NON-FORMALITY OF GALOIS COHOMOLOGY MODULO ALL PRIMES

ALEXANDER MERKURJEV AND FEDERICO SCAVIA

Abstract. Let p be a prime number and let F be a field of characteristic different from p. We prove that there exist a field extension L/F and a, b, c, d in $L^\times$ such that $(a,b) = (b,c) = (c,d) = 0$ in $\mathrm{Br}(F)[p]$ but $\langle a,b,c,d\rangle$ is not defined over L. Thus the Strong Massey Vanishing Conjecture at the prime p fails for L, and the cochain differential graded ring $C^\cdot(\Gamma_L, \mathbb{Z}/p\mathbb{Z})$ of the absolute Galois group Γ_L of L is not formal. This answers a question of Positselski.

1. Introduction

Let p be a prime number, let F be a field of characteristic different from p and containing a primitive p-th root of unity ζ, and let Γ_F be the absolute Galois group of F. The Norm-Residue Isomorphism Theorem of Voevodsky and Rost [HW19] gives an explicit presentation by generators and relations of the cohomology ring $H^\cdot(F, \mathbb{Z}/p\mathbb{Z}) = H^\cdot(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$. In view of this complete description of the cup product, the research on $H^\cdot(F, \mathbb{Z}/p\mathbb{Z})$ shifted in recent years to external operations, defined in terms of the differential graded ring of continuous cochains $C^\cdot(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$.

Hopkins–Wickelgren [HW15] asked whether $C^\cdot(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ is formal for every field F and every prime p. Loosely speaking, this amounts to saying that no essential information is lost when passing from $C^\cdot(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ to $H^\cdot(F, \mathbb{Z}/p\mathbb{Z})$. Positselski [Pos17] showed that $C^\cdot(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ is not formal for some finite extensions F of $\mathbb{Q}_\ell$ and $\mathbb{F}_\ell((z))$, where $\ell \neq p$. He then posed the following question; see [Pos17, p. 226].

Question 1.1 (Positselski)**.** *Does there exist a field F containing all roots of unity of p-power order such that $C^\cdot(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ is not formal?*

We showed in [MS22, Theorem 1.6] that Question 1.1 has a positive answer when $p = 2$. In the present work we provide examples showing that the answer to Question 1.1 is affirmative for all primes p.

Theorem 1.2. *Let p be a prime number and let F be a field of characteristic different from p. There exists a field L containing F such that the differential graded ring $C^\cdot(\Gamma_L, \mathbb{Z}/p\mathbb{Z})$ is not formal.*

In order to detect non-formality of the cochain differential graded ring, we use Massey products. For any $n \geq 2$ and all $\chi_1, \dots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$, the Massey product of $\chi_1, \dots, \chi_n$ is a certain subset $\langle \chi_1, \dots, \chi_n\rangle \subset H^2(F, \mathbb{Z}/p\mathbb{Z})$; see Section 2.2 for the definition. We say that $\langle \chi_1, \dots, \chi_n\rangle$ is defined if it is not empty, and that it vanishes if it contains 0. When $\mathrm{char}(F) \neq p$ and F contains a primitive p-th root of unity ζ, Kummer Theory gives an identification

Date: September 2023.

2020 *Mathematics Subject Classification.* 12G05; 55S30, 16K50.

$H^1(F, \mathbb{Z}/p\mathbb{Z}) = F^\times/F^{\times p}$, and we may thus consider Massey products $\langle a_1, \ldots, a_n \rangle$, where $a_i \in F^\times$ for $1 \leq i \leq n$.

Let $n \geq 3$ be an integer, let $\chi_1, \ldots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$, and consider the following assertions:

(1.1) The Massey product $\langle \chi_1, \ldots, \chi_n \rangle$ vanishes.

(1.2) The Massey product $\langle \chi_1, \ldots, \chi_n \rangle$ is defined.

(1.3) We have $\chi_i \cup \chi_{i+1} = 0$ for all $1 \leq i \leq n-1$.

We have that (1.1) implies (1.2), and that (1.2) implies (1.3). The Massey Vanishing Conjecture, due to Mináč–Tân [MT17b] and inspired by the earlier work of Hopkins–Wickelgren [HW15], predicts that (1.2) implies (1.1). This conjecture has sparked a lot of activity in recent years. When F is an arbitrary field, the conjecture is known when either $n = 3$ and p is arbitrary, by Efrat–Matzri and Mináč–Tân [Mat18, EM17, MT16], or $n = 4$ and $p = 2$, by [MS23]. When F is a number field, the conjecture was proved for all $n \geq 3$ and all primes p, by Harpaz–Wittenberg [HW23].

When $n = 3$, it is a direct consequence of the definition of Massey product that (1.3) implies (1.2). Thus (1.1), (1.2) and (1.3) are equivalent when $n = 3$.

In [MT17a, Question 4.2], Mináč and Tân asked whether (1.3) implies (1.1). This became known as the Strong Massey Vanishing Conjecture (see e.g. [PS18]): If F is a field, p is a prime number and $n \geq 3$ is an integer then, for all characters $\chi_1, \ldots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$ such that $\chi_i \cup \chi_{i+1} = 0$ for all $1 \leq i \leq n-1$, the Massey product $\langle \chi_1, \ldots, \chi_n \rangle$ vanishes.

The Strong Massey Vanishing Conjecture implies the Massey Vanishing Conjecture. However, Harpaz and Wittenberg produced a counterexample to the Strong Massey Vanishing Conjecture, for $n = 4$, $p = 2$ and $F = \mathbb{Q}$; see [GMT18, Example A.15]. More precisely, if we let $b = 2$, $c = 17$ and $a = d = bc = 34$, then $(a, b) = (b, c) = (c, d) = 0$ in $\mathrm{Br}(\mathbb{Q})$ but $\langle a, b, c, d \rangle$ is not defined over $\mathbb{Q}$. In this example, the classes of a, b, c, d in $F^\times/F^{\times 2}$ are not $\mathbb{F}_2$-linearly independent modulo squares. In fact, by a theorem of Guillot–Mináč–Topaz–Wittenberg [GMT18], if F is a number field and a, b, c, d are independent in $F^\times/F^{\times 2}$ and satisfy $(a, b) = (b, c) = (c, d) = 0$ in $\mathrm{Br}(F)$, then $\langle a, b, c, d \rangle$ vanishes.

If F is a field for which the Strong Massey Vanishing Conjecture fails, for some $n \geq 3$ and some prime p, then $C^\cdot(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ is not formal; see Lemma 2.3 for the $n = 4$ case. Therefore Theorem 1.2 follows from the next more precise result.

Theorem 1.3. *Let p be a prime number, let F be a field of characteristic different from p. There exist a field L containing F and $\chi_1, \chi_2, \chi_3, \chi_4 \in H^1(L, \mathbb{Z}/p\mathbb{Z})$ such that $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = \chi_3 \cup \chi_4 = 0$ in $H^2(L, \mathbb{Z}/p\mathbb{Z})$ but $\langle \chi_1, \chi_2, \chi_3, \chi_4 \rangle$ is not defined. Thus the Strong Massey Vanishing conjecture at $n = 4$ and the prime p fails for L, and $C^\cdot(\Gamma_L, \mathbb{Z}/p\mathbb{Z})$ is not formal.*

This gives the first counterexamples to the Strong Massey Vanishing Conjecture for all odd primes p. We easily deduce that (1.3) does not imply (1.2) for all $n \geq 4$, in general: indeed, if the fourfold Massey product $\langle \chi_1, \chi_2, \chi_3, \chi_4 \rangle$ is not defined, neither is the n-fold Massey product $\langle \chi_1, \chi_2, \chi_3, \chi_4, 0, \ldots, 0 \rangle$. Theorem 1.3 was proved in [MS22, Theorem 1.6] when $p = 2$, and is new when p is odd. Our proof of Theorem 1.3 is uniform in p.

We now describe the main ideas that go into the proof of Theorem 1.3. We may assume without loss of generality that F contains a primitive p-th root of unity. In Section 2, we collect preliminaries on formality, Massey products and Galois algebras. In particular, we recall Dwyer's Theorem (see Theorem 2.4): a Massey product $\langle \chi_1, \ldots, \chi_n \rangle \subset H^2(F, \mathbb{Z}/p\mathbb{Z})$ vanishes (resp. is defined) if and only if the homomorphism $(\chi_1, \ldots, \chi_n)\colon \Gamma_F \to (\mathbb{Z}/p\mathbb{Z})^n$ lifts to the group U_{n+1} of upper unitriangular matrices in $\mathrm{GL}_{n+1}(\mathbb{F}_p)$ (resp. to the group $\overline{U}_{n+1}$ of upper unitriangular matrices in $\mathrm{GL}_{n+1}(\mathbb{F}_p)$ with top-right corner removed). As for [MS22, Theorem 1.6], our approach is based on Corollary 2.5, which is a restatement of Theorem 2.4 in terms of Galois algebras.

In Section 3, we show that a fourfold Massey product $\langle a, b, c, d \rangle$ is defined over F if and only if a certain system of equations admits a solution over F, and the variety defined by these equations is a torsor under a torus; see Proposition 3.7. This is done by using Dwyer's Theorem 2.4 to rephrase the property that $\langle a, b, c, d \rangle$ is defined in terms of $\overline{U}_5$-Galois algebras, and then by a detailed study of Galois G-algebras, for $G = U_3, \overline{U}_4, U_4, \overline{U}_5$. As a consequence, we also obtain an alternative proof of the Massey Vanishing Conjecture for $n = 3$ and any prime p; see Proposition 3.6.

In Section 4, we use the work of Section 3.4 to construct a "generic variety" for the property that $\langle a, b, c, d \rangle$ is defined. More precisely, under the assumption that $(a, b) = (c, d) = 0$ in $\mathrm{Br}(F)$ and letting X be the Severi-Brauer variety of (b, c), we construct an F-torus T, and a $T_{F(X)}$-torsor E_w such that, if E_w is non-trivial, then $\langle a, b, c, d \rangle$ is not defined over $F(X)$; see Corollary 4.5. The definition of E_w depends on a rational function $w \in F(X)^\times$, which we construct in Lemma 4.1(3).

Since $(a, b) = (b, c) = (c, d) = 0$ in $\mathrm{Br}(F(X))$, the proof of Theorem 1.3 will be complete once we give an example of a, b, c, d for which the corresponding torsor E_w is non-trivial. Here we consider the generic quadruple a, b, c, d such that (a, b) and (c, d) are trivial. More precisely, we let x, y be two variables over F, and replace F by $E \coloneqq F(x, y)$. We then set $a \coloneqq 1 - x$, $b \coloneqq x$, $c \coloneqq y$ and $d \coloneqq 1 - y$ over E. We have $(a, b) = (b, c) = 0$ in $\mathrm{Br}(E)$. The class (b, c) is not zero in $\mathrm{Br}(E)$, so that the Severi-Brauer variety X/E of (b, c) is non-trivial, but $(b, c) = 0$ over $L \coloneqq E(X)$.

It is natural to attempt to prove that E_w is non-trivial over L by performing residue calculations to deduce that this torsor is ramified. However, the torsor E_w is in fact unramified. We are thus led to consider a finer obstruction to the triviality of E_w. This "secondary obstruction" is only defined for unramified torsors. We describe the necessary homological algebra in Appendix A, and we define the obstruction and give a method to compute it in Appendix B. In Section 5, an explicit calculation shows that the obstruction is non-zero on E_w, and hence E_w is non-trivial, as desired.

Notation. Let F be a field, let F_s be a separable closure of F, and denote by $\Gamma_F \coloneqq \mathrm{Gal}(F_s/F)$ the absolute Galois group of F.

If E is an F-algebra, we let $H^i(E, -)$ be the étale cohomology of $\mathrm{Spec}(E)$ (possibly non-abelian if $i \leq 1$). If E is a field, $H^i(E, -)$ may be identified with the continuous cohomology of Γ_E.

We fix a prime p, and we suppose that $\mathrm{char}(F) \neq p$. If E is an F-algebra and $a_1, \ldots, a_n \in E^\times$, we define the étale E-algebra $E_{a_1,\ldots,a_n}$ by

$$E_{a_1,\ldots,a_n} \coloneqq E[x_1, \ldots, x_n]/(x_1^p - a_1, \ldots, x_n^p - a_n)$$

and we set $(a_i)^{1/p} \coloneqq x_i$. More generally, for all integers d, we set $(a_i)^{d/p} \coloneqq x_i^d$. We denote by $R_{a_1,\dots,a_n}(-)$ the functor of Weil restriction along $F_{a_1,\dots,a_n}/F$. In particular $R_{a_1,\dots,a_n}(\mathbb{G}_\mathrm{m})$ is the quasi-trivial torus associated to $F_{a_1,\dots,a_n}/F$, and we denote by $R^{(1)}_{a_1,\dots,a_n}(\mathbb{G}_\mathrm{m})$ the norm-one subtorus of $R_{a_1,\dots,a_n}(\mathbb{G}_\mathrm{m})$. We denote by $N_{a_1,\dots,a_n}$ the norm map from $F_{a_1,\dots,a_n}$ to F.

We write $\mathrm{Br}(F)$ for the Brauer group of F. If $\mathrm{char}(F) \neq p$ and F contains a primitive p-th root of unity, for all $a, b \in F^\times$ we let (a, b) be the corresponding degree-p cyclic algebra and for its class in $\mathrm{Br}(F)$; see Section 2.1. We denote by $N_{a_1,\dots,a_n} \colon \mathrm{Br}(F_{a_1,\dots,a_n}) \to \mathrm{Br}(F)$ for the corestriction map along $F_{a_1,\dots,a_n}/F$.

An F-variety is a separated integral F-scheme of finite type. If X is an F-variety, we denote by $F(X)$ the function field of X, and we write $X^{(1)}$ for the collection of all points of codimension 1 in X. We set $X_s \coloneqq X \times_F F_s$. If K is an étale algebra over F, we write X_K for $X \times_F K$. For all $a_1, \dots, a_n \in F^\times$, we write $X_{a_1,\dots,a_n}$ for $X_{F_{a_1,\dots,a_n}}$. When $X = \mathbb{P}^d_F$ is a d-dimensional projective space, we denote by $\mathbb{P}^d_{a_1,\dots,a_n}$ the base change of $\mathbb{P}^d_F$ to $F_{a_1,\dots,a_d}$.

2. Preliminaries

2.1. **Galois algebras and Kummer Theory.** Let F be a field and let G be a finite group. A *G-algebra* is an étale F-algebra L on which G acts via F-algebra automorphisms. The G-algebra L is *Galois* if $|G| = \dim_F(L)$ and $L^G = F$; see [KMRT98, Definitions (18.15)]. A G-algebra L/F is Galois if and only if the morphism of schemes $\mathrm{Spec}(L) \to \mathrm{Spec}(F)$ is an étale G-torsor. If L/F is a Galois G-algebra, the group algebra $\mathbb{Z}[G]$ acts on the multiplicative group $L^\times$: an element $\sum_{i=1}^r m_i g_i \in \mathbb{Z}[G]$, where $m_i \in \mathbb{Z}$ and $g_i \in G$, sends $x \in L^\times$ to $\prod_{i=1}^r g_i(x)^{m_i}$.

