty}, Q_p(2))^{\mathbb{Z}_p}.$$ 

On the other hand, for $p$ regular, we have

$$(\ast\ast) \quad Q_p \otimes_{\mathbb{Z}_p} (\mathbb{Z}[T^{-1}, \zeta_{p^n}]^*/p)(1) = H^1(G_{T,\infty}, Q_p(2)).$$

The subscript $/p$ indicates $p$-adic completion. The argument here may be summarized as follows: there’s always an injection from the left to the right coming from the Kummer exact sequence; the cokernel lives inside the Picard group (suitably interpreted), whose (pro-)order is (pro-)coprime to $p$. A study of the action of $\mathbb{Z}_p^*$ on $Q_p \otimes_{\mathbb{Z}_p} (\mathbb{Z}[T^{-1}, \zeta_{p^n}]^*/p)(1)$ now leads to the conclusion that

$$H^1(G_T, Q_p(2)) = Q_p.$$ 

Finally, Poitou-Tate duality is used as a vehicle to get to $H^2$.

Actually, throughout most of the proof, Sharifi works with $n$ finite. For $n$ finite, statements analogous to $(\ast)$, $(\ast\ast)$ fail. Their failure however, is measured by groups whose order turns out to be finite and bounded in $n$.

3.2. Sharifi’s use of Poitou-Tate duality presents for us an obstacle. On the other hand, since many regular primes are known to exist (see, for instance §5.3 of Washington [Was]), the stipulation that $p$ be regular is relatively harmless. So a possible approach may be to attack the vanishing of $H^2$ (or at least of the relevant elements of $H^2$) directly, by methods inspired by Sharifi’s computation of $H^1$. To do so, we would replace $3.1(\ast)$ by an analysis of the map

$$(\diamond) \quad H^2(G_T, Q_p(2)) \rightarrow H^2(G_{T,\infty}, Q_p(2))^{\mathbb{Z}_p},$$

and we would replace $3.1(\ast\ast)$ by the map

$$(\diamond\diamond) \quad Q_p \otimes_{\mathbb{Z}_p} K_2^M(\mathbb{Z}[\zeta_{p^\infty}, T^{-1}]) \rightarrow H^2(G_{T,\infty}, Q_p(2)),$$

while keeping track of the $\mathbb{Z}_p^*$ action.
4. AN ENSUING FAMILY OF SPECTRAL SEQUENCES IN GALOIS COHOMOLOGY

4.1. If $3.2(\Phi)$ fails to be bijective, the failure is best measured by certain terms in an associated family of spectral sequences. Let

$$1 \to N \to G \to Q \to 1$$

be a short exact sequence of (topological) groups, and $A$ a (continuous) $\mathbb{Z}[G]$-module whose addition law we denote by $\ast$. Then the (continuous) cohomology groups $H^q(N, A)$ have a natural structure of (continuous) $\mathbb{Z}[Q]$-module, and there's a spectral sequence

$$E_2^{p,q} = H^p(Q, H^q(N, A)) \Rightarrow H^{p+q}(G, A) .$$

Elements of $H^1(N, A)$ may be represented by (continuous) maps $\phi : N \to A$ which satisfy

$$\phi(\sigma \tau) = \phi(\sigma) \ast \sigma \phi(\tau) .$$

If $\phi$ is such a map and $\alpha$ is an arbitrary element of $Q$, then the action of $Q$ on $H^1(N, A)$ is given in terms of cocycles by lifting $\alpha$ arbitrarily to an element $\gamma$ of $G$ and declaring that for any $\eta \in N$,

$$\phi^\alpha(\eta) = \alpha^{-1} \phi(\gamma \eta \gamma^{-1}) .$$

See §5, 6 of Chapter VII of [Ser].

4.2. For each $n > m$, we may apply this to the short exact sequence

$$1 \to G_{T,n} \to G_T \to (\mathbb{Z}/p^n)^* \to 1 ,$$

with coefficients in $(\mathbb{Z}/p^m)(2)$. If we set

$$m_n E_2^{p,q} := H^p((\mathbb{Z}/p^n)^*; H^q(G_{T,n}; \mathbb{Z}/p^m(2)))$$

and

$$m_n H^r := H^r(G_T; \mathbb{Z}/p^m(2)) ,$$

then there’s a spectral sequence

$$m_n E_2^{p,q} \Rightarrow m_n H^r .$$

Relevant terms and arrows of this spectral sequence are pictured below.

