



# COMPOSITIO MATHEMATICA

## Non-formality of Galois cohomology modulo all primes

Alexander Merkurjev  and Federico Scavia 

Compositio Math. **161** (2025), 831–858.

doi: [10.1112/S0010437X25007018](https://doi.org/10.1112/S0010437X25007018)



FOUNDATION  
COMPOSITIO  
MATHEMATICA



LONDON  
MATHEMATICAL  
SOCIETY  
EST. 1865





# 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  $\text{Br}(L)[p]$  but the mod  $p$  Massey product  $\langle a, b, c, d \rangle$  is not defined over  $L$ . Thus, the strong Massey vanishing conjecture at the prime  $p$  fails for  $L$ , and the cochain differential graded ring  $C^*(\Gamma_L, \mathbb{Z}/p\mathbb{Z})$  of the absolute Galois group  $\Gamma_L$  of  $L$  is not formal. This answers a question of Positselski. As our main tool, we define a secondary obstruction that detects non-triviality of unramified torsors under tori, and which is of independent interest.

## 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  $\zeta$ , and let  $\Gamma_F$  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  $H^*(F, \mathbb{Z}/p\mathbb{Z}) = H^*(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ . In view of this complete description of the cup product, the research on  $H^*(F, \mathbb{Z}/p\mathbb{Z})$  shifted in recent years to external operations, defined in terms of the differential graded ring of continuous cochains  $C^*(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ .

Hopkins and Wickelgren [HW15] asked whether  $C^*(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$  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  $C^*(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$  to  $H^*(F, \mathbb{Z}/p\mathbb{Z})$ . The authors of [HW15] were unaware of earlier work of Positselski, who had already shown in [Pos11, Section 9.11] that  $C^*(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$  is not formal for some finite extensions  $F$  of  $\mathbb{Q}_\ell$  and  $\mathbb{F}_\ell((z))$ , where  $\ell \neq p$ . Positselski then wrote a detailed exposition of his counterexamples in [Pos17].

For Positselski's method to work, it seemed important that  $F$  did not contain all the roots of unity of  $p$ -power order. This motivated 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  $C^*(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$  is not formal?

---

Received 5 October 2023, accepted in final form 8 November 2024.

2020 *Mathematics Subject Classification* 12G05 (primary), 55S30, 16K50 (secondary).

*Keywords*: Galois cohomology; Massey products; formality; Galois algebras; torsors.

© The Author(s), 2025. The publishing rights in this article are licensed to Foundation Compositio Mathematica under an exclusive licence. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

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  $C^*(\Gamma_L, \mathbb{Z}/p\mathbb{Z})$  is not formal.*

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  $\text{char}(F) \neq p$  and  $F$  contains a primitive  $p$ th root of unity  $\zeta$ , Kummer theory gives an identification  $H^1(F, \mathbb{Z}/p\mathbb{Z}) = F^\times / F^{\times p}$ , and we may thus consider Massey products  $\langle a_1, \dots, a_n \rangle$ , where  $a_i \in F^\times$  for  $1 \leq i \leq n$ .

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

$$\text{The Massey product } \langle \chi_1, \dots, \chi_n \rangle \text{ vanishes.} \quad (1.1)$$

$$\text{The Massey product } \langle \chi_1, \dots, \chi_n \rangle \text{ is defined.} \quad (1.2)$$

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

We have that (1.1) implies (1.2), and that (1.2) implies (1.3). The Massey vanishing conjecture, due to Mináč and Tân [MT17b] and inspired by the earlier work of Hopkins and 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 was shown when either  $n = 3$  and  $p$  is arbitrary, by Efrat and Matzri and Mináč and Tân [Mat18, EM17, MT16], or when  $n = 4$  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 and Wittenberg [HW23].

When  $n = 3$ , it is a direct consequence of the definition of the 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  $\chi_1, \dots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$  such that  $\chi_i \cup \chi_{i+1} = 0$  for all  $1 \leq i \leq n-1$ , the Massey product  $\langle \chi_1, \dots, \chi_n \rangle$  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  $\text{Br}(\mathbb{Q})$  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 and 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  $\text{Br}(F)$ , 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  $C^*(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$  is not formal; see Lemma 2.3. Therefore, Theorem 1.2 follows from the next more precise result.

**THEOREM 1.3.** *Let  $p$  be a prime number and 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  $C^*(\Gamma_L, \mathbb{Z}/p\mathbb{Z})$  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  $\langle \chi_1, \chi_2, \chi_3, \chi_4, 0, \dots, 0 \rangle$ . 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 §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  $\langle \chi_1, \dots, \chi_n \rangle \subset H^2(F, \mathbb{Z}/p\mathbb{Z})$  vanishes (respectively, is defined) if and only if the homomorphism  $(\chi_1, \dots, \chi_n): \Gamma_F \rightarrow (\mathbb{Z}/p\mathbb{Z})^n$  lifts to the group  $U_{n+1}$  of upper unitriangular matrices in  $\mathrm{GL}_{n+1}(\mathbb{F}_p)$  (respectively, 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 §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  $F$ . Moreover, the variety defined by these equations is a torsor under a torus; see Proposition 3.7. This equivalence is proved 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 §4, we use the work of §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 independent variables over  $F$ , and replace  $F$  by  $E := F(x, y)$ . We then set  $a := 1 - x$ ,  $b := x$ ,  $c := y$  and  $d := 1 - y$  over  $E$ . We have  $(a, b) = (c, d) = 0$  in  $\mathrm{Br}(E)$ . The class  $(b, c)$  is not zero in  $\mathrm{Br}(E)$ , so the Severi–Brauer variety  $X/E$  of  $(b, c)$  is non-trivial, but  $(b, c) = 0$  over  $L := E(X)$ .

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 §5, an explicit calculation shows that the obstruction is non-zero on  $E_w$ , and hence  $E_w$  is non-trivial, as desired.

## 1.1 Notation

Let  $F$  be a field, let  $F_s$  be a separable closure of  $F$  and denote by  $\Gamma_F := \mathrm{Gal}(F_s/F)$  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  $\Gamma_E$ .

