Chapter 12
On 3-nilpotent obstructions to π_1 sections for $\mathbb{P}^1_{\mathbb{Q}} - \{0,1,\infty\}$

Kirsten Wickelgren*

Abstract We study which rational points of the Jacobian of $\mathbb{P}^1_k - \{0,1,\infty\}$ can be lifted to sections of geometrically 3-nilpotent quotients of étale π_1 over the absolute Galois group. This is equivalent to evaluating certain triple Massey products of elements of $k^* \subseteq \mathrm{H}^1(G_k, \hat{\mathbb{Z}}(1))$ or $\mathrm{H}^1(G_k, \mathbb{Z}/2)$. For $k = \mathbb{Q}_p$ or $\mathbb{R}$, we give a complete mod 2 calculation. This permits some mod 2 calculations for $k = \mathbb{Q}$. These are computations of obstructions of Jordan Ellenberg.

Key words: Anabelian geometry, nilpotent approximation.

12.1 Introduction

The generalized Jacobian of a pointed smooth curve can be viewed as its abelian approximation. It is natural to consider non-abelian nilpotent approximations. Grothendieck's anabelian conjectures predict that smooth hyperbolic curves over certain fields are controlled by their étale fundamental groups. In particular, approximating π_1 should be similar to approximating the curve. We study the effect of 2 and 3-nilpotent quotients of the étale fundamental group of $\mathbb{P}^1 - \{0,1,\infty\}$ on its rational points, using obstructions of Jordan Ellenberg.

More specifically, a pointed smooth curve X embeds into its generalized Jacobian via the Abel-Jacobi map. Applying π_1 to the Abel-Jacobi map gives the abelianization of the étale fundamental group of X. Quotients by subgroups in the lower central series lie between $\pi_1(X)$ and its abelianization, giving rise to obstructions to

Kirsten Wickelgren
Harvard University, Cambridge MA USA
e-mail: wickelgren@post.harvard.edu

* Supported by an NSF Graduate Research Fellowship, a Stanford Graduate Fellowship, and an American Institute of Math Five Year Fellowship

a rational point of the Jacobian lying in the image of the Abel-Jacobi map. These obstructions were defined by Ellenberg in [Ell00].

For simplicity, first assume that X is a proper, smooth, geometrically connected curve over a field k. The absolute Galois group of k will be denoted by

$$G_k = \mathrm{Gal}(\overline{k}/k)$$

where $\overline{k}$ denotes an algebraic closure of k. Assume that X is equipped with a k point, denoted b and used as a base point; a k-variety will be said to be *pointed* if it is equipped with a k-point. The point b gives rise to an Abel-Jacobi map

$$\alpha : X \to \mathrm{Jac}\, X$$

from X to its Jacobian, sending b to the identity, and applying π_1 to $\alpha \otimes \overline{k}$ produces the abelianization of $\pi_1(X_{\overline{k}})$. For any pointed variety Z over k, there is a natural map

$$\kappa : Z(k) \to \mathrm{H}^1(G_k, \pi_1(Z_{\overline{k}}))$$

where $Z(k)$ denotes the k points of Z. In particular, we have the commutative diagram

$$\begin{array}{ccc} \mathrm{Jac}(X)(k) & \longrightarrow & \mathrm{H}^1(G_k, \pi_1(X_{\overline{k}})^{\mathrm{ab}}) \\ \uparrow & & \uparrow \\ X(k) & \longrightarrow & \mathrm{H}^1(G_k, \pi_1(X_{\overline{k}})) \end{array} \tag{12.1}$$

Any k point of $\mathrm{Jac}(X)$ which is in the image of the Abel-Jacobi map satisfies the condition that its associated element of $\mathrm{H}^1(G_k, \pi_1(X_{\overline{k}})^{\mathrm{ab}})$ lifts through the map

$$\mathrm{H}^1(G_k, \pi_1(X_{\overline{k}})) \to \mathrm{H}^1(G_k, \pi_1(X_{\overline{k}})^{\mathrm{ab}}). \tag{12.2}$$

Therefore showing that the associated element of $\mathrm{H}^1(G_k, \pi_1(X_{\overline{k}})^{\mathrm{ab}})$ does not admit such a lift obstructs this point of the Jacobian from lying on the curve. Ellenberg's obstructions are obstructions to lifting through the map (12.2). Since they obstruct a conjugacy class of sections of π_1 of $\mathrm{Jac}\, X \to \mathrm{Spec}\, k$ from being the image of a conjugacy class of sections of π_1 of $X \to \mathrm{Spec}\, k$, they are being called "obstructions to π_1 sections" in the title. They arise from the lower central series and are defined in 12.2.

More specifically, Ellenberg's obstruction δ_n is the $\mathrm{H}^1 \to \mathrm{H}^2$ boundary map in G_k cohomology for the extension

$$1 \to [\pi]_n/[\pi]_{n+1} \to \pi/[\pi]_{n+1} \to \pi/[\pi]_n \to 1 \tag{12.3}$$

where π is the étale fundamental group of $X_{\overline{k}}$, and

$$\pi = [\pi]_1 \supset [\pi]_2 \supset [\pi]_3 \supset \dots$$

denotes the lower central series of π. The obstruction δ_n is regarded as a multi-valued function on $\mathrm{H}^1(G_k,\pi^{\mathrm{ab}})$ via $\mathrm{H}^1(G_k,\pi/[\pi]_n)\to\mathrm{H}^1(G_k,\pi^{\mathrm{ab}})$ and also on $\mathrm{Jac}X(k)$ via κ.

Now assume that $X=\mathbb{P}^1_k-\{0,1,\infty\}$ and that k is a subfield of $\mathbb{C}$ or a completion of a number field. By replacing the Jacobian by the generalized Jacobian and enlarging $X(k)$ to include k rational tangential base points, we obtain a commutative diagram generalizing (12.1). The same obstructions to lifting through (12.2) define obstructions δ_n for X. As there is an isomorphism

$$\pi\cong\langle x,y\rangle^{\wedge}$$

between π and the profinite completion of the topological fundamental group of $\mathbb{P}^1_{\mathbb{C}}-\{0,1,\infty\}$, bases of

$$[\pi]_n/[\pi]_{n+1}\cong\hat{\mathbb{Z}}(n)^{N(n)}$$

can be specified by order n commutators of x and y, decomposing the obstructions δ_n into multi-valued, partially defined maps

$$\mathrm{H}^1(G_k,\hat{\mathbb{Z}}(1)\oplus\hat{\mathbb{Z}}(1))\dashrightarrow\mathrm{H}^2(G_k,\hat{\mathbb{Z}}(n)).$$

Section 12.3 expresses δ_2 and δ_3 in terms of cup products and Massey products. For a in k^*, let $\{a\}$ denote the image of a in $\mathrm{H}^1(G_k,\hat{\mathbb{Z}}(1))$ under the Kummer map. For (b,a) in $\mathrm{Jac}X(k)\cong(\mathbb{G}_m\times\mathbb{G}_m)(k)$, the obstruction δ_2 is given [Ell00] by $\delta_2(b,a)=\{b\}\cup\{a\}$. It is a charming observation of Jordan Ellenberg that this computation shows that the cup product factors through $\mathrm{K}_2(k)$ (Remark 28). The obstruction δ_3 is computed by Theorem 19

$$\delta_{3,[[x,y],x]}(b,a)=\langle\{-b\},\{b\},\{a\}\rangle$$

$$\delta_{3,[[x,y],y]}(b,a)=-\langle\{-a\},\{a\},\{b\}\rangle-f\cup\{a\},$$

where $f\in\mathrm{H}^1(G_k,\hat{\mathbb{Z}}(2))$ is associated to the monodromy between 0 and 1. The indeterminacy of the Massey product and the conditions required for its definition coincide with the multiple values assumed by δ_3 and the condition for its definition.

Section 12.4 contains computations of δ_2, and its mod 2 reduction. In particular, 12.4.4 provides points on which to evaluate δ_3, which can be phrased as the failure of a 2-nilpotent section conjecture for $\mathbb{P}^1_k-\{0,1,\infty\}$. Tate's computation of $\mathrm{K}_2(\mathbb{Q})$ gives a finite algorithm for determining whether or not $\delta_2(b,a)=0$ for $k=\mathbb{Q}$ described in 12.4.5.

The main results of this paper are in Section 12.5. The mod 2 reduction of δ_3 for a finite extension k_v of $\mathbb{Q}_p$ with p odd is computed:

Theorem 36 *Suppose that $\delta_2^{\mathrm{mod}\,2}(b,a)=0$. Then $\delta_3^{\mathrm{mod}\,2}(b,a)\neq 0$ if and only if one of the following holds:*

- $\{-b\}=0$ *and* $\{2\sqrt{-b}\}\cup\{a\}\neq 0$.
- $\{-a\}=0$ *and* $\{2\sqrt{-a}\}\cup\{b\}+\{2\}\cup\{a\}\neq 0$.
- $\{b\}=\{a\}$ *and* $\{2\sqrt{b}\sqrt{a}\}\cup\{a\}\neq 0$.

where equalities such as $\{-b\} = 0$ take place in $\mathrm{H}^1(G_{k_v}, \mathbb{Z}/2)$ and non-equalities such as $\{2\sqrt{-b}\} \cup a \neq 0$ take place in $\mathrm{H}^2(G_{k_v}, \mathbb{Z}/2)$. The cocycle

$$f : G_k \to [\pi]_2/([\pi]_3([\pi]_2)^2) \cong \mathbb{Z}/2$$

described above is known due to contributions of Anderson, Coleman, Deligne, Ihara, Kaneko, and Yukinari, and f's computation is inputed to Theorem 36. For points

$$(b,a) \in (\mathbb{Z} - \{0\}) \times (\mathbb{Z} - \{0\}) \subset \mathrm{Jac}\, X(\mathbb{Q}_p)$$

such that p divides ab exactly once, the vanishing of $\delta_3^{\mathrm{mod}\,2}$ for $\mathbb{Q}_p$ can be expressed in terms of the congruence conditions

- $\delta_2^{\mathrm{mod}\,2}(b,a) = 0 \iff a+b$ is a square mod p
- When $\delta_2^{\mathrm{mod}\,2}(b,a) = 0$, $\delta_3^{\mathrm{mod}\,2}(b,a) = 0 \iff a+b$ is a fourth power mod p

This is Corollary 38. As the image of X in its Jacobian consists of (b,a) such that $b+a=1$, and the image of the tangential points of X are (b,a) such that $b+a=0$, or $b=1$, or $a=1$, we see in Corollary 38 that $\delta_3^{\mathrm{mod}\,2}$ vanishes on the points and tangential points of X. Of course, $\delta_3^{\mathrm{mod}\,2}$ is constructed to satisfy this property, but here it is visible that $\delta_2^{\mathrm{mod}\,2}$ and $\delta_3^{\mathrm{mod}\,2}$ are increasingly accurate approximations to X inside its Jacobian.

The obstruction $\delta_3^{\mathrm{mod}\,2}$ for $k = \mathbb{R}$ is computed in 12.5.3. Consider $k = \mathbb{Q}$. Although an element of $\mathrm{H}^2(G_{\mathbb{Q}}, \mathbb{Z}/2)$ is 0 if and only if its restriction to all places, or all but one place, vanishes, the previous local calculations can only be combined to produce a global calculation when the Massey products are evaluated locally using compatible defining systems. This involves the local-global comparison map on Galois cohomology with coefficients in a 2-nilpotent group. See Remark 46. In 12.5.5, such lifts are arranged and the local calculations are used to show that

$$\delta_3^{\mathrm{mod}\,2}(-p^3, p) = 0$$

for $k = \mathbb{Q}$. Proposition 48 computes $\delta_3^{\mathrm{mod}\,2}$ on a specific lift of $(-p^3, p)$ for $k = \mathbb{Q}$, which is equivalent to the calculation of the $G_{\mathbb{Q}}$ Massey products with $\mathbb{Z}/2$ coefficients $\langle \{p^3\}, \{-p^3\}, \{p\} \rangle$ and $\langle \{-p\}, \{p\}, \{-p^3\} \rangle$ for any specified defining system.

Acknowledgments: I wish to thank Gunnar Carlsson, Jordan Ellenberg, and Mike Hopkins for many useful discussions. I thank the referee for correcting sign errors in Proposition 17 and 12.5.2. I also thank Jakob Stix for clarifying 12.4.4, shortening the proofs of Lemma 34, Propositions 32 and 45, and for extensive and thoughtful editing.

12.2 Ellenberg's obstructions to π_1 sections for $\mathbb{P}^1_k - \{0,1,\infty\}$

We work with fields k which are subfields of $\mathbb{C}$ or completions of a number field. In the latter case, fix an embedding of the number field into $\mathbb{C}$, as well as an algebraic closure $\overline{k}$ of k, and an embedding $\overline{\mathbb{Q}} \subset \overline{k}$, where $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. These specifications serve to choose maps between topological and étale fundamental groups, as in (12.11).

This section defines Ellenberg's obstructions. In 12.2.1, we recall Deligne's notion of a tangential point [Del89, §15] [Nak99], and define in (12.5) the map κ from k points and tangential points to $\mathrm{H}^1(G_k, \pi_1(X_{\overline{k}}))$. We then specialize to $X = \mathbb{P}^1_k - \{0,1,\infty\}$, give the computation of κ composed with

$$\mathrm{H}^1(G_k, \pi_1(X_{\overline{k}})) \to \mathrm{H}^1(G_k, \pi_1(X_{\overline{k}})^{\mathrm{ab}})$$

in (12.15) and Lemma 4, and define Ellenberg's obstructions in 12.2.3.

12.2.1 Tangential base points, path torsors, and the Galois action

Let X be a smooth, geometrically connected curve over k with smooth compactification $X \subseteq \overline{X}$ and $x \in \overline{X}(k)$, so in particular, x could be in $(\overline{X} - X)(k)$.

A local parameter z at x gives rise to an isomorphism $\widehat{\mathcal{O}}_{\overline{X},x} \xleftarrow{\cong} k[[z]]$, where $\widehat{\mathcal{O}}_{\overline{X},x}$ denotes the completion of the local ring of x.

Let $\overline{k}$ be a fixed algebraic closure of k. Since we assume that k has characteristic 0, the field of Puiseux series

$$\overline{k}((z^{\mathbb{Q}})) := \cup_{n \in \mathbb{Z}_{>0}} \overline{k}((z^{1/n}))$$

is algebraically closed. The composition

$$\operatorname{Spec} \overline{k}((z^{\mathbb{Q}})) \to \operatorname{Spec} k[[z]] \cong \operatorname{Spec} \widehat{\mathcal{O}}_{\overline{X},x} \to \overline{X}$$

factors through the generic point of $\overline{X}$ and thus defines a geometric point of X

$$b_z : \operatorname{Spec} \overline{k}((z^{\mathbb{Q}})) \to X$$

that will be called the *tangential base point* of X at x in the direction of z. The tangential base point b_z determines an embedding

$$k(X) \subset k((z)) \subset \overline{k}((z^{\mathbb{Q}})).$$

The coefficientwise action of $G_k = \mathrm{Gal}(\overline{k}/k)$ on $\cup_{n \in \mathbb{Z}_{>0}} \overline{k}((z^{1/n}))$ gives a splitting of $G_{k((z))} \to G_k$. Combined with the embedding $k(X) \subset k((z))$, this splitting gives a splitting of $G_{k(X)} \to G_k$ and therefore a splitting of

$$\pi_1^{et}(X, b_z) \to G_k,$$

see [SGAI, V Prop 8.2], and a G_k action on $\pi_1^{et}(X_{\overline{k}}, b_z)$.

A *geometric point associated to a k point or tangential point* will mean

$$x : \operatorname{Spec} \Omega_x \to X$$

where Ω_x is an algebraically closed extension of $\overline{k}$, such that either x arises as a tangential base point as described above or x has a k point as its image. Such a geometric point determines a canonical geometric point of $X_{\overline{k}}$, and the associated fiber functor has a canonical G_k action. A path between two such geometric points b and x is a natural transformation of the associated fiber functors, and the set of paths

$$\pi_1(X_{\overline{k}}; b, x)$$

from b to x form a trivial $\pi_1^{et}(X_{\overline{k}}, b)$ torsor whose G_k action determines an element

$$[\pi_1(X_{\overline{k}}; b, x)] \in \mathrm{H}^1(G_k, \pi_1^{et}(X_{\overline{k}}, b))$$

represented by the cocycle

$$g \mapsto \gamma^{-1} \circ g(\gamma) \tag{12.4}$$

where γ is any path from b to x. Composition of paths is written right to left so that $\gamma^{-1} \circ g(\gamma)$ is the path formed by first traversing $g(\gamma)$ and then γ^{-1}.

A local parameter z at a point x of $\overline{X}$ determines a tangent vector

$$\operatorname{Spec} k[[z]]/\langle z^2 \rangle \to \overline{X}.$$

For b or x a tangental base point, the associated element of $\mathrm{H}^1(G_k, \pi_1^{et}(X_{\overline{k}}, b))$ only depends on the choice of local parameter up to the associated tangent vector. Furthermore, if x is a k tangential point which comes from a tangent vector at a point p of X, then

$$[\pi_1(X_{\overline{k}}; b, x)] = [\pi_1(X_{\overline{k}}; b, p)].$$

This describes a map

$$\kappa = \kappa_{(X,b)} \; : \; X(k) \cup \bigcup_{x \in \overline{X} - X} (T_x \overline{X}(k) - \{0\}) \to \mathrm{H}^1(G_k, \pi_1(X_{\overline{k}}, b)). \tag{12.5}$$

Example 1. The boundary map for the Kummer sequence

$$1 \to \mathbb{Z}/n\mathbb{Z}(1) \to \mathbb{G}_{\mathrm{m}} \xrightarrow{n\cdot} \mathbb{G}_{\mathrm{m}} \to 1 \tag{12.6}$$

yields in the limit over all n the Kummer map

$$k^* \to \mathrm{H}^1(G_k, \hat{\mathbb{Z}}(1)) \tag{12.7}$$

which is represented on the level of cocycles by

$$\sigma \mapsto \{z\}(\sigma) = \left(\sigma(\sqrt[n]{z})/\sqrt[n]{z}\right)_n \tag{12.8}$$

for any compatible choice of n^{th} roots of $z \in \overline{k}^*$. This cocycle, or by abuse of notation also the class it represents, will also be denoted by z, or denoted by $\{z\}$ if there is possible confusion.

When $n = 2$, both choices of square root of z produce the same cocycle. Furthermore, canonically $\mu_2 = \mathbb{Z}/2\mathbb{Z}$ and thus we have a well-defined homomorphism

$$k^* \to C^1(G_k, \mathbb{Z}/2\mathbb{Z}),$$

with $C^1(G_k, \mathbb{Z}/2\mathbb{Z})$ the group of continuous 1-cocycles of G_k with values in $\mathbb{Z}/2\mathbb{Z}$.

For $(X,b) = (\mathbb{G}_m, 1)$, the map κ is the Kummer map: for

$$x \in \mathbb{G}_{\mathrm{m},k}(k) = k^*,$$

choose compatible n^{th} roots $\sqrt[n]{x}$ of x, and choose 1 as the n^{th} root of unity for each $n \in \mathbb{Z}_{>0}$. These choices determine a path γ from 1 to x as follows. On the degree n cover

$$p_n \ : \ \mathbb{G}_{\mathrm{m},\overline{k}} \to \mathbb{G}_{\mathrm{m},\overline{k}}$$

given by $t \mapsto t^n$, the path γ maps

$$\gamma \ : \ p_n^{-1}(1) \to p_n^{-1}(x)$$

by multiplication by $\sqrt[n]{x}$. For $g \in G_k$, the path $g\gamma$ is the path sending $g1$ to $g(\sqrt[n]{x})$, thus multiplies by $g(\sqrt[n]{x})$. We conclude

$$\kappa(x) = \gamma^{-1} \circ g(\gamma) = g(\sqrt[n]{x})/\sqrt[n]{x} = \{x\}(g).$$

Identifying the choice of path from 1 to x with the choice of compatible n^{th} roots of x, there is an equality of cocycles $\kappa(x) = \{x\}$.

Similarly, for $w \in T_0\mathbb{P}^1_k(k) - \{0\} = k^*$, a compatible choice of n^{th} roots $\sqrt[n]{w}$ of w determines a path γ from 1 to $\overrightarrow{0w}$, where $\overrightarrow{0w}$ is the k tangential point

$$\operatorname{Spec} \overline{k}((z^{\mathbb{Q}})) \to \operatorname{Spec} k[t, \frac{1}{t}] \tag{12.9}$$

given by $t \mapsto wz$, by defining γ to map $\zeta \in \mu_n(\overline{k}) = p_n^{-1}(1)$ to the point of $p_n^{-1}(\overrightarrow{0w})$ given by (12.9) and $t \mapsto \sqrt[n]{w}\zeta z^{1/n}$. For any $g \in G_k$, we have $g(\gamma)(\zeta) = g(\gamma(g^{-1}\zeta))$ is the path given by (12.9) and $t \mapsto (g\sqrt[n]{w})\zeta z^{1/n}$, whence $\gamma((g\sqrt[n]{w})\zeta/\sqrt[n]{w}) = g(\gamma)(\zeta)$. We conclude

$$\kappa(\overrightarrow{0w}) = \gamma^{-1} \circ g(\gamma) = g(\sqrt[n]{w})/\sqrt[n]{w} = \{w\}(g) = \kappa(w).$$

Example 2. The map $\kappa_{(X,b)}$ depends on the choice of base point, even when $\pi_1(X_{\overline{k}}, b)$ is abelian and is therefore independent of b. In this case, if b_1 and b_2 are two geometric points associated to a k point or tangential point of X, a straightforward

cocycle manipulation shows that

$$\kappa_{(X,b_2)}(x) = \kappa_{(X,b_1)}(x) - \kappa_{(X,b_1)}(b_2)$$

for any k point or tangential point x. In particular, Example 1 implies that

$$\kappa_{(\mathbb{G}_m,\overrightarrow{01})} = \kappa_{(\mathbb{G}_m,1)}.$$

κ is often called a non-abelian Kummer map.