4.3. We now discuss the terms $m_n E_2^{2,0}$. We set $n = m$ for simplicity.

**Proposition.** Each $m_n E_2^{2,0} = H^2((\mathbb{Z}/p^n)^*, H^0(G_{T,n}, \mathbb{Z}/p^n(2)))$ is a finite group of bounded order.

The proof is in segments 4.4–4.6.
4.4. $G_{T,n}$ acts trivially on $\mathbb{Z}/p^n(2)$, so

$$H^0(G_{T,n}, \mathbb{Z}/p^n(2)) = \mathbb{Z}/p^n(2).$$

We have a short exact sequence of groups

$$0 \to 1 + (p) \to (\mathbb{Z}/p^n)^* \to \mathbb{F}_p^* \to 0$$

from which we obtain a spectral sequence

$$F_2^{p,q} = H^p(\mathbb{F}_p, H^q(1 + (p), \mathbb{Z}/p^n(2))) \Rightarrow H^{p+q}((\mathbb{Z}/p^n)^*, \mathbb{Z}/p^n(2)).$$

It suffices to show that the terms $F_2^{2,0}$, $F_2^{1,1}$, $F_2^{0,2}$ are finite groups of bounded order. But since $\mathbb{F}_p^*$ itself is finite cyclic of bounded order, it suffices to show that the three cohomologies $H^0, H^1, H^2(1 + (p), (\mathbb{Z}/p^n(2)))$ are finite groups of bounded order.

4.5. Let $C$ be a finite cyclic group with generator $\sigma$, consider the elements $1 - \sigma$, $N := \sum_{\tau \in C} \tau$ of the group algebra $\mathbb{Z}[C]$, and let $A$ be a $\mathbb{Z}[C]$-module. Then the sequence

$$0 \to A \xrightarrow{\sigma - 1} A \xrightarrow{N} A \xrightarrow{\sigma - 1} A \xrightarrow{N} \cdots,$$

in which the first $A$ is in degree zero, forms a complex $A^\bullet$ and

$$H^i(C, A) = H^iA^\bullet.$$

4.6. Returning to the situation and the notation of the proposition, we note that $1 + (p)$ is generated by the element $e^p = 1 + p + \frac{e^p}{2p} + \cdots$ and that $e^p$ acts on $\mathbb{Z}/p^n(2)$ by multiplication by $e^{2p}$. Thus, to complete the proof of the proposition, we need only note that (under our assumption that $p \neq 2$)

$$v_p(e^{2p} - 1) = 1,$$

so that the endomorphism of $\mathbb{Z}/p^n$ given by multiplication by $e^{2p} - 1$ has kernel $(p^{n-1})$ and cokernel $\mathbb{F}_p$, both of which have order $p$, hence in particular bounded, as hoped.

4.7. For the remainder of the section we focus our attention on the terms

$$m_nE_2^{1,1} = H^1((\mathbb{Z}/p^n)^*; H^1(G_{T,n}; \mathbb{Z}/p^n(2))).$$

We again set $n = m$ for simplicity.

4.8. We denote the group $\mu_{p^n}(\mathbb{Q}(\zeta_{p^n}))$ of $(p^n)^{\text{th}}$ roots of 1 in $\mathbb{Q}(\zeta_{p^n})$ by $\mu_{p^n}$ for short. $\mu_{p^n}$ is isomorphic to $\mathbb{Z}/p^n(2)$ as a $\mathbb{Z}/p^n$-module. Moreover, if we let an arbitrary element $\alpha$ of $(\mathbb{Z}/p^n)^*$ act on an arbitrary element $\zeta$ of $\mu_{p^n}$ by $\zeta^{\alpha^2}$, then any such isomorphism becomes equivariant with the action of $(\mathbb{Z}/p^n)^*$. Recalling our formula for the action of a quotient group on the first cohomology of the kernel in terms of cocycles ([1.1]), and noting that $G_{T,n}$ acts trivially on $\mathbb{Z}/p^n(2)$, we obtain an isomorphism