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

$$E_{a_1, \dots, a_n} := E[x_1, \dots, x_n] / (x_1^p - a_1, \dots, x_n^p - a_n),$$

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

We write  $\text{Br}(F)$  for the Brauer group of  $F$ . If  $\text{char}(F) \neq p$  and  $F$  contains a primitive  $p$ th root of unity, for all  $a, b \in F^\times$  we denote by  $(a, b)$  the corresponding degree- $p$  cyclic algebra and also its class in  $\text{Br}(F)$ ; see § 2.1. We denote by  $N_{a_1, \dots, a_n} : \text{Br}(F_{a_1, \dots, a_n}) \rightarrow \text{Br}(F)$  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 let  $F(X)$  be the function field of  $X$ , and we write  $X^{(1)}$  for the collection of all points of codimension 1 in  $X$ . We set  $X_s := X \times_F F_s$ . 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  $X = \mathbb{P}_F^d$  is a  $d$ -dimensional projective space, we denote by  $\mathbb{P}_{a_1, \dots, a_n}^d$  the base change of  $\mathbb{P}_F^d$  to  $F_{a_1, \dots, a_n}$ .

## 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  $\text{Spec}(L) \rightarrow \text{Spec}(F)$  is an étale  $G$ -torsor. If  $L/F$  is a Galois  $G$ -algebra, then 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

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

where, if  $f_1, f_2 : \Gamma_F \rightarrow G$  are continuous group homomorphisms, we say that  $f_1 \sim f_2$  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  $\text{Hom}_{\text{cont}}(\Gamma_F, G) / \sim \rightarrow \text{Hom}_{\text{cont}}(\Gamma_F, G/H) / \sim$  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 following square is cartesian.*

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

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

- (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 we are given  $G$ -equivariant algebra homomorphisms  $E \rightarrow K$  and  $E \rightarrow K'$ . Endow the tensor product  $L := K \otimes_E K'$  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 following 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 homomorphism  $L^H \otimes_{L^S} L^{H'} \rightarrow L$  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 the following  $G$ -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  $G/H \rightarrow G/S$ . Therefore, the base change of  $\mathrm{Spec}(K) \rightarrow \mathrm{Spec}(E)$  to  $F_s$  is  $G$ -equivariantly isomorphic to the projection  $G/H \rightarrow G/S$ . Similarly for  $\mathrm{Spec}(K') \rightarrow \mathrm{Spec}(E)$ . Therefore, the base change of  $\mathrm{Spec}(L) \rightarrow \mathrm{Spec}(F)$  over  $F_s$  is  $G$ -equivariantly isomorphic to  $(G/H) \times_{G/S} (G/H') \simeq G$ , that is, the morphism  $\mathrm{Spec}(L) \rightarrow \mathrm{Spec}(F)$  is an étale  $G$ -torsor.  $\square$

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

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

For every  $a \in F^\times$ , we let  $\chi_a: \Gamma_F \rightarrow \mathbb{Z}/p\mathbb{Z}$  be the homomorphism corresponding to the coset  $aF^{\times p}$  under (2.3). Explicitly, letting  $a' \in F_s^\times$  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  $\sigma_i$  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 by  $(\sigma_i - 1)a_j^{1/p} = 1$  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

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

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

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

For all  $a, b \in F^\times$ , we have  $\iota(\chi_a \cup \chi_b) = (a, b)$  in  $\text{Br}(F)$ ; 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  $\zeta$ . The following are equivalent.*

- (i) *We have  $(a, b) = 0$  in  $\text{Br}(F)$ .*
- (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  $(A, \partial)$  be a differential graded ring, that is,  $A = \bigoplus_{i \geq 0} A^i$  is a non-negatively graded abelian group with an associative multiplication which respects the grading, and  $\partial: A \rightarrow A$  is a group homomorphism of degree 1 such that  $\partial \circ \partial = 0$  and  $\partial(ab) = \partial(a)b + (-1)^i a\partial(b)$  for all  $i \geq 0$ ,  $a \in A^i$  and  $b \in A$ . We denote by  $H^*(A) := \text{Ker}(\partial)/\text{Im}(\partial)$  the cohomology of  $(A, \partial)$ , and we write  $\cup$  for the multiplication (cup product) on  $H^*(A)$ .

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

Let  $n \geq 2$  be an integer and let  $a_1, \dots, a_n \in H^1(A)$ . A *defining system* for the  $n$ th order Massey product  $\langle a_1, \dots, a_n \rangle$  is a collection  $M$  of elements  $a_{ij} \in A^1$ , 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  $(A, \partial)$  be a differential graded ring, let  $n \geq 3$  be an integer and let  $\alpha_1, \dots, \alpha_n$  be elements of  $H^1(A)$  satisfying  $\alpha_i \cup \alpha_{i+1} = 0$  for all  $1 \leq i \leq n-1$ . If  $A$  is formal, then  $\langle \alpha_1, \dots, \alpha_n \rangle$  vanishes.*

*Proof.* See [PQ22, Theorem 3.8]. □

## 2.3 Dwyer's theorem

Let  $p$  be a prime, and let  $U_{n+1} \subset \text{GL}_{n+1}(\mathbb{F}_p)$  be the subgroup of  $(n+1) \times (n+1)$  upper unitriangular matrices. For all  $1 \leq i < j \leq n+1$ , we denote by  $e_{ij} \in U_{n+1}$  the matrix whose non-diagonal entries are all zero except for the entry  $(i, j)$ , which is equal to 1. We set  $\sigma_i := e_{i,i+1}$  for all  $1 \leq i \leq n$ . By [BD01, Theorem 1], the group  $U_{n+1}$  admits a presentation with generators the  $\sigma_i$  and the following relations:

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

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



$$[\sigma_i, [\sigma_i, \sigma_{i+1}]] = [\sigma_{i+1}, [\sigma_i, \sigma_{i+1}]] = 1 \quad \text{for all } 1 \leq i \leq n-2, \quad (2.6)$$

$$[[\sigma_i, \sigma_{i+1}], [\sigma_{i+1}, \sigma_{i+2}]] = 1 \quad \text{for all } 1 \leq i \leq n-3. \quad (2.7)$$

The following relations holds in  $U_{n+1}$ :

