



Alexander Merkurjev · Federico Scavia

# Degenerate fourfold Massey products over arbitrary fields

Received 1 September 2022; revised 11 October 2023

**Abstract.** We prove that, for all fields  $F$  of characteristic different from 2 and all  $a, b, c \in F^\times$ , the mod 2 Massey product  $\langle a, b, c, a \rangle$  vanishes as soon as it is defined. For every field  $F_0$ , we construct a field  $F$  containing  $F_0$  and  $a, b, c, d \in F^\times$  such that  $\langle a, b, c \rangle$  and  $\langle b, c, d \rangle$  vanish but  $\langle a, b, c, d \rangle$  is not defined. As a consequence, we answer a question of Positselski by constructing the first examples of fields containing all roots of unity and such that the mod 2 cochain differential graded algebra of the absolute Galois group is not formal.

*Keywords:* Massey products, Galois cohomology, absolute Galois group, formality, Brauer group.

## 1. Introduction

A fundamental and difficult problem in Galois theory is to characterize those profinite groups which are realizable as absolute Galois groups of fields. The first result in this direction is due to Artin and Schreier, who proved that the only non-trivial finite subgroups of an absolute Galois group are cyclic of order 2. The structure of absolute Galois groups of general fields has been investigated by a large number of authors. The highlights of this theory are the study of projective profinite groups, pseudo-algebraically closed fields, the  $p$ -descending series and the  $p$ -Zassenhaus series, where  $p$  is a prime number.

Another approach to this problem is to find constraints on the cohomology of absolute Galois groups. The most spectacular development in this direction is the proof of the Bloch–Kato conjecture by Rost and Voevodsky. This gives very strong restrictions on the mod  $p$  cohomology of the absolute Galois group of a field of characteristic not  $p$  and containing a primitive  $p$ -th root of unity: it admits a presentation with generators in degree 1 and relations in degree 2.

---

Alexander Merkurjev: Department of Mathematics, University of California at Los Angeles, 520 Portola Plaza, Box 951555, Los Angeles, CA 90095-1555, USA; [merkurev@math.ucla.edu](mailto:merkurev@math.ucla.edu)

Federico Scavia: Department of Mathematics, University of California at Los Angeles, 520 Portola Plaza, Box 951555, Los Angeles, CA 90095-1555, USA; CNRS and Institut Galilée – LAGA, Université Sorbonne Paris Nord, 99 Avenue Jean-Baptiste Clément, 93430 Villetaneuse, France; [scavia@math.univ-paris13.fr](mailto:scavia@math.univ-paris13.fr)

*Mathematics Subject Classification 2020:* 12G05 (primary); 55S30, 11E04 (secondary).

Let  $p$  be a prime number, let  $F$  be a field, and let  $\Gamma_F$  be the absolute Galois group of  $F$ . For all  $n \geq 3$  and all  $\chi_1, \dots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$ , we denote by

$$\langle \chi_1, \dots, \chi_n \rangle \subset H^2(F, \mathbb{Z}/p\mathbb{Z})$$

the Massey product of  $\chi_1, \dots, \chi_n$ ; see Section 2 for the definition. We say  $\langle \chi_1, \dots, \chi_n \rangle$  is defined if it is non-empty, and that it vanishes if it contains 0. In [9], Hopkins and Wickelgren proved that all defined Massey products vanish when  $n = 3$ ,  $p = 2$  and  $F$  is a number field. In [18], Mináč and Tân generalized this result to the case when the field  $F$  is arbitrary, and formulated the following conjecture.

**Conjecture 1.1** (Mináč, Tân). *For every field  $F$ , every prime  $p$ , every  $n \geq 3$  and all  $\chi_1, \dots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$ , if the Massey product  $\langle \chi_1, \dots, \chi_n \rangle \subset H^2(F, \mathbb{Z}/p\mathbb{Z})$  is defined, then it vanishes.*

It was observed by Mináč and Tân that all mod  $p$  Massey products are defined and vanish when  $F$  has characteristic  $p$ ; see [18, Remark 4.1]. Therefore, for the purpose of proving Conjecture 1.1 one may assume that  $\text{char}(F) \neq p$ . Moreover, if  $F$  contains a primitive  $p$ -th root of unity (this is automatic if  $p = 2$ ), then by Kummer theory homomorphisms  $\Gamma_F \rightarrow \mathbb{Z}/p\mathbb{Z}$  correspond to elements of  $F^\times/F^{\times p}$ , and hence we may talk about Massey products of elements of  $F^\times$ . In this case, Conjecture 1.1 is equivalent to the prediction that for all  $a_1, \dots, a_n \in F^\times$ , the Massey product  $\langle a_1, \dots, a_n \rangle$  vanishes as soon as it is defined.

Conjecture 1.1 has stimulated a large number of works in recent years. It is now known to be true when  $n = 3$ , for all fields  $F$  and primes  $p$ , by work of Efrat and Matzri and of Mináč and Tân [5, 13, 16]. Conjecture 1.1 is also known when  $F$  is a number field, by Guillot, Mináč, Topaz and Wittenberg [7] in the case  $p = 2$  and  $n = 4$ , and Harpaz and Wittenberg [8] in the case of arbitrary  $p$  and  $n \geq 3$ .

If  $n \geq 3$  and  $\langle \chi_1, \dots, \chi_n \rangle \subset H^2(F, \mathbb{Z}/p\mathbb{Z})$  is defined, then  $\chi_i \cup \chi_{i+1} = 0$  for all  $i = 1, \dots, n - 1$ ; see Remark 2.2. In [17, Question 4.2], Mináč and Tân asked whether the converse is also true.

**Question 1.2** (Mináč, Tân). *Let  $F$  be a field, let  $p$  be a prime number and let  $n \geq 3$  be an integer. Is it true that for all  $\chi_1, \dots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$  such that  $\chi_i \cup \chi_{i+1} = 0$  in  $H^2(F, \mathbb{Z}/p\mathbb{Z})$  for all  $i = 1, \dots, n - 1$ , the Massey product  $\langle \chi_1, \dots, \chi_n \rangle$  is defined?*

Again, if  $F$  contains a primitive  $p$ -th root of unity, by Kummer theory in Question 1.2 we may replace elements of  $H^1(F, \mathbb{Z}/p\mathbb{Z})$  by elements of  $F^\times$ . Question 1.2 has an affirmative answer when  $n = 3$ . Harpaz and Wittenberg produced a counterexample to Question 1.2, for  $n = 4$ ,  $p = 2$  and  $F = \mathbb{Q}$ ; see [7, Example A.15]. More precisely, if  $b = 2$ ,  $c = 17$  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  $\mathbb{Q}$ . We will refer to this example as the Harpaz–Wittenberg example. In contrast, [7, Theorem 6.2] shows that over any number field  $F$ , if  $a, b, c, d$  are independent in  $F^\times/F^{\times 2}$ , the identity  $(a, b) = (b, c) = (c, d) = 0$  in  $\text{Br}(F)$  implies that  $\langle a, b, c, d \rangle$  vanishes.

The aforementioned examples and results suggest studying Conjecture 1.1 and Question 1.2 for mod 2 Massey products of the form  $\langle a, b, c, a \rangle$ , or even  $\langle bc, b, c, bc \rangle$ , over an arbitrary field  $F$  of characteristic different from 2. Our first theorem is a proof of Conjecture 1.1 for all mod 2 Massey products of the form  $\langle a, b, c, a \rangle$ .

**Theorem 1.3.** *Let  $p = 2$ , let  $F$  be a field of characteristic different from 2, and let  $a, b, c, d \in F^\times$  be such that  $ad$  is a square in  $F$ . Then the Massey product  $\langle a, b, c, d \rangle$  vanishes if and only if it is defined.*

We can be more explicit when  $a = d = bc$ , that is, for Massey products of the form  $\langle bc, b, c, bc \rangle$ .

**Theorem 1.4.** *Let  $p = 2$ , let  $F$  be a field of characteristic different from 2, and let  $a, b, c, d \in F^\times$  be such that  $ad$  and  $abc$  are squares in  $F$ . Then the following are equivalent:*

- (1) *the Massey product  $\langle a, b, c, d \rangle$  is defined,*
- (2) *the Massey product  $\langle a, b, c, d \rangle$  vanishes,*
- (3)  *$(b, c) = 0$  in  $\text{Br}(F)$  and  $-1 \in N_{b,c}$ .*

Here  $N_{b,c}$  denotes the image of the norm map  $F_{b,c}^\times \rightarrow F^\times$ , where

$$F_{b,c} := F[x_b, x_c]/(x_b^2 - b, x_c^2 - c);$$

see the notation section below. In particular, Question 1.2 has a positive answer for mod 2 Massey products of the form  $\langle bc, b, c, bc \rangle$  if  $F$  contains a primitive 8-th root of unity. Condition (3) of Theorem 1.4 allows us to recover the Harpaz–Wittenberg example; see Proposition 5.3.

We say that a differential graded ring  $A$  is *formal* if it is quasi-isomorphic to its cohomology ring  $H^*(A)$ , viewed as a differential graded ring with zero differential. We write  $C^*(F, \mathbb{Z}/p\mathbb{Z})$  for the differential graded algebra (DGA) of mod  $p$  continuous cochains of  $\Gamma_F$ . If  $C^*(F, \mathbb{Z}/p\mathbb{Z})$  is formal, then Conjecture 1.1 holds for  $F$  and Question 1.2 has a positive answer for  $F$ ; see [19, Theorem 3.8].

In [9, Question 1.4], Hopkins and Wickelgren asked whether  $C^*(F, \mathbb{Z}/p\mathbb{Z})$  is formal for every field  $F$ . Positselski [22, Example 6.3] showed that the answer to this question is negative. More precisely, Positselski proved that  $C^*(F, \mathbb{Z}/p\mathbb{Z})$  is not formal when  $F$  is a local field of residue characteristic different from  $p$  and containing a primitive  $p$ -th root of unity if  $p$  is odd, or a square root of  $-1$  if  $p = 2$ . (In contrast, Conjecture 1.1 is known and Question 1.2 has an affirmative answer for local fields.) The Harpaz–Wittenberg example implies that  $C^*(F, \mathbb{Z}/p\mathbb{Z})$  is not formal for  $F = \mathbb{Q}$ .

Pál and Quick showed that  $C^*(F, \mathbb{Z}/2\mathbb{Z})$  is formal for every field  $F$  of cohomological dimension  $\leq 1$ ; see [19, Theorem 1.8]. (Pál and Szabó [21] had previously shown that Question 1.2 has a positive answer for such  $F$ .)

The following refinement of the question of Hopkins and Wickelgren, due to Positselski [22, p. 226], is well known among experts.

**Question 1.5** (Positselski). Do there exist a prime number  $p$  and a field  $F$  of characteristic different from  $p$  and containing all the  $p$ -power roots of unity such that  $C^*(F, \mathbb{Z}/p\mathbb{Z})$  is not formal?

We settle Question 1.5 in the affirmative.

**Theorem 1.6** (Theorem 6.3). *For every field  $F_0$  of characteristic different from 2, there exists a field extension  $F/F_0$  such that Question 1.2 has a negative answer for  $F$ ,  $p = 2$  and  $n = 4$ . In particular, Question 1.5 has a positive answer.*

It follows that Question 1.2 has a negative answer in general, even if  $F$  contains an algebraically closed subfield. (The more precise Theorem 6.3 (a) shows that we may even find counterexamples of the form  $\langle a, b, c, a \rangle$ . By Theorem 1.4, there are no such examples if we further assume that  $a = bc$ .) In view of the recent work of Quadrelli [23], it seems natural to amend Question 1.2 by requiring that  $F$  contains a square root of  $-1$  when  $p = 2$ . By Theorem 1.6, even this weakening of Question 1.2 has a negative answer.

The main ingredient in the proof of Theorem 1.6 is a new criterion for when a fourfold Massey product is defined; see Propositions 3.7 and 4.1 (a). As we explain below, this criterion also plays an important role in the proof of Theorem 1.3.

We now explain the main ideas of the proof of Theorem 1.3. For every  $n \geq 2$ , let  $U_{n+1} \subset \text{GL}_{n+1}(\mathbb{F}_2)$  be the group of unipotent upper triangular matrices, and let  $\bar{U}_{n+1}$  be the group of unipotent upper triangular matrices with entry  $(1, n + 1)$  erased; see (2.5). Given  $a, b, c, d \in F^\times$ , consider the Galois  $(\mathbb{Z}/2\mathbb{Z})^4$ -algebra

$$F_{a,b,c,d} := F[x_a, x_b, x_c, x_d]/(x_a^2 - a, x_b^2 - b, x_c^2 - c, x_d^2 - d),$$

where the first (resp. second, third, fourth) factor of  $(\mathbb{Z}/2\mathbb{Z})^4$  sends  $x_a$  (resp.  $x_b, x_c, x_d$ ) to its opposite and fixes the other three variables. By a theorem of Dwyer [4], the Massey product  $\langle a, b, c, d \rangle$  is defined (resp. vanishes) if and only if  $F_{a,b,c,d}/F$  can be embedded into a Galois  $\bar{U}_5$ -algebra (resp.  $U_5$ -algebra) over  $F$ ; see Corollary 2.6 for the precise statement.

If  $u \in F^\times$ , we let  $N_u$  be the image of the norm map  $F_u^\times \rightarrow F^\times$ , where  $F_u$  is the étale  $F$ -algebra  $F[x_u]/(x_u^2 - u)$ . Suppose that  $(a, b) = (b, c) = (c, d) = 0$  in  $\text{Br}(F)$ . (As we mentioned before Question 1.2, this condition is satisfied if  $\langle a, b, c, d \rangle$  is defined.) By a careful study of Galois  $U_3$ -algebras,  $U_4$ -algebras and  $\bar{U}_5$ -algebras over  $F$ , in Proposition 3.7 we associate to  $a, b, c, d$  a scalar  $e \in F^\times$ , uniquely determined in the quotient  $F^\times/N_a N_{ac} N_d N_{bd}$ , such that  $\langle a, b, c, d \rangle$  is defined if and only if  $e \in N_a N_{ac} N_d N_{bd}$ . The scalar  $e$  is defined in terms of a pair  $(\varepsilon, \nu) \in F_{a,c}^\times \times F_{b,d}^\times$  satisfying certain properties: roughly speaking,  $\varepsilon$  and  $\nu$  correspond to Galois  $U_4$ -algebras  $K_1/F$  and  $K_2/F$  inducing  $F_{a,b,c}/F$  and  $F_{b,c,d}/F$  (whose existence essentially amounts to the validity of Conjecture 1.1 for  $n = 3$  and  $p = 2$ ), and  $e$  measures the failure of  $K_1$  and  $K_2$  of being induced by a common Galois  $\bar{U}_5$ -algebra  $K/F$ .

Let  $\alpha \in F_a^\times$  and  $\delta \in F_d^\times$  be such that  $N_a(\alpha) = b$  and  $N_d(\delta) = c$  in  $F^\times$ . (Such  $\alpha$  and  $\delta$  exist because  $(a, b) = (c, d) = 0$ .) It was shown in [7, Theorem A] that  $\langle a, b, c, d \rangle$  vanishes if and only if there exist  $x, y \in F^\times$  such that  $(\alpha x, \delta y) = 0$  in  $\text{Br}(F_{a,d})$ ; see

Proposition 3.11 and Corollary 3.12 for a short proof. In order to prove Conjecture 1.1 for  $n = 4$  and  $p = 2$ , it suffices to show that our condition is equivalent to that of [7, Theorem A]. We are able to show the equivalence when  $a = d$ , thus proving Theorem 1.3, by the following strategy. Conjecture 1.1 is true when  $F$  is finite (see Corollary 2.5), hence we may suppose that  $F$  is infinite. Since  $(b, c) = 0$ , multiplying  $b$  and  $c$  by non-zero squares if necessary, we may suppose that  $b + c = 1$ , and since  $(a, b) = (c, d) = 0$ , there exist  $v_1, v_2, u_1, u_2 \in F^\times$  such that  $v_1^2 - bv_2^2 = a$  and  $u_1^2 - cu_2^2 = d$ . If  $v_1, v_2, u_1, u_2$  are general enough, we may use them to define three scalars  $r, s, t \in F^\times$ ; see below (4.1). The conclusion follows from the diagram of equivalences below:

$$\begin{array}{ccc}
 r \in N_a N_{ab} N_{ac} & \xleftrightarrow{\text{Proposition 4.2}} & s \in N_b N_{ab} N_{bc} & \xleftrightarrow{\text{Proposition 4.2}} & t \in N_c N_{ac} N_{bc} \\
 \Downarrow \text{Proposition 4.1 (a)} & & & & \Downarrow \text{Proposition 4.1 (b)} \\
 \langle a, b, c, a \rangle \text{ defined} & & & & \langle a, b, c, a \rangle \text{ vanishes.}
 \end{array}$$

We will prove the vertical equivalence on the left by showing that  $e = r$  in the group  $F^\times / N_a N_{ab} N_{ac}$  via an explicit computation; see Proposition 4.3. (Note that, when  $a = d$ , the subgroup  $N_a N_{ac} N_d N_{bd}$  is equal to  $N_a N_{ab} N_{ac}$ .) The equivalences in the top row are formal consequences of the identity  $(r, a) + (s, b) + (t, c) = 0$  in  $\text{Br}(F)$ , which is also proved by a computation; see Lemmas 4.8 and 4.9.

For the vertical equivalence on the right, we show that  $t \in N_c N_{ac} N_{bc}$  is equivalent to the condition of [7, Theorem A]. The key point is that, under the assumption  $a = d$ , the condition of [7, Theorem A] may be replaced by the system of two equations  $(\alpha x, \delta y) = 0$  and  $(\alpha x, c) = 0$  in  $\text{Br}(F_a)$ ; see Corollary 3.13. The first equation has a solution  $(x, y) \in F^\times \times F^\times$  if and only if  $x \in N_c N_{bc}$ : we prove this in Corollary 4.5 using the theory of Albert forms attached to biquaternion algebras. As we prove in Lemma 4.7, a scalar  $x \in F^\times$  solves the second equation if and only if  $x \in t N_c N_{ac}$ . All in all, the condition of [7, Theorem A] is satisfied if and only if  $t N_c N_{ac} \cap N_c N_{bc} \neq \emptyset$ , that is,  $t \in N_c N_{ac} N_{bc}$ . This proves the vertical equivalence on the right and completes our sketch of proof of Theorem 1.3.

We conclude this introduction by describing the content of each section. In Section 2, we collect the definitions and basic properties of Galois algebras and Massey products in Galois cohomology, and we recall Dwyer’s theorem, which connects the two notions. We then establish some specialization lemmas for Massey products, which will be used in the proof of Theorem 1.6. Section 3 is devoted to the proof of Propositions 3.5 and 3.7, which give the aforementioned equivalent condition for a fourfold Massey product to be defined. Some of our results may be interpreted in terms of splitting varieties; see Section 3.4. In Corollary 3.12, we give a proof of [7, Theorem A] using our methods, and in Corollary 3.13, we specialize to the case  $a = d$ . Section 4 is devoted to the proof of Propositions 4.1 and 4.2, from which Theorem 1.3 follows. In Section 5, we prove Theorem 1.4 and use it to recover the Harpaz–Wittenberg example. Theorem 1.6 is a direct consequence of Theorem 6.3, which is proved in Section 6. Finally, Appendix A contains some known results about biquadratic extensions which are used throughout the paper.