By [KMRT98, Example (28.15)], we have a canonical bijection

$$\mathrm{Hom}_{\mathrm{cont}}(\Gamma_F, G)/_\sim \xrightarrow{\sim} \{\text{Isomorphism classes of Galois } G\text{-algebras over } F\}, \tag{2.1}$$

where, if $f_1, f_2 \colon \Gamma_F \to G$ are continuous group homomorphisms, we say that $f_1 \simeq f_2$ if there exists $g \in G$ such that $g f_1(\sigma) g^{-1} = f_2(\sigma)$ for all $\sigma \in \Gamma_F$.

Let H be a normal subgroup of G. Under the correspondence (2.1), the map $\mathrm{Hom}_{\mathrm{cont}}(\Gamma_F, G)/_\sim \to \mathrm{Hom}_{\mathrm{cont}}(\Gamma_F, G/H)/_\sim$ sends the class of a Galois G-algebra L to the class of the Galois G/H-algebra L^H.

Lemma 2.1. *Let G be a finite group, and let H, H', S be normal subgroups of G such that $H \subset S$, $H' \subset S$, and the square*

$$\begin{array}{ccc} G & \longrightarrow & G/H \\ \downarrow & & \downarrow \\ G/H' & \longrightarrow & G/S \end{array} \tag{2.2}$$

is cartesian.

(1) Let L be a Galois G-algebra. Then the tensor product $L^H \otimes_{L^S} L^{H'}$ has a Galois G-algebra structure given by $g(x \otimes x') \coloneqq g(x) \otimes g(x')$ for all $x \in L^H$ and $x' \in L^{H'}$. Moreover, the inclusions $L^H \to L$ and $L^{H'} \to L$ induce an isomorphism of Galois G-algebras $L^H \otimes_{L^S} L^{H'} \to L$.

(2) Conversely, let K be a Galois G/H-algebra, let K' be a Galois G/H'-algebra, and let E be a Galois G/S-algebra. Suppose given G-equivariant algebra homomorphisms $E \to K$ and $E \to K'$. Endow the tensor product $L \coloneqq K \otimes_E K'$ with the

structure of a G-algebra given by $g(x\otimes x') := g(x)\otimes g(x')$ for all $x \in K$ and $x' \in K'$. Then L is a Galois G-algebra such that $L^H \simeq K$ as G/H-algebras, and $L^{H'} \simeq K'$ as G/H'-algebras.

The condition that (2.2) is cartesian is equivalent to $H\cap H' = \{1\}$ and $S = HH'$.

Proof. (1) It is clear that the formula $g(x\otimes x') := g(x)\otimes g(x')$ makes $L^H \otimes_{L^S} L^{H'}$ into a G-algebra. Consider the commutative square of F-schemes

$$\begin{array}{ccc} \mathrm{Spec}(L) & \longrightarrow & \mathrm{Spec}(L)/H' \\ \downarrow & & \downarrow \\ \mathrm{Spec}(L)/H & \longrightarrow & \mathrm{Spec}(L)/S. \end{array}$$

After base change to a separable closure of F, this square becomes the cartesian square (2.2), and therefore it is cartesian. Passing to coordinate rings, we deduce that the map $L^H \otimes_{L^S} L^{H'} \to L$ is an isomorphism of G-algebras. In particular, since L is a Galois G-algebra, so is $L^H \otimes_{L^S} L^{H'}$.

(2) We have a G-equivariant cartesian diagram

$$\begin{array}{ccc} \mathrm{Spec}(L) & \longrightarrow & \mathrm{Spec}(K') \\ \downarrow & & \downarrow \\ \mathrm{Spec}(K) & \longrightarrow & \mathrm{Spec}(E). \end{array}$$

Every G-equivariant morphism between G/H and G/S is isomorphic to the projection map $G/H \to G/S$. Therefore the base change of $\mathrm{Spec}(K) \to \mathrm{Spec}(E)$ to F_s is G-equivariantly isomorphic to the projection $G/H \to G/S$. Similarly for $\mathrm{Spec}(K') \to \mathrm{Spec}(E)$. Therefore the base change of $\mathrm{Spec}(L) \to \mathrm{Spec}(F)$ over F_s is G-equivariantly isomorphic to $(G/H)\times_{G/S}(G/H') \simeq G$, that is, the morphism $\mathrm{Spec}(L) \to \mathrm{Spec}(F)$ is an étale G-torsor. □

Suppose that $\mathrm{char}(F) \neq p$ and that F contains a primitive p-th root of unity. We fix a primitive p-th root of unity $\zeta \in F^\times$. This determines an isomorphism of Galois modules $\mathbb{Z}/p\mathbb{Z} \simeq \mu_p$, given by $1 \mapsto \zeta$, and so the Kummer sequence yields an isomorphism

$$\mathrm{Hom}_{\mathrm{cont}}(\Gamma_F, \mathbb{Z}/p\mathbb{Z}) = H^1(F, \mathbb{Z}/p\mathbb{Z}) \simeq H^1(F, \mu_p) \simeq F^\times/F^{\times p}. \tag{2.3}$$

For every $a \in F^\times$, we let $\chi_a\colon \Gamma_F \to \mathbb{Z}/p\mathbb{Z}$ be the homomorphism corresponding to the coset $aF^{\times p}$ under (2.3). Explicitly, letting $a' \in F^\times_{\mathrm{sep}}$ be such that $(a')^p = a$, we have $g(a') = \zeta^{\chi_a(g)}a'$ for all $g \in \Gamma_F$. This definition does not depend on the choice of a'.

Now let $n \geq 1$ be an integer. For all $i = 1, \dots, n$, let σ_i be the canonical generator of the i-th factor $\mathbb{Z}/p\mathbb{Z}$ of $(\mathbb{Z}/p\mathbb{Z})^n$. By (2.3) all Galois $(\mathbb{Z}/p\mathbb{Z})^n$-algebras over F are of the form $F_{a_1,\dots,a_n}$, where $a_1, \dots, a_n \in F^\times$ and the Galois $(\mathbb{Z}/p\mathbb{Z})^n$-algebra structure is defined by $(\sigma_i - 1)a_i^{1/p} = \zeta$ for all i and $(\sigma_i - 1)a_j^{1/p} = 1$ for all $j \neq i$.

We write (a, b) for the cyclic degree-p central simple algebra over F generated, as an F-algebra, by F_a and an element y such that

$$y^p = b, \qquad ty = y\sigma_a(t) \text{ for all } t \in F_a.$$

We also write (a,b) for the class of (a,b) in $\mathrm{Br}(F)$. The Kummer sequence yields a group isomorphism

$$\iota\colon H^2(F,\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\sim} \mathrm{Br}(F)[p].$$

For all $a,b\in F^\times$, we have $\iota(\chi_a\cup\chi_b)=(a,b)$ in $\mathrm{Br}(F)$; see [Ser79, Chapter XIV, Proposition 5].

Lemma 2.2. *Let p be a prime, and let F be a field of characteristic different from p and containing a primitive p-th root of unity ζ. The following are equivalent:*
(i) $(a,b)=0$ in $\mathrm{Br}(F)$;
(ii) there exists $\alpha\in F_a^\times$ such that $b=N_a(\alpha)$;
(iii) there exists $\beta\in F_b^\times$ such that $a=N_b(\beta)$.

Proof. See [Ser79, Chapter XIV, Proposition 4(iii)]. □

2.2. **Formality and Massey products.** Let (A,∂) be a differential graded ring, i.e, $A=\oplus_{i\geq 0}A^i$ is a non-negatively graded abelian group with an associative multiplication which respects the grading, and $\partial\colon A\to A$ is a group homomorphism of degree 1 such that $\partial\circ\partial=0$ and $\partial(ab)=\partial(a)b+(-1)^ia\partial(b)$ for all $i\geq 0$, $a\in A^i$ and $b\in A$. We denote by $H^\bullet(A)\coloneqq \mathrm{Ker}(\partial)/\mathrm{Im}(\partial)$ the cohomology of (A,∂), and we write $\cup$ for the multiplication (cup product) on $H^\bullet(A)$.

We say that A is *formal* if it is quasi-isomorphic, as a differential graded ring, to $H^\bullet(A)$ with the zero differential.

Let $n\geq 2$ be an integer and $a_1,\dots,a_n\in H^1(A)$. A *defining system* for the n-th order Massey product $\langle a_1,\dots,a_n\rangle$ is a collection M of elements of $a_{ij}\in A^1$, where $1\leq i<j\leq n+1$, $(i,j)\neq(1,n+1)$, such that

(1) $\partial(a_{i,i+1})=0$ and $a_{i,i+1}$ represents a_i in $H^1(A)$, and
(2) $\partial(a_{ij})=-\sum_{l=i+1}^{j-1}a_{il}a_{lj}$ for all $i<j-1$.

It follows from (2) that $-\sum_{l=2}^{n}a_{1l}a_{l,n+1}$ is a 2-cocycle: we write $\langle a_1,\dots,a_n\rangle_M$ for its cohomology class in $H^2(A)$, called the *value* of $\langle a_1,\dots,a_n\rangle$ corresponding to M. By definition, the *Massey product* of $a_1,\dots,a_n$ is the subset $\langle a_1,\dots,a_n\rangle$ of $H^2(A)$ consisting of the values $\langle a_1,\dots,a_n\rangle_M$ of all defining systems M. We say that the Massey product $\langle a_1,\dots,a_n\rangle$ is *defined* if it is non-empty, and that it *vanishes* if $0\in\langle a_1,\dots,a_n\rangle$.

Lemma 2.3. *Let (A,∂) be a differential graded ring, and let $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ be elements of $H^1(A)$ satisfying $\alpha_1\cup\alpha_2=\alpha_2\cup\alpha_3=\alpha_3\cup\alpha_4=0$. If A is formal, then $\langle\alpha_1,\alpha_2,\alpha_3,\alpha_4\rangle$ is defined.*

Proof. This was proved in [MS22, Lemma B.1] under the assumption that A is a differential graded $\mathbb{F}_2$-algebra. The proof for an arbitrary differential graded ring remains the same. □

In fact, one could prove the following: If the differential graded ring A is formal, then for all $n\geq 3$ and all $\alpha_1,\dots,\alpha_n\in H^1(A)$ such that $\alpha_i\cup\alpha_{i+1}=0$ for all $1\leq i\leq n-1$, then $\langle\alpha_1,\dots,\alpha_n\rangle$ vanishes.

2.3. **Dwyer's Theorem.** Let p be a prime, and let $U_{n+1}\subset\mathrm{GL}_{n+1}(\mathbb{F}_p)$ be the subgroup of $(n+1)\times(n+1)$ upper unitriangular matrices. For all $1\leq i<j\leq n+1$, we denote by e_{ij} the matrix whose non-diagonal entries are all zero except for the entry (i,j), which is equal to 1. We set $\sigma_i\coloneqq e_{i,i+1}$ for all $1\leq i\leq n$. By [BD01,

Theorem 1], the group U_{n+1} admits a presentation with generators the σ_i and relations:

$$\sigma_i^p = 1 \qquad \text{for all } 1 \le i \le n, \tag{2.4}$$

$$[\sigma_i, \sigma_j] = 1 \qquad \text{for all } 1 \le i \le j-2 \le n-2, \tag{2.5}$$

$$[\sigma_i, [\sigma_i, \sigma_{i+1}]] = [\sigma_{i+1}, [\sigma_i, \sigma_{i+1}]] \qquad \text{for all } 1 \le i \le n-2, \tag{2.6}$$

$$[[\sigma_i, \sigma_{i+1}], [\sigma_{i+1}, \sigma_{i+2}]] = 1 \qquad \text{for all } 1 \le i \le n-3. \tag{2.7}$$

The following relation holds in U_{n+1}:

$$[e_{ij}, e_{jk}] = e_{ik} \qquad \text{for all } 1 \le i < j < k \le n+1.$$

By induction, we deduce that

$$e_{1,n+1} = [\sigma_1, [\sigma_2, \dots, [\sigma_{n-2}, [\sigma_{n-1}, \sigma_n]] \dots]].$$

The center Z_{n+1} of U_{n+1} is the subgroup generated by $e_{1,n+1}$. The factor group $\overline{U}_{n+1} \coloneqq U_{n+1}/Z_{n+1}$ may be identified with the group of all $(n+1) \times (n+1)$ upper unitriangular matrices with entry $(1, n+1)$ omitted. For all $1 \le i < j \le n+1$, let $\overline{e}_{ij}$ be the coset of e_{ij} in $\overline{U}_{n+1}$, and set $\overline{\sigma}_i \coloneqq \overline{e}_{i,i+1}$ for all $1 \le i \le n$. Then $\overline{U}_{n+1}$ is generated by all the $\overline{e}_{ij}$ modulo the relations

$$\overline{\sigma}_i^p = 1 \qquad \text{for all } 1 \le i \le n, \tag{2.8}$$

$$[\overline{\sigma}_i, \overline{\sigma}_j] = 1 \qquad \text{for all } 1 \le i \le j-2 \le n-2, \tag{2.9}$$

$$[\overline{\sigma}_i, [\overline{\sigma}_i, \overline{\sigma}_{i+1}] = [\overline{\sigma}_{i+1}, [\overline{\sigma}_i, \overline{\sigma}_{i+1}]] \qquad \text{for all } 1 \le i \le n-2, \tag{2.10}$$

$$[[\overline{\sigma}_i, \overline{\sigma}_{i+1}], [\overline{\sigma}_{i+1}, \overline{\sigma}_{i+2}]] = 1 \qquad \text{for all } 1 \le i \le n-3. \tag{2.11}$$

$$[\overline{\sigma}_1, [\overline{\sigma}_2, \dots, [\overline{\sigma}_{n-2}, [\overline{\sigma}_{n-1}, \overline{\sigma}_n]] \dots]] = 1. \tag{2.12}$$

We write $u_{ij} \colon U_{n+1} \to \mathbb{Z}/p\mathbb{Z}$ for the (i,j)-th coordinate function on U_{n+1}. Note that u_{ij} is not a group homomorphism unless $j = i+1$. We have commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Z_{n+1} & \longrightarrow & U_{n+1} & \longrightarrow & \overline{U}_{n+1} & \longrightarrow & 1 \\ & & & & & \searrow & \downarrow & & \\ & & & & & & (\mathbb{Z}/p\mathbb{Z})^n & & \end{array} \tag{2.13}$$

where the row is a central exact sequence and the homomorphism $U_{n+1} \to (\mathbb{Z}/p\mathbb{Z})^n$ is given by $(u_{12}, u_{23}, \dots, u_{n,n+1})$. We also let

$$Q_{n+1} \coloneqq \mathrm{Ker}[U_{n+1} \to (\mathbb{Z}/p\mathbb{Z})^n], \quad \overline{Q}_{n+1} \coloneqq \mathrm{Ker}[\overline{U}_{n+1} \to (\mathbb{Z}/p\mathbb{Z})^n] = Q_{n+1}/Z_{n+1}.$$

Note that $Z_{n+1} \subset Q_{n+1}$, with equality when $n = 2$.

Let G be a profinite group. The complex $(C^\cdot(G, \mathbb{Z}/p\mathbb{Z}), \partial)$ of mod p non-homogeneous continuous cochains of G with the standard cup product is a differential graded ring. Therefore $H^\cdot(G, \mathbb{Z}/p\mathbb{Z}) = H^\cdot(C^\cdot(G, \mathbb{Z}/p\mathbb{Z}), \partial)$ is endowed with Massey products. The following theorem is due to Dwyer [Dwy75].