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

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

$$\bar{\sigma}_i^p = 1 \quad \text{for all } 1 \leq i \leq n, \quad (2.8)$$

$$[\bar{\sigma}_i, \bar{\sigma}_j] = 1 \quad \text{for all } 1 \leq i \leq j-2 \leq n-2, \quad (2.9)$$

$$[\bar{\sigma}_i, [\bar{\sigma}_i, \bar{\sigma}_{i+1}]] = [\bar{\sigma}_{i+1}, [\bar{\sigma}_i, \bar{\sigma}_{i+1}]] = 1 \quad \text{for all } 1 \leq i \leq n-2, \quad (2.10)$$

$$[[\bar{\sigma}_i, \bar{\sigma}_{i+1}], [\bar{\sigma}_{i+1}, \bar{\sigma}_{i+2}]] = 1 \quad \text{for all } 1 \leq i \leq n-3, \quad (2.11)$$

$$[\bar{\sigma}_1, [\bar{\sigma}_2, \dots, [\bar{\sigma}_{n-2}, [\bar{\sigma}_{n-1}, \bar{\sigma}_n]] \dots]] = 1. \quad (2.12)$$

We write  $u_{ij}: U_{n+1} \rightarrow \mathbb{Z}/p\mathbb{Z}$  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 a commutative diagram

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

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

$$Q_{n+1} := \text{Ker}[U_{n+1} \rightarrow (\mathbb{Z}/p\mathbb{Z})^n], \quad \bar{Q}_{n+1} := \text{Ker}[\bar{U}_{n+1} \rightarrow (\mathbb{Z}/p\mathbb{Z})^n] = Q_{n+1}/Z_{n+1}.$$

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

Let  $G$  be a profinite group. The complex  $(C^*(G, \mathbb{Z}/p\mathbb{Z}), \partial)$  of mod  $p$  non-homogeneous continuous cochains of  $G$  with the standard cup product is a differential graded ring. Therefore,  $H^*(G, \mathbb{Z}/p\mathbb{Z}) = H^*(C^*(G, \mathbb{Z}/p\mathbb{Z}), \partial)$  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  $\chi: G \rightarrow (\mathbb{Z}/p\mathbb{Z})^n$  for the continuous homomorphism with components  $(\chi_1, \dots, \chi_n)$ . Consider diagram (2.13).*

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



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

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

Theorem 2.4 may be rephrased as follows.

**COROLLARY 2.5.** Let  $p$  be a prime, let  $F$  be a field of characteristic different from  $p$  and containing a primitive  $p$ th root of unity  $\zeta$ , 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 (respectively, vanishes) if and only if there exists a Galois  $\overline{U}_{n+1}$ -algebra  $K/F$  (respectively, a Galois  $U_{n+1}$ -algebra  $L/F$ ) such that  $K^{\overline{Q}_{n+1}} \simeq F_{a_1, \dots, a_n}$  (respectively,  $L^{Q_{n+1}} \simeq F_{a_1, \dots, a_n}$ ) as  $(\mathbb{Z}/p\mathbb{Z})^n$ -algebras.

*Proof.* This follows from Theorem 2.4 and (2.1).  $\square$

We will apply Lemma 2.1 to the cartesian square of groups

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

where  $\varphi_{n+1}$  (respectively,  $\varphi'_{n+1}$ ) is the restriction homomorphism from  $U_{n+1}$  or from  $\overline{U}_{n+1}$  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.

*Remark 2.6.* The presentations of  $U_{n+1}$  and  $\overline{U}_{n+1}$  of [BD01] given above will allow us to avoid lengthy calculations in §3, but they are not essential for our arguments. One could instead use the following classical presentations of  $U_{n+1}$  and  $\overline{U}_{n+1}$ , which are reminiscent of the Steinberg relations for the Steinberg group of a ring in algebraic K-theory.

The group  $U_{n+1}$  admits a presentation with generators  $\{e_{ij} : 1 \leq i < j \leq n+1\}$  and the following relations:

$$\begin{aligned} e_{ij}^p &= 1 \quad \text{for all } 1 \leq i < j \leq n+1, \\ [e_{ij}, e_{jk}] &= e_{ik} \quad \text{for all } 1 \leq i < j < k \leq n+1, \\ [e_{ij}, e_{kl}] &= 1 \quad \text{for all } 1 \leq i < j \leq n+1, 1 \leq k < l \leq n+1, i \neq l, j \neq k. \end{aligned}$$

This is a particular case of [AB08, Proposition 7.108], where we choose  $w$  to be the longest element of the Weyl group of  $\mathrm{GL}_{n+1}$  over  $\mathbb{F}_p$ . One obtains a presentation of  $\overline{U}_{n+1}$  with generating set  $\{\bar{e}_{ij} : 1 \leq i < j \leq n+1\}$ , modulo the relations induced by the above relations for the  $e_{ij}$ , together with the relation  $\bar{e}_{1, n+1} = 1$ .

### 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  $\zeta$ .

#### 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 § 2.1. The projection  $U_3 \rightarrow \bar{U}_3 = (\mathbb{Z}/p\mathbb{Z})^2$  sends  $e_{12} \mapsto \sigma_a$  and  $e_{23} \mapsto \sigma_b$ . We define the following elements of  $U_3$ :

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

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

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

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

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

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

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

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

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

In (3.2) and (3.4), the relations involving  $\tau$  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  $\bar{U}_3 = \text{Gal}(F_{a,b}/F)$  on  $F_{a,b}$  and

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

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  $\bar{U}_3 = \text{Gal}(F_{a,b}/F)$  on  $F_{a,b}$  and

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

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 (3.3), 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  $\sigma_b: F_{a,b} \rightarrow F_{a,b}$  extends to an isomorphism of étale algebras  $f: (F_{a,b})_{ax} \rightarrow (F_{a,b})_x$  by sending  $(ax)^{1/p}$  to  $a^{1/p}x^{1/p}$ . The map  $f$  is well defined because  $f((ax)^{1/p})^p = (a^{1/p}x^{1/p})^p = ax$ . We now show that  $f$  is  $U_3$ -equivariant. The restriction of  $f$  to  $F_{a,b}$  is  $U_3$ -equivariant because  $\sigma_a\sigma_b = \sigma_b\sigma_a$  on  $F_{a,b}$ . We have

$$\sigma_a(f((ax)^{1/p})) = \sigma_a(a^{1/p}) \cdot \sigma_a(x^{1/p}) = \zeta \cdot a^{1/p} \cdot \frac{b^{1/p}}{\alpha} \cdot x^{1/p} = \frac{\zeta a^{1/p} b^{1/p} x^{1/p}}{\alpha}$$

and

$$f(\sigma_a((ax)^{1/p})) = f((b^{1/p}/\alpha) \cdot (ax)^{1/p}) = \zeta \cdot \frac{b^{1/p}}{\alpha} \cdot a^{1/p} \cdot x^{1/p} = \frac{\zeta a^{1/p} b^{1/p} x^{1/p}}{\alpha}.$$

Thus,  $f$  is  $\langle \sigma_a \rangle$ -equivariant. We also have

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

and

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

Thus,  $f$  is  $\langle \sigma_b \rangle$ -equivariant. Since  $\sigma_a$  and  $\sigma_b$  generate  $U_3$ , we conclude that  $f$  is  $U_3$ -equivariant, as desired.