*Notation*

In this paper, we let  $F$  be a field,  $F_{\text{sep}}$  be a separable closure of  $F$ , and  $\Gamma_F := \text{Gal}(F_{\text{sep}}/F)$  be the absolute Galois group of  $F$ . We often use additive notation while working with elements of  $\Gamma_F$ : for all  $\sigma, \tau \in \Gamma_F$  and  $x \in F$ , we have

$$(\sigma + \tau)(x) = \sigma(x)\tau(x) \quad \text{and} \quad (\sigma\tau)(x) = \sigma(\tau(x)).$$

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

Suppose that  $\text{char}(F) \neq 2$ . 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

$$E_{a_1, \dots, a_n} := E[x_1, \dots, x_n]/(x_1^2 - a_1, \dots, x_n^2 - a_n),$$

and we set  $\sqrt{a_i} := x_i$ . Thus, for all  $a \in F^\times$ , the elements  $1, \sqrt{a}$  form an  $F$ -basis of  $F_a$ . We denote by  $R_{a_1, \dots, a_n}(-)$  the Weil restriction functor along  $F_{a_1, \dots, a_n}/F$ . If  $u \in F_{a_1, \dots, a_n}$ , we denote by  $N_{a_1, \dots, a_n}(u)$  and  $\text{Tr}_{a_1, \dots, a_n}(u)$  the norm and trace of  $u$  with respect to  $F_{a_1, \dots, a_n}/F$ , respectively. We also let  $N_{a_1, \dots, a_n}$  be the image of the norm map.

We write  $\text{Br}(F)$  for the Brauer group of  $F$ . The group operation on  $\text{Br}(F)$  is denoted additively. If  $\text{char}(F) \neq 2$  and  $a, b \in F^\times$ , we write  $(a, b)$  for the corresponding quaternion algebra over  $F$  and for its class in  $\text{Br}(F)$ . We write  $N_{a_1, \dots, a_n}: \text{Br}(F_{a_1, \dots, a_n}) \rightarrow \text{Br}(F)$  for the corestriction map along  $F_{a_1, \dots, a_n}/F$ .

An  $F$ -variety is a separated integral  $F$ -scheme of finite type. If  $X$  is an  $F$ -variety, we denote by  $F(X)$  the function field of  $X$ . If  $x$  is a point of  $X$ , we denote by  $O_{X,x}$  the local ring of  $X$  at  $x$  and by  $F(x)$  the residue field of  $x$ .

**2. Preliminaries**

*2.1. Galois algebras*

Let  $G$  be a finite (abstract) group. By definition, a  $G$ -algebra  $L/F$  is an étale  $F$ -algebra on which  $G$  acts via  $F$ -algebra automorphisms. We say that the  $G$ -algebra  $L$  is *Galois* if  $|G| = \dim_F L$  and  $L^G = F$ ; see [11, 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. By [11, Example 28.15], we have a canonical bijection

$$H^1(F, G) \xrightarrow{\sim} \{\text{Isomorphism classes of Galois } G\text{-algebras over } F\} \quad (2.1)$$

which is functorial in  $F$  and  $G$ .

Suppose now that  $G = N \rtimes S$ , where  $N$  is a normal subgroup of  $G$  and  $S$  is a subgroup of  $G$ . Let  $E$  be a Galois  $S$ -algebra over  $F$ , and let  $\pi: \Gamma_F \rightarrow S$  be a continuous group homomorphism whose class in  $H^1(F, S)$  coincides with the class of  $E/F$ . The

group  $S$  acts on  $N$  by conjugation. We view  $N$  as a  $\Gamma_F$ -module via  $\pi$ , and we write  $N_\pi$  for the twist; see [11, §28.C]. We have a canonical bijection

$$H^1(F, N_\pi) \xrightarrow{\sim} \left\{ \begin{array}{l} \text{Isomorphism classes of pairs } (K, \varphi), \\ \text{where } K/F \text{ is a Galois } G\text{-algebra} \\ \text{and } \varphi: K^N \rightarrow E \text{ is an isomorphism of Galois } S\text{-algebras} \end{array} \right\}, \quad (2.2)$$

which is functorial in  $F$ . Here, an isomorphism of pairs  $(K, \varphi) \rightarrow (K', \varphi')$  is defined as an isomorphism of Galois  $G$ -algebras  $\sigma: K \rightarrow K'$  over  $F$  such that  $\varphi = \varphi' \circ \sigma$  on  $K^N$ . Under the identification of (2.2), the surjective twisting map

$$H^1(F, N_\pi) \rightarrow \text{Fiber}_\pi[H^1(F, G) \rightarrow H^1(F, S)] \quad (2.3)$$

of [11, Proposition 28.11] sends the class of a pair  $(K, \varphi)$  to the class of  $K$ .

2.2. Kummer theory

Suppose that  $\text{char}(F) \neq 2$ . Then  $\mathbb{Z}/2\mathbb{Z} \simeq \mu_2$  over  $F$ , and so the Kummer sequence yields an isomorphism

$$\text{Hom}(\Gamma_F, \mathbb{Z}/2\mathbb{Z}) = H^1(F, \mathbb{Z}/2\mathbb{Z}) \simeq H^1(F, \mu_2) \simeq F^\times / F^{\times 2}. \quad (2.4)$$

For every  $a \in F^\times$ , we let  $\chi_a: \Gamma_F \rightarrow \mathbb{Z}/2\mathbb{Z}$  be the homomorphism corresponding to the coset  $aF^{\times 2}$  under (2.4). Explicitly, letting  $a' \in F_{\text{sep}}^\times$  be such that  $(a')^2 = a$ , we have  $g(a') = (-1)^{\chi_a(g)} a'$  for all  $g \in \Gamma_F$ . The definition of  $\chi_a$  does not depend on the choice of  $a'$ .

Now let  $n \geq 1$ . For all  $i = 1, \dots, n$ , let  $\sigma_i$  be the canonical generator of the  $i$ -th factor  $\mathbb{Z}/2\mathbb{Z}$  of  $(\mathbb{Z}/2\mathbb{Z})^n$ . It follows from (2.4) that all Galois  $(\mathbb{Z}/2\mathbb{Z})^n$ -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  $(\mathbb{Z}/2\mathbb{Z})^n$ -algebra structure is defined by  $\sigma_i(\sqrt{a_i}) = -\sqrt{a_i}$  for all  $i$  and  $\sigma_i(\sqrt{a_j}) = \sqrt{a_j}$  for all  $j \neq i$ . The elements  $a_1, \dots, a_n$  are uniquely determined modulo  $F^{\times 2}$ .

The Kummer sequence provides a group isomorphism

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

For all  $a, b \in F^\times$ ,  $\iota(\chi_a \cup \chi_b)$  is equal to  $(a, b)$ ; see [24, Chapter XIV, Proposition 5]. The next lemma is well known and will be used several times in what follows.

**Lemma 2.1.** *Suppose that  $\text{char}(F) \neq 2$  and let  $a, b \in F^\times$ . The following are equivalent:*

- (i)  $(a, b) = 0$  in  $\text{Br}(F)$ ;
- (ii)  $b \in N_a$ ;
- (iii)  $a \in N_b$ ;
- (iv) *the smooth projective  $F$ -conic of equation  $aX^2 + bY^2 = Z^2$  has an  $F$ -point (equivalently, it is isomorphic to  $\mathbb{P}_F^1$ ).*

*Proof.* See [6, Propositions 1.1.7 and 1.3.2]. ■

2.3. Massey products

Let  $(A, \partial)$  be a DGA over  $\mathbb{F}_2$ , that is, a graded associative  $\mathbb{F}_2$ -algebra  $A = \bigoplus_{i \geq 0} A^i$  with a homomorphism  $\partial: A \rightarrow A$  of degree 1 (called the differential) such that

$$\partial \circ \partial = 0 \quad \text{and} \quad \partial(ab) = \partial(a)b + a\partial(b)$$

for all  $a, b \in A$ . 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  $H^*(A)$ .

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

- (1)  $\partial(a_{i,i+1}) = 0$  and  $a_{i,i+1}$  represents  $a_i$  in  $H^1(A)$ .
- (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  $H^2(A)$ . By definition, the *Massey product* of  $a_1, \dots, a_n$  is the subset  $\langle a_1, \dots, a_n \rangle \subset H^2(A)$  of elements of the form  $\langle a_1, \dots, a_n \rangle_M$  for some defining system  $M$ .

We say that the Massey product  $\langle a_1, \dots, a_n \rangle$  is *defined* if it is non-empty, that is, if there exists a defining system for  $\langle a_1, \dots, a_n \rangle$ . We say that  $\langle a_1, \dots, a_n \rangle$  *vanishes* if  $0 \in \langle a_1, \dots, a_n \rangle$ . If  $\langle a_1, \dots, a_n \rangle$  vanishes, then it is defined.

**Remark 2.2.** Suppose that  $n \geq 3$ , and let  $a_1, \dots, a_n \in H^1(A)$  and  $M = (a_{ij})$  be a defining system for the Massey product  $\langle a_1, \dots, a_n \rangle$ . As a special case of (2),  $\partial(a_{i,i+2}) = a_{i,i+1}a_{i+1,i+2}$  represents  $a_i \cup a_{i+1}$  in  $H^2(A)$ . Thus, if  $\langle a_1, \dots, a_n \rangle$  is defined, then  $a_1 \cup a_2 = a_2 \cup a_3 = \dots = a_{n-1} \cup a_n = 0$  in  $H^2(A)$ .

**Example 2.3.** (a) Let  $\Gamma$  be a profinite group. The complex  $(C^*(\Gamma, \mathbb{Z}/2\mathbb{Z}), \partial)$  of mod 2 non-homogeneous continuous cochains of  $\Gamma$  with the standard cup product is a DGA over  $\mathbb{F}_2$ . We write  $H^*(\Gamma, \mathbb{Z}/2\mathbb{Z})$  for the cohomology of  $(C^*(\Gamma, \mathbb{Z}/2\mathbb{Z}), \partial)$ . By the previous discussion, it makes sense to talk about (mod 2) Massey products of elements of  $H^1(\Gamma, \mathbb{Z}/2\mathbb{Z})$ .

(b) As a special case of (a) when  $\Gamma = \Gamma_F$ , we may talk about (mod 2) Massey products of elements of  $H^1(F, \mathbb{Z}/2\mathbb{Z})$ . Suppose that  $\text{char}(F) \neq 2$ . By Section 2.1, elements of  $H^1(F, \mathbb{Z}/2\mathbb{Z})$  correspond to elements of  $F^\times / F^{\times 2}$ , hence it makes sense to talk about Massey products of elements of  $F^\times$ . If  $a_1, \dots, a_n \in F^\times$ , we denote by  $\langle a_1, \dots, a_n \rangle \subset H^2(F, \mathbb{Z}/2\mathbb{Z})$  their (mod 2) Massey product. By definition,  $\langle a_1, \dots, a_n \rangle$  is defined (resp. vanishes) if and only if so does  $\langle \chi_{a_1}, \dots, \chi_{a_n} \rangle$ .

Let  $U_{n+1} \subset \text{GL}_{n+1}(\mathbb{F}_2)$  be the subgroup of all upper-triangular unipotent matrices. For all  $1 \leq i < j \leq n + 1$ , we denote by  $u_{i,j}: U_{n+1} \rightarrow \mathbb{Z}/2\mathbb{Z}$  the  $(i, j)$ -th coordinate function on  $U_{n+1}$ . The functions  $u_{i,j}$  are group homomorphisms only when  $j = i + 1$ .

The center  $Z_{n+1}$  of  $U_{n+1}$  is the subgroup of all matrices such that  $u_{i,j} = 0$  when  $(i, j) \neq (1, n + 1)$ ; in particular,  $Z_{n+1} \simeq \mathbb{Z}/2\mathbb{Z}$ . We have a commutative diagram

$$\begin{array}{ccccccc}
 1 & \longrightarrow & Z_{n+1} & \longrightarrow & U_{n+1} & \longrightarrow & \bar{U}_{n+1} \longrightarrow 1, \\
 & & & & & \searrow & \downarrow \\
 & & & & & & (\mathbb{Z}/2\mathbb{Z})^n
 \end{array} \tag{2.5}$$

where the homomorphism  $U_{n+1} \rightarrow (\mathbb{Z}/2\mathbb{Z})^n$  is given by  $(u_{1,2}, u_{2,3}, \dots, u_{n,n+1})$  and the row is exact. The group  $\bar{U}_{n+1}$  may be identified with the group of all upper triangular unipotent matrices of size  $(n + 1) \times (n + 1)$  with the entry  $(1, n + 1)$  omitted.

The following result is due to Dwyer [4].

**Theorem 2.4.** *Let  $\Gamma$  be a profinite group,  $\chi = (\chi_1, \dots, \chi_n): \Gamma \rightarrow (\mathbb{Z}/2\mathbb{Z})^n$  be a continuous group homomorphism, and consider the mod 2 Massey product  $\langle \chi_1, \dots, \chi_n \rangle$ .*

- (i) *If  $\tilde{\chi}: \Gamma \rightarrow \bar{U}_{n+1}$  is a continuous homomorphism lifting  $\chi$ , then the collection of 1-cochains  $M_{\tilde{\chi}} := \{u_{i,j} \circ \tilde{\chi}\}$  forms a defining system for  $\langle \chi_1, \dots, \chi_n \rangle$ .*
- (ii) *There is a bijective correspondence between continuous lifts of  $\chi$  and defining systems for  $\langle \chi_1, \dots, \chi_n \rangle$ , given by sending a lift  $\tilde{\chi}: \Gamma \rightarrow \bar{U}_{n+1}$  to  $M_{\tilde{\chi}}$ .*
- (iii) *Let  $\partial: H^1(\Gamma, \bar{U}_{n+1}) \rightarrow H^2(\Gamma, \mathbb{Z}/2\mathbb{Z})$  be the connecting homomorphism induced by (2.5). Then*

$$\langle \chi_1, \dots, \chi_n \rangle = \{\partial([\tilde{\chi}]) : \tilde{\chi}: \Gamma \rightarrow \bar{U}_{n+1} \text{ is a continuous lift of } \chi\}.$$

- (iv) *In particular,  $\langle \chi_1, \dots, \chi_n \rangle$  is defined (resp. vanishes) if and only if  $\chi$  lifts to a continuous homomorphism  $\Gamma \rightarrow \bar{U}_{n+1}$  (resp.  $\Gamma \rightarrow U_{n+1}$ ).*

*Proof.* See [4] or [8, Proposition 2.2]. Although the theorem had originally been stated by Dwyer for discrete groups  $\Gamma$ , it can be readily extended to the case of profinite groups. ■

**Corollary 2.5.** *Let  $\Gamma$  be a profinite group such that the group  $H^2(\Gamma, \mathbb{Z}/2)$  is trivial. Then, for all  $n \geq 1$  and all continuous homomorphisms  $\chi_1, \dots, \chi_n: \Gamma \rightarrow \mathbb{Z}/2\mathbb{Z}$ , the Massey product  $\langle \chi_1, \dots, \chi_n \rangle$  is either empty or equal to  $\{0\}$ .*

The assumptions of Corollary 2.5 are satisfied, for example, when  $\Gamma$  is the absolute Galois group of a field of characteristic 2 or of a finite field; see [25, Chapter II, §§3.3 (a) and 2, Proposition 3].

*Proof.* This is an immediate consequence of Theorem 2.4 (iii). ■

We also let

$$Q_{n+1} := \text{Ker}(U_{n+1} \rightarrow (\mathbb{Z}/2\mathbb{Z})^n), \quad \bar{Q}_{n+1} := \text{Ker}(\bar{U}_{n+1} \rightarrow (\mathbb{Z}/2\mathbb{Z})^n) = Q_{n+1}/Z_{n+1}.$$

The induced maps

$$H^1(F, U_{n+1}) \rightarrow H^1(F, (\mathbb{Z}/2\mathbb{Z})^n), \quad H^1(F, \bar{U}_{n+1}) \rightarrow H^1(F, (\mathbb{Z}/2\mathbb{Z})^n)$$

send a Galois  $U_{n+1}$ -algebra  $L/F$  (resp. a Galois  $\bar{U}_{n+1}$ -algebra  $K/F$ ) to the  $(\mathbb{Z}/2\mathbb{Z})^n$ -algebra  $L^{\mathcal{Q}_{n+1}}/F$  (resp.  $K^{\bar{\mathcal{Q}}_{n+1}}/F$ ).

**Corollary 2.6.** *Suppose that  $\text{char}(F) \neq 2$ , and let  $a_1, \dots, a_n \in F^\times$ . Then the Massey product  $\langle a_1, \dots, a_n \rangle$  is defined (resp. vanishes) if and only if there exists a Galois  $\bar{U}_{n+1}$ -algebra  $K/F$  (resp. Galois  $U_{n+1}$ -algebra  $L/F$ ) such that  $K^{\bar{\mathcal{Q}}_{n+1}} = F_{a_1, \dots, a_n}$  (resp.  $L^{\mathcal{Q}_{n+1}} = F_{a_1, \dots, a_n}$ ).*

*Proof.* Immediate consequence of Theorem 2.4 (iv), Example 2.3 (b) and (2.1). ■

We conclude Section 2.3 with some observations. We have a Cartesian square of groups

$$\begin{CD} \bar{U}_{n+1} @>\varphi_{n+1}>> U_n \\ @V\varphi'_{n+1}VV @VV\varphi'_nV \\ U_n @>\varphi_n>> U_{n-1}, \end{CD} \tag{2.6}$$

where  $\varphi_n$  and  $\varphi_{n+1}$  (resp.  $\varphi'_n$  and  $\varphi'_{n+1}$ ) are given by forgetting the right-most column (resp. the top row).

**Proposition 2.7.** *The map*

$$H^1(F, \bar{U}_{n+1}) \rightarrow H^1(F, U_n) \times_{(\varphi_n)_*, H^1(F, U_{n-1}), (\varphi'_n)_*} H^1(F, U_n)$$

*induced by  $(\varphi'_{n+1}, \varphi'_n)$  is surjective.*

*Proof.* Since (2.6) is Cartesian, to give a continuous group homomorphism  $\Gamma_F \rightarrow \bar{U}_{n+1}$  is the same as to give two continuous homomorphisms  $f, f': \Gamma_F \rightarrow U_n$  such that  $\varphi_n \circ f = \varphi'_n \circ f'$ . It follows that the square of pointed sets

$$\begin{CD} \text{Hom}(\Gamma_F, \bar{U}_{n+1}) @>(\varphi_{n+1})_*>> \text{Hom}(\Gamma_F, U_n) \\ @V(\varphi'_{n+1})_*VV @VV(\varphi'_n)_*V \\ \text{Hom}(\Gamma_F, U_n) @>(\varphi_n)_*>> \text{Hom}(\Gamma_F, U_{n-1}) \end{CD} \tag{2.7}$$

is also Cartesian.

Recall that, for every finite group  $G$ , we have

$$H^1(F, G) = \text{Hom}(\Gamma_F, G)/\sim,$$

where if  $\psi, \psi': \Gamma_F \rightarrow G$  are continuous group homomorphisms, we write  $\psi \sim \psi'$  if and only if there exists  $g \in G$  such that  $g\psi'g^{-1} = \psi$ . Suppose given  $\psi, \psi': \Gamma_F \rightarrow U_n$  and  $g \in U_{n-1}$  such that

$$g((\varphi'_n)_*(\psi'))g^{-1} = (\varphi_n)_*(\psi) \quad \text{in } \text{Hom}(\Gamma_F, U_{n-1}).$$

Let  $\tilde{g} \in U_n$  be such that  $\varphi'_n(\tilde{g}) = g$ . Then  $(\varphi'_n)_*(\tilde{g}\psi'\tilde{g}^{-1}) = (\varphi_n)_*(\psi)$ . Since (2.7) is Cartesian, there exists  $\Psi \in \text{Hom}(\Gamma_F, \bar{U}_{n+1})$  lifting  $\psi$  and  $\tilde{g}\psi'\tilde{g}^{-1}$ . This completes the proof. ■

**Lemma 2.8.** *Suppose that  $\text{char}(F) \neq 2$ . Let  $n \geq 2$  be an integer and  $K$  be a Galois  $\bar{U}_{n+1}$ -algebra over  $F$ . Suppose that there exists a Galois  $U_{n+1}$ -algebra  $L$  such that  $L^{Z_{n+1}} \simeq K$ , and write  $L = K_\pi$  for some  $\pi \in K^\times$ . Then*

- (a) *for all  $t \in F^\times$ , the  $F$ -algebra  $K_{t\pi}$  has the structure of a Galois  $U_{n+1}$ -algebra such that  $K_{t\pi}^{Z_{n+1}} = K$ , and*
- (b) *all Galois  $U_{n+1}$ -algebras  $E$  such that  $E^{Z_{n+1}} \simeq K$  arise in this way.*

*Proof.* Passing to Galois cohomology in (2.5) yields an exact sequence of pointed sets

$$1 \rightarrow F^\times / F^{\times 2} \rightarrow H^1(F, U_{n+1}) \rightarrow H^1(F, \bar{U}_{n+1}).$$

The group  $F^\times / F^{\times 2}$  acts transitively on the fibers of  $H^1(F, U_{n+1}) \rightarrow H^1(F, \bar{U}_{n+1})$ . A simple cocycle calculation shows that  $t \in F^\times / F^{\times 2}$  sends the class of  $K_\pi / F$  to the class of  $K_{t\pi} / F$ . This proves (a) and (b) at once. ■

### 2.4. Specialization

In this section, we prove some specialization properties of Massey products. They can be useful to avoid case-by-case analysis, for example when certain quantities become zero or undefined.