Theorem 2.4 (Dwyer)**.** *Let p be a prime number, let G be a profinite group, let $\chi_1,\dots,\chi_n \in H^1(G,\mathbb{Z}/p\mathbb{Z})$, and write $\chi\colon G \to (\mathbb{Z}/p\mathbb{Z})^n$ for the continuous homomorphism with components $(\chi_1,\dots,\chi_n)$. Consider (2.13).*

(1) The Massey product $\langle\chi_1,\dots,\chi_n\rangle$ is defined if and only if χ lifts to a continuous homomorphism $G \to \overline{U}_{n+1}$.

(2) The Massey product $\langle\chi_1,\dots,\chi_n\rangle$ vanishes if and only if χ lifts to a continuous homomorphism $G \to U_{n+1}$.

Proof. See [Dwy75] for Dwyer's original proof in the setting of abstract groups, and [Efr14] or [HW23, Proposition 2.2] for the statement in the case of profinite groups. □

Theorem 2.4 may be rephrased as follows.

Corollary 2.5. *Let p be a prime, F be a field of characteristic different from p and containing a primitive p-th root of unity ζ, and let $a_1,\dots,a_n \in F^\times$. The Massey product $\langle a_1,\dots,a_n\rangle \subset H^2(F,\mathbb{Z}/p\mathbb{Z})$ is defined (resp. vanishes) if and only if there exists a Galois $\overline{U}_{n+1}$-algebra K/F (resp. a Galois U_{n+1}-algebra L/F) such that $K^{\overline{Q}_{n+1}} \simeq F_{a_1,\dots,a_n}$ (resp. $L^{Q_{n+1}} \simeq F_{a_1,\dots,a_n}$) as $(\mathbb{Z}/p\mathbb{Z})^n$-algebras.*

Proof. This follows from Theorem 2.4 and (2.1). □

We will apply Lemma 2.1 to the cartesian square of groups

$$\begin{array}{ccc} \overline{U}_{n+1} & \xrightarrow{\varphi_{n+1}} & U_n \\ \downarrow{\scriptstyle \varphi'_{n+1}} & & \downarrow{\scriptstyle \varphi'_n} \\ U_n & \xrightarrow{\varphi_n} & U_{n-1} \end{array} \tag{2.14}$$

where φ_{n+1} (respectively, φ'_{n+1}) is the restriction homomorphism from U_{n+1} or from U_{n+1} to the top-left (respectively, bottom-right) $n\times n$ subsquare U_n in U_{n+1}.

The fact that the square (2.14) is cartesian is proved in [MS22, Proposition 2.7] when $p = 2$. The proof extends to odd p without change.

3. Massey products and Galois algebras

In this section, we let p be a prime number and we let F be a field. With the exception of Proposition 3.6, we assume that $\mathrm{char}(F) \neq p$ and that F contains a primitive p-th root of unity ζ.

3.1. **Galois U_3-algebras.** Let $a, b \in F^\times$, and suppose that $(a,b) = 0$ in $\mathrm{Br}(F)$. By Lemma 2.2, we may fix $\alpha \in F_a^\times$ and $\beta \in F_b^\times$ such that $N_a(\alpha) = b$ and $N_b(\beta) = a$.

We write $(\mathbb{Z}/p\mathbb{Z})^2 = \langle\sigma_a,\sigma_b\rangle$, and we view $F_{a,b}$ as a Galois $(\mathbb{Z}/p\mathbb{Z})^2$-algebra as in Section 2.1. The projection $U_3 \to \overline{U}_3 = (\mathbb{Z}/p\mathbb{Z})^2$ sends $e_{12} \mapsto \sigma_a$ and $e_{23} \mapsto \sigma_b$. We define the following elements of U_3:

$$\sigma_a := e_{12}, \qquad \sigma_b := e_{23}, \qquad \tau := e_{13} = [\sigma_a,\sigma_b].$$

Suppose given $x \in F_a^\times$ such that

$$(\sigma_a - 1)x = \frac{b}{\alpha^p}. \tag{3.1}$$

The étale F-algebra $K := (F_{a,b})_x$ has the structure of a Galois U_3-algebra such that the Galois $(\mathbb{Z}/p\mathbb{Z})^2$-algebra K^{Q_3} is equal to $F_{a,b}$, and

$$(\sigma_a - 1)x^{1/p} = \frac{b^{1/p}}{\alpha}, \qquad (\sigma_b - 1)x^{1/p} = 1, \qquad (\tau - 1)x^{1/p} = \zeta^{-1}. \tag{3.2}$$

Similarly, suppose given $y \in F_b^\times$ such that

$$(\sigma_b - 1)y = \frac{a}{\beta^p}. \tag{3.3}$$

The étale F-algebra $K := (F_{a,b})_y$ has the structure of a Galois U_3-algebra, such that the Galois $(\mathbb{Z}/p\mathbb{Z})^2$-algebra K^{Q_3} is equal to $F_{a,b}$, and

$$(\sigma_a - 1)y^{1/p} = 1, \qquad (\sigma_b - 1)y^{1/p} = \frac{a^{1/p}}{\beta}, \qquad (\tau - 1)y^{1/p} = \zeta. \tag{3.4}$$

In (3.2) and (3.4), the relation involving τ follows from the first two.

If $x \in F_a^\times$ satisfies (3.1), then so does ax. We may thus apply (3.2) to $(F_{a,b})_{ax}$. Therefore $(F_{a,b})_{ax}$ has the structure of a Galois U_3-algebra, where U_3 acts via $\overline{U}_3 = \mathrm{Gal}(F_{a,b}/F)$ on $F_{a,b}$, and

$$(\sigma_a - 1)(ax)^{1/p} = \frac{b^{1/p}}{\alpha}, \qquad (\sigma_b - 1)(ax)^{1/p} = 1, \qquad (\tau - 1)(ax)^{1/p} = \zeta^{-1}.$$

Similarly, if $y \in F_b^\times$ satisfies (3.3), we may apply (3.4) to $(F_{a,b})_{by}$. Therefore $(F_{a,b})_{by}$ admits a Galois U_3-algebra structure, where U_3 acts via $\overline{U}_3 = \mathrm{Gal}(F_{a,b}/F)$ on $F_{a,b}$, and

$$(\sigma_a - 1)(by)^{1/p} = 1, \qquad (\sigma_b - 1)(by)^{1/p} = \frac{a^{1/p}}{\beta}, \qquad (\tau - 1)(by)^{1/p} = \zeta.$$

Lemma 3.1. *(1) Let $x \in F_a^\times$ satisfy (3.1), and consider the Galois U_3-algebras $(F_{a,b})_x$ and $(F_{a,b})_{ax}$ as in (3.2). Then $(F_{a,b})_x \simeq (F_{a,b})_{ax}$ as Galois U_3-algebras.*

(2) Let $y \in F_b^\times$ satisfy (3.1), and consider the Galois U_3-algebras $(F_{a,b})_y$ and $(F_{a,b})_{by}$ as in (3.4). Then $(F_{a,b})_y \simeq (F_{a,b})_{by}$ as Galois U_3-algebras.

Proof. (1) The automorphism $\sigma_b \colon F_{a,b} \to F_{a,b}$ extends to an isomorphism of étale algebras $f \colon (F_{a,b})_x \to (F_{a,b})_{ax}$ by sending $x^{1/p}$ to $(ax)^{1/p}a^{-1/p}$. The map f is well defined because $f(x^{1/p})^p = x = [(ax)^{1/p}a^{-1/p}]^p$. We check that it is U_3-equivariant. This is true on $F_{a,b}$ because $\sigma_a\sigma_b = \sigma_b\sigma_a$ on $F_{a,b}$. Moreover,

$$\begin{aligned}\sigma_a(f(x^{1/p})) &= \sigma_a((ax)^{1/p}) \cdot \sigma_a(a^{-1/p}) = (b^{1/p}/\alpha)(ax)^{1/p} \cdot \zeta a^{-1/p} \\ &= (\zeta b^{1/p}/\alpha) \cdot (ax)^{1/p}a^{-1/p} = f((b^{1/p}/\alpha)(x^{1/p})) = f(\sigma_a(x^{1/p}))\end{aligned}$$

and

$$\sigma_b(f(x^{1/p})) = \sigma_b((ax)^{1/p}) \cdot \sigma_b(a^{-1/p}) = (ax)^{1/p}a^{-1/p} = f(x^{1/p}) = f(\sigma_b(x^{1/p})).$$

Thus f is U_3-equivariant, as desired.

(2) The proof is similar to that of (1). □

Proposition 3.2. *Let $a, b \in F^\times$ be such that $(a, b) = 0$ in $\mathrm{Br}(F)$, and fix $\alpha \in F_a^\times$ and $\beta \in F_b^\times$ such that $N_a(\alpha) = b$ and $N_b(\beta) = a$.*

(1) Every Galois U_3-algebra K over F such that $K^{Q_3} \simeq F_{a,b}$ as $(\mathbb{Z}/p\mathbb{Z})^2$-algebras is of the form $(F_{a,b})_x$ for some $x \in F_a^\times$ as in (3.1), with U_3-action given by (3.2).

(2) Every Galois U_3-algebra K over F such that $K^{Q_3} \simeq F_{a,b}$ as $(\mathbb{Z}/p\mathbb{Z})^2$-algebras is of the form $(F_{a,b})_y$ for some $y \in F_b^\times$ as in (3.3), with U_3-action given by (3.4).

(3) Let $(F_{a,b})_x$ and $(F_{a,b})_y$ be Galois U_3-algebras as in (3.2) and (3.4), respectively. The Galois U_3-algebras $(F_{a,b})_x$ and $(F_{a,b})_y$ are isomorphic if and only if there exists $w \in F_{a,b}^\times$ such that

$$w^p = xy, \qquad (\sigma_a - 1)(\sigma_b - 1)w = \zeta.$$

Proof. (1) Since $Q_3 = \langle \tau \rangle \simeq \mathbb{Z}/p\mathbb{Z}$ and $K^{Q_3} \simeq F_{a,b}$ as $(\mathbb{Z}/p\mathbb{Z})^2$-algebras, we have an isomorphism of étale $F_{a,b}$-algebras $K \simeq (F_{a,b})_z$, for some $z \in F_{a,b}^\times$ such that $(\tau - 1)z^{1/p} = \zeta^{-1}$. We may suppose that $K = (F_{a,b})_z$. As τ commutes with σ_b we have

$$(\tau - 1)(\sigma_b - 1)z^{1/p} = (\sigma_b - 1)(\tau - 1)z^{1/p} = (\sigma_b - 1)\zeta^{-1} = 1,$$

hence $(\sigma_b - 1)z^{1/p} \in F_{a,b}^\times$. By Hilbert's Theorem 90 for the extension $F_{a,b}/F_a$, there is $t \in F_{a,b}^\times$ such that $(\sigma_b - 1)z^{1/p} = (\sigma_b - 1)t$. Replacing z by zt^{-p}, we may thus assume that $(\sigma_b - 1)z^{1/p} = 1$. In particular, $z \in F_a^\times$. Since $(\tau - 1)z^{1/p} = \zeta^{-1}$, we have $\sigma_b\sigma_a(z^{1/p}) = \zeta\sigma_a\sigma_b(z^{1/p})$. Thus

$$(\sigma_b - 1)(\sigma_a - 1)z^{1/p} = (\sigma_b\sigma_a - \sigma_a\sigma_b + (\sigma_a - 1)(\sigma_b - 1))z^{1/p} = \zeta(\sigma_a - 1)(\sigma_b - 1)z^{1/p} = \zeta,$$

and hence $(\sigma_a - 1)z^{1/p} = b^{1/p}/\alpha'$ for some $\alpha' \in F_a^\times$. Moreover $N_a(\alpha'/\alpha) = b/b = 1$, and so by Hilbert's Theorem 90 there exists $\theta \in F_a^\times$ such that $\alpha'/\alpha = (\sigma_a - 1)\theta$. We define $x := z\theta^p \in F_a^\times$, and set $x^{1/p} := z^{1/p}\theta \in (F_{a,b})_z^\times$. Then $K = (F_{a,b})_x$, where

$$(\sigma_a - 1)x^{1/p} = (\sigma_a - 1)w \cdot (\sigma_a - 1)\theta = \frac{b^{1/p}}{\alpha'} \cdot \frac{\alpha'}{\alpha} = \frac{b^{1/p}}{\alpha}$$

and $(\sigma_b - 1)x^{1/p} = 1$, as desired.

(2) The proof is analogous to that of (1).

(3) Suppose given an isomorphism of Galois U_3-algebras between $(F_{a,b})_x$ and $(F_{a,b})_y$. Let $t \in (F_{a,b})_x$ be the image of $y^{1/p}$ under the isomorphism and set

$$w' := x^{1/p}t \in (F_{a,b})_x.$$

Set $y' := t^p$. We have $(\tau - 1)w' = \zeta^{-1} \cdot \zeta = 1$, and hence $w' \in F_{a,b}^\times$. We have $(w')^p = xy'$. Since F_b coincides with the $\langle \sigma_a, \tau \rangle$-invariant subalgebra of $(F_{a,b})_x$ and $(F_{a,b})_y$, the isomorphism $(F_{a,b})_y \to (F_{a,b})_x$ restricts to an isomorphism of Galois $\mathbb{Z}/p\mathbb{Z}$-algebras $F_b \to F_b$. Since the automorphism group of F_b as a Galois $(\mathbb{Z}/p\mathbb{Z})$-algebra is $\mathbb{Z}/p\mathbb{Z}$, generated by σ_b, this isomorphism $F_b \to F_b$ is equal to σ_b^i for some $i \geq 0$. Thus $y' = \sigma_b^i(y)$. Define

$$w := (w'a^{i/p}) / \prod_{j=0}^{i} \sigma_b^j(\beta) \in F_{a,b}^\times.$$

We have

$$(1 - \sigma_b^i)y = (\sum_{j=0}^{i} \sigma_b^j(1 - \sigma_b))y = a^i / (\prod_{j=0}^{i} \sigma_b^j(\beta^p)) = w^p/(w')^p.$$

Therefore

$$w^p = (w')^p(1 - \sigma_b^i)y = x\sigma_b^i(y)(1 - \sigma_b^i)y = xy. \tag{3.5}$$

We have $(\sigma_b - 1)x^{1/p} = 1$ and

$$(\sigma_a - 1)(\sigma_b - 1)t = (\sigma_a - 1)(\sigma_b - 1)y^{1/p} = (\sigma_a - 1)(a^{1/p}/\beta) = \zeta,$$

therefore

$$(\sigma_a - 1)(\sigma_b - 1)w' = (\sigma_a - 1)(\sigma_b - 1)t = \zeta.$$

Since $(\sigma_a - 1)(\sigma_b - 1)a^{1/p} = 1$ and $(\sigma_a - 1)(\sigma_b - 1)\beta = 1$, we conclude that

$$(\sigma_a - 1)(\sigma_b - 1)w = (\sigma_a - 1)(\sigma_b - 1)w' = 1. \tag{3.6}$$

Putting (3.5) and (3.6) together, we see that w satisfies the conditions of (3).