$$H^1(G_{T,n}, \mathbb{Z}/p^n(2)) \cong \text{Hom}(G_{T,n}, \mu_{p^n})$$

which is not canonical, but is nevertheless equivariant for the action of $(\mathbb{Z}/p^n)^*$ on $\text{Hom}(G_{T,n}, \mu_{p^n})$ given in terms of a continuous map

$$\phi : G_{T,n} \to \mu_{p^n},$$

an $\eta \in G_{T,n}$, an $\alpha \in (\mathbb{Z}/p^n)^*$, and a lifting $\gamma$ of $\alpha$ to $G_T$, by the formula

$$\phi^\alpha(\eta) = (\phi(\gamma\eta\gamma^{-1}))^{\alpha^2}.$$
4.9. Let
\[ E = \{ a \in \mathbb{Q}(\zeta_{p^n})^* \mid v(a) \equiv 0 \mod p^n \quad \forall v \not| T \} . \]
Given an element \( \alpha \in (\mathbb{Z}/p^n)^* \), and an element \( a \in E/\mathbb{Q}(\zeta_{p^n})^*p^n \), we let \( \alpha \) act on \( a \) by
\[ \alpha^{-1}(a)^{\alpha^{-1}} . \]
Here, the \( \alpha^{-1} \) on the left acts on \( a \) through the Galois action of \((\mathbb{Z}/p^n)^* \) on \( \mathbb{Q}(\zeta_{p^n}) \), while the \( \alpha^{-1} \) in the exponent (which may equivalently be put inside the parentheses) denotes multiplication of the base by itself “\( \alpha^{-1} \) many times”, an operation which is only well defined modulo \( \mathbb{Q}(\zeta_{p^n})p^n \).

4.10. An element \( a \in E \) gives rise to a Kummer cocycle \( \kappa_a \), which is unramified outside \( T \). This means that \( \kappa_a \) defines a map \( G_{T,n} \to \mu_{p^n} \) given in terms of an element \( \eta \in G_{T,n} \) and a \((p^n)\)th root \( a^{1/p^n} \) of \( a \), by the formula
\[ \kappa_a(\eta) = \frac{\eta(a^{1/p^n})}{a^{1/p^n}} . \]

4.11. Proposition. In the notation and the situation of paragraphs 4.9 and 4.10, the assignment
\[ a \mapsto \kappa_a \]
defines a \((\mathbb{Z}/p^n)^*\)-equivariant isomorphism
\[ E/\mathbb{Q}(\zeta_{p^n})^*p^n \cong \text{Hom}(G_{T,n}, \mu_{p^n}) . \]
The proof is in segments 4.12–4.13.

4.12. Fix an algebraic closure \( \overline{\mathbb{Q}} \) of \( \mathbb{Q}(\zeta_{p^n}) \), let \( H \) denote the Galois group of \( \overline{\mathbb{Q}} \) over \( \mathbb{Q}(\zeta_{p^n}) \) and let \( N \) denote the Galois group of \( K_T \) over \( \mathbb{Q}(\zeta_{p^n}) \):

\[
\begin{array}{c}
\overline{\mathbb{Q}} \\
\downarrow \quad \downarrow \quad \downarrow \\
K_T \\
\downarrow \quad \downarrow \quad \downarrow \\
G_{T,n} \\
\downarrow \quad \downarrow \quad \downarrow \\
\mathbb{Q}(\zeta_{p^n})
\end{array}
\]