**Lemma 2.9.** *Let  $R$  be a discrete valuation ring with fraction field  $K$  and residue field  $k$ , and suppose that  $\text{char}(k) \neq 2$ . Let  $a_1, \dots, a_n \in R^\times$ , and let  $\bar{a}_1, \dots, \bar{a}_n \in k^\times$  be their reductions.*

- (a) *If the Massey product  $\langle a_1, \dots, a_n \rangle$  is defined over  $K$ , then  $\langle \bar{a}_1, \dots, \bar{a}_n \rangle$  is defined over  $k$ .*
- (b) *If the Massey product  $\langle a_1, \dots, a_n \rangle$  vanishes over  $K$ , then  $\langle \bar{a}_1, \dots, \bar{a}_n \rangle$  vanishes over  $k$ .*

*Proof.* The completion of  $R$  has residue field equal to  $k$  and fraction field containing  $K$ . We may thus replace  $R$  by its completion and assume that  $R$  is complete.

Let  $q \geq 1$  be the characteristic exponent of  $K$ , that is,  $q = \text{char}(K)$  if  $\text{char}(K) > 0$  and  $q = 1$  if  $\text{char}(K) = 0$ . Let  $\pi \in R$  be a uniformizer. For every  $d \geq 1$  prime to  $q$ , choose a  $d$ -th root  $\pi^{1/d}$  of  $\pi$  such that for all  $d_1, d_2 \geq 1$  prime to  $q$ , we have that  $(\pi^{1/d_1 d_2})^{d_1} = \pi^{1/d_2}$ . Define  $K_\infty := \bigcup_d K(\pi^{1/d})$ , where  $d \geq 1$  ranges over all integers prime to  $q$ . Let  $\Delta := \Gamma_{K_\infty}$ , and define  $L := K_{\text{nr}} K_\infty$ . Then  $\Gamma_L$  is a pro- $q$ -group (trivial if  $q = 1$ ) and  $\text{Gal}(L/K_\infty) = \text{Gal}(K_{\text{nr}}/K) = \Gamma_k$ . It follows that for every finite 2-group  $G$ , the natural map

$$\text{Hom}(\Gamma_k, G) = \text{Hom}(\text{Gal}(L/K_\infty), G) \rightarrow \text{Hom}(\Delta, G)$$

is an isomorphism. The map

$$\text{Hom}(\Gamma_K, G) \rightarrow \text{Hom}(\Delta, G) = \text{Hom}(\Gamma_k, G)$$

induces a specialization map

$$s: H^1(K, G) \rightarrow H^1(k, G),$$

which is covariant in  $G$ .

For all  $a \in R^\times$ , we denote by  $\bar{a} \in k^\times$  the reduction of  $a$  modulo the maximal ideal of  $R$ . Under the identification of (2.4),  $s: H^1(K, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^1(k, \mathbb{Z}/2\mathbb{Z})$  sends  $aK^{\times 2}$  to  $\bar{a}k^{\times 2}$ . Therefore, for all  $n \geq 1$ ,

$$\begin{aligned} \text{The map } s: H^1(K, (\mathbb{Z}/2\mathbb{Z})^n) &\rightarrow H^1(k, (\mathbb{Z}/2\mathbb{Z})^n) \\ &\text{sends } (a_1, \dots, a_n) \text{ to } (\bar{a}_1, \dots, \bar{a}_n). \end{aligned} \tag{2.8}$$

(a) We have a commutative square of pointed sets

$$\begin{CD} H^1(K, \bar{U}_{n+1}) @>s>> H^1(k, \bar{U}_{n+1}) \\ @VVV @VVV \\ H^1(K, (\mathbb{Z}/2\mathbb{Z})^n) @>s>> H^1(k, (\mathbb{Z}/2\mathbb{Z})^n). \end{CD} \tag{2.9}$$

By Corollary 2.6,  $(a_1, \dots, a_n)$  lifts to  $H^1(K, \bar{U}_{n+1})$ , hence (2.8) and (2.9) imply that  $(\bar{a}_1, \dots, \bar{a}_n) \in H^1(k, (\mathbb{Z}/2\mathbb{Z})^n)$  lifts to  $H^1(k, \bar{U}_{n+1})$ . The conclusion follows from Theorem 2.4 (iv).

(b) We may argue as in the proof of (a), replacing  $\bar{U}_{n+1}$  by  $U_{n+1}$  everywhere. ■

**Proposition 2.10.** *Let  $a_1, \dots, a_n \in F^\times$ , let  $X$  be an  $F$ -variety with a regular  $F$ -point. Then we have the following:*

- (a) *The Massey product  $\langle a_1, \dots, a_n \rangle$  is defined over  $F$  if and only if it is defined over  $F(X)$ .*
- (b) *The Massey product  $\langle a_1, \dots, a_n \rangle$  vanishes over  $F$  if and only if it vanishes over  $F(X)$ .*

*Proof.* It is clear that if  $\langle a_1, \dots, a_n \rangle$  is defined (resp. it vanishes) over  $F$ , then it is defined (resp. it vanishes) over  $F(X)$ .

For the converse, let  $x \in X(F)$  be a regular  $F$ -point, that is, the local ring  $O_{X,x}$  is regular. Let  $d$  be the dimension of  $X$  and  $t_1, \dots, t_d \in O_{X,x}$  be a regular system of parameters. For every  $i = 1, \dots, d$ , let  $O_i$  be the localization of  $O_{X,x}/(t_1, \dots, t_{i-1})$  at the prime ideal generated by the image of  $t_i$ . Since  $O_{X,x}$  is regular, the quotient of a regular local ring by a non-zero divisor is regular, and the localization of a regular local ring is regular, every  $O_i$  is a regular local ring of dimension 1, that is, a discrete valuation ring. Moreover, the fraction field of  $O_1$  is  $F(X)$ , the residue field of  $O_d$  is  $F$ , and for all  $i = 1, \dots, d - 1$ , the residue field of  $O_i$  coincides with the fraction field of  $O_{i+1}$ . Now (a) (resp. (b)) follows from Lemma 2.9 (a) (resp. (b)), applied to  $R = O_i$  for  $i = 1, \dots, d$ . ■

**Remark 2.11.** Let  $p$  be a prime number, and suppose that  $\text{char}(F) \neq p$  and that  $F$  contains a primitive  $p$ -th root of unity. Then the definition of mod  $p$  Massey product given in Example 2.3 (b) for  $p = 2$  extends to all  $p$ . The constructions and the results of Sections 2.3 and 2.4 extend to arbitrary  $p$ , with the same proofs.

### 3. Massey products and Galois algebras

From now on in this paper, we suppose that  $\text{char}(F) \neq 2$ .

#### 3.1. Galois $U_3$ -algebras

Let  $a, b \in F^\times$ , and suppose that  $(a, b) = 0$  in  $\text{Br}(F)$ . We write  $(\mathbb{Z}/2\mathbb{Z})^2 = \langle \sigma_a, \sigma_b \rangle$ , and we view  $F_{a,b}$  as a Galois  $(\mathbb{Z}/2\mathbb{Z})^2$ -algebra as in Section 2.1. Let  $\alpha \in F_a^\times$  satisfy  $N_a(\alpha) = bx^2$  for some  $x \in F^\times$ , and consider the étale  $F$ -algebra  $(F_{a,b})_\alpha$ . We have

$$U_3 = \langle \sigma_a, \sigma_b : \sigma_a^2 = \sigma_b^2 = [\sigma_a, \sigma_b]^2 = 1 \rangle.$$

Moreover,  $\bar{U}_3 = (\mathbb{Z}/2\mathbb{Z})^2$  and the surjective homomorphism  $U_3 \rightarrow \bar{U}_3$  is given by  $\sigma_a \mapsto \sigma_a$  and  $\sigma_b \mapsto \sigma_b$ . Observe that

$$\sigma_a(\alpha) = \frac{bx^2}{\alpha} \quad \text{and} \quad \sigma_b(\alpha) = \alpha.$$

We may thus define a Galois  $U_3$ -algebra structure on  $(F_{a,b})_\alpha$  by letting  $U_3$  act on  $F_{a,b}$  via  $\bar{U}_3$  and by setting

$$\sigma_a(\sqrt{\alpha}) = x \frac{\sqrt{b}}{\sqrt{\alpha}}, \quad \sigma_b(\sqrt{\alpha}) = \sqrt{\alpha}. \tag{3.1}$$

We leave to the reader the verification that  $\sigma_a^2 = \sigma_b^2 = [\sigma_a, \sigma_b]^2 = 1$  on  $(F_{a,b})_\alpha$ , that  $(F_{a,b})_\alpha$  is a Galois  $U_3$ -algebra and that the subalgebra of  $Q_3$ -invariants is  $F_{a,b}$ .

**Lemma 3.1.** *Let  $K^+ := (F_{a,b})_\alpha$  with the Galois  $U_3$ -algebra structure of (3.1) and  $K^- := (F_{a,b})_\alpha$ , with the Galois  $U_3$ -algebra structure given by*

$$\sigma_a(\sqrt{\alpha}) = -x \frac{\sqrt{b}}{\sqrt{\alpha}}, \quad \sigma_b(\sqrt{\alpha}) = \sqrt{\alpha}.$$

*Then  $\sigma_b: K^+ \rightarrow K^-$  is an isomorphism of Galois  $U_3$ -algebras.*

Note that  $\sigma_b: K^+ \rightarrow K^-$  is not  $F_{a,b}$ -linear.

*Proof.* For all  $\eta \in (F_{a,b})_\alpha$ , we write  $\eta^+$  and  $\eta^-$  for the element  $\eta$ , viewed as an element of  $K^+$  and  $K^-$ , respectively. Then  $\sigma_b: K^+ \rightarrow K^-$  sends  $\eta^+$  to  $\sigma_b(\eta^+) = \sigma_b(\eta)^-$ . Since  $\sigma_b$  is an isomorphism of étale algebras, it suffices to check that it is compatible with the Galois  $U_3$ -algebra structures. This follows from the fact that  $\sigma_a\sigma_b = \sigma_b\sigma_a$  on  $F_{a,b}$ , and

$$\sigma_b(\sigma_a(\sqrt{\alpha^+})) = \sigma_b\left(x \frac{\sqrt{b^+}}{\sqrt{\alpha^+}}\right) = -x \frac{\sqrt{b^-}}{\sqrt{\alpha^-}} = \sigma_a(\sqrt{\alpha^-}) = \sigma_a(\sigma_b(\sqrt{\alpha^+})). \quad \blacksquare$$

Symmetrically, if  $\beta \in F_b^\times$  satisfies  $N_b(\beta) = ay^2$  for some  $y \in F^\times$ , the étale  $F$ -algebra  $(F_{a,b})_\beta$  has structure of a Galois  $U_3$ -algebra defined by

$$\sigma_a(\sqrt{\beta}) = \sqrt{\beta}, \quad \sigma_b(\sqrt{\beta}) = y \frac{\sqrt{a}}{\sqrt{\beta}}. \tag{3.2}$$

**Proposition 3.2.** *Let  $a, b \in F^\times$ .*

- (a) *Every Galois  $U_3$ -algebra  $K$  over  $F$  such that  $K^{\mathcal{Q}_3} = F_{a,b}$  is of the form  $(F_{a,b})_\alpha$  for some  $\alpha \in F_a^\times$  with the property  $N_a(\alpha) = b$  in  $F^\times / F^{\times 2}$  and  $U_3$ -algebra structure as in (3.1).*
- (b) *Every Galois  $U_3$ -algebra  $K$  over  $F$  such that  $K^{\mathcal{Q}_3} = F_{a,b}$  is of the form  $(F_{a,b})_\beta$  for some  $\beta \in F_b^\times$  with the property  $N_b(\beta) = a$  in  $F^\times / F^{\times 2}$  and  $U_3$ -algebra structure as in (3.2).*
- (c) *Let  $\alpha \in F_a^\times, \beta \in F_b^\times$  be such that  $N_a(\alpha) = b$  in  $F^\times / F^{\times 2}$  and  $N_b(\beta) = a$  in  $F^\times / F^{\times 2}$ . The two Galois  $U_3$ -algebras  $(F_{a,b})_\alpha$  and  $(F_{a,b})_\beta$  (with  $U_3$ -algebra structure as in (3.1) and (3.2), respectively) are isomorphic if and only if there exists  $\omega \in F_{a,b}^\times$  such that*

$$\alpha\beta = \omega^2, \quad (\sigma_a - 1)(\sigma_b - 1)\omega = -1.$$

*Proof.* (a) We have  $U_3 = N \rtimes S$ , where

$$N = \begin{bmatrix} 1 & 0 & * \\ & 1 & * \\ & & 1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & * & 0 \\ & 1 & 0 \\ & & 1 \end{bmatrix}.$$

We let  $S$  act on  $N$  by conjugation. Then  $N$  has a permutation basis given by

$$\begin{bmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix}.$$

Therefore, we have a commutative square of  $S$ -modules:

$$\begin{array}{ccc} N & \xrightarrow{\sim} & \text{Ind}_{\{1\}}^S(\mathbb{Z}/2\mathbb{Z}) \\ \downarrow u_{23} & & \downarrow \text{Norm} \\ \mathbb{Z}/2\mathbb{Z} & \xlongequal{\quad} & \mathbb{Z}/2\mathbb{Z}. \end{array} \tag{3.3}$$

Let  $p: U_3 \rightarrow S$  be the projection map, and let  $N_p$  be the twist of  $N$  by  $p$ ; see [11, §28.C]. Then (3.3) induces a commutative square of  $U_3$ -modules:

$$\begin{array}{ccc} N_p & \xrightarrow{\sim} & \text{Ind}_N^{U_3}(\mathbb{Z}/2\mathbb{Z}) \\ \downarrow (u_{23})_p & & \downarrow \text{Norm} \\ \mathbb{Z}/2\mathbb{Z} & \xlongequal{\quad} & \mathbb{Z}/2\mathbb{Z}. \end{array} \tag{3.4}$$

Let  $\rho: \Gamma_F \rightarrow U_3$  be a continuous homomorphism whose class in  $H^1(F, U_3)$  coincides with that of  $K$ , and define  $\pi: \Gamma_F \rightarrow S$  by  $\pi := p \circ \rho$ . Since  $K^N = F_a$ , the class of  $\pi$  in  $H^1(F, S) = H^1(F, \mathbb{Z}/2\mathbb{Z})$  is equal to  $\chi_a$ . Pullback of (3.4) along  $\rho$  yields the following commutative square:

$$\begin{array}{ccc} N_\pi & \xrightarrow{\sim} & \text{Ind}_{F_a}^F(\mathbb{Z}/2\mathbb{Z}) \\ \downarrow (u_{23})_\pi & & \downarrow N_a \\ \mathbb{Z}/2\mathbb{Z} & \xlongequal{\quad} & \mathbb{Z}/2\mathbb{Z}. \end{array} \tag{3.5}$$

Here  $\text{Ind}_{F_a}^F(\mathbb{Z}/2\mathbb{Z})$  indicates the  $\Gamma_F$ -module corresponding to the pushforward of the constant étale sheaf  $\mathbb{Z}/2\mathbb{Z}$  on  $\text{Spec}(F_a)$  to  $\text{Spec}(F)$ ; see [14, Theorem II.1.9]. Combining (3.5) with Faddeev–Shapiro’s lemma, we deduce that the composition

$$\Phi: H^1(F, N_\pi) \xrightarrow{\text{Res}} H^1(F_a, N) \xrightarrow{u_{13}} H^1(F_a, \mathbb{Z}/2\mathbb{Z})$$

is an isomorphism fitting in the commutative diagram

$$\begin{CD} H^1(F, N_\pi) @>\Phi>> H^1(F_a, \mathbb{Z}/2\mathbb{Z}) @= F_a^\times / F_a^{\times 2} \\ @VV(u_{23})_\pi V @VVN_a V @VVN_a V \\ H^1(F, \mathbb{Z}/2\mathbb{Z}) @= H^1(F, \mathbb{Z}/2\mathbb{Z}) @= F^\times / F^{\times 2}. \end{CD} \tag{3.6}$$

Let  $E$  be a Galois  $U_3$ -algebra and  $\varphi: E^N \rightarrow F_a$  be an isomorphism of Galois  $U_3$ -algebras over  $F$ . By base change, we obtain an isomorphism of Galois  $U_3$ -algebras  $\varphi_{F_a}: (E^N)_a \rightarrow (F_a)_a = \prod_{\sigma \in S} F_a$  over  $F_a$ . Therefore, we may write  $E_a = \prod_{\sigma \in S} E_{\varphi, \sigma}$ , where  $E_{\varphi, \sigma}$  is the subalgebra of  $E_a$  lying over the inverse image of the factor in  $\prod_{\sigma \in S} F_a$  corresponding to  $\sigma$ . In terms of identification (2.2), the Faddeev–Shapiro isomorphism  $\Phi$  sends the class of the pair  $(E, \varphi)$  to the class of the  $\mathbb{Z}/2\mathbb{Z}$ -Galois algebra  $E_{\varphi, 0}/F_a$ , where  $0 \in S$  is the identity element.

Since  $K^{Q_3} = F_{a,b}$ , the pair  $(K, \text{id})$  defines an element in  $H^1(F, N_\pi)$ . Let  $\alpha \in F_a^\times$  be such that  $\Phi$  sends the class of  $(K, \text{id})$  to  $(F_a)_\alpha/F_a$ . By (3.6), we have  $N_a(\alpha) = bx^2$  for some  $x \in F^\times$ . The pair  $((F_{a,b})_\alpha, \text{id})$ , where  $(F_{a,b})_\alpha$  is the Galois  $U_3$ -algebra of (3.1), also defines an element of  $H^1(F, N_\pi)$  which is mapped to  $(F_a)_\alpha/F_a$  by  $\Phi$ . The injectivity of  $\Phi$  now implies that the Galois  $U_3$ -algebras  $K$  and  $(F_{a,b})_\alpha$  are isomorphic over  $F$ , as desired.

(b) Analogous to (a), after replacing  $N$  and  $S$  by

$$N' = \begin{bmatrix} 1 & * & * \\ & 1 & 0 \\ & & 1 \end{bmatrix} \quad \text{and} \quad S' = \begin{bmatrix} 1 & 0 & 0 \\ & 1 & * \\ & & 1 \end{bmatrix},$$

respectively.

(c) Suppose given an isomorphism between two  $U_3$ -algebras  $(F_{a,b})_\alpha$  and  $(F_{a,b})_\beta$ . Write  $\beta' \in (F_{a,b})_\alpha$  for the image of  $\beta$  under the isomorphism and set

$$\omega := \sqrt{\alpha} \cdot \sqrt{\beta'}.$$

We have  $[\sigma_a, \sigma_b]\omega = \omega$ , that is,  $\omega$  is invariant under  $Z_3 = Q_3$ , and hence  $\omega \in F_{a,b}^\times$ . Moreover,

$$(\sigma_a - 1)(\sigma_b - 1)\omega = (\sigma_a - 1)\left(y \frac{\sqrt{\alpha}}{\sqrt{\beta'}}\right) = -1.$$

We have  $\omega^2 = \alpha\beta'$ . Since  $F_b$  coincides with the  $N'$ -invariant subalgebra of  $(F_{a,b})_\beta$  and  $(F_{a,b})_\alpha$ , the isomorphism  $(F_{a,b})_\alpha \rightarrow (F_{a,b})_\beta$  restricts to an automorphism of  $F_b$ .