Conversely, suppose given $w' \in F_{a,b}^\times$ such that

$$xy = (w')^p, \qquad (\sigma_a - 1)(\sigma_b - 1)w' = \zeta.$$

Claim 3.3. There exists $w \in F_{a,b}^\times$ such that

$$xy = w^p, \qquad (\sigma_a - 1)w = \zeta^{-i}\frac{b^{1/p}}{\alpha}, \qquad (\sigma_b - 1)w = \zeta^{-j}\frac{a^{1/p}}{\beta}$$

for some integers i and j.

Proof of Claim 3.3. We first find $\eta_a \in F_a^\times$ such that

$$\eta_a^p = 1, \qquad (\sigma_a - 1)(w'/\eta_a) = \zeta^{-i}\frac{b^{1/p}}{\alpha}. \tag{3.7}$$

We have

$$(\sigma_a - 1)(w')^p = (\sigma_a - 1)x = \frac{b}{\alpha^p}.$$

Let

$$\zeta_a := (\sigma_a - 1)w' \cdot \alpha \cdot b^{-1/p} \in F_{a,b}^\times.$$

We have $\zeta_a^p = 1$. Moreover, $(\sigma_b - 1)\zeta_a = \zeta \cdot 1 \cdot \zeta^{-1} = 1$, that is, ζ_a belongs to $F_a^\times$. If F_a is a field, this implies that $\zeta_a = \zeta^i$ for some integer i, and (3.7) holds for $\eta_a = 1$.

Suppose that F_a is not a field. Then $F_a \simeq F^p$, where σ_a acts by cyclically permuting the coordinates:

$$\sigma_a(x_1, x_2, \dots, x_p) = (x_2, \dots, x_p, x_1).$$

We have $\zeta_a = (\zeta_1, \dots, \zeta_p)$ in $F_a = F^p$, where $\zeta_i \in F^\times$ is a p-th root of unity for all i. We have $N_a(\zeta_a) = N_a(\alpha)/b = 1$, and so $\zeta_1 \cdots \zeta_p = 1$. Inductively define $\eta_1 := 1$ and $\eta_{i+1} := \zeta_i\eta_i$ for all $i = 1, \dots, p-1$. Then

$$\eta_1/\eta_p = (\eta_1/\eta_2) \cdot (\eta_2/\eta_3) \cdots (\eta_{p-1}/\eta_p) = \zeta_1^{-1}\zeta_2^{-1} \cdots \zeta_{p-1}^{-1} = \zeta_p.$$

Therefore the element $\eta_a := (\eta_1, \dots, \eta_p) \in F^p = F_a$ satisfies $\eta_a^p = 1$ and

$$(\sigma_a - 1)\eta_a = (\eta_2/\eta_1, \dots, \eta_p/\eta_{p-1}, \eta_1/\eta_p) = (\zeta_1, \dots, \zeta_{p-1}, \zeta_p) = \zeta_a.$$

Thus

$$\eta_a^p = 1, \qquad (\sigma_a - 1)(w'/\eta_a) = (\sigma_a - 1)w' \cdot \zeta_a^{-1} = \frac{b^{1/p}}{\alpha}.$$

Independently of whether F_a is a field or not, we have found η_a satisfying (3.7).

Similarly, we construct $\eta_b \in F_b^\times$ such that

$$\eta_b^p = 1, \qquad (\sigma_b - 1)(w'/\eta_b) = \zeta^{-j}\frac{a^{1/p}}{\beta}, \tag{3.8}$$

for some integer j. Set $w := w'/(\eta_a\eta_b) \in F_{a,b}^\times$. Putting together (3.7) and (3.8), we deduce that w satisfies the conclusion of Claim 3.3. □

Let $w \in F_{a,b}^\times$ be as in Claim 3.3. By Lemma 3.1(1), applied i times, the Galois U_3-algebra $(F_{a,b})_x$ is isomorphic to $(F_{a,b})_{a^i x}$, where

$$(\sigma_a - 1)(a^i x)^{1/p} = \frac{b^{1/p}}{\alpha}, \qquad (\sigma_b - 1)(a^i x)^{1/p} = 1,$$

By Lemma 3.1(2), applied j times, the Galois U_3-algebra $(F_{a,b})_y$ is isomorphic to $(F_{a,b})_{b^j y}$, where

$$(\sigma_a - 1)(b^j y)^{1/p} = 1, \qquad (\sigma_b - 1)(b^j y)^{1/p} = \frac{a^{1/p}}{\beta}.$$

It thus suffices to construct an isomorphism of U_3-algebras $(F_{a,b})_{a^i x} \simeq (F_{a,b})_{b^j y}$. Let

$$\tilde{w} \coloneqq w a^{i/p} b^{j/p} \in F_{a,b}^\times,$$

so that

$$(\sigma_a - 1)\tilde{w} = \frac{a^{1/p}}{\beta}, \qquad (\sigma_b - 1)\tilde{w} = \frac{b^{1/p}}{\alpha}.$$

Let $f\colon (F_{a,b})_{a^i x} \to (F_{a,b})_{b^j y}$ be the isomorphism of étale algebras which is the identity on $F_{a,b}$ and sends $(a^i x)^{1/p}$ to $\tilde{w}/(b^j y)^{1/p}$. Note that f is well defined because

$$(\tilde{w})^p = w a^i b^j = (a^i x)(b^j y).$$

Moreover,

$$(\sigma_a - 1)(\tilde{w}/(b^j y)^{1/p}) = \frac{a^{1/p}}{\beta} = (\sigma_a - 1)(a^i x)^{1/p},$$

$$(\sigma_b - 1)(\tilde{w}/(b^j y)^{1/p}) = \frac{b^{1/p}}{\alpha} \cdot \frac{\alpha}{b^{1/p}} = 1 = (\sigma_b - 1)(a^i x)^{1/p},$$

and hence f is U_3-equivariant. □

3.2. **Galois $\overline{U}_4$-algebras.** Let $a, b, c \in F^\times$ be such that $(a, b) = (b, c) = 0$ in $\mathrm{Br}(F)$. By Lemma 2.2, we may fix $\alpha \in F_a^\times$ and $\gamma \in F_c^\times$ be such that $N_a(\alpha) = N_c(\gamma) = b$. We have $\mathrm{Gal}(F_{a,b,c}/F) = \langle \sigma_a, \sigma_b, \sigma_c \rangle$. The projection map $\overline{U}_4 \to (\mathbb{Z}/p\mathbb{Z})^3$ is given by $\overline{e}_{12} \mapsto \sigma_a$, $\overline{e}_{23} \mapsto \sigma_b$, $\overline{e}_{34} \mapsto \sigma_c$. Its kernel $\overline{Q}_4 \subset \overline{U}_4$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$, generated by $\overline{e}_{13}$ and $\overline{e}_{24}$. We define the following elements of $\overline{U}_4$:

$$\sigma_a \coloneqq \overline{e}_{12}, \qquad \sigma_b \coloneqq \overline{e}_{23}, \qquad \sigma_c \coloneqq \overline{e}_{34}, \qquad \tau_{ab} \coloneqq \overline{e}_{13}, \qquad \tau_{bc} \coloneqq \overline{e}_{24}.$$

Let $x \in F_a^\times$ and $z \in F_c^\times$ be such that

$$(\sigma_a - 1)x = \frac{b}{\alpha^p}, \qquad (\sigma_c - 1)z = \frac{b}{\gamma^p}, \tag{3.9}$$

and consider the Galois $\overline{U}_4$-algebra $K \coloneqq (F_{a,b,c})_{x,z}$, where $\overline{U}_4$ acts on $F_{a,b,c}$ via the surjection onto $\mathrm{Gal}(F_{a,b,c}/F)$, and

$$(\sigma_a - 1)x^{1/p} = \frac{b^{1/p}}{\alpha}, \qquad (\sigma_b - 1)x^{1/p} = 1, \qquad (\sigma_c - 1)x^{1/p} = 1, \tag{3.10}$$

$$(\tau_{ab} - 1)x^{1/p} = \zeta^{-1}, \qquad (\tau_{bc} - 1)x^{1/p} = 1, \tag{3.11}$$

$$(\sigma_a - 1)(x')^{1/p} = 1, \qquad (\sigma_b - 1)(x')^{1/p} = 1, \qquad (\sigma_c - 1)(x')^{1/p} = \frac{b^{1/p}}{\gamma}, \tag{3.12}$$

$$(\tau_{ab} - 1)(x')^{1/p} = 1, \qquad (\tau_{bc} - 1)(x')^{1/p} = \zeta. \tag{3.13}$$

Note that (3.11) follows from (3.10) and (3.13) follows from (3.12). We leave to the reader to check that the relations (2.8)-(2.12) are satisfied.

Proposition 3.4. *Let $a,b,c \in F^\times$ be such that $(a,b)=(b,c)=0$ in $\mathrm{Br}(F)$. Fix $\alpha \in F_a^\times$ and $\gamma \in F_c^\times$ such that $N_a(\alpha)=N_c(\gamma)=b$. Let K be a Galois $\overline{U}_4$-algebra such that $K^{\overline{Q}_4} \simeq F_{a,b,c}$ as $(\mathbb{Z}/p\mathbb{Z})^3$-algebras. Then there exist $x \in F_a^\times$ and $x' \in F_c^\times$ such that $K \simeq (F_{a,b,c})_{x,x'}$ as Galois $\overline{U}_4$-algebras, where $\overline{U}_4$ acts on $(F_{a,b,c})_{x,x'}$ by (3.10)-(3.13).*

Proof. Let H (resp. H') be the subgroup of $\overline{U}_4$ generated by σ_c and τ_{bc} (resp. σ_b and τ_{ab}), and let S be the subgroup of $\overline{U}_4$ generated by H and H'. Note that K^H is a Galois U_3-algebra over F such that $(K^H)^{Q_3} \simeq F_{a,b}$ as $(\mathbb{Z}/p\mathbb{Z})^2$-algebras and $K^S \simeq F_b$ as $(\mathbb{Z}/p\mathbb{Z})$-algebras. Thus by Proposition 3.2(1) there exists $x \in F_a^\times$ such that $K^H \simeq (F_{a,b})_x$ as Galois U_3-algebras. Similarly, by Proposition 3.2(2) there exists $x' \in F_c^\times$ such that $K^{H'} \simeq (F_{b,c})_{x'}$ as Galois U_3-algebras. Therefore x satisfies (3.10) and x' satisfies (3.12). We apply Lemma 2.1(2) to (2.14). We obtain the isomorphisms of $\overline{U}_4$-algebras

$$K \simeq K^H \otimes_{K^S} K^{H'} \simeq (F_{a,b,c})_{x,x'},$$

where $(F_{a,b,c})_{x,x'}$ is the $\overline{U}_4$-algebra given by (3.10) and (3.12). □

3.3. **Galois U_4-algebras.** Let $a,b,c \in F^\times$, and suppose that $(a,b)=(b,c)=0$ in $\mathrm{Br}(F)$. We write $(\mathbb{Z}/p\mathbb{Z})^3 = \langle \sigma_a, \sigma_b, \sigma_c \rangle$ and view $F_{a,b,c}$ as a Galois $(\mathbb{Z}/p\mathbb{Z})^3$-algebra over F as in Section 2.1. The quotient map $U_4 \to (\mathbb{Z}/p\mathbb{Z})^3$ is given by $e_{12} \mapsto \sigma_a$, $e_{23} \mapsto \sigma_b$ and $e_{34} \mapsto \sigma_c$. The kernel Q_4 of this map is generated by e_{13}, e_{24} and e_{14} and is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$. We define the following elements of U_4:

$$\sigma_a \coloneqq e_{12}, \qquad \sigma_b \coloneqq e_{23}, \qquad \sigma_c \coloneqq e_{34},$$

$$\tau_{ab} \coloneqq e_{13} = [\sigma_a, \sigma_b], \qquad \tau_{bc} \coloneqq e_{24} = [\sigma_b, \sigma_c], \qquad \rho \coloneqq e_{14} = [\sigma_a, \tau_{bc}] = [\tau_{ab}, \sigma_c].$$

Proposition 3.5. *Let $a,b,c \in F^\times$ be such that $(a,b)=(b,c)=0$ in $\mathrm{Br}(F)$. Let $\alpha \in F_a^\times$ and $\gamma \in F_c^\times$ be such that $N_a(\alpha)=b$ and $N_c(\gamma)=b$. Let K be a Galois $\overline{U}_4$-algebra such that $K^{\overline{Q}_4} \simeq F_{a,b,c}$ as $(\mathbb{Z}/p\mathbb{Z})^3$-algebras.*

There exists a Galois U_4-algebra L over F such that $L^{Z_4} \simeq K$ as $\overline{U}_4$-algebras if and only if there exist $u,u' \in F_{a,c}^\times$ such that

$$\alpha \cdot (\sigma_a - 1)u = \gamma \cdot (\sigma_c - 1)u'.$$

and such that K is isomorphic to the Galois $\overline{U}_4$-algebra $(F_{a,b,c})_{x,x'}$ determined by (3.10)-(3.13), where $x = N_c(u) \in F_a^\times$ and $x' = N_a(u') \in F_c^\times$.

Proof. Suppose that $K = (F_{a,b,c})_{x,x'}$, with $\overline{U}_4$-action determined by (3.10)-(3.13). Let L be a Galois U_4-algebra over F be such that $L^{Z_4} = K$, and let $y \in K^\times$ be such that $L = K_y$.