For higher dimensional geometrically connected varieties Z over k, we will not need the notion of a tangential base point, but we will use the map

$$\kappa = \kappa_{(Z,b)} \,:\, Z(k) \to \mathrm{H}^1(G_k, \pi_1(Z_{\overline{k}}, b)) \tag{12.10}$$

defined precisely as in the case of curves above.

Let $X = \mathbb{P}^1_k - \{0,1,\infty\} = \operatorname{Spec} k[t, \frac{1}{t}, \frac{1}{1-t}]$, and base X at $\overrightarrow{01}$ as in Example 1 (12.9). We fix an isomorphism

$$\pi = \pi_1^{et}(\mathbb{P}^1_{\overline{k}} - \{0,1,\infty\}, \overrightarrow{01}) \cong \langle x, y\rangle^\wedge \tag{12.11}$$

between π and the profinite completion of the free group on two generators as follows: recall that we assume that k is a subfield of $\mathbb{C}$ or the completion of a number field at a place, and we have fixed $\mathbb{C} \supset \overline{\mathbb{Q}} \subseteq \overline{k}$, see 12.2. The morphisms $\mathbb{C} \supset \overline{\mathbb{Q}} \subseteq \overline{k}$ and the Riemann existence theorem give an isomorphism $\pi \cong \pi_1^{top}(\mathbb{P}^1_{\mathbb{C}} - \{0,1,\infty\}, \overrightarrow{01})^\wedge$, where the base point for the topological fundamental group, also denoted $\overrightarrow{01}$, is the tangent vector at 0 pointing towards 1. Let x be a small counterclockwise loop around 0 based at $\overrightarrow{01}$. Let y' be the pushforward of x by automorphism of $\mathbb{P}^1_{\mathbb{C}} - \{0,1,\infty\}$ given $1 \mapsto 1-t$, so in particular, y' is a small loop around 1 based at $\overrightarrow{10}$, where $\overrightarrow{10}$ is the tangent vector at 1 pointing towards 0. Conjugating y' by the direct path along the real axis between $\overrightarrow{10}$ and $\overrightarrow{01}$ produces a loop y, and an isomorphism $\pi_1^{top}(\mathbb{P}^1_{\mathbb{C}} - \{0,1,\infty\}, \overrightarrow{01}) = \langle x, y\rangle$, giving (12.11).

An element $\sigma \in G_k$ acts on π by

$$\begin{aligned} \sigma(x) &= x^{\chi(\sigma)} \\ \sigma(y) &= \mathfrak{f}(\sigma)^{-1} y^{\chi(\sigma)} \mathfrak{f}(\sigma) = [\mathfrak{f}(\sigma)^{-1}, y^{\chi(\sigma)}] y^{\chi(\sigma)}, \end{aligned} \tag{12.12}$$

where $\mathfrak{f} : G_k \to [\pi]_2$ is a cocycle with values in the commutator subgroup $[\pi]_2$ of π (coming from the monodromy of the above path from $\overrightarrow{01}$ to $\overrightarrow{10}$), and $\chi : G_k \to \hat{\mathbb{Z}}^*$ denotes the cyclotomic character, see [Iha94].

12.2.2 The Abel-Jacobi map for $\mathbb{P}^1_k - \{0,1,\infty\}$

Let $X \subseteq \overline{X}$ denote a smooth curve over k inside its smooth compactification. The generalized Jacobian $\mathrm{Jac}X$ of X, is the algebraic group of equivalence classes of degree 0 divisors of X, where two divisors are considered equivalent if they differ by $\mathrm{Div}(\phi)$ for a rational function ϕ such that $\phi(p) = 1$ for all p in $\overline{X} - X$. It follows that $\mathrm{Jac}(X)$ is an extension of $\mathrm{Jac}(\overline{X})$ by the torus

$$\mathbb{T} = \Big(\prod_{p \in \overline{X} - X} \mathrm{Res}_{k(p)/k} \mathbb{G}_{\mathrm{m},k(p)} \Big) / \mathbb{G}_{\mathrm{m},k}$$

where p ranges over the closed points of $\overline{X} - X$ with residue field $k(p)$, the torus $\mathrm{Res}_{k(p)/k} G_{m,k(p)}$ denotes the restriction of scalars of $\mathbb{G}_{\mathrm{m},k(p)}$ to k, and where $\mathbb{G}_{\mathrm{m},k}$ acts diagonally. For more information on generalized Jacobians see [Ser88].

For $X = \mathbb{P}^1_k - \{0,1,\infty\}$, the Jacobian of $\overline{X} = \mathbb{P}^1_k$ s trivial. The complement of X in $\overline{X}$ consists of three rational points and

$$\mathrm{Jac}(\mathbb{P}^1_k - \{0,1,\infty\}) \cong \mathbb{G}_{\mathrm{m},k} \times \mathbb{G}_{\mathrm{m},k}. \tag{12.13}$$

Since the fundamental group of a connected group is abelian, the fundamental group does not depend on base points. We find

$$\pi_1(\mathrm{Jac}(\mathbb{P}^1_{\bar{k}} - \{0,1,\infty\})) = \pi_1(\mathbb{G}_{\mathrm{m},\bar{k}}, 1) \times \pi_1(\mathbb{G}_{\mathrm{m},\bar{k}}, 1) = \hat{\mathbb{Z}}(1) \oplus \hat{\mathbb{Z}}(1).$$

We choose an isomorphism (12.13) by sending $\mathrm{Div}(f)$ for a rational function f on $\mathbb{P}^1$ to $f(0)/f(\infty) \times f(1)/f(\infty)$ in $\mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}}$.

The Abel-Jacobi map based at $\overrightarrow{01}$

$$\alpha \ : \ \mathbb{P}^1_k - \{0,1,\infty\} \to \mathrm{Jac}(\mathbb{P}^1_k - \{0,1,\infty\}) = \mathbb{G}_{\mathrm{m},k} \times \mathbb{G}_{\mathrm{m},k}$$

$$t \mapsto (t, 1-t)$$

induces the abelianization

$$\pi = \pi_1(\mathbb{P}^1_{\bar{k}} - \{0,1,\infty\}, \overrightarrow{01}) \twoheadrightarrow \pi^{\mathrm{ab}} = \pi_1(\mathrm{Jac}(\mathbb{P}^1_{\bar{k}} - \{0,1,\infty\})) = \hat{\mathbb{Z}}(1) \oplus \hat{\mathbb{Z}}(1). \tag{12.14}$$

Remark 3. From (12.11) and (12.12), we have fixed an isomorphism

$$\pi^{ab} \cong \hat{\mathbb{Z}}(\chi)x \oplus \hat{\mathbb{Z}}(\chi)y.$$

The isomorphism (12.14) above $\pi^{ab} \cong \hat{\mathbb{Z}}(1) \oplus \hat{\mathbb{Z}}(1)$ is the composition of the former with the isomorphism

$$\hat{\mathbb{Z}}(\chi) \cong \hat{\mathbb{Z}}(1) := \varprojlim_n \mu_{n,\bar{k}}$$

corresponding to the compatible choice of roots of unity given by the action of the loop x on the fiber over $\overrightarrow{01}$ on the finite étale covers of $\mathbb{G}_{m,\bar{k}}$, i.e. to the choice

$(\zeta_n)_{n\in\mathbb{Z}_{>0}}$, $\zeta_n = e^{2\pi i/n}$ of compatible primitive n^{th} roots of unity. We will hereafter identify

$$\hat{\mathbb{Z}}(1) = \hat{\mathbb{Z}}(\chi)$$

by this isomorphism, and for typographical reasons, we will use the notation $\hat{\mathbb{Z}}(n)$ for $\hat{\mathbb{Z}}(\chi^n)$, although the group law will be written additively.

By Example 1, the map κ for the k scheme $\mathbb{G}_\mathrm{m}\times\mathbb{G}_\mathrm{m}$ pointed by $(1,1)$ is two copies of the Kummer map:

$$k^*\times k^* \to \mathrm{H}^1(G_k,\hat{\mathbb{Z}}(1))\times \mathrm{H}^1(G_k,\hat{\mathbb{Z}}(1))$$

$$b\times a \mapsto \{b\}\times\{a\}.$$

By functoriality of κ and Example 2, the following diagram is commutative:

$$\begin{array}{ccc} H^1(G_k,\pi) & \longrightarrow & H^1(G_k,\pi^{ab}) \\ {\scriptstyle \kappa_{\overrightarrow{01}}}\uparrow & & \uparrow{\scriptstyle \kappa_{(1,1)}} \\ (\mathbb{P}^1_k-\{0,1,\infty\})(k) & \xrightarrow{t\mapsto(t,1-t)} & (\mathbb{G}_m\times\mathbb{G}_m)(k) \end{array} \tag{12.15}$$

We can similarly compute the image of the k tangential points of $\mathbb{P}^1_k-\{0,1,\infty\}$ in $\mathrm{H}^1(G_k,\pi^{ab})$, which is what we now do (also see [Ell00]). We define a map

$$\alpha \,:\, \cup_{t=0,1,\infty}(T_t\mathbb{P}^1-\{0\})(k)\to(\mathbb{G}_m\times\mathbb{G}_m)(k)$$

by, for $w\in k^*$,

$$\alpha(\overrightarrow{0w}) = (w,1),\quad \alpha(\overrightarrow{1w}) = (1,-w),\quad \alpha(\overrightarrow{\infty w}) = (w^{-1},-w^{-1})$$

where $\overrightarrow{1w}$ is the pushforward of $\overrightarrow{0w}$ under $t\mapsto t+1$, and $\overrightarrow{\infty w}$ is the pushforward of $\overrightarrow{0w}$ under $t\mapsto 1/t$.

Lemma 4. *The following diagram commutes:*

$$\begin{array}{ccc} \mathrm{H}^1(G_k,\pi) & \longrightarrow & \mathrm{H}^1(G_k,\pi^{\mathrm{ab}}) \\ \uparrow & & \uparrow \\ \cup_{t=0,1,\infty}(T_t\mathbb{P}^1-\{0\})(k) & \xrightarrow{\alpha} & (\mathbb{G}_m\times\mathbb{G}_m)(k) \end{array}$$

Proof. The commutativity of the two diagrams

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & \mathrm{Jac}\,X \\ \downarrow{\scriptstyle t\mapsto 1-t} & & \downarrow{\scriptstyle (b,a)\mapsto(a,b)} \\ X & \xrightarrow{\alpha} & \mathrm{Jac}\,X \end{array} \qquad \begin{array}{ccc} X & \xrightarrow{\alpha} & \mathrm{Jac}\,X \\ \downarrow{\scriptstyle t\mapsto 1/t} & & \downarrow{\scriptstyle (b,a)\mapsto(\frac{1}{b},\frac{-a}{b})} \\ X & \xrightarrow{\alpha} & \mathrm{Jac}\,X \end{array}$$

reduces the lemma for $t = 1$ or ∞ (respectively) to the case $t = 0$.

By functoriality of κ applied to the Abel-Jacobi map $t \mapsto (t, 1-t)$, we have that the image of $\kappa_{(\mathbb{P}^1_k - \{0,1,\infty\}, \overrightarrow{01})}(\overrightarrow{0w})$ in $\mathrm{H}^1(G_k, \pi^{\mathrm{ab}})$ is

$$\kappa_{(\mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}}, \overrightarrow{01} \times 1)}(\overrightarrow{0w}, \overrightarrow{1(-w)}) = \kappa_{(\mathbb{G}_{\mathrm{m}}, \overrightarrow{01})}(\overrightarrow{0w}) \times \kappa_{(\mathbb{G}_{\mathrm{m}}, 1)}(\overrightarrow{1(-w)}).$$

The geometric point $\overrightarrow{1(-w)}$ factors through $1 - w\frac{\partial}{\partial t} : \operatorname{Spec} \bar{k}[[z]] \to \mathbb{G}_{\mathrm{m},\bar{k}}$

$$t \mapsto 1 - wz.$$

The quotient map $\operatorname{Spec} \bar{k} \to \operatorname{Spec} \bar{k}[[z]]$ given by $z \mapsto 0$ gives a bijection between the fiber over $1 - w\frac{\partial}{\partial t}$ and the fiber over 1 of the multiplication by n cover

$$p_n : \mathbb{G}_{\mathrm{m},\bar{k}} \to \mathbb{G}_{\mathrm{m},\bar{k}}.$$

These bijections determine a Galois equivariant path between 1 and $\overrightarrow{1(-w)}$ showing that

$$\kappa_{(\mathbb{G}_{\mathrm{m}}, 1)}(\overrightarrow{1(-w)}) = \kappa_{(\mathbb{G}_{\mathrm{m}}, 1)}(1).$$

The lemma now follows from Examples 1 and 2. □

12.2.3 Ellenberg's obstructions

Let π be $\pi_1(\mathbb{P}^1_{\bar{k}} - \{0,1,\infty\}, \overrightarrow{01})$ or more generally π can be any profinite group with a continuous G_k action, e.g. the étale fundamental group of a k-variety after base change to $\bar{k}$.

The lower central series of π is the filtration of closed characteristic subgroups

$$\pi = [\pi]_1 \supset [\pi]_2 \supset \ldots \supset [\pi]_n \supset \ldots$$

where the commutator is defined $[x,y] = xyx^{-1}y^{-1}$, and $[\pi]_{n+1} = \overline{[\pi, [\pi]_n]}$ is the closure of the subgroup generated by commutators of elements of $[\pi]_n$ with elements of π.

The central extension

$$1 \to [\pi]_n/[\pi]_{n+1} \to \pi/[\pi]_{n+1} \to \pi/[\pi]_n \to 1$$

gives rise to a boundary map in continuous group cohomology

$$\delta_n : \mathrm{H}^1(G_k, \pi/[\pi]_n) \to \mathrm{H}^2(G_k, [\pi]_n/[\pi]_{n+1})$$

that is part of an exact sequence of pointed sets (see for instance [Ser02, I 5.7]),

$$\begin{aligned}1 \to &([\pi]_n/[\pi]_{n+1})^{G_k} \to (\pi/[\pi]_{n+1})^{G_k} \to (\pi/[\pi]_n)^{G_k}\\ &\to \mathrm{H}^1(G_k,[\pi]_n/[\pi]_{n+1}) \to \mathrm{H}^1(G_k,\pi/[\pi]_{n+1}) \to \mathrm{H}^1(G_k,\pi/[\pi]_n)\\ &\to \mathrm{H}^2(G_k,[\pi]_n/[\pi]_{n+1}).\end{aligned}$$

The δ_n give a series of obstructions to an element of $\mathrm{H}^1(G_k,\pi/[\pi]_2)$ being the image of an element of $\mathrm{H}^1(G_k,\pi)$, thereby also providing a series of obstructions to a rational point of the Jacobian coming from a rational point of the curve: to a given element x of $\mathrm{H}^1(G_k,\pi/[\pi]_2)$, if $\delta_2(x)\neq 0$, then x is not the image of an element of $\mathrm{H}^1(G_k,\pi)$. Otherwise, x lifts to $\mathrm{H}^1(G_K,\pi/[\pi]_3)$. Apply δ_3 to all the lifts of x. If δ_3 is never 0, then x is not the image of an element of $\mathrm{H}^1(G_k,\pi)$. Otherwise, x lifts to $\mathrm{H}^1(G_k,\pi/[\pi]_4)$, and so on.

Definition 5. For x in $\mathrm{H}^1(G_k,\pi/[\pi]_2)$, say that $\delta_n x=0$ if x is in the image of

$$\mathrm{H}^1(G_k,\pi/[\pi]_{n+1}) \to \mathrm{H}^1(G_k,\pi/[\pi]_2). \tag{12.16}$$

Otherwise, say $\delta_n x\neq 0$.

Let $X=\mathbb{P}^1_k-\{0,1,\infty\}$, or more generally X could be a smooth, geometrically connected, pointed curve over k, with an Abel-Jacobi map $X\to \mathrm{Jac}X$. As we are interested in obstructing points of the Jacobian from lying on X, it is convenient to identify a rational point of $\mathrm{Jac}X$ with its image under κ cf. (12.5).

Definition 6. For a k-point x of $\mathrm{Jac}X$, say that $\delta_n x=0$ if $\kappa_{(\mathrm{Jac},0)}x$ is in the image of (12.16), where 0 denotes the identity of $\mathrm{Jac}X$. Otherwise, say $\delta_n x\neq 0$.

For k a number field, and K the completion of k at a place v, the obstruction δ_n for K will sometimes be denoted δ_n^v, and applied to elements of $\mathrm{H}^1(G_k,\pi/[\pi]_n)$; it is to be understood that one first restricts to $\mathrm{H}^1(G_K,\pi/[\pi]_n)$. In other words, given x in $\mathrm{H}^1(G_k,\pi/[\pi]_2)$, the meaning of $\delta_n^v x=0$ is that there exists x_{n+1} in $\mathrm{H}^1(G_K,\pi/[\pi]_{n+1})$ lifting the restriction of x to $H^1(G_K,\pi/[\pi]_2)$. For x a point of $\mathrm{Jac}X(k)$, the meaning of $\delta_n^v x=0$ is that $\delta_n^v\kappa_{(\mathrm{Jac}X,0)}x=0$. This is equivalent to taking the image of x under $\mathrm{Jac}X(k)\to \mathrm{Jac}X_K(K)$ and applying Definition 6 with K as the base field.

Any filtration of π by characteristic subgroups such that successive quotients give rise to central extensions produces an analogous sequence of obstructions. For instance, consider the lower exponent 2 central series

$$\pi=[\pi]_1^2\supset[\pi]_2^2\supset\ldots\supset[\pi]_n^2\supset\ldots,$$

defined inductively by

$$[\pi]_{n+1}^2=\overline{[\pi,[\pi]_n^2]\cdot([\pi]_n^2)^2}$$

where $[\pi,[\pi]_n^2]\cdot([\pi]_n^2)^2$ denotes the subgroup generated by the indicated commutators and the squares of elements of $[\pi]_n^2$. The resulting obstructions are denoted δ_n^2, and will also be evaluated on $\mathrm{Jac}X(k)$ in the following manner: π^{ab} maps to $(\pi/[\pi]_{n+1}^2)^{\mathrm{ab}}$, giving a map

$$\mathrm{H}^1(G_K,\pi^{\mathrm{ab}}) \to \mathrm{H}^1(G_K,(\pi/[\pi]^2_{n+1})^{\mathrm{ab}}),$$

where either $K=k$ or K is the completion of a number field $k\subset\mathbb{C}$ at a place v as above. Precomposing with κ for the Jacobian (12.5) gives a map

$$\mathrm{Jac}(X)(k) \to H^1(G_K,(\pi/[\pi]^2_{n+1})^{\mathrm{ab}}).$$

For x in $\mathrm{Jac}(X)(k)$, say $\delta^2_n x=0$ (respectively $\delta^{(2,v)}_n x=0$) if there exists x_{n+1} in $\mathrm{H}^1(G_K,\pi/[\pi]^2_{n+1})$ such that x and x_{n+1} have equal image in $\mathrm{H}^1(G_K,(\pi/[\pi]^2_{n+1})^{ab})$. Otherwise, say $\delta^2_n x\neq 0$ (respectively $\delta^{(2,v)}_n x\neq 0$). The obstruction δ^v_n for v the place 2 will not be considered, so the notation δ^2_n will not be ambiguous. Obstructions δ^m_n corresponding to the lower exponent m central series,

$$[\pi]^m_{n+1}=\overline{[\pi,[\pi]^m_n]\cdot([\pi]^m_n)^m}$$

are defined similarly.

As one final note of caution, $\mathrm{H}^1(G_K,\pi/[\pi]_n)$ is in general only a pointed set. Furthermore, even for $n=2$, the map δ_2 is not a homomorphism, see Proposition 7.

12.3 The obstructions δ_2 and δ_3 as cohomology operations

We express δ_2 and δ_3 for $\mathbb{P}^1_k-\{0,1,\infty\}$ in terms of cohomology operations, where k is a subfield of $\mathbb{C}$ or the completion of a number field at a place; in the latter case, fix an embedding of the number field into $\mathbb{C}$ and an embedding $\overline{\mathbb{Q}}\subset\bar{k}$, giving the isomorphism $\pi=\pi_1^{et}(\mathbb{P}^1_{\bar{k}}-\{0,1,\infty\},\overrightarrow{01})\cong\langle x,y\rangle^\wedge$ of (12.11). We will use the following notation:

For elements x and y of a group, let $[x,y]=xyx^{-1}y^{-1}$ denote their commutator. For a profinite group G and a profinite abelian group A with a continuous action of G, let $(C^*(G,A),D)$ be the complex of inhomogeneous cochains of G with coefficients in A as in [NSW08, I.2 p. 14]. For $c\in C^p(G,A)$ and $d\in C^q(G,A')$, where A' is a profinite abelian group with a continuous action of G, let $c\cup d$ denote the cup product $c\cup d\in C^{p+q}(G,A\otimes A')$

$$(c\cup d)(g_1,\ldots,g_{p+q})=c(g_1,\ldots,g_p)\otimes g_1\cdots g_p d(g_{p+1},\ldots,g_{p+q}),$$

which induces a well defined map on cohomology, and gives $C^*(G,A)$ the structure of a differential graded algebra, for A a commutative ring, via $A\otimes A\to A$. For a profinite group Q, no longer assumed to be abelian, the continuous 1-cocycles

$$Z^1(G_k,Q)=\{s:G_k\to Q | s \text{ is continuous, } s(gh)=s(g)gs(h)\}$$

of G_k with values in Q form a subset of the set of continuous inhomogeneous cochains

$$C^1(G_k,Q)=\{s:G_k\to Q | s \text{ is continuous}\}.$$

See [Ser02, I §5] for instance. For $s \in C^1(G_k, Q)$, let $Ds : G_k \times G_k \to Q$ denote the function $Ds(g,h) = s(g)gs(h)s(gh)^{-1}$.