If this automorphism is the identity, then  $\beta' = \beta$ , and hence  $\omega^2 = \alpha\beta$ . If this automorphism is non-trivial, then it must be equal to  $\sigma_b$ , and hence  $\beta' = \sigma_b(\beta)$ . Define  $\omega' := (\omega\beta)/(y\sqrt{a}) \in F_{a,b}^\times$ . Then

$$(\omega')^2 = \frac{\omega^2\beta^2}{y^2a} = \frac{\alpha\sigma_b(\beta)\beta^2}{y^2a} = \alpha\beta.$$

Since  $\beta/(y\sqrt{a})$  belongs to  $F_{a,b}^\times$ , we have  $(\sigma_a - 1)(\sigma_b - 1)(\beta/y\sqrt{a}) = 1$ , and hence

$$(\sigma_a - 1)(\sigma_b - 1)\omega' = (\sigma_a - 1)(\sigma_b - 1)\omega = -1.$$

It thus suffices to replace  $\omega$  by  $\omega'$ .

Conversely, suppose  $\alpha\beta = \omega^2$  for some  $\omega \in F_{a,b}^\times$  such that  $(\sigma_a - 1)(\sigma_b - 1)\omega = -1$ . We have

$$(\sigma_a - 1)\omega^2 = (\sigma_a - 1)\alpha = x^2 \frac{b}{\alpha^2} = \left(x \frac{\sqrt{b}}{\alpha}\right)^2.$$

Let

$$\zeta_a := (\sigma_a - 1)\omega \cdot \left(\frac{\alpha}{x\sqrt{b}}\right) \in F_{a,b}^\times.$$

Then  $(\sigma_b - 1)\eta_a = (-1) \cdot (-1) = 1$ , and hence  $\eta_a \in F_a^\times$ . Moreover, we have  $\eta_a^2 = 1$  and  $N_a(\eta_a) = N_a(\alpha)/(x^2b) = 1$ . It follows that  $\eta_a = \pm 1$ , which is equivalent to

$$(\sigma_a - 1)\omega = \pm x \frac{\sqrt{b}}{\alpha}.$$

Replacing  $x$  by  $-x$  if necessary (by Lemma 3.1, this does not change the  $U_3$ -algebra up to isomorphism), we may assume that  $(\sigma_a - 1)\omega = x\sqrt{b}/\alpha$ . Similarly, we have  $(\sigma_b - 1)\omega = y\sqrt{a}/\beta$ . A calculation shows that the assignment  $\sqrt{\alpha} \mapsto \omega/\sqrt{\beta}$  yields an isomorphism of  $U_3$ -algebras  $(F_{a,b})_\alpha$  and  $(F_{a,b})_\beta$ . ■

### 3.2. 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  $(\mathbb{Z}/2\mathbb{Z})^3 = \langle \sigma_a, \sigma_b, \sigma_c \rangle$  and view  $F_{a,b,c}$  as a Galois  $(\mathbb{Z}/2\mathbb{Z})^3$ -algebra over  $F$  as in Section 2.1. Let  $\varepsilon \in F_{a,c}^\times$  satisfy  $N_{a,c}(\varepsilon) = bx^2$  for some  $x \in F^\times$ . Set  $\alpha = N_c(\varepsilon) \in F_a^\times$  and  $\gamma = N_a(\varepsilon) \in F_c^\times$ .

We have

$$U_4 = \langle \sigma_a, \sigma_b, \sigma_c : \sigma_a^2 = \sigma_b^2 = \sigma_c^2 = 1, [\sigma_a, \sigma_b]^2 = [\sigma_b, \sigma_c]^2 = [\sigma_a, \sigma_c] = 1, \\ [[\sigma_a, \sigma_b], \sigma_c] = [\sigma_a, [\sigma_b, \sigma_c]], [[\sigma_a, \sigma_b], \sigma_c]^2 = 1 \rangle.$$

The quotient map  $U_4 \rightarrow (\mathbb{Z}/2\mathbb{Z})^3$  is given by  $\sigma_a \mapsto \sigma_a, \sigma_b \mapsto \sigma_b$  and  $\sigma_c \mapsto \sigma_c$ . The étale  $F$ -algebra  $(F_{a,b,c})_{\alpha,\gamma,\varepsilon}$  may be given the structure of a Galois  $U_4$ -algebra as follows: we let  $\sigma_a, \sigma_b, \sigma_c$  act on  $F_{a,b,c}$  via the quotient  $(\mathbb{Z}/2\mathbb{Z})^3$ , and set

$$\sigma_a(\sqrt{\varepsilon}) = \frac{\sqrt{\gamma}}{\sqrt{\varepsilon}}, \quad \sigma_c(\sqrt{\varepsilon}) = \frac{\sqrt{\alpha}}{\sqrt{\varepsilon}}, \quad \sigma_a(\sqrt{\alpha}) = x \frac{\sqrt{b}}{\sqrt{\alpha}}, \quad \sigma_c(\sqrt{\gamma}) = x \frac{\sqrt{b}}{\sqrt{\gamma}},$$

$$(\sigma_b - 1)(\sqrt{\alpha}) = (\sigma_b - 1)(\sqrt{\gamma}) = (\sigma_b - 1)(\sqrt{\varepsilon}) = (\sigma_a - 1)(\sqrt{\gamma}) = (\sigma_c - 1)(\sqrt{\alpha}) = 1.$$

We leave it to the reader to verify that this defines a Galois  $U_4$ -algebra structure on  $(F_{a,b,c})_{\alpha,\gamma,\varepsilon}$ , that is, that  $\sigma_a, \sigma_b, \sigma_c$  act via  $F$ -algebra automorphisms, that these automorphisms satisfy the above relations, and that the subalgebra of  $Q_4$ -invariants is  $F_{a,b,c}$ .

**Proposition 3.3.** *Let  $a, b, c \in F^\times$ . Then every Galois  $U_4$ -algebra  $K$  over  $F$  such that  $K^{Q_4} = F_{a,b,c}$  is of the form  $(F_{a,b,c})_{N_c(\varepsilon), N_a(\varepsilon), \varepsilon}$  for some  $\varepsilon \in F_{a,c}^\times$  with the property  $N_{a,c}(\varepsilon) = b$  in  $F^\times/F^{\times 2}$ .*

*Proof.* The proof is similar to that of Proposition 3.2 (a). We have  $U_4 = N \rtimes S$ , where

$$N = \begin{bmatrix} 1 & 0 & * & * \\ & 1 & * & * \\ & & 1 & 0 \\ & & & 1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & * & 0 & 0 \\ & 1 & 0 & 0 \\ & & 1 & * \\ & & & 1 \end{bmatrix}.$$

The coordinate functions  $u_{12}$  and  $u_{34}$  determine a group isomorphism  $S \simeq (\mathbb{Z}/2\mathbb{Z})^2$ .

Let  $\rho: \Gamma_F \rightarrow U_4$  be a homomorphism whose class in  $H^1(F, U_4)$  is equal to the class of  $K$ , and let  $\pi := p \circ \rho$ , so that the class of  $\pi$  in  $H^1(F, S) = H^1(F, (\mathbb{Z}/2\mathbb{Z})^2)$  is equal to  $(\chi_a, \chi_b)$ . Write  $N_\pi$  for the twist of  $N$ . The  $S$ -module  $N$  has a permutation basis given by

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ & 1 & 1 & 0 \\ & & 1 & 0 \\ & & & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 & 0 \\ & 1 & 1 & 0 \\ & & 1 & 0 \\ & & & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ & 1 & 1 & 1 \\ & & 1 & 0 \\ & & & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 & 1 \\ & 1 & 1 & 1 \\ & & 1 & 0 \\ & & & 1 \end{bmatrix}.$$

This choice of basis gives a commutative square of continuous  $\Gamma_F$ -modules

$$\begin{array}{ccc} N_\pi & \xrightarrow{\sim} & \text{Ind}_{F_{a,c}}^F(\mathbb{Z}/2\mathbb{Z}) \\ \downarrow (u_{23})_\pi & & \downarrow N_{a,c} \\ \mathbb{Z}/2\mathbb{Z} & \xlongequal{\quad} & \mathbb{Z}/2\mathbb{Z}. \end{array}$$

From Faddeev–Shapiro’s lemma, we obtain an isomorphism

$$\Phi: H^1(F, N_\pi) \rightarrow H^1(F_{a,c}, N) \xrightarrow{u_{14}} H^1(F_{a,c}, \mathbb{Z}/2\mathbb{Z})$$

fitting into the commutative diagram

$$\begin{array}{ccccc} H^1(F, N_\pi) & \xrightarrow{\Phi} & H^1(F_{a,c}, \mathbb{Z}/2\mathbb{Z}) & \xlongequal{\quad} & F_{a,c}^\times / F_{a,c}^{\times 2} \\ \downarrow (u_{23})_\pi & & \downarrow N_{a,c} & & \downarrow N_{a,c} \\ H^1(F, \mathbb{Z}/2\mathbb{Z}) & \xlongequal{\quad} & H^1(F, \mathbb{Z}/2\mathbb{Z}) & \xlongequal{\quad} & F^\times / F^{\times 2}. \end{array} \tag{3.7}$$

Let  $E$  be a Galois  $U_4$ -algebra over  $F$  and  $\varphi: E^{Q_4} \rightarrow F_{a,b,c}$  be an isomorphism. Base change to  $F_{a,c}$  yields an isomorphism  $\varphi_{F_{a,c}}: (E^N)_{a,c} \rightarrow (F_{a,c})_{a,c} = \prod_{\sigma \in S} F_{a,c}$ , and so we may write  $E_{a,c} = \prod_{\sigma \in S} E_{\varphi,\sigma}$ , where  $E_{\varphi,\sigma}$  is the subalgebra of  $E_{a,c}$  lying over

the inverse image of the factor of  $\prod_{\sigma \in S} F_{a,c}$  corresponding to  $\sigma$ . Under the identification of (2.2), the map  $\Phi$  sends the pair  $(E, \varphi)$  to the class of the Galois  $\mathbb{Z}/2\mathbb{Z}$ -algebra  $E_{\varphi,0}/F_{a,c}$ , where  $0 \in S$  is the identity element.

Since  $K^{Q^4} = F_{a,b,c}$ , the pair  $(K, \text{id})$  defines an element of  $H^1(F, N_{\pi})$ . Let  $\varepsilon \in F_{a,c}^{\times}$  be such that  $\Phi$  sends the class of  $(K, \text{id})$  to  $(F_{a,c})_{\varepsilon}$ . By (3.7), we have  $N_{a,c}(\varepsilon) = bx^2$  for some  $x \in F^{\times}$ . Let  $\alpha := N_c(\varepsilon) \in F_a^{\times}$  and  $\gamma := N_a(\varepsilon) \in F_c^{\times}$ , and consider on  $(F_{a,b,c})_{\alpha,\gamma,\varepsilon}$  the Galois  $U_4$ -algebra structure over  $F$  given by (3.3). Then  $\Phi$  sends the class of the pair  $((F_{a,b,c})_{\alpha,\delta,\varepsilon}, \text{id})$  to the class of the  $\mathbb{Z}/2\mathbb{Z}$ -algebra  $(F_{a,c})_{\varepsilon}/F_{a,c}$ . Since  $\Phi$  is injective, we deduce an isomorphism  $K \cong (F_{a,b,c})_{\alpha,\gamma,\varepsilon}$  of Galois  $U_4$ -algebras over  $F$ . ■

The following theorem was proved by Hopkins and Wickelgren [9] when  $F$  is a number field, and by Mináč and Tân [15] when  $F$  is arbitrary. We give an alternative proof.

**Corollary 3.4.** *Suppose that  $p = 2$ , and let  $a, b, c \in F^{\times}$  be such that  $(a, b) = (b, c) = 0$  in  $\text{Br}(F)$ . Then the Massey product  $\langle a, b, c \rangle$  is defined and vanishes.*

*Proof.* Since  $(a, b) = (b, c) = 0$ , by Lemma 2.1 we have  $b \in N_a \cap N_c$ . By Lemma A.5, there exists  $\varepsilon \in F_{a,c}^{\times}$  such that  $N_{a,c}(\varepsilon) = b$  in  $F^{\times}/F^{\times 2}$ . By the discussion preceding Proposition 3.3,  $K := (F_{a,b,c})_{N_c(\varepsilon), N_a(\varepsilon), \varepsilon}$  is a Galois  $U_4$ -algebra over  $F$  such that  $K^{Q^4} = F_{a,b,c}$ . The conclusion follows from Corollary 2.6. ■

### 3.3. Galois $\bar{U}_5$ -algebras

Let  $a, b, c, d \in F^{\times}$ . We write  $(\mathbb{Z}/2\mathbb{Z})^4 = \langle \sigma_a, \sigma_b, \sigma_c, \sigma_d \rangle$  and regard  $F_{a,b,c,d}$  as a Galois  $(\mathbb{Z}/2\mathbb{Z})^4$ -algebra over  $F$  as in Section 2.1.

**Proposition 3.5.** *Let  $a, b, c, d \in F^{\times}$ . Then the Massey product  $\langle a, b, c, d \rangle$  is defined if and only if there are  $\varepsilon \in F_{a,c}^{\times}$ ,  $v \in F_{b,d}^{\times}$  and  $\omega \in F_{b,c}^{\times}$  such that*

- (1)  $N_{a,c}(\varepsilon) = b$  in  $F^{\times}/F^{\times 2}$ ;
- (2)  $N_{b,d}(v) = c$  in  $F^{\times}/F^{\times 2}$ ;
- (3)  $N_a(\varepsilon)N_d(v) = \omega^2$ ;
- (4)  $(\sigma_b - 1)(\sigma_c - 1)\omega = -1$ .

*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  $U_4^+ \rightarrow (\mathbb{Z}/2\mathbb{Z})^3$  and  $U_4^- \rightarrow (\mathbb{Z}/2\mathbb{Z})^3$ , respectively, and  $P_4^+$  and  $P_4^-$  be the kernels of the maps  $U_4^+ \rightarrow U_3$  and  $U_4^- \rightarrow U_3$ , respectively. By Proposition 2.7, there exists a Galois  $\bar{U}_5$ -algebra  $K/F$  such that  $K^{Q^5} = F_{a,b,c,d}$  if and only if there are a Galois  $U_4^+$ -algebra  $K_1/F$  and a Galois  $U_4^-$ -algebra  $K_2/F$  such that

- (i)  $K_1^{Q_4^+} = F_{a,b,c}$ ,  $K_2^{Q_4^-} = F_{b,c,d}$ , and
- (ii) the  $U_3$ -algebras  $K_1^{P_4^+}$  and  $K_2^{P_4^-}$  are isomorphic.

By Proposition 3.3, giving  $K_1$  and  $K_2$  satisfying (i) is equivalent to giving two elements  $\varepsilon \in F_{a,c}^{\times}$  and  $v \in F_{b,d}^{\times}$  such that  $N_{a,c}(\varepsilon) = b$  and  $N_{b,d}(v) = c$  in  $F^{\times}/F^{\times 2}$ . According

to Proposition 3.2 (c),  $K_1$  and  $K_2$  satisfy (ii) if and only if there is  $\omega \in F_{b,c}^\times$  such that  $N_a(\varepsilon)N_d(v) = \omega^2$  and  $(\sigma_b - 1)(\sigma_c - 1)\omega = -1$ . ■

**Remark 3.6.** Let  $\varepsilon \in F_{a,c}^\times$ ,  $v \in F_{b,d}^\times$ ,  $e \in F^\times$ ,  $\omega \in F_{b,c}^\times$  be such that  $N_a(\varepsilon)N_d(v) = e\omega^2$ . Then  $(\sigma_b - 1)N_a(\varepsilon) = 1$  and  $(\sigma_c - 1)N_d(v) = 1$ , hence  $(\sigma_b - 1)(\sigma_c - 1)\omega^2 = 1$ . Therefore,  $(\sigma_b - 1)(\sigma_c - 1)\omega \in \{\pm 1\}$ .

Suppose now that  $a, b, c, d \in F^\times$  satisfy  $(a, b) = (b, c) = (c, d) = 0$ . By Lemma A.5, there exist  $\varepsilon \in F_{a,c}^\times$ ,  $v \in F_{b,d}^\times$  such that  $N_{a,c}(\varepsilon) = b$  in  $F^\times/F^{\times 2}$  and  $N_{b,d}(v) = c$  in  $F^\times/F^{\times 2}$ . Even if  $\langle a, b, c, d \rangle$  is defined, it is not true that one may find  $\omega \in F_{b,c}^\times$  such that  $(\varepsilon, v, \omega)$  satisfies the equations of Proposition 3.5: one might need to change  $\varepsilon$  and  $v$ . It will be useful to have a criterion for  $\langle a, b, c, d \rangle$  to be defined in terms of any given  $\varepsilon$  and  $v$ . This is the content of the next proposition.

**Proposition 3.7.** Let  $a, b, c, d \in F^\times$  be such that  $(a, b) = (b, c) = (c, d) = 0$ . Let  $\varepsilon \in F_{a,c}^\times$  and  $v \in F_{b,d}^\times$  be such that  $N_{a,c}(\varepsilon) = b$  in  $F^\times/F^{\times 2}$  and  $N_{b,d}(v) = c$  in  $F^\times/F^{\times 2}$ .

(a) There exist  $e \in F^\times$  and  $\omega \in F_{b,c}^\times$  such that

$$N_a(\varepsilon)N_d(v) = e\omega^2, \quad (\sigma_b - 1)(\sigma_c - 1)\omega = -1.$$

(b) Letting  $\varepsilon$  and  $v$  vary, the corresponding  $e$  form an  $N_aN_{ac}N_dN_{bd}$ -coset of  $F^\times$ .

(c) The Massey product  $\langle a, b, c, d \rangle$  is defined if and only if  $e \in N_aN_{ac}N_dN_{bd}$ .

*Proof.* (a) By Lemma 2.8, there exists  $e \in F^\times$  such that  $(F_{b,c})_{N_a(\varepsilon)} \simeq (F_{b,c})_{eN_d(v)}$ . Thus Proposition 3.2 (c) implies the existence of  $\omega \in F_{b,c}^\times$  such that

$$N_a(\varepsilon)N_d(v) = e\omega^2, \quad (\sigma_b - 1)(\sigma_c - 1)\omega = -1.$$

(b) We first show that any two values of  $e$  differ by an element of  $N_aN_{ac}N_dN_{bd}$ . For this, we suppose given  $\varepsilon \in F_{a,c}^\times$ ,  $v \in F_{b,d}^\times$ ,  $x, y, e \in F^\times$  and  $\omega \in F_{b,c}^\times$  such that  $N_{a,c}(\varepsilon) = x^2$ ,  $N_{b,d}(v) = y^2$ ,  $N_a(\varepsilon)N_d(v) = e\omega^2$ , and we prove that  $e \in N_aN_{ac}N_dN_{bd}$ . (We could also assume that  $(\sigma_b - 1)(\sigma_c - 1)\omega = 1$ , but we will see that it follows from the rest.)

By Lemma A.3 (1), there exist  $\varepsilon_a \in F_a^\times$ ,  $\varepsilon_c \in F_c^\times$  and  $\varepsilon_{ac} \in F_{ac}^\times$  such that  $\varepsilon = \varepsilon_a\varepsilon_c\varepsilon_{ac}$ , as well as  $v_b \in F_b^\times$ ,  $v_d \in F_d^\times$  and  $v_{bd} \in F_{bd}^\times$  such that  $v = v_bv_dv_{bd}$ .