We have $\mathrm{Gal}(L/F_{a,b,c}) = Q_4 = \langle \tau_{ab}, \tau_{bc}, \rho \rangle \simeq (\mathbb{Z}/p\mathbb{Z})^3$, and hence one may choose y in $F_{a,b,c}^\times$ and such that

$$(\tau_{ab} - 1)y^{1/p} = 1, \qquad (\tau_{bc} - 1)y^{1/p} = 1, \qquad (\rho - 1)y^{1/p} = \zeta^{-1}.$$

The element σ_b commutes with τ_{ab}, τ_{bc} and ρ. Hence

$$\tau_{ab}(\sigma_b - 1)(y^{1/p}) = (\sigma_b - 1)\tau_{ab}(y^{1/p}) = (\sigma_b - 1)(y^{1/p}).$$

Similarly
$$\tau_{bc}(\sigma_b-1)(y^{1/p})=(\sigma_b-1)(y^{1/p})$$
and
$$\rho(\sigma_b-1)(y^{1/p})=(\sigma_b-1)(\zeta\cdot y^{1/p})=(\sigma_b-1)(y^{1/p}).$$
It follows that $(\sigma_b-1)(y^{1/p})\in F^\times_{a,b,c}$. By Hilbert's Theorem 90, applied to $F_{a,b,c}/F_{a,c}$, there is $q\in F^\times_{a,b,c}$ such that $(\sigma_b-1)(y^{1/p})=(\sigma_b-1)q$. Replacing y by y/q^p, we may assume that $\sigma_b(y^{1/p})=y^{1/p}$. In particular, $y\in F^\times_{a,c}$. We have:
$$\rho(\sigma_a-1)(y^{1/p})=(\sigma_a-1)\rho(y^{1/p})=(\sigma_a-1)(\zeta^{-1}\cdot y^{1/p})=(\sigma_a-1)(y^{1/p}),$$
$$\sigma_b(\sigma_a-1)(y^{1/p})=(\sigma_a\sigma_b{\tau_{ab}}^{-1}-\sigma_b)(y^{1/p})=(\sigma_a-1)(y^{1/p}),$$
$$\tau_{ab}(\sigma_a-1)(y^{1/p})=(\sigma_a-1)\tau_{ab}(y^{1/p})=(\sigma_a-1)(y^{1/p}),$$
$$\tau_{bc}(\sigma_a-1)(y^{1/p})=(\rho^{-1}\sigma_a-1)\tau_{bc}(y^{1/p})=(\sigma_a\rho^{-1}-1)(y^{1/p})=\zeta\cdot(\sigma_a-1)(y^{1/p}).$$
By (3.12)-(3.13), analogous identities are satisfied by $(x')^{1/p}$:
$$(\rho-1)(x')^{1/p}=(\sigma_b-1)(x')^{1/p}=(\tau_{ab}-1)(x')^{1/p}=1,\qquad(\tau_{bc}-1)(x')^{1/p}=\zeta.$$
Therefore
$$(\sigma_a-1)(y^{1/p})=\frac{(x')^{1/p}}{u'}$$
for some $u'\in F^\times_{a,c}$. In particular, $x'=N_a(u')$. A similar computation shows that
$$(\sigma_c-1)(y^{1/p})=\frac{x^{1/p}}{u}$$
for some $u\in F^\times_{a,c}$. In particular, $x=N_c(u)$. In addition,
$$\frac{b^{1/p}}{\alpha}=(\sigma_a-1)(x^{1/p})=(\sigma_a-1)[u\cdot(\sigma_c-1)(y^{1/p})],$$
$$\frac{b^{1/p}}{\gamma}=(\sigma_c-1)((x')^{1/p})=(\sigma_c-1)[u'\cdot(\sigma_a-1)(y^{1/p})].$$
Therefore
$$\alpha\cdot(\sigma_a-1)u=\gamma\cdot(\sigma_c-1)u'.$$
Conversely, suppose given $u,u'\in F^\times_{a,c}$ such that
$$\alpha\cdot(\sigma_a-1)u=\gamma\cdot(\sigma_c-1)u',\qquad x=N_c(u),\qquad x'=N_a(u').$$
Then
$$(\sigma_a-1)x=(\sigma_a-1)N_c(u)=N_c(\sigma_a-1)u=N_c\left(\frac{\gamma}{\alpha}\right)=\frac{b}{\alpha^p},$$
$$(\sigma_c-1)x'=(\sigma_c-1)N_a(u')=N_a(\sigma_c-1)u'=N_a\left(\frac{\alpha}{\gamma}\right)=\frac{b}{\gamma^p}.$$
We have
$$N_c\left(\frac{x}{u^p}\right)=\frac{N_c(x)}{N_c(u^p)}=\frac{x^p}{x^p}=1,$$
$$N_a\left(\frac{x'}{(u')^p}\right)=\frac{N_a(x')}{N_a((u')^p)}=\frac{(x')^p}{(x')^p}=1,$$
$$(\sigma_a-1)\left(\frac{x}{u^p}\right)=\frac{b}{\alpha^p\cdot(\sigma_a-1)u^p}=\frac{b}{\gamma^p\cdot(\sigma_c-1)(u')^p}=(\sigma_c-1)\left(\frac{x'}{(u')^p}\right).$$

By Hilbert's Theorem 90 applied to $F_{a,c}/F$, there is $y \in F_{a,c}^{\times}$ such that

$$(\sigma_a - 1)y = \frac{x'}{(u')^p} \quad \text{and} \quad (\sigma_c - 1)y = \frac{x}{u^p}.$$

We consider the étale F-algebra $L \coloneqq K_y$ and make it into a Galois U_4-algebra such that $L^{Z_4} = K$. It suffices to describe the U_4-action on $y^{1/p}$. We set:

$$(\sigma_a - 1)(y^{1/p}) = \frac{(x')^{1/p}}{u'}, \quad (\sigma_b - 1)(y^{1/p}) = 1, \quad (\sigma_c - 1)(y^{1/p}) = \frac{x^{1/p}}{u},$$

One checks that this definition is compatible with the relations (2.4)-(2.7), and hence that it makes L into a Galois U_4-algebra such that $L^{Z_4} = K$. □

We use Proposition 3.5 to give an alternative proof for the Massey Vanishing Conjecture for $n = 3$ and arbitrary p.

Proposition 3.6. *Let p be a prime, let F be a field, and let $\chi_1, \chi_2, \chi_3 \in H^1(F, \mathbb{Z}/p\mathbb{Z})$. The following are equivalent.*

1. *(1) We have $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$ in $H^2(F, \mathbb{Z}/p\mathbb{Z})$.*
2. *(2) The Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle \subset H^2(F, \mathbb{Z}/p\mathbb{Z})$ is defined.*
3. *(3) The Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle \subset H^2(F, \mathbb{Z}/p\mathbb{Z})$ vanishes.*

Proof. It is clear that (3) implies (2) and that (2) implies (1). We now prove that (1) implies (3). The first part of the proof is a reduction to the case when $\mathrm{char}(F) \neq p$ and F contains a primitive p-th root of unity, and follows [MT16, Proposition 4.14].

Consider the short exact sequence

$$1 \to Q_4 \to U_4 \to (\mathbb{Z}/p\mathbb{Z})^3 \to 1, \tag{3.14}$$

where the map $U_4 \to (\mathbb{Z}/p\mathbb{Z})^3$ comes from (2.13). Recall from the paragraph preceding Proposition 3.5 that the group Q_4 is abelian. Therefore, the homomorphism $\chi \coloneqq (\chi_1, \chi_2, \chi_3) \colon \Gamma_F \to (\mathbb{Z}/p\mathbb{Z})^3$ induces a pullback map

$$H^2((\mathbb{Z}/p\mathbb{Z})^3, Q_4) \to H^2(F, Q_4).$$

We let $A \in H^2(F, Q_4)$ be the image of the class of (3.14) under this map. By Theorem 2.4, for every finite extension F'/F the Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ vanishes over F' if and only if the restriction of χ to $\Gamma_{F'}$ lifts to U_4, and this happens if and only if A restricts to zero in $H^2(F', Q_4)$.

When $\mathrm{char}(F) = p$, we have $\mathrm{cd}(F) \leq 1$ by [Ser97, §2.2, Proposition 3]. Therefore $H^2(F, Q_4) = 0$ and hence $A = 0$. Thus (1) implies (3) when $\mathrm{char}(F) = p$.

Suppose that $\mathrm{char}(F) \neq p$. There exists an extension F'/F of prime-to-p degree such that F' contains a primitive p-th root of 1. If (1) implies (3) for F', then A restricts to zero in $H^2(F', Q_4)$. By a restriction-corestriction argument, we deduce that A vanishes, that is, (1) implies (3) for F. We may thus assume that F contains a primitive p-th root of unity ζ.

Let $a, b, c \in F^{\times}$ be such that $\chi_a = \chi_1$, $\chi_b = \chi_2$ and $\chi_c = \chi_3$ in $H^1(F, \mathbb{Z}/p\mathbb{Z})$. Since $(a, b) = (b, c) = 0$ in $\mathrm{Br}(F)$, there exists $\alpha \in F_a^{\times}$ and $\gamma \in F_c^{\times}$ such that $N_a(\alpha) = N_c(\gamma) = b$. Since $N_{ac}(\gamma/\alpha) = N_c(\gamma)/N_a(\alpha) = 1$ in $F_{ac}^{\times}$, by Hilbert's Theorem 90 there exists $t \in F_{a,c}^{\times}$ such that $\gamma/\alpha = (\sigma_a\sigma_c - 1)t$. Define $u, u' \in F_{a,c}^{\times}$ by $u \coloneqq \sigma_c(t)$ and $u' \coloneqq t^{-1}$. Then

$$\alpha \cdot (\sigma_a - 1)u = \alpha \cdot (\sigma_a\sigma_c - \sigma_c)t = \alpha \cdot (\sigma_a\sigma_c - 1)t \cdot (\sigma_c - 1)t^{-1} = \gamma \cdot (\sigma_c - 1)u'.$$

Let $x \coloneqq N_c(u) \in F_a^\times$ and $x' \coloneqq N_a(u') \in F_c^\times$. Since $\sigma_a\sigma_c = \sigma_c\sigma_a$ on $F_{a,c}^\times$, we have

$$(\sigma_a - 1)x = N_c((\sigma_a - 1)u) = N_c((\sigma_c - 1)u' \cdot (\gamma/\alpha)) = N_c(\gamma)/N_c(\alpha) = b/\alpha^p.$$

Similarly, $(\sigma_c - 1)x' = b/\gamma^p$. Therefore x, x' satisfy (3.9). Let $K \coloneqq (F_{a,b,c})_{x,x'}$ be the Galois $\overline{U}_4$-algebra over F, with the $\overline{U}_4$-action given by (3.10)-(3.13). By Proposition 3.4, there exists a Galois U_4-algebra L over F such that $L^{Z_4} \simeq (F_{a,b,c})_{x,x'}$ as $\overline{U}_4$-algebras. In particular, $L^{Q_4} \simeq F_{a,b,c}$ as $(\mathbb{Z}/p\mathbb{Z})^3$-algebras. By Corollary 2.5, we conclude that $\langle a, b, c\rangle$ vanishes. □

3.4. **Galois $\overline{U}_5$-algebras.** Let $a, b, c, d \in F^\times$. We write $(\mathbb{Z}/p\mathbb{Z})^4 = \langle \sigma_a, \sigma_b, \sigma_c, \sigma_d\rangle$ and regard $F_{a,b,c,d}$ as a Galois $(\mathbb{Z}/p\mathbb{Z})^4$-algebra over F as in Section 2.1.

Proposition 3.7. *Let $a, b, c, d \in F^\times$ be such that $(a, b) = (b, c) = (c, d) = 0$ in $\mathrm{Br}(F)$. Then the Massey product $\langle a, b, c, d\rangle$ is defined if and only if there exist $u \in F_{a,c}^\times$, $v \in F_{b,d}^\times$ and $w \in F_{b,c}^\times$ such that*

$$N_a(u) \cdot N_d(v) = w^p, \qquad (\sigma_b - 1)(\sigma_c - 1)w = \zeta.$$

Proof. Denote by U_4^+ and U_4^- the top-left and bottom-right 4×4 corners of U_5, respectively, and let $S \coloneqq U_4^+ \cap U_4^-$ be the middle subgroup U_3. Let Q_4^+ and Q_4^- be the kernel of the map $U_4^+ \to (\mathbb{Z}/p\mathbb{Z})^3$ and $U_4^- \to (\mathbb{Z}/p\mathbb{Z})^3$, respectively, and let P_4^+ and P_4^- be the kernel of the maps $U_4^+ \to U_3$ and $U_4^- \to U_3$, respectively.

Suppose $\langle a, b, c, d\rangle$ is defined. By Corollary 2.5, there exists a $\overline{U}_5$-algebra L such that $L^{\overline{Q}_5} \simeq F_{a,b,c,d}$ as $(\mathbb{Z}/p\mathbb{Z})^4$-algebras. Using Lemma 2.2, we fix $\alpha \in F_a^\times$ and $\gamma \in F_c^\times$ such that $N_a(\alpha) = b$ and $N_c(\gamma) = b$. By Proposition 3.5, there exist $u, u' \in F_{a,c}^\times$ such that, letting $x' \coloneqq N_c(u')$ and $x \coloneqq N_a(u)$, the $\overline{U}_4^+$-algebra K_1 induced by L is isomorphic to the $\overline{U}_4^+$-algebra $(F_{a,b,c})_{x',x}$, where $\overline{U}_4^+$ acts via (3.10)-(3.13), and where the roles of x and x' have been switched.

Similarly, there exist $v, v' \in F_{b,d}^\times$ such that, letting $z \coloneqq N_d(v)$ and $z' \coloneqq N_b(v')$, the $\overline{U}_4^-$-algebra K_2 induced by L is isomorphic to $(F_{b,c,d})_{z,z'}$. Since the U_3-algebras $(K_1)^{P_4^+}$ and $(K_2)^{P_4^-}$ are equal, by Proposition 3.2(3) there exists $w \in F_{b,c}^\times$ such that

$$N_a(u) \cdot N_d(v) = xz = w^p, \qquad (\sigma_b - 1)(\sigma_c - 1)w = \zeta.$$

Conversely, let $u \in F_{a,c}^\times$, $v \in F_{b,d}^\times$, and $w \in F_{b,c}^\times$ be such that

$$N_a(u) \cdot N_d(v) = w^p, \qquad (\sigma_b - 1)(\sigma_c - 1)w = \zeta.$$

By Lemma 2.2, there exist $\alpha \in F_a^\times$ and $\delta \in F_d^\times$ such that $N_a(\alpha) = b$ and $N_d(\delta) = c$. We may write

$$(\sigma_b - 1)w = \frac{c^{1/p}}{\beta}, \qquad (\sigma_c - 1)w = \frac{b^{1/p}}{\gamma}.$$

For some $\beta \in F_b^\times$ and $\gamma \in F_c^\times$. We have

$$N_a((\sigma_c - 1)u \cdot (\gamma/\alpha)) = (\sigma_c - 1)N_a(u) \cdot N_a(\gamma/\alpha) = (\sigma_c - 1)w^p \cdot (\gamma^p/b) = 1.$$

By Hilbert's Theorem 90, there is $u' \in F_{a,c}^\times$ such that

$$\alpha \cdot (\sigma_a - 1)u' = \gamma \cdot (\sigma_c - 1)u.$$

By Proposition 3.5, we obtain a Galois U_4^+-algebra K_1 over F with the property that $(K_1)^{Q_4^+} \simeq F_{a,b,c}$ as $(\mathbb{Z}/p\mathbb{Z})^3$-algebras. Similarly, we get a Galois U_4^--algebra over F such that $(K_2)^{Q_4^-} \simeq F_{b,c,d}$ as $(\mathbb{Z}/p\mathbb{Z})^3$-algebras. Since $N_a(u) \cdot N_d(v) = w^p$, by Proposition 3.2(3) the U_3-algebras $(K_1)^{P_4^+}$ and $(K_2)^{P_4^-}$ are isomorphic. Now Lemma 2.1 applied to the cartesian square (2.14) for $n = 4$ yields a $\overline{U}_5$-Galois algebra L such that $L^{Q_5} \simeq F_{a,b,c,d}$ as $(\mathbb{Z}/p\mathbb{Z})^4$-algebras. By Corollary 2.5, this implies that $\langle a, b, c, d\rangle$ is defined. □

Lemma 3.8. *Let $b, c \in F^\times$ and $w \in F_{b,c}^\times$. Then $(\sigma_b - 1)(\sigma_c - 1)w = 1$ if and only if there exist $w_b \in F_b^\times$ and $w_c \in F_c^\times$ such that $w = w_b w_c$ in $F_{b,c}^\times$.*

Proof. We have $(\sigma_b - 1)(\sigma_c - 1)(w_b w_c) = (\sigma_b - 1)w_c = 1$ for all $w_b \in F_b^\times$ and $w_c \in F_c^\times$. Conversely, if $w \in F_{b,c}^\times$ satisfies $(\sigma_b-1)(\sigma_c-1)w = 1$, then $(\sigma_c-1)w \in F_c^\times$ and $N_c((\sigma_c - 1)w) = 1$, and hence by Hilbert's Theorem 90 there exists $w_c \in F_c^\times$ such that $(\sigma_c - 1)w_c = (\sigma_c - 1)w$. Letting $w_b := w/w_c \in F_{b,c}^\times$, we have

$$(\sigma_c - 1)w_b = (\sigma_c - 1)(w/w_c) = 1,$$

that is, $w_b \in F_b^\times$. □

From Proposition 3.7, we derive the following necessary condition for a fourfold Massey product to be defined.