12.3.1 The obstruction δ_2 as a cup product

For any based curve X over k with fundamental group of $X_{\overline{k}}$ denoted π_1, [Zar74, Thm p 242] or [Ell00, Prop. 1]) show that

$$\delta_2(p+q) - \delta_2(p) - \delta_2(q) = [-,-]_* p \cup q,$$

where $[-,-]_*$ is the map on H^2 induced by the commutator

$$[-,-] : \pi_1^{ab} \otimes \pi_1^{ab} \to [\pi_1]_2/[\pi_1]_3$$

defined

$$[\overline{\gamma}, \overline{\ell}] \mapsto \gamma\ell\gamma^{-1}\ell^{-1},$$

where $\overline{\gamma} \in \pi_1^{ab}$ is the image of $\gamma \in \pi_1/[\pi_1]_3$ and similarly for ℓ. It follows that δ_2 is the sum of a cup product term and a linear term, after inverting 2. For $X = \mathbb{P}^1_k - \{0,1,\infty\}$ based at $\overrightarrow{01}$, the linear term vanishes and we can avoid inverting 2 by slightly changing what is meant by the cup-product term. This was shown by Ellenberg, who gave a complete calculation of δ_2 in this case [Ell00, p. 11]. Here is an alternative calculation of this δ_2, showing the same result: let $\pi = \pi_1^{et}(\mathbb{P}^1_{\overline{k}} - \{0,1,\infty\}, \overrightarrow{01}) \cong \langle x,y \rangle^\wedge$. Identify $\pi/[\pi]_2$ with $\hat{\mathbb{Z}}(1) \oplus \hat{\mathbb{Z}}(1)$ using the basis $\{x,y\}$, and identify $[\pi]_2/[\pi]_3$ with $\hat{\mathbb{Z}}(2)$ using the basis $\{[x,y]\}$, so δ_2 is identified with a map

$$H^1(G_k, \hat{\mathbb{Z}}(1) \oplus \hat{\mathbb{Z}}(1)) \to H^2(G_k, \hat{\mathbb{Z}}(2)).$$

Proposition 7. *Let $p(g) = y^{a(g)}x^{b(g)}$ be a 1-cocycle of G_k with values in $\pi/[\pi]_2$, so*

$$b, a : G_k \to \hat{\mathbb{Z}}(1)$$

are the cocycles produced by the isomorphism $\pi/[\pi]_2 \cong \hat{\mathbb{Z}}(1)x \oplus \hat{\mathbb{Z}}(1)y$. Then

$$\delta_2 p = b \cup a.$$

Proof. Sending $y^a x^b \in \pi/[\pi]_2$ to $y^a x^b \in \pi/[\pi]_3$ determines a set-theoretic section s of the quotient map $\pi/[\pi]_3 \to \pi/[\pi]_2$. Then $\delta_2(p)$ is represented by the cocycle

$$(g,h) \mapsto \delta_2(p)(g,h) = s(p(g))gs(p(h))s(p(gh))^{-1}$$

Using (12.12) and since $\mathfrak{f}(g) \in [\pi]_2$ is mapped to a central element in $\pi/[\pi]_3$ we find

$$\delta_2(p)(g,h) = \left(y^{a(g)}x^{b(g)}\right)\left(\left(\mathfrak{f}(g)^{-1}y^{\chi(g)}\mathfrak{f}(g)\right)^{a(h)}x^{\chi(g)b(h)}\right)\left(y^{a(gh)}x^{b(gh)}\right)^{-1}$$

$$= \left(y^{a(g)}x^{b(g)}\right)\left(y^{\chi(g)a(h)}x^{\chi(g)b(h)}\right)\left(x^{-b(g)-\chi(g)b(h)}y^{-a(g)-\chi(g)a(h)}\right)$$

$$= y^{a(g)}[x^{b(g)}, y^{\chi(g)a(h)}]y^{-a(g)} = [x^{b(g)}, y^{\chi(g)a(h)}] = [x,y]^{b(g)\cdot\chi(g)a(h)} = [x,y]^{(b\cup a)(g,h)}$$

giving the desired result. □

Proposition 7 characterizes the lifts to $\mathrm{H}^1(G_k, \pi/[\pi]_3)$ of an element of

$$\mathrm{H}^1(G_k, \pi^{ab}) \cong \mathrm{H}^1(G_k, \hat{\mathbb{Z}}(1)) \oplus \mathrm{H}^1(G_k, \hat{\mathbb{Z}}(1)) :$$

let $b, a : G_k \to \hat{\mathbb{Z}}(1)$ be cochains. For any $c \in C^1(G_k, \hat{\mathbb{Z}}(2))$, define

$$(b,a)_c : G_k \to \pi/[\pi]_3 \quad \text{by} \quad (b,a)_c(g) = y^{a(g)}x^{b(g)}[x,y]^{c(g)} \tag{12.17}$$

Corollary 8. *Let $p(g) = y^{a(g)}x^{b(g)}$ be a 1-cocycle of G_k with values in $\pi/[\pi]_2$. The lifts of p to a cocycle in $C^1(G_k, \pi/[\pi]_3)$ are in bijection with the set of cochains $c \in C^1(G_k, \hat{\mathbb{Z}}(2))$ such that*

$$Dc = -b \cup a$$

by

$$c \leftrightarrow (b,a)_c$$

Proof. $D((b,a)_c) = \delta_2(p) + Dc$, where $D((b,a)_c)$ is as above (cf. 12.3), and $\delta_2(p)$ denotes its cocycle representative given in the proof of Proposition 7. □

12.3.2 The obstruction δ_3 as a Massey product

Note that $\chi(g) - 1$ is divisible by 2 in $\hat{\mathbb{Z}}$ for any $g \in G_k$, where χ denotes the cyclotomic character, allowing us to define

$$\frac{\chi - 1}{2} : G_k \to \hat{\mathbb{Z}}(\chi) \quad \text{by} \quad g \mapsto \frac{\chi(g) - 1}{2} \in \hat{\mathbb{Z}}(\chi).$$

For any compatible system of primitive n^{th} roots of unity in $\hat{\mathbb{Z}}(1)$ giving an identification $\hat{\mathbb{Z}}(1) = \hat{\mathbb{Z}}(\chi)$, and in particular for (ζ_n) determined by Remark 3, we have

$$\{-1\} = \frac{\chi - 1}{2} \tag{12.18}$$

in $H^1(G_k, \hat{\mathbb{Z}}(1))$, where $\{-1\}$ denotes the image of -1 under the Kummer map. The equality (12.18) holds as an equality of cocycles in $C^1(G_k, \hat{\mathbb{Z}}(1))$ when $\{-1\}$ is considered as the cocycle $G_k \to \hat{\mathbb{Z}}(1)$ given by choosing as the n^{th} root of -1, the chosen primitive $(2n)^{th}$ root of unity; this is shown by the calculation

$$\{-1\}(g) = \left(g(\zeta_{2n})/\zeta_{2n}\right)_n = \left(\zeta_{2n}^{\chi(g)-1}\right)_n = \left(\zeta_n^{\frac{\chi(g)-1}{2}}\right)_n,$$

where for an element $a \in \hat{\mathbb{Z}}(1)$, the reduction of a in $\mathbb{Z}/n(1)$ is denoted $(a)_n$.

Definition 9. Profinite binomial coefficients are the maps $\binom{}{m}:\hat{\mathbb{Z}}\to\hat{\mathbb{Z}}$ for $m\geq 0$ defined for $a\in\hat{\mathbb{Z}}$ with $a\equiv a_n \mod n$ by

$$\binom{a}{m}\equiv a_{m!n}(a_{m!n}-1)(a_{m!n}-2)\dots(a_{m!n}-m+1)/m! \mod n$$

for every $n\in\mathbb{N}$.

Example 10. For a cocycle $b\in C^1(G_k,\hat{\mathbb{Z}}(\chi))$, let $\binom{b}{2}$ in $C^1(G_k,\hat{\mathbb{Z}}(\chi^2))$ denote the cochain given by

$$g\mapsto\binom{b(g)}{2}.$$

We have

$$D\binom{b}{2}=-(b+\frac{\chi-1}{2})\cup b,$$

as shown the the computation:

$$D\binom{b}{2}(g,h)=\binom{b(g)}{2}+\chi(g)^2\binom{b(h)}{2}-\binom{b(gh)}{2}=$$

$$\frac{b(g)(b(g)-1)}{2}+\frac{\chi(g)^2b(h)(b(h)-1)}{2}-\frac{(b(g)+\chi(g)b(h))(b(g)+\chi(g)b(h)-1)}{2}$$

$$=-b(g)\chi(g)b(h)-\frac{\chi(g)^2b(h)-\chi(g)b(h)}{2}$$

$$=-(b\cup b)(g,h)-(\frac{\chi-1}{2}\cup b)(g,h).$$

Example 11. Let b be an element of k^* with compatibly chosen n^{th} roots $\sqrt[n]{b}$ in $\bar{k}$, giving a cocycle $b:G_k\to\hat{\mathbb{Z}}(1)$ via the Kummer map. Identify $\hat{\mathbb{Z}}(1)=\hat{\mathbb{Z}}(\chi)$ with $(\zeta_n)_{n\in\mathbb{Z}_{>0}}$ from Remark 3. When restricted to an element of $C^1(G_{k(\sqrt{b})},\mathbb{Z}/2)$,

$$\binom{b}{2}=\{\sqrt{b}\}\quad\in C^1(G_{k(\sqrt{b})},\mathbb{Z}/2),$$

where $\{\sqrt{b}\}$ denotes the image of $\sqrt{b}$ under the Kummer map, which is independent of the choice of $\sqrt{\sqrt{b}}$. To see this, note that $\big(\{b\}(g)\big)_4=2\big(\{\sqrt{b}\}(g)\big)_4$ is even, whence $\big(\{b\}(g)-1\big)_2=1$, and the value of $\frac{1}{2}(\big(\{b\}(g)\big)_4)$ in $\mathbb{Z}/2$ is $\big(\{\sqrt{b}\}(g)\big)_2$. Here, as above, the reduction mod n of an element $a\in\hat{\mathbb{Z}}$ is denoted $(a)_n$.

Remark 12. Note that $\binom{b}{2}$ is a cochain taking values $\hat{\mathbb{Z}}(\chi^2)$, but Example 11 identifies its image in $C^1(G_{k(\sqrt{b})},\mathbb{Z}/2)$ with a cocycle taking values in $\mathbb{Z}/2(1)$. Furthermore, the cohomology class of the image of $\binom{b}{2}$ in $\mathrm{H}^1(G_{k(\sqrt{b})},\mathbb{Z}/2)$ depends on the choice of $\sqrt{b}$ used to define $b:G_k\to\hat{\mathbb{Z}}(1)$. Nevertheless, $\binom{b}{2}$ appears in the expressions for δ_3 which will be given in Proposition 17; it is involved in expressions

which make the choice of $\sqrt[n]{b}$ irrelevant cf. Remark 37. In writing down elements of π in terms of x and y, we have identified $\hat{\mathbb{Z}}(1)$ and $\hat{\mathbb{Z}}(\chi)$ because monodromy around x distinguishes a compatible system of roots of unity.

Identify $\hat{\mathbb{Z}}(1)$ and $\hat{\mathbb{Z}}(\chi)$ using (ζ_n) as in Remark 3. In particular, we can apply profinite binomial coefficients to elements of $\hat{\mathbb{Z}}(1)$ or any $\hat{\mathbb{Z}}(n)$.

We define a 1-cocycle $f(\sigma) \in C^1(G_k, \hat{\mathbb{Z}}(2))$ by

$$\mathfrak{f}(\sigma) = [x,y]^{f(\sigma)} \mod [\pi]_3 \tag{12.19}$$

where $\mathfrak{f}(\sigma)$ is the 1-cocycle from (12.12) that describes the Galois action on π.

The basis $\{[[x,y],x],[[x,y],y]\}$ for $[\pi]_3/[\pi]_4$ as a $\hat{\mathbb{Z}}$ module decomposes δ_3 into two obstructions

$$\delta_{3,[[x,y],x]}, \delta_{3,[[x,y],y]} : \mathrm{H}^1(G_k, \pi/[\pi]_3) \to \mathrm{H}^2(G_k, \hat{\mathbb{Z}}(3)).$$

Since an arbitrary element of $\pi/[\pi]_3$ can be written uniquely in the form $y^a x^b [x,y]^c$ for $a,b,c \in \hat{\mathbb{Z}}$, an arbitrary element of $C^1(G_k, \pi/[\pi]_3)$ is of the form $(b,a)_c$, as in (12.17). The obstruction δ_3 is therefore computed by the following:

Proposition 13. *Let $(b,a)_c$ be a 1-cocycle for G_k with values in $\pi/[\pi]_3$. Then:*

(1) *$\delta_{3,[[x,y],x]}(b,a)_c$ is represented by the cocycle*

$$\begin{aligned}(g,h) \quad \mapsto \quad & c(g)\chi(g)b(h) + \binom{b(g)+1}{2}\chi(g)a(h) \\ & + b(g)\chi(g)^2 a(h)b(h) - \frac{\chi(g)-1}{2}\chi(g)^2 c(h),\end{aligned}$$

(2) *$\delta_{3,[[x,y],y]}(b,a)_c$ is represented by the cocycle*

$$\begin{aligned}(g,h) \quad \mapsto \quad & c(g)\chi(g)a(h) + b(g)\binom{\chi(g)a(h)+1}{2} \\ & - \frac{\chi(g)-1}{2}\chi(g)^2 c(h) - f(g)\chi(g)a(h).\end{aligned}$$

Proof. We have the following equalities in $\pi/[\pi]_4$:

$$x^b y^a = y^a x^b [x,y]^{ab} [[x,y],y]^{b\binom{a+1}{2}} [[x,y],x]^{a\binom{b+1}{2}} \tag{12.20}$$

Replacing b and a by $-a$ in (12.20), yields:

$$[x^a, y^a] = [x,y]^{a^2} [[x,y],x]^{-a\binom{a}{2}} [[x,y],y]^{-a\binom{a}{2}} \tag{12.21}$$

For any $g \in G_k$, a straightforward computation using (12.12), (12.21) and (12.19) shows that:

$$g(y^a x^b [x,y]^c) = \tag{12.22}$$
$$y^{\chi(g)a} x^{\chi(g)b} [x,y]^{\chi(g)^2 c} [[x,y],x]^{-\frac{\chi(g)-1}{2}\chi(g)^2 c} [[x,y],y]^{-\frac{\chi(g)-1}{2}\chi(g)^2 c - f(g)\chi(g)a}$$

An arbitrary element of $\pi/[\pi]_3$ can be written uniquely in the form $y^a x^b [x,y]^c$ for $a,b,c \in \hat{\mathbb{Z}}$. Sending $y^a x^b [x,y]^c \in \pi/[\pi]_3$ to $y^a x^b [x,y]^c \in \pi/[\pi]_4$ determines a section s of the quotient map $\pi/[\pi]_4 \to \pi/[\pi]_3$. Let $p = (b,a)_c$. $\delta_3 p$ is represented by the cocycle

$$(g,h) \mapsto s(p(g))gs(p(h))s(p(gh))^{-1}$$

which gives cocycles representing $\delta_{3,[[x,y],x]} p$ and $\delta_{3,[[x,y],y]} p$. Combining (12.20) and (12.22) gives the desired result. □

We give a formula for δ_3 in terms of triple Massey products of elements of $\mathrm{H}^1(G_k, \hat{\mathbb{Z}}(1))$.

Definition 14. The triple Massey product $\langle \alpha, \beta, \gamma \rangle$ for 1 cocycles α, β, γ such that $\alpha \cup \beta = 0$ and $\beta \cup \gamma = 0$ is described by choosing cochains A, B such that $DA = \alpha \cup \beta$ and $DB = \beta \cup \gamma$, and setting $\langle \alpha, \beta, \gamma \rangle = A \cup \gamma + \alpha \cup B$. The choice $\{A, B\}$ is the called the defining system. The triple Massey product determines a partially defined multivalued product on H^1.

Remark 15. Results of Dwyer and Stallings [Dwy75] relate the element of

$$\mathrm{H}^2(\pi/[\pi]_n, [\pi]_n/[\pi]_{n+1})$$

classifying the central extension

$$1 \to [\pi]_n/[\pi]_{n+1} \to \pi/[\pi]_{n+1} \to \pi/[\pi]_n \to 1$$

to n^{th} order Massey products. The computation of δ_3 is equivalent to computing the element of $\mathrm{H}^2(\pi/[\pi]_3 \rtimes G_k, [\pi]_3/[\pi]_4)$ classifying

$$1 \to [\pi]_3/[\pi]_4 \to \pi/[\pi]_4 \rtimes G_k \to \pi/[\pi]_3 \rtimes G_k \to 1.$$

Because $Dc = -b \cup a$ and $D\binom{b+1}{2} = -(b - \frac{\chi-1}{2}) \cup b$ (by the same argument in Example 10), the expression for $\delta_{3,[[x,y],x]}(b,a)_c$ given in Proposition 13 looks similar to a triple Massey product $\pm\langle \{\pm b\}, \{\pm b\}, a \rangle$, except the $c \cup b$ term should be $b \cup c$. The cup product on cohomology is graded commutative, and the analogue on the level of cochains, given below in Lemma 16, allows us to change the order of c and b, which will express $\delta_{3,[[x,y],x]}(b,a)_c$ as a Massey product.

For cochains $c \in C^1(G_k, \hat{\mathbb{Z}}(n))$ and $b \in C^1(G_k, \hat{\mathbb{Z}}(m))$, define

$$cb : G_k \to \hat{\mathbb{Z}}(n+m) \quad \text{by } (cb)(g) = c(g)b(g).$$

Lemma 16. *Let $c \in C^1(G_k, \hat{\mathbb{Z}}(n))$ be an arbitrary cochain, and b in $C^1(G_k, \hat{\mathbb{Z}}(m))$ be a cocycle. Then*

$$(D(cb) + b \cup c + c \cup b)(g,h) = Dc(g,h)b(g) + Dc(g,h)\chi(g)^m b(h)$$

Proof. By definition of D, for any $g,h \in G_k$,

$$D(cb)(g,h) = (cb)(g) + \chi(g)^{n+m}(cb)(h) - (cb)(gh),$$

$$c(gh) = c(g) + \chi(g)^n c(h) - Dc(g,h).$$

Since b is a cocycle, $b(gh) = b(g) + \chi(g)^m b(h)$. Combining equations, we have

$$\begin{aligned} D(cb)(g,h) =& c(g)b(g) + \chi(g)^{n+m}c(h)b(h) \\ & - (c(g) + \chi(g)^n c(h) - Dc(g,h))(b(g) + \chi(g)^m b(h)) \\ =& Dc(g,h)b(g) + Dc(g,h)\chi(g)^m b(h) - (c \cup b(g,h) + b \cup c(g,h)) \end{aligned}$$

□

Proposition 17. *Let $p = (b,a)_c \in C^1(G_k, \pi/[\pi]_3)$ be a 1-cocycle, where $(b,a)_c$ is as in the notation of* (12.17)*. Then the following holds.*

(1) $\delta_{3,[[x,y],x]}(p) = -(b + \frac{\chi-1}{2}) \cup c - \binom{b}{2} \cup a,$

(2) $\delta_{3,[[x,y],y]}(p) = (a + \frac{\chi-1}{2}) \cup (ab - c) + \binom{a}{2} \cup b - f \cup a.$

Proof. By Corollary 8 and Lemma 16, we have that $-D(cb)(g,h) =$

$$c(g)\chi(g)b(h) + b(g)\chi(g)^2 c(h) + b(g)^2\chi(g)a(h) + b(g)\chi(g)^2 a(h)b(h).$$

Subtracting this expression for $-D(cb)$ from the cocycle representing $\delta_{3,[[x,y],x]}p$ given in Proposition 13 shows that $\delta_{3,[[x,y],x]}p$ is represented by the cocycle sending (g,h) to

$$-b(g)\chi(g)^2 c(h) - b(g)^2\chi(g)a(h) + \binom{b(g)+1}{2}\chi(g)a(h) - \frac{\chi(g)-1}{2}\chi(g)^2 c(h).$$

Note that

$$-b(g)^2\chi(g)a(h) + \binom{b(g)+1}{2}\chi(g)a(h) = \frac{b(g)(-b(g)+1)}{2}\chi(g)a(h)$$

$$= -\Big(\binom{b}{2} \cup a\Big)(g,h).$$

Therefore

$$\delta_{3,[[x,y],x]}p = -b \cup c - \binom{b}{2} \cup a - \frac{\chi-1}{2} \cup c,$$

giving the claimed expression for $\delta_{3,[[x,y],x]}p$.