We have

$$N_a(\varepsilon) = N_a(\varepsilon_a)N_{ac}(\varepsilon_{ac})\varepsilon_c^2, \quad N_d(v) = N_d(v_d)N_{bd}(v_{bd})v_b^2.$$

Define  $\omega_1 := \omega/(\varepsilon_cv_b) \in F_{b,c}^\times$ . Then  $N_a(\varepsilon)N_d(v) = e\omega^2$  may be rewritten as

$$N_a(\varepsilon_a)N_{ac}(\varepsilon_{ac})N_d(v_d)N_{bd}(v_{bd}) = e\omega_1^2. \tag{3.8}$$

In particular,  $\omega_1^2$  belongs to  $F^\times$ , therefore  $\omega_1$  belongs to at least one of  $F_b^\times$ ,  $F_c^\times$  and  $F_{bc}^\times$ . A simple computation now shows that  $\omega_1 = f\sqrt{b}^i\sqrt{c}^j$ , where  $f \in F^\times$  and  $i, j \in \{0, 1\}$ .

Since  $b = (-d) \cdot (-bd) \cdot d^{-2} \in N_d N_{bd}$  and  $c = (-a) \cdot (-ac) \cdot c^{-2} \in N_a N_{ac}$ , we deduce that  $\omega_1^2 \in N_a N_{ac} N_d N_{bd}$ . Now (3.8) implies that  $e \in N_a N_{ac} N_d N_{bd}$ , as desired.

For the converse, suppose that  $e = N_a(\varepsilon_a) N_{ac}(\varepsilon_{ac}) N_d(v_d) N_{bd}(v_{bd})$ , where  $\varepsilon_a \in F_a^\times$ ,  $\varepsilon_{ac} \in F_{ac}^\times$ ,  $v_d \in F_d^\times$  and  $v_{bd} \in F_{bd}^\times$ . Set  $\varepsilon = \varepsilon_a \varepsilon_{ac}$ ,  $v = v_d v_{bd}$  and  $\omega = 1$ . Then  $N_{a,c}(\varepsilon) \in F^{\times 2}$ ,  $N_{b,d}(v) \in F^{\times 2}$ ,  $N_a(\varepsilon) N_d(v) = e \omega^2$  and  $(\sigma_b - 1)(\sigma_c - 1)\omega = 1$ , as desired.

(c) This follows from (b) and Proposition 3.5. ■

### 3.4. Splitting varieties

We now interpret Proposition 3.5 in terms of splitting varieties. The material of this section is not needed for the proofs of Theorems 1.3, 1.4 and 1.6.

Let  $n \geq 2$  be an integer,  $a_1, \dots, a_n \in F^\times$ , and  $V$  be an  $F$ -variety. Consider the following property: For all field extensions  $K/F$ , we have

$$V(K) \neq \emptyset \Leftrightarrow \langle a_1, \dots, a_n \rangle \text{ vanishes over } K. \tag{3.9}$$

In the literature, a variety  $V$  satisfying (3.9) is sometimes called a *splitting variety* for  $\langle a_1, \dots, a_n \rangle$ .

The geometry of splitting varieties becomes increasingly complicated as  $n$  gets bigger. When  $n = 2$ , a splitting variety for  $\langle a_1, a_2 \rangle$  is the  $F$ -conic corresponding to the symbol  $(a_1, a_2)$ . Hopkins and Wickelgren [9] constructed a splitting variety for  $n = 3$ : it is a torus under a torus. When  $n = 4$ , a splitting variety was obtained in [7]. Pál and Schläpfl [20] constructed splitting varieties for all  $n$ : their examples are homogeneous spaces under  $SL_n$  with finite supersolvable stabilizers. These varieties were exploited by [8] for the proof of Conjecture 1.1 when  $F$  is a number field.

Let  $a, b, c, d \in F^\times$ , and consider the  $F$ -torus

$$S := R_{a,c}(\mathbb{G}_m) \times R_{b,d}(\mathbb{G}_m) \times \mathbb{G}_m^2 \times R_{b,c}(\mathbb{G}_m),$$

whose coordinates we denote by  $(\varepsilon, v, x, y, \omega)$ . Let  $T \subset S$  be the  $F$ -subgroup defined by the equations

- (1)  $(\sigma_c - 1)\omega = x/N_a(\varepsilon)$ ;
- (2)  $(\sigma_b - 1)\omega = y/N_d(v)$ ;
- (3)  $N_a(\varepsilon)N_d(v) = \omega^2$ .

Lattice computations show that  $T$  is a torus. Consider the  $T$ -torsor  $X \subset S$  given by the equations

- (1')  $(\sigma_c - 1)\omega = x\sqrt{b}/N_a(\varepsilon)$ ;
- (2')  $(\sigma_b - 1)\omega = y\sqrt{c}/N_d(v)$ ;
- (3')  $N_a(\varepsilon)N_d(v) = \omega^2$ .

We now show that  $X$  satisfies a variant of (3.9), where “vanishes” is replaced by “is defined”.

**Proposition 3.8.** *For all field extensions  $K/F$ , we have that  $X(K) \neq \emptyset$  if and only if  $\langle a, b, c, d \rangle$  is defined over  $K$ .*

*Proof.* Since the formation of  $T$  and  $X$  commutes with arbitrary field extensions, we may suppose that  $K = F$ . If  $(\varepsilon, v, x, y, \omega)$  belongs to  $X(F)$ , then

$$N_{a,c}(\varepsilon) = bx^2, \quad N_{b,d}(v) = cy^2$$

and

$$(\sigma_b - 1)(\sigma_c - 1)\omega = (\sigma_b - 1)\left(x \frac{\sqrt{b}}{N_a(\varepsilon)}\right) = -1,$$

hence  $\langle a, b, c, d \rangle$  is defined by Proposition 3.5.

Conversely, suppose that  $\langle a, b, c, d \rangle$  is defined. By Proposition 3.5, there exist  $\varepsilon \in F_{a,c}^\times$ ,  $v \in F_{b,d}^\times$  and  $\omega \in F_{b,c}^\times$  such that

$$N_a(\varepsilon)N_d(v) = \omega^2, \quad (\sigma_b - 1)(\sigma_c - 1)\omega = -1.$$

Define  $x, y \in F_{b,c}^\times$  by

$$x := \frac{(\sigma_c - 1)\omega \cdot N_a(\varepsilon)}{\sqrt{b}}, \quad y := \frac{(\sigma_b - 1)\omega \cdot N_d(v)}{\sqrt{c}}.$$

Then

$$(\sigma_b - 1)x = (\sigma_b - 1)(\sigma_c - 1)\omega \cdot (\sigma_b - 1)(N_a(\varepsilon)) \cdot (1 - \sigma_b)\sqrt{b} = (-1) \cdot 1 \cdot (-1) = 1.$$

Moreover, since  $N_d(v) \in F_b^\times$ , we have  $(\sigma_c - 1)(N_d(v)) = (\sigma_c - 1)(\omega^2)$ , therefore

$$(\sigma_c - 1)x = (\sigma_c - 1)^2(\omega) \cdot (\sigma_c - 1)(N_a(\varepsilon)) = (2 - 2\sigma_c)(\omega) \cdot (\sigma_c - 1)(\omega^2) = 1.$$

It follows that  $x$  belongs to  $F^\times$ . Similar calculations show that  $y$  belongs to  $F^\times$ , and hence  $(\varepsilon, v, x, y, \omega)$  belongs to  $X(F)$ . This completes the proof. ■

**Corollary 3.9.** *Let  $a, b, c, d \in F^\times$ . Then  $\langle a, b, c, d \rangle$  is defined over  $F$  if and only if there exists a finite field extension of odd degree  $F'/F$  such that  $\langle a, b, c, d \rangle$  is defined over  $F'$ .*

*Proof.* The Massey product  $\langle a, b, c, d \rangle$  vanishes if  $a, b, c, d$  are all squares (this is immediate, for example, from Theorem 2.4 (iv)), hence  $\langle a, b, c, d \rangle$  vanishes over  $F_{a,b,c,d}$ . By Proposition 3.8, this implies that  $X(F_{a,b,c,d}) \neq \emptyset$ , that is, the  $T$ -torsor  $X$  is split by  $F_{a,b,c,d}/F$ . Thus, by a restriction-corestriction argument, the order of  $[X] \in H^1(F, T)$  is a power of 2. Therefore, if  $X$  is split by an extension of odd degree, the order of  $[X]$  in  $H^1(F, T)$  is odd and a power of two, hence 1. ■

**Remark 3.10.** The variety  $X$  is a torsor under a torus. In contrast, all known splitting varieties for  $n = 4$  are quite involved. In particular, while Conjecture 1.1 predicts that Corollary 3.9 should also be true if “defined” is replaced by “vanishing”, we do not know how to prove it.

3.5. Galois  $U_5$ -algebras

Let  $a, b, c, d \in F^\times$ . In [7, Theorem A], an equivalent condition for the vanishing of the Massey product  $\langle a, b, c, d \rangle$  was given. In this section, we recover this result using our methods, and then we specialize to the case  $a = d$ . Our proof and that of [7, Theorem A] are closely related. In particular, the short exact sequence (3.10) below has been used in the proof of [7, Theorem A]; see [7, §2.4 and proof of Theorem 3.3].

**Proposition 3.11.** *Let  $a, b, c, d \in F^\times$ . The Massey product  $\langle a, b, c, d \rangle$  vanishes if and only if there exist  $\alpha \in F_a^\times$  and  $\delta \in F_d^\times$  such that*

- (1)  $N_a(\alpha) = b$  in  $F^\times/F^{\times 2}$ ;
- (2)  $N_d(\delta) = c$  in  $F^\times/F^{\times 2}$ ;
- (3)  $(\alpha, \delta) = 0$  in  $\text{Br}(F_{a,d})$ .

*Proof.* Write  $P$  for the subgroup of  $U_5$  defined by  $u_{12} = u_{13} = u_{23} = u_{34} = u_{35} = u_{45} = 0$ . This is an abelian normal subgroup of  $U_5$ . There is an exact sequence

$$1 \rightarrow P \rightarrow U_5 \rightarrow U_3 \times U_3 \rightarrow 1, \tag{3.10}$$

so  $P$  has a natural structure of a  $(U_3 \times U_3)$ -module.

Let  $N$  and  $S$  be the subgroups of  $U_3$  as in the proof of Proposition 3.2 (a). In particular,  $N$  is an  $S$ -module (by conjugation). Let  $N'$  and  $S'$  be the corresponding subgroups of  $U_3$  as in the proof of Proposition 3.2 (b).

The bilinear map

$$N \times N' \rightarrow P$$

taking a pair of matrices

$$\begin{bmatrix} 1 & 0 & f_1 \\ & 1 & e_1 \\ & & 1 \end{bmatrix}, \begin{bmatrix} 1 & e_2 & f_2 \\ & 1 & 0 \\ & & 1 \end{bmatrix}$$

to

$$\begin{bmatrix} 1 & 0 & 0 & f_1 e_2 & f_1 f_2 \\ & 1 & 0 & e_1 e_2 & e_1 f_2 \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix}$$

yields an isomorphism of  $(U_3 \times U_3)$ -modules

$$N \otimes N' \xrightarrow{\sim} P.$$

The natural projections  $t: U_3 \rightarrow N$  and  $t': U_3 \rightarrow N'$  are 1-cocycles. A direct calculation shows that the class in  $H^2(U_3 \times U_3, P) \simeq H^2(U_3 \times U_3, N \otimes N')$  of the exact sequence (3.10) is equal to the cup-product  $t \cup t'$ .

Let  $\alpha \in F_a^\times$  be such that  $N_a(\alpha) = b \in F^\times/F^{\times 2}$ , and let  $h: \Gamma_F \rightarrow U_3$  be a group homomorphism corresponding to the Galois  $U_3$ -algebra  $(F_{a,b})_\alpha$  via (2.1). Similarly, let  $\delta \in F_d^\times$  be such that  $N_d(\delta) = c \in F^\times/F^{\times 2}$ , and let  $h': \Gamma_F \rightarrow U_3$  be a group homomorphism corresponding to  $(F_{c,d})_\delta$  via (2.1).

As in the proof of Proposition 3.2, the  $\Gamma_F$ -module  $N$ , where  $\Gamma_F$  acts via  $h$ , is the induced module  $\text{Ind}_{F_a}^F(\mathbb{Z}/2\mathbb{Z})$ . It follows that the image of  $t$  under the composition

$$H^1(U_3, N) \xrightarrow{h^*} H^1(F, N) = H^1(F_a, \mathbb{Z}/2\mathbb{Z}) = F_a^\times / F_a^{\times 2}$$

is equal to the class of  $\alpha$ . Similarly, the image of  $t'$  under the composition

$$H^1(U_3, N') \xrightarrow{(h')^*} H^1(F, N') = H^1(F_d, \mathbb{Z}/2\mathbb{Z}) = F_d^\times / F_d^{\times 2}$$

is equal to the class of  $\delta$ .

Note that

$$P = N \otimes N' = \text{Ind}_{F_{a,d}}^F(\mathbb{Z}/2\mathbb{Z}),$$

where we view  $P$  as a  $\Gamma_F$ -module via  $(h, h'): \Gamma_F \rightarrow U_3 \times U_3$ .

Consider the commutative diagram

$$\begin{CD} H^1(U_3, N) \otimes H^1(U_3, N') @>\cup>> H^2(U_3 \times U_3, P) \\ @VVh^* \otimes (h')^*V @VV(h, h')^*V \\ H^1(F, N) \otimes H^1(F, N') @>\cup>> H^2(F, P) \\ @| @| \\ H^1(F_a, \mathbb{Z}/2\mathbb{Z}) \otimes H^1(F_d, \mathbb{Z}/2\mathbb{Z}) @>\cup>> H^2(F_{a,d}, \mathbb{Z}/2\mathbb{Z}). \end{CD}$$

It follows that the image of  $t \otimes t'$  under the composition

$$H^2(U_3 \times U_3, P) \xrightarrow{(h, h')^*} H^2(F, P) = H^2(F_{a,d}, \mathbb{Z}/2\mathbb{Z}) \subset \text{Br}(F_{a,d})$$

is equal to the cup-product  $(\alpha, \delta)$ . The homomorphism  $(h, h'): \Gamma_F \rightarrow U_3 \times U_3$  lifts to a homomorphism  $\Gamma_F \rightarrow U_5$  if and only if the pullback of the exact sequence (3.10) via  $(h, h')$  is split, that is, if and only if the image of  $t \otimes t'$  in  $H^2(F, P) = H^2(F_{a,d}, \mathbb{Z}/2\mathbb{Z})$  is trivial. Since this image is  $(\alpha, \delta) \in H^2(F_{a,d}, \mathbb{Z}/2\mathbb{Z}) \subset \text{Br}(F_{a,d})$ , this and Theorem 2.4 (iv) imply the conclusion. ■

The following result is a reformulation of [7, Theorem A].

**Corollary 3.12.** *Let  $a, b, c, d \in F^\times$  be such that  $(a, b) = (c, d) = 0$  in  $\text{Br}(F)$ . Let  $\alpha \in F_a^\times$  and  $\delta \in F_d^\times$  be such that  $N_a(\alpha) = b$  in  $F^\times/F^{\times 2}$  and  $N_d(\delta) = c$  in  $F^\times/F^{\times 2}$ . The Massey product  $\langle a, b, c, d \rangle$  vanishes if and only if there exist  $x, y \in F^\times$  such that  $(\alpha x, \delta y) = 0$  in  $\text{Br}(F_{a,d})$ .*

*Proof.* Recall that  $\alpha$  and  $\delta$  exist by Lemma 2.1. Suppose  $(\alpha x, \delta y) = 0$  in  $\text{Br}(F_{a,d})$  for some  $x, y \in F^\times$ . Since  $N_a(\alpha x) = b$  in  $F^\times/F^{\times 2}$  and  $N_d(\delta y) = c$  in  $F^\times/F^{\times 2}$ , the Massey product  $\langle a, b, c, d \rangle$  vanishes by Proposition 3.11.

Conversely, if  $\langle a, b, c, d \rangle$  vanishes, then Proposition 3.11 gives  $\alpha' \in F_a^\times$  and  $\delta' \in F_d^\times$  such that  $N_a(\alpha') = b$  in  $F^\times/F^{\times 2}$ ,  $N_d(\delta') = c$  in  $F^\times/F^{\times 2}$  and  $(\alpha', \delta') = 0$  in  $\text{Br}(F_{a,d})$ . There exist  $u_a \in F^\times$  and  $u_d \in F^\times$  such that  $N_a(\alpha') = N_a(\alpha)u_a^2 = N_a(\alpha u_a)$  and  $N_d(\delta') = N_d(\delta)u_d^2 = N_d(\delta u_d)$ . Now Hilbert's Theorem 90 implies the existence of  $\eta_a \in F_a^\times$  such that  $\alpha' = \alpha u_a(\sigma_a - 1)\eta_a = \alpha u_a N_a(\eta_a)\eta_a^{-2}$ . Similarly, there exists  $\eta_d \in F_d^\times$  such that  $\delta' = \delta u_d N_d(\eta_d)\eta_d^{-2}$ . Set

$$x := N_a(\eta_a)u_a \in F^\times \quad \text{and} \quad y := N_d(\eta_d)u_d \in F^\times.$$

Then

$$0 = (\alpha', \delta') = (\alpha x \eta_a^{-2}, \delta y \eta_d^{-2}) = (\alpha x, \delta y) \quad \text{in } \text{Br}(F_{a,d}).$$

as desired. ■

**Corollary 3.13.** *Let  $a, b, c \in F^\times$  be such that  $(a, b) = (c, a) = 0$  in  $\text{Br}(F)$ . Let  $\alpha, \delta \in F_a^\times$  be such that  $N_a(\alpha) = b$  and  $N_a(\delta) = c$ . The Massey product  $\langle a, b, c, a \rangle$  vanishes over  $F$  if and only if there exist  $x, y \in F^\times$  such that  $(\alpha x, \delta y) = (\alpha x, c) = 0$  in  $\text{Br}(F_a)$ .*

*Proof.* Write  $F_a = F[u_a]/(u_a^2 - a)$  and  $F_{a,a} = F[v_a, w_a]/(v_a^2 - a, w_a^2 - a)$ . We have an  $F$ -algebra isomorphism

$$\varphi: F_{a,a} \xrightarrow{\sim} F_a \times F_a, \quad v_a \mapsto (u_a, u_a), \quad w_a \mapsto (u_a, -u_a).$$

If  $\pi = \pi_1 + \pi_2 v_a + \pi_3 w_a + \pi_4 v_a w_a \in F_{a,a}$ , then

$$\varphi(\pi) = (\pi_1 + a\pi_4 + (\pi_2 + \pi_3)u_a, \pi_1 - a\pi_4 + (\pi_2 - \pi_3)u_a). \tag{3.11}$$

Let  $x, y \in F^\times$ . Since  $\alpha$  is in the  $F$ -span of 1 and  $v_a$ , and  $\delta$  is in the  $F$ -span of 1 and  $w_a$ , by (3.11) we have

$$\varphi(\alpha x) = (\alpha x, \alpha x) \quad \text{and} \quad \varphi(\delta y) = (\delta y, \sigma_a(\delta)y).$$

It follows that, letting

$$\varphi_*: \text{Br}(F_{a,a}) \xrightarrow{\sim} \text{Br}(F_a) \times \text{Br}(F_a)$$

be the isomorphism induced by  $\varphi$ , we have

$$\varphi_*((\alpha x, \delta y)) = ((\alpha x, \delta y), (\alpha x, \sigma_a(\delta)y)).$$

In particular,  $(\alpha x, \delta y) = 0$  in  $\text{Br}(F_{a,a})$  if and only if  $(\alpha x, \delta y) = (\alpha x, \sigma_a(\delta)y) = 0$  in  $\text{Br}(F_a)$ . Since

$$(\alpha x, \delta y) + (\alpha x, \sigma_a(\delta)y) = (\alpha x, c) \quad \text{in } \text{Br}(F_a),$$

we deduce that  $(\alpha x, \delta y) = 0$  in  $\text{Br}(F_{a,a})$  if and only if  $(\alpha x, \delta y) = (\alpha x, c) = 0$  in  $\text{Br}(F_a)$ . The conclusion follows from Corollary 3.12. ■

**4. Proof of Theorem 1.3**

Let  $a, b, c, d \in F^\times$ , suppose that  $b + c = 1$  and let  $v_1, v_2, u_1, u_2 \in F$  be such that

$$\begin{cases} v_1^2 - bv_2^2 = a, \\ u_1^2 - cu_2^2 = d, \\ v_1v_2u_1u_2(v_1 + v_2)(u_1 + u_2)(v_1 + u_1) \neq 0. \end{cases} \tag{4.1}$$

By Lemma 2.1, this implies that  $(a, b) = (b, c) = (c, d) = 0$  in  $\text{Br}(F)$ .