Evaluating the Kummer exact sequence
\[ 1 \to \mu_{p^n} \to \mathbb{G}_m \to \mathbb{G}_m \to 1 \]
on \( \overline{\mathbb{Q}} \), applying invariants with respect to the action of \( H \), recalling Hilbert’s theorem 90, and noting that \( H \) acts trivially on \( \mu_{p^n} \), we obtain an isomorphism
\[ \kappa : \mathbb{Q}(\zeta_{p^n})^*/\mathbb{Q}(\zeta_{p^n})^{*p^n} \cong \text{Hom}(H, \mu_{p^n}) . \]
Then
\[ \kappa^{-1}(\text{Hom}(G_{T,n}, \mu_{p^n})) = E/\mathbb{Q}(\zeta_{p^n})^{*p^n} \]
Indeed, given \( a \in E \), \( \kappa_a \) factors through \( G_{T,n} \) if and only if
\[ \eta(a^{1/p^n}) = a^{1/p^n} \]
for all \( \eta \in N \), if and only if
\[ \mathbb{Q}(\zeta_{p^n})(a^{1/p^n}) \subset K_T , \]
if and only if \( \mathbb{Q}(\zeta_{p^n})(a^{1/p^n}) \) is unramified outside \( T \), if and only if
\[ v(a) \equiv 0 \mod p^n \quad \forall v \not| T . \]
4.13. It remains to verify that the map $\kappa$ is equivariant with respect to the action of $(\mathbb{Z}/p^n)^*$. To this end, fix $\alpha \in (\mathbb{Z}/p^n)^*$, $a \in E$, $\eta \in G_{T,n}$, and $\gamma \in G_T$ mapping to $\eta$. Then we have
\[
\kappa_\alpha^a(\eta) = (\kappa_\alpha(\gamma\eta^{-1}))^\alpha^{-2} = (\gamma\eta^{-1}(a^{1/p^n}))^{\alpha^{-2}} = (\gamma\eta(\gamma^{-1}a)^{1/p^n})^{\alpha^{-2}} = (\eta(\alpha^{-1}a)^{1/p^n})^{\alpha^{-1}} = (\eta(\alpha^{-1}a\alpha^{-1})^{1/p^n} = (\kappa_{\alpha^{-1}a^{-1}}(\eta),
\]
indeed.

4.14. **Proposition.** Let $\tilde{T}$ denote the set of primes of $\mathbb{Z}[\zeta_{p^n}]$ above $T$. We identify $\tilde{T}$ with the set of corresponding valuations of $\mathbb{Q}(\zeta_{p^n})$. Given $\alpha \in (\mathbb{Z}/p^n)^*$ and $b \in (\mathbb{Z}/p^n)^\tilde{T}$, we let $\alpha$ act on $b$ by
\[
(\alpha \star b)_v = \alpha^{-1}b_{\alpha^{-1}(v)}.
\]
Then the formula
\[
a \mapsto (v(a))_{v \in \tilde{T}}
\]
defines a $(\mathbb{Z}/p^n)^*$-equivariant isomorphism
\[
E_{\mathbb{Q}(\zeta_{p^n})^*/\mathbb{Z}[\zeta_{p^n}]^*} \to (\mathbb{Z}/p^n)^{\tilde{T}}.
\]

**Proof.** By [Was, Corollary 10.5], the $p$-part of the Picard group of $\mathbb{Z}[\zeta_{p^n}]$ vanishes, so multiplication by $p^n$ on $\text{Pic} \mathbb{Z}[\zeta_{p^n}]$ is an automorphism. Evaluating the short exact sequence of sheaves
\[
0 \to \mathcal{O}^* \to \mathcal{K}^* \to \text{Div} \to 0,
\]
together with the endomorphism given by multiplication by $p^n$, on $\mathbb{Z}[\zeta_{p^n}]$ (and recalling that on an integral scheme, $\mathcal{K}^*$ is flasque), we obtain the following diagram
\[
\begin{array}{ccccccc}
0 & \to & \mathbb{Q}(\zeta_{p^n})^*/\mathbb{Z}[\zeta_{p^n}]^* & \to & \text{Div} \mathbb{Z}[\zeta_{p^n}] & \to & \text{Pic} \mathbb{Z}[\zeta_{p^n}] & \to & 0 \\
p^n & \downarrow & p^n & & p^n & & p^n & & 0 \\
0 & \to & \mathbb{Q}(\zeta_{p^n})^*/\mathbb{Z}[\zeta_{p^n}]^* & \to & \text{Div} \mathbb{Z}[\zeta_{p^n}] & \to & \text{Pic} \mathbb{Z}[\zeta_{p^n}] & \to & 0 \\
& & & & & & & \downarrow & & 0 \\
& & & & & & & \downarrow & & 0 \\
& & & & & & & \downarrow & & 0 \\
& & & & & & & \downarrow & & 0 \\
& & & & & & & \downarrow & & 0 \\
& & & & & & & 0 & & 0
\end{array}
\]
in which all rows and columns are exact. Here \([\mathbb{Z}[\zeta_p^n]]_0\) denotes the set of (nonzero) primes of \([\mathbb{Z}[\zeta_p^n]]\) (in this notation, \(\text{Div} \mathbb{Z}[\zeta_p^n] = \mathbb{Z}[\mathbb{Z}[\zeta_p^n]]_0\)). The snake lemma produces an isomorphism
\[
\mathbb{Q}(\zeta_p^n)^*/\mathbb{Z}[\zeta_p^n]^* \overset{\cong}{\longrightarrow} (\mathbb{Z}/p^n)^{[\mathbb{Z}[\zeta_p^n]]_0}.
\]
It is clear now that the preimage of \((\mathbb{Z}/p^n)^\sim\) is as stated in the theorem.