The claimed expression for $\delta_{3,[[x,y],y]}p$ follows from this formula for $\delta_{3,[[x,y],x]}p$ and a symmetry argument. Consider the action of G_k on the profinite completion of the free group on two generators $F_2^\wedge = \langle x,y\rangle^\wedge$ given by

$$g(x) = x^{\chi(g)}$$

$$g(y) = y^{\chi(g)}.$$

The G_k action on π described by (12.12) would reduce to this action on $F_2^\wedge$ if $\mathfrak{f}$ where in the center of π. In particular, sending x to x and y to y induces isomorphisms of profinite groups with G_k actions

$$\pi/[\pi]_3 \cong F_2^\wedge/[F_2^\wedge]_3$$

$$[\pi]_3/[\pi]_4 \cong [F_2^\wedge]_3/[F_2^\wedge]_4$$

Furthermore, viewing f as a formal variable in the proof of Proposition 13, we see that Proposition 13 implies that these isomorphisms fit into the commutative diagram

$$\begin{array}{ccc} \mathrm{H}^1(G_k, \pi/[\pi]_3) & \xrightarrow{\delta_3 + \mathfrak{f}\cup a} & \mathrm{H}^2(G_k, [\pi]_3/[\pi]_4) \\ \downarrow \cong & & \cong \uparrow \\ \mathrm{H}^1(G_k, F_2^\wedge/[F_2^\wedge]_3) & \xrightarrow{\delta_3} & \mathrm{H}^2(G_k, [F_2^\wedge]_3/[F_2^\wedge]_4) \end{array} \tag{12.23}$$

Let $i : F_2^\wedge \to F_2^\wedge$ be the G_k equivariant involution defined by

$$i(x) = y$$

$$i(y) = x.$$

Note that i induces an endomorphism of the short exact sequence of G_k modules

$$1 \to [F_2^\wedge]_3/[F_2^\wedge]_4 \to F_2^\wedge/[F_2^\wedge]_4 \to F_2^\wedge/[F_2^\wedge]_3 \to 1.$$

Thus we have a commutative diagram

$$\begin{array}{ccc} \mathrm{H}^1(G_k, F_2^\wedge/[F_2^\wedge]_3) & \xrightarrow{\delta_3} & \mathrm{H}^2(G_k, [F_2^\wedge]_3/[F_2^\wedge]_4) \\ {\scriptstyle i_*}\uparrow & & {\scriptstyle i_*}\uparrow \\ \mathrm{H}^1(G_k, F_2^\wedge/[F_2^\wedge]_3) & \xrightarrow{\delta_3} & \mathrm{H}^2(G_k, [F_2^\wedge]_3/[F_2^\wedge]_4) \end{array}$$

Since i is an involution, so is i_*, whence

$$\delta_3 = i_* \delta_3 i_*.$$

With respect to the decomposition

$$\mathrm{H}^2(G_k, [F_2^\wedge]_3/[F_2^\wedge]_4) = \mathrm{H}^2(G_k, \hat{\mathbb{Z}}(3)) \cdot [[x,y],x] \oplus \mathrm{H}^2(G_k, \hat{\mathbb{Z}}(3)) \cdot [[x,y],y]. \tag{12.24}$$

i_* acts by the matrix

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix},$$

or in other terms,

$$\delta_{3,[[x,y],y]} = -\delta_{3,[[x,y],x]} i_*. \tag{12.25}$$

The map i_* on $\mathrm{H}^1(G_k, F_2^\wedge/[F_2^\wedge]_3)$ we compute as

$$i_*((b,a)_c)(g) = x^{a(g)}y^{b(g)}[y,x]^{c(g)}$$

$$= [x^{a(g)}, y^{b(g)}]y^{b(g)}x^{a(g)}[x,y]^{-c(g)} = y^{b(g)}x^{a(g)}[x,y]^{a(g)b(g)-c(g)} = (a,b)_{ab-c}(g).$$

Combining (12.23) with (12.25)

$$\delta_{3,[[x,y],y]}((b,a)_c) = \delta^{F_2^\wedge}_{3,[[x,y],y]}((b,a)_c) - f\cup a = -\delta^{F_2^\wedge}_{3,[[x,y],x]}(i_*(b,a)_c) - f\cup a$$

$$= -\delta^{F_2^\wedge}_{3,[[x,y],x]}((a,b)_{ab-c}) - f\cup a = -\delta_{3,[[x,y],x]}((a,b)_{ab-c}) - f\cup a$$

$$= (a+\frac{\chi-1}{2})\cup(ab-c) + \binom{a}{2}\cup b - f\cup a$$

as claimed by the proposition. In the above manipulation, we have marked obstructions corresponding to $F_2^\wedge$ with a superscript to avoid confusion.

□

Remark 18. The above symmetry argument combined with the explicit cocycle for $\delta_{3,[[x,y],y]}$ given in Proposition 13 gives unexploited computational information.

Theorem 19. *Let p be an element of $\mathrm{H}^1(G_k, \pi/[\pi]_3)$, so p is represented by a cocycle $(b,a)_c \in C^1(G_k, \pi/[\pi]_3)$ in the notation of* (12.17)*. Then*

$$\delta_{3,[[x,y],x]}(p) = \langle (b+\frac{\chi-1}{2}), b, a\rangle \qquad \textit{defining system:} \{-\binom{b}{2}, -c\}$$

$$\delta_{3,[[x,y],y]}(p) = -\langle (a+\frac{\chi-1}{2}), a, b\rangle - f\cup a \qquad \textit{defining system:} \{-\binom{a}{2}, c-ab\}.$$

In particular, for $(b,a) \in \mathrm{Jac}(\mathbb{P}^1_k - \{0,1,\infty\})(k) = k^*\times k^*$, we have

$$\delta_{3,[[x,y],x]}(b,a) = \langle \{-b\}, b, a\rangle$$

$$\delta_{3,[[x,y],y]}(b,a) = -\langle \{-a\}, a, b\rangle - f\cup a.$$

Remark 20. (i) As above, an element of k^* also denotes its image in $\mathrm{H}^1(G_k, \hat{\mathbb{Z}}(1))$ under the Kummer map in the last two equations. The brackets in the notation $\{-b\}, \{-a\}$ serve to distinguish between the additive inverse of b in $H^1(G_k, \hat{\mathbb{Z}}(1))$ and the image of $-b$ under the Kummer map. We note the obvious remark that the Kummer map is a homomorphism, because this will appear in (iii) of this remark on the level of cocycles; namely given $a, b \in k^*$ with compatibly chosen n^{th} roots $\sqrt[n]{a}$ and $\sqrt[n]{b}$, then $\{a\}+\{b\} : G_k \to \hat{\mathbb{Z}}(1)$ is the image under the Kummer map of ab with $\sqrt[n]{a}\sqrt[n]{b}$ chosen as the n^{th} root of ab. This means that if one has chosen compatible primitive roots of -1, as is the case by (12.18) and Remark 3, the cocycle

$\{-1\}+\{a\}$ is different from $-\{-1\}+\{a\}$ although both give the same class in cohomology, namely the class $\{-a\}$.

(ii) Expressing δ_3 in terms of Massey products reduces the dependency on c to the choices of the defining systems. In fact, after restricting to defining systems of the appropriate form, the choice of these defining systems and the choice of lift are equivalent. More explicitly, we will say that a choice for the defining systems $\{A,B\}$ of $\langle\{-x\},x,y\rangle$ and $\{C,D\}$ of $\langle\{-y\},y,x\rangle$ is *compatible* if $B+D=-xy$, $A=-\binom{x}{2}$, and $C=-\binom{y}{2}$. The choice of defining system also encompasses choosing cocycle representatives for the cohomology classes involved; the cocycle representative for $\{-x\}$ is the representative for x plus $\frac{\chi-1}{2}$, and similarly for $\{-y\}$, as in (i). Then choosing a lift of (b,a) in $\mathrm{H}^1(G_k,\pi/[\pi]_2)$ to $(b,a)_c$ in $\mathrm{H}^1(G_k,\pi/[\pi]_3)$ is equivalent to choosing compatible defining systems for $\langle\{-b\},b,a\rangle$ and $\langle\{-a\},a,b\rangle$, by Corollary 8 and Theorem 19. As we are ultimately interested in obstructing points of the Jacobian from lying on the curve, it is natural to suppress both the defining system in the Massey product and the choice of lift, and view δ_3 and triple Massey products as multivalued functions on $\mathrm{H}^1(G_k,\pi/[\pi]_2)$.

Proof. Comparing the expression for $\delta_{3,[[x,y],x]}(b,a)_c$ of Proposition 17, and the equations $D(-\binom{b}{2})=(b+\frac{\chi-1}{2})\cup b$ of Example 10, and $D(-c)=b\cup a$ of Corollary 8 with the definition of the triple Massey product (Definition 14) shows

$$\delta_{3,[[x,y],x]}(b,a)_c=\langle(b+\frac{\chi-1}{2}),b,a\rangle$$

with the defining system $\{-\binom{b}{2},-c\}$.

By Lemma 16,

$$-D(ab)=a\cup b+b\cup a,$$

whence $D(c-ab)=a\cup b$ by Corollary 8. Comparing $D(-\binom{a}{2})=(a+\frac{\chi-1}{2})\cup a$, $D(c-ab)=a\cup b$, and the expression for $\delta_{3,[[x,y],y]}(b,a)_c$ of Proposition 17 with the definition of the triple Massey product shows

$$\delta_{3,[[x,y],y]}(b,a)_c=-\langle(a+\frac{\chi-1}{2}),a,b\rangle-f\cup a$$

with defining system $\{-\binom{a}{2},c-ab\}$. By (12.18), we have $a+\frac{\chi-1}{2}=\{-a\}$ and $b+\frac{\chi-1}{2}=\{-b\}$, showing the theorem. □

12.4 Evaluating δ_2 on $\mathrm{Jac}(k)$

Let k be a subfield of $\mathbb{C}$ or a completion of a number field equipped with $\mathbb{C}\supset\overline{\mathbb{Q}}\subseteq\bar{k}$ as in 12.2. Let $X=\mathbb{P}^1_k-\{0,1,\infty\}$ and recall that in 12.2.2 we fixed an isomorphism $\mathrm{Jac}(X)=\mathbb{G}_{m,k}\times\mathbb{G}_{m,k}$. Let $\pi=\pi_1(X_{\bar{k}},\overrightarrow{01})$. In (12.11), we specified an isomorphism $\pi=\langle x,y\rangle^{\wedge}$.

The obstruction δ_2 is given on (b,a) in $\mathrm{Jac}(X)(k)$ by $\delta_2(b,a) = b \cup a$, so evaluating δ_2 is equivalent to evaluating the cup product

$$\mathrm{H}^1(G_k, \hat{\mathbb{Z}}(1)) \otimes \mathrm{H}^1(G_k, \hat{\mathbb{Z}}(1)) \to \mathrm{H}^2(G_k, \hat{\mathbb{Z}}(2)). \tag{12.26}$$

Evaluating the obstruction δ_2^2 coming from the lower exponent 2 central series (cf. 12.2.3) is equivalent to evaluating the mod 2 cup product

$$\mathrm{H}^1(G_k, \mathbb{Z}/2) \otimes \mathrm{H}^1(G_k, \mathbb{Z}/2) \to \mathrm{H}^2(G_k, \mathbb{Z}/2), \tag{12.27}$$

and this evaluation is recalled for $k = \mathbb{Q}_p$, $\mathbb{R}$, and $\mathbb{Q}$ in 12.4.1– 12.4.3. The remainder of Section 12.4 gives evaluation results for the obstruction δ_2 itself. From the bilinearity of δ_2, Proposition 24 finds infinite families of points of $\mathrm{Jac}(k)$ which are unobstructed by δ_2, but which are not the image of a rational point or tangential point under the Abel-Jacobi map. This is rephrased as "the 2-nilpotent section conjecture is false" in 12.4.4 and Proposition 25. These families provide a certain supply of points on which to evaluate δ_3. The subsection 12.4.5 contains a finite algorithm for determining if δ_2 is zero or not for $k = \mathbb{Q}$, using Tate's calculation of $\mathrm{K}_2(\mathbb{Q})$, and gives Jordan Ellenberg's geometric proof that the cup product factors through K_2.

12.4.1 The mod 2 *cup product for* k_v

Let p be an odd prime. Let k_v be a finite extension of $\mathbb{Q}_p$ with valuation $v : k_v^* \twoheadrightarrow \mathbb{Z}$, integer ring $\mathcal{O}_v$ and residue field $\mathbb{F}_v$. Let $\mathfrak{p}$ be a uniformizer of $\mathcal{O}_v$ and $u \in \mathcal{O}_v$ be a unit and not a square, so $\{\mathfrak{p}, u\}$ is a basis for the $\mathbb{Z}/2$ vector space

$$k_v^*/(k_v^*)^2 \cong \mathrm{H}^1(G_{k_v}, \mathbb{Z}/2),$$

where the isomorphism follows from the Kummer exact sequence (12.6) and Hilbert 90. By Hilbert 90, we have that $\mathrm{H}^2(G_{k_v}, \mathbb{Z}/2)$ is the 2 torsion of the Brauer group $\mathrm{H}^2(G_{k_v}, \overline{k_v}^*)$ of k_v, which is isomorphic to $\mathbb{Q}/\mathbb{Z}$ by the invariant (see [CF67, VI], for instance), so

$$\mathrm{H}^2(G_K, \mathbb{Z}/2) \cong (\mathbb{Q}/\mathbb{Z})[2] = (\frac{1}{2}\mathbb{Z})/\mathbb{Z}.$$

The (distributive and commutative) mod 2 cup product (12.27) is given by the table

$\cup$	u	$\mathfrak{p}$
u	0	$1/2$
$\mathfrak{p}$	$1/2$	$\{-1\} \cup \mathfrak{p}$

where $\{-1\} \cup \mathfrak{p} = 0$ if -1 is a square in $\mathbb{F}_v$ and $\{-1\} \cup \mathfrak{p} = 1/2$ otherwise.

We include a derivation of this well-known calculation: as $\mathrm{H}^2(G_{k_v}, \mathbb{Z}/2)$ injects into $\mathrm{H}^2(G_{k_v}, \overline{k_v}^*)$, we may calculate in the Brauer group. For $(a,b) \in k_v^* \oplus k_v^*$, define $E_{(\sqrt{a},b)} \in C^1(G_{k_v}, \overline{k_v}^*)$ by

$$E_{(\sqrt{a},b)}(\sigma) = (\sqrt{a})^{b(\sigma)},$$

where $b : G_{k_v} \to \{0,1\}$ is defined by $(-1)^{a(\sigma)} = (\sigma\sqrt{a})/\sqrt{a}$. A short calculation shows that

$$DE_{(\sqrt{a},b)}(\sigma,\tau) = (-1)^{a(\sigma)b(\tau)} a^{b(\sigma)b(\tau)},$$

whence $a \cup b$ in $\mathrm{H}^2(G_{k_v}, \overline{k_v}^*)$ is represented by

$$(\sigma,\tau) \mapsto a^{b(\sigma)b(\tau)}. \tag{12.28}$$

Let k_v^{nr} denote the maximal unramified extension of k_v, and $v : (k_v^{nr})^* \to \mathbb{Z}$ the extension of the valuation. For $b = u$, the cocycle (12.28) factors through $\mathrm{Gal}({k_v}^{nr}/k_v)^2$, and by [CF67, Chap VI 1.1 Thm 2 pg 130],

$$v_* : \mathrm{H}^2(\mathrm{Gal}({k_v}^{nr}/k_v), (k_v^{nr})^*) \to \mathrm{H}^2(\mathrm{Gal}(k_v^{nr}/k_v), \mathbb{Z})$$

is an isomorphism, showing that $\{u\} \cup \{u\} = 0$, and the invariant of $\{\mathfrak{p}\} \cup \{u\}$ is $1/2$ as claimed (see [CF67, pg 130]). To compute $\mathfrak{p} \cup \mathfrak{p}$, note that for $a = -1$, the cochain $(\sigma,\tau) \mapsto a^{b(\sigma)b(\tau)}$ equals $b \cup b$. By the above, $a \cup b$ is also represented by $(\sigma,\tau) \mapsto a^{b(\sigma)b(\tau)}$, so it follows that

$$\{-1\} \cup \mathfrak{p} = \mathfrak{p} \cup \mathfrak{p}.$$

It follows that δ_2 is non-trivial: let $X = \mathbb{P}^1_{\mathbb{Q}} - \{0,1,\infty\}$. Let $\delta_2^{(2,p)}$ denote δ_2^2 for $k = \mathbb{Q}_p$ and $X_{\mathbb{Q}_p}$. Consider $\delta_2^{(2,p)}$ as a function on $\mathrm{Jac}(X)(\mathbb{Q})$ by evaluating $\delta_2^{(2,p)}$ on the corresponding $\mathbb{Q}_p$ point of $\mathrm{Jac}(X_{\mathbb{Q}_p})$.

Corollary 21. *Choose x,y in $\mathbb{Q}^*$. Let p be an odd prime and u be an integer which is not a quadratic residue mod p. Then $\delta_2^{(2,p)}(uy^2, px^2) \neq 0$, and therefore $\delta_2^2(uy^2, px^2) \neq 0$ and $\delta_2(uy^2, px^2) \neq 0$.*

12.4.2 The mod 2 *cohomology of* $G_{\mathbb{R}}$

By [Hat02, III Example 3.40 p. 250] or [Bro94, III.1 Ex 2 p.58 p.108], there is a ring isomorphism

$$\mathrm{H}^*(G_{\mathbb{R}}, \mathbb{Z}/2) \cong \mathrm{H}^*(\mathbb{Z}/2, \mathbb{Z}/2) \cong \mathbb{Z}/2[\alpha]$$

where α is the nontrivial class in degree 1, namely

$$\alpha = \{-1\} \in \mathbb{R}^*/(\mathbb{R}^*)^2 = \mathrm{H}^1(G_{\mathbb{R}}, \mu_2) = \mathrm{H}^1(G_{\mathbb{R}}, \mathbb{Z}/2\mathbb{Z}).$$

In particular, the cup product is an isomorphism

$$\mathrm{H}^1(G_{\mathbb{R}}, \mathbb{Z}/2\mathbb{Z}(1)) \otimes \mathrm{H}^1(G_{\mathbb{R}}, \mathbb{Z}/2\mathbb{Z}(1)) \to \mathrm{H}^2(G_{\mathbb{R}}, \mathbb{Z}/2\mathbb{Z}(2)).$$

The map $C^2(G_{\mathbb{R}},\mathbb{Z}/2)\to\mathbb{Z}/2$ given by evaluating a cochain at (τ,τ) for τ the non-trivial element of $G_{\mathbb{R}}$ determines an isomorphism $\mathrm{H}^2(G_{\mathbb{R}},\mathbb{Z}/2)\to\mathbb{Z}/2$.

Let $X=\mathbb{P}^1_{\mathbb{Q}}-\{0,1,\infty\}$, and let $\delta_2^{(2,\mathbb{R})}$ denote δ_2^2 for $k=\mathbb{R}$ and $X_{\mathbb{R}}$. Consider $\delta_2^{(2,\mathbb{R})}$ as a function on $\mathrm{Jac}(X)(\mathbb{Q})$ by evaluating $\delta_2^{(2,\mathbb{R})}$ on the corresponding $\mathbb{R}$ point of $\mathrm{Jac}(X_{\mathbb{R}})$.

Corollary 22. *Let b,a be elements of $\mathbb{Q}^*$. Then $\delta_2^{(2,\mathbb{R})}(b,a)\neq 0$ if and only if $a,b<0$. If $a,b<0$, then $\delta_2^2(b,a)\neq 0$ and $\delta_2(b,a)\neq 0$.*

12.4.3 The mod 2 cup product for $G_{\mathbb{Q}}$

There is a finite algorithm for computing the cup product of two Kummer classes

$$\mathbb{Q}^*\otimes\mathbb{Q}^*\to\mathrm{H}^1(G_{\mathbb{Q}},\mathbb{Z}/2\mathbb{Z}(1))\otimes\mathrm{H}^1(G_{\mathbb{Q}},\mathbb{Z}/2\mathbb{Z}(1))\to\mathrm{H}^2(G_{\mathbb{Q}},\mathbb{Z}/2\mathbb{Z}(2)).$$

The phrase "computing an element of $\mathrm{H}^2(G_{\mathbb{Q}},\mathbb{Z}/2\mathbb{Z}(2))$" means the following. By the local-global principle for the Brauer group, the theorem of Hasse, Brauer, and Noether, see [NSW08, 8.1.17 Thm p. 436], we have an isomorphism

$$\mathrm{H}^2(G_{\mathbb{Q}},\mathbb{Z}/2\mathbb{Z}(2))=\mathrm{Br}(\mathbb{Q})_2\otimes\mu_2=\ker\Big(\bigoplus_v\mathrm{Br}(\mathbb{Q}_v)_2\xrightarrow{\Sigma_v\mathrm{inv}_v}\mathbb{Q}/\mathbb{Z}\Big)\otimes\mu_2$$

where A_2 is the 2-torsion of an abelian group A and $\mathrm{inv}_v:\mathrm{Br}(k_v)\hookrightarrow\mathbb{Q}/\mathbb{Z}$ is the local invariant map for the Brauer group of the local field k_v, see [CF67, VI], and v ranges over all places of $\mathbb{Q}$. The class in $\mathrm{H}^2(G_{\mathbb{Q}},\mathbb{Z}/2\mathbb{Z}(2))$ is therefore completely determined by its restrictions to local cohomology groups with the freedom to ignore one place by reciprocity. We will benefit from this freedom by ignoring the prime 2 for which we did not describe the mod 2 cup product computation above.