(2) The proof is similar to that of (1).  $\square$

**PROPOSITION 3.2.** *Let  $a, b \in F^\times$  be such that  $(a, b) = 0$  in  $\text{Br}(F)$ , 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*

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

*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  $\tau$  commutes with  $\sigma_b$ ,

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

and 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 we set  $x^{1/p} := z^{1/p}\theta \in (F_{a,b})_z^\times$ . Then  $K = (F_{a,b})_x$ , where

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

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

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

(3) Suppose we are 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  $(F_{a,b})_y \rightarrow (F_{a,b})_x$  restricts to an isomorphism of Galois  $\mathbb{Z}/p\mathbb{Z}$ -algebras  $F_b \rightarrow F_b$ . Since the

automorphism group of  $F_b$  as a Galois  $(\mathbb{Z}/p\mathbb{Z})$ -algebra is  $\mathbb{Z}/p\mathbb{Z}$ , generated by  $\sigma_b$ , this isomorphism  $F_b \rightarrow F_b$  is equal to  $\sigma_b^i$  for some integer  $i \geq 0$ . 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  $(1 - \sigma_b)y = \beta^p/a$ , and hence

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

Therefore,

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

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

$$(\sigma_a - 1)(\sigma_b - 1)w = (\sigma_a - 1)(\sigma_b - 1)w' = \zeta. \quad (3.6)$$

Putting (3.5) and (3.6) together, we see that  $w$  satisfies the conditions of (3). Conversely, suppose we are given  $w' \in F_{a,b}^\times$  such that

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

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

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

for some integers  $i$  and  $j$ .

*Proof of Claim 3.3.* First, we find  $\eta_a \in F_a^\times$  such that

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

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,  $\zeta_a$  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  $\sigma_a$  acts on  $F^p$  by cyclically permuting the coordinates, that is,

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

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,

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

All in all, independent of whether  $F_a$  is a field or not, we have found  $\eta_a$  satisfying (3.7).

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

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

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.  $\square$

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

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

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

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

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

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

so that

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

Let  $f: (F_{a,b})_{a^i x} \rightarrow (F_{a,b})_{b^j y}$  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

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

Moreover,

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

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

and hence  $f$  is  $U_3$ -equivariant.  $\square$

### 3.2 Galois $\overline{U}_4$ -algebras

Let  $a, b, c \in F^\times$  be such that  $(a, b) = (b, c) = 0$  in  $\text{Br}(F)$ . By Lemma 2.2, we may fix  $\alpha \in F_a^\times$  and  $\gamma \in F_c^\times$  such that  $N_a(\alpha) = N_c(\gamma) = b$ . We have  $\text{Gal}(F_{a,b,c}/F) = (\mathbb{Z}/p\mathbb{Z})^3 = \langle \sigma_a, \sigma_b, \sigma_c \rangle$ . The

projection map  $\overline{U}_4 \rightarrow (\mathbb{Z}/p\mathbb{Z})^3$  is given by  $\bar{e}_{12} \mapsto \sigma_a$ ,  $\bar{e}_{23} \mapsto \sigma_b$ ,  $\bar{e}_{34} \mapsto \sigma_c$ . Its kernel  $\overline{Q}_4 \subset \overline{U}_4$  is isomorphic to  $(\mathbb{Z}/p\mathbb{Z})^2$ , generated by  $\bar{e}_{13}$  and  $\bar{e}_{24}$ . We define the following elements of  $\overline{U}_4$ :

$$\sigma_a := \bar{e}_{12}, \quad \sigma_b := \bar{e}_{23}, \quad \sigma_c := \bar{e}_{34}, \quad \tau_{ab} := \bar{e}_{13}, \quad \tau_{bc} := \bar{e}_{24}.$$

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

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

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

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

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

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

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

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  $\text{Br}(F)$ . 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  $H$  (respectively,  $H'$ ) be the subgroup of  $\overline{U}_4$  generated by  $\sigma_c$  and  $\tau_{bc}$  (respectively,  $\sigma_a$  and  $\tau_{ab}$ ), 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 determined by (3.10) and (3.12).  $\square$

### 3.3 Galois $U_4$ -algebras

Let  $a, b, c \in F^\times$ , and suppose that  $(a, b) = (b, c) = 0$  in  $\text{Br}(F)$ . 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 §2.1. The quotient map  $U_4 \rightarrow (\mathbb{Z}/p\mathbb{Z})^3$  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 homomorphism 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  $U_4$ :

$$\sigma_a := e_{12}, \quad \sigma_b := e_{23}, \quad \sigma_c := e_{34},$$

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

PROPOSITION 3.5. Let  $a, b, c \in F^\times$  be such that  $(a, b) = (b, c) = 0$  in  $\text{Br}(F)$ . 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  $F$  such that  $L^{Z_4} = K$ , and let  $y \in K^\times$  be such that  $L = K_y$ .