Proposition 3.9. *Let p be a prime, let F be a field of characteristic different from p and containing a primitive p-th root of unity ζ, let $a, b, c, d \in F^\times$, and suppose that $\langle a, b, c, d\rangle$ is defined over F. For every $w \in F_{b,c}^\times$ such that $(\sigma_b-1)(\sigma_c-1)w = \zeta$, there exist $u \in F_{a,c}^\times$ and $v \in F_{b,d}^\times$ such that $N_a(u)N_d(v) = w^p$.*

Proof. By Proposition 3.7, there exist $u_0 \in F_{a,c}^\times$, $v_0 \in F_{b,d}^\times$ and $w_0 \in F_{a,c}^\times$ such that

$$N_a(u_0)N_d(v_0) = w_0^p, \qquad (\sigma_b - 1)(\sigma_c - 1)w_0 = \zeta.$$

We have $(\sigma_b-1)(\sigma_c-1)(w_0/w) = 1$. By Lemma 3.8, this implies that $w_0 = w w_b w_c$, where $w_b \in F_b^\times$ and $w_c \in F_c^\times$. If we define $u = u_0 w_c$ and $v = v_0 w_b$, then

$$N_a(u)N_d(v) = N_a(u_0)N_a(w_c)N_d(v_0)N_d(w_b) = w_0^p w_c^p w_b^p = w^p.$$ □

4. A generic variety

In this section, we let p be a prime number, and we let F be a field of characteristic different from p and containing a primitive p-th root of unity ζ.

Let $b, c \in F^\times$, and let X be the Severi-Brauer variety associated to (b, c) over F; see [GS17, Chapter 5]. For every étale F-algebra K, we have $(b, c) = 0$ in $\mathrm{Br}(K)$ if and only if $X_K \simeq \mathbb{P}_K^{p-1}$ over K. In particular, $X_b \simeq \mathbb{P}_b^{p-1}$ over F_b. By [GS17, Theorem 5.4.1], the central simple algebra (b, c) is split over $F(X)$.

We define the degree map $\deg\colon \mathrm{Pic}(X) \to \mathbb{Z}$ as the composition of the pullback map $\mathrm{Pic}(X) \to \mathrm{Pic}(X_b) \simeq \mathrm{Pic}(\mathbb{P}_b^{p-1})$ and the degree isomorphism $\mathrm{Pic}(\mathbb{P}_b^{p-1}) \to \mathbb{Z}$. This does not depend on the choice of isomorphism $X_b \simeq \mathbb{P}_b^{p-1}$.

Lemma 4.1. *Let $b, c \in F^\times$, let $G_b := \mathrm{Gal}(F_b/F)$, and let X be the Severi-Brauer variety of (b, c) over F. Let $s_1, \dots, s_p$ be homogeneous coordinates on $\mathbb{P}_F^{p-1}$.*

(1) There exists a G_b-equivariant isomorphism $X_b \xrightarrow{\sim} \mathbb{P}_b^{p-1}$, where G_b acts on X_b via its action on F_b, and on $\mathbb{P}_b^{p-1}$ by

$$\sigma_b^*(s_1) = c s_p, \qquad \sigma_b^*(s_i) = s_{i-1} \quad (i = 2, \dots, p).$$

(2) If $(b, c) \neq 0$ in $\mathrm{Br}(F)$, the image of $\deg\colon \mathrm{Pic}(X) \to \mathbb{Z}$ is equal to $p\mathbb{Z}$.

(3) There exists a rational function $w \in F_{b,c}(X)^\times$ such that

$$(\sigma_b - 1)(\sigma_c - 1)w = \zeta$$

and

$$\operatorname{div}(w) = x - y \qquad \textit{in } \operatorname{Div}(X_{b,c}),$$

where $x, y \in (X_{b,c})^{(1)}$ satisfy $\deg(x) = \deg(y) = 1$, $\sigma_b(x) = x$ and $\sigma_c(y) = y$.

Proof. (1) Consider the 1-cocycle $z\colon G_b \to \mathrm{PGL}_p(F_b)$ given by

$$\sigma_b \mapsto \begin{bmatrix} 0 & 0 & \dots & 0 & c \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}.$$

By [GS17, Construction 2.5.1], the class $[z] \in H^1(G_b, \mathrm{PGL}_p(F_b))$ coincides with the class of the degree-p central simple algebra over F with Brauer class (b, c), and hence with the class of the associated Severi-Brauer variety X. It follows that we have a G_b-equivariant isomorphism $X_b \simeq \mathbb{P}^{p-1}_b$, where G_b acts on X_b via its action on F_b, and on $\mathbb{P}^{p-1}_b$ via the cocycle z. This proves (1).

(2) By a theorem of Lichtenbaum [GS17, Theorem 5.4.10], we have an exact sequence

$$\operatorname{Pic}(X) \xrightarrow{\deg} \mathbb{Z} \xrightarrow{\delta} \operatorname{Br}(F),$$

where $\delta(1) = (b, c)$. Since (b, c) has exponent p, we conclude that the image of deg is equal to $p\mathbb{Z}$.

(3) Let $G_{b,c} := \operatorname{Gal}(F_{b,c}/F) = \langle \sigma_b, \sigma_c \rangle$. By (1), there is a $G_{b,c}$-equivariant isomorphism $f\colon \mathbb{P}^{p-1}_{b,c} \to X_{b,c}$, where $G_{b,c}$ acts on $X_{b,c}$ via its action on $F_{b,c}$, the action of σ_c on $\mathbb{P}^{p-1}_{b,c}$ is trivial and the action of σ_b on $\mathbb{P}^{p-1}_{b,c}$ is determined by

$$\sigma_b^*(s_1) = cs_p, \qquad \sigma_b^*(s_i) = s_{i-1} \quad (i = 2, \dots, p).$$

Consider the linear form $l := \sum_{i=1}^p c^{i/p} \cdot s_i$ on $\mathbb{P}^{p-1}_{b,c}$ and set $w' := l/s_p \in F_{b,c}(\mathbb{P}^{p-1})^\times$. We have $\sigma_b^*(l) = c^{1/p} \cdot l$, and hence $(\sigma_b - 1)w' = c^{1/p} \cdot (s_p/s_{p-1})$. It follows that $(\sigma_c - 1)(\sigma_b - 1)w' = \xi$. Let $x', y' \in \operatorname{Div}(\mathbb{P}^{p-1}_{b,c})$ be the classes of linear subspaces of $\mathbb{P}^{p-1}_{b,c}$ given by $l = 0$ and $s_p = 0$, respectively. Then

$$\operatorname{div}(w') = x' - y', \qquad \sigma_b(x') = x', \qquad \sigma_c(y') = y'.$$

Define

$$w := w' \circ f^{-1} \in F_{b,c}(X)^\times, \qquad x' := f_*(x) \in (X_{b,c})^{(1)}, \qquad y' := f_*(y) \in (X_{b,c})^{(1)}.$$

Then w, x, y satisfy the conclusion of (3). □

Lemma 4.2. *Let $a, b, c, d \in F^\times$. The complex of tori*

$$R_{a,c}(\mathbb{G}_\mathrm{m}) \times R_{b,d}(\mathbb{G}_\mathrm{m}) \xrightarrow{\varphi} R_{b,c}(\mathbb{G}_\mathrm{m}) \xrightarrow{\psi} R_{b,c}(\mathbb{G}_\mathrm{m}),$$

where $\varphi(u, v) := N_a(u)N_d(v)$ and $\psi(z) = (\sigma_b - 1)(\sigma_c - 1)z$, is exact.

Proof. By Lemma 3.8, we have an exact sequence

$$R_c(\mathbb{G}_\mathrm{m}) \times R_b(\mathbb{G}_\mathrm{m}) \xrightarrow{\varphi'} R_{b,c}(\mathbb{G}_\mathrm{m}) \xrightarrow{\psi} R_{b,c}(\mathbb{G}_\mathrm{m}),$$

where $\varphi'(x,y) = xy$. The homomorphism φ factors as

$$R_{a,c}(\mathbb{G}_\mathrm{m}) \times R_{b,d}(\mathbb{G}_\mathrm{m}) \xrightarrow{N_a \times N_d} R_c(\mathbb{G}_\mathrm{m}) \times R_b(\mathbb{G}_\mathrm{m}) \xrightarrow{\varphi'} R_{b,c}(\mathbb{G}_\mathrm{m}).$$

Since the homomorphisms N_a and N_d are surjective, so is $N_a \times N_d$. We conclude that $\mathrm{Im}(\varphi) = \mathrm{Im}(\varphi') = \mathrm{Ker}(\psi)$, as desired. □

Let $a, b, c, d \in F^\times$, and consider the complex of tori of Lemma 4.2. We define the following groups of multiplicative type over F:

$$P \coloneqq R_{a,c}(\mathbb{G}_\mathrm{m}) \times R_{b,d}(\mathbb{G}_\mathrm{m}), \qquad S \coloneqq \mathrm{Ker}(\psi) = \mathrm{Im}(\varphi), \qquad T \coloneqq \mathrm{Ker}(\varphi) \subset P.$$

By Lemma 4.2, we get a short exact sequence

$$1 \to T \xrightarrow{\iota} P \xrightarrow{\pi} S \to 1, \tag{4.1}$$

where ι is the inclusion map and π is induced by φ.

Lemma 4.3. *The groups of multiplicative type T, P and S are tori.*

Proof. It is clear that P and S are tori. We now prove that T is a torus. Consider the subgroup $Q \subset R_{a,c}(\mathbb{G}_\mathrm{m})$ which makes the following commutative square cartesian:

$$\begin{array}{ccc} Q & \hookrightarrow & R_{a,c}(\mathbb{G}_\mathrm{m}) \\ \downarrow & & \downarrow N_a \\ \mathbb{G}_\mathrm{m} & \hookrightarrow & R_c(\mathbb{G}_\mathrm{m}). \end{array} \tag{4.2}$$

Here the bottom horizontal map is the obvious inclusion. It follows that Q is an $R_c(R^{(1)}_a(\mathbb{G}_\mathrm{m}))$-torsor over $\mathbb{G}_\mathrm{m}$, and hence it is smooth and connected. Therefore Q is a torus.

The image of the projection $T \xhookrightarrow{\iota} P \to R_{a,c}(\mathbb{G}_\mathrm{m})$ is contained in the torus Q. Moreover, the kernel U of the projection is $R_b(R^{(1)}_{F_{b,d}/F_b}(\mathbb{G}_\mathrm{m}))$, and hence it is also a torus. We have an exact sequence

$$1 \to U \to T \to Q.$$

We have $\dim(U) = p(p-1)$. From (4.1), we see that $\dim(T) = 2p^2 - 2p + 1$, and from (4.2) that $\dim(Q) = p^2 - p + 1$. Therefore $\dim(T) = \dim(U) + \dim(Q)$, and so the sequence

$$1 \to U \to T \to Q \to 1$$

is exact. As U and Q are tori, so is T. □

Proposition 4.4. *Let p be a prime, let F be a field of characteristic different from p and containing a primitive p-th root of unity ζ, and let $a, b, c, d \in F^\times$. Suppose that $(a,b) = (b,c) = (c,d) = 0$ in $\mathrm{Br}(F)$, and let $w \in F^\times_{b,c}$ be such that $(\sigma_b - 1)(\sigma_c - 1)w = \zeta$. Let T and P be the tori appearing in (4.1), and let $E_w \subset P$ be the T-torsor given by the equation $N_a(u)N_d(v) = w^p$. Then the mod p Massey product $\langle a, b, c, d\rangle$ is defined if and only if E_w is trivial.*

The construction of E_w is functorial in F. Therefore, for every field extension K/F, the mod p Massey product $\langle a,b,c,d\rangle$ is defined if and only if E_w is split by K. We may thus call E_w a generic variety for the property "the Massey product $\langle a,b,c,d\rangle$ is defined."

Proof. By Proposition 3.9, the Massey product $\langle a,b,c,d\rangle$ is defined over F if and only if there exist $u\in F_{a,c}^\times$ and $v\in F_{b,d}^\times$ such that the equation $N_a(u)N_d(v)=w^p$ has a solution over F, that is, if and only if the T-torsor E_w is trivial. □

Corollary 4.5. *Let p be a prime, let F be a field of characteristic different from p and containing a primitive p-th root of unity ζ, and let $a,b,c,d\in F^\times$. Let X be the Severi-Brauer variety of (b,c) over F, fix $w\in F_{b,c}(X)^\times$ as in Lemma 4.1(3), and let $E_w\subset P_{F(X)}$ be the $T_{F(X)}$-torsor given by the equation $N_a(u)N_d(v)=w^p$.*

Then $\langle a,b,c,d\rangle$ is defined over $F(X)$ if and only if E_w is trivial over $F(X)$.

Proof. This is a special case of Proposition 4.4, applied over the ground field $F(X)$. □

5. Proof of Theorem 1.3

Let p be a prime, and let F be a field of characteristic different from p and containing a primitive p-th root of unity ζ. Let $a,b,c,d\in F^\times$ be such that their cosets in $F^\times/F^{\times p}$ are $\mathbb{F}_p$-linearly independent. Consider the field $K := F_{a,b,c,d}$, and write $G=\mathrm{Gal}(K/F)=\langle\sigma_a,\sigma_b,\sigma_c,\sigma_d\rangle$ as in Section 2.1. We set $N_a:=\sum_{j=0}^{p-1}\sigma_a^j\in\mathbb{Z}[G]$. For every subgroup H of G, we also write N_a for the image of $N_a\in\mathbb{Z}[G]$ under the canonical map $\mathbb{Z}[G]\to\mathbb{Z}[G/H]$. We define N_b, N_c and N_d in a similar way.

Let

$$1\to T\xrightarrow{\iota} P\xrightarrow{\pi} S\to 1$$

be the short exact sequence of F-tori (4.1). It induces a short exact sequence of cocharacter G-lattices

$$0\to T_*\xrightarrow{\iota_*} P_*\xrightarrow{\pi_*} S_*\to 1.$$

By definition of P and S, we have

$$P_*=\mathbb{Z}[G/\langle\sigma_b,\sigma_d\rangle]\oplus\mathbb{Z}[G/\langle\sigma_a,\sigma_c\rangle],\qquad S_*=\langle N_b,N_c\rangle\subset\mathbb{Z}[G/\langle\sigma_a,\sigma_d\rangle].$$

Let X be the Severi-Brauer variety associated to $(b,c)\in\mathrm{Br}(F)$. Since $X_K\simeq\mathbb{P}^{p-1}_K$, the degree map $\mathrm{Pic}(X_K)\to\mathbb{Z}$ is an isomorphism, and so the map $\mathrm{Div}(X_K)\to\mathrm{Pic}(X_K)$ is identified with the degree map $\deg\colon\mathrm{Div}(X_K)\to\mathbb{Z}$. The sequence (B.2) for the torus T thus takes the form

$$1\to T(K)\to T(K(X))\xrightarrow{\mathrm{div}}\mathrm{Div}(X_K)\otimes T_*\xrightarrow{\deg} T_*\to 0,\tag{5.1}$$

where T_* denotes the cocharacter lattice of T.