Given b and a in $\mathbb{Q}^*$, we give a finite algorithm for computing $\mathrm{inv}_v(\{b\}\cup\{a\})$ for every $v\neq 2$. By (12.4.1), for an odd prime p with $p\nmid ab$ we have $\{b\}\cup\{a\}=0$. It therefore remains to evaluate

$$\mathrm{inv}_v(\{b\}\cup\{a\})$$

for $v=\mathbb{R}$ and the finitely many odd primes $v=p$ with $p\mid ab$. This is accomplished in finitely many steps by 12.4.1 and 12.4.2.

In fact, given any field extension $\mathbb{Q}\subset E$ and any cocycle in $C^2(\mathrm{Gal}(E/\mathbb{Q}),\mathbb{Z}/2)$ (for instance the ones given in Proposition 17), there is a finite algorithm for computing the associated element of $H^2(G_{\mathbb{Q}},\mathbb{Z}/2)$.

12.4.4 The 2-nilpotent section conjecture for number fields is false

We describe several families of points of $\mathrm{Jac}(\mathbb{P}^1_k - \{0,1,\infty\})(k)$ such that δ_2 vanishes.

Example 23. (1) The map δ_2 vanishes on the k points and tangential points of the curve $\mathbb{P}^1_k - \{0,1,\infty\}$ by design. Therefore, the k points of

$$\mathrm{Jac}(\mathbb{P}^1_k - \{0,1,\infty\}) = \mathbb{G}_{m,k} \times \mathbb{G}_{m,k}$$

of the form $(x, 1-x)$ or $(-x,x)$ satisfy $\delta_2 = 0$ by (12.15) and Lemma 4.

From a more computational point of view, the vanishing of δ_2 on $(-x,x)$ follows from the the calculation in Lemma 10 identifying the cochain whose boundary is $\{-x\} \cup \{x\}$ (use Lemma 12.18 and 1, to identify $\{-x\}$ and $\{x\} + \frac{\chi-1}{2}$). I do not presently see a specific cochain in $C^1(G_k, \hat{\mathbb{Z}}(2))$ whose boundary is $\{x\} \cup \{1-x\}$, although I would not be surprised if such a cochain could be written down explicitly.

(2) Since $\delta_2(b,a) = \{b\} \cup \{a\}$ by Proposition 7, the map δ_2 is bilinear in both coordinates of

$$k^* \oplus k^* = (\mathbb{G}_m \times \mathbb{G}_m)(k) = \mathrm{Jac}(\mathbb{P}^1_k - \{0,1,\infty\})(k)$$

Therefore, for any (b,a) in $k^* \oplus k^*$, such that $\delta_2(b,a) = 0$, the points of the form (b^m, a^n), for integers m and n, satisfy $\delta_2(b^m, a^n) = 0$ as well. Likewise for any (b,a), (b,c) such that $\delta_2(b,a) = \delta_2(b,c) = 0$, the point of the Jacobian (b,ac) also satisfies $\delta_2(b,ac) = 0$. As was pointed out by Jordan Ellenberg, this produces many families of k points of $\mathrm{Jac}(\mathbb{P}^1_k - \{0,1,\infty\})$ which are unobstructed by δ_2. A special case of this is mentioned in Proposition 24 below.

Proposition 24. *Let $X = \mathbb{P}^1_k - \{0,1,\infty\}$. For any x in k^*, the map δ_2 vanishes on*

$$(x, (1-x)^m), \quad ((-x)^m, x), \quad ((1-x)(-x), x),$$

$$(x^{n_1}(1 - ((1-x)^{n_2}(-x)^{n_3})), (1-x)^{n_2}(-x)^{n_3}).$$

Proof. This follows immediately from the discussion in Example 23 above. □

Say the "n-nilpotent section conjecture" for a smooth curve X over a field k holds if the natural map from k points and tangential points to conjugacy classes of sections of

$$1 \to \pi_1(X_{\bar{k}})^{\mathrm{ab}} \to \pi_1(X)/[\pi_1(X_{\bar{k}})]_2 \to G_k \to 1 \tag{12.29}$$

which arise from k points of $\mathrm{Jac}\, X$, and lift to sections of

$$1 \to \pi_1(X_{\bar{k}})/[\pi_1(X_{\bar{k}})]_{n+1} \to \pi_1(X)/[\pi(X_{\bar{k}})]_{n+1} \to G_k \to 1 \tag{12.30}$$

is a bijection. This is similar to the notion of "minimalistic" birational section conjectures introduced by Florian Pop [Pop10]. The notion given here has the disadvantage that it mentions the points of the Jacobian, and is therefore not entirely group

theoretic. The reason for this is that finite nilpotent groups decompose as a product of p groups, so the sections of (12.29) and (12.30) decompose similarly, allowing for sections which at different primes arise from different rational points of X. Restricting to a single prime will not give a "minimalistic" section conjecture by results of Hoshi [Hos10].

Because the conjugacy classes of sections of a split short exact sequence of profinite groups

$$1 \to Q \to Q \rtimes G \to G \to 1$$

are in natural bijective correspondence with the elements of $\mathrm{H}^1(G,Q)$, the n-nilpotent section conjecture for a curve with a rational point is equivalent to: *the natural map from k points and tangential points to the kernel of δ_n is a bijection,* where the kernel of δ_n is considered as a subset of $\mathrm{Jac}\,X$. More precisely, a smooth, pointed curve X gives rise to a commutative diagram

$$\begin{array}{ccc}
\mathrm{H}^1(G_k,\pi/[\pi]_n) & \xrightarrow{\delta_n} & \mathrm{H}^2(G_k,[\pi]_n/[\pi]_{n+1}) \\
\Big\downarrow{\scriptstyle pr} & & \\
\mathrm{H}^1(G_k,\pi/[\pi]_2) & \xleftarrow[\alpha]{} & X(k)\cup\textstyle\bigcup_{x\in\overline{X}-X}(T_x\overline{X}(k)-\{0\}) \\
\Big\uparrow{\scriptstyle \kappa} & & \\
\mathrm{Jac}(X)(k) & &
\end{array}$$

where $\overline{X}$ denotes the smooth compactification of X, and π denotes the fundamental group of $X_{\overline{k}}$. The n-nilpotent section conjecture is the claim α induces a bijection

$$X(k)\cup\bigcup_{x\in\overline{X}-X}(T_x\overline{X}(k)-\{0\})\to\kappa(\mathrm{Jac}(X)(k))\cap pr(\ker(\delta_n)).$$

Say the "n-nilpotent section conjecture" holds for a field k, if for all smooth, hyperbolic curves over k, the n-nilpotent section conjecture holds.

Proposition 25. *The 2-nilpotent section conjecture fails for any subfield k of $\mathbb{C}$ or k the completion of a number field. In fact, the 2-nilpotent section conjecture does not hold for $\mathbb{P}^1_k-\{0,1,\infty\}$.*

Proof. Choose $x\neq 1$ in k^* such that $(1-x)^2$ does not equal $-x$. Then the k point of $\mathrm{Jac}(\mathbb{P}^1_k-\{0,1,\infty\})$ given by $(x,(1-x)^2)$ is not the image of a k point or tangential point of $\mathbb{P}^1_k-\{0,1,\infty\}$ by Lemmas 12.15 and 4. By Proposition 24, the section of (12.29) determined by $(x,(1-x)^2)$ lifts to a section of (12.30) for $n=2$. □

While the failure of a "minimalistic section conjecture" is not surprising at all, some do hold. Moreover, the "minimalistic section conjectures" in [Pop10] [Wic10] do not mention the points of the Jacobian and so control the rational points of X group theoretically.

12.4.5 The obstruction δ_2 over $\mathbb{Q}$

By [Tat76] Theorem 3.1, the cup product (12.26) composed with the Kummer map (12.7)

$$k^* \otimes k^* \to \mathrm{H}^2(G_k, \hat{\mathbb{Z}}(2)) \tag{12.31}$$

factors through the Milnor K_2-group of k

$$\mathrm{K}_2(k) = k^* \otimes_{\mathbb{Z}} k^* / \langle x \otimes (1-x) : x \in k^* \rangle$$

mapping to $\mathrm{H}^2(G_k, \hat{\mathbb{Z}}(2))$ by the Galois symbol $h_k : \mathrm{K}_2(k) \to \mathrm{H}^2(G_k, \hat{\mathbb{Z}}(2))$.

Proposition 26. *Let k be a finite extension of $\mathbb{Q}$, and $X = \mathbb{P}^1_k - \{0,1,\infty\}$. For any $(b,a) \in \mathrm{Jac}(X)(k) = k^* \times k^*$ we have $\delta_2(b,a) = 0$ if and only if $b \otimes a = 0$ in $\mathrm{K}_2(k)$.*

Proof. Since $\delta_2(b,a) = b \cup a$ by Proposition 7, we have that δ_2 factors through h_k. By [Tat76] Theorem 5.4, h_k is an isomorphism onto the torsion subgroup of $\mathrm{H}^2(G_k, \hat{\mathbb{Z}}(2))$. □

Tate's computation of $\mathrm{K}_2(\mathbb{Q})$ thus gives an algorithm for computing δ_2 for $\mathbb{P}^1_{\mathbb{Q}} - \{0,1,\infty\}$ on any rational point (b,a) of $\mathrm{Jac}(\mathbb{P}^1_{\mathbb{Q}} - \{0,1,\infty\})(\mathbb{Q}) = \mathbb{Q}^* \times \mathbb{Q}^*$: by [Mil71, Thm 11.6], there is an isomorphism

$$\mathrm{K}_2(\mathbb{Q}) \cong \mu_2 \oplus_{p \text{ odd prime}} \mathbb{F}_p^*$$

given by the tame symbols: for odd p (with p-adic valuation v_p)

$$\mathrm{K}_2(\mathbb{Q}) \to \mathbb{F}_p^*$$

$$x \otimes y \mapsto (x,y)_p = (-1)^{v_p(x)v_p(y)} x^{v_p(y)} y^{-v_p(x)} \in \mathbb{F}_p^*,$$

and a map at the prime 2

$$\mathrm{K}_2(\mathbb{Q}) \to \mu_2$$
$$x \otimes y \mapsto (x,y)_2 = (-1)^{iI+jK+kJ}$$

where $x = (-1)^i 2^j 5^k u$ and $y = (-1)^I 2^J 5^K u'$ with $k, K = 0$ or 1, and u, u' quotients of integers congruent to 1 mod 8.

By Proposition 26, we have $\delta_2(b,a) = 0$ if and only if $(b,a)_p = 0$ for $p = 2$ and for p equal to all odd primes dividing a or b.

Example 27. As an example of this algorithm, consider $\delta_2(p,-p)$ for p an odd prime: for q different from p and 2, we have $(p,-p)_q = 1$ because $v_q(p)$ and $v_q(-p)$ vanish. At the prime p, we have $(p,-p)_p = (-1)^1 p/(-p) = 1$. For the prime 2, express p in the form $p = (-1)^i 2^j 5^k u$ with $k = 0,1$ and u a quotient of integers congruent to 1 mod 8. Then $-p = (-1)^{i+1} 2^j 5^k u$, and

$$(p,-p)_2 = (-1)^{i(i+1)+2jk} = 1.$$

Thus $\delta_2(p,-p)=0$, as also followed from Lemma 4, as $(p,-p)$ is the image of a tangential point of $\mathbb{P}^1_{\mathbb{Q}}-\{0,1,\infty\}$, or can be deduced from the Steinberg relation.

Remark 28. The computation of δ_2 for $\mathbb{P}^1_k-\{0,1,\infty\}$ gives a geometric proof that (12.31) factors through $\mathrm{K}_2(k)$, as observed by Jordan Ellenberg. Namely, by construction δ_2 vanishes on the image of

$$\mathbb{P}^1_k-\{0,1,\infty\}(k)\to \mathrm{Jac}(\mathbb{P}^1_k-\{0,1,\infty\})(k)=k^*\times k^*.$$

By (12.15), this image is $(x,1-x)$, and by Proposition 7, the obstruction δ_2 is given by $\delta_2(b,a)=b\cup a$. Thus, the map (12.31) vanishes on $x\otimes(1-x)$, and therefore factors through $\mathrm{K}_2(k)$.

12.5 Evaluating quotients of δ_3

We keep the notation k, $X=\mathbb{P}^1_k-\{0,1,\infty\}$, and $\pi=\pi_1(\mathbb{P}^1_{\bar{k}}-\{0,1,\infty\},\overrightarrow{01})$ from 12.4. In particular, we have a chosen isomorphism $\pi=\langle x,y\rangle^{\hat{}}$ as above. To evaluate δ_3 on points in $\operatorname{Ker}\delta_2$ requires Galois cohomology computations with coefficients in $[\pi]_3/[\pi]_4\cong\hat{\mathbb{Z}}(3)\oplus\hat{\mathbb{Z}}(3)$. As computing in $\mathrm{H}^2(G_k,\hat{\mathbb{Z}}(3))$ seems difficult, we will evaluate a quotient of δ_3 which can be computed in $\mathrm{H}^2(G_k,\mathbb{Z}/2(3))=\mathrm{H}^2(G_k,\mathbb{Z}/2)$. This quotient is denoted $\delta_3^{\mathrm{mod}\,2}$ and can be described as "the reduction of δ_3 mod 2" as well as "the 3-nilpotent piece of δ_3^2," where δ_3^2 is the obstruction coming from the lower exponent 2 central series as in 12.2.3.

12.5.1 Definition of $\delta_3^{\mathrm{mod}\,2}$

Composing the obstruction

$$\delta_3:\mathrm{H}^1(G_k,\pi/[\pi]_3)\to\mathrm{H}^2(G_k,[\pi]_3/[\pi]_4)$$

with the map on H^2 induced from the quotient

$$\begin{array}{c}[\pi]_3/[\pi]_4\cong\hat{\mathbb{Z}}(3)[[x,y],x]\oplus\hat{\mathbb{Z}}(3)[[x,y],y]\\ \downarrow\\ [\pi]_3/[\pi]_4([\pi]_3)^2\cong\mathbb{Z}/2\mathbb{Z}[[x,y],x]\oplus\mathbb{Z}/2\mathbb{Z}[[x,y],y]\end{array}$$

gives a map $\mathrm{H}^1(G_k,\pi/[\pi]_3)\to\mathrm{H}^2(G_k,[\pi]_3/[\pi]_4([\pi]_3)^2)$ which factors through

$$\mathrm{H}^1(G_k,\pi/[\pi]_3)\to\mathrm{H}^1(G_k,\pi/[\pi]_3^2)$$

(as follows from Proposition 17) where $[\pi]_n^2$ denotes the n^{th} subgroup of the lower exponent 2 central series (cf. 12.2.3). The resulting map

$$\delta_3^{\mathrm{mod}\,2} : \mathrm{H}^1(G_k, \pi/[\pi]_3^2) \to \mathrm{H}^1(G_k, [\pi]_3/[\pi]_4([\pi]_3)^2)$$

is defined as $\delta_3^{\mathrm{mod}\,2}$. The basis $\{[[x,y],x],[[x,y],y]\}$ decomposes $\delta_3^{\mathrm{mod}\,2}$ into two obstructions

$$\delta^2_{3,[[x,y],x]}, \delta^2_{3,[[x,y],y]} : H^1(G_k, \pi/[\pi]_3^2) \to H^2(G_k, \mathbb{Z}/2)$$

which are compatible with the previously defined $\delta_{3,[[x,y],x]}$, $\delta_{3,[[x,y],y]}$ in the obvious manner. In words, $\delta_3^{\mathrm{mod}\,2}$ is δ_3 reduced mod 2.

The obstruction $\delta_3^{\mathrm{mod}\,2}$ can also be constructed from a central extension extension of groups with an action of G_k. To see this, we recall certain well-known results on the lower (exponent p) central series of free groups: for a free group F, the successive quotient $[F]_n/[F]_{n+1}$ of the lower central series is isomorphic to the homogeneous degree n component of the free Lie algebra on the same generators. The Lie basis theorem gives bases for $[F]_n/[F]_{n+1}$ explicitly via bases for the free Lie algebra [MKS04, Thm 5.8]. For the free group on 2 generators x and y,

$$\{x,y\},\{[x,y]\},\{[[x,y],x],[[x,y],y]\},\{[[[x,y],x],x],[[[x,y],y],y],[[[x,y],y],x]\}$$

are bases for $n = 1,2,3,4$. Results of [MKS04] and [Laz54] can be used to show that if β_i is a basis for $[F]_i/[F]_{i+1}$ for $i = 1,\ldots,n$ and $\beta_i^{p^{n-i}}$ denotes the set whose elements are the elements of β_i raised to the p^{n-i}, then

$$\beta_1^{p^{n-1}} \cup \beta_2^{p^{n-2}} \cup \beta_3^{p^{n-3}} \cup \ldots \cup \beta_n$$

is a basis for $[F]_n^p/[F]_{n+1}^p$, where $[F]_n^p$ denotes the n^{th} subgroup of the lower exponent p central series. Thus, as a G_k-module we have

$$[\pi]_3^p/[\pi]_4^p = \mathbb{Z}/p\mathbb{Z}(3)\cdot[[x,y],x] \oplus \mathbb{Z}/p\mathbb{Z}(3)\cdot[[x,y],y]$$

$$\oplus \mathbb{Z}/p\mathbb{Z}(2)\cdot[x,y]^2 \oplus \mathbb{Z}/p\mathbb{Z}(1)\cdot x^4 \oplus \mathbb{Z}/p\mathbb{Z}(1)\cdot y^4.$$

It follows that

$$1 \to [\pi]_3/[\pi]_4([\pi]_3)^p \to \pi/[\pi]_4^p([\pi]_2^p)^p \to \pi/[\pi]_3^p \to 1 \tag{12.32}$$

is an exact sequence, and $\delta_3^{\mathrm{mod}\,2}$ is also the boundary map in G_k cohomology of (12.32) for $p = 2$.

Since we view Ellenberg's obstructions as constraints for points on the Jacobian, we will define a *lift* of a point of $\mathrm{Jac}(X)(k)$ to $\mathrm{H}^1(G_k, \pi/[\pi]_3^2)$ and then define

$$\delta_3^{\mathrm{mod}\,2} \ : \ \mathrm{Ker}\left(\delta_2^2 : \mathrm{Jac}(\mathbb{P}^1_k - \{0,1,\infty\})(k) \to \mathrm{H}^2(G_k, [\pi]_2^2/[\pi]_3^2)\right) \to \{0,1\}$$

which assigns to (b,a) in $k^* \times k^*$ the element 0 if there exists a lift of (b,a) such that $\delta_3^{\mathrm{mod}\,2} = 0$, and assigns to (b,a) the element 1 if there does not exist such a lift.

If $\delta_3^{\mathrm{mod}\,2}(b,a) \neq 0$, it follows that (b,a) is not the image of a k point or tangential point under the Abel-Jacobi map.

For (b,a) in $k^* \times k^* = \mathrm{Jac}(\mathbb{P}^1_k - \{0,1,\infty\})(k)$, let (b,a) also denote the associated element of $\mathrm{H}^1(G_k, \pi^{ab})$. For a characteristic closed subgroup $N < \pi$, a *lift* of (b,a) to $\mathrm{H}^1(G_k, \pi/N)$ is an element whose image under

$$\mathrm{H}^1(G_k, \pi/N) \to \mathrm{H}^1(G_k, (\pi/N)^{\mathrm{ab}})$$

equals the image of (b,a) under

$$\mathrm{Jac}(X)(k) \to \mathrm{H}^1(G_k, \pi^{\mathrm{ab}}) \to \mathrm{H}^1(G_k, (\pi/N)^{\mathrm{ab}}).$$

For example, the lifts of (b,a) to $\mathrm{H}^1(G_k, \pi/[\pi]_3^2)$ can be described as follows. The fixed embeddings $\mathbb{C} \supset \overline{\mathbb{Q}} \subseteq \bar{k}$ and resulting identification $\pi = \langle x,y \rangle^\wedge$ give canonical identifications

$$(\pi/[\pi]_3^2)^{\mathrm{ab}} = \mathbb{Z}/4(1) \cdot x \times \mathbb{Z}/4(1) \cdot y$$
$$\mathrm{Ker}(\pi/[\pi]_3^2 \to (\pi/[\pi]_3^2)^{\mathrm{ab}}) = \mathbb{Z}/2(2) \cdot [x,y].$$

Choose fourth roots of b and a. These choices give cocycles via the Kummer map

$$b,a : G_k \to \mathbb{Z}/4(1),$$

and $g \mapsto y^{a(g)}x^{b(g)}$ represents (b,a) in $\mathrm{H}^1(G_k, (\pi/[\pi]_3^2)^{\mathrm{ab}})$. The obstruction to lifting (b,a) to $\mathrm{H}^1(G_k, \pi/[\pi]_3^2)$ is $\delta_2^2(b,a) = b \cup a \in \mathrm{H}^1(G_k, \mathbb{Z}/2(2))$.

For (b,a) such that $\delta_2^2(b,a) = 0$, the lifts of (b,a) are in bijection with the set of cochains $c \in C^1(G_k, \mathbb{Z}/2)$ such that $dc = -b \cup a$ (note the minus sign) up to coboundary by

$$c \leftrightarrow (b,a)_c,$$

where

$$(b,a)_c(g) = y^{a(g)}x^{b(g)}[x,y]^{c(g)}.$$

The set of these lifts is a $\mathrm{H}^1(G_k, \mathbb{Z}/2(2))$ torsor. We could have equivalently considered the set of cochains c such that $dc = -b \cup a$, as the G_k action on $\mathbb{Z}/2(2)$ is trivial c.f. Corollary 8.