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

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

The element  $\sigma_b$  commutes with  $\tau_{ab}, \tau_{bc}$  and  $\rho$ . 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  $(\sigma_b - 1)(y^{1/p}) \in F_{a,b,c}^\times$ . By Hilbert's Theorem 90, applied to  $F_{a,b,c}/F_{a,c}$ , there is  $q \in F_{a,b,c}^\times$  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,  $y \in F_{a,c}^\times$ . We have

$$\begin{aligned} \rho(\sigma_a - 1)(y^{1/p}) &= (\sigma_a - 1)\rho(y^{1/p}) = (\sigma_a - 1)(\zeta^{-1} \cdot y^{1/p}) = (\sigma_a - 1)(y^{1/p}), \\ \sigma_b(\sigma_a - 1)(y^{1/p}) &= (\sigma_a \sigma_b \tau_{ab}^{-1} - \sigma_b)(y^{1/p}) = (\sigma_a - 1)(y^{1/p}), \\ \tau_{ab}(\sigma_a - 1)(y^{1/p}) &= (\sigma_a - 1)\tau_{ab}(y^{1/p}) = (\sigma_a - 1)(y^{1/p}), \\ \tau_{bc}(\sigma_a - 1)(y^{1/p}) &= (\rho^{-1} \sigma_a - 1)\tau_{bc}(y^{1/p}) = (\sigma_a \rho^{-1} - 1)(y^{1/p}) = \zeta \cdot (\sigma_a - 1)(y^{1/p}). \end{aligned}$$

By (3.12)–(3.13), analogous identities are satisfied by  $(x')^{1/p}$ , that is,

$$(\rho - 1)(x')^{1/p} = (\sigma_b - 1)(x')^{1/p} = (\tau_{ab} - 1)(x')^{1/p} = 1, \quad (\tau_{bc} - 1)(x')^{1/p} = \zeta.$$

Therefore,

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

for some  $u' \in F_{a,c}^\times$ . In particular,  $x' = N_a(u')$ . A similar computation shows that

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

for some  $u \in F_{a,c}^\times$ . 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 we are given  $u, u' \in F_{a,c}^\times$  such that

$$\alpha \cdot (\sigma_a - 1)u = \gamma \cdot (\sigma_c - 1)u', \quad x = N_c(u), \quad x' = N_a(u').$$

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

$$N_c\left(\frac{x}{u^p}\right) = \frac{N_c(x)}{N_c(u^p)} = \frac{x^p}{u^p} = 1,$$

$$N_a\left(\frac{x'}{(u')^p}\right) = \frac{N_a(x')}{N_a((u')^p)} = \frac{(x')^p}{(u')^p} = 1,$$

$$(\sigma_a - 1)\left(\frac{x}{u^p}\right) = \frac{b}{\alpha^p \cdot (\sigma_a - 1)u^p} = \frac{b}{\gamma^p \cdot (\sigma_c - 1)(u')^p} = (\sigma_c - 1)\left(\frac{x'}{(u')^p}\right).$$

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  $L := K_y$  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 can check that this definition is compatible with relations (2.4)–(2.7), and hence that it makes  $L$  into a Galois  $U_4$ -algebra such that  $L^{Z_4} = K$ .  $\square$

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) We have  $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$  in  $H^2(F, \mathbb{Z}/p\mathbb{Z})$ .
- (2) The Massey product  $\langle \chi_1, \chi_2, \chi_3 \rangle \subset H^2(F, \mathbb{Z}/p\mathbb{Z})$  is defined.
- (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  $\text{char}(F) \neq p$  and  $F$  contains a primitive  $p$ th root of unity, and it follows [MT16, Proposition 4.14].

Consider the short exact sequence

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

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

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

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

Suppose that  $\text{char}(F) \neq p$ . 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  $F$ . Thus, we may assume that  $F$  contains a primitive  $p$ th root of unity  $\zeta$ .

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  $\text{Br}(F)$ , 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  $u := \sigma_c(t)$  and  $u' := t^{-1}$ . 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  $x := N_c(u) \in F_a^\times$  and  $x' := N_a(u') \in F_c^\times$ . Since  $\sigma_a \sigma_c = \sigma_c \sigma_a$  on  $F_{a,c}^\times$ ,

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

Similarly,  $(\sigma_c - 1)x' = b/\gamma^p$ . Therefore,  $x, x'$  satisfy (3.9). Let  $K := (F_{a,b,c})_{x,x'}$  be the Galois  $\overline{U}_4$ -algebra over  $F$ , with the  $\overline{U}_4$ -action given by (3.10)–(3.13). By Proposition 3.5, there exists a Galois  $U_4$ -algebra  $L$  over  $F$  such that  $L^{\mathbb{Z}_4} \simeq (F_{a,b,c})_{x,x'}$  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.  $\square$

### 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 §2.1.

**PROPOSITION 3.7.** *Let  $a, b, c, d \in F^\times$  be such that  $(a, b) = (b, c) = (c, d) = 0$  in  $\text{Br}(F)$ . 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*

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

*Proof.* Denote by  $U_4^+$  and  $U_4^-$  the top-left and bottom-right  $4 \times 4$  corners of  $U_5$ , respectively, and let  $S := U_4^+ \cap U_4^-$  be the middle subgroup  $U_3$ . Let  $Q_4^+$  and  $Q_4^-$  be the kernels of the maps  $U_4^+ \rightarrow (\mathbb{Z}/p\mathbb{Z})^3$  and  $U_4^- \rightarrow (\mathbb{Z}/p\mathbb{Z})^3$ , respectively, and let  $P_4^+$  and  $P_4^-$  be the kernels of the maps  $U_4^+ \rightarrow U_3$  and  $U_4^- \rightarrow U_3$ , 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  $x' := N_c(u')$  and  $x := N_a(u)$ , 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  $z := N_d(v)$  and  $z' := N_b(v')$ , 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

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

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

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

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

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

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

LEMMA 3.8. *Let  $b, c \in F^\times$  and  $w \in F_{b,c}^\times$ . We have  $(\sigma_b - 1)(\sigma_c - 1)w = 1$  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,  $w_b \in F_b^\times$ .  $\square$

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  $\zeta$ , 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  $w_0 \in F_{b,c}^\times$  such that

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

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

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

## 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  $\zeta$ .

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  $\text{Br}(K)$  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  $F_b$ . (Recall that we write  $(\mathbb{P}_b^{p-1}$  for  $\mathbb{P}_{F_b}^{p-1}$ .) By [GS17, Theorem 5.4.1], the central simple algebra  $(b, c)$  is split over  $F(X)$ .