Define  $r, s, t \in F^\times$  as follows:

$$\begin{aligned} r &:= 2(v_1 + v_2)(u_1 + u_2)v_2u_2, \\ s &:= 2(v_1 + u_1)(u_1 + u_2), \\ t &:= 2(v_1 + u_1)(v_1 + v_2). \end{aligned}$$

As we will explain in Section 4.4, the proof of Theorem 1.3 will follow from the next two propositions.

**Proposition 4.1.** *Suppose that  $a = d$ .*

- (a) *The Massey product  $\langle a, b, c, a \rangle$  is defined over  $F$  if and only if  $r \in N_a N_{ab} N_{ac}$ .*
- (b) *The Massey product  $\langle a, b, c, a \rangle$  vanishes over  $F$  if and only if  $t \in N_c N_{ac} N_{bc}$ .*

**Proposition 4.2.** *Suppose that  $a = d$ . Then*

$$r \in N_a N_{ab} N_{ac} \Leftrightarrow s \in N_b N_{ab} N_{bc} \Leftrightarrow t \in N_c N_{ac} N_{bc}.$$

4.1. *Proof of Proposition 4.1 (a)*

We maintain the notations and assumptions of the beginning of Section 4. Since  $(a, b) = (b, c) = (c, d) = 0$  in  $\text{Br}(F)$ , by Corollary 3.4 the Massey products  $\langle a, b, c \rangle$  and  $\langle b, c, d \rangle$  vanish. Therefore, by Proposition 3.3, there exist  $\varepsilon \in F_{a,c}^\times$  and  $v \in F_{b,d}^\times$  such that  $K_1 = (F_{a,b,c})_{N_c(\varepsilon), N_a(\varepsilon), \varepsilon}$  and  $K_2 = (F_{b,c,d})_{N_d(v), N_b(v), v}$  are Galois  $U_4$ -algebras such that  $K_1^{Q_4} = F_{a,b,c}$  and  $K_2^{Q_4} = F_{b,c,d}$ . By Proposition 3.7 (a), there exist  $e \in F^\times$  and  $\omega \in F_{b,c}^\times$  such that

$$N_a(\varepsilon)N_d(v) = e\omega^2, \quad (\sigma_b - 1)(\sigma_c - 1)\omega = -1.$$

**Proposition 4.3.** *We have  $e = r$  in  $F^\times/N_a N_{ac} N_d N_{bd}$ . In particular,  $\langle a, b, c, d \rangle$  is defined if and only if  $r \in N_a N_{ac} N_d N_{bd}$ .*

*Proof.* (a) Define

$$\begin{aligned} \alpha &:= \frac{v_1}{v_2} + \frac{1}{v_2}\sqrt{a} \in F_a^\times, & \beta &:= 1 + \sqrt{b} \in F_b^\times, \\ \gamma &:= 1 + \sqrt{c} \in F_c^\times, & \delta &:= \frac{u_1}{u_2} + \frac{1}{u_2}\sqrt{d} \in F_d^\times. \end{aligned}$$

Note that  $N_a(\alpha) = b = N_c(\gamma)$  and  $N_b(\beta) = c = N_d(\delta)$ . Set

$$\varepsilon := \alpha + \gamma \in F_{a,c}^\times, \quad v := \beta + \delta \in F_{b,d}^\times.$$

By Lemma A.4(1), we have

$$N_a(\varepsilon) = \gamma x, \quad N_d(v) = \beta y,$$

where

$$\begin{aligned} x &:= \text{Tr}_a(\alpha) + \text{Tr}_c(\gamma) = 2\left(\frac{v_1}{v_2} + 1\right) \in F^\times, \\ y &:= \text{Tr}_b(\beta) + \text{Tr}_d(\delta) = 2\left(1 + \frac{u_1}{u_2}\right) \in F^\times. \end{aligned}$$

In particular,

$$N_{a,c}(\varepsilon) = bx^2, \quad N_{b,d}(v) = cy^2.$$

Define

$$\omega := \frac{1 + \sqrt{b} + \sqrt{c}}{v_2 u_2} \in F_{b,c}^\times.$$

Note that  $\omega \neq 0$  because  $1, \sqrt{b}$  and  $\sqrt{c}$  are linearly independent over  $F$ . Moreover,

$$\begin{aligned} (\sigma_b - 1)(\sigma_c - 1)\omega &= \frac{(\sigma_b \sigma_c + 1)\omega}{(\sigma_b + \sigma_c)\omega} = \frac{(1 + \sqrt{b} + \sqrt{c})(1 - \sqrt{b} - \sqrt{c})}{(1 - \sqrt{b} + \sqrt{c})(1 + \sqrt{b} - \sqrt{c})} \\ &= \frac{-2\sqrt{bc}}{2\sqrt{bc}} = -1. \end{aligned}$$

We have  $(1 + \sqrt{b} + \sqrt{c})^2 = 2(1 + \sqrt{b})(1 + \sqrt{c})$ , hence

$$\begin{aligned} \frac{N_a(\varepsilon)N_d(v)}{\omega^2} &= \frac{xy(1 + \sqrt{b})(1 + \sqrt{c})v_2^2 u_2^2}{(1 + \sqrt{b} + \sqrt{c})^2} = \frac{xyv_2^2 u_2^2}{2} \\ &= 2\left(\frac{v_1}{v_2} + 1\right)\left(1 + \frac{u_1}{u_2}\right)v_2^2 u_2^2 = r. \end{aligned}$$

Thus  $N_a(\varepsilon)N_d(v) = r\omega^2$ . We conclude from Proposition 3.7(b) that  $e = r$  modulo  $N_a N_{ac} N_d N_{bd}$ . ■

*Proof of Proposition 4.1(a).* Since  $a = d$ , we have  $N_a N_{ac} N_d N_{bd} = N_a N_{ab} N_{ac}$ . The conclusion follows from Propositions 4.3 and 3.7. ■

#### 4.2. Proof of Proposition 4.1(b)

The next proposition is the key step for our proof of Proposition 4.1(b). Its proof is the only place where we need to use quadratic form theory in this paper.

**Proposition 4.4.** *Let  $a \in F^\times$  and  $\pi, \mu \in F_a^\times$  be such that  $N_a(\pi, \mu) = 0$  in  $\text{Br}(F)$ . Then there exists  $z \in F^\times$  such that  $(\pi, \mu z) = 0$  in  $\text{Br}(F_a)$ .*

*Proof.* Here we use the theory of Albert forms attached to biquaternion algebras; see [11, §16.A]. As explained in [11, Example 16.4], given a biquaternion  $F$ -algebra  $A := (a_1, b_1) \otimes (a_2, b_2)$ , the quadratic form  $\langle a_1, b_1, -a_1b_1, -a_2, -b_2, a_2b_2 \rangle$  is an Albert form of  $A$ . Given two presentations of  $A$  as a tensor product of two quaternion algebras, the corresponding Albert forms are similar to each other; see [11, Proposition 16.3].

Let  $K/F$  be an étale algebra of degree 2, let  $s: K \rightarrow F$  be a non-zero linear map such that  $s(1) = 0$ , let  $Q$  be a quaternion algebra over  $K$ , let  $Q^0 \subset Q$  be the subspace of pure quaternions, let  $q: Q^0 \rightarrow K$  be the quadratic form given by squaring, and let  $s_*(q)$  be the transfer of  $q$ ; see [12, Chapter VII, §1]. Then it follows from [11, Propositions 16.23 and 16.27] that  $s_*(q)$  is similar to an Albert form over  $F$  of the biquaternion  $F$ -algebra given by the corestriction  $N_{K/F}(Q)$ ; see the proof of [11, Corollary 16.28]. Thus, by Albert’s theorem [11, Theorem 16.5]:

$$\text{If } N_{K/F}(Q) \text{ is split, then } s_*(q) \text{ is hyperbolic.} \tag{4.2}$$

Now let  $K = F_a$ , let  $s: F_a \rightarrow F$  be a non-zero  $F$ -linear map such that  $s(1) = 0$ , and let  $Q = (\pi, \mu)$ . Then  $q = \langle \pi, \mu, -\pi\mu \rangle$ . By assumption,  $N_a(\pi, \mu)$  is split, hence by (4.2) the 6-dimensional quadratic form  $s_*(q)$  is hyperbolic. Since  $4 > 6/2$ , the 4-dimensional subform  $s_*\langle \mu, -\pi\mu \rangle$  of  $s_*(q)$  is isotropic. We deduce that the form  $\langle \mu, -\pi\mu \rangle$  over  $F_a$  represents an element of  $F$ . If  $\langle \mu, -\pi\mu \rangle$  is isotropic, then  $\pi \in F_a^{\times 2}$ , hence  $(\pi, \mu) = 0$  in  $\text{Br}(F_a)$ , and we may take  $z = 1$ . Otherwise, the form  $\langle \mu, -\pi\mu \rangle$  over  $F_a$  represents an element  $z \in F^\times$ , then  $\mu z$  is represented by  $\langle 1, -\pi \rangle$ . By Lemma 2.1, this implies that  $(\pi, \mu z) = 0$  in  $\text{Br}(F_a)$  and completes the proof. ■

We maintain the notations and assumptions of the beginning of Section 4. Suppose further that  $a = d$ . Let

$$l := v_1 + u_1, \quad \alpha := lv_1 + l\sqrt{a} \in F_a^\times, \quad \delta := lu_1 + l\sqrt{a} \in F_a^\times. \tag{4.3}$$

By (4.1), we have

$$N_a(\alpha) = b(lv_2)^2, \quad N_a(\delta) = c(lu_2)^2.$$

- Corollary 4.5.** (a) *If  $N_a(\alpha x, \delta y) = 0$  in  $\text{Br}(F)$  for some  $x, y \in F^\times$ , then  $x \in N_c N_{bc}$ .*  
 (b) *For every  $x \in N_c N_{bc}$ , there exists  $y \in F^\times$  such that  $(\alpha x, \delta y) = 0$  in  $\text{Br}(F_a)$ .*

*Proof.* We first show that for all  $x, y \in F^\times$ :

$$N_a(\alpha x, \delta y) = (b, y) + (x, c) \quad \text{in } \text{Br}(F). \tag{4.4}$$

Indeed, since  $\alpha + \sigma_a(\delta) = l^2$ , by Lemma 2.1 we have  $(\alpha, \sigma_a(\delta)) = 0$  in  $\text{Br}(F_a)$ , hence

$$(\alpha, \delta) = (\alpha, \delta) + (\alpha, \sigma_a(\delta)) = (\alpha, N_a(\delta)) = (\alpha, c) \quad \text{in } \text{Br}(F_a).$$

It follows that

$$\begin{aligned} (\alpha x, \delta y) &= (\alpha, \delta) + (\alpha, y) + (x, \delta) + (x, y) \\ &= (\alpha, c) + (\alpha, y) + (x, \delta) + (x, y) \quad \text{in } \text{Br}(F_a). \end{aligned} \quad \blacksquare$$

Now (4.4) follows by applying  $N_a$  and using that  $N_a(\alpha) = b$ ,  $N_a(\delta) = c$ ,  $(b, c) = 0$  and  $N_a(x, y) = 2(x, y) = 0$ .

(a) By (4.4), we have  $(b, y) + (x, c) = 0$ . The conclusion follows from Lemma A.1.

(b) Write  $x = n_c n_{bc}$ , where  $n_c \in N_c$  and  $n_{bc} \in N_{bc}$ . Then by formula (4.4), we have  $N_a(\alpha x, \delta n_{bc}) = 0$ . By Proposition 4.4 applied to  $\pi = \alpha x$  and  $\mu = \delta n_{bc}$ , there exists  $z \in F^\times$  such that  $(\alpha x, \delta n_{bc} z) = 0$  in  $\text{Br}(F_a)$ . Letting  $y := n_{bc} z$ , we obtain  $(\alpha x, \delta y) = 0$  in  $\text{Br}(F_a)$ , as desired.

**Remark 4.6.** We give a proof of Corollary 4.5 (b) that minimizes the use of quadratic form theory. Let  $x \in F^\times$  and consider the quadratic form  $q_x := \langle \delta, -\alpha x \delta \rangle$  over  $F_a$ . We first show that

$$(\alpha x, \delta y) = 0 \text{ for some } y \in F^\times \Leftrightarrow q_x \text{ represents an element of } F^\times. \tag{4.5}$$

Indeed, let  $y \in F^\times$ . Then  $(\alpha x, \delta y) = 0$  in  $\text{Br}(F_a)$  if and only if the quadratic form  $\langle 1, -\alpha x \rangle$  over  $F_a$  represents  $\delta y$ . This is in turn equivalent to  $y$  being represented by  $q_x$ . This proves (4.5).

Now let  $s: F_a \rightarrow F$  be the  $F$ -linear map such that  $s(1) = 0$  and  $s(\sqrt{a}) = 1$ . The form  $q_x$  over  $F_a$  represents a value in  $F$  if and only if the form  $s_*(q_x)$  over  $F$  is isotropic.

Suppose first that  $q_x$  is isotropic. Then  $\alpha x \in F_a^{\times 2}$ , hence  $(\alpha x, \delta) = 0$  in  $\text{Br}(F_a)$ , that is, the conclusion of Corollary 4.5 (b) is true for  $y = 1$ .

Suppose now that  $q_x$  is anisotropic. A simple computation shows that

$$s_*(q_x) = \langle l, -lc, -lx, lbcx \rangle. \tag{4.6}$$

Since  $x \in N_c N_{bc}$ , there exist  $w_1, w_2, w_3, w_4 \in F$  such that

$$w_1^2 - cw_2^2 = x(w_3^2 - bcw_4^2) \neq 0.$$

Multiplying both sides by  $l$  and using (4.6), we deduce that  $s_*(q_x)$  is isotropic. It follows that  $q_x$  represents a value in  $F$ . Since  $q_x$  is anisotropic, it represents a value in  $F^\times$ , and so by (4.5) there exists  $y \in F^\times$  such that  $(\alpha x, \delta y) = 0$  in  $\text{Br}(F_a)$ . This implies Corollary 4.5 (b) when  $q_x$  is anisotropic, thus completing the proof.

**Lemma 4.7.** *Let  $x \in F^\times$ . Then  $(\alpha x, c) = 0$  in  $\text{Br}(F_a)$  if and only if  $x \in tN_c N_{ac}$ .*

*Proof.* We have

$$N_a(\alpha) = b(lv_2)^2 = (1 - c)(lv_2)^2 = N_c(lv_2(1 + \sqrt{c}))$$

and

$$\text{Tr}_a(\alpha) + \text{Tr}_c(lv_2(1 + \sqrt{c})) = 2lv_1 + 2lv_2 = t.$$

Now Lemma A.4 (3) implies  $(\alpha, c) = (t, c)$  in  $\text{Br}(F_a)$ , hence, adding  $(x, c)$  to both sides,

$$(\alpha x, c) = (tx, c) \text{ in } \text{Br}(F_a).$$

Thus  $(\alpha x, c) = 0$  in  $\text{Br}(F_a)$  if and only if  $(tx, c) = 0$  in  $\text{Br}(F_a)$ . By [24, Chapter XIV, Proposition 2], this is in turn equivalent to the existence of  $y \in F^\times$  such that  $(tx, c) = (a, y)$  in  $\text{Br}(F)$ . By Lemma A.1, this is equivalent to  $tx \in N_c N_{ac}$ , that is,  $x \in tN_c N_{ac}$ . ■

*Proof of Proposition 4.1 (b).* By Corollary 3.13, the Massey product  $\langle a, b, c, a \rangle$  vanishes over  $F$  if and only if there exist  $x, y \in F^\times$  such that

$$(\alpha x, \delta y) = (\alpha x, c) = 0 \quad \text{in } \text{Br}(F_a).$$

According to Corollary 4.5 (a) and Lemma 4.7, the two equations are satisfied if and only if  $tN_cN_{ac} \cap N_cN_{bc}$  is non-empty, that is,  $t \in N_cN_{ac}N_{bc}$ . ■

4.3. *Proof of Proposition 4.2*

We maintain the notations and assumptions of the beginning of Section 4.

**Lemma 4.8.** *We have  $(r, a) + (s, b) + (t, c) = 0$  in  $\text{Br}(F)$ .*

*Proof.* We have

$$u_1^2 + v_2^2 = (v_1^2 - bv_2^2 + cu_2^2) + v_2^2 = v_1^2 + c(v_2^2 + u_2^2),$$

hence

$$\begin{aligned} (v_1 + u_1 + v_2)^2 &= v_1^2 + (u_1^2 + v_2^2) + 2v_1u_1 + 2v_1v_2 + 2u_1v_2 \\ &= 2v_1^2 + c(v_2^2 + u_2^2) + 2v_1u_1 + 2v_1v_2 + 2u_1v_2 \\ &= t + c(v_2^2 + u_2^2). \end{aligned}$$

In other terms, the conic of equation  $tX^2 + c(v_2^2 + u_2^2)Y^2 = Z^2$  (which is smooth if  $v_2^2 + u_2^2 \neq 0$ ) has the  $F$ -point  $(1 : 1 : v_1 + u_1 + u_2)$ . Thus by Lemma 2.1,

$$(t, c) = (t, v_2^2 + u_2^2) \quad \text{if } v_2^2 + u_2^2 \neq 0, \tag{4.7}$$

and  $(t, c) = 0$  if  $v_2^2 + u_2^2 = 0$ . Similarly,

$$(s, b) = (s, v_2^2 + u_2^2) \quad \text{if } v_2^2 + u_2^2 \neq 0,$$

and  $(s, b) = 0$  if  $v_2^2 + u_2^2 = 0$ . We also have

$$\begin{aligned} &(v_2u_2 + v_1u_2 + v_2u_1)^2 \\ &= v_2^2u_2^2 + v_1^2u_2^2 + v_2^2u_1^2 + 2v_2u_2(v_1u_1 + v_1u_2 + v_2u_1) \\ &= -v_2^2u_2^2 + v_1^2u_2^2 + v_2^2u_1^2 + 2v_2u_2(v_1u_1 + v_1u_2 + v_2u_1 + v_2u_2) \\ &= -v_2^2u_2^2 + (a + bv_2^2)u_2^2 + v_2^2(a + cu_2^2) + r = a(v_2^2 + u_2^2) + r. \end{aligned}$$

Now Lemma 2.1 implies

$$(r, a) = (r, v_2^2 + u_2^2) \quad \text{if } v_2^2 + u_2^2 \neq 0,$$

and  $(r, a) = 0$  if  $v_2^2 + u_2^2 = 0$ . In particular, when  $v_2^2 + u_2^2 = 0$ , we have  $(r, a) = (s, b) = (t, c) = 0$ , which implies the conclusion in this case. Suppose now that  $v_2^2 + u_2^2 \neq 0$ . Note that

$$rst = 2v_2u_2 \cdot \left( \frac{rl}{v_2u_2} \right)^2.$$

Finally,

$$(2v_2u_2, v_2^2 + u_2^2) = 0 \tag{4.8}$$

since the smooth conic of equation  $(2v_2u_2)X^2 + (v_2^2 + u_2^2)Y^2 = Z^2$  has the  $F$ -point  $(1 : 1 : v_2 + u_2)$ . Putting (4.7) and (4.8) together, we conclude that

$$\begin{aligned} (r, a) + (s, b) + (t, c) &= (r, v_2^2 + u_2^2) + (s, v_2^2 + u_2^2) + (t, v_2^2 + u_2^2) \\ &= (rst, v_2^2 + u_2^2) = (2v_2u_2, v_2^2 + u_2^2) = 0, \end{aligned}$$

which completes the proof. ■

**Lemma 4.9.** *Let  $a', b', c' \in F^\times$  be such that  $(a', a) + (b', b) + (c', c) = 0$  in  $\text{Br}(F)$ , then*

$$a' \in N_a N_{ab} N_{ac} \Leftrightarrow b' \in N_b N_{ab} N_{bc} \Leftrightarrow c' \in N_c N_{ac} N_{bc}.$$

*Proof.* Suppose that  $c' = n_c n_{ac} n_{bc}$ , where  $n_c \in N_c, n_{ac} \in N_{ac}$  and  $n_{bc} \in N_{bc}$ . Then

$$\begin{aligned} 0 &= (c', c) + (b', b) + (a', a) = (n_c n_{ac} n_{bc}, c) + (b', b) + (a', a) \\ &= (n_{ac}, c) + (n_{bc}, c) + (b', b) + (a', a) = (n_{ac}, a) + (n_{bc}, b) + (b', b) + (a', a) \\ &= (n_{ac} a', a) + (n_{bc} b', b). \end{aligned}$$

Thus Lemma A.1 implies that  $n_{ac} a' \in N_a N_{ab}$  and  $n_{bc} b' \in N_b N_{ab}$ . Since the statement of Lemma 4.9 is symmetric in  $a, b, c$ , this completes the proof. ■

*Proof of Proposition 4.2.* Immediate from Lemmas 4.8 and 4.9. ■

#### 4.4. Proof of Theorem 1.3

As anticipated, Theorem 1.3 will follow from Propositions 4.1 and 4.2.