Example 29. (1) Let $(b,a) \in \mathrm{Jac}(X)(k)$ be the image of a rational point or a rational tangential point of $X = \mathbb{P}^1_k - \{0,1,\infty\}$. For $x,y \in k^*$ then (bx^4, ay^4) is unobstructed by $\delta_2^{\mathrm{mod}\,2}$ and $\delta_3^{\mathrm{mod}\,2}$ since (b,a) is unobstructed and defines the same class in $\mathrm{H}^1(G_k, \pi^{\mathrm{ab}} \otimes \mathbb{Z}/4\mathbb{Z})$.

(2) Similarly, the mod m obstructions $\delta_n^{\mathrm{mod}\,m}$ coming from the lower m-central series of π are m-adically continuous in the sense that the obstruction map $\delta_{n+1}^{\mathrm{mod}\,m}$ is constant on cosets by $(k^*)^{m^n}$.

(3) $(b,(1-b)^4)$ determines the same element of $\mathrm{H}^1(G_K, \pi/([\pi]_2\pi^4))$ as $(b,1)$ which is the image of a k tangential point at 0 (Lemma 4). Therefore

$$\delta_3^{\mathrm{mod}\,2}(b,(1-b)^4) = 0.$$

This is an example of a point of the Jacobian unobstructed both by δ_2 (Proposition 24) and $\delta_3^{\mathrm{mod}\,2}$.

We can also compute $\delta_3^{\mathrm{mod}\,2}(b,(1-b)^4)$ directly using Proposition 13. We include the calculation. Let $[\pi]_4^m$ denote the subgroup of the lower exponent m central series c.f. 12.2.3.

Proposition 30. *The conjugacy class of the section of*

$$1 \to \pi^{ab}/(\pi)^{m^3} \to \pi_1(\mathbb{P}^1_k - \{0,1,\infty\}, \overrightarrow{01})/([\pi]_2[\pi]_4^m) \to G_k \to 1 \tag{12.33}$$

determined by $(b,(1-b)^{m^2})$ *lifts to a section of*

$$1 \to \pi/[\pi]_4^m \to \pi_1(\mathbb{P}^1_k - \{0,1,\infty\}, \overrightarrow{01})/[\pi]_4^m \to G_k \to 1.$$

Proof. Let $(b,a) = (b,(1-b)^{m^2})$. Choose compatible systems of n^{th} roots of b and $1-b$, giving cocycles $b, 1-b : G_k \to \hat{\mathbb{Z}}(1)$, and let $a : G_k \to \hat{\mathbb{Z}}(1)$ be $m^2(1-b)$. Conjugacy classes of sections of (12.33) are in bijection with $\mathrm{H}^1(G_k, \pi^{ab}/(\pi)^{m^3})$ using $\overrightarrow{01}$ as the marked splitting. We claim that

$$g \mapsto y^{a(g)}x^{b(g)} \tag{12.34}$$

defines a cocycle $G_k \to \pi/[\pi]_4^m$, showing the proposition. Note that the reduction mod m^2 of a is 0, showing that $b \cup a = 0 \bmod m^2$, whence (12.34) is a cocycle valued in $\pi/[\pi]_3^m$. By Proposition 13 with $a = 0 \bmod m$ and $c = 0$, we have that $\delta^m_{3,[[x,y],x]} = 0$. An easy algebraic manipulation shows that $\binom{\chi(g)a(h)+1}{2}$ is 0 mod m^2 for m odd, and 0 mod m for any m, so the expression for $\delta_{3,[[x,y],y]}$ of Proposition 13 with $a = c = 0 \bmod m$ shows that $\delta^m_{3,[[x,y],y]} = 0$. □

12.5.2 Evaluating the 2-nilpotent quotient of $\mathfrak{f}$

The cocycle $\mathfrak{f} : G_k \to [\pi]_2$ in the description given in (12.12) of the Galois action on $\pi_1(\mathbb{P}^1_{\bar{k}} - \{0,1,\infty\}, \overrightarrow{01})$ records the monodromy of the standard path from $\overrightarrow{01}$ to $\overrightarrow{10}$. To evaluate $\delta^2_{[[x,y],y]}$, we will need to evaluate the 2-nilpotent quotient $f : G_k \to \hat{\mathbb{Z}}(2)[x,y]$ of $\mathfrak{f}$ that was introduced in (12.19), or more precisely its mod 2 reduction. Work of Anderson [And89], Coleman [Col89], Deligne, Ihara [Iha91, 6.3 Thm p.115], Kaneko, and Yukinari [IKY87] gives the equation

$$f(\sigma) = \frac{1}{24}(\chi(\sigma)^2 - 1) \tag{12.35}$$

where we recall that $\chi : G_k \to \hat{\mathbb{Z}}^*$ denotes the cyclotomic character. For the convenience of the reader, we introduce enough of the notation of [Iha91] to check (12.35) from the statement given in loc. cit. 6.3 Thm p.115.

Let $\hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle$ denote the non-commutative power series algebra in two variables over $\hat{\mathbb{Z}}$. The Magnus embedding of the free group on two generators in $\hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle$ gives rise to an injective map

$$\mathcal{M} \ : \ \pi \cong \langle x, y \rangle^{\wedge} \hookrightarrow \hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle$$

defined by

$$\mathcal{M}(x) = 1 + \xi$$
$$\mathcal{M}(y) = 1 + \eta$$

By [MKS04] Cor 5.7, $\mathcal{M}$ takes $[\pi]_n$ to elements of the form $1 + \sum_{m \geq n} u_m$, where u_m is homogeneous of degree m. By [MKS04, §5.5] Lemma 5.4, for any $j \in \hat{\mathbb{Z}}$,

$$\mathcal{M}([x, y]^j) = 1 + j(\xi\eta - \eta\xi) + \sum_{m>2} u_m$$

where u_m is some homogeneous element of degree m (depending on j). More generally, to lowest order in $\hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle$, $\mathcal{M}$ takes the commutator of the group π to the Lie bracket of the associative algebra $\hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle$, in the manner made precise by loc. cit. §5.5 Lemma 5.4 (7). Thus

$$\mathfrak{f}(\sigma) = 1 + f(\sigma)(\xi\eta - \eta\xi) + \mathcal{O}(3) \tag{12.36}$$

where $\mathcal{O}(3)$ is a sum of monomials of degree ≥ 3.

As a $\hat{\mathbb{Z}}$ module, $\hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle$ is the direct sum

$$\hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle \cong \hat{\mathbb{Z}} \oplus \hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle\xi \oplus \hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle\eta.$$

Define $\psi : G_k \to \hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle$ to be the projection of $(\mathfrak{f})^{-1}$ onto the direct summand $\hat{\mathbb{Z}} \oplus \hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle\xi$ i.e.

$$(\mathfrak{f}(\sigma))^{-1} = 1 + a_1\xi + a_2\eta$$
$$\psi(\sigma) = 1 + a_1\xi$$

By (12.36), we have

$$(\mathfrak{f}(\sigma))^{-1} = 1 - f(\sigma)(\xi\eta - \eta\xi) + \mathcal{O}(3),$$

so $f(\sigma)$ is the coefficient of $\eta\xi$ in $\psi(\sigma)$. As the only degree 2 terms that $\psi(\sigma)$ can contain are $\hat{\mathbb{Z}}$ linear combinations of $\eta\xi$ and ξ^2, the cocycle f is determined by the degree 2 terms of the projection of $\psi(\sigma)$ to the commutative power series ring. More explicitly, let $\psi^{ab} : G_k \to \hat{\mathbb{Z}}[[\xi, \eta]]$ denote the composition of ψ with the quotient

$$\hat{\mathbb{Z}}\langle\langle \xi, \eta \rangle\rangle \to \hat{\mathbb{Z}}[[\xi, \eta]]$$

where $\hat{\mathbb{Z}}[[\xi, \eta]]$ denotes the commutative power series ring. Then

$$\psi^{ab}(\sigma) = 1 + f(\sigma)\eta\xi + r$$

where r is a sum a monomial of the form $b\xi^2$ with $b \in \hat{\mathbb{Z}}$ and monomials of degree greater than one.

The formula in [Iha91, 6.3 Thm p.115] expresses $\psi^{ab}(\sigma)$ in terms of the Bernoulli numbers and the variables $X = \log(1+\xi)$, and $Y = \log(1+\eta)$. This formula gives

$$\psi^{ab}(\sigma) = 1 - \frac{1}{2} b_2 (1-\chi(\sigma)^2)\eta\xi + \mathcal{O}(3)$$

where $\mathcal{O}(3)$ is a sum of monomial terms in the variables η,ξ of degree ≥ 3, and $b_2 = \frac{1}{12}$. This implies (12.35).

We denote the mod 2 reduction of f by

$$\overline{f} \,:\, G_k \to \hat{\mathbb{Z}}(2) \to \mathbb{Z}/2Z(2) = \mathbb{Z}/2\mathbb{Z}.$$

Lemma 31. *The class represented by $\overline{f}$ in $\mathrm{H}^1(G_k, \mathbb{Z}/2\mathbb{Z})$ is the class of 2 under the Kummer map.*

Proof. We may assume that $k = \mathbb{Q}$ by functoriality. The value of $\frac{1}{24}(1-\chi(\sigma)^2)$ mod 2 is determined by $1-\chi(\sigma)^2$ mod 48, which in turn is determined by $\chi(\sigma)$ mod 24. A direct check shows that $\overline{f}(\sigma) = 1$ when $\chi(\sigma)$ is ± 3 mod 8, and $\overline{f}(\sigma) = 0$ otherwise. Thus $\overline{f}$ corresponds to the quadratic extension $k \subset k(\zeta_8 + \zeta_8^{-1}) = k(\sqrt{2})$ inside $k \subset k(\zeta_8)$.

12.5.3 Local 3-nilpotent obstructions mod 2 at $\mathbb{R}$

We compute $\delta_3^{\mathrm{mod}\,2}$ for $k = \mathbb{R}$. For a point (b,a) of $\mathbb{R}^* \times \mathbb{R}^* \cong \mathrm{Jac}(\mathbb{P}^1_{\mathbb{R}} - \{0,1,\infty\})(\mathbb{R})$, we have the associated element of $\mathrm{H}^1(G_{\mathbb{R}}, \pi^{ab})$. Recall the notation $(b,a)_c$ and characterization of the lifts of this element to $\mathrm{H}^1(G_{\mathbb{R}}, \pi/[\pi]_3^2)$ of 12.5.1. Recall as well that $\{-1\}$ in $C^1(G_k, \mathbb{Z}/2)$ denotes the image of -1 under the Kummer map, and note that given c in $C^1(G_{\mathbb{R}}, \mathbb{Z}/2(2))$ such that $Dc = -b \cup a$, we have that $c + \{-1\}$ is another cochain such that $D(c+\{-1\}) = -b \cup a$. Thus $(b,a)_c$ and $(b,a)_{c+\{-1\}}$ are two lifts of (b,a) to $\mathrm{H}^1(G_{\mathbb{R}}, \pi/[\pi]_3^2)$, and they are the only two as $\mathrm{H}^1(G_{\mathbb{R}}, \mathbb{Z}/2(2)) = \mathbb{Z}/2$.

Proposition 32. *For any $(b,a)_c$ in $\mathrm{H}^1(G_{\mathbb{R}}, \pi/[\pi]_3^2)$, either*

$$\delta_3^{\mathrm{mod}\,2}(b,a)_c = 0 \quad \text{or} \quad \delta_3^{\mathrm{mod}\,2}(b,a)_{c+\{-1\}} = 0.$$

Proof. Since $\overline{f} = 2 \in \mathrm{H}^1(G_{\mathbb{R}}, \mathbb{Z}/2\mathbb{Z})$ vanishes (Lemma 31), it suffices by Theorem 19 to show that the triple Massey products

$$\delta^{\mathrm{mod}\,2}_{3,[[x,y],x]}(b,a) = \langle \{-b\}, b, a\rangle \in \mathrm{H}^2(G_{\mathbb{R}}, \mathbb{Z}/2\mathbb{Z})$$

$$\delta^{\mathrm{mod}\,2}_{3,[[x,y],y]}(b,a) = \langle \{-a\}, a, b\rangle - \overline{f} \cup b = \langle \{-a\}, a, b\rangle \in \mathrm{H}^2(G_{\mathbb{R}}, \mathbb{Z}/2\mathbb{Z})$$

admit the value 0 for a compatible choice of the defining systems as in Remark 20 (ii). Changing c by a 1-cocycle $\varepsilon \in C^1(G_{\mathbb{R}}, \mathbb{Z}/2\mathbb{Z})$ has the effect by Proposition 17 that

$$\delta_3^{\mathrm{mod}\,2}(b,a)_c - \delta_3^{\mathrm{mod}\,2}(b,a)_{c+\varepsilon} = \{-b\} \cup \varepsilon \cdot [[x,y],x] + \{-a\} \cup \varepsilon \cdot [[x,y],y].$$

Since $a \cup b = 0$ we conclude that at most one of a, b is negative.

Case $a, b > 0$: we may choose trivial defining systems (i.e. the defining system for $\langle \{-b\}, b, a\rangle$ is $\{\binom{b}{2}, 0\} = \{0,0\}$ and the defining system for $\langle \{-a\}, a, b\rangle$ is $\{\binom{a}{2}, ab+0\} = \{0,0\}$) so the obstruction vanishes.

Case $a > 0$ *and* $b < 0$: regardless of the defining system, the Massey product $\langle \{-b\}, b, a\rangle$ always vanishes. The other Massey product can be adjusted if necessary by $\varepsilon = -1$ since $\{-1\} \cup \{-1\}$ generates $\mathrm{H}^2(G_{\mathbb{R}}, \mathbb{Z}/2\mathbb{Z})$.

Case $a < 0$ *and* $b > 0$: regardless of the defining system, the Massey product $\langle \{-a\}, a, b\rangle$ always vanishes. The other Massey product can be adjusted if necessary by $\varepsilon = -1$ since $\{-1\} \cup \{-1\}$ generates $\mathrm{H}^2(G_{\mathbb{R}}, \mathbb{Z}/2\mathbb{Z})$. □

12.5.4 Local 3-nilpotent obstructions mod 2 above odd primes

Let k be a number field embedded into $\mathbb{C}$. Let $p \in \mathbb{Z}$ be an odd prime, k_v the completion of k at a prime v above p, and choose an embedding $\overline{\mathbb{Q}} \subset \overline{k_v}$, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

We compute $\delta_3^{(\mathrm{mod}\,2,v)}$ for all k_v-points of the Jacobian of $\mathbb{P}^1_{k_v} - \{0,1,\infty\}$ in the kernel of $\delta_2^{(\mathrm{mod}\,2,v)}$. Note that 12.4.1 and

$$\delta_2^{\mathrm{mod}\,2,v}(b,a) = a \cup b \in \mathrm{H}^2(G_{k_v}, \mathbb{Z}/2\mathbb{Z}(2))$$

characterize this kernel, and recall the notation $(b,a)_c$ for lifts of $(b,a) \in \mathrm{Ker}\,\delta_2^{\mathrm{mod}\,2,v}$ to $\mathrm{H}^1(G_{k_v}, \pi/[\pi]^2_3)$ given in 12.5.1.

Lemma 33. *Let (b,a) in $\mathrm{Jac}(\mathbb{P}^1_{k_v} - \{0,1,\infty\})(k_v)$ be in the kernel of $\delta_2^{\mathrm{mod}\,2,v}$ and let $(b,a)_c$ be a lift of (b,a) to $H^1(G_{k_v}, \pi/[\pi]^2_3)$.*

1. *If $\{-b\} = 0$ in $\mathrm{H}^1(G_{k_v}, \mathbb{Z}/2)$, then $\delta^{(2,v)}_{3,[[x,y],x]}(b,a)_c = \binom{b}{2} \cup a$ is independent of c.*
2. *If $\{-a\} = 0$ in $\mathrm{H}^1(G_{k_v}, \mathbb{Z}/2)$, then $\delta^{(2,v)}_{3,[[x,y],y]}(b,a)_c = \binom{a}{2} \cup b + \overline{f} \cup a$ is independent of c.*
3. *If $\{b\} = \{a\}$ in $\mathrm{H}^1(G_{k_v}, \mathbb{Z}/2)$, then*

$$\delta^{(2,v)}_{3,[[x,y],x]}(b,a)_c + \delta^{(2,v)}_{3,[[x,y],y]}(b,a)_c = (\binom{a}{2} + \binom{b}{2} + \overline{f}) \cup a$$

is independent of c.

Otherwise

$$\delta_3^{(\mathrm{mod}\,2,v)}(b,a)_c = 0.$$

Proof. Changing the lift is equivalent to adding a 1-cocycle $\varepsilon \in C^1(G_{k_v}, \mathbb{Z}/2\mathbb{Z})$ to c with the effect by Proposition 17 that

$$\delta_3^{\mathrm{mod}\,2}(a,b)_c - \delta_3^{\mathrm{mod}\,2}(a,b)_{c+\varepsilon} = \{-b\} \cup \varepsilon \cdot [[x,y],x] + \{-a\} \cup \varepsilon \cdot [[x,y],y]. \quad (12.37)$$

We abbreviate the differences componentwise by introducing the notation

$$\Delta^2_{3,[[x,y],x]}(b,a,z) = \{-b\} \cup z,$$

$$\Delta^2_{3,[[x,y],y]}(b,a,z) = \{-a\} \cup z.$$

Using Proposition 17, case (1) and (2) are now immediate. In case (3), note that Proposition 17 implies that

$$\delta^{(2,v)}_{3,[[x,y],x]}(b,a)_c + \delta^{(2,v)}_{3,[[x,y],y]}(b,a)_c = (a + \frac{\chi - 1}{2}) \cup (ab) + \binom{b}{2} \cup a + \binom{a}{2} \cup b + \overline{f} \cup a$$

Since $a = b$, we have $(ab) = a^2 = a$, so

$$(a + \frac{\chi - 1}{2}) \cup (ab) = (a + \frac{\chi - 1}{2}) \cup a = 0.$$

This equation and $a = b$ show case (3).

If the map

$$\Delta \ : \ \mathrm{H}^1(G_{k_v}, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{H}^2(G_{k_v}, \mathbb{Z}/2\mathbb{Z}) \oplus \mathrm{H}^2(G_{k_v}, \mathbb{Z}/2\mathbb{Z}) \quad (12.38)$$

$$z \mapsto \left(\Delta^2_{3,[[x,y],x]}(b,a,z), \Delta^2_{3,[[x,y],y]}(b,a,z)\right) = \left(\{-b\} \cup z, \{-a\} \cup z\right)$$

is surjective, namely by the nondegeneracy of the cup product pairing, if $\{-a\}, \{-b\}$ forms a basis of $\mathrm{H}^1(G_{k_v}, \mathbb{Z}/2\mathbb{Z})$, then for a suitable choice of correction term z, the corresponding c will lead to a vanishing

$$\delta_3^{\mathrm{mod}\,2}((b,a)_c) = 0.$$

Since $\mathrm{H}^1(G_{k_v}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, the elements $\{-a\}, \{-b\}$ form a basis unless at least one of cases (1), (2), or (3) holds. □

To compute when there is a local obstruction as in case (1) or (2), we need to understand the cochain

$$\binom{a}{2} : G_{k_v} \to \mathbb{Z}/2$$

when $\{-a\}$ is 0 in $C^1(G_{k_v}, \mathbb{Z}/2)$ cf. Examples 10 and 11.

Lemma 34. *Let K be a field of characteristic $\neq 2$, and let ζ_4 be a primitive fourth root of unity in a fixed algebraic closure of K. Let $-x \in (K^*)^2$ be a square, and choose a fourth root $\sqrt[4]{x}$ of x giving a Kummer cocycle $x : G_K \to \mathbb{Z}/4\mathbb{Z}(1)$ and the*

cochain $\binom{x}{2} : G_K \to \mathbb{Z}/2\mathbb{Z}$ *obtained by the identification* $\mathbb{Z}/4\mathbb{Z}(1) = \mathbb{Z}/4\mathbb{Z}(\chi)$ *using* ζ_4*. Then there is an equality of cocycles*

$$\binom{x}{2} = \{2\sqrt{-x}\} : G_K \to \mathbb{Z}/2\mathbb{Z}$$

where $\sqrt{-x} = \zeta_4(\sqrt[4]{x})^2$.

Proof. Note that squaring $(1+\zeta_4)\sqrt[4]{x}$ gives $2\sqrt{-x}$, so letting $\eta = 2\sqrt{-x} \in K$, we see that $K(\sqrt[4]{x}, \zeta_4) = K(\sqrt{\eta}, \zeta_4)$. Both cochains $\binom{x}{2}, \{2\sqrt{-x}\} : G_K \to \mathbb{Z}/2\mathbb{Z}$ factor through $\mathrm{Gal}(K(\sqrt[4]{x}, \zeta_4)/K)$, and there are four possibilities for the action of $g \in G_K$ on $\sqrt{\eta}$ and ζ_4. It is enough to check that $\binom{x}{2}(g)$ and $\{\eta\}(g)$ agree in each case:

$g(\sqrt{\eta})$	$g(\zeta_4)$	$x(g)$	$\binom{x(g)}{2}$
$\sqrt{\eta}$	ζ_4	$(\zeta_4)^0$	0
$\sqrt{\eta}$	$(\zeta_4)^3$	$(\zeta_4)^1$	0
$-\sqrt{\eta}$	ζ_4	$(\zeta_4)^2$	1
$-\sqrt{\eta}$	$(\zeta_4)^3$	$(\zeta_4)^3$	1

This shows the claim $\binom{x}{2} = \{\eta\} = \{2\sqrt{-x}\}$. □

To compute when there is a local obstruction as in case (3), we need to understand the cochain

$$\binom{a}{2} + \binom{b}{2} : G_{k_v} \to \mathbb{Z}/2$$

when $a = b$ in $C^1(G_{k_v}, \mathbb{Z}/2)$.