We define the degree map  $\deg: \text{Pic}(X) \rightarrow \mathbb{Z}$  as the composite of the pullback map  $\text{Pic}(X) \rightarrow \text{Pic}(X_b) \simeq \text{Pic}(\mathbb{P}_b^{p-1})$  and the degree isomorphism  $\text{Pic}(\mathbb{P}_b^{p-1}) \rightarrow \mathbb{Z}$ . 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  $G_b := \text{Gal}(F_b/F)$  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*

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

- (2) *If  $(b, c) \neq 0$  in  $\text{Br}(F)$ , the image of  $\deg: \text{Pic}(X) \rightarrow \mathbb{Z}$  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

$$\text{div}(w) = x - y \quad \text{in } \text{Div}(X_{b,c}),$$

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  $z: G_b \rightarrow \text{PGL}_p(F_b)$  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  $[z] \in H^1(G_b, \text{PGL}_p(F_b))$  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  $X_b \simeq \mathbb{P}_b^{p-1}$ , where  $G_b$  acts on  $X_b$  via its action on  $F_b$ , and on  $\mathbb{P}_b^{p-1}$  via the cocycle  $z$ . This proves (1).

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

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

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

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

Consider the linear form  $l := \sum_{i=1}^p c^{i/p} \cdot s_i$  on  $\mathbb{P}_{b,c}^{p-1}$  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  $x', y' \in \text{Div}(\mathbb{P}_{b,c}^{p-1})$  be the classes of the linear subspaces of  $\mathbb{P}_{b,c}^{p-1}$  given by  $l = 0$  and  $s_p = 0$ , respectively. Then

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

Define

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

Then  $w, x, y$  satisfy the conclusion of (3).  $\square$

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

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

where  $\varphi(u, v) := N_a(u)N_d(v)$  and  $\psi(z) = (\sigma_b - 1)(\sigma_c - 1)z$ , is exact. Furthermore, the torus  $\text{Im}(\varphi) = \text{Ker}(\psi)$  has dimension  $2p - 1$ .

*Proof.* By Lemma 3.8, we have an exact sequence

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

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

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

Since the homomorphisms  $N_a$  and  $N_d$  are surjective, so is  $N_a \times N_d$ . We conclude that  $\text{Im}(\varphi) = \text{Im}(\varphi') = \text{Ker}(\psi)$ , as desired. Finally, it is immediate to see that  $\text{Ker}(\varphi') = \mathbb{G}_m$ , embedded anti-diagonally in  $R_c(\mathbb{G}_m) \times R_b(\mathbb{G}_m)$ . Thus,

$$\dim(\text{Im}(\varphi)) = \dim(\text{Im}(\varphi')) = 2p - \dim(\text{Ker}(\varphi')) = 2p - 1. \quad \square$$

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  $F$ :

$$P := R_{a,c}(\mathbb{G}_m) \times R_{b,d}(\mathbb{G}_m), \quad S := \text{Ker}(\psi) = \text{Im}(\varphi), \quad T := \text{Ker}(\varphi) \subset P.$$

By Lemma 4.2, we get a short exact sequence

$$1 \rightarrow T \xrightarrow{\iota} P \xrightarrow{\pi} S \rightarrow 1, \quad (4.1)$$

where  $\iota$  is the inclusion map and  $\pi$  is induced by  $\varphi$ .

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  $Q \subset R_{a,c}(\mathbb{G}_m)$ , which makes the following commutative square cartesian.

$$\begin{array}{ccc} Q & \hookrightarrow & R_{a,c}(\mathbb{G}_m) \\ \downarrow & & \downarrow N_a \\ \mathbb{G}_m & \hookrightarrow & R_c(\mathbb{G}_m) \end{array} \quad (4.2)$$

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

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

$$1 \rightarrow U \rightarrow T \rightarrow Q.$$

We have  $\dim(U) = p(p-1)$ , and we see from the cartesian square (4.2) that  $\dim(Q) = p^2 - p + 1$ . By Lemma 4.2, we have  $\dim(S) = 2p - 1$ . From (4.1), we deduce that

$$\dim(T) = \dim(P) - \dim(S) = 2p^2 - (2p - 1) = 2p^2 - 2p + 1.$$

Therefore,  $\dim(T) = \dim(U) + \dim(Q)$ , and so the sequence

$$1 \rightarrow U \rightarrow T \rightarrow Q \rightarrow 1$$

is exact. As  $U$  and  $Q$  are tori, so is  $T$ .  $\square$

**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  $\zeta$ , and let  $a, b, c, d \in F^\times$ . Suppose that  $(a, b) = (b, c) = (c, d) = 0$  in  $\text{Br}(F)$ , and let  $w \in F_{b,c}^\times$  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 over  $F$  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 over  $K$  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.* Suppose that the Massey product  $\langle a, b, c, d \rangle$  is defined over  $F$ . By Proposition 3.9, there exist  $u \in F_{a,c}^\times$ ,  $v \in F_{b,d}^\times$  such that  $N_a(u)N_d(v) = w^p$ . This means precisely that  $E_w \subset P$  has the  $F$ -point  $(u, v)$ . Thus, the  $T$ -torsor  $E_w$  is trivial.

Conversely, suppose that the  $T$ -torsor  $E_w$  is trivial and let  $(u, v)$  be an  $F$ -point of  $E_w$ . Then we have  $N_a(u)N_d(v) = w^p$  and, by assumption, we also have  $(\sigma_b - 1)(\sigma_c - 1)w = \zeta$ . Proposition 3.7 now implies that the Massey product  $\langle a, b, c, d \rangle$  is defined over  $F$ .  $\square$

**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  $\zeta$ , and let  $a, b, c, d \in F^\times$  be such that  $(a, b) = (c, d) = 0$  in  $\text{Br}(F)$ . 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  $N_a(u)N_d(v) = w^p$ .*

*The Massey product  $\langle a, b, c, d \rangle$  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  $F(X)$ .  $\square$

## 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  $\zeta$ . 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  $G = \text{Gal}(K/F) = \langle \sigma_a, \sigma_b, \sigma_c, \sigma_d \rangle$  as in § 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  $\mathbb{Z}[G] \rightarrow \mathbb{Z}[G/H]$ . We define  $N_b$ ,  $N_c$  and  $N_d$  in a similar way.

Let

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

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

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

By definition of  $P$  and  $S$ ,

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

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

$$1 \rightarrow T(K) \rightarrow T(K(X)) \xrightarrow{\text{div}} \text{Div}(X_K) \otimes T_* \xrightarrow{\text{deg}} T_* \rightarrow 0, \quad (5.1)$$

where  $T_*$  denotes the cocharacter lattice of  $T$ .

LEMMA 5.1.