Lemma 5.1. *(1) We have $(T_*)^G=\mathbb{Z}\cdot\eta$, where $\iota_*(\eta)=(N_aN_c,-N_bN_d)$ in $(P_*)^G$.*

(2) If $(b,c)\neq 0$ in $\mathrm{Br}(F)$, the image of $\deg\colon(\mathrm{Div}(X_{b,c})\otimes T_*)^G\to(T_*)^G$ is equal to $p(T_*)^G$.

Proof. (1) The free $\mathbb{Z}$-module $(P_*)^G$ has a basis consisting of the elements $(N_aN_c,0)$ and $(0,N_bN_d)$. The map $\pi_*\colon P_*\to S_*\subset\mathbb{Z}[G/\langle\sigma_a,\sigma_d\rangle]$ takes $(1,0)$ to N_b and $(0,1)$ to N_c. It follows that $\mathrm{Ker}(\pi_*)^G$ is generated by $(N_aN_c,-N_bN_d)$.

(2) By Lemma 4.1(2), the image of the composition

$$\mathrm{Div}(X)\otimes T_*^G=(\mathrm{Div}(X)\otimes T_*)^G\to(\mathrm{Div}(X_{b,c})\otimes T_*)^G\xrightarrow{\deg}(T_*)^G$$

is equal to $p(T_*)^G$. Thus the image of the degree map contains $p(T_*)^G$. We now show that the image the degree map is contained in $p(T_*)^G$.

For every $x\in X^{(1)}$, pick $x'\in(X_{b,c})^{(1)}$ lying over x, and write H_x for the G-stabilizer of x'. The injective homomorphisms of G-modules

$$j_x\colon \mathbb{Z}[G/H_x]\hookrightarrow\mathrm{Div}(X_{b,c}),\qquad gH_x\mapsto g(x')$$

yield an isomorphism of G-modules

$$\oplus_{x\in X^{(1)}}j_x\colon\ \oplus_{x\in X^{(1)}}\mathbb{Z}[G/H_x]\xrightarrow{\sim}\mathrm{Div}(X_{b,c}).$$

In order to conclude, it suffices to show that the image of

$$(T_*)^{H_x}=(\mathbb{Z}[G/H_x]\otimes T_*)^G\to(\mathrm{Div}(X_{b,c})\otimes T_*)^G\xrightarrow{\deg}(T_*)^G \tag{5.2}$$

is contained in $p(T_*)^G$ for all $x\in X^{(1)}$. Set $H:=H_x$.

The composition (5.2) takes a cocharacter $q\in(T_*)^H$ to

$$\deg(\sum_{gH\in G/H}gx'\otimes gq)=\deg(x')\cdot N_{G/H}(q).$$

Thus (5.2) coincides with the norm map $N_{G/H}$ times the degree of x'.

Suppose that $G=H$. Then $\deg(x')=\deg(x)$ and, since $(b,c)\neq 0$, the degree of x is divisible by p by Lemma 4.1(2).

Suppose that $G\neq H$. Then either $\langle\sigma_a,\sigma_c\rangle$ or $\langle\sigma_b,\sigma_d\rangle$ is not contained in H. Suppose $\langle\sigma_b,\sigma_d\rangle$ is not in H, and let N be the subgroup generated by H,σ_b,σ_d. Note that H is a proper subgroup of N.

The norm map $N_{G/H}:(T_*)^H\to(T_*)^G$ is the composition of the two norm maps

$$(T_*)^H\xrightarrow{N_{N/H}}(T_*)^N\xrightarrow{N_{G/N}}(T_*)^G.$$

Since $\mathbb{Z}[G/\langle\sigma_b,\sigma_d\rangle]^H=\mathbb{Z}[G/\langle\sigma_b,\sigma_d\rangle]^N$, the norm map $(T_*)^H\to(T_*)^N$ is multiplication by $[N:H]\in p\mathbb{Z}$ on the first component of T_* with respect to the inclusion ι_* of T_* into $P_*=\mathbb{Z}[G/\langle\sigma_b,\sigma_d\rangle]\oplus\mathbb{Z}[G/\langle\sigma_a,\sigma_c\rangle]$.

By Lemma 5.1(1), $(T_*)^G=\mathbb{Z}\cdot\eta$, where $\iota_*(\eta)=(N_aN_c,-N_bN_d)$ in $(P_*)^G$. Since N_aN_c is not divisible by p in $\mathbb{Z}[G/\langle\sigma_b,\sigma_d\rangle]$, the image of (5.2) is contained in $p\mathbb{Z}\cdot\eta=p(T_*)^G$, as desired. □

We write

$$\overline{\eta}\in\mathrm{Coker}[(\mathrm{Div}(X_{b,c})\otimes T_*)^G\xrightarrow{\deg}(T_*)^G]$$

for the coset of the generator $\eta\in(T_*)^G$ appearing in Lemma 5.1(1). If $(b,c)\neq 0$, then we have $\overline{\eta}\neq 0$ by Lemma 5.1(2). We consider the subgroup of unramified torsors

$$H^1(G,T(K(X)))_{\mathrm{nr}}:=\mathrm{Ker}[H^1(G,T(K(X)))\xrightarrow{\mathrm{div}}H^1(G,\mathrm{Div}(X_K\otimes T_*))],$$

and the homomorphism

$$\theta\colon H^1(G,T(K(X)))_{\mathrm{nr}}\to\mathrm{Coker}[\mathrm{Div}(X_K)\otimes T_*\xrightarrow{\deg}T_*],$$

which are defined in (B.3).

Lemma 5.2. *Let $b, c \in F^\times$ be such that $(b, c) \neq 0$ in $\mathrm{Br}(F)$, let $w \in F_{b,c}(X)^\times$ be such that $(\sigma_b - 1)(\sigma_c - 1)w = \zeta$ and $\mathrm{div}(w) = x - y$, where $\deg(x) = \deg(y) = 1$ and $\sigma_b(x) = x$ and $\sigma_c(y) = y$. Let $E_w \subset P_{F(X)}$ be the $T_{F(X)}$-torsor given by the equation $N_a(u)N_d(v) = w^p$, and write $[E_w]$ for the class of E_w in $H^1(G, T(K(X)))$.*

(1) We have $[E_w] \in H^1(G, T(K(X)))_{\mathrm{nr}}$.

(2) Let θ be the homomorphism of (B.3). We have $\theta([E_w]) = -\overline{\eta} \neq 0$.

Proof. The F-tori T, P and S of (4.1) are split by $K = F_{a,b,c,d}$. Therefore, we may consider diagram (B.6) for the short exact sequence (4.1), the splitting field K/F, and X the Severi-Brauer variety of (b, c) over F:

$$\begin{array}{ccccc}
 & & \mathrm{Div}((X_K) \otimes T_*)^G & \xrightarrow{\deg} & (T_*)^G \\
 & & \downarrow{\scriptstyle \iota_*} & & \downarrow{\scriptstyle \iota_*} \\
P(F(X)) & \xrightarrow{\mathrm{div}} & (\mathrm{Div}(X_K) \otimes P_*)^G & \xrightarrow{\deg} & (P_*)^G \\
\downarrow{\scriptstyle \pi_*} & & \downarrow{\scriptstyle \pi_*} & & \downarrow{\scriptstyle \pi_*} \\
S(F(X)) & \xrightarrow{\mathrm{div}} & (\mathrm{Div}(X_K) \otimes S_*)^G & \xrightarrow{\deg} & (S_*)^G \\
\downarrow{\scriptstyle \partial} & & \downarrow{\scriptstyle \partial} & & \\
H^1(G, T(K(X))) & \xrightarrow{\mathrm{div}} & H^1(G, \mathrm{Div}(X_K \otimes T_*)). & &
\end{array}$$

Since $(\sigma_b - 1)(\sigma_c - 1)w^p = 1$, we have $w^p \in S(F(X))$. The image of w^p under ∂ is equal to $[E_w] \in H^1(G, T(K(X)))$.

Let $H \subset G$ be the subgroup generated by σ_a and σ_d. The canonical isomorphism

$$\mathrm{Div}(X_{b,c}) = \mathrm{Div}(X_K)^H = (\mathrm{Div}(X_K) \otimes \mathbb{Z}[G/H])^G$$

sends the divisor $\mathrm{div}(w) = x - y$ to $\sum_{i,j} \sigma_b^i \sigma_c^j (x - y) \otimes \sigma_b^i \sigma_c^j$. Therefore, the element $\mathrm{div}(w^p)$ in $(\mathrm{Div}(X_K) \otimes S_*)^G \subset (\mathrm{Div}(X_K) \otimes \mathbb{Z}[G/H])^G$ is equal to

$$e := p \sum_{i,j=0}^{p-1} (\sigma_b^i \sigma_c^j (x - y) \otimes \sigma_b^i \sigma_c^j) = p \sum_{j=0}^{p-1} (\sigma_c^j x \otimes \sigma_c^j N_b) - p \sum_{i=0}^{p-1} (\sigma_b^i y \otimes \sigma_b^i N_c).$$

Since S_* is the sublattice of $\mathbb{Z}[G/\langle \sigma_a, \sigma_d \rangle]$ generated by N_b and N_c, this implies that e belongs to S_*. Then $e = \pi_*(f)$, where

$$f := \sum_{j=0}^{p-1} (\sigma_c^j x \otimes \sigma_c^j N_a) - \sum_{i=0}^{p-1} (\sigma_b^i y \otimes \sigma_b^i N_d) \in (\mathrm{Div}(X_K) \otimes P_*)^G.$$

It follows that $\mathrm{div}(E_w) = \partial(e) = \partial(\pi_*(f)) = 0$, which proves (1).

Moreover, since $\deg(x) = \deg(y) = 1$ we have

$$\deg(f) = (N_a N_c, -N_b N_d) = \iota_*(\eta) \qquad \text{in } (P_*)^G.$$

In view of (B.7), this implies that $\theta([E_w]) = -\overline{\eta}$. We know from Lemma 5.1(2) that $\overline{\eta} \neq 0$. This completes the proof of (2). □

Proof of Theorem 1.3. Replacing F by a finite extension if necessary, we may suppose that F contains a primitive p-th root of unity ζ. Let $E := F(x, y)$, where x and y are independent variables over F, let X be the Severi-Brauer variety of the degree-p cyclic algebra (x, y) over E, and let $L := E(X)$. Consider the following elements of $E^\times$:

$$a := 1 - x, \quad b := x, \quad c := y, \quad d := 1 - y.$$

We have $(a,b)=(c,d)=0$ in $\mathrm{Br}(E)$ by the Steinberg relations [Ser79, Chapter XIV, Proposition 4(iv)], and hence $(a,b)=(b,c)=0$ in $\mathrm{Br}(L)$. Moreover, $(b,c)\neq 0$ in $\mathrm{Br}(E)$ because the residue of (b,c) along $x=0$ is non-zero, while $(b,c)=0$ in $\mathrm{Br}(L)$ by [GS17, Theorem 5.4.1]. Thus $(a,b)=(b,c)=(c,d)=0$ in $\mathrm{Br}(L)$.

Consider the sequence of tori (4.1) over the ground field E, associated to the scalars $a,b,c,d\in E^\times$ chosen above:

$$1\to T\to P\to S\to 1.$$

Let $E_w\subset P_L$ be the T_L-torsor given by the equation $N_a(u)N_d(v)=w^p$. By Lemma 5.2(2), the torsor E_w is non-trivial over L. Now Corollary 4.5 implies that the Massey product $\langle a,b,c,d\rangle$ is not defined over L. In particular, by Lemma 2.3, the differential graded ring $C^\bullet(\Gamma_L,\mathbb{Z}/p\mathbb{Z})$ is not formal. □

Appendix A. Homological algebra

Let G be a profinite group, and let

$$0\to A_0\xrightarrow{\alpha_0}A_1\xrightarrow{\alpha_1}A_2\xrightarrow{\alpha_2}A_3\to 0 \tag{A.1}$$

be an exact sequence of discrete G-modules. We break (A.1) into two short exact sequences

$$0\to A_0\xrightarrow{\alpha_0}A_1\to A\to 0,$$
$$0\to A\to A_2\xrightarrow{\alpha_2}A_3\to 0.$$

We obtain a homomorphism

$$\theta\colon\ \mathrm{Ker}[H^1(G,A_1)\xrightarrow{\alpha_1}H^1(G,A_2)]\to\mathrm{Coker}[A_2^G\xrightarrow{\alpha_2}A_3^G] \tag{A.2}$$

defined as the composition of the map

$$\mathrm{Ker}[H^1(G,A_1)\xrightarrow{\alpha_1}H^1(G,A_2)]\to\mathrm{Ker}[H^1(G,A)\to H^1(G,A_2)]$$

and the inverse of the isomorphism

$$\mathrm{Coker}[A_2^G\xrightarrow{\alpha_2}A_3^G]\xrightarrow{\sim}\mathrm{Ker}[H^1(G,A)\to H^1(G,A_2)] \tag{A.3}$$

induced by the connecting homomorphism $A_3^G\to H^1(G,A)$.

Lemma A.1. *We have an exact sequence*

$$H^1(G,A_0)\xrightarrow{\alpha_0}\mathrm{Ker}[H^1(G,A_1)\xrightarrow{\alpha_1}H^1(G,A_2)]\xrightarrow{\theta}\mathrm{Coker}[A_2^G\to A_3^G]\to H^2(G,A_0),$$

where the last map is defined as the composition of (A.3) and the connecting homomorphism $H^1(G,A)\to H^2(G,A_0)$.

Proof. The proof follows from the definition of θ and the exactness of (A.1). □

Consider a commutative diagram of discrete G-modules

$$\begin{array}{ccccccc}
A_0 & \xhookrightarrow{\alpha_0} & A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 \\
\big\downarrow{\scriptstyle \iota_0} & & \big\downarrow{\scriptstyle \iota_1} & & \big\downarrow{\scriptstyle \iota_2} & & \big\downarrow{\scriptstyle \iota_3} \\
B_0 & \xhookrightarrow{\beta_0} & B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 \\
\big\downarrow{\scriptstyle \pi_0} & & \big\downarrow{\scriptstyle \pi_1} & & \big\downarrow{\scriptstyle \pi_2} & & \big\downarrow{\scriptstyle \pi_3} \\
C_0 & \xhookrightarrow{\gamma_0} & C_1 & \xrightarrow{\gamma_1} & C_2 & \xrightarrow{\gamma_2} & C_3
\end{array} \tag{A.4}$$

with exact rows and columns. It yields a commutative diagram of abelian groups

$$\begin{array}{ccccc} A_1^G & \xrightarrow{\alpha_1} & A_2^G & \xrightarrow{\alpha_2} & A_3^G \\ \downarrow{\scriptstyle \iota_1} & & \downarrow{\scriptstyle \iota_2} & & \downarrow{\scriptstyle \iota_3} \\ B_1^G & \xrightarrow{\beta_1} & B_2^G & \xrightarrow{\beta_2} & B_3^G \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle \pi_3} \\ C_1^G & \xrightarrow{\gamma_1} & C_2^G & \xrightarrow{\gamma_2} & C_3^G \\ \downarrow{\scriptstyle \partial_1} & & \downarrow{\scriptstyle \partial_2} & & \\ H^1(G,A_1) & \xrightarrow{\alpha_1} & H^1(G,A_2) & & \end{array} \tag{A.5}$$

where the columns are exact and the rows are complexes. Suppose that the connecting homomorphism $\partial_1\colon C_1^G \to H^1(G,A_1)$ is surjective. We define a function

$$\theta'\colon \operatorname{Ker}[H^1(G,A_1) \xrightarrow{\alpha_1} H^1(G,A_2)] \to \operatorname{Coker}(A_2^G \xrightarrow{\alpha_2} A_3^G)$$

as follows. Let $z \in H^1(G,A_1)$ such that $\alpha_1(z) = 0$ in $H^1(G,A_2)$. By assumption, there exists $c_1 \in C_1^G$ such that $\partial_1(c_1) = z$. By the exactness of the second column, there exists $b_2 \in B_2^G$ such that $\pi_2(b_2) = \gamma_1(c_1)$. By the exactness of the first column and the injectivity of ι_3, there exists a unique element $a_3 \in A_3^G$ such that $\beta_2(b_2) = \iota_3(a_3)$. We set

$$\theta'(z) := a_3 + \alpha_2(A_2^G).$$

A diagram chase shows that θ' is a well-defined homomorphism.