Lemma 35. *Let K be a field of characteristic $\neq 2$, and let ζ_4 be a primitive fourth root of unity in a fixed algebraic closure of K. Let a, b be non-zero elements of K such that a/b is a square $a/b \in (K^*)^2$. Choose fourth roots of both, and let $a, b : G_K \to \mathbb{Z}/4(1)$ denote the corresponding cocyles. Then*

$$\binom{a}{2} + \binom{b}{2} : G_K \to \mathbb{Z}/2$$

equals the cocycle

$$\{\sqrt{b}/\sqrt{a}\} : G_K \to \mathbb{Z}/2,$$

where $\sqrt{b}$, $\sqrt{a}$ are defined as the squares of the chosen fourth roots of b, a respectively.

Proof. For any two elements d_1, d_2 in $\mathbb{Z}/4$, direct calculation shows that in $\mathbb{Z}/2$

$$\binom{d_1+d_2}{2} - \binom{d_1}{2} - \binom{d_2}{2} = d_1 d_2.$$

Therefore for all g in G_K,

$$\binom{a(g)}{2}+\binom{b(g)}{2}=\binom{a(g)+b(g)}{2}-a(g)b(g)$$

Since mod 2, $a(g)=b(g)$, we have that $a(g)b(g)=a(g) \bmod 2$. Therefore

$$\binom{a(g)}{2}+\binom{b(g)}{2}=\binom{a(g)+b(g)}{2}-a(g)$$

Since b/a is a square in K, ab is also a square in K. Let $\sqrt{a},\sqrt{b}$ denote the squares of our chosen fourth roots of a and b respectively.

By Lemma 11, and because ab is a square in K,

$$g \mapsto \binom{a(g)+b(g)}{2}$$

equals $\{\sqrt{a}\sqrt{b}\}$. Therefore

$$\binom{a}{2}+\binom{b}{2}=\{\sqrt{a}\sqrt{b}\}-a.$$

Since $\{\sqrt{a}\sqrt{b}\}-a=\{\sqrt{b}/\sqrt{a}\}$, the lemma is shown. □

The previous results combine to give necessary and sufficient conditions for $\delta_3^{(\mathrm{mod}\,2,v)}$ to obstruct a k_v-point of the Jacobian in the kernel of $\delta_2^{(\mathrm{mod}\,2,v)}$ from lying on the curve (i.e. from being the image of a k_v-point or tangential point of X). For any given point (b,a) of $\mathrm{Jac}X$, these conditions are easy to verify using 12.4.1.

Theorem 36. *Let k_v be the completion of a number field k at a place above an odd prime. For $(b,a)\in \mathrm{Jac}(\mathbb{P}^1_{k_v}-\{0,1,\infty\})(k_v)$ such that $\delta_2^{(\mathrm{mod}\,2,v)}(b,a)=0$, we have $\delta_3^{\mathrm{mod}\,2}(b,a)\neq 0$ if and only if one of the following holds.*

(i) $-b\in(k_v^*)^2$ *and* $\{2\sqrt{-b}\}\cup a\neq 0$.
(ii) $-a\in(k_v^*)^2$ *and* $\{2\sqrt{-a}\}\cup b+\{2\}\cup a\neq 0$
(iii) $ab\in(k_v^*)^2$ *and* $\{2\sqrt{b}\sqrt{a}\}\cup a\neq 0$

Remark 37. In case (i), the notation $\sqrt{-b}$ denotes either square root of $-b$, both of which are in k_v. The expression $\{2\sqrt{-b}\}\cup a$ denotes the corresponding element of $\mathrm{H}^2(G_{k_v},\mathbb{Z}/2\mathbb{Z})$, which is independent of the choice of square root because

$$\{-1\}\cup a=\{-b\}\cup a-b\cup a=0.$$

Similar remarks hold in cases (ii) and (iii).

Note that obstructions such as $\{2\sqrt{-b}\}\cup a$ look as though they are naturally elements of $\mathrm{H}^2(G_{\mathbb{Q}_p},\mathbb{Z}/2\mathbb{Z}(2))$, but $\delta^{(2,p)}_{3,[[x,y],x]}(b,a)_c$ is in $\mathrm{H}^2(G_{\mathbb{Q}_p},\mathbb{Z}/2\mathbb{Z}(3))$. The shift in weight happened in Lemmas 11, 34, and 35.

Proof. Fix $\mathbb{C}\supset\overline{k}\subset\overline{k_v}$. It is sufficient to show that in Lemma 33 case (i) (ii) (iii) respectively, we have

$$\binom{b}{2} \cup a = \{2\sqrt{-b}\} \cup a,$$

$$\binom{a}{2} \cup b + \overline{f} \cup a = \{2\sqrt{-a}\} \cup b + \{2\} \cup a,$$

$$(\binom{a}{2} + \binom{b}{2} + \overline{f}) \cup a = \{2\sqrt{b}\sqrt{a}\} \cup a.$$

For cases (i) and (ii), this follows immediately from Lemmas 34 and 31. In case (iii), Proposition 35 and 31 show that

$$(\binom{a}{2} + \binom{b}{2} + \overline{f}) \cup a = \{2\sqrt{b}/\sqrt{a}\} \cup a.$$

Since $\sqrt{b}/\sqrt{a}$ is in k_v, we have that $a\sqrt{b}/\sqrt{a} = \sqrt{b}\sqrt{a}$ is in k_v. As $a \cup b = 0$ and $a = b$, it follows that $\{2\sqrt{b}/\sqrt{a}\} \cup a$ is also equal to $\{2\sqrt{b}/\sqrt{a}\} \cup a + a \cup a$, which in turn equals $\{2\sqrt{b}\sqrt{a}\} \cup a$. □

Corollary 38. *Let (b,a) be a rational point of* $\mathrm{Jac}(\mathbb{P}^1_{\mathbb{Q}} - \{0,1,\infty\})$ *such that (b,a) is in $(\mathbb{Z} - \{0\}) \times (\mathbb{Z} - \{0\})$ and p divides ab exactly once. Then*

1. $\delta_2^{(\mathrm{mod}\,2,p)}(b,a) = 0 \iff a+b$ *is a square mod p*
2. *When (1) holds,* $\delta_3^{(\mathrm{mod}\,2,p)}(b,a) = 0 \iff a+b$ *is a fourth power mod p*

Remark 39. (1) Note that under the hypotheses of Corollary 38, the condition that $a+b$ is congruent to a $(2^n)^{th}$ power mod p is equivalent to the condition that whichever of a or b not divisible by p is a $(2^n)^{th}$ power mod p.

(2) For the points of the Jacobian satisfying the conditions described in its statement, Corollary 38 computes $\delta_3^{(\mathrm{mod}\,2,p)}$ and $\delta_2^{(\mathrm{mod}\,2,p)}$ in terms of congruence conditions mod p. These congruence conditions allow us to see that $\delta_3^{(\mathrm{mod}\,2,p)}$ and $\delta_2^{(\mathrm{mod}\,2,p)}$ vanish on the points and tangential points of the curve which satisfy the hypotheses of the Corollary. Namely, by (12.15) and Lemmas 4, the image of $\mathbb{P}^1 - \{0,1,\infty\}$ and its tangential points is the set of (b,a) such that $a+b=0$, $a+b=1$, $a=1$, or $b=1$. As 0 and 1 are fourth powers mod every prime, we see the vanishing of Ellenberg's obstructions on the points of the curve.

(3) It is tempting to hope that under certain hypotheses

- $\delta_n^{(\mathrm{mod}\,2,p)}(b,a) = 0 \iff a+b$ is a 2^{n-1} power mod p.

Since 0 and 1 are the only integers which are 2^{n-1} powers for every n, mod every prime, such a result could show that the nilpotent completion of π determines the points and tangential points of $\mathbb{P}^1 - \{0,1,\infty\}$ from those of the Jacobian. This is a mod 2, pro-nilpotent section conjecture for $\mathbb{P}^1 - \{0,1,\infty\}$ cf. 12.4.4.

Proof. To prove (1): note that by hypothesis, exactly one of b and a equals $\mathfrak{p}$ or $u+\mathfrak{p}$ in $\mathrm{H}^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2(1))$, where the notation $\mathfrak{p}$,u is as defined in 12.4.1. By 12.4.1, it follows that the other is 0 in $\mathrm{H}^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2(1))$ if and only if $b \cup a$ vanishes. By

Hensel's Lemma, this is equivalent to the other being a square mod p, which in turn is equivalent to the condition that $a+b$ is a square mod p.

To prove (2): exactly one of b and a is not divisible by p. Call this element r. The only case listed in Theorem 36 that can hold is $\{-r\}=0$ in $\mathrm{H}^1(G_{\mathbb{Q}_p},\mathbb{Z}/2\mathbb{Z}(1))$. By (1), we have that r is a square mod p, whence $\{-r\}=\{-1\}$ in $\mathrm{H}^1(G_{\mathbb{Q}_p},\mathbb{Z}/2\mathbb{Z}(1))$. Note also that if $r=a$, then $\overline{f}\cup a=\{2\}\cup a=0$, as neither 2 nor a is divisible by p. Therefore, $\delta_3^{(\mathrm{mod}\,2,p)}(b,a)\neq 0$ if and only if $p=1$ mod 4, and $\{2\sqrt{-r}\}\cup p\neq 0$.

For $p=1$ mod 4, and r and $-r$ squares mod p,

$$\{2\sqrt{-r}\}\cup p=\{\sqrt{r}\}\cup p$$

in $\mathrm{H}^1(G_{\mathbb{Q}_p},\mathbb{Z}/2\mathbb{Z}(1))$ where either square root of r or $-r$ in $\mathbb{Q}_p$ can be chosen. To see this: note that since -1 is a square, it is clear that changing the square root has no effect. Note that $(1+\xi_4)^2=2\xi_4$, for ξ_4 a primitive fourth root of unity in $\mathbb{Q}_p$, from which it follows that $\{\sqrt{r}\}=\{\sqrt{r}(1+\xi_4)^2\}=\{2\sqrt{-r}\}$. (In the last equality $\sqrt{-r}$ is $\xi_4\sqrt{r}$, but we are free to choose either square root to see the claimed equality.)

Thus, $\delta_3^{(\mathrm{mod}\,2,p)}(b,a)\neq 0$ if and only if $p=1$ mod 4, and $\{\sqrt{r}\}\cup p\neq 0$ in $\mathrm{H}^1(G_{\mathbb{Q}_p},\mathbb{Z}/2\mathbb{Z}(1))$. Note that $\{\sqrt{r}\}\cup p\neq 0$ if and only if $\{\sqrt{r}\}\neq 0$, since r is not divisible by p. The condition $p=1$ mod 4 and $\{\sqrt{r}\}\neq 0$ is equivalent to the condition $p=1$ mod 4 and r is not a fourth power mod p. Since r is a square mod p, the condition that r is not a fourth power implies that $p=1$ mod 4. Thus, $\delta_3^{(\mathrm{mod}\,2,p)}(b,a)\neq 0$ if and only if r is not a fourth power mod p. This last condition is equivalent to $a+b$ is not a fourth power mod p. □

Remark 40. The proof of Corollary 38 only uses the computation of $\overline{f}$ given in 31 to ensure that $f\in\{0,\mathfrak{u}\}\subset\mathrm{H}^1(G_{\mathbb{Q}_p},\mathbb{Z}/2)$.

Definition 41. For an obstruction δ' which is defined on the vanishing locus of an obstruction δ, we say that δ' **is not redundant with** δ if δ' does not vanish identically.

Example 42. We compare the obstruction $\delta_3^{\mathrm{mod}\,2}$ with δ_2 for $k=\mathbb{Q}$.

(1) As $4=(-1)+5$ is a square but not a fourth power mod 5, Corollary 38 implies that $\delta_2^{(\mathrm{mod}\,2,5)}(-1,5)=0$, and

$$\delta_3^{(\mathrm{mod}\,2,5)}(-1,5)\neq 0.$$

In other words, the 3-nilpotent obstruction $\delta_3^{(\mathrm{mod}\,2,p)}$ is not redundant with the 2-nilpotent obstruction $\delta_2^{(\mathrm{mod}\,2,p)}$.

(2) In fact, it is easy to check that $\{-1\}\cup\{5\}=0$ in $\mathrm{H}^2(G_{\mathbb{Q}},\mathbb{Z}/2\mathbb{Z})$ since

$$\{-1\}\cup\{5\}=\{-1\}\cup\{5\}+\{1-5\}\cup\{5\}=\{4\}\cup\{5\}=2\cdot(\{2\}\cup\{5\})=0.$$

Alternatively, $\{-1\}\cup\{5\}=0$ in $\mathrm{H}^2(G_{\mathbb{Q}},\mathbb{Z}/2)$ because the Brauer-Severi variety

$$-u^2+5v^2=w^2$$

has the rational point $[u,v,w] = [1,1,2]$. Thus, $\delta_3^{(\mathrm{mod}\,2,p)}$ is not redundant with the global obstruction $\delta_2^{\mathrm{mod}\,2}$. It also follows that the global 3-nilpotent obstruction $\delta_3^{\mathrm{mod}\,2}$ is not redundant with the global 2-nilpotent obstruction $\delta_2^{\mathrm{mod}\,2}$.

(3) One can ask whether $\delta_3^{(\mathrm{mod}\,2,p)}$ is redundant with the global obstruction δ_2 for $k = \mathbb{Q}$. The tame symbol at p

$$b \otimes a \mapsto (b,a)_p = (-1)^{v_p(b)v_p(a)} \frac{b^{v_p(a)}}{a^{v_p(b)}} \in \mathbb{F}_p^*$$

vanishes on any (b,a) such that $\delta_2(b,a) = 0$. In particular, given $b,a \in \mathbb{Z}$ such that p divides $ab \neq 0$ exactly once, we will have that

$$\frac{b^{v_p(a)}}{a^{v_p(b)}} = 1 \mod p$$

and that $\frac{b^{v_p(a)}}{a^{v_p(b)}}$ equals either b or $1/a$ depending on which of b or a is divisible by p. In particular, $a+b = 1 \mod p$, and thus, Corollary 38 does not show that δ_3 is not redundant with δ_2 for $k = \mathbb{Q}$.

The points (b,a) of $\mathrm{Jac}(\mathbb{P}^1_{\mathbb{Q}} - \{0,1,\infty\})(\mathbb{Q}) = \mathbb{Q}^* \times \mathbb{Q}^*$ considered in Corollary 38 and satisfying $\delta_2^{(\mathrm{mod}\,2,p)}(b,a) = 0$ have the property that at any finite prime p, either b or a determines the 0 element of

$$C^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2) \cong \mathrm{H}^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2).$$

Thus a lift $(b,a)_c$ of (b,a) to a class of $\mathrm{H}^1(G_{\mathbb{Q}_p}, \pi/[\pi]_3^2)$ is such that c is a cocycle, as opposed to a cochain. By Theorem 19, Corollary 38 consists of evaluations of Massey products where certain cup products of cochains are not only coboundaries, but 0 as a cochains. Indeed, a direct proof of Corollary 38 can be given along these lines, although the methods involved are not sufficiently different from those of Theorem 36 to merit inclusion.

Let p vary through the odd primes, and let m vary through the positive integers. The points $((-p)^{2m+1}, p)$ satisfy $\delta_2 = 0$ by Proposition 24, but both $(-p)^{2m+1}$ and p determine non-zero elements of $C^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2)$ via the Kummer map, unlike the examples computed via Corollary 38. Theorem 36 allows us to evaluate $\delta_3^{(\mathrm{mod}\,2,p)}$ on these points.

Example 43. Let p be an odd prime and m a positive integer. Then $\delta_3^{(\mathrm{mod}\,2,p)}$ vanishes on the following rational points of $\mathrm{Jac}(\mathbb{P}^1_{\mathbb{Q}} - \{0,1,\infty\})$

(1) $(-p^{2m+1}, p)$,
(2) (p^{2m}, p).

For $(-p^{2m+1}, p)$ we show that neither case (i)-(iii) of Theorem 36 holds. Note that $\{p^{2m+1}\}$ (resp. $\{-p\}$) is nontrivial in $\mathrm{H}^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2)$, so case (i) (resp. case (ii))

does not hold. When $p \equiv 3 \bmod 4$, the class $\{-p^{2m+1} \cdot p\} = \{-1\}$ is nontrivial in $\mathrm{H}^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2)$ and case (iii) does not hold.

For $p \equiv 1 \bmod 4$, we have a fourth root of unity $\zeta_4 \in \mathbb{Q}_p$ and thus the product $-p^{2m+1} \cdot p$ is a square in $\mathbb{Q}_p$. In this case the first equation of (iii) is satisfied, but the second is not:

$$\{2\sqrt{-p^{2m+2}}\} \cup p = \{2p^{m+1}\zeta_4\} \cup p = \{2\zeta_4\} \cup p = \{(1+\zeta_4)^2\} \cup p = 0$$

because $p \cup p = 0$ by 12.4.1.

For (p^{2m}, p) one shows similarly that $\delta_3^{(\bmod 2, p)}(p^{2m}, p) = 0$. Now cases (ii) and (iii) do not apply for obvious reasons and (i) can at most apply for $p \equiv 1 \bmod 4$. But then

$$\{2\sqrt{-p^{2m}}\} \cup \{p\} = (\{2\zeta_4\} + m\{p\}) \cup \{p\} = \{(1+\zeta_4)^2 \cup p = 0$$

vanishes as well.

Example 44. Let p be a prime congruent to 3 mod 4. Let $x \in \mathbb{Z} - \{0,1\}$ be divisible by p. Then

$$\delta_3^{(\bmod 2, p)}((1-x)(-x), x) = 0.$$

Note that by Proposition 24, the point $((1-x)(-x), x)$ is in the kernel of $\delta_2^{(\bmod 2, p)}$, and even in the kernel of δ_2.

We again show that neither case (i)-(iii) of Theorem 36 holds. The element $1-x$ is a square in $\mathbb{Q}_p$, as $1 - x \equiv 1 \bmod p$, whence

$$\{(1-x)(-x)\} = \{-x\} \in \mathrm{H}^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2).$$

Since $p \equiv 3 \bmod 4$, the class $\{-1\}$ is nonzero in $\mathrm{H}^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2)$. Therefore case (iii) does not hold. Case (ii) holds if and only if $\{-x\} = 0$ and

$$\{2\sqrt{-x}\} \cup \{(1-x)(-x)\} + \{2\} \cup \{x\} \neq 0.$$

Since $(-x, x)$ is the image of a rational tangential base point by Lemma 4, the obstruction $\delta_3^{(\bmod 2, p)}(-x, x) = 0$ vanishes. By Theorem 36 case (ii), this implies that

$$\{2\sqrt{-x}\} \cup \{(-x)\} + \{2\} \cup \{x\} = 0$$

when $\{-x\} = 0$, so (ii) does not hold for $((1-x)(-x), x)$, because

$$\{(1-x)(-x)\} = \{(-x)\}.$$

Case (i) holds if and only if $\{(1-x)(x)\} = \{x\} = 0$ and

$$\{2\sqrt{(1-x)x}\} \cup \{x\} \neq 0$$

which is impossible.

12.5.5 A global mod 2 calculation

The local calculations of 12.5.4 and 12.5.3 allow us to evaluate the global obstruction $\delta_3^{\mathrm{mod}\,2}$ on $(-p^3,p)$ in $\mathrm{Jac}(\mathbb{P}^1_{\mathbb{Q}}-\{0,1,\infty\})(\mathbb{Q})$. This evaluation relies on the Hasse–Brauer–Noether local/global principle for the (2-torsion) of the Brauer group, see [NSW08] Theorem 8.1.17,

$$0\to \mathrm{H}^2(G_{\mathbb{Q}},\mathbb{Z}/2)\to \bigoplus_v \mathrm{H}^2(G_{\mathbb{Q}_p},\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\Sigma_v \mathrm{inv}_v} \frac{1}{2}\mathbb{Z}/\mathbb{Z}\to 0 \tag{12.39}$$

but is more subtle, as the evaluation of $\delta_3^{\mathrm{mod}\,2}$ over $\mathbb{Q}$ depends on the lifts of a point of the Jacobian to $\mathrm{H}^1(G_{\mathbb{Q}},\pi/[\pi]_3^2)$, whereas each evaluation of $\delta_3^{(\mathrm{mod}\,2,p)}$ depends on the lifts to $\mathrm{H}^1(G_{\mathbb{Q}_p},\pi/[\pi]_3^2)$. One may not be able to find a global lift to restricting to some given set of local lifts.

In Proposition 30, it was shown that

$$\delta_3^{\mathrm{mod}\,2}(b,(1-b)^4)=0$$

for k a number field and b in $k-\{0,1\}=\mathbb{P}^1_k-\{0,1,\infty\}(k)$, giving a calculation of the global obstruction $\delta_3^{\mathrm{mod}\,2}$ on a point of the Jacobian not lying on the curve or coming from a tangential base point. However, the point $(b,(1-b)^4)$ determines the same element of $\mathrm{H}^1(G_{\mathbb{Q}},\pi/([\pi]_2\pi^4))$ as the point $(b,1)$ which is the image of a rational tangential point by Lemma 4, so this vanishing is trivial.