Regarding equivariance, we note that if \(K/k\) is a Galois extension, \(a \in K\), \(\alpha\) is an automorphism of \(K/k\), and \(v\) is a place of \(K\), then \(\alpha\) induces an isomorphism
\[
K_v \overset{\cong}{\longrightarrow} K_{\alpha(v)},
\]
so \(v(\alpha(a)) = \alpha(v)(a)\). This completes the proof of the proposition. □

4.15. The sequence
\[
0 \to \mu_p^n \to \mathbb{Z}[\zeta_p^n]^* \overset{p^n}{\longrightarrow} \mathbb{Z}[\zeta_p^n]^* \to E \overset{\mathbb{Q}(\zeta_p^n)^*p^n}{\longrightarrow} \mathbb{Z}[\zeta_p^n]^* \overset{\mathbb{Q}(\zeta_p^n)^*p^n}{\longrightarrow} 0
\]
is exact.
This is clear.

4.16. Summarizing, we have the following diagram of \((\mathbb{Z}/p^n)^*\)-modules, in which the vertical sequence is exact.

\[
\begin{array}{c}
0 \\
\mathbb{Z}[\zeta_p^n]^* \\
\mathbb{Z}[\zeta_p^n]^*p^n \\
E \\
\mathbb{Q}(\zeta_p^n)^*p^n \\
\text{Hom}(G_{T,n}, \mu_p^n) \\
(\mathbb{Z}/p^n)^\sim \\
0
\end{array}
\]

We end our study of the terms \(nE_2^{1,1}\) with a discussion of the structure of
\[
\frac{\mathbb{Z}[\zeta_p^n]^*}{\mathbb{Z}[\zeta_p^n]^*p^n}
\]
as \((\mathbb{Z}/p^n)^*\)-module.

4.17. Proposition. Denote \(\zeta_p^n\) by \(\zeta\) for short. For \(a \in (\mathbb{Z}/p^n)^*\), let
\[
\xi_a = \zeta^{\frac{1-a}{2}} - \frac{1}{1 - \zeta}.
\]
Then we have
(1) \(\xi_1 = 1\),
and for each \(a \in (\mathbb{Z}/p^n)^*\),
(2) \(\xi_a \equiv \xi_{-a} \mod \mathbb{Z}[\zeta_p^n]^*p^n\).
The elements $\xi_a$ of $\mathbb{Z}[\zeta_{p^n}]^*/\mathbb{Z}[\zeta_{p^n}]^{*p^n}$ parametrized by

$$a \in (\mathbb{Z}/p^n)^*/(-1)$$

are free except for the single relation (1). If $B$ denotes the $\mathbb{Z}/p^n$-submodule generated by these elements, then

$$\mathbb{Z}[\zeta_{p^n}]^*/\mathbb{Z}[\zeta_{p^n}]^{*p^n} = \mu_{p^n} \oplus B .$$

The proof is in paragraphs 4.18–4.19.