Lemma A.2. *Let G be a profinite group, and suppose given an exact sequence (A.1) and a commutative diagram (A.4) such that the connecting homomorphism $\partial_1\colon C_1^G \to H^1(G,A_1)$ is surjective. Then $\theta = -\theta'$.*

Proof. Let $z \in H^1(G,A_1)$ be such that $\alpha_1(z) = 0$ in $H^1(G,A_2)$. Since the map $\partial_1\colon C_1^G \to H^1(G,A_1)$ is surjective, there exists $c_1 \in C_1^G$ such that $\partial_1(c_1) = z$. Let $b_1 \in B_1$ be such that $\pi_1(b_1) = c_1$, and for all $g \in G$ let a_{1g} be the unique element of A_1 such that $\iota(a_{1g}) = gb - b$. Then $\partial_1(c_1)$ is represented by the 1-cocycle $\{a_{1g}\}_{g\in G}$.

Define $b_2 := \beta_1(b_1)$ and $c_2 := \gamma_1(c_1)$, so that $\pi_2(b_2) = c_2$. Since $\alpha_1(z) = 0$ is represented by the cocycle $\{\alpha_1(a_{1g})\}_{g\in G}$, we deduce that there exists $a_2 \in A_2$ such that $\alpha_1(a_{1g}) = ga_2 - a_2$ for all $g \in G$. It follows that $gb_2 - b_2 = \iota_2(ga_2 - a_2)$ for all $g \in G$, that is, $b_2 - \iota_2(a_2)$ belongs to B_2^G. Moreover, we have

$$\pi_2(b_2 - \iota_2(a_2)) = \pi_2(b_2) = \gamma_1(c_1).$$

Finally, we have

$$\beta_2(b_2 - \iota_2(a_2)) = \beta_2(\beta_1(b_1)) - \iota_3(\alpha_2(a_2)) = \iota_3(-\alpha_2(a_2)).$$

By definition, $\theta'(z) = -\alpha_2(a_2) + \alpha_2(A_2^G)$. Note that $\alpha_2(a_2)$ belongs to A_2^G because for all $g \in G$ we have

$$g\alpha_2(a_2) - \alpha_2(a_2) = \alpha_2(ga_2 - a_2) = \alpha_2(\alpha_1(a_{1g})) = 0.$$

For all $g \in G$, let $a_g \in A$ be the image of a_{1g}. The homomorphism

$$\operatorname{Ker}[H^1(G,A_1) \xrightarrow{\alpha_1} H^1(G,A_2)] \to \operatorname{Ker}[H^1(G,A) \to H^1(G,A_2)]$$

induced by the map $A_1 \to A$ sends the class of $\{a_{1g}\}_{g\in G}$ to the class of $\{a_g\}_{g\in G}$.

The element $a_2 \in A_2$ is a lift of $\alpha_2(a_2)$. As $ga_2 - a_2 = \alpha_1(a_{1g})$ for all $g \in G$, the injective map $A \to A_2$ sends a_g to $ga_2 - a_2$ for all $g \in G$. Therefore, the connecting homomorphism $A_3^G \to H^1(G, A)$ sends $\alpha_2(a_2)$ to the class of $\{a_g\}_{g\in G}$. It follows that the isomorphism

$$\mathrm{Coker}[A_2^G \xrightarrow{\alpha_2} A_3^G] \xrightarrow{\sim} \mathrm{Ker}[H^1(G, A) \to H^1(G, A_2)]$$

induced by $A_3^G \to H^1(G, A)$ sends $\alpha_2(a_2)+\alpha_2(A_2^G)$ to the class of $\{a_g\}_{g\in G}$. By the definition of θ, we conclude that $\theta(z) = \alpha_2(a_2) + \alpha_2(A_2^G) = -\theta'(z)$. □

Appendix B. Unramified torsors under tori

Let F be a field, let X be a smooth projective geometrically connected F-variety, let K be a Galois extension of F (possibly of infinite degree over F), and let $G := \mathrm{Gal}(K/F)$. We have an exact sequence of discrete G-modules

$$1 \to K^\times \to K(X)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}(X_K) \xrightarrow{\lambda} \mathrm{Pic}(X_K) \to 0, \tag{B.1}$$

where div takes a non-zero rational function $f \in K(X)^\times$ to its divisor, and λ takes a divisor on X_K to its class in $\mathrm{Pic}(X_K)$.

Let T be an F-torus split by K. Write T_* for the cocharacter lattice of T: it is a finitely generated $\mathbb{Z}$-free G-module. Tensoring (B.1) with T_*, we obtain an exact sequence of G-modules

$$1 \to T(K) \to T(K(X)) \xrightarrow{\mathrm{div}} \mathrm{Div}(X_K) \otimes T_* \xrightarrow{\lambda} \mathrm{Pic}(X_K) \otimes T_* \to 0, \tag{B.2}$$

where we have used the fact that $K^\times \otimes T_* = T(K)$.

We define the subgroup of unramified torsors

$$H^1(G, T(K(X)))_{\mathrm{nr}} := \mathrm{Ker}[H^1(G, T(K(X))) \xrightarrow{\mathrm{div}} H^1(G, \mathrm{Div}(X_K \otimes T_*))].$$

The sequence (B.1) is a special case of (A.1). In this case, the map θ of (A.1) takes the form

$$\theta\colon H^1(G, T(K(X)))_{\mathrm{nr}} \to \mathrm{Coker}[\mathrm{Div}(X_K) \otimes T_* \xrightarrow{\lambda} \mathrm{Pic}(X_K) \otimes T_*]. \tag{B.3}$$

Proposition B.1. *We have an exact sequence*

$$H^1(G, T(K)) \to H^1(G, T(K(X)))_{\mathrm{nr}} \xrightarrow{\theta} \mathrm{Coker}[(\mathrm{Div}(X_K) \otimes T_*)^G \xrightarrow{\lambda} (\mathrm{Pic}(X_K) \otimes T_*)^G] \to H^2(G, T(K)),$$

where the first map and the last map are induced by (B.2).

Proof. This is a special case of Lemma A.1. □

By Lemma A.2, the map θ may be computed as follows. Let

$$1 \to T \xrightarrow{\iota} P \xrightarrow{\pi} S \to 1 \tag{B.4}$$

be a short exact sequence of F-tori split by K such that P is a quasi-trivial torus. Passing to cocharacter lattices, we obtain a short exact sequence of G-modules

$$0 \to T_* \xrightarrow{\iota_*} P_* \xrightarrow{\pi_*} S_* \to 0. \tag{B.5}$$

We tensor (B.1) with T_*, P_* and S_* respectively, and pass to group cohomology to obtain the following commutative diagram, where the columns are exact and the rows are complexes:

(B.6)
$$\begin{array}{ccccc} & & \mathrm{Div}((X_K)\otimes T_*)^G & \xrightarrow{\lambda} & (\mathrm{Pic}(X_K)\otimes T_*)^G \\ & & \downarrow{\scriptstyle \iota_*} & & \downarrow{\scriptstyle \iota_*} \\ P(F(X)) & \xrightarrow{\mathrm{div}} & (\mathrm{Div}(X_K)\otimes P_*)^G & \xrightarrow{\lambda} & (\mathrm{Pic}(X_K)\otimes P_*)^G \\ \downarrow{\scriptstyle \pi_*} & & \downarrow{\scriptstyle \pi_*} & & \downarrow{\scriptstyle \pi_*} \\ S(F(X)) & \xrightarrow{\mathrm{div}} & (\mathrm{Div}(X_K)\otimes S_*)^G & \xrightarrow{\lambda} & (\mathrm{Pic}(X_K)\otimes S_*)^G \\ \downarrow{\scriptstyle \partial} & & \downarrow{\scriptstyle \partial} & & \\ H^1(G,T(K(X))) & \xrightarrow{\mathrm{div}} & H^1(G,\mathrm{Div}(X_K\otimes T_*)). & & \end{array}$$

Note that $\mathrm{Gal}(K(X)/F(X)) = G$. Therefore $H^1(G, P(K(X)))$ is trivial, and hence $\partial\colon S(F(X)) \to H^1(G,T(K(X)))$ is surjective.

Let $\tau \in H^1(G,T(K(X)))_{\mathrm{nr}}$, choose $\sigma \in S(F(X))$ such that $\partial(\sigma) = \tau$. Then pick $\rho \in (\mathrm{Div}(X_K)\otimes P_*)^G$ such that $\pi_*(\rho) = \mathrm{div}(\sigma)$, and let t be the unique element in $(\mathrm{Pic}(X_K)\otimes T_*)^G$ such that $\lambda(\rho) = \iota_*(t)$. Lemma A.2 implies

(B.7) $$\theta(\tau) = -t.$$

Finally, suppose that $K = F_s$ is a separable closure of F, so that $G = \Gamma_F$, and write X_s for $X \times_F F_s$. The exact sequence (B.2) for $K = F_s$ takes the form

(B.8) $$1 \to T(F_s) \to T(F_s(X)) \xrightarrow{\mathrm{div}} \mathrm{Div}(X_s)\otimes T_* \xrightarrow{\lambda} \mathrm{Pic}(X_s)\otimes T_* \to 0.$$

We have the inflation-restriction sequence

$$0 \to H^1(F,T(F_s(X))) \xrightarrow{\mathrm{Inf}} H^1(F(X),T) \xrightarrow{\mathrm{Res}} H^1(F_s(X),T).$$

Since T is defined over F, it is split by F_s, and hence by Hilbert's Theorem 90 we have $H^1(F_s(X),T)$=0. Thus the inflation map $H^1(F,T(F_s(X))) \to H^1(F(X),T)$ is an isomorphism. We identify $H^1(F,T(F_s(X)))$ with $H^1(F(X),T)$ via the inflation map. If we define

$$H^1(F(X),T)_{\mathrm{nr}} \coloneqq \mathrm{Ker}[H^1(F(X),T) \xrightarrow{\mathrm{div}} H^1(F,\mathrm{Div}(X_s)\otimes T_*)],$$

the map θ of (A.2) takes the form

$$\theta\colon H^1(F(X),T)_{\mathrm{nr}} \to \mathrm{Coker}[\mathrm{Div}(X_s)\otimes T_* \to \mathrm{Pic}(X_s)\otimes T_*].$$

Corollary B.2. *We have an exact sequence*

$$H^1(F,T) \to H^1(F(X),T)_{\mathrm{nr}} \xrightarrow{\theta} \mathrm{Coker}[(\mathrm{Div}(X_s)\otimes T_*)^{\Gamma_F} \xrightarrow{\lambda} (\mathrm{Pic}(X_s)\otimes T_*)^{\Gamma_F}] \to H^2(F,T),$$

where the first and last map are induced by (B.8).

Proof. This is a special case of Proposition B.1. □

References

[BD01] Daniel K. Biss and Samit Dasgupta. A presentation for the unipotent group over rings with identity. *J. Algebra*, 237(2):691–707, 2001. 7

[Dwy75] William G. Dwyer. Homology, Massey products and maps between groups. *J. Pure Appl. Algebra*, 6(2):177–190, 1975. 7, 8

[Efr14] Ido Efrat. The Zassenhaus filtration, Massey products, and representations of profinite groups. *Adv. Math.*, 263:389–411, 2014. 8

[EM17] Ido Efrat and Eliyahu Matzri. Triple Massey products and absolute Galois groups. *J. Eur. Math. Soc. (JEMS)*, 19(12):3629–3640, 2017. 2

[GMT18] Pierre Guillot, Ján Mináč, and Adam Topaz. Four-fold Massey products in Galois cohomology. *Compos. Math.*, 154(9):1921–1959, 2018. With an appendix by Olivier Wittenberg. 2

[GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. Second edition. 17, 18, 23

[HW15] Michael J. Hopkins and Kirsten G. Wickelgren. Splitting varieties for triple Massey products. *J. Pure Appl. Algebra*, 219(5):1304–1319, 2015. 1, 2

[HW19] Christian Haesemeyer and Charles A. Weibel. *The norm residue theorem in motivic cohomology*, volume 200 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2019. 1

[HW23] Yonatan Harpaz and Olivier Wittenberg. The Massey vanishing conjecture for number fields. *Duke Math. J.*, 172(1):1–41, 2023. 2, 8

[KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The book of involutions*, volume 44 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits. 4

[Mat18] Eliyahu Matzri. Triple Massey products of weight $(1, n, 1)$ in Galois cohomology. *J. Algebra*, 499:272–280, 2018. 2

[MS22] Alexander Merkurjev and Federico Scavia. Degenerate fourfold Massey products over arbitrary fields. *arXiv:2208.13011*, 2022. 1, 2, 3, 6, 8

[MS23] Alexander Merkurjev and Federico Scavia. The Massey vanishing conjecture for fourfold Massey products modulo 2. *arXiv:2301.09290*, 2023. 2

[MT16] Ján Mináč and Nguyen Duy Tân. Triple Massey products vanish over all fields. *J. Lond. Math. Soc. (2)*, 94(3):909–932, 2016. 2, 15

[MT17a] Ján Mináč and Nguyen Duy Tân. Counting Galois $\mathbb{U}_4(\mathbb{F}_p)$-extensions using Massey products. *J. Number Theory*, 176:76–112, 2017. 2

[MT17b] Ján Mináč and Nguyen Duy Tân. Triple Massey products and Galois theory. *J. Eur. Math. Soc. (JEMS)*, 19(1):255–284, 2017. 2

[PS18] Ambrus Pál and Endre Szabó. The strong Massey vanishing conjecture for fields with virtual cohomological dimension at most 1. *arXiv:1811.06192* (2018). 2

[Pos17] Leonid Positselski. Koszulity of cohomology = $K(\pi, 1)$-ness + quasi-formality. *J. Algebra*, 483:188–229, 2017. 1

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. 6, 23

[Ser97] Jean-Pierre Serre. *Galois cohomology*. Springer-Verlag, Berlin, 1997. Translated from the French by Patrick Ion and revised by the author. 15

Department of Mathematics, University of California, Los Angeles, CA 90095, United States of America

Email address: merkurev@math.ucla.edu

Email address: scavia@math.ucla.edu