We now let p vary through the primes congruent to 1 mod 4, and evaluate $\delta_3^{\mathrm{mod}\,2}$ on the family of points $(-p^3,p)$. Note that $(-p^3,p)$ does not determine the same element of $\mathrm{H}^1(G_{\mathbb{Q}},\pi/([\pi]_2\pi^4))$ as a rational point or tangential point of $\mathbb{P}^1_{\mathbb{Q}}-\{0,1,\infty\}$ by (12.15) and Lemma 4, so this gives a nontrivial calculation of $\delta_3^{\mathrm{mod}\,2}$ over $\mathbb{Q}$.

Proposition 45. *Let p be a prime congruent to 5 mod 8. Consider $(-p^3,p)$ in $\mathrm{Jac}(\mathbb{P}^1_{\mathbb{Q}}-\{0,1,\infty\})(\mathbb{Q})$. Then $\delta_3^{\mathrm{mod}\,2}(-p^3,p)=0$.*

Proof. We evaluate the obstruction as triple Massey products with compatible defining systems by Theorem 19

$$\delta^2_{3,[[x,y],x]}(-p^3,p)=\langle p^3,-p^3,p\rangle \tag{12.40}$$

$$\delta^2_{3,[[x,y],y]}(-p^3,p)=-\langle -p,p,-p^3\rangle-\{2\}\cup p$$

valued in $\mathrm{H}^2(G_{\mathbb{Q}},\mathbb{Z}/2\mathbb{Z})$, using Lemma 31 to evaluate $\overline{f}$.

Let $S=\{2,p,\infty\}$ and let $\mathbb{Q}_S$ denote the maximal extension of $\mathbb{Q}$ unramified outside S. Then all classes $\{-1\}$, $\{\pm p\}$, $\{2\}$, etc. involved in (12.40) are unramified outside S, i.e. they already lie in $\mathrm{H}^1(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}),\mathbb{Z}/2\mathbb{Z})$. The map

$$\mathrm{H}^2(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}),\mathbb{Z}/2\mathbb{Z})\hookrightarrow \mathrm{H}^2(G_{\mathbb{Q}},\mathbb{Z}/2\mathbb{Z}) \tag{12.41}$$

is injective. One way to see this injectivity is: let $\mathcal{O}_{\mathbb{Q},S}$ denote the S integers of $\mathbb{Q}$ and let $U = \operatorname{Spec} \mathcal{O}_{\mathbb{Q},S}$. The étale cohomology groups $\mathrm{H}^*(U, \mathbb{Z}/2\mathbb{Z})$ are isomorphic to the Galois cohomology groups $\mathrm{H}^*(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$ by [Hab78, Appendix 2 Prop 3.3.1], and by the Kummer exact sequence, the sequence

$$\mathrm{H}^1(U, \mathbb{G}_m) \to \mathrm{H}^2(U, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{H}^2(U, \mathbb{G}_m)$$

is exact in the middle. Since $\mathcal{O}_{\mathbb{Q},S}$ is a principal ideal domain, $\mathrm{H}^1(U, \mathbb{G}_m) = 0$, and by [Mil80, III 2.22], the natural map $\mathrm{H}^2(U, \mathbb{G}_m) \to \mathrm{H}^2(G_{\mathbb{Q}}, \mathbb{G}_m)$ is an injection. Thus (12.41) is injective. Its image consists of the classes whose image under (12.39) have vanishing local component except possibly at 2,p and ∞. It follows we can restrict to defining systems of cochains for $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$. Thus the Massey product takes values in $\mathrm{H}^2(\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})$ and the local components for primes not in S vanish a priori.

We will show the vanishing of a global lift at p and ∞, and deduce the vanishing at 2 from reciprocity (12.39).

Since $p \equiv 5 \bmod 8$, we have that 2 is not a quadratic residue mod p, so $\{2\}$ and $\{p\}$ span $\mathrm{H}^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2)$ (as in 12.4.1). Thus the set of lifts $(-p^3, p)_c$ where c varies among the cochains factoring through $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ surjects onto the set of all lifts of $(-p^3, p)$ to $\mathrm{H}^1(G_{\mathbb{Q}_p}, \pi/[\pi]_3^2)$. By Example 43, we can therefore choose such a lift such that $\delta_3^{(2,p)}(-p^3, p)_c = 0$.

Since p is congruent to 1 mod 4, the restriction of $\{-1\}$ to $C^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2\mathbb{Z})$ is 0. By Proposition 32, either $\delta_3^{\mathrm{mod}\,2}(-p^3, p)_c = 0$ or $\delta_3^{\mathrm{mod}\,2}(-p^3, p)_{c+\{-1\}} = 0$, so we can choose a lift factoring through $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ such that $\delta_3^{\mathrm{mod}\,2}$ vanishes at both p and $\mathbb{R}$. □

Remark 46. (1) In the proof of Proposition 45, the vanishing of $\delta_3^{\mathrm{mod}\,2}(-p^3, p)$ was shown for $p \equiv 5 \bmod 8$ by using the local vanishing of $\delta_3^{(\mathrm{mod}\,2,v)}(-p^3, p)$ and showing that the global lifts of $(-p^3, p)$ to $\mathrm{H}^1(G_{\mathbb{Q}}, \pi/[\pi]_3^2)$ with ramification constrained to lie above $S = \{2, p, \infty\}$ surjected onto the product over the local lifts of $(-p^3, p)$ to $\mathrm{H}^1(G_{\mathbb{Q}_v}, \pi/[\pi]_3^2)$ for the places p and ∞.

(2) It would be desirable to relate $\delta_3^{\mathrm{mod}\,2} = 0$ to the simultaneous vanishing of all (or all but one) $\delta_3^{(2,v)}$, where v varies over the places of a given number field k. For this, we would need to compare the set of restrictions to the k_v of lifts of (b,a) to $H^1(G_k, \pi/[\pi]_3^2)$ with the set of independently chosen lifts of (b,a) to $H^1(G_{k_v}, \pi/[\pi]_3^2)$ for all v. In other words, we are interested in the map

$$H^1_{(b,a)}(G_k, \pi/[\pi]_3^2) \to \prod_v H^1_{(b,a)}(G_{k_v}, \pi/[\pi]_3^2) \tag{12.42}$$

where $H^1_{(b,a)}(G_k, \pi/[\pi]_3^2)$ denotes the subset of $H^1(G_k, \pi/[\pi]_3^2)$ of lifts of (b,a) and similarly for each $H^1_{(b,a)}(G_{k_v}, \pi/[\pi]_3^2)$. A nonabelian version of Poitou-Tate duality would give information about (12.42).

We can also evaluate $\delta^2_{3,[[x,y],x]}$ and $\delta^2_{3,[[x,y],y]}$ on a specific lift of $(-p^3,p)$, which is equivalent to the calculation of the Massey products $\langle p^3,-p^3,p\rangle$ and $\langle -p,p,-p^3\rangle$ with the defining systems specified in Remark 20 (ii), and the mod 2 cup product $\{2\}\cup\{p\}$. The cup product $\{2\}\cup\{p\}$ can be calculated with 12.4.3; it vanishes except at 2 and p, and at p, $\{2\}\cup\{p\}$ vanishes if and only if $p\equiv\pm1$ mod 8. An arbitrary defining system for $\langle p^3,-p^3,p\rangle$ or $\langle -p,p,-p^3\rangle$ produces Massey products differing from the originals by cup products, which can also be evaluated with 12.4.3. So evaluating $\delta^2_{3,[[x,y],x]}$ and $\delta^2_{3,[[x,y],y]}$ on a specific lift allows for the computation of $\langle p^3,-p^3,p\rangle$ and $\langle -p,p,-p^3\rangle$ in $\mathrm{H}^2(G_{\mathbb{Q}},\mathbb{Z}/2)$ with any defining system. We remark that a complete computation of the triple Massey product on $\mathrm{H}^1(\mathrm{Gal}(k_S(2)/k),\mathbb{Z}/2)$ for certain maximal 2-extensions with restricted ramification $k_S(2)$ of a number field k is given in [Vog04, II §1].

Remark 47. Note that $\{-p^3\}=\{-p\}$ and $\{p^3\}=\{p\}$ in $\mathrm{H}^1(G_{\mathbb{Q}},\mathbb{Z}/2)$. The reason for distinguishing between, say, $-p^3$ and $-p$ in $\langle p^3,-p^3,p\rangle$ is that the defining systems to evaluate $\delta^2_{3,[[x,y],x]}$ and $\delta^2_{3,[[x,y],y]}$ are different for $-p^3$ and $-p$, as they depend on the image of $-p^3$ in $\mathrm{H}^1(G_{\mathbb{Q}},\mathbb{Z}/4(1))$. However, for the discussion of evaluating triple Massey products of elements of $\mathrm{H}^1(G_{\mathbb{Q}},\mathbb{Z}/2)$ for any defining system, the distinction is of course irrelevant.

Consider the following lift of $(-p^3,p)$: choose compatible n^{th} roots of p, and let $\{p\}$ denote the corresponding element of $C^1(G_{\mathbb{Q}},\hat{\mathbb{Z}}(1))$ via the Kummer map 1. (As above, $\{p\}$ will sometimes be abbreviated by p.) Note that the chosen n^{th} roots of p give rise to a choice of compatible n^{th} roots of $-p^3$ such that the corresponding element of $C^1(G_{\mathbb{Q}},\hat{\mathbb{Z}}(1))$ is $3(p+\frac{\chi-1}{2})$. It is therefore consistent to let $\{-p^3\}$ and $-p^3$ denote $3(p+\frac{\chi-1}{2})$. Let $c_0=3\binom{p}{2}$ in $C^1(G_{\mathbb{Q}},\hat{\mathbb{Z}}(2))$. Let $(-p^3,p)_{c_0}$ in $C^1(G_{\mathbb{Q}},\pi/[\pi]_3)$ be as in Corollary 8, i.e. for all g in $G_{\mathbb{Q}}$

$$(-p^3,p)_{c_0}(g)=y^{\{p\}(g)}x^{\{-p^3\}(g)}[x,y]^{c_0(g)},$$

so $(-p^3,p)_{c_0}$ is a cocycle lifting $(-p^3,p)$. The image of $(-p^3,p)_{c_0}$ under the map $C^1(G_{\mathbb{Q}},\pi/[\pi]_3)\to C^1(G_{\mathbb{Q}},\pi/[\pi]_3^2)$ will also be denoted $(-p^3,p)_{c_0}$.

Proposition 48. *Let p be a prime congruent to 1 mod 4. Let $(-p^3,p)_{c_0}$ be as above. $\delta_3^{\mathrm{mod}\,2}(-p^3,p)_{c_0}$ is the element of $H^2(G_{\mathbb{Q}},[\pi]_3/[\pi]_4([\pi]_3)^2)$ determined by*

$$\delta^{(2,p)}_{3,[[x,y],x]}(-p^3,p)_{c_0}=\delta^{(2,p)}_{3,[[x,y],y]}(-p^3,p)_{c_0}=2\cup p=\begin{cases}\frac{1}{2} & \text{if } p\equiv 5 \mod 8,\\ 0 & \text{if } p\equiv 1 \mod 8.\end{cases}$$

$$\delta^{(2,\nu)}_{3,[[x,y],x]}(-p^3,p)_{c_0}=\delta^{(2,\nu)}_{3,[[x,y],y]}(-p^3,p)_{c_0}=0$$

for ν equal to $\mathbb{R}$ or a finite odd prime not equal to p.

Here, $\mathrm{H}^2(G_{\mathbb{Q}_p},\mathbb{Z}/2\mathbb{Z})$ is identified with the two torsion of $\mathbb{Q}/\mathbb{Z}$ for all finite primes p via the invariant map, and elements of $H^2(G_{\mathbb{Q}},\mathbb{Z}/2)$ are identified with their images under (12.39) .

Proof. Let $S = \{2, p, \infty\}$ and let $\mathbb{Q}_S$ denote the maximal extension of $\mathbb{Q}$ unramified outside S. The cocycle $(-p^3, p)_{c_0}$ factors through $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$, and it follows that

$$\delta^{(2,\nu)}_{3,[[x,y],x]}(-p^3,p)_{c_0} = \delta^{(2,\nu)}_{3,[[x,y],y]}(-p^3,p)_{c_0} = 0$$

for ν equal to any prime not in S.

The obstruction $\delta^{(2,\nu)}_3(-p^3,p)_{c_0}$ for $\nu = \mathbb{R}$ decomposes into two elements $\delta^{(2,\mathbb{R})}_{3,[[x,y],x]}(-p^3,p)_{c_0}$ and $\delta^{(2,\mathbb{R})}_{3,[[x,y],y]}(-p^3,p)_{c_0}$ of $\mathbb{Z}/2 \cong H^2(G_{\mathbb{R}}, \mathbb{Z}/2)$, obtained by evaluating each of the cocycles given in Proposition 13 at $(g_1, g_2) = (\tau, \tau)$, where τ denote complex conjugation in $G_{\mathbb{Q}}$ c.f. 12.4.2. Note that since p is positive, the equalities $\{-p^3\}(\tau) = 1$, $\{p\}(\tau) = 0$, $\binom{-\{p\}(\tau)+1}{2} = 0$, and $c_0(\tau) = 0$ hold in $\mathbb{Z}/2$. Substituting these equations into the cocycles in Proposition 13 shows that $\delta^{(2,\mathbb{R})}_{3,[[x,y],x]}(-p^3,p)_{c_0} = 0$ and $\delta^{(2,\mathbb{R})}_{3,[[x,y],y]}(-p^3,p)_{c_0} = 0$.

By Lemma 33 case (3), we have that

$$\delta^{(2,p)}_{3,[[x,y],x]}(-p^3,p)_c + \delta^{(2,p)}_{3,[[x,y],y]}(-p^3,p)_c \tag{12.43}$$

does not depend on the choice of lift. By Example 43, there is a lift $(-p^3,p)_c$ such that

$$\delta^{(2,p)}_{3,[[x,y],x]}(-p^3,p)_c = \delta^{(2,p)}_{3,[[x,y],y]}(-p^3,p)_c = 0$$

and it follows that (12.43) vanishes.

It follows from Proposition 13 that

$$\delta^{(2,p)}_{3,[[x,y],x]}(-p^3,p)_{c_0} = (\binom{p}{2} + \binom{-(p+\frac{\chi-1}{2})}{2}) \cup p. \tag{12.44}$$

To see this, note that $\frac{\chi-1}{2} = 0$ and $-p^3 = p$ in $C^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2)$. Thus the cocycle $g \mapsto p(g)3(p+\frac{\chi-1}{2})(g)$ equals the cocycle $g \mapsto p(g)$ in $C^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2)$. (Note that equating these two cocycles requires identifying $\mathbb{Z}/2(1)$ with $\mathbb{Z}/2(2)$, so the weight is not being respected!) Substituting these equalities into Proposition 13 implies

$$\delta^{(2,p)}_{3,[[x,y],x]}(-p^3,p)_{c_0} = \binom{p}{2} \cup p + \binom{3(p+\frac{\chi-1}{2})+1}{2} \cup p + p \cup p.$$

Then note that in $C^1(G_{\mathbb{Q}_p}, \mathbb{Z}/2)$,

$$\binom{3(p+\frac{\chi-1}{2})+1}{2} = \binom{3(p+\frac{\chi-1}{2})}{2} + 3(p+\frac{\chi-1}{2}) = \binom{-(p+\frac{\chi-1}{2})}{2} + p,$$

showing (12.44). (It is important to distinguish between $3(p+\frac{\chi-1}{2})$ and p in the binomial coefficient as these two cocycles are not equal in $C^1(G_{\mathbb{Q}_p}, \mathbb{Z}/4(1))$.)

For any two elements d_1, d_2 in $\mathbb{Z}/4$, direct calculation shows

$$\binom{d_1+d_2}{2} - \binom{d_1}{2} - \binom{d_2}{2} = d_1 d_2$$

in $\mathbb{Z}/2$. Thus

$$\binom{p}{2} + \binom{-(p+\frac{\chi-1}{2})}{2} = \binom{-\frac{\chi-1}{2}}{2} + p(p+\frac{\chi-1}{2}) = \binom{-\frac{\chi-1}{2}}{2} + p.$$

Combining with the above, we see

$$\delta^2_{3,[[x,y],x]}(-p^3,p)_{c_0} = \binom{-\frac{\chi-1}{2}}{2} \cup p.$$

Since p is congruent to 1 mod 4, $\mathbb{Q}_p$ contains a primitive fourth root of unity and $\chi(g) \equiv 1 \mod 4$ for every g in $G_{\mathbb{Q}_p}$. Therefore, $\frac{\chi(g)-1}{2}$ is 0 or 2 mod 4, whence $\binom{-\frac{\chi-1}{2}}{2}$ is 0 for g fixing the eight roots of unity and 1 otherwise. It follows that

$$\delta^2_{3,[[x,y],x]}(-p^3,p)_{c_0} = \begin{cases} \frac{1}{2} & \text{if } p \equiv 5 \mod 8, \\ 0 & \text{if } p \equiv 1 \mod 8. \end{cases}$$

□

References

[And89] Greg W. Anderson, *The hyperadelic gamma function*, Invent. Math. **95** (1989), no. 1, 63–131. MR MR969414 (89j:11118)

[Bro94] Kenneth S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994, Corrected reprint of the 1982 original. MR MR1324339 (96a:20072)

[CF67] *Algebraic number theory*, Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich, Academic Press, London, 1967. MR 0215665 (35 #6500)

[Col89] R. F. Coleman, *Anderson-Ihara theory: Gauss sums and circular units*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 55–72. MR MR1097609 (92f:11159)

[Del89] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, Galois groups over **Q** (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 79–297. MR MR1012168 (90m:14016)

[Dwy75] William G. Dwyer, *Homology, Massey products and maps between groups*, J. Pure Appl. Algebra **6** (1975), no. 2, 177–190. MR MR0385851 (52 #6710)

[Ell00] Jordan Ellenberg, *2-nilpotent quotients of fundamental groups of curves*, Preprint, 2000.

[Hab78] Klaus Haberland, *Galois cohomology of algebraic number fields*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1978, With two appendices by Helmut Koch and Thomas Zink. MR 519872 (81i:12009)

[Hat02] Allen Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002. MR 1867354 (2002k:55001)

[Hos10] Yuichiro Hoshi, *Existence of nongeometric pro-p Galois sections of hyperbolic curves*, RIMS-1689, January, 2010.

[Iha91] Yasutaka Ihara, *Braids, Galois groups, and some arithmetic functions*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990) (Tokyo), Math. Soc. Japan, 1991, pp. 99–120. MR MR1159208 (95c:11073)

[Iha94] ———, *On the embedding of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *into* $\widehat{\mathrm{GT}}$, The Grothendieck theory of dessins d'enfants (Luminy, 1993), London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, With an appendix: the action of the absolute Galois group on the moduli space of spheres with four marked points by Michel Emsalem and Pierre Lochak, pp. 289–321. MR MR1305402 (96b:14014)

[IKY87] Yasutaka Ihara, Masanobu Kaneko, and Atsushi Yukinari, *On some properties of the universal power series for Jacobi sums*, Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986), Adv. Stud. Pure Math., vol. 12, North-Holland, Amsterdam, 1987, pp. 65–86. MR MR948237 (90d:11122)

[Laz54] Michel Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. Ecole Norm. Sup. (3) **71** (1954), 101–190. MR 0088496 (19,529b)

[Mil71] John Milnor, *Introduction to algebraic K-theory*, Princeton University Press, Princeton, N.J., 1971, Annals of Mathematics Studies, No. 72. MR 0349811 (50 #2304)

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR 559531 (81j:14002)

[MKS04] Wilhelm Magnus, Abraham Karrass, and Donald Solitar, *Combinatorial group theory*, second ed., Dover Publications Inc., Mineola, NY, 2004, Presentations of groups in terms of generators and relations. MR MR2109550 (2005h:20052)

[Nak99] Hiroaki Nakamura, *Tangential base points and Eisenstein power series*, Aspects of Galois theory (Gainesville, FL, 1996), London Math. Soc. Lecture Note Ser., vol. 256, Cambridge Univ. Press, Cambridge, 1999, pp. 202–217. MR 1708607 (2000j:14038)

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR MR2392026 (2008m:11223)

[Pop10] Florian Pop, *On the birational p-adic section conjecture*, Compos. Math. **146** (2010), no. 3, 621–637. MR 2644930

[Ser88] Jean-Pierre Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988, Translated from the French. MR MR918564 (88i:14041)

[Ser02] ———, *Galois cohomology*, english ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author. MR MR1867431 (2002i:12004)

[SGAI] *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3, Société Mathématique de France, Paris, 2003, Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)]. MR MR2017446 (2004g:14017)

[Tat76] John Tate, *Relations between* K_2 *and Galois cohomology*, Invent. Math. **36** (1976), 257–274. MR 0429837 (55 #2847)

[Vog04] Denis Vogel, *Massey products in the galois cohomology of number fields*, Thesis: Universität Heidelberg, 2004.

[Wic10] Kirsten Wickelgren, *2-nilpotent real section conjecture*, Preprint arXiv:1006.0265, 2010.

[Zar74] Yu. G. Zarkhin, *Noncommutative cohomology and Mumford groups*, Mat. Zametki **15** (1974), 415–419. MR MR0354612 (50 #7090)