*Proof of Theorem 1.3.* Suppose that the Massey product  $\langle a, b, c, a \rangle$  is defined over  $F$ . By Remark 2.2, we have  $(a, b) = (b, c) = (c, a) = 0$  in  $\text{Br}(F)$ . If  $F$  is a finite field,  $\langle a, b, c, a \rangle$  vanishes by Corollary 2.5. We may thus assume that  $F$  is infinite. The Massey product  $\langle a, b, c, a \rangle$  depends only on the classes of  $a, b, c$  in  $F^\times / F^{\times 2}$ . Since  $(b, c) = 0$ , by Lemma 2.1 there exist  $x, y \in F^\times$  such that  $bx^2 + cy^2 = 1$ . Replacing  $b$  by  $bx^2$  and  $c$  by  $cy^2$ , we may suppose that  $b + c = 1$ .

Consider  $(\mathbb{A}_F^2)^2$  with coordinates  $(v_1, v_2, u_1, u_2)$ , and let  $Y \subset (\mathbb{A}_F^2)^2$  be the locally-closed subvariety given by (4.1). Since  $(a, b) = (a, c) = 0$  in  $\text{Br}(F)$  and  $F$  is infinite,  $Y$  is  $F$ -rational and so has an  $F$ -point, that is, (4.1) has a solution. Now Proposition 4.1 (a) implies that  $r \in N_a N_{ab} N_{ac}$ . It follows from Proposition 4.2 that  $t \in N_c N_{ac} N_{bc}$ . By Proposition 4.1 (b), the Massey product  $\langle a, b, c, a \rangle$  vanishes, as desired. ■

**Remark 4.10.** The final part of the proof of Theorem 1.3 may be replaced by the following specialization argument. Suppose that  $F$  is infinite, consider  $(\mathbb{A}_F^2)^2$  with coordinates  $(v_1, v_2, u_1, u_2)$ , and let  $Z \subset (\mathbb{A}_F^2)^2$  be the smooth variety given by the first two equalities of (4.1). Then the restrictions to  $Z$  of the coordinate functions of  $(\mathbb{A}_F^2)^2$  satisfy (4.1)

over  $F(Z)$ . Since  $Z$  is smooth and has an  $F$ -point, by Proposition 2.10 we may replace  $F$  by  $F(Z)$ . The conclusion then follows from Propositions 4.1 and 4.2. A similar argument could also be used for the proof of Theorem 1.4 in the next section.

**5. Proof of Theorem 1.4**

Let  $b, c \in F^\times$  be such that  $b + c = 1$ . In particular,  $(b, c) = 0$  in  $\text{Br}(F)$ . Suppose further that  $(bc, b) = (bc, c) = 0$ . This is equivalent to  $(b, -1) = (c, -1) = 0$ , that is, by Lemma 2.1, to  $-1 \in N_b \cap N_c$ .

Before moving to the proof of Theorem 1.4, we specialize some of the definitions of Section 4 to the case  $a = d = bc$ . Let  $(v_1, v_2, u_1, u_2) \in (F^\times)^4$  be a solution of (4.1), where we set  $a = d = bc$ . Set

$$v := v_1 + v_2\sqrt{b} \in F_b^\times, \quad u := u_1 + u_2\sqrt{c} \in F_c^\times,$$

so that  $N_b(v) = N_c(u) = bc$ . The definition of (4.3) specializes to

$$l := v_1 + u_1, \quad \alpha := lv_1 + l\sqrt{bc} \in F_{bc}^\times, \quad \delta := lu_1 + l\sqrt{bc} \in F_{bc}^\times. \tag{5.1}$$

We have

$$N_{bc}(\alpha) = b(lv_2)^2, \quad N_{bc}(\delta) = c(lu_2)^2.$$

We may also write

$$N_{bc}(\alpha) = b(lv_2)^2 = (1 - c)(lv_2)^2 = N_c(lv_2(1 + \sqrt{c})).$$

Following the definition given after (4.1), we have

$$t := 2l(v_1 + v_2) = \text{Tr}_{bc}(\alpha) + \text{Tr}_c(lv_2(1 + \sqrt{c})).$$

Since  $v_1 + v_2 \neq 0$  by (4.1), we have  $t \neq 0$ .

**Lemma 5.1.** *We have  $-t^2 \in N_{b,c}$ .*

*Proof.* According to Lemma A.4 (2) applied to  $\rho = \alpha$  and  $\mu = lv_2(1 + \sqrt{c})$ , we have that  $b(lv_2)^2t^2 \in N_{b,c}$ . Thus, in order to prove that  $-t^2 \in N_{b,c}$ , it suffices to show that  $-b(lv_2)^2 \in N_{b,c}$ . Since  $N_b(v) = N_c(u)$ , by Lemma A.4 (2) applied to  $\rho = v$  and  $\mu = u$ , we have  $4bcl^2 \in N_{b,c}$ .

We also have

$$N_b\left(\frac{v}{\sqrt{b}}\right) = -c = N_c(\sqrt{c}),$$

hence by Lemma A.4 (2) applied to  $\rho = v/\sqrt{b}$  and  $\mu = \sqrt{c}$ , we obtain that  $-4cv_2^2 \in N_{b,c}$ . Since  $16c^2 = N_{b,c}(2\sqrt{c})$ , it follows that

$$-b(lv_2)^2 = (4bcl^2) \cdot (-4cv_2^2) \cdot (16c^2)^{-1} \in N_{b,c},$$

as desired. ■

*Proof of Theorem 1.4.* If  $F$  is a finite field, then  $N_{b,c} = F^\times$  and by Corollary 2.5 every Massey product over  $F$  vanishes, hence Theorem 1.4 is true in this case. From now on, we suppose that  $F$  is infinite. Multiplying  $a, b, c, d$  by non-zero squares does not alter the Massey product  $\langle a, b, c, d \rangle$ , hence we may suppose that

$$a = d = bc \quad \text{and} \quad b + c = 1.$$

By Theorem 1.3, we know that (1) is equivalent to (2).

We now prove that (2) is equivalent to (3). We have  $(b, c) = 0$ , and we may suppose that  $(bc, b) = (bc, c) = 0$ , as it is implied by either (2) or (3). Consider  $(\mathbb{A}_F^2)^2$  with coordinates  $(v_1, v_2, u_1, u_2)$ , and let  $Y \subset (\mathbb{A}_F^2)^2$  be the locally-closed subvariety given by (4.1). The  $F$ -variety  $Y$  is rational because  $(bc, b) = (bc, c) = 0$ . Thus, since  $F$  is infinite,  $Y$  has an  $F$ -point, that is, (4.1) has a solution.

Recall that we defined  $\alpha \in F_a^\times$  and  $\delta \in F_d^\times$  such that  $N_{bc}(\alpha) = b$  in  $F^\times/F^{\times 2}$  and  $N_{bc}(\delta) = c$  in  $F^\times/F^{\times 2}$  in (5.1), as a special case of (4.3). By Corollary 3.13, the Massey product  $\langle bc, b, c, bc \rangle$  vanishes if and only if there exist  $x, y \in F^\times$  such that  $(\alpha x, c) = (\alpha x, \delta y) = 0$  in  $\text{Br}(F_{bc})$ . By Corollary 4.5 and Lemma 4.7, these equalities are equivalent to  $N_c N_{bc} \cap t N_b N_c \neq \emptyset$ . The latter is equivalent to  $t \in N_b N_c N_{bc}$ , which by Lemma A.3 (2) is equivalent to  $t^2 \in N_{b,c}$ . By Lemma 5.1, this is equivalent to  $-1 \in N_{b,c}$ , as desired. This shows that (2) is equivalent to (3), as desired. ■

As an application of Theorem 1.4, we recover the Harpaz–Wittenberg example [7, Example A.15].

Let  $K/F$  be a Galois extension of number fields,  $v$  be a place of  $F$  and  $w$  be a place of  $K$  above  $v$ . Let  $F_v$  be the completion of  $F$  at  $v$  and  $K_w$  be the completion of  $K$  at  $w$ . By definition, the local degree of  $K/F$  at  $v$  is equal to  $[K_w : F_v]$ .

Let  $w_1, \dots, w_m$  be the places of  $K$  above  $v$ . Since  $\text{Gal}(K/F)$  acts transitively on the  $w_i$ , the local degree of  $v$  does not depend on the choice of  $w$ . Moreover, the natural homomorphism of  $F_v$ -algebras  $K \otimes_F F_v \rightarrow \prod_{i=1}^m K_{w_i}$  is an isomorphism (see, e.g., [1, Chapter VII, proof of Proposition 1.2]), hence the local degree of  $v$  is a divisor of  $[K : F]$ , and it is equal to  $[K : F]$  if and only if  $m = 1$ , that is, if and only if  $K \otimes_F F_v$  is a field.

**Lemma 5.2.** *Let  $F = \mathbb{Q}$ . Then  $-1$  does not belong to  $N_{2,17}$ .*

*Proof.* Let  $K := \mathbb{Q}(\sqrt{2}, \sqrt{17})$ . It is not difficult to prove that the local degree of  $K/\mathbb{Q}$  at any place  $v$  of  $\mathbb{Q}$  is either 1 or 2. For all  $c \in \mathbb{Q}^\times$ , define

$$\omega(c) := \prod_{v \in S_1} (17, c)_v,$$

where  $S_1$  is the set of places  $v$  of  $\mathbb{Q}$  that split in  $\mathbb{Q}(\sqrt{2})$ , and  $(17, c)_v$  denotes the symbol  $(17, c)$  in  $\text{Br}(\mathbb{Q}_v)$ . By a result due to Serre and Tate,  $c$  belongs to  $N_2 N_{17} N_{34}$  if and only if  $\omega(c) = 1$ ; see [1, Exercise 5.2] or [10, p. 114, Lemma].

Note that 3 does not belong to  $S_1$  while 17 belongs to  $S_1$ . Moreover, 3 is not square modulo 17, and hence  $\omega(3) = (17, 3)_{17} = -1$ . By the aforementioned result of Serre

and Tate, 3 is not in  $N_2N_{17}N_{34}$ , which by Lemma A.3 (2) implies that 9 does not belong to  $N_{2,17}$ . On the other hand,

$$-9 = N_{2,17}\left(1 - \frac{3}{2}\sqrt{2} - \frac{1}{2}\sqrt{34}\right),$$

and hence  $-1$  does not belong to  $N_{2,17}$ . ■

**Proposition 5.3** (Harpaz–Wittenberg). *Let  $F = \mathbb{Q}$ ,  $b = 2$ ,  $c = 17$  and  $a = d = bc = 34$ . Then  $(a, b) = (b, c) = (c, d) = 0$  but the Massey product  $\langle a, b, c, d \rangle$  is not defined.*

*Proof.* We first show that  $(34, 2) = (2, 17) = (17, 34) = 0$ , or equivalently  $(2, 17) = (2, -1) = (17, -1) = 0$ . These follow from the identities

$$2 \cdot 4^2 + 17 \cdot 1^2 = 7^2, \quad 2 \cdot 1^2 - 1 \cdot 1^2 = 1, \quad 17 \cdot 1^2 - 1 \cdot 4^2 = 1^2.$$

By Theorem 1.4, to prove that  $\langle a, b, c, d \rangle$  is not defined, it suffices to show that  $-1$  does not belong to  $N_{2,17}$ , which was proved in Lemma 5.2. ■

### 6. Proof of Theorem 1.6

Recall that a field  $E$  is said to be *2-special* if the degree of every finite field extension of  $E$  is a power of 2.

**Lemma 6.1.** *Suppose that  $F$  is a 2-special field, and let  $a \in F^\times \setminus F^{\times 2}$ . Let  $X$  be a non-split smooth projective conic over  $F$ , let  $\varphi: X_{F_a} \rightarrow X$  be the projection map, and consider the proper pushforward homomorphism*

$$\varphi_*: \text{Div}(X_{F_a}) \rightarrow \text{Div}(X).$$

*Let  $\sum m_x x \in \text{Div}(X)$  be a principal divisor in the image of  $\varphi_*$ . Then the sum of the  $m_x$  over all closed points  $x \in X$  such that  $F(x) \simeq F_a$  is even.*

*Proof.* Let  $x \in X$  be a closed point. Note that  $\text{deg}(x) := [F(x) : F]$  is a power of 2, and it is different from 1 since  $X(F) = \emptyset$ . Moreover,  $\varphi^{-1}(x) = \text{Spec}(F_a \otimes_F F(x))$  and  $[F_a \otimes_F F(x) : F(x)] = 2$ , hence either  $F_a \otimes_F F(x) \simeq F_a \times F_a$  or it is a quadratic field extension of  $F(x)$ . In other words, either  $\varphi^{-1}(x)$  is the union of two closed points of degree 1 over  $x$ , or it consists of a single closed point of degree 2 over  $x$ . Therefore, there are three mutually exclusive possibilities for the closed point  $x$ :

- (i)  $\text{deg}(x)$  is divisible by 4,
- (ii)  $\text{deg}(x) = 2$  and  $\varphi^{-1}(x)$  consists of a single closed point of degree 2 over  $x$ ,
- (iii)  $\text{deg}(x) = 2$  and  $\varphi^{-1}(x)$  consists of two closed points of degree 1 over  $x$ .

Moreover,  $x$  satisfies (iii) if and only if  $\text{deg}(x) = 2$  and  $a \in F(x)^{\times 2}$ , that is, if and only if  $F(x) \simeq F_a$ . Thus, the proof will be complete once we show that the sum of the  $m_x$  over all closed points  $x \in X$  satisfying (iii) is divisible by 4.

If  $x$  satisfies (i), the number  $m_x \deg(x)$  is divisible by 4. If  $x$  satisfies (ii), then  $m_x$  is divisible by 2, hence  $m_x \deg(x)$  is divisible by 4. Since the divisor  $\sum m_x x$  is principal, its degree is equal to zero, that is,  $\sum m_x \deg(x) = 0$ . It follows that the sum of the  $m_x x$  for those  $x$  as in case (iii) is divisible by 4, as desired. ■

**Lemma 6.2.** *Let  $E$  be a 2-special field, and let  $a, b \in E^\times$  be such that*

- (1)  $a, b$  and  $c := 1 - b$  are independent in  $E^\times / E^{\times 2}$ , and
- (2)  $(a, c) = 0$  and  $(a, b) \neq 0$  in  $\text{Br}(E)$ .

*Let  $X$  be the smooth projective conic over  $E$  corresponding to  $(a, b)$ , and set  $F := E(X)$ . Then  $(a, b) = (a, c) = (b, c) = 0$  in  $\text{Br}(F)$  but the Massey product  $\langle a, b, c, a \rangle$  is not defined over  $F$ .*

*Proof.* We have  $(a, b) = (b, c) = (c, a) = 0$  in  $\text{Br}(F)$  because  $b + c = 1$  and every quaternion algebra splits over the function field of the corresponding conic.

Consider the projective plane  $\mathbb{P}_E^2$  with homogeneous coordinates  $v_0, v_1, v_2$ , and choose a model of  $X \subset \mathbb{P}_E^2$  given by the equation

$$v_1^2 - bv_2^2 = av_0^2.$$

Define

$$f := \frac{v_1 + v_2}{v_2} \in F^\times.$$

Simple computations show that the equation  $v_1 + v_2 = 0$  cuts out a point  $x_1 \in X$  of degree 2 with residue field  $E(x_1) = E_{ac}$ , and that the equation  $v_2 = 0$  cuts out a point  $x_2 \in X$  of degree 2 with  $E(x_2) = E_a$ . Thus

$$\text{div}(f) = x_1 - x_2.$$

Since  $(a, b) \neq 0$  in  $\text{Br}(E)$ , the field  $E$  must be infinite. Thus, as  $(a, c) = 0$  in  $\text{Br}(E)$ , we may find  $u_1, u_2 \in E^\times$  such that  $u_1 + u_2 \neq 0$  and  $u_1^2 - cu_2^2 = a$ . Suppose by contradiction that the Massey product  $\langle a, b, c, a \rangle$  is defined. Then by Proposition 4.1 (a), we have

$$2(u_1 + u_2)u_2 f = 2(v_1 + v_2)(u_1 + u_2)v_2 u_2 v_2^{-2} \in N_a N_{ab} N_{ac}.$$

Since  $2(u_1 + u_2)u_2 \in E^\times$ , we may write

$$f = f_0 n_a n_{ab} n_{ac}$$

for some  $f_0 \in E^\times, n_a \in N_a, n_{ab} \in N_{ab}$  and  $n_{ac} \in N_{ac}$ . Passing to divisors and using that  $\text{div}(f_0) = 0$ , we conclude that

$$\text{div}(f) = \text{div}(n_a) + \text{div}(n_{ab}) + \text{div}(n_{ac}). \tag{6.1}$$

We write  $\text{div}(n_a) = \sum m_x x, \text{div}(n_{ab}) = \sum m'_x x$  and  $\text{div}(n_{ac}) = \sum m''_x x$ . By Lemma 6.1, the sum of the  $m_x$  over all closed points  $x$  such that  $E(x) \simeq E_a$  is even. By assumption  $ab$  and  $ac$  are not squares in  $E$ . It follows that the inverse image of  $X_{ab} \rightarrow X$  and  $X_{ac} \rightarrow X$

at every closed point of  $x$  with residue field  $E(x) \simeq E_a$  consists of a single closed point whose residue field has degree 2 over  $E(x)$ . Therefore, the sum of the  $m'_x$  (resp.  $m''_x$ ) over all closed points  $x$  such that  $E(x) \simeq E_a$  is also even. However, by (6.1) the sum of the  $m_x + m'_x + m''_x$  over all closed points  $x$  such that  $E(x) \simeq E_a$  is equal to 1, which is a contradiction. Therefore, the Massey product  $\langle a, b, c, a \rangle$  is not defined over  $F$ . ■

Recall from the introduction that the DGA  $C^*(F, \mathbb{Z}/2\mathbb{Z})$  is formal if it is quasi-isomorphic to its cohomology algebra  $H^*(F, \mathbb{Z}/2\mathbb{Z})$ , viewed as a DGA with zero differential. If  $C^*(F, \mathbb{Z}/2\mathbb{Z})$  is formal, then by [19, Theorem 3.8] for all  $n \geq 3$  and all  $a_1, \dots, a_n \in F^\times$  such that  $a_1 \cup a_2 = a_2 \cup a_3 = \dots = a_{n-1} \cup a_n = 0$ , the Massey product  $\langle a_1, \dots, a_n \rangle$  vanishes. Therefore, the next theorem, which implies Theorem 1.6, answers Positselski’s Question 1.5 affirmatively.