- (1) We have  $(T_*)^G = \mathbb{Z} \cdot \eta$ , where  $\iota_*(\eta) = (N_a N_c, -N_b N_d)$  in  $(P_*)^G$ .
- (2) If  $(b, c) \neq 0$  in  $\text{Br}(F)$ , the image of  $\text{deg}: (\text{Div}(X_{b,c}) \otimes T_*)^G \rightarrow (T_*)^G$  is equal to  $p(T_*)^G$ .

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

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

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

is equal to  $p(T_*)^G$ . Thus, the image of the degree map contains  $p(T_*)^G$ .

We now show that the image of 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

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

yield an isomorphism of  $G$ -modules

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

To conclude, it suffices to show that the image of

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

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

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

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

Suppose that  $G = H$ . Then  $\text{deg}(x') = \text{deg}(x)$  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 that  $\langle \sigma_b, \sigma_d \rangle$  is not contained in  $H$  and let  $N$  be the subgroup generated by  $H, \sigma_b, \sigma_d$ . Note that  $H$  is a proper subgroup of  $N$ .



The norm map  $N_{G/H} : (T_*)^H \rightarrow (T_*)^G$  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  $(T_*)^H \rightarrow (T_*)^N$  is multiplication by  $[N:H] \in p\mathbb{Z}$  on the first component of  $T_*$  with respect to the inclusion  $\iota_*$  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  $\iota_*(\eta) = (N_a N_c, -N_b N_d)$  in  $(P_*)^G$ . Since  $N_a N_c$  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. The proof in the case when  $\langle \sigma_a, \sigma_c \rangle$  is not contained in  $H$  is entirely analogous.  $\square$

We write

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

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

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

and the homomorphism

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

which are defined in (B.3).

LEMMA 5.2. *Let  $b, c \in F^\times$  be such that  $(b, c) \neq 0$  in  $\text{Br}(F)$  and let  $w \in F_{b,c}(X)^\times$  be such that  $(\sigma_b - 1)(\sigma_c - 1)w = \zeta$  and  $\text{div}(w) = x - y$ , 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  $[E_w] \in H^1(G, T(K(X)))_{\text{nr}}$ .*

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

*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 the Severi–Brauer variety  $X$  of  $(b, c)$  over  $F$ .

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

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

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

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

sends the divisor  $\operatorname{div}(w) = x - y$  to  $\sum_{i,j=0}^{p-1} \sigma_b^i \sigma_c^j (x - y) \otimes \sigma_b^i \sigma_c^j$ . Therefore, the element  $\operatorname{div}(w^p)$  in  $(\operatorname{Div}(X_K) \otimes S_*)^G \subset (\operatorname{Div}(X_K) \otimes \mathbb{Z}[G/H])^G$  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  $G$ -sublattice of  $\mathbb{Z}[G/\langle \sigma_a, \sigma_d \rangle]$  generated by  $N_b$  and  $N_c$ , this implies that  $e$  belongs to  $(\operatorname{Div}(X_K) \otimes S_*)^G$ . Then  $e = \pi_*(f)$ , where

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

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

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

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

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

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

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:

$$1 \rightarrow T \rightarrow P \rightarrow S \rightarrow 1.$$

Let  $w \in L_{b,c}(X)$  be as in Lemma 4.1(3), and 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  $C^*(\Gamma_L, \mathbb{Z}/p\mathbb{Z})$  is not formal.  $\square$

## Appendix A. Homological algebra

Let  $G$  be a profinite group, and let

$$0 \rightarrow A_0 \xrightarrow{\alpha_0} A_1 \xrightarrow{\alpha_1} A_2 \xrightarrow{\alpha_2} A_3 \rightarrow 0 \quad (\text{A.1})$$

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

$$\begin{aligned} 0 \rightarrow A_0 \xrightarrow{\alpha_0} A_1 \rightarrow A \rightarrow 0, \\ 0 \rightarrow A \rightarrow A_2 \xrightarrow{\alpha_2} A_3 \rightarrow 0. \end{aligned}$$

We obtain a homomorphism

$$\theta: \operatorname{Ker}[H^1(G, A_1) \xrightarrow{\alpha_1} H^1(G, A_2)] \rightarrow \operatorname{Coker}[A_2^G \xrightarrow{\alpha_2} A_3^G], \quad (\text{A.2})$$

which is defined as the composition of the map

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

and the inverse of the isomorphism

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

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

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

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

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

*Proof.* The proof follows from the definition of  $\theta$  and the exactness of (A.1).  $\square$

Consider a commutative diagram of discrete  $G$ -modules with exact rows and columns.

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

It yields a commutative diagram of abelian groups where the columns are exact and the rows are complexes.

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

Suppose that the connecting homomorphism  $\partial_1: C_1^G \rightarrow H^1(G, A_1)$  is surjective. We define a function

$$\theta': \mathrm{Ker}[H^1(G, A_1) \xrightarrow{\alpha_1} H^1(G, A_2)] \rightarrow \mathrm{Coker}(A_2^G \xrightarrow{\alpha_2} A_3^G)$$

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 third column and the injectivity of  $\iota_3$ , 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  $\theta'$  is a well-defined homomorphism.

LEMMA A.2. *Let  $G$  be a profinite group, and suppose that we are given an exact sequence (A.1) and a commutative diagram (A.4) such that the connecting homomorphism  $\partial_1: C_1^G \rightarrow H^1(G, A_1)$  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  $\partial_1: C_1^G \rightarrow H^1(G, A_1)$  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  $\iota_1(a_{1g}) = gb_1 - b_1$ . 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,

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

Finally,

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

By definition,  $\theta'(z) = -\alpha_2(a_2) + \alpha_2(A_2^G)$ . Observe that  $\alpha_2(a_2)$  belongs to  $A_3^G$  because, for every  $g \in G$ ,

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

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

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

induced by the map  $A_1 \rightarrow A$ , 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  $A \rightarrow A_2$  sends  $a_g$  to  $ga_2 - a_2$  for all  $g \in G$ . Therefore, the connecting map  $A_3^G \rightarrow H^1(G, A)$  sends  $\alpha_2(a_2)$  to the class of  $\{a_g\}_{g \in G}$ . It follows that the isomorphism

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

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

## 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  $G := \text{Gal}(K/F)$ . We have an exact sequence of discrete  $G$ -modules

$$1 \rightarrow K^\times \rightarrow K(X)^\times \xrightarrow{\text{div}} \text{Div}(X_K) \xrightarrow{\lambda} \text{Pic}(X_K) \rightarrow 0, \quad (\text{B.1})$$