4.18. Equation (1) is clear. To verify (2), we carry out the following computation inside $\mathbb{Z}[\zeta_{p^n}]^*$:

$$\xi_{-a} = \zeta^{1+a} \cdot \frac{\zeta^a}{\zeta^a} \cdot \frac{1 - \zeta^{-a}}{1 - \zeta} \cdot \frac{1 - \zeta^a}{1 - \zeta}$$

$$= \zeta^{1+a} \cdot \frac{-1}{\zeta^a} \cdot \frac{1 - \zeta^{-a}}{1 - \zeta}$$

$$= -\xi_a ,$$

and note that

$$-1 = (-1)^{p^n} \equiv 1 \mod \mathbb{Z}[\zeta_{p^n}]^{*p^n} .$$

4.19. Let $U := \mathbb{Z}[\zeta_{p^n}]^*$, let $C^+$ denote the subgroup generated by the elements $\xi_a$, $a \in (\mathbb{Z}/p^n)^*$, and let $U^+$ denote the subgroup of $U$ of totally real units. Then by [Was, Theorem 8.2], $C^+$ is a subgroup of $U^+$ of index $h^+$, the class number of the maximal totally real subfield. By [Was, Theorem 4.12], $\mu_{p^n} \oplus U^+$ has index 1 or 2 in $U$. Since $h^+|h$ and $h$ is coprime to $p$, it follows that $\mu_{p^n} \oplus C^+ \leq U$ is a subgroup of finite index coprime to $p$. According to the Dirichlet unit theorem,

$$U \cong \mu_{p^n} \oplus \mathbb{Z}^{r+s-1}$$

where $r$ is the number of real places, and $s$ is the number of complex conjugate pairs of complex places. Thus, in our case, $r = 0$ and

$$s = \left| (\mathbb{Z}/p^n)^*/(-1) \right| .$$

It follows that the $\xi_a$ generate a free abelian group of rank $s - 1$, and that their image modulo $U^{p^n}$, together with $\mu_{p^n}$, generates all of $U/U^{p^n}$. This completes the proof of the proposition.

4.20. Let $(\mathbb{Z}/p^n)^*$ act on $\mathbb{Z}[\zeta_{p^n}]^*/\mathbb{Z}[\zeta_{p^n}]^{*p^n}$ by $\beta \circ a = \beta(a)^\beta$. This is the action induced by the action defined in paragraph 4.9 except for having taken the liberty to precompose with the automorphism of $(\mathbb{Z}/p^n)^*$ given by $\alpha \mapsto \alpha^{-1}$. We recall that here multiplication by $\beta$ on the left refers to the Galois action, while the exponent refers to multiplication inside $\mathbb{Z}[\zeta_{p^n}]^*$.

4.21. Proposition. We have

$$(3) \quad \beta \circ \zeta = \zeta^{\beta^2}$$

for any $\zeta \in \mu_{p^n}$, and

$$(4) \quad \beta \circ \xi_a = \xi_a^{\beta} \xi_{-\beta} .$$

Proof. Equation (3) is clear. To verify (4), we compute, focusing on the Galois action:

$$\beta(\xi_a) = \zeta^{\beta \frac{1-a}{2}} \frac{1 - \zeta^{-a}}{1 - \zeta^a}$$

$$= \zeta^{\frac{1-a}{2}} \cdot \frac{1 - \zeta^{-a}}{1 - \zeta} \cdot \frac{1 - \zeta^a}{1 - \zeta} \cdot \frac{1}{\zeta^{-1}}$$

$$= \xi_{\beta a} \xi_{-\beta} . \quad \square$$
References

[DCW] I. Dan-Cohen and S. Wewers. Explicit chabauty-kim theory for the thrice punctured line in depth two. Preprint.

[Ser] Jean-Pierre Serre. Corps locaux. Hermann, Paris, 1968. Deuxième édition, Publications de l’Université de Nancago, No. VIII.

[Sha] Romyar Sharifi. On a result of Soulé. Unpublished, available at http://math.arizona.edu/~sharifi/soule2.pdf, 2000.

[Was] Lawrence C. Washington. Introduction to cyclotomic fields, volume 83 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1982.

I.D.: FAKULTÄT FÜR MATHEMATIK, UNIVERSITÄT DUISBURG-ESSEN, UNIVERSITÄTSTRASSE 2, 45117 Essen, Germany
S.W.: UNIVERSITÄT ULM, INSTITUT FÜR REINE MATHEMATIK, HELMHOLTZSTRASSE 18, 89069 Ulm, Germany

E-mail address (I.D.): ishaidc@gmail.com
E-mail address (S.W.): stefan.wewers@uni-ulm.de