**Theorem 6.3.** *Let  $F_0$  be a field of characteristic different from 2.*

- (a) *There exist a field extension  $F/F_0$  and elements  $a, b, c \in F^\times$ , independent in  $F^\times/F^{\times 2}$ , such that  $(a, b) = (b, c) = (a, c) = 0$  in  $\text{Br}(F)$  but the Massey product  $\langle a, b, c, a \rangle$  is not defined over  $F$ .*
- (b) *There exist a field extension  $F/F_0$  and elements  $a, b, c, d \in F^\times$ , independent in  $F^\times/F^{\times 2}$ , such that  $(a, b) = (b, c) = (a, d) = 0$  in  $\text{Br}(F)$  but the Massey product  $\langle a, b, c, d \rangle$  is not defined over  $F$ .*

*Proof.* (a) Let  $a$  and  $b$  be algebraically independent variables over  $F_0$ , set  $F_1 := F_0(a, b)$ , and define  $c := 1 - b \in F_1$ . Write  $C$  for the smooth projective conic over  $F_1$  corresponding to  $(a, c) \in \text{Br}(F_1)$ , let  $F_2 := F_1(C)$ , and let  $F_3$  be a 2-closure of  $F_2$ , that is, the subfield of  $(F_2)_{\text{sep}}$  fixed by a Sylow 2-subgroup of  $\Gamma_{F_2}$ . The field  $F_3$  is 2-special. We have the inclusions

$$F_0 \subset F_1 \subset F_2 \subset F_3.$$

In order to complete the proof, it suffices to show that assumptions (1) and (2) of Lemma 6.2 are satisfied by  $a, b, c$  over  $E = F_3$ .

- (1) Consider the group homomorphisms

$$F_1^\times/F_1^{\times 2} \rightarrow F_2^\times/F_2^{\times 2} \rightarrow F_3^\times/F_3^{\times 2}.$$

The homomorphism on the left is injective because  $F_1$  is algebraically closed in  $F_2$ , and the homomorphism on the right is injective by a restriction–corestriction argument. It is clear that  $a, b, c$  are independent in  $F_1^\times/F_1^{\times 2}$ , hence they are independent in  $F_3^\times/F_3^{\times 2}$ .

(2) We have  $(a, c) = 0$  in  $\text{Br}(F_2)$  because  $C$  is the conic corresponding to  $(a, c)$ , hence  $(a, c) = 0$  in  $\text{Br}(F_3)$ . Suppose that  $(a, b) = 0$  in  $\text{Br}(F_3)$ . Then there exists a finite extension  $L/F_2$  of odd degree such that  $(a, b) = 0$  in  $\text{Br}(L)$ . Since  $[L : F_2]$  is odd, a restriction–corestriction argument shows that the restriction map  $\text{Br}(F_2) \rightarrow \text{Br}(L)$  is injective, hence  $(a, b) = 0$  in  $\text{Br}(F_2)$ . By [2, Proposition 7.2.4 (b)], the kernel of the restriction map  $\text{Br}(F_1) \rightarrow \text{Br}(F_2)$  is generated by  $(a, c)$ , hence either  $(a, b) = 0$  or  $(a, b) = (a, c)$  (that is,  $(a, b(1 - b)) = 0$ ) in  $\text{Br}(F_1)$ . Taking residues with respect to

the valuation determined by  $a$ , we see that neither of these equalities can be true, a contradiction. Therefore,  $(a, b) \neq 0$  in  $\text{Br}(F_3)$ , as desired.

(b) By (a), there exist a field extension  $L/F_0$  and  $a, b, c \in L^\times$ , independent in  $L^\times/L^{\times 2}$ , such that  $(a, b) = (b, c) = (c, a) = 0$  in  $\text{Br}(L)$  and the Massey product  $\langle a, b, c, a \rangle$  is not defined. Let  $F := L(u)$ , where  $u$  is a variable over  $L$ , let  $R := L[u]_{(u-1)} \subset F$ , and define  $d := ua \in L^\times$ . Then  $a, b, c, d$  belong to  $R^\times$ , they are independent in  $L^\times/L^{\times 2}$ , and by Lemma 2.9 the Massey product  $\langle a, b, c, d \rangle$  is not defined over  $F$ . ■

**Appendix A. Lemmas on biquadratic extensions**

We collect some known results on Galois  $(\mathbb{Z}/2\mathbb{Z})^2$ -algebras that are needed for the proofs of Theorems 1.3 and 1.4. They are all consequences of Hilbert’s Theorem 90.

Let  $F$  be a field of characteristic different from 2, let  $a, b \in F^\times$ , and let

$$F_{a,b} := F[x_a, x_b]/(x_a^2 - a, x_b^2 - b)$$

be the corresponding étale  $F$ -algebra. We write  $(\mathbb{Z}/2\mathbb{Z})^2 = \langle \sigma_a, \sigma_b \rangle$  and view  $F_{a,b}$  as a Galois  $(\mathbb{Z}/2\mathbb{Z})^2$ -algebra via

$$\sigma_a(x_a) = -x_a, \quad \sigma_a(x_b) = x_b, \quad \sigma_b(x_a) = x_a, \quad \sigma_b(x_b) = -x_b.$$

**Lemma A.1.** *Let  $u, v \in F^\times$ . Then  $(a, u) = (b, v)$  in  $\text{Br}(F)$  if and only if there exist  $n_a \in N_a, n_b \in N_b$  and  $n_{ab} \in N_{ab}$  such that  $u = n_a n_{ab}$  and  $v = n_b n_{ab}$ .*

*Proof.* It follows from Lemma 2.1 that  $(a, n_a n_{ab}) = (b, n_b n_{ab})$  for all  $n_a \in N_a, n_b \in N_b$  and  $n_{ab} \in N_{ab}$ . Conversely, if  $(a, u) = (b, v)$ , then, by the common slot theorem [12, Chapter III, Theorem 4.13], there exists  $w \in F^\times$  satisfying

$$(a, u) = (a, w) = (b, w) = (b, v).$$

It follows from Lemma 2.1 that  $w \in N_{ab}, u/w \in N_a$  and  $v/w \in N_b$ , as desired. ■

**Lemma A.2.** *For all  $\omega \in F_{a,b}^\times$ , we have  $(\sigma_a - 1)(\sigma_b - 1)\omega = 1$  if and only if  $\omega = \omega_a \omega_b$  for some  $\omega_a \in F_a^\times$  and  $\omega_b \in F_b^\times$ .*

*Proof.* See [3, Theorem 4]. Let  $T \subset R_{a,b}(\mathbb{G}_m)$  be the torus image of the multiplication map

$$\mu: R_a(\mathbb{G}_m) \times R_b(\mathbb{G}_m) \rightarrow R_{a,b}(\mathbb{G}_m).$$

A character lattice computation shows that the torus  $T$  is defined by the equation  $(\sigma_a - 1)(\sigma_b - 1)\omega = 1$  inside  $R_{a,b}(\mathbb{G}_m)$ . Therefore, for all  $\omega \in F_{a,b}^\times$ , we have  $\omega \in T(F)$  if and only if  $(\sigma_a - 1)(\sigma_b - 1)\omega = 1$ . We have a short exact sequence

$$1 \rightarrow \mathbb{G}_m \rightarrow R_a(\mathbb{G}_m) \times R_b(\mathbb{G}_m) \xrightarrow{\mu} T \rightarrow 1.$$

Passing to  $F$ -points, we see that an element  $\omega \in F_{a,b}^\times$  belongs to  $T(F)$  if and only if  $\omega = \omega_a \omega_b$  for some  $\omega_a \in F_a^\times$  and  $\omega_b \in F_b^\times$ . ■

**Lemma A.3.** (1) Let  $\rho \in F_{a,b}^\times$ . Then  $N_{a,b}(\rho) \in F^{\times 2}$  if and only if  $\rho \in F_a^\times F_b^\times F_{ab}^\times$ .

(2) Let  $u \in F^\times$ . Then  $u \in N_a N_b N_{ab}$  if and only if  $u^2 \in N_{a,b}$ .

*Proof.* (1) Suppose first that  $\rho = \rho_a \rho_b \rho_{ab}$ , where  $\rho_a \in F_a^\times$ ,  $\rho_b \in F_b^\times$  and  $\rho_{ab} \in F_{ab}^\times$ . Then

$$N_{a,b}(\rho) = N_{a,b}(\rho_a \rho_b \rho_{ab}) = N_a(\rho_a)^2 N_b(\rho_b)^2 N_{ab}(\rho_{ab})^2 \in F^{\times 2}.$$

Conversely, suppose that  $N_{a,b}(\rho) = x^2$  for some  $x \in F^\times$ . Let

$$\omega := \frac{N_{F_{a,b}/F_{ab}}(\rho)}{x} \in F_{ab}^\times.$$

Then  $N_{ab}(\omega) = N_{a,b}(\rho)/x^2 = 1$ , hence by Hilbert's Theorem 90 there is  $\rho_{ab} \in F_{ab}^\times$  such that  $(1 - \sigma_a)\rho_{ab} = \omega$ . Since  $\sigma_a \sigma_b$  fixes  $F_{ab}$ , we have

$$(\sigma_a - 1)(\sigma_b - 1)\rho_{ab} = (2 - 2\sigma_a)\rho_{ab} = \omega^2,$$

where the first equality follows from the fact that  $\sigma_a = \sigma_b$  on  $F_{ab}$ . On the other hand,

$$(\sigma_a - 1)(\sigma_b - 1)\rho = \frac{N_{F_{a,b}/F_{ab}}(\rho)^2}{N_{a,b}(\rho)} = \omega^2,$$

and hence

$$(\sigma_a - 1)(\sigma_b - 1)\frac{\rho}{\rho_{ab}} = 1.$$

By Lemma A.2, we deduce that  $\rho = \rho_{ab} \rho_a \rho_b$  for some  $\rho_a \in F_a^\times$  and  $\rho_b \in F_b^\times$ .

(2) See [1, Exercise 5.1]. Suppose that  $u = N_a(\rho_a)N_b(\rho_b)N_{ab}(\rho_{ab})$ , where  $\rho_a \in F_a^\times$ ,  $\rho_b \in F_b^\times$  and  $\rho_{ab} \in F_{ab}^\times$ . Then

$$N_{a,b}(\rho_a \rho_b \rho_{ab}) = N_a(\rho_a)^2 N_b(\rho_b)^2 N_{ab}(\rho_{ab})^2 = u^2.$$

Conversely, suppose that  $u^2 = N_{a,b}(\rho)$  for some  $\rho \in F_{a,b}^\times$ . By (1), there exist  $\rho_a \in F_a^\times$ ,  $\rho_b \in F_b^\times$  and  $\rho_{ab} \in F_{ab}^\times$  such that  $\rho = \rho_a \rho_b \rho_{ab}$ . It follows that

$$u^2 = N_{a,b}(\rho) = N_a(\rho_a)^2 N_b(\rho_b)^2 N_{ab}(\rho_{ab})^2,$$

hence either  $u = N_a(\rho_a)N_b(\rho_b)N_{ab}(\rho_{ab})$  or  $u = -N_a(\rho_a)N_b(\rho_b)N_{ab}(\rho_{ab})$ . Since  $-a \in N_a$ ,  $-b \in N_b$  and  $-ab \in N_{ab}$ , we have  $-1 \in N_a N_b N_{ab}$ , hence  $u \in N_a N_b N_{ab}$  in either case. ■

**Lemma A.4.** Let  $\rho \in F_a^\times$  and  $\mu \in F_b^\times$  be such that  $N_a(\rho) = N_b(\mu)$ . Set

$$d := \text{Tr}_a(\rho) + \text{Tr}_b(\mu).$$

Suppose that  $d \neq 0$ . Then

- (1)  $\mu d = N_a(\rho + \mu)$ ,
- (2)  $N_b(\mu)d^2 \in N_{a,b}$ , and
- (3)  $(\mu, a) = (d, a)$  in  $\text{Br}(F_b)$ .

*Proof.* We have

$$\begin{aligned} N_a(\rho + \mu) &= (\rho + \mu)(\sigma_a(\rho) + \mu) = \rho\sigma_a(\rho) + \rho\mu + \mu\sigma_a(\rho) + \mu^2 \\ &= \mu\sigma_b(\mu) + \rho\mu + \mu\sigma_a(\rho) + \mu^2 = \mu(\mathrm{Tr}_a(\rho) + \mathrm{Tr}_b(\mu)) = \mu d. \end{aligned}$$

This proves (1). Taking norms in (1) yields

$$N_{a,b}(\rho + \mu) = N_b(\mu d) = N_b(\mu)d^2,$$

which implies (2). Now Lemma 2.1 implies that  $(\mu d, a) = 0$  in  $\mathrm{Br}(F_b)$ , which is equivalent to (3). ■

**Lemma A.5.** *We have  $N_a \cap N_b = N_{a,b}F^{\times 2}$ .*

*Proof.* If  $F$  is finite, then  $N_a = N_b = N_{a,b} = F^\times$ , which implies the conclusion. We may thus assume that  $F$  is infinite.

Let  $u \in N_{a,b}F^{\times 2}$ , and let  $\varepsilon \in F_{a,b}^\times$  and  $v \in F^\times$  be such that  $u = N_{a,b}(\varepsilon)v^2$ . Then  $u = N_a(N_b(\varepsilon)v) \in N_a$ , and  $u = N_b(N_a(\varepsilon)v) \in N_b$ , hence  $u \in N_a \cap N_b$ .

Conversely, let  $u \in N_a \cap N_b$ . Let  $\mu \in F_b^\times$  such that  $N_b(\mu) = u$ . The solutions  $\rho \in F_a^\times$  to  $N_a(\rho) = u$  form the set of  $F$ -points of a smooth affine  $F$ -conic. Thus, since  $F$  is infinite, there exists  $\rho \in F_a^\times$  such that  $N_a(\rho) = u$  and  $\mathrm{Tr}_a(\rho) \neq 0$ . Therefore, replacing  $\rho$  by  $-\rho$  if necessary, we may suppose that  $d := \mathrm{Tr}_a(\rho) + \mathrm{Tr}_b(\mu)$  is non-zero. By Lemma A.4(2), we have  $ud^2 \in N_{a,b}$ , as desired. ■

*Acknowledgments.* We are grateful to Olivier Wittenberg for many helpful comments on an earlier version of this paper. We thank the anonymous referees for carefully reading our paper and for providing a number of useful comments and suggestions.

*Funding.* The first author was supported by the NSF grant DMS #1801530.

## References

- [1] Cassels, J. W. S., Fröhlich, A. (eds.): Algebraic number theory. Academic Press, London (1967) Zbl [0153.07403](#) MR [215665](#)
- [2] Colliot-Thélène, J.-L., Skorobogatov, A. N.: [The Brauer–Grothendieck group](#). *Ergeb. Math. Grenzgeb.* (3) 71, Springer, Cham (2021) Zbl [1490.14001](#) MR [4304038](#)
- [3] Dwilewicz, R., Mináč, J., Schultz, A., Swallow, J.: [Hilbert 90 for biquadratic extensions](#). *Amer. Math. Monthly* **114**, 577–587 (2007) Zbl [1137.12004](#) MR [2341321](#)
- [4] Dwyer, W. G.: [Homology, Massey products and maps between groups](#). *J. Pure Appl. Algebra* **6**, 177–190 (1975) Zbl [0338.20057](#) MR [385851](#)
- [5] Efrat, I., Matzri, E.: [Triple Massey products and absolute Galois groups](#). *J. Eur. Math. Soc. (JEMS)* **19**, 3629–3640 (2017) Zbl [1425.12004](#) MR [3730509](#)
- [6] Gille, P., Szamuely, T.: [Central simple algebras and Galois cohomology](#). *Cambridge Stud. Adv. Math.* 165, Cambridge University Press, Cambridge (2017) Zbl [1373.19001](#) MR [3727161](#)
- [7] Guillot, P., Mináč, J., Topaz, A.: [Four-fold Massey products in Galois cohomology \(with an appendix by Olivier Wittenberg\)](#). *Compos. Math.* **154**, 1921–1959 (2018) Zbl [1455.12005](#) MR [3867288](#)

- [8] Harpaz, Y., Wittenberg, O.: [The Massey vanishing conjecture for number fields](#). *Duke Math. J.* **172**, 1–41 (2023) Zbl [1521.11070](#) MR [4533716](#)
- [9] Hopkins, M. J., Wickelgren, K. G.: [Splitting varieties for triple Massey products](#). *J. Pure Appl. Algebra* **219**, 1304–1319 (2015) Zbl [1323.55014](#) MR [3299685](#)
- [10] Hürlimann, W.: [H<sup>3</sup> and rational points on biquadratic bicyclic norm forms](#). *Arch. Math. (Basel)* **47**, 113–116 (1986) Zbl [0583.12017](#) MR [859259](#)
- [11] Knus, M.-A., Merkurjev, A., Rost, M., Tignol, J.-P.: [The book of involutions](#). Amer. Math. Soc. Colloq. Publ. 44, American Mathematical Society, Providence, RI (1998) Zbl [0955.16001](#) MR [1632779](#)
- [12] Lam, T. Y.: [Introduction to quadratic forms over fields](#). Grad. Stud. Math. 67, American Mathematical Society, Providence, RI (2005) Zbl [1068.11023](#) MR [2104929](#)
- [13] Matzri, E.: [Triple Massey products in Galois cohomology](#). arXiv:[1411.4146](#) (2014)
- [14] Milne, J. S.: [Étale cohomology](#). Princeton Math. Ser. 33, Princeton University Press, Princeton, NJ (1980) Zbl [0433.14012](#) MR [559531](#)
- [15] Mináč, J., Tân, N. D.: [Triple Massey products over global fields](#). *Doc. Math.* **20**, 1467–1480 (2015) Zbl [1372.12003](#) MR [3452187](#)
- [16] Mináč, J., Tân, N. D.: [Triple Massey products vanish over all fields](#). *J. Lond. Math. Soc. (2)* **94**, 909–932 (2016) Zbl [1378.12002](#) MR [3614934](#)
- [17] Mináč, J., Tân, N. D.: [Counting Galois  \$\mathbb{U}\_4\(\mathbb{F}\_p\)\$ -extensions using Massey products](#). *J. Number Theory* **176**, 76–112 (2017) Zbl [1422.11232](#) MR [3622122](#)
- [18] Mináč, J., Tân, N. D.: [Triple Massey products and Galois theory](#). *J. Eur. Math. Soc. (JEMS)* **19**, 255–284 (2017) Zbl [1372.12004](#) MR [3584563](#)
- [19] Pál, A., Quick, G.: [Real projective groups are formal](#). arXiv:[2206.14645](#) (2022)
- [20] Pál, A., Schläpke, T. M.: [Brauer–Manin obstruction to the local-global principle for the embedding problem](#). *Int. J. Number Theory* **18**, 1535–1565 (2022) Zbl [1500.12005](#) MR [4439045](#)
- [21] Pál, A., Szabó, E.: [The strong Massey vanishing conjecture for fields with virtual cohomological dimension at most 1](#). arXiv:[1811.06192](#) (2022)
- [22] Positselski, L.: [Koszulity of cohomology =  \$K\(\pi, 1\)\$ -ness + quasi-formality](#). *J. Algebra* **483**, 188–229 (2017) Zbl [1454.16034](#) MR [3649818](#)
- [23] Quadrelli, C.: [Massey products in Galois cohomology and the elementary type conjecture](#). *J. Number Theory* **258**, 40–65 (2024) Zbl [1537.12006](#) MR [4685899](#)
- [24] Serre, J.-P.: [Local fields](#). Grad. Texts in Math. 67, Springer, New York (1979) Zbl [0423.12016](#) MR [554237](#)
- [25] Serre, J.-P.: [Galois cohomology](#). Springer Monogr. Math., Springer, Berlin (2002) Zbl [1004.12003](#) MR [1867431](#)