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

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

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

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

We define the subgroup of unramified torsors

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

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

$$\theta: H^1(G, T(K(X)))_{\text{nr}} \rightarrow \text{Coker}[(\text{Div}(X_K) \otimes T_*)^G \xrightarrow{\lambda} (\text{Pic}(X_K) \otimes T_*)^G]. \quad (\text{B.3})$$

PROPOSITION B.1. We have an exact sequence

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

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

*Proof.* This is a special case of Lemma A.1.  $\square$

By Lemma A.2, the map  $\theta$  may be computed as follows. Let

$$1 \rightarrow T \xrightarrow{\iota} P \xrightarrow{\pi} S \rightarrow 1 \quad (\text{B.4})$$

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

$$0 \rightarrow T_* \xrightarrow{\iota_*} P_* \xrightarrow{\pi_*} S_* \rightarrow 0. \quad (\text{B.5})$$

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.

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

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

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

$$\theta(\tau) = -t. \quad (\text{B.7})$$

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

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

We have the inflation–restriction sequence

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

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  $H^1(F, T(F_s(X))) \rightarrow H^1(F(X), T)$  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

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

the map  $\theta$  of (A.2) takes the form

$$\theta: H^1(F(X), T)_{\text{nr}} \rightarrow \text{Coker}[(\text{Div}(X_s) \otimes T_*)^{\Gamma_F} \rightarrow (\text{Pic}(X_s) \otimes T_*)^{\Gamma_F}].$$

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

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

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

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

#### ACKNOWLEDGEMENTS

We thank the anonymous referee for carefully reading our manuscript and for sending us comments which greatly improved the exposition.

#### CONFLICTS OF INTEREST

None.

#### JOURNAL INFORMATION

*Compositio Mathematica* is owned by the Foundation Compositio Mathematica and published by the London Mathematical Society in partnership with Cambridge University Press. All surplus income from the publication of *Compositio Mathematica* is returned to mathematics and higher education through the charitable activities of the Foundation, the London Mathematical Society and Cambridge University Press.

#### REFERENCES

- AB08 P. Abramenko and K. S. Brown, *Buildings*, Graduate Texts in Mathematics, vol. 248 (Springer, New York, 2008).
- BD01 D. K. Biss and S. Dasgupta, *A presentation for the unipotent group over rings with identity*, J. Algebra **237** (2001), 691–707.
- Dwy75 W. G. Dwyer, *Homology, Massey products and maps between groups*, J. Pure Appl. Algebra **6** (1975), 177–190.
- Efr14 I. Efrat, *The Zassenhaus filtration, Massey products, and representations of profinite groups*, Adv. Math. **263** (2014), 389–411.
- EM17 I. Efrat and E. Matzri, *Triple Massey products and absolute Galois groups*, J. Eur. Math. Soc. (JEMS) **19** (2017), 3629–3640.
- GS17 P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, second edition, vol. 165 (Cambridge University Press, Cambridge, 2017).
- GMT18 P. Guillot, J. Mináč and A. Topaz, *Four-fold Massey products in Galois cohomology*, Compositio Math. **154** (2018), 1921–1959, with an appendix by O. Wittenberg.
- HW19 C. Haesemeyer and C. A. Weibel, *The norm residue theorem in motivic cohomology*, Annals of Mathematics Studies, vol. 200 (Princeton University Press, Princeton, NJ, 2019).
- HW23 Y. Harpaz and O. Wittenberg, *The Massey vanishing conjecture for number fields*, Duke Math. J **172** (2023), 1–41.
- HW15 M. J. Hopkins and K. G. Wickelgren, *Splitting varieties for triple Massey products*, J. Pure Appl. Algebra **219** (2015), 1304–1319.

- KMRT98 M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44 (American Mathematical Society, Providence, RI, 1998), with a preface in French by J. Tits.
- Mat18 E. Matzri, *Triple Massey products of weight  $(1, n, 1)$  in Galois cohomology*, J. Algebra **499** (2018), 272–280.
- MS22 A. Merkurjev and F. Scavia, *Degenerate fourfold Massey products over arbitrary fields*, J. Eur. Math. Soc., to appear. Preprint (2022), [arXiv:2208.13011](#).
- MS23 A. Merkurjev and F. Scavia, *The Massey vanishing conjecture for fourfold Massey products modulo 2*, Ann. Sci. Éc. Norm. Supér., to appear. Preprint (2023), [arXiv:2301.09290](#).
- MT16 J. Mináč and N. D. Tân, *Triple Massey products vanish over all fields*, J. Lond. Math. Soc. (2) **94** (2016), 909–932.
- MT17a J. Mináč and N. D. Tân, *Counting Galois  $\mathbb{U}_4(\mathbb{F}_p)$ -extensions using Massey products*, J. Number Theory **176** (2017), 76–112.
- MT17b J. Mináč and N. D. Tân, *Triple Massey products and Galois theory*, J. Eur. Math. Soc. (JEMS) **19** (2017), 255–284.
- PQ22 A. Pál and G. Quick, *Real projective groups are formal*, Math. Ann. **392** (2025), 1833–1876; [MR4906311](#).
- PS18 A. Pál and E. Szabó, *The strong Massey vanishing conjecture for fields with virtual cohomological dimension at most 1*, Preprint (2018), [arXiv:1811.06192](#).
- Pos11 L. Positselski, *Mixed Artin-Tate motives with finite coefficients*, Mosc. Math. J. **11** (2011), 317–402, 407–408.
- Pos17 L. Positselski, *Koszulity of cohomology =  $K(\pi, 1)$ -ness + quasi-formality*, J. Algebra, **483** (2017), 188–229.
- Ser79 J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67 (Springer-Verlag, New York–Berlin, 1979), translated from the French by M. J. Greenberg.
- Ser97 J.-P. Serre, *Galois cohomology* (Springer-Verlag, Berlin, 1997), translated from the French by P. Ion and revised by the author.

Alexander Merkurjev [merkurev@math.ucla.edu](mailto:merkurev@math.ucla.edu)

Department of Mathematics, University of California, Los Angeles, CA 90095, USA

Federico Scavia [scavia@math.ucla.edu](mailto:scavia@math.ucla.edu)

Department of Mathematics, University of California, Los Angeles, CA 90095, USA